Міністерство освіти і науки України

Луцький національний технічний університет
(повне найменування закладу вищої освіти)

Факультет комп'ютерних та інформаційних технологій
(повне найменування факультету)

Кафедра комп'ютерної інженерії та безпеки
(повне найменування кафедри)

КВАЛІФІКАЦІЙНА РОБОТА ЗА СТУПЕНЕМ ВИЩОЇ ОСВІТИ «БАКАЛАВР»

МОДЕРНІЗОВАНА КОМП'ЮТЕРНА МЕРЕЖА КОЛКІВСЬКОГО ЦЕНТРУ ПРОФЕСІЙНОЇ ОСВІТИ

THE MODERNIZED COMPUTER NETWORK OF THE KOLKY CENTER OF PROFESSIONAL EDUCATION

спеціальність 123 Комп'ютерна інженерія
(шифр і назва спеціальності)

освітня програма Комп'ютерна інженерія
(назва освітньої програми)

Виконав: здобувач вищої освіти
групи КІс-21
Горайчук Василь Андрійович

(підпис)

Керівник:
к.т.н., доцент
Багнюк Наталія Володимирівна

(підпис)

Кваліфікаційну роботу
допущено до захисту
« 30 » червня 2025 р.
Гарант освітньої програми:
к.т.н., доцент
Лавренчук Світлана Василівна

(підпис)

Луцьк – 2025 року

ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Факультет *комп'ютерних та інформаційних технологій*
Кафедра *комп'ютерної інженерії та безпеки*
Ступінь вищої освіти: *бакалавр*
Галузь знань: *12 Інформаційні технології*
Спеціальність: *123 Комп'ютерна інженерія*
Освітня програма: *«Комп'ютерна інженерія»*

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ доц. Тарас ТЕРЛЕЦЬКИЙ
« 10 » 01 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ВИЩОЇ ОСВІТИ

Горайчуку Василю Андрійовичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи *Модернізована комп'ютерна мережа Колківського центру професійної освіти*

Керівник роботи *к.т.н., доц. Багнюк Наталія Володимирівна*

затверджені наказом закладу вищої освіти від «04» січня 2025 року № 11/01-02
2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 10.06.2025р.

3. Вихідні дані до роботи *джерелом розробки є науково-технічна література та публікації в періодичних виданнях з даного питання, опубліковані зарубіжні та вітчизняні роботи в даній області та різні інтернет-ресурси технічного спрямування.*

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити):
Вступ, аналіз існуючого стану мережі, проблеми та визначення вимог до модернізованої мережі, логічна та фізична топологія мережі, проєктування модернізованої мережі, налаштування мережевого обладнання та використання технології VLAN, забезпечення безпеки мережі, налаштування VPN, висновки.

5. Перелік графічного (ілюстративного) матеріалу:

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис	
		завдання видав	завдання прийняв
Аналіз існуючої мережі та рекомендації щодо модернізації	*Багнюк Н.В., доцент*		
Техніко-економічне обгрунтування	*Багнюк Н.В., доцент*		
Проєктування логічної та фізичної топології модернізованої мережі	*Багнюк Н.В., доцент*		
Нормоконтроль	*Багнюк Н.В., доцент*		
Гарант ОП	*Лавренчук С.В., доцент*		
Показник запозичень тексту	***___%***		
Академічна доброчесність	*Міскевич О.І.,ст.викладач*		

7. Дата видачі завдання 10.01.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	*Огляд літератури із досліджуваної проблеми, аналіз предметної області та наявних рішень*	до 10.02.2025 р.	Виконано
2.	*Аналіз існуючої мережі та рекомендації щодо модернізації*	до 02.03.2025 р.	Виконано
3.	*Налаштування мережевого обладнання*	до 02.04.2025 р.	Виконано
4.	*Висновки та пропозиції*	до 10.04.2025 р.	Виконано
5.	*Формування списку використаних джерел*	до 15.04.2025 р.	Виконано
6.	*Формування додатків*	до 02.05.2025 р.	Виконано
7.	*Оформлення ілюстративного матеріалу*	до 10.05.2025 р.	Виконано
8.	*Представлення остаточного варіанту кваліфікаційної роботи керівникові*	до 15.05.2025 р.	Виконано
9.	*Нормоконтроль*	до 30.05.2025 р.	Виконано
10	*Інструментальна перевірка на академічний плагіат*	до 03.06.2025 р	Виконано
11.	*Здача кваліфікаційної роботи та всіх супровідних документів на кафедру*	до 10.06.2025 р.	Виконано

Здобувач вищої освіти _____ Горайчук В.А..
(підпис) (прізвище, ініціали)

Керівник кваліфікаційної роботи _____ Багнюк Н.В.
(підпис) (прізвище, ініціали)

АНОТАЦІЯ

Горайчук В. А. Модернізована комп’ютерна мережа Колківського центру професійної освіти. Рукопис.

Кваліфікаційна робота бакалавра ОП «Комп’ютерна інженерія» спеціальності 123 Комп’ютерна інженерія. Луцький національний технічний університет. Луцьк, 2025.

Кваліфікаційна робота складається з вступу, трьох розділів, висновків, списку використаних джерел, додатків.

Перший розділ присвячений проведенню аналізу існуючої комп’ютерної мережі Колківського центру професійної освіти. Також розглянуто загальну організаційну структуру закладу, визначено потреби користувачів у мережевих ресурсах та виявлено основні недоліки діючої інфраструктури. Оцінено технічний стан мережевого обладнання, рівень інформаційної безпеки та можливості масштабування. На основі зібраних даних сформульовано основні вимоги до модернізації мережі та обґрунтовано необхідність впровадження нових технічних рішень.

В другому розділі здійснено вибір та обґрунтування мережевого обладнання. Розглянуто топології мереж. Виконано порівняння технічних характеристик старого та нового обладнання. Спроєктовано IP-адресацію з урахуванням підмереж для кожного поверху та службового призначення.

Третій розділ містить практичну реалізацію мережі в середовищі Cisco Packet Tracer. У ньому виконано налаштування маршрутизаторів, комутаторів, точок доступу, міжмережевого екрану, а також служби DHCP, DNS, NAT і ACL. Також налаштовано відалений доступ та VLAN.

Ключові слова: комп’ютерна мережа, комутатор, маршрутизація, інтернет, DHCP, DNS, VLAN.

ANNOTATION

Horaychuk V. The modernized computer network of the Kolky center of professional education.

Qualifying work of a bachelor of EP Computer Engineering specialty 123 Computer Engineering. Lutsk National Technical University. Lutsk, 2025.

Qualification work consists of an introduction, three sections, conclusions, a references, and an appendix.

The first section is devoted to the analysis of the existing computer network of the Kolky professional education center. The general organizational structure of the institution was also considered, the needs of users in network resources were determined, and the main shortcomings of the existing infrastructure were identified. The technical condition of the network equipment, the level of information security, and scalability were assessed. Based on the collected data, the main requirements for network modernization were formulated and the need for implementing new technical solutions was justified.

In the second section, the selection and justification of network equipment was carried out. Network topologies were considered. The technical characteristics of the old and new equipment were compared. IP addressing was designed taking into account subnets for each floor and service purpose.

The third section contains the practical implementation of the network in the Cisco Packet Tracer environment. It includes settings for routers, switches, access points, a firewall, as well as DHCP, DNS, NAT, and ACL services. Remote access and VLAN were also configured.

Keywords: computer network, switch, routing, Internet, DHCP, DNS, VLAN.

ЗМІСТ

ВСТУП 7
РОЗДІЛ 1 АНАЛІЗ ІСНУЮЧОГО СТАНУ МЕРЕЖІ 8
1.1 Характеристика Колківського центру професійної освіти 8
1.2 Проблеми та визначення вимог до модернізації мережі 10
РОЗДІЛ 2 ВИБІР ОБЛАДНАННЯ ТА ЛОГІЧНА СТРУКТУРА МЕРЕЖІ 11
2.1 Вибір фізичної топології 11
2.2 Вибір мережевого обладнання 12
2.3 Логічна схема мережі та IP-адресація 15
2.4 Технологія VLAN 20
2.5 Бездротовий доступ 21
РОЗДІЛ 3 ПРОЄКТУВАННЯ МЕРЕЖІ 24
3.1 Конфігурація маршрутизаторів та комутаторів 24
3.2 Налаштування серверів 30
3.3 Створення VLAN 33
3.4 Налаштування безпровідної мережі та точок доступу 35
3.5 Забезпечення доступу та його безпеки до мережі Інтернет 36
3.6 Створення та налаштування VPN 38
ВИСНОВКИ 43
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ 45
ДОДАТКИ 47

ВСТУП

На сьогоднішній день більшість закладів вищої освіти потребують високої якості комп’ютерної інфраструктури, щоб забезпечити кращу ефективність навчального процесу.

Основна ціль даної кваліфікаційної роботи полягає в покращенні ефективності роботи та захисту мережі Колківського центру професійної освіти.

Метою роботи є створення надійної, ефективної та безпечної мережевої інфраструктури, яка задовольняє потреби навчального закладу.

Об’єктом дослідження є мережева інфраструктура Колківського ЦПО.

Предметом дослідження є методи діагностики, проєктування, налаштування та оптимізації роботи комп’ютерної мережі навчального закладу.

Розробка комп’ютерної мережі для Колківського ЦПО включає такі завдання:

– аналіз існуючої мережі та виявлення проблем;

– вибір топології мережі;

– вибір мережевого обладнання;

– налаштування обладнання та організація безпеки мережі;

– проєктування модернізованої мережі;

– тестування та діагностика нової мережі.

Увагу приділено питанням безпеки даних, адже інформація потребує високого рівня захисту від несанкціонованого доступу та втрат. Важливо також забезпечити високу пропускну здатність і стабільність мережі, щоб забезпечити безперебійний доступ до інформації для персоналу.

У роботі використано сучасні методи і технології проєктування та впровадження комп’ютерних мереж з урахуванням вимог навчального закладу.

Таким чином, результатом цієї кваліфікаційної роботи є спроєктована комп’ютерна мережа для Колківського ЦПО, яка готова до використання і задовольняє всі вимоги для ефективного навчання та роботи в даному навчальному закладі.

РОЗДІЛ 1
АНАЛІЗ ІСНУЮЧОГО СТАНУ МЕРЕЖІ

1.1 Характеристика Колківського центру професійної освіти

Колківський центр професійної освіти – це навчальний заклад, який здійснює підготовку кваліфікованих спеціалістів різного профілю. У закладі розташовані аудиторії, адміністративні кабінети, лабораторія та спеціальні приміщення [1]. Для забезпечення ефективної навчальної та адміністративної діяльності необхідна сучасна комп'ютерна мережа, що забезпечує швидкий доступ до мережі Інтернет, локальних серверів та внутрішніх інформаційних ресурсів.

На рисунках 1.1-1.3 представлено плани поверхів головного корпусу Колківського ЦПО.

Рисунок 1.1 – План першого поверху

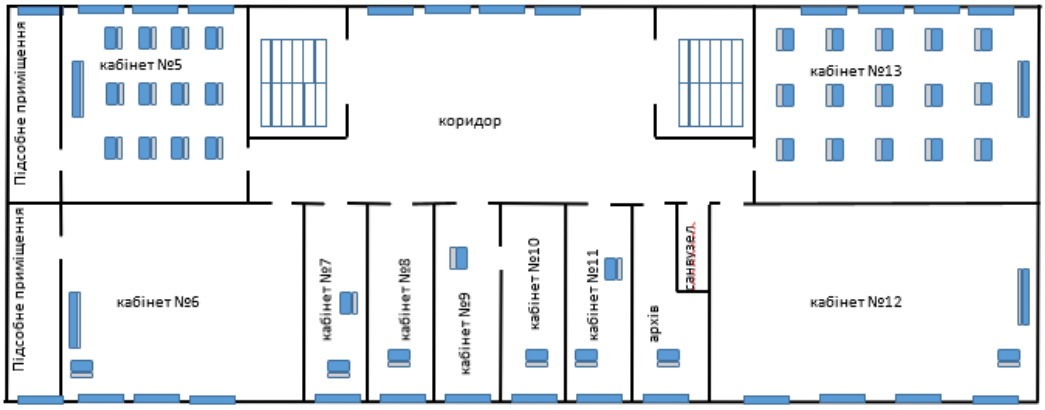

Рисунок 1.2 – План другого поверху

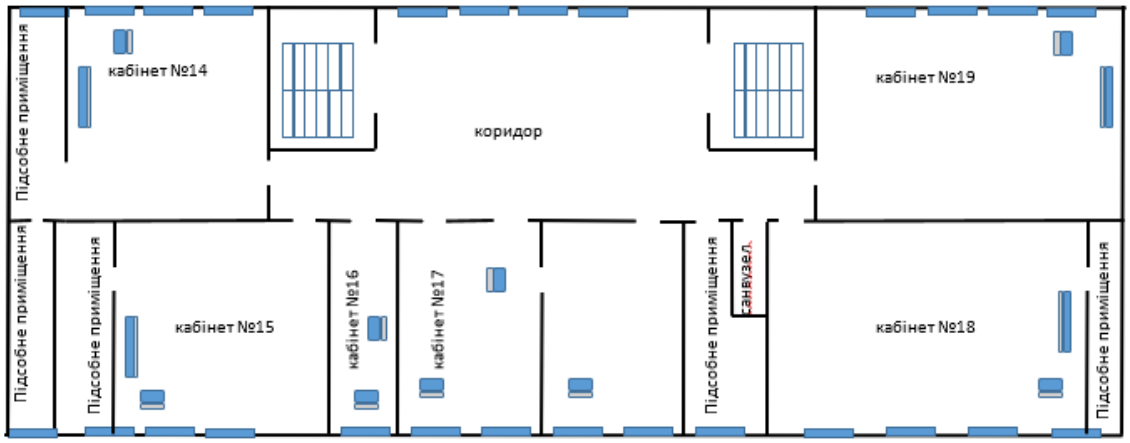

Рисунок 1.3 – План третього поверху

Колківський центр професійної освіти складається з різних кабінетів, які використовуються для навчання та адміністративних завдань. Відповідно до структури навчального закладу класи за функціональним призначенням поділяються:

– навчальні кабінети: математика, українська мова та література, історія, інформатика, біологія та географія, фізика, хімія;

– спеціалізовані кабінети: безпеки дорожнього руху, ПДР, агротехніки, права, бухгалтерії та навчанню харчової промисловості;

– адміністративні кабінети: директор, заступники директора, секретар, секретар відділу освіти;

– конференц-зал для загальних зустрічей та навчальних заходів.

Перелік кабінетів подані в таблиці 1.1.

Таблиця 1.1 – Перелік кабінетів в навчальному закладі

Номер кабінету	Назва кабінету
1	Математичний кабінет
2	Кабінет української мови та літератури
3	Кабінет історії
4	Кабінет інформатики
5	Кабінет безпеки дорожнього руху
6	Кабінет біології та географії
7	Кабінет секретаря навчальної частини
8	Кабінет заступника директора
9	Кабінет секретаря
10	Кабінет директора
11	Кабінет заступника директора з навчальної частини
12	Конференцзал

Продовження таблиці 1.1

Номер кабінету	Назва кабінету
13	Кабінет правил дорожнього руху
14	Кабінет агроінженерії
15	Кабінет фізики
16	Кабінет юриста
17	Бухгелтерія
18	Кабінет хімії
19	Кабінет устаткування харчової промисловості
20	Архів
21	Кадровий відділ
	Музей №1
	Музей №2
	Кабінет секретаря
	Кабінет секретаря

1.2 Проблеми та визнечення вимог до модернізації мережі

На сьогоднішній день мережа Колківського центру професійної освіти має ряд недоліків, які роблять її недостатньо ефективною. Метою кваліфікаційної роботи є визначення існуючих недоліків та створення більш ефективної мережі.

Через великий трафік Інтернет нестабільний і передача даних може тривати довго. Бездротовий інтернет доступний не у всіх кабінетах. Велика кількість підключень до однієї бездротової точки доступу. Існуюча мережа не розрахована на збільшення кількості комп’ютерів та інших пристроїв.

Для усунення виявлених проблем нова мережа повинна відповідати наступним вимогам:

– висока продуктивність – забезпечення швидкого та стабільного обміну даними між усіма пристроями;

– розширене покриття – надання якісного інтернету у всіх навчальних кабінетах та адміністративних приміщеннях;

– підтримка підключення нових пристроїв – гнучкість мережі для додавання додаткових комп’ютерів, ноутбуків чи іншого обладнання без порушень у роботі.

Модернізація мережі сприятиме підвищенню ефективності освітнього процесу та забезпечить комфортне використання для всіх користувачів.

РОЗДІЛ 2
ВИБІР ОБЛАДНАННЯ ТА ЛОГІЧНА СТРУКТУРА МЕРЕЖІ

2.1 Вибір фізичної топології

Фізична топологія визначає схему розташування комп'ютерів, серверів, маршрутизаторів та іншого мережевого обладнання, а також спосіб їхнього підключення між собою [2]. Ефективність, надійність, маштабованість, вартість побудови мережі залежить від правильно обраної топології, якщо обрати її неправильно, то можуть бути перенавантаження чи збої. Фізичні топології зображенні на рисунку 2.1.

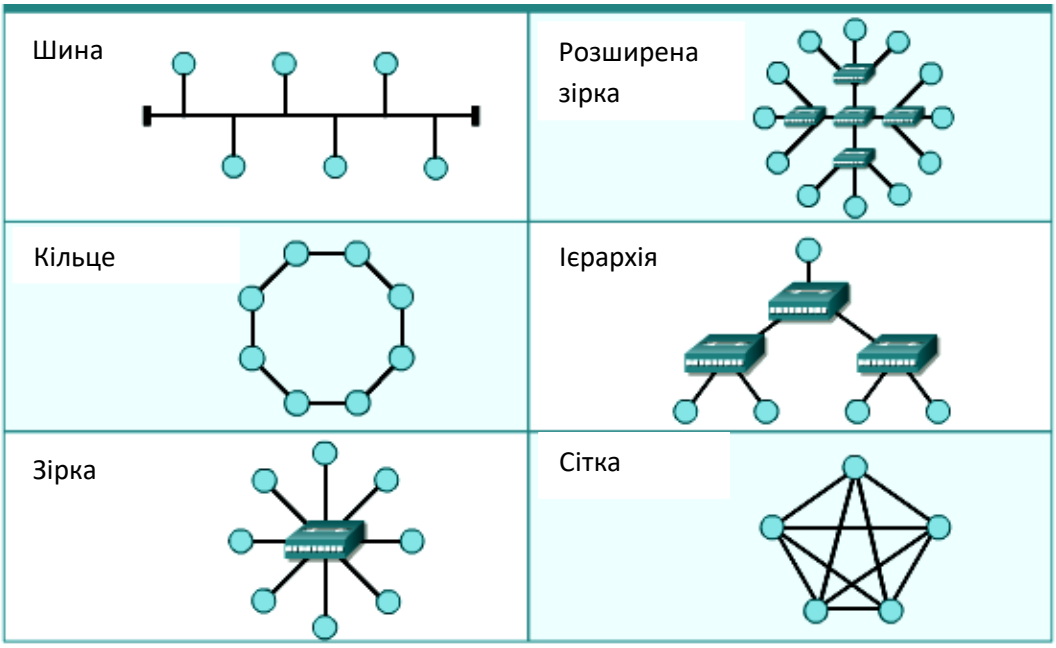

Рисунок 2.1 – Топології мережі [2]

Під час використання топології «шина» пристрої підключаються до єдиного кабелю, по якому передаються всі дані. Сигнал будуть отримувати всі підключені пристрої, але обробити його зможе тільки адресат.

Використовуючи кільцеву топологію всі пристрої з'єднуються послідовно, а дані будуть передаватись через кожен пристрій, але якщо один з пристроїв перестає працювати, то це виводить з ладу всю мережу.

Для більшої стійкості мережі можна використати топологію «зірки», тому

що при відсутності одного з пристроїв, інші пристрої будуть далі функціонувати в мережі.

Під час вибору топології варто звернути увагу на кількість пристроїв в мережі, призачення мережі, можливість вдосконалення, вартість побудови, рівень безпеки, фізичне розташування приміщень.

Для Колківського центру професійної освіти найкращим варіантом є гібридна топологія, яка поєднує елементи різних видів (наприклад зіркової, деревоподібної та шинної). Вона має такі переваги:

– стабільне з’єднання для всіх кабінетів і пристроїв;

– простота додавання нових пристроїв без значних змін у конфігурації мережі;

– вища надійність – у разі виходу з ладу одного кабелю чи пристрою робота всієї мережі не припиниться.

2.2 Вибір мережевого обладнання

Під час аналізу мережі Колківського ЦПО було виявлено застаріле обладнання, що впливає на продуктивність і надійність роботи. Для проєктування оновленої мережі передбачається використання сучасного обладнання.

Активне мережеве обладнання:

– комутатори – розподіляють дані між пристроями локальної мережі (рис. 2.2);

– маршрутизатори – керують потоками даних між частинами мережі та забезпечують підключення до Інтернету (рис. 2.3);

– точки доступу Wi-Fi – забезпечують бездротове підключення;

– міжмережевий екран – забезпечує захищене з’єднання з зовнішньою мережею;

– сервери – відповідають за зберігання файлів, управління мережею та роботу DHCP.

В таблицях 2.1-2.2 представлені порівняльні характеристики комутаторів та маршрутизаторів.

Рисунок 2.2 – Комутатор [3]

Таблиця 2.1 – Порівняння комутаторів

	Старе обладнання	Нове обладнання
Модель	D-Link DES-1008D (некерований)	Cisco Catalyst 2960X-24TS-L (керований)
Кількість портів	8 Fast Ethernet	24 Gigabit Ethernet + 4 SFP
Керування	Відсутнє	CLI, SNMP, VLAN, QoS
Пропускна здатність	До 100 Мбіт/с	До 1 Гбіт/с на порт
Ціна	≈ 900 грн	≈ 18 000–20 000 грн

Рисунок 2.3 – Маршрутизатор [3]

Таблиця 2.2 – Порівняння маршрутизаторів

	Старе обладнання	Нове обладнання
Модель	TP-Link TL-WR841N	Cisco ISR 4331
Інтерфейси	4 LAN + 1 WAN (Fast Ethernet)	3 GE + модульні порти
Підтримка протоколів	Статична маршрутизація	OSPF, EIGRP, BGP, NAT, VPN
Керування	Веб-інтерфейс	IOS CLI, SNMP, REST API
Ціна	≈ 800 грн	≈ 19 000–20 000 грн

На рисунках 2.4-2.6 зображено активне мережеве обладнання. Порівняльні характеристики мережевого обладнання зображені в таблицях 2.3-2.5.

Рисунок 2.4 – Точка доступу Wi-Fi [3]

Таблиця 2.3 – Порівняння точок доступу Wi-Fi

	Старе обладнання	Нове обладнання
Модель	TP-Link TL-WA801ND	Cisco Catalyst C9120AXI
Стандарти	802.11n (до 300 Мбіт/с)	802.11ax, MU-MIMO
Частоти	2.4 ГГц	2.4 ГГц та 5 ГГц
Продуктивність	Базова, без централізованого управління	Висока продуктивність, централізоване управління через Cisco DNA Center
Ціна	≈ 1 200 грн	≈ 18 000 грн

Рисунок 2.5 – Міжмережевий екран [3]

Таблиця 2.4 – Порівняння міжмережевих екранів

	Старе обладнання	Нове обладнання
Модель	Вбудований NAT на TP-Link	Cisco Firepower 1010 NGFW
Функції	Примітивний NAT	IPS/IDS, VPN, Web-фільтрація, AntiVirus
Пропускна здатність	До 100 Мбіт/с	До 1.2 Гбіт/с (NGFW), до 650 Мбіт/с
Керування	Відсутнє	Централізоване керування через Cisco FMC або CDO
Ціна	≈ 0 грн (вбудовано)	≈ 30 000 грн

Рисунок 2.6 – Сервер [4]

Таблиця 2.5 – Порівняння серверів

	Старе обладнання	Нове обладнання
Модель	Звичайний ПК	HPE ProLiant DL360 Gen10
ОС	Windows 7/10	Windows Server 2019
Призначення	DHCP вручну	DHCP, DNS, AD, файловий сервер
Переваги	Низька надійність	Централізоване адміністрування, резервування
Ціна	≈ 9 000 грн	≈ 19 000–20 000 грн

Пасивне мережеве обладнання (кабелі, роз’єми):

– Ethernet-кабелі – підключають комп’ютери до комутаторів і маршрутизаторів для швидкої та стабільної передачі даних;

– оптоволоконні кабелі – забезпечують магістральні з’єднання між основними маршрутизаторами і комутаторами з мінімальними затримками;

– конектори для оптоволоконних кабелів – гарантують надійне з’єднання між оптоволоконними магістралями і обладнанням.

Такий вибір обладнання створить баланс між швидкістю, надійністю та вартістю проєкту.

2.3 Логічна схема мережі та IP-адресація

У оновленій мережевій інфраструктурі використовується концепція поділу на підмережі в залежності від поверху та номеру кабінету, що дозволяє ефективно керувати трафіком та підвищити рівень безпеки. В таблиці 2.6 показана IP-адресація Колківського центру професійної освіти.

Таблиця 2.6 – IP-адресації корпусів і мережевих сегментів

Назва мережевого сегменту	IP-адреса мережі	Маска IP-адреси мережі
Сервери	192.168.1.0	255.255.255.0
Перший поверх – корпус 1	192.168.2.0	255.255.255.224
Другий поверх – корпус 1	192.168.3.0	255.255.255.224
Третій поверх – корпус 1	192.168.4.0	255.255.255.224
Віддалений корпус	192.168.6.0	255.255.255.0
Кабінет секретарів – корпус 2	192.168.10.0	255.255.255.0
Кабінет секретарів– корпус 2	192.168.20.0	255.255.255.0
Музей №1– корпус 2	192.168.30.0	255.255.255.0
Музей №2 – корпус 2	192.168.40.0	255.255.255.0

Маршрутизатори виконують ключову функцію управління мережевими потоками, спрямовуючи трафік між різними сегментами мережі. Вони забезпечують ефективну маршрутизацію пакетів даних, запобігаючи перевантаженню мережі та підвищуючи її продуктивність.

З метою підвищення ефективності роботи мережі та забезпечення високого рівня інформаційної безпеки було здійснено її поділ на окремі мережеві сегменти для адміністративного персоналу і навчальних аудиторій та серверів. В таблицях 2.7-2.9 представлена IP-адресація мережевих сегментів навчального закладу.

Таблиця 2.7 – IP-адресації мережевих сегментів корпусу 1

Номер каб.	Назва каб.	IP-адреса мережі/Маска IP-адреси	Діапазон IP-адрес	
			Перша IP-адреса	Остання IP-адреса
1	Кабінет математики	192.168.2.0/27	192.168.2.34	192.168.2.43
2	Кабінет укр. мови			
3	Кабінет історії			
	Кадровий відділ			
4	Кабінет Інформатики	192.168.2.0/27	192.168.2.2	192.168.2.30
5	Кабінет безпеки дорожнього руху	192.168.3.0/27	192.168.3.2	192.168.3.30
6	Кабінет біології та географії	192.168.3.0/27	192.168.3.67	192.168.3.86
7	Секретар навчальної частини			
8	Заступник директора			
9	Секретар			
10	Директор			
11	Заступник директора			
	Архів			
12	Конференцзал			
13	Кабінет ПДР	192.168.3.0/27	192.168.3.34	192.168.3.63

Продовження таблиці 2.7

Номер каб.	Назва каб.	IP-адреса мережі/Маска IP-адреси	Діапазон IP-адрес	
			Перша IP-адреса	Остання IP-адреса
14	Кабінет агроінженерії	192.168.4.0/27	192.168.4.2	192.168.4.21
15	Кабінет фізики			
16	Юрист			
17	Бухгалтерія			
18	Кабінет хімії			
19	Устаткування харчової промисловості			

Таблиця 2.8 – IP-адресації мережевих сегментів корпусу 2

Номер VLAN	Назва каб.	IP-адреса мережі/Маска IP-адреси	Діапазон IP-адрес	
			Перша IP-адреса	Остання IP-адреса
10	Секретарі	192.168.10.0/24	192.168.10.2	192.168.10.4
20	Секретарі	192.168.20.0/24	192.168.20.2	192.168.20.4
30	Музей №1	192.168.30.0/24	192.168.30.2	192.168.30.2
40	Музей №2	192.168.40.0/24	192.168.40.2	192.168.40.2

Таблиця 2.9 – IP-адресації мережевих сегментів серверів

Назва сервера	IP-адреса мережі/Маска IP-адреси	IP-адреса сервера	Шлюз за замовчуванням
DNS	192.168.1.0/24	192.168.1.10	192.168.1.1
DHCP	192.168.1.0/24	192.168.1.2	192.168.1.1
SYSLOG	192.168.1.0/24	192.168.1.4	192.168.1.1
HTTP(kvpu.com)	203.0.114.0/24	203.0.114.2	203.0.114.1
HTTP(chatgpt.com)	203.0.115.0/24	203.0.115.2	203.0.115.1

Подібна організація мережі надає значні переваги, серед яких можна виокремити такі аспекти:

– розподіл потоків даних: завдяки ізоляції даних різних груп користувачів зменшується їхній взаємний вплив, що позитивно позначається на швидкості передачі даних і загальній стабільності роботи мережі;

– підвищення рівня безпеки: конфіденційна інформація адміністративного характеру залишається доступною виключно уповноваженим особам, тоді як навчальна мережа функціонує окремо, не впливаючи на адміністративну інфраструктуру;

– можливість масштабування: така структура забезпечує легкий і зручний розвиток мережі в майбутньому, дозволяючи додавати нові підмережі без ризику порушення функціонування вже існуючих сегментів.

На рисунку 2.7 зображений приклад організації мережевих сегментів.

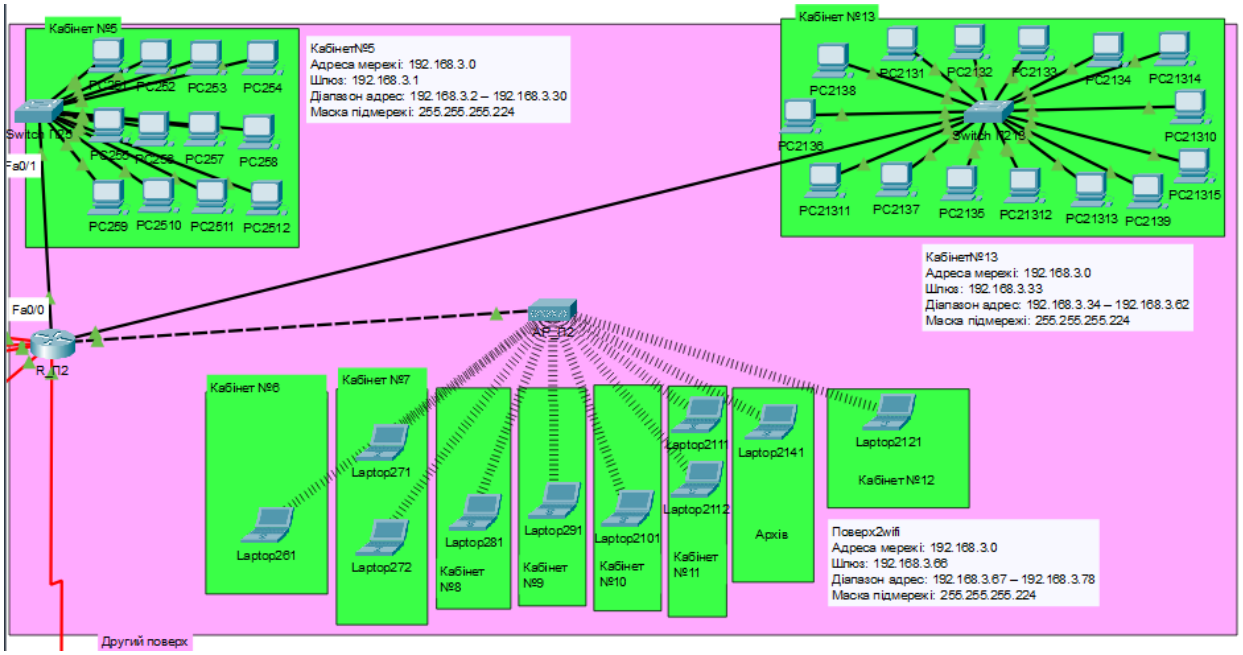

Рисунок 2.7 – Приклад мережевих сегментів

Для забезпечення маршрутизації використовується протокол RIP, який ефективно передає дані між підмережами, мінімізуючи затримки в передачі й одночасно покращуючи продуктивність роботи системи в цілому. Для оптимального управління комп’ютерною мережею використовується комбінація статичної та динамічної IP-адресації. Ця стратегія дозволяє гармонійно поєднати зручність адміністрування з ефективним розподілом ресурсів. Зокрема, для персональних комп’ютерів, ноутбуків та інших робочих станцій застосовується динамічне призначення IP-адрес через сервер DHCP. Це забезпечує автоматичний розподіл адрес для всіх пристроїв, які підключаються до мережі, що дає такі переваги:

– зручність в управлінні: адміністратор звільняється від необхідності ручного налаштування кожного нового пристрою [5];

– гнучке використання адресного простору: динамічне призначення

дозволяє змінювати адреси для оптимального використання ресурсів IP-простору;

– запобігання конфліктам: DHCP-сервер відповідає за розподіл адрес, мінімізуючи ризик дублювання або інших помилок.

Водночас для ключових пристроїв, таких як маршрутизатори, сервери (файлові та веб-сервери), точки доступу Wi-Fi та мережеві комутатори, використовується статична IP-адресація (табл. 2.10).

Таблиця 2.10 – IP-адресація з'єднань мережевих пристроїв

Назва мережевого сегменту	IP-адреса мережі/Маска IP-адреси	IP-адреси інтерфейсів мережевих пристроїв		Тип і номер інтерфейсу	
		Підкл. A	Підкл. B	Підкл. A	Підкл. B
R_П1-FW	192.168.100.0/24	192.168.100.3	192.168.100.1	Fa9/0	Et0/2
R_П1-R_K1	10.0.0.0/8	10.0.0.1	10.0.0.2	Se2/0	Se0/0/0
R_П1- R_П2	45.83.204.0/8	45.83.204.12	45.83.204.13	Se3/0	Se3/0
R_П1- R_П3	102.67.189.0/8	102.67.189.54	102.67.189.55	Se6/0	Se3/0
R_K1-FW	192.168.100.0/24	192.168.100.2	192.168.100.1	Gig0/1	Et0/1
R_K1-R_VPN	172.16.1.0/30	172.16.1.1	172.16.1.2	Tun1	Tun2
R_out-FW	203.0.113.0/30	203.0.113.2	203.0.113.1	Fa1/0	Et0/0
R_out-isp	203.0.114.0/24	203.0.114.1	203.0.114.2	Fa0/0	Fa0
R_out-chatgpt	203.0.115.0/24	203.0.115.1	203.0.115.2	Fa6/0	Fa0
R_П2- R_K1	20.0.0.0/8	20.0.0.1	20.0.0.2	Se2/0	Se0/0/1
R_П2- R_П3	185.214.97.0/16	185.214.97.37	185.214.97.36	Se4/0	Se2/0
R_П2- R_K2	196.245.32.0/24	196.245.32.116	196.245.32.115	Se8/0	Se2/0
R_П3- R_K1	30.0.0.0/8	30.0.0.1	30.0.0.2	Se6/0	Se0/1/0
R_П3- R_K2	23.156.98.0/8	23.156.98.200	23.156.98.201	Se7/0	Se3/0

У таких випадках кожному пристрою вручну призначається постійна адреса, яка залишається незмінною. Цей підхід є необхідним з кількох причин:

– стабільність роботи: постійна IP-адреса гарантує безперебійну доступність серверів і обладнання;

– простота адміністрування: адміністраторам значно легше знаходити та управляти такими пристроями в межах мережевої інфраструктури;

– забезпечення безпеки: завдяки статичним адресам можна налаштовувати фільтрування трафіку або обмеження доступу до певних ресурсів на основі унікальних IP-ідентифікаторів.

У результаті інтеграції статичної та динамічної IP-адресації створюється ефективна, гнучка й водночас надійна мережа, яка оптимально відповідає

сучасним вимогам управління та безпеки.

Для забезпечення стабільності та доступності мережі у випадку відмови деяких елементів інфраструктури потрібно налаштувати резервні маршрути між маршрутизаторами. Вона дозволяє підтримувати роботу мережі навіть у критичних ситуаціях, мінімізуючи ризики втрати даних і часу. Центральний маршрутизатор залишається ключовим елементом мережі, але додаткові механізми, такі як резервування маршрутів і використання динамічної маршрутизації, забезпечують високу доступність і надійність мережі.

2.4 Технологія VLAN

Virtual Local Area Network (VLAN) – це віртуальна локальна мережа, де комп'ютери, сервери та інші мережеві пристрої логічно з'єднані незалежно від їх фізичного розташування [6]. Тож якщо пристрої розкидані по різних місцях, це немає значення, тому що VLAN може логічно об'єднати їх в окремі віртуальні мережі. Віртуальну локальну мережу можна розглядати як окрему підмережу або широкомовний домен, тож для переміщення пакетів з однієї такої мережі в іншу використовується маршрутизатор або комутатор третього рівня. Також вони допомгають розбити велику мережу на кілька менших частин, через що обладнання буде менше навантаженим (рис. 2.8). Покращення безпеки теж входить в список можливостей таких мереж, тому що дані з інших підмереж можуть бути відсіяні та не пропускатись в інший VLAN [7].

Використовуючи VLAN можна надати ком'ютерам локальні адреси або налаштувати роздачу адрес з окремого DHCP серверу.

Віртуальні локальні мережі можна поділити на такі типи:

– Data VLAN: застосовується при передачі даних між комп'ютерами;

– Voice VLAN: голосові дані передаються за допомогою цього типу віртуальних мереж і через виділений канал він надає якісний зв'язок;

– Management VLAN: в більшості випадків цей тип VLAN відділений від інших, тому і має більший рівень безпеки, активне мережеве обладнання

керується з використанням цього типу;

– Native VLAN: завичай застосовується для необроблених даних, які проходять через trunk.

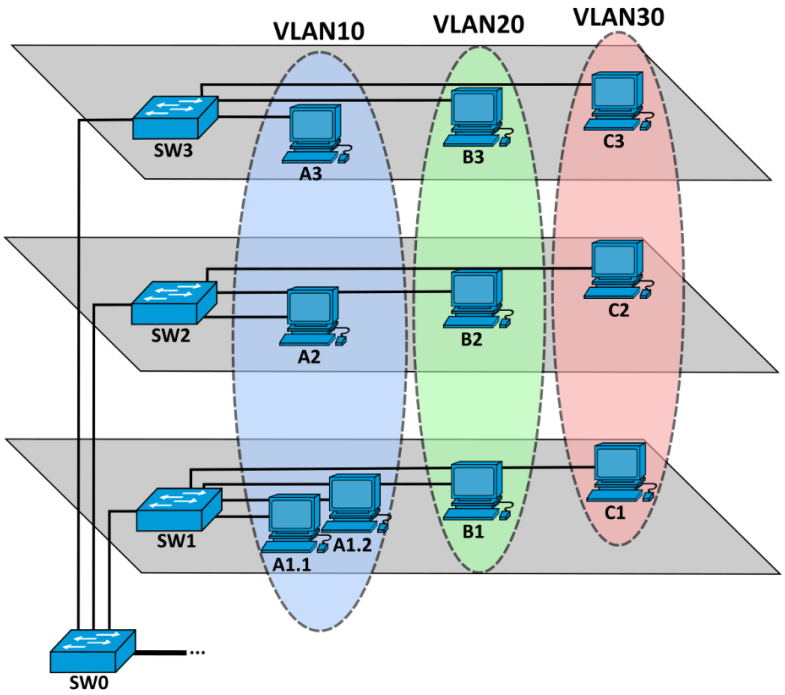

Рисунок 2.8 – Схема VLAN [6]

Створення вітуальних локальних мереж складається з кількох головних кроків:

– за допомогою командного рядка на комутаторі створити VLAN;

– призначення портів для VLAN;

– для зв’язку між різними VLAN потрібно налаштувати trunk-порт.

2.5 Бездротовий доступ

На сьогоднішній день бездротовий доступ до мережі став невід’ємною частиною повсякденного життя. Можливість підключення до Інтернету без використання кабелів значно полегшує більшість процесів нашого життя.

Використання бездротових мереж надають такі переваги:

– забезпечення високої швидкості передачі даних;

– можливість швидкого розгортання мережі;

– мобільність користувачів та свобода переміщення в межах покриття;

– можливість заміни або відмови від прокладання кабелів.

Однак, бездротові мережі мають і певні недоліки: вони схильні до впливу перешкод, мають обмежену зону покриття, а також потребують додаткових заходів безпеки через відкритий характер передавання даних.

Для проєктування WLAN потрібні мінімум один маршрутизатор або бездротова точка доступу (Access Point), які будуть відігравати роль мосту між провідною мережею та пристроями з вбудованими Wi-Fi адаптерами та не менше одного клієнта [8]. Тому маршрутизатор або точка доступу приймає трафік з кабельного каналу та перетворює його на радіосигнали, які будуть передаватись клієнтським пристроям, які в свою чергу за допомогою адаптерів перетворюють сигнали в цифрову інформацію.

На рисунку 2.9 зображений приклад організації бездротової мережі.

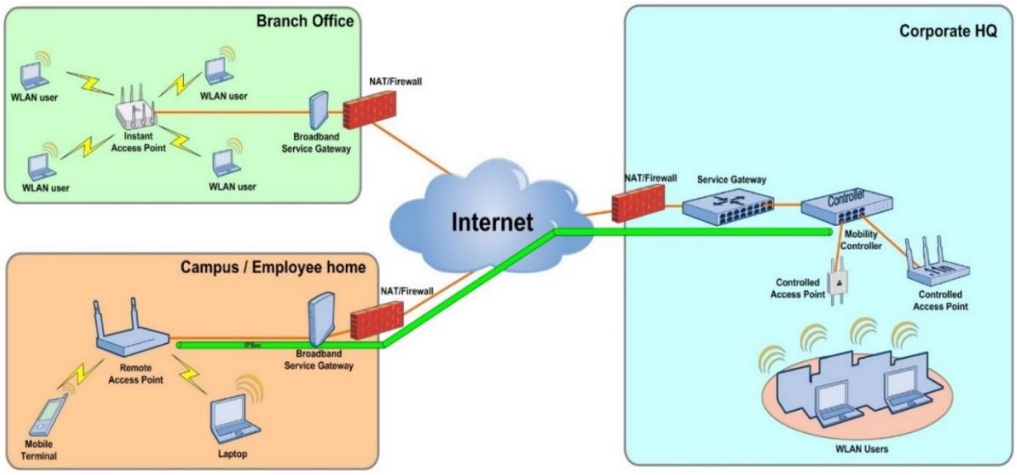

Рисунок 2.9 – Бездротова мережа за технологією Wi-Fi [9]

Кожна передача даних у Wi-Fi-мережі супроводжується двома ключовими процедурами:

1) аутентифікацією (перевіркою автентичності користувача):

– відкрита (Open Network): дозволяє підключатися будь-якому пристрою без перевірки, часто використовується у публічних місцях (кав’ярні, торгові

центри);

– з паролем (Shared Key): для підключення необхідно ввести ключ безпеки або пароль, це поширений варіант у домашніх та офісних мережах;

– через сервер (EAP): пристрій проходить перевірку через зовнішній сервер автентифікації (наприклад, RADIUS) [10]. Такий спосіб характерний для корпоративних мереж;

2) шифруванням (захистом переданих даних від несанкціонованого доступу):

– WEP (Wired Equivalent Privacy): застарілий протокол, який використовує шифр RC4 та ключі довжиною 64 або 128 біт, легко зламується, тому не рекомендований до використання [8];

– TKIP (Temporal Key Integrity Protocol): покращена версія WEP, динамічно генерує ключ для кожного пакета, зараз також вважається застарілим [10];

– AES (Advanced Encryption Standard): сучасний стандарт, який застосовується в WPA2 та WPA3, використовує 128-бітне або 256-бітне шифрування. Забезпечує найвищий рівень безпеки [11];

– None: означає повну відсутність шифрування, що створює серйозну загрозу безпеці даних.

У зв’язку з відкритістю середовища передавання, бездротові мережі є більш вразливими до атак, ніж дротові. Тому при розгортанні Wi-Fi мережі важливо забезпечити належний рівень захисту. Основні методи підвищення безпеки на точках доступу:

1) фільтрація MAC-адрес;

2) режим прихованого ідентифікатора SSID;

3) методи шифрування:

– WEP: застарілий стандарт, легко зламується;

– WPA: покращена версія WEP, але вже не вважається надійною;

– WPA2-PSK: надійний шифрувальний стандарт із використанням ключа.

РОЗДІЛ 3
ПРОЄКТУВАННЯ МЕРЕЖІ

3.1 Конфігурація маршрутизаторів та комутаторів

Для забезпечення надійної передачі даних та з’єднання між пристроями використовуються різні мережеві пристрої, серед яких ключову роль відіграють маршрутизатори (routers) та комутатори (switches).

«Маршрутизатор або роутер – електронний пристрій, що використовується для поєднання двох або більше мереж і керує процесом маршрутизації, тобто на підставі інформації про топологію мережі та певних правил приймає рішення про пересилання пакетів мережевого рівня (рівень 3 моделі OSI) між різними сегментами мережі» [12].

З точки зору пересічного користувача, маршрутизатор – це пристрій, який забезпечує з’єднання локальної мережі з Інтернетом. Окрім передавання даних між інтерфейсами, сучасні маршрутизатори часто виконують додаткові функції: захист мережі від зовнішніх загроз, контроль доступу до Інтернету, розподіл IP-адрес, шифрування трафіку, перетворення мережевих адрес, створення VPN-тунелів, слугувати DHCP-сервером, тощо.

Маршрутизатори працюють на мережевому рівні моделі OSI. Для передачі даних у правильному напрямку вони використовують таблицю маршрутизації, яка зберігається у внутрішній пам’яті. Ця таблиця може бути налаштована вручну (статично) або формуватися автоматично за допомогою протоколів динамічної маршрутизації [13]. На рисунку 3.1 зображено таблицю динамічної машрутизації.

На відміну від статичної маршрутизації, де маршрути задаються вручну, динамічна маршрутизація дозволяє маршрутизаторам самостійно визначати найкращі шляхи до інших мереж, оновлювати маршрути при зміні топології та забезпечувати безперервність передачі даних.

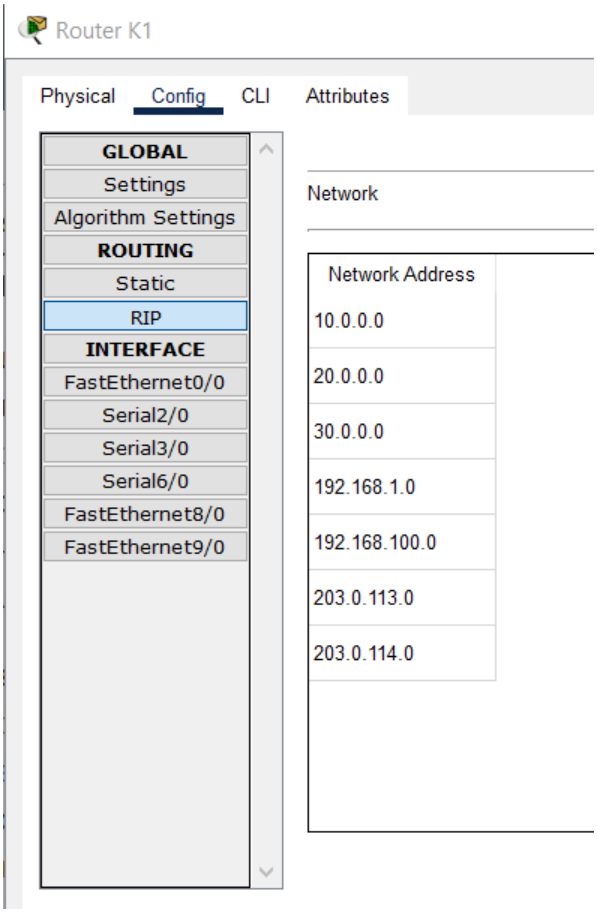

Рисунок 3.1 – Протокол динамічної машрутизації (RIP)

Ці протоколи працюють за певними алгоритмами, які аналізують різні параметри мережі – наприклад, кількість переходів (хопів), затримки, пропускну здатність тощо. На основі зібраної інформації кожен маршрутизатор створює та оновлює свою таблицю маршрутизації.

Протоколи динамічної маршрутизації поділяються на два основних типи:

1) внутрішні протоколи маршрутизації (IGP) – використовуються всередині однієї автономної системи. До них належать:

– RIP (Routing Information Protocol);

– EIGRP (Enhanced Interior Gateway Routing Protocol);

– OSPF (Open Shortest Path First);

2) зовнішні протоколи маршрутизації (EGP) – використовуються для обміну маршрутами між автономними системами. Найпоширенішим представником є BGP (Border Gateway Protocol).

Маршрутизатори, які працюють з динамічними протоколами, постійно

обмінюються інформацією зі своїми сусідами, що дає змогу адаптуватися до змін у мережі без втручання адміністратора [8].

На рисунку 3.2 зображено таблицю статичної машрутизації.

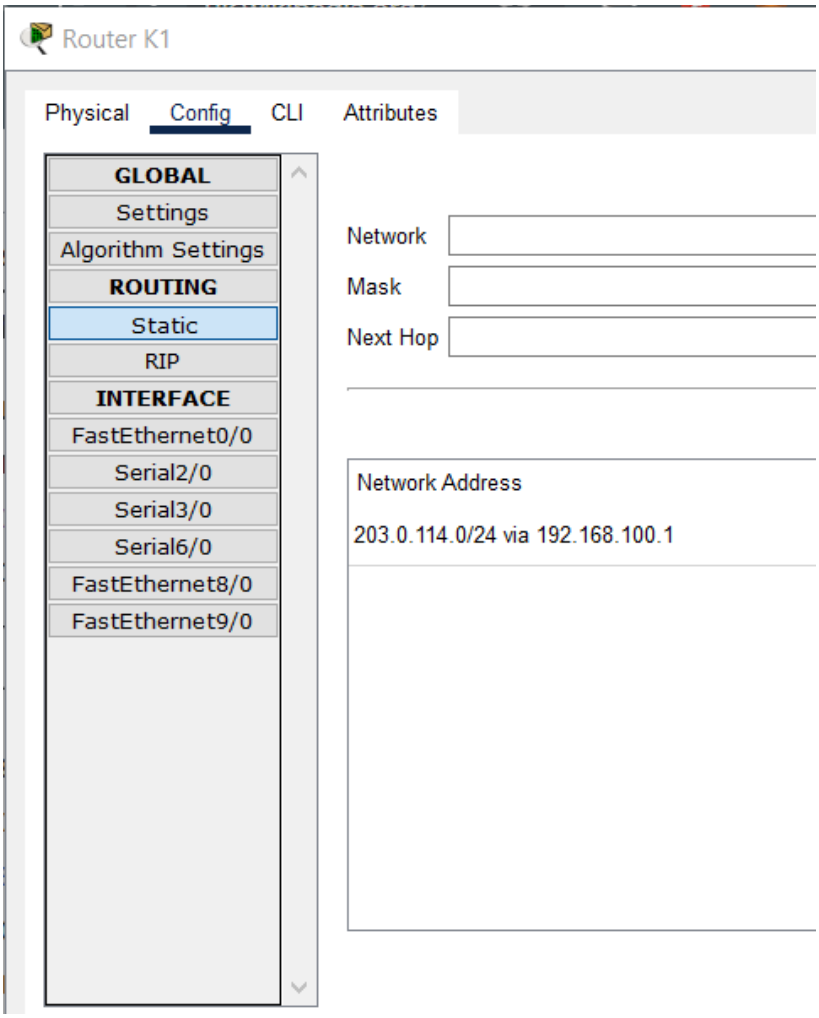

Рисунок 3.2 – Таблиця статичної маршрутизації

Крім основних функцій, маршрутизатори можуть виконувати трансляцію мережевих адрес, фільтрувати вхідний і вихідний трафік за заданими правилами, а також здійснювати шифрування і дешифрування переданих даних для підвищення безпеки.

Для базових налаштувань маршрузитора в Cisco Packet Tracer можна використовувати вкладку Config, для більш детального налаштування використовується командний рядок CLI (рис. 3.3).

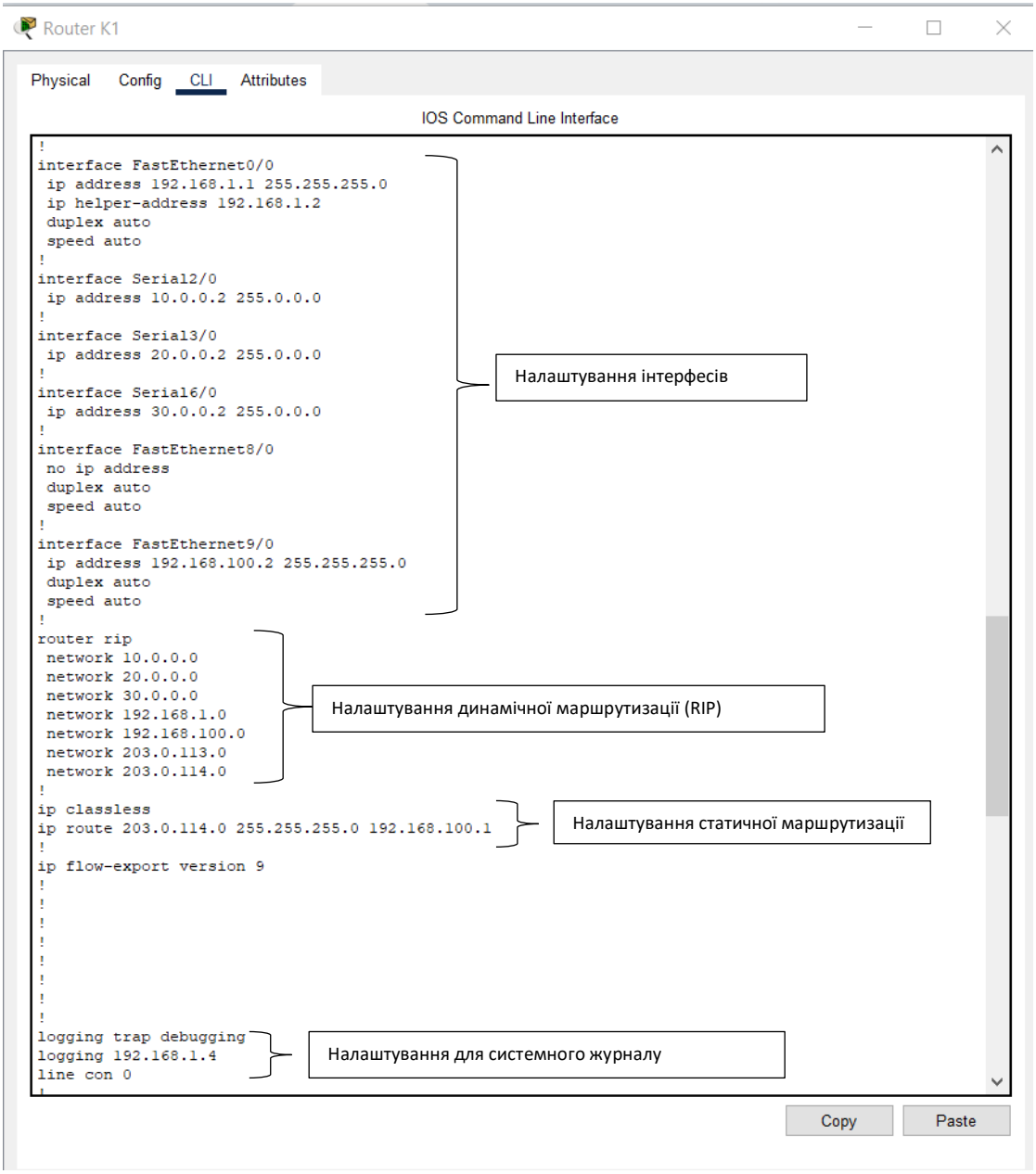

Рисунок 3.3 – Налаштування центрального маршрутизатора за допомогою CLI

Центральний маршрутизатор є ядром мережі. Його основними функціями є:

– маршрутизація між підмережами;

– доступ до Інтернету.

Однак, щоб не втратити функціональність мережі у разі виходу з ладу центрального маршрутизатора, налаштовуються резервні шляхи. Резервні маршрути дозволяють підтримувати з’єднання між сегментами мережі навіть у разі виходу центрального маршрутизатора з ладу. Це досягається завдяки

наступним підходам:

– резервні маршрутизатори: другорядні маршрутизатори налаштовані на забезпечення з'єднання між сегментами мережі. Вони мають альтернативні шляхи для передачі трафіку між підмережами, які активуються лише в разі відмови основного маршрутизатора;

– статичні резервні маршрути: кожен другорядний маршрутизатор налаштовується з використанням статичних маршрутів, що вказують альтернативний шлях для передачі даних. Резервний маршрут має вищий адміністративний пріоритет, тому він активується лише тоді, коли основний маршрут недоступний;

– динамічні протоколи маршрутизації: для автоматизації процесу перемикання між маршрутами використовуються динамічні протоколи маршрутизації. Вони дозволяють маршрутизаторам автоматично адаптувати маршрутизацію відповідно до змін у топології мережі. Це забезпечує швидке виявлення збоїв і їхнє усунення.

На рисунку 3.4 та рисунку 3.5 зображена організація резервних маршрутів для маршрутизатора другого поверху.

Device Name: Router П2
Device Model: Router-PT
Hostname: Router

Маршрутизатор другого поверху

Port	Link	IP Address	IPv6 Address	MAC Address
FastEthernet0/0	Up	192.168.3.1/27	<not set>	000A.F3D0.A96A
FastEthernet1/0	Up	192.168.3.66/27	<not set>	00E0.F9AB.3193
Serial2/0	Up	20.0.0.1/8	<not set>	<not set>
Serial3/0	Up	45.83.204.13/8	<not set>	<not set>
Serial4/0	Up	185.214.97.37/16	<not set>	<not set>
FastEthernet5/0	Up	192.168.1.1/24	<not set>	0003.E45E.04EB
FastEthernet6/0	Up	192.168.3.33/27	<not set>	0001.C988.23A4
FastEthernet7/0	Down	<not set>	<not set>	0090.2B2D.E316
Serial8/0	Up	196.245.32.116/24	<not set>	<not set>
Serial9/0	Down	<not set>	<not set>	<not set>

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Router П2

Рисунок 3.4 – Інтерфейси резевних маршрутів другого поверху

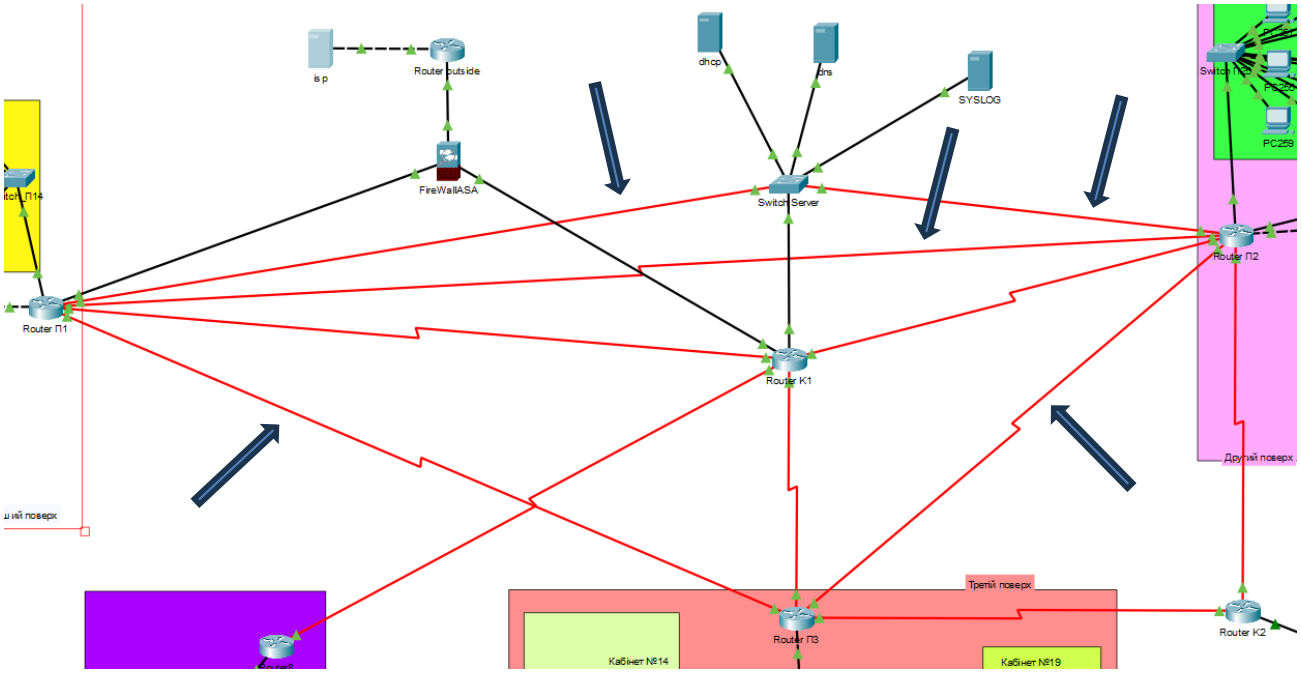

Рисунок 3.5 – Резервні маршрути мережі

«Комутатор – пристрій, призначений для з’єднання декількох вузлів комп’ютерної мережі в межах одного сегмента» [14]. Основна функція комутатора полягає в тому, щоб направляти пакети даних безпосередньо до потрібного одержувача, використовуючи для цього MAC-адреси пристроїв.

На відміну від простого концентратора, який розсилає дані всім підключеним пристроям, комутатор аналізує трафік і надсилає інформацію лише до відповідного порту, зменшуючи тим самим завантаження мережі та підвищуючи її ефективність.

Комутатори працюють на канальному рівні моделі OSI. Вони ведуть спеціальну таблицю MAC-адрес, за якою визначають, до якого порту підключено той чи інший пристрій [14]. Завдяки цьому комутатор «вчиться» мережевій топології й оптимізує процес передавання кадрів.

Багато сучасних комутаторів є керованими – це означає, що адміністратор може налаштовувати такі функції, як VLAN, контроль доступу, моніторинг трафіку, пріоритезація та інші параметри. Це робить їх ключовими елементами корпоративних і навчальних мереж. На рисунку 3.6 зображено базові налашутвання VLAN на комутаторі.

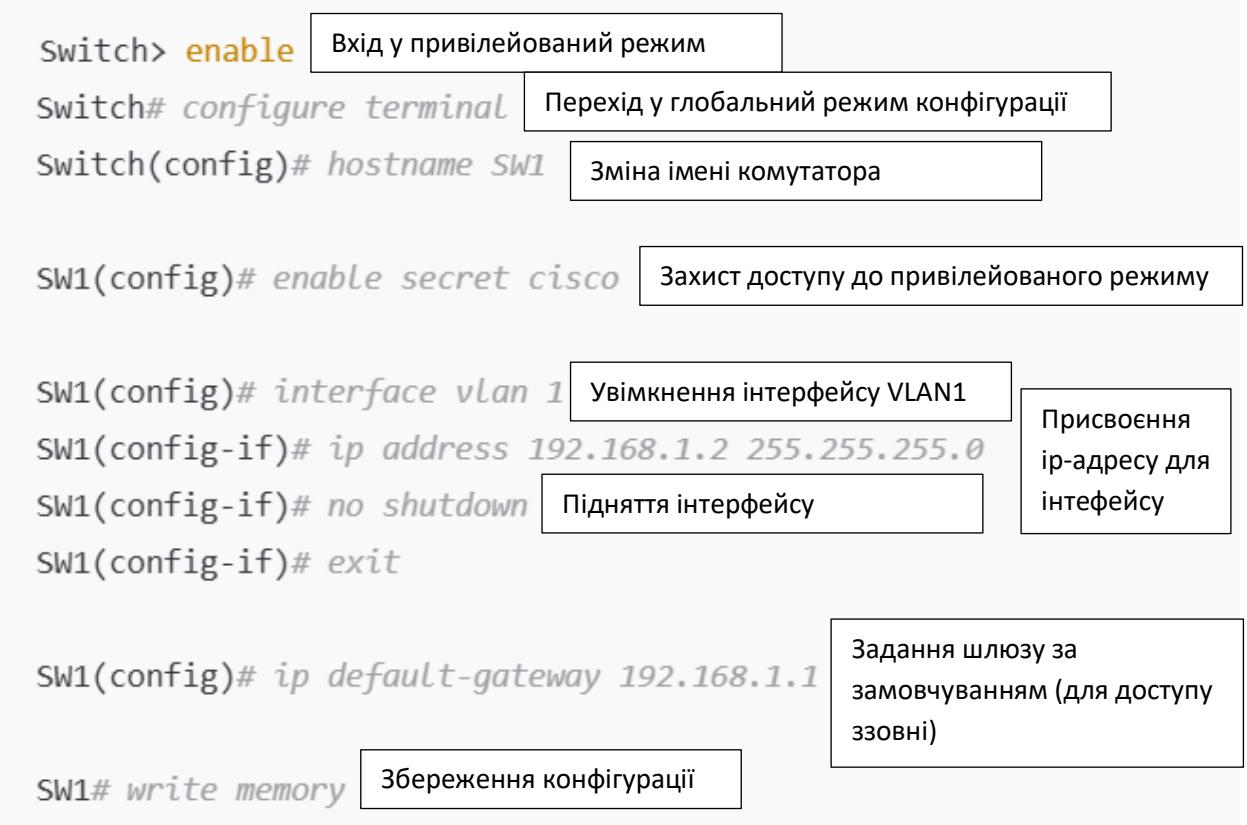

Рисунок 3.6 – Налаштування комутатора за допомогою CLI

Загалом, комутатор забезпечує швидку, надійну та організовану комунікацію всередині локальної мережі, відіграючи роль «вузла зв’язку» між усіма підключеними пристроями – комп’ютерами, принтерами, серверами тощо.

3.2 Налаштування серверів

DHCP – це мережевий протокол, який дозволяє клієнтам автоматично отримувати необхідні параметри для роботи в мережі, зокрема:

– IP-адресу;

– маску підмережі;

– шлюз за замовчуванням;

– адресу DNS-сервера.

Це дозволяє уникнути ручного конфігурування IP-адрес на кожному клієнтському пристрої та зменшує ймовірність конфліктів адрес [15]. На рисунку 3.7 зображено графічний інтерфейс DHCP-серверу в Cisco Packet Tracer.

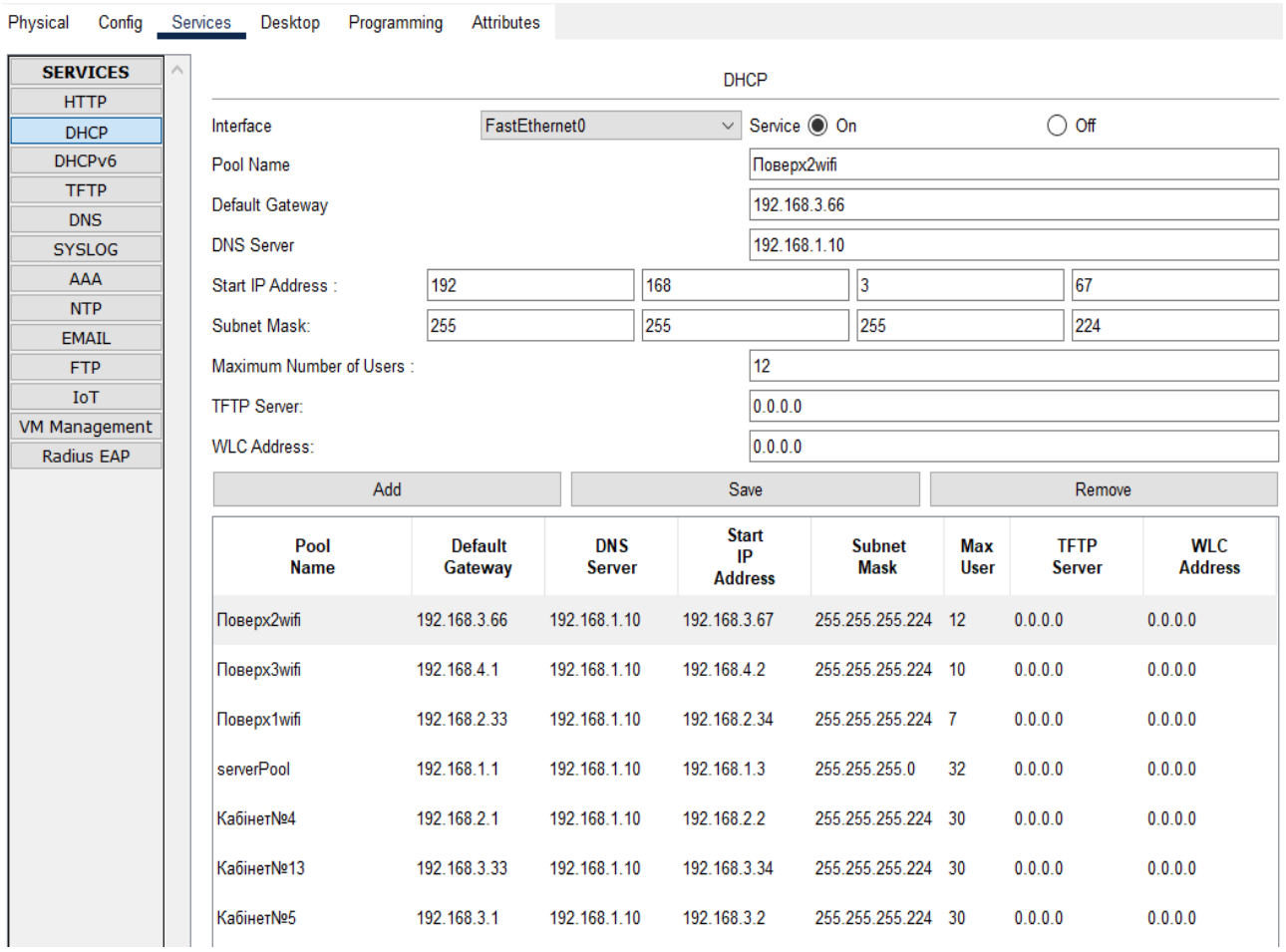

Рисунок 3.7 – Налаштування DHCP-серверу за допомогою графічного інтерфейсу

Після налаштування пулу DHCP потрібно на кожному маршрутизаторі, який з'єднаний з окремою підмережею вказати адресу DHCP-сервера за допомогою команди ip helper-address (рис. 3.8), налаштувати маршрутизацію між підмережами (рис. 3.1 та рис. 3.2) та перевірити на пристроях (рис. 3.9).

```
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 ip helper-address 192.168.1.2
 duplex auto
 speed auto
```

Рисунок 3.8 – Налаштування DHCP Relay на інтерфейсах маршрутизаторів

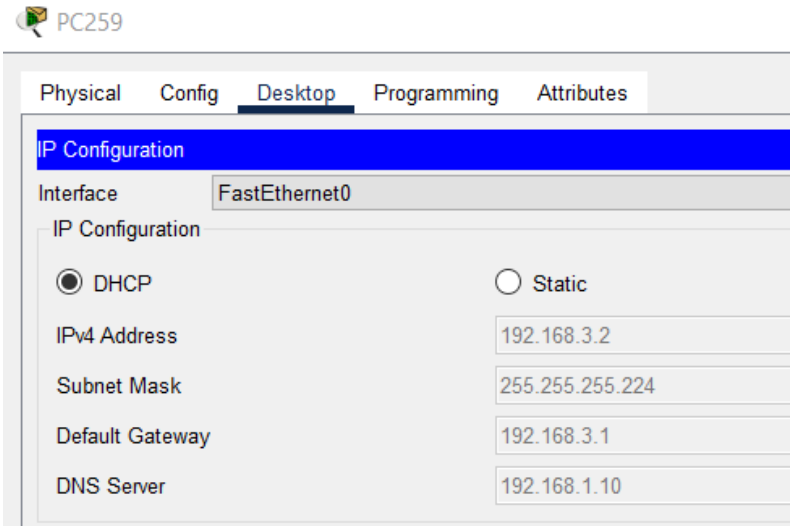

Рисунок 3.9 – Перевірка справності DHCP-серверу

DNS-сервер перетворює імена хостів на IP-адреси. Хоча можна отримати доступ до мережевого хоста, використовуючи його IP-адресу, DNS спрощує цей процес, дозволяючи використовувати доменні імена, які легше запам’ятовувати [16]. Наприклад, набагато легше отримати доступ до веб-сайту Google, ввівши http://www.google.com, ніж http://208.117.229.214.

Перш ніж будь-який хост зможе використовувати службу DNS, потрібно спочатку налаштувати DNS-сервер (рис. 3.10).

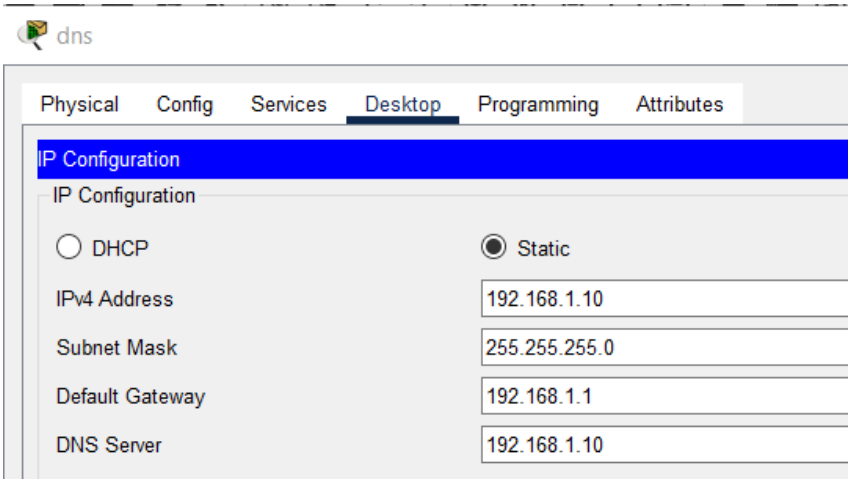

Рисунок 3.10 – Налаштування DNS-серверу

Ввімкнувши на сервері за допомогою графічного інтерфейсу службу DNS, додаємо до списку IP-адресу з її доменним ім’ям (рис. 3.11) [15].

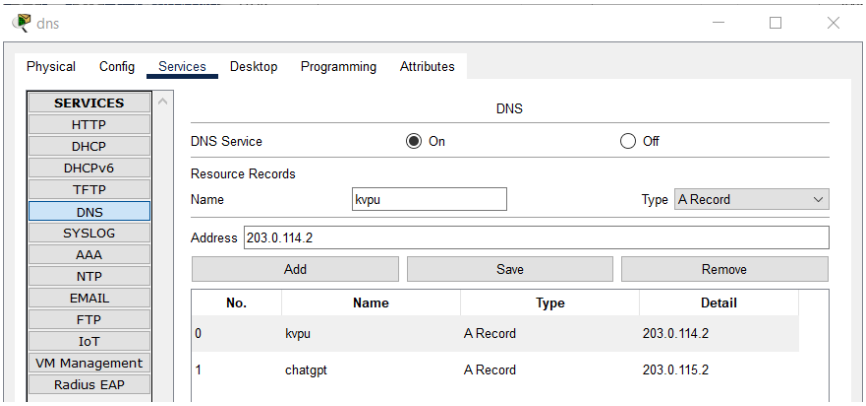

Рисунок 3.11 – Список доменних імен служби DNS

3.3 Створення VLAN

Для підвищення ефективності управління мережею та забезпечення логічного розділення трафіку було реалізовано впровадження віртуальних локальних мереж. VLAN дозволяють розділити одну фізичну мережу на декілька логічних сегментів, кожен з яких функціонує як окрема підмережа, незалежно від фізичного розташування пристроїв. На рисунку 3.12 зображено схему VLAN на базі комутатора.

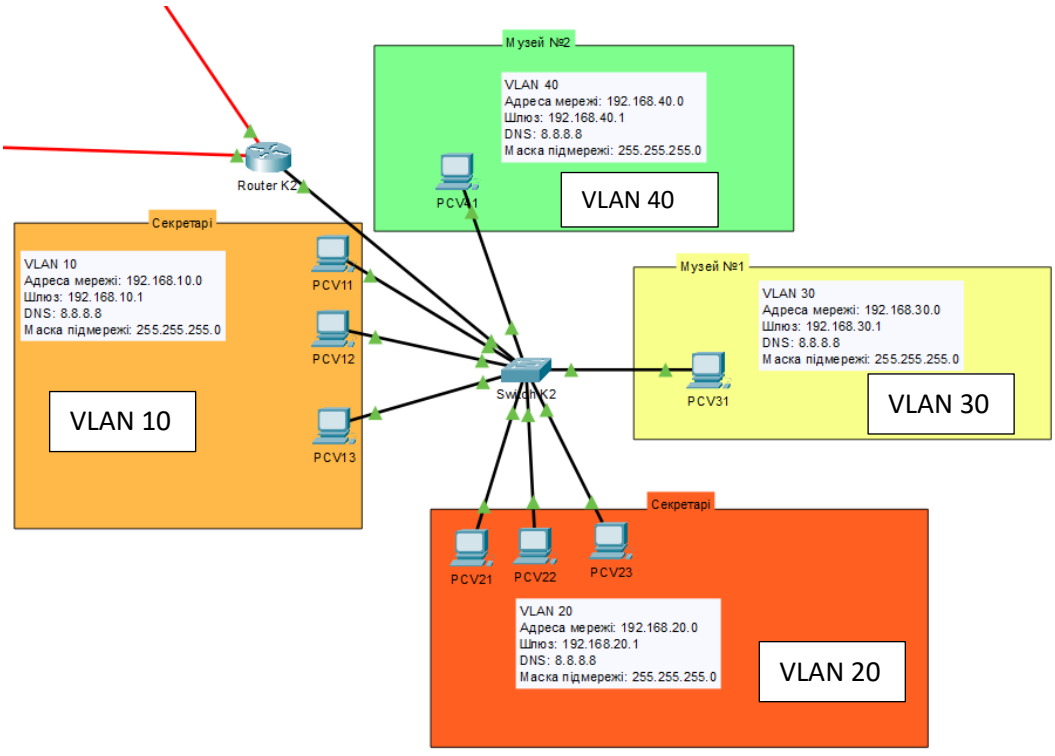

Рисунок 3.12 – Схема VLAN

В лістингах 3.1-3.2 наведено приклад створення та налаштування VLAN.

Лістинг 3.1 – Налаштування комутатора для VLAN

```
Switch> enable
Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# name Cabinet
Switch(config-vlan)# exit
Switch(config)# interface fastEthernet 0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# exit
Switch(config)# interface fastEthernet 0/24
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 10,20,30
```

кінець лістингу 3.1

Лістинг 3.2 – Налаштування маршрутизатора для VLAN

```
Router> enable
Router# configure terminal
Router(config)# interface fastethernet0/0.10
Router(config-subif)# encapsulation dot1Q 10
Router(config-subif)# ip address 192.168.10.1 255.255.255.0
Router(config-subif)# exit
Router(config)# interface fastethernet0/0
Router(config-if)# no shutdown
Router(config-if)# exit
Router# write memory
```

кінець лістингу 3.2

Віртуальні локальні мережі можуть створюватися на основі портів комутаторів (додаток А) [13]. Такий підхід є доволі простим у налаштуванні, проте має певні обмеження. Зокрема, кожен порт може належати лише до однієї VLAN, що знижує гнучкість управління. Крім того, будь-які зміни у структурі мережі потребують ручного втручання – тобто фізичного перепідключення пристроїв, що ускладнює модернізацію або переналаштування мережі.

Комутатори не мають можливості самостійно пересилати пакети між різними VLAN, оскільки вони працюють лише з MAC-адресами та не обробляють IP-адресацію. У ситуаціях, коли пристрої з різних VLAN мають обмінюватися даними, необхідна «міжвланова» маршрутизація.

Одним з ефективних способів реалізації такої маршрутизації є використання методу Router-on-a-Stick. Ця технологія, дозволяє маршрутизатору обслуговувати кілька VLAN через один фізичний інтерфейс, використовуючи підінтерфейси та протокол 802.1Q для тегування VLAN.

Принцип роботи Router-on-a-Stick заключається в тому, що один фізичний порт маршрутизатора підключається до комутатора, на цьому порту створюється кілька підінтерфейсів, кожен із яких відповідає певній VLAN. Для кожного підінтерфейсу задається тег VLAN через команду encapsulation dot1Q [номер VLAN]. Кожному сабінтерфейсу призначається IP-адреса, яка буде використовуватися як шлюз за замовчуванням для пристроїв VLAN [17]. На комутаторі порт, який підключений до маршрутизатора, повинен працювати в режимі trunk, щоб передавати трафік із тегами VLAN (додаток А).

3.4 Налаштування безпровідної мережі та точок доступу

Бездротова мережа є невід'ємною частиною сучасної інфраструктури, особливо у закладах освіти, де забезпечення мобільного доступу до ресурсів мережі є важливим для учнів, викладачів та персоналу.

Для створення безпровідних мереж в Колківському ЦПО використовується точка доступу Cisco Catalyst C9120AXI. Для забезпезпечення захисту мережі використано шифрувальний стандарт WPA2-PSK [11].

На рисунку 3.13 та рисунку 3.14 зображено приклад налаштування точки доступу та підключеного пристрою.

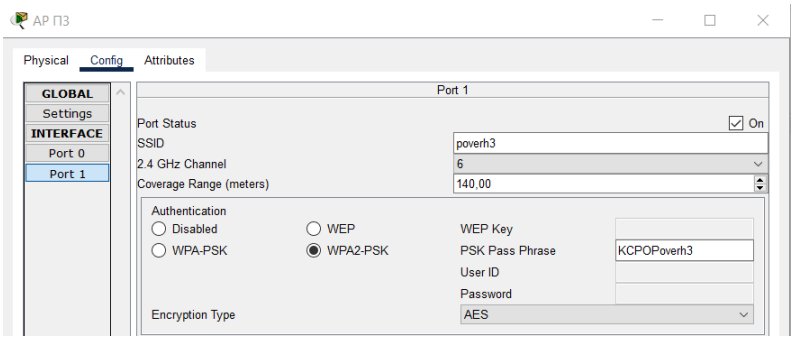

Рисунок 3.13 – Налаштування Access point за допомогою графічного інтерфейсу

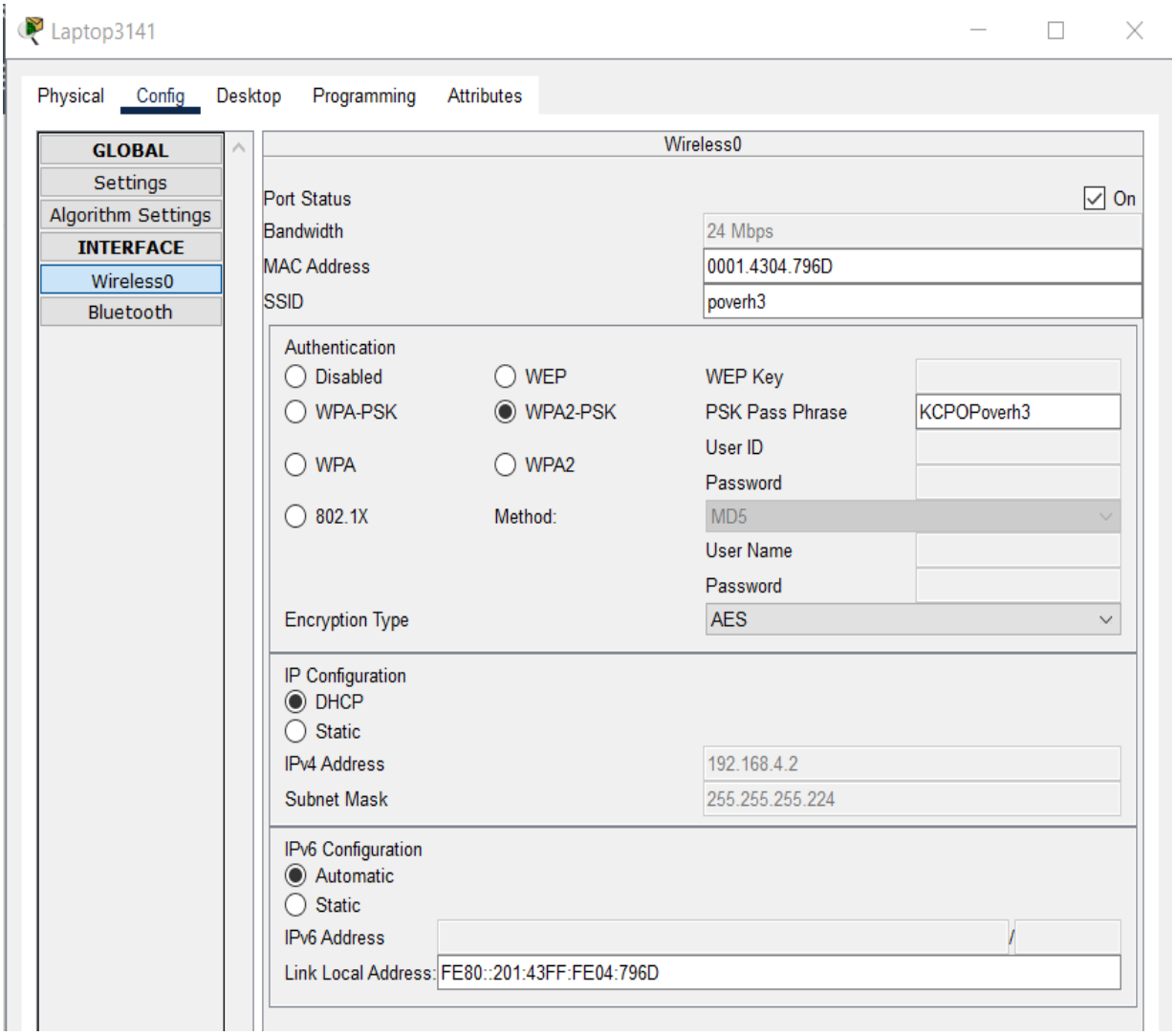

Рисунок 3.14 – Налаштування підключення клієнтського пристрою до точки доступу

3.5 Забезпечення доступу та його безпеки до мережі Інтернет

У процесі побудови комп’ютерної мережі навчального закладу налаштовано доступ до мережі Інтернет із забезпеченням відповідного рівня безпеки за допомогою міжмережевого екрану (рис. 3.15). Основне завдання міжмережевого екрану – захист локальної мережі від зовнішніх атак, контроль трафіку та організація NAT для роботи пристроїв із внутрішньою адресацією в мережі Інтернет [18].

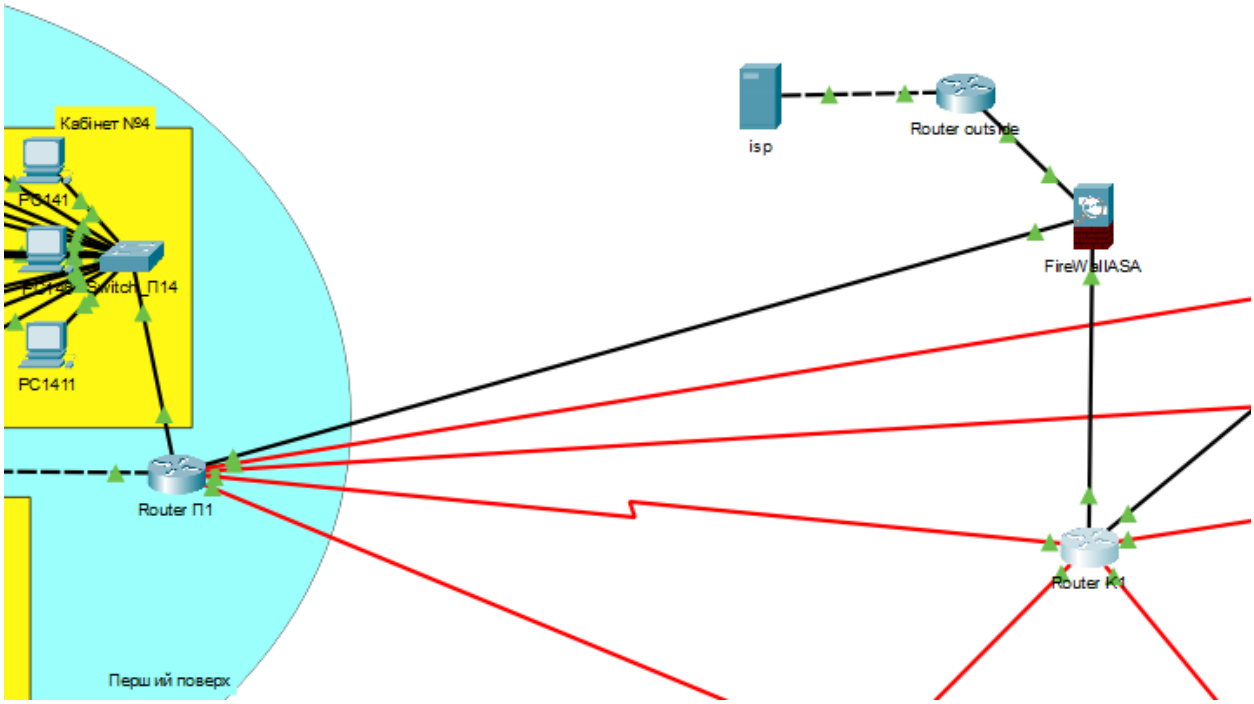

Рисунок 3.15 – Схема умовного виходу в зовнішню мережу

Для організації доступу клієнтів внутрішньої мережі в Інтернет додано динамічний NAT. Усі пристрої локальної мережі заміняють власні внутрішні IP-адреси на зовнішню IP-адресу інтерфейсу «outside». Такий підхід дає можливість з'єднатись з Інтернетом і приховати внутрішню структуру мережі від зовнішніх користувачів. Міжмережевий екран можна налаштувати з інших підмереж, налаштувавши SSH-доступ. Налаштування списків контролю доступу (ACL) значно підвищує рівень безпеки мережі. Вони дозволяють адміністраторам мережі задавати чіткі правила, які визначають, який трафік дозволений або заборонений у мережі [18].

Основні функції ACL:

– заборонити доступ із зовнішньої мережі до серверів у внутрішній мережі;

– дозволити лише певні типи трафіку (наприклад, HTTP або SSH);

– захист мережі від несанкціонованого доступу;

– дозволяє визначати, які пристрої або користувачі мають доступ до серверів, баз даних або інших критично важливих ресурсів.

На рисунку 3.16 зображена конфігурація Cisco ASA та можна побачити, що

до серверу 203.0.115.2 доступ дозволено всім, крім пристроїв, які знаходяться в мережі 192.168.4.0.

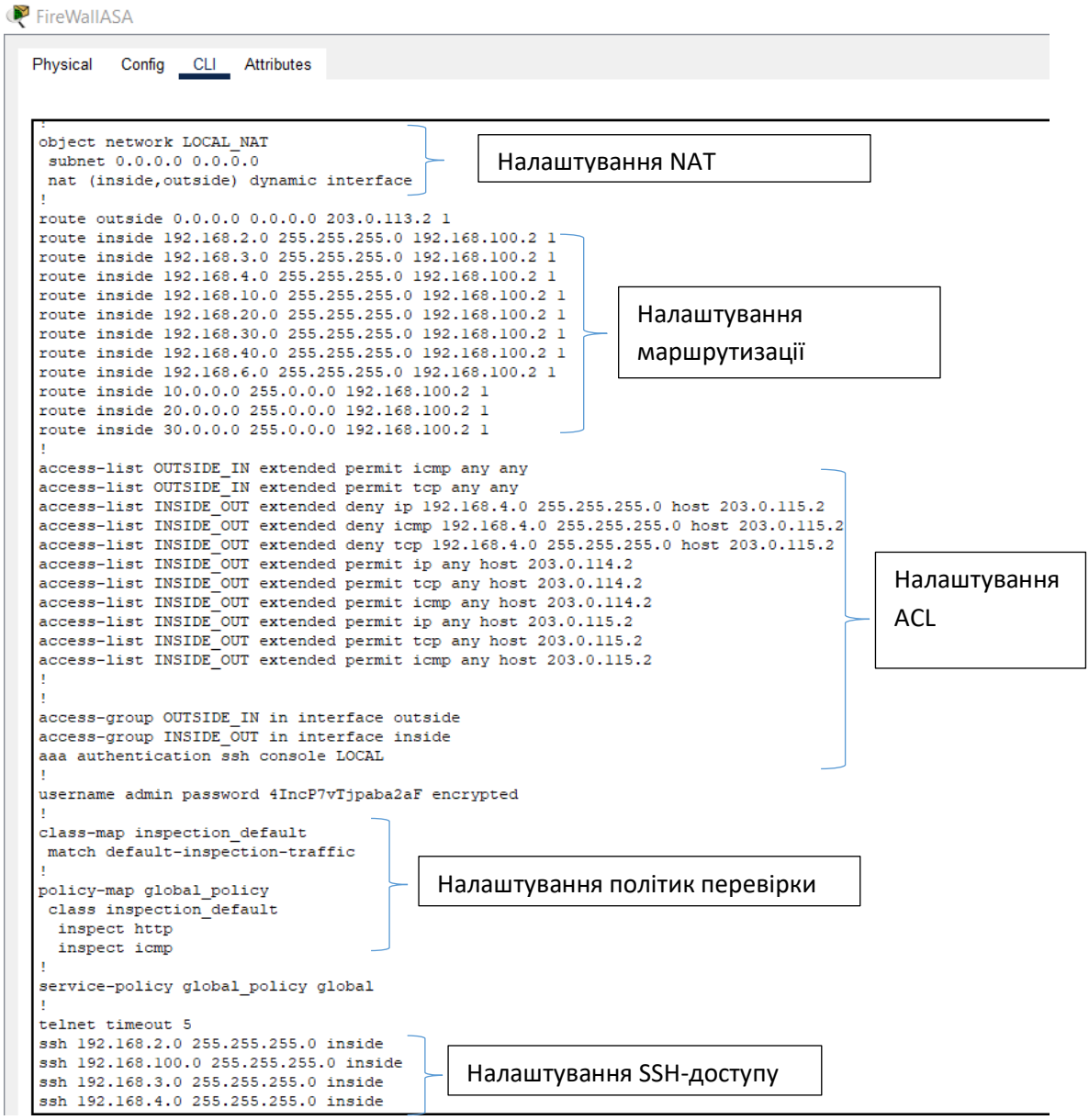

Рисунок 3.16 – Налаштування Cisco ASA

3.6 Створення та налаштування VPN

«VPN – узагальнена назва клієнт-серверних технологій, які дають змогу створювати віртуальні захищені мережі поверх інших мереж із нижчим рівнем довіри. VPN-тунель, який створюється між двома вузлами, дозволяє приєднаному пристрою чи користувачу бути повноцінним учасником віддаленої

мережі і користуватись її сервісами – внутрішніми сайтами, базами, принтерами, політиками виходу в інтернет» [19]. Організацію віртальних приватних мереж класифікують за призначенням віртуального розширення.

Конфігурація «хост-мережа» нагадує ситуацію, коли один або кілька комп'ютерів під'єднані до мережі, до якої безпосередньо неможливо потрапити. Цей вид з'єднання надає комп'ютеру можливість доступу до віддаленої локальної мережі або масштабнішої корпоративної мережі. Кожен комп'ютер самостійно відповідає за створення власного тунелю до мережі, до якої бажає підключитися. З'єднана мережа має інформацію лише про один віддалений хост на кожен такий тунель. Таке рішення може використовуватися для віддалених співробітників або для надання користувачам доступу до їхніх особистих домашніх або корпоративних ресурсів, не надаючи їм доступ до публічного інтернету. Тунелі віддаленого доступу можуть працювати як за запитом, так і постійно. Щоб ця конфігурація працювала коректно, віддалений хост повинен ініціювати з'єднання з центральною мережею, до якої він має доступ, адже розташування віддаленого хоста зазвичай невідоме центральній мережі до моменту спроби підключення.

Конфігурація «Site-to-Site» з'єднує дві різні мережі. Такий тип дозволяє розширити мережу на віддалених географічних локаціях. Тунелювання реалізується лише між двома пристроями (маршрутизатори, брандмауери, VPN-шлюзи, сервери тощо), котрі розміщені в кожній з мереж. Після цього ці пристрої надають тунель для інших хостів локальної мережі, яким необхідно досягти будь-якого хоста з іншого боку. Це вигідно для підтримки стабільного зв'язку між локаціями, наприклад, між мережею головного офісу та філіалом. У цьому сценарії будь-яку зі сторін можна налаштувати на ініціювання з'єднання, за умови, що вона знає, як встановити зв'язок з іншою стороною у внутрішній мережі.

Для можливості захищеного з'єднання з мережею корпусу, який знаходиться в іншому населеному пункті створено VPN-з'єднання на основі GRE-тунелю (рис. 3.17). GRE-тунель дає можливість інкапсулювати пакети

протоколу всередину IP, забезпечуючи логічне з’єднання між двома віддаленими вузлами. Це дозволяє створити віртуальну приватну мережу поверх публічної або небезпечної мережі, зокрема Інтернету.

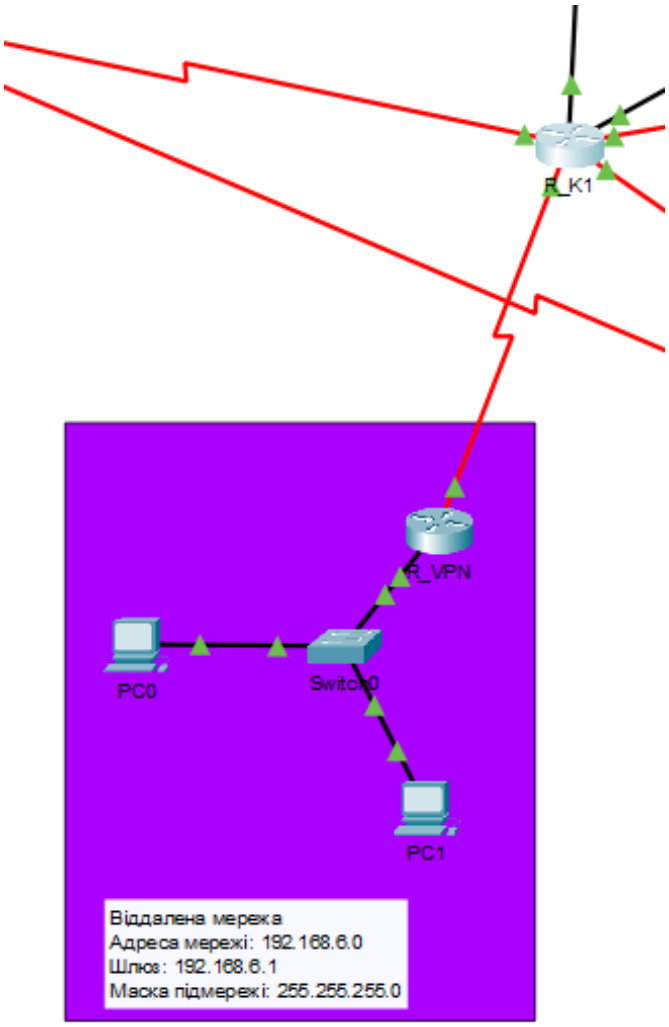

Рисунок 3.17 – Налаштуавння VPN-з’єднання

Хоч GRE сам по собі не шифрує дані, його можна поєднати з IPSec для захищеного тунелювання. У межах даної реалізації в Cisco Packet Tracer GRE використовується без IPSec, однак можливе подальше вдосконалення:

– додавання IPSec-шифрування поверх GRE;

– аутентифікація маршрутів (MD5);

– фільтрація дозволених IP-адрес для тунелю за допомогою ACL.

На рисунку 3.18 та рисунку 3.19 зображені налаштування GRE-тунелю на маршрутизаторах.

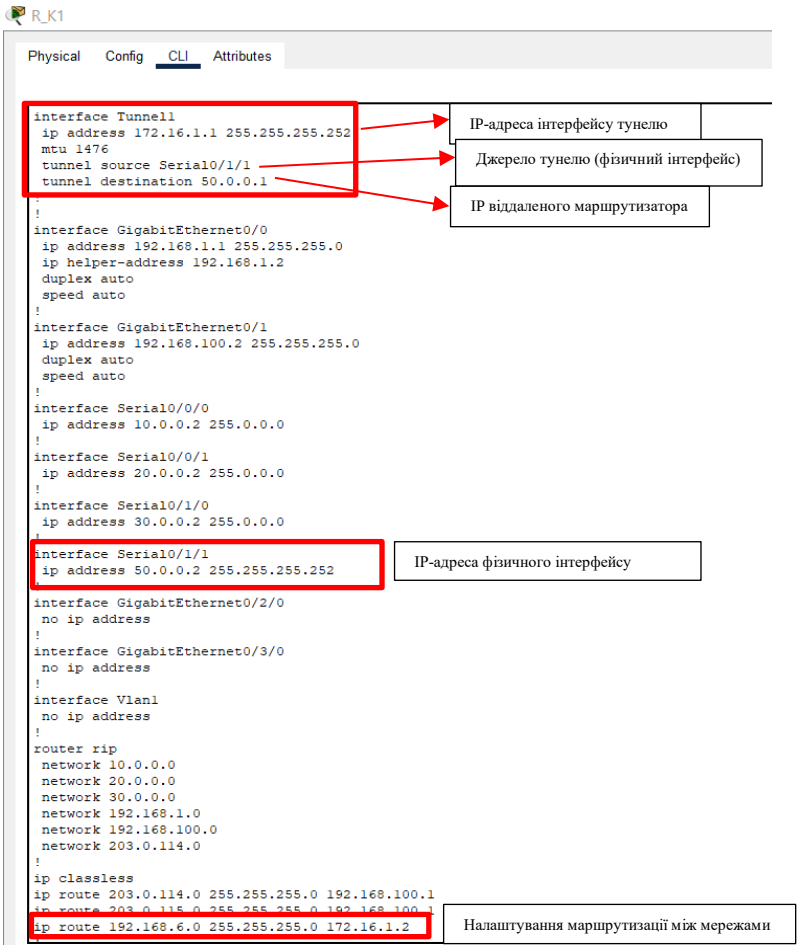

Рисунок 3.18 – Конфігурація GRE-тунелю на маршрутизаторі [20]

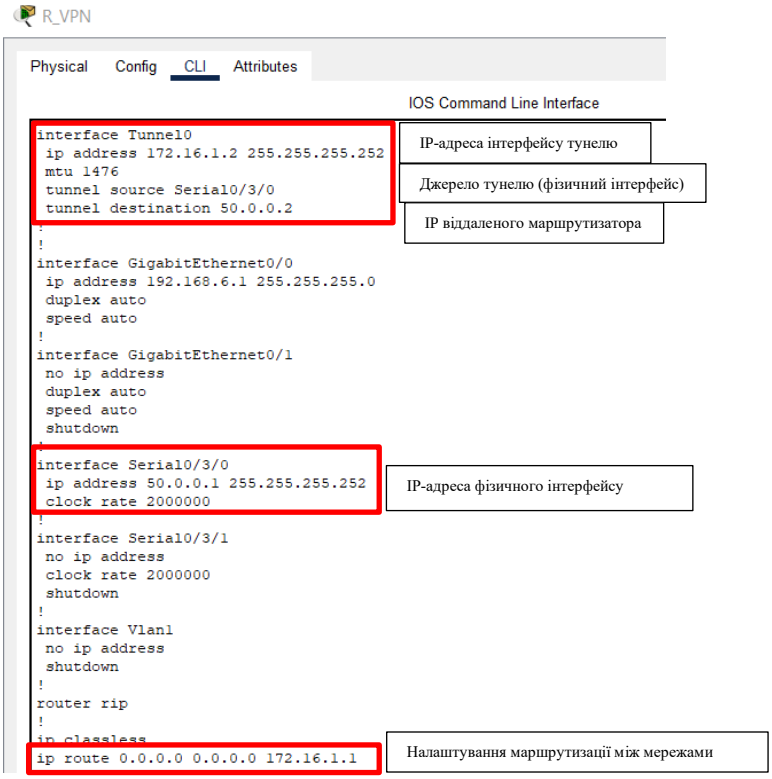

Рисунок 3.19 – Конфігурація GRE-тунелю на віддаленому маршрутизаторі [20]

Перевірити VPN-з’єднання можна за допомгою команди «ping». Для цього на віддаленому маршрутизаторі спробуємо «пропінгувати» одну з підмереж головного корпусу (рис. 3.20).

```
Router#ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/8/17 ms
```

Рисунок 3.20 – Перевірка VPN-з’єднання

На риснку 3.21 зображена модернізована мережа Колкіського центру професійної освіти.

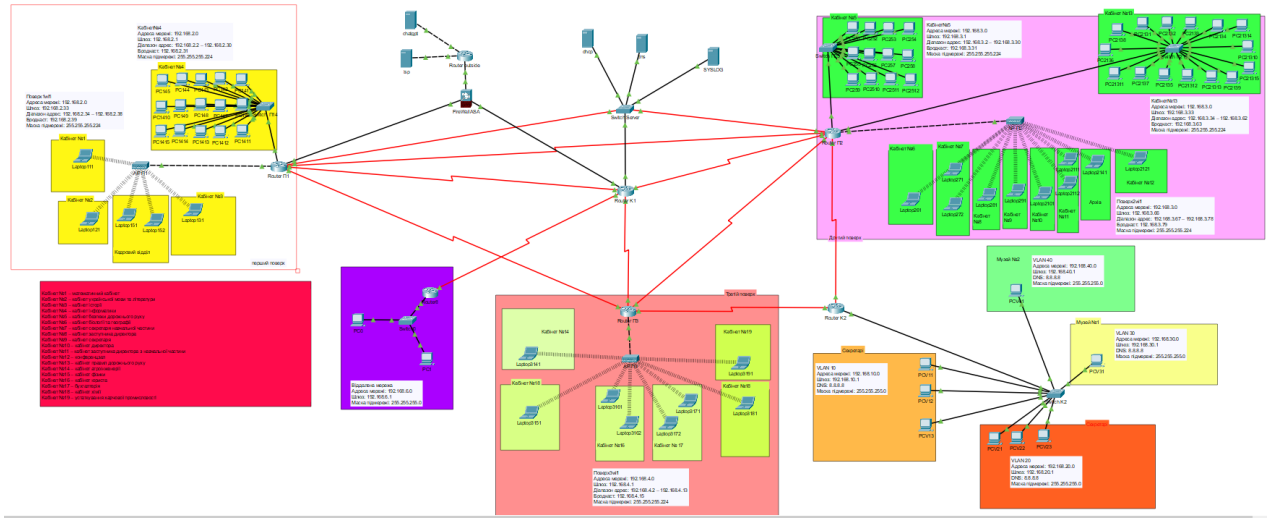

Рисунок 3.21 – Модернізована мережа Колківського ЦПО

Отже, розроблена схема модернізованої комп’ютерної мережі Колківського центру професійної освіти (рис. 3.21) демонструє повну реалізацію технічних рішень, описаних у попередніх розділах. Усі структурні елементи мережі взаємопов’язані, відповідають вимогам функціональності, безпеки та ефективного адміністрування. Архітектура мережі забезпечує гнучкість та готовність до подальшого масштабування.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи здійснено детальний аналіз існуючої мережі та потреб модернізованої мережі Колківського центру професійної освіти. В процесі проєктування нової мережевої інфаструктури створено ефективне, надійне та масштабоване рішення, відповідне потребам освітнього процесу.

Після аналізу мережі та потреб навчального закладу, визначено специфіку роботи закладу та необхідності інтеграції сучасних технологій у навчальний процес та вимог до продуктивності і безпеки мережі. Це дозволило розробити оптимальну логічну структуру мережі, яка враховує всі особливості функціонування закладу.

Також здійснено вибір та налаштування сучасного мережевого обладнання, що відповідає вимогам масштабованості, захищеності та ефективності роботи. Зокрема, були обрані маршрутизатори, комутатори, точки доступу та міжмережевий екран виробництва Cisco, що забезпечують стабільну роботу мережі навіть при значному навантаженні. Налаштування мережі здійснено з використанням технологій VLAN, NAT та резервування маршрутів, що підвищують її продуктивність і відмовостійкість.

Розроблено проєкт мережі, створено відповідну технічну документацію, яка описує всі аспекти мережевої інфраструктури – від топології мережі до правил безпеки та процедур резервного копіювання даних. Це дозволить зручніше адмініструвати, підтримувати і вдосконалювати мережу у майбутньому.

Модернізована мережа забезпечує високий рівень безпеки даних, стабільний доступ до Інтернету для всіх підрозділів закладу, а також дозволяє ефективно інтегрувати сучасні інформаційні технології в навчальний процес. Завдяки впровадженню резервних шляхів зв’язку між маршрутизаторами гарантується безперебійна робота мережі навіть у разі виходу з ладу центрального обладнання.

Результати роботи підтверджують, що створена комп’ютерна мережа відповідає сучасним стандартам, покращує якість організації освітнього процесу та забезпечує можливість подальшої модернізації. Впровадження розробленого проєкту дозволить Колківському центру професійної освіти стати більш технологічним, ефективним та готовим до нових викликів у галузі освіти.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Основна інформація. *Колківський ЦПО*. URL: https://kvpu.info (дата звернення: 02.03.2025).

2. Топологія мереж. *Вікіпедія*. URL: https://surl.li/vhxdag (дата звернення: 02.03.2025).

3. Бездротовий зв’язок. *Cisco.com.ua*. URL: https://xn--h1aemkx.com.ua/air (дата звернення: 10.03.2025).

4. Сервер HP ProLiant DL360 Gen10. *Serverparts*. URL: https://surl.li/oozfpv (дата звернення: 10.03.2025).

5. Адресація в IP-мережах. *Вікіпедія*. URL: https://surl.li/vgxytq (дата звернення: 13.03.2025).

6. VLAN. *Вікіпедія*. URL: https://uk.wikipedia.org/wiki/VLAN (дата звернення: 17.03.2025).

7. Що таке VLAN: логіка, технологія і налаштування. Реалізація VLAN в пристроях CISCO. *Мережеве обладнання*. URL: https://surli.cc/akvyct (дата звернення: 17.03.2025).

8. Лабораторний практикум. *Електронна бібліотека Житомирського державного університету*. URL: http://eprints.zu.edu.ua/33991/1/km.pdf (дата звернення: 18.03.2025).

9. Рішення бездротового доступу. *IT-Dialg*. URL: https://surl.li/wxolxu (дата звернення: 18.03.2025).

10. Реферат. Уразливості сучасних бездротових мереж маршрутизаторів і роутерів. *StudFiles*. URL: https://studfile.net/preview/16435981/ (дата звернення: 19.03.2025).

11. Побудова бездротових мереж в Cisco Packet Tracer. *UA5.org – Матеріали з інформаційних технологій*. URL: https://ua5.org/lan/1481-pobudova-bezdrotovyh-merezh-v-cisco-packet-tracer.html (дата звернення: 19.03.2025).

12. Маршрутизатор. *Вікіпедія*. URL: https://surl.li/orugnv (дата звернення: 19.03.2025).

13. Лабораторний практикум у Cisco Packet Tracer. *Репозитарій КПІ ім. Ігоря Сікорського*. URL: https://surl.li/imamck (дата звернення: 21.03.2025).

14. Мережевий комутатор. *Вікіпедія*. URL: https://surli.cc/yhwrpy (дата звернення: 21.03.2025).

15. Network for you. DHCP DNS and Web Server configuration in cisco packet tracer, 2023. *YouTube*. URL: https://www.youtube.com/watch?v=ZTNwwevT7S8 (дата звернення: 25.03.2025).

16. DNS server configuration in Packet Tracer. *Computer Networking Tips*. URL: https://computernetworking747640215.wordpress.com/2018/07/05/dns-server-configuration-in-packet-tracer/ (дата звернення: 25.03.2025).

17. VLT. Simple VLAN Configuration Cisco Packet Tracer, 2021. *YouTube*. URL: https://surl.li/ltwgsf (дата звернення: 26.03.2025).

18. Greg South. Configuring an ASA Firewall on Cisco Packet Tracer, 2020. *YouTube*. URL: https://surl.lu/skukpd (дата звернення: 28.03.2025).

19. VPN. *Вікіпедія*. URL: https://uk.wikipedia.org/wiki/VPN (дата звернення: 01.04.2025).

20. Gurutech Networking Training. CCNA DAY 60: GRE Tunnel Configuration in Cisco Packet Tracer | How to configure GRE VPN Tunnel, 2023. *YouTube*. URL: https://surli.cc/jlwuao (дата звернення: 01.04.2025).

ДОДАТКИ

Додаток А

Конфігурація мережевих пристроїв

Маршрутизатор R_K2:

```
Current configuration : 2151 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
ip dhcp excluded-address 192.168.10.1
ip dhcp excluded-address 192.168.20.1
ip dhcp excluded-address 192.168.30.1
ip dhcp excluded-address 192.168.40.1
!
ip dhcp pool VLAN10
network 192.168.10.0 255.255.255.0
default-router 192.168.10.1
dns-server 8.8.8.8
ip dhcp pool VLAN20
network 192.168.20.0 255.255.255.0
default-router 192.168.20.1
dns-server 8.8.8.8
ip dhcp pool VLAN30
network 192.168.30.0 255.255.255.0
default-router 192.168.30.1
dns-server 8.8.8.8
ip dhcp pool VLAN40
network 192.168.40.0 255.255.255.0
default-router 192.168.40.1
dns-server 8.8.8.8
!
no ip cef
no ipv6 cef
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
!
interface FastEthernet0/0.10
encapsulation dot1Q 10
ip address 192.168.10.1 255.255.255.0
!
interface FastEthernet0/0.20
encapsulation dot1Q 20
ip address 192.168.20.1 255.255.255.0
!
interface FastEthernet0/0.30
encapsulation dot1Q 30
ip address 192.168.30.1 255.255.255.0
!
interface FastEthernet0/0.40
encapsulation dot1Q 40
ip address 192.168.40.1 255.255.255.0
!
interface FastEthernet1/0
no ip address
duplex auto
speed auto
shutdown
!
interface Serial2/0
ip address 196.245.32.115 255.255.255.0
clock rate 2000000
!
interface Serial3/0
ip address 23.156.98.201 255.0.0.0
clock rate 2000000
!
router rip
network 23.0.0.0
network 192.168.1.0
network 196.245.32.0
!
ip classless
ip route 203.0.114.0 255.255.255.0 23.156.98.200
!
ip flow-export version 9
!
logging trap debugging
logging 192.168.1.4
l
end
```

Маршрутизатор R_П1:

```
Current configuration : 1445 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
no ip cef
no ipv6 cef
!
interface FastEthernet0/0
ip address 192.168.2.1 255.255.255.224
ip helper-address 192.168.1.2
duplex auto
speed 100
!
interface FastEthernet1/0
ip address 192.168.2.33 255.255.255.224
ip helper-address 192.168.1.2
duplex auto
speed auto
!
interface Serial2/0
ip address 10.0.0.1 255.0.0.0
clock rate 2000000
!
interface Serial3/0
ip address 45.83.204.12 255.0.0.0
!
interface FastEthernet4/0
ip address 192.168.1.1 255.255.255.0
!
interface FastEthernet5/0
no ip address
shutdown
!
interface Serial6/0
ip address 102.67.189.54 255.0.0.0
clock rate 2000000
!
interface Serial7/0
no ip address
clock rate 2000000
!
interface Serial8/0
ip address 154.91.18.77 255.255.0.0
clock rate 2000000
!
interface FastEthernet9/0
ip address 192.168.100.3 255.255.255.0
duplex auto
speed auto
!
router rip
network 10.0.0.0
network 45.0.0.0
network 102.0.0.0
network 154.91.0.0
network 192.168.1.0
network 192.168.2.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.0.0.2
ip route 203.0.114.0 255.255.255.0 192.168.100.1
ip route 203.0.115.0 255.255.255.0 192.168.100.1
!
ip flow-export version 9
!
logging trap debugging
logging 192.168.1.4
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
end
```

Маршрутизатор R_VPN:

```
Current configuration : 994 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
no ip cef
no ipv6 cef
!
license udi pid CISCO2901/K9 sn FTX1524APO7-
!
spanning-tree mode pvst
!
interface Tunnel0
ip address 172.16.1.2 255.255.255.252
mtu 1476
tunnel source Serial0/3/0
tunnel destination 50.0.0.2
!
interface GigabitEthernet0/0
ip address 192.168.6.1 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/3/0
ip address 50.0.0.1 255.255.255.252
clock rate 2000000
!
interface Serial0/3/1
no ip address
clock rate 2000000
shutdown
!
interface Vlan1
no ip address
shutdown
!
router rip
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.1.1
!
ip flow-export version 9
!
logging trap debugging
logging 192.168.1.4
line con 0
!
line aux 0
!
line vty 0 4
login
!
end
```

Маршрутизатор R_out:

```
Current configuration : 896 bytes
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname Router
ip cef
!
interface FastEthernet0/0
ip address 203.0.114.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 203.0.113.2 255.255.255.252
duplex auto
speed auto
interface FastEthernet6/0
ip address 203.0.115.1 255.255.255.0
duplex auto
speed auto
!
router rip
!
ip classless
ip route 0.0.0.0 0.0.0.0 203.0.113.1
!
ip flow-export version 9
line con 0
line aux 0
line vty 0 4
login
end
```

Маршрутизатор R_П2:

```
Current configuration : 1403 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
no ip cef
no ipv6 cef
!
interface FastEthernet0/0
ip address 192.168.3.1 255.255.255.224
ip helper-address 192.168.1.2
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 192.168.3.66 255.255.255.224
ip helper-address 192.168.1.2
duplex auto
speed auto
!
interface Serial2/0
ip address 20.0.0.1 255.0.0.0
clock rate 2000000
!
interface Serial3/0
ip address 45.83.204.13 255.0.0.0
clock rate 2000000
!
interface Serial4/0
ip address 185.214.97.37 255.255.0.0
!
interface FastEthernet5/0
ip address 192.168.1.1 255.255.255.0
!
interface FastEthernet6/0
ip address 192.168.3.33 255.255.255.224
ip helper-address 192.168.1.2
duplex auto
speed auto
!
interface FastEthernet7/0
no ip address
duplex auto
speed auto
shutdown
!
interface Serial8/0
ip address 196.245.32.116 255.255.255.0
!
interface Serial9/0
no ip address
clock rate 2000000
shutdown
!
router rip
network 20.0.0.0
network 45.0.0.0
network 185.214.0.0
network 192.168.1.0
network 192.168.3.0
network 196.245.32.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 20.0.0.2
!
ip flow-export version 9
!
logging trap debugging
logging 192.168.1.4
line con 0
!
line aux 0
!
line vty 0 4
login
!
end
```

Маршрутизатор R_ПЗ:

```
Current configuration : 1278 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
no ip cef
no ipv6 cef
!
interface FastEthernet0/0
ip address 192.168.4.1 255.255.255.224
ip helper-address 192.168.1.2
duplex auto
speed auto
!
interface FastEthernet1/0
no ip address
duplex auto
speed auto
!
interface Serial2/0
ip address 185.214.97.36 255.255.0.0
clock rate 2000000
!
interface Serial3/0
ip address 102.67.189.55 255.0.0.0
!
interface FastEthernet4/0
no ip address
shutdown
!
interface FastEthernet5/0
no ip address
shutdown
!
interface Serial6/0
ip address 30.0.0.1 255.0.0.0
clock rate 2000000
!
interface Serial7/0
ip address 23.156.98.200 255.0.0.0
!
interface Serial8/0
ip address 62.182.120.45 255.0.0.0
clock rate 2000000
!
interface FastEthernet9/0
no ip address
duplex auto
speed auto
!
router rip
network 23.0.0.0
network 30.0.0.0
network 102.0.0.0
network 185.214.0.0
network 192.168.1.0
network 192.168.4.0
network 192.168.100.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 30.0.0.2
!
ip flow-export version 9
!
logging trap debugging
logging 192.168.1.4
line con 0
!
line aux 0
!
line vty 0 4
login
!
end
```

Маршрутизатор R_K1:

```
Current configuration : 1431 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
no ip cef
no ipv6 cef
!
license udi pid CISCO2901/K9 sn FTX15247QQ5-
!
spanning-tree mode pvst
!
interface Tunnel1
ip address 172.16.1.1 255.255.255.252
mtu 1476
tunnel source Serial0/1/1
tunnel destination 50.0.0.1
!
!
interface GigabitEthernet0/0
ip address 192.168.1.1 255.255.255.0
ip helper-address 192.168.1.2
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 192.168.100.2 255.255.255.0
duplex auto
speed auto
!
interface Serial0/0/0
ip address 10.0.0.2 255.0.0.0
!
interface Serial0/0/1
ip address 20.0.0.2 255.0.0.0
!
interface Serial0/1/0
ip address 30.0.0.2 255.0.0.0
!
interface Serial0/1/1
ip address 50.0.0.2 255.255.255.252
!
interface GigabitEthernet0/2/0
no ip address
!
interface GigabitEthernet0/3/0
no ip address
!
interface Vlan1
no ip address
!
router rip
network 10.0.0.0
network 20.0.0.0
network 30.0.0.0
network 192.168.1.0
network 192.168.100.0
network 203.0.114.0
!
ip classless
ip route 203.0.114.0 255.255.255.0 192.168.100.1
ip route 203.0.115.0 255.255.255.0 192.168.100.1
ip route 192.168.6.0 255.255.255.0 172.16.1.2
!
ip flow-export version 9
!
logging trap debugging
logging 192.168.1.4
line con 0
!
line aux 0
!
line vty 0 4
login
!
end
```

Міжмережевий екран FW:

```
ASA Version 8.4(2)
!
hostname ciscoasa
enable password 4IncP7vTjpaba2aF encrypted
names
!
interface Ethernet0/0
switchport access vlan 2
!
interface Ethernet0/1
interface Ethernet0/2
interface Ethernet0/3
interface Ethernet0/4
interface Ethernet0/5
interface Ethernet0/6
interface Ethernet0/7
!
interface Vlan1
nameif inside
security-level 70
ip address 192.168.100.1 255.255.255.0
!
interface Vlan2
nameif outside
security-level 0
ip address 203.0.113.1 255.255.255.252
!
object network LOCAL_NAT
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic interface
!
route outside 0.0.0.0 0.0.0.0 203.0.113.2 1
route inside 192.168.2.0 255.255.255.0
192.168.100.2 1
route inside 192.168.3.0 255.255.255.0
192.168.100.2 1
route inside 192.168.4.0 255.255.255.0
192.168.100.2 1
route inside 192.168.10.0 255.255.255.0
192.168.100.2 1
route inside 192.168.20.0 255.255.255.0
192.168.100.2 1
route inside 192.168.30.0 255.255.255.0
192.168.100.2 1
route inside 192.168.40.0 255.255.255.0
192.168.100.2 1
route inside 192.168.6.0 255.255.255.0
192.168.100.2 1
route inside 10.0.0.0 255.0.0.0 192.168.100.2 1
route inside 20.0.0.0 255.0.0.0 192.168.100.2 1
route inside 30.0.0.0 255.0.0.0 192.168.100.2 1
route inside 23.0.0.0 255.0.0.0 192.168.100.2 1
!
access-list OUTSIDE_IN extended permit icmp any
any
access-list OUTSIDE_IN extended permit tcp any
any
access-list INSIDE_OUT extended deny ip
192.168.4.0 255.255.255.0 host 203.0.115.2
access-list INSIDE_OUT extended deny icmp
192.168.4.0 255.255.255.0 host 203.0.115.2
access-list INSIDE_OUT extended deny tcp
192.168.4.0 255.255.255.0 host 203.0.115.2
access-list INSIDE_OUT extended permit ip any
host 203.0.114.2
access-list INSIDE_OUT extended permit tcp any
host 203.0.114.2
access-list INSIDE_OUT extended permit icmp any
host 203.0.114.2
access-list INSIDE_OUT extended permit ip any
host 203.0.115.2
access-list INSIDE_OUT extended permit tcp any
host 203.0.115.2
access-list INSIDE_OUT extended permit icmp any
host 203.0.115.2
!
!
access-group OUTSIDE_IN in interface outside
access-group INSIDE_OUT in interface inside
aaa authentication ssh console LOCAL
!
username admin password 4IncP7vTjpaba2aF
encrypted
!
class-map inspection_default
match default-inspection-traffic
!
policy-map global_policy
class inspection_default
inspect http
inspect icmp
!
service-policy global_policy global
!
telnet timeout 5
ssh 192.168.2.0 255.255.255.0 inside
ssh 192.168.100.0 255.255.255.0 inside
ssh 192.168.3.0 255.255.255.0 inside
ssh 192.168.4.0 255.255.255.0 inside
ssh timeout 5
!
dhcpd auto_config outside
```

На рисунку А.1 зображена конфігурація комутатора Switch_K2.

```
interface FastEthernet0/1
 switchport mode trunk
!
interface FastEthernet1/1
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet2/1
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet3/1
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet4/1
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet5/1
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet6/1
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet7/1
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet8/1
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet9/1
 switchport mode access
!
interface Vlan1
 no ip address
 shutdown
```

Рисунок А.1 – Конфігурація комутатора Switch_K2 для VLAN