

Міністерство освіти і науки України  
Національний технічний університет  
«Дніпровська політехніка»

Навчально-науковий  
інститут електроенергетики  
(інститут)

Факультет інформаційних технологій  
(факультет)

Кафедра інформаційних технологій та комп'ютерної інженерії  
(повна назва)

**ПОЯСНЮВАЛЬНА ЗАПИСКА**  
**кваліфікаційної роботи ступеня бакалавра**

студента Швеця Івана Анатолійовича  
(ПІБ)

академічної групи 123-19-1  
(шифр)

спеціальності 123 Комп'ютерна інженерія  
(код і назва спеціальності)

за освітньо-професійною програмою 123 Комп'ютерна інженерія  
(офіційна назва)

на тему “Комп'ютерна система ІТ-компанії “Диверсіті ІТ” з реалізацією побудови, налаштування та безпеки корпоративної мережі та підсистеми клімат контролю.”  
(назва за наказом ректора)

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	проф. Цвіркун Л.І.			
розділів:				
розробка апаратної частини	доц. Бешта Д.О.			
розробка корпоративної мережі	ас. Панферова Я.В.			
<b>Рецензент</b>				
<b>Нормоконтролер</b>	проф. Цвіркун Л.І.			

Дніпро  
2023

**ЗАТВЕРДЖЕНО:**

завідувач кафедри

інформаційних

технологій та

комп'ютерної

інженерії

(повна назва)

Гнатушенко В.В.

(підпис)

(прізвище, ініціали)

"\_\_" \_\_\_\_\_ 2023 року

**ЗАВДАННЯ  
на кваліфікаційну  
роботу ступеня  
бакалавр**

студента Швець І.А.  
(прізвище та ініціали)

академічної групи 123-19-1  
(шифр)

спеціальності 123 «Комп'ютерна інженерія»

за освітньо-професійною програмою 123 «Комп'ютерна інженерія»  
(офіційна назва)

на тему “Комп'ютерна система ІТ-компанії “Диверсіті ІТ” з реалізацією побудови, налаштування та безпеки корпоративної мережі та підсистеми клімат контролю.”

затверджену наказом ректора НТУ «Дніпровська політехніка» від 16.05.2023 № 350-с

Розділ	Зміст	Термін виконання
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел конкретизується предмет та мету роботи та виконується постановка завдання	10.05.2023
Розробка апаратної частини	На основі аналізу підприємства формулюються технічні вимоги до комп'ютерної системи та розробляється апаратна частина системи	17.05.2023
Розробка корпоративної мережі	Виконується розрахунок налаштувань корпоративної мережі та перевірка роботи системи, розробляються методи та налаштування обладнання для захисту інформації в системі	30.05.2023
Розробка компонента системи	Виконується детальна розробка компонента системи	31.05.2023

Завдання видано \_\_\_\_\_

проф. Цвіркун Л.І.

Дата видачі 10.02.2023

Дата подання до екзаменаційної комісії 08.06.2023

Прийнято до виконання \_\_\_\_\_

Швець І.А.

## РЕФЕРАТ

Пояснювальна записка: 90 с., 47 рис., 7 табл., 3 дод., 35 джерел.

ПІДПРИЄМСТВО, КЛІМАТ КОНТРОЛЬ, КОРПОРАТИВНА МЕРЕЖА, БЕЗПЕКА, ПРОГРАМУВАННЯ, CISCO, LAN, WAN, VLAN, ROUTER, SWITCH

Об'єкт розробки – корпоративна мережа для ІТ-компанії «Диверсіті ІТ» з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі та підсистеми клімат контролю.

Мета роботи – розробка та налаштування корпоративної мережі для офісів ІТ-компанії «Диверсіті ІТ».

В першому розділі було розглянуто галузь, в якій працює ІТ компанія «Диверсіті ІТ», було проведено аналіз характеристики підприємства та умови застосування комп'ютерної системи. Також було розглянуто технічні способи, принципи, математичні методи забезпечення. Також було розглянуто вже існуючі рішення комп'ютерної системи та поставлено завдання.

В другому розділі було розглянуто усі вимоги, яким повинна відповідати корпоративна мережа, також було розроблено топологічну схему розміщення структурних підрозділів, розроблено загальну архітектуру підприємства, було обрано та обґрунтовано технічні засоби, які будуть використані, та розраховано інтенсивність вихідного трафіку.

В третьому розділі було виконано наступне: розраховано схему адресації, розроблено топологічну схему корпоративної мережі, розраховано маршрутизацію, виконане базове налаштування та перевірки комп'ютерної системи, а також проведено дії щодо захисту інформації в комп'ютерній системі.

В четвертому розділі було розроблено систему, яка виконує клімат контроль в офісі.

## ЗМІСТ

Перелік умовних позначень, символів, одиниць, скорочень і термінів .....	6
Вступ .....	7
1 Стан питання та постановка завдання .....	9
1.1 Стисла характеристика галузі розробки програмного забезпечення.....	9
1.2 Характеристика ІТ-компанії «Диверсіті ІТ» та умов застосування КС .....	11
1.3 Принципи, технічні способи та математичні методи інформаційного забезпечення підприємства .....	13
1.4 Організаційна структура ІТ-компанії «Диверсіті ІТ» .....	14
1.5 Топологічне розміщення структурних підрозділів .....	15
1.6 Постановка завдання .....	17
1.7 Огляд існуючих інженерних рішень КС в галузі.....	17
2 Розробка апаратної частини комп'ютерної або кіберфізичної системи.....	19
2.1 Технічні вимоги до комп'ютерної системи.....	19
2.1.1 Вимоги до системи в цілому .....	19
2.1.1.1 Вимоги до структури і функціонуванню системи .....	19
2.1.1.2 Вимоги до показників призначення .....	21
2.1.1.3 Вимоги до експлуатації, технічного обслуговування, ремонту і збереженню.....	21
2.1.1.4 Вимоги до патентної чистоти .....	23
2.1.3.5 Додаткові вимоги .....	24
2.1.2 Вимоги до задач (налаштувань), які виконуються у комп'ютерній системі .....	25
2.1.3 Вимоги до видів забезпечення комп'ютерної системи .....	27
2.1.3.1 Вимоги до математичного забезпечення .....	27
2.1.3.2 Вимоги до інформаційного забезпечення.....	27
2.1.3.3 Вимоги до лінгвістичного забезпечення.....	27
2.1.3.4 Вимоги до технічного забезпечення. ....	28
2.1.3.5 Вимоги до організаційного забезпечення.....	28
2.1.3.6 Вимоги до методичного забезпечення.....	28
2.2 Розробка інженерних рішень і комплексу технічних засобів .....	29

2.2.1	Вибір і обґрунтування структурної схеми комплексу технічних засобів комп'ютерної системи шляхом узгодження структури з топологічними особливостями об'єкту розробки .....	29
2.2.2	Розробка специфікацій апаратних засобів комп'ютерної системи .....	31
2.2.3	Розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі підприємства.....	36
3	Розробка корпоративної мережі підприємства .....	38
3.1	Розрахунок схеми адресації корпоративної мережі .....	38
3.2	Розрахунок схеми адресації пристроїв .....	39
3.3	Розробка топологічної схеми корпоративної мережі.....	41
3.4	Розрахунок налаштувань маршрутизації корпоративної мережі.....	44
3.5	Налаштування та перевірка роботи комп'ютерної системи .....	48
3.5.1	Базове налаштування конфігурації пристроїв.....	48
3.5.2	Налаштування маршрутизаторів корпоративної мережі .....	50
3.5.3	Налаштування агрегування каналів .....	53
3.5.4	Налаштування роботи Інтернет .....	54
3.6	Захист інформації в комп'ютерній системі від несанкціонованого доступу ..58	
3.6.1	Розробка методів для захисту інформації в комп'ютерній системі .....	58
3.6.2	Налаштування мереж VLAN.....	58
3.6.2	Налаштування параметрів безпеки комутаторів.....	62
3.6.3	Налаштування віртуальної приватної мережі site-to-site VPN з використанням IPsec.....	62
3.7	Перевірка роботи комп'ютерної системи.....	64
4	Розробка системи клімат контролю .....	73
4.1	Інженерне рішення по розробці компонента системи .....	73
4.2	Розробка системи клімат контролю .....	79
4.3	Перевірка роботи системи клімат контролю.....	83
	Висновки.....	86
	Перелік посилань .....	88
	Додаток А Загальна топологічна схема підприємства .....	91
	Додаток Б Текст програми налаштування комп'ютерної мережі підприємства...92	
	Додаток В Текст програми налаштування системи клімат контролю .....	119

## **ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ**

КС – комп'ютерна система.

ПК – персональний комп'ютер.

Ethernet – протокол кабельних комп'ютерних мереж.

VPN – віртуальна приватна мережа.

LAN – локальна (обчислювальна) мережа із групи комп'ютерів та/або інших пристроїв.

VLAN – це віртуальні мережі, які є на другому рівні моделі OSI.

ПЗ – програмне забезпечення.

## ВСТУП

Комп'ютерні мережі є невід'ємною частиною сучасного світу і бізнесу. Вони відіграють критичну роль у сприянні комунікації, обміні інформацією та ефективному управлінні ресурсами. Уявіть собі світ без комп'ютерних мереж – це було б неможливо у сучасній глобалізованій економіці.

У сфері ІТ-компаній комп'ютерні мережі мають ключове значення. Вони створюють основу для розробки, впровадження та управління програмними продуктами та послугами. Компанії залежать від мережевої інфраструктури для обміну даними між командами розробників, тестування продуктів та спілкування з клієнтами.

Одним з основних аспектів важливості комп'ютерних мереж для ІТ-компаній є забезпечення безпеки даних. У зв'язку зі зростаючою кількістю кібератак та загроз, захист інформації стає надзвичайно важливим завданням. Комп'ютерні мережі допомагають забезпечити захист даних, використовуючи різноманітні методи шифрування та механізми перевірки доступу.

Крім того, комп'ютерні мережі сприяють збільшенню продуктивності та ефективності роботи. Вони дозволяють працівникам спілкуватися, обмінюватися даними та співпрацювати над проектами в режимі реального часу, навіть якщо вони знаходяться на різних місцях світу. Це дозволяє прискорити процеси розробки програмного забезпечення та підвищити рівень виробничої діяльності.

Комп'ютерні мережі також допомагають забезпечити важливу складову управління та координації бізнес-процесів в ІТ-компаніях. Вони дозволяють вести моніторинг та керування ресурсами, включаючи обладнання, програмне забезпечення та персонал. Завдяки цьому, компанії можуть оптимізувати робочі процеси, забезпечити раціональне використання ресурсів і підвищити ефективність роботи.

Крім внутрішньої ефективності, комп'ютерні мережі грають важливу роль у взаємодії з зовнішнім світом, зокрема з клієнтами, партнерами та постачальниками.

Вони дозволяють забезпечити швидкий та надійний обмін даними, здійснювати електронну комунікацію та вести онлайн-транзакції. Це сприяє розвитку бізнесу, залученню нових клієнтів та розширенню географії діяльності компанії.

Загалом, комп'ютерні мережі є невід'ємною складовою сучасного світу та бізнесу. Вони забезпечують швидкий, надійний та безпечний обмін даними, сприяють зростанню продуктивності та ефективності роботи, а також сприяють розвитку бізнесу та взаємодії зі зовнішнім середовищем. Тому, усвідомлюючи важливість комп'ютерних мереж, ІТ-компанії вкладають значні зусилля у їх розвиток та підтримку, щоб бути конкурентоспроможними на ринку.



# 1 СТАН ПИТАННЯ ТА ПОСТАНОВКА ЗАВДАННЯ

## 1.1 Стисла характеристика галузі розробки програмного забезпечення

Галузь розробки програмного забезпечення є надзвичайно важливою у сучасному світі, оскільки комп'ютери та програмне забезпечення є невід'ємною частиною нашого життя. Велика кількість компаній та інституцій у всьому світі використовують програмне забезпечення для автоматизації бізнес-процесів, управління клієнтською базою, ведення обліку та багатьох інших завдань.

Завдяки розробці програмного забезпечення, бізнес-процеси можуть бути більш ефективними та продуктивними, що дозволяє компаніям збільшувати свої прибутки та конкурентоспроможність на ринку. Крім того, розробка програмного забезпечення дозволяє забезпечити безпеку та захист важливої інформації від несанкціонованого доступу.

Сучасні технології та інтернет роблять розробку програмного забезпечення дедалі більш доступною та швидкою, що дозволяє компаніям розробляти та впроваджувати програмне забезпечення відповідно до своїх потреб.

Галузь розробки програмного забезпечення є надзвичайно важливою для ефективного та продуктивного функціонування бізнесу у сучасному світі. Розвиток цієї галузі приведе до збільшення ефективності та конкурентоспроможності компаній та інституцій, що має велике значення для розвитку економіки та суспільства в цілому.

Окрім того, розробка програмного забезпечення є невід'ємною частиною розвитку нових технологій та інновацій. Сучасні технології, такі як штучний інтелект, блокчейн, Інтернет ресурсів та багато інших, потребують розробки нових програмних продуктів та рішень. Розробники програмного забезпечення відіграють важливу роль у цьому процесі, розробляючи та вдосконалюючи програмні продукти для реалізації нових технологій та інноваційних проєктів.

Також, галузь розробки програмного забезпечення забезпечує велику кількість робочих місць у всьому світі. Розробники програмного забезпечення є

одними з найбільш шуканих фахівців на ринку праці, а їхні навички та знання є важливим ресурсом для багатьох компаній та інституцій. Тому галузь розробки програмного забезпечення має важливе значення для розвитку економіки та соціальної сфери в багатьох країнах світу.

Напрямки розробки програмного забезпечення постійно розширюються та удосконалюються, що відкриває нові можливості для компаній та інституцій. Наприклад, у зв'язку з розвитком технологій штучного інтелекту та машинного навчання, компанії можуть розробляти та використовувати програмні продукти, які здатні автоматично аналізувати великі об'єми даних та робити прогнози, що дозволяє більш точно прогнозувати ринкові тенденції та підвищувати ефективність прийняття рішень.

Розробка програмного забезпечення також грає важливу роль у розвитку мобільних технологій та Інтернету речей. Розробники програмного забезпечення розробляють мобільні додатки та програмне забезпечення для різних пристроїв, що дозволяє компаніям та інституціям бути більш доступними та зручними для своїх клієнтів та співробітників.

Крім того, розробка програмного забезпечення є важливим елементом в забезпеченні безпеки та захисту інформації. Зараз комп'ютерні системи та мережі знаходяться під постійною загрозою кібератак та вірусних атак. Розробники програмного забезпечення мають важливу роль у створенні програмних засобів захисту, які дозволяють забезпечувати безпеку та захист важливої інформації від несанкціонованого доступу.

Галузь розробки програмного забезпечення також є важливою для розвитку електронної комерції та онлайн-бізнесу. Розробники програмного забезпечення розробляють електронні магазини та інтернет-платформи, що дозволяє компаніям та бізнесам бути більш доступними та зручними для своїх клієнтів та споживачів.

Також, галузь розробки програмного забезпечення має значний вплив на розвиток інших галузей та індустрій, таких як медицина, фінанси, транспорт, телекомунікації та багато інших. Розробка програмного забезпечення дозволяє

вдосконалювати та автоматизувати бізнес-процеси в різних галузях та індустріях, що дозволяє покращувати якість та ефективність надання послуг та продуктів для клієнтів та споживачів.

У цілому, галузь розробки програмного забезпечення є дуже важливою та перспективною галуззю у сучасному світі. Розвиток цієї галузі є важливим чинником розвитку економіки та соціальної сфери, а також дозволяє компаніям та інституціям бути більш ефективними та продуктивними у своїй діяльності.

## **1.2 Характеристика ІТ-компанії «Диверсіті ІТ» та умов застосування КС**

ІТ-компанії «Диверсіті ІТ» – це ІТ-компанія, яка спеціалізується на розробці програмного забезпечення, наданні ІТ-послуг для бізнесу та має команду висококваліфікованих професіоналів з великим досвідом роботи у галузі програмної розробки. Компанія завжди відкрита до нових ідей та готова реалізувати будь-яку задумку своїх клієнтів.

Компанія «Диверсіті ІТ» володіє сучасними технологіями та інструментами для розробки програмного забезпечення та використовує найновіші технології та методики, що дозволяють надавати якісні та надійні рішення для своїх клієнтів.

«Диверсіті ІТ» має широкий діапазон клієнтів, що включає малі підприємства, середні та великі корпорації різних галузей та індустрій. Також завжди відкрита до співпраці з будь-якими клієнтами.

Місія компанії ІТ-компанії «Диверсіті ІТ» полягає в тому, щоб надавати якісні та надійні ІТ-послуги для своїх клієнтів та допомогти їм збільшити продуктивність та ефективність їхнього бізнесу. Компанія працює над тим, щоб бути на чолі інноваційних технологій та методик у галузі ІТ, та постійно вдосконалює свої процеси та методики, щоб забезпечити клієнтам максимальну якість та ефективність своїх послуг.

Також забезпечується конфіденційність та безпека даних своїх клієнтів. Компанія ретельно дотримується стандартів безпеки та конфіденційності даних, щоб гарантувати захист конфіденційної інформації своїх клієнтів.

«Диверсіті ІТ» є надійним та досвідченим партнером у галузі ІТ. Вона готова надати свої послуги та допомогти клієнтам з усіх питань, пов'язаних з ІТ, та забезпечити найвищу якість та ефективність своїх рішень.

На сьогодні компанія надає широкий спектр ІТ-послуг, серед яких можна виділити наступні:

- розробка корпоративних веб-сайтів. Компанія розробляє веб-сайти різної складності та функціональності для компаній різного розміру та галузей. Розроблені веб-сайти можуть мати різні функції та можливості, такі як онлайн-замовлення, інтерактивні форми зв'язку з клієнтами, вбудовані калькулятори та інше;

- створення програмного забезпечення на замовлення. Компанія розробляє програмне забезпечення за індивідуальними потребами клієнта. Розроблене програмне забезпечення може мати різні функції та можливості, такі як автоматизація бізнес-процесів, облік та збереження даних, аналіз даних та багато іншого;

- розробка мобільних додатків для Android та iOS. Компанія розробляє мобільні додатки для різних платформ, таких як Android та iOS. Розроблені мобільні додатки можуть мати різні функції та можливості, такі як онлайн-замовлення, інтерактивні форми зв'язку з клієнтами, вбудовані калькулятори та інше;

- впровадження систем управління взаємодією з клієнтами (CRM). Компанія розробляє та впроваджує системи управління взаємодією з клієнтами (CRM), що дозволяє компаніям ефективніше взаємодіяти зі своїми клієнтами;

- розробка індивідуальних рішень в галузі ІТ. Компанія надає послуги з розробки індивідуальних рішень в галузі ІТ, які відповідають конкретним потребам та вимогам клієнта. Ці рішення можуть бути розроблені для різних галузей та індустрій, включаючи медицину, фінанси, транспорт, телекомунікації та інші;

- консультаційні послуги. Компанія надає консультаційні послуги з розробки програмного забезпечення та ІТ-проекування для клієнтів з різних галузей та

індустрій. Консультанти компанії допомагають клієнтам у виборі оптимального рішення та стратегії розробки, що відповідає їхнім потребам та вимогам;

– технічна підтримка та обслуговування. Компанія надає технічну підтримку та обслуговування для розробленого програмного забезпечення та ІТ-інфраструктури клієнта. Компанія допомагає клієнтам у підтримці та вдосконаленні розробленого програмного забезпечення, а також у вирішенні технічних проблем та неполадок.

### **1.3 Принципи, технічні способи та математичні методи інформаційного забезпечення підприємства**

Компанія «Диверсіті ІТ» повинна використовувати різні принципи, технічні способи та математичні методи для забезпечення інформаційної безпеки підприємства та забезпечення ефективної роботи ІТ-інфраструктури клієнтів. Деякі з цих принципів, технічних способів та математичних методів можуть включати:

– захист від несанкціонованого доступу. Компанія повинна використовувати різні методи захисту від несанкціонованого доступу до даних, включаючи захист паролями;

– захист від вірусів та шкідливих програм. Компанія повинна використовувати антивірусні програми та інші інструменти захисту від вірусів та шкідливих програм на персональних комп'ютерах, щоб забезпечити безпеку даних клієнтів;

– захист від витоку даних. Організаційні заходи повинні включати у себе встановлення політики безпеки даних, забезпечення належної підготовки персоналу щодо безпеки даних, а також контроль доступу до даних та відстеження дій користувачів;

– використання VPN. Компанія повинна використовувати VPN для забезпечення компанії можливість віддаленого доступу до важливої інформації в безпечному середовищі, що є важливим так як у компанії декілька офісів.

Усі ці принципи, технічні способи та математичні методи повині використовуватися компанією «Диверсіті ІТ» для забезпечення високої якості та ефективності послуг для своїх клієнтів, а також для забезпечення безпеки даних та ІТ-інфраструктури.

#### **1.4 Організаційна структура ІТ-компанії «Диверсіті ІТ»**

Організаційна структура ІТ-компанії «Диверсіті ІТ» складається з:

- генеральний директор;
- менеджери проектів;
- розробники;
- дизайнери;
- тестувальники;
- консультанти з ІТ;
- аналітики.

Генеральний директор – відповідає за керування компанією в цілому, ведення стратегічного планування та взаємодію з клієнтами.

Менеджери проектів – забезпечують успішне виконання проектів, ведення команди розробників, контроль за термінами та якістю роботи.

Розробники – відповідають за програмну розробку продуктів, дотримання технічних вимог та якість коду.

Дизайнери – забезпечують високий рівень дизайну продуктів, створення користувацьких інтерфейсів та рекламної продукції.

Тестувальники – проводять тестування програмного забезпечення та виявляють помилки перед випуском продукту.

Консультанти з ІТ – надають консультації з питань технічної підтримки клієнтів та вирішення проблем з ІТ.

Аналітики – проводять аналіз ринку, клієнтів та конкурентів, допомагають в формулюванні стратегії та плануванні розвитку компанії.

Крім внутрішньої команди, компанія «Диверсіті ІТ» також може привласнювати зовнішніх консультантів та партнерів, які допомагають забезпечити виконання проектів та забезпечення потреб клієнтів у певних областях. Наприклад, компанія може співпрацювати з партнерами, які спеціалізуються на інтеграції різноманітного програмного забезпечення, розширенні можливостей технічної інфраструктури, або наданні інших інноваційних послуг.

Загалом, успішність компанії залежить від того, наскільки добре вона використовує свої ресурси та здібності, технічні та інноваційні рішення, які вона використовує, а також від ефективної взаємодії з клієнтами та партнерами.

Схему організаційної структури ІТ-компанії наведено на рисунку 1.1.

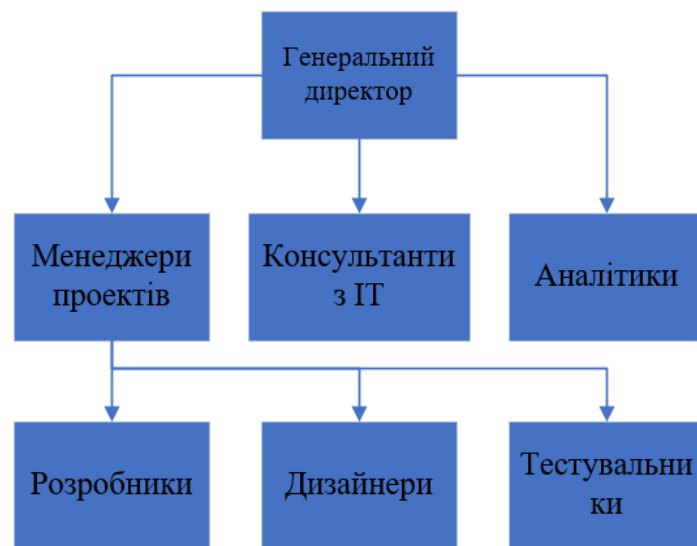


Рисунок 1.1 – Схема організаційної структури ІТ-компанії

### 1.5 Топологічне розміщення структурних підрозділів

ІТ-компанії «Диверсіті ІТ» складається з 2 офісів у Дніпрі.

Головний офіс складається з офісів орендованих на чотирьох поверхах, а саме 5, 6, 7 та 8 поверх, в будівлі що знаходиться за адресою вулиця Глінки 7. Віддалений офіс знаходиться за адресою вул. Європейська 30 на 2 поверсі.

У головному офісі розділи розміщені:

- 5 поверх: генеральний директор, відділ розробників;
- 6 поверх: відділ дизайнерів;
- 7 поверх: відділ консультантів з ІТ;
- 8 поверх: відділ менеджерів проектів, відділ аналітиків.

У віддаленому офісі на 2 поверсі знаходиться відділ тестувальників.

Топографічна схема розміщення структурних підрозділів підприємства офісів зображено на рисунку 1.2.



Рисунок 1.2 – Топографічна схема розміщення структурних підрозділів підприємства



## 1.6 Постановка завдання

Завданням для кваліфікаційної роботи є розробка комп'ютерної системи ІТ-компанії «Диверсіті ІТ» з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі та підсистеми клімат контролю.

Для вирішення цього завдання необхідно виконати наступні пункти:

- ознайомитися зі структурою компанії;
- розробка технічних вимог для КС;
- вибір комплексу технічних засобів КС;
- обрання топології, враховуючи варіант вектору розвитку корпоративної мережі;
- розрахунок налаштувань для заданої топології мережі, вибір інтерфейсу каналів зв'язку та протоколу обміну;
- створення топологічної схеми (логічної) комп'ютерної системи;
- розрахунок налаштувань маршрутизації комп'ютерної мережі;
- налаштування корпоративної мережі та її тестування;
- налаштування підсистеми клімат контролю та її тестування;
- підбір обладнання та програмного забезпечення;
- розробка системи клімат контролю, її програмування та вибір комплексу технічних засобів.

Результатом виконання кваліфікаційної роботи є мережа, яка вже налаштована, враховуючи підсистему клімат контролю, та є гнучкою, надійною, масштабованою та безпечною.

## 1.7 Огляд існуючих інженерних рішень КС в галузі

В галузі комп'ютерних систем існує безліч різних інженерних рішень, які можуть використовуватись підприємствами для забезпечення ефективної роботи та безпеки. Ось деякі з можливих напрямків рішень:

- хмарні технології: хмарні технології забезпечують доступ до потрібної інформації з будь-якого місця та пристрою, що дозволяє забезпечити ефективну

роботу та спрощує управління даними. Більшість провайдерів хмарних послуг забезпечують високий рівень захисту даних та мають відповідні сертифікації, що робить їх відповідними для використання в галузі;

– віртуалізація: віртуалізація дозволяє створювати віртуальні середовища, що дозволяє краще використовувати ресурси та забезпечує більш ефективну роботу. Віртуалізація дозволяє також забезпечити більш ефективне управління ресурсами та більш швидку розгортку та налаштування середовищ;

– біг-дата та аналітика: використання біг-дата та аналітики дозволяє забезпечити краще управління даними, що в свою чергу забезпечує ефективнішу роботу та покращення бізнес-процесів. Аналітика даних дозволяє виявляти тренди та недоліки в роботі та приймати правильні рішення для покращення ефективності;

– інтернет речей: використання технології Інтернету речей дозволяє збирати дані про роботу підприємства та його пристроїв, що дозволяє забезпечити краще управління та планування ресурсів та процесів. Це також може забезпечити моніторинг стану обладнання та уникнення непередбачуваних відмов, що допомагає уникнути зупинок у роботі та зниження продуктивності;

– розподілені системи: розподілені системи дозволяють забезпечити високу доступність та надійність, а також забезпечують масштабованість та можливість розвитку в майбутньому. Використання розподілених систем також дозволяє забезпечити більш ефективне використання ресурсів та покращити продуктивність.

Усі ці напрямки рішень можуть використовуватись для забезпечення ефективної роботи та забезпечення безпеки в галузі комп'ютерних систем. Вибір конкретного рішення залежить від потреб підприємства, розміру та складності бізнес-процесів, а також від доступних ресурсів та технічної бази.

## **2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ АБО КІБЕРФІЗИЧНОЇ СИСТЕМИ**

### **2.1 Технічні вимоги до комп'ютерної системи**

#### **2.1.1 Вимоги до системи в цілому**

##### **2.1.1.1 Вимоги до структури і функціонуванню системи**

Система повинна представлятися комп'ютерною мережею, що має бути розроблена для передачі різної інформації між підмережами ІТ-компанії «Диверсіті ІТ».

Вимоги, які будуть описані в цьому розділі, повинні бути використані як основа для проектування корпоративної мережі ІТ-компанії «Диверсіті ІТ».

##### **2.1.1.1.1 Перелік підсистем, їхнє призначення й основні характеристики, вимоги до числа рівнів ієрархії та ступені централізації Системи**

Підсистемами у мережі є локальні мережі підрозділів ІТ-компанії «Диверсіті ІТ», які об'єднані в загальну комп'ютерну мережу.

Підсистеми підприємства:

- підсистема головного офісу №1 (LAN1);
- підсистема головного офісу №2 (LAN2);
- підсистема головного офісу №3 (LAN3);
- підсистема головного офісу №4 (LAN5);
- підсистема віддаленого офісу (LAN4).

Загальна топологічна схема розміщення структурних підрозділів зображена у додатку А.

Підсистема головного офісу №1 повинна забезпечувати зв'язком між підсистемами, включаючи віддалену підсистему. Підсистема №1 має підтримувати до 55 вузлів.

Підсистема головного офісу №2 повинна включати в себе систему клімат контролю. Ця підсистема повинна підтримувати до 29 вузлів.

Підсистема головного офісу №3 повинна мати можливість підключення сервера DNS та HTTP. Ця система повинна підтримувати до 83 вузлів.

Підсистема головного офісу №4 повинна підтримувати до 78 вузлів.

Підсистема віддаленого офісу повинна підтримувати підключення сервера TFTP та має підтримувати до 80 вузлів.

#### **2.1.1.1.2 Вимоги до способів і засобів зв'язку для інформаційного обміну між компонентами Системи**

Система повинна бути обладнана необхідним мережевим обладнанням для передачі інформації між підсистемами.

Для каналів зв'язку повинні використовуватися вита пара та оптичне волокно.

#### **2.1.1.1.3 Вимоги до характеристик взаємозв'язків створюваної Системи із суміжними Системами**

Система повинна мати можливість підключення до суміжних систем за допомогою наступних мережевих інтерфейсів – Ethernet та Оптоволоконний.

#### **2.1.1.1.4 Вимоги до режимів функціонування Системи**

Мережеве обладнання повинно забезпечувати функціонування системи 24/7.

#### **2.1.1.1.5 Вимоги до діагностування Системи**

Діагностування системи можна поділити на дві частини – фізичне та програмне.

Фізичне діагностування включає в себе перевірку цілісності каналі зв'язку та мережевого обладнання.

Програмне діагностування включає в себе перевірку через консолі, вводячи необхідні команди.

#### **2.1.1.1.6 Перспективи розвитку, модернізації Системи**

Модернізація системи повинна проводитися шляхом заміни старого обладнання на нове, яке відповідає вимогам програмного та апаратного комплексу системи.

#### **2.1.1.2 Вимоги до показників призначення**

Корпоративна мережа ІТ-компанії «Диверсіті ІТ» повинна розраховуватися переважно для передачі інформації між офісами, враховуючи вимоги щодо безпеки корпоративної мережі.

Система повинна використовуватися для передачі файлів та іноді для проведення нарад.

#### **2.1.1.3 Вимоги до експлуатації, технічного обслуговування, ремонту і збереженню**

##### **2.1.1.3.1 Умови і регламент (режим) експлуатації, що повинні забезпечувати використання технічних засобів (ТЗ) системи з заданими технічними показниками**

Система повинна працювати безперебійно 24 години на день.

Допускається вимкнення з ціллю обслуговування технічних засобів, яке повинно виконуватися згідно відповідних інструкцій, але не менше ніж 1 раз на рік.

Згідно ДСТУ ГОСТ 21552-84 «Засоби обчислювальної техніки. Загальні технічні вимоги, приймання, методи випробувань, маркування, упаковка, транспортування та зберігання» для коректної роботи корпоративної мережі повинні бути виконані наступні вимоги:

- температура в офісі повинна складати  $20 \pm 5$  °С;
- відносна вологість в офісі повинна складати  $60 \pm 15\%$ ;
- атмосферний тиск повинен бути не менше 84 та не більше 107кПА (680-800 мм. Рт. Ст.);

- запиленість у приміщені повітря повинна бути не більше 1 мг / куб. м , якщо розмір часток не більше ніж 3 мкм;
- напруженість поля зовнішнього необхідно щоб було не більше ніж 5.0 А/м;
- частота вібрацій повинна бути не більше ніж 25 Гц при амплітуді зсувів не більше 0.1 мм.

Також, в повітрі офісів, а саме його приміщень, не має бути агресивних речовин, що могли би викликати корозію.

Повинно бути забезпечено контроль за температурою, відносною вологістю та атмосферним тиском у приміщеннях, де перебуває персонал та технічне обладнання.

#### **2.1.1.3.2 Вимоги до параметрів мереж енергопостачання**

Живлення від мережі змінної напруги повинно проходити через фільтри напруги.

Нормальне допустиме відхилення напруги це  $220\text{В} \pm 15\%$ , нормальне допустиме відхилення частоти це  $50\text{Гц} \pm 0,2\text{Гц}$ , коефіцієнт несинусоїдальності – нормально допустиме до 8%, максимум граничне до 12% згідно ДСТУ ГОСТ 13109-97.

Обладнання повинно мати забезпечення комплектом, призначене для експлуатації та ремонту техніки.

У разі виходу із строю мережевого обладнання мають бути запасні частини та вироби для оперативного відновлення роботи.

Персонал, який займається технічним обслуговуванням та ремонтом, має мати певну кваліфікацію з ремонту мережевого обладнання.

### **2.1.1.3.3 Вимоги до кількості, кваліфікації обслуговуючого персоналу і режимам його роботи**

Персонал, який буде обслуговувати систему, повинен пройти спеціалізовані курси від відповідних фірм, мережеве обладнання яких використовуються на підприємстві.

До роботи допускаються тільки персонал попередньо навчений та тільки після проходження інструктажу.

Для забезпечення обслуговування системи в головному офісі має бути 2 системних адміністраторів з графіком роботи 5/2, а у віддаленому офісі 1 системний адміністратор з графіком 5/2.

### **2.1.1.3.4 Вимоги до складу, розміщенню й умовам збереження комплексу запасних виробів і приладів**

КС повинна бути забезпечена комплексом запасних виробів і приладів, до якого входять – комутатор, маршрутизатор.

Такий комплекс запасних виробів повинен мати головний офіс та віддалений офіс, та повинні зберігатися у окремому приміщенні.

### **2.1.1.3.5 Вимоги до регламенту обслуговування**

Технічні засоби повинні обслуговуватися згідно інструкцій експлуатації, де вказані вимоги, але не менше ніж 1 раз на рік.

### **2.1.1.4 Вимоги до патентної чистоти**

Використані програмні та технічні забезпечення повинні забезпечувати патентну чистоту та не порушувати її. Слід пам'ятати, що авторські права виробників мережевого та не тільки обладнання, а також програмне забезпечення охороняються не тільки міжнародним, а й Українським законодавством, тому дозволяється тільки цільове використання обладнання або програмного забезпечення.

### **2.1.3.5 Додаткові вимоги**

#### **2.1.3.5.1 Вимоги до Системи, пов'язані з особливими умовами її експлуатації**

Особливих вимог не має.

#### **2.1.3.5.2 Вимоги до активного обладнання**

Активне обладнання, до якого входять маршрутизатори, комутатори, повинне забезпечити комунікації в мережі між усіма під системами КС.

#### **2.1.3.5.3 Вимоги до кабель-каналів, інформаційним та електричним розеткам**

Кабель канали повинні відповідати вимогам наказу 25.06.2013 №366 «Про затвердження Технічних вимог до створення технічної інфраструктури телекомунікаційних мереж доступу».

#### **2.1.3.5.4 Вимоги до комунікаційного обладнання і його розташування**

Комунікаційне обладнання повинно бути розташоване в окремому приміщенні у шафі під мережеве обладнання під замком або в основному приміщенні, але у шафі під замком.

#### **2.1.3.5.5 Вимоги до однорідності**

Кабелі повинні відповідати розрахункам проекту.

Кількість електророзеток та розеток Ethernet повинно мати запас 30%.

Кабель каналі повинні використовуватися тільки закритого типу.

#### **2.1.3.5.6 Вимоги до резервування**

В підсистемі головного офісу №1 необхідно забезпечити виконати з'єднання комутаторів топологією – кільце, забезпечивши тим самим у разі розриву одного каналу зв'язку, переключення на другий канал зв'язку і подальшої передачі даних.



### **2.1.3.5.7 Вимоги до розробки компонента системи**

Система повинна забезпечити увімкнення нагрівача від 15°C до 21°C градуса, а від 25°C до 37°C повинен бути увімкнута охолоджувача. Під час іншої температури охолоджувач та нагрівач повинні бути у вимкненому стані.

### **2.1.2 Вимоги до задач (налаштувань), які виконуються у комп'ютерній системі**

Корпоративна мережа має складатися з п'яти підмереж LAN1 – LAN5.

Кількість вузлів у кожній підмережі відповідно має бути: 50, 27, 79, 39, 76.

Блок адрес для виділення підмережі має бути 10.23.IPn.0/23 де IPNn – 84.

Інтенсивність трафіку в мережі повинна бути  $\mu=129$  (кадрів/с).

Для маршрутизації між роутерами в локальній мережі має використовуватися блок адрес 10.0.18.0/24.

Враховуючи вищеописані вимоги повинна бути розроблена адресація підмереж.

Під час розрахунку необхідно враховувати наступні вимоги:

- використання блоку адрес версії IPV4;
- перші з можливих адрес необхідно назначити інтерфейсам та під інтерфейсам маршрутизаторів у локальній мережі;
- другі з можливих адрес необхідно назначити комутаторам у локальній мережі;
- серверам необхідно назначити IP адреси згідно певних правил, а саме: IP-адрес дорівнює першому можливому адресу у мережі + 9 + номер, де номер це – 18;
- останні з IP адрес необхідно назначити вузлам за допомогою DHCP;
- у мережі LAN4 виконати налаштування VLAN.

Також окрім цього, необхідно виконати і базове налаштування конфігурацій пристроїв:

- призначення ім'я пристроїв за таким правилом: Shvec\_тип пристрою\_номер пристрою;
- на всіх комутаторах та маршрутизаторах призначати пароль cisco до консолі, а також vty;
- на всіх комутаторах та маршрутизаторах призначати пароль class до привілейованого режиму;
- необхідно всі паролі, які зберігаються у відкритому вигляді, зашифрувати;
- налаштувати банер MOTD;
- назначити на усіх лініях vty використовувати протокол ssh;
- на всіх комутаторах та маршрутизаторах налаштувати користувача 123-19-1\_Shvec з паролем admincisco;
- у якості домену необхідно використовувати ім'я пристрою;
- для шифрування даних використовувати ключ RSA завдовжки 1024 біт;
- на DCE – інтерфейсах у маршрутизаторів необхідно встановити тактову частоту 128000.

На маршрутизаторах необхідно виконати такі налаштування:

- задати пропускну спроможність на serial-інтерфейсах = 128 Кб/с, вартість метрики = 7500;
- налаштування DHCP.

Також потрібно виконати налаштування всіх маршрутизаторів на підтримку служби AAA таким чином:

- для перевірки підключень до VTY ліній на маршрутизаторі необхідно використовувати локальну базу даних користувачів;
- для доступу до консолі використовувати аутентифікацію на основі протоколу RADIUS і якщо немає – локальну базу даних;
- radius-сервер налаштувати наступним чином: ключове слово – radius123;
- в якості облікового запису користувачів використовувати ім'я пристрою з паролем admin123.

У LAN1 необхідно виконати агрегацію каналів.

Для виходу робочих станцій в Інтернет необхідно налаштувати пограничний маршрутизатор з динамічним NAT за такими даними: ім'я пула – Internet, пул адресів з 209.165.200.5 по 209.165.200.30, номер списку доступу 18.

Необхідно налаштувати сервер НТТР, щоб на вузлах при вводі в рядку браузера <http://123.dnipro.ua> (<http://209.165.200.4>) відкривався веб-сайт.

Для захисту інформації у комп'ютерній системі підприємства необхідно:

- налаштувати мереж VLAN та також маршрутизації між ними;
- на портах комутаторів підключених до серверів налаштувати функцію безпеки портів;
- налаштувати VPN між LAN3 головного офісу та LAN4 віддаленого офісу.

Окремі підмережі повинні бути підключені через віртуальний канал передачі даних VPN, щоб забезпечити безпечну передачу даних. Необхідно використовувати підключення site-to-site з використанням IPsec для трафіку.

### **2.1.3 Вимоги до видів забезпечення комп'ютерної системи**

#### **2.1.3.1 Вимоги до математичного забезпечення**

Необхідно зробити розрахунок пропускнуєї спроможності мережі, щоб перевірити що мережа не буде перенавантажена. Швидкість надходження пакетів не повинна перевищувати швидкість її відправлення.

#### **2.1.3.2 Вимоги до інформаційного забезпечення**

Необхідно надати інформаційне забезпечення для усієї КС, а саме інформаційне забезпечення масивів даних , баз даних та іншої інформації у КС.

Системним адміністраторам має бути надана технічна документація обладнання над яким буде виконуватися обслуговування.

#### **2.1.3.3 Вимоги до лінгвістичного забезпечення.**

ПЗ можна поділити на два види: спеціальне та загальне.

До загального ПЗ відноситься програмне забезпечення для ПК, де повинне бути встановлена операційна система Windows 10, яка має підтримувати англійську та українську мову.

Спеціальне ПЗ повинне використовуватися для роботи з мережевим обладнанням, та підтримувати англійську мову інтерфейсу.

#### **2.1.3.4 Вимоги до технічного забезпечення.**

Під час проектування мережі, потрібно використовувати мережеве обладнання компанії CISCO та дотримуватися усіх норм та міжнародних стандартів.

Комутатори повинні мати не менше 24 портів Ethernet та не менше 2 портів Gigabit Ethernet.

Сервери повинні мати не менше 8ГБ оперативної пам'яті та мати Gigabit Ethernet порт.

Маршрутизатори повинні підтримувати слот розширення HWIC.

ПК має мати відеокарту не менше 16 ГБ оперативної пам'яті та не менше 480 ГБ пам'яті типу SSD.

#### **2.1.3.5 Вимоги до організаційного забезпечення**

Системні адміністратори повинні мати доступ до мережевого обладнання тільки з використанням аутентифікації.

#### **2.1.3.6 Вимоги до методичного забезпечення**

Мають бути надані топологічні схеми мережі, документація мережевого обладнання.

## **2.2 Розробка інженерних рішень і комплексу технічних засобів**

### **2.2.1 Вибір і обґрунтування структурної схеми комплексу технічних засобів комп'ютерної системи шляхом узгодження структури з топологічними особливостями об'єкту розробки**

Комп'ютерна мережа підприємства це складна та взаємозалежна система. До складу мережі підприємства входять: ПК, сервери, комутатори, маршрутизатори.

Основна функція для якої необхідна КС – це доступ до інтернету та зв'язок між підмережами.

Враховуючи раніше наведені вимоги, було розроблено структурну схему підприємства, яка зображена на рисунку 2.1.

Структурна схема поділяється на:

- internet – для комунікації з глобальною мережею та віддаленим офісом;
- маршрутизатори на рівні ядра – слугують для маршрутизації пакетів на мережевому рівні;
- комутатори рівня доступу – слугують для з'єднання вузлів;
- ПК – використовуються згідно з потребами підприємства;
- файловий сервер TFTP – слугує для операцій з файлами;
- web-сервер HTTP – слугує для обслуговування веб-сторінки;
- сервер DNS – слугує для перетворення доменних імен в IP-адреси і навпаки.

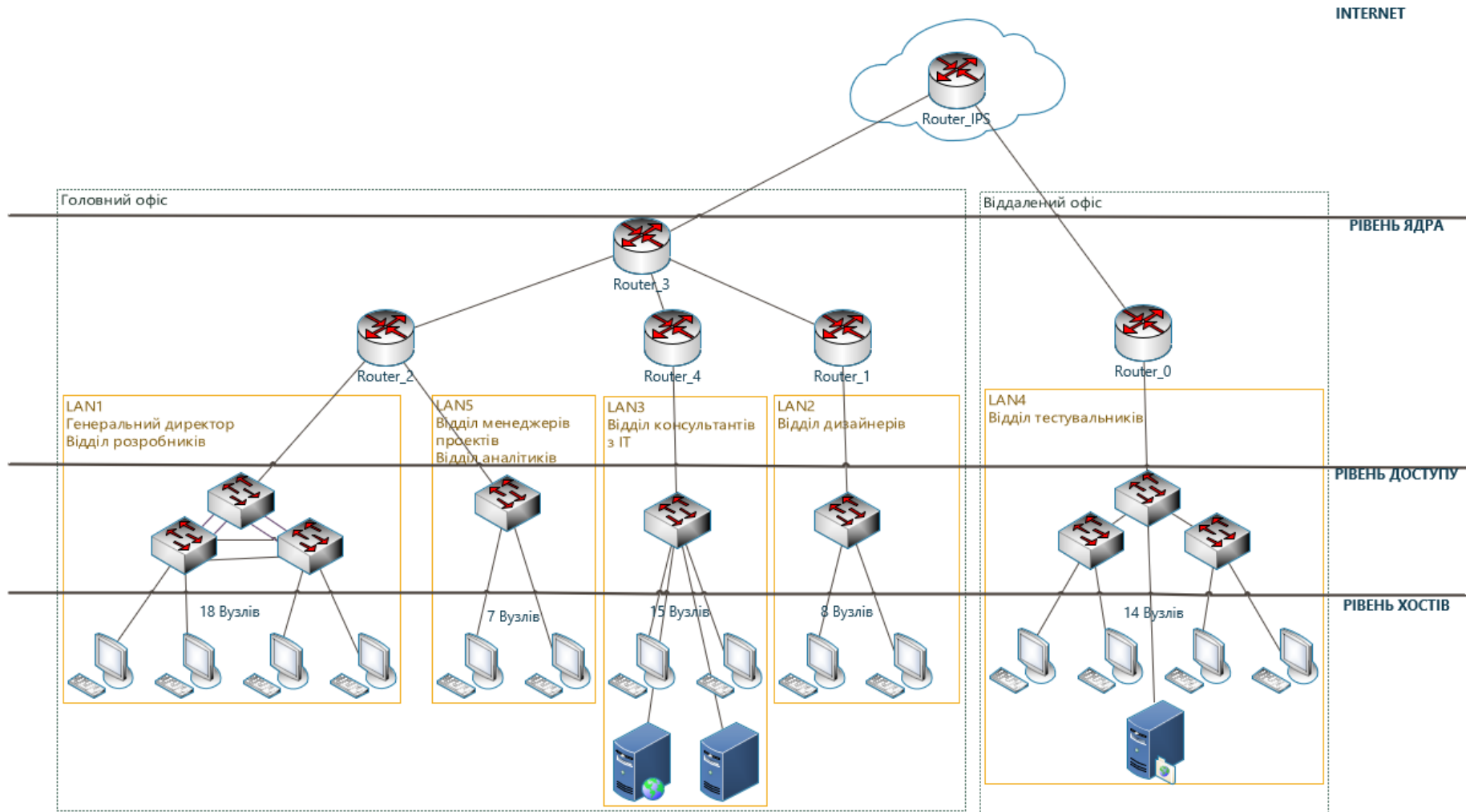


Рисунок 2.1 – Структурна схема підприємства

### 2.2.2 Розробка специфікацій апаратних засобів комп'ютерної системи

Вибір обладнання має великий вплив на ефективність і надійність мережі. Недостатньо потужне обладнання може призвести до перевантаження мережі та погіршення її продуктивності, тоді як надлишкове обладнання може бути зайвим та займати забагато місця.

Також варто враховувати потреби мережі в майбутньому та здатність обладнання працювати відповідно до збільшення обсягу даних.

Загалом, вибір обладнання є важливим етапом при проектуванні та налагодженні мережі, оскільки він визначає її продуктивність, надійність та здатність відповідати вимогам користувачів.

Cisco – це провідний виробник мережевого обладнання, і використання обладнання Cisco має декілька переваг:

- висока надійність. Обладнання Cisco відоме своєю високою надійністю, оскільки воно проходить високі стандарти тестування та валідації перед випуском на ринок;
- висока захищеність. Cisco надає безпеку на різних рівнях мережі, від захисту від шкідливого програмного забезпечення до захисту від кібератак;
- підтримка технологій майбутнього. Cisco завжди на передовій у впровадженні нових технологій, таких як мережі п'ятого покоління (5G), хмарні технології та штучний інтелект;
- гнучкість в налаштуванні. Обладнання Cisco має різні параметри та налаштування, що дозволяє адаптувати мережу до конкретних потреб підприємства.

Саме тому в мережі використовується обладнання цього виробника. В таблиці 2.1 зображено специфікацію мережевого та офісного обладнання.

В LAN1 – 18 ПК, для маршрутизації було обрано 3 комутатори по 24 порти, так як через 3 місяці кількість ПК, як і співробітників має вирости у 3 рази. Розраховуючи на те, що через 3 місяці штат робітників буде збільшений, а саме 51 ПК +10% , то такого комутатора буде достатньо для мережі.

В LAN2 – 8 ПК, та враховуючи, що кількість співробітників може збільшитись у 2 рази через декілька місяців, було вирішено узяти комутатор на 24 порти, що також задовільнить потреби запасу у 10%.

В LAN3 – 13 ПК та 2 сервери, враховуючи запас 10% , комутатор на 24 порти буде достатньо.

В LAN4 –13 ПК та 1 сервер, враховуючи, що через 3 місяці штат співробітників також виросте у 3 рази, було вирішено обрати 3 комутатори по 24 порти.

В LAN5 – 7 ПК , враховуючи, що штат співробітників також планує вирости у 2 рази, було обрано взяти комутатор на 24 порти.

Таблиця 2.1 – Специфікація обладнання

Позиція	Найменування і технічна характеристика	Тип, марка, позначення документа, опитувального листа	Одиниці виміру	Кількість	Примітки
1	2	3	4	5	6
1.	Маршрутизатор RJ-45 Ports: 3 Тип слота розширення: HWIC, PVDM Технологія Ethernet: Гігабітний Ethernet Вхідна напруга: 110 В змінного струму 220 В змінного струму	Cisco 2911/K9	од.	6	
2.	Інтерфейсний модуль Синхронна максимальна швидкість (на порт): 8 Мбіт/с Послідовні протоколи EIA-232, EIA-449, EIA-530, EIA-530A, V.35 і X.21	Cisco HWIC-2T	од.	7	



Продовження таблиці 2.1

Позиція	Найменування і технічна характеристика	Тип, марка, позначення документа, опитувального листа	Одиниці виміру	Кількість	Примітки
1	2	3	4	5	6
3.	<p>Коммутатор Деталі порту/слота розширення: 24 x Fast Ethernet Network 2 x Gigabit Ethernet Uplink 2 x Gigabit Ethernet Expansion Slot</p> <p>Управління: RMON, SNMP v1,2c,3, VLAN, QoS, CLI, DHCP, Telnet, HTTP, HTTPS, Системний журнал</p> <p>Вхідна напруга: 110 В змінного струму 220 В змінного струму</p>	Cisco WS-C2960-24LC-S	од.	9	Головний офіс – 6 од. Віддалений офіс – 3 од.
4.	<p>Сервер Кількість портів Ethernet 2 x RJ45 Швидкість з'єднання 1 Гбіт/с Тип процесора Intel Xeon E5 v3/v4</p>	Cisco UCS C240 M4 12 LFF 2U	од.	3	Головний офіс – 2 од. Віддалений офіс – 1 од.
5.	<p>Комп'ютер Відеокарта: GeForce RTX3060 Процесор: AMD Ryzen 5 5500 Обсяг оперативної пам'яті: 16 ГБ Обсяг SSD: 480 ГБ</p>	COBRA Advanced (A55.16.H1S 4.36.16983)	од.	59	Головний офіс – 45 од. Віддалений офіс – 13 од.

Кінець таблиці 2.1

Позиція	Найменування і технічна характеристика	Тип, марка, позначення документа, опитувального листа	Одиниці виміру	Кількість	Примітки
1	2	3	4	5	6
6.	Монітор Максимальна роздільна здатність дисплея: 1920x1080 Інтерфейси: VGA, DisplayPort, 2 x HDMI Споживана потужність: У режимі роботи: 22 Вт У режимі очікування: 0.3 Вт У вимкненому стані: 0.3 Вт	АОС 24G2SAE/B К	од.	59	Головний офіс – 45 од. Віддалений офіс – 13 од.
7.	Клавіатура та мишка (набір) Розкладка: Eng / Ru / Ukr Максимальна роздільна здатність сенсора, dpi: 1000 Комплектація набору: 2 в 1 Тип клавіатури: Мембранні Комплектація: Клавіатура Мишка, USB адаптер	Xiaomi Miiw Wireless	од.	59	Головний офіс – 45 од. Віддалений офіс – 13 од.

Розглянемо підбір системи кабельних каналів на прикладі відділу консультантів з ІТ (LAN3), який знаходиться у головному офісі. Для цього спроектуємо план розміщення вузлів КС та кабельні канали, що зображено на рисунку 2.2.

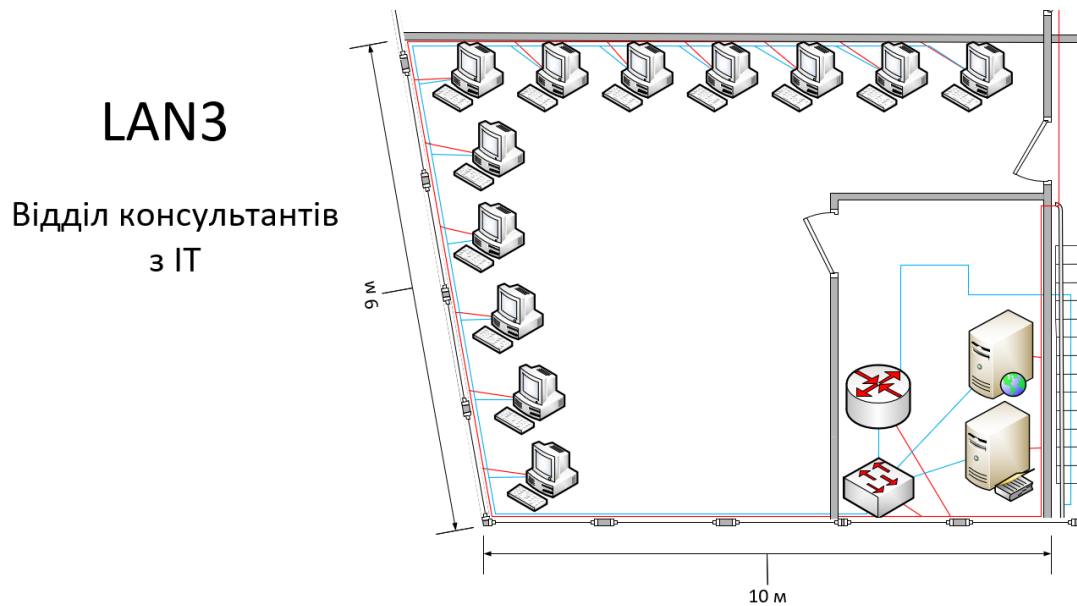


Рисунок 2.2 – Схема розташування кабельних каналів КС

Після проектування плану розміщення, складемо специфікацію кабельних каналів, яку зображено в таблиці 2.2.

Таблиця 2.2 – Специфікація кабельних каналів

Позиція	Найменування і технічна характеристика	Тип, марка, позначення документа, опитувального листа	Одиниці виміру	Кількість	Примітки
1	2	3	4	5	6
1.	Розетка RJ45 5e UTP Клас захисту: IP20 Кількість портів: 1	Schneider Electric Asfora RJ45	од.	15	Для LAN3
2.	Розетка живлення Asfora із заземленням Клас захисту: IP20	Розетка Schneider Electric	од.	18	Для LAN3
3.	Лан кабель	Патч-корд RZTK CAT5e RJ45 UTP	м	360	Для LAN3

Продовження таблиці 2.2

Позиція	Найменування і технічна характеристика	Тип, марка, позначення документа, опитувального листа	Одиниці виміру	Кількість	Примітки
1	2	3	4	5	6
4.	Кабель живлення	Мідний провід ПВС 3x1	м	40	Для LAN3
5.	Комутаційна коробка для комунікацій	Комутаційна коробка	од.	1	Для LAN3
6.	Кабель канал	Кабель канал 20x40 мм Копос	м	80	Для LAN3

### 2.2.3 Розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі підприємства.

В корпоративній мережі, яка використовується, встановлено обладнання компанії Cisco, а саме комутатори та маршрутизатори.

Трафік пересилається в лінію з пропускнуою здатністю, яка дорівнює 1000 мб/с.

Щоб мережа не була перенавантажена, швидкість надходження пакетів не повинна перевищувати швидкість її відправлення.

Під час обчислення будемо вважати, що мережею користуються 100% користувачів.

Середня інтенсивність трафіку  $\mu=129$  (кадрів/с), а середня довжина повідомлення – 650 байт.

В найбільшій мережі 18 ПК.

Пропускную здатність мережі необхідно обчислювати за наступною формулою:

$$F_{p.p} = \mu * 1 * N * 8 = 129 * 650 * 18 * 8 = 12,07 \text{ (Мбіт/с)} \quad (2.1)$$

З результатів видно, що в мережі не буде перевантажень.

Комутатор в мережі пересилає трафік до маршрутизатора, через лінію зі швидкістю 1000 Мбіт/с.

Розрахуємо кількість пакетів на секунду, яка не повина перевищувати на комутаторі:

$$\mu_{\text{вих}} = 1\,000\,000\,000 / (650 * 8) = 20830 \text{ пакетів/с} \quad (2.2)$$

Навантаження максимальне знаходимо так:

$$N = 20830 / 129 = 161 \text{ джерел} \quad (2.3)$$

Розрахуємо також інтенсивність вихідного трафіку від всіх користувачів, що дорівнює:

$$\lambda = N * \mu = 2322 \text{ (пакетів/с)} \quad (2.4)$$

Розрахуємо коефіцієнт затримки:

$$\rho = \lambda / \mu_{\text{вих}} = 2322 / 20830 = 0,11 \quad (2.5)$$

Коефіцієнт зайнятості комутатора розрахуємо наступним чином:

$$r = \rho / (1 - \rho) = 0,11 / (1 - 0,11) = 0,12 \quad (2.6)$$

Середня затримка кадру, яка пов'язана з чергою М/М/1 буде дорівнювати:

$$T = 1 / (\mu - \lambda) = 1 / (20830 - 2322) = 5,4 * 10^{-6} \text{ с} \quad (2.7)$$

Розрахуємо середню довжину черги:

$$L_{\text{чер}} = \rho^2 / (1 - \rho) = 0,11^2 / (1 - 0,11) = 0,0136 \quad (2.8)$$

Середній час, який перебуває пакет у черзі:

$$T_{\text{оч}} = L_{\text{чер}} / \lambda = 0,0136 / 2322 = 5,8 \text{ мкс} \quad (2.9)$$

Розрахуємо пропускну здатність для каналу:

$$\lambda = \text{пропускна здатність} / \text{довжина кадру} = b / l$$

$$b = \lambda * l = 2322 * 650 * 8 = 12,07 \text{ Мбіт/с} \quad (2.10)$$

Що є нормою та задовольняє потреби.

### 3 РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ ПІДПРИЄМСТВА

#### 3.1 Розрахунок схеми адресації корпоративної мережі

Для адресації в мережах LAN1 – LAN5 було виділено блок адресів 10.23.84.0/22, а для розподілення на підмережі, для збереження адресного простору обрано – VLSM.

Для адресації між маршрутизаторами в локальній мережі було виділено наступний блок адресів 10.0.18.0/24.

Згідно з вимогами замовника розбиваємо на 5 підмереж, кількість пристроїв мінімальну, під яку необхідно розраховувати зображено в таблиці 3.1.

Таблиця 3.1 – Розрахована кількість вузлів для підмереж

Підмережа	LAN1 Головний офіс	LAN2 Головний офіс	LAN3 Головний офіс	LAN4 Віддалений офіс	LAN5 Головний офіс
Кількість вузлів	50	27	79	39	76

LAN1– генеральний директор, відділ розробників.

LAN2 – відділ дизайнерів.

LAN3 – відділ консультантів з ІТ.

LAN4 – відділ тестувальників.

LAN5 – відділ менеджерів проектів, відділ аналітиків.

Почнемо розрахунок з найбільшої кількості підмереж – 79. Для цього потрібно вибрати маску підмережі, яка покриє 79 підмереж. Знайдемо найближчу степінь двійки, яка більша або рівна 79. В цьому випадку,  $2^7 = 128$ , тому нам потрібно 7 біт для представлення 79 підмереж. Маска підмережі буде /25 ( $32 - 7 = 25$ ). Перший доступний IP-адрес для підмережі буде 10.23.84.1, а останній – 10.23.84.126.

Подальші розрахунки виконуються аналогічно.

Результати розрахунків подано у таблиці 3.2.

Таблиця 3.2 – Схема адресації мережі

Назва мережі	Кількість вузлів	Номер мережі	Маска мережі	Початкове значення діапазону можливих адрес вузлів у підмережі	Кінцеве значення діапазону можливих адрес вузлів у підмережі
LAN1	22	10.23.85.0	255.255.255.192	10.23.85.1	10.23.85.62
LAN2	10	10.23.85.64	255.255.255.224	10.23.85.65	10.23.85.94
LAN3	16	10.23.84.0	255.255.255.128	10.23.84.1	10.23.84.126
LAN4 VLAN28	6	10.23.85.96	255.255.255.240	10.23.85.97	10.23.85.110
LAN4 VLAN38	6	10.23.85.112	255.255.255.240	10.23.85.113	10.23.85.126
LAN4 VLAN48	4	10.23.85.128	255.255.255.240	10.23.85.129	10.23.85.142
VLAN99	5	10.23.85.144	255.255.255.248	10.23.85.145	10.23.85.150
LAN5	9	10.23.84.128	255.255.255.128	10.23.84.129	10.23.84.254
LAN6	2	10.0.18.0	255.255.255.252	10.0.18.1	10.0.18.2
LAN7	2	10.0.18.4	255.255.255.252	10.0.18.5	10.0.18.6
LAN8	2	10.0.18.8	255.255.255.252	10.0.18.9	10.0.18.10
WAN1	2	209.165.202.0	255.255.255.252	209.165.202.1	209.165.202.2
WAN2	30	209.165.200.0	255.255.255.224	209.165.200.1	209.165.200.30
WAN3	2	64.100.13.0	255.255.255.252	64.100.13.1	64.100.13.2
WAN4	2	209.165.201.0	255.255.255.240	209.165.201.1	209.165.201.14

Налаштування у цьому розділі у вигляді конфігурацій деяких основних пристроїв будуть наведені у додатку Б.

### 3.2 Розрахунок схеми адресації пристроїв

В таблиці 3.3 наведена адресація мережевого обладнання що присутні у мережі.

Таблиця 3.3 – Схема адресація мережевого обладнання

Пристрій	Інтерфейс	IP-адреса	Маска	Номер мережі
Shvec_Router_0	Gig0/1.28	10.23.85.97	255.255.255.240	10.23.85.96
	Gig0/1.38	10.23.85.113	255.255.255.240	10.23.85.112
	Gig0/1.48	10.23.85.129	255.255.255.240	10.23.85.128
	Gig0/1.99	10.23.85.145	255.255.255.248	10.23.85.144
	Se0/1/0	64.100.13.1	255.255.255.252	64.100.13.0
Shvec_Router_1	Gig0/0	10.23.85.65	255.255.255.224	10.23.85.64
	Se0/0/1	10.0.18.5	255.255.255.252	10.0.18.0
Shvec_Router_2	Gig0/0	10.23.85.1	255.255.255.192	10.23.85.0
	Gig0/1	10.23.84.129	255.255.255.128	10.23.84.128
	Se0/0/0	10.0.18.1	255.255.255.252	10.0.18.0
Shvec_Router_3	Se0/0/0	10.0.18.2	255.255.255.252	10.0.18.0
	Se0/0/1	10.0.18.6	255.255.255.252	10.0.18.4
	Se0/1/0	10.0.18.10	255.255.255.252	10.0.18.8
	Se0/1/1	209.165.202.2	255.255.255.252	209.165.202.0
Shvec_Router_4	Gig0/0	10.23.84.1	255.255.255.128	10.23.84.0
	Se0/1/0	10.0.18.9	255.255.255.252	10.0.18.8
Shvec_Router_IPS	Gig0/0	209.165.201.1	255.255.255.240	209.165.201.0
	Se0/1/0	64.100.13.2	255.255.255.252	64.100.13.0
	Se0/1/1	209.165.202.1	255.255.255.252	209.165.202.0
Shvec_Switch_0	Vlan99	10.23.85.146	255.255.255.248	10.23.85.144
Shvec_Switch_1	Vlan99	10.23.85.147	255.255.255.248	10.23.85.144
Shvec_Switch_2	Vlan99	10.23.85.148	255.255.255.248	10.23.85.144
Shvec_Switch_3	Vlan1	10.23.84.130	255.255.255.128	10.23.84.128
Shvec_Switch_4	Vlan1	10.23.85.2	255.255.255.192	10.23.85.0
Shvec_Switch_5	Vlan1	10.23.85.3	255.255.255.192	10.23.85.0
Shvec_Switch_6	Vlan1	10.23.85.4	255.255.255.192	10.23.85.0
Shvec_Switch_7	Vlan1	10.23.85.66	255.255.255.224	10.23.85.64
Shvec_Switch_8	Vlan1	10.23.84.2	255.255.255.128	10.23.84.0
Shvec_Server_DNS	Vlan1	10.23.84.28	255.255.255.128	10.23.84.1
Shvec_Server_HTTP	Vlan1	10.23.84.29	255.255.255.128	10.23.84.1
Shvec_Server_TFTP	Vlan28	10.23.85.98	255.255.255.240	10.23.85.96

В таблиці 3.4 наведено адресацію всіх ПК в мережах.



Таблиця 3.4 – Схема адресація ПК

Пристрій	Інтерфейс	IP-адреса	Маска	Шлюз	VLAN
Shvec_PC_1 – Shvec_PC_18	Fa0	DHCP	255.255.255.19 2	10.23.85.1	1
Shvec_PC_19 – Shvec_PC_26	Fa0	DHCP	255.255.255.22 4	10.23.85.65	1
Shvec_PC_27 – Shvec_PC_33	Fa0	DHCP	255.255.255.12 8	10.23.84.129	1
Shvec_PC_34 - Shvec_PC_45	Fa0	DHCP	255.255.255.12 8	10.23.84.1	1
Shvec_PC_46	Fa0	209.165.201. 5	255.255.255.24 0	209.165.201. 1	1
Shvec_PC_47, Shvec_PC_58, Shvec_PC_59	Fa0	DHCP	255.255.255.24 0	10.23.85.97	48
Shvec_PC_48, Shvec_PC_50, Shvec_PC_51 Shvec_PC_56, Shvec_PC_57	Fa0	DHCP	255.255.255.24 0	10.23.85.113	38
Shvec_PC_49, Shvec_PC_52, Shvec_PC_53, Shvec_PC_54, Shvec_PC_55	Fa0	DHCP	255.255.255.24 0	10.23.85.129	28

### 3.3 Розробка топологічної схеми корпоративної мережі

Загальна топологічна схема підприємства була розроблена в програмі Cisco Packet Tracer. Схема мережі складається з 5 мереж LAN або 2 офісів.

Загальну топологічну схему підприємства зображено на рисунку 3.1.

Топологічні схемі підмереж зображено на рисунках 3.2 – 3.6.

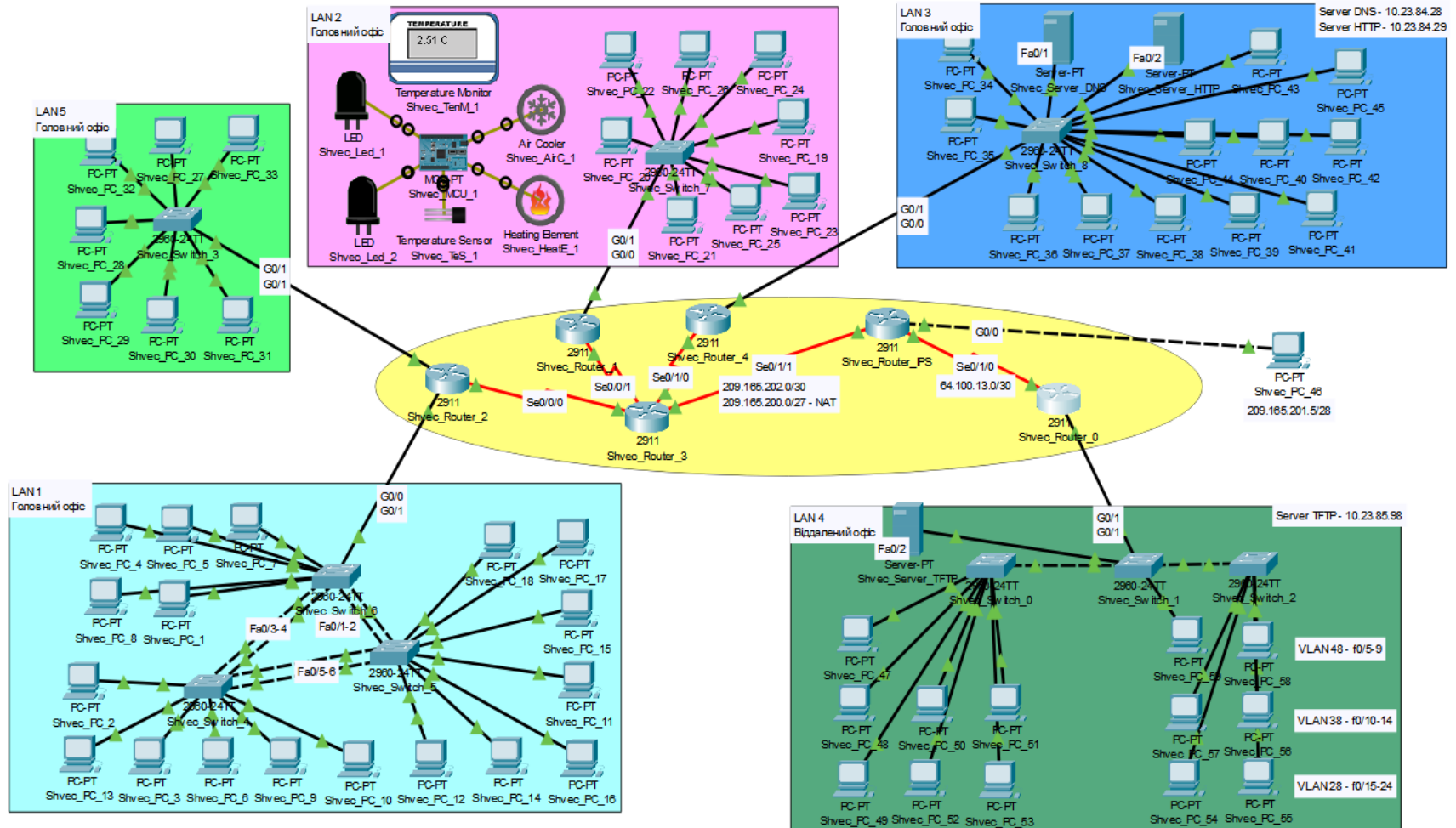


Рисунок 3.1 – Топологічна схема (логічна) комп’ютерної системи

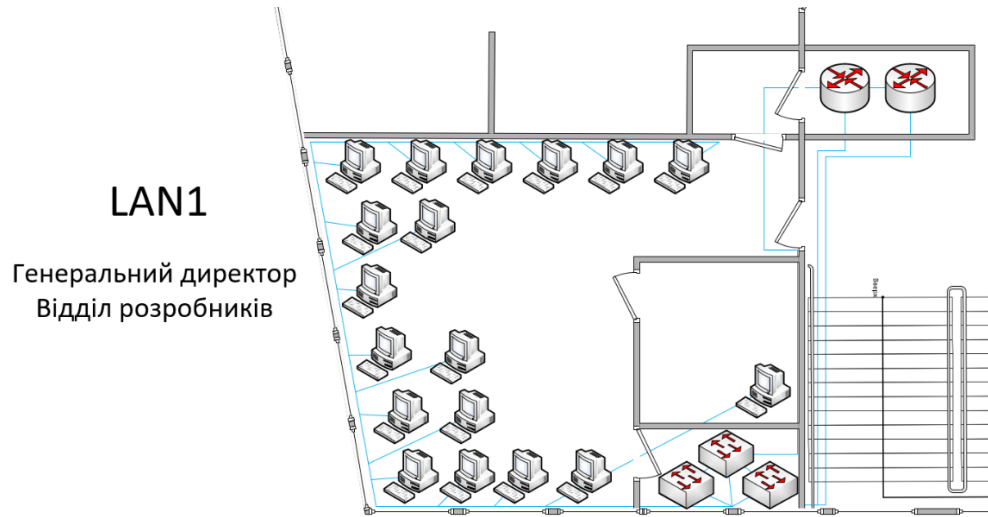


Рисунок 3.2 – Топологічна схема LAN1



Рисунок 3.3 – Топологічна схема LAN2

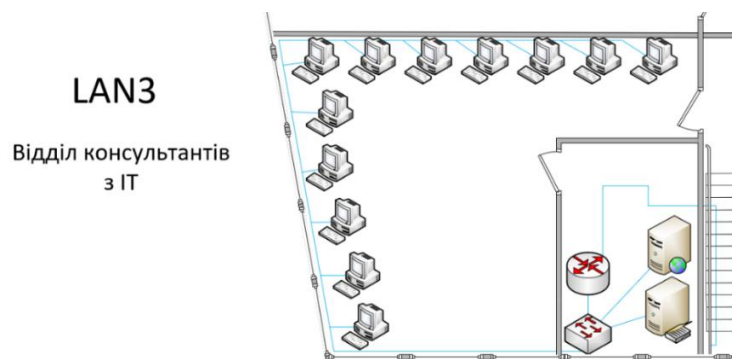


Рисунок 3.4 – Топологічна схема LAN3

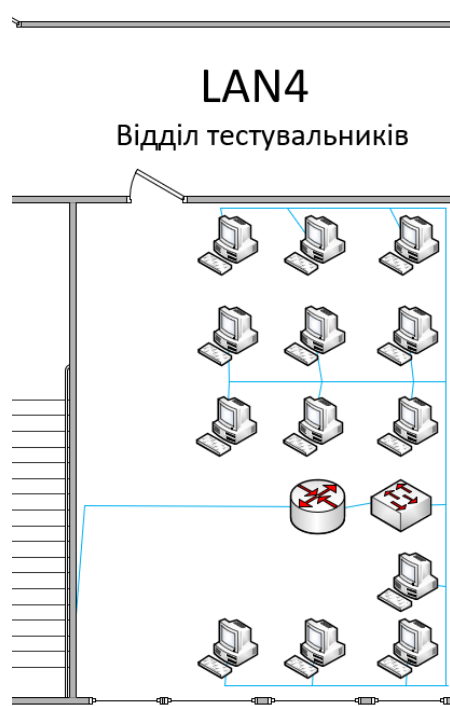


Рисунок 3.5 – Топологічна схема LAN4



Рисунок 3.6 – Топологічна схема LAN5

### 3.4 Розрахунок налаштувань маршрутизації корпоративної мережі

Маршрутизація – це процес передачі пакетів даних в мережі з одного вузла до іншого. У процесі маршрутизації, маршрутизатори визначають оптимальний

шлях для пересилання пакетів на основі інформації про стан мережі та вмісту таблиці маршрутизацій.

Існують різні два види маршрутизації:

- статична маршрутизація. При статичній маршрутизації адміністратор вручну налаштовує маршрутизатор для визначення шляху пересилання пакетів. Ці маршрути задаються вручну та не змінюються автоматично при зміні стану мережі. Статична маршрутизація використовується, коли мережева топологія стабільна та зміни в маршрутах відбуваються рідко;

- динамічна маршрутизація. У динамічній маршрутизації маршрутизатори обмінюються інформацією про стан мережі та автоматично оновлюють свої маршрути. Інформація про стан мережі передається за допомогою протоколів маршрутизації, таких як OSPF (Open Shortest Path First), RIP (Routing Information Protocol), EIGRP (Enhanced Interior Gateway Routing Protocol) тощо. Динамічна маршрутизація зручна для мереж змінної топології, оскільки маршрути автоматично оновлюються при зміні стану мережі.

В мережі маршрутизація була налаштована за допомогою динамічного протоколу маршрутизації OSPF.

OSPF має такі переваги:

- висока швидкість збіжності проти дистанційно-векторних протоколів маршрутизації;
- підтримка мережевих масок змінної довжини (VLSM);
- оптимальне використання пропускної спроможності з побудовою дерева найкоротших шляхів.

Перед налаштуванням маршрутизації необхідно усім мережевим пристроям назначити IP адресу, маску мережі згідно таблиць маршрутизації.

Приклад налаштування для Shvec\_Router\_2.

```
Shvec_Router_2(config)#interface GigabitEthernet0/0
```

```
Shvec_Router_2(config-if)#ip address 10.23.85.1 255.255.255.192
```

```
Shvec_Router_2(config)#interface GigabitEthernet0/1
```

```
Shvec_Router_2(config-if)#ip address 10.23.84.129 255.255.255.128
```

```
Shvec_Router_2(config-if)#
```

```
Shvec_Router_2(config-if)#exit
```

```
Shvec_Router_2(config)#interface Serial0/0/0
```

```
Shvec_Router_2(config-if)#ip address 10.0.18.1 255.255.255.252
```

Для інших пристроїв налаштування буде схожим чином.

Налаштування OSPF здійснюється наступним чином.

Включимо прокол OSPF на маршрутизаторі командою.

```
Shvec_Router_2(config)#router ospf 1
```

Відключимо поширення оновлень маршрутизації на всі інтерфейси, вбивши команду.

```
Shvec_Router_2(config-router)#passive-interface default
```

Наступною командою вкажемо інтерфейси, на які необхідно передавати оновлення.

```
Shvec_Router_2(config-router)#no passive-interface se0/0/0
```

Далі вкажемо всі мережі, які підключені до маршрутизатора.

```
Shvec_Router_2(config-router)#network 10.23.85.0 0.0.0.63 area 0
```

```
Shvec_Router_2(config-router)#network 10.23.84.128 0.0.0.127 area 0
```

```
Shvec_Router_2(config-router)#network 10.0.18.0 0.0.0.3 area 0
```

Так як використовується протокол OSPF, то необхідно змінити еталонну пропускну спроможність для обчислення вартості за умовчанням для дозволу інтерфейсів Gigabit на значення = 1000, що виконаємо наступними командами.

```
Shvec_Router_2(config)#interface gigabitEthernet 0/0
```

```
Shvec_Router_2(config-if)#ip ospf cost 1000
```

```
Shvec_Router_2(config-if)#ex
```

```
Shvec_Router_2(config)#interface gigabitEthernet 0/1
```

```
Shvec_Router_2(config-if)#ip ospf cost 1000
```

```
Shvec_Router_2(config-if)#
```

Також на маршрутизаторі Shvec\_Router\_3 вкажемо статичний маршрут для виходу в інтернет, який вказує, що якщо в локальній мережі немає пристроїв з таким адресом, то пересилати пакети на маршрутизатор провайдера для подальшої маршрутизації. Виконаємо налаштування наступною командою.

```
Shvec_Router_3(config)#ip route 0.0.0.0 0.0.0.0 Serial0/1/1
```

Виконаємо перевірку таблиць маршрутизації (рисунок 3.7-3.10). Кожен із маршрутизаторів, окрім підключених мереж з символом “С”, має відомості про відділені мережі, отримані по протоколу OSPF з символом “О”.

```
Shvec_Router_1#sh ip rou
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is 10.0.18.6 to network 0.0.0.0

    10.0.0.0/8 is variably subnetted, 9 subnets, 5 masks
O       10.0.18.0/30 [110/128] via 10.0.18.6, 00:23:52, Serial0/0/1
C       10.0.18.4/30 is directly connected, Serial0/0/1
L       10.0.18.5/32 is directly connected, Serial0/0/1
O       10.0.18.8/30 [110/128] via 10.0.18.6, 00:23:52, Serial0/0/1
O       10.23.84.0/25 [110/129] via 10.0.18.6, 00:23:42, Serial0/0/1
O       10.23.84.128/25 [110/1128] via 10.0.18.6, 00:04:50, Serial0/0/1
O       10.23.85.0/26 [110/1128] via 10.0.18.6, 00:23:42, Serial0/0/1
C       10.23.85.64/27 is directly connected, GigabitEthernet0/0
L       10.23.85.65/32 is directly connected, GigabitEthernet0/0
O*E2 0.0.0.0/0 [110/1] via 10.0.18.6, 00:23:52, Serial0/0/1

Shvec Router 1#
```

Рисунок 3.7 – Таблиця маршрутизації на Shvec\_Router\_1

```
Shvec_Router_2#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is 10.0.18.2 to network 0.0.0.0

    10.0.0.0/8 is variably subnetted, 10 subnets, 5 masks
C       10.0.18.0/30 is directly connected, Serial0/0/0
L       10.0.18.1/32 is directly connected, Serial0/0/0
O       10.0.18.4/30 [110/7564] via 10.0.18.2, 00:13:10, Serial0/0/0
O       10.0.18.8/30 [110/7564] via 10.0.18.2, 00:13:10, Serial0/0/0
O       10.23.84.0/25 [110/7565] via 10.0.18.2, 00:13:10, Serial0/0/0
C       10.23.84.128/25 is directly connected, GigabitEthernet0/1
L       10.23.84.129/32 is directly connected, GigabitEthernet0/1
C       10.23.85.0/26 is directly connected, GigabitEthernet0/0
L       10.23.85.1/32 is directly connected, GigabitEthernet0/0
O       10.23.85.64/27 [110/7565] via 10.0.18.2, 00:13:10, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 10.0.18.2, 00:13:10, Serial0/0/0
```

Рисунок 3.8 – Таблиця маршрутизації на Shvec\_Router\_2

```

Shvec_Router_3#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

10.0.0.0/8 is variably subnetted, 10 subnets, 5 masks
C 10.0.18.0/30 is directly connected, Serial0/0/0
L 10.0.18.2/32 is directly connected, Serial0/0/0
C 10.0.18.4/30 is directly connected, Serial0/0/1
L 10.0.18.6/32 is directly connected, Serial0/0/1
C 10.0.18.8/30 is directly connected, Serial0/1/0
L 10.0.18.10/32 is directly connected, Serial0/1/0
O 10.23.84.0/25 [110/65] via 10.0.18.9, 00:23:01, Serial0/1/0
O 10.23.84.128/25 [110/1064] via 10.0.18.1, 00:03:59, Serial0/0/0
O 10.23.85.0/26 [110/1064] via 10.0.18.1, 00:23:01, Serial0/0/0
O 10.23.85.64/27 [110/65] via 10.0.18.5, 00:23:01, Serial0/0/1
209.165.202.0/24 is variably subnetted, 2 subnets, 2 masks
C 209.165.202.0/30 is directly connected, Serial0/1/1
L 209.165.202.2/32 is directly connected, Serial0/1/1
S* 0.0.0.0/0 is directly connected, Serial0/1/1

Shvec_Router_3#

```

Рисунок 3.9 – Таблиця маршрутизації на Shvec\_Router\_3

```

Shvec_Router_4#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 10.0.18.10 to network 0.0.0.0

10.0.0.0/8 is variably subnetted, 9 subnets, 5 masks
O 10.0.18.0/30 [110/128] via 10.0.18.10, 00:24:37, Serial0/1/0
O 10.0.18.4/30 [110/128] via 10.0.18.10, 00:24:37, Serial0/1/0
C 10.0.18.8/30 is directly connected, Serial0/1/0
L 10.0.18.9/32 is directly connected, Serial0/1/0
C 10.23.84.0/25 is directly connected, GigabitEthernet0/0
L 10.23.84.1/32 is directly connected, GigabitEthernet0/0
O 10.23.84.128/25 [110/1128] via 10.0.18.10, 00:05:45, Serial0/1/0
O 10.23.85.0/26 [110/1128] via 10.0.18.10, 00:24:08, Serial0/1/0
O 10.23.85.64/27 [110/129] via 10.0.18.10, 00:24:37, Serial0/1/0
O*E2 0.0.0.0/0 [110/1] via 10.0.18.10, 00:24:37, Serial0/1/0

Shvec Router 4#

```

Рисунок 3.10 – Таблиця маршрутизації на Shvec\_Router\_4

## 3.5 Налаштування та перевірка роботи комп'ютерної системи

### 3.5.1 Базове налаштування конфігурації пристроїв

Згідно з технічними вимогами та в цілях забезпечення безпеки, необхідно зробити базове налаштування конфігурації пристроїв, що і було виконано:

- назначити назви пристроям за наступним правилом Shvec\_Пристрій\_Номер;
- на всіх пристроях назначити пароль cisco до консолі і vty;
- на всіх пристроях назначити пароль class до привілейованого режиму;



- усі паролі, що зберігаються у відкритому вигляді, під час налаштування моделі комп'ютерної системи зашифрувати;
- розробити банер MOTD;
- назначити на усіх лініях vty використання протоколу ssh;
- призначити на всіх пристроях користувача за правилом: 123191\_Shvec з паролем admincisco;
- в якості імені домена використати ім'я пристрою. Для шифрування даних створити ключ RSA завдовжки 1024 біт;
- на DCE-інтерфейсах маршрутизаторів призначити встановлення значення тактової частоти – 128000.

Приклад налаштування на маршрутизаторі Shvec\_Router\_2.

Призначимо назву за правилом Shvec\_Пристрій\_Номер.

```
Shvec_Router_2(config)#hostname Shvec_Router_2
```

Призначимо пароль cisco до консолі і vty.

```
Shvec_Router_2(config)#line console 0
```

```
Shvec_Router_2(config-line)#password cisco
```

```
Shvec_Router_2(config-line)#login
```

```
Shvec_Router_2(config-line)#exit
```

```
Shvec_Router_2(config)#line vty 0 15
```

```
Shvec_Router_2(config-line)#password cisco
```

```
Shvec_Router_2(config-line)#login
```

```
Shvec_Router_2(config-line)#
```

Призначимо пароль class до привілейованого режиму

```
Shvec_Router_2(config)#enable secret class
```

Паролі, що зберігаються у відкритому вигляді зашифруємо.

```
Shvec_Router_2(config)#service password-encryption
```

Розробимо банер MOTD.

```
Shvec_Router_2(config)#banner motd "Welcome to Shvec_Router_2"
```

Призначимо на усіх лініях vty використання протоколу ssh.

```
Shvec_Router_2(config)#line vty 0 15
```

```
Shvec_Router_2(config-line)#transport input ssh
```

Призначимо на всіх пристроях користувача за правилом: 123191\_Shvec з паролем admincisco.

```
Shvec_Router_2(config)#username 123191_Shvec privilege 15 secret admincisco
```

В якості імені домена використаємо ім'я пристрою.

```
Shvec_Router_2(config)#ip domain name Shvec_Router_2
```

Для шифрування даних створимо ключ RSA завдовжки 1024 біт.

```
Shvec_Router_2(config)#crypto key generate rsa
```

The name for the keys will be: Shvec\_Router\_2.Shvec\_Router\_2

Choose the size of the key modulus in the range of 360 to 4096 for your

General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]: 1024

На DCE-інтерфейсах маршрутизаторів призначимо встановлення значення тактової частоти – 128000.

```
Shvec_Router_2(config-if)#clock rate 128000
```

Після налаштування збережемо конфігурацію пристрою.

```
Shvec_Router_2#copy running-config startup-config
```

### **3.5.2 Налаштування маршрутизаторів корпоративної мережі**

Окрім OSPF та статичних маршрутів на маршрутизаторах необхідно виконати ще ряд налаштувань, а саме:

- задати пропускну спроможність на serial-інтерфейсах = 128 Кб/с, вартість метрики = 7500;

- налаштування DHCP.

Також необхідно виконати налаштування всіх маршрутизаторів на підтримку служби AAA таким чином:

- для перевірки підключень до VTY ліній на маршрутизаторі використовувати локальну базу даних користувачів;
- для доступу до консолі використовувати аутентифікацію на основі протоколу RADIUS і якщо немає – локальну базу даних;
- radius-сервер налаштувати наступним чином: ключове слово – radius123;
- в якості облікового запису користувачів використовувати ім'я пристрою з паролем admin123.

Налаштування на прикладі Shvec\_Router\_3.

Задамо пропускну спроможність на serial-інтерфейсах = 128 Кб/с, вартість метрики = 7500.

```
Shvec_Router_3(config)#interface Serial0/0/0
```

```
Shvec_Router_3(config-if)#bandwidth 128
```

```
Shvec_Router_3(config-if)#delay 7500
```

Наступні налаштування виконаємо на прикладі Shvec\_Router\_2.

Налаштуємо DHCP для мережі LAN5.

```
Shvec_Router_2(config)#ip dhcp pool 18
```

```
Shvec_Router_2(dhcp-config)# network 10.23.84.128 255.255.255.128
```

```
Shvec_Router_2(dhcp-config)# default-router 10.23.84.129
```

```
Shvec_Router_2(dhcp-config)# dns-server 10.23.84.28
```

```
Shvec_Router_2(dhcp-config)#exit
```

```
Shvec_Router_2(config)#ip dhcp pool 19
```

```
Shvec_Router_2(dhcp-config)# network 10.23.85.0 255.255.255.192
```

```
Shvec_Router_2(dhcp-config)# default-router 10.23.85.1
```

```
Shvec_Router_2(dhcp-config)# dns-server 10.23.84.28
```

```
Shvec_Router_2(dhcp-config)#
```

Далі вмажемо виключення з пулу адресів для DHCP.

```
Shvec_Router_2(config)#ip dhcp excluded-address 10.23.84.129 10.23.84.138
```

```
Shvec_Router_2(config)#ip dhcp excluded-address 10.23.85.1 10.23.85.10
```

Для перевірки підключень до VTY ліній на маршрутизаторі використовуємо локальну базу даних користувачів.

```
Shvec_Router_2(config)#line vty 0 15
```

```
Shvec_Router_2(config-line)#login local
```

Для доступу до консолі використовувати аутентифікацію на основі протоколу RADIUS і якщо немає – локальну базу даних.

```
Shvec_Router_2(config)#aaa new-model
```

```
Shvec_Router_2(config)#aaa authentication login default group radius local
```

```
Shvec_Router_2(config)#radius-server host 10.23.84.28 key radius123
```

RADIUS-сервер налаштовуємо наступним чином: ключове слово – radius123, в якості облікового запису користувачів використовувати ім'я пристрою з паролем admin123. Приклад налаштування для Shvec\_Router\_2 зображено на рисунку 3.11.

В якості Radius сервера будемо використовувати сервер який вже використовується для DNS, для зменшення витрат.

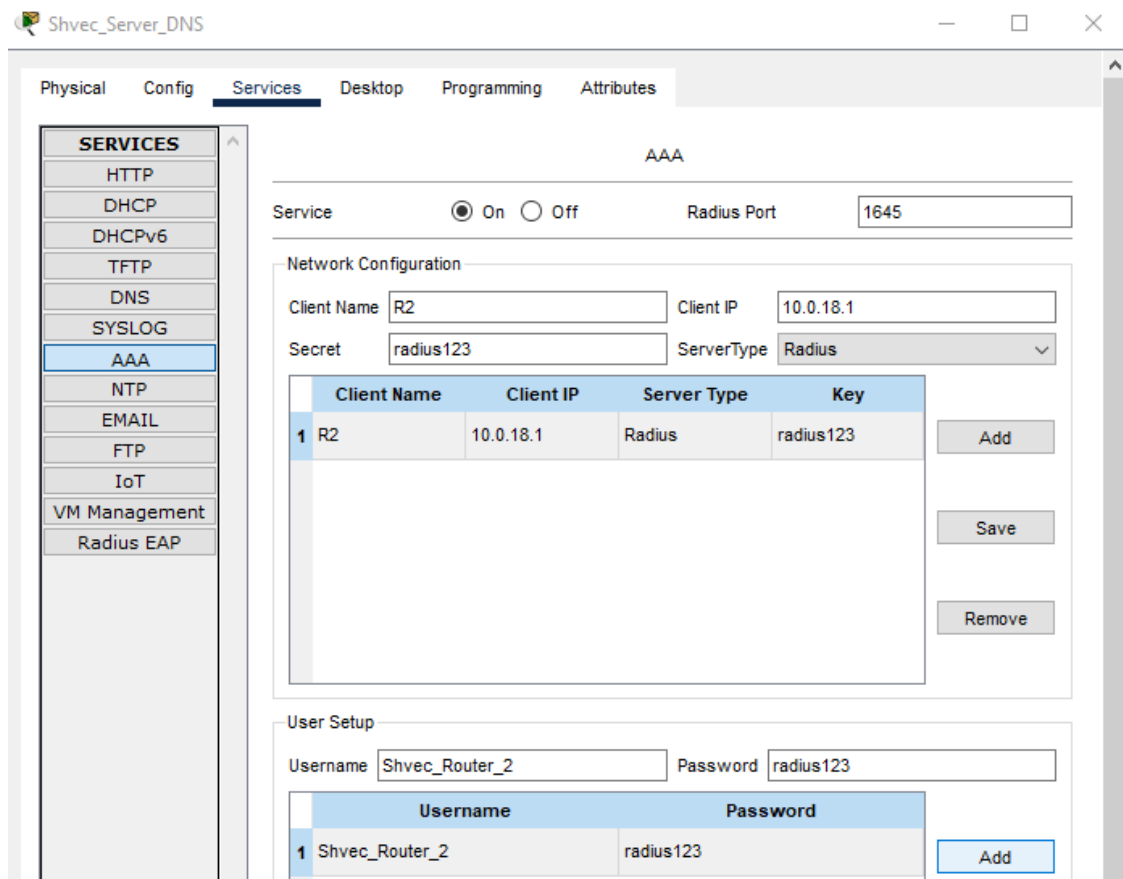


Рисунок 3.11 – Налаштування Radius сервера

### 3.5.3 Налаштування агрегування каналів

Агрегація каналів (channel aggregation) дозволяє комбінувати кілька фізичних каналів в один логічний канал для збільшення пропускної здатності та надійності з'єднання. Для агрегації каналів на маршрутизаторі Cisco ви можна використовувати технологію EtherChannel, яка дозволяє створювати логічні групи з фізичних інтерфейсів.

Згідно технічного завдання в мережі Lan1 необхідно виконати агрегування каналів.

Налаштування комутатора Shvec\_Switch\_6.

```
Shvec_Switch_6(config)#interface range f0/1-4
```

```
Shvec_Switch_6(config)#shutdown
```

```
Shvec_Switch_6(config)#interface range f0/1-2
```

```
Shvec_Switch_6(config-if-range)#channel-group 1 mode auto
```

```
Shvec_Switch_6(config-if-range)#interface range f0/3-4
```

```
Shvec_Switch_6(config-if-range)#channel-group 3 mode auto
```

```
Shvec_Switch_6(config-if-range)#interface Port-channel 1
```

```
Shvec_Switch_6(config-if)# switchport mode trunk
```

```
Shvec_Switch_6(config-if)# interface Port-channel 3
```

```
Shvec_Switch_6(config-if)# switchport mode trunk
```

```
Shvec_Switch_6(config)#interface range f0/1-4
```

```
Shvec_Switch_6(config)#no shutdown
```

Налаштування комутатора Shvec\_Switch\_5.

```
Shvec_Switch_6(config)#interface range f0/1-2
```

```
Shvec_Switch_6(config)# shutdown
```

```
Shvec_Switch_6(config)#interface range f0/5-6
```

```
Shvec_Switch_6(config)# shutdown
```

```
Shvec_Switch_5(config)#interface range f0/1-2
```

```
Shvec_Switch_5(config-if-range)#channel-group 1 mode desirable
```

```
Shvec_Switch_5(config-if-range)#interface range f0/5-6
```

```

Shvec_Switch_5(config-if-range)#channel-group 2 mode desirable
Shvec_Switch_5(config-if-range)#interface Port-channel 1
Shvec_Switch_5(config-if)#switchport mode trunk
Shvec_Switch_5(config-if)#interface Port-channel 2
Shvec_Switch_5(config-if)#switchport mode trunk
Shvec_Switch_6(config)#interface range f0/1-2
Shvec_Switch_6(config)# no shutdown
Shvec_Switch_6(config)#interface range f0/5-6
Shvec_Switch_6(config)# no shutdown
Налаштування комутатора Shvec_Switch_4.
Shvec_Switch_6(config)#interface range f0/3-6
Shvec_Switch_6(config)# shutdown
Shvec_Switch_4(config)#interface range f0/3-4
Shvec_Switch_4(config-if-range)#channel-group 3 mode auto
Shvec_Switch_4(config-if-range)#interface range f0/5-6
Shvec_Switch_4(config-if-range)#channel-group 2 mode desirable
Shvec_Switch_4(config-if-range)#interface Port-channel 2
Shvec_Switch_4(config-if)#switchport mode trunk
Shvec_Switch_4(config-if)#interface Port-channel 3
Shvec_Switch_4(config-if)#switchport mode trunk
Shvec_Switch_6(config)#interface range f0/3-6
Shvec_Switch_6(config)#no shutdown

```

### 3.5.4 Налаштування роботи Інтернет

Згідно технічного завдання необхідно:

- для виходу робочих станцій в Інтернет необхідно налаштувати пограничний маршрутизатор з динамічним NAT за такими даними: ім'я пула – Internet, пул адресів з 209.165.200.5 по 209.165.200.30, номер списку доступу 18;

– налаштувати сервер HTTP, щоб на вузлах при вводі в рядку браузера `http://123.dnipro.ua` (`http://209.165.200.4`) відкривався веб-сайт з відомостями про тему та завдання на кваліфікаційну роботу студента.

Налаштування проводимо на маршрутизаторі, який граничить з маршрутизатором провайдера.

Налаштування NAT на `Shvec_Router_3`.

Створимо пул Internet.

```
Shvec_Router_3(config)#ip nat pool Internet 209.165.200.5 209.165.200.30
netmask 255.255.255.224
```

Налаштуємо списки доступу.

```
Shvec_Router_3(config)#access-list 18 permit 10.23.84.0 0.0.3.255
```

```
Shvec_Router_3(config)#access-list 18 permit 10.0.18.0 0.0.0.255
```

Налаштуємо NAT.

```
Shvec_Router_3(config)#ip nat inside source list 18 pool Internet
```

Далі вкажемо, які інтерфейси вихідні, а які вхідні.

```
Shvec_Router_3(config-if)#int se0/1/0
```

```
Shvec_Router_3(config-if)#ip nat inside
```

```
Shvec_Router_3(config-if)#int se0/0/1
```

```
Shvec_Router_3(config-if)#ip nat inside
```

```
Shvec_Router_3(config-if)#int se0/0/0
```

```
Shvec_Router_3(config-if)#ip nat inside
```

```
Shvec_Router_3(config-if)#int se0/1/1
```

```
Shvec_Router_3(config-if)#ip nat out
```

Тепер налаштуємо статичний нат для серверу HTTP та DNS.

```
Shvec_Router_3(config-if)#ip nat inside source static 10.23.84.29 209.165.200.4
```

```
Shvec_Router_3(config)#ip nat inside source static 10.23.84.28 209.165.200.3
```

Налаштуємо сервер DNS щоб при вводі `http://123.dnipro.ua` (`http://209.165.200.4`) відкривався веб-сайт з відомостями про тему та завдання на кваліфікаційну роботу студента.

Результат налаштування серверу DNS зображено на рисунку 3.12.

Результат переходу на сайт зображено на рисунку 3.13.

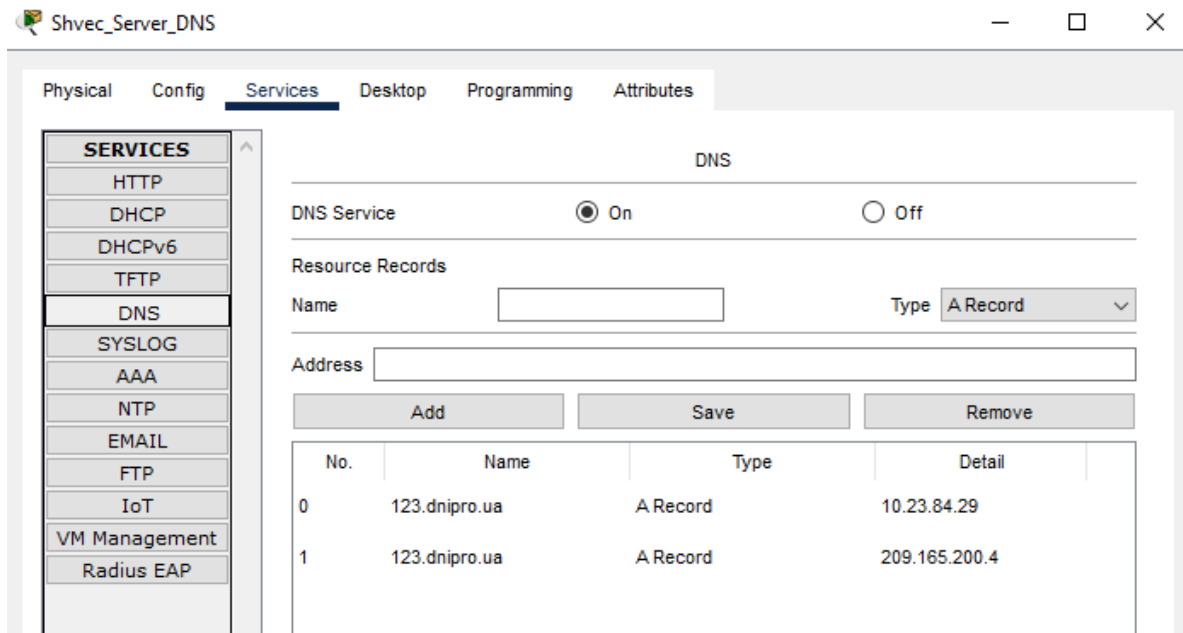


Рисунок 3.12 – Налаштування DNS серверу

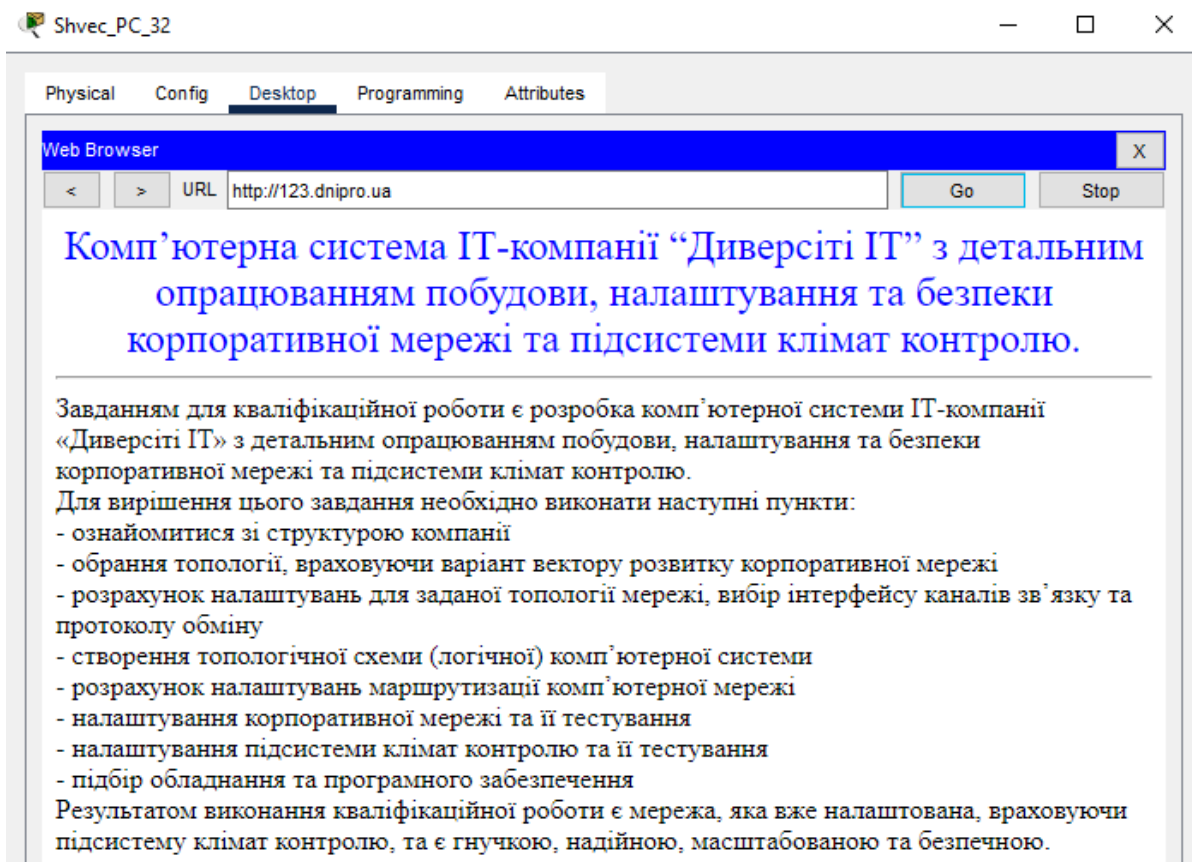


Рисунок 3.13 – Сайт <http://123.dnipro.ua>



Налаштування NAT на Shvec\_Router\_0.

Вкажемо вхідні та вихідні інтерфейси.

```
Shvec_Router_0(config-if)#ip nat outside
```

```
Shvec_Router_0(config-if)#int g0/1.10
```

```
Shvec_Router_0(config-subif)#ip nat in
```

```
Shvec_Router_0(config-subif)#int g0/1.20
```

```
Shvec_Router_0(config-subif)#ip nat in
```

```
Shvec_Router_0(config-subif)#int g0/1.30
```

```
Shvec_Router_0(config-subif)#ip nat in
```

Вкажемо, що пакети, які йдуть у невідому мережу, відправляти на маршрутизатор провайдера для подальшої відправки.

```
Shvec_Router_0(config)#ip route 0.0.0.0 0.0.0.0 se0/1/0
```

Налаштуємо список доступу, мережі яким буде надаватися адреса за допомогою NAT.

```
Shvec_Router_0(config)#ip access-list standard 1
```

```
Shvec_Router_0(config-std-nacl)#permit 10.23.85.96 0.0.0.15
```

```
Shvec_Router_0(config-std-nacl)#permit 10.23.85.112 0.0.0.15
```

```
Shvec_Router_0(config-std-nacl)#permit 10.23.85.128 0.0.0.15
```

Завершимо налаштування NAT.

```
Shvec_Router_0(config)#ip nat inside source list 1 interface se0/1/0 overload
```

Між маршрутизаторами Shvec\_Router\_IPS та Shvec\_Router\_3 використовуються IP з 209.165.202.0/30. Для того щоб маршрутизатор знав куди відправляти пакети які йдуть з або у мережу 209.165.200.0/27 (використовується для NAT), вкажемо йому статичний IP цієї мережі наступною командою.

```
Shvec_Router_IPS(config)#ip route 209.165.200.0 255.255.255.224 Serial0/1/1
```

## **3.6 Захист інформації в комп'ютерній системі від несанкціонованого доступу**

### **3.6.1 Розробка методів для захисту інформації в комп'ютерній системі**

Для захисту інформації у комп'ютерній системі підприємства використовують:

- налаштування мереж VLAN та також маршрутизації між ними;
- на портах комутаторів підключених до серверів налаштовується функція безпеки портів;
- налаштування VPN між LAN3 головного офісу та LAN4 віддаленого офісу.

### **3.6.2 Налаштування мереж VLAN**

VLAN (Virtual Local Area Network) – це технологія, яка дозволяє логічно розділити одну фізичну мережу на декілька віртуальних мереж. Кожен VLAN створює ізольовану групу пристроїв, які можуть спілкуватись між собою, незалежно від пристроїв в інших VLAN. Використовуючи VLAN, можна логічно розділити мережу на основі логічних груп або функціональності, незалежно від фізичної конфігурації мережевого обладнання.

Основні особливості та переваги використання VLAN:

- розділення мережі. VLAN дозволяє створювати логічні групи, які можуть спілкуватись між собою, але ізольовані від інших груп. Це дозволяє ефективно керувати трафіком та забезпечувати безпеку у мережі;
- безпека. VLAN дозволяє контролювати доступ до ресурсів мережі. Прискорюється реакція на атаки та знижується ризик несанкціонованого доступу до ресурсів;
- зниження трафіку. Завдяки використанню VLAN можна знизити навантаження на мережу шляхом обмеження передачі пакетів на відповідні VLAN. Це допомагає поліпшити ефективність та продуктивність мережі.

Так як розділ тестувальників планується збільшитися в майбутньому й іншими робітниками з інших розділів, було обрано зробити декілька VLAN.

Для налаштування мереж VLAN і маршрутизації між ними необхідно:

- створити 28, 38, 48, 99, 100 Vlan;
- вимкнути усі невикористовувані фізичні порти комутаторів;
- налаштувати Vlan;
- налаштувати транкові порти і порти доступу;
- налаштувати SVI-інтерфейси на комутаторах;
- налаштувати маршрутизацію між мережами VLAN;
- налаштувати маршрутизатор, що здійснює маршрутизацію між VLAN, в якості сервера DHCP для мереж VLAN;
- створити пули DHCP під назвою pollvlan№, де № – номер VLAN;
- виключити з пулу адреса мережевого обладнання;
- для кожного пулу вказати адресу DNS-сервера і шлюз за умовчанням.

Приклад налаштування для Shvec\_Switch\_1.

Створимо 28, 38, 48, 99, 100 Vlan.

```
Shvec_Switch_1(config)#vlan 28
Shvec_Switch_1(config-vlan)#name 28
Shvec_Switch_1(config-vlan)#vlan 38
Shvec_Switch_1(config-vlan)#name 38
Shvec_Switch_1(config-vlan)#vlan 48
Shvec_Switch_1(config-vlan)#name 48
Shvec_Switch_1(config-vlan)#vlan 99
Shvec_Switch_1(config-vlan)#name 99
Shvec_Switch_1(config-vlan)#vlan 100
Shvec_Switch_1(config-vlan)#name 100
```

Вимкнемо усі невикористовувані фізичні порти комутаторів.

```
Shvec_Switch_1(config)#interface r fa0/3-24
Shvec_Switch_1(config-if-range)#shutdown
```

Налаштуємо Vlan.

```
Shvec_Switch_1(config)#interface r fa0/5-9
```

```
Shvec_Switch_1(config-if-range)#no shutdown
```

```
Shvec_Switch_1(config-if-range)#switchport mode access
```

```
Shvec_Switch_1(config-if-range)#switchport access vlan 48
```

```
Shvec_Switch_1(config-if-range)#interface r fa0/10-14
```

```
Shvec_Switch_1(config-if-range)#no shutdown
```

```
Shvec_Switch_1(config-if-range)#switchport mode access
```

```
Shvec_Switch_1(config-if-range)#switchport access vlan 38
```

```
Shvec_Switch_1(config-if-range)#interface r fa0/15-24
```

```
Shvec_Switch_1(config-if-range)#no shutdown
```

```
Shvec_Switch_1(config-if-range)#switchport mode access
```

```
Shvec_Switch_1(config-if-range)#switchport access vlan 28
```

Налаштуємо транкові порти і порти доступу.

```
Shvec_Switch_1(config)#interface range GigabitEthernet0/1-2
```

```
Shvec_Switch_1(config-if-range)#switchport mode trunk
```

```
Shvec_Switch_1(config-if-range)#sw tr all vlan 10,20,30,99,100
```

```
Shvec_Switch_1(config-if-range)#exit
```

```
Shvec_Switch_1(config)#interface fastEthernet0/1
```

```
Shvec_Switch_1(config-if)#switchport mode trunk
```

```
Shvec_Switch_1(config-if)#sw tr all vlan 10,20,30,99,100
```

Налаштуємо SVI-інтерфейс на комутаторі.

```
Shvec_Switch_1(config)#interface vlan 99
```

```
Shvec_Switch_1(config-if)#ip address 10.23.85.146 255.255.255.248
```

Далі налаштування робимо на маршрутизаторі Shvec\_Router\_0.

Налаштуємо маршрутизацію між мережами VLAN.

```
Shvec_Router_0(config)#int g0/1.28
```

```
Shvec_Router_0(config-subif)#encapsulation dot1Q 28
```

```
Shvec_Router_0(config-subif)#ip address 10.23.85.97 255.255.255.240
```

```
Shvec_Router_0(config-subif)#int g0/1.38
```

```
Shvec_Router_0(config-subif)#encapsulation dot1Q 38
```

```

Shvec_Router_0(config-subif)#ip address 10.23.85.113 255.255.255.240
Shvec_Router_0(config-subif)#int g0/1.48
Shvec_Router_0(config-subif)#encapsulation dot1Q 48
Shvec_Router_0(config-subif)#ip address 10.23.85.129 255.255.255.240
Shvec_Router_0(config-subif)#encapsulation dot1Q 99
Shvec_Router_0(config-subif)#ip address 10.23.85.147 255.255.255.248

```

Налаштуємо маршрутизатор, що здійснює маршрутизацію між VLAN, в якості сервера DHCP для мереж VLAN та створимо пули DHCP під назвою pollvlan №, де № – номер VLAN. Також для кожного пулу вкажемо адресу DNS-сервера і шлюз за умовчанням

```

Shvec_Router_0(config)#ip dhcp pool 28
Shvec_Router_0(dhcp-config)#network 10.23.85.96 255.255.255.240
Shvec_Router_0(dhcp-config)#default-router 10.23.85.97
Shvec_Router_0(dhcp-config)#dns-server 209.165.200.3
Shvec_Router_0(dhcp-config)#ip dhcp pool 38
Shvec_Router_0(dhcp-config)#network 10.23.85.112 255.255.255.240
Shvec_Router_0(dhcp-config)#default-router 10.23.85.113
Shvec_Router_0(dhcp-config)#dns-server 209.165.200.3
Shvec_Router_0(dhcp-config)#ip dhcp pool 48
Shvec_Router_0(dhcp-config)#network 10.23.85.128 255.255.255.240
Shvec_Router_0(dhcp-config)#default-router 10.23.85.129
Shvec_Router_0(dhcp-config)#dns-server 209.165.200.3
Shvec_Router_0(dhcp-config)#exit

```

Виключимо з пулу адреса мережеве обладнання.

```

Shvec_Router_0(config)#ip dhcp excluded-address 10.23.85.97 10.23.85.98
Shvec_Router_0(config)#ip dhcp excluded-address 10.23.85.113
Shvec_Router_0(config)#ip dhcp excluded-address 10.23.85.129

```

### 3.6.2 Налаштування параметрів безпеки комутаторів

З ціллю забезпечення безпеки, на портах комутаторів, підключених до серверів, необхідно налаштувати функцію безпеки портів так, щоб:

- тільки двом унікальним пристроям був дозволений доступ до порту;
- MAC-адрес пристрою розпізнавався динамічно і додавався в поточну конфігурацію;
- під час порушенні системи безпеки з'являлося повідомлення, а порт залишався включеним.

Налаштування слід провести на портах комутаторів Shvec\_Switch\_1 та Shvec\_Switch\_8 до яких під'єднані сервери DNS, HTTP та FTP.

Налаштування для всіх ідентичні, приклад налаштування для Shvec\_Switch\_8.

```
Shvec_Switch_8(config)#interface FastEthernet0/1
Shvec_Switch_8(config-if)#switchport mode access
Shvec_Switch_8(config-if)#switchport port-security
Shvec_Switch_8(config-if)#switchport port-security maximum 2
Shvec_Switch_8(config-if)#switchport port-security mac-address sticky
Shvec_Switch_8(config-if)#switchport port-security violation restrict
```

### 3.6.3 Налаштування віртуальної приватної мережі site-to-site VPN з використанням IPsec

Для доступу віддаленої мережі LAN4 до мережі головного офісі LAN3, згідно технічного завдання необхідно використовувати site-to-site VPN з використанням IPsec для трафіку.

Виконаємо налаштування на Shvec\_Router\_3.

Першим кроком створимо access-list, де вкажемо з якої мережі в яку необхідно використовувати VPN.

```
Shvec_Router_3(config)#access-list 110 permit ip 10.23.84.0 0.0.0.127
10.23.85.96 0.0.0.15
```

```
Shvec_Router_3(config)#access-list 110 permit ip 10.23.84.0 0.0.0.127
10.23.85.112 0.0.0.15
```

```
Shvec_Router_3(config)#access-list 110 permit ip 10.23.84.0 0.0.0.127
10.23.85.128 0.0.0.15
```

Налаштуємо параметри 1 фази ISAKMP.

```
Shvec_Router_3(config)#crypto isakmp policy 10
```

```
Shvec_Router_3(config-isakmp)# encr aes
```

```
Shvec_Router_3(config-isakmp)# authentication pre-share
```

```
Shvec_Router_3(config-isakmp)# group 2
```

```
Shvec_Router_3(config-crypto-map)#exit
```

```
Shvec_Router_3(config)# crypto isakmp key cisco address 64.100.13.1
```

Налаштуємо параметри 2 фрази ISAKMP.

```
Shvec_Router_3(config)#crypto map VPN-MAP 10 ipsec-isakmp
```

```
Shvec_Router_3(config-crypto-map)# description VPN connection to R3
```

```
Shvec_Router_3(config-crypto-map)# set peer 64.100.13.1
```

```
Shvec_Router_3(config-crypto-map)# set transform-set VPN-SET
```

```
Shvec_Router_3(config-crypto-map)# match address 110
```

Налаштуємо криптографічне співвідношення для інтерфейсу.

```
Shvec_Router_3(config)#interface Serial0/1/1
```

```
Shvec_Router_3(config-if)#crypto map VPN-MAP
```

Налаштування для Shvec\_Router\_0 будуть майже ідентичні.

Налаштуємо параметри 1 фази ISAKMP.

```
Shvec_Router_0(config)#crypto isakmp policy 10
```

```
Shvec_Router_0(config-isakmp)# encr aes
```

```
Shvec_Router_0(config-isakmp)# authentication pre-share
```

```
Shvec_Router_0(config-isakmp)# group 2
```

```
Shvec_Router_0(config-crypto-map)#exit
```

```
Shvec_Router_0(config)# crypto isakmp key cisco address 209.165.202.2
```

Налаштуємо параметри 2 фрази ISAKMP.

```
Shvec_Router_0(config)#crypto map VPN-MAP 10 ipsec-isakmp
```

```
Shvec_Router_0(config-crypto-map)# description VPN connection to R3
```

```
Shvec_Router_0(config-crypto-map)# set peer 209.165.202.2
```

```
Shvec_Router_0(config-crypto-map)# set transform-set VPN-SET
```

```
Shvec_Router_0(config-crypto-map)# match address 110
```

Налаштуємо криптографічне співвідношення для інтерфейсу.

```
Shvec_Router_0(config)#interface Serial0/1/0
```

```
Shvec_Router_0(config-if)# crypto map VPN-MAP
```

Відредагуємо списки доступу так, щоб трафік, який йде у віддалену або з віддаленої мережі, не проходив через NAT.

```
Access-list 110 permit ip 10.23.85.96 0.0.0.15 10.23.84.0 0.0.0.127
```

```
access-list 110 permit ip 10.23.85.112 0.0.0.15 10.23.84.0 0.0.0.127
```

```
access-list 110 permit ip 10.23.85.128 0.0.0.15 10.23.84.0 0.0.0.127
```

```
ip access-list extended p1
```

```
deny ip 10.23.85.96 0.0.0.15 10.23.84.0 0.0.0.127
```

```
deny ip 10.23.85.112 0.0.0.15 10.23.84.0 0.0.0.127
```

```
deny ip 10.23.85.128 0.0.0.15 10.23.84.0 0.0.0.127
```

```
permit ip 10.23.85.128 0.0.0.15 any
```

```
permit ip 10.23.85.112 0.0.0.15 any
```

```
permit ip 10.23.85.96 0.0.0.15 any
```

### 3.7 Перевірка роботи комп'ютерної системи

Першим кроком перевіримо як працює маршрутизація між маршрутизаторами основного офісу з використанням протоколу OSPF, зробивши відправку пакетів між маршрутизаторами (рисунок 3.14).



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	Shvec_Router_2	Shvec_Router_3	ICMP		0.000	N	0	(edit)
	Successful	Shvec_Router_2	Shvec_Router_1	ICMP		0.000	N	1	(edit)
	Successful	Shvec_Router_2	Shvec_Router_4	ICMP		0.000	N	2	(edit)
	Successful	Shvec_Router_1	Shvec_Router_3	ICMP		0.000	N	3	(edit)

Рисунок 3.14 – Відправка пакетів між маршрутизаторами

Як бачимо з рисунку маршрутизація працює коректно.

Далі перевіримо коректність роботи DHCP серверу на кожному ПК основного офісу. Як бачимо з конфігурацій ПК основного офісу, з кожної підмережі (Рисунок 3.15-3.118) DHCP працює коректно.

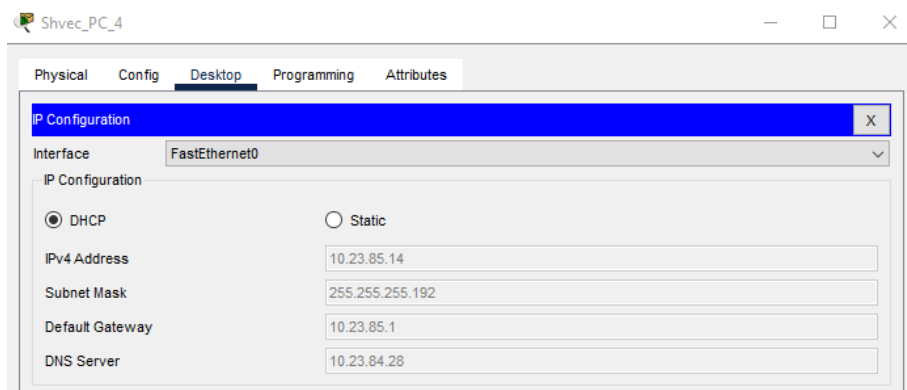


Рисунок 3.15 – IP конфігурація ПК з мережі LAN1

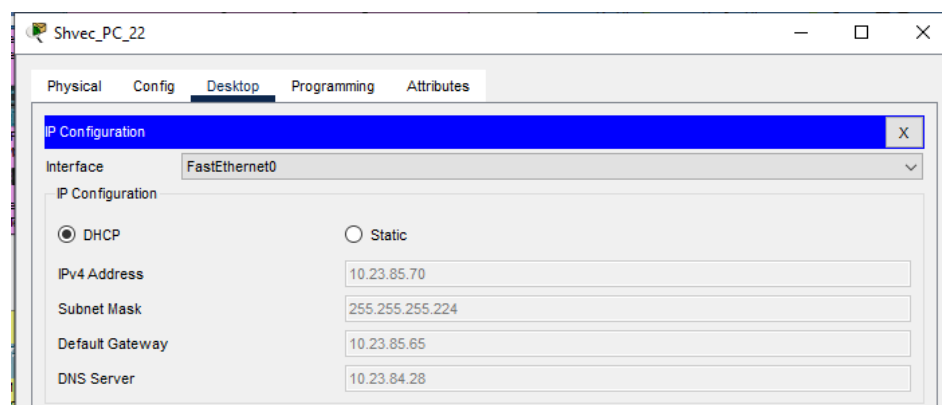


Рисунок 3.16 – IP конфігурація ПК з мережі LAN2

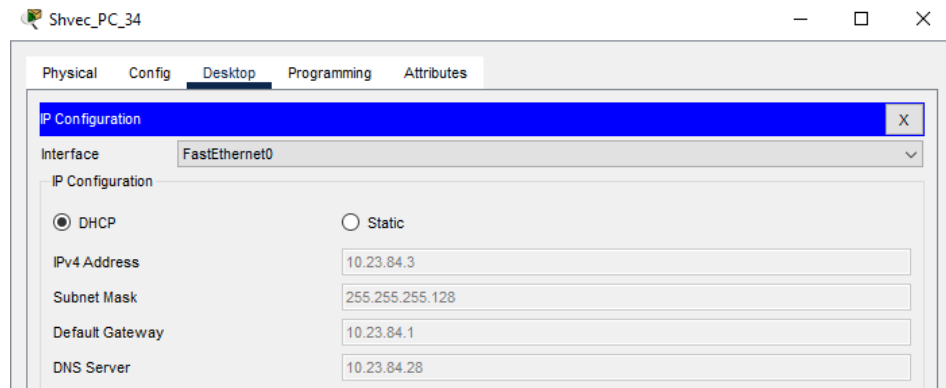


Рисунок 3.17 – IP конфігурація ПК з мережі LAN3

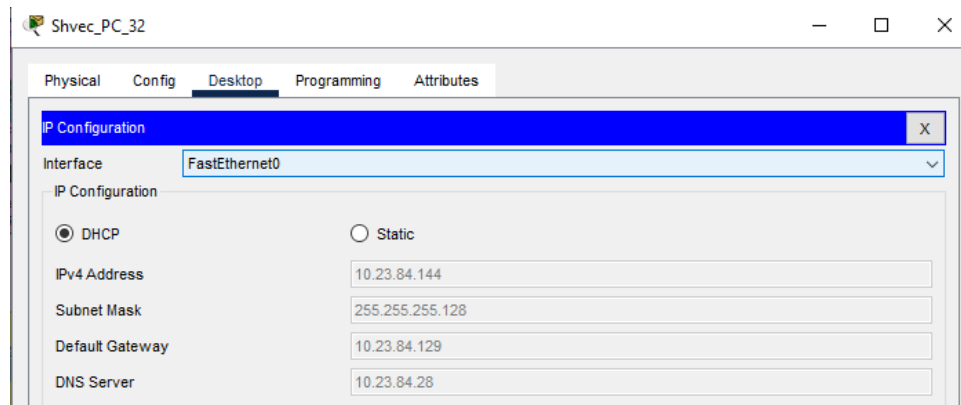


Рисунок 3.18 – IP конфігурація ПК з мережі LAN5

Виконаємо перевірку маршрутизації між мережами LAN1, LAN2, LAN3 та LAN5 відправивши пакети за допомогою команди пінг в інші мережі з мережі LAN1.

Результати пінгів з ПК мережі LAN1 у ПК мереж LAN2, LAN3 та LAN5 зображено на рисунках 3.19 – 3.21.

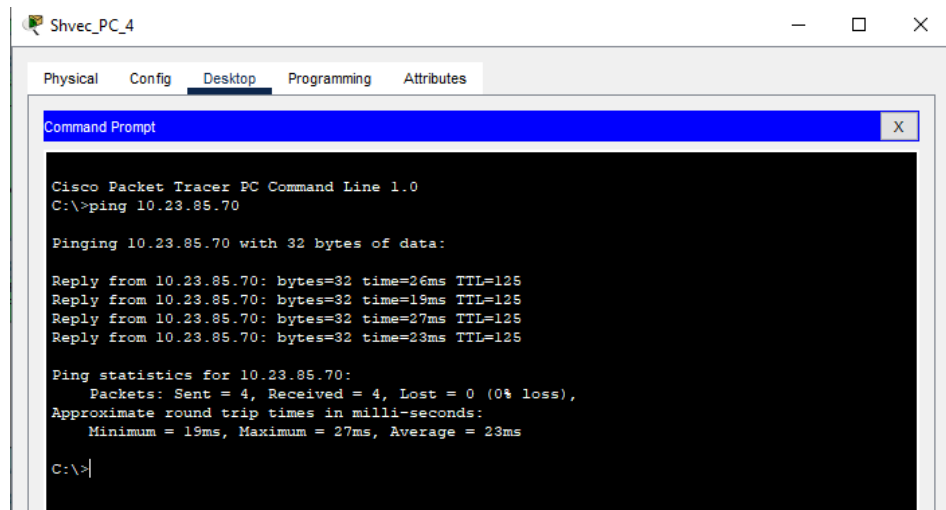


Рисунок 3.19 – Ping з ПК мережі LAN1 до ПК мережі LAN2

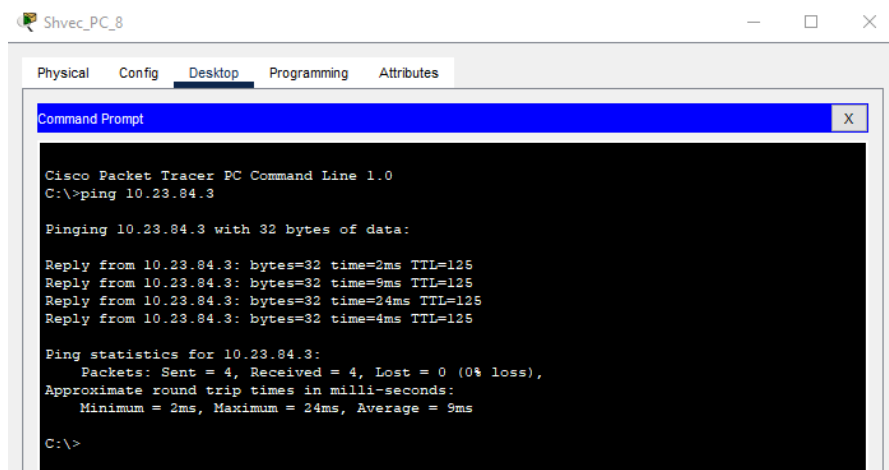


Рисунок 3.20 – Ping з ПК мережі LAN1 до ПК мережі LAN3

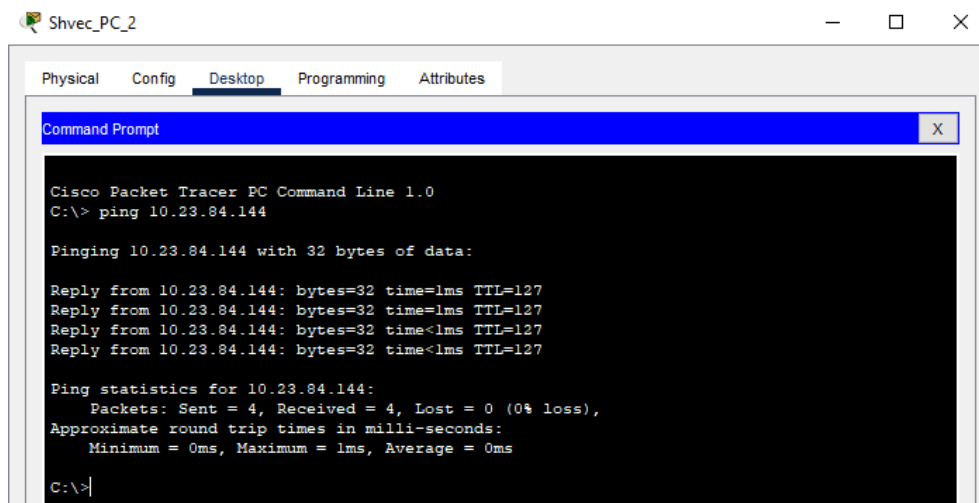
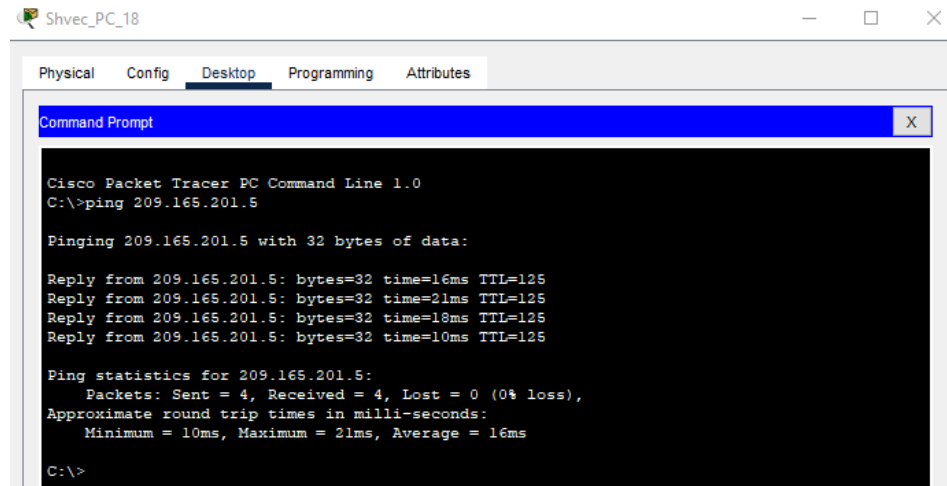


Рисунок 3.21 – Ping з ПК мережі LAN1 до ПК мережі LAN5

Як бачимо з рисунків, маршрутизація в мережах основного офісу працює коректно.

Далі перевіримо налаштування NAT для ПК, зробивши ping з ПК основного офісу, що зображено на рисунку 3.22.



```

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 209.165.201.5

Pinging 209.165.201.5 with 32 bytes of data:

Reply from 209.165.201.5: bytes=32 time=16ms TTL=125
Reply from 209.165.201.5: bytes=32 time=21ms TTL=125
Reply from 209.165.201.5: bytes=32 time=18ms TTL=125
Reply from 209.165.201.5: bytes=32 time=10ms TTL=125

Ping statistics for 209.165.201.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 21ms, Average = 16ms
C:\>
  
```

Рисунок 3.22 – Ping з ПК мережі LAN1 до ПК з адресою 209.165.201.5

Перевіримо одразу статичний NAT для серверів DNS та HTTP перейшовши за адресою 123.dnipro.ua з ПК з адресою 209.165.201.5, що зображено на рисунку 3.23.

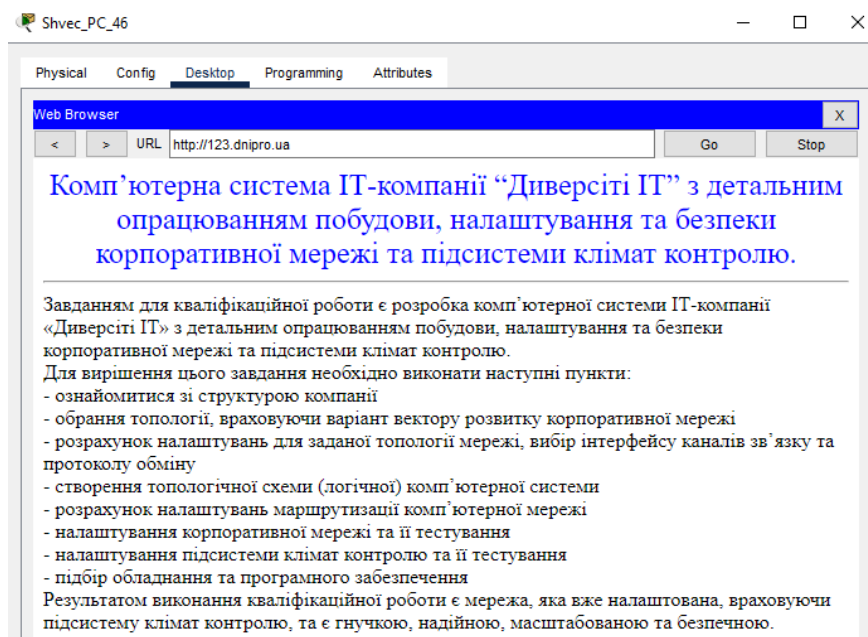


Рисунок 3.23 – Перехід на сайт 123.dnipro.ua з ПК з адресою 209.165.201.5

Як бачимо з рисунку 3.23 статичний NAT налаштований на маршрутизаторі Shvec\_Router\_3 працює коректно.

Тепер виконаємо перевірку налаштувань VLAN, перевіривши коректність налаштувань портів, результат перевірки показано на рисунку 3.24.

VLAN	Name	Status	Ports
1	default	active	Fa0/3, Fa0/4
10	10	active	Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24
20	20	active	Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14
30	30	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9
99	99	active	Fa0/2
100	100	active	

Рисунок 3.24 – Перевірка налаштувань VLAN на Shvec\_Switch\_1

Далі перевіримо коректність роботи DHCP у VLAN 28, 38, 48 перевіривши конфігурацію пристроїв відповідних VLAN, результати чого зображено на рисунках 3.25 – 3.27.

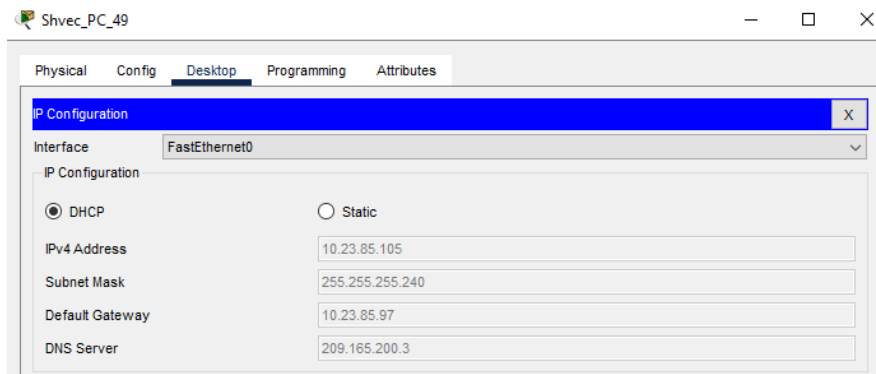


Рисунок 3.25 – IP конфігурація ПК з VLAN 28

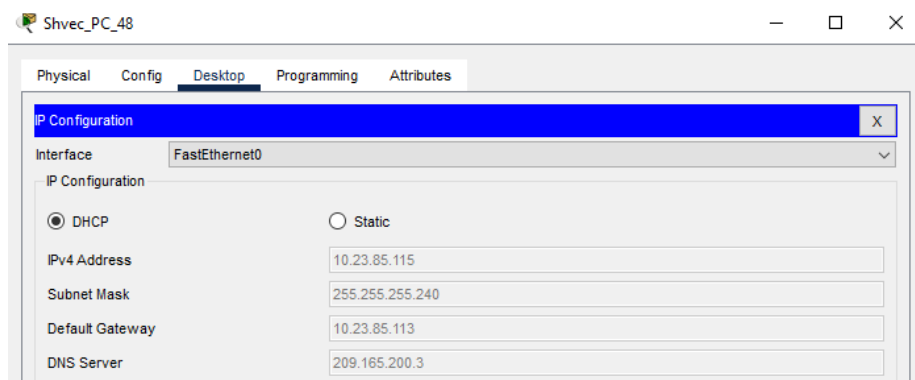


Рисунок 3.26 – IP конфігурація ПК з VLAN 38

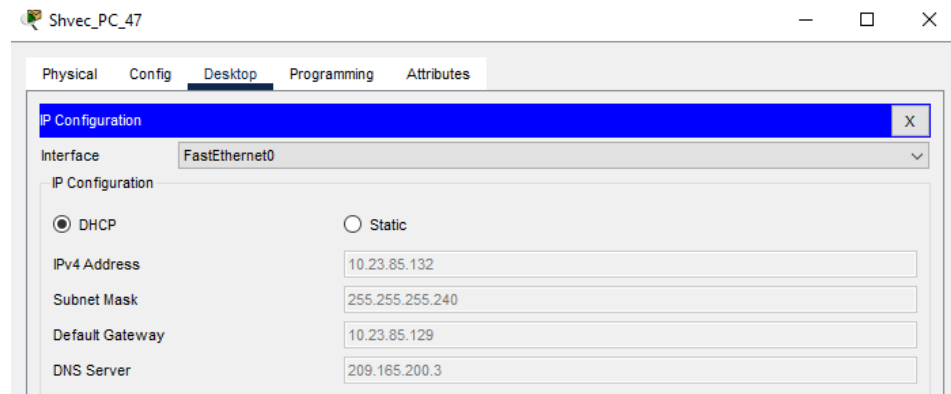


Рисунок 3.27 – IP конфігурація ПК з VLAN 48

Перевіримо маршрутизацію між VLAN зробивши ping з ПК VLAN 28 у інші VLAN. Результати перевірки зображені на рисунку 3.28-3.29.

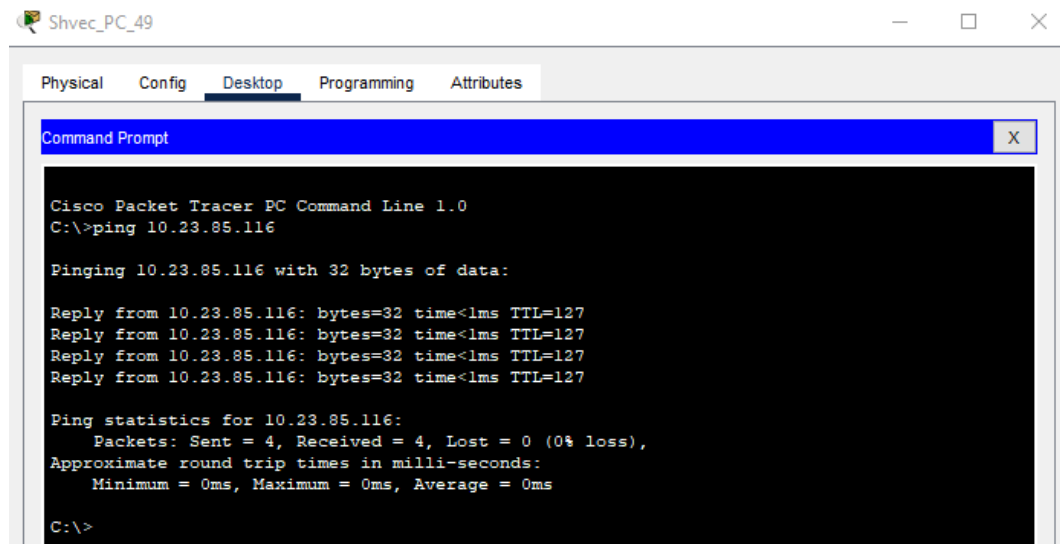


Рисунок 3.28 – Ping з ПК VLAN 28 до ПК VLAN 38

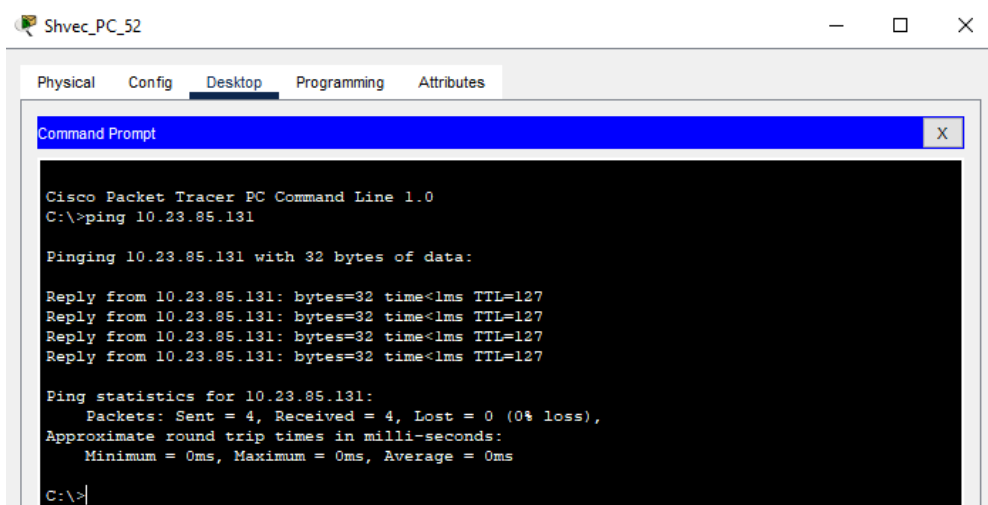


Рисунок 3.29 – Ping з ПК VLAN 28 до ПК VLAN 48

Як бачимо, маршрутизація між VLAN працює коректно.

Далі перевіримо налаштування NAT на маршрутизаторі віддаленого офісу, перейшовши на сайт за адресою 123.dnipro.ua з ПК локальної мережі віддаленого офісу що зображено на рисунку 3.30.

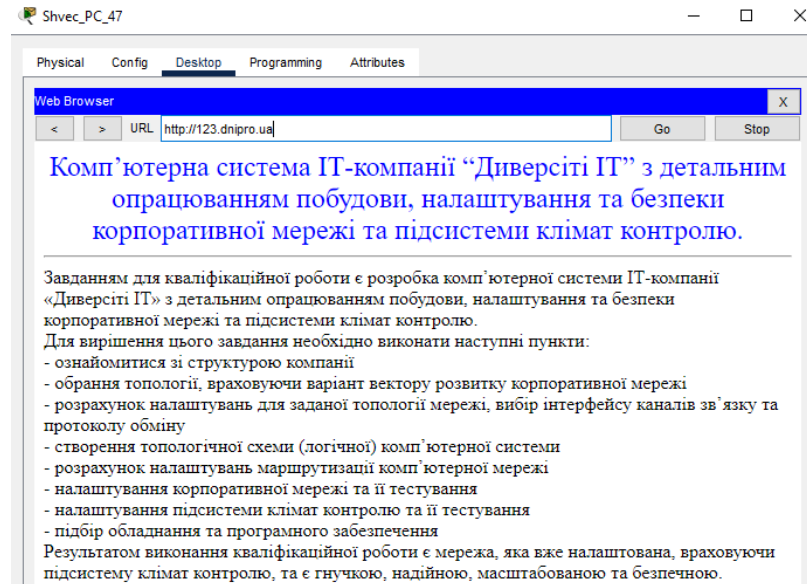


Рисунок 3.30 – Перехід на сайт 123.dnipro.ua з ПК Shvec\_PC\_47

Тепер перевіримо VPN налаштування, виконавши ping декілька раз з ПК віддаленої мережі до ПК основного офісу мережі LAN3, що зображено на рисунку 3.31.

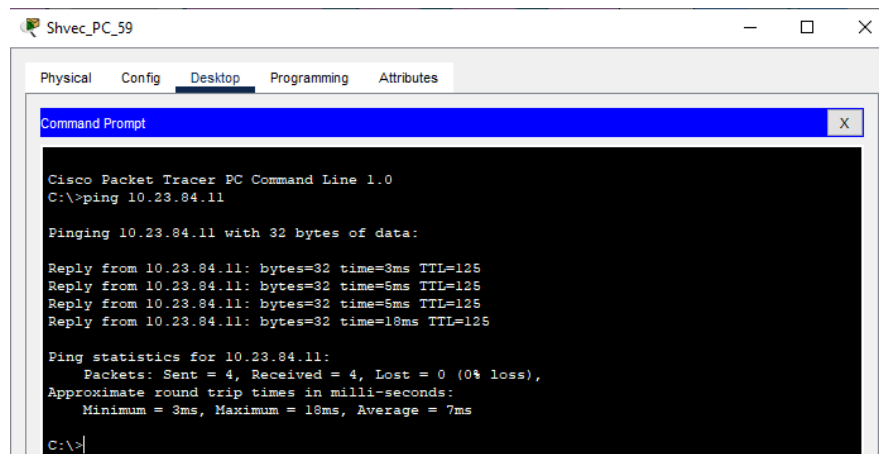


Рисунок 3.31 – Виконання ping з ПК віддаленої мережі до ПК основного офісу мережі LAN3

На рисунках 3.32 – 3.34 видно що кількість пакетів encapsulation та decapsulation збільшується, а отже трафік йде через VPN.

```

#pkts encaps: 1, #pkts encrypt: 1, #pkts digest: 0
#pkts decaps: 1, #pkts decrypt: 1, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0

```

Рисунок 3.32 – Перша перевірка роботи VPN на Shvec\_Router\_0

```

#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 0
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0

```

Рисунок 3.33 – Друга перевірка роботи VPN на Shvec\_Router\_0

```

#pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 0
#pkts decaps: 7, #pkts decrypt: 7, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0

```

Рисунок 3.34 – Третя перевірка роботи VPN на Shvec\_Router\_0



## 4 РОЗРОБКА СИСТЕМИ КЛІМАТ КОНТРОЛЮ

### 4.1 Інженерне рішення по розробці компонента системи

Система клімат контролю дозволяє керувати температурою в приміщенні за допомогою нагрівача і охолоджувача. Ось деякі переваги використання таких систем:

- комфорт. Система клімат контролю дозволить забезпечити комфортні умови в приміщенні;
- енергоефективність. Завдяки системам клімат контролю можна ефективно управляти енергоспоживанням. Наприклад, в літній період ви можете використовувати охолодження для підтримки комфортної температури;
- здоров'я. Правильне керування температурою в приміщенні може позитивно позначитися на здоров'ї людей. Забезпечення комфортних умов може допомогти знизити ризик стресу, втоми та впливу негативних факторів на здоров'я;
- збереження ресурсів. Ефективне використання систем клімат контролю може допомогти знизити споживання енергії і ресурсів.

Система клімат контролю знаходиться на 6 поверсі головного офісу, в LAN2 та складається з декількох основних компонентів:

- нагрівач;
- охолоджувач;
- плата контролю;
- температурний сенсор;
- 2 led лампи;
- монітор температури.

Загальна архітектура системи клімат контролю зображена на рисунку 4.1.

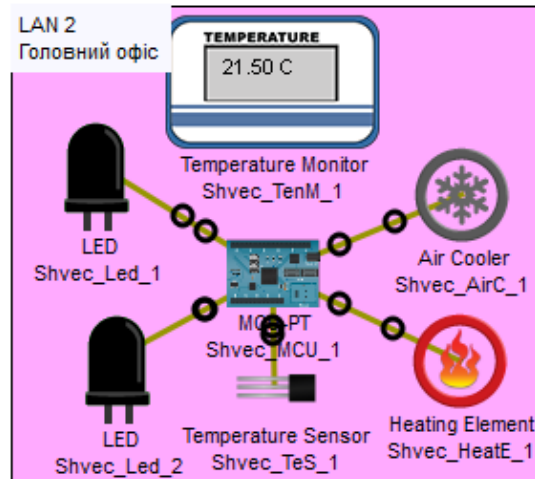


Рисунок 4.1 – Загальна архітектура системи клімат контролю

Контролер підтримує декілька мов програмування.

Код, на якому функціонал системи клімат контролю, було написано на мові – JavaScript.

JavaScript є мовою програмування, що широко використовується для розробки додатків та динамічної взаємодії з користувачем на веб-сторінках.

JavaScript є інтерпретованою мовою програмування, яка використовується для створення інтерактивності на веб-сторінках. Вона підтримується всіма сучасними веб-браузерами і може бути виконана безпосередньо на клієнтському боці (клієнтський JavaScript) або на серверному боці (серверний JavaScript, такий як Node.js).

Переваги:

- взаємодія з користувачем. JavaScript дозволяє створювати динамічні елементи на веб-сторінках і взаємодіяти з користувачем без перезавантаження сторінки. Це дозволяє створювати багатофункціональні та інтерактивні додатки;

- асинхронність. JavaScript підтримує асинхронні операції, що дозволяє виконувати завдання без затримок і не блокувати виконання інших частин програми. Це особливо важливо для роботи з мережевими запитами, базами даних та іншими завданнями, які можуть займати багато часу;

- багатofункціональність. JavaScript має велику кількість стандартних функцій і бібліотек, які дозволяють виконувати різноманітні завдання.

Arduino – це відкрита платформа для розробки електронних пристроїв, що включають мікроконтролери та середовище програмування. Ось деякі плюси використання Arduino:

- простота використання. Arduino має простий інтерфейс та легко зрозумілу мову програмування, що робить його доступним для початківців. Багато документації, прикладів та підтримки спільноти допомагають швидко освоїти Arduino;

- розширюваність. Arduino підтримує велику кількість модулів та додаткових пристроїв, які можна легко підключити до платформи. Це дозволяє розширювати функціональність вашого проекту, додавати сенсори, мотори, дисплеї та багато іншого;

- наявність багатьох готових бібліотек. Arduino має велику спільноту розробників, що призводить до наявності великої кількості готових бібліотек і коду. Ви можете використовувати ці бібліотеки для спрощення розробки, отримання швидких результатів та використання готових функцій;

- низька вартість. Arduino є відносно недорогою платформою, що робить її доступною для широкого кола користувачів. Це дає можливість експериментувати, робити прототипи та реалізовувати проекти з обмеженим бюджетом;

- широке застосування. Arduino можна використовувати в багатьох різних сферах.

Саме через ці переваги під час проектування було обрано саме плату на базі Arduino. Функцій Arduino Uno буде достатньо для системи клімат контролю, а також буде можливість підключити ще більше компонентів у разі необхідності до цієї плати.

Для особистого перегляду температури в кімнаті було обрано монітор температури від Xiaomi. Для виведення статусу роботи системи, було додано два світлодіоди.

Кондиціонер та обігрівач було підібрано таким чином, щоб після подачі електроенергії вони починали працювати.

Реле було підібрано з урахуванням потужності приладів, які до нього будуть підключатися.

Так як офіційно плати Arduino не мають підтримки JavaScript, то ми будемо використовувати для цього Johnny-Five.

Johnny-Five – це JavaScript-фреймворк для робототехніки та IoT, який дозволяє керувати платою Arduino (включаючи Arduino Uno) та іншими мікроконтролерами за допомогою JavaScript.

Специфікацію обладнання для системи клімат контролю зображено в таблиці 4.1.

Таблиця 4.1 – Специфікація обладнання

Позиція	Найменування і технічна характеристика	Тип, марка, позначення документа, опитувального листа	Одиниці виміру	Кількість	Примітки
1	2	3	4	5	6
1.	Монітор температури Temperature and Humidity Monitor 2 Живлення: Батарейки Діапазон вимірюваної температури: 0-60 °C	Датчик температури та вологості Xiaomi Mi	од.	1	
2.	Світлодіод червоний	Led 5mm ArduinoKit	од.	2	
3.	Датчик температури Робоча напруга: 3-5 В	Датчик температури, вологості DHT11	од.	1	

Продовження таблиці 4.1

Позиція	Найменування і технічна характеристика	Тип, марка, позначення документа, опитувального листа	Одиниці виміру	Кількість	Примітки
1	2	3	4	5	6
4.	Кондиціонер Режими роботи: Вентилятор, Осушення Охолодження Електроживлення: 220 В / 50 Гц	Кондиціонер мобільний TCL KY- 18/QY(MZ)( NX)	од.	1	
5.	Обігрівач Потужність, Вт 2000	Конвектор COOPER & HUNTER CH-2000 MC	од.	1	
6.	Плата контролю Цифрові контакт вводу/виводу: 14 Контакти аналогового входу: 6 Напруга: 5 В Вхідна напруга (номінальна) 7-12В	Arduino UNO R3	од.	1	
7.	Блок живлення 9 В. 1 А Arduino Uno	Блок живлення палати контролю	од.	1	
8.	Кабель підключення ARDUINO 10см	Кабель підключення	од.	11	
9.	Модуль реле 5В 10А з опторозв'язкою	Реле	од.	2	
10.	Кабель живлення	Мідний провід ПВС 3x1	м	6	
11.	Корпус з бічними панелями N11В H2K	Корпус	од.	1	
12.	220 Ом резистор	Резистор	од.	2	

Схема підключення на платі зображено на рисунку 4.2.

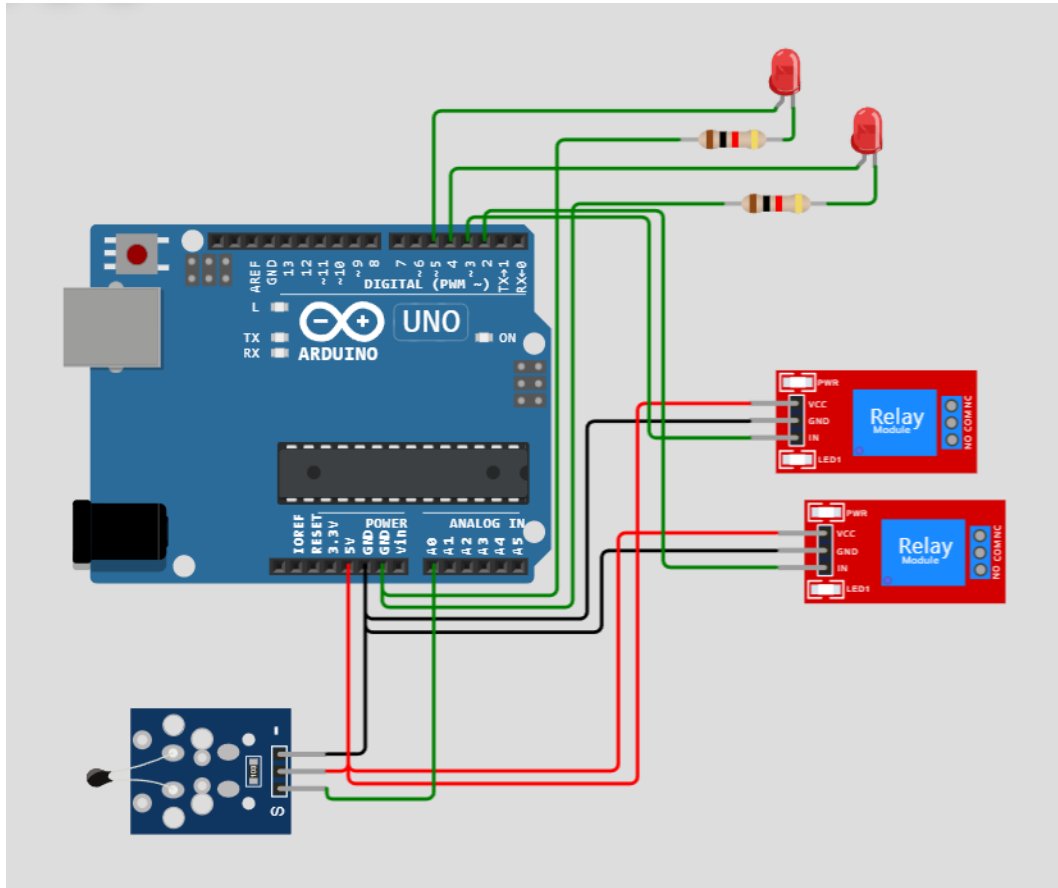


Рисунок 4.2 – Схема підключення Arduino

Схема розташування системи клімат контролю в офісі зображено на рисунку 4.3.

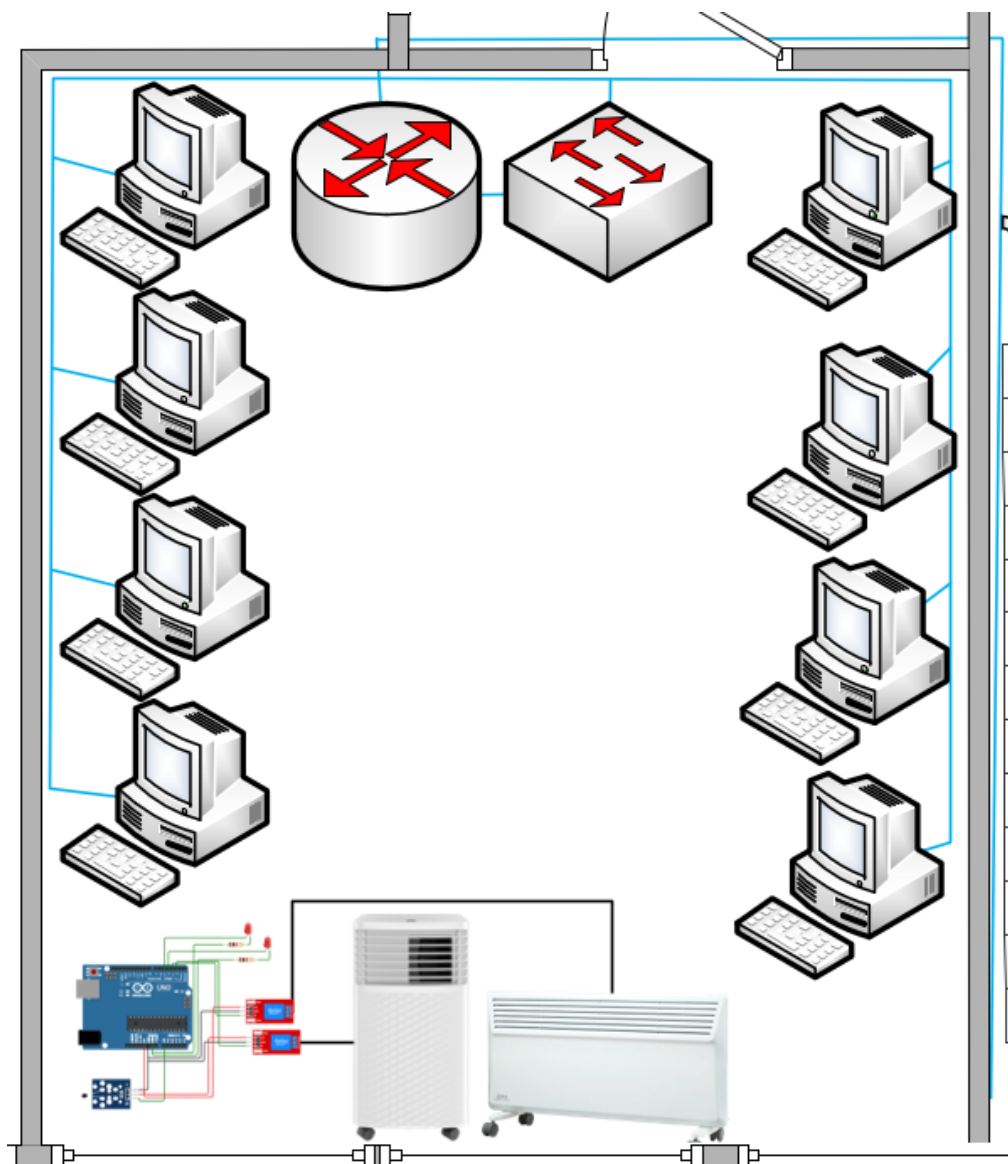


Рисунок 4.3 – Схема розташування системи клімат контролю

## 4.2 Розробка системи клімат контролю

Почнемо з розробки алгоритму роботи коду програми, який зображено на рисунку 4.4.

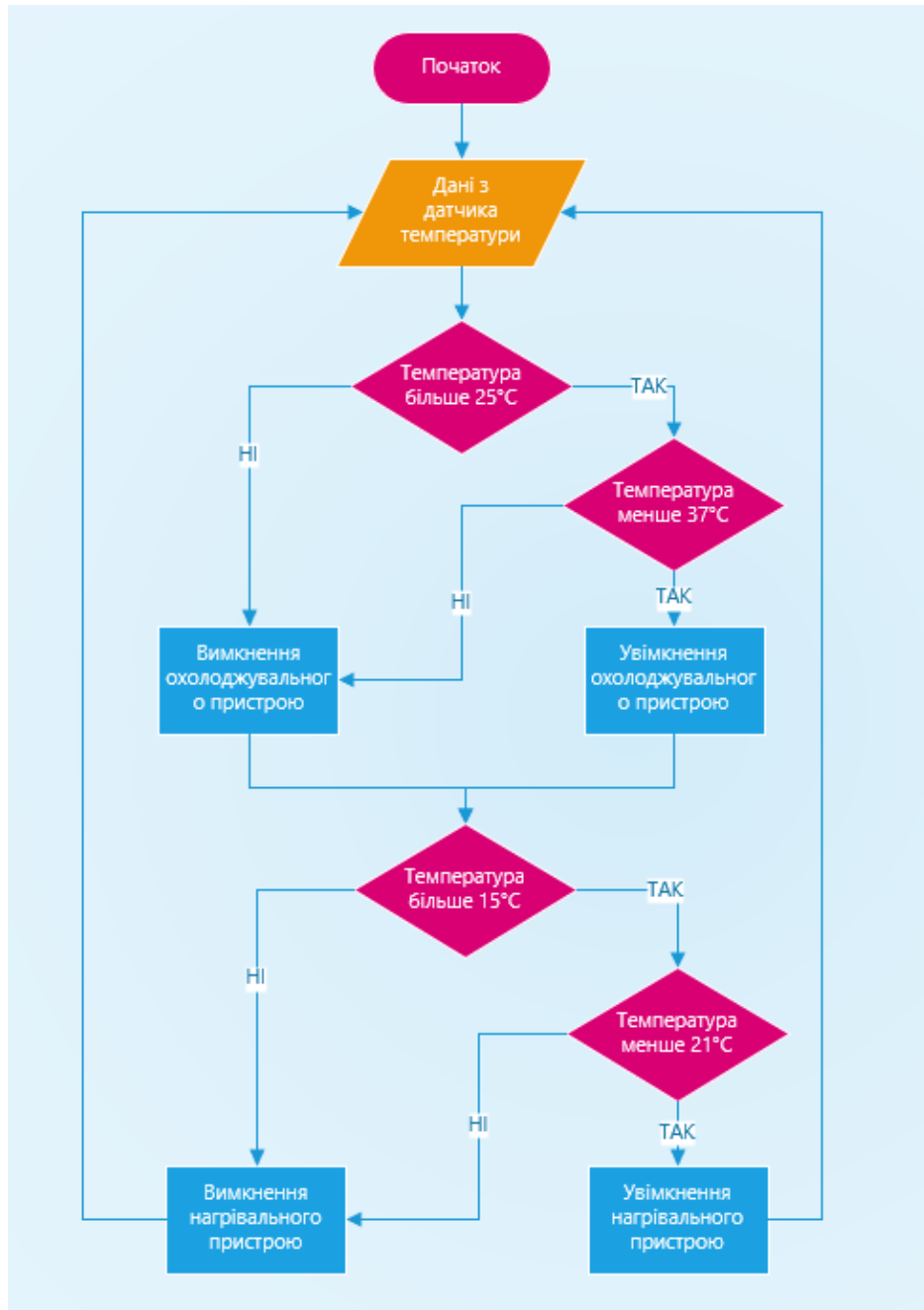


Рисунок 4.4 – Схема алгоритму системи клімат контролю

Тепер перейдемо до коду плати керування.

Визначимо змінні, які використовуються для керування підключеними пристроями.

```
Var ledPin = 5;
```

```
var ledPin2 = 4;
```

```
var potPin = A0;
```



```
var value = 0;
var cool = 2;
var heat = 3;
```

Наступним кроком вказуємо, які пристрої являються вихідними.

```
Function setup() {
    pinMode(ledPin, OUTPUT);
    pinMode(ledPin2, OUTPUT);
    pinMode(cool, OUTPUT);
    pinMode(heat, OUTPUT);

}
```

Далі виконаємо зчитування температури з датчика температури.

```
Function loop() {
    var newValue = analogRead(potPin);
    newValue = ((analogRead(A0) *200/1023)-100);
    if (newValue != value) {
        Serial.println(«new value: « + newValue);
        analogWrite(ledPin, newValue);
        value = newValue; }
}
```

Далі допишемо, що якщо температура в межах від 25 °С до 37 °С, то необхідно включити охолоджувач, та вимкнути у разі температури або нижче або дорівнює 25 °С та коли або вище або дорівнює 37 °С.

```
If(value>25)
{
    if(value<37)
    {
        digitalWrite(2, HIGH)
        digitalWrite(4, HIGH)
        digitalWrite(5, HIGH)
    }
}
```

```

        delay(1);
        digitalWrite(4, LOW)
        digitalWrite(5, LOW)
    }
    else
    {
        digitalWrite(2, LOW)
    }
}
else
{
    digitalWrite(2, LOW)
}

```

Тепер напишемо код для налаштування нагрівача. Якщо температура в межах від 15 °С до 21 °С , то необхідно увімкнути нагрівач. Якщо температура нижче або дорівнює 15 °С, то необхідно вимкнути нагрівач. Якщо температура вище або дорівнює 21 °С, то необхідно вимкнути нагрівач.

```

If(value>15)
{
    if(value<21)
    {
        digitalWrite(3, HIGH)
        digitalWrite(4, HIGH)
        digitalWrite(5, HIGH)
        delay(1);
        digitalWrite(4, LOW)
        digitalWrite(5, LOW)
    }
}

```

```

else
{
    digitalWrite(3, LOW)
}
}
else
{
    digitalWrite(3, LOW)
}
}

```

Повний код програми наведено у додатку В.

### 4.3 Перевірка роботи системи клімат контролю

Перше, обігрівач та охолоджувач повинні бути вимкнуті при температурі менше 15 °C включно, що і зображено на рисунку 4.5.

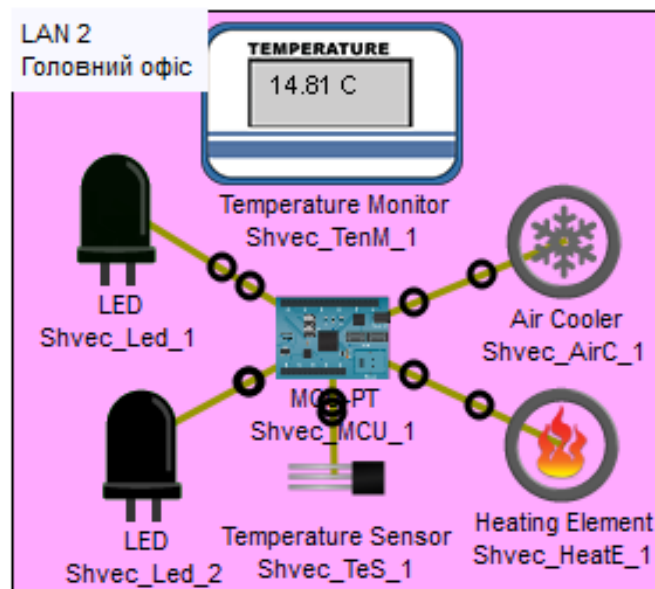


Рисунок 4.5 – Результат перевірки під час температури менше 15 °C включно

Друге, охолоджувач повинен бути вимкнтий, а обігрівач увімкнений при температурі від 15 °С до 23 °С, що і зображено на рисунку 4.6.

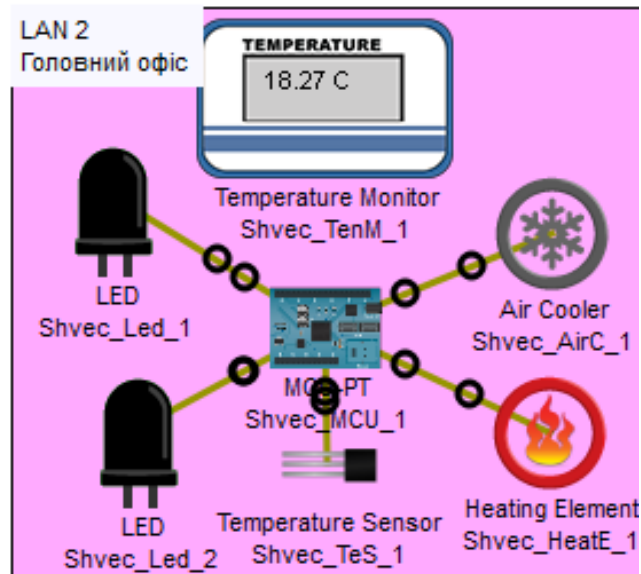


Рисунок 4.6 – Результат перевірки під час температури від 15 °С до 23 °С

Обігрівач та охолоджувач повинні бути вимкнуті при температурі від 23 °С до 25 °С включно, що і зображено на рисунку 4.7.

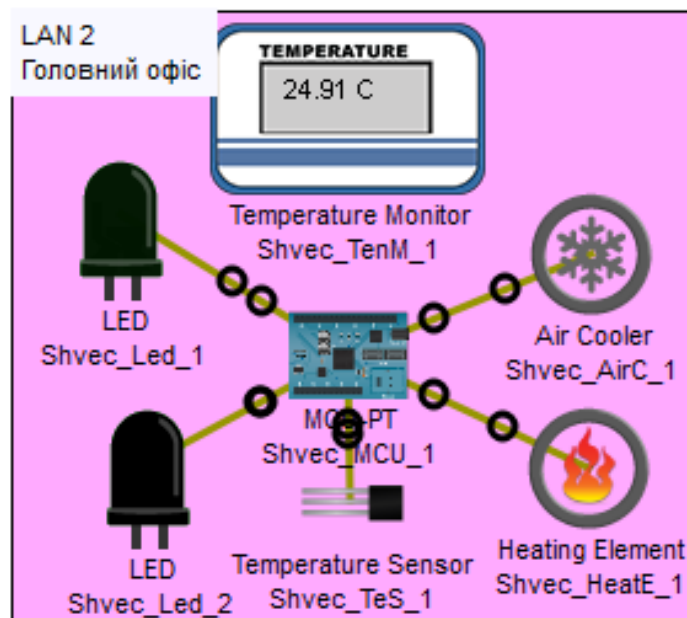


Рисунок 4.7 – Результат перевірки під час температури від 23 °С до 25 °С

ВКЛЮЧНО

Охолоджувач повинен бути увімкнений, а обігрівач вимкнений при температурі від 25 °С до 37 °С, що і зображено на рисунку 4.8.

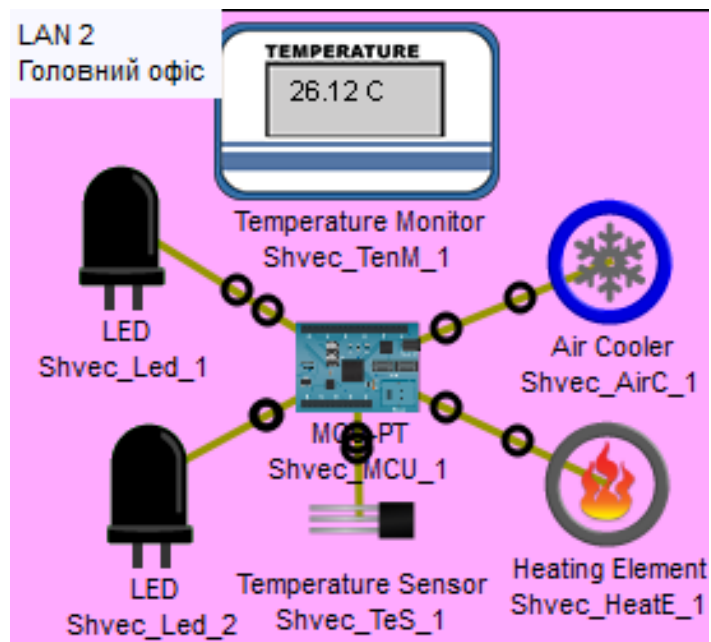


Рисунок 4.8 – Результат перевірки під час температури від 25 °С до 37 °С

Обігрівач та охолоджувач повинні бути вимкнуті при температурі вище 37 °С включно, що і зображено на рисунку 4.9.

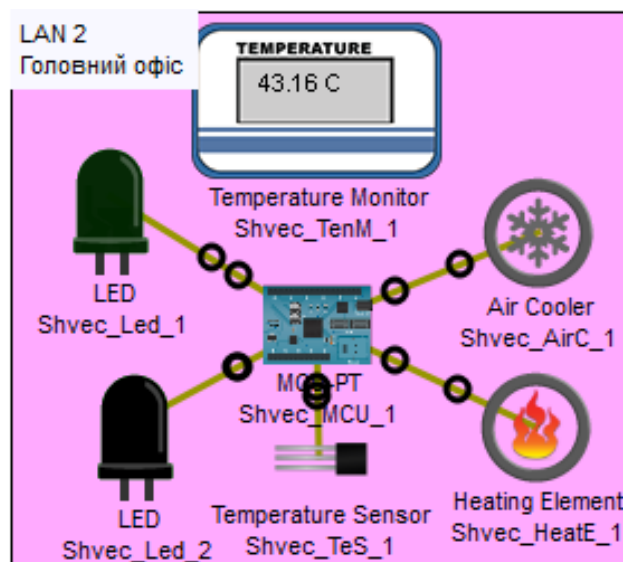


Рисунок 4.9 – Результат перевірки під час температури вище 37 °С включно

## ВИСНОВКИ

Під час виконання кваліфікаційної роботи було виконано ряд завдань, пов'язаних з розробкою комп'ютерної системи для підприємства. Було визначено умови застосування комп'ютерної системи, розглянуто існуючі інженерні рішення в галузі та визначено можливі напрямки рішення поставлених завдань. Також була розроблена схема організаційної структури підприємства та поставлено завдання на розробку комп'ютерної системи.

У другій частині були встановлені технічні вимоги до комп'ютерної системи, зокрема вимоги до структури й функціонування системи, показників призначення, вимог до експлуатації, технічного обслуговування, ремонту і збереження, а також до патентної чистоти. Були визначені вимоги до функцій, які повинна виконувати КС, а також до видів забезпечення комп'ютерної системи, зокрема інформаційного та програмного забезпечення.

Далі була розроблена апаратна частина комп'ютерної системи та схема топологічного розміщення всіх підрозділів ІТ-компанії «Диверсіті ІТ», а також і архітектура мережі. Було виконано вибір та обґрунтування комплексу технічних засобів в мережі.

У третій частині, у ході роботи було проведено розробку та налаштування комп'ютерної мережі підприємства. В рамках цього було здійснено розрахунок схем адресацій та топологічної схеми мережі. Були налаштовані маршрутизатори та здійснено розрахунок необхідних налаштувань маршрутизації для ефективної передачі даних.

Також була проведена базова налаштування конфігурації пристроїв, включаючи маршрутизатори, агрегатори каналів та налаштування підключення до Інтернету. Була налаштована віртуальна приватна мережа з використанням протоколу Ірsec для забезпечення безпеки та конфіденційності даних.

Після були розроблені методи захисту інформації в комп'ютерній системі та налаштовані мережеві VLAN. Були прийняті заходи з налаштування параметрів

безпеки комутаторів та маршрутизаторів на підтримку служби AAA (аутентифікації, авторизації та обліку).

Крім того, у четвертій частині, була розроблена система клімат контролю для забезпечення комфортних умов у приміщенні.

Як бачимо, цілі кваліфікаційної роботи було виконано на 100 відсотків.

## ПЕРЕЛІК ПОСИЛАНЬ

1. Математичні методи, моделі та інформаційні технології в економіці. URL: [http://www.econom.stateandregions.zp.ua/journal/2018/1\\_2018/17.pdf](http://www.econom.stateandregions.zp.ua/journal/2018/1_2018/17.pdf)
2. Інформаційні системи та технології на підприємстві. URL: <http://surl.li/ctko>
3. Розробка програмного забезпечення. URL: <http://surl.li/uuof>
4. Розробка ПЗ. URL: <https://tryengineering.org/uk/profile/software-development/>
5. Основні етапи розробки софта на замовлення. URL: <https://avada-media.ua/ua/services/software-development/>
6. Захист інформації в локальних мережах. <http://surl.li/azfvh>
7. Захист інформації в комп'ютерних системах. URL: <https://uzhnu.edu.ua/en/infocentre/get/42935>
8. Засоби та методи захисту інформації. URL: <https://buklib.net/books/28625/>
9. Антивірусна програма. URL: <http://surl.li/fpdb>
10. Резервне копіювання даних. URL: <https://cip.gov.ua/ua/faqs/sho-take-rezervne-kopiyuvannya-danikh-yak-iogo-zdiisnyuvati-i-de-krashe-zberigati-informaciyu>
11. Шифрування: типи і алгоритми. URL: <https://hostpro.ua/wiki/ua/security/encryption-types-algorithms>
12. Криптографічні методи захисту інформації. URL: <https://naurok.com.ua/tema-kriptografichni-metodi-zahistu-informaci-kontrol-cilisnosti-programnih-i-informaciynih-resursiv-210574.html>
13. Як захистити бізнес від витоку даних. URL: <https://gigatrans.ua/ua/news/6-sposobov-kak-zash-itit-biznes-ot-utechki-dannuh>
14. Захист від витоку даних. URL: <http://integritysys.com.ua/security/dlp/>
15. Віддалений доступ vpn. URL: <https://businessyield.com/uk/management/remote-access-vpn-meaning-how-it-works-and-best-vpn/>



16. Хмарні технології. URL: <https://business.diaa.gov.ua/cases/tehnologii/so-take-hmarni-tehnologii-i-ak-voni-mozut-dopomogti-vasomu-pidpriemstvu>
17. Хмарні технології та їхня користь для бізнесу. URL: <https://vps.ua/blog/ukr/cloud-technologies-for-business/>
18. Big Data (великі дані). URL: <https://futurenow.com.ua/shho-take-big-data-velyki-dani/>
19. Big Data (Біг Дата / Великі дані). URL: <https://termin.in.ua/big-data-velyki-dani/>
20. Інтернет речей. <http://surl.li/aezfc>
21. Як працює Інтернет речей. URL: <https://focus.ua/uk/digital/521863-kak-rabotaet-internet-veshchey-sut-tehnologii-i-ee-primenenie-v-sovremennom-mire>
22. Розподілені системи. URL: <http://surl.li/gxndp>
23. Cisco 2911/K9. URL: <https://stack-systems.com.ua/marshrutizator-cisco-2911-k9>
24. Cisco HWIC-2T. URL: <https://stack-systems.com.ua/interfejsnyj-modul-cisco-hwic-2t>
25. Cisco WS-C2960-24LC-S. URL: <https://stack-systems.com.ua/kommutator-cisco-ws-c2960-24lc-s>
26. Cisco UCS C240 M4 12 LFF 2U. URL: <https://hard.kiev.ua/server-cisco-ucs-c240-m4-12-lff-2u/>
27. Мережева академія cisco – <https://www.netacad.com/>
28. Хамбракен, Д. Комп'ютерні мережі: Пер. з англ. / Д. Хамбракен. – М.: ДМК Прес, 2004. – 449 с.
29. Методичні рекомендації до виконання кваліфікаційної роботи бакалавра студентами галузі знань 12 інформаційні технології спеціальності 123 комп'ютерна інженерія / Л.І. Цвіркун, В.В. Гнатушенко, С.М. Ткаченко ; М-во освіти і науки України, НТУ “ДП” – Дніпро: 2023. – 29 с

30. OSPF налаштування —  
<https://computernetworking747640215.wordpress.com/2018/05/24/ospf-configuration-in-packet-tracer/>
31. Статичний NAT, налаштування —  
<https://www.computernetworkingnotes.com/ccna-study-guide/how-to-configure-static-nat-in-cisco-router.html>
32. Динамічний NAT, налаштування —  
<https://www.youtube.com/watch?v=kvfVdaIwkos>
33. DHCP налаштування —  
<https://computernetworking747640215.wordpress.com/2018/07/05/how-to-configure-dhcp-server-in-packet-tracer/>
34. VLAN налаштування — <https://www.youtube.com/watch?v=kCf5sFnTB6U>
35. IPSec VPN налаштування — <https://cybersecfaith.com/2020/11/01/setting-up-an-ipsec-vpn-using-cisco-packet-tracer/>

## Додаток А

## Загальна топологічна схема підприємства

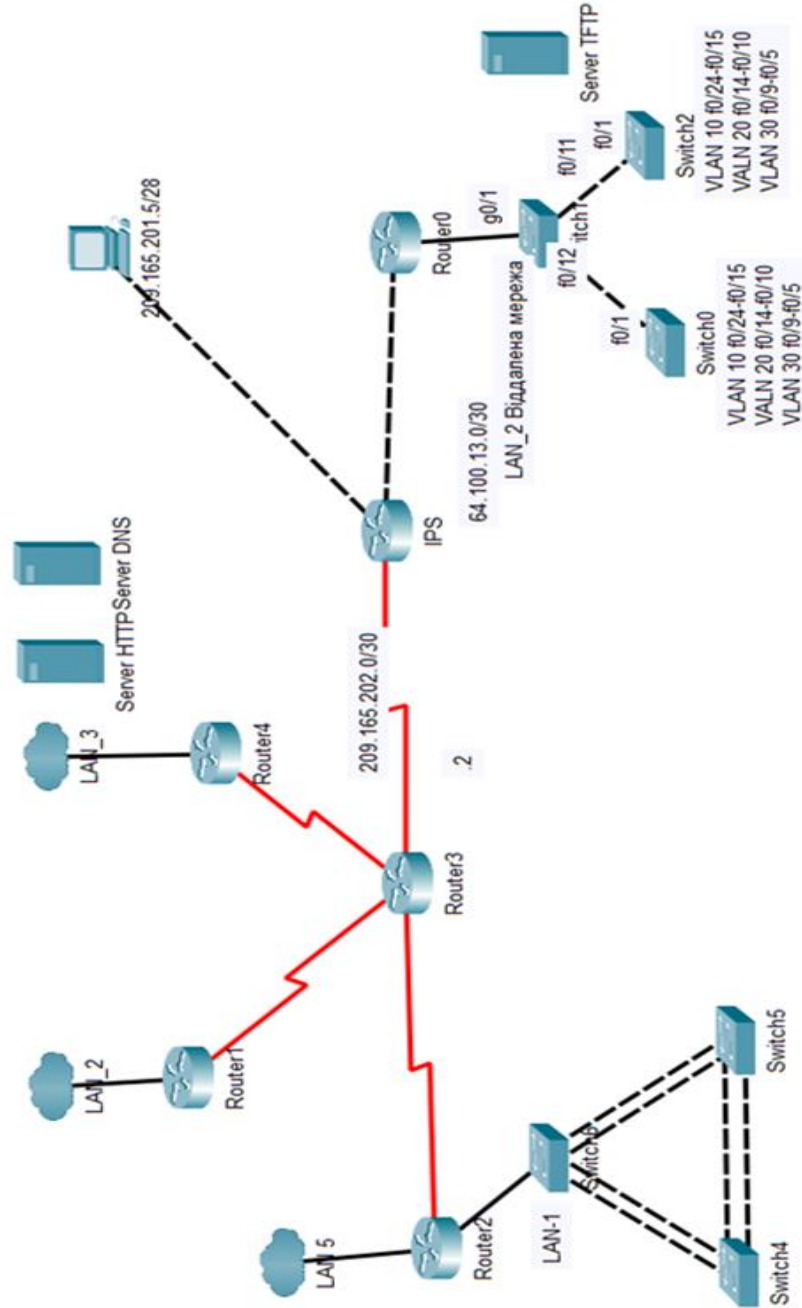


Рисунок А.1 – Загальна топологічна схема підприємства

## Додаток Б

Текст програми налаштування комп'ютерної  
мережі підприємства

**Міністерство освіти і науки України  
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ  
“ДНІПРОВСЬКА ПОЛІТЕХНІКА”**

**ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ  
НАЛАШТУВАННЯ МЕРЕЖІ КОМП'ЮТЕРНОЇ СИСТЕМИ**

Текст програми

804.02070743.23019-01 12 01

Листів 26

## АНОТАЦІЯ

Цей документ включає в себе програмне забезпечення налаштувань маршрутизаторів та комутаторів Cisco.

Текст програм для маршрутизаторів та комутаторів було реалізовано на мові конфігураційних пристроїв мережевого обладнання Cisco.

Середовище розробки, яке використовувалось для налаштування конфігураційних скриптів – Cisco Packet Tracer.

## ЗМІСТ

1. Налаштування маршрутизатора Shvec_Router_0 .....	4
2. Налаштування маршрутизатора Shvec_Router_3 .....	9
3. Налаштування маршрутизатора Shvec_Router_IPS.....	14
4. Налаштування комутатора Shvec_Switch_1 .....	17
5. Налаштування комутатора Shvec_Switch_6.....	23

## 1. Налаштування маршрутизатора Shvec\_Router\_0

```
!  
version 15.1  
no service timestamps log datetime msec  
no service timestamps debug datetime msec  
//Шифрування паролів  
service password-encryption  
!  
//Ім'я пристрою  
hostname Shvec_Router_0  
!  
//Пароль до привілейованого режиму  
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1  
!  
//Виключення адрес з пулу DHCP  
ip dhcp excluded-address 10.23.85.97 10.23.85.98  
ip dhcp excluded-address 10.23.85.113  
ip dhcp excluded-address 10.23.85.129  
!  
//Налаштування DHCP  
ip dhcp pool 28  
network 10.23.85.96 255.255.255.240  
default-router 10.23.85.97  
dns-server 209.165.200.3  
ip dhcp pool 38  
network 10.23.85.112 255.255.255.240  
default-router 10.23.85.113  
dns-server 209.165.200.3  
ip dhcp pool 48  
network 10.23.85.128 255.255.255.240
```



```

default-router 10.23.85.129
dns-server 209.165.200.3
!
//Налаштування AAA
aaa new-model
!
aaa authentication login default group radius local
!
no ip cef
no ipv6 cef
!
//Створення користувача з паролем
username      123191_Shvec      privilege      15      secret      5
$1$mERr$MKp6WULHmjLdYVBw6rbD11
!
license udi pid CISCO2911/K9 sn FTX1524NGCV-
license boot module c2900 technology-package securityk9
!
//Створення VPN
crypto isakmp policy 10
  encr aes
  authentication pre-share
  group 2
!
crypto isakmp key cisco address 209.165.202.2
!
crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
!
crypto map VPN-MAP 10 ipsec-isakmp
  description VPN connection to R3

```

```
set peer 209.165.202.2
set transform-set VPN-SET
match address 110
!
//Створення домену и ssh
ip domain-name Shvec_Router_0
!
spanning-tree mode pvst
!
//Налаштування інтерфейсів
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
!
interface GigabitEthernet0/1.28
encapsulation dot1Q 28
ip address 10.23.85.97 255.255.255.240
ip nat inside
!
interface GigabitEthernet0/1.38
encapsulation dot1Q 38
ip address 10.23.85.113 255.255.255.240
ip nat inside
```

```
!  
interface GigabitEthernet0/1.48  
  encapsulation dot1Q 48  
  ip address 10.23.85.129 255.255.255.240  
  ip nat inside  
!  
interface GigabitEthernet0/1.99  
  encapsulation dot1Q 99  
  ip address 10.23.85.145 255.255.255.248  
  ip nat inside  
!  
interface GigabitEthernet0/2  
  no ip address  
  duplex auto  
  speed auto  
  shutdown  
!  
interface Serial0/1/0  
  ip address 64.100.13.1 255.255.255.252  
  ip nat outside  
  clock rate 2000000  
  crypto map VPN-MAP  
!  
interface Serial0/1/1  
  no ip address  
  clock rate 2000000  
  shutdown  
!  
interface Vlan1  
  no ip address
```

```
shutdown
!
//Налаштування NAT
ip nat inside source list p1 interface Serial0/1/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/1/0
!
ip flow-export version 9
!
access-list 110 permit ip 10.23.85.96 0.0.0.15 10.23.84.0 0.0.0.127
access-list 110 permit ip 10.23.85.112 0.0.0.15 10.23.84.0 0.0.0.127
access-list 110 permit ip 10.23.85.128 0.0.0.15 10.23.84.0 0.0.0.127
ip access-list extended p1
deny ip 10.23.85.96 0.0.0.15 10.23.84.0 0.0.0.127
deny ip 10.23.85.112 0.0.0.15 10.23.84.0 0.0.0.127
deny ip 10.23.85.128 0.0.0.15 10.23.84.0 0.0.0.127
permit ip 10.23.85.128 0.0.0.15 any
permit ip 10.23.85.112 0.0.0.15 any
permit ip 10.23.85.96 0.0.0.15 any
permit ip 10.23.85.144 0.0.0.7 any
access-list 1 permit 10.23.85.96 0.0.0.15
access-list 1 permit 10.23.85.112 0.0.0.15
access-list 1 permit 10.23.85.128 0.0.0.15
!
no cdp run
!
banner motd "Welcome to Shvec_Router"
!
//Налаштування AAA
radius server 209.165.200.3
```

```
address ipv4 209.165.200.3 auth-port 1645
key radius123
!
line con 0
password 7 0822455D0A16
!
line aux 0
!
line vty 0 4
password 7 0822455D0A16
transport input ssh
line vty 5 15
password 7 0822455D0A16
transport input ssh
!
end
```

## **2. Налаштування маршрутизатора Shvec\_Router\_3**

```
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
//Шифрування паролів
service password-encryption
!
//Ім'я пристрою
hostname Shvec_Router_3
!
//Пароль до привілейованого режиму
```

```

enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
//Налаштування AAA
aaa new-model
!
aaa authentication login default group radius local
!
no ip cef
no ipv6 cef
!
//Створення користувача з паролем
username      123-19-1_Shvec      privilege      15      secret      5
$1$mERr$MKp6WULHmjLdYVBw6rbD11
username      123191_Shvec      privilege      15      secret      5
$1$mERr$MKp6WULHmjLdYVBw6rbD11
!
license udi pid CISCO2911/K9 sn FTX152494FL-
license boot module c2900 technology-package securityk9
!
//Створення VPN
crypto isakmp policy 10
  encr aes
  authentication pre-share
  group 2
!
crypto isakmp key cisco address 64.100.13.1
!
crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
!
crypto map VPN-MAP 10 ipsec-isakmp

```

```
description VPN connection to R3
set peer 64.100.13.1
set transform-set VPN-SET
match address 110
!
//Створення домену и ssh
ip domain-name 1
!
spanning-tree mode pvst
!
//Налаштування інтерфейсів
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/0/0
```

```
bandwidth 128
ip address 10.0.18.2 255.255.255.252
delay 7500
ip nat inside
clock rate 128000
!
interface Serial0/0/1
bandwidth 128
ip address 10.0.18.6 255.255.255.252
delay 7500
ip nat inside
!
interface Serial0/1/0
bandwidth 128
ip address 10.0.18.10 255.255.255.252
delay 7500
ip nat inside
!
interface Serial0/1/1
ip address 209.165.202.2 255.255.255.252
ip nat outside
crypto map VPN-MAP
!
interface Vlan1
no ip address
shutdown
!
//Налаштування OSPF
router ospf 1
log-adjacency-changes
```



```
passive-interface default
no passive-interface Serial0/0/0
no passive-interface Serial0/0/1
no passive-interface Serial0/1/0
network 10.23.84.0 0.0.3.255 area 0
network 10.0.18.0 0.0.0.255 area 0
!
//Налаштування NAT
ip nat pool Internet 209.165.200.5 209.165.200.30 netmask 255.255.255.224
ip nat inside source list p18 pool Internet
ip nat inside source static 10.23.84.29 209.165.200.4
ip nat inside source static 10.23.84.28 209.165.200.3
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/1/1
!
ip flow-export version 9
!
access-list 110 permit ip 10.23.84.0 0.0.0.127 10.23.85.96 0.0.0.15
access-list 110 permit ip 10.23.84.0 0.0.0.127 10.23.85.112 0.0.0.15
access-list 110 permit ip 10.23.84.0 0.0.0.127 10.23.85.128 0.0.0.15
ip access-list extended p18
deny ip 10.23.84.0 0.0.0.127 10.23.85.96 0.0.0.15
deny ip 10.23.84.0 0.0.0.127 10.23.85.112 0.0.0.15
deny ip 10.23.84.0 0.0.0.127 10.23.85.128 0.0.0.15
permit ip 10.23.84.0 0.0.0.127 any
permit ip 10.23.84.0 0.0.3.255 any
!
no cdp run
!
banner motd "Welcome to Shvec_Router"
```

```
!  
//Налаштування AAA  
radius server 10.23.84.28  
  address ipv4 10.23.84.28 auth-port 1645  
  key radius123  
!  
line con 0  
  password 7 0822455D0A16  
!  
line aux 0  
!  
line vty 0 4  
  password 7 0822455D0A16  
  transport input ssh  
line vty 5 15  
  password 7 0822455D0A16  
  transport input ssh  
!  
end
```

### **3. Налаштування маршрутизатора Shvec\_Router\_IPS**

```
!  
version 15.1  
no service timestamps log datetime msec  
no service timestamps debug datetime msec  
//Шифрування паролів  
service password-encryption  
!  
//Ім'я пристрою
```

```

hostname Shvec_Router_IPS
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
aaa new-model
!
//Пароль до привілейованого режиму
aaa authentication login default group radius local
!
no ip cef
no ipv6 cef
!
//Створення користувача з паролем
username          123191_Shvec          privilege          15          secret          5
$1$mERr$MKp6WULHmjLdYVBw6rbD11
!
license udi pid CISCO2911/K9 sn FTX1524C145-
!
ip domain-name Shvec_Router_IPS
!
spanning-tree mode pvst
!
//Налаштування інтерфейсів
interface GigabitEthernet0/0
ip address 209.165.201.1 255.255.255.240
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address

```

```
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/1/0
ip address 64.100.13.2 255.255.255.252
!
interface Serial0/1/1
ip address 209.165.202.1 255.255.255.252
clock rate 128000
!
interface Vlan1
no ip address
shutdown
!
ip classless
ip route 209.165.200.0 255.255.255.224 Serial0/1/1
!
ip flow-export version 9
!
no cdp run
!
banner motd "Welcome to Shvec_Router"
!
```

```
//Налаштування AAA
radius server 209.165.200.3
  address ipv4 209.165.200.3 auth-port 1645
  key radius123
!
line con 0
  password 7 0822455D0A16
!
line aux 0
!
line vty 0 4
  password 7 0822455D0A16
  transport input ssh
line vty 5 15
  password 7 0822455D0A16
  transport input ssh
!
end
```

#### **4. Налаштування комутатора Shvec\_Switch\_1**

```
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
//Шифрування паролів
service password-encryption
!
//Ім'я пристрою
hostname Shvec_Switch_1
```

```
!  
//Пароль до привілейованого режиму  
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1  
!  
//Налаштування AAA  
aaa new-model  
!  
aaa authentication login default group radius local  
!  
ip domain-name Shvec_Switch_1  
!  
//Створення користувача з паролем  
username 123191_Shvec secret 5 $1$mERr$MKp6WULHmjLdYVBw6rbD11  
!  
spanning-tree mode pvst  
spanning-tree extend system-id  
!  
//Налаштування VLAN та інтерфейсів  
interface FastEthernet0/1  
  switchport trunk allowed vlan 28,38,48,99-100  
  switchport mode trunk  
!  
interface FastEthernet0/2  
  switchport access vlan 28  
  switchport mode access  
  switchport port-security  
  switchport port-security maximum 2  
  switchport port-security mac-address sticky  
  switchport port-security violation restrict  
  switchport port-security mac-address sticky 0040.0BC9.6C87
```

```
!  
interface FastEthernet0/3  
shutdown  
!  
interface FastEthernet0/4  
shutdown  
!  
interface FastEthernet0/5  
switchport access vlan 48  
switchport mode access  
!  
interface FastEthernet0/6  
switchport access vlan 48  
switchport mode access  
!  
interface FastEthernet0/7  
switchport access vlan 48  
switchport mode access  
!  
interface FastEthernet0/8  
switchport access vlan 48  
switchport mode access  
!  
interface FastEthernet0/9  
switchport access vlan 48  
switchport mode access  
!  
interface FastEthernet0/10  
switchport access vlan 38  
switchport mode access
```

```
!  
interface FastEthernet0/11  
  switchport access vlan 38  
  switchport mode access  
!  
interface FastEthernet0/12  
  switchport access vlan 38  
  switchport mode access  
!  
interface FastEthernet0/13  
  switchport access vlan 38  
  switchport mode access  
!  
interface FastEthernet0/14  
  switchport access vlan 38  
  switchport mode access  
!  
interface FastEthernet0/15  
  switchport access vlan 28  
  switchport mode access  
!  
interface FastEthernet0/16  
  switchport access vlan 28  
  switchport mode access  
!  
interface FastEthernet0/17  
  switchport access vlan 28  
  switchport mode access  
!  
interface FastEthernet0/18
```



```
switchport access vlan 28
switchport mode access
!
interface FastEthernet0/19
switchport access vlan 28
switchport mode access
!
interface FastEthernet0/20
switchport access vlan 28
switchport mode access
!
interface FastEthernet0/21
switchport access vlan 28
switchport mode access
!
interface FastEthernet0/22
switchport access vlan 28
switchport mode access
!
interface FastEthernet0/23
switchport access vlan 28
switchport mode access
!
interface FastEthernet0/24
switchport access vlan 28
switchport mode access
!
interface GigabitEthernet0/1
switchport trunk allowed vlan 28,38,48,99-100
switchport mode trunk
```

```
!  
interface GigabitEthernet0/2  
  switchport trunk allowed vlan 28,38,48,99-100  
  switchport mode trunk  
!  
interface Vlan1  
  no ip address  
  shutdown  
!  
interface Vlan99  
  ip address 10.23.85.147 255.255.255.248  
!  
ip default-gateway 10.23.85.145  
!  
banner motd "Welcome to Shvec_Router"  
radius-server host 209.165.200.3 auth-port 1645 key cisco  
!  
line con 0  
  password 7 0822455D0A16  
  login  
!  
line vty 0 4  
  password 7 0822455D0A16  
  transport input ssh  
line vty 5 15  
  password 7 0822455D0A16  
  transport input ssh  
!  
end
```

## 5. Налаштування комутатора Shvec\_Switch\_6

```
!  
version 15.0  
no service timestamps log datetime msec  
no service timestamps debug datetime msec  
//Шифрування паролів  
service password-encryption  
!  
//Ім'я пристрою  
hostname Shvec_Switch_6  
!  
//Пароль до привілейованого режиму  
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1  
!  
//Налштування AAA  
aaa new-model  
!  
aaa authentication login default group radius local  
!  
ip domain-name Shvec_Switch_6  
!  
//Створення користувача з паролем  
username 123191_Shvec secret 5 $1$mERr$MKp6WULHmjLdYVBw6rbD11  
!  
spanning-tree mode pvst  
spanning-tree extend system-id  
!  
//Налаштування інтерфейсів  
interface Port-channel1
```

```
switchport mode trunk
!
interface Port-channel3
switchport mode trunk
!
interface FastEthernet0/1
switchport mode trunk
channel-group 1 mode auto
!
interface FastEthernet0/2
switchport mode trunk
channel-group 1 mode auto
!
interface FastEthernet0/3
switchport mode trunk
channel-group 3 mode desirable
!
interface FastEthernet0/4
switchport mode trunk
channel-group 3 mode desirable
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
```

```
!  
interface FastEthernet0/10  
!  
interface FastEthernet0/11  
!  
interface FastEthernet0/12  
!  
interface FastEthernet0/13  
!  
interface FastEthernet0/14  
!  
interface FastEthernet0/15  
!  
interface FastEthernet0/16  
!  
interface FastEthernet0/17  
!  
interface FastEthernet0/18  
!  
interface FastEthernet0/19  
!  
interface FastEthernet0/20  
!  
interface FastEthernet0/21  
!  
interface FastEthernet0/22  
!  
interface FastEthernet0/23  
!  
interface FastEthernet0/24
```

```
!  
interface GigabitEthernet0/1  
!  
interface GigabitEthernet0/2  
!  
interface Vlan1  
  ip address 10.23.85.4 255.255.255.192  
!  
  ip default-gateway 10.23.85.1  
!  
  banner motd "Welcome to Shvec_Router"  
  radius-server host 10.23.84.28 auth-port 1645 key cisco  
!  
line con 0  
  password 7 0822455D0A16  
  login  
!  
line vty 0 4  
  password 7 0822455D0A16  
  transport input ssh  
line vty 5 15  
  password 7 0822455D0A16  
  transport input ssh  
!  
end
```

## Додаток В

Текст програми налаштування  
системи клімат контролю

**Міністерство освіти і науки України  
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ  
“ДНІПРОВСЬКА ПОЛІТЕХНІКА”**

**ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ  
СИСТЕМИ КЛІМАТ КОНТРОЛЮ**

Текст програми

804.02070743.23019-02 12 01

Листів 6



## АНОТАЦІЯ

Цей документ включає в себе програмне забезпечення системи клімат контролю.

Текст програм для системи клімат контролю було реалізовано на мові JavaScript.

## ЗМІСТ

1. Налаштування плати клімат контролю .....	4
---	---

## 1. Налаштування плати клімат контролю

//Визначимо змінні, які використовуються для керування підключеними пристроями

```
var ledPin = 5;  
var ledPin2 = 4;  
var potPin = A0;  
var value = 0;  
var cool = 2;  
var heat = 3;
```

//Вказуємо, які пристрої являються вихідними.

```
function setup() {  
    pinMode(ledPin, OUTPUT);  
    pinMode(ledPin2, OUTPUT);  
    pinMode(cool, OUTPUT);  
    pinMode(heat, OUTPUT);  
  
}
```

//Виконаємо зчитування температури з датчика температури

```
function loop() {  
    var newValue = analogRead(potPin);  
    newValue = ((analogRead(A0) *200/1023)-100);  
    if (newValue != value) {  
        Serial.println("new value: " + newValue);  
        analogWrite(ledPin, newValue);  
        value = newValue;  
    }  
}
```

*/\* Якщо температура в межах від 25 °C до 37 °C, то необхідно включити охолоджувач, та вимкнути у разі температури або нижче або дорівнює 25 °C та коли або вище або дорівнює 37 °C \*/*

```

    if(value>25)
    {
        if(value<37)
        {
            digitalWrite(2, HIGH)
            digitalWrite(4, HIGH)
            digitalWrite(5, HIGH)
            delay(1);
            digitalWrite(4, LOW)
            digitalWrite(5, LOW)
        }
        else
        {
            digitalWrite(2, LOW)
        }
    }
    else
    {
        digitalWrite(2, LOW)
    }

```

*/\* Якщо температура в межах від 15 °C до 23 °C , то необхідно увімкнути нагрівач. Якщо температура нижче або дорівнює 15 °C, то необхідно вимкнути нагрівач. Якщо температура вище або дорівнює 21 °C, то необхідно вимкнути нагрівач. \*/*

```

    if(value>15)
    {

```

```
if(value<21)
{
    digitalWrite(3, HIGH)
    digitalWrite(4, HIGH)
    digitalWrite(5, HIGH)
    delay(1);
    digitalWrite(4, LOW)
    digitalWrite(5, LOW)
}
else
{
    digitalWrite(3, LOW)
}
}
else
{
    digitalWrite(3, LOW)
}
}
```