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

БАКАЛАВРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Комп'ютерна мережа для школи-ліцею №1 міста Вінниці»

08-54.БКР.022.00.000 ПЗ

Виконав: студент 4 курсу, групи 2КІ-21б
спеціальності 123 — «Комп'ютерна інженерія»
освітня програма — «Комп'ютерна інженерія»
Белан С.Ю. _____

Керівник к.т.н., проф. каф. ОТ
Захарченко С.М. _____

Рецензент д.ф.н., доц. каф. МБІС
Салієва О.В. _____

Допущено до захисту
Завідувач кафедри ОТ
д.т.н., проф. Азаров О. Д.
«16» 06 2025 р.

Вінниця ВНТУ – 2025 рік

Вінницький національний технічний університет

Факультет інформаційних технологій та комп'ютерної інженерії

Кафедра обчислювальної техніки

Освітньо—кваліфікаційний рівень бакалавр

Галузь знань — 12 Інформаційні технології

Спеціальність — 123 Комп'ютерна інженерія

Освітня програма — Комп'ютерна інженерія

ЗАТВЕРДЖУЮ

Завідувач кафедри ОТ

д.т.н., проф. Азаров О. Д.

«21» березня 2025 р.

З А В Д А Н Н Я

НА БАКАЛАВРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Белану Станіславу Юрійовичу

1 Тема роботи: Комп'ютерна мережа для школи-ліцею №1 міста Вінниці, керівник роботи Захарченко Сергій Михайлович, к.т.н., професор кафедри ОТ, затверджено наказом вищого навчального закладу від «20» березня 2025 року №97.

2 Термін подання студентом роботи 13 травня 2025 р.

3 Вихідні дані до роботи: призначення — проєктування комп'ютерних мереж; основні підтримувані функції — передача пакетів між робочими станціями.;

4 Зміст розрахунково-пояснювальної записки: вступ; аналіз існуючих прототипів та визначення вимог до створюваної системи; обгрунтування структури та принципів роботи системи; розробка й тестування апаратно-програмної системи; висновки.

5 Перелік ілюстративного матеріалу:логічна топологія корпусів молодших та старших класів, структурна схема мережі школи-ліцею №1.

6 Консультанти розділів роботи приведені в таблиці 1

Таблиця 1 — Консультанти роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1-3	к.т.н., проф. каф. ОТ Захарченко С.М.	21.03.25	13.05.25
Нормоконтроль	ас.. каф. ОТ Швець С. І.	04.06.25	30.05.25

7. Дата видачі завдання 21.03.2025 р.

8. Календарний план приведений в таблиці 2.

Таблиця 2 — Календарний план

№ з/п	Назва етапів дипломної Роботи	Строк виконання	Підпис
1	Постановка задачі роботи	21.03.25	вик.
2	Аналіз технологій для створення комп'ютерних мереж	21.03.25— 30.03.25	вик.
3	Аналіз та обгрунтування вибору технологій	21.03.25— 30.03.25	вик.
4	Реалізація та тестування комп'ютерної мережі	31.03.25— 13.04.25	вик.
5	Підготовка тезових матеріалів для публікації	14.04.25— 27.04.25	вик.
7	Оформлення пояснювальної записки та демонстраційної презентації для доповіді	28.04.25— 11.05.25	вик.
8	Перевірка якості виконання бакалаврської кваліфікаційної роботи та усунення недоліків та проходження тесту на плагіат	05.06.25	вик.

Студент Станіслав БЕЛАН

Керівник роботи к.т.н., проф. Сергій ЗАХАРЧЕНКО

АНОТАЦІЯ

УДК 004.7

Белан С. Ю. Комп'ютерна мережа для школи-ліцею №1 міста Вінниці. Бакалаврська дипломна робота зі спеціальності 123 — Комп’ютерна інженерія, освітня програма — Комп’ютерна інженерія. Вінниця: ВНТУ, 2025. 92 с.

На укр. мові. Бібліогр. назв: 25, рис.: 18, табл.: 20;

У цій бакалаврській кваліфікаційній роботі здійснено комплексний аналіз сучасних технологій проєктування та вдосконалення комп’ютерних мереж для закладів освіти. Розглянуто базові мережеві моделі OSI та TCP/IP, а також технології локальних мереж (Ethernet, Wi-Fi), методи IP-адресації у межах протоколу IPv4. Окрему увагу приділену багаторівневій архітектурі мережі, що включає реалізацію віртуальних локальних мереж (VLAN) з централізованим управлінням за допомогою протоколу VTP.Розглянуто принципи трансляції мережевих адрес (NAT) як засобу оптимізації використання обмеженого IPv4-простору та підвищення рівня безпеки при доступі до зовнішніх ресурсів. Проаналізовано особливості динамічного протоколу маршрутизації OSPF, придатного для ієрархічної організації мережевої інфраструктури та забезпечення масштабованості.

На основі аналізу потреб школи та вимог до безпеки побудовано проєкт мережі, що включає розробку схеми IP-адресації, вибір маршрутизаторів і комутаторів з урахуванням підтримки VLAN, налаштування базових параметрів обладнання та реалізацію логічного розмежування зон. Значна увага приділена питанням інформаційної безпеки — впроваджено списки контролю доступу (ACL), налаштовано захищений протокол доступу до обладнання (SSH), реалізовано міжмережевий екран та VPN-доступ із фільтрацією.

Ключові слова: комп’ютерна мережа, навчальний заклад, IP-адресація, VLAN, VTP, NAT, OSPF, ACL, SSH, VPN, інформаційна безпека

ABSTRACT

UDC 004.7

Belan S.Y. Computer network for the school-lyceum №1 in Vinnytsia. Bachelor's thesis in specialty 123 - Computer Engineering, educational program - Computer Engineering. Vinnytsia: VNTU, 2025. 92 p.

In Ukrainian. Bibliogr. titles: 25, Figures: 18, Table: 20;

This bachelor's thesis provides a comprehensive analysis of modern technologies for designing and improving computer networks for educational institutions. The basic network models OSI and TCP/IP, as well as local area network technologies (Ethernet, Wi-Fi), IP addressing methods within the IPv4 protocol are considered. Particular attention is paid to the multi-level network architecture, including the implementation of virtual local area networks (VLANs) with centralized management using the VTP protocol.The principles of network address translation (NAT) as a means of optimizing the use of limited IPv4 space and increasing security when accessing external resources are considered. The features of the dynamic OSPF routing protocol, suitable for hierarchical organization of network infrastructure and scalability, are analyzed.

Based on the analysis of the school's needs and security requirements, a network design is built, including the development of an IP addressing scheme, the selection of routers and switches with VLAN support, the configuration of basic equipment parameters, and the implementation of logical zone delimitation. Considerable attention is paid to information security issues: access control lists (ACLs) are implemented, a secure hardware access protocol (SSH) is configured, and firewall and VPN access with filtering are implemented.

Keywords: computer network, educational institution, IP addressing, VLAN, VTP, NAT, OSPF, ACL, SSH, VPN, information security.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ, ТЕРМІНІВ

OSPF — Open Shortest Path First

TCP/IP — Transmission Control Protocol/Internet Protocol

LAN — Local Area Network

VLAN — Virtual Local Area Network

VPN — Vitual Private Network

VTP — VLAN Trunking Protocol

IPv4 — Internet Protocol Version 4

IPv6 — Internet Protocol Version 6

NAT — Network Address Translation

EIGRP — Enhanced Interior Gateway Routing Protocol

RIP — Routing Information Protocol

DHCP — Dynamic Host Configuration Protocol

ACL — Access Control List

SSH — Secure Shell

FW — Firewall

Ethernet — Ethernet Technology

Wi-Fi — Wireless Fidelit

ЗМІСТ

ВСТУП

Комп’ютерні мережі стали невід’ємною частиною сучасного освітнього процесу, зокрема в закладах середньої освіти, таких як школи-ліцеї. Їх наявність забезпечує зручний обмін інформацією, спільне користування ресурсами, інтеграцію навчальних платформ, а також ефективну організацію як навчального процесу, так і адміністративної діяльності.

У випадку школи-ліцею м. Вінниці важливими характеристиками комп’ютерної мережі є стабільність, безпека, швидкість передачі даних, підтримка віддаленого доступу, а також можливість централізованого керування. Така мережа має забезпечити ефективне використання освітніх онлайн-ресурсів, системи управління навчанням (LMS), а також інтеграцію мультимедійних засобів навчання.

Актуальність теми полягає в тому, що грамотно спроєктована та оптимізована комп’ютерна мережа є необхідною умовою ефективного функціонування сучасного навчального закладу. Вона дозволяє підвищити якість освіти, спростити доступ до навчальних матеріалів і забезпечити єдиний інформаційний простір для учнів і вчителів.

Мета дипломної роботи є створення оптимізованої логічної структури та конфігурації комп’ютерної мережі школи-ліцею м. Вінниці з урахуванням реальних потреб та існуючої інфраструктури.

Для досягнення мети необхідно виконати такі **завдання**:

— провести аналіз сучасних технологій побудови шкільних комп’ютерних мереж;

— розробити логічну структуру мережі для школи-ліцею м. Вінниці;

— обґрунтувати вибір мережевого обладнання для реалізації проєкту;

— виконати налаштування активного обладнання згідно з обраною топологією;

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

Об’єктом дослідження є процес побудови та функціонування локальної комп’ютерної мережі у навчальному закладі.

Предметом дослідження є логічна структура та конфігурація комп’ютерної мережі школи-ліцею м. Вінниці.

Методи дослідження, що використовуються в роботі, включають аналіз наукової та технічної літератури з тематики комп’ютерних мереж; моделювання мережевої інфраструктури в середовищі Cisco Packet Tracer; методи тестування працездатності мережевих рішень у віртуальному середовищі.

Основні результати роботи були представлені у вигляді тези та опубліковані в наукових матеріалах конференції [1].

1 АНАЛІЗ ТЕХНОЛОГІЙ ДЛЯ СТВОРЕННЯ КОМП'ЮТЕРНИХ МЕРЕЖ

1.1 Основні мережеві моделі: OSI та TCP/IP

У сфері комп'ютерних мереж надзвичайно важливим є стандартизований підхід до організації процесів передавання даних між пристроями. Для забезпечення такої уніфікації були розроблені концептуальні мережеві моделі, які описують принципи функціонування мережі, її структуру та розподіл функцій між окремими компонентами. Серед найбільш впливових моделей виділяють еталонну модель OSI та модель протоколів TCP/IP. Обидві моделі використовуються для розуміння мережевої архітектури, побудови стандартів та протоколів, а також для практичного аналізу роботи мереж.

Модель OSI (Open Systems Interconnection Reference Model) була запропонована Міжнародною організацією зі стандартизації (ISO) в 1983 році як основа для побудови відкритих систем, що можуть взаємодіяти між собою незалежно від їх реалізації. Модель є теоретичною концепцією, яка визначає ієрархічну структуру з сімох послідовних рівнів, кожен з яких виконує визначені функції та взаємодіє з сусідніми рівнями за чітко встановленими правилами, що наведені у таблиці 1.1 [2].

Основна мета моделі OSI полягає у формалізації взаємодії між різними мережевими системами, забезпеченні взаємної сумісності обладнання і програмного забезпечення різних виробників, а також у полегшенні процесу проєктування та впровадження нових технологій у сфері телекомунікацій.

Кожен рівень моделі OSI має свою чітко визначену функціональність; спирається на послуги нижчого рівня; надає сервіси рівню, що знаходиться вище.

Цей принцип часто називають принципом модульності. Завдяки йому кожен рівень може бути розроблений, оптимізований або оновлений незалежно від інших, що сприяє гнучкості та масштабованості мережевих рішень [3].

Рівні моделі OSI та їх функції:

Фізичний рівень відповідає за передачу необроблених бітів через фізичне середовище, перетворюючи їх на сигнали (електричні, оптичні або

радіохвильові) та навпаки. Він визначає характеристики середовища передачі, такі як типи кабелів (мідні, коаксіальні, оптоволоконні), бездротові технології (Wi-Fi, Bluetooth), швидкість передачі даних, методи модуляції та синхронізації сигналів.

Таблиця 1.1 — Основні функції рівнів моделі OSI

Рівень	Назва рівня	Основні функції
7	Прикладний	Доступ до мережевих сервісів для користувача
6	Представлення	Перетворення, шифрування та стиснення даних
5	Сеансовий	Управління сеансами зв'язку між додатками
4	Транспортний	Надійна передача даних, контроль потоку та помилок
3	Мережевий	Маршрутизація, логічна адресація, фрагментація пакетів
2	Канальний	Фреймінг, виявлення та виправлення помилок, MAC-адресація
1	Фізичний	Передача бітів через фізичне середовище

Канальний рівень забезпечує надійну передачу даних між вузлами мережі, розбиваючи дані на кадри (фрейми), додаючи заголовки та контрольні суми для виявлення та виправлення помилок. Він також керує доступом до середовища передачі, вирішує проблеми колізій та контролює потік даних.

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

Транспортний рівень забезпечує надійну передачу даних між кінцевими

пристроями, використовуючи протоколи TCP та UDP. Він також відповідає за мультиплексування та демультиплексування даних, контроль потоку та адаптацію швидкості передачі.

Сеансовий рівень керує сеансами зв'язку між пристроями, створюючи, підтримуючи та завершуючи сеанси. Він також забезпечує синхронізацію даних та безпеку обміну.

Рівень представлення стандартизує представлення даних для обміну між пристроями, відповідаючи за перетворення даних у стандартний формат, компресію, шифрування та забезпечення незалежності від мови та платформи.

Рівень застосунків визначає програми та протоколи для взаємодії користувачів з мережевими ресурсами, такими як електронна пошта, веб-браузери та інші. Він включає протоколи, як-от HTTP, SMTP та FTP, і відповідає за обробку та адаптацію даних для користувача, забезпечуючи їхню безпеку та конфіденційність під час передачі.

На відміну від моделі OSI, модель TCP/IP (Transmission Control Protocol / Internet Protocol) виникла не як абстрактна концепція, а як практична модель, побудована на базі реальних мережевих протоколів, що лягли в основу функціонування Інтернету. Вона була розроблена в рамках дослідницького проєкту DARPA у США у 1970-х роках, а її остаточна структура була сформована в 1980-х.

Модель TCP/IP є протокольно-орієнтованою, тобто її рівні визначаються не стільки функціональністю, як у OSI, скільки наявними протоколами, які реалізують ту чи іншу функцію. Основу становлять два ключові протоколи: IP (Internet Protocol) — забезпечує логічну адресацію та маршрутизацію даних між вузлами мережі та TCP (Transmission Control Protocol) — гарантує надійне передавання даних, контроль цілісності та коректну послідовність доставки.

Після впровадження цієї моделі та її масового розповсюдження вона стала де-факто стандартом мережевої взаємодії для глобального Інтернету. Незважаючи на меншу кількість рівнів (чотири основні), TCP/IP охоплює всі необхідні функції для забезпечення ефективної та стабільної передачі даних у

комп’ютерних мережах.

Модель TCP/IP також дотримується ідеї ієрархії рівнів , де кожен вищий рівень використовує сервіси нижчого. Вона демонструє високу гнучкість, практичну придатність і зручність реалізації як у великих, так і у малих мережевих структурах.

Ця модель складається з чотирьох рівнів, кожен з яких виконує специфічні функції для забезпечення повноцінного процесу обміну інформацією.

Мережевий інтерфейс, що також називається фізичним рівнем, визначає механізми передачі даних між пристроями через різні середовища, такі як дротові й бездротові технології. Це може бути оптоволоконний зв’язок, коаксіальний кабель або радіочастотна передача. На цьому рівні відбувається формування фреймів та кодування сигналів, які дозволяють коректно передавати інформацію.

Інтернет-рівень забезпечує маршрутизацію даних у мережі, дозволяючи пакетам знайти шлях від відправника до отримувача незалежно від топології мережі. Він використовує IP-адресацію, яка визначає унікальне розташування кожного пристрою в мережевому середовищі. Завдяки цьому рівню дані можуть передаватися між мережами різної структури, а маршрутизатори виконують критичну роль у процесі їхнього пересилання.

Транспортний рівень відповідає за встановлення та підтримку з’єднання між пристроями, забезпечуючи надійність передачі даних. TCP гарантує коректність отриманих повідомлень, перевіряючи їхню цілісність і використовуючи механізми виправлення помилок. UDP пропонує швидке передавання без перевірки надійності, що робить його корисним для реального часу, наприклад у потоковому відео або VoIP-зв’язку.

Рівень застосунків є найвищим рівнем цієї моделі, визначаючи стандарти для взаємодії програм та користувачів із мережею. Він містить різні протоколи, такі як HTTP, FTP, SMTP, які забезпечують відповідно роботу веб-сайтів, обмін файлами та передачу електронної пошти. Цей рівень гарантує, що користувачі можуть легко взаємодіяти з мережею без необхідності розбиратися в її

внутрішній структурі.

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 14 моделлю у реальних мережевих середовищах через свою простоту та ефективність [4]. 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	OSI	TCP/IP
Кількість рівнів	7	4
Ідентифікація рівнів	Фізичний, Канал зв'язку, Мережевий, Транспорт, Сеансовий, Представлення, Застосунків	Мережевий, Інтернет, Транспорт, Застосунків
Використання у реальних системах	Непоширена	Поширена
Типові протоколи на рівні мережі	IP	IPv4,IPv6

Модель OSI широко застосовується як інструмент для моделювання та аналізу, що дозволяє логічно уявити, як саме функціонують мережеві системи. Вона відрізняється чітким розмежуванням функцій між рівнями, що сприяє кращому розумінню процесів. Проте, через свою теоретичну природу, вона рідко втілюється в повному обсязі в реальних мережах.

Натомість TCP/IP — це реальна реалізація, яка лежить в основі сучасного Інтернету. Її менша кількість рівнів компенсується практичністю, зосередженістю на ефективній маршрутизації та масштабованості, що зробило її універсальним рішенням для більшості мережевих середовищ:

Ієрархія рівнів — кожен рівень виконує визначені функції та передає дані на сусідній;

Абстрагування — завдяки чіткому розподілу ролей між рівнями можлива незалежна оптимізація окремих функціональних блоків;

Інкапсуляція даних — дані передаються від прикладного рівня до фізичного з додаванням службової інформації (заголовків), що забезпечує керування з'єднанням, маршрутизацію тощо .

1.2 Протоколи рівнів комп'ютерної мережі

У структурі мережевих моделей, таких як OSI або TCP/IP, кожен рівень виконує певні функції, які реалізуються за допомогою протоколів. Протокол є набором правил та процедур, що регулюють обмін даними між пристроями мережі. Взаємодія між рівнями моделі передбачає використання протоколів, які забезпечують правильне, узгоджене та ефективне передавання інформації. Основну увагу в контексті аналізу функціонування мережі слід приділити протоколам від канального до прикладного рівня, оскільки саме вони відіграють ключову роль у встановленні, підтримці й управлінні мережею.

Канальний рівень відповідає за формування логічного каналу зв'язку між двома безпосередньо з'єднаними вузлами. Протоколи цього рівня займаються фізичним доступом до середовища передавання та забезпечують надійність передачі даних шляхом виявлення та іноді виправлення помилок. Одним з найвідоміших протоколів цього рівня є Ethernet (IEEE 802.3), який забезпечує доступ до середовища за допомогою методу CSMA/CD (Carrier Sense Multiple Access with Collision Detection). Інші протоколи, такі як PPP (Point-to-Point Protocol), використовуються для встановлення з'єднання між двома вузлами через послідовні канали, наприклад, при комутованому з'єднанні або в мережах типу WAN [6].

На мережевому рівні відбувається логічна адресація та маршрутизація пакетів між підмережами. Найбільш фундаментальним протоколом цього рівня є Internet Protocol (IP), зокрема його версії IPv4 та IPv6. IP забезпечує

незалежність мережевих технологій нижчих рівнів та дає змогу доставляти пакети між хостами, які можуть бути розташовані на різних мережах. Разом з IP часто використовуються допоміжні протоколи, такі як ICMP (Internet Control Message Protocol), який відповідає за передачу службових повідомлень (наприклад, повідомлення про недоступність вузлів або перевищення часу життя пакету) .

Транспортний рівень виконує функції логічного зв'язку між прикладними процесами на різних вузлах. Основними протоколами цього рівня є TCP (Transmission Control Protocol) та UDP (User Datagram Protocol). TCP є протоколом з встановленням з'єднання, який гарантує доставку даних у правильному порядку, забезпечує контроль потоку та контроль помилок. Він використовується в ситуаціях, де важлива надійність передавання (наприклад, під час передачі файлів або електронної пошти). Натомість UDP є простішим, протоколом без встановлення з'єднання, який не гарантує доставку, але забезпечує менші затримки. Його використовують у реальному часі, наприклад, для потокового відео чи аудіо, де важливіше мінімізувати затримки, ніж забезпечити ідеальну цілісність потоку.

На прикладному рівні розташовуються протоколи, які безпосередньо взаємодіють із прикладними програмами та користувачем. Цей рівень надає сервіси, які підтримують такі функції, як передавання електронної пошти, доступ до веб-ресурсів, передавання файлів, іменування ресурсів тощо. Найпоширенішими протоколами прикладного рівня є HTTP (HyperText Transfer Protocol), що забезпечує доступ до веб-сторінок; SMTP (Simple Mail Transfer Protocol) — для надсилання електронної пошти; FTP (File Transfer Protocol) — для передавання файлів; DNS (Domain Name System) — для перетворення доменних імен на IP-адреси .

Ці протоколи часто не працюють окремо, а взаємодіють між собою у вигляді стеку. Наприклад, веб-браузер (прикладний рівень) надсилає HTTP-запит через TCP (транспортний рівень), який у свою чергу використовує IP (мережевий рівень), а дані передаються через Ethernet (канальний рівень). Це

явище називається інкапсуляцією, коли кожен рівень додає свою службову інформацію до даних перед передачею, що наведено у таблиці 1.3.

Таблиця 1.3 — Ієрархічна структура моделі TCP/IP

Рівень (TCP/IP)	Основні протоколи	Призначення
Прикладний	HTTP, FTP, SMTP, DNS, Telnet	Надання сервісів прикладним програмам
Транспортний	TCP, UDP	Надійна або швидка передача даних між хостами
Інтернет-рівень	IP (IPv4, IPv6), ICMP, ARP, IGMP	Логічна адресація, маршрутизація, управління
Канальний (мережевий інтерфейс)	Ethernet, Wi-Fi (802.11), PPP, HDLC	Фізичний доступ до середовища, передача кадрів

Коли пакет проходить крізь мережу, кожен рівень додає свій "заголовок", формуючи блок службової інформації. Після досягнення вузла призначення ці заголовки по черзі знімаються — це процес деінкапсуляції, що дозволяє приймаючому пристрою обробити отриману інформацію відповідно до протоколу кожного рівня.

Важливо зазначити, що протоколи постійно еволюціонують. Наприклад, нові версії HTTP (наприклад, HTTP/2 або HTTP/3) забезпечують більшу ефективність обміну, зменшення накладних витрат та покращене управління з’єднаннями. Аналогічно, перехід від IPv4 до IPv6 обумовлений обмеженням адресного простору у старшій версії IP і потребою у підтримці мільярдів пристроїв, підключених до Інтернету.

Протоколи рівнів від канального до прикладного утворюють повноцінну інфраструктуру для передавання, маршрутизації, обробки та доставки інформації у комп’ютерних мережах. Їх правильне функціонування, взаємодія та

узгодженість є критичними для забезпечення ефективної, безпечної та надійної роботи мережевого середовища.

1.3 IP-адресація в комп’ютерних мережах

Адресація в IP-мережах є фундаментальною складовою логічної ідентифікації вузлів та маршрутизації пакетів у глобальних і локальних комп’ютерних мережах. Вона дозволяє унікально визначати кожен мережевий інтерфейс та забезпечує механізми доставки даних до призначення незалежно від фізичної структури мережі. Сучасна IP-адресація реалізується через два протоколи — IPv4 та IPv6, кожен з яких має власну схему побудови, обробки та поділу на підмережі. Крім того, з появою більш гнучких методів маршрутизації було запроваджено концепцію CIDR (Classless Inter-Domain Routing), яка суттєво змінила принципи поділу адресного простору [6].

IPv4 — це четверта версія протоколу Інтернету, яка історично склалася як основа глобальної адресації. Вона використовує 32-бітну адресну схему, що забезпечує теоретичну кількість приблизно 4,29 мільярда унікальних IP-адрес. Ці адреси традиційно записуються у десятковій формі, розділеній крапками, наприклад: 192.168.1.1. З технічної точки зору, така адреса складається з чотирьох байтів, кожен з яких може приймати значення від 0 до 255. Спочатку для впорядкування та організації адресного простору IPv4 було створено класову систему, де адреси поділялися на класи A, B, C, D і E, однак така класифікація виявилась неефективною для оптимального використання обмеженого простору адрес [7].

Саме тому у 1993 році була впроваджена технологія CIDR, яка дозволила гнучкіше управляти простором IP-адрес. CIDR замінив класову модель, використовуючи позначення через префікс, яке визначає кількість біт, що належать до мережевої частини адреси. Наприклад, запис 192.168.10.0/24 означає, що перші 24 біти (три байти) використовуються для адресації мережі, а решта 8 біт — для вузлів. Завдяки цьому стала можливою гнучка агрегація маршрутів, зменшення таблиць маршрутизації та ефективніший розподіл

адресного простору [8,10].

Особливу роль у практичній реалізації адресації відіграє субнетування — тобто поділ однієї великої мережі на менші логічні частини, які називаються підмережами. Це дає змогу ефективно організовувати структуру корпоративної або освітньої мережі, розділяти відділи, обмежувати широкомовний трафік та оптимізувати безпеку. При створенні підмереж застосовується маска підмережі, яка, подібно до префіксу CIDR, визначає кількість бітів, що становлять ідентифікатор мережі. Наприклад, маска 255.255.255.0 відповідає префіксу /24, тобто означає 256 IP-адрес у підмережі (включно з адресою мережі та широкомовною адресою). Таке дроблення дозволяє системним адміністраторам детально управляти маршрутизацією та контролем доступу між сегментами мережі [9].

Зі стрімким зростанням кількості пристроїв, підключених до мережі, виникла потреба у розширенні адресного простору, що привело до розробки IPv6 — шостої версії Інтернет-протоколу, яка використовує 128-бітну систему адресації. Це забезпечує кількість можливих унікальних адрес, що перевищує 3.4×10383.4 \times 10^{38}3.4×1038, тобто практично необмежену кількість пристроїв, що можуть існувати у глобальному просторі. Формат запису IPv6-адрес значно відрізняється від IPv4: він використовує шістнадцяткові значення та розділяється двокрапками, наприклад: 2001:0db8:85a3:0000:0000:8a2e:0370:7334. Щоб спростити читання, IPv6 дозволяє скорочення: нулі можуть бути опущені, і декілька поспіль ідучих груп нулів можуть бути замінені подвійною двокрапкою (::), але тільки один раз у межах однієї адреси [10].

IPv6 також не використовує класову модель і підтримує CIDR-нотацію. Крім того, він вводить нову концепцію автоматичної адресації (Stateless Address Autoconfiguration), що дозволяє пристроям самостійно отримувати унікальні адреси без централізованого сервера DHCP. Це надзвичайно актуально у сучасних великих мережах, де централізоване керування мільйонами адрес було б надто ресурсоємним [11].

У таблиці 1.4 представлено основні відмінності між IPv4 та IPv6 у контексті адресації:

Таблиця 1.4 — Порівняльна характеристика IPv4 та IPv6

Характеристика	IPv4	IPv6	Характеристика
Довжина адреси	32 біти	128 біт	Довжина адреси
Кількість адрес	~4,29 млрд	3.4×10383.4 \times 10^{38}3.4×1038	Кількість адрес
Формат запису	Десятковий, через крапку	Шістнадцятковий, через двокрапку	Формат запису
CIDR-підтримка	Так	Так	CIDR-підтримка
Характеристика	IPv4	IPv6	Характеристика
Довжина адреси	32 біти	128 біт	Довжина адреси
Кількість адрес	~4,29 млрд	$3.4\times10^{383.4}$	Кількість адрес

У контексті розробки сучасних мереж все більшої популярності набуває практика без NAT-мереж, характерна для IPv6. На відміну від IPv4, де через дефіцит адрес активно використовуються механізми трансляції адрес (NAT — Network Address Translation), IPv6 надає можливість кожному пристрою мати глобально унікальну адресу, що значно полегшує маршрутизацію та забезпечує повну доступність пристроїв у мережі Інтернет. Проте це одночасно вимагає нових підходів до захисту адресного простору, адже традиційні бар’єри NAT більше не слугують додатковим рівнем безпеки [12].

Ще одним важливим аспектом є сумісність двох версій протоколів. IPv4 та IPv6 є несумісними на рівні протоколу, отже, необхідне використання технологій переходу, таких як dual stack (одночасна підтримка обох протоколів на пристрої), tunneling (інкапсуляція одного протоколу в інший), або translation (перетворення

протоколів через спеціальні шлюзи). У локальних мережах перехід часто виконується поступово: спочатку вводиться підтримка IPv6 паралельно з IPv4, з подальшим поступовим виведенням останнього .

IP-адресація, як у версіях IPv4, так і IPv6, є складною і багаторівневою системою, яка поєднує логічну структуру ідентифікації, механізми поділу мережі, маршрутизації та гнучкого управління адресним простором. Використання CIDR і підмереж дозволяє ефективно масштабувати мережі, а впровадження IPv6 відкриває нові можливості у глобальному просторі адрес, одночасно ставлячи нові виклики у сфері адміністрування та інформаційної безпеки.

1.4 Сучасні стандарти побудови локальних мереж

Локальні мережі є фундаментом цифрової інфраструктури для більшості організацій, установ та домогосподарств. З розвитком інформаційних технологій, стрімким зростанням обсягів переданої інформації, зростанням кількості підключених пристроїв і необхідністю забезпечення надійного та безпечного зв’язку, виникає потреба у впровадженні новітніх стандартів побудови мереж. Вибір технології локальної мережі, зокрема типу фізичного середовища передачі даних, протоколів і топології, значною мірою впливає на її продуктивність, масштабованість, стабільність і рівень захисту.

Основними напрямками розвитку локальних мереж є провідні технології на основі Ethernet, які забезпечують високу пропускну здатність і стабільність, а також бездротові рішення на основі Wi-Fi, що гарантують гнучкість у використанні та швидке розгортання. Крім того, значну увагу приділяють питанням інформаційної безпеки, зокрема шифруванню трафіку, автентифікації користувачів і протидії загрозам, пов’язаним із бездротовим доступом.

1.4.1 Технічні характеристики Ethernet

Ethernet є домінуючим стандартом фізичного та канального рівнів моделі OSI для побудови локальних обчислювальних мереж (LAN). Його популярність

пояснюється високою пропускною здатністю, надійністю, масштабованістю, гнучкістю інтеграції з іншими технологіями та стабільністю роботи у складних мережевих середовищах. Поява Ethernet стала відповіддю на потребу у простій та доступній технології передачі даних, яка може бути ефективно реалізована у межах однієї будівлі, кампусу чи локалізованої мережевої інфраструктури.

Ethernet був уперше розроблений у 1973 році в компанії Xerox PARC, однак його перша стандартна реалізація з'явилася у 1980-х роках. Важливим етапом стало прийняття стандарту IEEE 802.3, який описує фізичні аспекти, методи доступу до середовища (CSMA/CD) та інші технічні характеристики. Початкові версії Ethernet функціонували на швидкості 10 Мбіт/с, використовуючи коаксіальні кабелі товстого або тонкого типу (10BASE5, 10BASE2). З часом, у міру розвитку технологій та зростання потреб, з’явилися нові реалізації: Fast Ethernet (100 Мбіт/с), Gigabit Ethernet (1 Гбіт/с), 10 Gigabit Ethernet (10 Гбіт/с), а також надшвидкі варіанти 40, 100 та 400 Гбіт/с[13,14].

Однією з ключових характеристик Ethernet є використання фреймів фіксованої структури для передачі даних. Кожен Ethernet-фрейм містить префікс синхронізації (Preamble), MAC-адреси відправника та отримувача, поле типу або довжини, дані користувача (Payload), а також контрольну суму CRC. Така структура дозволяє ефективно здійснювати перевірку цілісності переданих даних, що критично важливо у середовищах з великою кількістю вузлів[15].

З технічного боку Ethernet працює за принципом розподіленого доступу до спільного середовища з використанням методу CSMA/CD (Carrier Sense Multiple Access with Collision Detection), який передбачає прослуховування середовища перед передачею та виявлення колізій. У сучасних реалізаціях Ethernet, що функціонують через комутатори (switches), колізії практично виключені, оскільки кожен порт працює в режимі full-duplex, тобто передача і прийом даних можуть відбуватись одночасно, що суттєво підвищує продуктивність і зменшує затримки.

Фізичне середовище Ethernet включає в себе мідні кабелі типу UTP (Unshielded Twisted Pair) категорій 5e, 6, 6a, 7 та 8, які дозволяють досягати

швидкостей до 10 Гбіт/с на відстанях до 100 метрів. Для вищих швидкостей, наприклад 40/100 Гбіт/с, перевагу отримують оптоволоконні лінії зв’язку, що мають менші втрати та вищу пропускну здатність на великих відстанях. Використання SFP-модулів, QSFP, MPO-конекторів дозволяє масштабувати мережу у межах дата-центрів і корпоративних інфраструктур [16].

На сьогодні Ethernet продовжує розвиватися у напрямку підвищення швидкості, зменшення затримок та оптимізації енергоспоживання. Наприклад, впровадження Energy-Efficient Ethernet (EEE), як це визначено у стандарті IEEE 802.3az, дозволяє знижувати енергоспоживання пристроїв у періоди низького навантаження. Окрім цього, підтримка PoE (Power over Ethernet) у рамках специфікацій IEEE 802.3af/at/bt надає можливість передавати електроживлення разом із даними через стандартний кабель Ethernet, що надзвичайно зручно для підключення таких пристроїв як IP-камери, точки доступу Wi-Fi, SIP-телефони тощо [17].

1.4.2 Технічні характеристики бездротових мереж Wi-Fi

Wi-Fi (Wireless Fidelity) є найбільш поширеною технологією бездротової передачі даних у межах локальних мереж, що базується на стандартах IEEE 802.11. Вона забезпечує високошвидкісне з'єднання між кінцевими пристроями — ноутбуками, смартфонами, планшетами, камерами, а також мережею Інтернет через бездротові точки доступу. Основною метою Wi-Fi є забезпечення мобільності, гнучкості розгортання та мінімізації затрат на фізичне з'єднання пристроїв.

Перший стандарт IEEE 802.11 був затверджений у 1997 році і дозволяв передавати дані на швидкості до 2 Мбіт/с. З того часу технологія зазнала значного розвитку через зростаючі потреби користувачів, збільшення кількості пристроїв та зростання трафіку. Із плином часу з’являлися нові версії стандартів: 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, а останнім часом — 802.11ax (Wi-Fi 6) та 802.11be (Wi-Fi 7) [18].

Основною технічною характеристикою кожного стандарту є діапазон

частот, ширина каналу, модуляція, кількість одночасно підтримуваних потоків та максимальна пропускна здатність. Наприклад, 802.11n (Wi-Fi 4) підтримує одночасне використання двох частотних діапазонів — 2,4 ГГц та 5 ГГц, а також впроваджує технологію MIMO (Multiple Input Multiple Output), яка дозволяє значно підвищити продуктивність за рахунок паралельної передачі кількох потоків даних. Стандарт 802.11ac (Wi-Fi 5) суттєво розширює використання діапазону 5 ГГц, підтримуючи 8 просторових потоків, ширину каналу до 160 МГц і модуляцію 256-QAM, що дає змогу досягати швидкості понад 1 Гбіт/с.

Найновіший стандарт 802.11ax (Wi-Fi 6), ратифікований у 2021 році, значною мірою змінює підхід до побудови бездротової мережі. Він орієнтований не стільки на пікову швидкість, скільки на ефективність у багатокористувацьких середовищах. У Wi-Fi 6 використовується технологія OFDMA (Orthogonal Frequency Division Multiple Access), що дозволяє ділити канал на підканали й обслуговувати декілька пристроїв одночасно. Крім того, впроваджено TWT (Target Wake Time) — механізм, який дозволяє клієнтським пристроям узгоджувати час пробудження для обміну даними, значно зменшуючи енергоспоживання [19].

Однією з важливих характеристик Wi-Fi є зона покриття. У межах приміщення вона здебільшого обмежена 30–50 метрами через фізичні перешкоди та ефект загасання сигналу. У відкритому середовищі досягається покриття до 100 метрів і більше. Для розширення покриття використовуються репітери (ретранслятори), точки доступу з підключенням до основного маршрутизатора через Ethernet або спеціалізовані mesh-системи, які автоматично формують єдину мережу з декількох вузлів.

Варто також враховувати питання сумісності. Пристрої з новими модулями Wi-Fi зазвичай зберігають зворотну сумісність з попередніми версіями стандарту. Наприклад, точка доступу з підтримкою Wi-Fi 6 здатна працювати з клієнтами, що підтримують лише Wi-Fi 4 або Wi-Fi 5, хоча при цьому можливості новітніх технологій можуть бути частково обмежені.

Інтеграція Wi-Fi у структуру локальних мереж вимагає також урахування

питань безпеки, про що детальніше йтиметься в наступному підпункті. Проте слід зазначити, що розвиток бездротових стандартів паралельно зростає з підвищенням вимог до конфіденційності, автентифікації та захисту даних, переданих через повітряне середовище. У сукупності Wi-Fi перетворився з допоміжного засобу підключення на основний канал доступу до мережі в більшості корпоративних і побутових середовищ, де мобільність, масштабованість і швидкість відіграють вирішальну роль

1.5 Технології динамічної маршрутизації

У мережевій інфраструктурі маршрутизація є ключовим процесом, що забезпечує доставку пакетів даних від джерела до місця призначення через одну або кілька проміжних мереж. Різні типи маршрутизації — статична, динамічна та гібридна — визначають, як формується таблиця маршрутизації та яким чином відбувається вибір найоптимальнішого шляху для передавання трафіку. Кожен з цих підходів має свої переваги, недоліки та сфери застосування.

Статична маршрутизація передбачає ручне налаштування маршрутів адміністраторами мережі. Вона проста у реалізації та не вимагає додаткових ресурсів, однак не адаптується до змін у мережевій топології, що робить її менш гнучкою в масштабних або динамічних середовищах.

Динамічна маршрутизація базується на використанні протоколів, що дозволяють маршрутизаторам автоматично обмінюватися інформацією про топологію мережі та адаптуватися до змін. До таких протоколів належать OSPF, EIGRP, RIP та інші.Динамічні протоколи враховують такі метрики, як затримка, кількість хопів, пропускна здатність, що дозволяє оптимізувати передачу даних.

Гібридна маршрутизація поєднує риси обох підходів: частина маршрутів налаштовується вручну, інші — визначаються динамічно. Такий підхід дозволяє гнучко адаптувати мережу до вимог продуктивності та безпеки

1.5.1 Основний протокол динамічної маршрутизації OSPF

Одним із найпотужніших та найбільш використовуваних протоколів

динамічної маршрутизації у локальних та корпоративних мережах є OSPF (Open Shortest Path First). Він належить до групи протоколів внутрішньої маршрутизації (IGP — Interior Gateway Protocol) і був розроблений для заміни простого, але застарілого протоколу RIP. OSPF базується на алгоритмі Дейкстри (Shortest Path First), який дозволяє обчислювати найкоротший маршрут до кожної відомої мережі[20].

На відміну від протоколів на основі відстані (distance-vector), які просто інформують сусідів про свої маршрути, OSPF використовує підхід на основі стану каналів (link-state). Кожен маршрутизатор формує повну карту топології мережі та самостійно обчислює найкращі маршрути, що підвищує точність і швидкість прийняття рішень.

Основні особливості OSPF: Ієрархічна структура мережі. OSPF підтримує поділ на області (areas), що дозволяє зменшити обсяг обміну маршрутною інформацією. Найважливішою є Area 0 (backbone area) — центральна область, через яку мають бути з’єднані всі інші області. Приклад поділу мережі OSPF на сектори показано на рисунку 1.1.

Така структура покращує масштабованість мережі й дозволяє розділяти велику інфраструктуру на логічні сегменти; Використання Hello-повідомлень. OSPF періодично надсилає невеликі Hello-пакети для встановлення та підтримки сусідських відносин (neighborship). Це дозволяє маршрутизаторам автоматично виявляти один одного та узгоджувати параметри для обміну маршрутами; Типи маршрутів. Протокол підтримує маршрути всередині однієї області (intra-area), між різними областями (inter-area) та до зовнішніх мереж (external routes), що забезпечує гнучкість при інтеграції з іншими протоколами та з Інтернетом; Швидке реагування на зміни. OSPF надзвичайно чутливий до змін у мережі. У разі відмови каналу або пристрою маршрутизатор одразу створює нову топологічну карту та обирає альтернативний маршрут, забезпечуючи мінімальні простої; Використання SPF-алгоритму. Кожен маршрутизатор будує дерево найкоротших шляхів, яке забезпечує мінімальний трафік і затримку. Такий підхід дуже ефективний у навчальних закладах, де важливо забезпечити

стабільний доступ до освітніх онлайн-ресурсів, електронних щоденників та внутрішніх серверів; Надійність та безпека. OSPF підтримує автентифікацію між маршрутизаторами, включаючи MD5, що дозволяє запобігти ін’єкції фальшивих маршрутів. Це особливо важливо в мережах з підвищеними вимогами до безпеки.

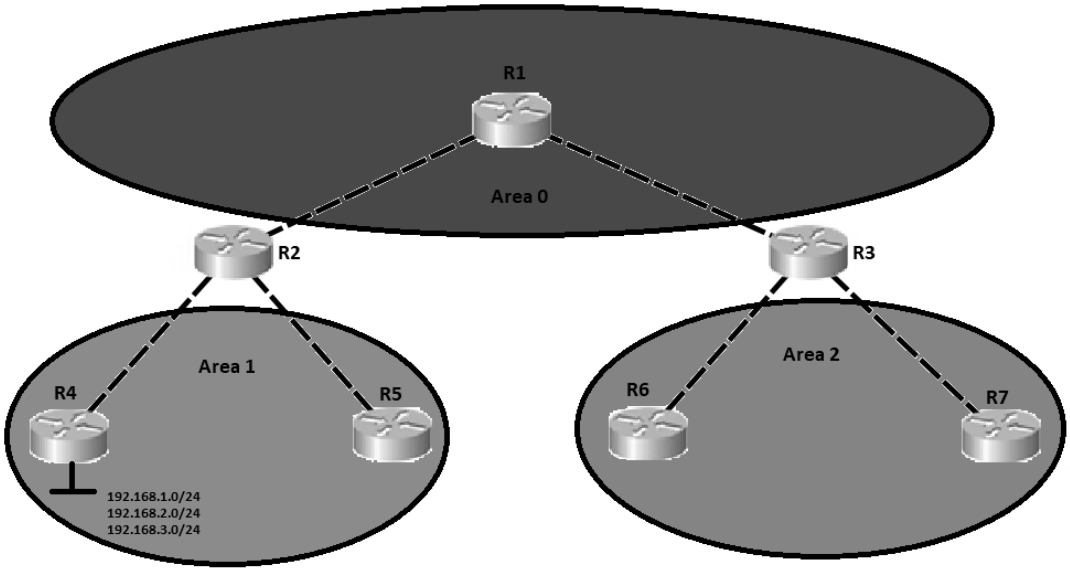


Рисунок 1.1 – Приклад поділу мережі OSPF на сектори

Для прикладу, у шкільній комп’ютерній мережі, яка складається з декількох корпусів, обладнаних окремими комутаторами та маршрутизаторами, OSPF дозволяє централізовано управляти маршрутизацією. Якщо в одному корпусі відключився маршрутизатор, OSPF автоматично перенаправляє трафік через резервний шлях, не вимагаючи втручання адміністратора. Завдяки цьому учні продовжують користуватися мережею без перерв.

Ще однією перевагою OSPF є відсутність обмеження на 15 стрибків (hops), яке має RIP. Це означає, що навіть у великих мережах з численними сегментами та підмережами маршрути будуть передаватися без втрат та затримок.

Для підвищення ефективності, OSPF підтримує агрегацію маршрутів — тобто об'єднання кількох маршрутів у один оголошуваний маршрут. Це дозволяє значно зменшити розмір таблиці маршрутизації та покращити продуктивність маршрутизатора.

Також, важливо відзначити, що OSPF є відкритим стандартом, тому його

підтримують пристрої різних виробників — Cisco, MikroTik, HP, Juniper та інші. Це дає свободу вибору обладнання та спрощує інтеграцію мережі в майбутньому.

1.5.2 Протокол вдосконаленої динамічної маршрутизації EIGRP

Enhanced Interior Gateway Routing Protocol (EIGRP) є пропрієтарним протоколом маршрутизації, розробленим компанією Cisco Systems. Він поєднує риси як дистанційно-векторних, так і лінк-стейт протоколів, і належить до категорії гібридних. Завдяки цьому EIGRP забезпечує швидку конвергенцію, гнучке налаштування та надійну маршрутизацію всередині автономної системи.

Однією з основних переваг EIGRP є використання алгоритму Diffusing Update Algorithm (DUAL), який гарантує відсутність петель маршрутизації та оптимальність обраного маршруту. DUAL дозволяє попередньо обчислити резервні маршрути (feasible successors), які миттєво активуються у разі відмови основного маршруту без необхідності повторної конвергенції [21].

EIGRP підтримує інкапсуляцію IP, IPv6, AppleTalk та IPX, що робить його універсальним у гетерогенних мережах. Протокол використовує кілька метрик: пропускну здатність, затримку, надійність, завантаженість каналу та максимальний розмір MTU — для розрахунку вартості маршруту. Ці параметри можуть бути гнучко налаштовані адміністратором відповідно до потреб мережі.

Ще однією перевагою є можливість розділення трафіку між кількома рівноцінними маршрутами (Equal-Cost Multi-Path, ECMP), що підвищує продуктивність і рівномірно розподіляє навантаження.

Хоча EIGRP був довгий час обмежений лише пристроями Cisco, з 2013 року протокол частково відкрито через публікацію стандарту в RFC 7868, що дозволило іншим виробникам реалізовувати його у своїх пристроях. Водночас повна сумісність усе ще може вимагати використання обладнання Cisco.

EIGRP найбільш ефективний у середовищах з високими вимогами до надійності, масштабованості та швидкої реакції на зміни в мережевій топології. Він часто використовується у корпоративних мережах, кампусних інфраструктурах, а також у дата-центрах із високою динамікою трафіку.

1.5.3 Базовий протокол динамічної маршрутизації RIP

Routing Information Protocol (RIP) є одним із найстаріших динамічних протоколів маршрутизації, який усе ще застосовується в окремих сегментах мережевих систем. RIP класифікується як дистанційно-векторний протокол і працює на основі метрики кількості переходів (hops), де максимальна допустима кількість хопів становить 15.

RIP функціонує за принципом періодичної передачі всієї таблиці маршрутів між сусідніми маршрутизаторами кожні 30 секунд. Такий підхід забезпечує простоту реалізації, однак призводить до повільної конвергенції та високого навантаження на мережу, особливо в великих або швидкозмінних середовищах. RIP не враховує затримку, пропускну здатність чи завантаженість каналів, що робить його менш ефективним у сучасних інфраструктурах із високими вимогами до якості обслуговування (QoS) [22].

Існує кілька версій RIP: RIP v1, що передає маршрути без підтримки CIDR та маски підмережі; RIP v2 — із підтримкою VLSM, CIDR, автентифікації; та RIPng (RIP next generation), розроблений для підтримки IPv6. Версія v2 також підтримує мультикастинг для надсилання оновлень, що зменшує мережеве навантаження порівняно з широкомовними повідомленнями RIP v1.

RIP має низку механізмів для запобігання маршрутизаторним петлям, серед яких: Split Horizon, Route Poisoning, Hold-Down Timers та інші. Попри свою простоту та історичну значущість, RIP поступово витісняється більш ефективними протоколами, такими як OSPF чи EIGRP.

Застосування RIP доцільне лише в невеликих, простих мережах з обмеженою топологією та невисокими вимогами до швидкості адаптації до змін. Проте його легкість налаштування, сумісність і підтримка широким колом мережевого обладнання роблять його корисним у навчальних цілях і початкових рівнях адміністрування мереж.

1.6 NAT та його роль в ізоляції внутрішньої мережі

Network Address Translation (NAT) — це ключова технологія в сучасних

комп'ютерних мережах, яка забезпечує трансляцію IP-адрес між приватною та публічною мережами. Цей механізм дозволяє пристроям у внутрішній мережі взаємодіяти з Інтернетом через обмежену кількість публічних IP-адрес, що особливо актуально в умовах обмеженого простору адрес IPv4.

З технічної точки зору NAT є проміжною ланкою між двома типами адресного простору: приватним (RFC 1918) і публічним. Залежно від потреб мережі та доступного пулу публічних адрес, реалізується статичний NAT для фіксованих відповідностей, динамічний NAT для тимчасових сесій, або ж PAT (Port Address Translation), який дозволяє тисячам пристроїв спільно використовувати одну публічну IP-адресу завдяки унікальним номерам портів. Такий підхід особливо ефективний у домашніх мережах, навчальних закладах і малих офісах, де ресурси обмежені, а доступ до Інтернету потрібен широкому колу пристроїв.

Існує кілька типів NAT, кожен з яких має свої особливості та застосування. Статичний NAT забезпечує постійну відповідність між однією приватною та однією публічною IP-адресою. Цей тип трансляції підходить для серверів, які повинні бути доступними з Інтернету, наприклад, веб-серверів або поштових серверів. Однак він вимагає наявності достатньої кількості публічних IP-адрес. Динамічний NAT використовує пул публічних IP-адрес, які динамічно призначаються внутрішнім пристроям на час сесії. Після завершення сесії адреса повертається до пулу для повторного використання. Це дозволяє ефективніше використовувати обмежений пул публічних IP-адрес. Port Address Translation (PAT), також відомий як NAT Overload, дозволяє багатьом пристроям у приватній мережі використовувати одну публічну IP-адресу, розрізняючи з'єднання за номерами портів. Це найбільш поширений тип NAT, особливо в домашніх та малих офісних мережах. Симетричний NAT створює унікальні відповідності між внутрішніми та зовнішніми адресами та портами для кожного з'єднання [23].

Використання NAT забезпечує декілька критично важливих переваг, зокрема зменшення витрат на IP-адреси, підвищення безпеки за рахунок ізоляції

внутрішньої мережі та централізацію управління. Разом з тим, деякі протоколи (наприклад, SIP, FTP у активному режимі або IPsec) можуть стикатися з труднощами через модифікацію пакетів NAT-ом, що вимагає використання спеціальних механізмів обходу (NAPT-aware NAT, ALG тощо). Нижче наведено таблицю 1.5, яка узагальнює основні переваги та недоліки використання NAT.

Таблиця 1.5 — Переваги та недоліки використання технології NAT

Переваги NAT	Недоліки NAT
Економія публічних IP-адрес	Може спричинити проблеми з протоколами, що вбудовують IP
Підвищення безпеки мережі шляхом приховування внутрішніх адрес	Ускладнення організації вхідних з’єднань ззовні
Зменшення конфліктів IP-адрес між мережами	Можливість затримок або зниження продуктивності
Централізоване управління виходом в Інтернет	Втрати прозорості при аналізі трафіку (відсутність оригінального IP)
Простота конфігурації для користувачів	Необхідність додаткових налаштувань для деяких сервісів
Покращення масштабованості внутрішньої мережі	Може ускладнити діагностику мережевих проблем

Аналізуючи наведені у таблиці переваги та недоліки технології NAT, можна виявити кілька суттєвих тенденцій, що відображають її вплив на функціонування комп’ютерних мереж. NAT, безперечно, забезпечує низку стратегічних переваг, зокрема дозволяє ефективно використовувати обмежений пул публічних IP-адрес, що має критичне значення у зв'язку з вичерпанням простору адрес IPv4. Завдяки трансляції адрес кілька внутрішніх пристроїв можуть використовувати одну публічну IP-адресу, що дозволяє значно зменшити витрати на інфраструктуру і уникнути дублювання адрес у різних сегментах мережі.

Крім цього, NAT сприяє підвищенню загального рівня безпеки, оскільки

внутрішні IP-адреси залишаються невидимими для зовнішніх вузлів, що ускладнює виконання несанкціонованих сканувань і атак ззовні. Така ізоляція значно підвищує стійкість до загроз, особливо в корпоративних і державних мережах. Централізація виходу в Інтернет через один або кілька шлюзів NAT також дає змогу адміністраторам краще контролювати трафік, застосовувати політики безпеки та фільтрацію, що особливо цінне в мережах з великою кількістю користувачів. Простота налаштування NAT з боку кінцевих користувачів також виступає перевагою, оскільки не потребує від них специфічних знань або змін конфігурації обладнання, що полегшує розгортання мереж у масштабі.

Однак, ізольованість внутрішніх адрес одночасно створює низку обмежень. Однією з головних проблем є порушення прозорості мережевого трафіку: оригінальні адреси джерела замінюються адресами шлюзу NAT, що ускладнює трасування маршрутів пакетів і глибокий аналіз мережевої активності. Це створює труднощі при впровадженні засобів моніторингу та систем виявлення атак, які залежать від точного знання джерела трафіку. Крім того, сервіси, що використовують вбудовану вмістову IP-адресу в протоколі, такі як SIP або FTP, можуть некоректно працювати за NAT без додаткових механізмів, таких як ALG (Application Layer Gateway) або проксі-сервери.

Ще однією критичною проблемою є ускладнення встановлення вхідних з’єднань, що особливо впливає на серверні застосунки або P2P-системи. NAT перешкоджає зовнішнім пристроям ініціювати прямі з’єднання з внутрішніми хостами, що потребує використання спеціальних протоколів пробиття NAT або ручної переадресації портів. Це, в свою чергу, може призводити до помилок конфігурації та зниження надійності системи. У деяких випадках, залежно від типу NAT, можливе виникнення затримок через обробку таблиць трансляцій, що впливає на продуктивність при високих навантаженнях. Особливо це стосується пристроїв з обмеженими ресурсами, таких як домашні маршрутизатори.

Також варто зазначити, що NAT знижує ефективність використання деяких сучасних протоколів, таких як IPsec, який працює з оригінальними IP-

адресами для встановлення захищених тунелів. Це ускладнює реалізацію рішень на базі VPN і змушує адміністраторів вдаватися до модифікацій, як-от NAT Traversal (NAT-T). У загальному контексті це означає, що NAT, хоч і вирішує проблему адресації та підвищує керованість, одночасно створює нові виклики для проектування, моніторингу та підтримки мережевої інфраструктури.

1.7 Потенційні загрози комп’ютерних мереж та загальні принципи захисту

Зі стрімким розвитком цифрових технологій і мережевої інфраструктури, комп’ютерні мережі стали основою більшості інформаційних систем, включаючи ті, що забезпечують критично важливі функції у державному, комерційному та освітньому секторах. Відповідно зростає значущість питань безпеки, які стосуються не лише захисту від зовнішніх атак, але й побудови внутрішньо безпечної архітектури передачі даних. Одними з важливих інструментів у цій сфері є віртуальні технології, зокрема VLAN та VPN, які, окрім переваг, також мають свої потенційні вразливості, що потребують додаткової уваги в рамках загальної стратегії кіберзахисту.

Комплексний підхід до безпеки мереж передбачає, з одного боку, виявлення і класифікацію загроз, а з іншого — впровадження ефективних механізмів протидії. Серед типових небезпек: несанкціонований доступ, перехоплення трафіку, зміна маршрутизації, атаки типу man-in-the-middle (MitM), спуфінг (DNS, ARP), відмова в обслуговуванні (DoS/DDoS), а також впровадження шкідливого ПЗ через вразливості мережевих служб або користувацькі помилки.

1.7.1 VLAN і загрози в логічному поділі мереж

Віртуальні локальні мережі (VLAN) є ключовим інструментом для логічного поділу комп’ютерних мереж, що дозволяє підвищити їхню безпеку, ефективність та керованість. Завдяки VLAN можна об'єднувати пристрої в окремі логічні сегменти, незалежно від їх фізичного розташування, що сприяє

оптимізації трафіку, зменшенню навантаження на мережу та підвищенню загального рівня безпеки.

Принцип роботи VLAN базується на використанні тегування кадрів за допомогою протоколу IEEE 802.1Q. Кожен кадр, що передається через мережу, отримує спеціальний тег, який вказує на його належність до певного VLAN. Комутатори, що підтримують цей протокол, аналізують теги та направляють трафік лише до пристроїв, які входять до відповідного VLAN. Це дозволяє створювати ізольовані логічні сегменти мережі, навіть якщо пристрої фізично підключені до одного комутатора [24].

Однак, використання VLAN не позбавлене ризиків. Однією з основних загроз є атаки типу VLAN hopping, які дозволяють зловмисникам обходити обмеження між VLAN та отримувати доступ до трафіку інших сегментів мережі. Це можливо через неправильну конфігурацію комутаторів або використання стандартного VLAN для кількох портів. Також, недостатня ізоляція між VLAN може призвести до витоку конфіденційної інформації та ускладнити виявлення та реагування на інциденти безпеки.

Для мінімізації цих ризиків рекомендується впроваджувати додаткові заходи безпеки, такі як мікросегментація, використання міжмережевих екранів та політик Zero Trust. Ці методи дозволяють забезпечити більш детальний контроль над трафіком, обмежити можливості для горизонтального переміщення зловмисників у мережі та підвищити загальний рівень захисту інформаційних систем.

Таким чином, хоча VLAN є потужним засобом для логічного поділу мережі, їх ефективне використання вимагає ретельного планування, правильної конфігурації та впровадження додаткових заходів безпеки для забезпечення надійного захисту від потенційних загроз.

1.7.2 VPN як інструмент захисту й потенційна загроза

Віртуальна приватна мережа (VPN) є невід'ємною складовою сучасної інформаційної безпеки, забезпечуючи захищений канал передачі даних через

публічні або ненадійні мережі, такі як Інтернет. Основна мета VPN полягає в створенні зашифрованого тунелю між пристроєм користувача та віддаленим сервером, через який передається весь мережевий трафік. Цей тунель гарантує конфіденційність, цілісність та автентичність переданої інформації, запобігаючи її перехопленню або модифікації третіми сторонами.

Принцип роботи VPN базується на двох ключових технологіях: шифруванні та тунелюванні. Шифрування забезпечує перетворення даних у формат, недоступний для розуміння без відповідного ключа, що унеможливлює їх прочитання у разі перехоплення. Тунелювання, в свою чергу, створює віртуальний канал, через який передається зашифрований трафік, ізолюючи його від загального мережевого середовища. Це дозволяє користувачам безпечно обмінюватися даними, навіть перебуваючи в публічних мережах або використовуючи незахищені точки доступу [25].

Існують різні типи VPN, кожен з яких має свої особливості та сфери застосування. Remote Access VPN дозволяє окремим користувачам підключатися до корпоративної мережі з будь-якого місця, забезпечуючи безпечний доступ до внутрішніх ресурсів. Site-to-Site VPN використовується для об'єднання декількох мереж, наприклад, філій компанії, в єдину захищену мережу. Personal VPN орієнтований на індивідуальних користувачів, надаючи їм можливість захистити свою онлайн-активність та обійти географічні обмеження.

Незважаючи на переваги, використання VPN може супроводжуватися певними ризиками. Однією з поширених проблем є витік DNS-запитів (DNS leak), коли запити на розпізнавання доменних імен обходять зашифрований тунель VPN і надсилаються через стандартні DNS-сервери провайдера, що може призвести до розкриття відвідуваних сайтів. Іншою загрозою є витік реальної IP-адреси користувача, що може статися через неправильну конфігурацію VPN або використання застарілих протоколів, таких як PPTP.

Для мінімізації цих ризиків рекомендується використовувати сучасні протоколи тунелювання, такі як OpenVPN, WireGuard або IPsec з IKEv2, які забезпечують високий рівень шифрування та безпеки. Багатофакторна

автентифікація додає додатковий рівень захисту, вимагаючи від користувача підтвердження особи за допомогою кількох факторів. Використання сертифікатів з коротким строком дії зменшує ймовірність їх компрометації. Жорстке обмеження доступу до внутрішніх ресурсів за принципом мінімальних привілеїв гарантує, що користувачі мають доступ лише до необхідних для їх роботи ресурсів. Моніторинг сесій у режимі реального часу дозволяє виявляти та реагувати на підозрілу активність. Механізм "kill switch" автоматично розриває інтернет-з'єднання у разі втрати VPN-з'єднання, запобігаючи витоку даних. Використання DNS over HTTPS забезпечує шифрування DNS-запитів, захищаючи їх від перехоплення.

VPN є потужним інструментом для забезпечення безпеки та конфіденційності в мережах, однак його ефективне використання вимагає правильного впровадження, налаштування та постійного моніторингу. Тільки за умови дотримання всіх рекомендацій та найкращих практик VPN може повністю виконувати свою функцію захисту даних та забезпечення безпечного доступу до мережевих ресурсів.

2 АНАЛІЗ ТА ОБГРУНТУВАННЯ ТЕХНОЛОГІЙ

2.1 Аналіз інфраструктури навчального закладу

Розробка структурної схеми пристрою є важливим етапом його розробки. За допомогою структурної схеми можна зрозуміти принцип роботи пристрою, знайти помилки у його роботі. Структурна схема може бути дуже корисним інструментом для візуалізації зв'язків між різними компонентами пристрою, . Якщо пристрій не працює з помилками, структурна схема може допомогти вирішити проблему. Розуміючи, як працює пристрій, ми можемо визначити конкретні компоненти, які можуть спричиняти проблему.

Для реалізації сучасної комп'ютерної мережі було проаналізовано планування та особливості інфраструктури навчального закладу, який складається з двох окремих корпусів: головного (триповерхового) та корпусу початкових класів (двоповерхового), що знаходяться на невеликій відстані одне від одного. Загалом, навчальний заклад включає низку спеціалізованих кабінетів, адміністративних приміщень, загальноосвітніх класів та зон загального доступу.

У структурі школи передбачено наявність трьох комп'ютерних класів. Кожен з них обладнаний 13 стаціонарними комп'ютерами, що потребують підключення до локальної мережі з високою пропускною здатністю та надійним доступом до Інтернету. Для забезпечення ефективної передачі даних у цих класах доцільно використовувати комутатори з підтримкою стандарту Gigabit Ethernet.

Крім того, в адміністративному відділі розміщено ~10 комп'ютерів, які будуть під'єднані до окремого VLAN-сегменту з розширеними правами доступу та підвищеним рівнем безпеки. Саме в адміністративному блоці доцільно передбачити встановлення основного серверного обладнання, включаючи DHCP-сервер, DNS-сервер, а також пристрої маршрутизації з реалізованими механізмами NAT, ACL та VPN.

Для навчального процесу у вчительській розташовано 15 комп'ютерів; у звичайних класах (українська мова, англійська мова, математика, фізика, хімія, біологія) передбачено використання по одному комп'ютеру та SmartTV на кожен

кабінет. Додатково, у п’яти початкових класах також передбачено використання по кілька комп’ютерів, кілька ноутбуків та телевізорів із підтримкою Wi-Fi. Для забезпечення підключення ноутбуків, та телевізорів до мережі по бездротовому каналу використовуються Wi-Fi маршрутизатори (точки доступу). Загалом планується встановити 3 точки доступу, розміщених у різних частинах навчального закладу для покриття всієї площі.

Орієнтовний розподіл робочих місць показано в таблиці 2.1.

Таблиця 2.1 — Потреби школи-ліцею

	Кількість приміщень	Кількість ПК	Кількість інших інтернет речей(SmartTV, телефони вчителів, сервери)
Адміністрація	3	5	–
Комп’ютерні класи	3	39	6
Загальноосвітні кабінети та вчительська	17	17	32
Початкові класи	6	10	6
Серверна зона	1	1	3
Разом	29	72	47

Для побудови безпечної та масштабованої мережі буде реалізовано розподіл на VLAN:

— окремий VLAN для адміністрації;

— VLAN для комп’ютерних класів;

— VLAN для учнів середніх та старших класів;

— VLAN для початкових класів;

— VLAN для Серверної зони та керуючого пк.

Також мережа передбачає централізоване керування доступом, маршрутизацію між VLAN-сегментами, шифрування VPN-з’єднань для

захищеного віддаленого доступу та використання фільтрації трафіку за допомогою списків контролю доступу (ACL).Загальна кількість активних клієнтських пристроїв становить понад 100 одиниць, що вимагає ретельно спроєктованої логічної та фізичної топології мережі.

2.2 Розподіл адресного простору мережі

Для забезпечення ефективної маршрутизації та ізоляції трафіку між різними сегментами мережі навчального закладу було прийнято рішення про використання приватного IP-адресного простору згідно з RFC 1918. Основним діапазоном для розподілу адрес обрано мережу 192.168.0.0/16, яка буде поділена на підмережі за допомогою технології VLAN.Кожному логічному сегменту (віртуальній локальній мережі) призначено окрему підмережу, як наведено у таблиці 2.2

Таблиця 2.2 — Розподіл адрес кожному сегменту школи-ліцею

VLAN	Назва сегменту	CIDR	Кількість пристроїв	Призначення
10	Адміністрація	192.168.10.0/28	5-10	Бухгалтерія, дирекція
20	Комп’ютерні класи	192.168.20.0/26	39	Учнівські ПК, вчительські ПК
30	Загальноосвітні кабінети та вчительська	192.168.30.0/26	~39	Пристрої вчителів
40	Початкові класи	192.168.40.0/27	~22	Ноутбуки та SmartTV початкових класах
50	Серверна зона	192.168.50.0/29	~4	Сервери та ПК для доступу керування обладнанням

Процес структуризації мережевого середовища навчального закладу передбачає раціональне використання доступного простору адрес, що забезпечує

відповідність вимогам комунікації, безпеки та адміністрування. Для ефективного управління мережевою інфраструктурою були визначені логічні сегменти, кожен з яких відповідає певній функціональній зоні закладу. Відповідно до призначення кожного сегмента було здійснено ретельний аналіз необхідної кількості адресних ідентифікаторів, щоб гарантувати баланс між актуальними потребами та перспективами розширення.

Адміністративний сектор відіграє ключову роль у забезпеченні роботи бухгалтерії та керівництва навчального закладу. В межах цього сегмента працює від 5 до 10 пристроїв, включаючи комп'ютери працівників, сервери для збереження документації та мережеве обладнання для доступу до централізованих інформаційних систем. Кількість адрес у цьому секторі визначена таким чином, щоб забезпечити стабільну роботу існуючих пристроїв та залишити простір для можливого розширення у разі збільшення штату працівників або впровадження нових цифрових інструментів управління.

Сегмент, що відповідає за роботу комп'ютерних класів, об'єднує значну кількість техніки — загалом 39 учнівських та вчительських комп'ютерів. Простір адрес у цьому секторі підібраний так, щоб гарантувати достатню кількість унікальних мережевих ідентифікаторів для кожного пристрою, враховуючи потенційні зміни в структурі навчального процесу. Окрім основних робочих станцій, цей сегмент може включати додаткові мережеві вузли, такі як принтери, інтерактивні панелі або допоміжні сервери, що забезпечують функціонування освітніх програм.

Зона загальноосвітніх кабінетів та робочих місць педагогічного персоналу є ще одним важливим структурним компонентом мережі. В межах цього сегмента функціонує близько 39 пристроїв, до яких належать персональні комп'ютери вчителів, допоміжне обладнання для забезпечення навчального процесу, а також пристрої для адміністрування доступу до навчальних матеріалів. Простір адрес у цій зоні структурований таким чином, щоб гарантувати гнучкість у розширенні цифрових освітніх ініціатив, включаючи інтеграцію додаткових мультимедійних інструментів.

Сегмент, що забезпечує роботу початкових класів, включає приблизно 22 пристрої, серед яких ноутбуки, мультимедійні панелі та інтерактивні екрани. Обраний формат організації адресного простору враховує специфіку молодшої шкільної програми, яка передбачає активне використання цифрових ресурсів. Завдяки цьому можна гнучко масштабувати навчальну техніку та адаптувати мережеві ресурси відповідно до потреб освітнього процесу.

Окремо слід розглядати серверну зону, що забезпечує керування всією мережею навчального закладу. У цьому сегменті функціонує близько 4 пристроїв, включаючи сервери, мережеві контролери та робочі станції адміністраторів. Розподіл адресного простору у даному секторі побудований таким чином, щоб підтримувати надійність зв’язку та безпеку обробки даних. Завдяки чітко структурованій системі управління забезпечується безперебійна робота критично важливих служб, що гарантує стабільність всієї мережі.

Усі підмережі мають достатній резерв адрес для масштабування. Межі кожної VLAN строго дотримуються за допомогою списків контролю доступу (ACL), а міжвланова маршрутизація виконується на рівні маршрутизатора або L3-комутатора.

Сервер DHCP надає IP-адреси динамічно для користувацьких VLAN (20, 30, 40), тоді як серверна зона та адміністративні пристрої можуть бути налаштовані зі статичними адресами. Для доступу до Інтернету використовується NAT-трансляція, реалізована на маршрутизаторі із зовнішнім інтерфейсом, підключеним до провайдера.

Загальна організація адресного простору комп’ютерної мережі навчального закладу побудована таким чином, щоб відповідати принципам ефективності та безперебійності функціонування. Це рішення забезпечує не лише поточну працездатність, а й можливість динамічного вдосконалення.

2.3 Сегментація адресного простору мережі

Комп’ютерна мережа школи-ліцею побудована з урахуванням сучасних вимог до безпеки, продуктивності та ефективного використання мережевих

ресурсів. Загальна структуризація інформаційного середовища здійснена на основі логічної сегментації, що дозволяє гнучко керувати потоками даних та забезпечити стабільний зв’язок між різними підрозділами закладу. Для досягнення цих цілей були впроваджені віртуальні локальні мережі VLAN, що забезпечують розмежування трафіку на рівні другого шару OSI-моделі, а маршрутизація між ними організована за допомогою протоколу OSPF, який гарантує швидку конвергенцію маршрутів та стабільну роботу мережевих вузлів. Основним принципом, що закладено у проектування мережі, є адаптивність до змін у кількості пристроїв, безперервність роботи та зручність адміністрування.

На рівні фізичного з’єднання мережа містить кілька ключових секторів, кожен із яких обслуговує певну категорію пристроїв відповідно до їхнього функціонального призначення. Адміністративний сегмент включає комп’ютери дирекції та бухгалтерії, яким відведено окремий логічний блок. Його параметри визначено на основі поточного рівня навантаження та перспектив розширення. Враховуючи обмежене число пристроїв у цьому секторі, обраний формат адресного простору дозволяє не лише забезпечити всі наявні потреби, а й залишити додатковий резерв у разі збільшення кількості робочих станцій. Комп’ютерні класи утворюють один із найбільш насичених інформаційних вузлів, оскільки в межах цього сегмента функціонує значна кількість учнівських та викладацьких ПК. Вибір параметрів адресації обґрунтований тим, що в перспективі може виникнути необхідність розширення цього простору, тому під час проектування було передбачено запас для нових підключень без необхідності повної зміни маршрутизаційних політик.

Аналогічним чином структурована зона загальноосвітніх кабінетів, де розміщено пристрої викладацького складу, які використовуються для підготовки навчальних матеріалів та інтеграції мультимедійного контенту до освітнього процесу. В межах цього сегмента реалізовані механізми, що дозволяють мінімізувати внутрішні взаємодії між окремими категоріями пристроїв і забезпечити пріоритетний доступ до ресурсів для службових обчислень. Початкові класи мають окрему підмережу, яка адаптована до специфіки

навчального процесу у молодших групах. Вона містить ноутбуки та інтерактивні панелі, необхідні для організації навчального простору, а також передбачає можливість поступового розширення із збереженням стабільності мережевого середовища.

Серверна зона у структурі мережі школи-ліцею виконує функцію централізованого вузла для керування доступом до обчислювальних ресурсів, забезпечуючи маршрутизацію даних між локальними вузлами та зовнішніми інформаційними системами. Тут розміщені сервери, які відповідають за безперебійний доступ до навчальних матеріалів, розгортання внутрішніх сервісів та підтримку загальної продуктивності мережевого середовища. Важливим аспектом роботи цього сегмента є його оптимізована взаємодія з магістральними вузлами, що здійснюють маршрутизацію потоків даних, тому конфігурація серверного простору враховує необхідність підтримки максимальної стабільності та ізоляції критично важливих інформаційних потоків.

Вибір OSPF як основного механізму маршрутизації в мережі школи-ліцею був зумовлений вимогами до швидкої адаптації у разі змін у структурі з’єднань та мінімізації затримок при передачі даних між логічними сегментами. На відміну від RIP, що працює на основі періодичного обміну таблицями, OSPF дозволяє здійснювати миттєве оновлення маршрутів без зайвого навантаження на комунікаційні канали. Завдяки цьому кожен вузол у мережі отримує актуальну інформацію про стан зв’язності без необхідності чекати певний часовий інтервал для оновлення параметрів. Додатковою перевагою є можливість точного налаштування метрик вартості маршрутів, що дозволяє забезпечити пріоритетний доступ до основних каналів зв’язку, зокрема оптоволоконних магістралей, які використовуються для стабільного доступу до зовнішніх сервісів.

Всі VLAN у мережі школи-ліцею підключені безпосередньо до маршрутизатора через підінтерфейси, що дозволяє централізовано керувати маршрутизацією та зберігати гнучкість у налаштуванні логічних сегментів. Така схема значно спрощує адміністрування, оскільки кожен підінтерфейс можна

налаштувати окремо з урахуванням вимог конкретного сегмента. В результаті загальна структура мережі гарантує ефективне розподілення ресурсів без ризику перевантаження вузлів.

Для взаємодії між корпусами навчального закладу використовується схема статичної маршрутизації, що забезпечує точне прогнозування проходження пакетів без зайвих службових запитів. Усі внутрішні префікси вже згорнуті у компактні адресні блоки, тому застосування OSPF на цьому рівні не дає суттєвих переваг. Завдяки статичним маршрутам оператор отримує можливість швидко аналізувати точки відмови без необхідності перегляду змін у таблицях маршрутизації. Це рішення також сприяє збереженню ресурсів, оскільки маршрутизатор не витрачає обчислювальні потужності на динамічне оновлення маршрутів.

Загальна конфігурація мережевого середовища школи-ліцею орієнтована на довготривалу стабільність та адаптивність до змін у структурі обладнання. Використання VLAN, маршрутизації OSPF у межах логічних сегментів та статичних маршрутів між магістральними вузлами забезпечує баланс між автоматизацією та точлістним керуванням мережевими ресурсами. Завдяки цим технологічним рішенням навчальний заклад отримує можливість підтримувати ефективну інформаційну інфраструктуру без потреби у регулярному перегляді адресації або значних змінах у конфігурації обладнання. Це дозволяє зберігати мережу гнучкою, продуктивною та готовою до подальшого розвитку.

2.4 Технології забезпечення безпеки комп’ютерної мережі

Комп’ютерна мережа ліцею №1 реалізована з урахуванням актуальних вимог до інформаційної безпеки та організована з акцентом на централізований контроль трафіку, захищене адміністрування й базову фільтрацію доступу на межі з глобальною мережею. Основний захист реалізовано на головному маршрутизаторі, який виступає як точка входу та виходу до зовнішньої мережі, водночас виконуючи функції маршрутизації, фільтрації та шифрування.

На периметрі мережі встановлено міжмережевий екран у вигляді вбудованого брандмауера на маршрутизаторі, який підтримує механізми stateful-інспекції з аналізом стану з’єднання та глибокою перевіркою пакетів. Через нього дозволяється лише певний набір сервісів, наприклад, HTTPS та DNS, тоді як інші запити блокуються за замовчуванням, зокрема ті, що пов’язані з небезпечними або застарілими протоколами, такими як Telnet, FTP чи SMB. Весь інший трафік, який не відповідає заданим правилам, автоматично відкидається, що дозволяє зменшити площу потенційної атаки та обмежити можливості для несанкціонованого доступу.

Для детальнішого контролю застосовано списки контролю доступу (ACL), які виконують фільтрацію на основі IP-адрес, номерів портів і протоколів. Зокрема, дозволено лише вихідні з’єднання з певних локальних підмереж до конкретних зовнішніх ресурсів, при цьому блокуються будь-які вхідні з’єднання, не ініційовані зсередини. ACL розміщено безпосередньо на інтерфейсах маршрутизатора, що дозволяє фільтрувати трафік «якнайближче до джерела».

Важливим компонентом безпеки виступає організація захищеного віддаленого доступу до мережевого обладнання. Для цього використовується VPN-тунелювання на основі протоколу IPsec з використанням ISAKMP для обміну ключами. Шифрування забезпечується алгоритмами із використанням стійких криптографічних методів, що гарантує цілісність та конфіденційність адміністративного трафіку. Доступ до VPN надається виключно адміністраторам з визначених IP-адрес, що дозволяє обмежити можливість несанкціонованих підключень ззовні.

Управлінські інтерфейси маршрутизатора та інші критичні служби доступні лише через VPN-з’єднання, що додатково ізолює їх від звичайного трафіку. Навіть за відсутності окремих VLAN або спеціалізованих сегментів, трафік до інтерфейсів адміністрування фільтрується окремими правилами ACL, що дозволяє ефективно обмежити доступ до ключових ресурсів.

Журналювання подій безпеки налаштовано через вбудовану систему логування маршрутизатора. Усі спроби підключення, автентифікації та помилки

передаються до централізованого лог-сервера або зберігаються локально з подальшою обробкою. Це дозволяє проводити аналіз активності та швидко реагувати на інциденти безпеки. Система також дозволяє фіксувати зміни в конфігурації, що особливо важливо для контролю над змінами мережевої інфраструктури.

2.4.1 Налаштування списків доступу ACL

У структурі комп'ютерної мережі школи-ліцею №1 реалізовано централізовану маршрутизацію на основі маршрутизатора Cisco 2911, що виконує роль основного маршрутизатора для всієї локальної інфраструктури. Для виходу в глобальну мережу використовується окремий маршрутизатор Cisco 2811, який відповідає за NAT та фільтрацію зовнішнього трафіку. Завдяки використанню підінтерфейсів на маршрутизаторі 2911, забезпечується логічне розділення трафіку між VLAN, із подальшим застосуванням ACL (Access Control Lists) для реалізації політики безпеки.

Ключовим елементом мережевої безпеки є розширені списки доступу (Extended ACL), які ретельно визначають дозволений та заборонений трафік між сегментами VLAN. Сегменти VLAN 10 та VLAN 50 мають пріоритет у політиці безпеки, оскільки містять критичні компоненти інфраструктури: адміністративні комп'ютери та сервери з DHCP, DNS і локальним вебсервером. Саме ці VLAN найбільше ізольовані від решти мережі.

Водночас важливо, щоб VLAN 10 та 50 мали змогу взаємодіяти з усіма іншими сегментами для реалізації централізованого управління та обслуговування. Наприклад, у VLAN 10 необхідно дозволити DNS-запити до сервера у VLAN 50, доступ до внутрішнього вебресурсу по HTTPS, а також вихід у глобальну мережу. VLAN 50, крім цього, виконує функції підтримки та обслуговування, отже має доступ до будь-яких інших сегментів для відповіді на запити клієнтів. Водночас у зворотному напрямку — з VLAN 20, 30 та 40 — заборонено доступ до VLAN 10 та до адміністративних сервісів VLAN 50. Єдиним винятком є дозвіл HTTPS-з'єднань з вебклієнтів до вебсервера у VLAN

50, що дозволяє організувати доступ до навчального порталу чи внутрішніх сервісів.

На маршрутизаторі Cisco 2911 використано детальні ACL для фільтрації трафіку на кожному підінтерфейсі. Ці списки враховують IP-адреси кожного VLAN, використовують префіксні маски, а також блокують ICMP, Telnet та SMB-протоколи, які має доступ тільки серверна зона. Особлива увага приділена VPN-з’єднанню, яке дозволяє адміністративному персоналу отримати повний доступ до всієї мережі ззовні, але лише через захищені протоколи (HTTPS, SSH, DNS).Нижче наведено приклад розширеного ACL, що застосовується на інтерфейсі маршрутизатора що під’єднаний до VLAN10, що зображено у лістингу 2.1

Лістинг 2.1 — Початкове налаштування ACL для адміністративного сегменту

```
ip access-list extended VLAN10-IN
 permit tcp 192.168.10.0 0.0.0.31 192.168.50.0 0.0.0.15 eq 443
permit udp 192.168.10.0 0.0.0.31 192.168.50.0 0.0.0.15 eq 53
 permit tcp 192.168.10.0 0.0.0.31 any eq 80
 permit tcp 192.168.10.0 0.0.0.31 any eq 443
 deny   ip any 192.168.10.0 0.0.0.31 log
 permit ip any any
```

Для VLAN 20, 30 та 40 конфігурація подібна, але з явним блокуванням доступу до адміністративного та серверного сегментів, що зображено у лістингу 2.2.

Важливо, що на всіх ACL наприкінці додається команда permit ip any any, яка дозволяє трафік, не описаний раніше в списку, але лише після того, як були заблоковані критичні шляхи. Також усі deny-рядки мають параметр log, завдяки чому записи про відхилені з'єднання надсилаються на сервер Syslog, розміщений у VLAN 50. Це дозволяє адміністраторам здійснювати постійний моніторинг безпеки та швидко реагувати на потенційні загрози або спроби несанкціонованого доступу. Такі фільтри забороняють небезпечні протоколи (Telnet, NetBIOS), обмежують широкомовний трафік і локальні ініціативи користувачів.

Лістинг 2.2 — Початкове налаштування ACL для сегменту комп’ютерних класів

```
ip access-list extended VLAN20-IN
 deny ip 192.168.20.0 0.0.0.63 192.168.10.0 0.0.0.31 log
 deny ip 192.168.20.0 0.0.0.63 192.168.50.0 0.0.0.15 log
 permit tcp 192.168.20.0 0.0.0.63 192.168.50.10 0.0.0.0 eq 443
 permit tcp 192.168.20.0 0.0.0.63 any eq 80
 permit tcp 192.168.20.0 0.0.0.63 any eq 443
 permit udp 192.168.20.0 0.0.0.63 192.168.50.0 0.0.0.15 eq 53
 permit ip any any
```

На деяких комутаторах доступу додатково реалізовано портові ACL, які забезпечують попередню фільтрацію трафіку ще до того, як він досягне маршрутизатора. Це зменшує навантаження на маршрутизатор і підвищує загальну ефективність обробки даних. Такі фільтри забороняють небезпечні протоколи (Telnet, NetBIOS), обмежують широкомовний трафік і локальні ініціативи користувачів.

Під час проєктування мережі особлива увага приділялась VPN-підключенню, яке дає змогу обслуговуючому персоналу здійснювати повний контроль над мережею. VPN має доступ до всієї адресної просторової схеми і може звертатись до всіх внутрішніх VLAN, однак із використанням лише дозволених служб — вебдоступу, DNS, SSH.

2.4.2 Адміністрування брандмауера, та встановлення управління доступом

Брандмауер у даній мережевій архітектурі виконує роль останнього та найзовнішнього захисного рубежу. Саме він контролює весь трафік між локальними підмережами у просторі 10.0.0.0/8 та глобальною мережею Інтернет, що досягається через інтерфейс Se0/3/0 маршрутизатора, якому призначено адресу 213.234.10.1. Основною перевагою такого вузла є централізоване забезпечення безпеки для всіх VLAN.

Зовнішній фільтр працює за принципом stateful-інспекції: запам’ятовуючи встановлені з’єднання, маршрутизатор дозволяє лише повернення відповідей на легітимні запити зсередини. Будь-який пакет, ініційований ззовні без існуючої сесії, блокується негайно, що надійно захищає внутрішні вузли від сканування,

атак типу SYN-Flood чи спроб вторгнення.

Всі внутрішні підмережі отримують вихід до Інтернету через NAT, що транслює їхні адреси на зовнішній IP — 213.234.10.1. Це не лише приховує реальну топологію школи-ліцею, а й ускладнює потенційному зловмиснику спроби прямої ідентифікації вузлів. Сам NAT виконується динамічно з пулу внутрішніх адрес за допомогою списку NAT_INSIDE, який визначає, з яких джерел дозволено трансляцію.

Політика доступу ззовні максимально жорстка. Усі спроби ініціації вхідного з'єднання блокуються. У поточному варіанті мережі не передбачено публікацію DMZ-ресурсів або зовнішніх служб (на кшталт вебсерверів чи VPN-шлюзів), тому дозволені лише зворотні потоки — відповіді на внутрішні HTTPS, DNS або інші запити. Фрагмент конфігурації ACL на головному маршрутизаторі зображено у лістингу 2.3.

Лістинг 2.3 — Початкова конфігурація брандмауера

```
interface Se0/3/0
 description External link to ISP
 ip address 213.234.10.1 255.255.255.252
 ip access-group OUTSIDE_IN in
 ip nat outside
 no shutdown
interface GigabitEthernet0/0
 description Core VLANs 10 & 50
 ip address 10.0.1.1 255.255.255.0
 ip access-group INSIDE_OUT in
 ip nat inside
 no shutdown
interface GigabitEthernet0/1
description VLANs 20 & 30
 ip address 10.0.2.1 255.255.255.0
 ip access-group INSIDE_OUT in
 ip nat inside
 no shutdown
interface GigabitEthernet0/2
description VLAN 40
 ip address 10.0.3.1 255.255.255.0
 ip access-group INSIDE_OUT in
 ip nat inside
 no shutdown
ip access-list extended OUTSIDE_IN
 deny ip any any log
ip access-list extended INSIDE_OUT
 remark Permit HTTPS and HTTP
 permit tcp 10.0.0.0 0.255.255.255 any eq 443
```

```
 permit tcp 10.0.0.0 0.255.255.255 any eq 80
 remark Permit DNS lookups
 permit udp 10.0.0.0 0.255.255.255 any eq 53
 remark Explicit deny for other traffic
 deny ip any any log
ip access-list standard NAT_INSIDE
 permit 10.0.0.0 0.255.255.255
ip nat inside source list NAT_INSIDE interface Se0/3/0 overload
```

Цей набір правил забезпечує:

— ізоляцію внутрішньої мережі від зовнішнього середовища;

— вихід в Інтернет виключно для авторизованого трафіку;

— чіткий контроль і аудит усіх відхилених спроб підключення через параметр log, що надсилається до централізованого Syslog-сервера;

— підтримку NAT-трансляції, що приховує внутрішні адреси за єдиним публічним IP 213.234.10.1.

Завдяки цим налаштуванням навіть у випадку спроби атаки ззовні жоден трафік не досягне серверної або адміністративної VLAN, а спроби вторгнення буде зафіксовано. Такий підхід зберігає архітектурну цілісність мережі та дає змогу оперативно масштабувати захист, зокрема, при впровадженні нових сервісів або розширенні VPN-інфраструктури.

Конфігурація брандмауера рекомендується до регулярного аудиту: наприкінці кожного семестру аналізується журнал Syslog, проводиться оцінка потреб в оновленні портів або сервісів, і вносяться мінімальні зміни до ACL. Таким чином забезпечується актуальність безпеки без порушення стабільної роботи мережевих сегментів.

2.5 Аналіз та обґрунтування використання технології NAT

У мережі навчального закладу NAT (Network Address Translation) є основним механізмом, що дозволяє внутрішнім хостам із приватними IP-адресами отримувати доступ до глобального Інтернету. Уся внутрішня адресація побудована в діапазоні 192.168.0.0/16 — це приватний простір, який не маршрутизується у глобальній мережі. Тому для виходу назовні необхідна трансляція адрес на публічну IP-адресу, видану провайдером. Центральний маршрутизатор, підключений до Інтернету через інтерфейс Serial0/3/0, виконує

роль NAT-шлюзу. Він змінює джерело кожного внутрішнього пакета на публічну IP-адресу (213.234.10.1), зберігаючи унікальний номер порту — така технологія зветься PAT (Port Address Translation), або перевантаження NAT.

Це дозволяє десяткам і сотням пристроїв використовувати одну й ту саму публічну адресу одночасно, без конфліктів. Крім цього, NAT забезпечує базовий рівень безпеки: з Інтернету неможливо ініціювати з’єднання без попереднього запиту зсередини мережі. Завдяки цьому внутрішня структура залишається невидимою для сторонніх, що зображено у лістингу 2.4.

Лістинг 2.4 — Початкове налаштування NAT на головному маршрутизаторі

```
interface Serial0/3/0
 ip address 213.234.10.1 255.255.255.252
 ip nat outside
interface GigabitEthernet0/0
ip address 10.0.1.1 255.255.255.0
 ip nat inside
interface GigabitEthernet0/1
 ip address 10.0.2.1 255.255.255.0
ip nat inside
interface GigabitEthernet0/2
 ip address 10.0.3.1 255.255.255.0
ip nat inside
access-list 1 permit 192.168.0.0 0.0.255.255
ip nat inside source list 1 interface Serial0/3/0 overload
```

Усі внутрішні інтерфейси (G0/0, G0/1, G0/2) позначені як ip nat inside, а зовнішній інтерфейс (Serial0/3/0) — як ip nat outside. Списком доступу access-list 1 дозволяється NAT для всіх джерел з діапазону 192.168.0.0/16. Завдяки команді ip nat inside source list 1 interface Serial0/3/0 overload здійснюється перевантажена трансляція всього внутрішнього трафіку через одну публічну адресу інтерфейсу. Налаштування є простим і гнучким — за потреби адміністратор може додати статичну трансляцію для окремих серверів або змінити обсяг NAT, не змінюючи саму топологію. Це робить NAT незамінною складовою будь-якої мережі з виходом у публічний простір.

2.6 Вибір мережевого обладнання

Для проектування було обрано дворівневу модель комп’ютерної мережі на

основі комутаторів рівня доступу та центрального маршрутизатора, що виконує функції маршрутизації між VLAN, NAT-перетворення, а також транспортування між окремими підмережами та серверною зоною. Архітектура базується на використанні шести 24-портових керованих комутаторів Cisco Catalyst 2960-24TT та чотирьох маршрутизаторів Cisco 2811, один з яких виконує роль граничного вузла з зовнішнім доступом до Інтернету. Додатково інтегровано один сервер DHCP на базі фізичного обладнання для централізованої автоматичної роздачі IP-адрес у внутрішній мережі.

Комутатори Cisco Catalyst 2960-24TT забезпечують достатню кількість портів FastEthernet для підключення кінцевих пристроїв у кожному функціональному блоці закладу: адміністрація, комп'ютерні класи, загальноосвітні кабінети, початкові класи та серверна зона. Обрані моделі підтримують VLAN-сегментацію, статичне резервування портів, обмеження пропускної здатності, моніторинг STP та базову CLI-конфігурацію. Пропускна здатність кожного комутатора у межах 16 Gbps забезпечує безперешкодну передачу трафіку в межах сегментів. Усі пристрої відповідають вимогам стандарту IEEE 802.1Q та підтримують trunk-з'єднання, необхідні для транспортування трафіку між VLAN через маршрутизатори.

Комутатори 2960-24TT були обрані як економічно доцільний і технічно виправданий варіант для рівня доступу, що дозволяє обслуговувати до 24 пристроїв у кожному сегменті. Вони повністю сумісні з Packet Tracer, що дозволяє візуалізувати, тестувати та документувати мережеву інфраструктуру у симуляційному середовищі. Їх програмна архітектура базується на Cisco IOS, що спрощує адміністрування та уніфікує CLI-інтерфейс з іншими пристроями Cisco.

Альтернативи для комутаторів Cisco 2960-24TT на українському ринку представлені в таблиці 2.3. Порівняння включає вартість, кількість портів, наявність PoE, підтримку VLAN та сумісність з Packet Tracer.

З огляду на сумісність, уніфікацію інтерфейсів управління, стабільність програмного забезпечення та вимоги до навчального середовища було обрано саме Cisco Catalyst 2960-24TT.

Таблиця 2.3 — Порівняння комутаторів рівня доступу

Модель	PoE	VLAN	Пропускна здатність	Ціна (грн)	Сумісність з Packet Tracer
Cisco Catalyst 2960-24TT	Ні	Так	16 Gbps	~9 500	Так
TP-Link JetStream T1600-28PS	Так	Так	12.8 Gbps	~8 300	Ні
MikroTik CSS326-24G-2S+RM	Ні	Так	52 Gbps	~7 600	Ні
Ubiquiti UniFi Switch 24	Так	Так	26 Gbps	~10 500	Ні

З огляду на сумісність, уніфікацію інтерфейсів управління, стабільність програмного забезпечення та вимоги до навчального середовища було обрано саме Cisco Catalyst 2960-24TT.

У якості маршрутизаторів міжмережевого рівня обрано чотири пристрої Cisco 2811, що підтримують протоколи OSPF, NAT, ACL, DHCP Relay та працюють на операційній системі Cisco IOS. Ці пристрої мають можливість розширення через модулі HWIC/WIC, включаючи інтерфейси FastEthernet, DSL, Serial та голосові порти. Таке апаратне виконання дозволяє масштабувати кількість інтерфейсів залежно від потреб мережі, у тому числі із можливістю підключення до зовнішніх провайдерів.

Cisco 2811 призначені для маршрутизації між VLAN-сегментами, організації NAT для доступу до Інтернету, реалізації політик безпеки через ACL та передачі DHCP-запитів від кінцевих пристроїв до DHCP-сервера. Додатковий маршрутизатор Cisco 2811 використовується як граничний маршрутизатор із виходом у зовнішнє середовище через WAN-інтерфейс (Serial).

Cisco 2811 було обрано як оптимальний варіант завдяки модульній побудові, гнучкості конфігурації та повній сумісності з Packet Tracer. Це забезпечує уніфікацію із вибраними комутаторами та дозволяє реалізувати багатофункціональну маршрутизацію з мінімальними витратами на інтеграцію.

Порівняльна таблиця 2.4 демонструє можливі альтернативи на ринку з

аналогічною функціональністю, але різним рівнем масштабованості та ціною.

Таблиця 2.4 — Порівняння моделей маршрутизаторів

Модель маршрутизатора	WAN-порти	Пропускна здатність	NAT / VPN / ACL	Слоти HWIC	CLI	Середня ціна, грн
Cisco 2811	2x FE	до 45 Мбіт/с	Так	2	Так	12 500
MikroTik RB4011	10x GE	до 1 Гбіт/с	Частково	Ні	Так	9 700
Ubiquiti EdgeRouter 4	3x GE	до 3,4 Гбіт/с	Частково	Ні	Частково	11 200
TP-Link ER7206	1x GE WAN, 1x GE LAN	до 1 Гбіт/с	Частково	Ні	Обмежено	7 500

Орієнтовна вартість обраного обладнання подана у таблиці 2.5 за середніми цінами на українському ринку станом на травень 2025 року.

Таблиця 2.5 — Орієнтовна вартість мережевого обладнання

Пристрій	Кількість	≈ Ціна за од., грн	Підсумок, грн
Cisco Catalyst 2960-24TT	7	9 500	66 500
Cisco 2811	5	11 500	57 500
DHCP-сервер (HW + SW)	1	37 000	37 000
Разом	—	—	161 000

Обране мережеве обладнання відповідає усім технічним вимогам щодо побудови комп’ютерної мережі середнього навчального закладу з розрахунком на подальше масштабування. Комбінація перевірених пристроїв Cisco, зокрема моделей 2960-24TT та 2811, дозволяє забезпечити стабільну, уніфіковану й керовану інфраструктуру з підтримкою VLAN, міжвланової маршрутизації, DHCP, NAT та безпечного підключення до зовнішніх ресурсів.

3 РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ

3.1 Проєктування фізичної та логічної топології мережі

Під час реалізації комп'ютерної мережі школи-ліцею необхідно було поєднати технічні вимоги з обмеженим бюджетом і наявним обладнанням. У проєкті використано ієрархічну модель мережі, що складається з трьох рівнів: ядра, розподілу та доступу. Така архітектура дозволяє оптимізувати трафік, спростити адміністрування та забезпечити масштабованість у майбутньому. Кожен рівень виконує окремі функції, що сприяє підвищенню надійності та гнучкості інфраструктури.

Ядро мережі реалізовано за допомогою маршрутизаторів Cisco 2811, які забезпечують маршрутизацію між окремими VLAN та між корпусами школи. Центральний маршрутизатор з'єднує інші маршрутизатори за допомогою Gigabit-зв'язків, які формують резервовану топологію з високою пропускною здатністю. Для міжкорпусної комунікації виділено підмережу 192.168.100.0/30. Такий підхід забезпечує централізований контроль і високу швидкість обміну між ключовими сегментами мережі.

На рівні розподілу використовуються також маршрутизатори Cisco 2811, які розташовані у кожному корпусі та відповідають за агрегацію трафіку від комутаторів доступу. Вони об'єднані в єдину зону динамічного маршрутизування OSPF (Area 0). Це дає змогу досягти швидкої конвергенції та автоматичного переналаштування маршрутів у разі аварії. OSPF також спрощує масштабування, дозволяючи легко інтегрувати нові підмережі або корпуси.Логічна тополоя всієї мережі школи-ліцею зображена на рисунку 3.1

Комутатори рівня доступу — Cisco Catalyst 2960-24TT — встановлені в аудиторіях та технічних приміщеннях. Вони підключені до маршрутизаторів через trunk-порти, що передають кілька VLAN одночасно. Завдяки підтримці Rapid-PVST+ забезпечується відмовостійкість без суттєвих затримок, а функція Auto-MDIX полегшує монтаж без потреби в кросоверах. Комутатори мають 24 порти FastEthernet, чого достатньо для підключення всіх необхідних пристроїв з резервом на майбутнє.

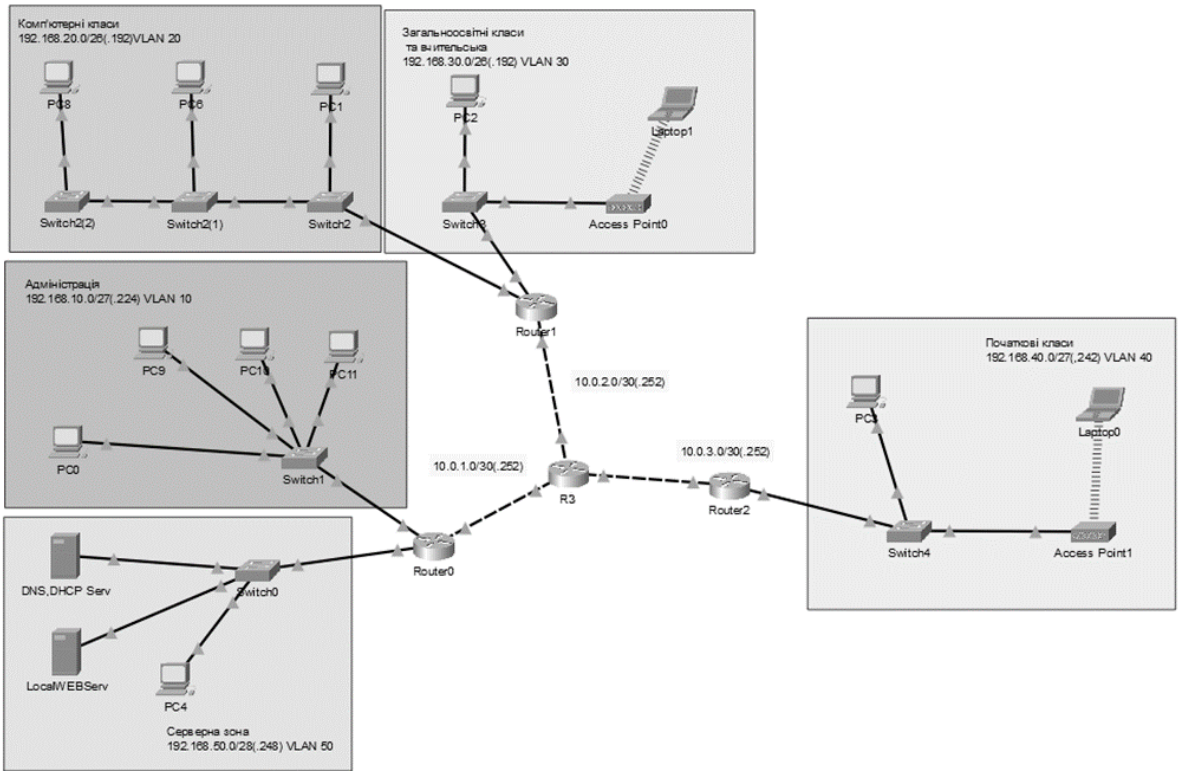


Рисунок 3.1 — Логічна топологія мережі школи-ліцею

Фізичне розташування мережевого обладнання узгоджено з архітектурною структурою школи, яка складається з двох основних корпусів: старшої школи (зображено на рисунку 3.2) та молодшої школи (рисунок 3.3). Загалом охоплено 29 приміщень, включно з навчальними класами, адміністративними кабінетами, технічними та серверними кімнатами. У кожному приміщенні передбачено наявність комп’ютерного або іншого мережевого обладнання, зокрема IoT-пристроїв, які забезпечують автоматизацію певних процесів (наприклад, систем контролю доступу, відеоспостереження або клімат-контролю).

Всі ці пристрої фізично підключені до комутаторів доступу, що встановлені у відповідних слаботочних шафах або серверних приміщеннях на кожному поверсі. Комутатори доступу з’єднані з маршрутизаторами, які обслуговують відповідні поверхи або сегменти мережі, забезпечуючи передачу даних у межах локальної мережі та її маршрутизацію до інших VLAN або зовнішніх ресурсів.

Центральна серверна зона, яка функціонує як ядро мережевої інфраструктури, розташована окремо від основних потоків користувацького трафіку — це підвищує рівень безпеки та стабільності. У цій серверній, що

входить до VLAN 50, розміщено основні мережеві сервіси школи, зокрема сервери DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol) і WEB-сервер для внутрішніх потреб. Така організація дозволяє централізовано керувати конфігурацією мережі, забезпечувати автоматичну видачу IP-адрес, а також розміщувати веб-ресурси, доступні в межах внутрішньої мережі.

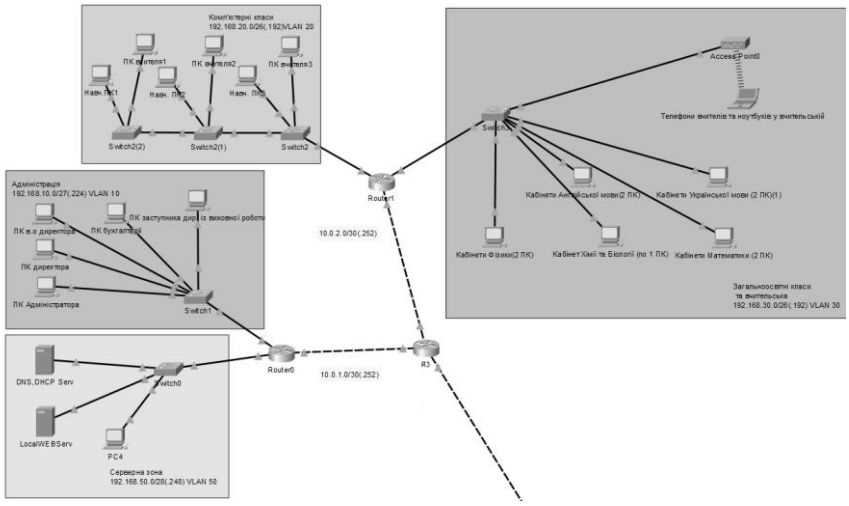


Рисунок 3.2 — Фізична топологія старшого корпусу (3 поверхи)

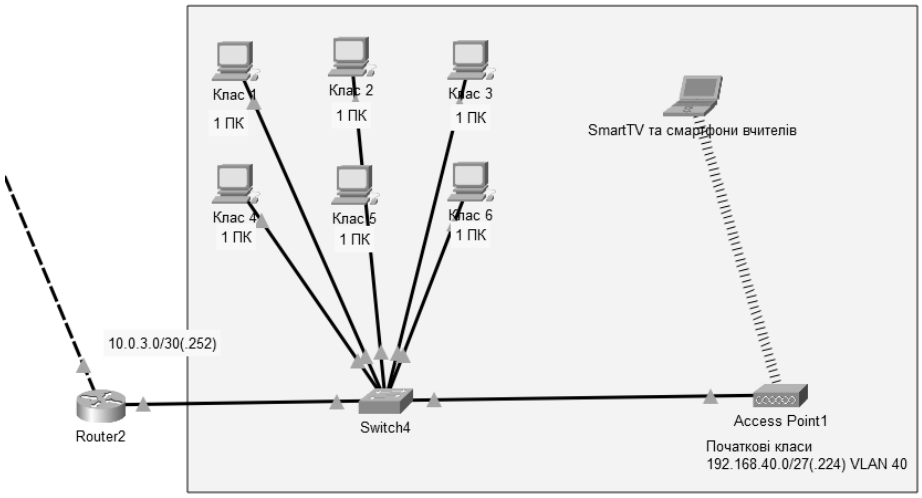


Рисунок 3.3 — Фізична топологія молодшого корпусу (2 поверхи)

Завдяки такому поділу кожен функціональний сегмент мережі ізольовано на рівні 2-го рівня OSI, що підвищує безпеку та дозволяє будувати гнучкі політики доступу. DHCP Relay налаштовано на маршрутизаторах, які перенаправляють broadcast-запити з усіх VLAN до централізованого DHCP-

сервера. Це дає змогу видавати IP-адреси швидко та зберігати централізований облік MAC-адрес пристроїв.

Далі буде показаний вміст інтерфейса командного рядку (CLI) в процесі налаштування та моніторингу пристроїв комп'ютерної мережі. На рисунку 3.4 міститься вивід команди show vlan brief у консоль, що підтверджує коректне створення VLAN і їхній активний стан. Також на рисунку 3.5. показано команду show spanning-tree vlan 40, де видно Rapid-PVST+ у дії.

```
Switch#sh vlan br

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Gig0/1, Gig0/2
40   Primary                             active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                   Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                   Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                   Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                   Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                   Fa0/21, Fa0/22, Fa0/23
1002 fddi-default                        active
1003 token-ring-default                  active
1004 fddinet-default                     active
1005 trnet-default                       active
```

Рисунок 3.4 — Результат виконання команди show vlan brief (підтвердження VLAN)

```
Switch#sh spanning-tree vlan 40
VLAN0040
  Spanning tree enabled protocol ieee
  Root ID     Priority    32808
              Address     00E0.F793.76D7
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32808  (priority 32768 sys-id-ext 40)
              Address     00E0.F793.76D7
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/6            Desg FWD 19        128.6    P2p
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    Shr
Fa0/5            Desg FWD 19        128.5    P2p
Fa0/4            Desg FWD 19        128.4    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/24           Desg FWD 19        128.24   P2p
```

Рисунок 3.5 — Результат виконання команди show spanning-tree vlan 40

На рисунку 3.6 представлено консольний вивід команди show ip route, що

підтверджує появу префікса поверху в таблиці маршрутизації та його анонсування через OSPF. Скриншот ілюструє взаємодію без використання агрегованих каналів, акцентуючи увагу на гнучкості конфігурації та рівні відмовостійкості, забезпеченому протоколами spanning-tree та OSPF.

```
Router# sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 213.234.10.2 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C       10.0.1.0/30 is directly connected, FastEthernet0/0
L       10.0.1.1/32 is directly connected, FastEthernet0/0
C       10.0.2.0/30 is directly connected, FastEthernet0/1
L       10.0.2.1/32 is directly connected, FastEthernet0/1
C       10.0.3.0/30 is directly connected, FastEthernet1/0
L       10.0.3.1/32 is directly connected, FastEthernet1/0
     192.168.10.0/27 is subnetted, 1 subnets
O       192.168.10.0/27 [110/2] via 10.0.1.2, 02:32:00, FastEthernet0/0
     192.168.20.0/26 is subnetted, 1 subnets
O       192.168.20.0/26 [110/2] via 10.0.2.2, 00:56:09, FastEthernet0/1
     192.168.30.0/26 is subnetted, 1 subnets
O       192.168.30.0/26 [110/2] via 10.0.2.2, 02:31:50, FastEthernet0/1
     192.168.40.0/27 is subnetted, 1 subnets
O       192.168.40.0/27 [110/2] via 10.0.3.2, 02:31:50, FastEthernet1/0
     192.168.50.0/29 is subnetted, 1 subnets
O       192.168.50.0/29 [110/2] via 10.0.1.2, 02:32:00, FastEthernet0/0
     213.234.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       213.234.10.0/30 is directly connected, Serial0/3/1
L       213.234.10.1/32 is directly connected, Serial0/3/1
S*   0.0.0.0/0 [1/0] via 213.234.10.2
```

Рисунок 3.6 — Результат виконання команди show ip route (OSPF)

На рисунку 3.7 наведено консольний вивід команди `show vtp status`, де відображається, що комутатор працює в режимі **Server**. Це забезпечує централізоване управління конфігурацією VLAN, яка поширюється на інші мережеві пристрої. Усі корпуси дотримуються єдиного шаблону налаштувань, що уніфікує процес конфігурації.

У майбутньому масштабування мережі (додавання нових поверхів або корпусів) відбуватиметься шляхом повторення шаблону підключення VLAN і

пристроїв. Це гарантує уніфікований підхід до адміністрування та зменшує вірогідність помилок.

```
Switch#sh vtp status
VTP Version capable             : 1 to 2
VTP version running             : 1
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0001.C9C6.C000
Configuration last modified by 0.0.0.0 at 3-1-93 00:52:09
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN :
--------------
VTP Operating Mode                : Server
Maximum VLANs supported locally   : 255
Number of existing VLANs          : 6
Configuration Revision            : 2
MD5 digest                        : 0x20 0x77 0xE5 0x8D 0x42 0xD2 0x24 0xE8
                                    0x3A 0x14 0x86 0x6F 0x30 0xF5 0x9C 0x04
```

Рисунок 3.7 — Результат виконання команди show vtp status

Завдяки правильному проєктуванню топології, мережа школи-ліцею є надійною, масштабованою та економічно обґрунтованою. Вона забезпечує якісне покриття для 72 ПК та 47 IoT-пристроїв, розподілених по 29 приміщеннях у двох корпусах.

3.2 Базове налаштування мережевого обладнання DHCP

Налагодження служби автоматичної роздачі IP-адрес за допомогою DHCP у межах комп’ютерної мережі навчального закладу передбачає попереднє розміщення віртуального сервера на схемі проєкту у середовищі Cisco Packet Tracer. Для цього використовується стандартний мережевий пристрій типу Server, доступний у відповідному наборі компонентів симулятора. Сервер підключається за допомогою прямого мідного кабелю до службового маршрутизатора, який має фізичне з'єднання з комутатором рівня ядра Cisco Catalyst 2960 через порт GigabitEthernet0/1. Вказаний порт комутатора надалі переводиться до окремої службової VLAN із номером 40, призначеної для потреб адміністрування та централізованого керування мережею. На сервері вручну задаються основні параметри IP-конфігурації: IP-адреса 192.168.50.3, маска

підмережі 255.255.255.248, шлюз за замовчуванням 192.168.40.1. Це дає змогу забезпечити коректну маршрутизацію між сервером і вузлами інших логічних сегментів.

Для забезпечення повноцінної взаємодії серверної частини з периферійними пристроями необхідно внести зміни до таблиць маршрутів. На комутаторі третього рівня (Layer 3) створюється статичний маршрут до підмережі, в якій знаходиться DHCP-сервер, а на службовому маршрутизаторі додається статичний маршрут до всієї підмережі поверху — 192.168.40.0/24. Це гарантує наявність логічного шляху для доставки DHCP-запитів у разі міжвланової маршрутизації.

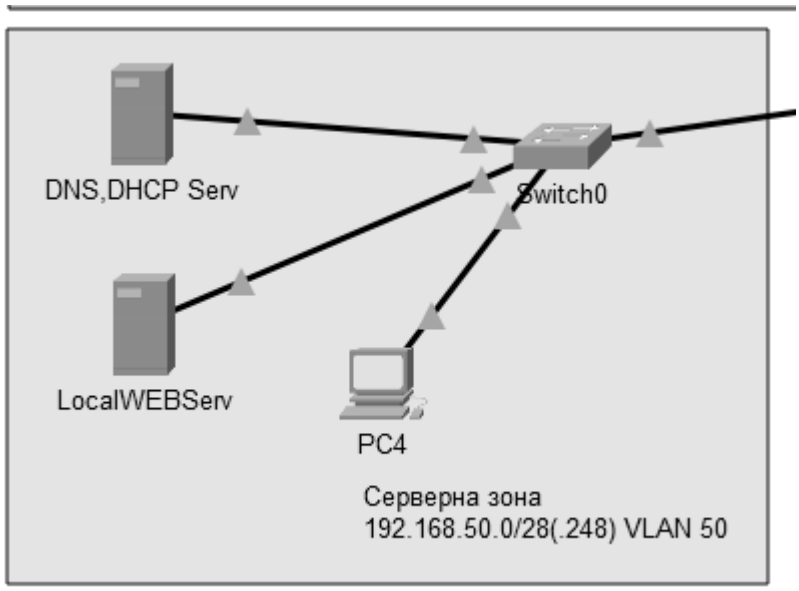


Рисунок 3.8 — Підключення DHCP-сервера до ядра мережі та VLAN40

Після завершення етапу фізичного та логічного підключення виконується активація маршрутизації на комутаторі Cisco 2960 шляхом введення глобальної команди ip routing, яка дозволяє використовувати інтерфейси VLAN як маршрутизовані інтерфейси третього рівня. Далі конфігурується інтерфейс VLAN40. Йому надається IP-адреса 192.168.40.2 з маскою 255.255.255.224. Окрім цього, вказується IP-адреса допоміжного сервера DHCP — 192.168.50.3 — за допомогою команди ip helper-address, що активує функціонування DHCP-релєя. Цей механізм дозволяє пристроям, підключеним до VLAN40, автоматично отримувати IP-конфігурацію, навіть якщо DHCP-сервер фізично розташований у

іншій підмережі.

Лістинг 3.1 — Конфігурація інтерфейсу VLAN40 на комутаторі з DHCP-relay

```
interface vlan 40
 ip address 192.168.40.2 255.255.255.224
 ip helper-address 192.168.50.3
 no shutdown
```

На самому сервері конфігурування служби DHCP починається з переходу до вкладки Services, де обирається пункт DHCP. Далі натискається кнопка Add, після чого створюється новий пул з назвою VLAN40, зображено у рисунку 3.9. У полі стартової адреси зазначається 192.168.40.2, у масці — 255.255.255.224, у полі шлюзу — 192.168.40.1. DNS-сервером задається IP-адреса 192.168.50.3. Автоматично визначене значення параметра Maximum Users встановлюється на 30, що відповідає допустимій кількості активних клієнтів у зазначеному діапазоні адрес. Після збереження налаштувань, процедура повторюється для інших VLAN, що потребують автоматичної адресації. Завершальний етап — активація служби DHCP натисканням кнопки On у верхній частині вікна інтерфейсу. Це забезпечує готовність сервера до обробки запитів клієнтів із різних логічних сегментів.

Для перевірки правильності функціонування DHCP-релєя здійснюється тестове підключення клієнтського пристрою. ПК під’єднується до порту FastEthernet0/1 комутатора Cisco 2960, встановленого на першому поверсі старшого корпусу. У графічному інтерфейсі ПК відкривається вкладка Desktop, потім розділ IP Configuration, де обирається параметр DHCP. Протягом короткого проміжку часу пристрій отримує динамічно призначені параметри: IP-адресу 192.168.40.2, маску підмережі /27, шлюз за замовчуванням 192.168.40.1, DNS-сервер 192.168.50.3. Факт автоматичного отримання адреси підтверджує коректну роботу DHCP-релєя, відсутність помилок у маршрутах та функціональність усієї архітектури динамічного конфігурування. Таким чином, реалізоване рішення дозволяє ефективно керувати IP-адресним простором і централізовано обслуговувати всі кінцеві пристрої комп’ютерної мережі школи-

ліцею без залучення локальних DHCP-серверів у кожному сегменті, зображено у рисунку 3.10.

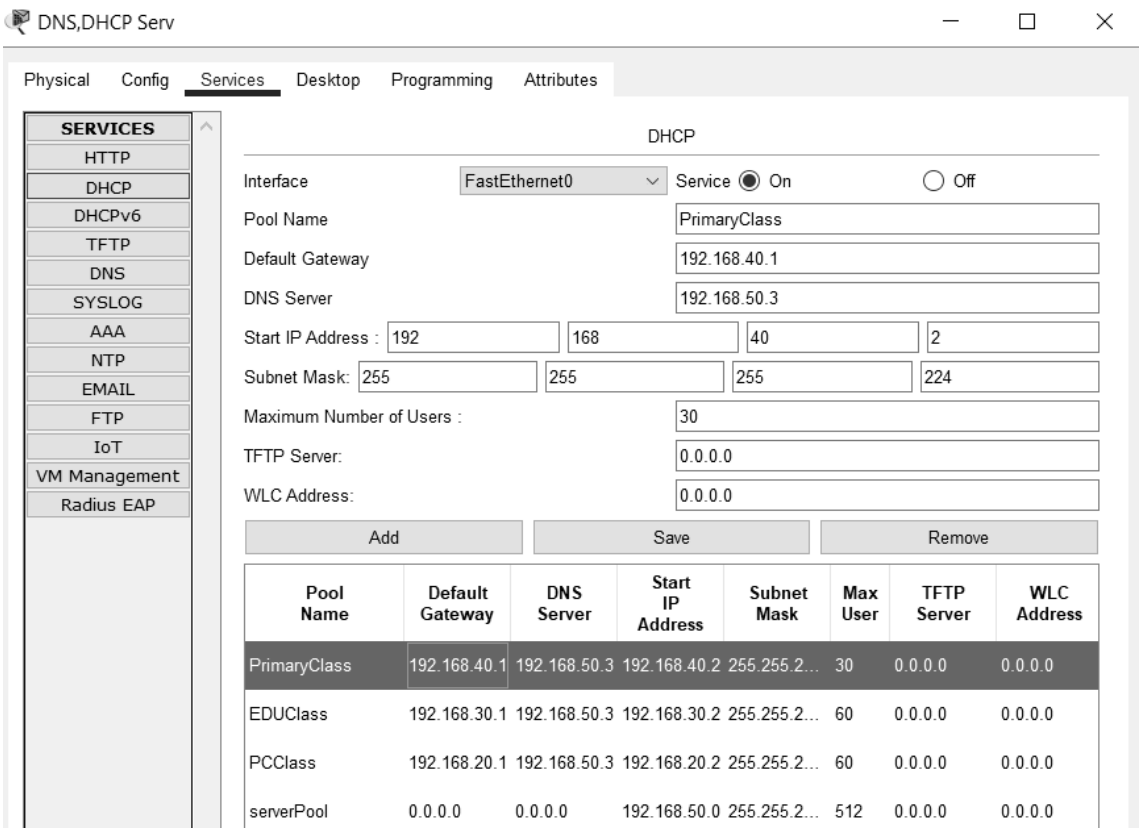


Рисунок 3.9 — Створення DHCP-пулу для VLAN40 та активація служби DHCP

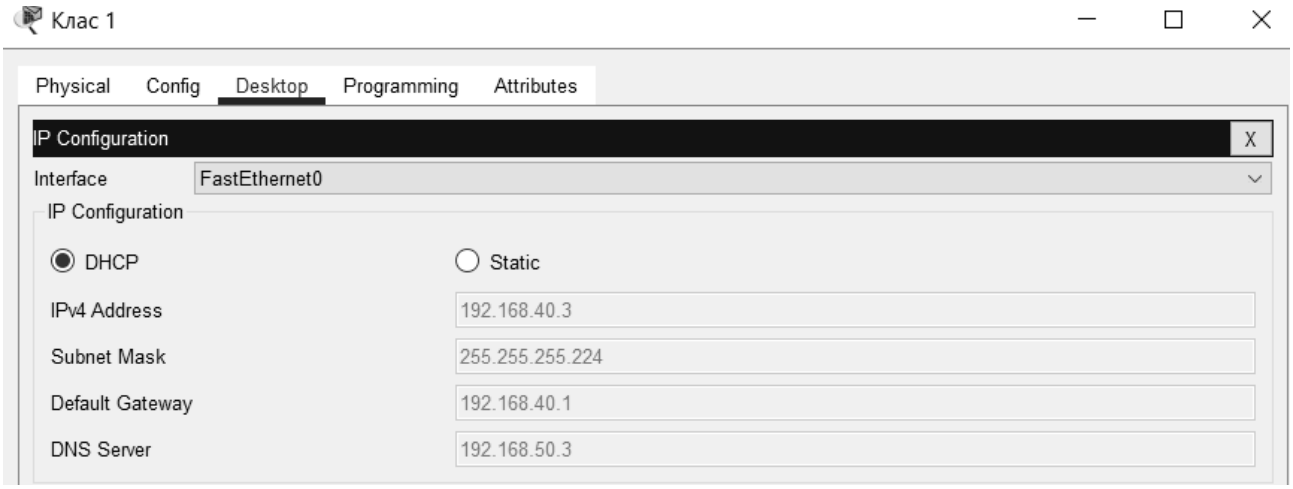


Рисунок 3.10 — Автоматичне отримання IP-конфігурації клієнтом через DHCP-релєй

3.3 Налаштування VPN IPsec для захищенного віддаленого доступу

У сучасній освітній інфраструктурі важливою вимогою до мережевої

архітектури є можливість безпечного дистанційного доступу до локальних ресурсів, особливо для IT-персоналу та адміністрації. В умовах школи-ліцею №1 така потреба реалізується шляхом впровадження тунельного з'єднання за допомогою протоколу VPN на основі IPsec. Це дозволяє адміністраторам та довіреним віддаленим користувачам підключатися до внутрішніх сегментів мережі, зокрема до VLAN 10 (Адміністрація) та VLAN 50 (Серверна зона), при цьому зберігаючи суворий контроль доступу.

Фізично реалізація VPN передбачає маршрутизацію вхідного трафіку з глобальної мережі через маршрутизатори R5 та R4, які імітують підключення до зовнішнього провайдера. Основна VPN-конфігурація виконується на маршрутизаторі Router0, що підключений до підмереж VLAN 10 і VLAN 50. Його інтерфейс G0/0 є точкою прийому з'єднань з Інтернету (через мережу 10.0.1.0/30).

Перед налаштуванням VPN-з'єднання необхідно переконатися, що маршрутизатор підтримує криптографічні служби. Далі формується політика ISAKMP — набір параметрів, що визначають, яким чином відбуватиметься початковий обмін ключами. Тут застосовуються сучасні криптографічні алгоритми, такі як AES для шифрування та SHA-256 для хешування. Для автентифікації використовується попередньо визначений ключ, узгоджений між сторонами, що зображено у лістингу 3.2.

Лістинг 3.2 — Налаштування політики ISAKMP та ключа VPN

```
crypto isakmp policy 10
 encryption aes
 hash sha256
 authentication pre-share
 group 14
crypto isakmp key SCHOOLVPN address 213.234.20.2
```

Далі налаштовується трансформаційний набір для IPsec — він вказує, які алгоритми шифрування і перевірки цілісності будуть використовуватись під час передачі трафіку. Створюється IPsec-профіль(лістинг 3.3) у вигляді crypto map, де зазначається IP-адреса віддаленого VPN-піра, трансформаційний набір та список доступу, що визначає, який саме трафік підлягає шифруванню.

Лістинг 3.3 — Налаштування IPsec профілю

```
crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
crypto map SCHOOL-MAP 10 ipsec-isakmp
 set peer 213.234.20.2
 set transform-set VPN-SET
 match address 110
```

Далі створюється ACL, яка описує дозволені сеанси: у даному випадку — дозволений доступ з підмережі VPN-клієнтів (умовно 192.168.100.0/24) до двох локальних сегментів: адміністративного і серверного(лістинг 3.4). Це забезпечує контрольований доступ виключно до потрібних служб.

Лістинг 3.4 — Створення списків доступа для адміністративного та серверного сегментів

```
access-list 110 permit ip 192.168.10.0 0.0.0.127 192.168.100.0 0.0.0.255
access-list 110 permit ip 192.168.50.0 0.0.0.7 192.168.100.0 0.0.0.255
```

Після налаштування карти шифрування її потрібно прикріпити до зовнішнього інтерфейсу маршрутизатора. Це активує механізм IPsec на відповідному інтерфейсі. Додатково у випадку реалізації VPN з динамічною адресацією на стороні клієнта можливе використання Virtual Tunnel Interface (VTI) або Easy VPN. Проте у цьому проєкті реалізовано класичне Site-to-Site з фіксованою IP-адресою віддаленого піра (213.234.20.2), що відповідає реальній топології.

Для перевірки успішного встановлення тунелю використовуються діагностичні команди. Вони дозволяють проаналізувати статус фази 1 (ISAKMP SA) та фази 2 (IPsec SA), а також кількість зашифрованих пакетів. Важливою перевагою такого підходу є те, що IPsec VPN дозволяє безпечно передавати дані навіть через публічні канали зв’язку, зберігаючи конфіденційність та цілісність інформації. У межах цього проєкту реалізовано централізовану точку входу через Router0, що забезпечує легкість моніторингу, управління доступом та інтеграцію з існуючою інфраструктурою (Syslog, VLAN, ACL).

Завдяки IPsec VPN адміністратор може з будь-якого місця виконати керування локальними серверами (наприклад, DNS/DHCP та WEB), а також дистанційно підтримувати внутрішні ресурси без необхідності прямого

фізичного доступу. Це особливо актуально для технічного обслуговування у позаурочний час або під час дистанційної роботи.

3.4 Тестування комп’ютерної мережі

Після завершення етапів конфігурації всієї інфраструктури школи-ліцею №1, виконується комплексне тестування працездатності мережі з метою перевірки правильності реалізації як фізичних з’єднань, так і логічних налаштувань. Насамперед увага зосереджується на апаратному стані мережевих пристроїв. Візуальний контроль індикаторів портів дозволяє переконатися в активності всіх лінків, а також у наявності живлення на кінцевих пристроях, зокрема точках доступу з підтримкою PoE. У разі виявлення неактивних інтерфейсів, колізій або помилок на статистиці портів, імовірною причиною може бути некоректне підключення кабелю, що усувається ще до проведення подальших перевірок.

На наступному етапі виконується аналіз коректності IP-адресації у кожному з віртуальних локальних сегментів (VLAN). Декілька комп’ютерів у різних VLAN конфігуруються на автоматичне отримання мережевих параметрів через DHCP. Успішне отримання правильної IP-адреси, маски підмережі, шлюзу за замовчуванням та DNS-сервера свідчить про належну роботу служби DHCP та коректне перенаправлення запитів через DHCP relay на рівні комутаторів. За відсутності відповіді з боку сервера одразу локалізується сегмент, у якому виникла помилка.

Після підтвердження стабільної адресації переходять до перевірки внутрішньої маршрутизації між підмережами в межах навчального корпусу. За допомогою тестових робочих станцій, розташованих у різних VLAN та на різних поверхах, імітується взаємодія між окремими мережевими сегментами. Успішна передача даних між ними підтверджує, що внутрішній динамічний протокол маршрутизації OSPF зійшовся, сформував таблиці маршрутизації та визначив оптимальні шляхи.

Додатково виконується міжкорпусна перевірка. Один із тестових

комп’ютерів намагається здійснити доступ до сервера, розміщеного в іншому приміщенні школи. Якщо з’єднання встановлюється без затримок, це вказує на правильну реалізацію статичних маршрутів, які забезпечують зв’язок між логічно відокремленими ділянками мережі.

З метою оцінки ефективності магістральних каналів проводиться короткочасне навантажувальне тестування. Одночасна передача великих файлів з кількох робочих станцій дозволяє проаналізувати пропускну здатність мережі. За відсутності затримок і втрат під час копіювання можна зробити висновок, що конфігурація магістральних з’єднань відповідає потребам навчального процесу.

Фінальним етапом базового тестування є перевірка відмовостійкості мережевої інфраструктури. Один із основних кабельних лінків між вузлами штучно відключається, після чого спостерігається за поведінкою трафіку. Якщо підключення клієнтів не переривається, а усі сервіси залишаються доступними, це свідчить про правильну реалізацію протоколу резервування spanning-tree та динамічну перебудову маршрутів у межах OSPF. Це підтверджує, що мережа здатна витримати одиничний фізичний збій без критичного впливу на функціонування.

3.5 Тестування у межах локальної мережі

У процесі побудови корпоративної мережі навчального закладу критично важливим етапом є перевірка міжвіртуальної маршрутизації в межах локальної інфраструктури корпусів. Особливу увагу приділяють аналізу взаємодії між різними VLAN, які належать до одного фізичного сегмента — наприклад, до одного поверху або блоку комутаторів доступу. Така перевірка дозволяє переконатися, що логічна сегментація, яка реалізована для ізоляції трафіку між службовими підрозділами, не перешкоджає внутрішній взаємодії й підтримує належну швидкодію.

У рамках одного з таких тестувань було обрано VLAN 10, призначену для адміністрації, та VLAN 50, у якій функціонує серверна зона. Обидві ці VLAN фізично підключені до інтерфейсу GigabitEthernet 0/1 та GigabitEthernet 0/2

маршрутизатора Cisco 2911. На тестових кінцевих пристроях, розташованих у цих VLAN, виконується взаємний обмін даними, який передбачає передавання ICMP-запитів і звернення до внутрішнього веб-сервера, розташованого у VLAN 50. Як показують результати перевірки(рисунок 3.11), мережеві пакети успішно передаються з одного сегмента до іншого, минаючи access-комутатори та потрапляючи на маршрутизатор, де реалізовано логічні інтерфейси SVI для відповідних VLAN.

Трафік між VLAN 10 і VLAN 50 маршрутизується виключно через внутрішню мережу без виходу в глобальний Інтернет, а шлюзові інтерфейси налаштовані коректно. На всіх тестових пристроях було зафіксовано стабільну відповідь на ICMP-запити та коректну роботу служб прикладного рівня. Зокрема, ПК у VLAN 10 мав змогу звернутися до веб-інтерфейсу серверного обладнання у VLAN 50, що свідчить про наявність правильного маршруту та відсутність обмежень з боку списків контролю доступу (ACL), які регламентують допустимість такої взаємодії.

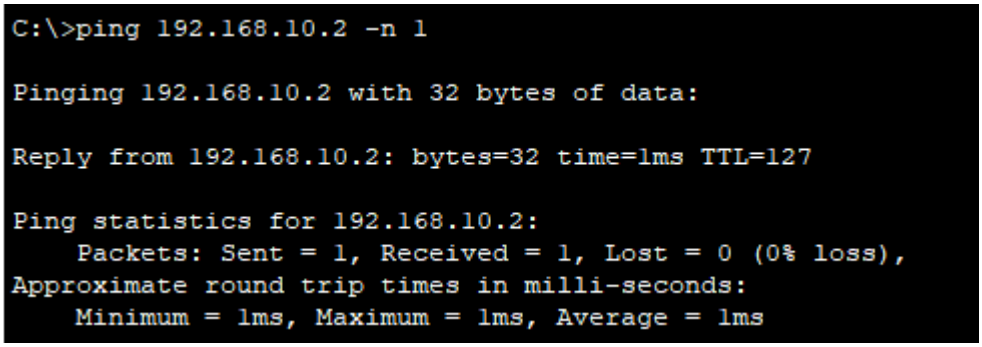


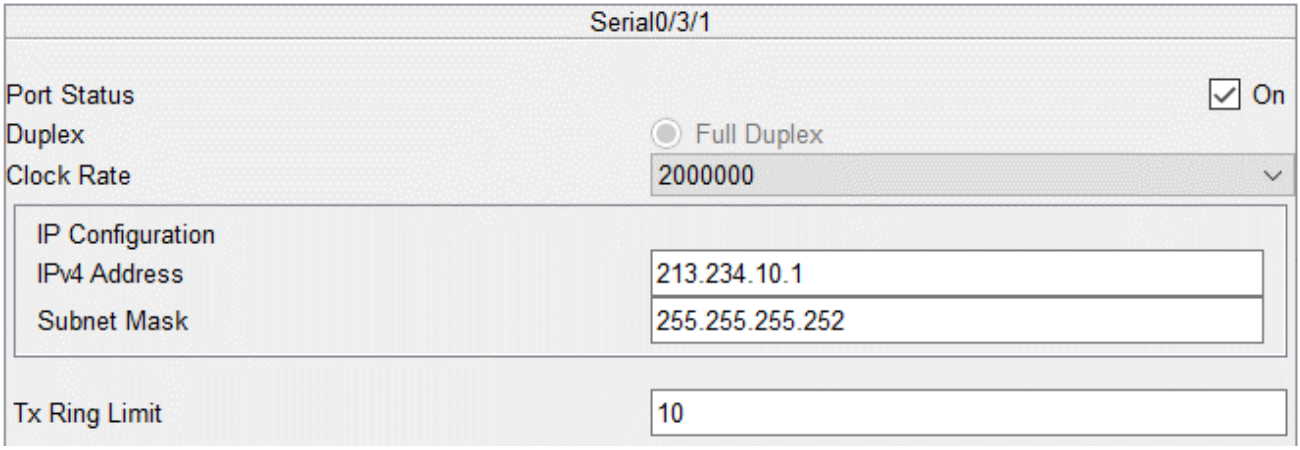
Рисунок 3.11 — Передача пакетів між ПК в локальній мережі

3.6 Тестування комп’ютерної мережі до глобального інтернету

Тестування доступу до глобальної мережі виконувалося для перевірки працездатності маршрутизації, трансляції адрес NAT та доступності зовнішніх ресурсів з внутрішніх сегментів локальної мережі. Для цього в структурі Cisco Packet Tracer було змодельовано підключення шкільного маршрутизатора Cisco 2811 до провайдерського маршрутизатора через серійний інтерфейс Se0/3/0. На цьому інтерфейсі було встановлено IP-адресу 213.234.10.1 з маскою

255.255.255.252, а на стороні провайдера — 213.234.10.2/30, як вказано на рисунку 3.12. З’єднання здійснювалося за допомогою послідовного кабелю (Serial DCE), при цьому на провайдерському маршрутизаторі вручну вказувалася тактова частота командою clock rate 64000, що дозволяло забезпечити синхронізацію каналу.

На провайдерському маршрутизаторі до Ethernet-інтерфейсу FastEthernet0/0 було підключено зовнішній сервер, який виконував роль публічного ресурсу. Цей сервер отримав адресу 213.234.20.5/30, а шлюзом для нього виступала IP-адреса 203.234.20.6, призначена на інтерфейсі маршрутизатора провайдера(рисунок 3.13). На сервері було активовано службу HTTP




```
interface Serial0/3/0
 no ip address
 ip access-group FIREWALL_IN in
 ip nat outside
 clock rate 2000000
```

Рисунок 3.12 — Налаштування серійного інтерфейсу головного маршрутизатора

Тестування здійснювалося з внутрішньої станції VLAN 10. Спочатку виконувалися пінги до шлюзу 10.0.1.1, далі — до зовнішнього інтерфейсу 213.234.10.2, після чого — до публічного сервера 203.0.113.1. На кожному етапі отримувалася відповідь, що свідчило про успішну маршрутизацію,що зображено у рисунку 3.14).

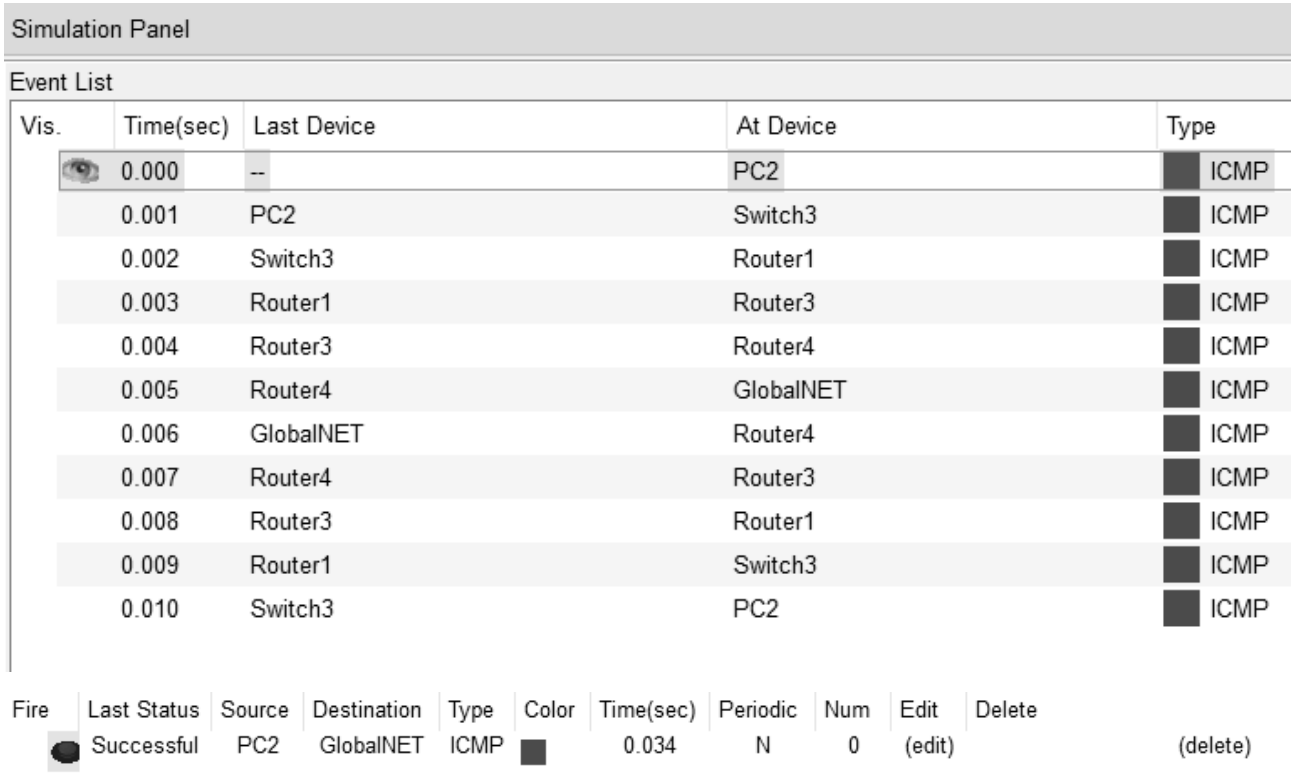


Рисунок 3.14 — Перевірка підключення з клієнтської машини

Налаштування HTTP-служби на сервері та перевірка доступу до неї через браузер з різних клієнтських пристроїв забезпечує створення базової інфраструктури для обміну веб-контентом у локальній мережі школи-ліцею. Тестування проводилося з використанням різних операційних систем і браузерів, що гарантує коректну взаємодію між усіма пристроями та забезпечує кросплатформену сумісність.

Ця система дозволяє централізовано зберігати та розповсюджувати навчальні матеріали, створюючи єдину точку доступу до спільних ресурсів, необхідних для освітнього процесу. HTTP-сервіс виступає платформою для розміщення методичних рекомендацій, електронних навчальних матеріалів та результатів лабораторних робіт учнів.

Коректне відображення сторінок schoolnet(що відкритий у локальній мережі школи ліцею) та globalnet у браузері підтверджує правильність конфігурації мережевих параметрів, маршрутизації та брандмауера, що є основою для подальшого розгортання більш складних веб-застосунків, зображено на рисунку 3.15. Це дозволяє реалізувати внутрішні освітні портали,

системи управління контентом або цифрові платформи для дистанційного навчання в межах мережі школи-ліцею.

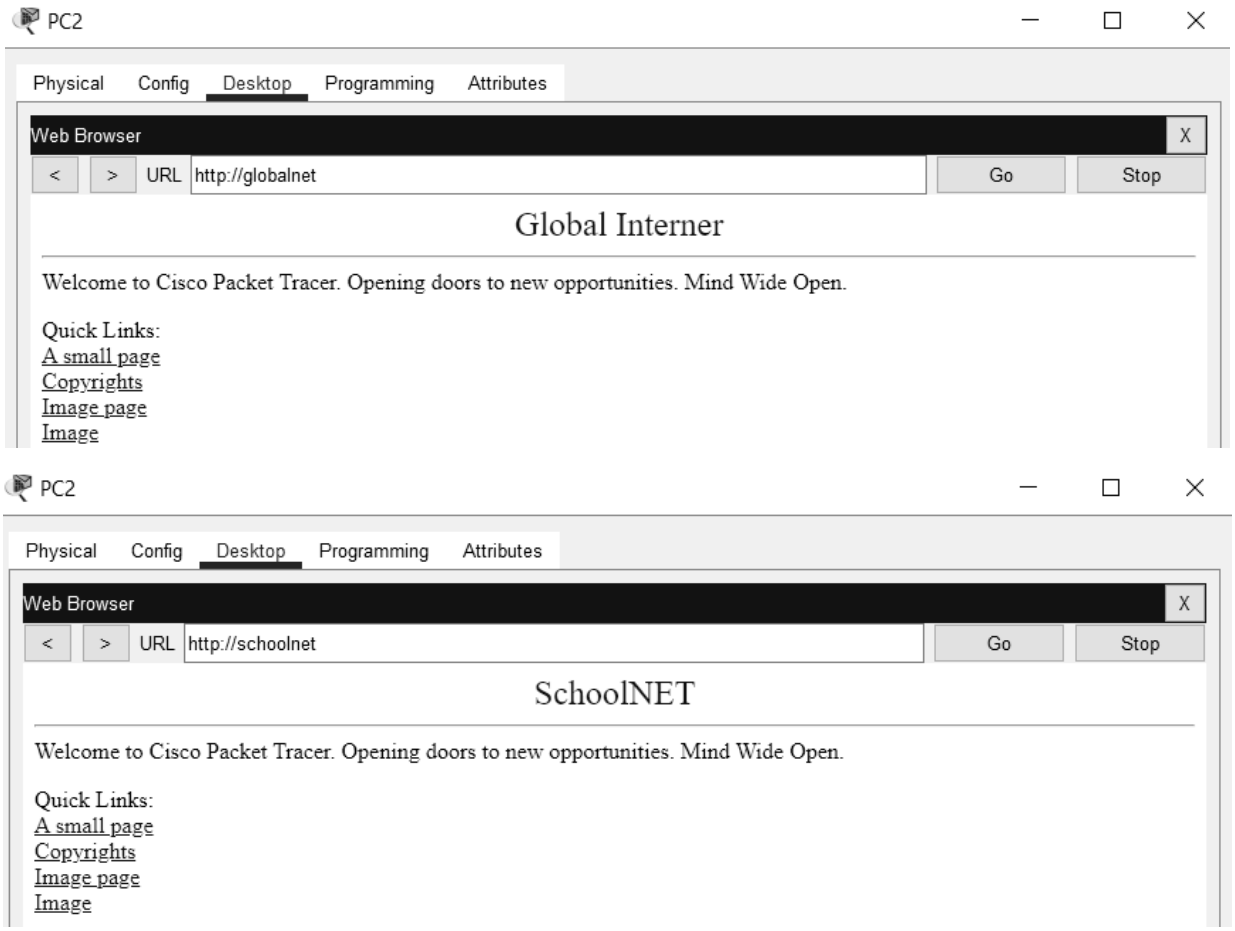


Рисунок 3.15 —Перевірка роботи глобального та локального з’єднання

3.7 Тестування функціонування комп’ютерної мережі

У межах локальної мережі школи-ліцею первинне тестування розпочинається з перевірки працездатності кожного VLAN-сегмента. На цьому етапі з кінцевих пристроїв, підключених до різних VLAN, виконується перевірка зв’язку з власним шлюзом за допомогою ICMP-запитів. Надалі здійснюється обмін пакетами між хостами в межах однієї підмережі. Успішні відповіді на ping-запити підтверджують правильне налаштування IP-адрес, відсутність конфліктів ARP та стабільну роботу access-портів на комутаторах доступу. Додатково перевіряється, що trunk-з’єднання між комутаторами та маршрутизаторами пропускають лише дозволені VLAN-и. Це важливо для недопущення помилок у VLAN-фільтрації, які можуть призвести до часткової ізоляції мережі.

На наступному етапі тестується міжвланова маршрутизація. Кожна тестова станція, що належить до певного VLAN, надсилає ICMP-запити на шлюзи інших VLAN, які реалізовані у вигляді SVI на маршрутизаторі Cisco 2911. Додатково використовується команда traceroute, яка дозволяє простежити маршрут пакетів через усі проміжні мережеві пристрої. У випадку коректного маршрутування пакети долають усі необхідні вузли мережі без втрат та з мінімальною затримкою. Це підтверджує, що таблиці маршрутизації на центральному маршрутизаторі містять записи про всі внутрішні підмережі, а комутація між інтерфейсами працює коректно.

Третім кроком виконується перевірка функціонування NAT. З одного з внутрішніх клієнтів запускаються ping-запити до зовнішнього інтерфейсу маршрутизатора (наприклад, 213.234.10.2), а також до змодельованого зовнішнього сервера з IP-адресою 213.234.20.5. На маршрутизаторі командою show ip nat translations переглядається таблиця активних трансляцій. Якщо видно, що внутрішні IP-адреси перетворюються на зовнішню адресу, що відповідає інтерфейсу Serial0/3/0, а зовнішні сервери успішно відповідають на запити.

Паралельно здійснюється перевірка роботи DHCP, ACL та SSH. DHCP Relay на маршрутизаторі коректно передає запити до централізованого DHCP-сервера, після чого клієнти отримують IP-адресу, маску підмережі, шлюз і DNS-сервер. Робота списків контролю доступу перевіряється спробами звернення до заборонених VLAN: наприклад, клієнт VLAN 20 пробує надіслати запит на веб-сервер VLAN 50, однак відповідь не надходить — отже, правила ACL спрацювали. Водночас підключення через SSH дозволене лише з IP VLAN 50 — спроба встановлення з’єднання з іншого сегмента завершується відмовою.

Завершальне тестування пов’язане з перевіркою стабільності й надійності мережі. Для цього використовуються команди ping з великою кількістю пакетів (ping 192.168.50.4 repeat 100) і вбудований генератор трафіку Packet Tracer (вкладка Simulation). Спостерігається, що середній час проходження пакетів не перевищує 1 мс, втрати відсутні, інтерфейси не фіксують помилок, а завантаження процесорів мережевого обладнання залишається в межах норми

навіть при активному використанні мережі.

3.7.1 Перевірка маршрутизації між підмережами

Для перевірки маршрутизації між підмережами, що обслуговують різні корпуси навчального закладу, здійснюється обмін ICMP-запитами між кінцевими пристроями, розташованими у відповідних VLAN. З одного з клієнтів у VLAN першого корпусу надсилається ping-запит на віртуальні інтерфейси VLAN другого корпусу та центрального вузла. Якщо всі запити отримують позитивні відповіді без втрат пакетів і з незначною затримкою, це свідчить про коректну маршрутизацію, правильну взаємодію між маршрутизаторами агрегаційного рівня та центральним маршрутизатором, а також про відсутність помилок у конфігурації VLAN і маршрутів(рисунок 3.16).

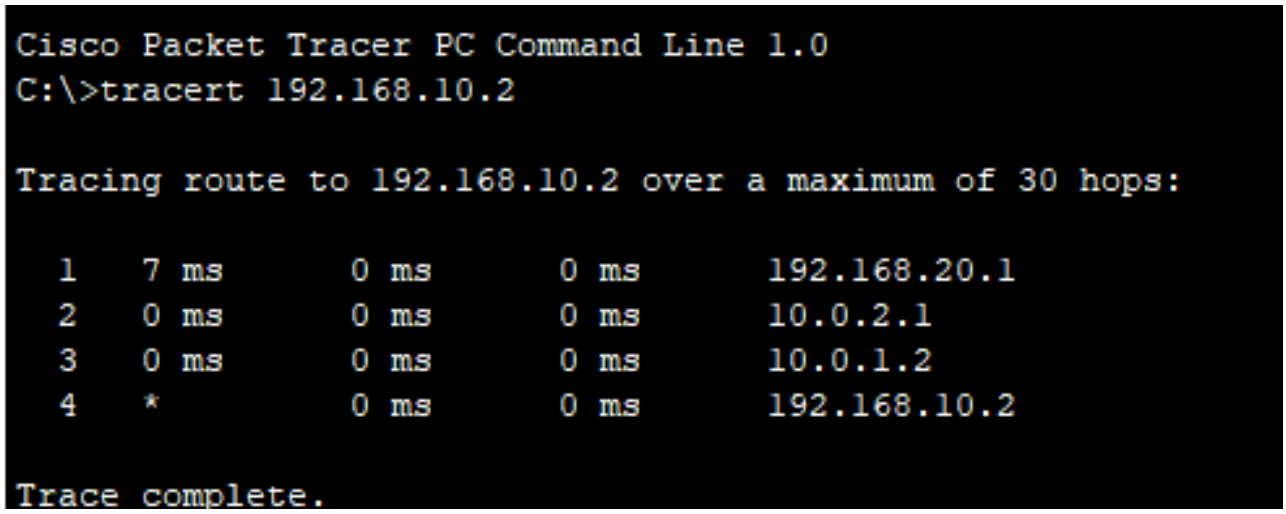


Рисунок 3.16 — Перевірка зв’язку між корпусами

Команда traceout дозволяє відобразити повний маршрут руху пакетів між вузлами, показуючи кожен проміжний хоп — інтерфейси маршрутизаторів і комутаторів третього рівня. Якщо вивід команди містить IP-адреси всіх очікуваних проміжних точок без втрат або затримок типу «Request timed out», це підтверджує стабільність міжкорпусного зв’язку, правильну реалізацію маршрутизації та відсутність недоступних ділянок(рисунок 3.17).

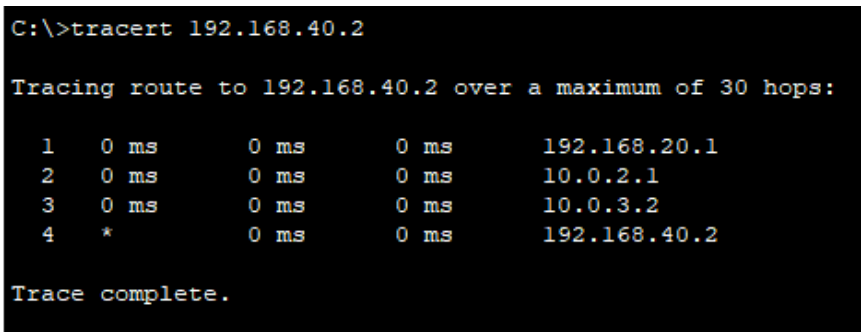


Рисунок 3.17 — Вивід команди traceroute для перевірки маршруту шляху пакету

3.7.2 Перевірка роботи NAT та DHCP

Щоб реалізувати PAT-NAT на центральному маршрутизаторі у межах глобального сегмента мережі, спочатку виконується маркування інтерфейсів відповідно до їхнього призначення. Усі інтерфейси, які з'єднані з внутрішніми мережами — наприклад, ті, що підключені до комутаторів третього рівня корпусів — позначаються як ip nat inside. Натомість зовнішній канал, що з’єднує мережу з провайдером (в даному випадку інтерфейс Serial0/3/1 з IP-адресою 213.234.10.2/30), визначається як ip nat outside. Це дозволяє системі NAT розрізняти трафік зсередини та ззовні. Приклад такого налаштування наведено в лістингу 3.5.

Після цього створюється список доступу, який охоплює всі приватні підмережі університету, наприклад 10.0.1.0/24 та 10.0.2.0/24. Цей список використовується для визначення джерел трафіку, що підлягають трансляції. Далі застосовується команда перевантаженого NAT (overload), що дозволяє великій кількості внутрішніх клієнтів одночасно використовувати одну публічну IP-адресу – тобто адресу зовнішнього інтерфейсу маршрутизатора. Це забезпечує ефективне використання адресного простору та безперебійну взаємодію з Інтернетом(лістинг 3.6).

Лістинг 3.5 — Послідовність налаштування розділення NAT-простору

```
interface Serial4/0
 ip address 10.0.3.13 255.255.255.252
 ip nat outside
 no shutdown
```

```
interface Gig0/1
 ip nat inside
interface Gig0/2
 ip nat inside
```

Лістинг 3.6 — Створення списків доступу

```
access-list 1 permit 10.0.1.0 0.0.0.255
access-list 1 permit 10.0.2.0 0.0.0.255
access-list 1 permit 10.0.3.0 0.0.0.255
ip nat inside source list 1 interface Serial0/3/1 overload
```

Тепер усі пакети з локальних адрес (inside local) автоматично перекодовуються в адресу інтерфейсу Serial0/3/1 (inside global), а порти динамічно відображаються в таблиці трансляцій.

3.7.3 Тестування налаштувань безпеки

Для захисту доступу до мережевого обладнання адміністративного сегмента VLAN 10 було реалізовано механізм контролю доступу на основі розширених списків доступу (ACL). У межах цієї політики дозволяється встановлення з’єднань до адміністративного пристрою з IP-адресою 192.168.10.2 лише з боку серверної зони VLAN 50, а саме з вузла 192.168.50.3. Такий підхід дозволяє обмежити критичний трафік лише уповноваженим хостам, при цьому блокуючи будь-які інші спроби встановлення SSH-з’єднання до адміністративного вузла.

Для реалізації цього правила на маршрутизаторі було створено розширений ACL із назвою ADMIN_ACCESS. У ньому явно дозволено доступ по протоколу TCP з IP-адреси 192.168.50.3 до 192.168.10.2 лише на порт 22, що використовується для SSH. Усі інші спроби підключення до даного порту блокуються. Також дозволено увесь інший трафік, який не підпадає під перші два правила, що запобігає небажаним побічним ефектам. Конфігурація представлена на лістингу 3.7.

Цей ACL було застосовано у вхідному напрямку на інтерфейсі VLAN 10, до якого підключено адміністративний пристрій. Це гарантує, що кожен вхідний пакет перевіряється згідно з визначеними правилами ще до потрапляння в локальну підмережу.

Лістинг 3.7— конфігурування розширеного ACL для обмеженого доступу до адміністрації

```
ip access-list extended ADMIN_ACCESS
 remark Дозволити SSH лише з вузла серверної зони
 permit tcp host 192.168.50.3 host 192.168.10.2 eq 22
remark Заборонити SSH з інших адрес
 deny   tcp any host 192.168.10.2 eq 22
 remark Дозволити увесь інший трафік
 permit ip any any
```

Крім фільтрації трафіку, налаштовується захищений віддалений доступ до пристрою VLAN 10 з використанням лише протоколу SSH. Для цього встановлюється доменне ім’я, генерується пара RSA-ключів із довжиною 2048 біт, створюється обліковий запис користувача з рівнем привілеїв 15 та задається надійний пароль. Всі з’єднання через Telnet вимикаються, а у лініях VTY дозволяється лише SSH. Приклад відповідної конфігурації наведено у лістингу 3.8.

Лістинг 3.8 – Налаштування SSH-доступу до кабінету директора

```
hostname Admin-RTR
ip domain-name licey.local
crypto key generate rsa modulus 2048
username admin privilege 15 secret StrongPass2025
line vty 0 4
 transport input ssh
 login local
```

У результаті, пристрій адміністрації приймає тільки SSH-з’єднання виключно з IP-адреси 192.168.50.3. Будь-які інші спроби доступу до адміністративної системи, зокрема з Wi-Fi-сегментів чи навчальних VLAN, блокуються на рівні маршрутизатора. Такий підхід відповідає вимогам ізоляції критичних зон та дотриманню принципу найменших привілеїв.

3.7.4 Оцінювання продуктивності та стабільності мережі

У процесі тестування мережевої інфраструктури було проведено серію випробувань із передачею даних між різними корпусами навчального закладу.

Зокрема перевірялася швидкість копіювання великих файлів, і результати засвідчили, що передача відбувається майже миттєво — користувачі не помічають жодних затримок навіть під час інтенсивного навантаження.

Під час звичайної повсякденної активності, зокрема обміну повідомленнями чи перегляду навчального відеоконтенту, мережа функціонує стабільно, без зависань чи зниження швидкості. Середня затримка між корпусами становить приблизно 1–2 мс, що забезпечує якісний онлайн-зв’язок, у тому числі для проведення лекцій у реальному часі або голосових дзвінків.

З метою перевірки надійності були імітовані збої — вручну відключалися окремі канали зв’язку між комутаторами. У всіх випадках система автоматично переходила на резервні траси маршрутизації, не викликаючи відчутних змін у роботі кінцевих користувачів. Це підтверджує ефективність реалізованої надлишковості та здатність мережі адаптуватися до несподіваних ситуацій без втрати працездатності.

За результатами регулярного моніторингу протягом останнього місяця не було зафіксовано жодних серйозних збоїв або помітного зниження швидкодії. Усі точки доступу функціонують стабільно, а навантаження на магістральні інтерфейси перебуває в межах норми.

Таким чином, побудована мережа забезпечує високий рівень продуктивності та надійності, повністю відповідає вимогам масштабної освітньої установи й здатна витримувати як повсякденні робочі навантаження, так і пікові періоди активності під час проведення іспитів або конференцій.

ВИСНОВКИ

У результаті виконання бакалаврської кваліфікаційної роботи було успішно спроєктовано та реалізовано комп’ютерну мережу для навчального закладу — школи-ліцею №1. Побудована мережева інфраструктура охоплює декілька логічних сегментів, забезпечує централізоване управління, контроль доступу до ресурсів та захищений вихід у глобальну мережу. Проведені дослідження й тестування дозволили досягти основної мети — створення надійної та безпечної комп’ютерної мережі з підтримкою ізоляції VLAN та віддаленого доступу через VPN.

У процесі реалізації проєкту було виконано такі завдання:

— проведено детальний аналіз сучасних мережевих технологій, включно з моделями OSI і TCP/IP, технологіями Ethernet та Wi-Fi, IP-адресацією (IPv4), методами маршрутизації та сегментації мережі;

— спроєктовано логічну топологію з урахуванням специфіки шкільної інфраструктури, де реалізовано багаторівневу архітектуру з розділенням зон доступу (адміністрація, серверна, навчальні корпуси, Wi-Fi);

— обґрунтовано вибір маршрутизаторів Cisco серії 2911 і 2811, комутаторів з підтримкою VLAN і VTP, а також використання централізованого Syslog для збору журналів;

— впроваджено віртуальні локальні мережі (VLAN) для логічного розмежування трафіку між адміністрацією, серверною, навчальними аудиторіями, Wi-Fi-зонами та VPN-доступом;

— налаштовано протокол VLAN Trunking Protocol (VTP) для централізованого керування VLAN на всіх комутаторах доступу;

— реалізовано контроль доступу за допомогою розширених списків ACL, зокрема для обмеження доступу до чутливих ресурсів, таких як сервер у VLAN 50 чи адміністраторські станції у VLAN 10;

— налаштовано NAT (PAT) на центральному маршрутизаторі для забезпечення виходу у глобальну мережу всіх внутрішніх вузлів через одну публічну IP-адресу;

— реалізовано захищений віддалений доступ через IPsec VPN для адміністраторів мережі, з доступом до всіх VLAN з дотриманням політик безпеки;

— налаштовано безпечний доступ до мережевого обладнання через SSH з відключеним Telnet;

— протестовано стійкість та надійність мережі, включно з перевіркою перемикань на резервні траси та моніторингом стабільності каналів.

Запропонована мережева архітектура відповідає актуальним стандартам побудови корпоративних мереж та передбачає:

— ефективне логічне розмежування трафіку через VLAN;

— масштабованість і можливість подальшого розширення;

— централізоване адміністрування та спрощене управління безпекою;

— захищений віддалений доступ з автентифікацією;

— стійкість до збоїв завдяки резервуванню маршрутів і надійним ACL.

Новизна запропонованого проєкту полягає в інтеграції кількох рівнів захисту (ACL, VPN, SSH), гнучкому зонуванні через VLAN та балансі між безпекою, продуктивністю і економічною ефективністю. Побудована мережа може слугувати типовим прикладом для впровадження або модернізації мережевої інфраструктури в інших навчальних закладах подібного типу.

Практична значущість роботи підтверджується успішними результатами випробувань: система стабільно працює навіть під час пікових навантажень, демонструє низькі затримки, швидке відновлення зв’язку при збої каналів і забезпечує необхідний рівень безпеки даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Особливості побудови локальних мереж навчальних закладів. / О. О. Завадинський , С. Ю. Белан, С. М. Захарченко // Матеріали конференції LIV Всеукраїнської науково-технічної конференції факультету інформаційних технологій та комп'ютерної інженерії. Вінниця 2025 р. [Електронний ресурс]. Режим доступу: https://conf.vntu.edu.ua/index.php/all-fitki/all-fitki2025/paper/view/23699.

2. Одом В. Офіційне керівництво Cisco з підготовки до сертифікаційних іспитів CCNA 200-301. К.: Вільямс, 2020. 1200 с.

3. Комп'ютерні мережі: підручник / Азаров О. Д., Захарченко С. М., Кадук О. В., Орлова М. М., Тарасенко В. П. - Вінниця: ВНТУ, 2020. 378 с.

4. Коробейнікова Т. І., Захарченко С. М. Комп'ютерні мережі. Львів: Видавництво Львівської політехніки, 2022. 228 с.

5. RFC 7348. Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks. Network Working Group, 2022. Режим доступу: https://www.rfc-editor.org/rfc/rfc7348.txt

6. Clark D. D. The Design Philosophy of the DARPA Internet Protocols. ACM SIGCOMM Computer Communication Review, 2021, vol. 51(1), pp. 59-67.

7. IEEE Standard for Information Technology - Telecommunications and Information Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Std 802.11-2020. IEEE, 2020.

8. Мікротік. MikroTik RouterOS v7 Basic Setup Guide. 2022. Режим доступу: https://help.mikrotik.com/docs/display/ROS/Basic+Setup+Guide

9. Хант К. TCP/IP. Мережеве адміністрування. 3-є вид. К.: Символ-Плюс, 2021. 816 с.

10. Comer D. E. Computer Networks and Internets. 6th ed. 2020. 672 p.

11. Feamster N., Rexford J., Zegura E. The Road to SDN: An Intellectual

12. Stallings W. Computer Networking with Internet Protocols and Technology. Prentice Hall, 2023. 752 p.

13. Kurose J. F., Ross K. W. Computer Networking: A Top-Down Approach. 8th ed. Pearson, 2021. 800 p.

14. Peterson L. L., Davie B. S. Computer Networks: A Systems Approach. 6th ed. Morgan Kaufmann, 2021. 920 p.

15. Akyildiz I. F., Nie S., Liu C. 6G and Beyond: A Comprehensive Survey on Applications, Technologies, and Open Research Problems. IEEE Communications Surveys & Tutorials, 2023, vol. 25(1), pp. 584-632.

16. Cisco. Enterprise Campus Network Architecture. Cisco Press, 2022. Режим доступу:https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/campover.html

17. Гейер Д. Безпровідні мережі. Перше знайомство. М. 2020. 192 с.

18. McNab C. Network Security Assessment: Know Your Network. 3rd ed. O'Reilly Media, 2021. 512 p.

19. Comer D. E. Computer Networks and Internets. 6th ed. 2020. 672 p.

20. RFC 2328. OSPF Version 2. Network Working Group, 2021. Режим доступу: https://www.ietf.org/rfc/rfc2328.txt

21. Feamster N., Rexford J., Zegura E. The Road to SDN: An Intellectual History of Programmable Networks. ACM SIGCOMM Computer Communication Review, 2022, vol. 52(1), pp. 138-148.

22. History of Programmable Networks. ACM SIGCOMM Computer Communication Review, 2022, vol. 52(1), pp. 138-148.

23. RFC 3022. Traditional IP Network Address Translator (Traditional NAT). Network Working Group, 2020. Режим доступу: https://datatracker.ietf.org/doc/html/rfc3022

24. Лін В. Д. Комп'ютерні мережі: архітектура, технології, захист. К.: Техніка, 2021. 456 с.

25. Scott, C., Wolfe, P., Erwin, M. Virtual Private Networks: Second Edition.: O’Reilly Media, 1999. – 288 с. – ISBN 1-56592-529-7.

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.
21 березня 2025 р.

ТЕХНІЧНЕ ЗАВДАННЯ
на виконання бакалаврської кваліфікаційної роботи
«Комп’ютерна мережа для школи-ліцею №1 міста Вінниці»

08-54.БКР.022.00.000 ТЗ

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

Студент групи 2КІ-23мс
_____Белан С.Ю.

м. Вінниця — 2025

1 Підстава для використання бакалаврської кваліфікаційної роботи (БКР)

1.1 Актуальність розробки полягає у необхідності впровадження надійних мережевих рішень у школі-ліцеї № 1 міста Вінниці через зростання обсягів переданої інформації та великої кількості мережевих операцій. Розробка інтегрованої мережевої системи дасть можливість оптимізувати управління освітнім процесом, підвищити якість комунікації між структурними підрозділами та забезпечити високий рівень безпеки даних.

1.2 Головним завданням розробки є створення сучасної, надійної та ефективної комп'ютерної мережі для шеоли-ліцею з використанням багаторівневої архітектури, технологій VLAN та VTP, механізмів безпеки та оптимізації IP-адресації.

1.3 Наказ про затвердження теми бакалаврської дипломної роботи від 21 березня 2025 р. №97.

2 Мета і призначення БКР

2.1 Мета проєкту полягає у вдосконаленні сегменту комп'ютерної мережі школи-ліцею з метою забезпечення високого рівня інформаційної безпеки, що повністю відповідає сучасним міжнародним стандартам, через проєктування багаторівневої архітектури з використанням VLAN і VPN, оптимізацію IP-адресації з NAT та підтримкою IPv6, розробку політик доступу (ACL), а також організацію захищеного віддаленого адміністрування SSH і конфігурацію міжмережевого екрану.

2.2 Призначення розробки полягає у виконанні бакалаврської дипломної роботи, за результатами якої буде впроваджено новий проект комп'ютерної мережі з подальшим розвитком інформаційної інфраструктури школи-ліцею.

3 Вихідні дані для виконання БКР

3.1 Опис існуючої комп'ютерної мережі школи-ліцею №1, включно з наявними мережевими з'єднаннями, обладнанням та програмним забезпеченням.

3.2 Огляд і аналіз сучасних мережевих технологій: моделей OSI та TCP/IP, технологій локальних мереж (Ethernet, Wi-Fi), IP-адресації (IPv4 та IPv6), багаторівневої архітектури, VLAN, VPN, NAT та протоколів динамічної маршрутизації.

3.3 Визначення вимог до мережевого обладнання та програмного забезпечення для трирівневої архітектури, які відповідають потребам університету і забезпечують високий рівень продуктивності, надійності та безпеки.

3.4 Планування структури та топології мережі, включаючи фізичне та логічне розміщення мережевих вузлів, сегментацію через VLAN та маршрутизацію між підмережами.

3.5 Оцінка вартості і вибір оптимальних рішень щодо мережевого обладнання з погляду ефективності для забезпечення потреб школи-ліцею.

3.6 Розробка плану впровадження та тестування нової мережі з урахуванням необхідності перевірки внутрішньої та зовнішньої комунікації.

4 Вимоги до виконання БКР

Головна вимога полягає в створенні ефективної та надійної комп'ютерної мережі з багаторівневою архітектурою, яка забезпечить:

— логічне розділення мережі через VLAN та централізоване управління конфігурацією через VTP;

— забезпечення дистанційного доступу до лакльної мережі через VPN

— надійну маршрутизацію між підмережами на основі протоколу OSPF;

— ефективне використання адресного простору через NAT та підготовку до впровадження IPv6;

— високий рівень безпеки з використанням ACL, SSH та міжмережевого екрану;

— оптимальне співвідношення ціна/продуктивність для обраного мережевого обладнання.

5 Етапи БКР та очікувані результати

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

Таблиця А.1 — Етапи БКР

№ етапу	Назва етапу	Термін виконання		Очікувані результати
		Початок	Кінець	
1	Постановка задачі	21.03.25	21.03.25	Розділ 1
2	Аналіз технологій для створення комп'ютерних мереж	21.03.25	30.03.25	Розділ 1
3	Аналіз та обґрунтування вибору технологій	21.03.25	30.04.25	Розділ 2
4	Реалізація комп'ютерної мережі	31.03.25	13.04.25	Розділ 3
5	Тестування комп'ютерної мережі	14.04.25	27.04.25	Розділ 4
6	Підготовка тезових матеріалів для публікації	21.04.25	28.04.25	Тези
7	Оформлення пояснювальної записки та демонстраційної презентації для доповіді	29.04.25	12.05.25	ТЗ, презентація
8	Підготовка супровідної документації, перевірка відповідності нормам та проходження тесту на плагіат	05.06.25	06.06.25	ТЗ, презентація

6 Матеріали, що подаються до захисту БКР

До захисту подаються: пояснювальна записка БКР, ілюстративні матеріали (схеми логічної та фізичної топології мережі, діаграми розподілу адресного простору), протокол попереднього захисту БКР на кафедрі, відгук наукового керівника, анотації до БКР українською та іноземною мовами, довідка про відповідність оформлення БКР чинним вимогам.

7 Порядок контролю виконання та захисту БКР

Виконання етапів графічної та розрахункової документації БКР контролюється науковим керівником к.т.н., проф. каф. ОТ Захарченком С. М.

згідно зі встановленими термінами. Захист БКР відбувається на засіданні Екзаменаційної комісії, затвердженої наказом ректора ВНТУ.

8 Вимоги до оформлювання та порядок виконання БКР

8.1 При оформлюванні БКР використовуються:

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

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

— 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

ПРОТОКОЛ ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Назва роботи: Комп'ютерна мереж для школи-ліцею №1 міста Вінниці

Тип роботи: бакалаврська кваліфікаційна робота
(бакалаврська кваліфікаційна робота / магістерська кваліфікаційна робота)

Підрозділ кафедра обчислювальної техніки
(кафедра, факультет, навчальна група)

Коефіцієнт подібності текстових запозичень, виявлених у роботі системою StrikePlagiarism 2 %

Висновок щодо перевірки кваліфікаційної роботи (відмітити потрібне)

- ✓ Запозичення, виявлені у роботі, є законними і не містять ознак плагіату, фабрикації, фальсифікації. Роботу прийняти до захисту

- ☐ У роботі не виявлено ознак плагіату, фабрикації, фальсифікації, але надмірна кількість текстових запозичень та/або наявність типових розрахунків не дозволяють прийняти рішення про оригінальність та самостійність її виконання. Роботу направити на доопрацювання.

- ☐ У роботі виявлено ознаки плагіату та/або текстових маніпуляцій як спроб укриття плагіату, фабрикації, фальсифікації, що суперечить вимогам законодавства та нормам академічної доброчесності. Робота до захисту не приймається.

Експертна комісія:

Азаров О.Д., зав. каф. ОТ _____ _____
(прізвище, ініціали, посада) (підпис)

Крупельницький Л.В., доц. каф ОТ _____ _____
(прізвище, ініціали, посада) (підпис)

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

З висновком експертної комісії ознайомлений(-на)

Керівник _____ _____
(підпис) (прізвище, ініціали, посада)

Здобувач _____ _____
(підпис) (прізвище, ініціали)

ДОДАТОК В

ІЛЮСТРАТИВНА ЧАСТИНА

КОМП’ЮТЕРНА МЕРЕЖА ШКОЛИ-ЛІЦЕЮ №1

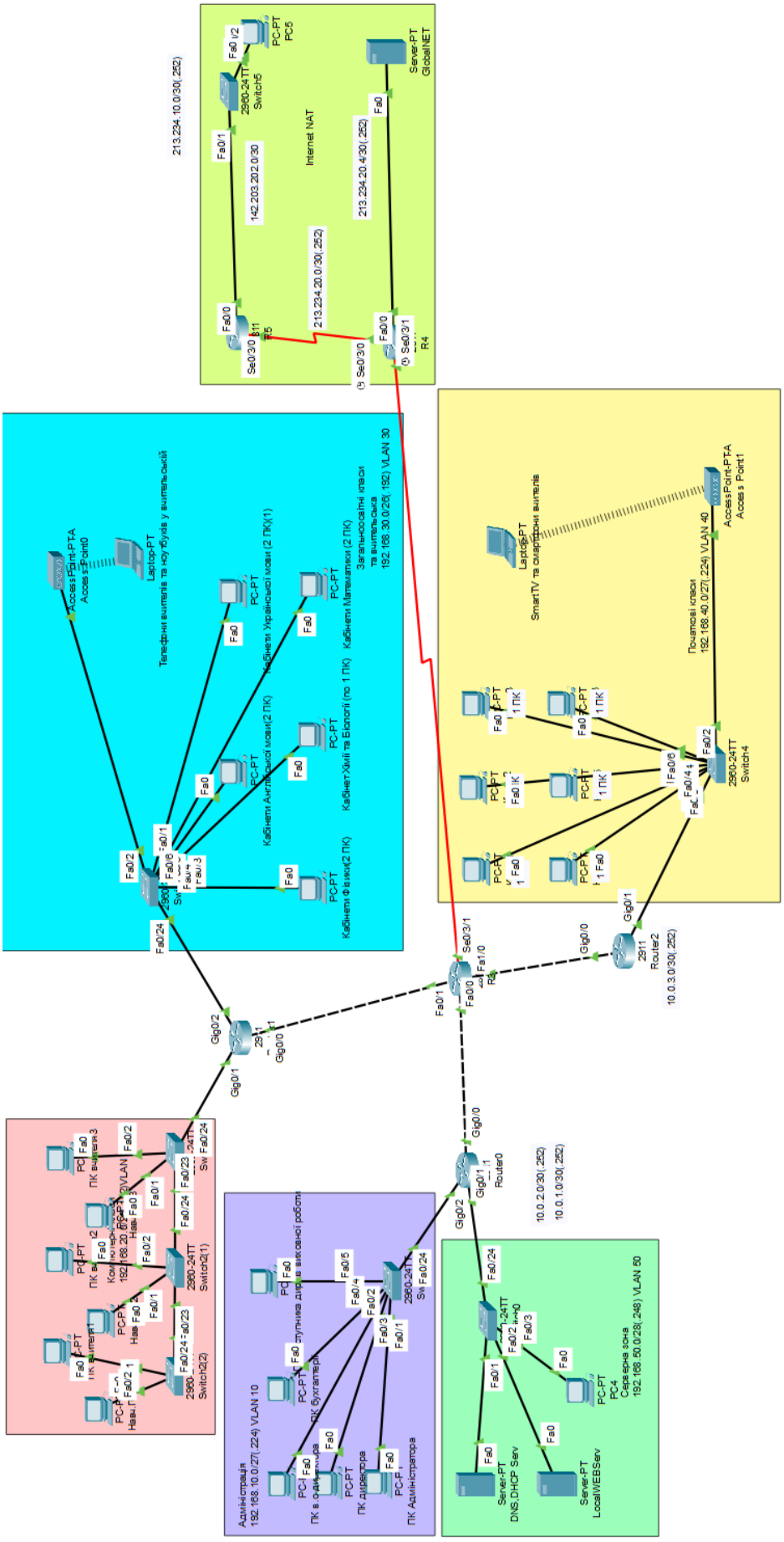


Рисунок В.1 – Логічна топологія мережі корпусів молодших та старших класів

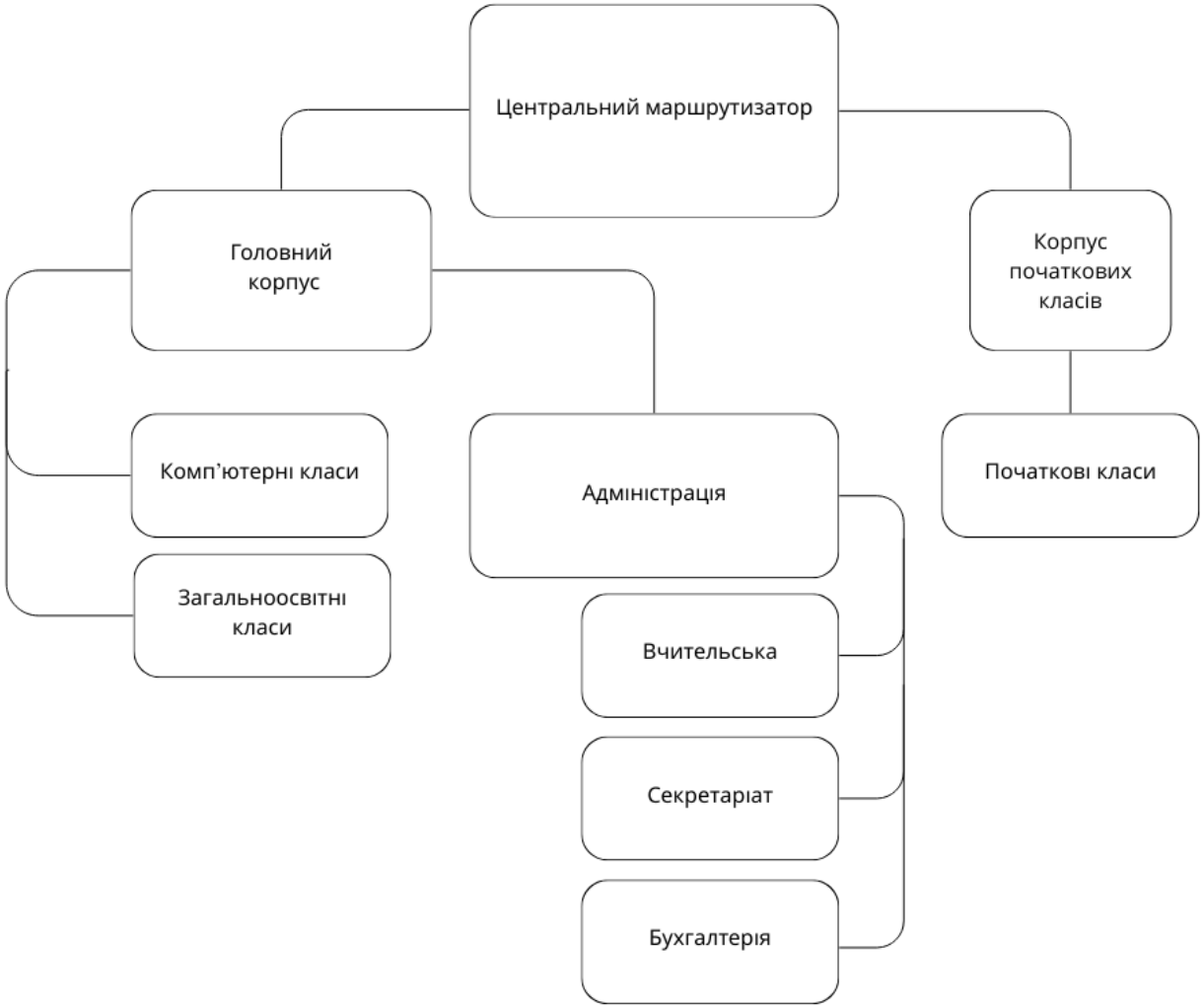


Рисунок В.2 — Структурна схема мережі школи-ліцею №1

ДОДАТОК Г

Лістинги конфігураційних файлів

Лістинг Г.1 — Конфігураційний файл центрального маршрутизатора

```
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname Router
aaa new-model
aaa authentication login REMOTE local
aaa authorization network REMOTE local
no ip cef
no ipv6 cef
username VPN secret 5 $1$mERr$59rIgSGFPOvINohMkktWj0
license udi pid CISCO2811/K9 sn FTX1017X7EW-
crypto isakmp policy 10
encr aes 256
hash md5
authentication pre-share
group 2
crypto isakmp client configuration group REMOTE
key CISCO
pool VPN-POOL
crypto ipsec transform-set MYSET esp-aes 256 esp-md5-hmac
crypto dynamic-map DYNMAP 10
set transform-set MYSET
reverse-route
crypto map CLIENT_MAP client authentication list REMOTE
crypto map CLIENT_MAP isakmp authorization list REMOTE
crypto map CLIENT_MAP client configuration address respond
crypto map CLIENT_MAP 10 ipsec-isakmp dynamic DYNMAP
spanning-tree mode pvst
interface FastEthernet0/0
ip address 10.0.1.1 255.255.255.252
ip nat inside
duplex auto
speed auto
interface FastEthernet0/1
ip address 10.0.2.1 255.255.255.252
ip nat inside
duplex auto
speed auto
interface Serial0/3/0
no ip address
ip access-group FIREWALL_IN in
ip nat outside
clock rate 2000000
interface Serial0/3/1
ip address 213.234.10.1 255.255.255.252
ip access-group FIREWALL_IN in
ip nat outside
crypto map CLIENT_MAP
```

```
interface FastEthernet1/0
ip address 10.0.3.1 255.255.255.252
ip nat inside
duplex auto
speed auto
interface FastEthernet1/1
no ip address
duplex auto
speed auto
shutdown
interface Vlan1
no ip address
shutdown
router ospf 1
log-adjacency-changes
network 10.0.1.0 0.0.0.3 area 0
network 10.0.2.0 0.0.0.3 area 0
network 10.0.3.0 0.0.0.3 area 0
network 192.168.200.0 0.0.0.255 area 0
default-information originate
ip local pool VPN-POOL 192.168.200.10 192.168.200.20
ip nat inside source list FOR-NAT interface Serial0/3/1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 213.234.10.2
ip flow-export version 9
ip access-list standard FOR-NAT
permit 192.168.0.0 0.0.255.255
permit 142.203.202.0 0.0.0.3
permit 192.168.200.0 0.0.0.255
ip access-list extended FIREWALL_IN
permit tcp any any established
permit gre any any
permit udp any any eq isakmp
permit esp any any
permit ip 192.168.200.0 0.0.0.255 any
deny ip any any
line con 0
line aux 0
line vty 0 4
end
```

Лістинг Г.2 – Конфігураційний файл L3-комутатора із адміністративного сегменту

```
Switch#show run
Building configuration...
Current configuration : 2512 bytes
version 12.2(55)SE5
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
hostname Admin-Switch
ip routing
spanning-tree mode pvst
interface FastEthernet0/1
 description Trunk to Main Router
```

```
 switchport trunk encapsulation dot1q
 switchport mode trunk
interface FastEthernet0/2
 description Access port for Director PC
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
interface FastEthernet0/3
 description Access port for Accountant PC
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
interface FastEthernet0/4
 description Access port for HR PC
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
interface FastEthernet0/5
 description Trunk to Core Switch
 switchport trunk encapsulation dot1q
 switchport mode trunk
interface FastEthernet0/6
 switchport access vlan 10
 switchport mode access
interface FastEthernet0/7
 switchport access vlan 10
 switchport mode access
interface FastEthernet0/8
 switchport access vlan 10
 switchport mode access
interface FastEthernet0/9
 switchport access vlan 10
 switchport mode access
interface FastEthernet0/10
 switchport access vlan 10
 switchport mode access
interface FastEthernet0/11
 switchport access vlan 10
 switchport mode access
interface FastEthernet0/12
 switchport access vlan 10
 switchport mode access
interface FastEthernet0/13
 switchport access vlan 10
 switchport mode access
interface FastEthernet0/14
 switchport access vlan 10
 switchport mode access
interface FastEthernet0/15
 switchport access vlan 10
 switchport mode access
interface FastEthernet0/16
 switchport access vlan 10
 switchport mode access
interface FastEthernet0/17
 switchport access vlan 10
```

```
 switchport mode access
interface FastEthernet0/18
 switchport access vlan 10
 switchport mode access
interface FastEthernet0/19
 switchport access vlan 10
 switchport mode access
interface FastEthernet0/20
 switchport access vlan 10
 switchport mode access
interface FastEthernet0/21
 switchport access vlan 10
 switchport mode access
interface FastEthernet0/22
 switchport access vlan 10
 switchport mode access
interface FastEthernet0/23
 switchport access vlan 10
 switchport mode access
interface FastEthernet0/24
 switchport mode trunk
interface Vlan1
 no ip address
 shutdown
interface Vlan10
 ip address 192.168.10.2 255.255.255.0
 ip helper-address 192.168.50.4
ip route 0.0.0.0 0.0.0.0 192.168.10.1
ip access-list standard ADMIN_ACCESS
 permit 192.168.10.0 0.0.0.255
line con 0
 password cisco
 login
line vty 0 4
 transport input ssh
 login local
username admin privilege 15 secret 5 $1$9d3f$ZkO0saeUJzmefNgU0cMJy0
end
```

Лістинг Г.3 – Конфігураційний файл L3-комутатора із корпусу №2

```
Switch#show run
Building configuration...
Current configuration : 2568 bytes
version 12.2(55)SE5
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
hostname Server-Switch
ip routing
spanning-tree mode pvst
interface FastEthernet0/1
 description Trunk to Core Router
 switchport trunk encapsulation dot1q
 switchport mode trunk
interface FastEthernet0/2
```

```
 description Access port for Web Server
 switchport access vlan 50
 switchport mode access
 spanning-tree portfast
interface FastEthernet0/3
 description Access port for File Server
 switchport access vlan 50
 switchport mode access
 spanning-tree portfast
interface FastEthernet0/4
 description Access port for Backup Server
 switchport access vlan 50
 switchport mode access
 spanning-tree portfast
interface FastEthernet0/5
switchport access vlan 50
switchport mode access
interface FastEthernet0/6
switchport access vlan 50
switchport mode access
interface FastEthernet0/7
switchport access vlan 50
switchport mode access
interface FastEthernet0/8
switchport access vlan 50
switchport mode access
interface FastEthernet0/9
switchport access vlan 50
switchport mode access
interface FastEthernet0/10
switchport access vlan 50
switchport mode access
interface FastEthernet0/11
switchport access vlan 50
switchport mode access
interface FastEthernet0/12
switchport access vlan 50
switchport mode access
interface FastEthernet0/13
switchport access vlan 50
switchport mode access
interface FastEthernet0/14
switchport access vlan 50
switchport mode access
interface FastEthernet0/15
switchport access vlan 50
switchport mode access
interface FastEthernet0/16
switchport access vlan 50
switchport mode access
interface FastEthernet0/17
switchport access vlan 50
switchport mode access
interface FastEthernet0/18
switchport access vlan 50
switchport mode access
```

```
interface FastEthernet0/19
switchport access vlan 50
switchport mode access
interface FastEthernet0/20
switchport access vlan 50
switchport mode access
interface FastEthernet0/21
switchport access vlan 50
switchport mode access
interface FastEthernet0/22
switchport access vlan 50
switchport mode access
interface FastEthernet0/23
switchport access vlan 50
switchport mode access
interface FastEthernet0/24
switchport mode trunk
interface GigabitEthernet0/1
interface GigabitEthernet0/2
interface Vlan1
 no ip address
 shutdown
interface Vlan50
 ip address 192.168.50.2 255.255.255.0
 ip helper-address 192.168.50.4
ip route 0.0.0.0 0.0.0.0 192.168.50.1
ip access-list standard SERVER_ACCESS
 permit 192.168.10.0 0.0.0.255
 permit 192.168.50.0 0.0.0.255
 deny   any
line con 0
 password cisco
 login
line vty 0 4
 transport input ssh
 login local
username serveradmin privilege 15 secret 5 $1$8a3b$DWtO/1zYm6shwQ9C7E6.J.
end
```