Вінницький національний технічний університет
(повне найменування вищого навчального закладу)

Факультет інформаційних технологій та комп'ютерної інженерії
(повне найменування інституту, назва факультету (відділення))

Кафедра обчислювальної техніки
(повна назва кафедри (предметної, циклової комісії))

БАКАЛАВРСЬКА ДИПЛОМНА РОБОТА

на тему:

Комп'ютерна мережа Вінницького технічного фахового коледжу

ПОЯСНЮВАЛЬНА ЗАПИСКА

Виконав: студент 2 курсу, групи 1КІ-22мс

спеціальності 123 — Комп'ютерна інженерія
(шифр і назва напряму підготовки, спеціальності)

_____ Хільчук Б. С.
(прізвище та ініціали)

Керівник: к.т.н., проф. каф. ОТ

_____ Захарченко С. М.
(прізвище та ініціали)

«04» червня 2024 р.

Рецензент: к.т.н., доцент, завідувач каф. МБІС

_____ Карпінець В. В.
(прізвище та ініціали)

«05» червня 2024 р.

Допущено до захисту

Завідувач кафедри ОТ

д.т.н., проф. Азаров О. Д.

«12» червня 2024 р.

Вінниця ВНТУ — 2024 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»

Освітньо-професійна програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Завідувач кафедри ОТ

д.т.н., проф. Азаров О. Д.

06. 2024 р.

З А В Д А Н Н Я

НА БАКАЛАВРСЬКУ ДИПЛОМНУ РОБОТУ СТУДЕНТУ

Хільчуку Богдану Сергійовичу

1 Тема роботи: «Комп'ютерна мережа Вінницького технічного фахового коледжу», керівник роботи к.т.н., проф. каф. ОТ Захарченко С.М., затверджена наказом вищого навчального закладу від 11 березня 2024 р. №80

2 Термін подання студентом роботи 10 червня 2024 р.

3 Вихідні дані до роботи: призначення — проєктування комп'ютерних мереж; основні підтримувані функції — передача пакетів між робочими станціями; пропускна спроможність мережі не менше 100Мб/сек.; кількість кінцевих пристроїв: 372; підключення до мережі Інтернет.

4 Зміст розрахунково-пояснювальної записки: вступ, аналіз технологій для створення комп'ютерних мереж, обґрунтування вибору технологій, реалізація та тестування комп'ютерної мережі.

5 Перелік необхідного матеріалу (з точним зазначенням обов'язкових креслень): технічне завдання, структурна схема мережі коледжу, логічна

структура комп'ютерної мережі, розподіл IP-адрес 1 та 2 підмережі, порівняльна характеристика властивостей маршрутизаторів Cisco ASR 1001 та MikroTik RB4011IGS + RM.

6 Дата видачі завдання 12 березня 2024 р.

7 Календарний план виконання БДР приведений в таблиці 1

Таблиця 1 — Календарний план виконання БДР

№ етапу	Назва етапу	Термін виконання		Очікувані результати
		Початок	Кінець	
1	Постановка задачі	12.03.24	16.03.24	Розділ 1
2	Аналіз технологій для створення комп'ютерних мереж	17.03.24	28.03.24	Розділ 1
3	Аналіз та обґрунтування вибору технологій	29.03.24	09.04.24	Розділ 2
4	Реалізація комп'ютерної мережі	10.04.24	19.04.24	Розділ 3
5	Тестування комп'ютерної мережі	20.04.24	26.04.24	Розділ 4
6	Підготовка тезових матеріалів для публікації	27.04.24	28.04.24	Тези
7	Оформлення пояснювальної записки та демонстраційної презентації для доповіді	29.04.24	17.05.24	ПЗ, презентація
8	Підготовка супровідної документації, перевірка відповідності нормам та проходження тесту на плагіат	18.05.24	26.05.24	ПЗ, презентація

Студент _____ Хільчук Б. С.

Керівник _____ Захарченко С. М

ВСТУП

Комп'ютерні мережі стали необхідною складовою сучасного навчального процесу, включаючи Вінницький технічний фаховий коледж. Вони забезпечують зручний обмін даними, спільний доступ до ресурсів та полегшують виконання різноманітних завдань. Основні характеристики комп'ютерних мереж, що мають велике значення для навчального закладу, включають швидку передачу інформації між користувачами, зручну передачу та можливість обміну даними.

Актуальність розробки полягає у тому, що оптимізована комп'ютерна мережа стає невіддільною частиною інфраструктури освітнього закладу, забезпечуючи зручний обмін даними та швидку передачу інформації між користувачами. Розробка логічної структури та конфігурації мережі допомагає оптимізувати роботу коледжу, забезпечуючи зручність для студентів і викладачів та підвищуючи загальний рівень організації навчального процесу.

Дослідження у сфері оптимізації комп'ютерних мереж у навчальних закладах визначають ключові етапи для вдосконалення мережі. Аналіз технологій для створення та вдосконалення комп'ютерних мереж полягає у вивченні різних методів та технологій, які використовуються для побудови та управління мережами. Цей процес охоплює огляд наявних технологічних рішень, аналіз їх переваг і недоліків, а також визначення найбільш відповідних варіантів для конкретного середовища та потреб користувачів.

Мета дипломної роботи полягає у вдосконаленні шляхом оптимізації логічної структури та конфігурації комп'ютерної мережі Вінницького технічного фахового коледжу.

Для досягнення поставленої мети необхідно розв'язати такі **завдання**:

— провести аналіз сучасних технологій побудови корпоративних комп'ютерних мереж;

— розробити логічну структуру комп’ютерної мережі Вінницького технічного фахового коледжу;

— обґрунтувати вибір обладнання для реалізації мережі та провести конфігурування активних пристроїв;

— провести моделювання та тестування мережі за допомогою симулятора Cisco Packet Tracer.

Об'єктом дослідження є процес функціонування комп’ютерної мережі.

Предметом дослідження є логічна структура та конфігурація комп'ютерної мережі Вінницького технічного фахового коледжу.

Методи дослідження, що застосовуються у бакалаврській дипломній роботі, включають аналіз літературних джерел та аналіз технологій у галузі комп'ютерних мереж; методи моделювання комп’ютерних мереж; методи тестування працездатності комп’ютерних мереж.

Новизна одержаних результатів полягає в удосконаленні комп’ютерної мережі Вінницького технічного фахового коледжу за рахунок оптимізації структури мережі та застосуванню динамічної маршрутизації.

Апробація результатів роботи здійснена під час доповіді на конференції Молодь в науці: дослідження, проблеми, перспективи (МН-2024) факультету інформаційних технологій та комп'ютерної інженерії.

Матеріали роботи доповідались та публікувались [1]:

Комп’ютерна мережа Вінницького технічного фахового коледжу / Б. С. Хільчук, С. М. Захарченко // Матеріали конференції Молодь в науці: дослідження, проблеми, перспективи (МН-2024) факультету інформаційних технологій та комп'ютерної інженерії. Вінниця 2024 р. [Електронний ресурс]. Режим доступу: https://conferences.vntu.edu.ua/index.php/mn/mn2024/paper/view/21064/0

1 АНАЛІЗ ТЕХНОЛОГІЙ ДЛЯ СТВОРЕННЯ КОМП'ЮТЕРНИХ МЕРЕЖ

1.1 Основні моделі мережі OSI та TCP/IP

Модель OSI (Open Systems Interconnection) — це стандарт, розроблений Міжнародною організацією зі стандартизації (ISO), що визначає сім рівнів абстракції для опису функцій мережевих пристроїв. Починаючи з фізичного рівня, де визначаються методи передачі даних по кабелю чи бездротовій мережі, і закінчуючи рівнем застосунків, де реалізується взаємодія програмних додатків [2]. Кожен рівень виконує конкретні функції, і комунікація між рівнями відбувається за допомогою протоколів. Ця модель забезпечує стандартизований підхід до проєктування мереж та взаємодії пристроїв. Основні функції рівнів моделі OSI показані у таблиці 1.1

Таблиця 1.1 — Основні функції рівнів моделі OSI

Тип	Рівень	Функції
Дані	7. Прикладний	Доступ до мережевих служб
	6. Представницький	Представлення і шифрування даних
	5. Сеансовий	Управління сеансом зв'язку
Сегменти	4. Транспортний	Прямий зв'язок між кінцевими пунктами та надійність
Пакети	3. Мережевий	Визначення маршруту та логічна адресація
Кадри	2. Канальний	Фізична адресація
Біти	1. Фізичний	Робота з середовищем передачі, сигналами та двійковими даними

Фізичний рівень моделі OSI визначає механізми передачі даних через мережеве середовище, включаючи кабелі, бездротові зв'язки та оптичні канали. Він забезпечує надійність передачі та визначає характеристики фізичного середовища, такі як швидкість передачі даних та характеристики сигналу [3].

Рівень каналу зв'язку відповідає за поділ вхідних даних на фрейми, додавання заголовків і контрольних сум, а також за контроль передачі даних та виправлення помилок. Він також визначає методи доступу до мережі та розв’язує проблеми колізій та керування потоком даних.

Мережевий рівень визначає оптимальний шлях передачі даних між різними мережами, використовуючи IP-адресацію. Він відповідає за маршрутизацію пакетів даних, фрагментацію та збирання їх для передачі через мережу, а також за адресацію та ідентифікацію пристроїв у мережі.

На четвертому рівні моделі OSI — транспортний рівень. Він відповідає за надійну передачу даних між кінцевими пристроями, використовуючи протоколи TCP та UDP. Також цей рівень відповідає за мультиплексування та демультиплексування даних, контроль потоку даних та адаптацію швидкості передачі [3].

На п'ятому рівні — сеансовий рівень, що керує сеансами зв'язку між пристроями та координує обмін даними. Він відповідає за створення, управління та завершення сеансів зв'язку, а також синхронізацію даних та забезпечення безпеки обміну даними.

На шостому рівні — рівень представлення, який стандартизує представлення даних для обміну між пристроями. Він відповідає за перетворення даних у стандартний формат, компресію, шифрування та забезпечення незалежності від мови та платформи.

Рівень застосунків визначає програми та протоколи для зручної взаємодії користувачів з мережевими ресурсами, такими як електронна пошта, веббраузери та інші. Його функцією є надання доступу до мережевих служб та обробка запитів користувачів. Рівень застосунків включає такі протоколи, як HTTP для вебсторінок, SMTP для електронної пошти та FTP для передачі файлів. Він також відповідає за обробку та адаптацію даних для користувача та забезпечення їхньої безпеки та конфіденційності під час передачі через мережу [3].

Модель TCP/IP (Transmission Control Protocol/Internet Protocol) — це основна модель для Інтернету та більшості комп'ютерних мереж. Вона

складається з чотирьох рівнів: мережевого інтерфейсу, інтернет-рівня, транспортного рівня та рівня застосунків. Модель TCP/IP орієнтована на практичність та простоту, і вона активно використовується у реальних мережевих середовищах. Протокол IP (Internet Protocol) визначає правила адресації та маршрутизації даних, натомість протокол TCP (Transmission Control Protocol) відповідає за надійну передачу даних між пристроями [3].

Мережевий інтерфейс, також відомий як фізичний рівень, є найнижчим рівнем моделі TCP/IP. Цей рівень визначає методи передачі бітів через фізичні медіамережі, такі як мідні кабелі, оптичні волокна або бездротові зв'язки. Він включає стандарти і протоколи, необхідні для передачі бітів з одного пристрою до іншого, включаючи кодування сигналів, форматування фреймів та керування доступом до каналу передачі.

Інтернет-рівень, або мережевий рівень, займається маршрутизацією даних через мережу. Він визначає протоколи, які використовуються для передачі даних між різними мережами та вузлами. Цей рівень також охоплює роботу маршрутизаторів та комутаторів для ефективного пересилання даних з одного вузла до іншого.

Транспортний рівень відповідає за передачу даних між процесами, які працюють на різних вузлах мережі. Основними протоколами на цьому рівні є TCP (Transmission Control Protocol) та UDP (User Datagram Protocol). TCP забезпечує послуги надійної передачі даних, у той час, як UDP надає швидку, але менш надійну передачу даних без встановлення з'єднання.

Рівень застосунків — це верхній рівень моделі TCP/IP. Він відповідає за взаємодію програм та користувачів у мережі. На цьому рівні визначаються протоколи, такі як HTTP, FTP, SMTP, які використовуються для відповідно передачі вебсторінок, файлів та електронної пошти. Кожен з цих протоколів забезпечує конкретні послуги та механізми взаємодії між програмами.

Модель TCP/IP і модель OSI є двома основними моделями, які використовуються для опису та розуміння роботи мережевих протоколів. Модель TCP/IP, яка складається з чотирьох рівнів, є більш поширеною та практичною

моделлю у реальних мережевих середовищах через свою простоту та ефективність. Порівняльна характеристика моделей мережі TCP/IP та OSI наведена у таблиці 1.2

Таблиця 1.2 — Порівняльна характеристика моделей мережі TCP/IP та OSI

Характеристика	TCP/IP	OSI
Кількість рівнів	4	7
Ідентифікація рівнів	Транспорт, мережа, інтернет, зв'язок	Фізичний, Канал зв'язку, Мережевий, Транспорт, Сеансовий, Представлення, Застосунків
Використання у реальних системах	Поширена	Непоширена
Типові протоколи на рівні мережі	IPv4, IPv6	IP

Модель OSI складається з семи рівнів та є більш детальною та комплексною, що робить її важчою для реалізації, але водночас надає більший контекст для розуміння мережевої архітектури [5].

Хоча модель OSI зберігає важливість як концептуальний фреймворк для розуміння мережевих протоколів та їх взаємодії, більшість реальних мереж реалізуються з використанням моделі TCP/IP. Це сталося внаслідок того, що модель TCP/IP має більшу простоту у використанні та впровадженні, що робить її більш популярною серед інженерів та адміністраторів мереж. Розуміння обох моделей є важливим для спеціалістів у сфері мережевих технологій, оскільки це допомагає краще розуміти принципи роботи мереж та взаємодію їх компонентів.

1.2 IP-адреси

IP-адреса (Internet Protocol address) є ключовим елементом комп'ютерних мереж і є унікальним ідентифікатором, який призначається кожному пристрою в мережі з метою визначення його місця і можливості взаємодії з іншими

пристроями. Кожен пристрій, що підключений до мережі, включаючи комп'ютери, маршрутизатори, принтери та інші мережеві пристрої, повинен мати свою унікальну IP-адресу [6].

Зв'язок між різними пристроями у комп'ютерній мережі відбувається за допомогою пакетів даних. Кожен пакет даних містить не лише корисну інформацію, а й метадані, серед яких є IP-адреса відправника та отримувача. Коли пристрій відправляє дані, він включає свою власну IP-адресу, а також IP-адресу призначення, в заголовок пакета даних.

IP-адреса виконує ряд важливих функцій у комп'ютерних мережах. Перш за все, вона служить як унікальний ідентифікатор кожного пристрою, підключеного до мережі. Кожен пристрій має свою власну IP-адресу, яка відрізняє його від інших пристроїв у мережі. Це дозволяє встановлювати ідентифікацію та розпізнавання пристроїв у мережі, що є необхідним для забезпечення їх правильного функціонування [6].

IP-адреса використовується для адресації та маршрутизації даних в мережі. При передачі даних від відправника до отримувача, кожен пакет даних містить IP-адресу відправника та призначення. Це дозволяє маршрутизаторам та іншим пристроям в мережі визначати шлях, по якому повинні бути направлені дані. Іншими словами, IP-адреса вказує, куди потрібно доставити дані та звідки вони були відправлені, що є критично важливим для ефективної комунікації між пристроями в мережі.

IP-адреси дозволяють пристроям взаємодіяти між собою, обмінюватися даними та отримувати доступ до різних ресурсів у мережі. Вони служать основними адресами, за допомогою яких встановлюються з'єднання між пристроями, передаються дані та здійснюється комунікація. Без IP-адрес можливість зв'язку та обміну даними в мережі була б суттєво обмежена, що підкреслює важливість цього ідентифікатора в комп'ютерних мережах.

IP-адреси визначаються за допомогою двох основних версій протоколу: IPv4 і IPv6. IPv4, або Інтернет-протокол версії 4, є першою та найбільш поширеною версією IP-протоколу. Він складається з 32-бітових чисел, розділених

крапками, наприклад, 192.0.2.1. Кожна група чисел може приймати значення від 0 до 255. Завдяки цій структурі, IPv4 може підтримувати приблизно 4,3 мільярда унікальних IP-адрес [7].

Зі зростанням кількості підключених до Інтернету пристроїв, IPv4 адреси стають дефіцитними. Це привело до розробки нової версії протоколу - IPv6. IPv6, або Інтернет-протокол версії 6, використовує 128-бітові адреси, що значно збільшує кількість унікальних адрес, доступних у мережі. Відповідно до цього, IPv6 може практично надавати нескінченну кількість унікальних IP-адрес. Враховуючи швидкий розвиток Інтернету та збільшення кількості підключених пристроїв, перехід до IPv6 стає все більш важливим для забезпечення доступності адрес для всіх пристроїв у мережі. Порівняльна характеристика IPv4 та IPv6 відображена у таблиці 1.3

Таблиця 1.3 — Порівняльна характеристика IPv4 та IPv6

Характеристика	IPv4	IPv6
Довжина адреси	32 біти	128 бітів
Кількість адрес	Приблизно 4,3 млрд	Приблизно 3,4×10^38
Підтримка NAT	Усі мережі	Менша потреба
Автоматичне налаштування	DHCP	DHCPv6, SLAAC
Підтримка IPSec	Не вбудована	Вбудована
Підтримка мультимедіа	Залежно від реалізації	За замовчуванням

IP-адреси також можуть бути статичними або динамічними. Статичні IP-адреси — це адреси, що призначаються пристроям в мережі і залишаються постійними або незмінними протягом тривалого періоду часу. Коли пристрій отримує статичну IP-адресу, ця адреса залишається незмінною, навіть якщо пристрій перезавантажується або вимикається. Статичні IP-адреси використовуються там, де потрібно постійно відстежувати та забезпечувати доступ до конкретного пристрою в мережі. Наприклад, сервери, маршрутизатори

або пристрої з мережевими сервісами часто мають статичні IP-адреси, оскільки вони мають залишатися доступними для комунікації у будь-який час.

Динамічні IP-адреси, навпаки, призначаються пристроям у мережі тимчасово або динамічно за допомогою протоколу DHCP (Dynamic Host Configuration Protocol). Коли пристрій підключається до мережі, він надає запит DHCP-серверу для отримання IP-адреси. DHCP-сервер надає пристрою доступну IP-адресу, а також інші мережеві налаштування, такі як маску підмережі та адресу шлюзу. Динамічні IP-адреси зазвичай використовуються для пристроїв, які не потребують постійного доступу чи які не мають постійної потреби в одному і тому ж IP-адресі. Наприклад, динамічні IP-адреси часто використовуються для підключення комп'ютерів у домашніх мережах або для тимчасових пристроїв, які підключаються до гостьових мереж.

IP-адреси поділяються на приватні та публічні залежно від їхнього призначення та доступності з мережі Інтернет.

Публічні IP-адреси призначені для використання в Інтернеті та доступні з будь-якого місця в мережі. Ці адреси ідентифікують конкретний пристрій в Інтернеті і можуть бути використані для забезпечення зовнішнього зв'язку. Публічні IP-адреси розподіляються Інтернет-провайдерами та організаціями, які мають прямий доступ до Інтернету через мережу.

Приватні IP-адреси призначені для внутрішнього використання в приватних мережах, таких як домашні або корпоративні мережі. Ці адреси не доступні зовнішнім мережам, таким як Інтернет, і використовуються для ідентифікації пристроїв у межах однієї мережі. Приватні IP-адреси часто використовуються в домашніх маршрутизаторах або внутрішніх мережах організацій для забезпечення локального зв'язку між пристроями. Приватні IP-адреси визначені стандартами та призначені для використання в мережах, де не потрібний прямий зовнішній доступ до пристроїв. Вони дозволяють ефективно використовувати доступні адреси, зменшуючи кількість публічних IP-адрес, які потрібні для підключення до Інтернету.

У сучасних мережах IP-адреси є невіддільною частиною їхньої інфраструктури, забезпечуючи правильну ідентифікацію та комунікацію між пристроями в мережі [6].

1.3 Технології локальних мереж

1.3.1 Стандарт Ethernet

Основною технологією реалізації локальних мереж є технологія Ethernet. Ethernet є стандартом передачі даних, що визначає фізичні та канальні рівні моделі OSI і забезпечує зв'язок між пристроями в мережі.

Технологія Ethernet, як стандарт передачі даних, з'явилася в 1970-х роках і була розроблена в лабораторії Xerox PARC. Початково вона була використана для забезпечення зв'язку між різними комп'ютерами в одній локальній мережі. Однак з розвитком технології та її стандартизацією Ethernet стала широко використовуватися в різних типах мереж [8].

Стандарти Ethernet визначають параметри передачі даних в мережі, що включають швидкість передачі, тип кабелю та методи модуляції сигналів. Основні характеристики, які визначаються стандартами, включають швидкість передачі даних, яка може бути виражена в мегабітах за секунду (Mbps) або гігабітах за секунду (Gbps), тип кабелю, такий як вита пара (UTP), екранована вита пара (STP), оптоволокно тощо, а також методи модуляції та кодування сигналів.

Однією з ключових особливостей технології Ethernet є її висока масштабованість, що дозволяє використовувати її в різноманітних мережних середовищах. Вона може бути успішно впроваджена як у невеликих домашніх мережах з кількома пристроями, так і у великих корпоративних мережах з тисячами комп'ютерів і мережевих пристроїв. Ця масштабованість базується на різноманітних конфігураційних можливостях Ethernet, що дозволяють побудувати мережу відповідно до потреб користувачів та умов конкретного середовища.

Ethernet, оригінальний стандарт передачі даних в локальних комп'ютерних мережах, став повільним у порівнянні з дедалі більшими потребами сучасних

мереж. Початкова швидкість передачі даних у мережі Ethernet була обмежена до 10 мегабітів на секунду (Mbps), що стало недостатнім для передачі великих обсягів даних, особливо в умовах підвищеного використання мультимедійного контенту, великих файлів та інших вимог до швидкості.

Недоліками Ethernet були його обмежена швидкість передачі даних, що призводило до заторів у мережі при великих обсягах трафіку, а також обмежена сумісність з сучасним обладнанням та вимогами користувачів. Це спонукало до розробки нових стандартів, таких як Fast Ethernet і Gigabit Ethernet.

Fast Ethernet став стандартом мережі, який розвинув і покращив технологію Ethernet, забезпечуючи значне збільшення швидкості передачі даних. Цей стандарт вперше був представлений у 1995 році та став еволюційним кроком у розвитку мережевих технологій. Головною особливістю Fast Ethernet є здатність до передачі даних зі швидкістю до 100 мегабітів за секунду (Mbps), що вдвічі перевищує максимальну швидкість передачі даних в традиційній Ethernet [9].

Fast Ethernet використовує ті ж принципи та методи доступу до каналу, що і класичний Ethernet, але із збільшеною швидкістю передачі даних. Це дозволяє забезпечити більш ефективне використання мережевого каналу та підвищити продуктивність мережі. Щоб досягти цих високих швидкостей, Fast Ethernet використовує різні технології, такі як повторювачі з підтримкою Fast Ethernet, комутатори, а також нові типи кабелів, наприклад, категорія 5e у технології витої пари.

Стандарт Fast Ethernet використовує різні методи модуляції та кодування сигналів, які дозволяють досягти високої швидкості передачі даних. Більшість мережевих пристроїв, які підтримують Fast Ethernet, можуть автоматично визначати швидкість зв'язку та автоматично перемикатися на найвищу доступну швидкість, забезпечуючи сумісність з різними пристроями у мережі [9].

Fast Ethernet став популярним стандартом у бізнес та корпоративних мережах, де великі обсяги даних вимагають швидкої передачі. Його використання також дозволяє покращити продуктивність і ефективність роботи мережі, забезпечуючи швидку та надійну передачу даних.

Gigabit Ethernet — це технологія мережі, яка передає дані зі швидкістю до 1 гігабіт на секунду (або 1000 мегабітів на секунду). Вона є наступником технології Fast Ethernet і є швидшою і більш продуктивною. Gigabit Ethernet використовує різноманітні типи кабелів, такі як вита пара (UTP), оптоволокно і кілька інших, і зазвичай має максимальну довжину кабелю приблизно 100 метрів, подібно до Fast Ethernet.

Ця технологія дозволяє суттєво збільшити швидкість передачі даних в мережах, що робить її ідеальною для великих організацій, дата-центрів, споживачів контенту та будь-яких сценаріїв, де потрібна велика пропускна здатність мережі. Gigabit Ethernet також дозволяє ефективно передавати великі обсяги даних, такі як відео високої чіткості або великі файли, з максимальною швидкістю і мінімальними затримками. Порівняльна характеристика Fast Ethernet та Gigabit Ethernet відображена у таблиці 1.4

Таблиця 1.4 — Порівняльна характеристика Fast Ethernet та Gigabit Ethernet

Характеристика	Fast Ethernet	Gigabit Ethernet
Стандарт	IEEE 802.3u	IEEE 802.3z
Швидкість передачі даних	100 Mbps	1000 Mbps
Максимальна довжина кабелю	100 метрів	100 метрів
Тип кабелю	UTP, оптоволокно	UTP, оптоволокно
Метод доступу до середовища	CSMA/CD	CSMA/CD
Час затримки	5 мкс	0.1 мкс

Fast Ethernet і Gigabit Ethernet — це два різних стандарти передачі даних в локальних комп'ютерних мережах, які використовуються для забезпечення з'єднання між різними пристроями та комп'ютерами. Основна відмінність між ними полягає в швидкості передачі даних. Gigabit Ethernet надає швидкість

передачі даних до 1 гігабіта на секунду (або 1000 мегабітів на секунду), тоді як Fast Ethernet має швидкість передачі даних 100 мегабітів на секунду.

Однією з ключових переваг Gigabit Ethernet є значно підвищена швидкість передачі даних, що робить його ідеальним для великих обсягів даних і додатків з високими вимогами до швидкості. В порівнянні з Fast Ethernet, Gigabit Ethernet забезпечує значно більшу продуктивність та швидкість обміну даними в мережі.

Fast Ethernet, хоча і забезпечує швидшу передачу даних порівняно зі стандартом Ethernet, залишається менш продуктивним в порівнянні з Gigabit Ethernet. Gigabit Ethernet дозволяє підтримувати навіть більші обсяги даних і дозволяє працювати з великими файлами та додатками на вищому рівні продуктивності.

Вибір між Gigabit Ethernet і Fast Ethernet залежить від конкретних потреб та вимог вашої мережі. Якщо вам потрібна висока швидкість передачі даних і ви готові інвестувати у нове обладнання, то Gigabit Ethernet може бути кращим вибором. З іншого боку, якщо ваші потреби в мережевому з'єднанні менш вимогливі і вам потрібне більш економічне рішення, то Fast Ethernet може задовольнити ваші потреби.

1.3.2 Технологія Wi-Fi

Wi-Fi є технологією бездротового з'єднання, яка дозволяє пристроям з'єднуватися з мережею Інтернету та обмінюватися даними без потреби у фізичних кабелях. Ця технологія є особливо популярною завдяки своїй зручності та доступності, оскільки вона дозволяє підключати пристрої до мережі з будь-якого місця, де є наявність Wi-Fi сигналу.

Wi-Fi базується на серії стандартів, що були розроблені Інститутом інженерів електротехніки та електроніки (IEEE). Основними стандартами Wi-Fi є 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac та деякі інші. Кожен з цих стандартів має свої унікальні характеристики, які впливають на швидкість передачі даних, діапазон частот, зону покриття та інші параметри бездротового з'єднання.

Порівняльна характеристика стандартів 802.11a, 802.11b, 802.11g, 802.11n та 802.11ac відображена у таблиці 1.5

Однією з ключових переваг Wi-Fi є безпровідний доступ до Інтернету для різних пристроїв, таких як комп'ютери, смартфони, планшети та інші, що робить її популярною в домашніх умовах, офісах, громадських місцях та навчальних закладах. Ця технологія дозволяє користувачам підключатися до мережі з будь-якого місця, де є доступ до Wi-Fi сигналу, що забезпечує високий рівень зручності та мобільності.

Таблиця 1.5 — Порівняльна характеристика стандартів 802.11a, 802.11b, 802.11g, 802.11n та 802.11ac

Параметр	802.11a	802.11b	802.11g	802.11n	802.11ac
Швидкість передачі даних	До 54 Мбіт/с	До 11 Мбіт/с	До 54 Мбіт/с	До 600 Мбіт/с	До 3,47 Гбіт/с
Діапазон	5 ГГц	2,4 ГГц	2,4 ГГц	2,4 ГГц/ 5 ГГц	5 ГГц
MIMO	Ні	Ні	Ні	Так	Так
Підтримувані модуляції	OFDM	DSSS, CCK	OFDM	OFDM	OFDM, QAM
Зона покриття	2 м	4 м	4 м	5 м	5 м

Серед недоліків технології Wi-Fi:

— порівняно з провідними з'єднаннями, швидкість Wi-Fi може бути меншою, що може вплинути на продуктивність в мережі, особливо при великих обсягах даних або вимогах до швидкості;

— сигнал Wi-Fi може бути втрачений або затриманий між пристроями через перешкоди, такі як стіни, меблі або інші пристрої, що може призвести до зниження якості підключення;

— бездротові мережі можуть бути більш вразливими до несанкціонованого доступу або злому, що ставить під загрозу конфіденційність даних.

У навчальних закладах Wi-Fi технологія відіграє важливу роль у забезпеченні доступу до Інтернету для вчителів, студентів та персоналу. Вона надає можливість підключатися до мережі з будь-якої точки навчального закладу, що сприяє ефективній роботі та навчанню. Така мобільність і доступність до інформації є ключовими для успішного функціонування сучасних навчальних закладів.

1.4 Технології маршрутизації у комп’ютерних мережах

Маршрутизація в комп'ютерних мережах є критично важливою функцією, що забезпечує ефективну передачу даних між різними пристроями і мережними сегментами. Цей процес полягає у виборі оптимального шляху для кожного пакета даних, щоб вони дісталися від джерела до призначення.

У мережах існують дві головні категорії маршрутизації: внутрішня та зовнішня. Внутрішня маршрутизація відбувається всередині одного мережевого домену, тоді як зовнішня маршрутизація охоплює обмін маршрутами між різними мережами або доменами.

Дистанційно-векторні протоколи маршрутизації, такі як RIP і IGRP, мають просту реалізацію та малі вимоги до обчислювальних ресурсів, але вони менш ефективні в складних мережних топологіях і мають обмежену масштабованість.

Збалансовані гібридні протоколи, наприклад, EIGRP, поєднують в собі переваги дистанційно-векторних і протоколів з урахуванням стану каналу. Вони мають вищу швидкість збою в порівнянні з дистанційно-векторними протоколами і меншу кількість трафіку у порівнянні з протоколами, що враховують стан каналу. Однак вони можуть бути складнішими в реалізації і вимагають більше ресурсів.

Протоколи, що враховують стан каналу, такі як OSPF і IS-IS, надають оптимальні маршрути в складних мережних середовищах і мають високу масштабованість. Однак вони вимагають більшої кількості обчислювальних ресурсів і налаштувань для ефективної роботи.

Зовнішня маршрутизація за допомогою протоколу BGP є ідеальним варіантом для обміну маршрутною інформацією між різними провайдерами Інтернету і автономними системами, забезпечуючи гнучкість та роботоздатність в глобальному масштабі. Класифікація протоколів динамічної маршрутизації показані на рисунку 1.1

У порівнянні з іншими протоколами маршрутизації, OSPF відзначається високою надійністю, оперативним реагуванням на збої, властивістю масштабованості та здатністю працювати в складних мережевих середовищах. Ці характеристики роблять OSPF оптимальним вибором для внутрішньої маршрутизації.

Рисунок 1.1 — Класифікація протоколів динамічної маршрутизації

1.4.1 Маршрутизаційний протокол OSPF

Маршрутизаційний протокол OSPF (Open Shortest Path First) — це відкритий протокол маршрутизації, який використовується для визначення найкоротшого шляху між різними вузлами у мережі заснованій на IP. OSPF ідеально підходить для великих корпоративних мереж, оскільки дозволяє ефективно керувати трафіком і маршрутизацією, забезпечуючи швидке та надійне з'єднання між різними сегментами мережі [10].

OSPF дозволяє розділити мережу на логічні частини, відомі як зони або сектори. Цей підхід сприяє поліпшенню продуктивності та зменшенню обсягів обміну маршрутною інформацією, що особливо важливо в масштабних мережах.

Кожна зона в OSPF є логічною групою маршрутизаторів і мереж, які мають однакові параметри маршрутизації та обмінюються інформацією про маршрути лише з маршрутизаторами у тій же зоні. Це дозволяє скоротити обсяги обміну маршрутною інформацією, оскільки маршрутизатори у різних зонах не обмінюватимуться повною маршрутною таблицею.

Кожна зона має свій унікальний ідентифікатор, відомий як Area ID. Маршрутизатори у межах однієї зони обмінюються маршрутною інформацією лише з іншими маршрутизаторами у тій же зоні. Великі мережі можуть бути розділені на кілька зон для забезпечення більшої ефективності маршрутизації та зменшення навантаження на мережевий трафік [10].

Використання зон у OSPF дозволяє зменшити час відновлення мережі в разі виникнення проблем і підвищити її стійкість. Він також дозволяє більш гнучко керувати обсягами маршрутної інформації та оптимізувати маршрутизацію для конкретних вимог мережі. Приклад поділу мережі OSPF на сектори показано на рисунку 1.2

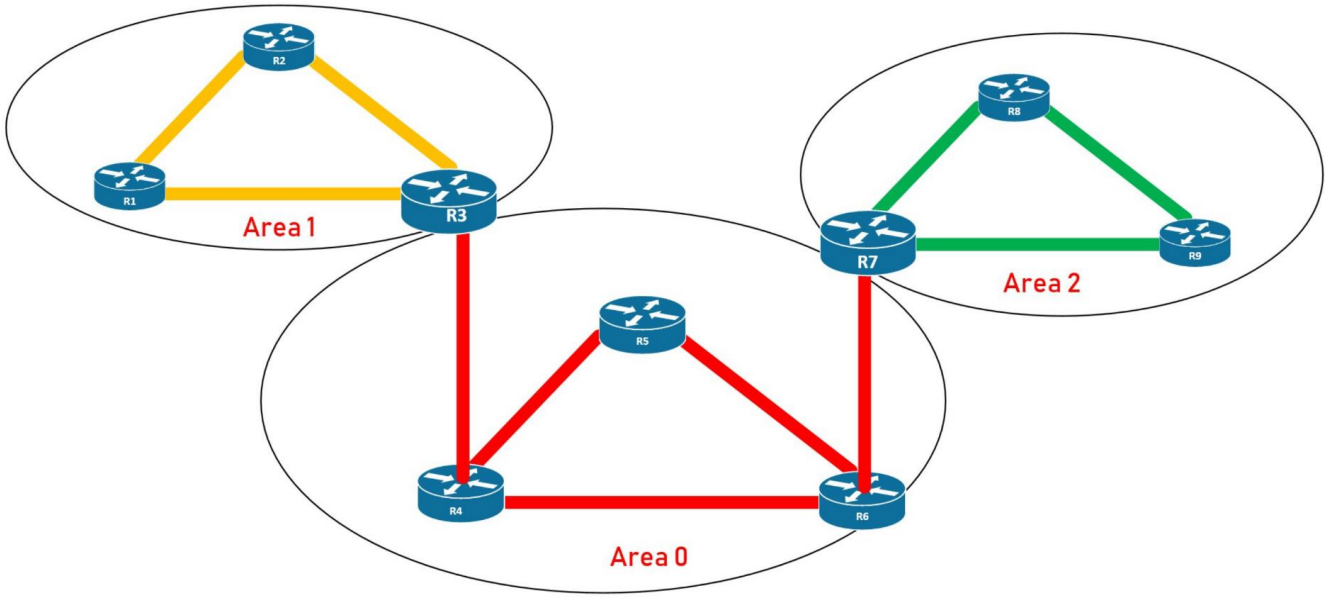

Рисунок 1.2 — Приклад поділу мережі OSPF на сектори

Однією з ключових особливостей протоколу OSPF є його здатність ефективно керувати великою кількістю маршрутів і динамічно реагувати на зміни у мережі. Ця особливість дозволяє OSPF працювати в різноманітних мережевих середовищах, включаючи мережі різних масштабів і складності. Протокол автоматично виявляє зміни у топології мережі, такі як з'єднання або відключення пристроїв, та самостійно оновлює інформацію про маршрути. Крім того, у випадку виникнення проблем чи змін у конфігурації мережі, OSPF перераховує маршрути, щоб забезпечити найбільш ефективний шлях для передачі даних [10].

Ця здатність протоколу до автоматичного адаптування до змін у мережі робить OSPF особливо корисним для побудови стабільних та надійних мережних інфраструктур. Навіть у складних умовах експлуатації, коли мережа піддається частим змінам або великій кількості трафіку, OSPF може ефективно керувати маршрутизацією, забезпечуючи оптимальне використання ресурсів мережі та високу доступність сервісів.

Протокол OSPF використовує алгоритм Дейкстри для визначення найкоротшого шляху між двома вузлами у мережі. Алгоритм Дейкстри шукає найменший шлях від одного початкового вузла до всіх інших вузлів у графі, при цьому враховуючи вагу кожного з'єднання між вузлами. У випадку OSPF, кожне з'єднання між маршрутизаторами має свою вагу, яка може відображати пропускну здатність каналу, його надійність або інші метрики [10].

Також важливою особливістю OSPF є підтримка аутентифікації. Ця функція дозволяє захистити мережу від несанкціонованого доступу та маніпуляцій з маршрутами. Використання аутентифікації забезпечує додатковий рівень безпеки для мережі та даних, що передаються по ній .

Механізми аутентифікації в OSPF дозволяють перевірити, що маршрутні оголошення, які маршрутизатори обмінюються між собою, є дійсними і не були змінені або підроблені третьою стороною. Це дозволяє захистити мережу від атак, таких як перехоплення маршрутних оголошень або внесення змін у маршрутну таблицю.

Підтримка аутентифікації дозволяє адміністраторам мережі встановлювати паролі або інші методи аутентифікації на маршрутизаторах OSPF. Такі методи можуть включати використання шифрованих ключів або перевірку за допомогою алгоритмів хешування, які забезпечують конфіденційність та цілісність маршрутної інформації [10].

В цілому, підтримка аутентифікації в OSPF робить протокол більш безпечним та надійним, допомагаючи запобігти несанкціонованому доступу. Це важливий аспект в розвитку та експлуатації сучасних комп'ютерних мереж.

Узагальнюючи, OSPF — це потужний і надійний маршрутизаційний протокол, який забезпечує ефективну маршрутизацію даних в складних мережних середовищах. Його гнучкість, висока швидкість та можливість масштабування роблять його популярним вибором для великих корпоративних мереж з вимогами до надійності та продуктивності.

1.5 Технологія NAT

Network Address Translation (NAT), або технологія перетворення мережевих адрес, є методом, який використовується в комп'ютерних мережах для перетворення IP-адрес між приватними та публічними мережами. Основна мета NAT — дозволити пристроям у приватній мережі спілкуватися з інтернетом, використовуючи лише одну публічну IP-адресу, а також захистити внутрішню мережу від прямого доступу зовнішніх пристроїв [11].

При використанні технології NAT, пристрої в приватній мережі отримують свої IP-адреси з зарезервованого діапазону. Цей діапазон IP-адрес, визначений спеціально для цілей приватних мереж, дозволяє уникнути конфліктів адресації між різними мережами та забезпечити внутрішню ідентифікацію пристроїв у мережі. Коли пристрій в приватній мережі намагається вийти в Інтернет, маршрутизатор або NAT-проксі на мережевому шлюзі перетворюють IP-адресу та номер порту пакета на публічну IP-адресу та унікальний номер порту.

Цей механізм дозволяє забезпечити ізоляцію внутрішньої мережі від зовнішнього світу та дозволяє більш ефективно використовувати доступні

публічні IP-адреси. Крім того, NAT надає додатковий рівень безпеки, оскільки зовнішні пристрої бачать лише публічну IP-адресу маршрутизатора або шлюзу NAT, а не окремі пристрої в приватній мережі [11].

Натуральним обмеженням доступу до Інтернету є обмежена кількість доступних публічних IP-адрес. Оскільки кожен пристрій, що підключений до Інтернету, потребує унікальної адреси для ідентифікації та комунікації в мережі, зростання кількості пристроїв призводить до зменшення доступних адрес. Стандартним рішенням для цього є придбання додаткових публічних IP-адрес.

На допомогу приходить технологія NAT, яка дозволяє маршрутизатору або іншому пристрою в мережі перетворювати приватні IP-адреси, які використовуються у внутрішній мережі, на одну або кілька публічних IP-адрес, які використовуються для зовнішнього зв'язку з Інтернетом. Завдяки цьому, внутрішні пристрої можуть залишатися прихованими за єдиною зовнішньою IP-адресою, а доступ до Інтернету здійснюється через цей зовнішній адрес. Таким чином, використання NAT дозволяє ефективно використовувати доступні публічні IP-адреси, що дозволяє зекономити кошти та ресурси. Взаємодія локальних та публічних IP-адрес за допомогою технології NAT показано на рисунку 1.3

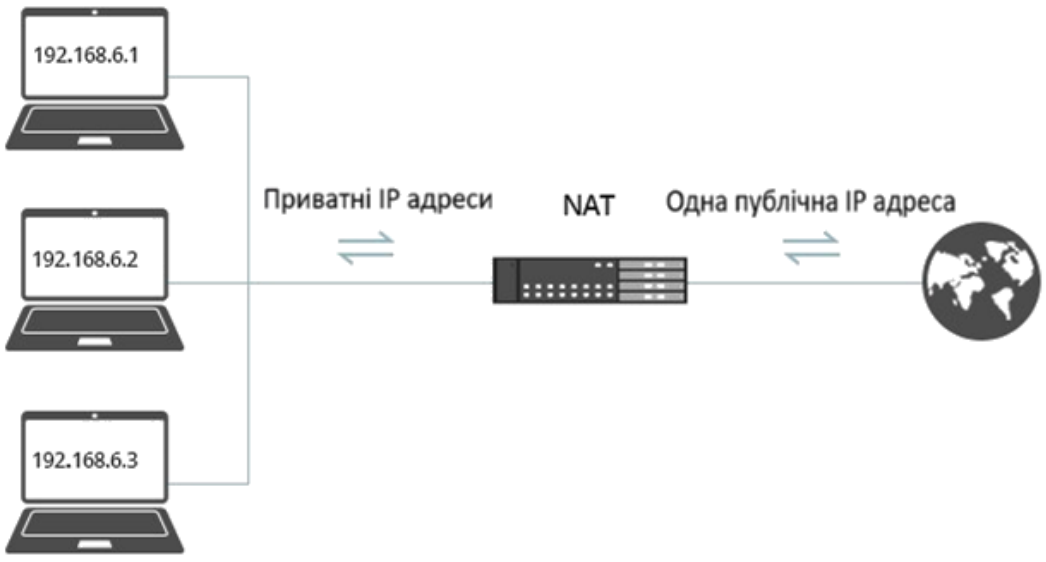

Рисунок 1.3 — Взаємодія локальних та публічних IP-адрес за допомогою технології NAT

Крім того, використання NAT спрощує адміністрування мережі, оскільки вимагає меншого обсягу конфігурації та керування. Замість того, щоб налаштовувати кожен пристрій з окремою публічною IP-адресою та відповідними параметрами маршрутизації, адміністратор може просто налаштувати маршрутизатор або NAT-проксі для перетворення приватних адрес у публічні адреси під час виходу в Інтернет. Це полегшує процес налаштування та управління мережею, зменшуючи ймовірність помилок та покращуючи її загальну продуктивність.

Під час використання NAT (Network Address Translation), пристрої в приватній мережі отримують свої IP-адреси з зарезервованого діапазону. Такі адреси відомі як приватні IP-адреси і вони призначені для використання у внутрішній мережі. Коли пристрій в приватній мережі намагається вийти в Інтернет, маршрутизатор або NAT-проксі на мережевому шлюзі перетворюють IP-адресу та номер порту пакета на публічну IP-адресу та унікальний номер порту. Цей процес називається перекладом адрес (Address Translation) [11]. Коли пакети повертаються назад, NAT перетворює їхні адреси назад на адреси в приватній мережі. Це дозволяє більшій кількості пристроїв внутрішньої мережі спілкуватися за допомогою лише одного чи кількох публічних IP-адрес.

Однією з основних переваг використання NAT є економія публічних IP-адрес. Завдяки NAT, компанії та домашні мережі можуть використовувати лише одну або кілька публічних IP-адрес для доступу до Інтернету, замість того, щоб надавати кожному пристрою в мережі свою унікальну публічну IP-адресу. Це дозволяє заощадити витрати на придбання додаткових IP-адрес та спростити адміністрування мережі.

Використання NAT може мати вплив на деякі типи з'єднань, такі як P2P (Peer-to-Peer) або деякі додатки, які використовують адресацію IP у своїй роботі. Причиною цього є те, що внутрішні пристрої в мережі за NAT використовують публічну IP-адресу маршрутизатора або шлюзу NAT для звернень до зовнішніх ресурсів в Інтернеті. Таким чином, виникає необхідність у складних механізмах, які б дозволяли пристроям ініціювати з'єднання та пройти через NAT [11].

Деякі типи NAT можуть створювати обмеження щодо можливості встановлення з'єднань зовнішніми пристроями. Наприклад, у випадку Symmetric NAT, порти, які відкриваються для вихідних з'єднань, різняться для кожного зовнішнього призначення, що робить важким встановлення назад з'єднання з зовнішніми пристроями, які не були ініціаторами з'єднання. Загальні переваги та недоліки технології NAT відображені у таблиці 1.6

Таблиця 1.6 — Переваги та недоліки технології NAT

Переваги технології NAT	Недоліки технології NAT
1. Підвищує безпеку мережі	1. Обмежує доступність послуг, що базуються на IP-адресах
2. Приховує внутрішню мережу від зовнішнього світу	2. Складності у налаштуванні та керуванні
3. Дозволяє економити глобальні IP-адреси	3. Може впливати на швидкість мережі
4. Дозволяє маршрутизаторам здійснювати перетворення адреси	4. Можливість виникнення проблем з сумісністю деяких додатків
5. Зменшує вразливість до атак на мережу	5. Обмежує рівень доступу для зовнішніх пристроїв
6. Покращує анонімність користувачів	6. Потребує додаткового обладнання та програмного забезпечення
7. Дозволяє налаштовувати доступ до Інтернету для внутрішніх пристроїв	7. Може ускладнювати налагодження проблем мережі
8. Забезпечує ізоляцію внутрішньої мережі від зовнішніх загроз	8. Можливість виникнення конфліктів між IP-адресами
9. Дозволяє використовувати внутрішні IP-адреси	9. Обмежує можливості деяких протоколів, таких як IPsec

2 АНАЛІЗ ТА ОБҐРУНТУВАННЯ ВИБОРУ ТЕХНОЛОГІЙ

2.1 Аналіз структури навчального закладу

Оскільки навчальний заклад, для якого розробляється комп'ютерна мережа, має обмежену територію, вузли мережі розташовані досить близько один до одного. Приміщення коледжу знаходяться на невеликій відстані одне від одного, що спрощує організацію мережевих з'єднань. Можна виділити три основні частини локальної мережі коледжу:

— адміністрацію;

— 1 корпус;

— 2 корпус.

Структурна схема мережі Вінницького технічного фахового коледжу представлена на рисунку 2.1

Рисунок 2.1 — Структурна схема мережі коледжу

В адміністрації коледжу розташовані кабінети, де знаходяться навчальна частина, секретаріат та бухгалтерія. Кабінети керівництва виконують ключові адміністративні функції, включаючи організацію навчального процесу та взаємодію зі студентами. Секретаріат здійснює обробку та зберігання документації, а також забезпечує зв'язок між структурними підрозділами. Бухгалтерія веде бухгалтерський облік та звітність, контролює фінансову діяльність та здійснює розрахунки з постачальниками. Кількість приладів в кабінетах адміністрації відображена у таблиці 2.1

Таблиця 2.1 — Кількість приладів в кабінетах адміністрації

Кабінет	Кількість ПК
Навчальна частина	3
Секретаріат	6
Бухгалтерія	3

У першому корпусі Вінницького технічного фахового коледжу розташовані фінансово-економічне та радіотехнічне відділення. Кожне з цих відділень має по чотири кабінети, де розміщені кінцеві пристрої для навчання та практичних робіт. Кількість приладів в аудиторіях першого корпусу відображена у таблиці 2.2

Таблиця 2.2 — Кількість приладів в аудиторіях першого корпусу

Кабінет	Кількість ПК
102	20
103	20
105	20
107	2
108	2
109	20
110	30
Бібліотека	10

Фінансово-економічне відділення включає кабінети з номерами 107 до 110, де студенти здійснюють вивчення економічних та фінансових дисциплін. Натомість радіотехнічне відділення має кабінети з номерами 102, 103, 105,

призначені для проведення занять з радіоелектроніки та радіотехнічних процесів. Крім того, у першому корпусі розташована бібліотека, де студенти можуть користуватися літературними джерелами для підготовки до занять та виконання наукових досліджень.

У другому корпусі Вінницького технічного фахового коледжу розташовані відділення транспортних технологій, електроенергетики та електромеханіки, а також комп'ютерне відділення. Відділення транспортних технологій складається з чотирьох кабінетів з номерами від 201 до 204. Відділення електроенергетики та електромеханіки має три кабінети з номерами 205, 210 і 211. Комп'ютерне відділення складається з п'яти кабінетів, номери яких від 214 до 218. Кількість приладів в аудиторіях другого корпусу відображена у таблиці 2.3

Таблиця 2.3 — Кількість приладів в аудиторіях другого корпусу

Кабінет	Кількість ПК
201	10
202	10
203	10
204	10
205	32
210	32
211	32
214	20
215	20
216	20
217	20
218	20

Загалом у відділі адміністрації потрібно під'єднати 12 кінцевих пристроїв до локальної мережі. У першому корпусі необхідно забезпечити підключення 124 кінцевих пристроїв, а у другому корпусі — 236 пристроїв. Загалом, для всього Вінницького технічного фахового коледжу необхідно підготувати мережеву інфраструктуру для 372 кінцевих пристроїв.

2.2 Розподіл адресного простору мережі

Мережа Вінницького технічного фахового коледжу буде розділена на дві підмережі для кращого управління мережевими ресурсами та підвищення ефективності мережі. Перша підмережа об'єднуватиме адміністративну частину та перший корпус коледжу, оскільки в цих частинах найменша кількість кабінетів. Друга підмережа буде відведена для другого корпусу, що має більшу кількість кабінетів та відділень. Це дозволить оптимізувати розподіл IP-адрес та керувати мережевим трафіком більш ефективно.

Адреса 192.168.0.0 буде використовуватися для виділення адресного простору в підмережах мережі. Ця адреса є базовою для створення підмереж та розподілу IP-адрес між різними частинами мережі. Вона дозволяє організувати структуру мережі та забезпечити комунікацію між пристроями, надаючи їм унікальні ідентифікатори в мережі. Розподіл IP-адрес локальної мережі відображено у таблиці 2.4

Таблиця 2.4 — Розподіл IP-адрес локальної мережі

IP-адреса	Маска підмережі	Назва об'єкта навчального закладу
192.168.31.0	255.255.255.0	Адміністрація та 1 корпус
192.168.30.0	255.255.255.0	2 корпус

Для ефективного використання адресного простору підмереж мережу було поділено за допомогою масок змінної довжини. Це допомагає забезпечити ефективне використання доступних IP-адрес та оптимізувати розподіл адресного простору між різними частинами мережі.

Адміністрацію та перший корпус було розділено на 6 секцій: радіотехнічне відділення, фінансово-економічне відділення, адміністрацію та 3 секції для маршрутизаторів, які призначені для обміну файлами між комп’ютерними мережами. Радіотехнічне відділення містить 126 хостів, фінансово-економічне відділення містить 62 хостів, а адміністрація містить 14 хостів. Маршрутизатори, загалом, займають 6 хостів.

Враховуючи кількість кінцевих пристроїв, в першому корпусі залишається невеликий діапазон IP-адрес для розширення першої підмережі, а саме IP-адреси з 192.168.31.216 по 192.168.31.255. Це необхідно для забезпечення можливості підключення нових пристроїв та збільшення кількості хостів у першій підмережі без необхідності переналаштування всієї мережної інфраструктури. Розподіл IP-адрес першої підмережі відображено у таблиці 2.5

Таблиця 2.5 — Розподіл IP-адрес першої підмережі

Секція підмережі	Адреса мережі	Адреса хостів	Широкомовна адреса	Маска мережі	Інвертована маска
Радіотехнічне відділення	192.168.31.0	1-126	192.168.31.127	/25(255.255.255.128)	0.0.0.127
Фінансове відділення	192.168.31.128	129-190	192.168.31.191	/26(255.255.255.192)	0.0.0.63
Адміністрація	192.168.31.192	193-206	192.168.31.207	/28(255.255.255.240)	0.0.0.15
Маршрутизатор 4-5	192.168.31.208	209-210	192.168.31.211	/30(255.255.255.252)	0.0.0.3
Маршрутизатор 4-8	192.168.31.212	213-214	192.168.31.215	/30(255.255.255.252)	0.0.0.3
Маршрутизатор 4-2	192.168.31.216	217-218	192.168.31.219	/30(255.255.255.252)	0.0.0.3
Вільно	192.168.31.216 - 192.168.31.255				

Друга підмережа поділена на 3 секції: комп’ютерне відділення, відділення електроенергетики та електромеханіки, і відділення транспортних технологій. Комп’ютерне відділення налічує 126 хостів, відділення електроенергетики та електромеханіки містить 62 хостів, а відділення транспортних технологій також має 62 хостів. Розподіл IP-адрес другої підмережі відображено у таблиці 2.6

Таблиця 2.6 — Розподіл IP-адрес другої підмережі

Секція підмережі	Адреса мережі	Адреса хостів	Широкомовна адреса	Маска мережі	Інвертована маска
Комп'ютерне відділення	192.168.30.0	1-126	192.168.30.127	/25(255.255.255.128)	0.0.0.127
Відділення техніки та електромеханіки	192.168.30.128	129-190	192.168.30.191	/26(255.255.255.192)	0.0.0.63
Відділення транспортних технологій	192.168.30.192	193-254	192.168.30.255	/26(255.255.255.192)	0.0.0.63

Маршрутизація всередині локальної мережі буде здійснюватися за допомогою протоколу OSPF, оскільки цей протокол дозволяє ефективно управляти маршрутизацією в середній та великій мережах, які мають складну топологію і потребують постійного оновлення маршрутної інформації. У нашому випадку, де мережа коледжу складається з кількох корпусів та різних відділень з різною кількістю хостів, OSPF забезпечить автоматичне виявлення мережних пристроїв, обмін маршрутною інформацією та швидке виявлення найкращого маршруту до кожного хоста в мережі. Крім того, OSPF підтримує розділення мережі на зони, що дозволяє зменшити обсяги обміну маршрутною інформацією та зробити мережу більш масштабованою і ефективною.

2.3 Розробка логічної топології мережі

Розробка логічної топології мережі — це процес створення моделі, яка визначає взаємозв'язки між різними пристроями і вузлами у комп'ютерній мережі. Головною метою цього процесу є створення плану розміщення та з'єднання мережевого обладнання для забезпечення ефективного обміну даними і забезпечення необхідної функціональності мережі. Розробка логічної топології важлива для того, щоб забезпечити оптимальну працездатність мережі, зменшити можливі проблеми зі з'єднанням і підвищити її надійність [12].

Під час розробки логічної топології мережі, спочатку проводиться аналіз вимог і потреб користувачів та організації, яка використовуватиме мережу. Потім визначаються типи та кількість пристроїв, що будуть підключені до мережі, і їхнє функціональне призначення. На основі цих вихідних даних створюється модель топології, де вказується розташування кожного пристрою та зв'язки між ними.

Розробка логічної топології включає також визначення маршрутів зв'язку між пристроями, встановлення правил і політик безпеки, а також розподіл ресурсів мережі для оптимізації швидкості передачі даних і мінімізації можливих конфліктів. Усі ці кроки спрямовані на створення мережевого середовища, яке відповідає потребам користувачів і забезпечує надійну та ефективну роботу мережі.

Логічна топологія мережі — це концептуальна модель або схема, яка визначає спосіб, яким дані передаються від одного пристрою до іншого у мережі. Вона вказує на зв'язки між пристроями та маршрутизаторами у мережі та визначає шляхи, по яких дані будуть передаватися від джерела до призначення. Логічна топологія визначає структуру мережі на рівні програмного забезпечення, умовно показуючи, як пристрої мережі спілкуються один з одним через протоколи і канали зв'язку [12].

Фізична топологія мережі — це реальна або фізична структура, яка визначає фактичне розташування пристроїв і з'єднання між ними у мережі. Вона показує, як фізично з'єднані пристрої розташовані один відносно одного і яким чином кабелі або бездротові зв'язки забезпечують зв'язок між ними. Фізична топологія може бути подана у вигляді схеми або мапи, на якій відображені всі пристрої мережі та їхні з'єднання [13].

Важливість фізичної топології полягає у тому, що вона визначає структуру мережі з боку розташування і зв'язків між пристроями. Це допомагає в плануванні та налагодженні мережі, а також у виявленні потенційних проблем і несправностей. Знання фізичної топології допомагає мережевим адміністраторам ефективно керувати мережею, виявляти і виправляти проблеми з'єднання та забезпечувати оптимальну продуктивність мережі.

Важливо розуміти, що логічна топологія може відрізнятися від фізичної топології, яка описує фактичні з'єднання між пристроями у мережі. У логічній топології можуть бути використані різні методи і протоколи, такі як Ethernet, Wi-Fi, TCP/IP тощо, для забезпечення зв'язку між пристроями, незалежно від того, як вони фізично підключені. Це дозволяє створити ефективну мережу з оптимальною продуктивністю і безпекою передачі даних.

Під час розгляду мережі навчального закладу важливо врахувати її структуру та складові елементи. Логічна топологія мережі Вінницького технічного фахового коледжу показана на рисунку 2.2. Мережа складається з двох основних підмереж. Перша підмережа містить два маршрутизатори, три комутатори та кінцеві пристрої, які з'єднані між собою прямими кабелями.

Маршрутизатори в цій підмережі використовуються для маршрутизації даних між різними сегментами мережі та забезпечення доступу до зовнішньої мережі.

Кожен з маршрутизаторів першої підмережі з'єднаний з центральним маршрутизатором за допомогою serial кабелю, що дозволяє організувати зв'язок між підмережами. Друга підмережа складається з одного маршрутизатора, трьох комутаторів і кінцевих пристроїв. Також кожен кінцевий пристрій з'єднаний з комутатором прямим кабелем. У цій підмережі маршрутизатор також з'єднується з центральним маршрутизатором, але використовується крос-кабель для забезпечення зв'язку.

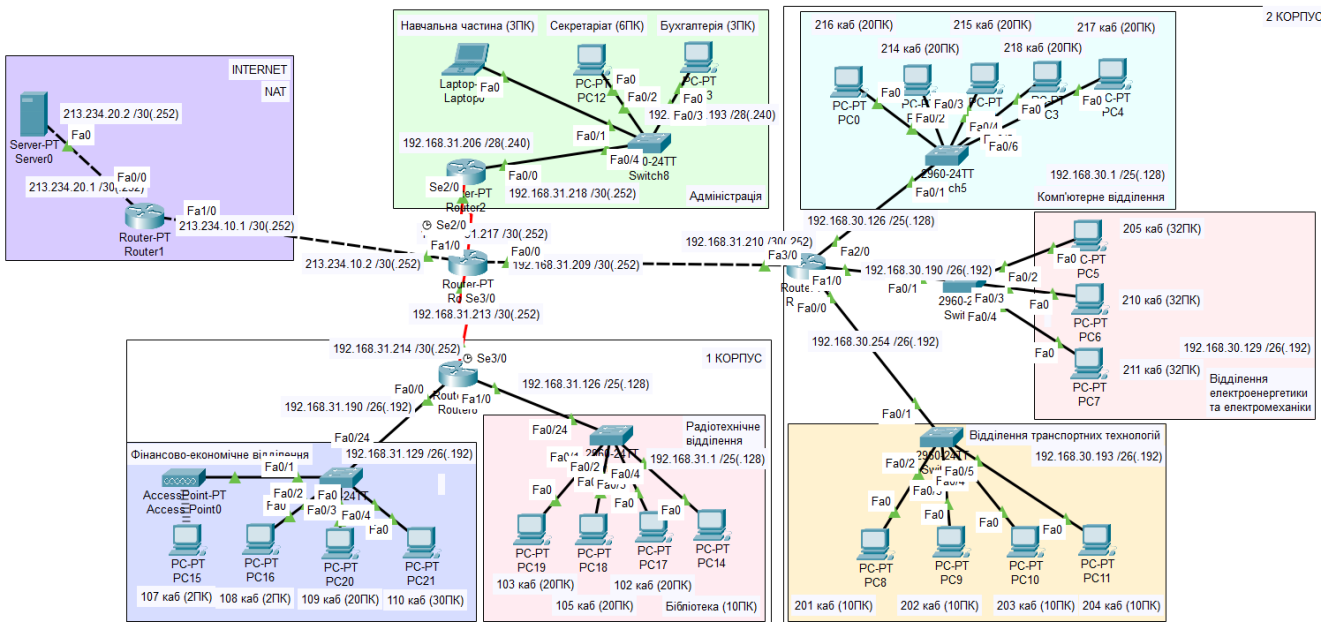

Рисунок 2.2 — Логічна топологія мережі Вінницького технічного фахового коледжу

Кінцеві пристрої у першій підмережі з’єднані за допомогою комутаторів до своїх відповідних маршрутизаторів. Ці маршрутизатори, разом із маршрутизатором другої підмережі, встановлюють зв'язок з центральним граничним маршрутизатором, який забезпечує вихід до мережі Інтернет. У другій підмережі кінцеві пристрої підключаються до комутаторів, які з'єднані з маршрутизатором, що також розташований у другому корпусі. Усі

маршрутизатори взаємодіють між собою та обмінюються даними між підмережами за допомогою протоколу динамічної маршрутизації OSPF.

Для забезпечення ефективної комунікації та оптимальної маршрутизації даних між мережами, центральний маршрутизатор також буде розсилати інформацію про маршрут за замовчуванням за допомогою пакетів OSPF. Це дозволяє керувати трафіком у мережі та забезпечити надійність підключення до Інтернету.

Для емуляції доступу до Інтернету у нашій мережі використовується спеціальний сервер та маршрутизатор, обидва з публічними IP-адресами. Основна функція маршрутизатора полягає у забезпеченні комунікації між локальною мережею та Інтернетом. Ця комунікація відбувається за допомогою технології мережевої адресації та трансляції адрес (NAT), що дозволяє приховати внутрішні адреси мережі від зовнішнього світу. Окрім того, для налаштування сервісу NAT використовуються списки доступу (ACL), які визначають правила, за якими дозволяється або блокується обмін даними між локальною мережею та Інтернетом.

2.4 Вибір пристроїв для створення комп'ютерної мережі

На основі порівняльних характеристик було обрано два провідних виробники мережевого обладнання: CISCO та MIKROTIK. При виборі між цими двома виробниками слід ретельно оцінити конкретні потреби та вимоги організації, а також розглянути технічні можливості та економічні фактори.

CISCO відома своїми високоякісними продуктами та широким спектром послуг у сфері мережевих технологій. Компанія надає рішення для провайдерів послуг, корпорацій, малих та середніх підприємств, державних установ та навчальних закладів. Їхнє обладнання використовується як у великих корпоративних мережах, так і в невеликих офісах. CISCO володіє великим досвідом у цій галузі та підтримується широкою мережею партнерів та сервісних центрів по всьому світу.

MIKROTIK відома своїм низьким вартісним порівняно з CISCO та широким спектром продуктів, які містять маршрутизатори, комутатори, антени та програмне забезпечення. Продукція MIKROTIK знайшла застосування у різних галузях, включаючи домашні мережі, бізнес-сектор та провайдерів інтернет-послуг. MIKROTIK славиться своєю простотою використання та широким функціоналом, що робить їхні пристрої привабливими для невеликих бізнесів та споживачів з обмеженим бюджетом.

2.4.1 Вибір моделі маршрутизаторів

Маршрутизатор — це мережевий пристрій, який використовується для передачі даних між різними мережами. Основна функція маршрутизатора полягає в прийнятті пакетів даних з одного мережевого інтерфейсу, визначенні оптимального шляху до маршрутизації цих пакетів та пересиланні їх до відповідного інтерфейсу для подальшої передачі [14].

Маршрутизатори є необхідними для забезпечення комунікації між різними мережами, включаючи локальні мережі (LAN), мережі великих підприємств, Інтернет, віддалені мережі та інші. Вони грають важливу роль у забезпеченні швидкої та надійної передачі даних. Приклад використання маршрутизатора у мережах показаний на рисунку 2.3

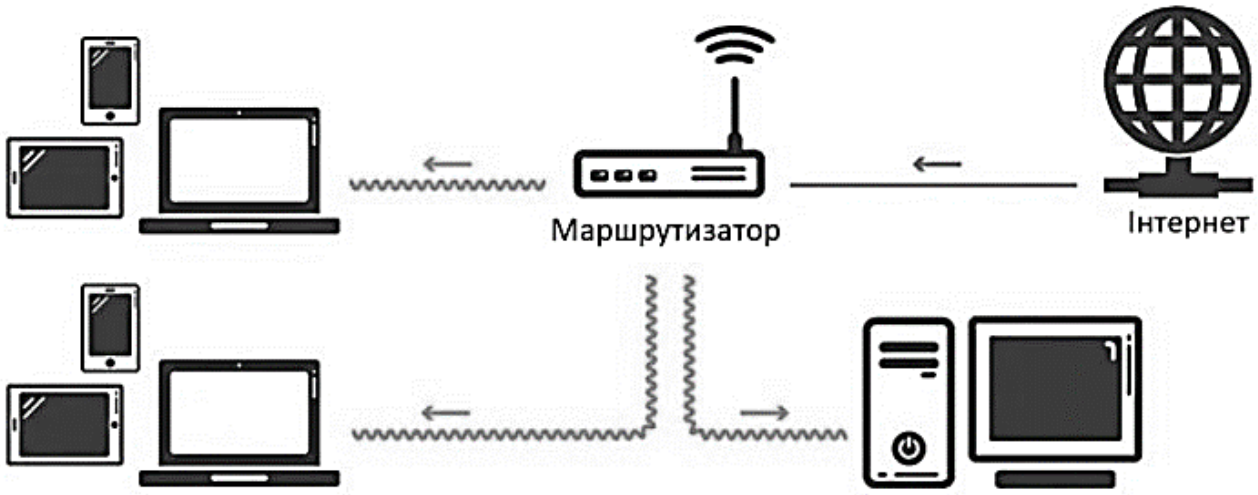

Рисунок 2.3 — Приклад використання маршрутизатора у мережах

Перевагами маршрутизаторів є їхня здатність працювати на рівні мережевого (Layer 3) моделі OSI, що дозволяє їм приймати рішення про найкращий шлях маршрутизації пакетів даних, та забезпечувати більшу гнучкість у керуванні мережею. Крім того, вони дозволяють забезпечити безпеку мережі шляхом фільтрації пакетів та використання VPN-підключень. Недоліками маршрутизаторів можуть бути їхня висока вартість, складність установки та налаштування, а також обмежена швидкодія на рівні програмного забезпечення [14].

При виборі маршрутизатора важливо враховувати такі параметри, як пропускна здатність, підтримувані мережеві протоколи, можливість роботи з великою кількістю підключень, надійність та підтримка технічної підтримки. Для Вінницького технічного фахового коледжу маршрутизатори є важливими для забезпечення надійного та швидкого з'єднання між різними частинами мережі, включаючи аудиторії, адміністративні приміщення, бібліотеку та інші відділи. Вони також дозволяють забезпечити безпеку мережі та доступ до Інтернету для студентів та викладачів.

Маршрутизатор складається з різноманітних компонентів, які спільно працюють для керування та маршрутизації мережевого трафіку. Основні компоненти маршрутизатора включають центральний процесор, оперативну пам'ять, постійну пам'ять, мережеві інтерфейси та програмне забезпечення [15].

Центральний процесор (CPU) є головним обчислювальним елементом маршрутизатора, відповідальним за обробку та керування мережевим трафіком. Він виконує різноманітні операції, такі як маршрутизація пакетів, обробка протоколів маршрутизації, фільтрація та керування трафіком.

Оперативна пам'ять (RAM) використовується для тимчасового зберігання даних та програм, які використовуються маршрутизатором у процесі його роботи. Вона виконує важливу роль у забезпеченні швидкодії та ефективності маршрутизатора, оскільки забезпечує швидкий доступ до даних.

Постійна пам'ять (ROM) містить основне програмне забезпечення (прошивку) маршрутизатора, яке завантажується при його запуску. Вона також

містить початкові налаштування та діагностичні програми, які дозволяють маршрутизатору працювати правильно [15].

Мережеві інтерфейси — це фізичні роз'єми або бездротові інтерфейси, які забезпечують з'єднання між маршрутизатором та іншими мережевими пристроями. Вони можуть включати Ethernet-порти, WAN-порти, а також бездротові антени для підключення до мережі. Розташування мережевих інтерфейсів маршрутизатора RB4011IGS + RM, який буде розглянутий далі, показане на рисунку 2.4

Рисунок 2.4 — Розташування мережевих інтерфейсів маршрутизатора MIKROTIK RB4011IGS + RM

Програмне забезпечення маршрутизатора включає операційну систему та додаткове програмне забезпечення для керування мережею та виконання різних функцій, таких як маршрутизація, безпека, керування пропускною здатністю та багато іншого [15]. Усі ці компоненти разом створюють складну мережеву інфраструктуру, яка дозволяє маршрутизатору ефективно керувати мережевим трафіком та забезпечувати надійну комунікацію між різними пристроями у мережі.

Оскільки розглядаються продукти виробників Cisco та MikroTik, то оберемо дві моделі маршрутизаторів для порівняння: Cisco ASR 1001 (PTSC2005) та MikroTik RB4011IGS + RM.

Cisco ASR 1001 є продуктом компанії Cisco Systems, світового лідера в галузі мережевих технологій. Цей маршрутизатор відомий своєю високою продуктивністю та надійністю. Він призначений для великих корпоративних

мереж та постачальників послуг і може обробляти значні обсяги мережевого трафіку [16].

MikroTik RB4011IGS + RM — це маршрутизатор від MikroTik, відомого виробника мережевого обладнання з Латвії. Цей маршрутизатор також має високу продуктивність та може використовуватися як для домашнього, так і для комерційного використання. Він славиться своєю доступністю та простотою у використанні [17].

Кожен з цих маршрутизаторів має свої особливості та переваги. Cisco ASR 1001 відзначається широким функціоналом та високою надійністю, що робить його ідеальним вибором для великих корпоративних мереж. MikroTik RB4011IGS + RM, з іншого боку, відомий своєю доступністю та простотою у використанні, що робить його привабливим для менших мереж з обмеженим бюджетом. Порівняльна характеристика властивостей маршрутизаторів Cisco ASR 1001 та MikroTik RB4011IGS + RM наведена у таблиці 2.7

Таблиця 2.7 — Порівняльна характеристика властивостей маршрутизаторів Cisco ASR 1001 та MikroTik RB4011IGS + RM

Характеристика	Cisco ASR 1001	MikroTik RB4011IGS + RM
Оперативна пам'ять	8 ГБ	1 ГБ
Flash пам'ять	8 ГБ	512 МБ
Інтерфейс для консолі	USB 2.0	USB 2.0
Параметри живлення	від 100 до 240 В	від 100 до 240 В
Максимальна споживана потужність	360 Вт	19 Вт
Робоча температура	від 0С до 40С	від мінус 40С до 70С
Габарити	(43 x 439 x 466) мм	(228 x 30 x 228) мм
Мережеві порти	WAN: 4 x GE	WAN: RJ-45
	LAN: 8 x GE	LAN: 8 x RJ-45
Вага	10210 г	1500 г
Частота	від 50 до 60 Гц	від 50 до 60 Гц
Кількість LAN-інтерфейсів	8	10
Ціна	7220 грн	5449 грн

Cisco ASR 1001 має оперативну пам'ять обсягом 8 ГБ та Flash пам'ять також обсягом 8 ГБ. Для підключення консолі використовується USB 2.0 інтерфейс. Щодо живлення, цей маршрутизатор працює в діапазоні від 100 до 240 В. Максимальна споживана потужність становить 360 Вт, а робоча температура — від 0С до 40С. Габарити пристрою складають 43 на 439 на 466 мм. Cisco ASR 1001 має 4 WAN порти типу GE та 8 LAN портів також типу GE. Вага маршрутизатора становить 10210 грамів. Частота роботи пристрою знаходиться в діапазоні від 50 до 60 Гц. Максимальна вихідна потужність становить 66 Вт [16].

MikroTik RB4011IGS + RM має оперативну пам'ять обсягом 1 ГБ та Flash пам'ять обсягом 512 МБ. Інтерфейс для консолі також USB 2.0. Живлення пристрою здійснюється в діапазоні від 100 до 240 В. Максимальна споживана потужність становить 19 Вт, а робоча температура може коливатися від мінус 40С до 70С. Габарити маршрутизатора складають 228 на 30 на 228 мм. MikroTik RB4011IGS + RM має 1 WAN порт типу RJ-45 та 8 LAN портів також типу RJ-45. Вага пристрою — 1500 грамів. Частота роботи пристрою також в діапазоні від 50 до 60 Гц. Максимальна вихідна потужність становить 24 Вт [17].

Обидва маршрутизатори можуть бути корисними для різних застосувань. Cisco ASR 1001 може бути оптимальним рішенням для великих корпоративних мереж, які вимагають високої надійності та продуктивності. MikroTik RB4011IGS + RM може стати ідеальним вибором для менших мереж з обмеженим бюджетом.

Після ретельного аналізу та врахування потреб Вінницького технічного фахового коледжу, було вирішено обрати маршрутизатор Cisco ASR 1001 (PTSC2005) як оптимальний вибір для цього навчального закладу. Ця модель маршрутизатора відповідає вимогам коледжу щодо забезпечення надійного та швидкого доступу до мережевих ресурсів для студентів, викладачів та адміністративного персоналу.

Завдяки високій продуктивності та широкому спектру функцій, Cisco ASR 1001 може забезпечити стабільну роботу мережі коледжу навіть у випадку великого навантаження. Крім того, підтримка резервного живлення та можливість встановлення додаткових модулів розширення дозволяють підлаштовувати

маршрутизатор під конкретні потреби коледжу. Також слід зазначити, що Cisco є одним з провідних виробників мережевого обладнання у світі, і вибір їхнього продукту забезпечує доступ до широкого спектра технічної підтримки та сервісних послуг, що є важливим для безперебійної роботи мережі коледжу.

2.4.2 Вибір моделі комутаторів

Комутатори — це мережеві пристрої, що використовуються для з'єднання комп'ютерів та інших мережевих пристроїв у локальній мережі (LAN). Основна їх функція полягає в пересиланні даних між пристроями в одній мережі, а також у розподілі трафіку, щоб забезпечити ефективну комунікацію всередині мережі [18].

Комутатори потрібні для створення локальної мережі, в якій комп'ютери та інші мережеві пристрої можуть взаємодіяти один з одним, обмінюватися даними та спільно використовувати ресурси. Вони дозволяють підключати багато пристроїв до мережі та забезпечують швидке та надійне передавання даних між ними. Схематичне зображення підключення кінцевих пристроїв та маршрутизатора до комутатора показане на рисунку 2.5

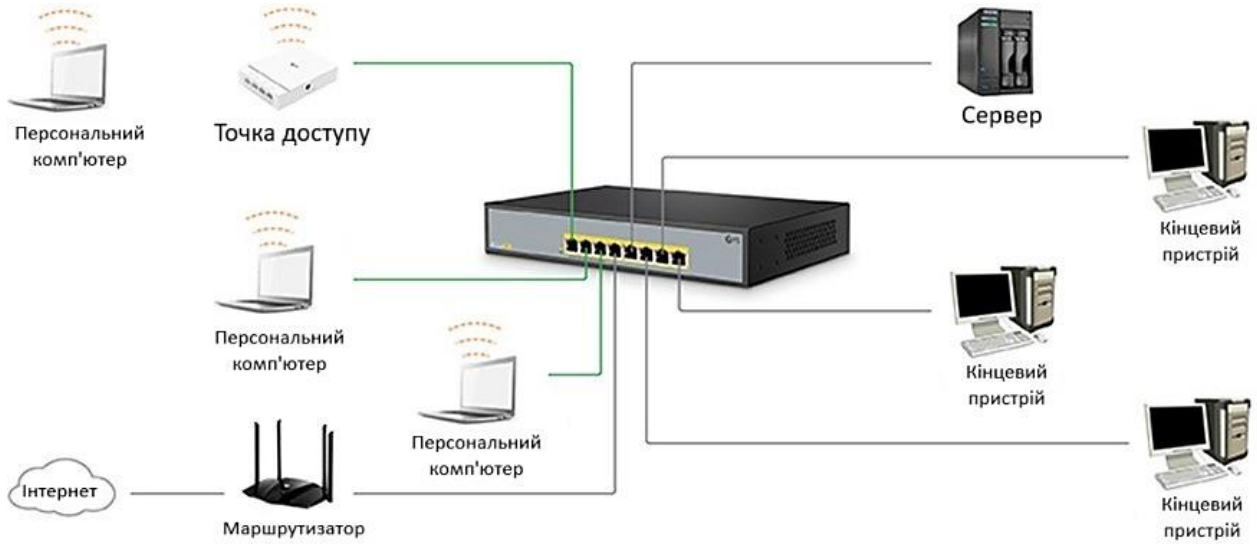

Рисунок 2.5 — Схематичне зображення підключення кінцевих пристроїв та маршрутизатора до комутатора

Серед аналогів комутаторів можна виділити хаби (hub), які також використовуються для підключення пристроїв до мережі. Однак, на відміну від комутаторів, хаби передають усі дані на кожен підключений пристрій, що може призводити до перенавантаження мережі та зниження її продуктивності [18].

Перевагами використання комутаторів є швидкість передачі даних, можливість розподілу трафіку для забезпечення оптимальної роботи мережі, підтримка різних швидкостей підключення, а також підтримка різноманітних мережевих протоколів. Однак, серед недоліків можна відзначити високу вартість деяких моделей комутаторів та можливість виникнення проблем з безпекою мережі, якщо не налаштувати правила доступу належним чином.

Будова комутатора має ряд основних компонентів. Перш за все, це порти, через які підключаються пристрої до комутатора. Кількість портів може варіюватися від кількох до десятків, залежно від моделі комутатора. Кожен порт може бути використаний для підключення окремого пристрою, наприклад, комп'ютера або принтера [18].

Для керування роботою комутатора він також має процесор, який відповідає за обробку та пересилання даних. Процесор комутатора визначає шлях передачі даних від вхідних портів до відповідних вихідних портів у мережі.

Окрім того, в комутаторі можуть бути вбудовані спеціальні чипи, які забезпечують функціональні можливості, такі як керування мережею, виявлення та усунення колізій та підтримка різних мережних протоколів.

Деякі комутатори також мають можливість керування з віддаленої точки, що дозволяє адміністраторам мережі віддалено налаштовувати та керувати роботою пристрою через мережеве підключення [18].

Розглянемо дві моделі комутаторів від провідних виробників мережевого обладнання — CISCO WS-C2960-24TT-L та MikroTik CRS112-8G-4S-IN, оскільки ми досліджуємо продукцію Cisco та MikroTik.

Cisco WS-C2960-24TT-L та MikroTik CRS112-8G-4S-IN — це дві моделі комутаторів від провідних виробників мережевого обладнання. Кожен з цих

пристроїв має свої характеристики та функціональні можливості, які можуть бути важливими для певних потреб в мережевому середовищі.

Cisco WS-C2960-24TT-L є комутатором з 24 портами, що підтримують технологію Fast Ethernet. Він призначений для використання в невеликих і середніх мережах і може забезпечити швидке та надійне з'єднання для підключення пристроїв у мережі.

Обидва ці комутатори мають свої переваги та обмеження. Cisco WS-C2960-24TT-L відомий своєю надійністю та простотою у використанні, а MikroTik CRS112-8G-4S-IN відомий своєю гнучкістю та розширеними можливостями налаштування. При виборі комутатора необхідно враховувати конкретні потреби та вимоги мережі, а також функціональні можливості кожної моделі. Порівняльна характеристика властивостей комутаторів CISCO SF220-24-K9-EU та MikroTik CRS112-8G-4S-IN наведена у таблиці 2.8

Таблиця 2.8 — Порівняльна характеристика властивостей комутаторів CISCO SF220-24-K9-EU та MikroTik CRS112-8G-4S-IN

Характеристика	CISCO SF220-24-K9-EU	MikroTik CRS112-8G-4S-IN
Кількість портів	24 x Ethernet 10/100/1000 Мбіт/сек	8 × Ethernet 4 × SFP Gigabit Ethernet 1 × serial port RJ45
Порти	SFP, Fast Ethernet, Gigabit Ethernet	SFP, Fast Ethernet, Gigabit Ethernet
Flash-пам'ять	100 Мб	16 Мб
Робоча температура	від 0C до 45C	від 0C до 60C
Діапазон вологості (робота)	від 10% до 85%	від 10% до 95%
Живлення	від 100 до 240 В	від 100 до 240 В
Вага	3600 г	950 г
Розміри	(445 x 44 x 236) мм	(200 x 44 x 143) мм
Ціна	2000 грн	3586 грн

Комутатор Cisco SF220-24-K9-EU являє собою мережевий пристрій з 24 портами, які підтримують швидкості передачі даних від 10 до 1000 Мбіт/с. Ці порти містять різні типи підключення, такі як SFP, Fast Ethernet та Gigabit Ethernet, що забезпечує широкий спектр можливостей для підключення різних пристроїв у мережі. З іншого боку, MikroTik CRS112-8G-4S-IN має лише 8 портів, із яких 4 —Gigabit Ethernet, а решта — SFP. Також цей комутатор має один серійний порт RJ45 для підключення до консолі.

Однією з ключових особливостей MikroTik CRS112-8G-4S-IN є підтримка технології Power over Ethernet (PoE), яка дозволяє живити підключені пристрої через Ethernet кабель. Це може бути корисним для підключення пристроїв, які потребують живлення, таких як IP-камери або точки доступу Wi-Fi.

Щодо обсягу пам'яті, Cisco SF220-24-K9-EU має 100 Мб флешпам'яті, тоді як MikroTik CRS112-8G-4S-IN обмежений 16 Мб пам'яті. Це може вплинути на можливості зберігання конфігурацій та програмного забезпечення, і, відповідно, на розширені можливості пристроїв.

Умови експлуатації також є важливим фактором. Cisco SF220-24-K9-EU може працювати при температурі від 0C до 45C та вологості від 10% до 85%, натомість MikroTik CRS112-8G-4S-IN здатний працювати при температурі від 0C до 60C та вологості від 10% до 95%. Це може бути важливим для вибору пристрою залежно від умов його експлуатації.

Обидва комутатори мають однакову можливість живлення від стандартної мережевої розетки, зі значенням напруги від 100 до 240 вольтів, що робить їх універсальними у використанні в різних країнах.

Щодо ваги та розмірів, Cisco SF220-24-K9-EU важить 3600 грамів та має розміри 445 x 44 x 236 міліметрів, тоді як MikroTik CRS112-8G-4S-IN має набагато меншу вагу — лише 950 грамів і менші розміри — 200 x 44 x 143 міліметри. Cisco SF220-24-K9-EU доступний за ціною 2000 гривень, натомість MikroTik CRS112-8G-4S-IN є трохи дорожчим варіантом, коштує 3586 гривень.

Підсумовуючи, обидва комутатори мають свої особливості та призначення. Cisco WS-C2960-24TT-L ідеально підходить для невеликих і середніх мереж, де

потрібне швидке та надійне з'єднання на основі технології Fast Ethernet. MikroTik CRS112-8G-4S-IN відзначається своєю високою пропускною здатністю та розширеними можливостями, що робить його ідеальним вибором для складних мережних середовищ.

Остаточне рішення про вибір між цими двома моделями залежить від конкретних потреб та вимог вашої мережі. Важливо врахувати такі фактори, як розмір мережі, типи підключених пристроїв, потреби у пропускній здатності та рівень безпеки. Після аналізу цих аспектів можна зробити обґрунтований вибір комутатора, який краще відповідає вашим потребам.

Оскільки наша мережа Вінницького технічного фахового коледжу потребує надійного та стабільного з'єднання, а також простоти у використанні та керуванні, ми обираємо комутатор Cisco WS-C2960-24TT-L. Ця модель відома своєю надійністю та швидкістю передачі даних, що дозволить забезпечити ефективну роботу мережі у навчальному закладі. Крім того, Cisco WS-C2960-24TT-L має простий інтерфейс та широкий функціонал, що робить його ідеальним вибором для потреб нашого коледжу.

2.4.3 Підрахунок витрат на реалізацію мережі

Підрахунок витрат на реалізацію мережі — це процес оцінки фінансових витрат, необхідних для побудови та впровадження мережевої інфраструктури. Цей процес включає аналіз вартості мережевого обладнання, програмного забезпечення, послуг з монтажу та налаштування, а також інших витрат, пов'язаних з імплементацією мережі. Метою підрахунку витрат на реалізацію мережі є:

— планування бюджету та ефективне розподілення коштів, щоб уникнути непередбачених витрат;

— раціональний вибір обладнання та послуг на основі точної суми, яка може бути витрачена на реалізацію мережі;

— оцінка рентабельності роботи та визначення його фінансової ефективності;

— прийняття обґрунтованих управлінських рішень та забезпечення успішності роботи в майбутньому.

Для Вінницького технічного фахового коледжу підрахунок витрат на реалізацію мережі є надзвичайно важливим, оскільки дозволяє ефективно розпланувати бюджет та забезпечити створення сучасної та надійної мережевої інфраструктури. Враховуючи обмежені фінансові ресурси навчального закладу, підрахунок витрат допоможе здійснити раціональний вибір обладнання та послуг, забезпечити максимальну ефективність витрат та підвищити загальну продуктивність мережі.

Після аналізу аналогів обрано маршрутизатор Cisco ASR 1001 (PTSC2005) та комутатор Cisco SF220-24-K9-EU для реалізації комп'ютерної мережі з ряду обґрунтованих причин. Маршрутизатор Cisco ASR 1001 відомий своєю надійністю, продуктивністю та широким функціоналом, що відповідає потребам у стабільній та ефективній мережі. Його висока швидкодія та можливості забезпечують необхідний рівень продуктивності та безпеки, що є ключовими для навчального закладу.

Комутатор Cisco SF220-24-K9-EU також ідеально підходить для Вінницького технічного фахового коледжу, маючи достатню кількість портів для підключення різноманітних пристроїв. Він підтримує різні швидкості передачі даних та володіє надійною підтримкою від Cisco, що забезпечить безперебійну роботу мережі у коледжі.

Обираючи продукцію Cisco, Вінницький технічний фаховий коледж може розраховувати на якість, надійність та ефективність мережевого обладнання, що є надзвичайно важливим для навчальних закладів. Ці пристрої гарантують ефективну роботу мережі, що дозволить забезпечити стабільний доступ до інформації та послуг для всіх користувачів коледжу.

Для реалізації мережі необхідно мати в наявності 4 маршрутизатори Cisco ASR 1001 та 6 комутаторів CISCO SF220-24-K9-EU. Така конфігурація дозволить забезпечити надійну та ефективну роботу мережі з урахуванням потреб і

можливостей Вінницького технічного фахового коледжу. Витрати на обладнання для реалізації комп’ютерної мережі наведені в таблиці 2.9

Маршрутизатори Cisco ASR 1001 забезпечать стабільне підключення до мережі Інтернет та інших зовнішніх ресурсів, водночас гарантуючи безпеку та ефективне управління трафіком.

Комутатори CISCO SF220-24-K9-EU забезпечать швидке та надійне підключення внутрішніх мережевих пристроїв, таких як комп'ютери, принтери, сервери та інші, забезпечуючи високу швидкість передачі даних і мінімізуючи можливість виникнення перешкод або збоїв у мережі.

Таблиця 2.9 — Витрати на обладнання для реалізації комп’ютерної мережі

Обладнання	Модель	Вартість за одиницю	Кількість	Загальна вартість
Маршрутизатор	Cisco ASR 1001	7220 грн	4	28880 грн
Комутатор	CISCO SF220-24-K9-EU	2000 грн	6	12000 грн

Для побудови мережі у Вінницькому технічному фаховому коледжі необхідно придбати обладнання в таких кількостях та вартостях: 4 маршрутизатори Cisco ASR 1001 по 7220 грн за одиницю та 6 комутаторів CISCO SF220-24-K9-EU по 2000 грн за одиницю. Загальна вартість маршрутизаторів складе 28880 грн, а комутаторів — 12000 грн.

Загальна вартість необхідного обладнання для побудови мережі у Вінницькому технічному фаховому коледжі складе 40880 грн. Ця сума враховує вартість усіх маршрутизаторів та комутаторів, необхідних для створення надійної та ефективної мережевої інфраструктури у коледжі.

3 РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ КОМП’ЮТЕРНОЇ МЕРЕЖІ

3.1 Призначення IP-адрес

Налаштування IP-адрес є необхідним етапом для забезпечення правильної функціональності комп'ютерних мереж. Цей процес полягає у присвоєнні унікальної адреси кожному пристрою в мережі, що дозволяє ідентифікувати його в контексті Інтернету або локальної мережі. Основна мета налаштування IP-адрес полягає у створенні можливості взаємодії між різними пристроями у мережі, а також у забезпеченні правильної маршрутизації пакетів даних.

Встановлення IP-адрес має вирішальне значення для забезпечення ефективної комунікації між різними мережевими пристроями, включаючи комп'ютери, маршрутизатори, комутатори та інші елементи інфраструктури. Цей процес гарантує, що кожен пристрій має унікальну адресу, за допомогою якої він може бути ідентифікований у мережі. Без належно налаштованих IP-адрес може виникнути конфлікт адрес або неможливість взаємодії пристроїв у мережі.

Процес налаштування IP-адрес може бути виконаний шляхом ручного призначення адрес адміністратором мережі або автоматично за допомогою протоколів динамічної адресації. Призначення IP-адрес передбачає визначення IP-адреси пристрою, маски підмережі та, за потреби, шлюзу за замовчуванням. Загалом, налаштування IP-адрес є фундаментальною складовою будь-якої комп'ютерної мережі, оскільки воно дозволяє забезпечити зв'язок між пристроями та забезпечити ефективну передачу даних у мережі.

Щоб налаштувати IP-адресу, потрібно клацнути правою кнопкою миші на обраному пристрої і вибрати "Desktop" та "IP Configuration". Вікно конфігурації IP-адресації кінцевого пристрою показане на рисунку 3.1. У вікні конфігурації спочатку необхідно ввести IP-адресу кожного пристрою, враховуючи його маску мережі та IP-адресу шлюзу за замовчуванням. Подібно слід налаштувати IP-адреси шлюзів маршрутизаторів.

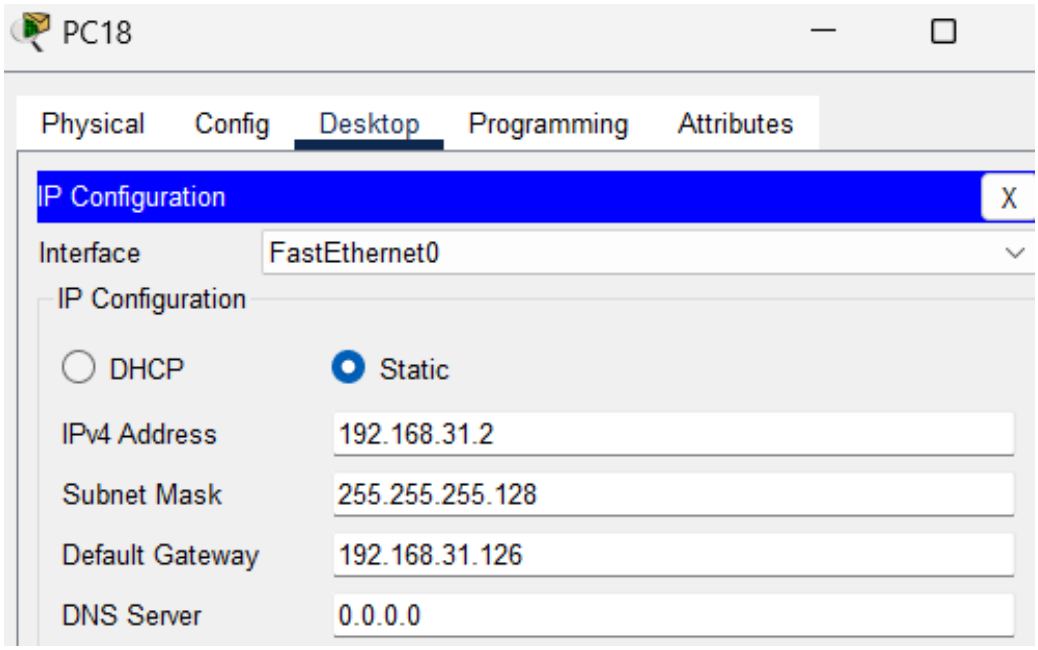

Рисунок 3.1 — Вікно налаштування IP-адресації кінцевого пристрою

3.2 Налаштування протоколу динамічної маршрутизації OSPF

Налаштування протоколу динамічної маршрутизації OSPF важливий аспект створення мережі, оскільки він визначає спосіб, яким маршрутизатори обмінюватимуться інформацією про маршрути в мережі. OSPF (Open Shortest Path First) — це один з найбільш популярних протоколів динамічної маршрутизації, який використовується в комп'ютерних мережах для визначення оптимальних маршрутів до призначення. Він базується на алгоритмі Дейкстри і визначає найкоротший шлях до кожного вузла в мережі, враховуючи метрики маршрутизації, такі як пропускна здатність каналу або відстань [19].

OSPF дозволяє мережевим пристроям обмінюватися інформацією про маршрути та автоматично адаптуватися до змін у топології мережі. Він використовує спеціальні пакети для обміну маршрутною інформацією між маршрутизаторами і визначає найкращі шляхи до кожного призначення.

Однією з особливостей OSPF є його підтримка ієрархічної структури мережі за допомогою областей маршрутизації. Це дозволяє розділити мережу на логічні групи та зменшити навантаження на маршрутизатори, покращуючи швидкість обчислення маршрутів і ефективність мережі в цілому.

Основна мета OSPF полягає в тому, щоб кожен маршрутизатор у мережі міг автоматично знаходити найкращі маршрути до всіх призначень і оновлювати цю інформацію при змінах в мережевій топології. Це дозволяє підтримувати високу доступність і надійність мережі, а також оптимальне використання мережевих ресурсів [19].

Першим кроком у налаштуванні OSPF є визначення областей маршрутизації, які дозволяють групувати маршрутизатори та мережі для ефективного керування ресурсами мережі. Області спрощують процес обчислення маршрутів та зменшують навантаження на мережевий трафік. Потім потрібно вказати, які мережі будуть анонсовані маршрутизаторами в рамках OSPF. Це виконується шляхом налаштування мережевих інтерфейсів маршрутизаторів та визначення їх мережевих адрес та масок підмереж.

Далі необхідно вибрати маршрутизатор, який буде виступати в ролі Designated Router (DR) та Backup Designated Router (BDR) для кожної мережевої області. Це дозволяє оптимізувати процеси обміну інформацією в мережі та зменшити навантаження на мережевий канал. Крім того, налаштовуються параметри маршрутизаторів OSPF, такі як метрики маршрутів, таймери перемикання та інші параметри, які впливають на роботу протоколу.

Після цього проводиться перевірка правильності налаштувань та виявлення можливих проблем з допомогою інструментів моніторингу мережі. Це включає перегляд таблиць маршрутизації, стану з'єднань OSPF та іншу діагностику. Важливо впевнитися, що OSPF правильно працює і обмін інформацією про маршрути відбувається без перешкод.

Крім того, слід розглянути впровадження механізмів безпеки для захисту протоколу OSPF від атак і несанкціонованого доступу до мережевої інформації. Це може включати використання аутентифікації для перевірки легітимності маршрутизаторів, а також налаштування списків доступу для обмеження доступу до протоколу OSPF.

Узагальнюючи, налаштування OSPF включає визначення областей маршрутизації, налаштування мережевих інтерфейсів, вибір DR і BDR,

налаштування параметрів протоколу та перевірку його правильності та безпеки. Відправленням правильно налаштованого OSPF забезпечується ефективна робота мережі та оптимізація обміну маршрутною інформацією.

Перший крок у налаштуванні цього протоколу — це призначення IP-адрес кінцевим пристроям та портам маршрутизаторів. Кінцевим пристроям надаються доступні IP-адреси хоста, а портам маршрутизаторів — останні доступні IP-адреси хоста.

Після призначення IP-адрес починається налаштування протоколу OSPF на маршрутизаторах. Це робиться шляхом входу на обраний маршрутизатор та введення в командному рядку CLI певних команд. Починається цей процес з команди "router ospf [номер маршрутизатора]", де номер маршрутизатора визначається користувачем.

Наступним кроком є введення команди "router-id [x.x.x.x]", де "x" - це номер маршрутизатора, який також визначається користувачем. Ця команда дозволяє визначити ідентифікатор маршрутизатора в мережі.

Після цього налаштовується протокол OSPF для всіх напряму підключених мереж до маршрутизатора. Це робиться за допомогою команди "network [адреса підмережі][зворотна маска] area 0", де адреса підмережі та зворотна маска визначаються відповідно до мережної топології. Ця команда додає підмережі до області маршрутизатора з номером 0, що є стандартним для OSPF. Команди конфігурування OSPF маршрутизатора 5 наведені у лістингу 3.1

Лістинг 3.1 — Команди конфігурування OSPF маршрутизатора 5

```
Router(config)#router ospf 5
Router(config-router)#router-id 5.5.5.5
Router(config-router)#netw 192.168.30.0 0.0.0.127 area 0
Router(config-router)#netw 192.168.30.128 0.0.0.63 area 0
Router(config-router)#netw 192.168.30.192 0.0.0.63 area 0
Router(config-router)#netw 192.168.30.208 0.0.0.3 area 0
```

Для налаштування маршруту за замовчуванням та розсилання цього маршруту використовується протокол OSPF (Open Shortest Path First). Початково за допомогою команди "ip route 0.0.0.0 0.0.0.0 [адреса інтерфейсу маршрутизатора провайдера]" задається маршрут за замовчуванням. Ця команда встановлює, що будь-який трафік, для якого не визначено конкретний маршрут, буде направлятися через вказаний інтерфейс маршрутизатора провайдера.

За допомогою команди "router ospf [номер маршрутизатора]" в командному рядку маршрутизатора вказується номер OSPF процесу. Після цього за допомогою команди "default-information originate" забезпечується розсилання раніше заданого маршруту за замовчуванням за допомогою OSPF. Це означає, що маршрутизатор OSPF поширює інформацію про маршрут за замовчуванням серед інших маршрутизаторів у мережі, щоб всі вони могли користуватися цим маршрутом для направлення трафіку до невідомих мереж. Налаштування та розсилання маршруту за замовчуванням засобами OSPF на центральному маршрутизаторі наведено у лістингу 3.2

Лістинг 3.2 — Налаштування та розсилання маршруту за замовчуванням засобами OSPF на центральному маршрутизаторі

```
Router(config)#ip route 0.0.0.0 0.0.0.0 213.234.10.1
Router(config)#router ospf 4
Router(config-router)#default-information originate
```

3.3 Налаштування технологій NAT та ACL

3.3.1 Налаштування NAT

NAT (Network Address Translation) — це технологія, що використовується в комп'ютерних мережах для перетворення IP-адрес. В основному, ця технологія використовується для трансформації або заміни IP-адрес пакетів даних, що проходять через маршрутизатор або фаєрвол. Основна мета NAT полягає у тому, щоб дозволити пристроям з приватними IP-адресами, які перебувають у локальній

мережі, з'єднуватися з глобальною мережею Інтернет, яка використовує публічні IP-адреси [10].

Коли пакети даних надходять від пристроїв у локальній мережі до маршрутизатора або фаєрволу, що використовують NAT, їхні приватні IP-адреси заміняються на публічні IP-адреси перед виходом на зовнішню мережу. Це дає можливість приватним пристроям з локальної мережі взаємодіяти з іншими пристроями у глобальній мережі, використовуючи лише один публічний IP-адрес.

Однією з ключових переваг використання NAT є ефективне використання публічних IP-адрес, оскільки велика кількість пристроїв може використовувати один і той самий публічний IP-адрес для з'єднання з Інтернетом. Крім того, NAT забезпечує певний рівень безпеки для локальної мережі, адже він приховує внутрішню структуру мережі від зовнішнього світу, знижуючи вразливість до атак з мережі [11].

На практиці NAT функціонує на маршрутизаторах або фаєрволах, які знаходяться на кордоні локальної мережі і Інтернету. Коли пакети даних відправляються з приватних пристроїв у локальній мережі до Інтернету, NAT перетворює їхні приватні IP-адреси на одну або декілька публічних IP-адрес, які надає Інтернет-провайдер.

Коли пристрій у локальній мережі намагається відправити пакет даних на зовнішню мережу, маршрутизатор NAT бере початкову IP-адресу пакета та замінює його на одну зі своїх публічних IP-адрес. Цей процес відбувається перед відправленням пакета на зовнішню мережу [11].

Коли відповідь приходить від зовнішньої мережі, маршрутизатор NAT перевіряє таблицю трансляції, щоб знайти відповідний приватний IP-адрес у своїй локальній мережі і переводить публічну IP-адресу назад у відповідний приватний IP-адрес.

Цей процес дозволяє багатьом пристроям у локальній мережі використовувати одну або декілька публічних IP-адрес для доступу до Інтернету, що зберігає публічні адреси та забезпечує безпеку мережі, приховуючи справжні адреси внутрішніх пристроїв від зовнішнього світу.

Для забезпечення доступу до сервера зовнішнім користувачам мережі ми використовуємо статичний NAT. Цей метод дозволяє перетворювати IP-адресу сервера з внутрішньої мережі на зовнішню IP-адресу, яку можна використовувати в Інтернеті. Після встановлення налаштувань статичного NAT ми перевіряємо правильність його роботи, введенням зовнішньої IP-адреси сервера у веббраузер на кінцевому пристрої користувача. Якщо вебсторінка сервера відображається у браузері, це свідчить про те, що статичний NAT налаштовано правильно і зовнішні користувачі мають доступ до сервера через Інтернет.

Для забезпечення безпечного зв'язку між корпоративною мережею та зовнішньою мережею потрібно налаштувати Network Address Translation (NAT). Перший крок у цьому процесі — призначення зовнішньої IP-адреси для мережі навчального закладу. Наприклад, зовнішня IP-адреса може бути 213.234.10.2 з префіксом 30, яка надається провайдером.

Далі, на маршрутизаторі необхідно налаштувати дефолтний маршрут, вказавши адресу інтерфейсу провайдера як наступний крок. Це дозволить маршрутизатору відправляти пакети на зовнішню мережу через відповідний інтерфейс.

Після цього потрібно визначити типи інтерфейсів для NAT. Є два основних типи: внутрішні (inside) і зовнішні (outside). Внутрішні інтерфейси — це ті, що спрямовують трафік в мережу, а зовнішні — це ті, що спрямовують трафік на зовнішню мережу. Команди конфігурування NAT центрального маршрутизатора наведені у лістингу 3.3

Лістинг 3.3 — Команди конфігурування NAT центрального маршрутизатора

```
Router(config)#interface fa 1/0
Router(config-if)#ip nat outside
Router(config-if)#ex
Router(config)#interface fa 0/0
Router(config-if)#ip nat inside
Router(config-if)#ex
```

```
Router(config)#interface se 2/0
Router(config-if)#ip nat inside
Router(config-if)#ex
Router(config)#interface se 3/0
Router(config-if)#ip nat inside
```

Наступним кроком є створення стандартного access-list. Наприклад, можна використовувати команду ip access-list standart FOR-NAT для цього. Цей access-list дозволяє визначити, які адреси в мережі будуть перекладатися за допомогою NAT.

3.3.2 Налаштування ACL для NAT

ACL (Access Control List) — це набір правил, які використовуються для керування доступом до мережевих ресурсів у комп'ютерних мережах. Основна мета ACL — це обмеження або дозвіл на передачу пакетів даних на основі різних критеріїв, таких як джерело, призначення, протокол, порти та інші параметри [20].

ACL може бути налаштований на маршрутизаторах, комутаторах або фаєрволах і використовується для фільтрації трафіку, який проходить через ці пристрої. Наприклад, за допомогою ACL можна дозволити або заборонити доступ до певних вебсайтів, послуг або мережевих ресурсів для конкретних користувачів або груп користувачів.

Налаштування ACL здійснюється шляхом визначення правил в конфігурації маршрутизатора або фаєрвола. Кожне правило включає критерії фільтрації, такі як IP-адреса джерела та призначення, порти, протоколи тощо, а також дію, яка повинна бути вжита з пакетами, що відповідають цим критеріям - дозволити або заборонити їхню передачу [20].

ACL є важливим інструментом для забезпечення безпеки мережі, обмеження доступу до конфіденційної інформації, управління ресурсами мережі та встановлення правил для призначення пріоритетів для різних типів трафіку.

Вони дозволяють адміністраторам мережі ефективно контролювати трафік і забезпечити безпеку та ефективність мережі.

У мережних налаштуваннях існують два основних види списків доступу, які допомагають у керуванні потоком даних:

— стандартні списки доступу (Standard ACL);

— розширені списки доступу (Extended ACL).

Стандартні списки доступу призначені для фільтрації трафіку, базуючись на джерелі IP-адреси. Стандартні списки доступу працюють на рівні мережевого рівня моделі OSI, що означає, що вони визначають доступ до мережевих ресурсів лише залежно від IP-адреси джерела.

Розширені списки доступу надають більше можливостей для фільтрації трафіку, оскільки можуть враховувати різні критерії, такі як IP-адреса джерела та призначення, порти TCP/UDP, а також протоколи. Розширені списки доступу працюють на рівні мережевого та транспортного рівнів OSI, що дозволяє більш гнучко налаштовувати фільтрацію трафіку.

Обидва типи списків доступу використовуються для реалізації стратегій безпеки мережі, обмеження доступу до ресурсів і керування потоком даних. Вони дозволяють системним адміністраторам точно визначити, який вид трафіку має проходити через мережеві пристрої, а який — блокуватися. Команди конфігурування списків доступу для NAT наведені у лістингу 3.4

Лістинг 3.4 — Команди конфігурування списків доступу для NAT

```
Router(config)#ip access-list stand FOR-NAT
Router(config-std-nacl)#permit 192.168.31.216 0.0.0.3
Router(config-std-nacl)#permit 192.168.31.212 0.0.0.3
Router(config-std-nacl)#permit 192.168.31.208 0.0.0.3
Router(config-std-nacl)#permit 192.168.31.192 0.0.0.15
Router(config-std-nacl)#permit 192.168.31.128 0.0.0.63
Router(config-std-nacl)#permit 192.168.31.0 0.0.0.127
Router(config-std-nacl)#permit 192.168.30.192 0.0.0.63
```

```
Router(config-std-nacl)#permit 192.168.30.128 0.0.0.63
Router(config-std-nacl)#permit 192.168.30.0 0.0.0.127
```

Завершальним етапом є створення правила NAT за допомогою команди ip nat inside source list FOR-NAT interface [назва_інтерфейсу] overload. Це правило вказує маршрутизатору, як перекладати внутрішні адреси в зовнішні, щоб забезпечити доступ до зовнішньої мережі для внутрішніх користувачів.

Щоб перевірити правильність налаштування з комп’ютера мережі навчального закладу виконаємо ping і вкажемо IP-адресу умовного сервера провайдера. Результат перевірки налаштування NAT командою ping показано у лістингу 3.5

Лістинг 3.5 — Результат перевірки налаштування NAT командою ping

```
Router(config)#ip access-list stand FOR-NAT
Router(config-std-nacl)#permit 192.168.31.216 0.0.0.3
Router(config-std-nacl)#permit 192.168.31.212 0.0.0.3
Router(config-std-nacl)#permit 192.168.31.208 0.0.0.3
Router(config-std-nacl)#permit 192.168.31.192 0.0.0.15
Router(config-std-nacl)#permit 192.168.31.128 0.0.0.63
Router(config-std-nacl)#permit 192.168.31.0 0.0.0.127
Router(config-std-nacl)#permit 192.168.30.192 0.0.0.63
Router(config-std-nacl)#permit 192.168.30.128 0.0.0.63
Router(config-std-nacl)#permit 192.168.30.0 0.0.0.127
```

У процесі реалізації комп'ютерної мережі було здійснено налаштування протоколу динамічної маршрутизації OSPF, що допомагає визначати найкоротші шляхи в комп'ютерних мережах для оптимізації передачі даних. Після налаштування протоколу OSPF був встановлений статичний маршрут. Також було налаштовано статичний NAT для забезпечення доступу зовнішнім користувачам до сервера через Інтернет. керування доступом до мережних ресурсів налаштовано ACL.

3.4 Тестування комп’ютерної мережі

Тестування комп'ютерної мережі — це важлива процедура, яка полягає в перевірці різних аспектів її функціонування з метою виявлення можливих проблем і забезпечення надійності та ефективності мережі. Під час тестування перевіряється працездатність мережевих пристроїв, якість з'єднань між ними, а також доступність різних мережевих послуг, таких як доступ до Інтернету, файлових ресурсів тощо.

Основними аспектами, які підлягають тестуванню, є перевірка підключення до мережі для всіх пристроїв, а також взаємозв'язок між ними. Це передбачає, що мережеві пристрої, які мають бути підключені до мережі, повинні бути доступні та функціональні, а комунікація між ними має бути належно налаштована та працювати без перебоїв.

Тестування комп'ютерної мережі допомагає виявити можливі проблеми та недоліки у конфігурації мережевого обладнання або програмного забезпечення. Воно може включати аналіз журналів подій, виявлення та розв'язання конфліктів мережевих адрес, відновлення несправних з'єднань та інші заходи.

Для Вінницького технічного фахового коледжу це особливо важливо, оскільки надійна та ефективна мережа є ключовим елементом забезпечення нормальної діяльності навчального закладу. Вона забезпечує доступ до необхідних ресурсів та Інтернету для всіх користувачів.

3.4.1 Тестування у межах локальної мережі

Для проведення тестування проходження пакетів всередині локальної мережі може використовуватися режим симуляції програми Cisco Packet Tracer. У цьому режимі можна перевіряти статус підключення на кожному мережевому пристрої. Тестування обміну пакетів між кабінетом 107 (1 корпус, фінансово-економічне відділення) та іншими відділеннями за допомогою режиму симуляції програми Cisco Packet Tracer показано на рисунку 3.2

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	PC15	Laptop0	ICMP		0.000	N	0
	Successful	PC15	PC19	ICMP		0.000	N	1
	Successful	PC15	PC8	ICMP		0.000	N	2
	Successful	PC15	PC5	ICMP		0.000	N	3
	Successful	PC15	PC2	ICMP		0.000	N	4

Рисунок 3.2 — Вікно тестування обміну пакетів між кабінетом 107 та іншими відділеннями режиму симуляції програми Cisco Packet Tracer

Тестування обміну пакетів між кабінетом 103 (1 корпус, радіотехнічне відділення) та іншими відділеннями за допомогою режиму симуляції програми Cisco Packet Tracer показано на рисунку 3.3

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	PC19	PC15	ICMP		0.000	N	0
	Successful	PC19	Laptop0	ICMP		0.000	N	1
	Successful	PC19	PC8	ICMP		0.000	N	2
	Successful	PC19	PC0	ICMP		0.000	N	3
	Successful	PC19	PC6	ICMP		0.000	N	4

Рисунок 3.3 — Вікно тестування обміну пакетів між кабінетом 103 та іншими відділеннями режиму симуляції програми Cisco Packet Tracer

Тестування обміну пакетів між адміністрацією (навчальна частина) та іншими відділеннями за допомогою режиму симуляції програми Cisco Packet Tracer показано на рисунку 3.4

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	Laptop0	PC15	ICMP		0.000	N	0
	Successful	Laptop0	PC19	ICMP		0.000	N	1
	Successful	Laptop0	PC0	ICMP		0.000	N	2
	Successful	Laptop0	PC9	ICMP		0.000	N	3
	Successful	Laptop0	PC6	ICMP		0.000	N	4

Рисунок 3.4 — Вікно тестування обміну пакетів між адміністрацією та іншими відділеннями режиму симуляції програми Cisco Packet Tracer

Тестування обміну пакетів між кабінетом 201 (2 корпус, відділення транспортних технологій) та іншими відділеннями за допомогою режиму симуляції програми Cisco Packet Tracer показано на рисунку 3.5

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	PC8	PC14	ICMP		0.000	N	0
	Successful	PC8	PC15	ICMP		0.000	N	1
	Successful	PC8	PC7	ICMP		0.000	N	2
	Successful	PC8	PC1	ICMP		0.000	N	3
	Successful	PC8	PC12	ICMP		0.000	N	4

Рисунок 3.5 — Вікно тестування обміну пакетів між кабінетом 201 та іншими відділеннями режиму симуляції програми Cisco Packet Tracer

Тестування обміну пакетів між кабінетом 216 (2 корпус, комп’ютерне відділення) та іншими відділеннями за допомогою режиму симуляції програми Cisco Packet Tracer показано на рисунку 3.6

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	PC0	PC5	ICMP		0.000	N	0
	Successful	PC0	PC11	ICMP		0.000	N	1
	Successful	PC0	PC14	ICMP		0.000	N	2
	Successful	PC0	PC16	ICMP		0.000	N	3
	Successful	PC0	PC12	ICMP		0.000	N	4
	Successful	PC0	PC4	ICMP		0.000	N	5

Рисунок 3.6 — Вікно тестування обміну пакетів між кабінетом 216 та іншими відділеннями режиму симуляції програми Cisco Packet Tracer

3.4.2 Тестування доступу до глобальної мережі

Для перевірки з'єднання до Інтернету з локальної мережі можна використовувати команду "ping". Ця команда дозволяє визначити, чи є доступність до конкретного пристрою за його IP-адресою. Наприклад, введення команди "ping <IP-адреса>" дозволяє перевірити, чи можна встановити зв'язок з цим пристроєм. Результатом виконання команди буде відповідь про доступність пристрою та час, який пройшов до отримання відповіді.

Тестування обміну пакетів між кабінетом 107 (1 корпус, фінансово-економічне відділення) та мережею Інтернет за допомогою команди ping наведено у лістингу 3.6

Лістинг 3.6 — Тестування обміну пакетів між кабінетом 107 та мережею Інтернет

```
C:\>ping 213.234.20.2
Pinging 213.234.20.2 with 32 bytes of data:
Reply from 213.234.20.2: bytes=32 time=23ms TTL=125
Reply from 213.234.20.2: bytes=32 time=26ms TTL=125
Reply from 213.234.20.2: bytes=32 time=33ms TTL=125
Reply from 213.234.20.2: bytes=32 time=26ms TTL=125
Ping statistics for 213.234.20.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 23ms, Maximum = 33ms, Average = 27ms
```

Результат тестування обміну пакетів між кабінетом 103 (1 корпус, радіотехнічне відділення) та мережею Інтернет за допомогою команди ping наведено у лістингу 3.7

Лістинг 3.7 — Тестування обміну пакетів між кабінетом 103 та мережею Інтернет за допомогою команди ping

```
Router(config)#ip access-list stand FOR-NAT
Router(config-std-nacl)#permit 192.168.31.216 0.0.0.3
Router(config-std-nacl)#permit 192.168.31.212 0.0.0.3
Router(config-std-nacl)#permit 192.168.31.208 0.0.0.3
Router(config-std-nacl)#permit 192.168.31.192 0.0.0.15
Router(config-std-nacl)#permit 192.168.31.128 0.0.0.63
Router(config-std-nacl)#permit 192.168.31.0 0.0.0.127
Router(config-std-nacl)#permit 192.168.30.192 0.0.0.63
```

Router(config-std-nacl)#permit 192.168.30.128 0.0.0.63
Router(config-std-nacl)#permit 192.168.30.0 0.0.0.127

Також можна провести тестування за допомогою режиму симуляції програми Cisco Packet Tracer, перевіривши стан підключення на кожному пристрої мережі. Тестування обміну пакетів між адміністрацією (навчальна частина), кабінетом 201 (2 корпус, відділення транспортних технологій), кабінетом 205 (2 корпус, відділення електроенергетики та електромеханіки) та кабінетом 216 (2 корпус, комп'ютерне відділення) до мережі Інтернет за допомогою режиму симуляції Cisco Packet Tracer наведено на рисунку 3.7

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Laptop0	Server0	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC8	Server0	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC5	Server0	ICMP		0.000	N	2	(edit)	(delete)
	Successful	PC0	Server0	ICMP		0.000	N	3	(edit)	(delete)

Рисунок 3.7 — Вікно тестування обміну пакетів між адміністрацією, кабінетами 201, 205, 216 та мережею Інтернет режиму симуляції Cisco Packet Tracer

Тепер потрібно спробувати зайти в Інтернет з комп'ютера, що знаходиться у кабінеті 216 (2 корпус, комп'ютерне відділення). В нашій мережевій схемі Інтернет емулюється за допомогою сервера з публічною IP-адресою та власною вебсторінкою на цьому сервері. Для входу на цю сторінку потрібно відкрити веббраузер. Сторінка входу у веббраузер з кінцевого пристрою у мережі показана на рисунку 3.8

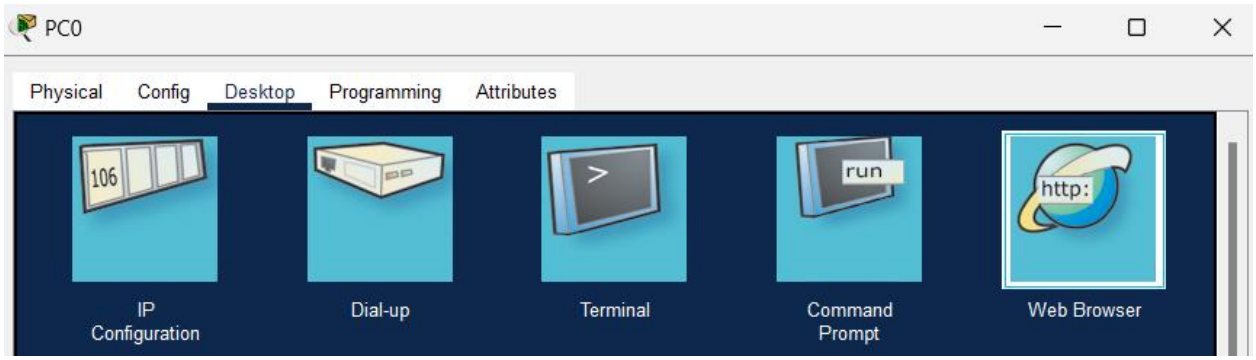

Рисунок 3.8 — Сторінка входу у веббраузер з кінцевого пристрою

Далі відкриваємо веббраузер і вводимо IP-адресу нашого сервера, який емулює Інтернет, в адресному рядку. Вхід на сторінку вебсервера по IP-адресі сервера показаний на рисунку 3.9

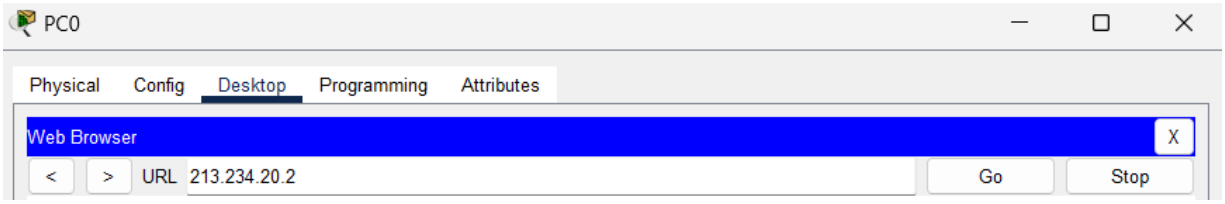

Рисунок 3.9 — Вхід на сторінку вебсервера по IP-адресі сервера

При успішному отриманні доступу до вебсторінки, яка розташована на сервері, ми можемо відкривати і переглядати вебсторінки. Результат перегляду вебсторінки на сервері з кінцевого пристрою показаний на рисунку 3.10

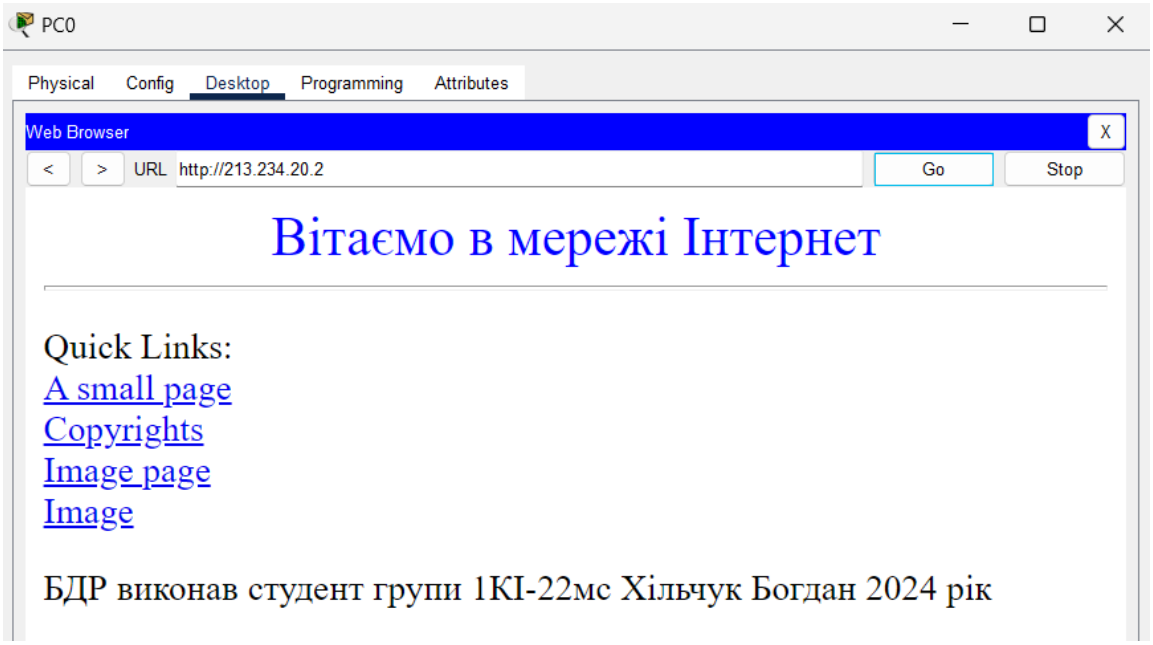

Рисунок 3.10 — Результат перегляду вебсторінки на сервері з кінцевого пристрою

Комп'ютерна мережа Вінницького технічного фахового коледжу була успішно протестована. У ході тестування було проведено перевірку обміну пакетами між кабінетами та іншими відділеннями за допомогою режиму симуляції програми Cisco Packet Tracer та команди "ping". В результаті виявлено, що наша система забезпечує надійний обмін даними між всіма вузлами мережі.

ВИСНОВКИ

На основі проведеного дослідження було спроєктовано та реалізовано комп’ютерну мережу для Вінницького технічного фахового коледжу. В ході аналізу були розглянуті сучасні технології та принципи побудови мереж, враховані потреби навчального закладу та вимоги до ефективності й безпеки. Після оцінки робочого процесу та потреб користувачів було визначено необхідний набір протоколів та обладнання для оптимального функціонування мережі.

Завдяки застосуванню передових технологій, таких як OSPF, NAT та ACL вдалося створити модель мережі, яка відповідає вимогам навчального закладу. Розроблена логічна топологія мережі дозволяє забезпечити ефективний обмін даними між різними корпусами та адміністративним підрозділом.

Загальна архітектура мережі була побудована з урахуванням потреб користувачів та особливостей навчального процесу, що дозволить забезпечити стабільну та безпечну роботу мережі у майбутньому. Використання протоколу OSPF для маршрутизації в межах локальної мережі забезпечить оптимальний обмін даними та підвищить її ефективність.

Розроблена комп’ютерна мережа для Вінницького технічного фахового коледжу відповідає сучасним вимогам та потребам навчального закладу, забезпечуючи надійний та ефективний обмін інформацією та забезпечуючи безпеку та доступність сервісів для користувачів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Комп’ютерна мережа Вінницького технічного фахового коледжу / Б. С. Хільчук, С. М. Захарченко // Матеріали конференції Молодь в науці: дослідження, проблеми, перспективи (МН-2024) факультету інформаційних технологій та комп'ютерної інженерії. Вінниця 2024 р. [Електронний ресурс]. Режим доступу: https://conferences.vntu.edu.ua/index.php/mn/mn2024/paper/view/21064/0

2. Комп’ютерні мережі / Азаров О.Д., Захарченко С.М. та інш. Вінниця, ВНТУ, 2020. — 377 с.

3. Модель OSI [Електронний ресурс]. Режим доступу: https://javarush.com/ua/quests/lectures/ua.questservlets.level08.lecture01

4. Комп’ютерні мережі / Коробейнікова Т. І., Захарченко С. М. Львів, Видавництво Львівської політехніки, 2022. — 228с.

5. TCP/IP проти моделі OSI — різниця між ними [Електронний ресурс]. Режим доступу: https://www.guru99.com/uk/difference-tcp-ip-vs-osi-model.html

6. IP-адреса [Електронний ресурс]. Режим доступу: https://uk.wikipedia.org/wiki/IP-адреса

7. IPv4 і IPv6: основні відмінності, вплив на хостинг і доступність сайту [Електронний ресурс]. Режим доступу: https://hyperhost.ua/info/uk/ipv4-i-ipv6-osnovni-vidminnosti-vpliv-na-xosting-i-dostupnist-saitu

8. Комп’ютерні мережі / Азаров О.Д., Захарченко С.М. та інш. Вінниця, ВНТУ, 2013. — 370 с.

9. Опис технології Fast Ethernet [Електронний ресурс]. Режим доступу: https://deps.ua/ua/knowegable-base/reference-information/opisanie-tehnologii-fast-ethernet.html

10. Загальні відомості та термінологія протоколу OSPF [Електронний ресурс]. Режим доступу: https://web.posibnyky.vntu.edu.ua/fitki/3yarovijk_komp_merezhi/4.9.1.html

11. NAT операторського класу [Електронний ресурс]. Режим доступу: https://iitd.com.ua/nat-operatorskogo-klassa/

12. Що таке топологія мережі: типи та її робота [Електронний ресурс]. Режим доступу: https://uk.fmuser.net/content/?21055.html

13. Топологія мережі [Електронний ресурс]. Режим доступу: https://pidru4niki.com/12631113/bankivska_sprava/topologiya_merezhi

14. Маршрутизатори локальної мережі [Електронний ресурс]. Режим доступу: https://infotel.ua/aktivne-merezheve-obladnannya/marshrutizatori-lokalnoi-merezhi

15. Роутер: принцип роботи, види, будова, порядок підключення [Електронний ресурс]. Режим доступу: https://what.com.ua/royter-princip-roboti-vidi/

16. Cisco ASR 1000 Series Aggregation Services Routers Data Sheet [Електронний ресурс]. Режим доступу: https://www.cisco.com/c/en/us/products/collateral/routers/asr-1000-series-aggregation-services-routers/datasheet-c78-731632.html

17. RB4011iGS+RM [Електронний ресурс]. Режим доступу: https://mikrotik.com/product/rb4011igs_rm

18. Застосування комутаторів [Електронний ресурс]. Режим доступу: https://web.posibnyky.vntu.edu.ua/fitki/3yarovijk_komp_merezhi/2.4.5.html

19. Налаштування роботи протоколу маршрутизації OSPF [Електронний ресурс]. Режим доступу: https://e-tk.lntu.edu.ua/pluginfile.php/19445/mod_resource/content/0/Практична%20робота%2011.%20Налаштування%20роботи%20протоколу%20маршрутизації%20OSPF.pdf

20. Access control list [Електронний ресурс]. Режим доступу: https://uk.wikipedia.org/wiki/Access_control_list

ДОДАТОК А

Технічне завдання

Міністерство освіти і науки України
Вінницький національний технічний університет
Факультет інформаційних технологій та комп’ютерної інженерії
Кафедра обчислювальної техніки

ЗАТВЕРДЖУЮ
Завідувач кафедри ОТ
проф., д.т.н.. Азаров О.Д.
06 травня 2024 р.

ТЕХНІЧНЕ ЗАВДАННЯ
на виконання бакалаврської дипломної роботи
«Комп’ютерна мережа Вінницького технічного фахового коледжу»
08-54.БДР.024.00.000 ПЗ

Науковий керівник: к.т.н., проф. каф. ОТ
_____ Захарченко С. М.

Студент групи 1КІ-22мс
 Хільчук Б. С.

м. Вінниця — 2024

1 Підстава для використання бакалаврської дипломної роботи (БДР)

1.1 Актуальність розробки полягає у потребі модернізації і підвищення ефективності інфраструктури комп’ютерної мережі Вінницького технічного фахового коледжу. З урахуванням швидкої динаміки технологічного розвитку та зростання вимог до забезпечення якості навчального процесу, важливо мати сучасну та надійну інфраструктуру мережі, яка забезпечить стабільну роботу та доступність ресурсів для викладачів і студентів.

1.2 Головним завданням розробки є створення сучасної, надійної та ефективної комп'ютерної мережі для Вінницького технічного фахового коледжу.

1.3 Наказ про затвердження теми бакалаврської дипломної роботи.

2 Мета і призначення БДР

2.1 Мета роботи полягає у вдосконаленні шляхом оптимізації логічної структури та конфігурації комп'ютерної мережі Вінницького технічного фахового коледжу.

2.2 Призначення розробки полягає у виконанні бакалаврської дипломної роботи, за якою буде наступне впровадження та подальший розвиток мережі.

3 Вихідні дані для виконання БДР

3.1. Опис наявної комп'ютерної інфраструктури Вінницького технічного фахового коледжу, включаючи наявні мережеві з'єднання, обладнання та програмне забезпечення.

3.2 Огляд і аналіз сучасних технологій та протоколів мережевого з'єднання, які можуть бути використані для реалізації нової мережі.

3.3 Визначення вимог до мережевого обладнання та програмного забезпечення, які відповідають потребам коледжу і забезпечують високий рівень продуктивності та надійності.

3.4 Планування структури та топології мережі, включаючи розміщення мережевих вузлів, сегментів і областей зв'язку.

3.5 Оцінка вартості і вибір оптимальних рішень з погляду ефективності та вартості у впровадженні нової комп'ютерної мережі.

3.6 Розробка плану впровадження та тестування нової мережі з урахуванням мінімізації перебоїв у роботі та забезпечення плавного переходу на нову інфраструктуру.

4 Вимоги до виконання БДР

Головна вимога полягає в створенні ефективної та надійної комп'ютерної мережі, яка забезпечить всі потреби Вінницького технічного фахового коледжу.

5 Етапи БДР та очікувані результати

Етапи розробки БДР та очікувані результати наведено у Таблиці А.1

Таблиця А.1 — Етапи БДР

№ етапу	Назва етапу	Термін виконання		Очікувані результати
		Початок	Кінець	
1	Постановка задачі	12.03.24	16.03.24	Розділ 1
2	Аналіз технологій для створення комп’ютерних мереж	17.03.24	28.03.24	Розділ 1
3	Аналіз та обґрунтування вибору технологій	29.03.24	09.04.24	Розділ 2
4	Реалізація комп’ютерної мережі	10.04.24	19.04.24	Розділ 3
5	Тестування комп’ютерної мережі	20.04.24	26.04.24	Розділ 4
6	Підготовка тезових матеріалів для публікації	27.04.24	28.04.24	Тези
7	Оформлення пояснювальної записки та демонстраційної презентації для доповіді	29.04.24	17.05.24	ПЗ, презентація
8	Підготовка супровідної документації, перевірка відповідності нормам та проходження тесту на плагіат	18.05.24	26.05.24	ПЗ, презентація

6 Матеріали, що подаються до захисту БДР

До захисту подаються: пояснювальна записка БДР, ілюстративні матеріали, протокол попереднього захисту БДР на кафедрі, відгук наукового керівника, анотації до БДР українською та іноземною мовами, довідка про відповідність оформлення БДР чинним вимогам.

7 Порядок контролю виконання та захисту БДР

Виконання етапів графічної та розрахункової документації БДР контролюється науковим керівником згідно зі встановленими термінами. Захист БДР відбувається на засіданні Екзаменаційної комісії, затвердженої наказом ректора.

8 Вимоги до оформлювання та порядок виконання БДР

8.1 При оформлюванні 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»;

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

— методичні вказівки до виконання бакалаврських кваліфікаційних робіт для студентів спеціальності 123 «Комп’ютерна інженерія» (освітня програма «Комп’ютерна інженерія») — кафедра обчислювальної техніки, ВНТУ 2023.

8.2 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

Конфігураційний файл головного маршрутизатора Router4

Лістинг Б.1 — Конфігураційний файл головного маршрутизатора Router4

```
hostname Router
ip cef
no ipv6 cef
interface FastEthernet0/0
ip address 192.168.31.209 255.255.255.252
ip nat inside
duplex auto
speed auto
interface FastEthernet1/0
ip address 213.234.10.2 255.255.255.252
ip nat outside
duplex auto
speed auto
interface Serial2/0
ip address 192.168.31.217 255.255.255.252
ip nat inside
clock rate 2000000
interface Serial3/0
ip address 192.168.31.213 255.255.255.252
ip nat inside
interface FastEthernet4/0
no ip address
shutdown
interface FastEthernet5/0
no ip address
shutdown
```

```
router ospf 4
router-id 4.4.4.4
log-adjacency-changes
passive-interface FastEthernet1/0
network 192.168.31.208 0.0.0.3 area 0
network 192.168.31.212 0.0.0.3 area 0
network 192.168.31.216 0.0.0.3 area 0
default-information originate
router rip
ip nat inside source list FOR-NAT interface FastEthernet1/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 213.234.10.1
ip flow-export version 9
ip access-list standard FOR-NAT
permit 192.168.31.216 0.0.0.3
permit 192.168.31.212 0.0.0.3
permit 192.168.31.208 0.0.0.3
permit 192.168.31.192 0.0.0.15
permit 192.168.31.128 0.0.0.63
permit 192.168.31.0 0.0.0.127
permit 192.168.30.192 0.0.0.63
permit 192.168.30.128 0.0.0.63
permit 192.168.30.0 0.0.0.127
line con 0
line aux 0
line vty 0 4
login
end
```

ДОДАТОК В

Конфігураційний файл комутатора SWITCH9

Лістинг В.1 — Конфігураційний файл комутатора SWITCH9

```
Current configuration : 1080 bytes
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname Switch
spanning-tree mode pvst
spanning-tree extend system-id
interface FastEthernet0/1
interface FastEthernet0/2
interface FastEthernet0/3
interface FastEthernet0/4
interface FastEthernet0/5
interface FastEthernet0/6
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
interface FastEthernet0/11
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
```

```
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
interface GigabitEthernet0/1
interface GigabitEthernet0/2
interface Vlan1
 no ip address
 shutdown
line con 0
line vty 0 4
 login
line vty 5 15
 login
end
```

ДОДАТОК Г

Інформація про мережі комп’ютера PC5

Лістинг Г.1 — Інформація про мережі комп’ютера PC5

FastEthernet0Connection:(default port)

Connection-specific DNS Suffix..:

Link-local IPv6 Address.....: FE80::250:FFF:FEED:B070

IPv6 Address.....: ::

IPv4 Address.....: 192.168.30.129

Subnet Mask.....: 255.255.255.192

Default Gateway.....: ::

192.168.30.190

BluetoothConnection:

Connection-specific DNS Suffix..:

Link-local IPv6 Address.....: ::

IPv6 Address.....: ::

IPv4 Address.....: 0.0.0.0

Subnet Mask.....: 0.0.0.0

Default Gateway.....: ::

0.0.0.0

ДОДАТОК Д

Інформація про приєднану мережу сервера №0

Лістинг Д.1 — Інформація про приєднану мережу сервера №0

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix..:

Link-local IPv6 Address.....: FE80::260:2FFF:FED1:CEB3

IPv6 Address.....: ::

IPv4 Address.....: 213.234.20.2

Subnet Mask.....: 255.255.255.252

Default Gateway.....: ::

213.234.20.1

ДОДАТОК Е

Логічна топологія мережі Вінницького технічного фахового коледжу

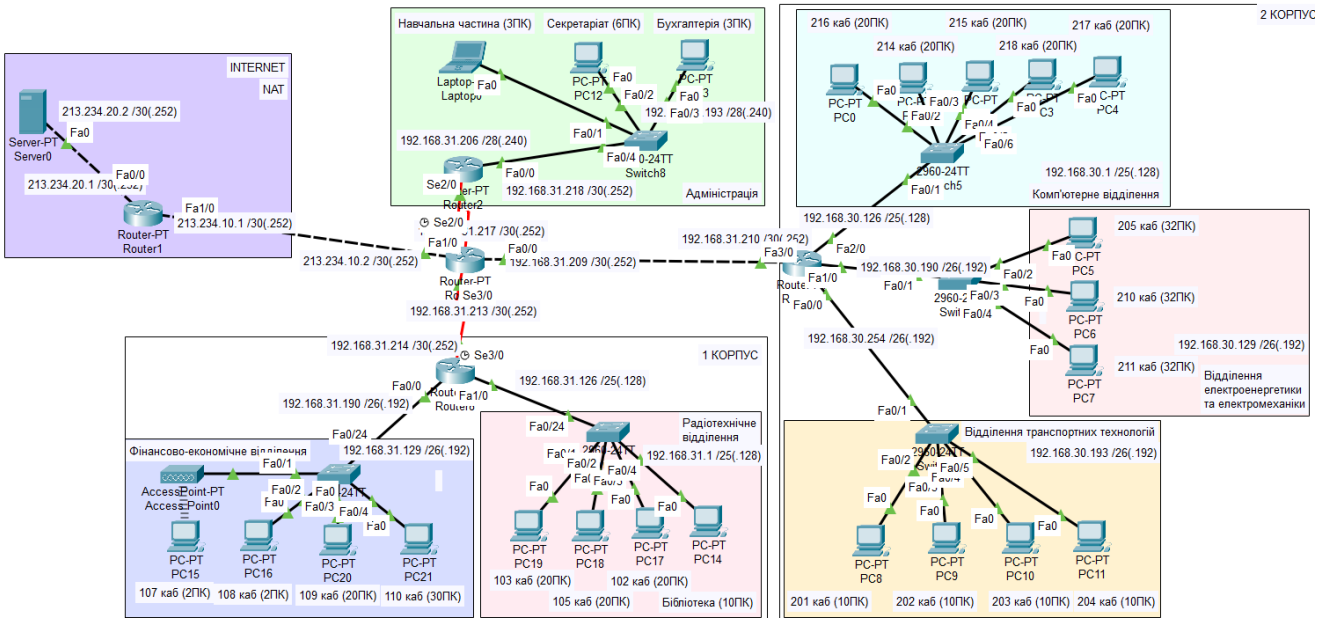

Рисунок Е.1 — Логічна топологія мережі Вінницького технічного фахового коледжу

ДОДАТОК Ж

ПРОТОКОЛ ПЕРЕВІРКИ БАКАЛАВРСЬКОЇ ДИПЛОМНОЇ РОБОТИ НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: «Комп'ютерна мережа Вінницького технічного фахового коледжу»
Тип роботи: бакалаврська дипломна робота
Підрозділ кафедра обчислювальної техніки

Показники звіту подібності Unicheck

Оригінальність _____97,7%_____ Схожість _____2,3%_____

Аналіз звіту подібності (відмітити потрібне):

✓ Запозичення, виявлення 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 виконання автором. Роботу направити на розгляд експертної комісії кафедри.
□ 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 Unicheck щодо роботи.

Автор роботи _____ Хільчук Б. С.
(підпис) (прізвище, ініціали)

Керівник роботи _____ Захарченко С. М.
(підпис) (прізвище, ініціали)