Вінницький національний технічний університет
Факультет інтелектуальних інформаційних технологій та автоматизації
Кафедра комп'ютерних систем управління

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

Створення імітаційної моделі мережі Ethernet з логічною сегментацією на основі VLAN у програмному середовищі Cisco Packet Tracer

Виконав: студент 2 курсу, групи _____ спеціальності 151 – Автоматизація та комп'ютерно-інтегровані технології

Павло СТРЕМБІЦЬКИЙ
Ім'я ПРІЗВИЩЕ

12 грудня 2022

Керівник: кандидат технічних наук, доцент кафедри АІІТ _____
степінь, звання, посада

Ольга СОФИНА
Ім'я ПРІЗВИЩЕ

«12» грудня 2022 р.

Опонент: к.т.н. доц. Козачко О.М.
степінь, звання, посада

Ім'я ПРІЗВИЩЕ

«13» грудня 2022 р.

Допущено до захисту
Зав. кафедри КСУ
В'ячеслав КОВТУН

«14» 12 2022

Вінниця ВНТУ – 2022 рік

Вінницький національний технічний університет
Факультет інтелектуальних інформаційних технологій та автоматизації
Кафедра комп'ютерних систем управління
Рівень вищої освіти другий (магістерський)
Галузь знань – 15 – Автоматизація та приладобудування
Спеціальність – 151 – Автоматизація та комп'ютерно-інтегровані технології
Освітньо - професійна програма – Інформаційні системи і Інтернет речей

ЗАТВЕРДЖУЮ
Завідувач кафедри КСУ

В'ячеслав КОВТУН

"03" жовтня 2022 року

ЗАВДАННЯ
НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Стрембіцькому Павлу Павловичу
(прізвище, ім'я, по батькові)

1. Тема роботи. Створення імітаційної моделі мережі ethernet з логічною сегментацією на основі vlan у програмному середовищі cisco packet tracer керівник роботи кандидат технічних наук, доцент кафедри АІІТ, Софина Ольга Юріївна
затверджені наказом ВНТУ від "14" вересня 2022 року №203
2. Термін подання студентом роботи "12" грудня 2022 року
3. Вихідні дані до роботи: Середовище розробки Cisco Packet Tracer, розробити комп'ютерну мережу, розрахувати адресний простір для мереж LAN1 LAN3, створити конфігураційні файли для всіх мережевих пристроїв, виконати моделювання мережі
4. Зміст текстової частини: Вступ; 1 Аналіз проблеми та постановка задач, 2 Принципи логічної сегментації мережі Ethernet на основі VLAN, 3 Розроблення схеми мережі Ethernet з логічною сегментацією на основі VLAN, 4 Створення імітаційної моделі мережі Ethernet з логічною сегментацією на основі VLAN у програмному середовищі Cisco Packet Tracer, 5 Проектування та налаштування мережі, Висновки.
5. Перелік ілюстративного матеріалу (з точним зазначенням обов'язкових креслень)

1. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	виконання прийняв
1	Софина О.Ю., к.т.н., доц. кафедри АІІТ	19.09.2022	07.12.22
2	Софина О.Ю., к.т.н., доц. кафедри АІІТ	19.09.2022	07.12.22
3	Софина О.Ю., к.т.н., доц. кафедри АІІТ	19.09.2022	07.12.22
4	Софина О.Ю., к.т.н., доц. кафедри АІІТ	19.09.2022	07.12.22
5	Софина О.Ю., к.т.н., доц. кафедри АІІТ	19.09.2022	07.12.22

2. Дата видачі завдання "03" жовтня 2022 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва та зміст етапу	Термін виконання		Примітка
		початок	закінчення	
1	Вступ	05.10.22	09.10.22	
2	Аналіз проблеми та постановка задач	10.10.22	11.10.22	
3	Принципи логічної сегментації мережі Ethernet на основі VLAN	15.10.22	18.10.22	
4	Розроблення схеми мережі Ethernet з логічною сегментацією на основі VLAN	10.11.22	20.11.22	
5	Створення імітаційної моделі мережі Ethernet з логічною сегментацією на основі VLAN у програмному середовищі Cisco Packet Tracer	22.11.22	25.11.22	
6	Проектування та налаштування мережі	30.11.22	30.11.22	
7	Висновки	02.12.22	02.12.22	
8	Попередній захист	06.12.22	06.12.22	

Студент **Павло СТРЕМБІЦЬКИЙ**

(підпис) (*Ім'я ПРІЗВИЩЕ*)

Керівник роботи **Ольга СОФИНА**

(підпис) (*Ім'я ПРІЗВИЩЕ*)

АНОТАЦІЯ

УДК 621.374.415

Стрембіцький П.П. Створення імітаційної моделі мережі Ethernet з логічною сегментацією на основі VLAN у програмному середовищі Cisco Packet Tracer. Магістерська кваліфікаційна робота зі спеціальності 151 – Автоматизація та комп’ютерно-інтегровані технології, освітня програма – Інформаційні системи і Інтернет речей. Вінниця: ВНТУ, 2022.

У магістерській кваліфікаційній роботі спроектовано захищену комп'ютерну мережу для підприємства з декількома філіями. Проект змодельовано в симуляторі Cisco Packet Tracer, який є поширеним середовищем проектування віртуальних мереж.

Розроблена комп'ютерна мережа складається з трьох локальних обчислюваних мереж (LAN). Всі три мережі з’єднанні між собою за допомогою послідовних з’єднань через один «центральний» роутер, на якому налаштована статична маршрутизація цих мереж.

Ключові слова: комп’ютерна мережа, VLAN, імітаційна модель, cisco packet tracer.

ANNOTATION

Creating a simulation model of Ethernet network with logical segmentation based on VLAN in the Cisco Packet Tracer software environment. Master's qualification work in the specialty 151 – Automation and computer-integrated technologies, educational program - Information systems and the Internet of things. Vinnytsia: VNTU, 2022.

In the master's qualification work, a protected computer network was designed for an enterprise with several branches. The project is simulated in the Cisco Packet Tracer simulator, which is a common virtual network design environment.

The developed computer network consists of three local computer networks (LAN). All three networks are interconnected using serial connections through one "central" router, on which static routing of these networks is configured.

Keywords: computer network, VLAN, simulation model, cisco packet tracer.

ВІДГУК
керівника магістерської кваліфікаційної роботи

студента (-ки) Стрембіцького Павла Павловича, групи ЗАКІТ-21м
(прізвище, ім'я, по батькові)

на тему Створення імітаційної моделі мережі Ethernet з логічною сегментацією на основі VLAN у програмному середовищі Cisco Packet Tracer.

Актуальність роботи в контексті спеціальності 151 «Автоматизація та комп'ютерно-інтегровані технології» доведена результатами інформаційного пошуку та аналізу літературних джерел. Додатковим підтвердженням актуальності роботи слугують опубліковані тези на Науково-практичній конференції «проблеми комп'ютерної інженерії» Державного Університету Телекомунікацій, кафедри комп'ютерної інженерії.

За змістом робота є закінченою та містить достатньо посилань на літературу. Викладення матеріалу є послідовним та логічно правильним. Наведені у роботі конфігурації, коди та висновки мають достатнє обґрунтування та детальне пояснення. Мова викладення роботи є технічно грамотною, зрозумілою та не перенасиченою спеціальними термінами. Дипломник показав хороший рівень спеціальних знань навичок. Студент проявив відповідальність, високу зацікавленість в темі розробки та надав гарний результат.

Результати представлені в роботі отримані студентом самостійно. Матеріалу роботи властивий високий ступінь оригінальності, що доведено результатами перевірники на наявність запозичень.

Недоліки: Дипломна робота могла би містити більше методів підвищення безпеки комп'ютерної мережі. Але ці побажання не впливають на загальну якість виконаної роботи. Загалом магістерська кваліфікаційна робота **відповідає** спеціальності 151 «Автоматизація та комп'ютерно-інтегровані технології», заслуговує на оцінку відмінно, а її автор **заслуговує** присудження кваліфікації: ступінь вищої освіти магістр, спеціальність «Автоматизація та комп'ютерно-інтегровані технології», освітня програма «Інтелектуальні системи і Інтернет речей».

Керівник магістерської кваліфікаційної роботи

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ * ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ * «ФАКУЛЬТЕТ ІНТЕЛЕКТУАЛЬНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА АВТОМАТИЗАЦІЇ»

к.т.н., доц. каф. АІІТ — (підпис) — Софина О.Ю.
(посада, науковий ступінь, вчене звання) — (підпис) — *Ім'я ПРІЗВИЩЕ*)

ВІДГУК
опонента на магістерську кваліфікаційну роботу

студента (-ки) Стрембіцького Павла Павловича, групи ЗАКІТ-21м
(прізвище, ім'я, по батькові)

на тему: Створення імітаційної моделі мережі Ethernet з логічною сегментацією на основі VLAN у програмному середовищі Cisco Packet Tracer

Актуальність роботи в контексті спеціальності 151 «Автоматизація та комп'ютерно-інтегровані технології» доведена результатами інформаційного пошуку та аналізу літературних джерел. Додатковим підтвердженням актуальності роботи слугують опубліковані тези на Науково-практичній конференції «проблеми комп'ютерної інженерії» Державного Університету Телекомунікацій, кафедри комп'ютерної інженерії

Перший розділ магістерської кваліфікаційної роботи повністю присвячений огляду літературних та інформаційних джерел за обраною темою. Проаналізовано не менш ніж три симулятора для проектування мережі.

Прийняті рішення обґрунтовані результатами огляду літератури, результатами проектування та створено імітаційну модель. Результати її тестування доводять правильність прийнятих рішень.

Експериментальні дослідження продумані і повні. Тести показують як працюють різні протоколи маршрутизації, та те як мережа, що складається з 3 віртуальних підмереж (VLAN), можуть «спілкуватись» між собою.

Вміст графічної частина повною мірою репрезентує всі отримані в магістерській кваліфікаційній роботі результати. Якість рисунків в графічній частині прийнятна.

Недоліки: Серйозних недоліків робота не містить. Присутні незначні неточності, орфографічні та стилістичні помилки, які не впливають на суть роботи.

Загалом магістерська кваліфікаційна робота відповідає спеціальності 151 «Автоматизація та комп'ютерно-інтегровані технології», заслуговує на оцінку відмінно, а її автор заслуговує присудження кваліфікації: ступінь вищої освіти магістр, спеціальність «Автоматизація та комп'ютерно-інтегровані технології», освітня програма «Інтелектуальні системи і Інтернет речей».

Опонент на магістерську кваліфікаційну роботу

к.т.н., доц. каф. САІТ — Козачко О.М.

ЗМІСТ

ЗМІСТ 6
ВСТУП 8
1 АНАЛІЗ ПРОБЛЕМИ ТА ПОСТАНОВКА ДОСЛІДНИЦЬКИХ ЗАДАЧ 10
1.1 Передумови створення захищеної комп'ютерної мережі 10
1.2 Мережеві атаки і методики захисту від них 13
1.2.1 Mailbombing 14
1.2.2 Застосування спеціалізованих додатків 15
1.2.3 Переповнення буфера 16
1.3 Аналіз існуючих програм та вибір актуального варіанту 16
1.3.1 Симулятор GNS3 17
1.3.2 Симулятор Verax SNMP Agent Simulator 18
1.3.3 Емулятор Dynamips 20
1.3.4 Опис симулятора Cisco Packet Tracer 21
2 ПРИНЦИПИ ЛОГІЧНОЇ СЕГМЕНТАЦІЇ МЕРЕЖІ ETHERNET НА ОСНОВІ ВІРТУАЛЬНИХ ЛОКАЛЬНИХ МЕРЕЖ VLAN 23
2.1 Основні властивості віртуальних локальних мереж 23
2.2 Віртуальні локальні мережі на основі портів 25
2.3 Віртуальні локальні мережі на основі стандарта IEEE 802.1q 28
3 РОЗРОБЛЕННЯ СХЕМИ МЕРЕЖІ ETHERNET З ЛОГІЧНОЮ СЕГМЕНТАЦІЄЮ НА ОСНОВІ VLAN 32
4 СТВОРЕННЯ ІМІТАЦІЙНОЇ МОДЕЛІ МЕРЕЖІ ETHERNET З ЛОГІЧНОЮ СЕГМЕНТАЦІЄЮ НА ОСНОВІ VLAN У ПРОГРАМНОМУ СЕРЕДОВИЩІ CISCO PACKET TRACER 35
5 ПРОЕКТУВАННЯ ТА НАЛАШТУВАННЯ ПРАЦЕЗДАТНОСТІ МЕРЕЖІ 40
5.1 Проектування мережі центрального офісу (LAN1) 40
5.1.1 Хід розрахунку 40
5.2 Проектування мережі віддаленого офісу (LAN2) 48
5.2.1 Хід розрахунку 51
5.3 Проектування мережі диспетчерського центру (LAN3) 53
5.3.1 Хід налаштування 54
5.4 З'єднання частин корпоративної мережі 61

5.4.1 Хід налаштування 61
5.5 Встановлення захисту від вільного доступу на роутері 68
ВИСНОВКИ 74
ПЕРЕЛІК ПОСИЛАНЬ 76
ДОДАТКИ 80
Додаток А – Технічне завдання 81
Додаток Б – Ілюстративна частина 85
Додаток В – Налаштування Router7 92
Додаток Г – Налаштування Router8 94
Додаток Ґ – Налаштування Router4 95
Додаток Д – Налаштування Router5 97

ВСТУП

Актуальність теми . У сучасному світі активно розвиваються мережні й інформаційні технології. В даний час неможливо знайти підприємство, яке функціонує без впровадженої мережі передач даних. Подібна мережа дозволяє виконувати величезну кількість завдань, максимально спрощуючи різні дії, такі як:

– обмін інформацією;

– робота з документами;

– доступ до всіляких ресурсів;

– управління додатками;

– зберігання інформації.

Інформація є цінним ресурсом, тому зловмисники нерідко намагаються отримати доступ до системи підприємства. Вони можуть завдати шкоди, що складається в крадіжці персональних даних і даних компанії, і зараженні системи з повним знищенням ресурсів. Засоби масової інформації дуже часто повідомляють про кібератаки на різні підприємства. Виходить, щоб цього уникнути, потрібно дуже уважно підійти до питання модернізації мережі, особливо з боку безпеки. Все це вказує на високу актуальність даної дипломної роботи.

Актуальність і значимість проблеми забезпечення інформаційної безпеки обумовлена наступними факторами:

- застосовувані засоби забезпечення інформаційної безпеки не відповідають високому рівню розвитку інформаційних технологій;
- повсюдне використання Інтернет тягне до появи загроз з боку віддалених користувачів;
- недосконаліть програм і мережевих технологій з точки зору інформаційної безпеки.

Основний науково-технічний результат. В даній роботі розроблено та спроектована імітаційна модель мережі підприємства на базі обладнання Cisco Systems з використанням динамічного соціального середовища Packet Tracer, що дозволило вирішити проблеми інформаційної безпеки та мережевого устаткування та дослідити сегментацію мережі на основі VLAN.

Об'єкт дослідження – методи побудови захищеної корпоративної мережі.

Метою дослідження є розробка проекту комп'ютерної мережі підприємства з використанням мережевого симулятора Cisco Packet Tracer.

Розроблена мережа повинна задовольняти потреби підприємства, який складається з декількох віддалених відділень. А саме, забезпечити передачу даних між її відділеннями з дотриманням високих вимог щодо забезпечення конфіденційності та захищеності обмінюваних даних. Також треба забезпечити можливість ефективного масштабування розміру мережі як в сторону збільшення кількості мережевого обладнання, так і в сторону його зменшення.

Предметом дослідження є побудова корпоративної мережі_ з логічною сегментацією на основі VLAN у програмному середовищі Cisco Packet Tracer.

Методи дослідження, використані в роботі: теоретичний аналіз, системний підхід, експеримент та порівняння.

Практична цінність дослідження полягає у розробці оптимальної, з точки зору ефективності, зручності, швидкодії та якості моделі мережі, яка у перспективі може бути поширена серед широкої маси споживачів.

Апробація. Робота та окремі її аспекти, одержані узагальнення та висновки були оприлюдненні на науково-практичній конференції «проблеми комп'ютерної інженерії» Державного Університету Телекомунікацій, кафедра комп'ютерної інженерії (2022) [2].

1 АНАЛІЗ ПРОБЛЕМИ ТА ПОСТАНОВКА ДОСЛІДНИЦЬКИХ ЗАДАЧ

1.1 Передумови створення захищеної комп’ютерної мережі

Комп'ютерна мережа – система, що забезпечує обмін даними між обчислювальними пристроями (комп'ютери, сервери, маршрутизатори та інше обладнання). Для передачі інформації можуть бути використані різні середовища.

В даний час використання комп'ютерних мереж є невід'ємною частиною нашого життя, область їх застосування охоплює всі сфери людської діяльності.

Комп'ютерна мережа – це сукупність комп'ютерів і різних пристроїв, що забезпечують інформаційний обмін між комп'ютерами в мережі без використання будь-яких проміжних носіїв інформації. Розвиток комп'ютерних мереж пов'язано як з розвитком власне ЕОМ, що входять до складу мережі, так і з розвитком засобів телекомунікацій [2]. Роботи зі створення комп'ютерних мереж почалися ще в 60-х роках XX століття. Прообразом комп'ютерних мереж з'явилися системи телеобробки даних, побудовані на базі великих (а пізніше і міні ЕОМ). Як засоби передачі даних використовувалася існуюча телефонна мережа. Загрози для IT-інфраструктури з кожним роком стають все складніше, для захисту від них потрібно застосовувати різні системи і засоби. П'ятнадцять років тому для захисту комп'ютера досить було встановити на ньому антивірус. З розвитком мережевих технологій виникла потреба в міжмережевих екранах, потім в системах запобігання вторгнень. Зараз для захисту персональних даних, крім антивіруса, брандмауера і засобів запобігання вторгнень, необхідно також використовувати засоби контролю цілісності і сканер вразливостей. Коли мережа піддається вторгненню, DoS-атаці або вірусної епідемії, під загрозою опиняється діяльність всієї організації. Це відбувається тому, що збільшується небезпека для операційних ресурсів, призначених для користувача даних,

власних коштів і технологій. Інтелектуальна власність може бути вкрадена і неправомірно використано третьою стороною.

Захист локальних мереж підприємств з кожним роком стає все більш складним завданням і сьогодні є одним з основних факторів, з якими стикається бізнес. Нові загрози з'являються на регулярній основі, і жодна організація від них не застрахована. Варто зазначити, що кожен раз при появі нового виду небезпечних загроз змінюється саме поняття «безпечна мережа».

Створення захищеної комп'ютерної мережі – це найкращий спосіб організації єдиного інформаційного середовища підприємства. Завдяки їй користувачі отримають доступ до загальних ресурсів, зможуть спільно використовувати принтери та інше мережеве обладнання. Правильно налаштувавши мережу, адміністратор може забезпечити належний рівень секретності і запобігти витоку даних, що становлять комерційну таємницю [3].

Актуальність і значимість проблеми забезпечення інформаційної безпеки обумовлена наступними факторами:

– застосовувані засоби забезпечення інформаційної безпеки не відповідають високому рівню розвитку інформаційних технологій;

– повсюдне використання інтернету тягне до появи загроз з боку віддалених користувачів;

– постійне збільшення кількості персональних комп'ютерів, захист яких не відповідає вимогам безпеки;

– зростання обсягів інформації, що обробляється і зберігається з використанням інформаційних технологій;

– недосконаліть програм і мережевих технологій з точки зору інформаційної безпеки [5].

Мета концепції захищеної корпоративної мережі – закрити трафік корпоративної мережі засобами захисту інформації мережевого рівня і організувати фільтрацію інформації в точках з'єднання з відкритими мережами.

В якості фільтрації інформації на інтерфейсах з відкритими мережами застосовуються традиційні рішення: міжмережевий екран (firewall) або сервіси захисту типу proxy.

Важливим елементом захисту від несанкціонованого проникнення в корпоративну мережу з відкритою є послідовне (каскадне) включення декількох фільтрів-ешелонів захисту. Як правило, між відкритою і корпоративною мережею встановлюється зона контрольованого доступу. Весь процес організації захищеної комп'ютерної мережі можна розділити на наступні етапи:

1) Розробка мережі. На цьому етапі фахівці обстежують територію підприємства, вислуховують побажання замовника по функціоналу, складають план, ТЗ і готують обладнання, необхідне для її установки.

2) Монтаж. На цьому етапі прокладаються кабелі, проводиться монтаж обладнання та налаштування необхідного програмного забезпечення.

3) Тестування. Фахівці перевіряють роботу, відповідність встановленої мережі загальноприйнятим стандартам якості.

4) Обслуговування. Цей етап включає модернізацію і при необхідності усунення неполадок [15].

Створена мережа підприємства повинна задовольняти таким основним вимогам:

– Бути легко керованою.

– Бути захищеною від хакерських атак. Захист корпоративної мережі

передбачає установку спеціального програмного забезпечення – файрвола.

– Бути адаптованою до основних типів мережевих пристроїв і кабелів.

Завдяки цьому мережа в будь-який момент можна модернізувати.

1.2 Мережеві атаки і методики захисту від них

Як приклади найбільш поширених мережевих атак можна навести такі види впливу:

- Застосування нестандартних протоколів. Тип протоколу пакета даних визначається по вмісту в ньому спеціальному полю. При зміні зловмисниками значення в цьому полі здійснюється передача даних, яку система не може визначити.
- Ping Flooding. Така атака може бути реалізована тільки за умови доступу до високошвидкісного інтернету. Вона передбачає застосування флудинг замість стандартної команди контролю пинга. В результаті створюється надмірне навантаження на мережу, що призводить до порушень в її роботі.
- Фрагментація даних. При передачі по IP пакет даних ділиться на частини, а на стороні одержувача – збирається. У разі атаки виконується відправка значного числа подібних фрагментів із засміченням буфера обміну і порушень роботи мережі.

У зв'язку з швидким розвитком інформаційних технологій і технічних засобів статичні механізми захисту від мережевих погроз часто виявляються неефективними. Забезпечити ефективний захист інформації дозволяють динамічні методи, здатні оперативно виявляти і усувати загрози. Робота динамічних технологій будується на оцінки рівня підозрілості дій в мережі з боку певної служби або процесу [6]. Алгоритм дії щодо усунення атак спрямований на ідентифікацію підозрілих об'єктів. Після цього система реагує необхідним чином на діяльність таких об'єктів, яка може бути націлена на ресурси мережі або комп'ютерного обладнання. Для захисту мереж від зовнішніх загроз можуть застосовуватися наступні основні методи і технології:

- застосування портів високої надійності, шифрування даних;

- використання ефективних антивірусів і сканерів;
- застосування програмного або апаратного мережевого екрану;
- установка блокувальників руткітів і сніфферов.

На сьогоднішній день відомі наступні види мережевих атак [7]:

- mailbombing;
- застосування спеціалізованих додатків;
- переповнення буфера;
- мережева розвідка (збір відомостей за допомогою додатків, які перебувають у вільному доступі);
- IP-спуфинг (хакер видає себе за законного користувача);
- DDOS-атака (шляхом перевантаження обслуговування звичайних користувачів унеможливлюється);
- Man-in-the-Middle (впровадження з метою отримання пакетів, переданих всередині системи);
- XSS-атака (ПК клієнта піддаються атаці через уразливості на сервері);
- фішинг (обман жертви шляхом відправки повідомлень з нібито знайомого адреси).

Різноманітність видів мережевих атак, яким можуть піддаватися корпоративні і приватні мережі, вимагає вироблення ефективних заходів щодо їх захисту. Такі заходи повинні розроблятися і застосовуватися завчасно. Ефективний захист від загроз допоможе зберегти недоторканними конфіденційні дані і забезпечити стабільну роботу мережі. Завдяки цьому багато разів окупаються витрати, понесені на впровадження такого захисту.

1.2.1 Mailbombing

Суть дії в тому, що e-mail користувача буквально завалюється листами. Для цього використовується масова розсилка. Мета – відмова роботи

поштової скриньки або всього поштового сервера. Для проведення цієї атаки не потрібні особливі навички. Досить знати електронну адресу потенційної жертви і адреса сервера, з якого можна відправляти повідомлення анонімно.

Перше правило захисту, до якого може вдатися кожен – не давати адресу своєї поштової адреси сумнівним джерелам. Спеціалісти задають певні настройки на web-сайті провайдера. Ліміт кількості листів, що надходять з певного IP, обмежений. Коли прикладна програма «бачить», що число повідомлень перевалило межа норми, листи «на автоматі» відправляються в кошик. Але ніщо не заважає злочинцеві проводити розсилку з різних адрес [14].

1.2.2 Застосування спеціалізованих додатків

Використання особливих додатків – найпоширеніший спосіб виведення серверів з ладу. У хід йдуть віруси, трояни, руткіти, сніфери. Вірус – шкідливий софт, заточений на виконання певної функції. Впроваджується в інші програми (легальні в тому числі) на ПК жертви. Після вбудовування приступає до здійснення прописаної «місії». Наприклад, проводить шифровку файлів, блокує завантаження комп'ютерної платформи, прописавши себе в BIOS [6].

«Троянський кінь» – це вже не програмна вставка, а повноцінне шкідливий додаток, яке маскується під нешкідливе. Троян може виглядати, наприклад, як гра. Якщо користувач її запустить, почнеться поширення файлу. Програма розсилає свої копії за всіма електронними адресами, які є на ПК жертви. Найчастіше «троянський кінь» викрадає дані банківських карт, електронних гаманців – словом, прагне отримати доступ до фінансових ресурсів.

Сніффер краде пакети даних, переправлялися ПК на різні сайти. Для цього використовується мережева плата, яка функціонує в режимі promicuous mode. У такому режимі всі пакети, переправлені через карту, відправляються

на обробку додатком. Таким чином, може бути відкритий доступ до конфіденційної інформації – наприклад, списку паролів і логінів від банківських рахунків. Руткіт приховує сліди злочинів зловмисників, маскує шкідливу
діяльність, через що адміністратор не помічає того, що відбувається.

1.2.3 Переповнення буфера

Зловмисник зайнятий пошуком програмних або системних вразливостей. При виявленні таких провокується порушення кордонів оперативної пам'яті, робота додатки завершується в аварійному режимі, виконується будь двійковий код. Захист полягає в тому, щоб виявити і усунути вразливості. Також використовуються нездійсненні буфера, але цей метод здатний запобігти тільки ті атаки, в яких застосовується код

1.3 Аналіз існуючих програм та вибір актуального варіанту

Завдання комп'ютерного моделювання телекомунікаційних систем на сьогоднішній день має досить багато рішень різного роду. Одними з популярних продуктів є OPNET, OMNET ++, NS2, NS3, які є потужним засобом моделювання за рахунок об'єктно-орієнтованих мов програмування як вбудованої мови опису моделей телекомунікаційних систем. Так само існують вузькоспеціалізовані симулятори, створені лише для моделювання певного обладнання.

Як правило, подібне програмне забезпечення випускається виробниками телекомунікаційного обладнання. Компанією Cisco Systems, що є виробником мережевого устаткування, були запропоновано програмне забезпечення для моделювання мереж, яке дозволяє експериментувати з різними топологіями мереж і їх поведінкою всередині: симулятори Packet Tracer, Dynamips, GNS3.

1.3.1 Симулятор GNS3

Graphical Network Simulator (рис. 1.1) – це графічний симулятор мережі, який дозволяє змоделювати віртуальну мережу з маршрутизаторів і віртуальних машин. Незамінний інструмент для навчання та тестів. Працює практично на всіх платформах. Дуже добре підходить для створення стендів на десктопних машинах [8].

Залежно від апаратної платформи, на якій буде використовуватися GNS3, можлива побудова комплексних проектів, що складаються з маршрутизаторів Cisco, Cisco ASA, Juniper, а також серверів під управлінням мережевих операційних систем.

GNS3 має декілька серйозних недоліків:

- сильно вимогливий до CPU і пам'яті. 10 маршрутизаторів вже всерйоз навантажать ПК. Використання процесора можна знизити за допомогою механізму Idle PC. Без цього і 3-4 насилу б, мабуть, пішли.
- дуже слабо підтримує функції L2. Є тільки подобу комутаторів, на яких можна максимум налаштувати Access / Trunk порти і свічовие плати для маршрутизаторів, L2-функціонал яких також дуже обмежений.
- відсутність можливості повноцінної симуляції комутаторів другого рівня Cisco. Цей недолік не буде виправлений в нових версіях, так як його причиною є кардинальна відмінність в апаратній платформі маршрутизаторів і світчей Cisco.
- до складу GNS3 не належать образи IOS / IPS / PIX / ASA / JunOS, так як вони є частиною комерційних продуктів відповідних компаній, і ніякого прямого відношення до проекту GNS3 не мають.

Однією з найцікавіших особливостей GNS3 є можливість з'єднання проектованої топології з реальною мережею. Це дає просто унікальну

можливість перевірити на практиці будь-який проект, без використання реального обладнання.

Використання WireShark дозволяє провести моніторинг трафіку всередині проектованої топології, що дає додаткову інформацію для розуміння досліджуваних технологій. При відсутності можливості отримати доступ до реального обладнання, GNS3 стане практично повноцінної лабораторією.

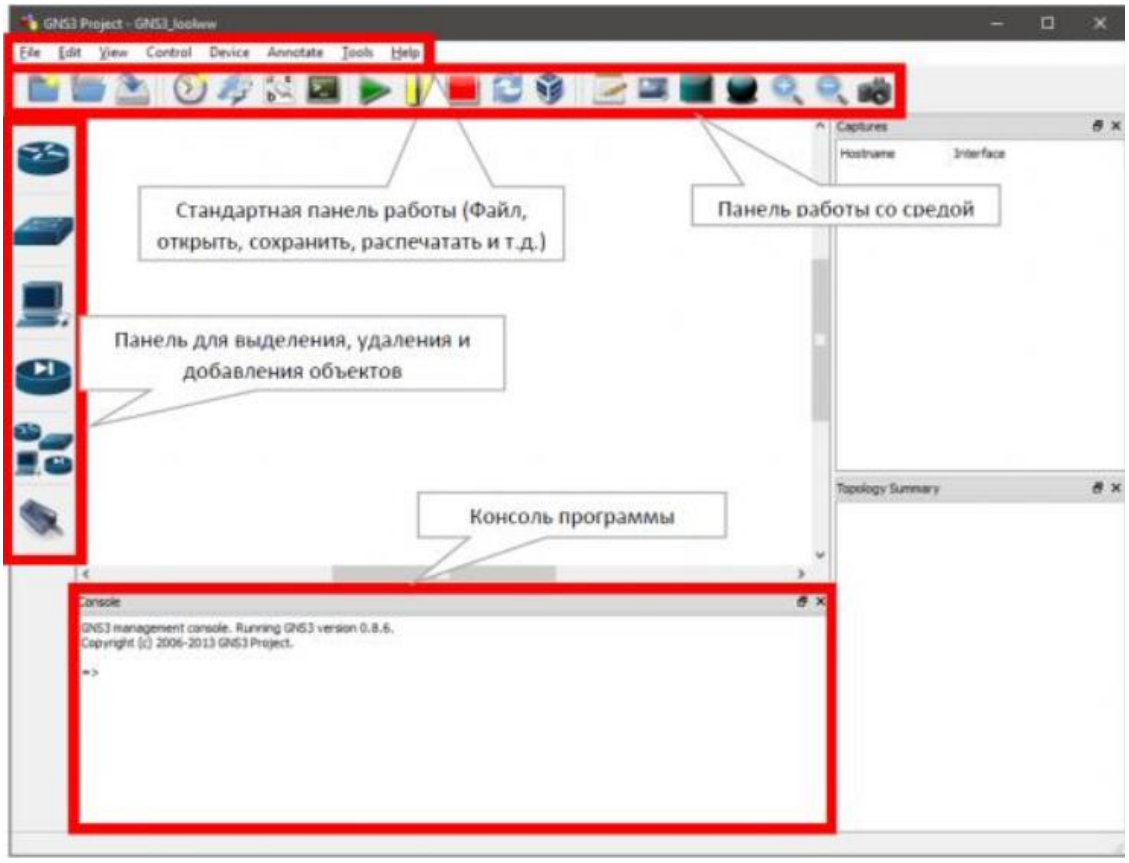


Рисунок 1.1 – Вікно програми GNS3 і його структура

1.3.2 Симулятор Verax SNMP Agent Simulator

Verax SNMP agent simulator дозволяє IT-персоналу створювати віртуальні моделюються мережі пристроїв без придбання будь-якого додаткового обладнання, наприклад, для тестування [9].

Verax SNMP Simulator (рис. 1.2) – це інструмент, який може імітувати кілька агентів SNMPv1 / v2c на одному хості через стандартний порт 161 через

мульти-мережу. Окремі відповіді змодельованого агента можуть бути спочатку отримані з існуючих пристроїв і змінені під час виконання за визначеними користувачем правилами.

Продукт може комбінувати різні поведінки агентів, налаштовувати події і шаблони поведінки або пасток. У варіанті віддаленого управління і в розподілених системах може бути кілька симуляторів, кожен має власне движок і графічну консоль управління. У множині варіанті застосування симуляторів –центральне управління має одна проста консоль.

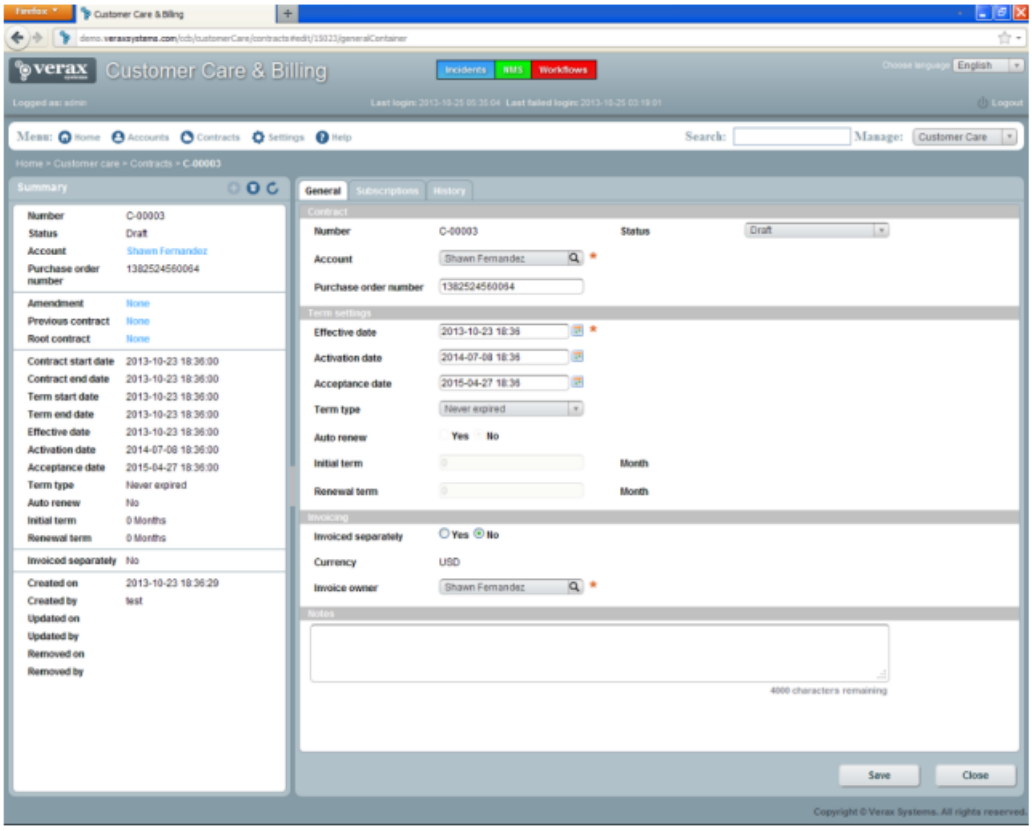


Рисунок 1.2 – Вікно симулятора Verax SNMP Simulator

Особливості:

– Консоль для управління типами пристроїв, адресами і їх екземплярами;
– Підтримка декількох агентів і декількох мереж на одному хості;

- Файли конфігурації відповідей SNMP, сумісні з вихідними даними SNMP, для легкого створення початкових змодельованих відповідей агента з існуючих пристроїв;
- Багатий набір правил для зміни відповідей агента;
- Генерація випадкових MAC-адрес і IP-адрес, включаючи розширені сценарії, такі як рандомізація тільки частини адреси (наприклад, мережева частина IP-адреси є фіксованою, хостової частина змінюється);
- Генерація випадкового цілого числа, лічильника і строкових значень, включаючи сценарії «один раз» або «кожен раз»;
- Підтримка цілочисельних арифметичних операцій (наприклад, яке значення на основі суми двох інших значень);
- Генерація значень на основі тренда (напрямок, діапазон кроків, порогове значення скидання), наприклад, для збільшення лічильників.

1.3.3 Емулятор Dynamips

Dynamips – це комп'ютерна програма емулятора (рис.1.3), яка була написана для емуляції маршрутизаторів Cisco. Він був створений Крістофом Філло, який почав свою роботу в серпні 2005 року. Емулятор маршрутизаторів Cisco, який може працювати в Windows, Linix і Mac OS X. Розповсюджується за ліцензією GNU GPLv2 (чого не можна сказати про образи, які він використовує). Дозволяє запускати віртуальну машину з оригінальним чином ОС від старих маршрутизаторів сімейств 1700, 3725, 7200 і деяких інших. Дозволяє імітувати інтерфейси Ethernet і вимираючі ATM і Serial. При цьому Dynamips не може працювати з прошивками комутаторів, так як їх ОС орієнтовані на використання ASIC, які у великій кількості зустрічаються в комутаторах і дуже складно імітуються на x86 системах.

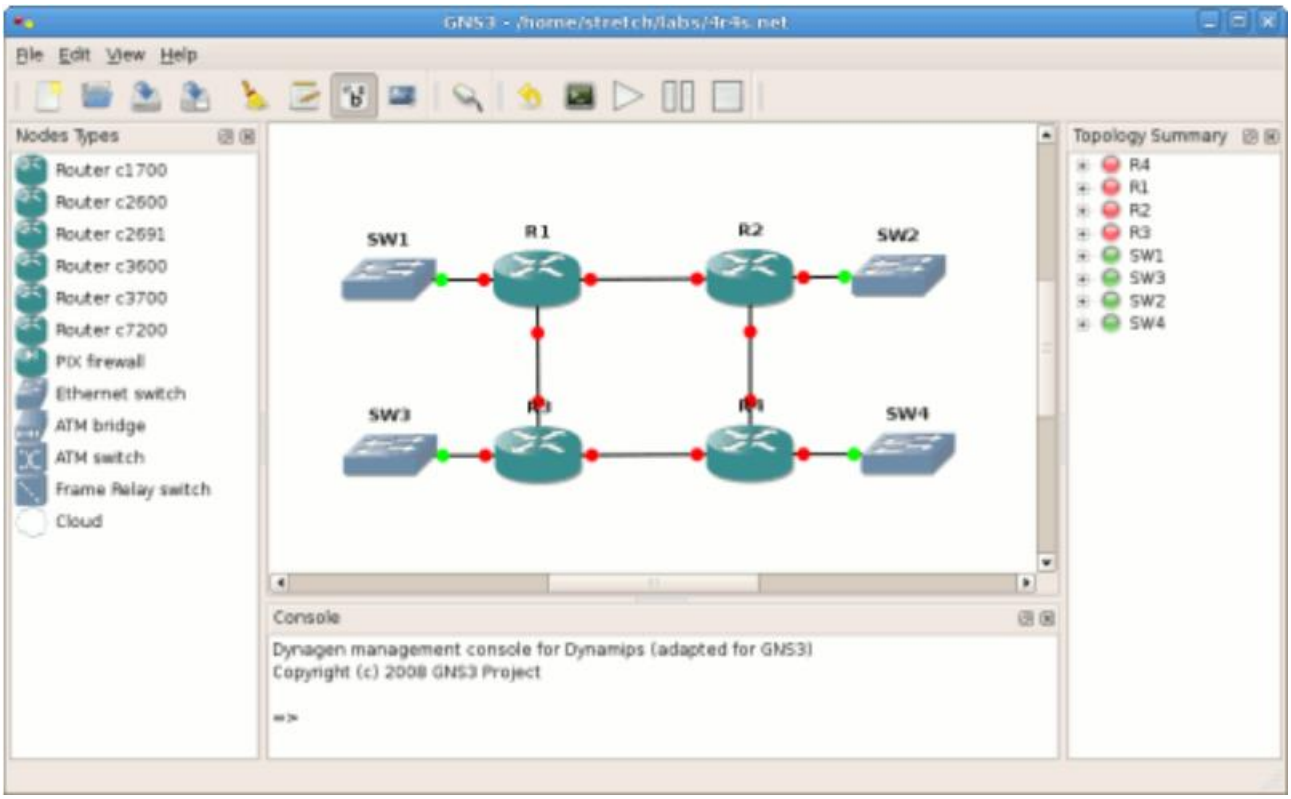


Рисунок 1.3 – Вікно емулятора Dynamips

1.3.4 Опис симулятора Cisco Packet Tracer

Даний програмний продукт розроблений компанією Cisco і рекомендований використовуватися при вивченні телекомунікаційних мереж і мережевого устаткування [1]. На основі програмного продукту Packet Tracer є можливість створювати мережеві топології з широкого безлічі маршрутизаторів і комутаторів компанії Cisco, робочих станцій і мережних з'єднань типу Ethernet, Serial, ISDN, Frame Relay. Функції симулятора можуть бути придатні як для навчання, так і для роботи, настройки мережі ще на етапі планування.

Packet Tracer включає наступні особливості:

– Робочий простір для створення мережі будь-якого розміру і складності;
– Моделювання в режимі реального часу;

– Моделювання в режимі симуляції;
– Графічний інтерфейс для взаємодії з користувачем під час налаштування мережевих пристроїв;
– Зображення мережевого обладнання з підтримкою додавання, видалення, переміщення різних компонентів.

Відмінною особливістю даного симулятора є наявність в ньому режиму симуляції (рис. 1.4). В даному режимі всі пакети, що пересилаються всередині мережі, відображаються графічно. Ця можливість дозволяє студентам наочно продемонструвати, за яким інтерфейсу в дані момент

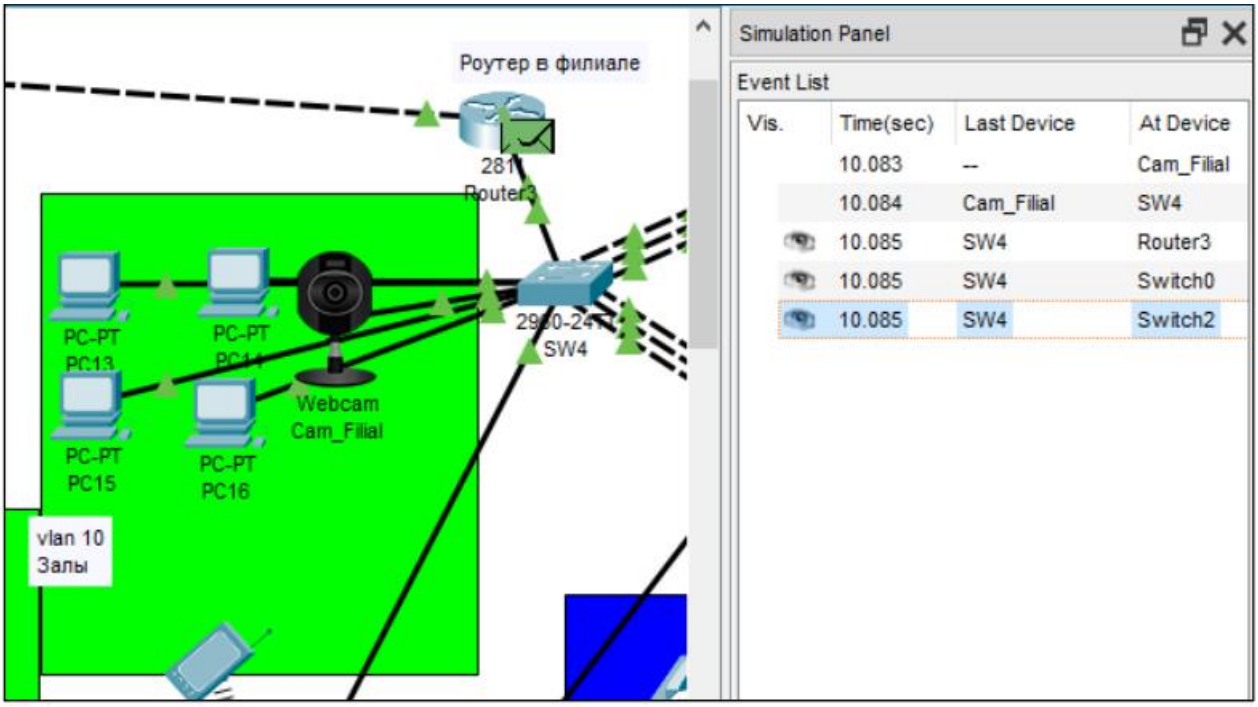


Рисунок 1.4 – Режим симуляції в Packet Tracer

Провівши аналіз симуляторів, для виконання роботи було вибрано Cisco packet tracer тому що даний симулятор дозволяє проектувати свої власні мережі, створюючи і відправляючи різні пакети даних, зберігати і коментувати свою роботу. Також надається можливість вивчати і використовувати такі мережеві пристрої, як комутатори, маршрутизатори, робочі станції, визначати типи зв'язків між ними і з'єднувати їх.

2 ПРИНЦИПИ ЛОГІЧНОЇ СЕГМЕНТАЦІЇ МЕРЕЖІ ETHERNET НА ОСНОВІ ВІРТУАЛЬНИХ ЛОКАЛЬНИХ МЕРЕЖ VLAN

2.1 Основні властивості віртуальних локальних мереж

Віртуальною локальною мережею VLAN (Virtual Local Area Network) будемо називати логічну групу вузлів мережі, кадри яких, у тому числі й широкомовні, на канальному рівні повністю ізольовані від інших вузлів мережі, що не входять до даної групи. Із цього випливає, що передача кадрів між різними VLAN на підставі MAC-адреси неможлива незалежно від типу адреси (одиночної, групової або широкомовної). У той же час усередині VLAN кадри передаються відповідно до технології канального рівня. Тому така логічна сегментація дозволяє логічну структуру мережі Ethernet зробити незалежною від її фізичної структури (рисунок 2.1).

Треба також відмітити, що вузли, які належать до однієї логічної групи можуть бути фізично приєднані до різних комутаторів. Таким чином, застосування VLAN призводить до обмеження розповсюдження широкомовних кадрів, а також кадрів, які розсилає комутатор по всіх своїх портах у випадку відсутності MAC-адреси отримувача кадру в його MAC-таблиці, тільки в межах однієї VLAN. Це в свою чергу дає можливість зменшити частку широкомовних кадрів у мережі й імовірність виникнення широкомовних штормів, що можуть суттєво погіршити характеристики продуктивності мережі.

Застосування VLAN забезпечує можливість гнучкого розділення користувачів на ізольовані групи, тобто кінцеві вузли користувачів (наприклад, персональні комп’ютери) будуть ізольовані один від одного на канальному рівні. Також VLAN дозволяє покращити характеристики безпеки мережі за рахунок обмеження області розповсюдження кадрів другого рівня і реалізації необхідної політики взаємодії користувачів з різних VLAN за

допомогою обладнання комутації третього рівня. Крім того, VLAN надає можливість спрямування за необхідними трактами передачі у випадку, якщо їх декілька, кадрів другого рівня, що дозволяє встановити необхідний розподіл потоків кадрів у певному сегменті мережі.

а) фізична структура мережі (для кожної з VLAN алгоритм прозорого моста виконується окремо); б) логічна структура мережі (один фізичний комутатор відповідає двом окремим умовним комутаторам, які знаходяться у різних VLAN)

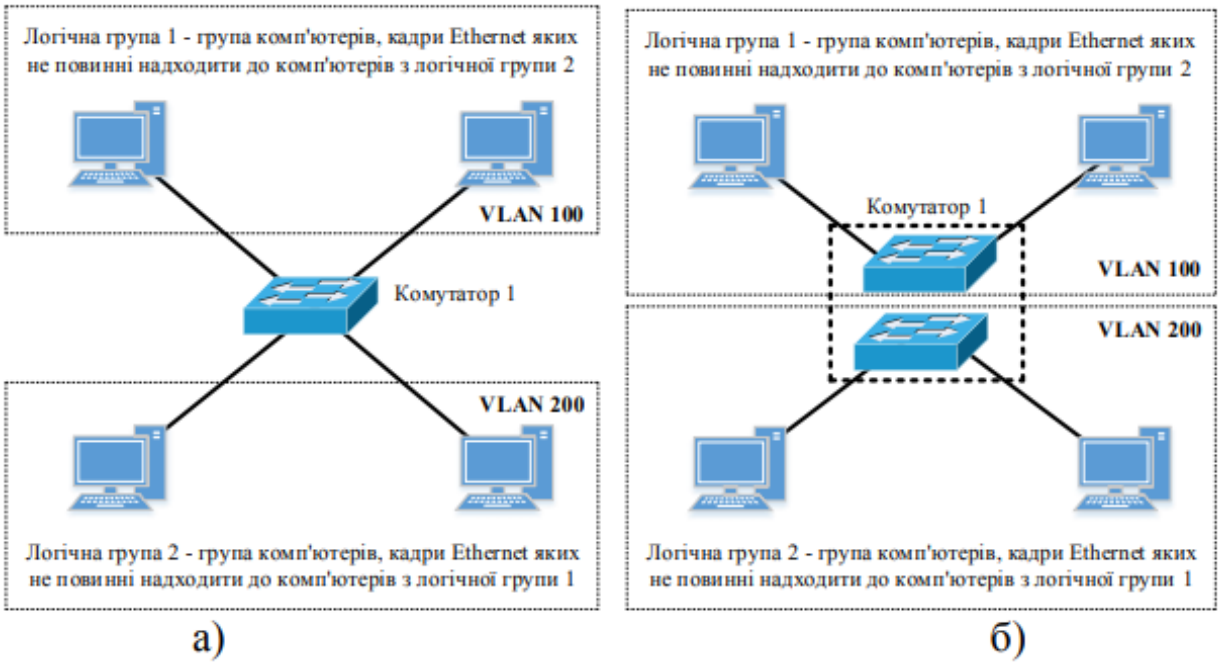


Рисунок 2.1 – Приклад сегментації мережі на основі VLAN

2.2 Віртуальні локальні мережі на основі портів

При використанні VLAN на основі портів кожен порт призначається у певну VLAN. Це означає, що всі користувачі, приєднані до цього порту, будуть членами однієї VLAN. Конфігурація портів статична й може бути змінена тільки вручну (рисунок 2.2).

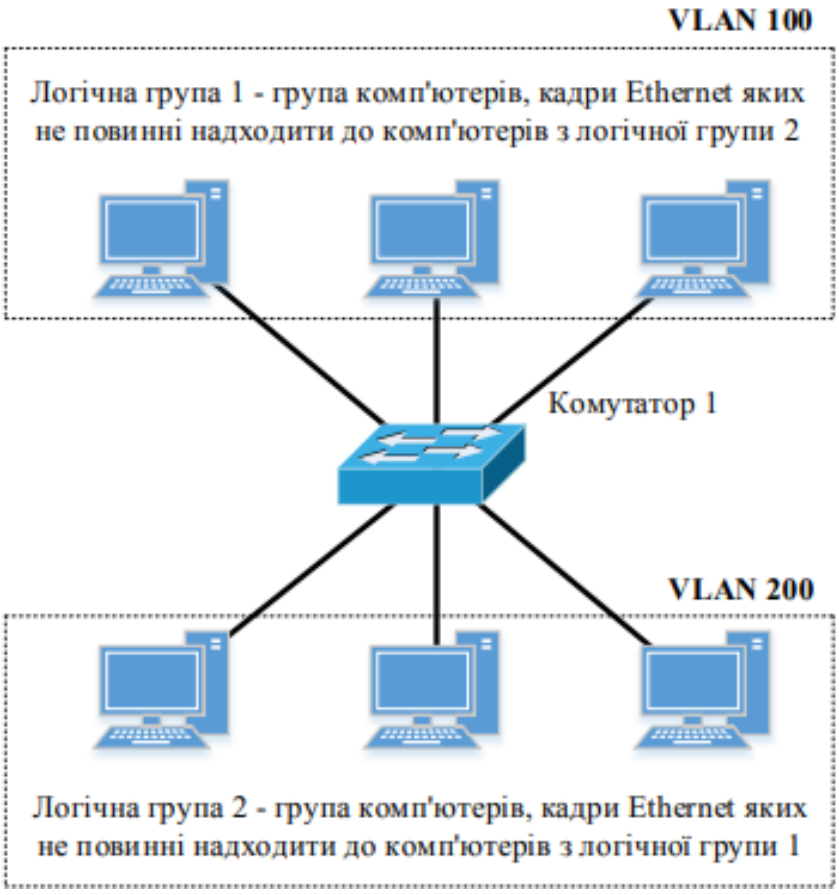


Рисунок 2.2 − VLAN на основі портів

Якщо вузли якої-небудь віртуальної мережі приєднані до різних комутаторів, то для з'єднання комутаторів між собою для кожної VLAN має бути виділено по одному порту (рисунок 2.3).

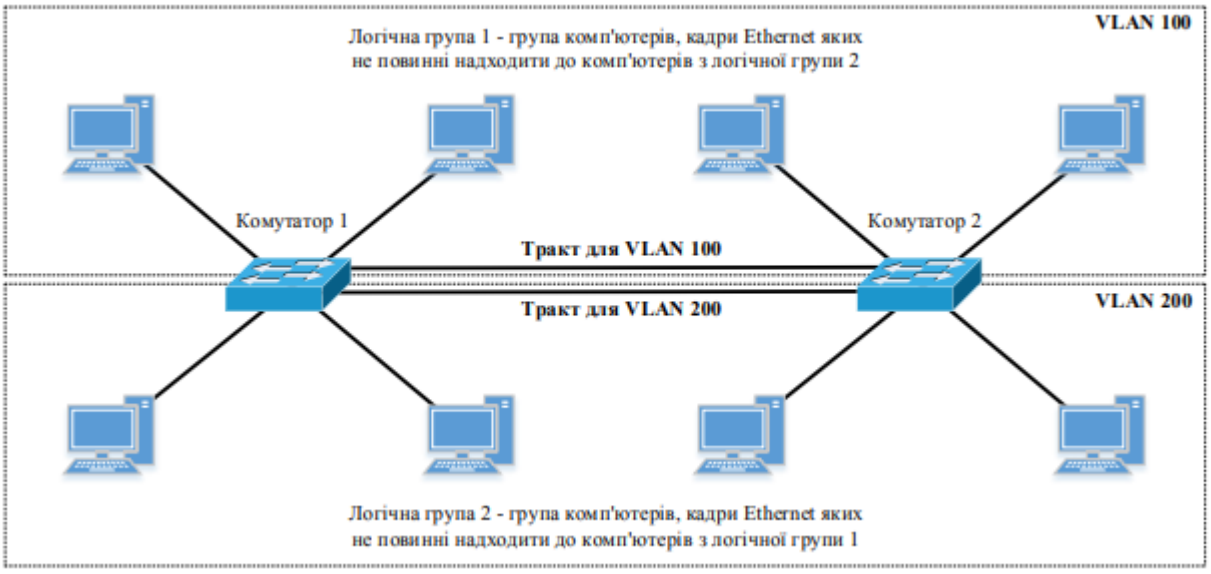


Рисунок 2.3 – VLAN на основі портів у мережі з декількома комутаторами

Передача інформації між користувачами з різних віртуальних мереж можлива тільки через мережевий рівень (на канальному рівні віртуальні мережі повністю незалежні). Для цього один з портів, що належить кожній VLAN, приєднується до окремого порту маршрутизатора, який забезпечує пересилання IP-пакетів між користувачами, що перебувають у різних віртуальних мережах (рисунок 2.4).

При цьому слід зазначити, що IP-адреси користувачів з різних віртуальних мереж повинні знаходиться у різних IP-мережах (підмережах), тобто префікси IP-мереж мають відрізнятися (це необхідно для того, щоб порти маршрутизатора перебували в різних IP-мережах).

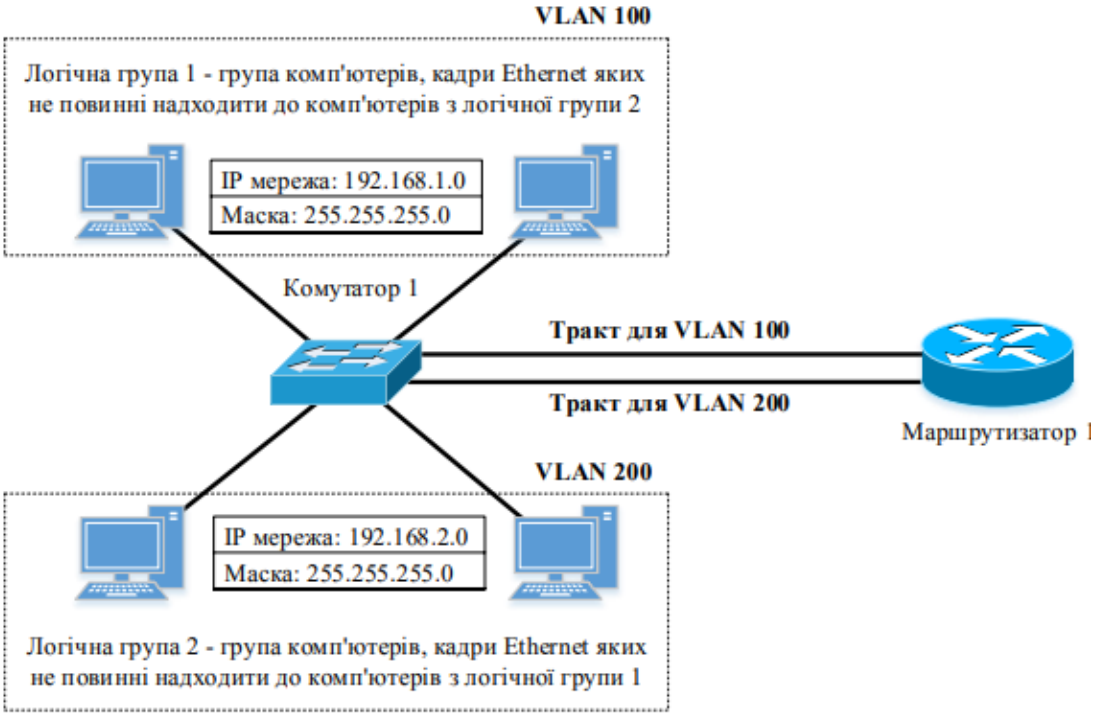


Рисунок 2.4 – Приклад організації можливості обміну інформацією між користувачами з різних VLAN на основі портів (IP-адреси користувачів з різних віртуальних мереж повинні знаходитись у різних IP-мережах)

Таким чином, спосіб утворення VLAN на основі портів у мережі з декількома комутаторами, а також при забезпечення можливості обміну інформацією між користувачами, що перебувають у різних віртуальних мережах, вимагає для своєї реалізації додаткового виділення такої кількості портів, скільки віртуальних мереж підтримується. Це є істотним недоліком даного способу при великій кількості віртуальних мереж.

2.3 Віртуальні локальні мережі на основі стандарта IEEE 802.1q

Побудова VLAN на основі портів заснована тільки на додаванні додаткової інформації до таблиці комутації комутатора й не використовує можливості вбудовування інформації про приналежність до віртуальної мережі в кадри, що передаються.

Спосіб організації VLAN основі стандарту IEEE 802.1q передбачає розміщення всередині кадру Ethernet додаткового службового поля розміром 4 байти, що дозволяє передавати таку інформацію (рисунок 2.5):

Tag Protocol Identifier (TPID) − ідентифікатор протоколу розміром 16 біт − 0x8100, який відповідає стандарту 802.1q, що вказує на використання у кадрі другого рівня цього стандарту;

Tag Control Information (TCI) – поле керування розміром 16 біт, що містить в собі такі поля:

- Priority – пріоритет кадру розміром 3 біти відповідно до стандарту IEEE 802.1p;
- Canonical Format Indicator (CFI) – індикатор канонічного формату розміром 1 біт, який вказує на формат MAC-адреси (0 – канонічний, 1 – неканонічний), що забезпечує сумісність між мережами Ethernet та Token Ring;
- VLAN Identifier (VID або VLAN ID) – ідентифікатор VLAN розміром 12 біт (діапазон можливих значень ідентифікатора в десятковому форматі становить від 0 до 4095, що надає можливість утворення 4095 віртуальних мереж). Відмітимо, що мінімальний та максимальний розміри поля даних кадру Ethernet зменшується на величину службових полів стандарту 802.1q, тобто на 4 байти, а контрольна сума FCS обчислюється знову з урахуванням цих полів.

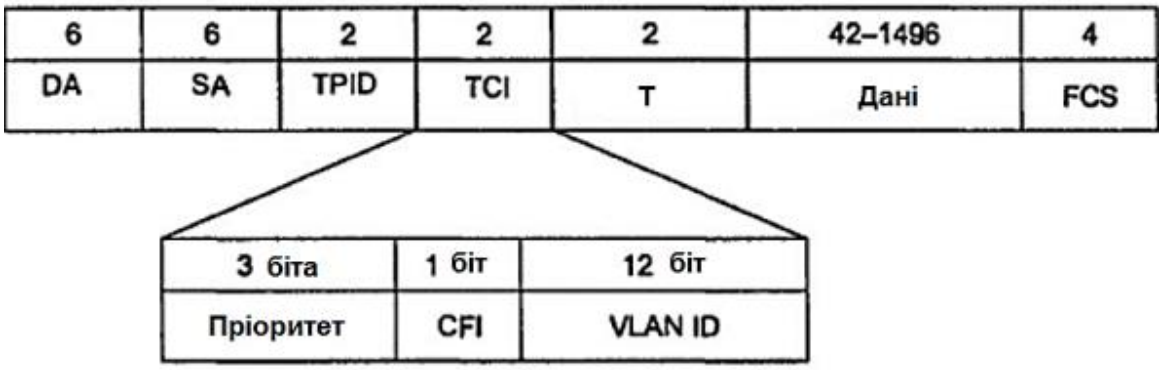


Рисунок 2.5 – Структура кадру Ethernet відповідно до стандарту 802.1q

Порти комутаторів, які використовуються для організації VLAN на основі стандарту 802.1q, мають тип Trunk (tagged, маркований порт). Ці порти можуть передавати кадри Ethernet, які містять службове поле відповідно до стандарту IEEE 802.1q, від декількох VLAN, що дозволяє здійснювати з'єднання комутаторів мережі тільки одним трактом передачі (рисунок 2.6), на відміну від VLAN на основі портів.

Для роботи комутатора з несумісним обладнанням, за стандартом IEEE 802.1q, передбачаються порти типу Access (untagged, немарковані порти). З рисунка 2.6 видно, що порти комутаторів, до яких приєднані персональні комп'ютери (тут вважається, що мережеві адаптери комп'ютерів не мають підтримки стандарту IEEE 802.1q), мають тип Access. Відмітимо, що порти типу Access можуть бути використані для організації VLAN на основі портів. Приклад організації можливості обміну інформацією між користувачами із різних VLAN на основі стандарту 802.1q за допомогою маршрутизатора показаний на рисунку 2.7, з якого видно, що комутатор з маршрутизатором з'єднуються між собою тільки одним трактом, утвореним портами типу Trunk, на відміну від застосування VLAN на основі портів. Зазначимо, що стандарт IEEE 802.1q передбачає передачу кадрів від портів, які не включено до будь-якої VLAN, через тракти передачі з портами типу Trunk (tagged). У цьому випадку кадри від не розподілених за віртуальними мережами портів автоматично включаються до нативної VLAN (Native VLAN), ідентифікатор

якої за замовчуванням дорівнює 1. Як правило, 11 Native VLAN використовується для передачі інформації керування комутаторами та маршрутизаторами, а також такими протоколами, як STP (Spaning Tree Protocol), VTP (VLAN Trunking Protocol), CDP (Cisco Discovery Protocol) та ін.

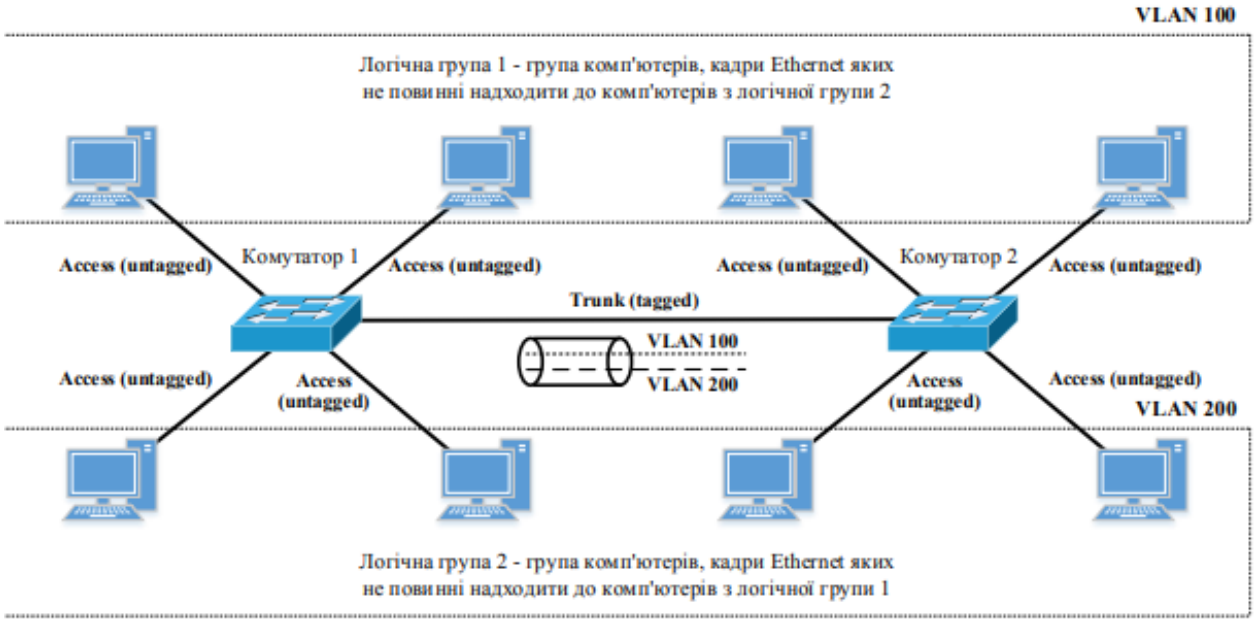


Рисунок 2.6 – VLAN на основі стандарту 802.1q в мережі з декількома комутаторами (комутатори з’єднані між собою тільки одним трактом, утвореним портами типу Trunk)

Таким чином, можна зробити висновок, що з погляду зручності й гнучкості настроювань, VLAN стандарту IEEE 802.1q є кращим рішенням у порівнянні з VLAN на основі портів. Крім того, VLAN стандарту IEEE 802.1q дозволяє на канальному рівні в мережі Ethernet застосовувати механізми забезпечення якості обслуговування QoS відповідно до стандарту IEEE 802.1p за рахунок поля Priority, передбаченого стандартом IEEE 802.1q. Без застосування стандартів IEEE 802.1q/p забезпечення якості обслуговування QoS на канальному рівні в мережі Ethernet неможливо, оскільки кадр Ethernet відповідно до стандарту IEEE 802.3 не містить службового поля для цих цілей.

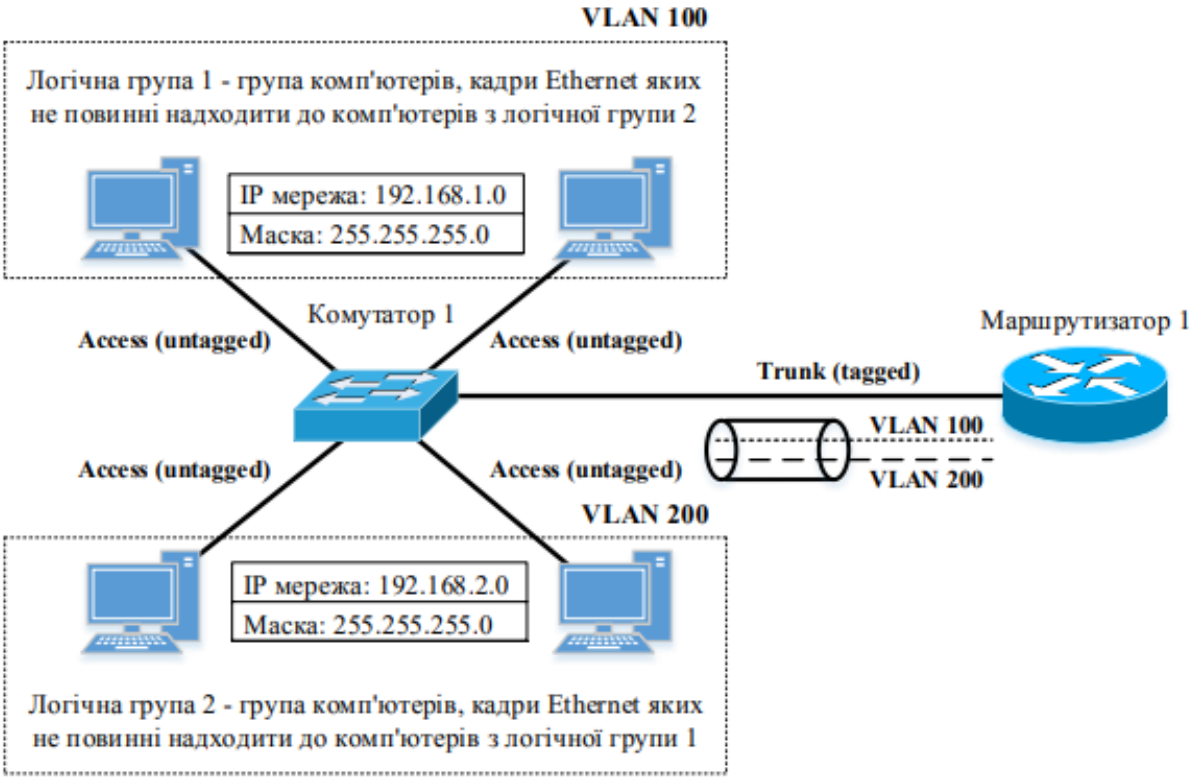


Рисунок 2.7 – Приклад організації можливості обміну інформацією між користувачами із різних VLAN на основі стандарту 802.1q (комутатор з маршрутизатором з’єднані між собою тільки одним трактом, утвореним портами типу Trunk; IPадреси користувачів із різних віртуальних мереж повинні знаходитися у різних IP-мережах)

3 РОЗРОБЛЕННЯ СХЕМИ МЕРЕЖІ ETHERNET З ЛОГІЧНОЮ СЕГМЕНТАЦІЄЮ НА ОСНОВІ VLAN

Схема мережі Ethernet з логічною сегментацією на основі VLAN та вихідні дані, необхідні для конфігурування обладнання, показані на рисунку 3.1. До складу імені кожного з комп’ютерів на рисунку 2.1 включена його IP-адреса. З рисунка 3.1 видно, що 12 комп’ютерів у мережі розділені на дві логічні групи незалежно від того, до якого з комутаторів вони приєднані. У даному випадку застосовуються два способи організації VLAN − на основі портів і на основі стандарту IEEE 802.1q.

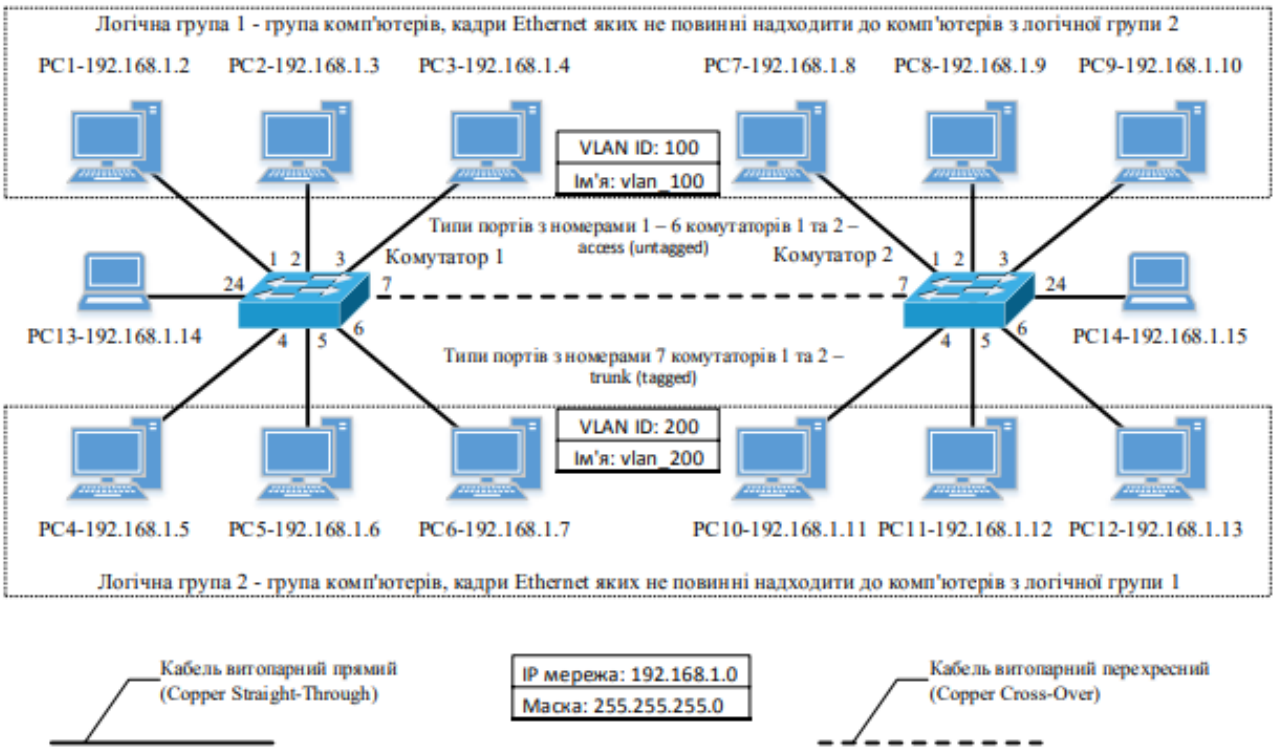


Рисунок 3.1 − Схема мережі на основі комутаторів другого рівня з логічною сегментацією на основі VLAN

Комп’ютери логічної групи 1 підключені до портів, які належать до VLAN з ідентифікатором VLAN ID (VLAN Identifier) 100, а комп’ютери логічної групи 2 − до портів, які належать до VLAN з ідентифікатором VLAN

ID 200, що відповідає способу утворення VLAN на основі портів. Відмітимо, що такий спосіб організації VLAN не дозволяє з'єднати комутатор 1 і 2 лише одним трактом передачі, оскільки для кожної з VLAN необхідно використовувати окремий тракт, порти якого належать тільки до однієї VLAN, що не є раціональним. Тому з метою з'єднання комутаторів розглядуваної мережі тільки одним трактом передачі у цьому тракті використано спосіб організації VLAN основі стандарту IEEE 802.1q.

Порти комутаторів, які використовуються для організації VLAN на основі портів мають тип Access (untagged), а порти комутаторів, які використовуються для організації VLAN на основі стандарту 802.1q, − тип Trunk (tagged). Також відмітимо, що стандарт IEEE 802.1q передбачає передачу кадрів від портів, які не включено до будь-якої VLAN, через тракт передачі з портами типу Trunk (tagged). У цьому випадку кадри від не розподілених за віртуальними мережами 14 портів автоматично включаються до нативної VLAN (Native VLAN), ідентифікатор якої за замовчуванням дорівнює 1. На рисунку 3.1 два комп'ютери не належать до жодної з віртуальних мереж, тому їх кадри при передачі через тракт між комутатором 1 і комутатором 2 будуть автоматично включені до Native VLAN з ідентифікатором 1 за замовчуванням. Розподіл портів комутаторів за номерами VLAN наведено в таблиці 3.1. Відмітимо, що у розглядуваному прикладі порти комутаторів, які мають тип Trunk (tagged), застосовуються для передачі кадрів з усіх VLAN, але існує можливість передавати по тракту кадри тільки від VLAN з визначеними VLAN ID.

Умовна назва комутатора	Номери портів комутатора	VLAN ID	Тип порту
Комутатор 1	1 – 3	100	Access
	4 – 6	200	Access
	7	–	Trunk
Комутатор 2	1 – 3	100	Access
	4 – 6	200	Access
	7	–	Trunk

Рисунок 3.1 – Розподіл портів комутаторів за номерами VLAN

Також з рисунка 3.1 видно, що при з’єднанні комп’ютерів з комутатором необхідно використовувати кабель витопарний прямий (без внутрішнього кросування), оскільки фізичні інтерфейси мережевих карт (порти) комп’ютерів мають тип MDI (Media Dependent Interface), а фізичні інтерфейси (порти) комутатора – тип MDI-X (Media Dependent Interface with Crossover). А при з’єднанні комутаторів між собою треба використовувати кабель витопарний перехресний (з внутрішнім кросуванням), оскільки в цьому випадку з’єднуються однакові типи портів MDI-X. Але треба відмітити, що в сучасних комутаторах застосовуються порти типу Auto-MDI(X) і, таким чином, використання кабелю витопарного перехресного не є обов’язковим.

4 СТВОРЕННЯ ІМІТАЦІЙНОЇ МОДЕЛІ МЕРЕЖІ ETHERNET З ЛОГІЧНОЮ СЕГМЕНТАЦІЄЮ НА ОСНОВІ VLAN У ПРОГРАМНОМУ СЕРЕДОВИЩІ CISCO PACKET TRACER

Для настроювання VLAN за допомогою графічного інтерфейсу симулятора на кожному з комутаторів необхідно у діалоговому вікні властивостей пристрою вибрати вкладку Config та виконати такі кроки: − в меню ліворуч натиснути на кнопку VLAN Database. І поля, що з'являться праворуч, VLAN Number та VLAN Name ввести відповідно ідентифікатори VLAN ID та імена VLAN, а потім натиснути на кнопку Add (рисунок 4.1); − в меню ліворуч натиснути на кнопку з типом і номером інтерфейсу. В меню, що з'являться праворуч, вибрати тип порту (Access, Trunk) та ідентифікатор VLAN (для порту типу Access цей ідентифікатор буде показувати приналежність інтерфейсу до відповідної VLAN, а для інтерфейсу типу Trunk – кадри яких VLAN має передавати), що показано на рисунках 4.2 та 4.3.

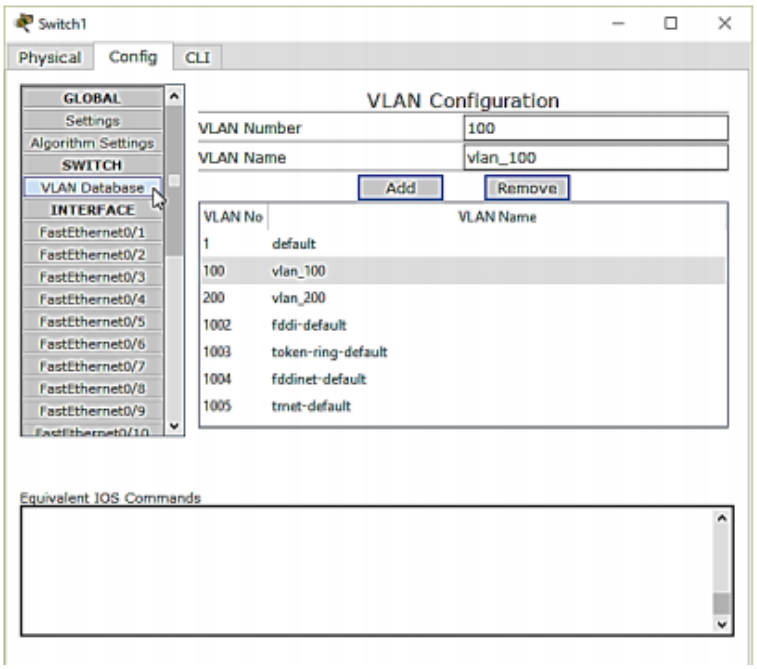


Рисунок 4.1 – Введення до бази даних віртуальних мереж VLAN ID та імені VLAN

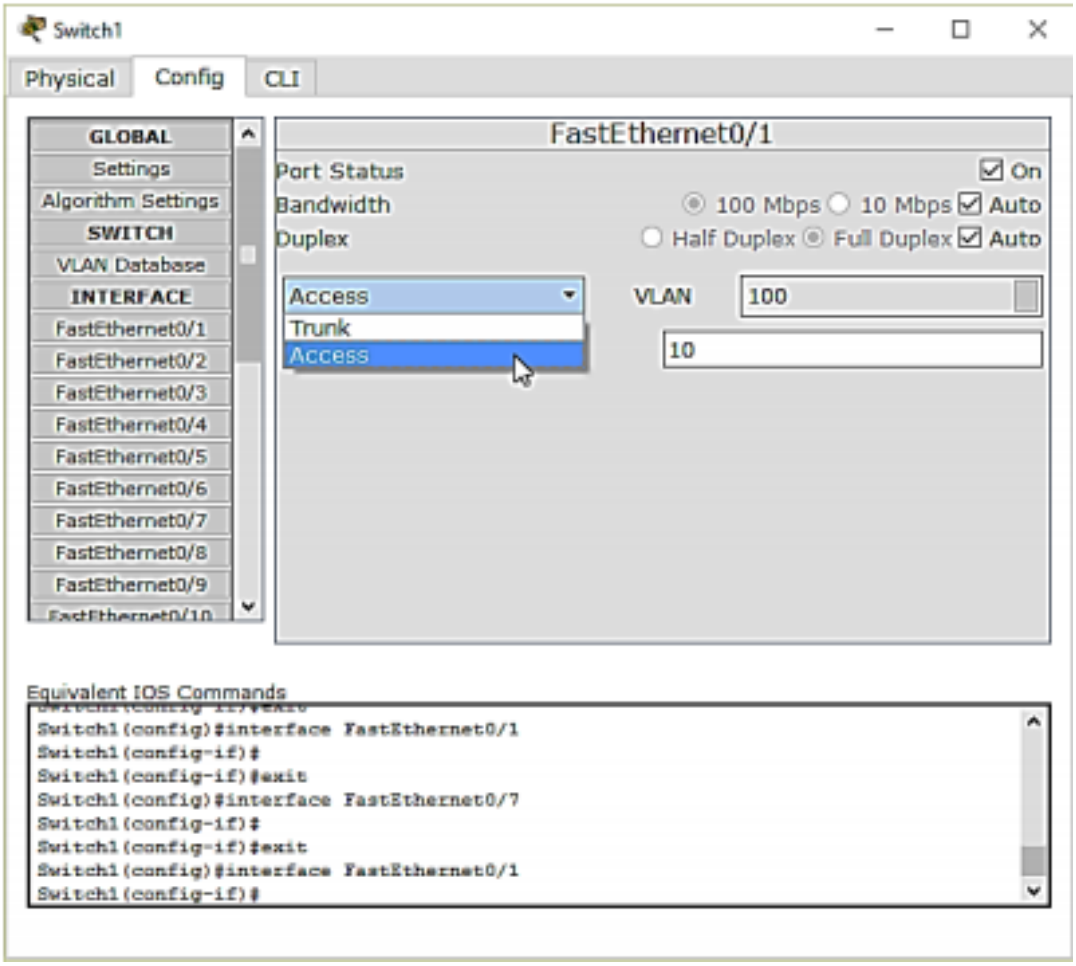


Рисунок 4.2 – Конфігурування інтерфейсу типу Access: вибір типу інтерфейсу (Access) та ідентифікатора VLAN (100)

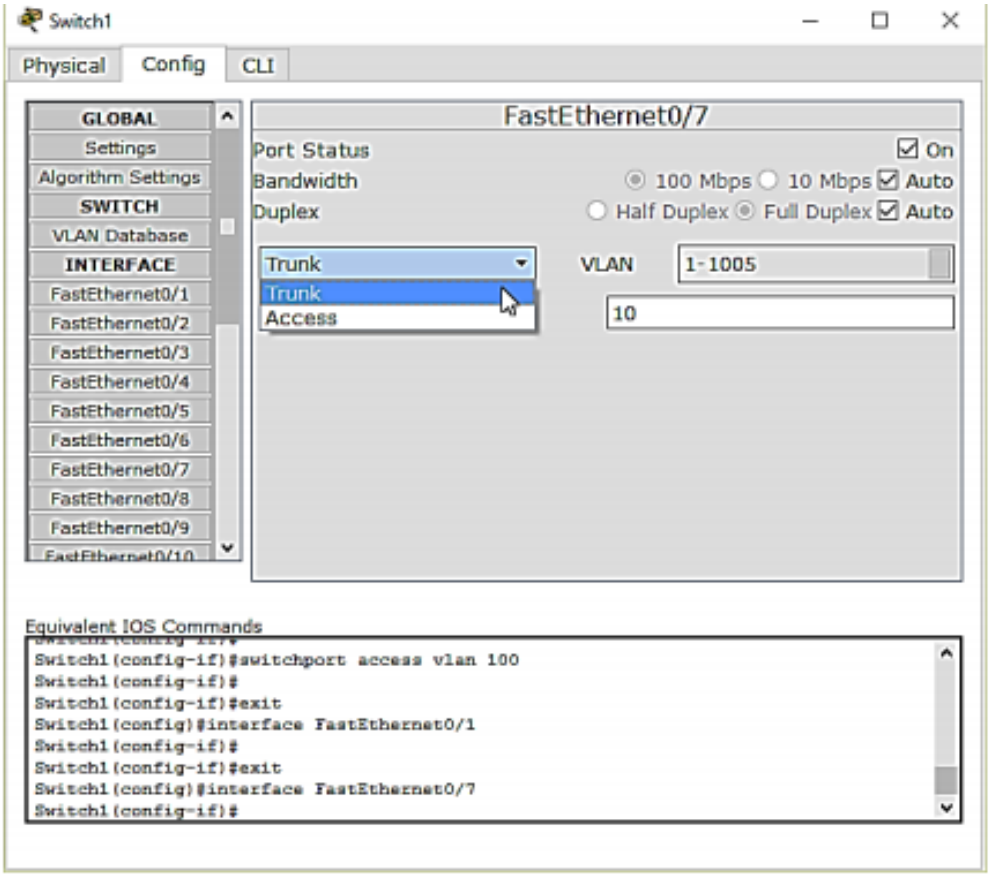


Рисунок 4.3 – Конфігурування інтерфейсу типу Trunk: вибір типу інтерфейсу (Trunk) та ідентифікатора VLAN (1 − 1005)

Далі розглянемо варіант конфігурування комутаторів за допомогою командного рядка операційної системи Cisco IOS. Утворення VLAN (введення до бази даних комутатора даних про ідентифікатор та ім’я віртуальної мережі) здійснюється командою vlan {ідентифікатор VLAN}, яка вводиться у привілейованому режимі, а присвоєння імені – командою name {ім’я VLAN}, яка вводиться у режимі детального конфігурування віртуальної мережі.

Switch>enable Switch#config

Switch(config)#vlan 100

Switch(config-vlan)#name vlan_100

Switch(config-vlan)#no shutdown

Switch(config-vlan)#exit

```
Switch(config)#vlan 200
 Switch(config-vlan)#name vlan_200
Switch(config-vlan)#no shutdown
Switch(config-vlan)#exit 18
```

Після утворення VLAN необхідно здійснити конфігурування інтерфейсів комутаторів з метою визначення типів інтерфейсів (Access, Trunk) та їх приналежності до VLAN, яке виконується у режимі детального конфігурування відповідного інтерфейсу. Встановлення типу інтерфейсу Access здійснюється командою switchport mode access, а встановлення приналежності до віртуальної мережі – командою switchport access vlan {ідентифікатор VLAN}. Наведемо приклад для інтерфейсу FastEthernet0/1.

```
 Switch (config)#interface FastEthernet0/1
 Switch (config-if)#switchport mode access
Switch (config-if)#switchport access vlan 100
Switch (config-if)#exit
```

Встановлення типу інтерфейсу Trunk здійснюється командою switchport mode trunk. Наведемо приклад для інтерфейсу FastEthernet0/7. Switch(config)#interface FastEthernet0/7

```
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
```

Після закінчення конфігурування усіх портів необхідно зберегти утворену конфігурацію в енергонезалежній пам'яті пристрою командою copy running-config startup-config, яка має вводитися у привілейованому режимі, тому перед збереженням необхідно перейти в цей режим введенням команди exit.

```
Switch(config)#exit
Switch#copy running-config startup-config
```

Далі можна перевірити утворену конфігурацію за допомогою команд, які необхідно вводити у привілейованому режимі.

```
Switch#show vlan
Switch#show interfaces trunk
Switch#show interfaces switchport
```

5 ПРОЕКТУВАННЯ ТА НАЛАШТУВАННЯ ПРАЦЕЗДАТНОСТІ МЕРЕЖІ

5.1 Проектування мережі центрального офісу (LAN1)

У центральному офісі LAN1 – для адресації мереж використати маски змінної довжини та статичну маршрутизацію.

На рисунку 5.1 зображена структурна схема мережі центрального офісу.

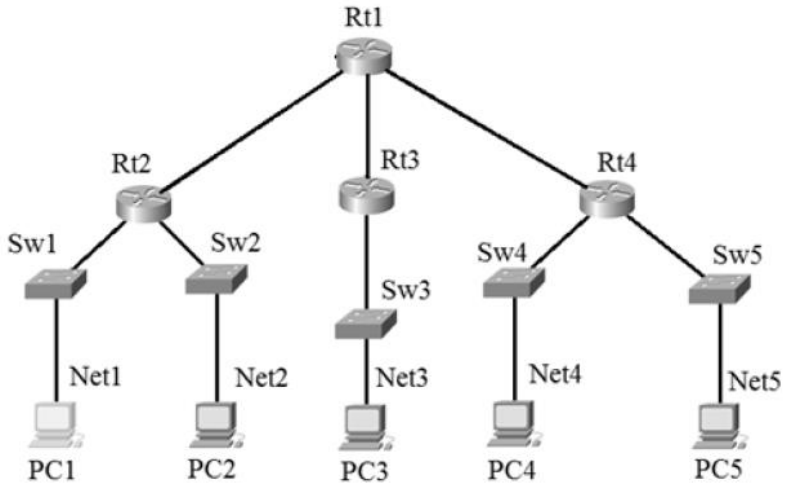


Рисунок 5.1 – Структурна схема мережі центрального офісу

5.1.1 Хід розрахунку

Таблиця 5.1 – Вихідні дані для адресації хостів мережі центрального офісу

Адреса мережі	Макс. к-ть хостів в сегменті				
	Net1	Net2	Net3	Net4	Net5
96.96.0.0	50	65	45	5	30

У таблиці 5.1 наведенні вхідні данні для розрахунку.

Для того щоб вмістити кількість хостів Net1 (10 хостів) необхідно – 4 біт, $2^4 = 16$, а 16 > 10. Аналогічно визначимо кількість біт для хостів інших підмереж.

Net1 (A) – 10 = 4b

Net2 (B) – 50 = 6b

Net3 (C) – 12 = 4b

Net4 (D) – 30 = 5b

Net5 (E) – 10 = 4b

Net6 (K) – 2 = 2b

Net7 (L) – 2 = 2b

Net6 (M) – 2 = 2b

Заповнимо таблицю 5.2 та пояснимо кожен крок

Таблиця 5.2 – Розрахунок підмереж

№	0 . 128 64 32 16 8 4 2 1 0 . 0 0 0 0 0 0 0 0	Net	Host	Mask	Broad cast	Незад іяні
B	0 . 0 0 0 0 0 0 0 1 0 . 0 1 1 1 1 1 1 0	0.0	0.1÷0.126	255.255.255.128	0.127	61
D	0 . 1 0 0 0 0 0 0 1 0 . 0 1 0 1 1 1 1 0	0.128	0.129÷0.190	255.255.255.192	0.191	12
A	0 . 0 1 1 0 0 0 0 1 0 . 1 1 1 1 1 1 1 0	0.192	0.193÷0.254	255.255.255.192	0.255	17
C	0 . 0 0 0 0 0 0 0 1 0 . 0 0 0 1 1 1 1 0	1.0	1.1÷1.30	255.255.255.224	1.31	0
E	0 . 0 0 1 0 0 0 0 1 0 . 0 0 1 0 0 1 1 0	1.32	1.33÷1.38	255.255.255.248	1.39	1
K	0 . 0 0 1 0 1 0 0 1 0 . 0 0 1 0 1 0 1 0	1.40	1.41÷1.42	255.255.255.252	1.43	0
L	0 . 0 0 1 0 1 1 0 1 0 . 0 0 1 0 1 1 1 0	1.44	1.45÷1.46	255.255.255.252	1.47	0
M	0 . 0 0 1 1 0 0 0 1 0 . 0 0 1 1 0 0 1 0	1.48	1.49÷1.50	255.255.255.252	1.51	0

1 стовпчик для нумерації мереж (мережі записуємо в порядку спадання кількості їхніх хостів), 2 в даній задачі використовується для запозичення біта мережі, 3 стовпчик заповнюється для визначення діапазону хостів і broadcast,

4 – мережа, 5 – діапазон хостів, 6 – broadcast, 7 – кількість незадіяних хостів, 8 – маска підмережі

Для того, щоб відмежувати біти відведені на хостову та підмережеву частину проведемо пунктирну лінію. В даному випадку нам потрібно 7 біт, отже справа на ліво відрахую 7 біт і проведемо лінію. Адреса підмережі знаходиться зліва від пунктирної лінії, в даному рядку вона 0.0, а до хостової частини відноситься 0000001. Адреса підмережі не враховує 7 біт, що відноситься до хостової частини, тому що коли ми говоримо про підмережу, в хостовій частині завжди 0. Отже адреса підмережі 0.0. Дані в записую таблицю.

Далі визначаю кількість хостів в даній підмережі. 00000001 в десятковій системі числення рівне 1 в десятковій системі числення. Отже початок нумерації хостів починається з 1. Тепер визначаю який хост буде кінцевим. 1111110 в десятковій системі числення – 126. Діапазон хостів 0.1 ÷ 0.126. Дані в записую таблицю.

Визначаю broadcast, який завжди має останню адресу в мережі. Переводимо число 1111111 в десяткову систему числення – 127. Отже broadcast буде рівним 0.127. Дані в записую таблицю.

Наступний крок це визначення кількості незадіяних хостів. Визначається різницею всіх хостів, з задіяними хостами (плюс адреса мережі і broadcast)

126 – 65 = 61. В даній підмережі незадіяні 61 хости. Дані в записую таблицю.

Визначаємо маску. Згідно з визначенням «маска» або «маска підмережі» це послідовність спочатку 1, а потім 0, що дозволяє поділити IP-адресу на дві частини: номер підмережі та номер пристрою у цій підмережі. Для знаходження маски необхідно відняти від максимального значення маски, що рівне 32 бітам, кількість бітів виділених на хостову частину.

Mask = MaxMask – HOST = 32 – 5 = 27 біт. Записую спочатку 27 одиниць а потім дописую 5 нулів.

11111111. 11111111. 11111111. 11100000

Якщо перевести маску в вигляд десяткової системи числення, то маска буде мати наступний вигляд – 255.255.255.128

Дані в записую таблицю. Надалі будуть проводитись аналогічні дії з наступними мережами.

1. Перший крок полягає в задані IP-адреси комп’ютеру, маски підмережі та шлюзу за замовченням (default gateway). Приклад задання цих параметрів зображено на рисунку 5.2 для комп’ютера PC0. Аналогічно сконфігурую параметри і для всіх інших кінцевих пристроїв.

2. Далі потрібно задати IP параметри порта роутера, для того, щоб комп’ютер PC0 міг обмінюватись інформацією з іншими комп’ютерами, які знаходяться в інших мережах. Для цього ми переходимо на відповідний інтерфейс роутера fa0/0 і задаємо йому ip-адресу та маску. Після цього ми піднімаємо порт роутера поставивши галочку on. На рисунку 5.3 наведений приклад налаштування.

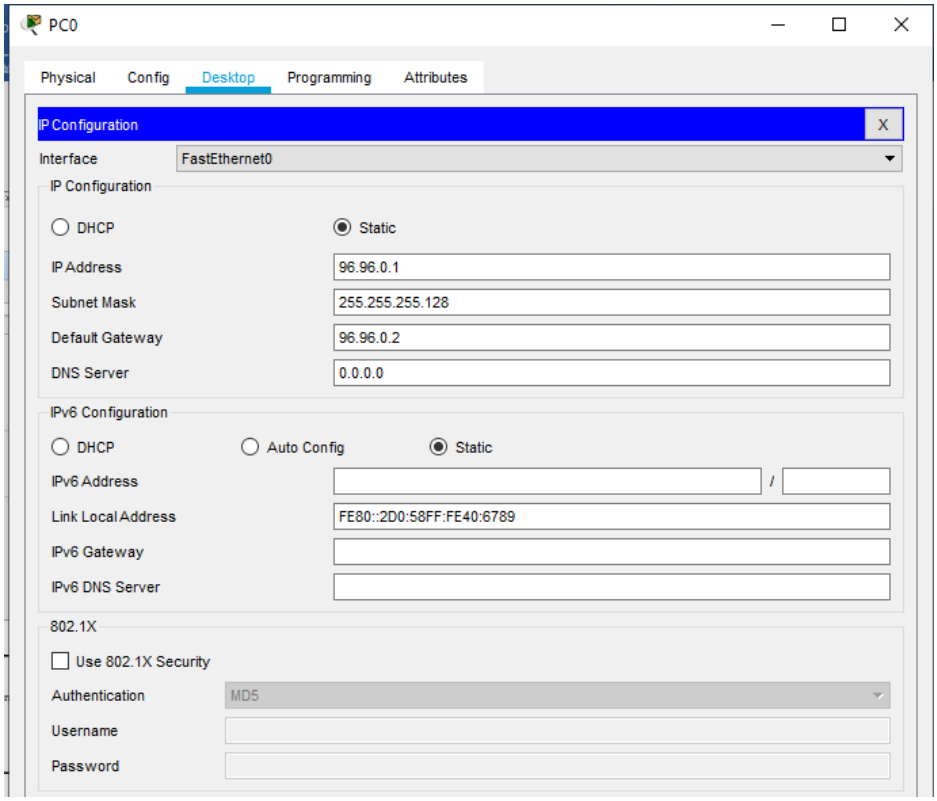


Рисунок 5.2 – Приклад конфігурування основних параметрів кінцевому пристрою

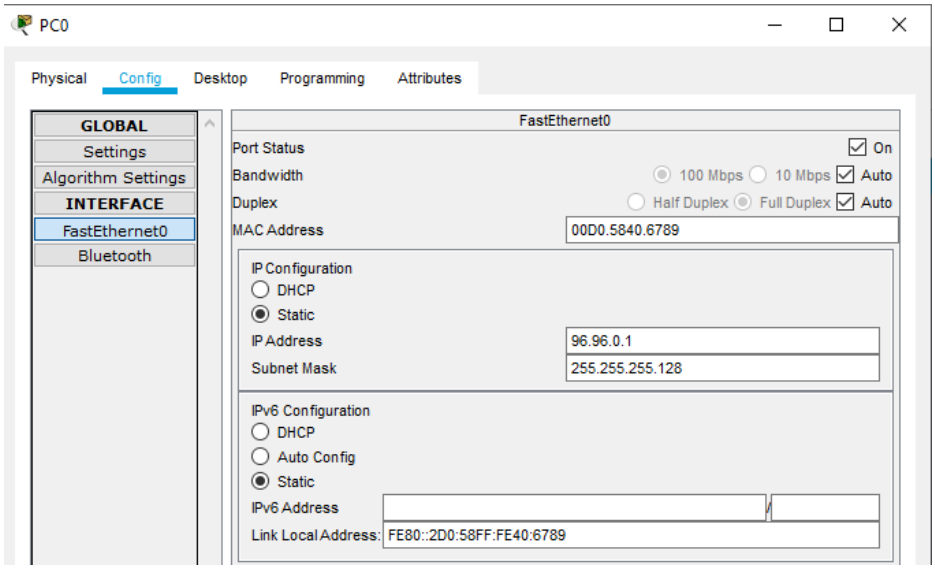


Рисунок 5.3 – Приклад налаштування роутера

3. Після того як всі ip-адреси, маски та шлюзи за замовченням прописані, потрібно прописати статичні маршрути. Для роутерів Router1, Router2, Router3, які підключені до головного роутера, задаємо статичні маршрути за

замовчуванням на головний роутер. Приклад такого налаштування Router1 зображений на рисунку 5.4. Аналогічно налаштовуємо Router2 та Router3.

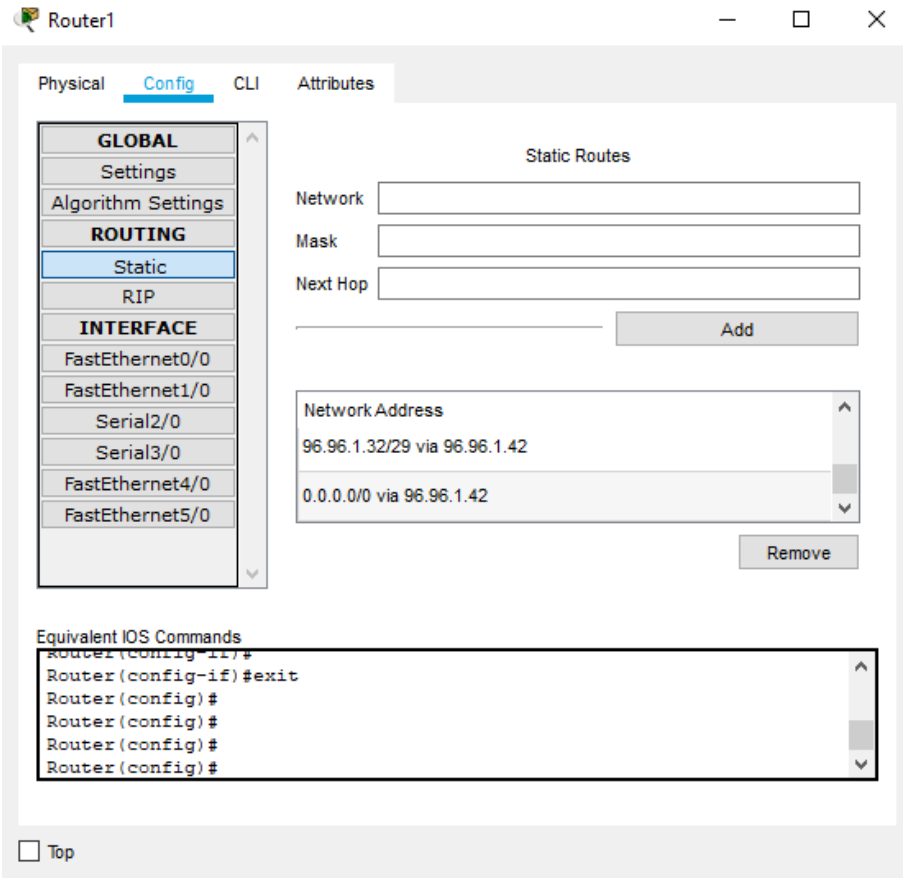


Рисунок 5.4 – Встановлення статичного маршруту за замовчуванням

4. Після задання статичних маршрутів , потрібно задати маршрути для головного роутера (Router0) у всі підмережі. Для цього вказую необхідну мережу, її маску та адресу наступного роутера (Next Hop). На рисунку 5.5 показана частина таблиці маршрутизації роутера (Router0).

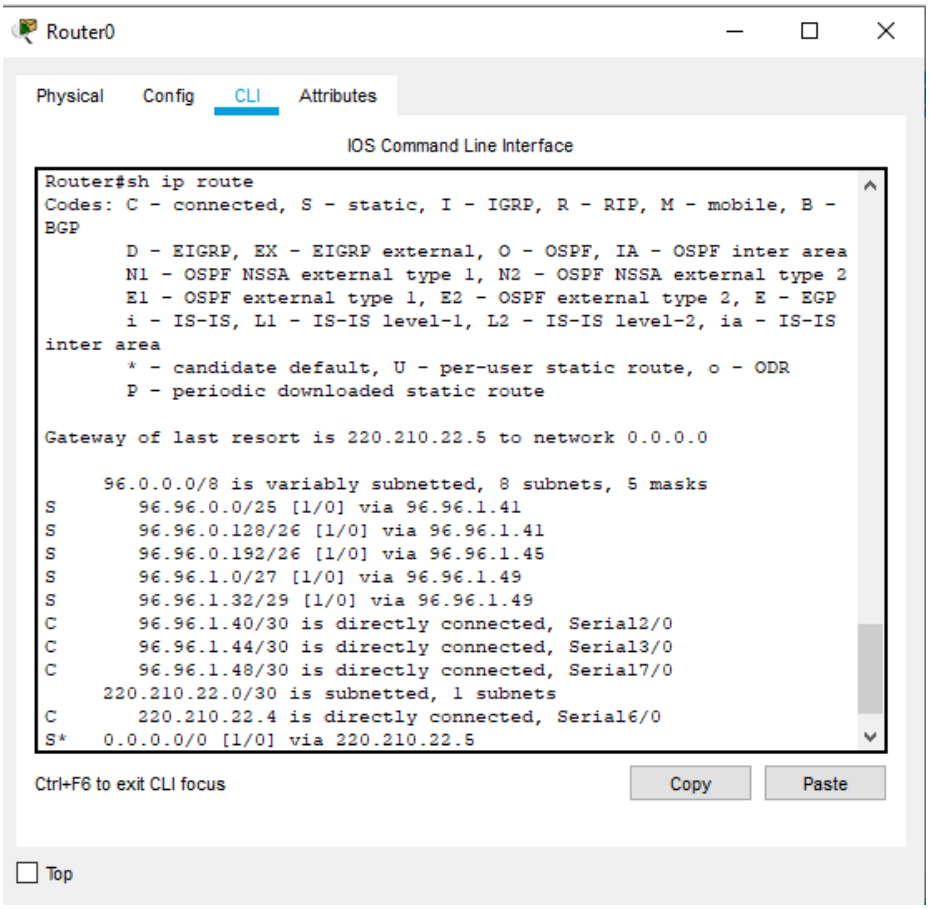


Рисунок 5.5 – Таблиця маршрутизації роутера (Router0)

Для завершення проектування перевіряю роботу мережі. Для цього пробую передати пакети від різних кінцевих пристроїв до будь-яких інших. Результат роботи мережі зображений на рисунку 5.6.

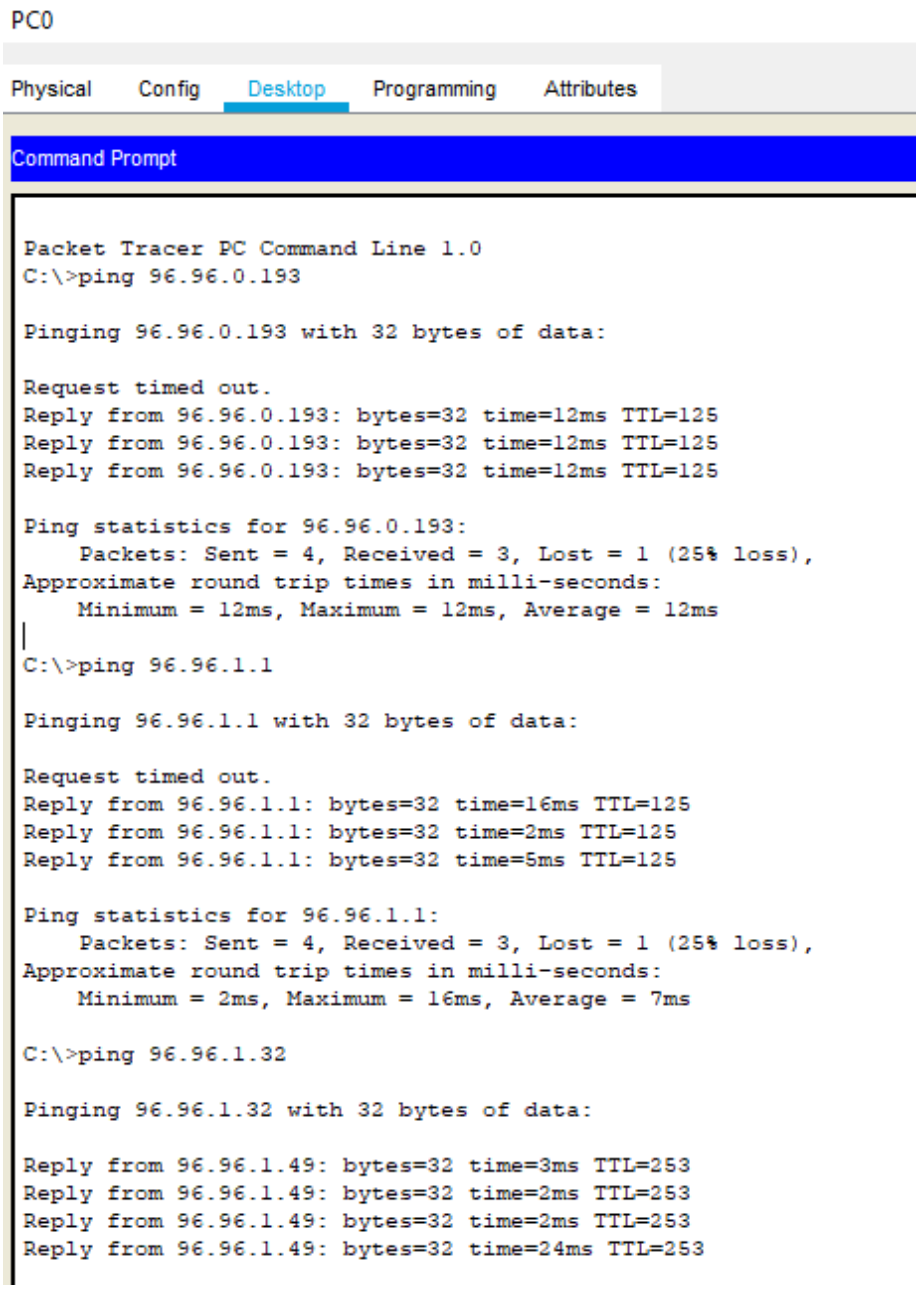


Рисунок 5.6 – Результат роботи мережі

5.2 Проектування мережі віддаленого офісу (LAN2)

Структура мережі віддаленого офісу наведена на рисунку 5.7

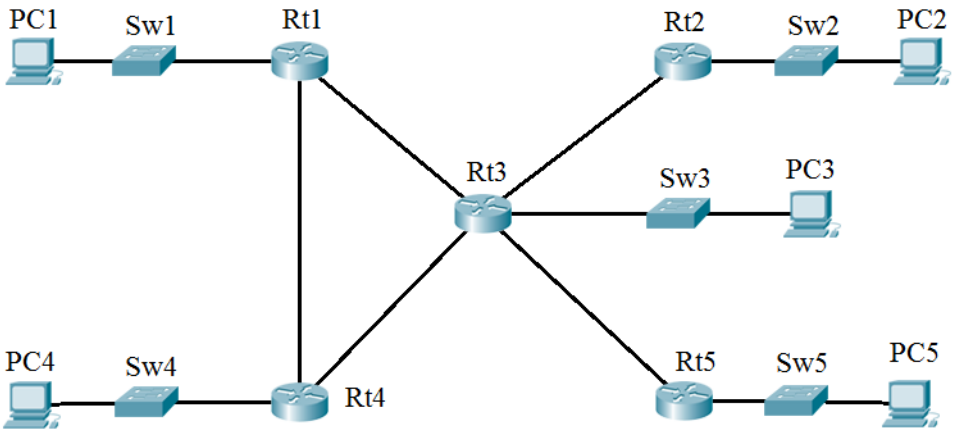


Рисунок 5.7 – Структура мережі віддаленого офісу

Таблиця 5.3 – Вихідні дані для адресації хостів мережі віддаленого офісу та протокол динамічної маршрутизації у даній мережі

Адреса мережі	Макс. кількість комп'ютерів у сегменті	Протокол динамічної маршрутизації
198.12.0.0	210	OSPF

У таблиці 5.3 наведені вхідні данні для розрахунку.

Дано ip-адресу 198.12.0.0. Розбити мережу на 11 підмереж, кількість хостів 210. Визначити № мережі, кількість хостів, які входять в дану мережу, broadcast, і маску.

NET = 11; bits = 4.

HOST = 210; bits = 8

IP-address 198.12.0.0

Для того щоб вмістити 11 підмереж потрібно виділити 4 біта, $2^4 = 16$, 16 > 11. Аналогічно визначимо кількість бітів для хостів $2^8 = 256$, 256 > 210, отже виділяємо 8 біт. Всього біт відведених для адресації мереж і хостів 4 + 8 = 12 біт, тому треба 2 байта (16 біт).

Заповнимо таблицю 5.4 і пояснимо кожен крок.

Спочатку виділяємо місце для нумерації, 2 і 3 стовпчик (по 8 біт) заповнюємо справа на ліво 10 нулями, 4 біта на мережу, а 6 біт на хостову частину і розділяємо пунктирною лінією, 4 стовпчик це номер мережі, 5 – кількість хостів, 6 – broadcast, 7 – маска.

Таблиця 5.4 – Розрахунок мережі

N	Max and min ip		Net	Host	Broadcast	Unused	Mask
1	0000 0000	.00000001 .11111110	0.0	0.1 ÷ 0.254	0.255	44	255.255.255.0
2	0001 0001	.00000001 .11111110	1.0	1.1 ÷ 1.254	1.255	44	255.255.255.0
3	0010 0010	.00000001 .11111110	2.0	2.1 ÷ 2.254	2.255	44	255.255.255.0
4	0011 0011	.00000001 .11111110	3.0	3.1 ÷ 3.254	3.255	44	255.255.255.0
5	0100 0100	.00000001 .11111110	4.0	4.1 ÷ 4.254	4.255	44	255.255.255.0
6	0101 0101	.00000001 .11111110	5.0	5.1 ÷ 5.254	5.255	44	255.255.255.0
7	0110 0110	.00000001 .11111110	6.0	6.1 ÷ 6.254	6.255	44	255.255.255.0
8	0111 0111	.00000001 .11111110	7.0	7.1 ÷ 7.254	7.255	44	255.255.255.0
9	1000 1000	.00000001 .11111110	8.0	8.1 ÷ 8.254	8.255	44	255.255.255.0
10	1001 1001	.00000001 .11111110	9.0	9.1 ÷ 9.254	9.255	44	255.255.255.0
11	1010 1010	.00000001 .11111110	10.0	10.1 ÷ 10.254	10.255	44	255.255.255.0
12	1011 1011	.00000001 .11111110	11.0	11.1 ÷ 11.254	11.255	44	255.255.255.0

Спочатку визначимо статичну маску, вона буде однакова для всіх і розраховується за такою ж формулою, що використовувалась в розрахунку LAN1:

Mask = MaxMask – HOST = 32 – 8 = 24 біт

11111111.11111111.11111111.00000000 - 255.255.255.0

Так як в нас 12 підмереж, то буде зроблено 12 записів.

Визначимо перший запис. Для визначення адреси підмережі ми дивимся що знаходиться зліва від крапки – 00, а справа від крапки – 00000001. Оскільки 0000001 відноситься до хостової частини то адреса підмережі не враховує цих 8 біт тому що коли ми говоримо про підмережу в хостовій частині завжди 0. Тому зліва 0 і справа 0. Отже адреса підмережі 0.0. Дані записую в таблицю

Далі визначаємо кількість хостів у даній підмережі. Зліва від крапки 4 нулі, а отже зліва буде 0. Тепер справа 00000001. Переводимо це число в десяткову систему числення буде 1. Отже початок нумерації хостів починається з 0.1. Тепер визначаю який хост буде кінцевим. Так само зліва від крапки 4 нулі, отже – 0, справа від крапки 11010010. Переводимо в десяткову систему числення і це буде рівним 210. Діапазон хостів 0.1 ÷ 0.254. Дані записую в таблицю.

Визначаємо broadcast. це тоді коли в хостовій частині всі одиниці. Зліва від крапки 4 нулі , а отже – 0. Тепер справа від крапки. Переводимо число 11111111 в десяткову систему числення, це буде 255. Отже broadcast буде 0.255. Дані записую таблицю.

Тепер по аналогії записуємо наступних 9 записів.

Таблиця 5.5 – IP-адреси перших і останніх хостів, а також broadcast кожної підмережі

№	IP-address мережі	IP-address першого хоста	IP-address останнього хоста	Broadcast
1	198.12.0.0	198.12.0.1	198.12.0.254	198.12.0.255

Продовження таблиці 5.5

2	198.12.1.0	198.12.1.1	198.12.1.254	198.12.1.255
3	198.12.2.0	198.12.2.1	198.12.2.254	198.12.2.255
4	198.12.3.0	198.12.3.1	198.12.3.254	198.12.3.255
5	198.12.4.0	198.12.4.1	198.12.4.254	198.12.4.255
6	198.12.5.0	198.12.5.1	198.12.5.254	198.12.5.255
7	198.12.6.0	198.12.6.1	198.12.6.254	198.12.6.255
8	198.12.7.0	198.12.7.1	198.12.7.254	198.12.7.255
9	198.12.8.0	198.12.8.1	198.12.8.254	198.12.8.255
10	198.12.9.0	198.12.9.1	198.12.9.254	198.12.9.255

5.2.1 Хід розрахунку

Змоделюю мережу за допомогою програми Packet Tracer та сконфігурую IP-адреси на маршрутизаторах та кінцевих пристроях згідно з отриманою таблицею 5.5

Після того як я завершив прописувати адреси на хостах і роутерах, я приступив до налаштовування динамічної маршрутизації протоколом OSPF.

Протокол OSPF (Open Shortest Path First, алгоритми запропоновані Дейкстри) є альтернативою RIP в якості внутрішнього протоколу маршрутизації. OSPF являє собою протокол стану маршруту (в якості метрики використовується - коефіцієнт якості обслуговування). Кожен маршрутизатор має повну інформацію про стан всіх інтерфейсів всіх маршрутизаторів (перемикачів) автономної системи. Він був винайдений для позбавлення мереж, що використовують RIP від таких напастей, як:

1) Циклічні маршрути. Так як в протоколі немає механізмів виявлення замкнутих маршрутів, необхідно або сліпо вірити партнерам, або приймати заходи для блокування такої можливості.

2) Для придушення нестабільностей RIP повинен використовувати мале значення максимально можливого числа кроків (<16).

3) Повільне поширення маршрутної інформації з мережі створює проблеми при динамічному зміну маршрутної ситуації (система не встигає за змінами). Мале граничне значення метрики покращує збіжність, але не усуває проблему.

Протокол OSPF являє собою класичний протокол маршрутизації класу Link-State, який забезпечує:

1) відсутність обмежень на розмір мережі;

2) підтримку позакласових мереж;

3) передачу оновлень маршрутів з використанням адрес типу multicast;

4) досить велику швидкість встановлення маршруту;

5) використання процедури authentication при передачі і отримання оновлень маршрутів.

Для того щоб почати конфігурувати протокол динамічної маршрутизації OSPF потрібно зайти на роутері в IOS Command Line Interface. Там ми зможемо побачити дане вікно (рис.5.8), в якому за допомогою команд я налаштовував протокол.

Приклад налаштування OSPF:

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#rout ospf 22
Router(config-router)#do sh ip route con
C     198.12.0.0/24 is directly connected, FastEthernet0/0
C     198.12.2.0/24 is directly connected, Serial2/0
C     198.12.4.0/24 is directly connected, Serial3/0
Router(config-router)#net 198.12.0.0 0.0.0.255 area 22
Router(config-router)#net 198.12.2.0 0.0.0.255 area 22
Router(config-router)#net 198.12.4.0 0.0.0.255 area 22
Router(config-router)#
```

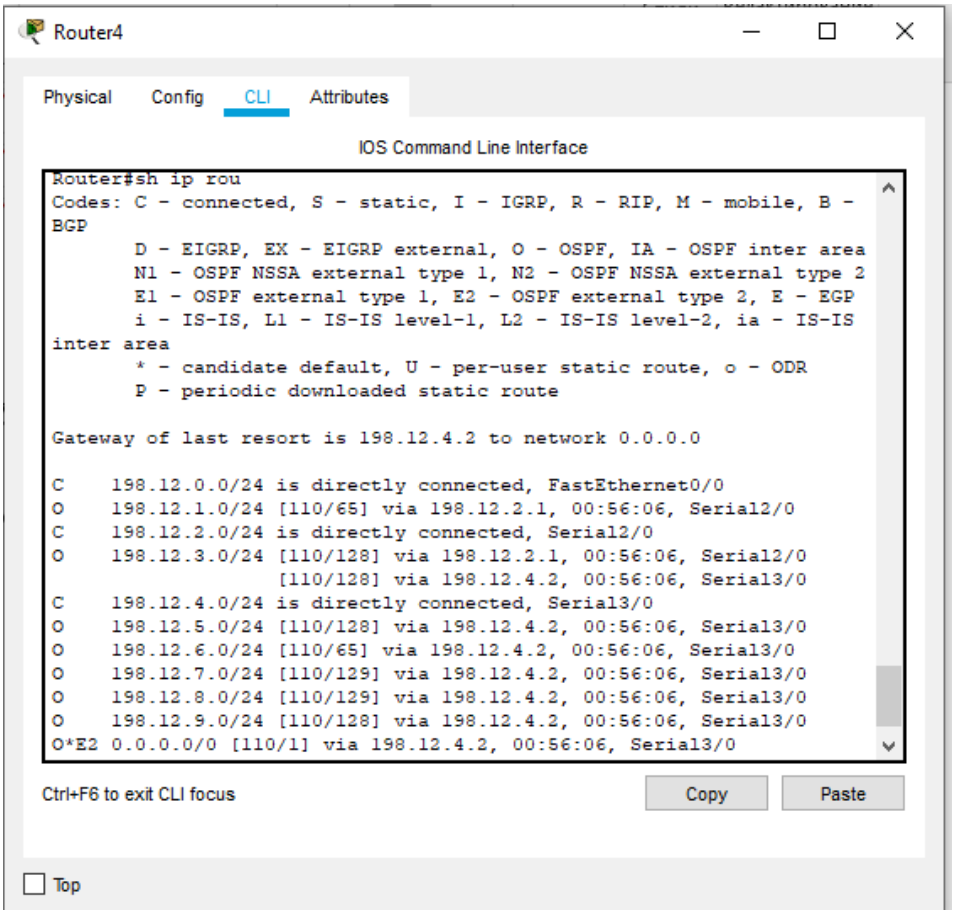


Рисунок 5.8 – Таблиця маршрутизації після конфігурування мережі

5.3 Проектування мережі диспетчерського центру (LAN3)

Для проектування мережі потрібно створити три віртуальні мережі відповідно завдання, наведеного у таблиці та налаштувати inter-VLAN роутинг.

Таблиця 5.6 – Завдання для проектування віртуальної локальної мережі

Віртуальна локальна мережа 10 (кінцеві пристрої)	Віртуальна локальна мережа 20 (кінцеві пристрої)	Віртуальна локальна мережа 30 (кінцеві пристрої)
10 1 4 7	8 11 2 5	9 0 3 6

Для адресації кінцевих пристроїв потрібно використати діапазон адрес 221.X.Y.0 255.255.255.0, де X – це номер студента по варіанту в групі Y – це номер віртуальної локальної мережі.

5.3.1 Хід налаштування

Налаштую IP-адреси на кожному кінцевому пристрої у діапазоні адрес, вказаному за умовою. Пристрою PC 10 присвоюю 221.22.10.1, так як кінцевий пристрій не може мати 0 у хостовій частині IP-адреси. Приклад конфігурування IP-адреси на кінцевому пристрої зображений на рисунку 5.9

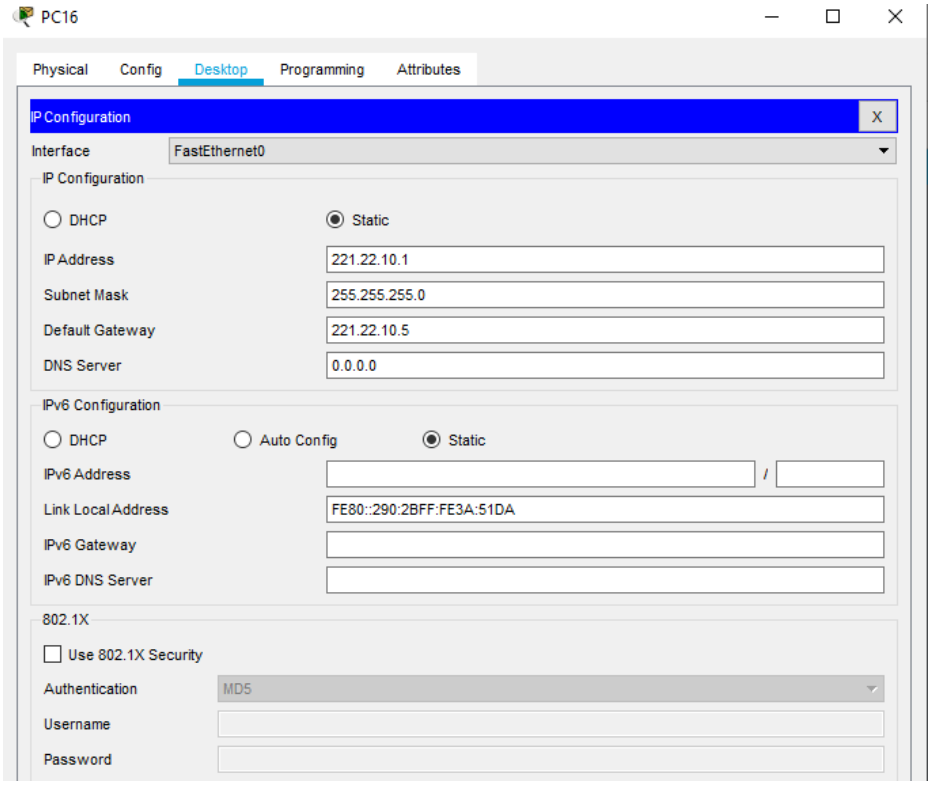


Рисунок 5.9 – Налаштування IP-адреси на кінцевому пристрої

1. Далі слідує конфігурування комутаторів (switches). Проаналізувавши схему, представлену у завданні, можна побачити, що світчі використовують лише одне з’єднання між собою, при наявних трьох віртуальних локальних мереж, а отже між світчами застосовуються trunk-з’єднання.

2. Спочатку налаштовуємо світчі, що під’єднані до кінцевих пристроїв. На кожному із цих світчів потрібно налаштувати по три віртуальні локальні

мережі враховуючи віртуальну мережу, до якої повинен бути підключений кінцевий пристрій. Розглянемо налаштування порту світча Switch13, що підключений до кінцевого пристрою PC10:

2.1 Визначимо який із портів потрібно конфігурувати. З рисунку 5.10 можна бачити, що це порт FastEthernet1/1 (Fa1/1).

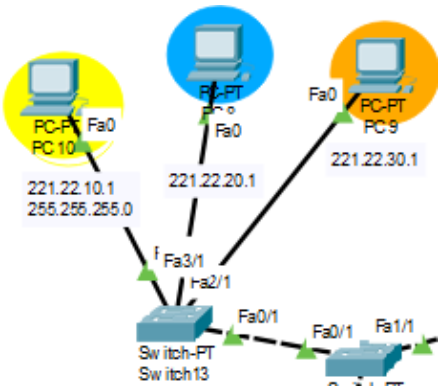


Рисунок 5.10 – Номер порту світча, під’єднаного до PC10

2.2 Заходимо до засобу налаштування світча - IOS Command Line Interface на світчеві Switch13.

2.3 Переходимо у привілейований режим командою enable, оскільки по замовчуванню стоїть користувацький режим:

Switch>enable

2.4 Входимо у режим глобального конфігурування світча за допомогою команди configure terminal:

Switch#configure terminal

2.5 PC10 за умовою належить до віртуальної мережі під номером 10, тому створюємо на Switch13 віртуальну мережу під даним номером за допомогою команди vlan [vlan_id]:

Switch(config)#vlan 10

Switch(config-vlan)#name VLAN10

Після виконання команди потрапимо у режим налаштування створеної VLAN.

2.6 Наступний крок - налаштування порту світча FastEthernet 1/1 до відповідної віртуальної локальної мережі. Для входу у режим налаштування порту виконаємо команду команду interface FastEthernet 1/1 :

2.8 Задамо порту світча FastEthernet 1/1 режим access та приналежність до VLAN 10, виконавши команду switchport access vlan [vlan_id]:

Switch(config-if)#switchport access vlan 10

2.9 Повторюю кроки 2.1 та 2.5-2.7 для налаштування портів світча, що під'єднанні до таких кінцевих пристроїв: PC 8 та PC 9:

Switch(config)#vlan 20
Switch(config-vlan)#name VLAN20
Switch(config-vlan)#vlan 30
Switch(config-vlan)#name VLAN30
Switch(config-vlan)#int fa 3/1
Switch(config-if)#sw m acc
Switch(config-if)#sw acc vlan 20
Switch(config-vlan)#int fa 2/1
Switch(config-if)#sw m acc
Switch(config-if)#sw acc vlan 30

2.10 Виконаємо крок 2.1 для визначення порту світча, що під'єднаний до іншого світча. Даний порт буде налаштований у trunk-режимі. Для цього у режимі глобального конфігурування світча зайдемо на цей порт, виконавши команду interface [interface_id]:

Switch(config)#interface fa 0/1

2.11 Для налаштування порту у trunk-режимі виконаємо команду switchport mode trunk:

Switch(config-if)#switchport mode trunk

2.12 Задам порту світча FastEthernet 0/1 режим trunk та приналежність до VLAN 40, виконавши команду switchport trunk native vlan 40:

На цьому конфігурування світча завершене.

Приклад виконання кроків 2.2-2.11 зображений на рисунку 5.11

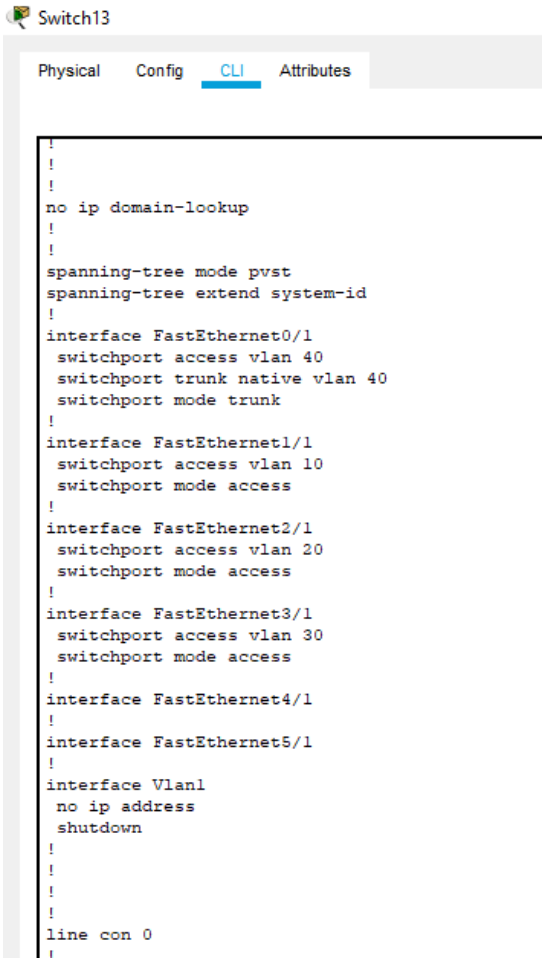


Рисунок 5.11 – Налаштування світча

2.13 Повторимо кроки 2.1-2.12 для світчів, що з’єднують наступні кінцеві пристрої.

До світчів Switch10 та Switch11 не під’єднано жодного кінцевого пристрою, а отже достатньо лише налаштувати порти у trunk-режимі. Для цього виконаємо кроки 2.1-2.4 та 2.10-2.12 для кожного порту кожного із перерахованих світчів. Приклад налаштування світча Switch10 наведений на рисунку 5.12.

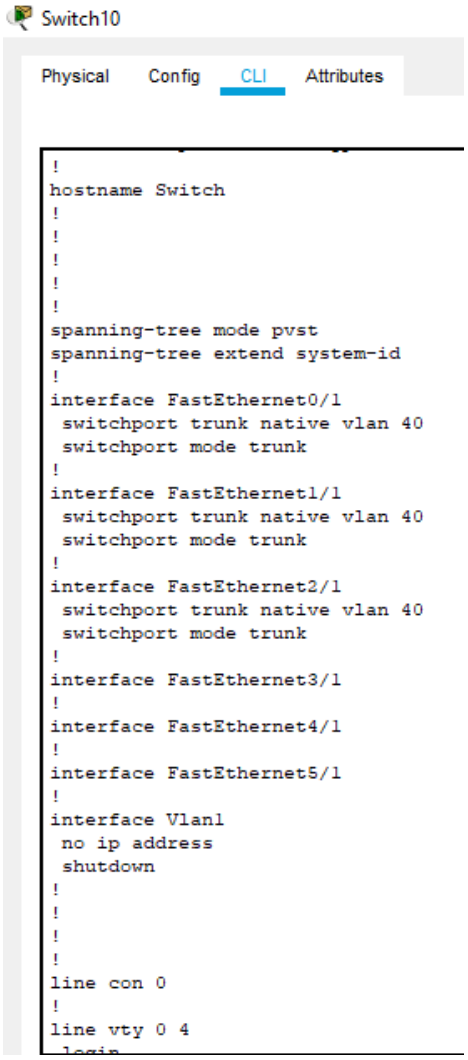


Рисунок 5.12 – Налаштування trunk-з’єднань на світчеві Switch10

3. Переходимо до конфігурування маршрутизатора. Проаналізувавши схему, можна побачити, що між світчем та роутером використовується лише одне з’єднання, при наявних трьох віртуальних локальних мереж. Робимо висновок, що інтерфейс роутера працює у trunk-режимі. Отже для реалізації inter-VLAN роутингу необхідно використовувати підхід Router-on-a-stick.

3.1 Перший крок - визначення порта роутера, що з’єднаний із світчем. З рисунку 5.13 можна бачити, що це порт FastEthernet0/0.

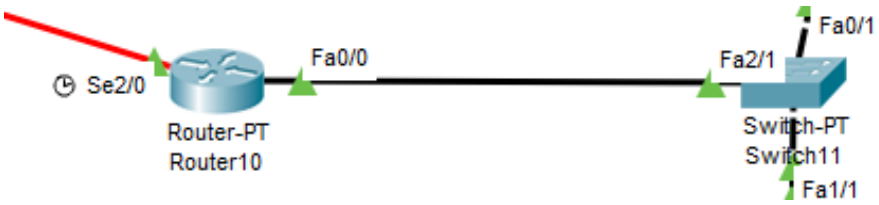


Рисунок 5.13– Роутер з’єднаний з світчем

3.2 Заходимо у засіб налаштування IOS Command Line Interface у маршрутизаторі Router0.

3.3 За замовчуванням стоїть користувацький режим конфігурування. Ввійдемо у привілейований режим за допомогою команди enable:

Router>enable

3.4 Ввійдемо у режим глобального конфігурування маршрутизатора за допомогою команди configure terminal:

Router#configure terminal

3.5 Для налаштування одного інтерфейсу (порту) роутера у якості trunk-з’єднання, потрібно створити у ньому кілька підінтерфейсів (у даному випадку –три підінтерфейси). Для створення підінтерфейсу необхідно виконати команду interface [interface_id.Subinterface_id]. Створимо підінтерфейс для віртуальної локальної мережі під номером 10:

Router(config)#interface fa0/0.10

3.6 Після створення підінтерфейсу, йому привласнюється номер віртуальної локальної мережі, використовуючи команду encapsulation dot1q [vlan_id]:

Router(config-subif)#encapsulation dot1q 10

3.7 Далі потрібно призначити підінтерфейсу його IP-адресу. Для цього використаємо команду ip address [ip_address subnet_mask]:

Router(config-subif)#ip add 221.22.10.5 255.255.255.0

3.8 Повторюю кроки 3.5-3.7 для створення інших підінтерфейсів для інших віртуальних LAN.

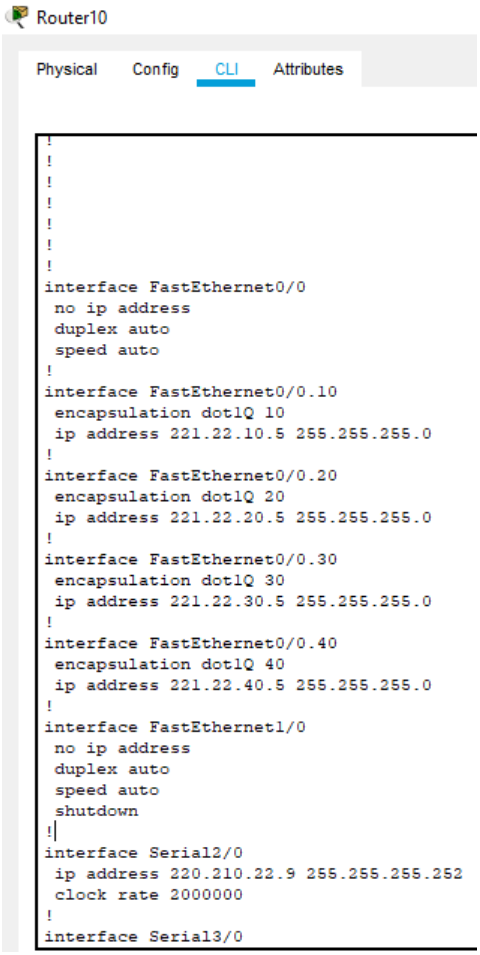
3.9 Після конфігурування підінтерфейсів необхідно ввімкнути інтерфейс. Для цього використовуємо наступні команди interface [interface_id] та no shutdown:

Router(config-subif)#interface fa0/0

Router(config-if)#no shutdown

3.10 На цьому конфігурування роутеру у режимі Router-on-a-stick завершено.

Конфігурування роутера Router10 зображене на рисунку 5.14



Рсиунок 5.14 – Конфігурування роутера у мережі колл-центру

Перевіряю роботу мережі, спробувавши передати пакети від різних кінцевих пристроїв до будь-яких інших. Результат роботи мережі зображений на рисунку 5.15.

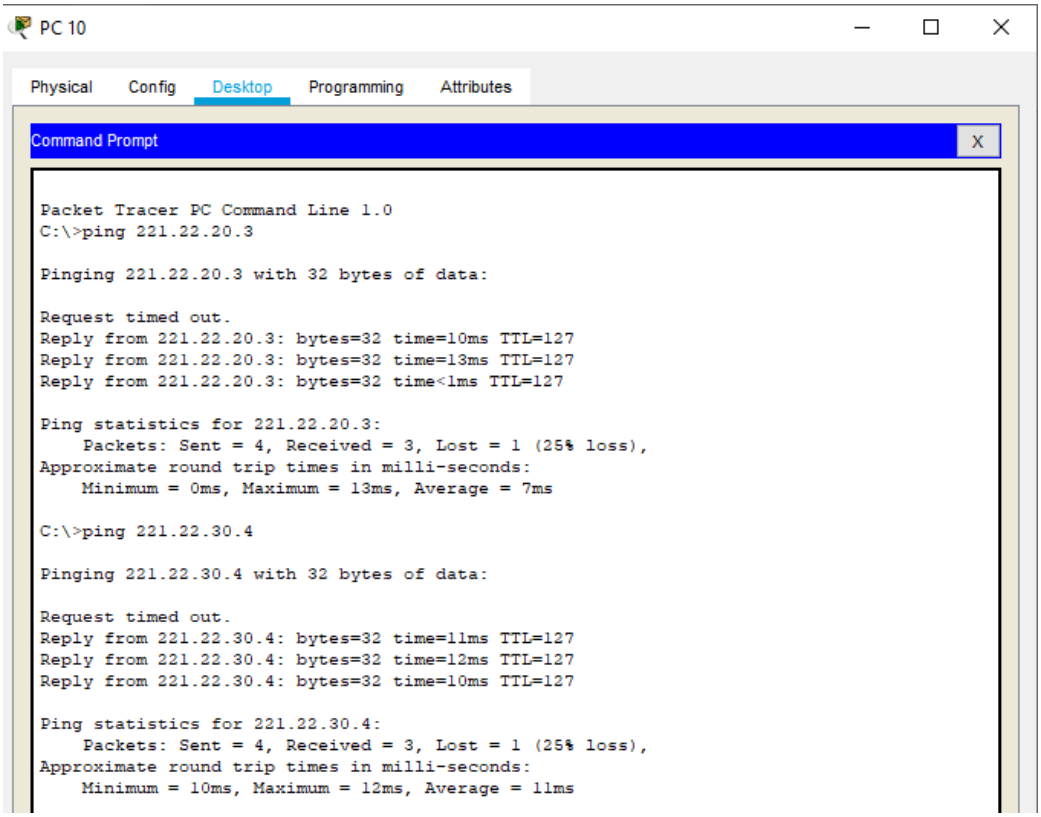


Рисунок 5.15 – Результат роботи мережі

На цьому проектування мережі диспетчерського центру завершене.

5.4 З’єднання частин корпоративної мережі

Розробити комп’ютерну мережу, що складається з 3 локальних мереж (центральний офіс, віддалений офіс, диспетчерський центр), з’єднаних serial з’єднаннями.

5.4.1 Хід налаштування

У центральному офісі – LAN1 – для адресації мереж та вузлів використовувати маски змінної довжини та статичну маршрутизацію; у віддаленому офісі – LAN2 – маски фіксованої довжини, динамічну

маршрутизацію; у LAN3 – налаштувати віртуальні локальні мережі та Inter-VLAN routing.

У кожній із мереж виберемо по одному роутеру, який і буде з'єднуватись з центральним роутером. У мережі центрального офісу візьмемо роутер, що виступає загальним роутером для мережі. У мережі диспетчерського центру є тільки один роутер, який ми і беремо. У мережі віддаленого офісу усі роутери рівні, тому берем будь-який. За умовою всі мережі підєднуються до одного роутера. Змоделюємо це у середовищі Packet Tracer. Також потрібно налаштувати IP-адреси на роутерах для послідовних з'єднань. Цей крок показаний на рисунку 5.16.

Схема всієї з'єднаної мережі зображена в додатку Б.

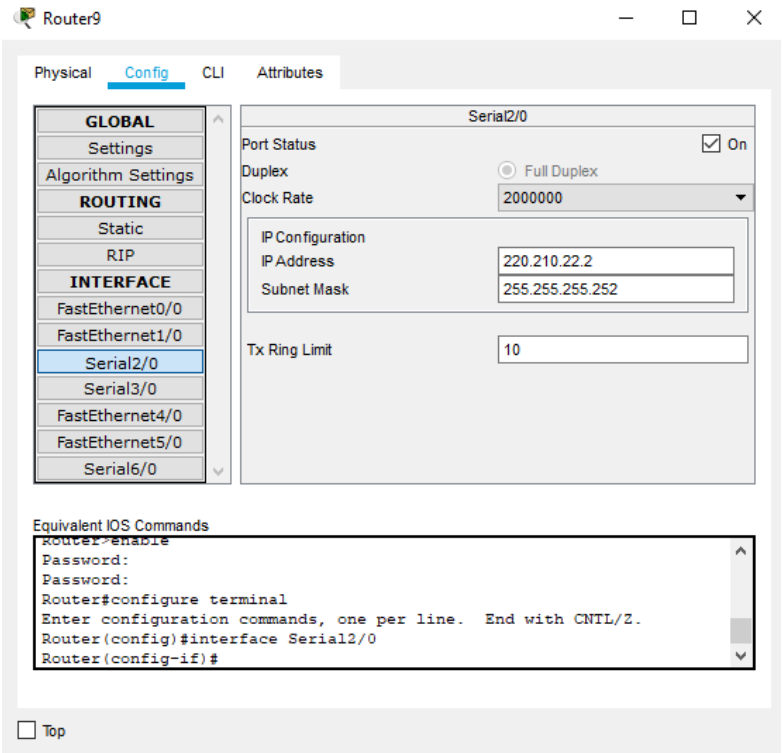


Рисунок 5.16 – Налаштування IP-адреси для послідовного з'єднання на роутері

Для головних роутерів LAN1 та LAN2 прописуємо статичну маршрутизацію за замовчуванням з некстхопом на центральному (загальному) роутері. На рисунках 5.17 показана таблиця маршрутизації Router0.

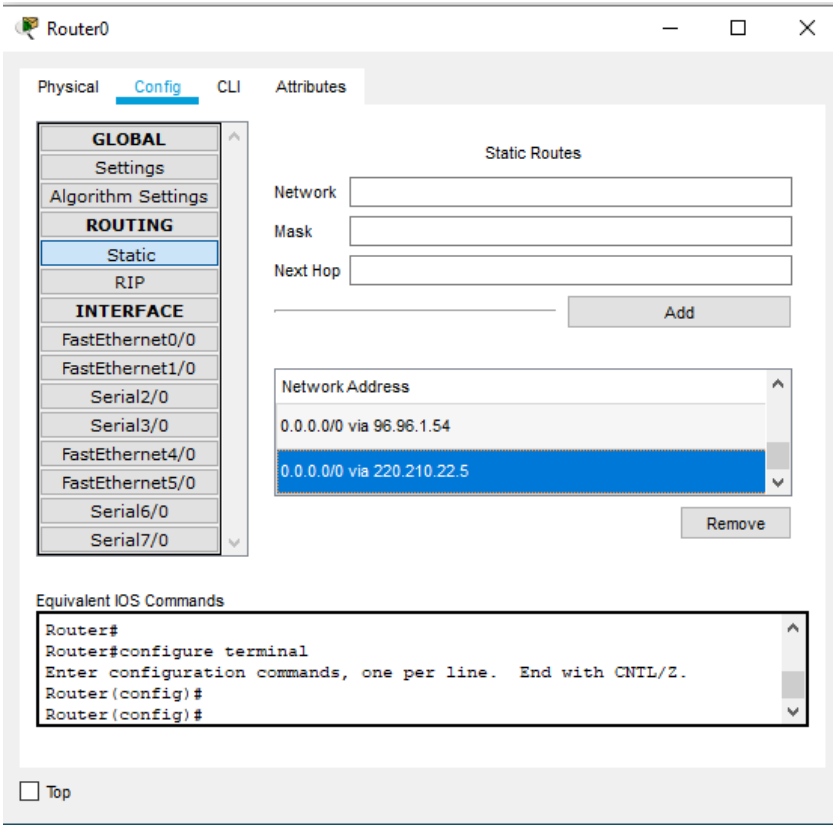


Рисунок 5.17 – Доданий маршрут за замовчуванням в таблиці маршрутизації LAN1

На центральному роутері потрібно прописати маршрути до роутерів LAN1 та LAN2, використовуючи сумаризований IP-адрес. Результати на рисунку на 5.18.

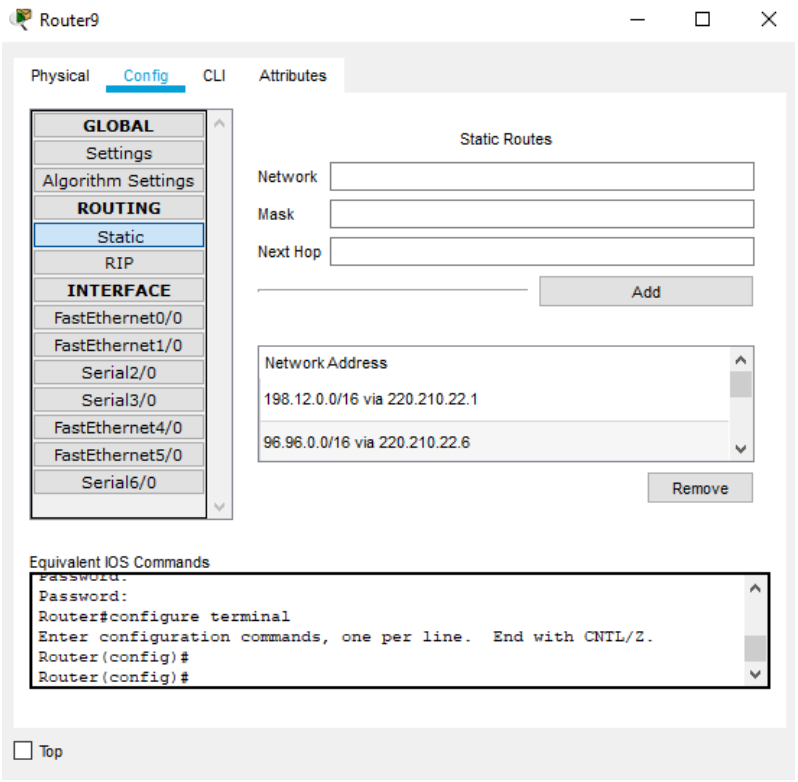


Рисунок 5.18 – Маршрути до роутерів LAN1 та LAN2 з сумаризованою адресою.

На головному роутері LAN2 за допомогою команди default information-originate потрібно поширити статичний маршрут між роутерами.Результати на рисунку 5.19

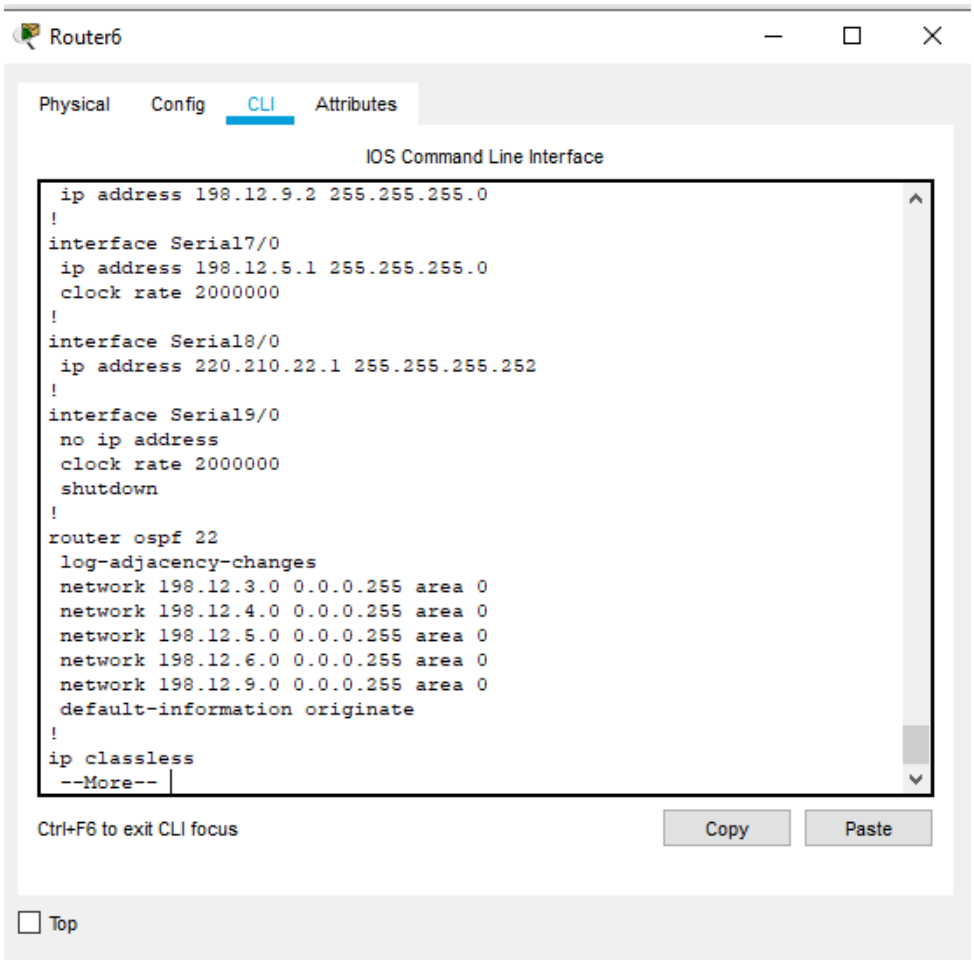


Рисунок 5.19 – Використання команди default information-originate

Останнім кроком є підключення LAN3. Тут потрібно на центральному та LAN3 роутерах прописати маршрути за замовчуванням один до одного. Цей крок показаний на рисунку 5.20 та рисунку 5.21.

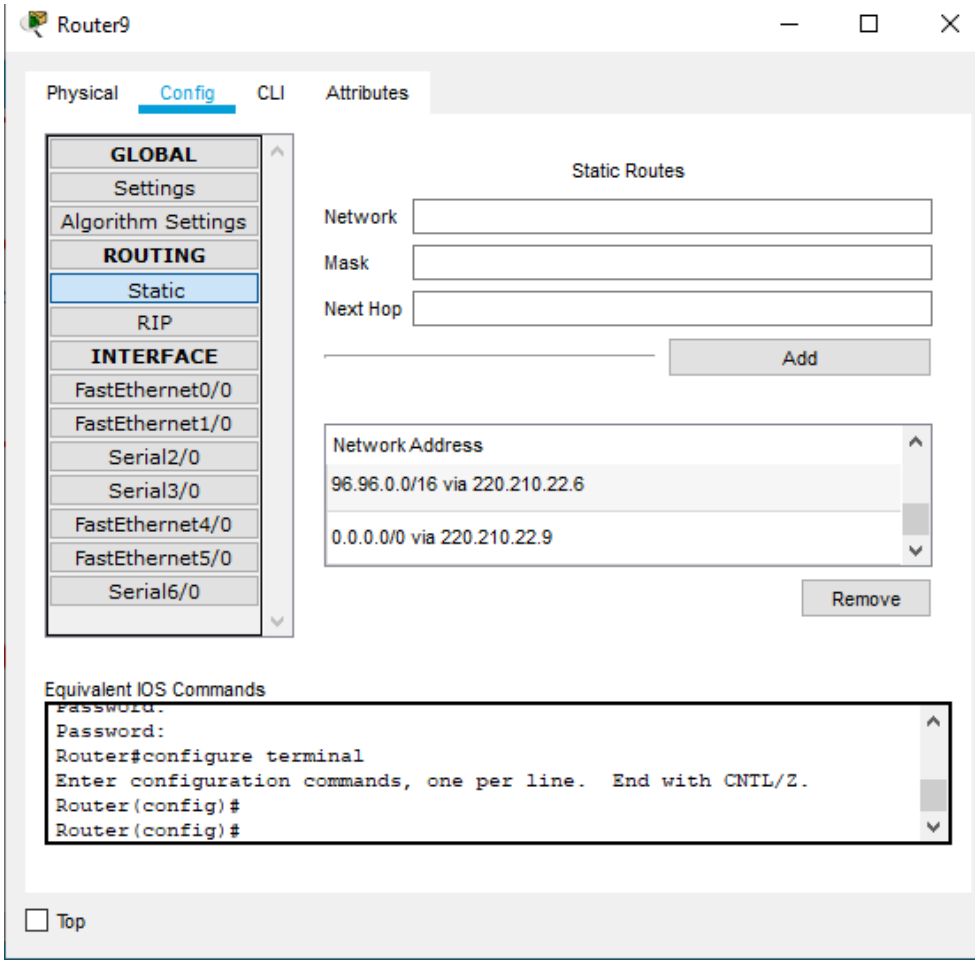


Рисунок 5.20 – Маршрут за замовчуванням на LAN3 маршрутизатор в головному маршрутизаторі

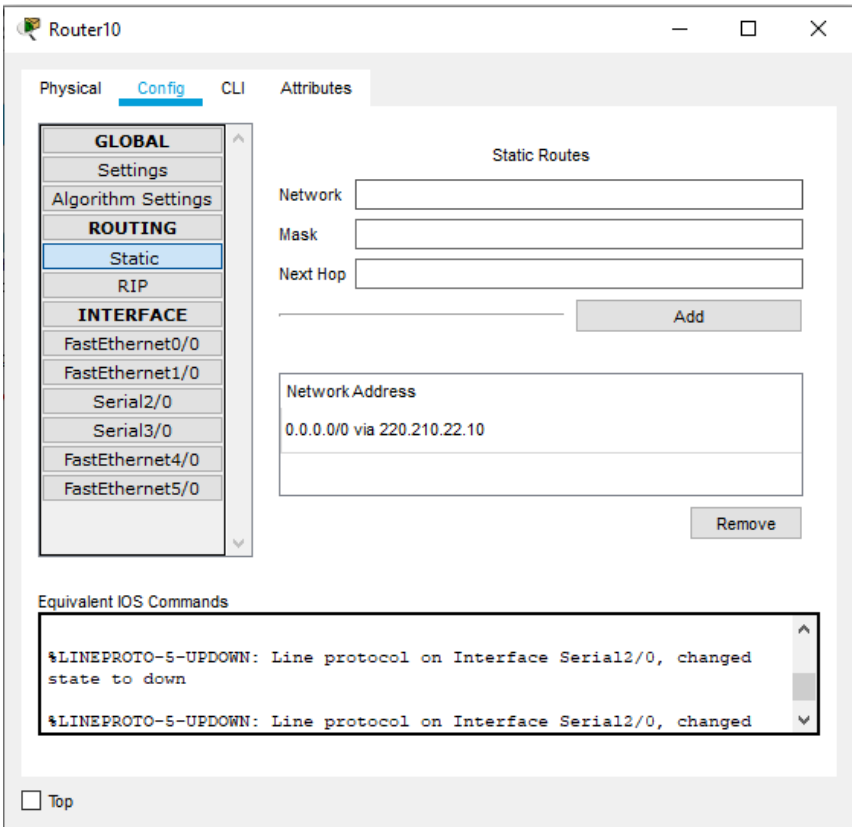


Рисунок 5.21 – Налаштування статичних маршрутів для Router10

Перевірю взаємодію мереж, змоделювавши їхню роботу. Для цього передам дані із різних кінцевих пристроїв до будь-яких інших. Результат зображений на рисунку 5.22.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	PC8	PC4	ICMP		0.000	N	0	(edit
	Successful	PC9	PC2 0	ICMP		0.000	N	1	(edit
	Successful	PC9	PC 6	ICMP		0.000	N	2	(edit

Рисунок 5.22 – Робота всієї мережі

5.5 Встановлення захисту від вільного доступу на роутері

На мережевому обладнанні (світчі, роутери) слід встановлювати паролі для запобігання вільного доступу до керування пристроєм третіми особами.

Встановимо на центральному роутері (Router 9) пароль на привілейований режим (рисунок 5.23) .

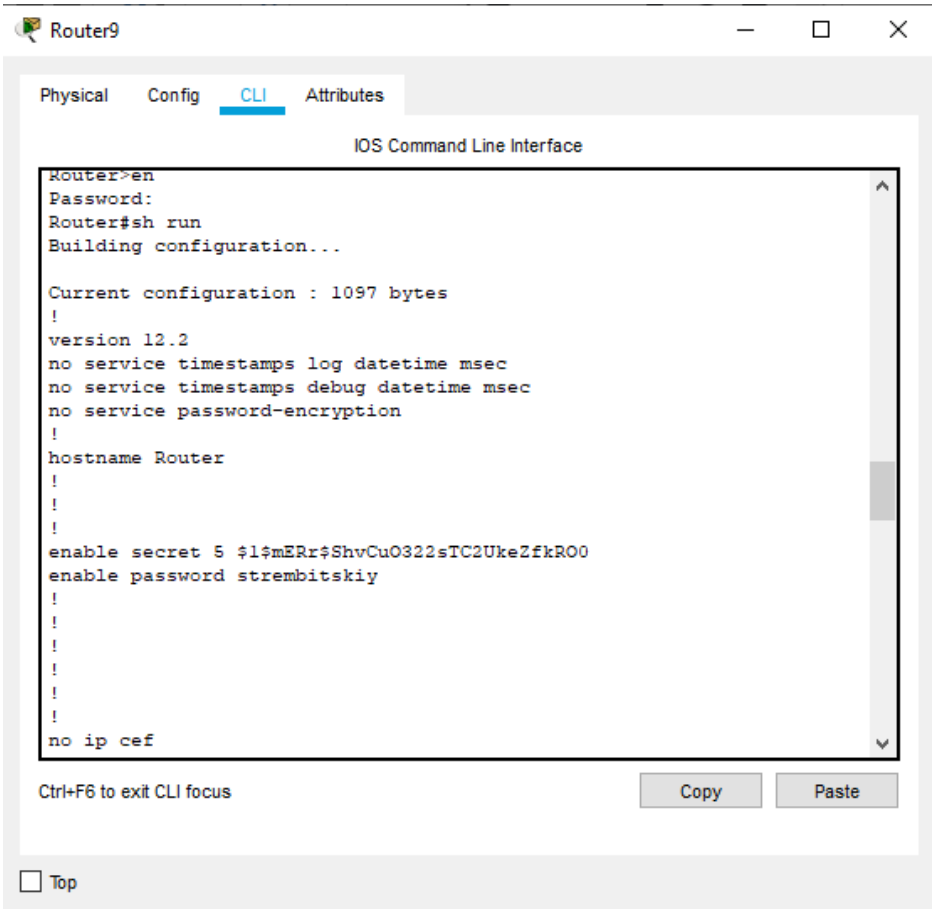


Рисунок 5.23 – Встановлення паролю на привілейований режим

При наступній спробі війти у привілейований режим, буде запитаний пароль (рисунок 5.24).

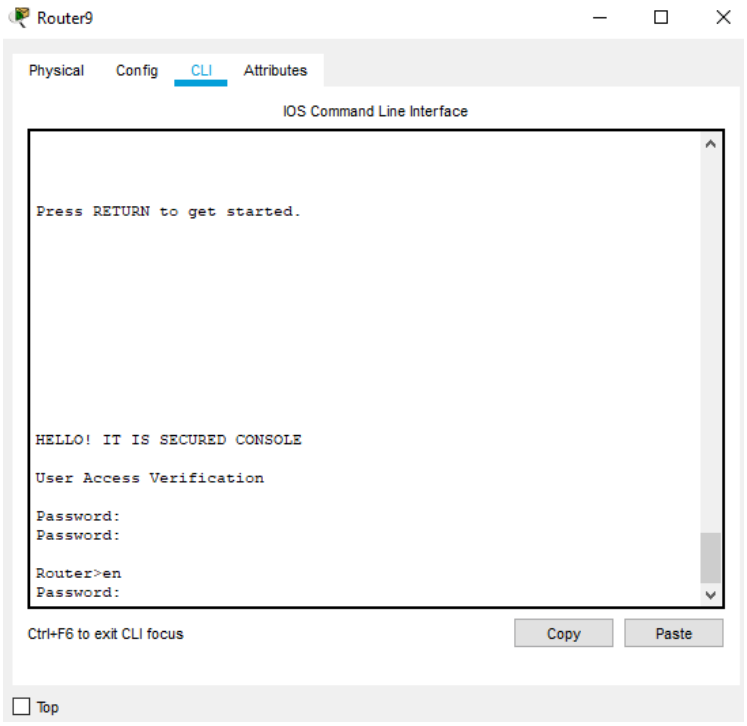


Рисунок 5.24 – При спробі війти у привілейований режим, користувача запитають пароль

Встановимо секретний ключ доступу та пароль на консоль (Рисунок 5.25). Слід зазначити, що секретний ключ «перекриває» дію звичайного паролю на привілейований режим доступу.

Секретний ключ дає змогу у майбутньому скинути налаштування мережевого пристрою.

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#enable secret pavlo
Router(config)#line console 0
Router(config-line)#password pav
Router(config-line)#login
Router(config-line)#ex
% Ambiguous command: "ex"
Router(config-line)#exit
Router(config)#
```

Рисунок 5.25 – Встановлення секретного слова та паролю на консоль

Для того щоб звичайний користувач розумів, що він потрапив у панель керування пристроєм, додамо напис (банер-привітання) (рисунок 5.26, рисунок 5.27).

Такий напис повинен повідомити користувача про те, що він потрапив у захищене вікно консолі, і якщо йому не відомі реквізити доступу, він не зможе нічого налаштувати

За замовчування такий напис відсутній.

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#enable secret pavlo
Router(config)#line console 0
Router(config-line)#password pav
Router(config-line)#login
Router(config-line)#ex
% Ambiguous command: "ex"
Router(config-line)#exit
Router(config)#banner m
% Incomplete command.
Router(config)#banner motd #HELLO! IT IS SECURED CONSOLE#
Router(config)#ex
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Рисунок 5.26 – Встановлення банеру-привітання

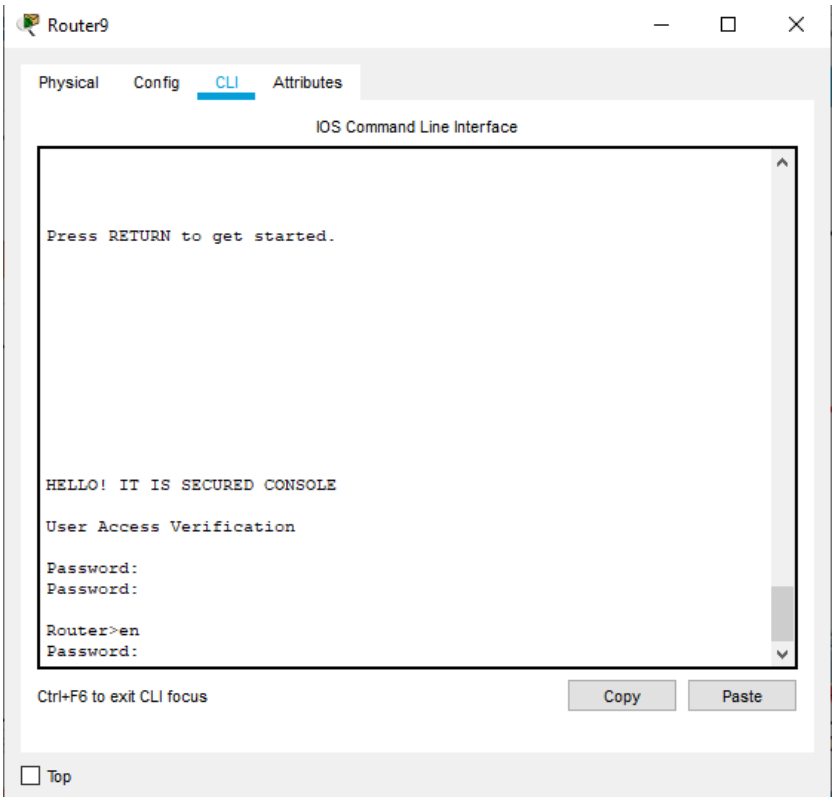


Рисунок 5.27 – Демонстація банеру-привітання

За замовчуванням усі паролі зберігається у відкритому вигляді (рисунок 5.28). Після введення паролів, треті особи можуть фізично отримати доступ до мережевого пристрою та його консолі і без складних зусиль ввести команду show run для перегнгляду усіх паролів.

Якщо флеш-пам’ять мережевого пристрою не зашифрована і паролі знаходяться у відкритому вигляді, то фізично отримавши доступ до флеш-пам’яті можна також отримати паролі доступу.

Для більшої надійності потрібно їх зашифрувати за допомогою команди service password-encryption (рисунок 5.29).

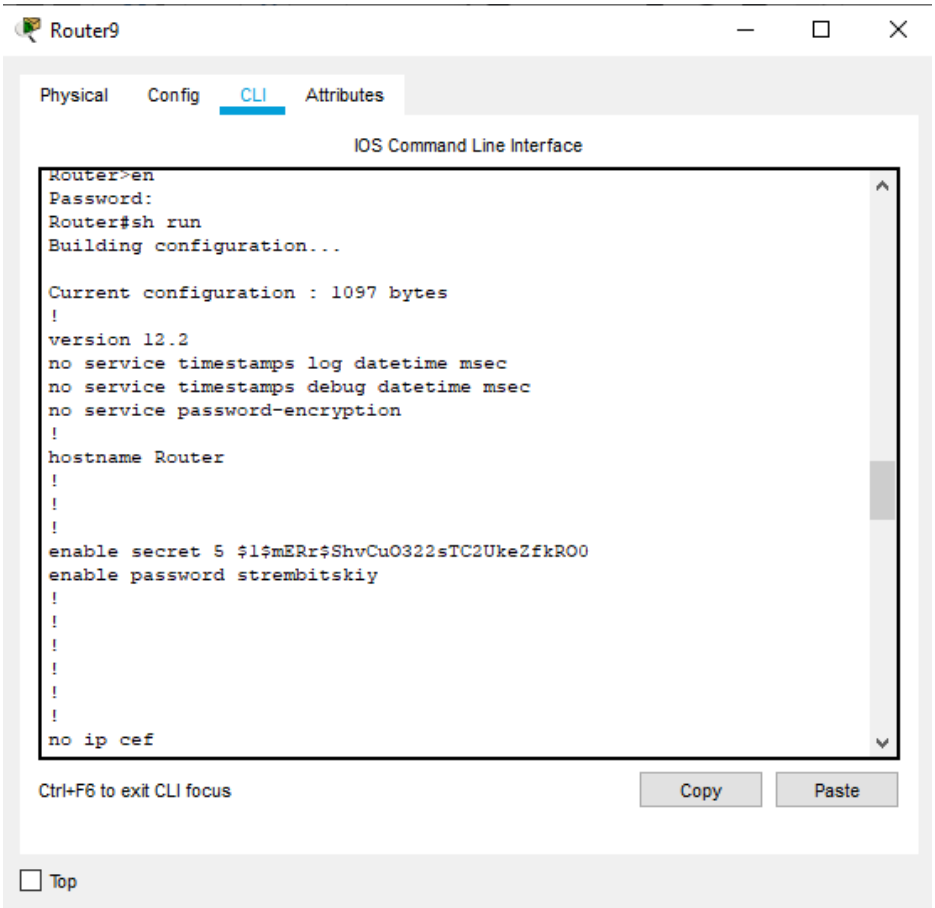


Рисунок 5.28 – Зберігання паролю у відкритому вигляді

Слід зазначити, що усі паролі можливо зашифрувати без зворотного процесу.

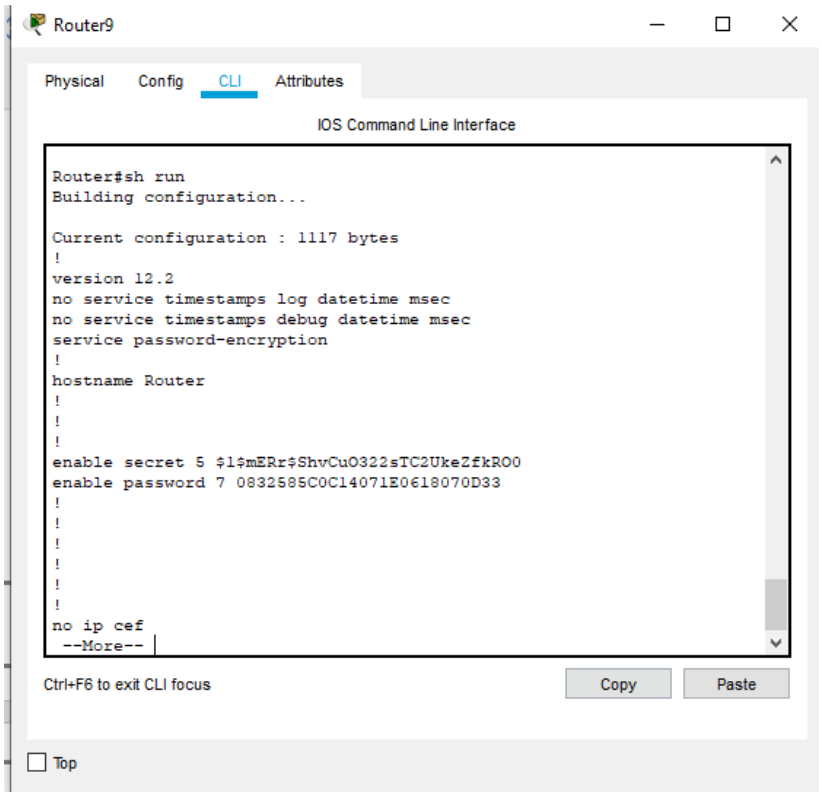


Рисунок 5.29 – Встановлення шифрування усіх паролів доступу

ВИСНОВКИ

У дипломній роботі було спроектовано захищену комп'ютерну мережу для підприємства з декількома філіями. Проект був змодельований в симуляторі Cisco Packet Tracer. Cisco Packet Tracer є зручним засобом проектування віртуальних мереж, дозволяючи створювати образи як нечисленних фізичних пристроїв, так і складних топологій, що включають в себе тривалу настройку конфігурацій.

Були всебічно вивчені і проаналізовані теоретичні відомості, які стосуються комп'ютерних мереж в загальному та способів захисту мережі. Також було проаналізовано, які актуальні на даний момент існують симулятори розробки комп’ютерних мереж, для того щоб обрати найбільш підходящий симулятор.

Завдання побудови віртуальної захищеної мережі вимагає комплексного підходу, врахування всіх тонкощів, особливостей роботи устаткування і глибоких системних знань з побудови мереж в цілому.

Мною була розроблена комп'ютерна мережа, що складається з трьох локальних обчислюваних мереж (LAN).

Перша локальна мережа – мережа центрального офісу з статичною маршрутизацією, яка складалася з 4 роутерів, 195 хостів та 8 підмереж з масками змінної довжини, що дозволяли оптимально використати адресний простір. Всі, крім «центрального» роутера, мали статичну маршрутизацію за замовчуванням (default route) через «центральний» роутер. Центральний роутер у своїй таблиці маршрутизації містив інформацію про статичні маршрути до інших підмереж цієї LAN та один статичний маршрут за замовчуванням для зв’язку з іншими мережами.

Друга локальна мережа – мережа віддаленого офісу з динамічною маршрутизацію за допомогою протоколу OSPF, складалася з 5 роутерів, 11 підмереж з 210 хостами у кожній. Використовувались маски фіксованої

довжини. Протокол динамічної маршрутизації дозволяв зручно керувати мережою та «розповідати» одній підмережі про інші.

Третя локальна мережа – мережа диспетчерського центру, що складалась з 3 віртуальних підмереж (VLAN), які «спілкувалися» між собою через роутер (inter vlan routing). VLAN дозволяла створювати декілька віртуальних підмереж, фізично розташованих у одній мережі, використовувати спільне середовище передачі даних. Це дозволяло зберегти кошти на мережеве обладнання (роутери, кабелі).

Ці три мережі були з’єднанні між собою за допомогою послідовних з’єднань через один «центральний» роутер, на якому налаштована статична маршрутиція цих мереж.

В ході розробки даного проекту було отримано знання про мережеве обладнання, його функціональне призначення, принципи роботи з ним та взаємодіють між собою. Під час виконання поставлених задач було отримано корисні навички налаштування мереж, які хоч і віртуальні, але наближені до реальності, що дасть можливість в подальшому швидше адаптуватись до реального налаштування та роботи з мережами.

ПЕРЕЛІК ПОСИЛАНЬ

1. Офіційний сайт компанії Cisco Packet Tracer (Електронний ресурс) Режим доступу: URL: https://www.cisco.com/
2. Стрембіцький П.П., Софина О.Ю. Створення імітаційної моделі мережі Ethernet з логічною сегментацією на основі VLAN у програмному середовищі Cisco Packet Tracer / науково-практична конференція «проблеми комп’ютерної інженерії» Державного Університету Телекомунікацій, кафедра комп’ютерної інженерії (2022)
3. В. Оліфер, Н. Оліфер Комп'ютерні мережі. Принципи, технології, протоколи – 5 видання (2016).
4. Керівництво за технологіями об'єднаних мереж. 4 видання. - М .: Вільямс, 2005
5. Протоколи передачі даних: що це, які бувають і в чому відмінності? (Електронний ресурс). Режим доступу: URL: https://tproger.ru/explain/protokoly-peredachi-dannyh-chto-jeto-kakiebyvajut-i-v-chjom-razlichija/
6. У. Одом "Офіційне керівництво Cisco по підготовці до сертифікаціонним іспитів CCNA ICND2 200-101. Маршрутизація і комутація" (2016)
7. Боршевніков, А. Е. Мережеві атаки. Види. Способи боротьби (2011)
8. Новини в світі технологій (Електронний ресурс). Режим доступу: URL: https://www.internet-technologies.ru/
9. Офіційний сайт емулятора GNS 3 (Електронний ресурс). Режим доступу: URL: https://gns3.com/
10. Офіційний сайт емулятора SNMP Agent Simulator (Електронний ресурс). Режим доступу: URL: https://veraxsystems.com/
11. Трояновська Т.І. Комп’ютерні системи та мережі», навчальний посібник для студентів 4 курсу усіх форм навчання спеціальності

5.05010201 «Обслуговування комп'ютерних систем та мереж» – Вінниця 2013 - 215 с.

12. Браун С. Віртуальні приватні мережі / Браун Сімеон - М.: Лорі, 2009. - 502с.
13. Нанс. Б. Комп’ютерні мережі: пер. з англ. / Нанс Бернард- М.: БИНОМ, 2006. - 400 с.
14. Петров А.А Комп’ютерна безпека. Криптографічні методи захисту / Петров Олексій. - М.: ДМК, 2010. - 448 с.
15. Методичні вказівки до практичних занять з дисциплін «Телекомунікаційні та інформаційні мережі», «Інтегральні цифрові мережі зв’язку» (розподіл IP-адрес) / С. І. Приходько, О. С. Жученко, К. А. Трубчанінова, С. С. Єременко. – Харків : УкрДАЗТ, 2012. – 42 с.
16. Center for Internet Security – Cybersecurity Threats [Електронний ресурс] / Center for Internet Security – Режим доступу: https://www.cisecurity.org/cybersecuritythreats/
17. Корпань Я.В. Класифікація загроз інформаційній безпеці в комп’ютерних системах при віддаленій обробці даних. Реєстрація, зберігання і обробка даних. 2015. Т.17. №2. (Електронний ресурс). Режим доступу: URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/ 131565/04-Korpan.pdf?sequence=1.
18. Про захист інформації в інформаційно-телекомунікаційних системах. Закон України від 19.04.2014 р. № 80/94-ВР. (Електронний ресурс). Режим доступу: URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80
19. Глоба Л.С. Розробка інформаційних ресурсів та систем : підручник. Київ : Політехніка, 2013. 380 с.
20. Кузнецова М.Г. Застосування механізмів підвищення живучості для забезпечення захищеності інформаційного ресурсу в розподілених системах. Реєстрація, зберігання і обробка даних. 2006. Т.8. №3. С. 40-

47. (Електронний ресурс). Режим доступу: URL: http://dspace.nbuv.gov.ua/handle/123456789/50851.

21. Романюк Б.В., Гавловський В.Д., Гуцалюк М.В., Бутузов В.М. Виявлення та розслідування злочинів, що вчиняються у сфері інформаційних технологій: наук.-практ. посіб. / за заг ред. проф. Я. Ю. Кондратьева. Київ, 2004. 144 с.
22. Бакін Д.С. Проблеми захисту інформації в комп'ютерних мережах: матеріали всеукр. наук.-практ. конф., м. Кропивницький, 23-25 листопада 2016 р. Кропивницький, 2016. С. 79-80. URL: http://dspace.kntu.kr.ua/jspui/bitstream/123456789/5101/1/AUConference CyberSecurity_November2016_p79.pdf
23. Про основні засади забезпечення кібербезпеки України: Закон України від 08.07.2018 р. № 2163-VIII. (Електронний ресурс). Режим доступу: URL: https://zakon.rada.gov.ua/laws/show/2163- 19#Text
24. Бухарєв В.В. Адміністративно-правові засади забезпечення кібербезпеки України: дис. ... канд. юр. наук : 12.00.07 / Сумський державний університет. Суми, 2018. 221 с.
25. Важинський С.Е. Щербак Т.І. Методика та організація наукових досліджень : навч. посіб. Суми : СумДПУ імені А.С. Макаренка, 2016. 260 с.
26. Jozef Janitor, Karol Kniewald. Visual Learning Tools for Teaching / Learning Computer Networks : Sixth International Conference on Networking and Services, 2010. P. 351-355.
27. Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network. (Електронний ресурс). Режим доступу: URL : http://index-of.es/EBooks/German/Hacking/maximum_security.pdf.
28. Матов О.Я., Василенко В.С. Модель загроз у розподілених мережах. Реєстрація, зберігання і обробка даних. 2008. Т.10. №1. С. 91-102.
29. Болехівський Н. Полотай О. Класифікація мережевих атак та методи протидії і ззахисту. (Електронний ресурс). Режим доступу: URL :

https://sci.ldubgd.edu.ua/bitstream/handle/123456789/6737/1.pdf?sequence=1&isAllowed=y.

30. Социальная инженерия – как не стать жертвой. (Електронний ресурс). Режим доступу: URL : https://efsol.ru/articles/social-engineering.html
31. Отличие межсетевого екрана от маршрутизатора (Firewall vs Router). (Електронний ресурс). Режим доступу: URL : http://blog.netskills.ru/2014/03/firewall-vs-router.html

ДОДАТКИ

ПРОТОКОЛ
ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ
НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: «Створення імітаційної моделі мережі Ethernet з логічною сегментацією на основі VLAN у програмному середовищі Cisco Packet Trace»

Тип роботи: Магістерська кваліфікаційна робота
(БДР, МКР)

Підрозділ КСУ, ФІТА
(кафедра, факультет)

Показники звіту подібності Unicheck

Оригінальність 88,5% Схожість 11,5%

Аналіз звіту подібності (відмітити потрібне)

☐ Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату.
☐ Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її автора. Роботу направити на розгляд експертної комісії кафедри.
☐ Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа, відповідальна за перевірку _____ Галущак А.В.
(підпис) (прізвище, ініціали)

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

Автор роботи _____ Стрембіцький П.П.
(підпис) (прізвище, ініціали)

Керівник роботи _____ Софина О.Ю.
(підпис) (прізвище, ініціали)

Додаток А
(обов'язковий)

ВНТУ

ЗАТВЕРДЖЕНО
Зав. кафедри КСУ ВНТУ,
д.т.н., доцент
_____В'ячеслав КОВТУН
"03" січня 2022 р.

ТЕХНІЧНЕ ЗАВДАННЯ

на виконання магістерської кваліфікаційної роботи

Створення імітаційної моделі мережі Ethernet з логічною сегментацією на основі VLAN у програмному середовищі Cisco Packet Tracer

(тема)

08-33.МКР.32.00.000 ТЗ
номер

Студент групи ЗАКІТ-21м

Підпис Павло СТРЕМБІЦЬКИЙ
Ім'я ПРІЗВИЩЕ

Керівник Ольга СОФИНА

Підпис Ім'я ПРІЗВИЩЕ

Вінниця 2022

1. Назва та галузь застосування

1.1. Назва – Створення імітаційної моделі мережі ethernet з логічною сегментацією на основі vlan у програмному середовищі cisco packet tracer

1.2. Галузь застосування – комп’ютерні мережі.

2. Підстава для проведення розробки.

Тема магістерської кваліфікаційної роботи затверджена наказом по ВНТУ від “14” вересня 2022 року №203

3. Мета та призначення розробки.

Метою магістерської кваліфікаційної роботи є підвищення безпеки комп’ютерної мережі підприємства.

4. Джерела розробки.

Магістерська кваліфікаційна робота виконується вперше. В ході проведення розробки повинні використовуватись такі документи:

1. Офіційний сайт компанії Cisco Packet Tracer (Електронний ресурс) Режим доступу: URL: https://www.cisco.com/

2. В. Оліфер, Н. Оліфер Комп'ютерні мережі. Принципи, технології, протоколи – 5 видання (2016).

3. Керівництво за технологіями об'єднаних мереж. 4 видання. - М .: Вільямс, 2005

4. Протоколи передачі даних: що це, які бувають і в чому відмінності? (Електронний ресурс). Режим доступу: URL: https://tproger.ru/explain/protokoly-peredachi-dannyh-chto-jeto-kakiebyvajut-i-v-chjom-razlichija/

5. У. Одом "Офіційне керівництво Cisco по підготовці до сертіфікаціонним іспитів CCNA ICND2 200-101. Маршрутизація і комутація" (2016)

5. Вимоги до розробки.

5.1. Перелік головних функцій:

- мережа змодельована в симуляторі Cisco Packet Tracer;
- захищена мережа;
- використані різні протоколи маршрутизації;
- показано способи створення віртуальних мереж.

5.2. Основні технічні вимоги до розробки:

- розробити комп’ютерну мережу;
- розрахувати адресний простір для мереж LAN1-LAN3;
- створити конфігураційні файли для всіх мережевих пристроїв;
- виконати моделювання мережі засобами Packet Tracer.

6. Стадії та етапи розробки.

6.1 Пояснювальна записка:

1. Аналіз методів, принципів, підходів і засобів реалізації задачі автоматизації процесами в об’єкті управління відповідно до теми кваліфікаційної роботи. Постановка задач дослідження «03» 09 2022 р.
2. Удосконалення технології прийняття рішень при автоматизації об’єкту управління «15 » 09 2022 р.
3. Визначення технічних характеристик системи «09» 10 2022 р.
4. Розробка програмного забезпечення системи «24» 10 2022 р.

6.2 Графічні матеріали:

1. Розробка імітаційної моделі мережі Ethernet з логічною сегментацією на основі VLAN «04» 11 2022 р.
2. Розробка та проектування комп’ютерної мережі «12» 11 2022 р.
3. Тестування комп’ютерної мережі «15» 11 2022 р.

7. Порядок контролю і приймання.

7.1. Хід виконання роботи контролюється керівником роботи. Рубіжний контроль провести до «28» 11 2022 р.

7.2. Атестація МКР здійснюється на попередньому захисті. Попередній захист магістерської кваліфікаційної роботи провести до «16» 12 2022 р.

7.3. Підсумкове рішення щодо оцінки якості виконання роботи приймається на засіданні ЕК. Захист магістерської кваліфікаційної роботи провести до «23» 12 2022 р.

Додаток Б
(обов'язковий)

ІЛЮСТРАТИВНА ЧАСТИНА

Створення імітаційної моделі мережі ethernet з логічною сегментацією на основі vlan у програмному середовищі cisco packet tracer
(тема)

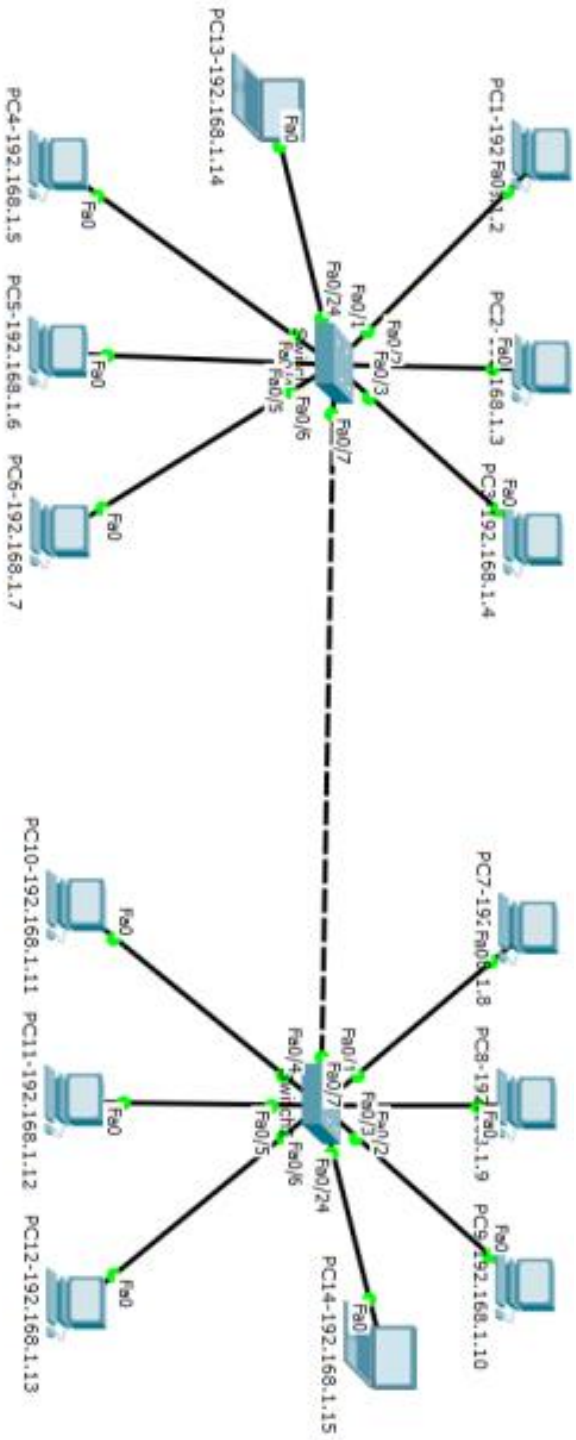
Студент групи 3АКІТ21м

Павло СТРЕМБІЦЬКИЙ
Підпис *Ім'я ПРІЗВИЩЕ*

Керівник

Ольга СОФИНА
Підпис *Ім'я ПРІЗВИЩЕ*

Схема імітаційної моделі мережі Ethernet з логічною сегментацією на основі VLAN



Структурна схема мережі

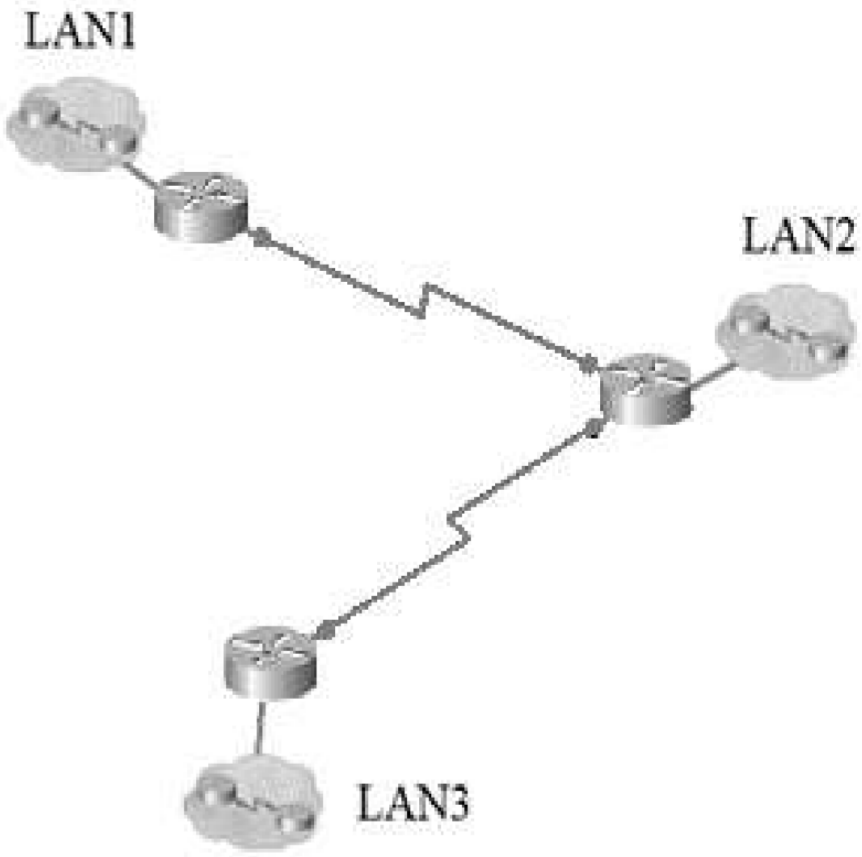
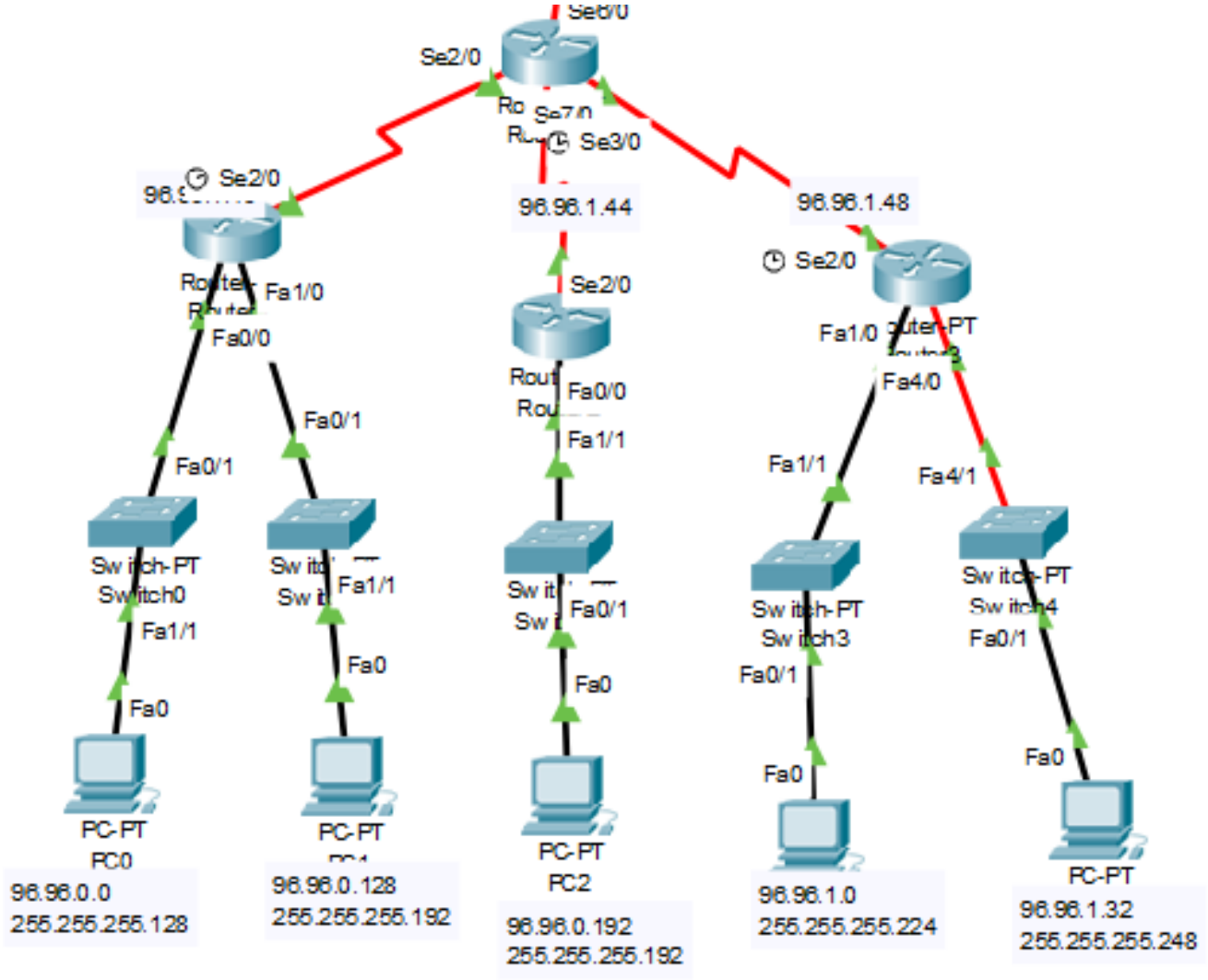
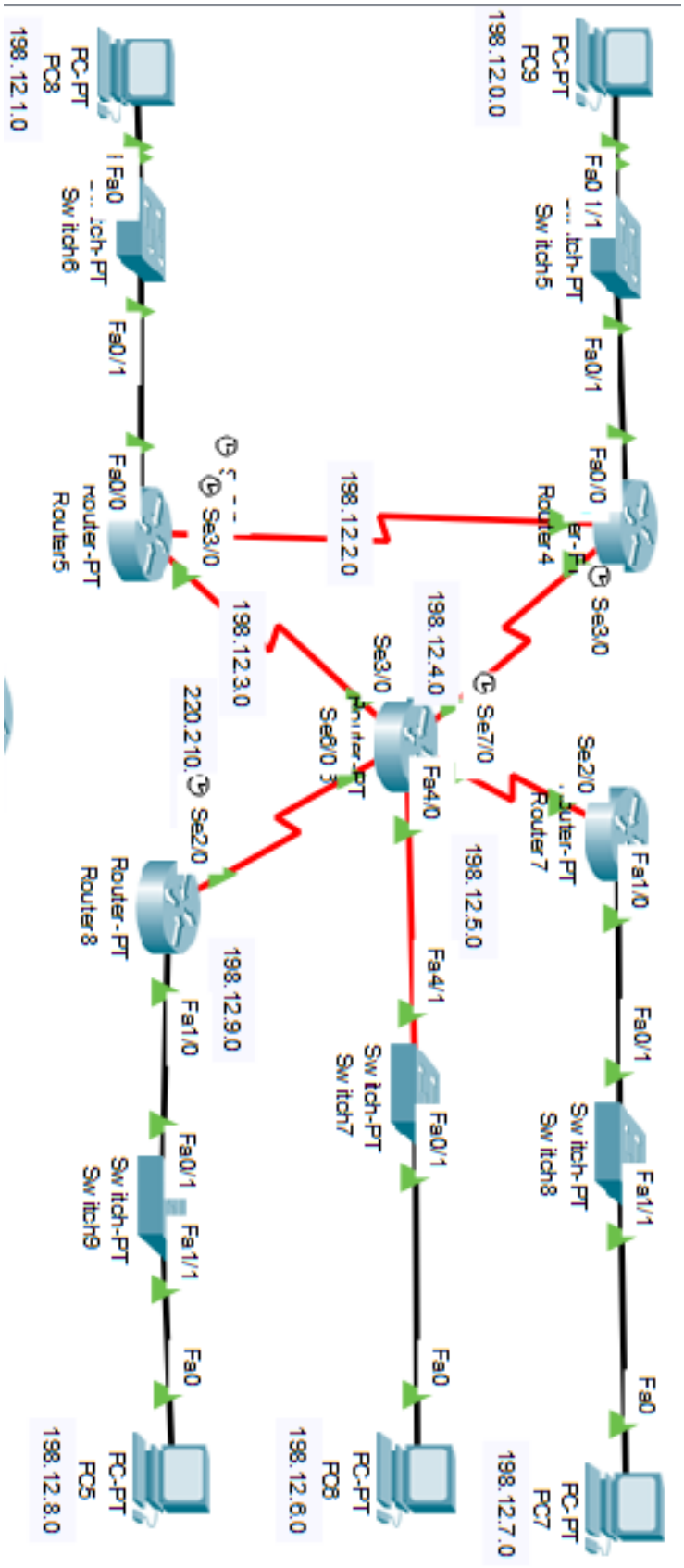


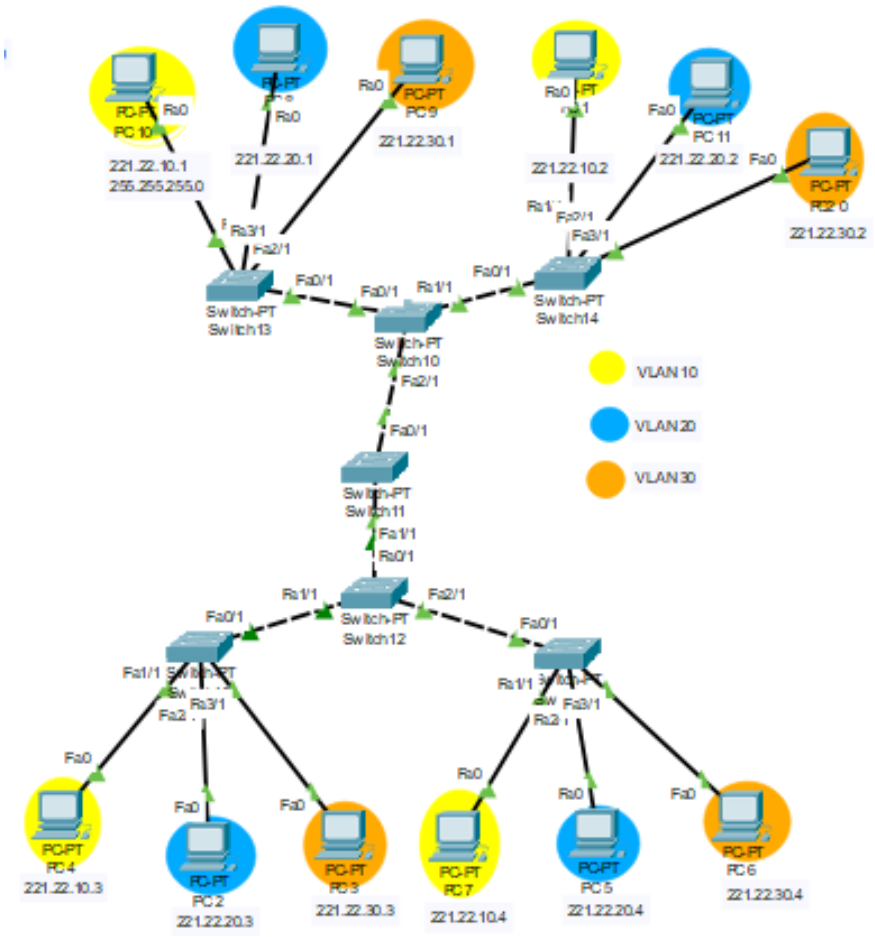
Схема мережі центрального офісу LAN1



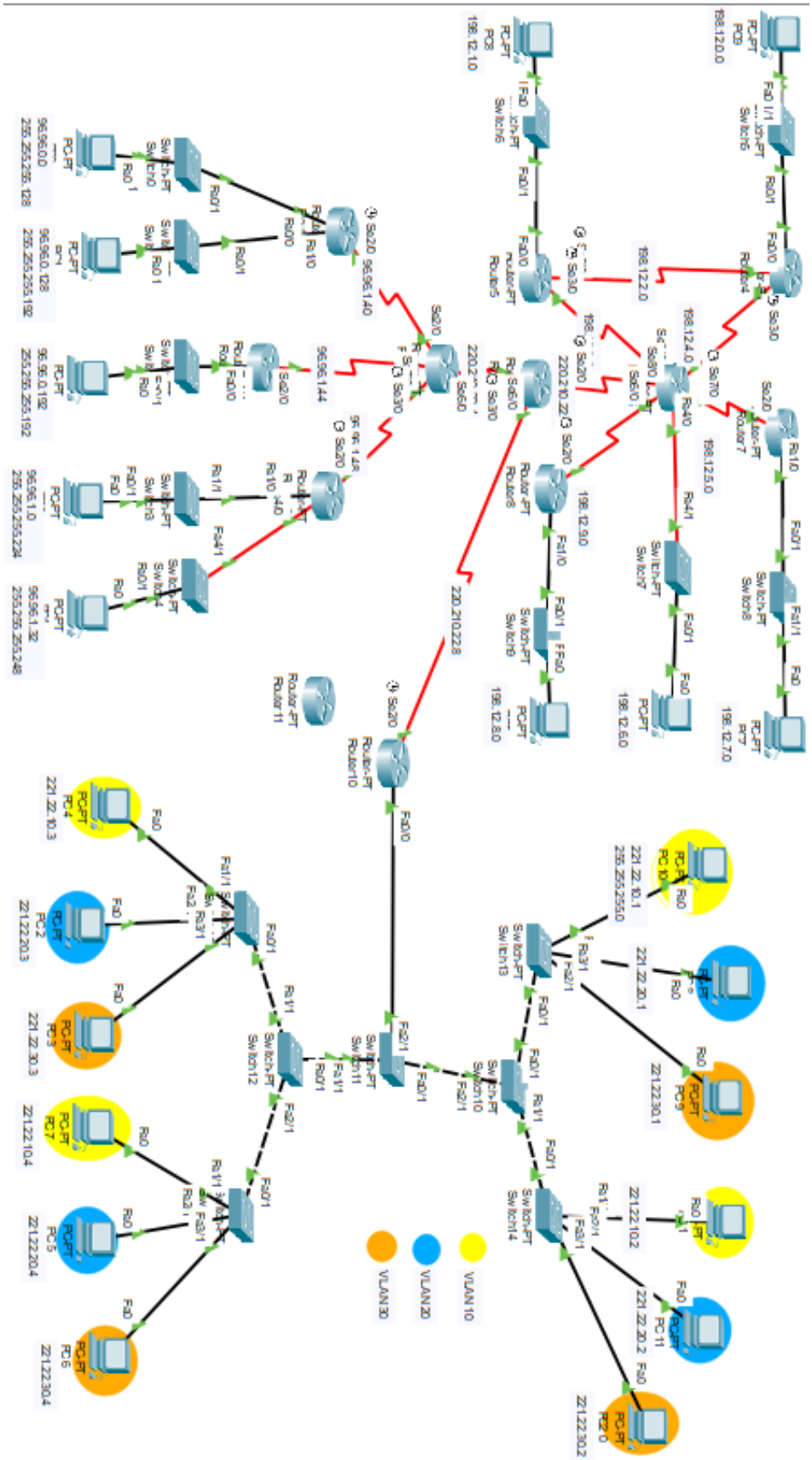
Мережа віддаленого офісу LAN2



Структура мережі диспетчерського центру LAN3



Загальна схема мережі



Додаток В – Налаштування Router7

```
Current configuration : 1436 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 198.12.10.1 255.255.255.0
duplex auto
speed auto
interface FastEthernet1/0
no ip address
duplex auto
speed auto
shutdown
interface Serial2/0
ip address 198.12.4.2 255.255.255.0
interface Serial3/0
ip address 198.12.3.2 255.255.255.0
!
interface FastEthernet4/0
ip address 198.12.6.1 255.255.255.0
interface FastEthernet5/0
no ip address
shutdown
interface Serial6/0
ip address 198.12.9.2 255.255.255.0
interface Serial7/0
ip address 198.12.5.1 255.255.255.0
```

```
clock rate 2000000
interface Serial8/0
ip address 220.210.22.1 255.255.255.252
interface Serial9/0
no ip address
clock rate 2000000
shutdown
router ospf 22
log-adjacency-changes
network 198.12.3.0 0.0.0.255 area 0
network 198.12.4.0 0.0.0.255 area 0
network 198.12.5.0 0.0.0.255 area 0
network 198.12.6.0 0.0.0.255 area 0
network 198.12.9.0 0.0.0.255 area 0
default-information originate
ip classless
ip route 198.12.10.0 255.255.255.0 198.12.10.2
ip route 96.96.1.52 255.255.255.252 198.12.11.2
ip route 0.0.0.0 0.0.0.0 220.210.22.2
ip route 0.0.0.0 0.0.0.0 198.12.11.2
ip flow-export version 9
line con 0
line aux 0
line vty 0 4
login
end
```

Додаток Г – Налаштування Router8

```
Current configuration : 1177 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
no ip address
duplex auto
speed auto
shutdown
interface FastEthernet1/0
no ip address
duplex auto
speed auto
shutdown
interface Serial2/0
ip address 96.96.1.42 255.255.255.252

interface Serial3/0
ip address 96.96.1.46 255.255.255.252
clock rate 2000000
interface FastEthernet4/0
no ip address
shutdown
interface FastEthernet5/0
no ip address
shutdown
interface Serial6/0
ip address 220.210.22.6 255.255.255.252
interface Serial7/0
ip address 96.96.1.50 255.255.255.252
ip classless
ip route 96.96.0.0 255.255.255.128 96.96.1.41
ip route 96.96.0.128 255.255.255.192 96.96.1.41
ip route 96.96.0.192 255.255.255.192 96.96.1.45
ip route 96.96.1.0 255.255.255.224 96.96.1.49
ip route 96.96.1.32 255.255.255.248 96.96.1.49
ip route 0.0.0.0 0.0.0.0 96.96.1.54
ip route 0.0.0.0 0.0.0.0 220.210.22.5
ip flow-export version 9
line con 0
line aux 0
line vty 0 4
login
end
```

Додаток Ґ – Налаштування Router4

```
Current configuration : 1144 bytes
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname Router
ip cef
no ipv6 cef
interface FastEthernet0/0
no ip address
duplex auto
speed auto
interface FastEthernet0/0.10
encapsulation dot1Q 10
ip address 221.22.10.5 255.255.255.0
interface FastEthernet0/0.20
encapsulation dot1Q 20
ip address 221.22.20.5 255.255.255.0
interface FastEthernet0/0.30
encapsulation dot1Q 30
ip address 221.22.30.5 255.255.255.0
interface FastEthernet0/0.40
encapsulation dot1Q 40
ip address 221.22.40.5 255.255.255.0
interface FastEthernet1/0
no ip address
duplex auto
speed auto
shutdown
interface Serial2/0
ip address 220.210.22.9 255.255.255.252
clock rate 2000000
interface Serial3/0
no ip address
clock rate 2000000
shutdown
interface FastEthernet4/0
no ip address
shutdown
interface FastEthernet5/0
no ip address
shutdown
ip classless
ip route 0.0.0.0 0.0.0.0 220.210.22.10
ip flow-export version 9
line con 0
line aux 0
line vty 0 4
```

Додаток Д – Налаштування Router5

```
Router#sh run
Building configuration...
Current configuration : 1117 bytes
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
hostname Router
enable secret 5 $1$mERr$ShvCuO322sTC2UkeZfkRO0
enable password 7 0832585C0C14071E0618070D33
no ip cef
no ipv6 cef
interface FastEthernet0/0
no ip address
duplex auto
speed auto
shutdown
interface FastEthernet1/0
no ip address
duplex auto
speed auto
shutdown
interface Serial2/0
ip address 220.210.22.2 255.255.255.252
clock rate 2000000
interface Serial3/0
ip address 220.210.22.5 255.255.255.252
clock rate 2000000
interface FastEthernet4/0
no ip address
shutdown
interface FastEthernet5/0
no ip address
shutdown
interface Serial6/0
ip address 220.210.22.10 255.255.255.252
ip classless
ip route 198.12.0.0 255.255.0.0 220.210.22.1
ip route 96.96.0.0 255.255.0.0 220.210.22.6
ip route 0.0.0.0 0.0.0.0 220.210.22.9
ip flow-export version 9
banner motd ^CHELLO! IT IS SECURED CONSOLE^C
line con 0
password 7 08314D58
login
line aux 0
line vty 0 4
login
```