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 Волков Владислав Русланович
(ПІБ)

академічної групи 123–19ск–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 комплексу кінотеатрів "Планета кіно" міста Дніпро з опрацюванням побудови, налаштування та безпеки корпоративної мережі"
(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.			
Рецензент				
Нормоконтролер	проф. Цвіркун Л.І.			

Дніпро
2022

ЗАТВЕРДЖЕНО:

завідувач кафедри
інформаційних технологій
та комп'ютерної інженерії
(повна назва)

_____ Гнатушенко В.В.
(підпис) (прізвище, ініціали)

"25" січня 2022 року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавр

студента Волков В.Р. **академічної групи** 123–19ск–1
(прізвище та ініціали) (шифр)

спеціальності 123 «Комп'ютерна інженерія»

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

на тему "Комп'ютерна система комплексу кінотеатрів "Планета кіно" міста Дніпро з опрацюванням побудови, налаштування та безпеки корпоративної мережі"
затверджену наказом ректора НТУ «Дніпровська політехніка» від 18.05.2022 № 268–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	10.05.2022
Розробка апаратної частини	На основі аналізу підприємства формулюються технічні вимоги до комп'ютерної системи та розробляється апаратна частина системи	17.05.2022
Розробка корпоративної мережі	Виконується розрахунок налаштувань корпоративної мережі та перевірка роботи системи, розробляються методи та налаштування обладнання для захисту інформації в системі	24.05.2022
Розробка компонента системи	Виконується детальна розробка компонента системи	31.05.2022

Завдання видано _____ проф. Цвіркун Л.І.
(підпис керівника) (прізвище, ініціали)

Дата видачі 25.01.2022

Дата подання до екзаменаційної комісії 14.06.2022

Прийнято до виконання _____ Волков В.Р.
(підпис керівника) (прізвище, ініціали)

РЕФЕРАТ

КОМП’ЮТЕРНІ СИСТЕМИ, CISCO, КОМП’ЮТЕРНА МЕРЕЖА, КІНОТЕАТР, IoT.

Пояснювальна записка: 93 с., 42 рис., 9 табл., 1 дод., 5 джерел.

Об’єкт дослідження – комп’ютерна система комплексу кінотеатрів «Планета кіно» міста Дніпро з опрацюванням побудови, налаштування та безпеки корпоративної мережі.

Мета роботи – розробка локальної мережі для комплексу кінотеатрів «Планета кіно» в місті Дніпро. Основна задача полягає в аналізі вимог до проектування комп’ютерної системи, підібрати необхідне обладнання для реалізації мережі, розглянути питання розробки апаратної частини комп’ютерної системи.

Розроблена комп’ютерна мережа з можливістю швидкого додання нових пристроїв, об’єднує підрозділи в єдину мережу, забезпечує зв’язок між кінцевими споживачами у різних підрозділах та надає доступ до Інтернету.

Розроблена комп’ютерна мережа виконана відповідно до завдання на кваліфікаційну роботу бакалавра.

Робота системи розроблена та перевірена за допомогою застосування програмного додатка Cisco Packet Tracer.

Результати перевірки описані і наводяться у вигляді таблиць та графіків у пояснювальній записці та додатках.

ЗМІСТ

Перелік скорочень, умовних позначень, одиниць і термінів 5
Вступ 6
1 Стан питання та постановка завдання 7
1.1 Стисла характеристика галузі та умови застосування КС 7
1.2 Огляд існуючих інженерних рішень КС в галузі та визначення можливих напрямків рішення поставлених завдань 7
1.3 Розробка схеми організаційної структури підприємства 8
2 Розробка апаратної частини комп'ютерної системи підприємства 15
2.1 Технічні вимоги до КС комплексу кінотеатрів «Планета кіно» 15
2.1.1 Вимоги до системи в цілому 15
2.1.1.1 Вимоги до структури і функціонування системи 15
2.1.1.2 Вимоги до показників призначення: 16
2.1.1.3 Вимоги до експлуатації, технічного обслуговування, ремонту і зберігання компонентів системи 16
2.1.1.4 Вимоги до патентної чистоти 17
2.1.1.5 Додаткові вимоги 17
2.1.2 Вимоги до функцій які виконує система 18
2.1.3 Вимоги до видів забезпечення системи 19
2.1.3.1 Вимоги до інформаційного забезпечення: 19
2.1.3.2 Вимоги до лінгвістичного забезпечення 19
2.1.3.3 Вимоги до програмного забезпечення 19
2.1.3.4 Вимоги до технічного забезпечення 19
2.2 Розробка інженерного рішення комп'ютерної системи підприємства «Планета кіно» 20
2.2.1 Вибір і обґрунтування структурної схеми комплексу технічних засобів комп'ютерної системи 25
2.2.2 Розробка специфікації апаратних засобів комп'ютерної системи 26
2.2.3 Розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі підприємства 31
3 Проектування корпоративної мережі та перевірка роботи комп'ютерної системи підприємства 34
3.1 Розрахунок схеми адресації корпоративної мережі 34
3.2 Налаштування та перевірка роботи комп'ютерної системи 39
3.2.1 Базове налаштування конфігурації пристроїв 39
3.2.2 Налаштування маршрутизаторів корпоративної мережі 40
3.2.3 Налаштування роботи Інтернет 45
3.2.4 Налаштування агрегування каналів PAgP 47
3.2.5 Налаштування віртуальної приватної мережі site–to–site VPN з 49

3.2.6 Перевірка роботи комп’ютерної системи 51
3.3 Захист інформації в КС від несанкціонованого доступу 55
3.3.1. Розробка методів для захисту інформації в комп’ютерній системі 55
3.3.2 Налаштування мереж VLAN 55
3.3.3 Налаштування параметрів безпеки комутаторів та адресації ПК в мережах VLAN 58
3.3.4 Налаштувати всі маршрутизатори на підтримку служби AAA та RADIUS–сервер. 63
4. Розробка компонента системи 65
4.1 Стан питання та постановка завдання 65
4.2 Реалізація системи 66
4.2.1 Налаштування мережі Strit 66
4.2.2 Налаштування мережі IPS Server 68
4.2.3 Налаштування пристроїв в мережі Office 74
4.2.4 Реалізація туманних обчислень 77
4.2.5 Реалізація хмарних обчислень 81
4.3 Перевірка роботи комп’ютерної системи 82
Додаток А Програмне забезпечення налаштування мережі комп’ютерної системи 87

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, ОДИНИЦЬ І ТЕРМІНІВ

КС – Комп’ютерна система

КМ – Комп’ютерна мережа

ПК – Портативний комп’ютер

DNS – Domain name Systems

DHCP – Dynamic Host Configuration Protocol

IoT – інтернет речі

IP – Internet Protocol

LAN – Local Area Network

NAT – Network Address Translation

OSPF – Open Shortest Path First

VPN – Virtual Privat Network

ВСТУП

На сьогоднішній день важко уявити створення бізнесу без використання комп’ютерних мереж у них. За останні роки інформаційні технології стали не від’ємною частиною нашохо побуту, тому було прийнято рішення упровадження комп’ютерної системи комплексу кінотеатрів «Планета кіно» міста Дніпро.

Дана комп’ютерна система після впровадження буде забезпечувати швидке з’єднання користувачів між відділами, забезпечення безпекових налаштування для запобігання стороннього доступу до мережі, та використані технології, які забезпечуються працездатність кінцевого рішення..

Дана комп’ютерна система являється сукупність, фізичної частини розробленого апаратного рішення, а з програмними налаштуваннями. Сучасні мережеві рішення спираються на програмно–апаратний комплекс, що забезпечує взаємодію співробітників підприємства. Розроблена комп’ютерна система спирається на впровадження мережевих рішень, які поділяються на корпоративні, локальні, так і глобальні мережні технології. При створенні офісної мережі необхідно створити або оновити локальну або корпоративну мережу та створити серверний центр. Отже, основною функцією комп’ютерних систем є обробка збереженим даних.

Головне призначення мережі, забезпечення зручного та надійного доступу користувачів до загально мережевих ресурсів, забезпечити надійним захист від несанкціонованого доступу та надати надійну і зручну можливість передавати данні між користувачами в мережі.

СТАН ПИТАННЯ ТА ПОСТАНОВКА ЗАВДАННЯ

1.1 Стисла характеристика галузі та умови застосування КС

Кіноіндустрія важлива складова сфери культури. Кіно допомагає особистості відгородитися від проблем, зануритися в іншу реальність. У 21 столітті кіно – не спосіб розважитися, а джерело для початку мислення, аналізу, а також пізнання. Кіноіндустрія – потужний важіль для розвитку країни.

Важливу роль в кіноіндустрії відіграє кінопрокат. Кінопрокат займається масовим розповсюдженням фільмів по мережам кінотеатрів. Один із представників демонстрації фільмів є мережа кінотеатрів «Планета кіно». Для показу фільмів використовується новітнє обладнання та сучасні технології такі, як IMAX, 4DX, RE`LUX та технологія власного виробництва CINETECH+ та CINETECH+Laser.

В мережі кінотеатрів «Планета кіно» налічується дев’ять кінотеатрів в шістьох містах України, тому важливо підтримувати зв’язок між усіма кінотеатрами. Для підтримки зв’язку використовується новітнє мережеве обладнання високої якості.

1.2 Огляд існуючих інженерних рішень КС в галузі та визначення можливих напрямків рішення поставлених завдань

Однією із вимог замовника для побудови мережі було використання обладнання Cisco. Головні переваги даного обладнання:

– забезпечення високого рівня адаптивності бізнесу рахунок автоматизації мережі;

– автоматичне відновлення даних та їх резервування після можливих збоїв;

– відмінні показники параметрів надійності та відмовостійкості;

– виняткова продуктивність бездротових мереж із високою щільністю підключення;

– комплексний підхід до контролю нормальної працездатності мереж та докладне інструктування щодо усунення збоїв;

– мінімізація вразливості у будь–яких точках мережі;

– можливість застосування аналітики для оптимізації продуктивності, програмного забезпечення;

Для рішення поставлених завдань використано сервіс DHCP, що дозволяє комп’ютерам автоматично отримувати IP-адресу та інші параметри, необхідні для роботи в мережі та обрано протокол динамічної маршрутизації OSPF, тому що, це вдосконалений дистанційно-векторний протокол, розроблений компанією Cisco. Для зв’язку між офісами здійснити налаштування NAT.

1.3 Розробка схеми організаційної структури підприємства

Компанія «Планета кіно» має два кінотеатри в місті Дніпро. Перший знаходиться в ТРК «APPOLO» за адресую вулиця Титова, 36, Дніпро, Дніпропетровська область, 49000, а другий в ТРК «МОСТ-сіті» за адресую улиця Глінки, 2, Дніпро, Дніпропетровська область, 49000. Відстань між двома офісами складає 5.03 км. Топологічна схема розміщення кінотеатрів представлена на рисунках 1.1 – 1.3.

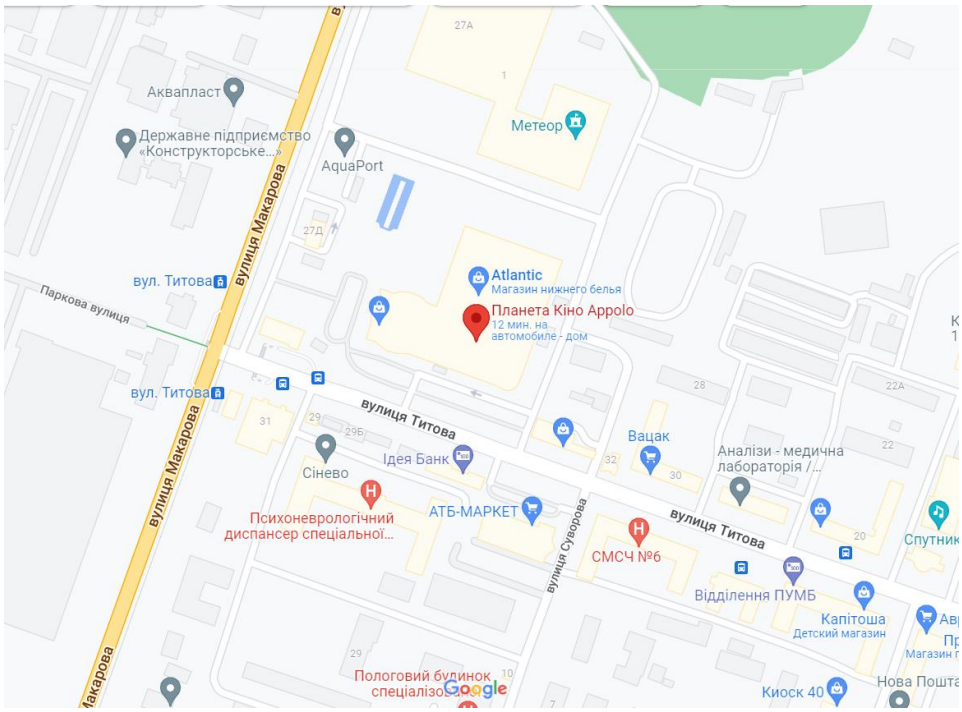

Рисунок 1.1 – Топологічна схема розміщення кінотеатру в ТРК «APPOLO»

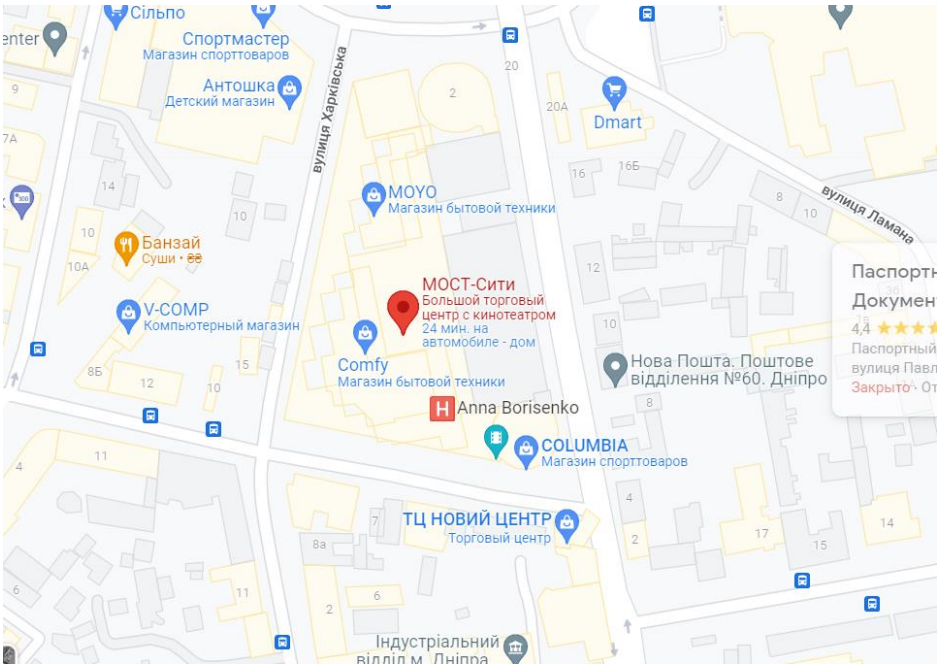

Рисунок 1.2 – Топологічна схема розміщення кінотеатру в ТРК «МОСТ–сіті»

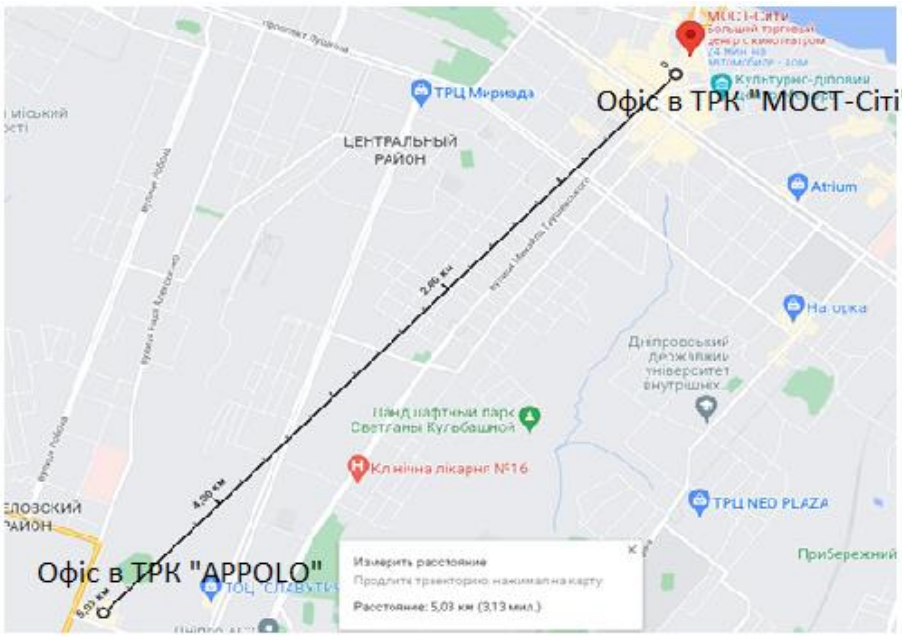

Рисунок 1.3 – Зображення відстані між двома кінотеатрами «Планета кіно» в місті Дніпро

Організаційна структура мережі кінотеатрів «Планета кіно» складається з наступних підрозділів:

– адміністративний відділ;

– фінансовий відділ;

– відділ управління персоналом;

– відділ маркетингу та продажу;

– відділ технічного забезпечення.

Адміністративна частина: керівник підприємства та підлеглі йому заступник та помічники. Керівник повинен мати доступ до усіх систем та надавати всю інформацію, стосовно робочого процесу до головного офісу.

Фінансовий відділ: бухгалтер та помічник. Бухгалтерія повинна мати можливість отримувати звіт від відділу продаж.

Відділ управління персоналом: керівник відділу кадрів, HR–менеджер. HR–менеджер виконує роботу з персоналом особисто та звітує безпосередньо перед головним керівником.

До відділу маркетингу та продаж входять: головний менеджер та його

персонал. Головний менеджер отримує звіти з продаж від кожного свого працівника та звітує його перед головним керівником та бухгалтерією.

Відділ технічного забезпечення: Головний інженер, кіномеханік та IT–спеціаліст, забезпечують надійне функціонування комп'ютерної та іншої техніки, її розвиток та адаптацію, автоматизацію різних напрямків діяльності мережі кінотеатру.

Офісна частина в ТРК «APPOLO» займає два поверхи та має такі відділи: на першому поверсі відділ маркетингу та продажу, відділ технічного забезпечення, фінансовий відділ, на другому поверсі адміністративний відділ.

Офісна частина в ТРК «МОСТ-сіті» має такі відділи: відділ управління персоналом.

Організаційна структурна схема наведена в рисунку1.4.

План приміщення наведено на рисунках 1.5 – 1.6.

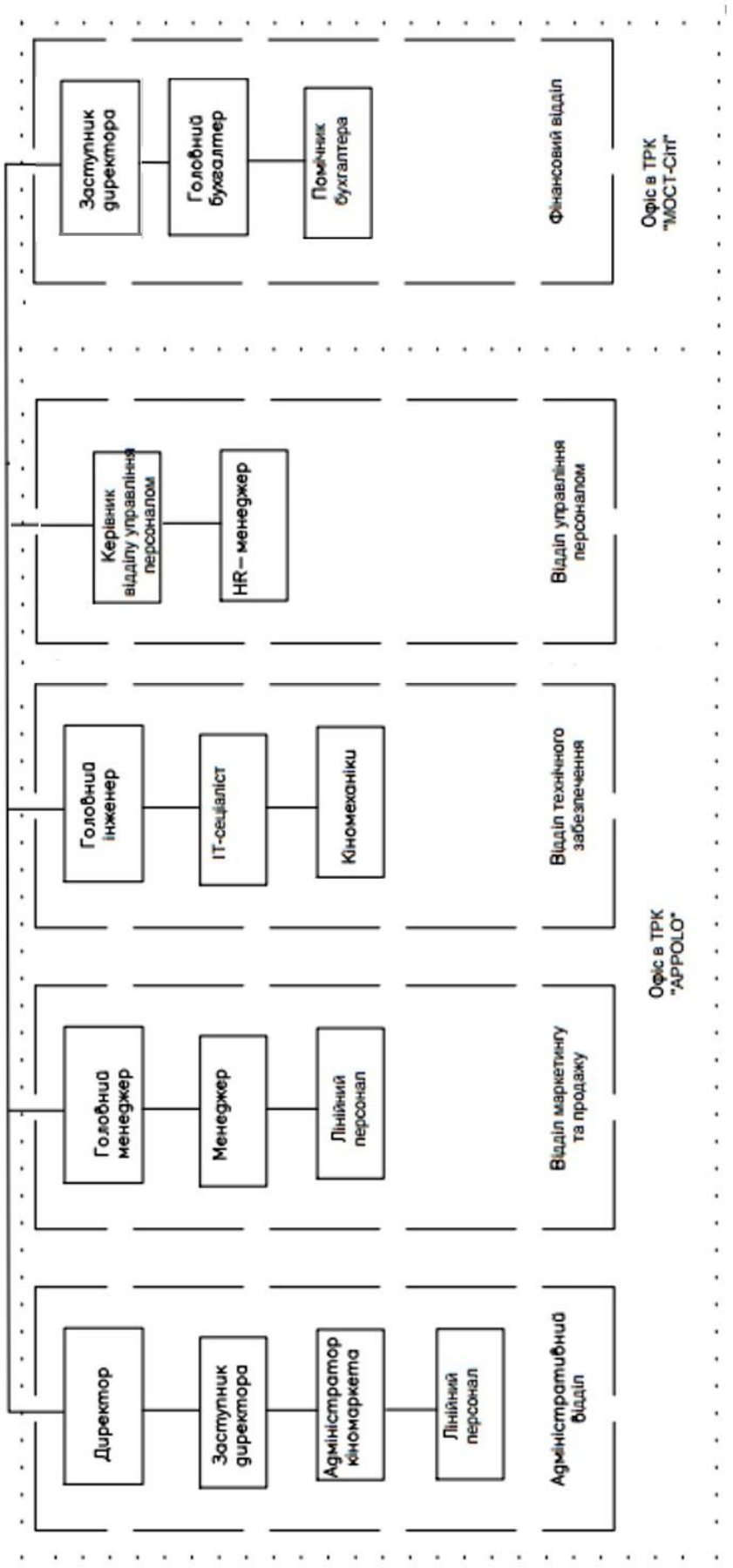

Рисунок 1.4 – Організаційна структурна схема

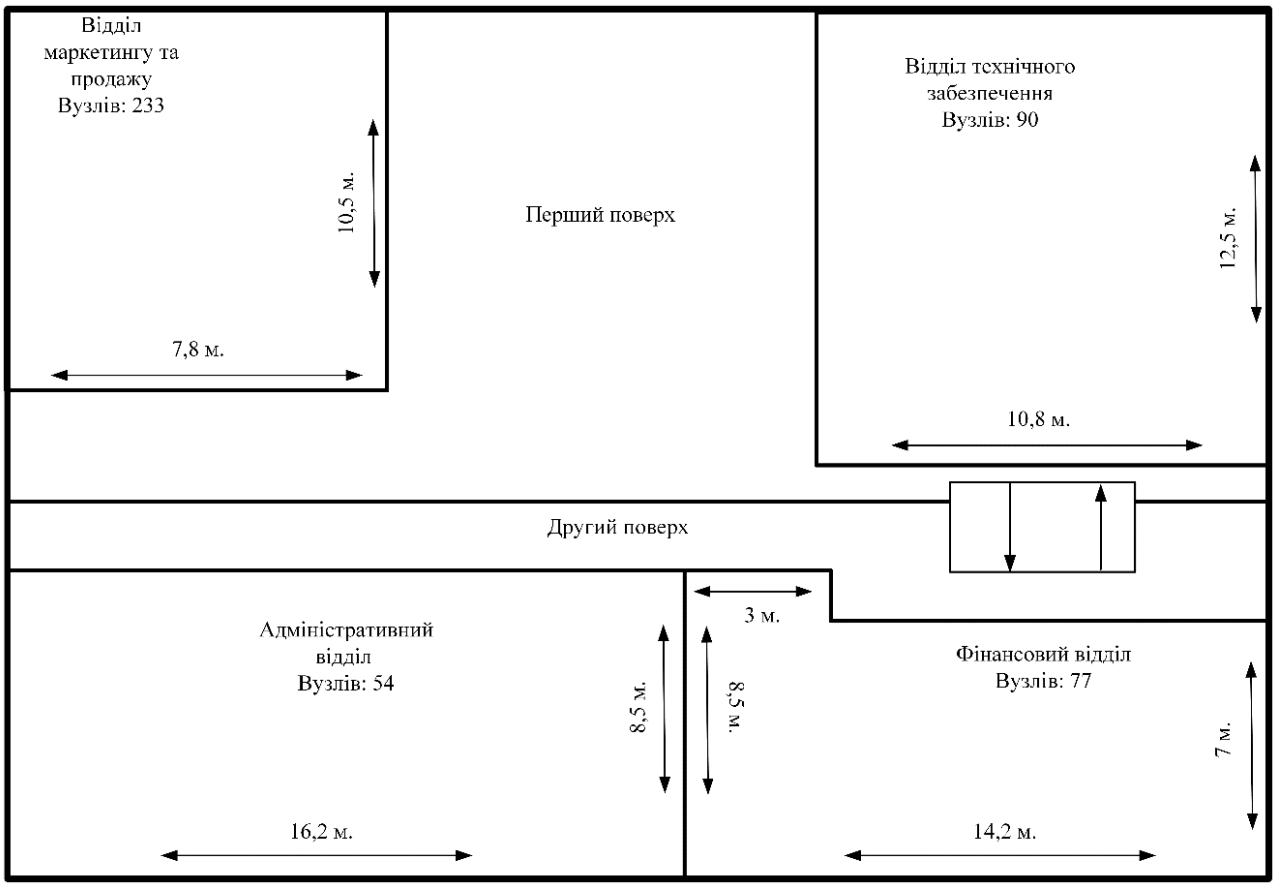

Рисунок 1.5 – План офісного приміщення в ТРЦ «APPOLO»

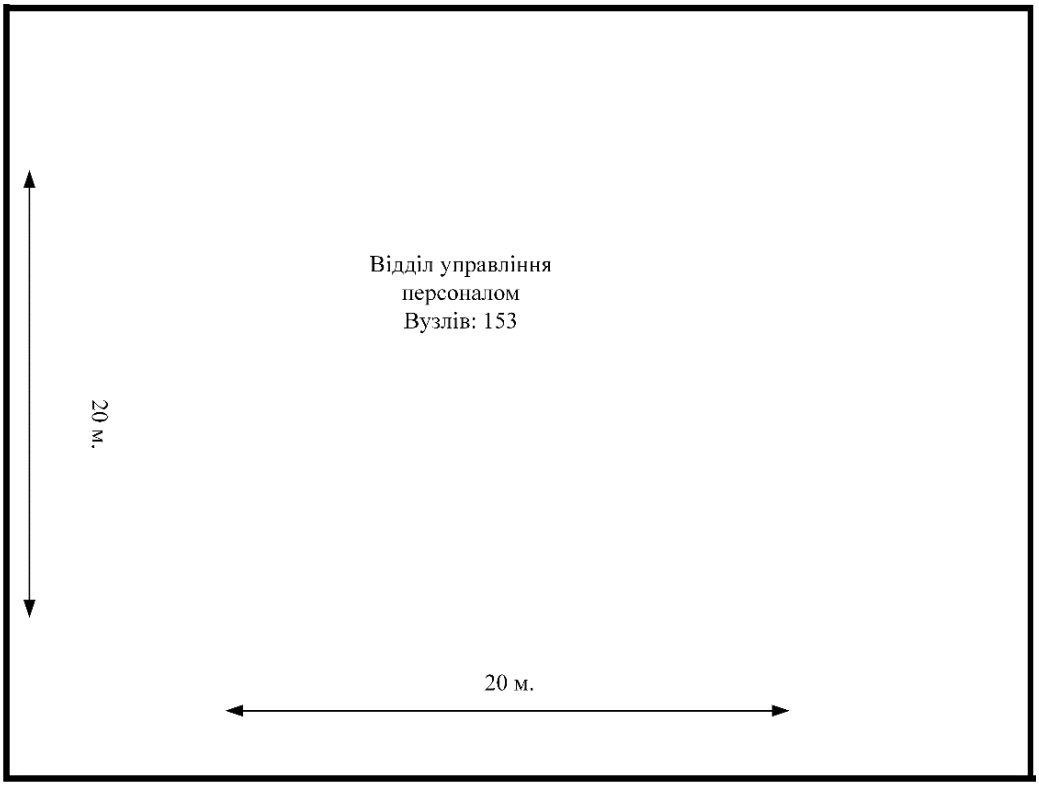

Рисунок 1.6 – План офісного приміщення в ТРЦ «МОСТ–сіті»

1.4 Постановка завдання

Згідно умов, які надав замовник, а саме забезпечити зв’язок між підмережами в головному офісі та можливість обміну даними з віддаленою мережею, налаштувати безпеку на мережевому обладнанні, тому виходячи з цього, для реалізації мережі, обрано мережеве обладнання фірми Cisco. Основні чинники вибору даного обладнання, висока надійність та відмовостійкість.

Для рішення поставлених завдань необхідно вирішити, який протокол динамічної маршрутизації використати, які відділи повинні мати захист та яким способом та як буде реалізовано роботу з провайдером.

Для реалізації маршрутизації, використано протокол динамічної маршрутизації OSPF. Це відкритий протокол оснований на технології відстеження стану каналів та використовується для знаходження найкоротшого шляху.

В підмережі «Відділ технічного забезпечення» встановлено два комутатори, тому доцільно буде виконати налаштування технології VLAN з підключенням технології DHCP, для коректного розподілу IP-адрес в мережах.

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ ПІДПРИЄМСТВА

2.1 Технічні вимоги до КС комплексу кінотеатрів «Планета кіно»

2.1.1 Вимоги до системи в цілому

2.1.1.1 Вимоги до структури і функціонування системи

В рамках створення комп'ютерної мережі для комплексу кінотеатрів, слід розробити наступні ключові підсистеми:

- підсистема адміністративного відділу;
- підсистема фінансового відділу;
- підсистема відділу маркетингу та продажу;
- підсистема відділу управління персоналу;
- підсистема технічного забезпечення.

Система повинна забезпечувати:

- підключення всіх комп'ютерів до мережі;
- передача та зберігання інформації;
- налаштування безпеки різних частин мережі;
- файловий сервер, який зберігає всі звіти протягом довгого часу;
- доступ до сервера з мережі інтернет.

Для підвищення пожежної безпеки за допомогою Інтернет речей створити систему, яка буде запобігати пожежу в «Відділі управління персоналом». Створити систему, яка за допомогою розумних пристроїв буде відстежувати стан системи пожежної безпеки за допомогою технології 3G/4G. Також слід виконати наступні налаштування:

- налаштувати DNS та IoT сервери для віддаленого підключення до виконавчих пристроїв;
- налаштувати DHCP–сервіс для виконавчих пристроїв;
- налаштувати сценарії для датчиків у разі пожежі;

– реалізувати систему з виконавчими датчиками, а саме датчики пожежної безпеки та сирена;

– налаштувати контролер MCU на мові Python для реалізації сценаріїв.

2.1.1.2 Вимоги до показників призначення:

Система повинна забезпечувати функціонування обладнання відповідно до умов технологічного процесу, а саме:

– використання технологій для захисту мережі;

– можливість віддаленого доступу працівників до робочого місця;

– відмовостійкість мережі для цілодобового використання;

– зберігання даних на серверному обладнанні.

2.1.1.3 Вимоги до експлуатації, технічного обслуговування, ремонту і зберігання компонентів системи

Технічний і фізичний захист апаратних компонентів системи, безперебійне енергопостачання для серверів, поточне обслуговування реалізується технічними та організаційними засобами.

Періодичне технічне обслуговування технічних засобів повинно проводитися відповідно до вимог технічної документації виробників, але не рідше одного разу на рік.

Періодичне технічне обслуговування і тестування технічних засобів повинні включати в себе обслуговування і тестування всіх використовуваних технічних засобів.

В процесі проведення періодичного технічного обслуговування повинні проводитися зовнішній і внутрішній огляд і чистка технічних засобів, перевірка контактних з'єднань, перевірка параметрів налаштувань працездатності технічних засобів і тестування їх взаємодії.

Розміщення обладнання, технічних засобів повинно відповідати вимогам техніки безпеки, санітарним нормам і вимогам пожежної безпеки.

2.1.1.4 Вимоги до патентної чистоти

Використовуване обладнання та програмне забезпечення повинно мати патентну частоту і бути сертифіковано для роботи у використовуваних режимах.

2.1.1.5 Додаткові вимоги

Усі елементи системи повинні мати захист не нижче IP30 для використання, як у серверних приміщеннях так і у звичайних.

Обладнання повинно мати близько 10% додаткових портів, для масштабованості мережі.

Встановлення активного обладнання має бути у стійках якщо розміщено в серверній кімнаті або на стінках у кімнатах загального використання.

Обладнання має забезпечувати безперебійне з'єднання, потрібну пропускну здатність та резерв по входах.

Тип кабелю повинен відповідати проектним розрахункам. Може бути вита–пара з екранованою оболонкою або оптоволокно. Використовується кабель типу UTP cat.5. Повинні встановлюватись інформаційні розетки.

Кількість та розміщення інформаційних розеток має відповідати розрахованій кількості та мати запас у 10% . Кількість електричних розеток має забезпечувати індивідуальне підключення мережевого обладнання і робочих станцій. Запас електричних розеток має складати 20%.

Для загальних кімнат сигнальні дроти мають розміщатись у коробах на стінах. Міжкімнатних та міжповерхових кабелів можуть бути прокладені у коробах і у лотках у верхній частині стелі.

При проектуванні слід закласти можливість для розширення мережі.

Додатково слід зазначити вимоги до надійності. Надійність компонентів мережі забезпечується виробником обладнання та додатковими протоколами та програмними засобами. Надійність повинна забезпечувати можливість швидкої заміни обладнання, яке вийшло з ладу. Також слід забезпечити надійність роботи

при відмові одного або декількох компонентів за рахунок їх резервування. Використовувати безперебійне живлення серверного обладнання.

Для безпеки мережі, необхідно забезпечити доступ до сервера тільки особам, які пройшли автентифікацію, створити облікові записи на AAA серверах, надати повний доступ до мережі лише адміністраторам та системному адміністратору, на ПК користувачів встановити антивірусне програмне забезпечення, компоненти мережі повинні мати високий рівень захисту налаштувань безпеки.

Для захисту інформації від несанкціонованого доступу слід використовувати програмні або апаратні мережеві екрани для фільтрації вхідних інформаційних потоків. Налаштування модулю автентифікації користувачів за допомогою логіна та пароля. Дані які передаються до мережі, мають буди зашифровані.

Для захисту від дії зовнішніх електромагнітних полів, слід використовувати екрановані кабелі типу вита пара. Для запобігання перепадів напруги у мережі, на вихідному кабелі повинен бути встановлений автоматичний вимикач. В серверній кімнаті повинна бути вентиляція, яка забезпечує нормальні кліматичні умови. Також повинно бути заземлення.

2.1.2 Вимоги до функцій які виконує система

Побудована комп’ютерна система підприємства буде складатись з п’яти підмереж. Мережеве обладнання повинно функціонувати кожного дня без перерви, без урахування часу необхідного для проведення регламентних робіт відповідно до рекомендацій виробника. У випадку не працездатності робочої станції, повинна бути можливість перейти на іншу робочу станцію для продовження роботи. Кожен відділ повинен підтримувати зв’язок один між одним, у співробітників повинен бути доступ до власного ПК. Повинна бути налагоджена система для гнучкого вирішення задач у найшвидший час.

Забезпечити систему IoT пристроїв для пожежної безпеки в відділі управління персоналом.

2.1.3 Вимоги до видів забезпечення системи

2.1.3.1 Вимоги до інформаційного забезпечення:

Інформаційне забезпечення повинно відповідати наступним вимогам:

– цілісність, а саме стійку роботу системи та автоматичне відновлення пристроїв у випадку виявлення системою потенційної помилки;

– контроль, на основі якого здійснюється адаптація системи;

– захист від несанкціонованого доступу;

2.1.3.2 Вимоги до лінгвістичного забезпечення

Для користувачі мережі, на всіх кінцевих пристроях інтерфейс повинен бути на українській мові.

2.1.3.3 Вимоги до програмного забезпечення

Програмне забезпечення повинно оновлюватись, обслуговуватись, поставляться та встановлюватись розробником на мережеве обладнання.

Системне програмне забезпечення встановлюється на станціях користувачів і на серверних станціях. У якості операційної системи для користувачів бажано використовувати windows10. А для серверних станцій можна встановити операційну систему Linux або windows server.

2.1.3.4 Вимоги до технічного забезпечення

Для створення мережевої частини повинно використовуватись мережеве обладнання фірми Cisco. Мережеве обладнання повинно відповідати наступним характеристикам:

Комутатор повинен мати такі конфігурації:

– кількість портів Gigabit Ethernet не менше 2;

– кількість портів SPF не менше 2 слоти;
– пропускна здатність не менше 64Мбайт;
– вбудована flach-пам’ять не менше 32Мб;
– кількість VLAN не менше 32.

Маршрутизатор повинен мати такі конфігурації:

– процесор ARM, не менш ніж 680 MHz;
– пам’ять не менше 256 Мб;
– Ethernet порти не менше 5 10/100/1000 Мбіт/с Ethernet портів;
– підтримка протоколів OSPF, RIP, BGP;
– підтримка VLAN необмежено;
– кількість NAT правил необмежено.

Комп’ютери користувачів повинні мати такі конфігурації:

– процесор Intel Core i5 або старша версія;
– процесор з тактовою частотою не менше 1,6 ГГц;
– об’єм оперативної пам’яті не менше 8Гб;
– жорсткий диск 256Гб;
– відеоадаптер не менше 16Mb.

Додатково має бути встановлено таке програмне забезпечення:

– Microsoft Office 2010;
– Microsoft Exel.

2.2 Розробка інженерного рішення комп’ютерної системи підприємства «Планета кіно»

Перед початком проектування комп’ютерної мережі, слід розробити схему розміщення структурних підрозділів. Головний офіс, який розташовано в ТРЦ «APPOLO» займає два поверхи: на першу знаходиться два відділи, відділ маркетингу та продажу і відділ технічного забезпечення, а на другому адміністративний відділ. Другий офіс розташований в ТРЦ «МОСТ-сіті», в

якому розміщено два відділи: фінансовий відділ та відділ управління персоналом.

Для реалізації комп'ютерної системи підприємства «Планета кіно» було обрано логічну топологію «зірка». В якості базової технології мережі обрана технологія Ethernet. Для під'єднання робочих груп застосовано FastEthernet, між маршрутизаторами – Serial Interface, та між маршрутизатором і комутатором – GigabitEthernet. Для підключення кінцевих пристроїв до мережі встановлюються інтернет розетки типу RJ-45.

Для комутації трафіку задіяно п'ять маршрутизаторів, що об'єднані мережами WAN. Для доступу локальних підмереж до маршрутизаторів застосовано технологію передачі даних GigabitEthernet. На прикордонному маршрутизаторі Volkov_RT3, виконується підключення проектованої мережі до Інтернет. Оскільки відстань між офісами сягає 5,03 км, щоб забезпечити зв'язок між маршрутизатором провайдера IPS та прикордонним маршрутизатором Volkov_RT3 налаштовано VPN для забезпечення захисту обміну трафіку між головним офісом там віддаленою мереже.

В мережі підприємства налаштовано єдиний адресний простір 172.22.64.0/20, а для каналів між маршрутизаторами використовується блок адрес 10.0.4.0. Мережа поділяється маршрутизаторами на п'ять підмереж. Оскільки використовується технологія адресації IPv4, тому для виходу в мережу Internet застосовується NAT. Для забезпечення маршрутизації, використовується протокол динамічної маршрутизації OSPF. На маршрутизаторі Volkov_RT0, для забезпечення маршрутизації між VLAN використовується технологія інкапсуляції 802.1Q та для адресації кінцевих пристроїв налаштовано протокол DHCP.

В підмережі «Відділ технічного забезпечення» встановлено два комутатори, тому всі користувачі підключається до мережі використовуючи технологію VLAN, для безпеки даних.

До підмережі «Адміністративний відділ» під’єднано три комутатори для розгортання PAgP, для підвищення швидкості передачі даних.

В усіх інших підмережах становлено по одному комутатору. Комутатори використовуються для об’єднання в локальну мережу кінцеві мережеві пристрої. В комп’ютерній системі «Планета кіно», до кінцевих пристроїв відносяться комп’ютери співробітників та сервери: сервер DNS в підмережі «Фінансовий відділ», Web–сервер HTTP в підмережі «Адміністративний відділ» та файловий сервер TFTP в підмережі «Відділ управління персоналом».

У віддаленій підмережі «Відділ управління персоналом» додатково встановлено пристрої Інтернет речей з можливістю контролювати температурний режим допомогою мобільного телефона через WI–FI або мобільний зв’язок та планшет, який знаходиться в офісі. Також встановлена пожежна сигналізація, яка у випадку спрацювання датчика полум’я , передає сигнал на сирену. Додатково для Інтернет речей налаштовано DNS-сервер та IoT-сервер**.**

Схему розміщення структурних підрозділів підприємства, можна переглянути на рисунках 2.1 – 2.2.

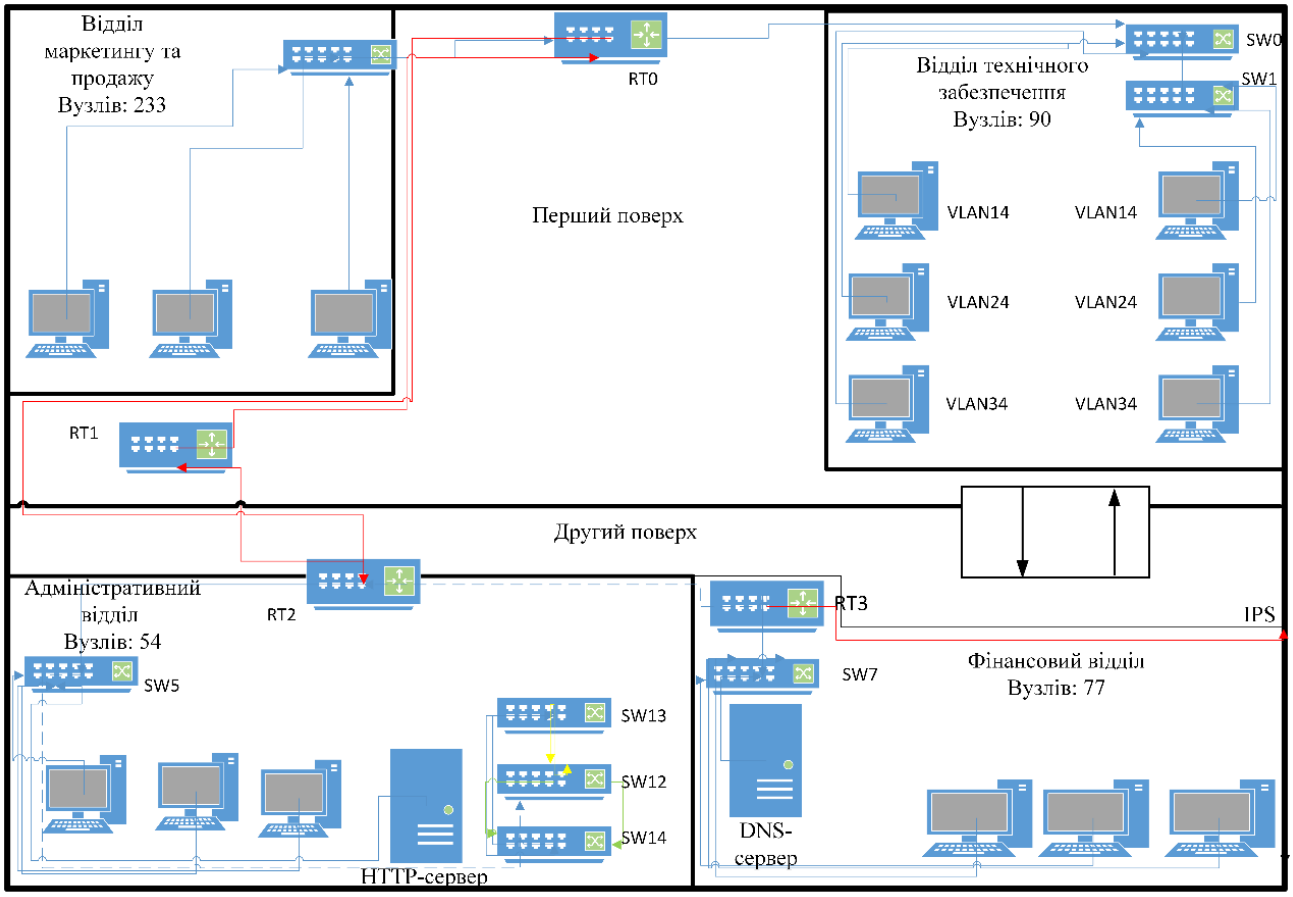

Рисунок 2.1 – Топологічна схема розміщення структурних підрозділів компанії в ТРЦ «APPOLO »

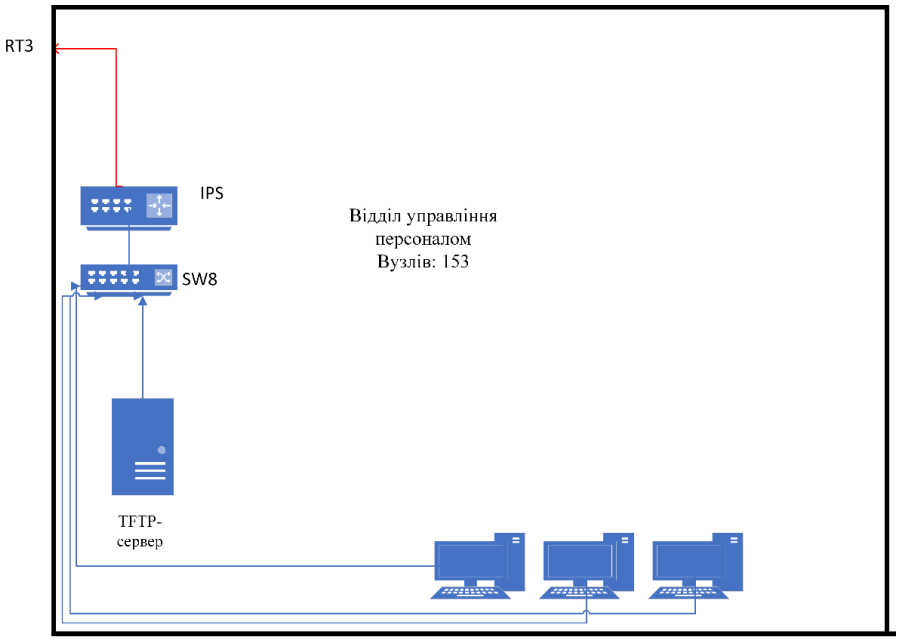

Рисунок 2.2 – Топологічна схема розміщення структурних підрозділів компанії в ТРЦ «МОСТ-сіті »

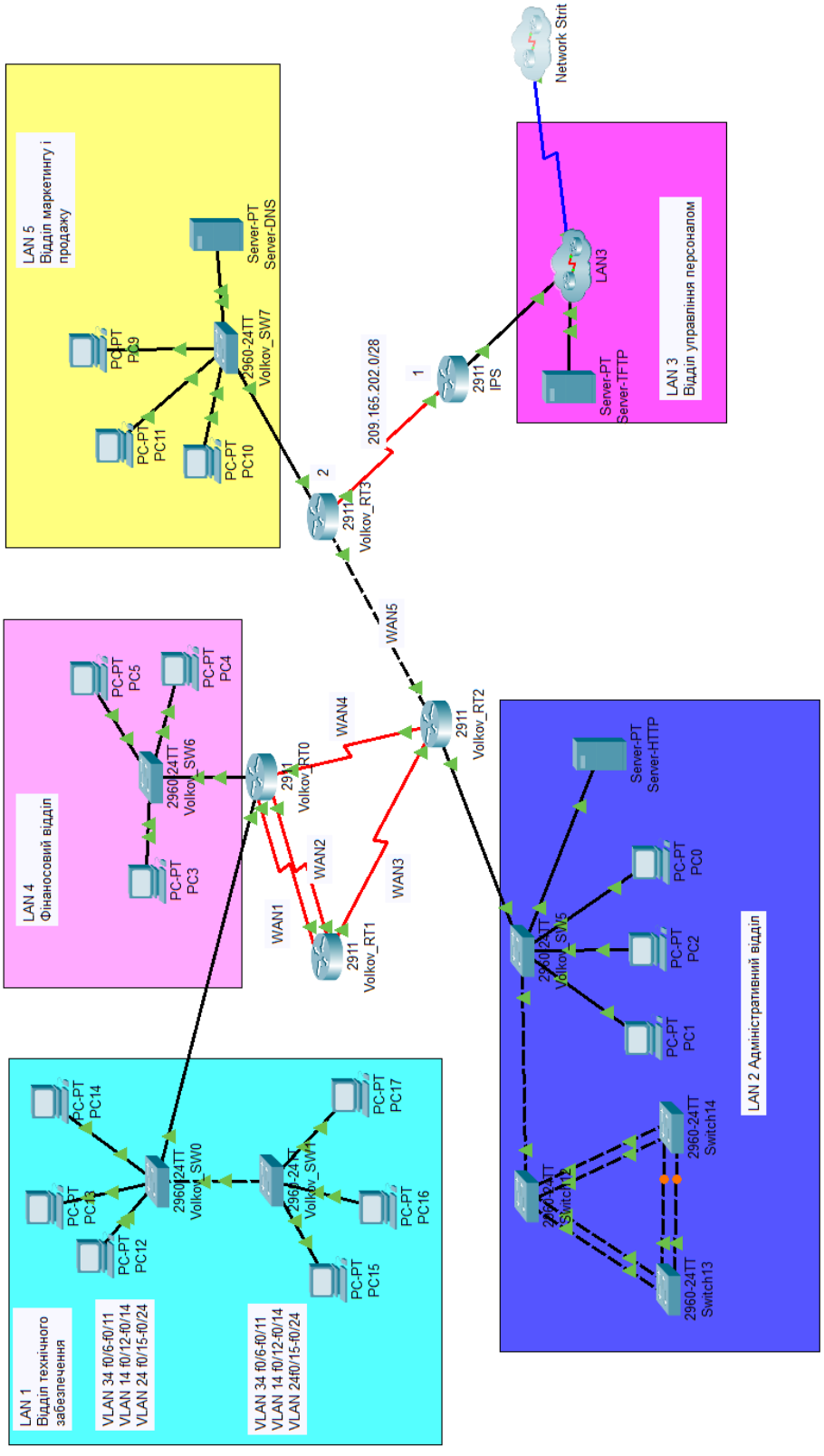

Рисунок 2.3 – Архітектура мережі підприємства «Планета кіно»

2.2.1 Вибір і обґрунтування структурної схеми комплексу технічних засобів комп’ютерної системи

Компанія «Планета кіно» має два офіси в місті Дніпро. Згідно поставлених технічних умов в корпоративній мережі цих кінотеатрів, буду знаходитись чотири маршрутизатори для зв’язку між відділами в середині компанії та один маршрутизатор для віддаленої підмережі. До маршрутизаторів будуть під’єднанні комутатори для підключення кінцевих пристроїв. Також в мережі використовується три сервери. Один із серверів це DNS, який використовується для збереження інформації про домени та її надання на запит користувачів.

Відділ «Технічного забезпечення» поділяється на три підвідділи. Для цієї мережі буде використана технологія VLAN, тому що це сприяє скороченню широкомовного трафіку між всіма користувачами мережі.

Кабельна система. Для з’єднання маршрутизаторів використовується технологія передачі даних Gigabit Ethernet та Serial, а для з’єднання комутаторів з кінцевими пристроями застосована технологія Fast Ethernet.

Відповідно до розробленої організаційної структури підприємства, наведена в пункті1.2 і згідно технічних вимог, наведених в пункті 2, формується структурна схема комплексу технічних засобів, рисунок 2.4. На ній зображені основні компоненти комп’ютерної системи підприємства з мережним обладнанням.

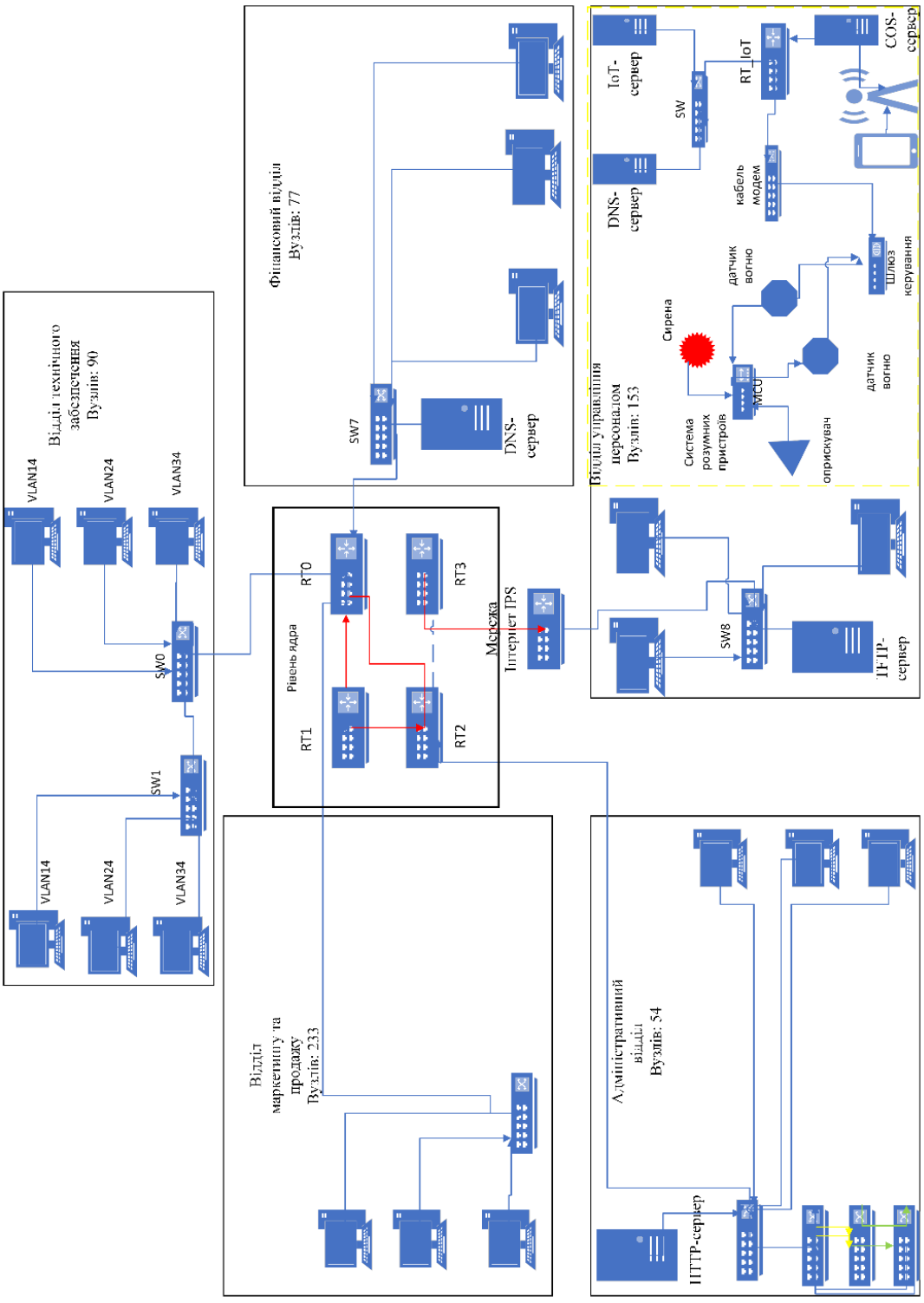

Рисунок 2.4 – Структурна схема комплексу технічних засобів комп'ютерної системи кінотеатрів «Планета кіно» м.Дніпро

2.2.2 Розробка специфікації апаратних засобів комп'ютерної системи

Для проектування комп'ютерної мережі в мережі кінотеатрів «Планета кіно» слід використовувати комутатори для зв'язку підмереж та маршрутизатори

для організації зв’язку між підмережами. Обрано мережеве обладнання компанії Cisco.

Для реалізації мережі, згідно технічних вимог наведених в пункті 2.1.3.4, в мережі буде використовується комутатор Cisco WS–C2960 24TC–L, так як він задовольняє всім умовам. Комутатори Cisco Catalyst 2960 серії є лінійкою комутаторів з фіксованою конфігурацією та портами Fast Ethernet та Gigabit Ethernet. Має підтримку Intelligent features (створення складних списків управління доступом, розширена безпека), комбіновані гігабітні аплінки (мідний 10/100/1000BASE–T Ethernet або SFP–модуль для переходу в інше середовище – Cisco 1000BASE–SX, 1000BASE–LX, 0 –FX, 100BASE–LX, CWDM SFP). Також, пристрої Catalyst 2960 підтримують QoS, покроковий Rate Limiting, ACL (на базі MAC або IP адрес, портів UDP/TCP) та multicast services, можливість регулювати швидкість передачі на кожному порту з кроком 64 кбіт, Link Aggregation для організації більш швидкісних з'єднань між комутаторами та серверами, можливість організації транкових з'єднань на кожному порту за допомогою тегів 802.1q, до 255 VLAN на комутатор, до 4000 VLAN ID.

Для реалізації мережі, згідно технічних вимог наведених в пункті 2.1.3.4, в мережі буде використовуватись маршрутизатор Cisco RV260W–E–K9–G5, тому що він задовольняє всім вимогам. Ці моделі мають двоядерний процесор. WAN–порт малого форм–фактора (SFP) забезпечує гнучке підключення. Як і інші моделі включають стандартні функції, такі як брандмауер Stateful Packet Inspection (SPI) корпоративного рівня, безпека VPN (IP Security [IPsec], протокол тунелювання «точка–точка» [PPTP].] і OpenVPN), фільтрації вмісту та майстрів пристроїв для спрощення налаштування.

Сервер ARTLINE Business має збалансовану продуктивність і невелике споживання енергії. Сервер побудований на базі материнської плати ASUS PRIME H370–PLUS. Особливості даного пристрою:

− комплекс захисних технологій 5x protection iii (захист від електричних навантажень, корозії, електростатичних розрядів), технологій підвищення

продуктивності (asus optimem) та управління ресурсами енергоспоживання (asus epu);

– фірмові оболонки та набори програмних утиліт: asus exclusive features, asus quiet thermal solution та інші;

– шина pci express із підтримкою двоканальної оперативної пам'яті;

– сучасні інтерфейси: швидкісні usb 3.1 gen 1 і usb 3.1 gen 2, роз'єм m.2 (nvme pcie) для підключення "реактивних" твердотільних накопичувачів з можливістю створення raid–масиву.

Специфікація обладнання наведена в таблиці 2.1.

Таблиця 2.1 – Специфікація обладнання

№	Найменування і технічна характеристика	Тип, марка, позначення документа, опитувального листа	Одиниці Виміру	Кількість	Примітка
1	2	3	4	5	6
1	Комутатор: Cisco WS–C2960–24TC–L Порти:24 Fast Ethernet/2 Gigabit Ethernet. Підтримка: QoS, Rate Limiting, ACL, multicast service, Link Aggregation	Switch0 Switch1 Switch2 Switch3 Switch4 Switch5 Switch6 Switch7 Switch8	Мбит/с	9 шт.	Для підключення пристроїв в мережі між собою.

Продовження таблиці 2.1

1	2	3	4	5	6
2	Маршрутизатор: Cisco RV260W–E–K9–G5 Стандарт WI–FI 802.11: n (до 300 Мбит/с), ac (до 867 Мбит/с). Порти LAN: Gigabit Ethernet (100/1000). Підтримка транспортних протоколів: PPPoE, PPTP, DHCP, PAT, DDNS, L2T. Функція мережевого екрану: NAT,	Volkov_RT0 Volkov_RT1 Volkov_RT2 Volkov_RT3 IPS	Мбит/с	5 шт.	Виконує функцію маршрутизацію всієї мережі
3	Сервер: Artline Business R13 (R13v08) Процесор: Intel Pentium. Кількість ядер:2. Частота: 3.7 ГГц. Оперативна пам'ять: DDR4. Об'єм встановленої пам'яті: 8 ГБ	Server DNS Server HTTP Server TFTP	Мбит/с	3 шт.	сервер для всієї мережі
4	Стаціонарний ПК: ASUS V222FAK–BA002M Процесор:Intel Core i5. ОЗУ: 8Гб Тип пам'яті: DDR4 SSD: 256Гб Частота: 1.6 ГГц			18 шт.	Робочі комп'ютери для персоналу

Продовження таблиці 2.1

5	Детектор вогню: AJAX FireProtect Бездротове з'єднання; діапазон темп: від 0 до 65 С0	AJAX FireProtect		2 шт.	Розумний пристрої
6	Aqara Door Sensor	Aqara Door Sensor		1 шт.	Розумний пристрої
7	Вентелятор	Silver Crest STV 45 D3 Black		1 шт.	Розумний пристрої
8	Датчиком температури Livolo	Livolo		1 шт.	Розумний пристрої
9	MCU AJAX WallSwitch	AJAX WallSwitch		1 шт.	Розумний пристрої
10	Розумна централь Ajax Hub	Ajax Hub		1 шт.	Розумний пристрої
11	Стійка мережева 42U, подвійна Розміри: 2025x550x960 мм	Стійка мережева 42U		2 шт.	

Технічні характеристики комутатора Cisco WS–C2960 24TC–L: порти: 24 x 10/100; 2 x 1000/SPF; підтримка PoE, 180W; пропускна здатність: 8,8 Гбіт/с; об'єм ОЗУ/flash пам'ять: 64/32 Мб; спосіб автентифікації: RADIUS; підтримка віддалених протоколів: HTTP, TFTP.

Технічні характеристики маршрутизатор Cisco RV260W–E–K9–G5: підтримка інтерфейсів Fastethernet, GigabitEthernet; порти 8 RJ–45, 1 SPF/RJ–45; робочий діапазон: 2,4 Гц, 5 Гц; протоколи: DHCP, DNS, NAT,PAT,PPTP; підтримка VPN: IPsec, Encryption, OpenVPN; захист інформації: SPI firewall, DoS

Згідно рисунку 1.5 «План офісного приміщення в ТРЦ «APPOLO» » та рисунку 2.1 «Топологічна схема розміщення структурних підрозділів компанії в ТРЦ «APPOLO» » розрахована необхідна кількість кабельної системи,

протяжність з’єднань склала 580 метрів. З’єднання між мережевим обладнанням сягає 95 метрів, для підключення пристроїв в відділі маркетингу та продажу 115 метрів, для підключення адміністративного відділу 125 метрів, для підключення відділу технічного забезпечення 135 метрів, для підключення фінансового відділу 110 метрів.

Таблиця 2.2 – Специфікація кабельної прокладки

№ п/п	Найменування і технічна характеристика	Тип, марка, позначення документа, опитувального листа	Одиниці Виміру	Кількість	Примітка
1	Розетка інформаційна RJ45	RJ45		607 шт	
2	Конектор RJ–45	RJ–45		610 шт	
3	Кабель мережевий 4x2x0.5 (FTP–cat 5)	FTP КПВЭ–ВП		915 м	
4	Силовий блок розеток 9 розеток; кабель 1.8м; 220В; 16А	Силовий блок eserver 19		136 шт.	
5	Розетка силова SCHUKO 16А; 250В; Кількість контактів 2P+E	Розетка силова SCHUKO		20 шт.	
6	Кабель живлення для ПК 220В; 1,8м; 0,75мм2	Кабель живлення		607	
7	Кабель канал Sokol Profesional 25x16 мм	Sokol Profesional		915 м	

2.2.3 Розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі підприємства

В підмережі «Відділ маркетингу і продажу» встановлений комутатор Cisco WS–C2960–24TC–L та маршрутизатора Cisco RV260W–E–K9–G5, що

об’єднуються ПК користувачів. Згідно технічним даним загальна кількість користувачів в даній підмережі дорівнює 233, найбільша підмережа з усієї мереі.

Вихідний трафіку пересилається на маршрутизатор Cisco RV260W–E–K9–G5 в лінію з пропускною здатністю 1000 Мбіт/с. Для того, щоб комутатор Cisco WS–C2960–24TC–L не був перенасиченим, швидкість надходження пакетів не повинна перевищувати швидкості їх відправлення. Якщо послугами одночасно користуються 100 % користувачів, то середня інтенсивність трафіку складає μ=133 кадрів/с, а середня довжина повідомлення 650 байт.

Відповідно отриманих даних, слід розрахувати пропускну здатність мережі.

Пропускна здатність мережі на рівні доступу, дорівнює:

$$Pp.p=\mu\times l\times N\times 8=133\times 650\times 233\times 6=690{,}2 \text{ (Мбіт/с)} \quad (2.1)$$

Комутатор пересилає трафік на маршрутизатор через вихідну лінію з пропускною здатністю 1000 Мбіт/с.

Загальне навантаження на комутатор не повинно перевищувати:

$$\mu_{вих}=\frac{100\,000\,000}{(650*8)}=192308 \text{ пакетів/с} \quad (2.2)$$

Кожне джерело виробляє в середньому 133 пакетів/с, то ми обмежені приєднанням до комутатора рівня доступу максимум:

$$N=\frac{192308}{133}=1446 \text{ джерел} \quad (2.3)$$

Кожен з 233 ПК посилає потік заявок з інтенсивністю 133 кадрів/с.

Інтенсивність вихідного трафіку від всіх користувачів:

$$\lambda=N\times\mu=233\times 133=30989 \text{ (пакетів/с)} \quad (2.4)$$

Коефіцієнт затримки на рівні розподілу, тобто показник завантаженості вихідного каналу зв’язку, який впливає на час стояння в черзі:

$$\rho=\frac{\lambda}{\mu_{вих}}=\frac{30989}{192308}=0.16 \quad (2.5)$$

Коефіцієнт зайнятості комутатора рівня розподілу:

$$r=\frac{\rho}{1-\rho}=\frac{0.16}{1-0.16}=0.19 \quad (2.6)$$

Середня затримка кадру, пов’язана з чергою M/M/1, дорівнює:

$$T=\frac{1}{\mu-\lambda}=\frac{1}{192308-30989}=6{,}2\times10^{-6}\text{с} \quad (2.7)$$

Середня довжина черги:

$$L_{чер}=\frac{\rho^2}{1-\rho}\frac{0.16^2}{1-0.16}=0{,}03 \quad (2.8)$$

Середній час перебування пакета в черзі:

$$T_{оч}=\frac{L_{чер}}{\lambda}=\frac{0{,}03}{30989}=10\text{мкс} \quad (2.9)$$

Отримане значення менше необхідного значення 6мс, що задовольняє вимогам.

Пропускна здатність каналу:

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

$$b=\lambda\times l=30989\times650\times8=161\ 142\ 800\ \text{біт/с}=161{,}1\ \text{Мбіт/с} \quad (2.10)$$

Отриманий результат, задовольняє пропускній здатності вихідного каналу в 1000 Мбіт/с

3 ПРОЕКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ ТА ПЕРЕВІРКА РОБОТИ КОМП'ЮТЕРНОЇ СИСТЕМИ ПІДПРИЄМСТВА

3.1 Розрахунок схеми адресації корпоративної мережі

Для побудови мережі підприємства «Планета кіно», згідно умов наведених в технічному завдані, використати адресний простір 172.22.64.0/20. Для послідовних каналів між маршрутизаторами використати адреси з діапазону 10.1.4.0/24 та одна мережа зовнішнього шлюзу з IP–адресою 209.165.202.0 .

Для розрахунку схеми IP–адресації, використано метод VLSM. Даний метод IP–адресації, дозволяє гнучко керувати простором IP-адрес, не використовуючи жорсткі рамки класової адресації. Використання цього методу дозволяє економно використовувати обмежений ресурс IP–адрес, оскільки можливе застосування різних масок підмереж до різних підмереж. Він ефективно використовує IP–адреси в порівняні з звичайним поділом на підмережі [2].

Дану мережу необхідно поділити на п'ять підмереж з наступною кількістю вузлів:

Таблиця 3.1 – Поділ підмереж на вузли

172.22.64.0/20				
LAN1	LAN2	LAN3	LAN4	LAN5
Відділ технічного забезпечення	Адміністративний відділ	Відділ управління персоналом	Фінансовий відділ	Відділ маркетингу і продажу
90	54	153	77	233

Далі необхідно визначити мінімальну кількість вузлів підмережі на яку можна поділити. Отже, для 90 вузлів – 128, для 54 вузлів – 64, для 153 вузлів – 256, для 77 вузлів – 128, для 233 вузлів 256. Тому підмережі LAN1 та LAN4 має префікс /25, підмережі LAN3 та LAN5 мають префікс /24, а підмережа LAN2 з префіксом /26.

Далі необхідно присвоїти IP–адреси кожній підмережі. Ми має дві підмережі з префіксом /24, тому адреси підмережі мають такий вигляд: LAN5 – 172.22.64.0/24, LAN3 – 172.22.65.0/24. Дві підмережі с префіксом /25 отримають такі IP–адреси: LAN1 – 172.22.66.0/25, LAN4 – 172.22.66.128/25. Підмережа LAN5 з префіксом /26 – 172.22.67.0/26.

Після визначення IP-адрес для кожної підмережі, далі необхідно визначити діапазон адрес (першу і останню адресу). Для цього необхідно, кожну адресу і маску підмережі представити у двійковій формі.

Розглянемо на прикладі підмережі LAN5:

172.22.64.0/24

IP–адреса:10101100.10110000.10000000.00000000

Маска: 11111111. 11111111. 11111111.00000000

Перша адреса: 00000001

Друга адреса: 11111110

Після двійкової форми переводимо в десяткову. Тоді підмережа LAN5 буде мати такий діапазон: перший 172.22.64.1/24 – другий 172.22.64.254/24, широкомовна адреса – 172.22.64.255.

В інших підмережах розбили таким же чином.

Отже, розрахунок методом VLSM дає можливість поділити адресний простір на невеликі підмережі, які максимально наближені до необхідної кількості вузлів в комп’ютерній мережі, згідно технічних вимог.

В таблиці 3.2 наведена схема IP–адресації мережі підприємства «Планета кіно».

Таблиця 3.2 – Схема адресації мережі

Назва мережі	Кількість вузлів	Адреса мережі	Маска мережі	Початкове значення діапазону	Кінцеве значення діапазону
LAN1	90	172.22.66.0	255.255.255.128/25	172.22.66.1	172.22.66.126
LAN2	54	172.22.67.0	255.255.255.192/26	172.22.67.1	172.22.67.62
LAN3	153	172.22.65.0	255.255.255.0/24	172.22.65.1	172.22.65.254
LAN4	77	172.22.66.128	255.255.255.128/25	172.22.66.129	172.22.66.254
LAN5	233	172.22.64.0	255.255.255.0/24	172.22.64.1	172.22.64.254
WAN1	2	10.0.4.0	255.255.255.252/30	10.0.4.1	10.0.4.2

Продовження таблиці 3.2

WAN2	2	10.0.4.4	255.255.255.252/30	10.0.4.5	10.0.4.6
WAN3	2	10.0.4.8	255.255.255.252/30	10.0.4.9	10.0.4.10
WAN4	2	10.0.4.12	255.255.255.252/30	10.0.4.13	10.0.4.14
WAN5	2	10.0.4.16	255.255.255.252/30	10.0.4.17	10.0.4.18

В таблиці 3.3 наведена адресація всіх пристроїв мережі підприємства «Планета кіно». Таблиця заповнена на основі таблиці 3.2 і відповідає логічній топології мережі.

Таблиця 3.2 – Схема адресації всіх пристроїв

Ім’я пристрою	Інтерфейс	IP–адреса	Маска	Шлюз	Vlan	Для ПК інтерфейс підключеного пристрою
Відділ технічного забезпечення						
Volkov_RT0	G0/0	–	–	–	–	Volkov_SW0
	G0/1	172.22.66.129	255.255.255.128	–	–	Volkov_SW6
	G0/0.14	172.22.66.1	255.255.255.224		14	
	G0/0.24	172.22.66.33	255.255.255.224		24	
	G0/0.34	172.22.66.65	255.255.255.224		34	
	G0/0.99	172.22.66.97	255.255.255.224		99	
	Se0/1/0	10.0.4.2	255.255.255.252	–	–	Volkov_RT1
	Se0/1/1	10.0.4.6	255.255.255.252	–	–	Volkov_RT1
	Se0/2/0	10.0.4.13	255.255.255.252	–	–	Volkov_RT2
Volkov_SW0	G0/1	–	255.255.255.128	172.22.66.1	–	Volkov_RT1
	F0/2	–	255.255.255.128	–	–	Volkov_SW1
	F0/6–11	–	255.255.255.128	172.22.66.1	Vlan34	PC12
	F0/15–24	–	255.255.255.128	172.22.66.1	Vlan24	PC14
	F0/12–14	–	255.255.255.128	172.22.66.1	Vlan14	PC13

Продовження таблиці 3.3

Ім’я пристрою	Інтерфейс	IP–адреса	Маска	Шлюз	Vlan	Для ПК інтерфейс підключеного пристрою
Volkov_SW1	F0/2	–	255.255.255.128	172.22.66.1	–	Volkov_SW0
	F0/6–11	–	255.255.255.128	172.22.66.1	Vlan34	PC15
	F0/15–24	–	255.255.255.128	172.22.66.1	Vlan24	PC17
	F0/12–14	–	255.255.255.128	172.22.66.1	Vlan14	PC16
PC12	F0	172.22.64.76	255.255.255.128	172.22.66.1	–	Volkov_SW0
PC13	F0	172.22.64.11	255.255.255.128	172.22.66.1	–	Volkov_SW0
PC14	F0	172.22.64.43	255.255.255.128	172.22.66.1	–	Volkov_SW0
PC15	F0	172.22.64.77	255.255.255.128	172.22.66.1	–	Volkov_SW1
PC16	F0	172.22.64.72	255.255.255.128	172.22.66.1	–	Volkov_SW1
PC17	F0	172.22.64.44	255.255.255.128	172.22.66.1	–	Volkov_SW1
Volkov_RT1	Se0/1/1	172.22.67.66	255.255.255.252	–	–	Volkov_RT0
	Se0/1/0	172.22.67.70	255.255.255.252	–	–	Volkov_RT0
	Se0/2/0	172.22.67.74	255.255.255.252	–	–	Volkov_RT2
Адміністративний відділ						
Volkov_RT2	G0/1	172.22.67.1	255.255.255.198	–	–	SW_5
	G0/0	172.22.67.81	255.255.255.252	–	–	Volkov_RT3
	Se0/1/0	172.22.67.74	255.255.255.252	–	–	Volkov_RT1
	Se0/2/0	172.22.67.78	255.255.255.252	–	–	Volkov_RT0
Volkov_SW5	G0/2	–	255.255.255.192	172.22.67.1	–	Volkov_RT2
	F0/4	–	255.255.255.192	172.22.67.1	–	SW_4
PC0	F0	172.22.67.3	255.255.255.192	172.22.67.1	–	Volkov_SW5

Продовження таблиці 3.3

Ім’я пристрою	Інтерфейс	IP–адреса	Маска	Шлюз	Vlan	Для ПК інтерфейс підключеного пристрою
PC1	F0	172.22.67.2	255.255.255.192	172.22.67.1	–	Volkov_SW5
PC2	F0	172.22.67.5	255.255.255.192	172.22.67.1	–	Volkov_SW5
HTTP	F0	172.22.67.16	255.255.255.192	172.22.67.1	–	Volkov_SW5
Відділ управління персоналом						
IPS	G0/0	172.22.65.0	255.255.255.0	–	–	Volkov_SW8
	Se0/1/0	209.165.202.1	255.255.255.240	–	–	Volkov_RT3
Volkov_SW8	G0/1	–	–	–	–	IPS
PC6–8	F0	172.22.65.2–172.22.65.4	255.255.255.224	172.22.65.1	–	Volkov_SW8
TFTP	F0	172.22.65.5	255.255.255.224	172.22.65.1	–	Volkov_SW8
Volkov_RT3	Se0/1/0	209.165.202.2	255.255.255.240	–	–	IPS
	G0/1	172.22.67.82	255.255.255.252	–	–	Volkov_RT2
	G0/0	172.22.64.1	255.255.255.0	–	–	Volkov_SW7
Відділ маркетингу і продажу						
Volkov_RT0	G0/0	172.22.66.129	255.255.255.128	–	–	Volkov_SW6
PC3–4	F0	172.22.66.130–172.22.66.132	255.255.255.128	172.22.66.129	–	Volkov_SW6
Фінансовий відділ						
Volkov_SW7	G0/1	–	–	–	–	Volkov_RT3
PC9–11	F0	172.22.64.2–172.22.64.4	255.255.255.0	172.22.64.1	–	Volkov_SW7
DNS	F0	172.22.64.16	255.255.255.0	172.22.64.1	–	Volkov_SW7

3.2 Налаштування та перевірка роботи комп’ютерної системи

3.2.1 Базове налаштування конфігурації пристроїв

Згідно технічних вимог було реалізовано базове налаштування мережних пристроїів комп’ютерної системи. До базових налаштувань пристроїв відносять наступні конфігурації:

- налаштування назви пристрою;
- встановлено пароль на привілейованого режиму;
- встановлено пароль для користувацького режиму EXEC;
- встановлено пароль для віддаленого доступу доTelnet/SSH;
- зашифровано всі відкриті паролі;
- налаштовано банер MOTD;
- створено користувача 123–19ск1_Volkov з паролем admincisco;
- для шифрування данних встановлено ключ RSA довжиною 1028 біт;
- налаштовано IP–адресацію пристроїв, згідно таблиці 3.2 .

Приклад налаштування наведенно на маршрутизаторі Volkov_RT0 .

```
Router(config)#no ip domain-lookup
```

Встановлення унікальної назви пристрою:

```
Router(config)#hostname Volkov_RT0
```

Зашифрування паролей, які зберігаються у відкритому вигляді:

```
Volkov_RT0(config)#service password-encryption
```

Встановлення паролю на вхід до привілейованого режиму:

```
Volkov_RT0(config)#enable secret class
```

Встановлення паролю на вхід до консольної лінії:

```
Volkov_RT0(config)#line console 0
Volkov_RT0(config-line)#password cisco
```

Налаштування запиту пароля:

```
Volkov_RT0(config-line)#login
Volkov_RT0(config-line)#exit
```

Налаштування банера MOTD:

```
Volkov_RT0(config)#banner motd $123-19ck1 Volkov access only with
password$
```

Створення користувача 123–19ck1_Volkov з паролем admincisco:

```
Volkov_RT0(config)#username 123-19ck1_Volkov password admincisco
```

Створення домену:

```
Volkov_RT0(config)#ip domain-name Volkov_RT0
```

Встановлення ключ шифрування RSA довжиною 1024 біт:

```
Volkov_RT0(config)#crypto key generate rsa
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

Налаштування лінії vty:

```
Volkov_RT0(config)#line vty 0 4
*Mar 1 0:2:50.849: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Встановлення логіна та пароля для входу лінії:

```
Volkov_RT0(config-line)#login local
```

Встановлення протоколу SSH для входу на лінію:

```
Volkov_RT0(config-line)#transport input ssh
Volkov_RT0(config-line)#exit
```

Зберігання даних

```
Volkov_RT0(config)#do write
```

3.2.2 Налаштування маршрутизаторів корпоративної мережі

Для реалізації мережі «Планета кіно» використано протокол динамічної маршрутизаціїї OSPF 1. 1 – ідентивікатор зони, в якій буде працювати інтерфейс маршрутизатора.

OSPF є протоколом маршрутизації з об'явленням стану про канал (link–state). Це означає, що він вимагає відправки об'явлення про стан каналу (link–state advertisement – LSA) в усі маршрутизатори, які знаходяться в межах однієї і тієї ж ієрархічної області. У об'яві LSA протоколу OSPF включається інформація про підключених інтерфейсах. У міру накопичення маршрутизатора OSPF

інформації про стан каналу, вони використовують алгоритм SPF для розрахунку найкоротшого шляху до кожного вузла [4].

Налаштування протоколу динамічної маршурутизації OSPF наведенно на прикладі маршрутизатора Volkov_RT0:

Ввімкнення протоколу OSPF 1 на маршрутизаторі:

```
Volkov_RT0(config)#router ospf 1
```

Об’явлення мереж, підключених до маршрутизатора:

```
Volkov_RT0(config-router)#network 172.22.66.0 0.0.0.127 area 0
Volkov_RT0(config-router)#network 172.22.66.128 0.0.0.127 area 0
Volkov_RT0(config-router)#network 10.0.4.0 0.0.0.3 area 0
Volkov_RT0(config-router)#network 10.0.4.4 0.0.0.3 area 0
Volkov_RT0(config-router)#network 10.0.4.12 0.0.0.3 area 0
Volkov_RT0(config-router)#network 172.22.66.32 0.0.0.31 area 0
Volkov_RT0(config-router)#network 172.22.66.64 0.0.0.31 area 0
Volkov_RT0(config-router)#network 172.22.66.96 0.0.0.31 area 0
```

Встановлення маршруту за замовчуванням:

```
Volkov_RT0(config)#ip route 0.0.0.0 0.0.0.0 209.165.202.1
```

На serial–інтерфейсах згідно технічних вимог задано пропускну спроможність 128 Кб/с та вартість метрики 7500.

```
Volkov_RT0(config)#int se0/1/0
Volkov_RT0(config-if)#bandwidth 128
Volkov_RT0(config-if)#ip ospf cost 7500
Volkov_RT0(config-if)#exi
Volkov_RT0(config)#int se0/1/1
Volkov_RT0(config-if)#bandwidth 128
Volkov_RT0(config-if)#ip ospf cost 7500
Volkov_RT0(config-if)#exi
Volkov_RT0(config)#int se0/2/0
Volkov_RT0(config-if)#bandwidth 128
Volkov_RT0(config-if)#ip ospf cost 7500
Volkov_RT0(config-if)#exi
```

Перевіривши таблиці маршрутизації на маршрутизаторах, наведено на рисуноках 3.1–3.4, бачимо, що символ «С» дає інформацію про підключені

інтерфейси в мережі, а символ «O» дає інформацію про всі віддалені мережі, які використовують протокол OSPF. «S*» ця строка дає відомості про статичний маршрут за замовчуванням.

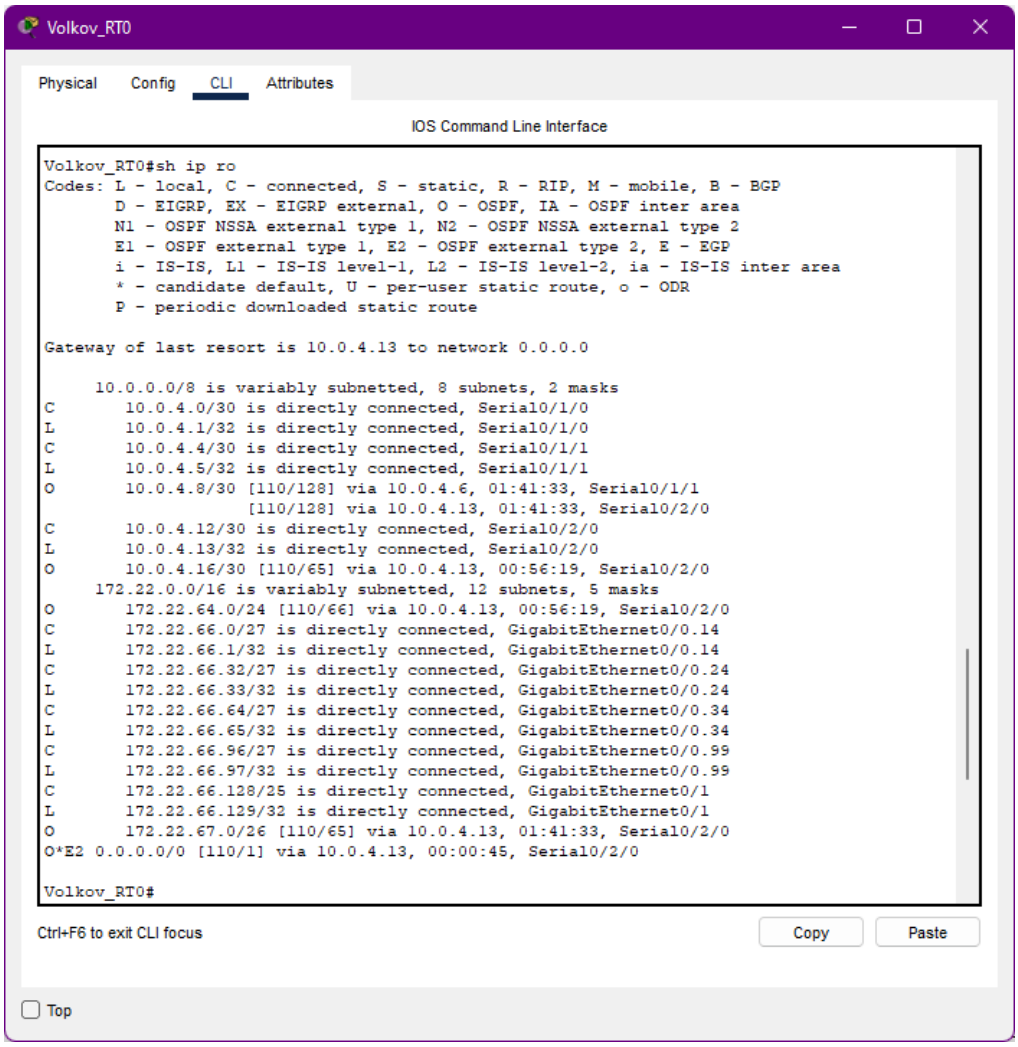

Рисунок 3.1 — Таблиця маршрутизації на Volkov_RT0

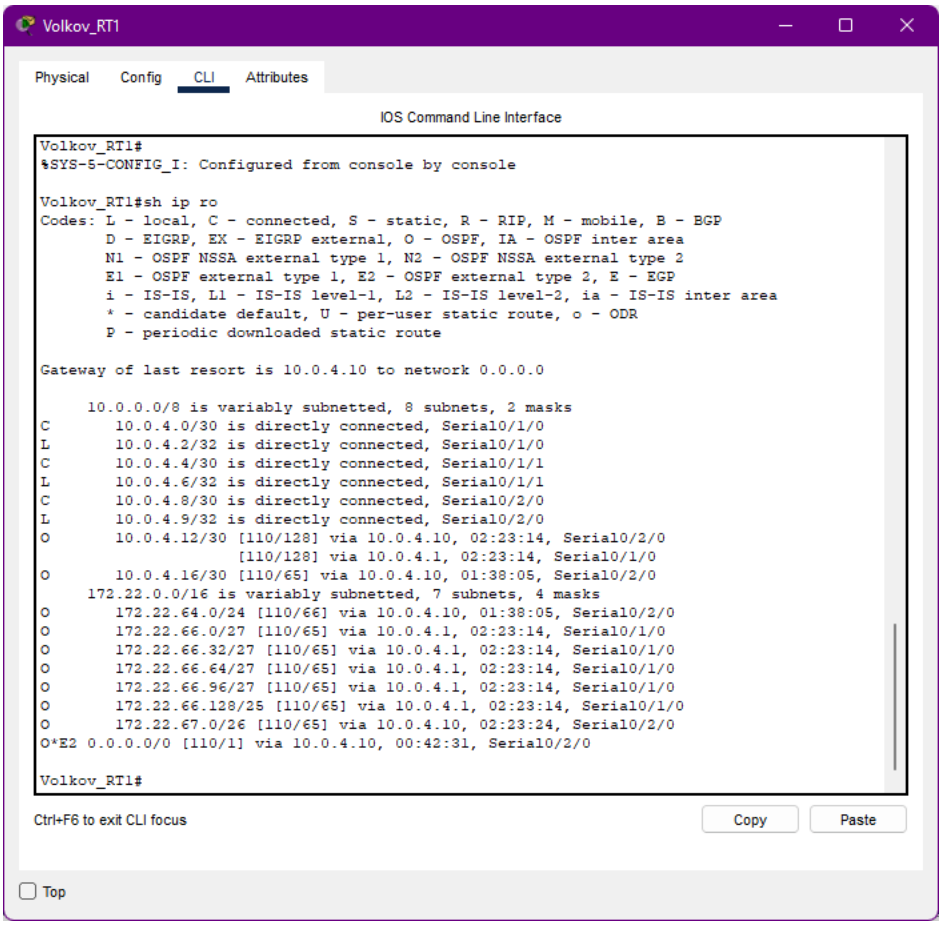

Рисунок 3.2 – Таблиця маршрутизації на Volkov_RT1

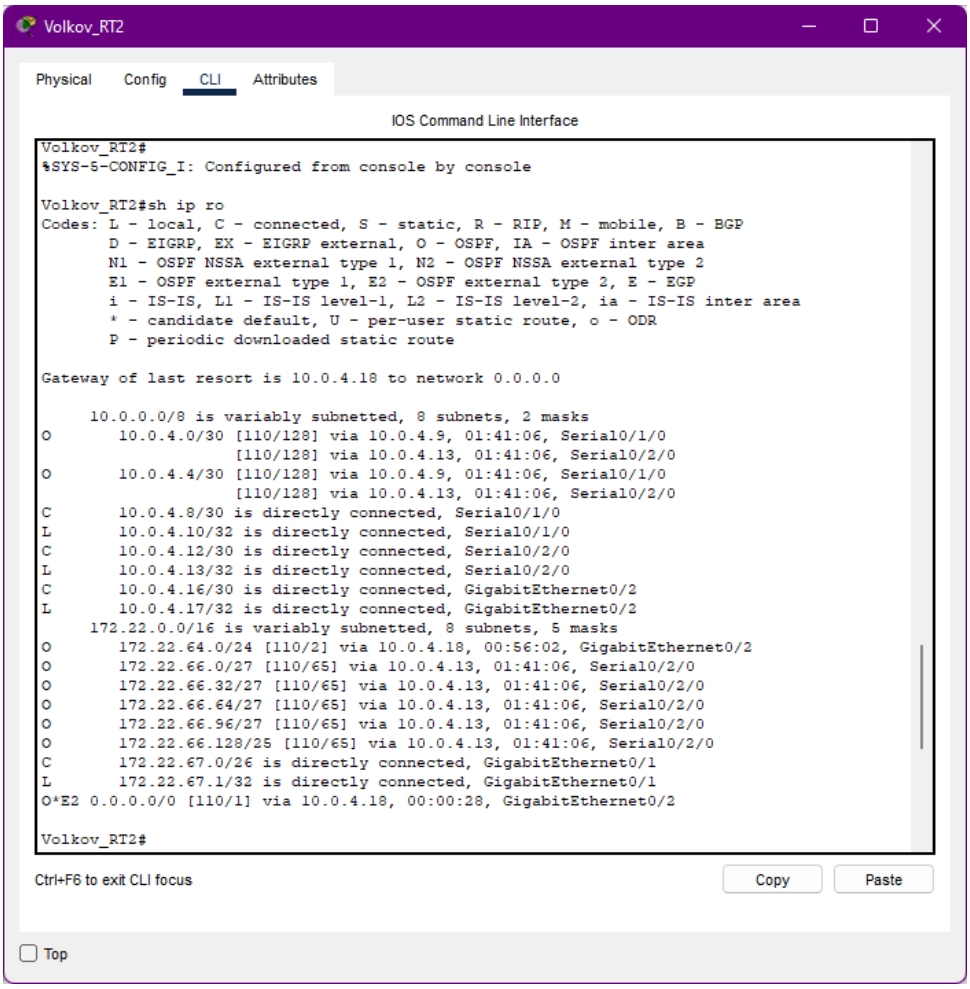

Рисунок 3.3 – Таблиця маршрутизації на Volkov_RT2

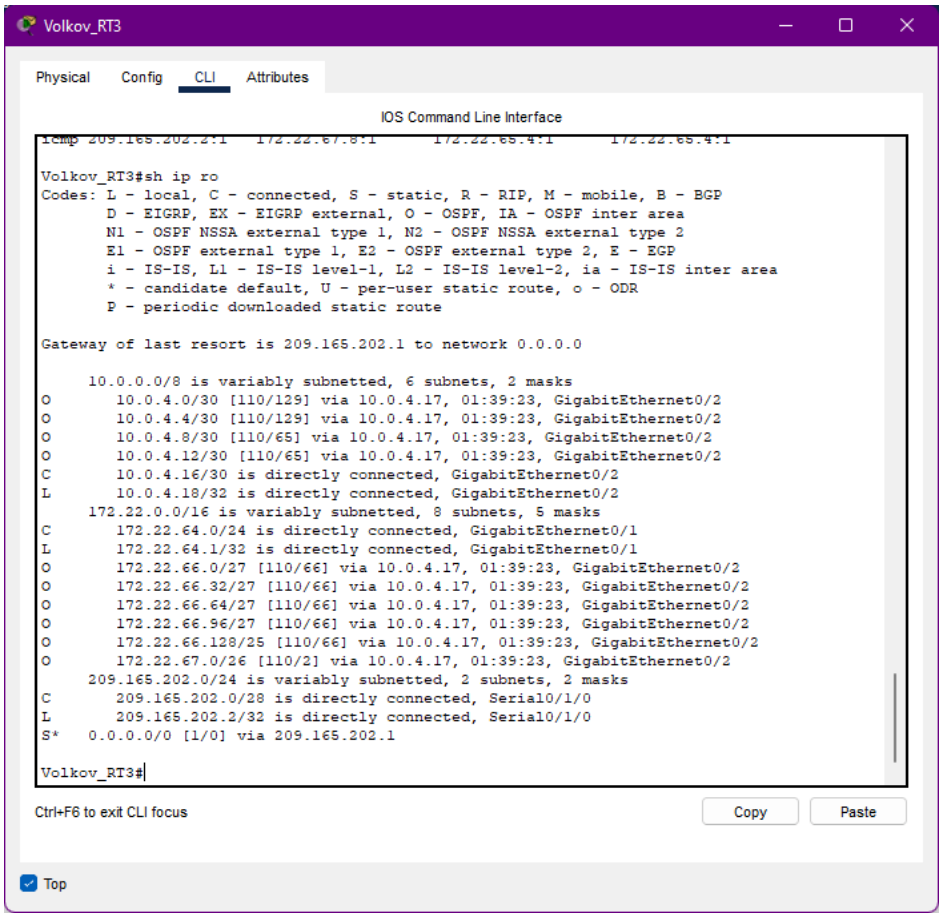

Рисунок 3.4 – Таблиця маршрутизації на Volkov_RT3

Отже, переглянувши таблиці маршрутизації, бачимо, що всі мережі вказані в таблицях сходяться, тому це означає, що відправивши повідомлення з однієї підмережі в іншу, воно буде прийняте.

3.2.3 Налаштування роботи Інтернет

Згідно поставленій задачі, для надання можливості доступу робочих станцій до мережі Інтернет, на прикордонному маршрутизаторі , слід здійснити налаштування технології NAT.

NAT призначений для спрощення і збереження IP–адрес. Він дозволяє приватним IP–мережам, які використовують незареєстровані IP–адреси, підключатися до Інтернету. NAT працює на маршрутизаторі, який зазвичай з'єднує дві мережі, і перетворює приватні адреси у внутрішній мережі в дійсні адреси перед відправкою пакетів в іншу мережу [6].

На прикордонному маршрутизаторі Volkov_RT3 здійснено налаштування NAT:

Розподіл вхідних/вихідних інтерфейсів

```
Volkov_RT3(config)#int s0/1/0
Volkov_RT3(config-if)#ip nat outside
Volkov_RT3(config-if)#exi
Volkov_RT3(config)#int g0/1
Volkov_RT3(config-if)#ip nat inside
Volkov_RT3(config-if)#exi
Volkov_RT3(config)#int g0/2
Volkov_RT3(config-if)#ip nat inside
Volkov_RT3(config-if)#exi
```

Створення access–list для вихідного трафіку в Інтернет

```
Volkov_RT3(config)#ip access-list standard Internet
Volkov_RT3(config-std-nacl)#permit 172.22.64.0 0.0.0.255
Volkov_RT3(config-std-nacl)#permit 172.22.67.0 0.0.0.127
Volkov_RT3(config-std-nacl)#permit 172.22.67.0 0.0.0.63
Volkov_RT3(config-std-nacl)#permit 172.22.66.128 0.0.0.127
Volkov_RT3(config-std-nacl)#permit 172.22.66.0 0.0.0.127
Volkov_RT3(config-std-nacl)#permit 172.22.65.0 0.0.0.255
Volkov_RT3(config-std-nacl)#exi
```

Ввімкнення NAT на інтерфейсі

```
Volkov_RT3(config)#ip nat inside source list Internet int s0/1/0
overload
```

Для перевірки налаштування протоколу NAT відобразимо таблицю перетворень на рисунку 3.5.

```
Volkov_RT3#sh ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.202.2:1024172.22.66.130:1    172.22.65.4:1      172.22.65.4:1024
icmp 209.165.202.2:1025172.22.64.3:1      172.22.65.4:1      172.22.65.4:1025
icmp 209.165.202.2:10  172.22.67.7:10     172.22.65.4:10     172.22.65.4:10
icmp 209.165.202.2:1   172.22.66.76:1     172.22.65.4:1      172.22.65.4:1
icmp 209.165.202.2:9   172.22.67.7:9      172.22.65.4:9      172.22.65.4:9
```

Рисунок 3.5 – Таблиця перетворень NAT на маршрутизаторі Volkov_RT3

3.2.4 Налаштування агрегування каналів PAgP

Протокол агрегації портів або PAgP – це технологія EtherChannel, яка є власним протоколом Cisco. Це форма логічного агрегування портів комутатора Cisco Ethernet, що забезпечує балансування навантаження даних/трафіку. PAgP EtherChannel може поєднувати до 8 фізичних каналів в один віртуальний канал. Ми також маємо відкритий стандарт IEEE, протокол управління агрегацією каналів, LACP [7].

Для збільшення пропускної здатності і надійності каналів в мережі LAN2 на комутаторах здійснено об’єднання фізичних портів, за допомогою технології EtherChannel. Дана технологія дозволяє об’єднати декілька фізичних портів на комутаторів в один логічний. Одна із переваг даного каналу є збільшення швидкості передачі даних.

В мережі LAN12 здійснимо на комутаторах налаштування PAgP каналів. Приклад налаштування наведено з комутатора Volkov_SW12:

Обираємо діапазон інтерфейсів

```
Volkov_SW12(config)#interface range fastEthernet 0/6-7
```

Вимикаємо інтерфейс

```
Volkov_SW12(config-if-range)#shutdown
```

Вказуємо активний режим

```
Volkov_SW12(config-if-range)#channel-group 1 mode active
Creating a port-channel interface Port-channel 1
```

Вмикаємо інтерфейс

```
Volkov_SW12(config-if-range)#no shutdown
```

Конфігуруємо логічну сутність, як транк

```
Volkov_SW12 (config-if-range)#int port-channel 1
Switch(config-if)#switchport  mode trunk
```

Перевірити налаштування протоколу PAgP, можна використавши команду `sh etherchannel summary`

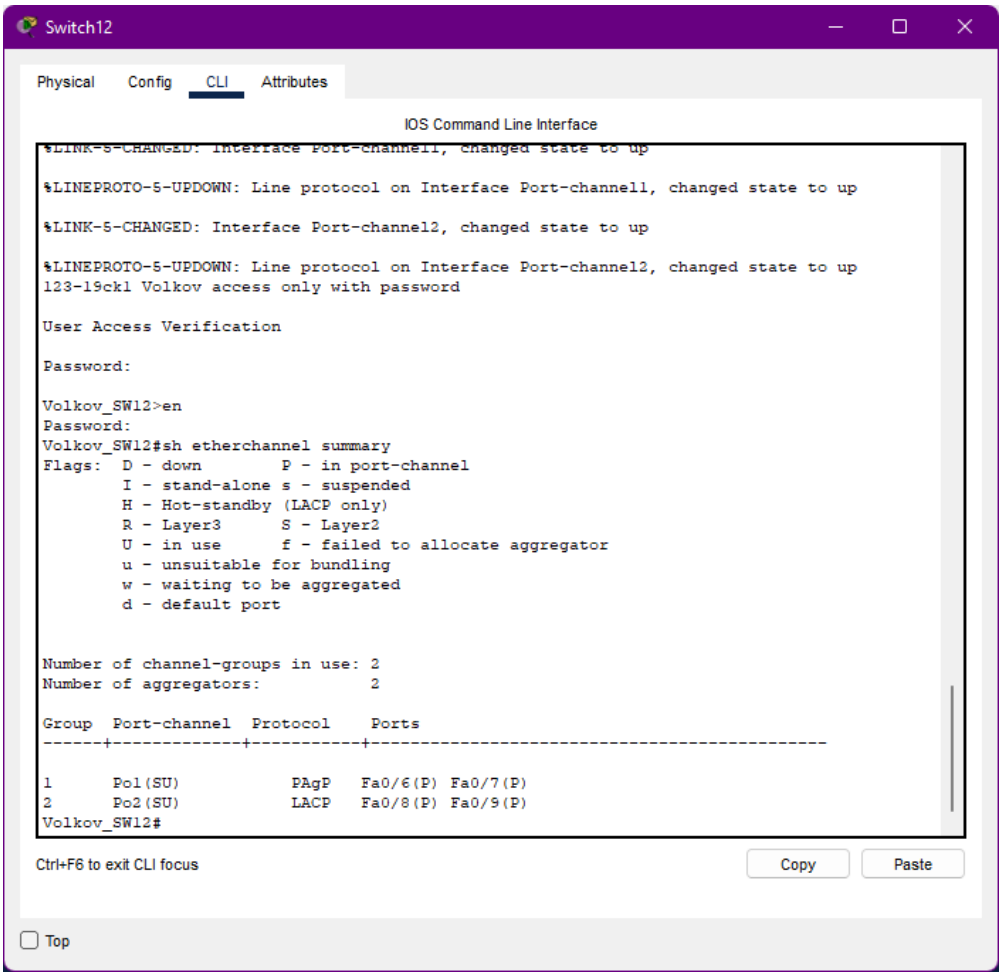

Рисунок 3.7 – Перевірка протоколу PAgP

Отже, отримавши результат роботи команди, бачимо, що налаштування виконано вірно.

3.2.5 Налаштування віртуальної приватної мережі site–to–site VPN з використанням IPsec

Налаштування приватної віртуальної мережі site–to–site VPN з використанням Ipsec, здійснюється для підмережі LAN4 та віддаленої мережі LAN3.

```
Volkov_RT3(config)#access-list 110 permit ip 172.22.64.0 0.0.0.255
172.22.65.0 0.0.0.255
Volkov_RT3(config)#crypto isakmp policy 10
```

Встановлення алгоритму шифрування

```
Volkov_RT3(config-isakmp)#encryption aes
```

Встановлення типу аутентифікації

```
Volkov_RT3(config-isakmp)#authentication pre-share
Volkov_RT3(config-isakmp)#group 2
Volkov_RT3(config-isakmp)#exi
```

Налаштування ключа для зв’язку з сусіднім маршрутизатором

```
Volkov_RT3(config)#crypto isakmp key cisco address 209.165.202.1
```

Налаштування параметрів для тунелю Ipsec

```
Volkov_RT3(config)#crypto ipsec transform-set VPN-SET esp-3des esp-
sha-hmac
```

Створення крипто–карти

```
Volkov_RT3(config)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
Volkov_RT3(config-crypto-map)#description VPN connection to IPS
```

Вказуємо зовнішню IP адресу маршрутизатора

```
Volkov_RT3(config-crypto-map)#set peer 209.165.202.1
```

Параметри Ipsec тунелю

```
Volkov_RT3(config-crypto-map)#set transform-set VPN-SET
```

Шифрування трафіку

```
Volkov_RT3(config-crypto-map)#match address 110
Volkov_RT3(config-crypto-map)#exi
```

Прив’язка крипто–карти до зовнішнього інтерфейсу

```
Volkov_RT3(config)#int s0/1/0
Volkov_RT3(config-if)#crypto map VPN-MAP
```

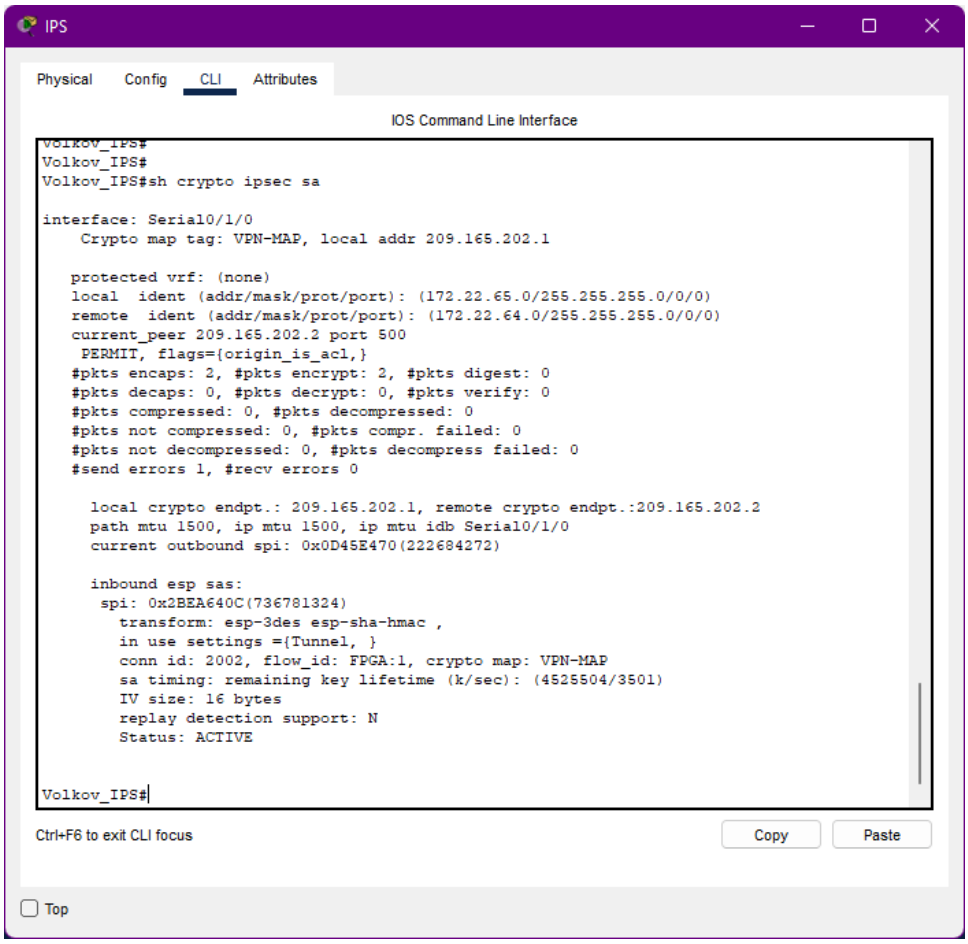

Рисунок 3.8 – Перевірка Ipsec SA на маршрутизаторі IPS

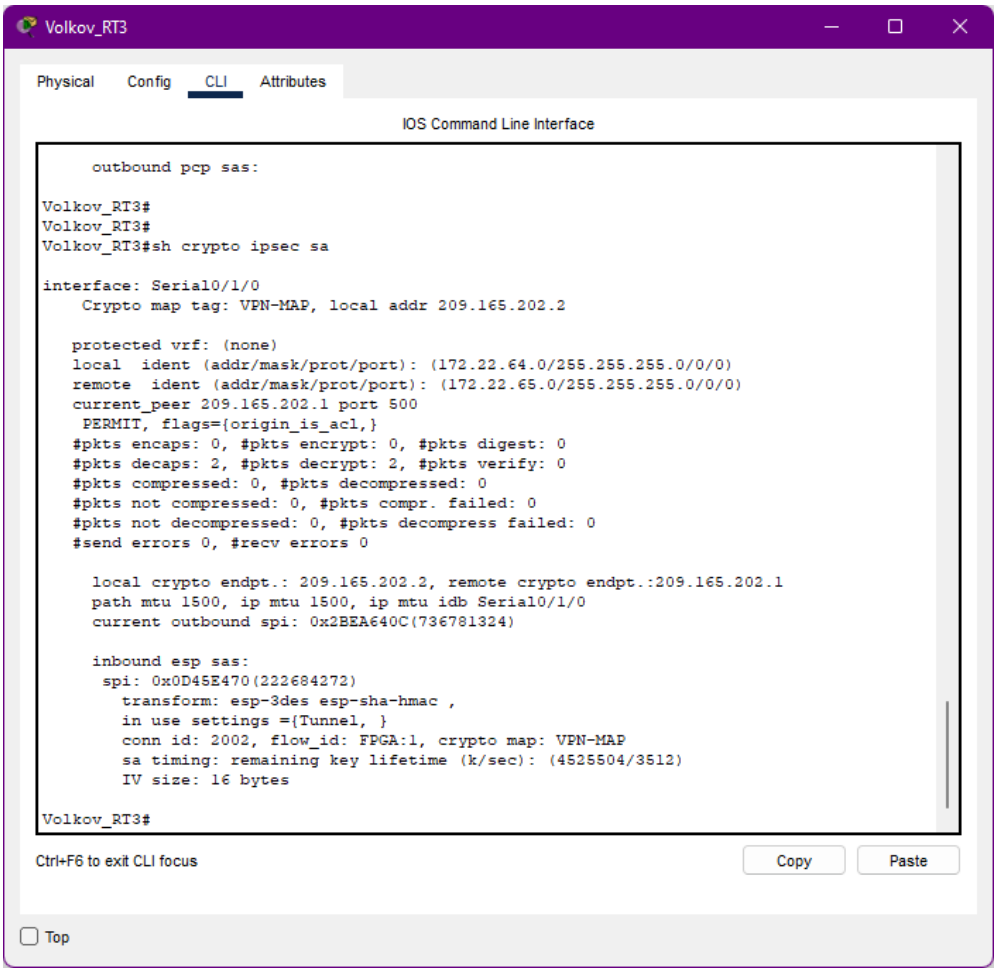

Рисунок 3.9 – Перевірка Ipsec SA на маршрутизаторі Volkov_RT3

3.2.6 Перевірка роботи комп'ютерної системи

Для перевірки працездатності комп'ютерної системи, здійснемо перевірку доступності вузлів мережі, перевіримо налаштування безпечного віддаленого доступу.

Для того, щоб виконати перевірки SSH необхідно виконати підключення з командного рядка PC17 з підмережі «Відділ технічного забезпечення» на маршрутизаторі Volkov_RT0 від користувача 123–19ck1_Volkov з паролем admincisco, результат наведено на рисунку 3.10.

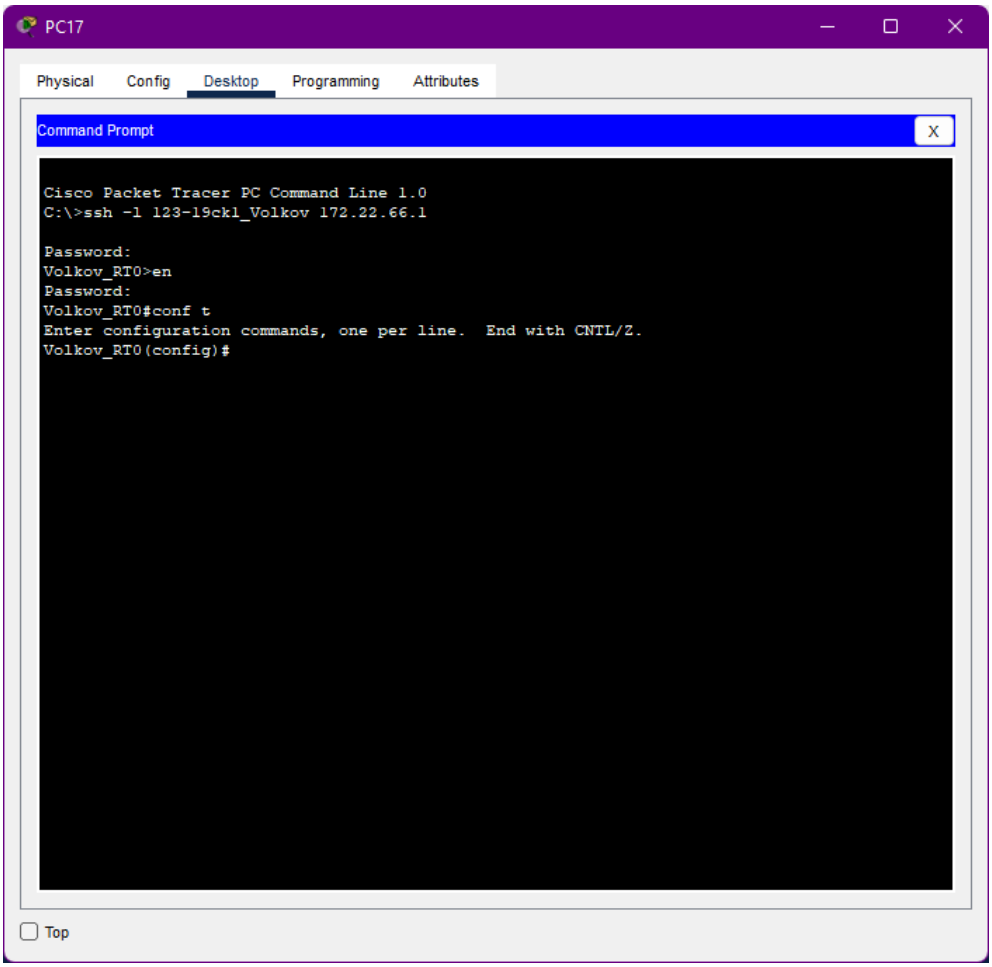

Рисунок 3.10 – Перевірка підключення до маршрутизатора за допомогою SSH

Для перевірки зв’язку між різними підрозділами, виконає команду ping з різним підмереж. Виконаємо команду ping з підмережі «Адміністративний відділ» в підмережу «Фінансовий відділ», результат наведено на рисунку 3.11.

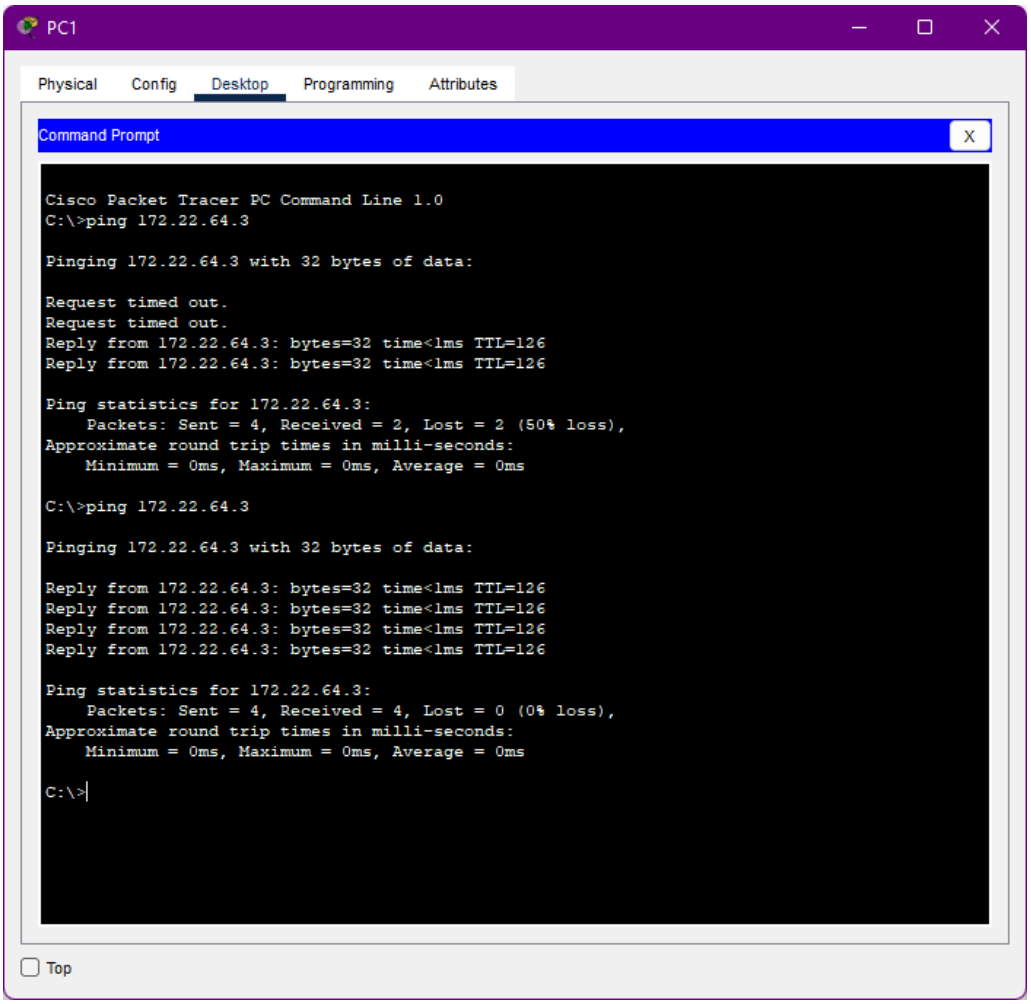

Рисунок 3.11 – Перевірка зв’язк між вузлами різним підмереж

В підмережі «Адміністративний відділ», здійсненно HTTP–сервера. Для перевірки налаштувань, з підмережі «Відділ маркетингу та продажу» у вікні браузера ввели доменне ім’я 123.dnipro.ua. Результат можна побачити на рисунку 3.12.

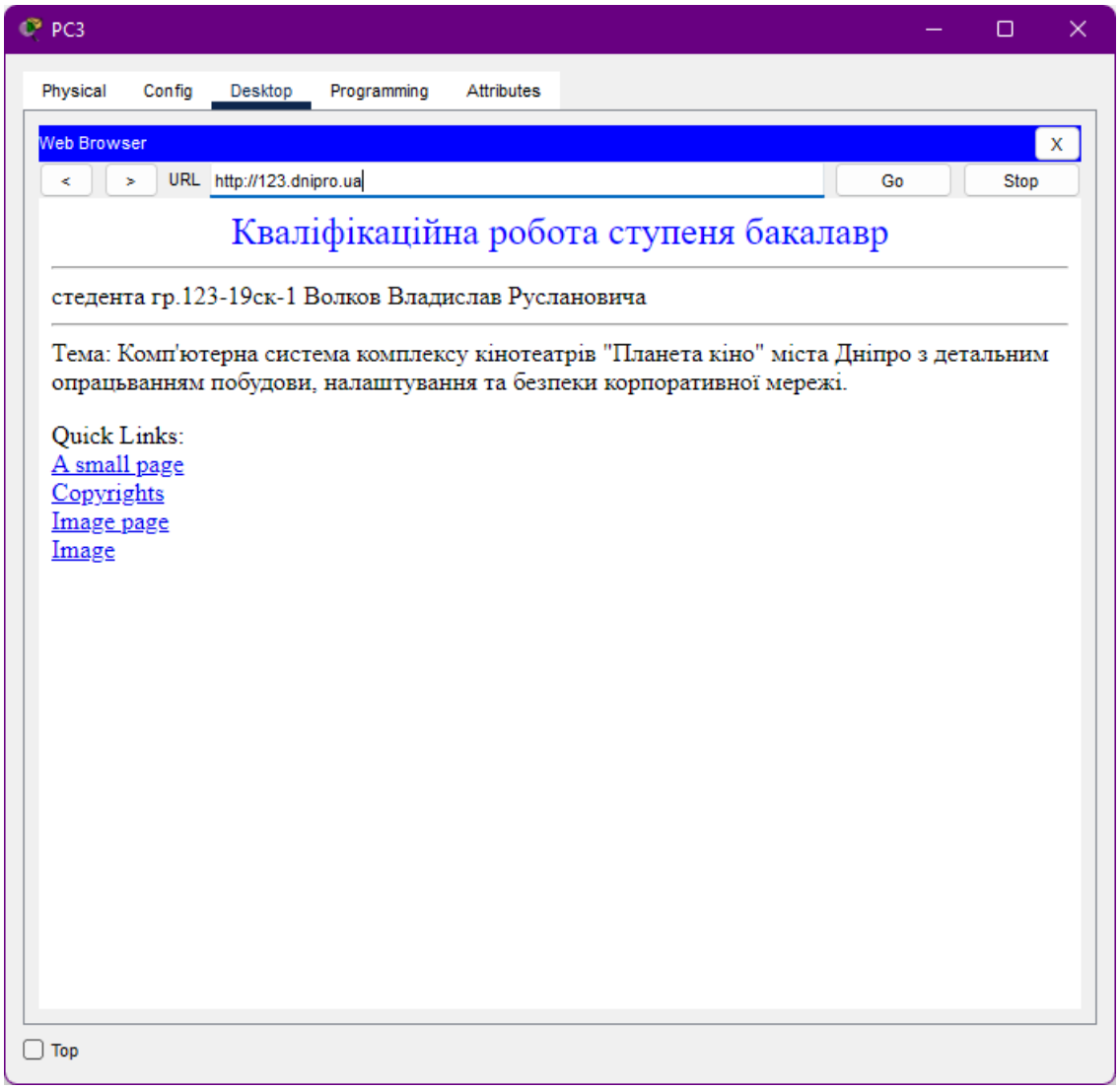

Рисунок 3.12 – Реалізація налаштування HTTP сервера

3.3 Захист інформації в КС від несанкціонованого доступу

3.3.1. Розробка методів для захисту інформації в комп'ютерній системі

Для захисту інформації в комп'ютерній системі від несанксіонованого доступу, слід розробити наступні методи:

– налаштувати мережу vlan та маршрутизацію між ним;

– налаштувати функцію безпеки портів , на портах комутаторів підключених до серверів та налаштвання адресації комп'ютерів в мережах vlan;

– налаштувати всі маршрутизатори на підтримку служби ааа та radius–сервер.

3.3.2 Налаштування мереж VLAN

Віртуальна локальна мережа (VLAN) – це логічна локальна мережа, яка розширює межі однієї традиційної локальної мережі до групи сегментів локальної мережі, з огляду на конкретні конфігурації [8]. VLAN є логічним об'єктом, тому його створення і конфігурація повністю виконуються в програмному забезпеченні. VLAN дозволяє декількох мереж працювати практично як одна локальна мережа. Одним з найбільш корисних елементів VLAN є те, що він усуває затримку в мережі, що економить мережеві ресурси і підвищує ефективність мережі. Крім того, VLAN створені для забезпечення сегментації і підтримки в таких питаннях, як безпека, управління мережею і масштабованість.

Для налаштування мереж VLAN і маршрутизації між ними необхідно:

– створити списки мереж VLAN і присвоїти кожній з ним ім'я, згідно таблиці 3.4;

– налаштувати транкові порти та порти доступу;

– налаштувати SVI–інтерфейси на комутаторах;

– налаштувати маршрутизацію між мережами VLAN.

Підмережу «Відділ технічного заббезпечення» сегменутємо на окремі віртуальні мережі, згідно таблиці 3.4.

Таблиця 3.4 — Список мереж VLAN

Номер VLAN	Ім’я VLAN	Примітка	Інтерфейс підключення
14	Accounting	Для бухгалтерії	Fa0/12–14
24	Resources Department	Для відділу кадрів	Fa0/15–24
34	Guest	Для гостей	Fa0/6–11
99	Management	Для управління пристроями	Fa0/1–5
100	Native	Власна мережа	G0/1

В таблиці 3.5 наведено схема адресації віртуальних логічних мереж.

Таблиця 3.5 – Таблиця адресації віртуальних логічних мереж

Назва підмережі	Розмір	VLAN	IP адреса	Маска	Діапазон адресів	Широкомовна адреса
Accounting	30	14	172.22.66.0	255.255.255.224	172.22.66.1 – 172.22.66.30	172.22.66.31
Resources Department	30	24	172.22.66.32	255.255.255.224	172.22.66.33 – 172.22.66.62	172.22.66.63
Guest	10	34	172.22.66.64	255.255.255.240	172.22.66.65 – 172.22.66.94	172.22.66.95
Management	10	99	172.22.66.96	255.255.255.240	172.22.66.97 – 172.22.66.126	172.22.66.127
Native	10	100	172.22.66.80	255.255.255.240	172.22.66.81 – 172.22.66.94	172.22.66.95

Налаштування технології VLAN на прикладі комутатора Volkov_SW0.

Оголошення VLAN

```
Volkov_SW0(config)#vlan 14
Volkov_SW0(config-vlan)#name Accounting
Volkov_SW0(config-vlan)#vlan 24
Volkov_SW0(config-vlan)#name Resources_Department
Volkov_SW0(config-vlan)#vlan 34
Volkov_SW0(config-vlan)#
Volkov_SW0(config-vlan)#name Guest
Volkov_SW0(config-vlan)#vlan 99
Volkov_SW0(config-vlan)#name Management
```

```
Volkov_SW0(config-vlan)#vlan 100
Volkov_SW0(config-vlan)#name Native
Volkov_SW0(config-vlan)#exit
```

Налаштування портів доступу

```
Volkov_SW0(config)#int range fastEthernet 0/12-14
Volkov_SW0(config-if-range)#switchport access vlan 14
Volkov_SW0(config-if-range)#exit
Volkov_SW0(config)#int range fastEthernet 0/15-24
Volkov_SW0(config-if-range)#switchport access vlan 24
Volkov_SW0(config-if-range)#exit
Volkov_SW0(config)#int range fastEthernet 0/6-11
Volkov_SW0(config-if-range)#switchport access vlan 34
Volkov_SW0(config-if-range)#exit
Volkov_SW0(config)#int range fa0/1-5
Volkov_SW0(config-if-range)#switchport access vlan 99
Volkov_SW0(config-if-range)#exit
```

Налаштування транкового каналу

```
Volkov_SW0(config)#int range gi0/1-2
Volkov_SW0(config-if)# switchport trunk native vlan 100
Volkov_SW0(config-if)#switchport trunk allowed vlan 14,24,34,99,100
Volkov_SW0(config-if-range)#switchport mode trunk
```

Налаштування SVI–інтерфейсу

```
Volkov_SW1(config)#int Vlan99
Volkov_SW1(config-if)#ip address 172.22.66.81 255.255.255.240
Volkov_SW1(config-if)#no sh
Volkov_SW1(config-if)#ip default-gateway 172.22.66.80
255.255.255.240
```

Після налаштування комутаторів та відповідних їм портів в підмережі «Відділ технічного забезпечення» відобразимо сумарну інформацію про налаштування VLAN. Результат наведено на рисунку 3.13–3.14.

```
Device Name: Switch0
Custom Device Model: 2960 IOS15
Hostname: Volkov_SW0

Port                Link   VLAN   IP Address         MAC Address
FastEthernet0/1     Down   99     --                 0001.6314.7689
FastEthernet0/2     Down   99     --                 0001.63CE.1D6E
FastEthernet0/3     Down   99     --                 0004.9A48.E085
FastEthernet0/4     Down   99     --                 0001.4265.5A76
FastEthernet0/5     Down   99     --                 00D0.977A.1E33
FastEthernet0/6     Up     34     --                 0060.5CD9.4994
FastEthernet0/7     Down   34     --                 0001.C975.8835
FastEthernet0/8     Down   34     --                 00E0.A36A.B683
FastEthernet0/9     Down   34     --                 0060.70A2.7735
FastEthernet0/10    Down   34     --                 00E0.8F1C.A74D
FastEthernet0/11    Down   34     --                 00E0.F936.7126
FastEthernet0/12    Up     14     --                 0003.E443.9BE9
FastEthernet0/13    Down   14     --                 000D.BD22.2390
FastEthernet0/14    Down   14     --                 000D.BD0B.DB65
FastEthernet0/15    Up     24     --                 0005.5E58.7A76
FastEthernet0/16    Down   24     --                 0000.0C2B.147A
FastEthernet0/17    Down   24     --                 0002.4A49.1196
FastEthernet0/18    Down   24     --                 00D0.FF7D.6310
FastEthernet0/19    Down   24     --                 0030.A33E.7A56
FastEthernet0/20    Down   24     --                 0002.4A6D.308E
FastEthernet0/21    Down   24     --                 0001.96EE.D671
FastEthernet0/22    Down   24     --                 0009.7C97.DBD8
FastEthernet0/23    Down   24     --                 0001.6466.3B11
FastEthernet0/24    Down   24     --                 0001.C981.49C8
GigabitEthernet0/1  Up     --     --                 0090.21CA.5521
GigabitEthernet0/2  Up     --     --                 0001.6409.EE3A
Vlan1               Down   1      <not set>          0007.EC11.C96B
Vlan99              Up     99     172.22.66.81/28    0007.EC11.C901

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Switch0(1)
```

Рисунок 3.13 – Налаштування VLAN на комутаторі Volkov_SW0

```
Device Name: Switch1
Custom Device Model: 2960 IOS15
Hostname: Volkov_SW1

Port                Link   VLAN   IP Address         MAC Address
FastEthernet0/1     Down   99     --                 000C.8583.9D17
FastEthernet0/2     Down   99     --                 0001.974C.680A
FastEthernet0/3     Down   99     --                 0005.5ECC.B3AE
FastEthernet0/4     Down   99     --                 00D0.D397.86B3
FastEthernet0/5     Down   99     --                 0030.F224.D2A9
FastEthernet0/6     Up     34     --                 00D0.BA25.AC7A
FastEthernet0/7     Down   34     --                 000C.8569.8A67
FastEthernet0/8     Down   34     --                 0002.170D.AAD5
FastEthernet0/9     Down   34     --                 0001.C939.0335
FastEthernet0/10    Down   34     --                 0003.E471.BD9D
FastEthernet0/11    Down   34     --                 0002.1685.A52A
FastEthernet0/12    Up     14     --                 0090.0C44.B464
FastEthernet0/13    Down   14     --                 000D.BDE4.01E9
FastEthernet0/14    Down   14     --                 0009.7C58.654A
FastEthernet0/15    Up     24     --                 0001.438E.D154
FastEthernet0/16    Down   24     --                 00E0.8FE8.DDDD
FastEthernet0/17    Down   24     --                 0002.1637.16DE
FastEthernet0/18    Down   24     --                 0002.4A08.60E5
FastEthernet0/19    Down   24     --                 0060.3E99.71B3
FastEthernet0/20    Down   24     --                 00D0.D333.64B6
FastEthernet0/21    Down   24     --                 00E0.8F2C.0987
FastEthernet0/22    Down   24     --                 0090.2B47.3B74
FastEthernet0/23    Down   24     --                 00E0.8F2C.2099
FastEthernet0/24    Down   24     --                 0060.2FD9.BB99
GigabitEthernet0/1  Down   --     --                 000D.BD49.60C7
GigabitEthernet0/2  Up     --     --                 0003.E460.27D5
Vlan1               Down   1      <not set>          00D0.9710.BDCD
Vlan99              Up     99     172.22.66.82/28    00D0.9710.BD01

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Switch1
```

Рисунок 3.14 – Налаштування VLAN на комутаторі Volkov_SW1

3.3.3 Налаштування параметрів безпеки комутаторів та адресації ПК в мережах VLAN

В усіх мережах, налаштовано технологію DHCP, для коректної роботи кінцевих пристроїв користувачів. Також DHCP протокол, дає можливість

автоматичного отримування IP-адрес та інших параметрів, які необхідні для роботи в мережі.

Відповідно технічним вимогам, налаштовано маршрутизатор Volkov_RT0, який здійснює маршрутизацію між VLAN та виступає в якості DHCP–сервера для логічних мереж VLAN14, VLAN24, VLAN34. Створені пули під назвами poolvlan14, poolvlan24, poolvan 34. З пулу виключити перші 10 адрес, та встановити для кожного пулу DNS–сервера та шлюз за замовчуванням.

Налаштування DHCP на VLAN виконано на маршрутизаторі Volkov_RT0.

Виключення перших 10 адрес в підмережах

```
Volkov_RT0(config)#ip dhcp excluded-address 172.22.66.1
172.22.66.10
Volkov_RT0(config)#ip dhcp excluded-address 172.22.66.33
172.22.66.42
Volkov_RT0(config)#ip dhcp excluded-address 172.22.66.65
172.22.66.75
```

Налаштування DHCP для підмереж у VLAN

```
Volkov_RT0(config)#ip dhcp pool poolvlan14
Volkov_RT0(dhcp-config)#network 172.22.66.1 255.255.255.224
Volkov_RT0(dhcp-config)#default-router 172.22.66.1
Volkov_RT0(dhcp-config)#exit
Volkov_RT0(config)#ip dhcp pool poolvlan24
Volkov_RT0(dhcp-config)#network 172.22.66.33 255.255.255.224
Volkov_RT0(dhcp-config)#default-router 172.22.66.33
Volkov_RT0(dhcp-config)#exit
Volkov_RT0(config)#ip dhcp pool poolvlan34
Volkov_RT0(dhcp-config)#network 172.22.66.65 255.255.255.224
Volkov_RT0(dhcp-config)#default-router 172.22.66.65
Volkov_RT0(dhcp-config)#exit
```

Налаштування технології інкапсуляції

```
Volkov_RT0(config)#interface GigabitEthernet0/1
Volkov_RT0(config-if)#no shutdown
Volkov_RT0(config-if)#interface GigabitEthernet0/1.14
Volkov_RT0(config-subif)#encapsulation dot1Q 14
```

```
Volkov_RT0(config-subif)#ip address 172.22.66.1 255.255.255.224
Volkov_RT0(config-subif)#exit
Volkov_RT0(config)#interface GigabitEthernet0/1.24
Volkov_RT0(config-subif)#encapsulation dot1Q 24
Volkov_RT0(config-subif)#ip address 172.22.66.33 255.255.255.224
Volkov_RT0(config-subif)#exit
Volkov_RT0(config)#interface GigabitEthernet0/1.34
Volkov_RT0(config-subif)#encapsulation dot1Q 34
Volkov_RT0(config-subif)#ip address 172.22.66.65 255.255.255.224
Volkov_RT0(config-subif)#exit
Volkov_RT0(config)#interface GigabitEthernet0/1.99
Volkov_RT0(config-subif)#encapsulation dot1Q 99
Volkov_RT0(config-subif)#ip address 172.22.66.97 255.255.255.224
Volkov_RT0(config-subif)#exit
```

Перевірка призначення IP-адрес призначених за допомогою протоколу DHCP, які знаходяться у VLAN, наведено на рисунку 3.15.

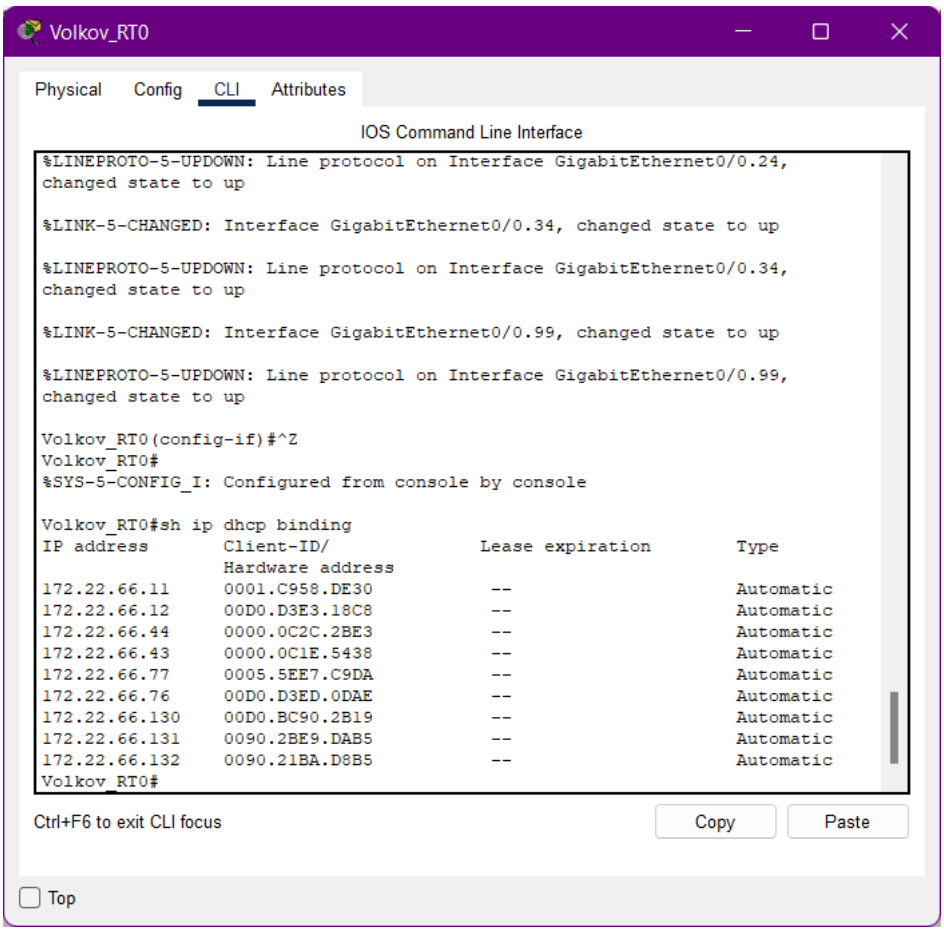

Рисунок 3.15 – Таблиця призначень IP-адрес вузлам за протоколом DHCP

Перевірка зв’язку між вузлами з різних VLAN при автоматичному призначенні IP-адрес через DHCP, наведена на рисунках 3.16 – 3.19.

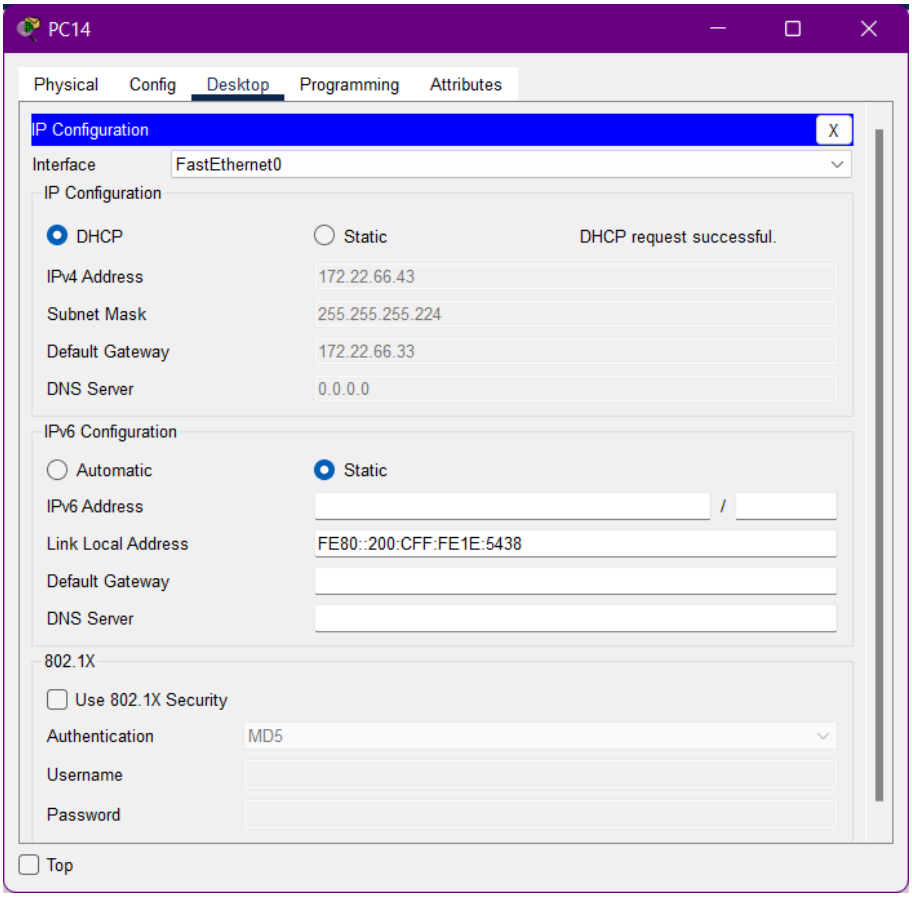

Рисунок 3.17 – Перевірка автоматичного призначення IP-адрес

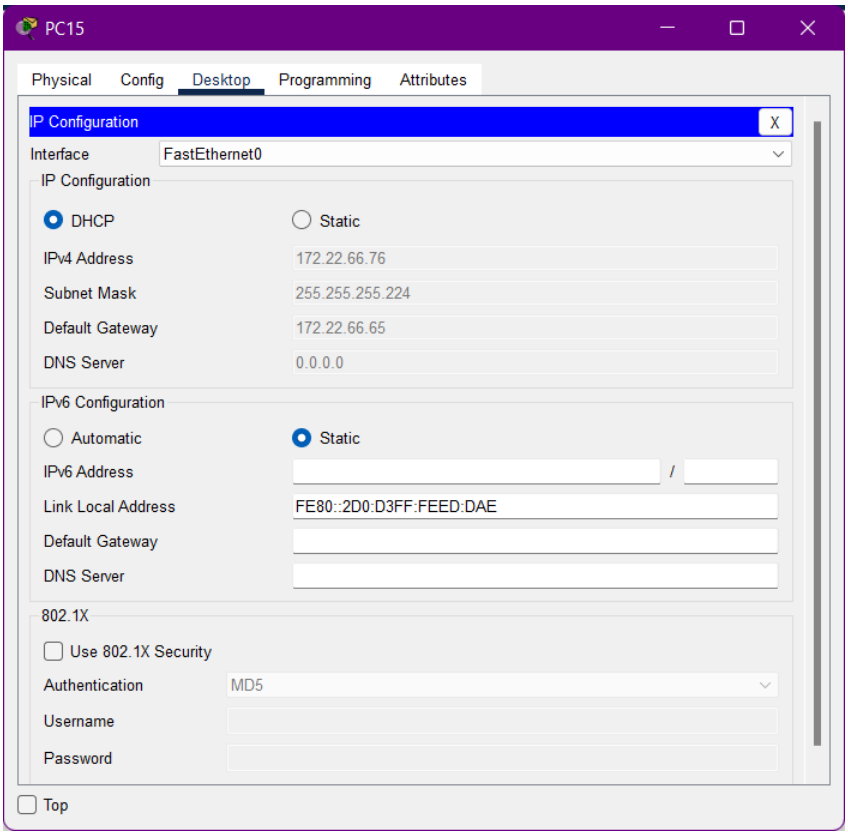

Рисунок 3.18 – Перевірка автоматичного призначення IP-адрес

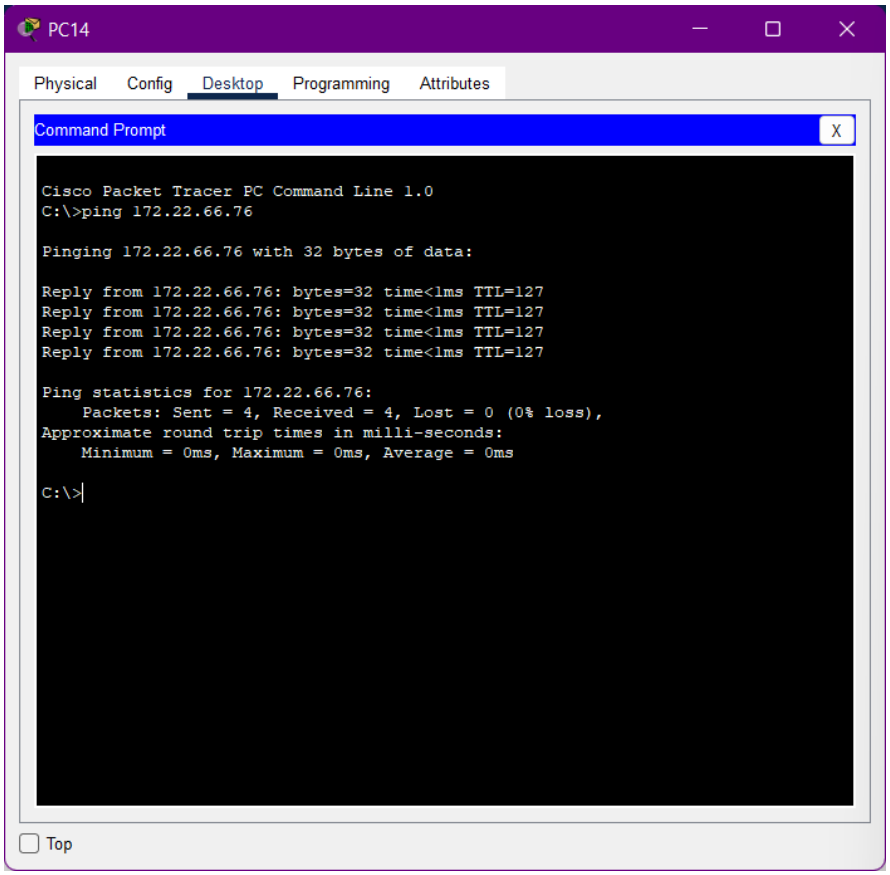

Рисунок 3.19 – Перевірка зв’язку між вузлами в різних VLAN

На комутаторах, які під’єднані то серверів, слід налаштувати функцію безпеки портів, таким чином, щоб:

– тільки двом унікальним пристроям був дозволенний доступ до порту;

– MAC-адреси пристрою розпізнавався динамічно і додавався в поточну конфігурацію;

– під час порушення системи безпеки з’являлось повідомлення, а порт залишався включеним.

Налаштування функції безпеки портів комутаторів під’єднаних до серверів

```
Volkov_SW0(config)#int range gi0/1
Volkov_SW0(config-if-range)#switchport mode access
Volkov_SW0(config-if-range)#switchport port-security maximum 2
```

Функція запам’ятовування MAC–адрес

```
Volkov_SW0(config-if-range)#switchport port-security mac-address sticky
```

У разі порушення безпеки порту, інтерфейс відкидає трафік з невідомих MAC–адресів

```
Volkov_SW0(config-if-range)#switchport port-security violation restric
```

3.3.4 Налаштувати всі маршрутизатори на підтримку служби AAA та RADIUS–сервер.

RADIUS є протоколом безпеки, який надає централізований метод аутентифікації користувачів шляхом звернення до зовнішнього сервера. Протокол RADIUS використовується для аутентифікації, авторизації та обліку. Сервер RADIUS використовує базу даних користувачів, яка містить дані автентифікації для кожного користувача. Таким чином використання протоколу RADIUS забезпечує додатковий захист при доступі до ресурсів мережі.

Згідно технічних вимог, на всіх маршрутизаторах слід наштувати підтримку служби AAA, таким чином:

– використовувати локальну базу даних користувачів , для перевірки підключень до VTY ліній;

– для доступу до консолі використовувати аутентифікацію на основі RADUIS і ящко немає – локальну базу;

– на RADUIS-сервері налаштувати ключове слово radius123; в якості облікового запису користувачів використовувати ім’я пристрою з паролем admin123.

Приклад налаштування RADUIS наведено на маршрутизаторі Volkov_RT3

```
Volkov_RT3(config)#aaa new-model
Volkov_RT3(config)#aaa auth
Volkov_RT3(config)#aaa authentication login default local
Volkov_RT3(config)#aaa authentication login Volkov_RT2 group radius
local
Volkov_RT3(config)#line console 0
Volkov_RT3(config-line)#login authentication Volkov_RT2
Volkov_RT3(config-line)#exit
Volkov_RT3(config)#line vty 0 4
Volkov_RT3(config-line)#login authentication default
Volkov_RT3(config-line)#username Volkov_RT2 password admin123
Volkov_RT3(config)#radius-server host 172.22.64.5 auth-port 1645
Volkov_RT3(config)#radius-server key radius123
```

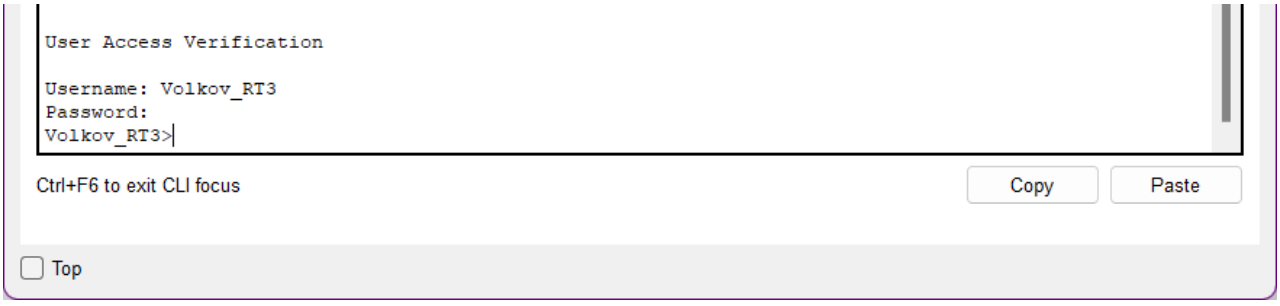

Рисунок 3.20 – Аутентифікація на маршрутизаторі за допомогою служби AAA та сервера RADIUS

4. РОЗРОБКА КОМПОНЕНТА СИСТЕМИ

4.1 Стан питання та постановка завдання

В комп'ютерній системі кінотеатра «Планета кіно», який розташований в ТРЦ «МОСТ-сіті», було прийнято рішення, для підмережі «Відділ управління персоналом» здійстини налаштування контролю температури в приміщенні та забезпечити протипожежну безпеки, за допомогою «Інтернет речей». Керування пристроями та моніторинг температури можна здійснювати з плантеша, який знаходиться в офісі та задопомогою мобільного телефона з налаштуванням 3G/4G технології.

Для початку необхідно реалізувати топологію мережі Network Strit, що реалізує стільниковий зв'язок. Кожному з пристроїв мережі призначити IP-адресу, маску і шлюз за замовчуванням за протоколом DHCP. Забезпечити підключення 3G/4G клієнтів до мережі. Мережу Network Strit представити двома пристроями Smartphone та вежу стільникового зв'язку Cell Tower. Для приєднання мережі Strit до маршрутизатора провайдера використовувати сервер Central Office.

Далі реалізовуємо топологію мережі Network ISP Servers, що реалізує сервіси провайдера. Мережу Network ISP Servers представити двома серверами, комутатором серії Cisco Catalyst 2960, маршрутизатором Cisco 2911та пристроєм PT-CLOUD.

На серверах провайдера необхідно виконати налаштування сервісів IoT, DHCP та DNS.

Виконати налаштування маршрутизатора провайдера. Налаштування виконати з урахуванням вимог: налаштувати базову конфігурацію маршрутизатора; налаштувати заходи з безпеки маршрутизатора. Використовувати адресацію, що наведена в таблиці 4.1.

Таблиця 4.1 – Документація схеми адресації і підключень пристроїв

Пристрій	Інтерфейс	IP–адреса	Префікс	Підключення	
				Назва пристрою	Інтерфейс
Rout_ISP	G0/0	119.4.201.225	/27	Central Office Server	Backbone
	G0/1	10.4.0.1	/24	Sw_ISP	G0/1
	G0/2	119.4.200.225	/27	Cloud_WAN	Eth6
Server_DNS	NIC	10.4.0.254	/24	Sw_ISP	F0/1
Server_IoT	NIC	10.4.0.253	/24	Sw_ISP	F0/2

Маршрутизатор повинен виконувати наступні функції: маршрутизацію між мережами; виконувати призначення унікальних динамічних IP–адрес і відповідних масок підмережі і шлюзів за замовчуванням для мережних пристроїв IoT smart devices в мережі Office та мережі Strit.

Далі реалізовуємо топологію мережі Office, що реалізує туманні та хмарні обчислення. Кожному з пристроїв мережі призначити IP–адресу, маску і шлюз за замовчуванням за протоколом DHCP. Виконати налаштування технології Wi-Fi на пристроях IoT для підключення до хмарного сервісу.

4.2 Реалізація системи

4.2.1 Налаштування мережі Strit

Мережа Strit складається з сервера Central Office Server, телефонної вишки Cell Tower та двух смартфонів.

На сервері, на інтерфейсі Backbone встановлено отримання IP-адреси за протоколом DHCP, результат наведено на рисунку 4.1.

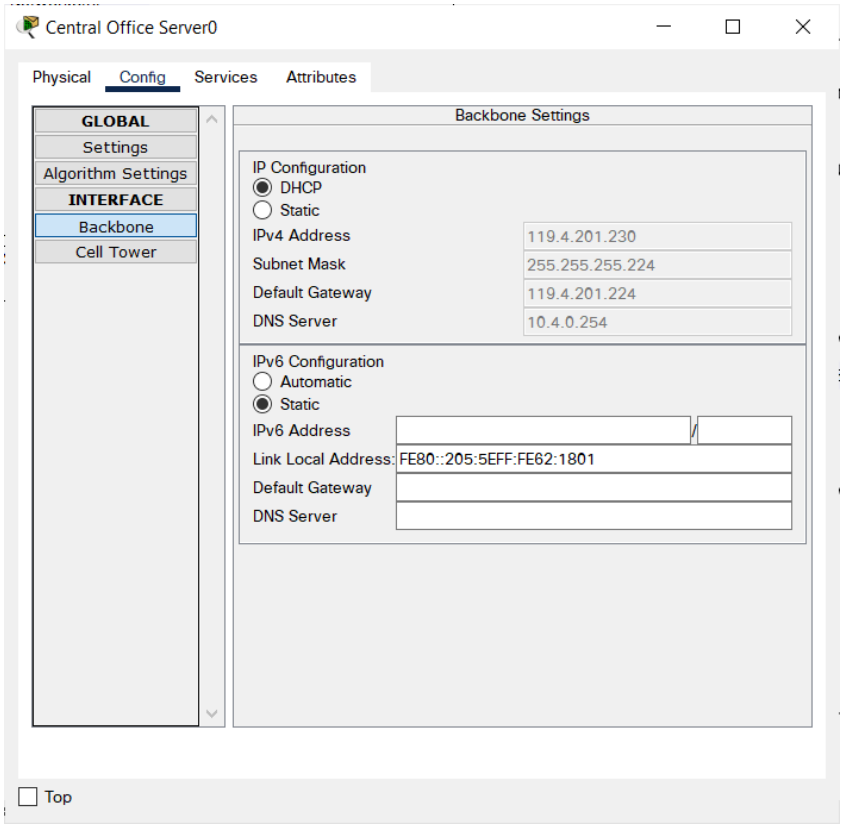

Рисунок 4.1 – Вкладка Config кінцевого пристрою Central Office Server

На вкладці Cell Tower залишив IP–адресу, що встановлена за замовчуванням , дивись рисунок 4.2

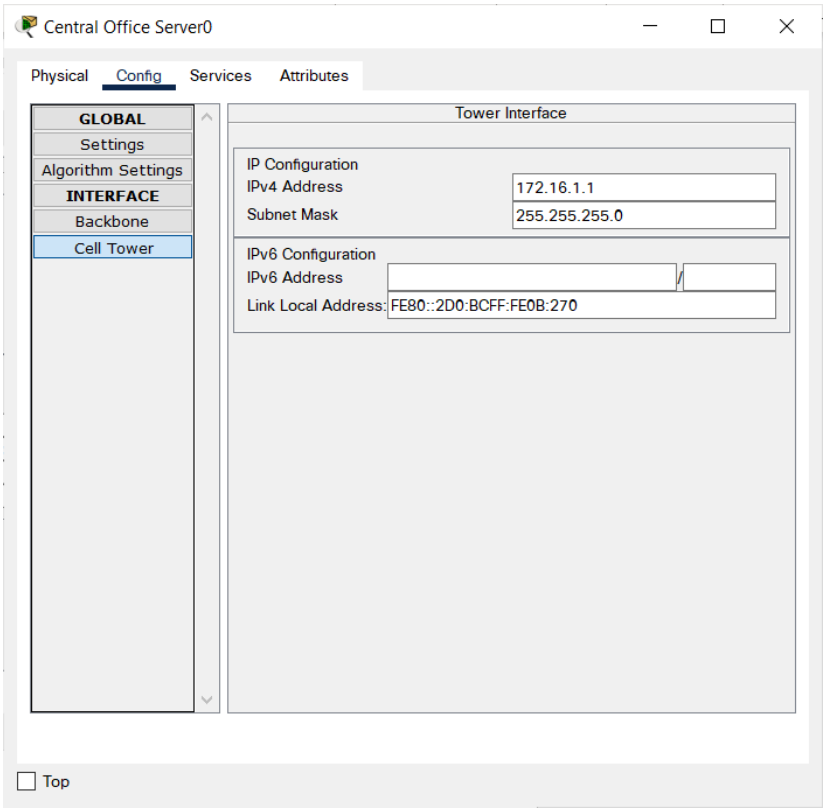

Рисунок 4.2 – Вкладка Config кінцевого пристрою Central Office Server

4.2.2 Налаштування мережі IPS Server

Мережа Network IPS Server складається з маршрутизатора Router_ISP, двох серверів DNS та IoT, та комутатора.

На маршрутизаторі Router_ISP виконавунаступні налаштування:

1) Виконав базову конфігурацію маршрутизатора:

– налаштування назви пристрою;

– встановлено пароль на привілейованого режиму;

– встановлено пароль для користувацького режиму EXEC;

– встановлено пароль для віддаленого доступу доTelnet/SSH;

– зашифровано всі відкриті паролі;

– налаштовано банер MOTD;

– Створено користувача 123–19ск1_Volkov з паролем cisco;

– Для шифрування данних встановлено ключ RSA довжиною 1024 біт.

```
Router(config)#no ip domain-lookup
Router(config)#hostname Volkov_RT0
```

```
Volkov_RT0(config)#service password-encryption
Volkov_RT0(config)#enable secret class
Volkov_RT0(config)#line console 0
Volkov_RT0(config-line)#password cisco
Volkov_RT0(config-line)#login
Volkov_RT0(config-line)#exit
Volkov_RT0(config)#banner motd $123-19ck1 Volkov access only with
password$
Volkov_RT0(config)#username 123-19ck1_Volkov password admincisco
Volkov_RT0(config)#ip domain-name Volkov_RT0
Volkov_RT0(config)#crypto key generate rsa
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
Volkov_RT0(config)#line vty 0 4
*Mar 1 0:2:50.849: %SSH-5-ENABLED: SSH 1.99 has been enabled
Volkov_RT0(config-line)#login local
Volkov_RT0(config-line)#transport input ssh
Volkov_RT0(config-line)#exit
Volkov_RT0(config)#do write
```

2) Задав IP-адреси на інтерфейсах відповідно таблиці 4.1

IP-адреса від Router_ISP до Central Office Server:

```
Router(config)#hostname Router_ISP
Router_ISP(config)#int 0/0
Router_ISP(config)#ip add 119.4.201.255 255.255.255.224
Router_ISP(config)# no sh
```

IP-адреса від Router_ISP до SW_ISP:

```
Router_ISP(config)#int 0/1
Router_ISP(config)#ip add 10.4.0.1 255.255.255.0
Router_ISP(config)# no sh
```

IP–адреса від Router_ISP до Cloud_WAN:

```
Router_ISP(config)#int 0/0
Router_ISP(config)#ip add 119.4.200.255 255.255.255.224
Router_ISP(config)# no sh
```

3) Виконаємо підключення сервісу DHCP в мережі Strit та Office. Для кожної мережі видалив перші чотири мережі з пулу.

Налаштування сервісу DHCP в мережі Strit:

```
Router_ISP(config)#service DHCP
Router_ISP(config)#   ip   dhcp   excluded-address   119.4.201.225
119.4.201.229
Router_ISP(config)#ip dhcp pool STRIR
Router_ISP(dhcp-config)#network 119.4.201.224 255.255.255.224
Router_ISP(dhcp-config)#default-router 119.4.201.224
```

```
Router_ISP(dhcp-config)#dns-server 10.4.0.254
Router_ISP(dhcp-config)#exi
```

Налаштування сервісу DHCP в мережі Office:

```
Router_ISP(config)#service DHCP
Router_ISP(config)#ip dhcp excluded-address 119.4.200.224
119.4.200.229
Router_ISP(config)#ip dhcp pool SMARTHOME
Router_ISP(dhcp-config)#network 119.4.200.224 255.255.255.224
Router_ISP(dhcp-config)#default-router 119.4.200.225
Router_ISP(dhcp-config)#dns-server 10.4.0.254
Router_ISP(dhcp-config)#exi
```

Наступним кроком виконав налаштування серверів DNS та IoT.

На сервері DNS виконав наступні налаштування:

1) Задав IP-адресу, маску мережі, шлюз за замовчуванням та DNS server, результат наведено на рисунку 4.3.

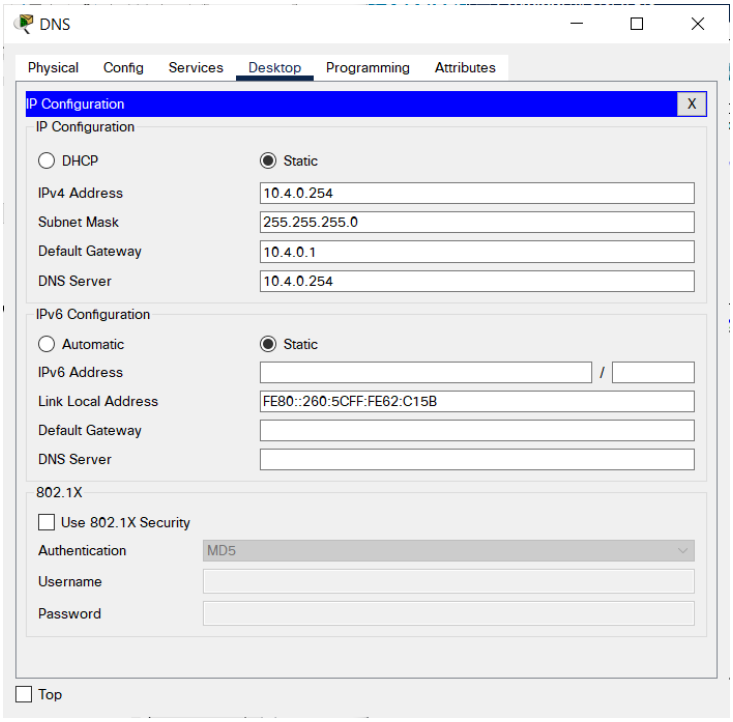

Рисунок 4.3 – Налаштування IP Configuration на DNS server

2) В діалоговому вікні налаштувань сервера на вкладці Services ввімкнув DNS, додав ім’я ресурсу www.iot.com, задав адресу сервера IoT та додав запис, результат наведено на рисунку 4.4.

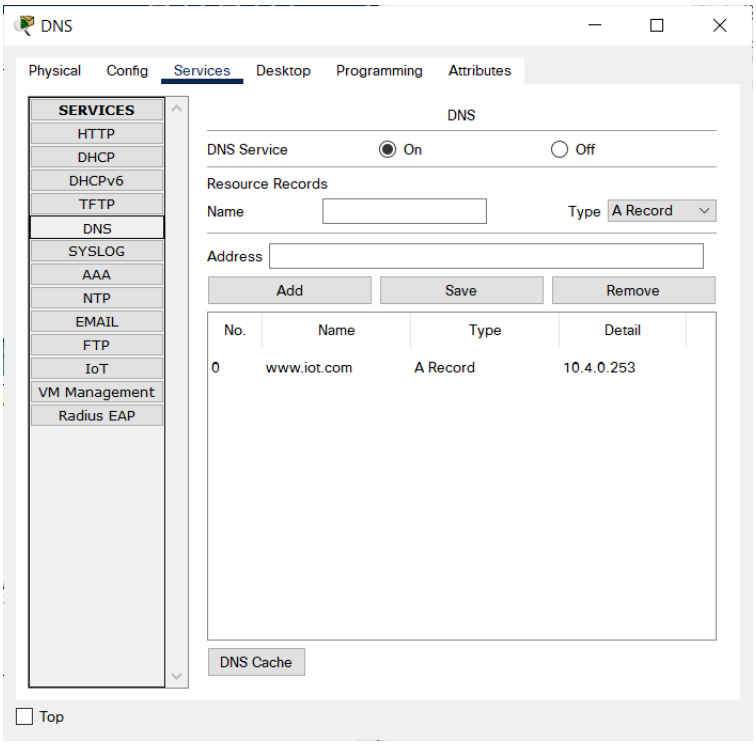

Рисунок 4.4 – Налаштування DNS сервера на вкладці Services

На сервері IoT виконав наступні налаштування:

1) Задав IP–адресу серверу IoT, маску мережі, шлюз за замовчуванням та DNS server, дивись рисунок 4.5.

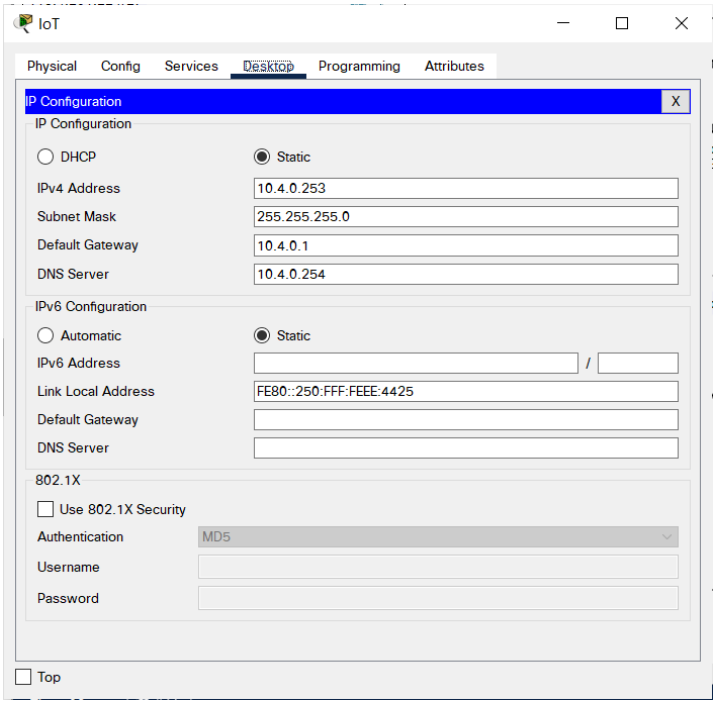

Рисунок 4.5 – Налаштування IP Configuration на IoT server

2) В діалоговому вікні налаштувань сервера на вкладці Services ввімкнув сервіс IoT, дивись рисунок 4.6.

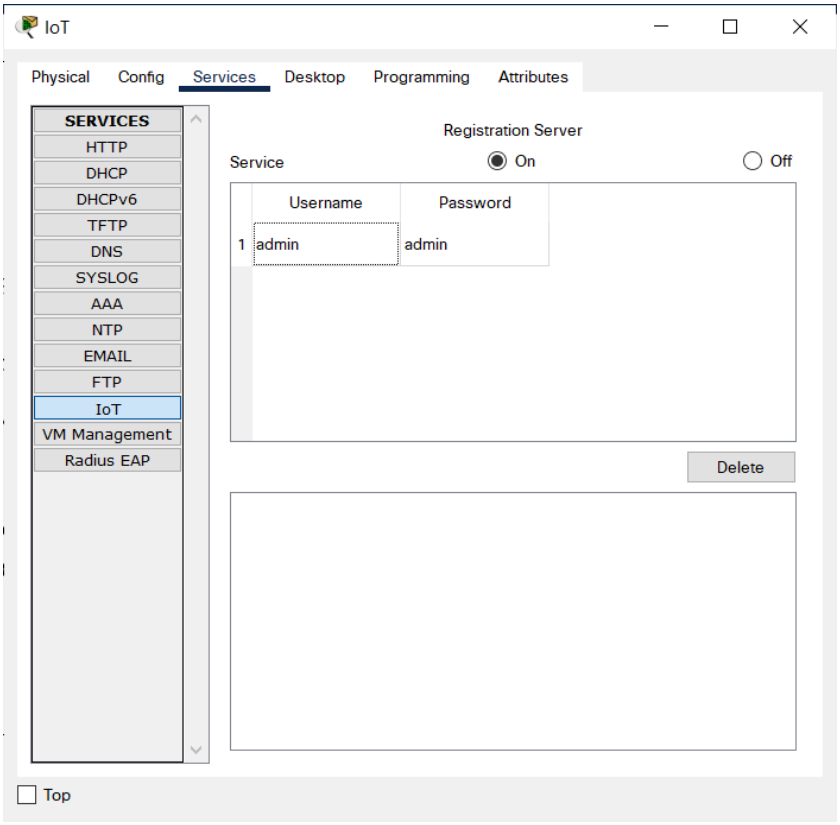

Рисунок 4.6 – Ввімкнення IoT сервера

Налаштування сервера Central Office Server:

1) На інтерфейсі Backbone встановив отримання IP-адрес за протоколом DHCP, дивись рисунок 4.7.

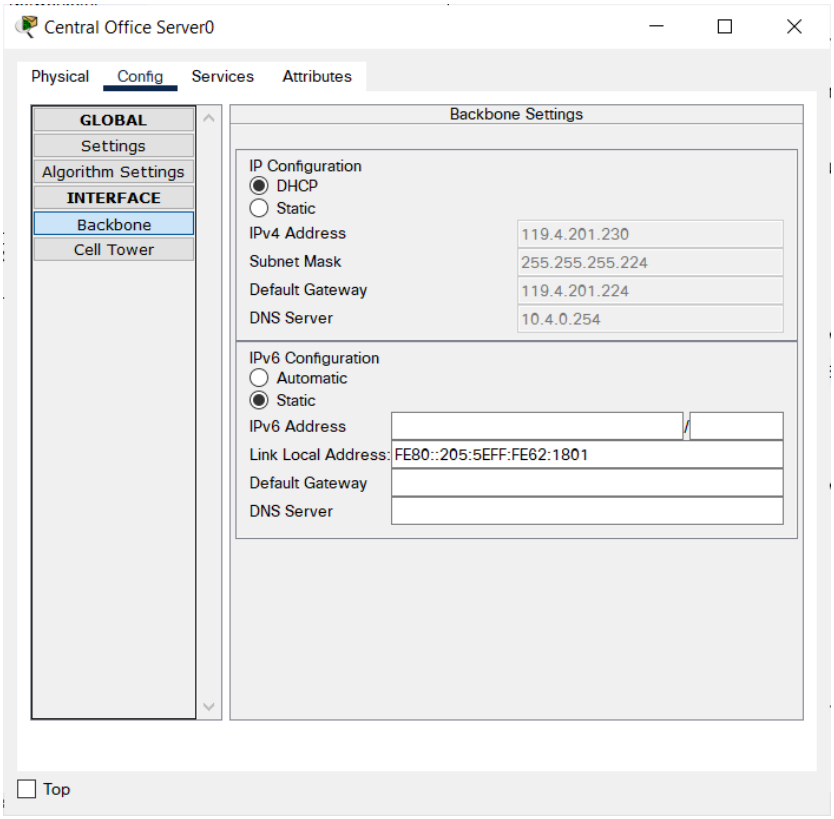

Рисунок 4.7 – Вкладка Config кінцевого пристрою Central Office Server

2) На інтерфейсі Cell Tower залишив IP–адресу, що встановлена за замовчуванням, дивись рисунок 4.8.

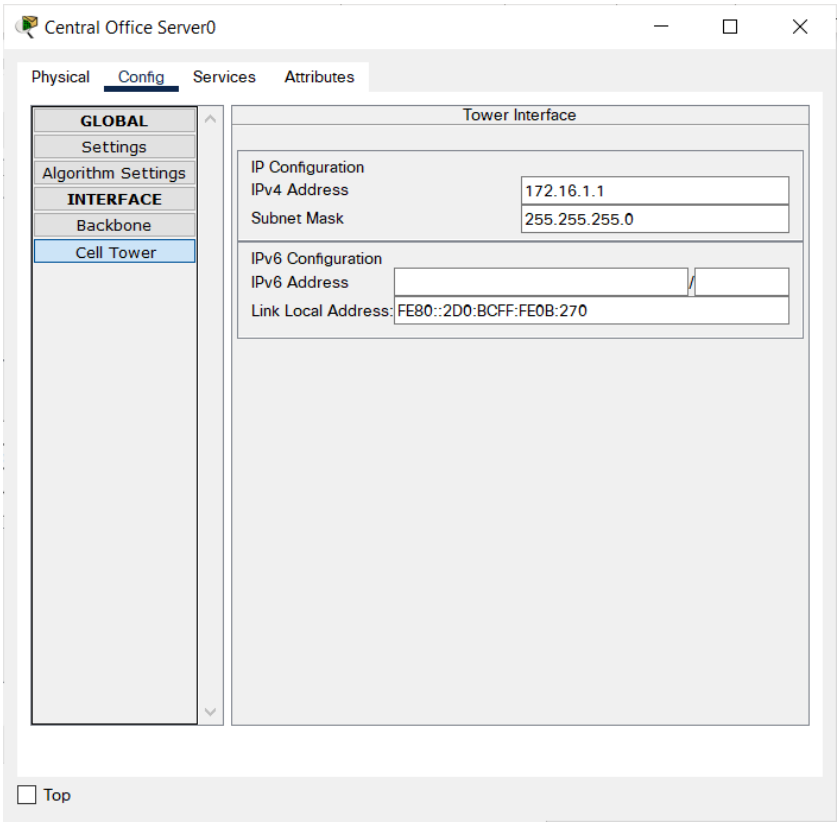

Рисунок 4.8 – Вкладка Config кінцевого пристрою Central Office Server

4.2.3 Налаштування пристроїв в мережі Office

На пристрої Cloud, в діалоговому вікні налаштувань на вкладці Config для інтерфейсу Ethernet6 вказав тип мережі провайдера – Cable. В діалоговому вікні налаштувань на вкладці Config –> CONNECTIONS виконав асоціацію coaxial7 та Ethernet6, результат налаштування наведено на рисунку 4.9.

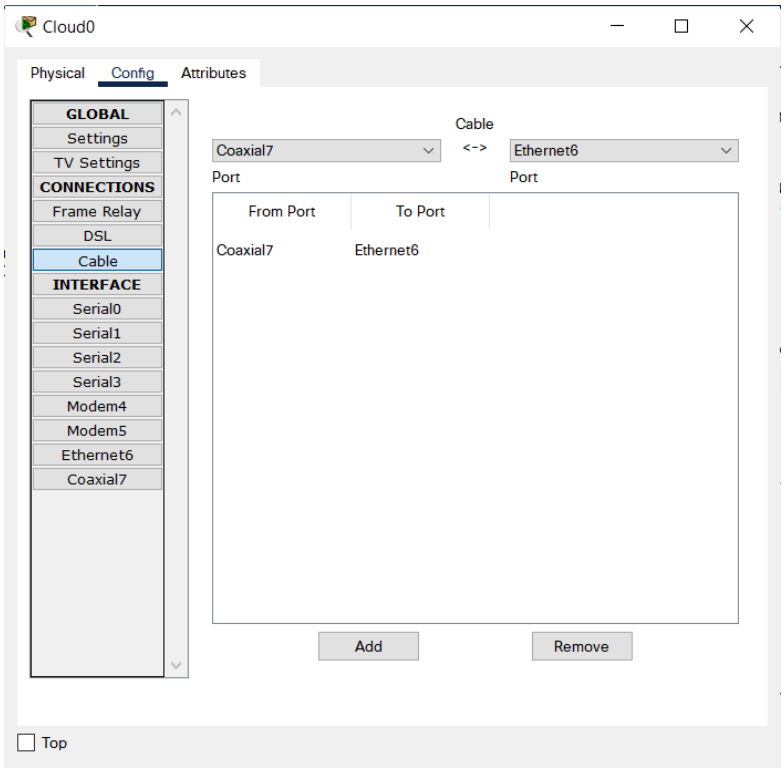

Рисунок 4.9 – Вкладка Config пристрою Cloud

Далі на пристрій Home Gateway, в діалоговому вікні налаштувань на вкладці Config для інтерфейсу Internet встановив отримання IP-адреси за протоколом DHCP, на вкладці Config для інтерфейсу LAN залишив IP–адресу, що встановлена за замовчуванням, на вкладці Config для інтерфейсу Wireless ввів ім’я мережі (SSID) HomeNet та обрав спосіб автентифікації WPA2-PSK встановивши пароль cisco1234, результат наведено на рисунку 4.10 – 4.12.

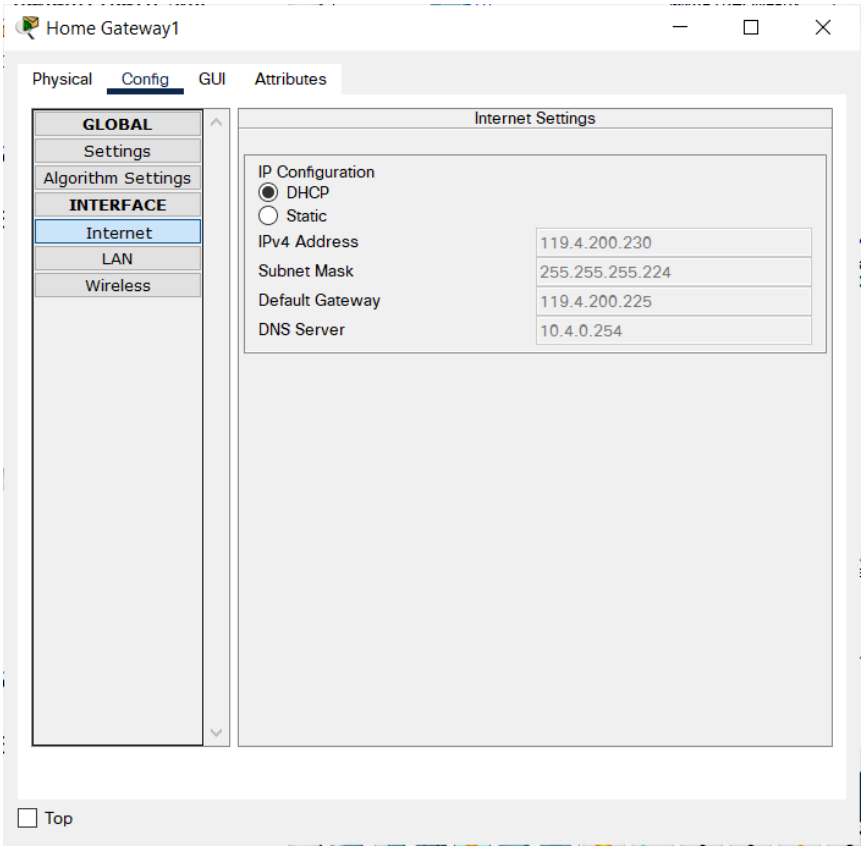

Рисунок 4.10 – Вкладка Config/Internet кінцевого пристрою Home Gateway

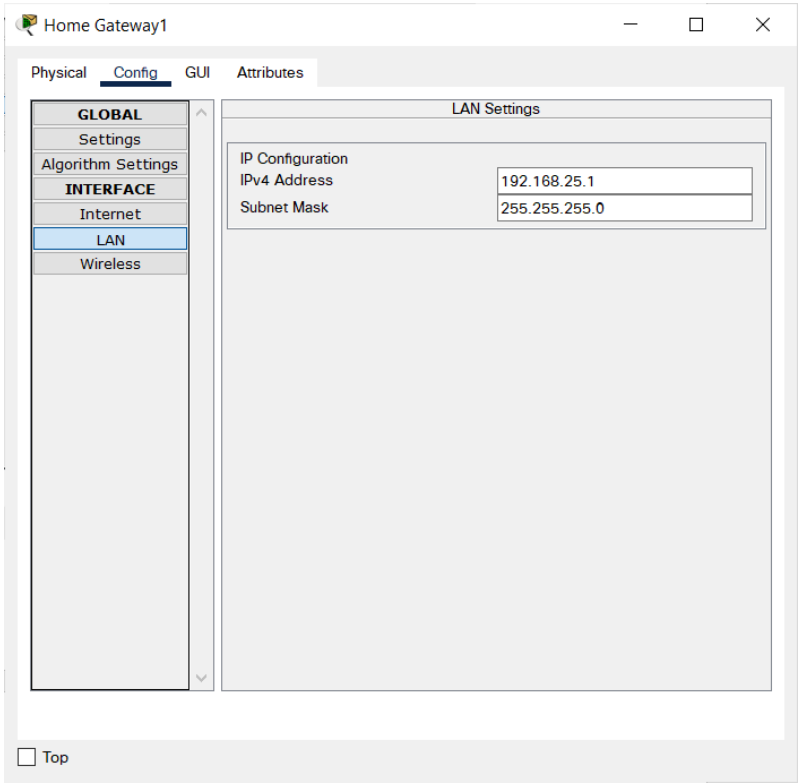

Рисунок 4.11 – Вкладка Config/LAN кінцевого пристрою Home Gateway

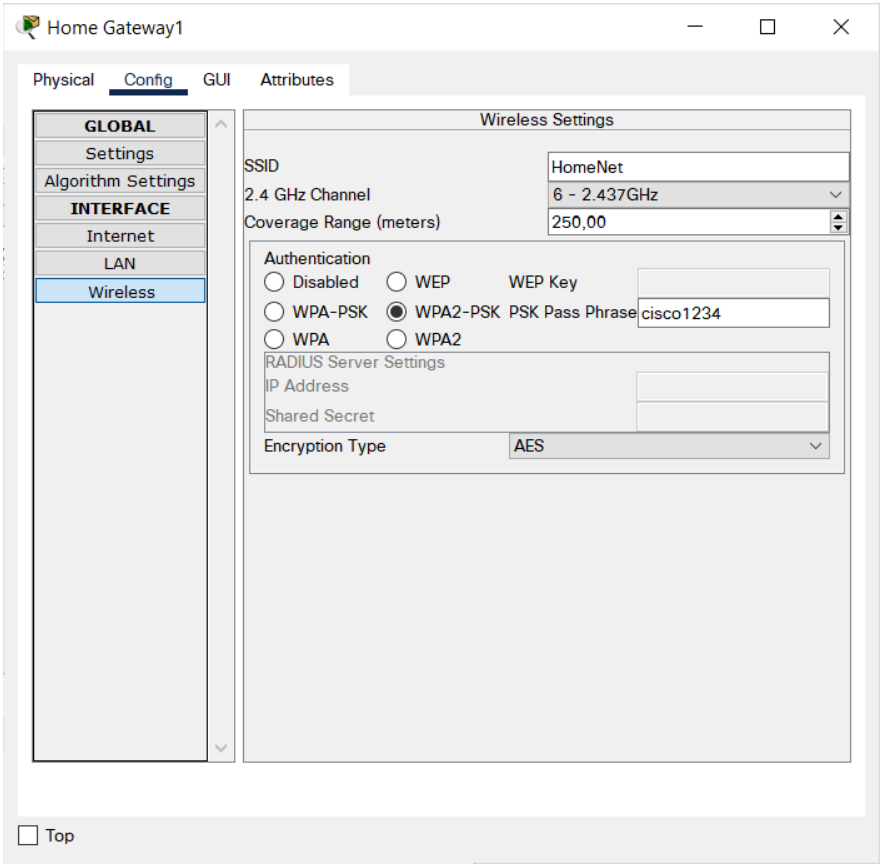

Рисунок 4.12 – Вкладка Config/Wireless кінцевого пристрою Home Gateway

4.2.4 Реалізація туманних обчислень

Туманні обрахунки виконанні для контролера MCU, який слідкує за станом навколишньої температури. Для контролера написано програму на мові Python, а також налаштовано IoT пристрої, які під’єднанні до Home Gateway, який забезпечує їм зв’язок один з одним.

На пристрої Tablet PC, на вкладці Config/Wireless0 вказав мережу HomeNet, в розділі аутентифікації встановив шифрування WPA2-PSK та ввів пароль cisco1234 та натиснув Connect, дивись рисунок 4.13.

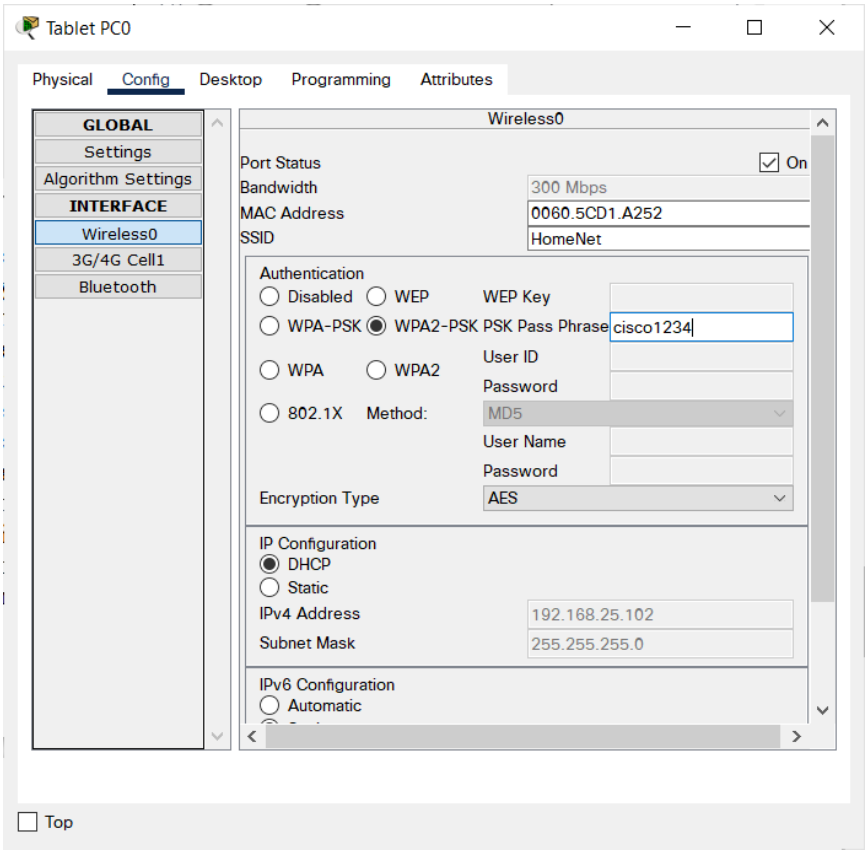

Рисунок 4.13 – Вкладка Config пристрою Tablet PC

Для пристроїв Термостат, Обігрівач, Вікно та Вентилятор, виконав аналогічні налаштування, як для Tablet PC, вказавши назву мережі HomeNet, встановив шифрування WPA2–PSK та ввів пароль cisco1234. В розділі Global Settings на вкладці IoT вказав IP-адресу IoT сервера, ім’я користувача та пароль, результат наведено на рисунку 4.14 – 4.15.

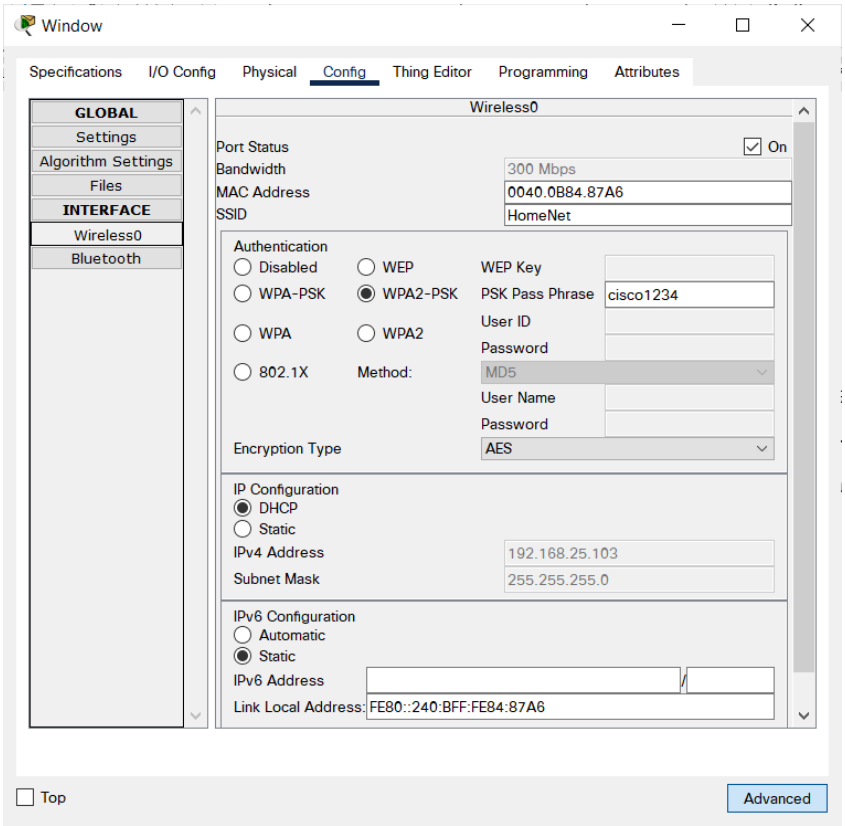

Рисунок 4.14 – Вкладка Config пристрою Window

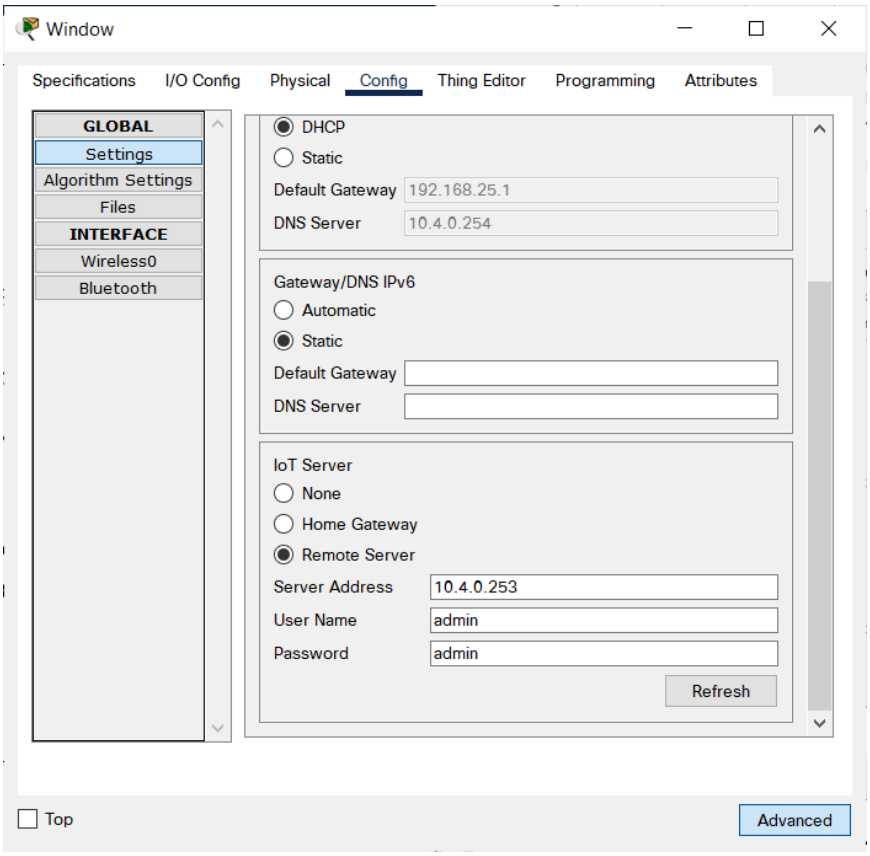

Рисунок 4.15 – Налаштування IoT сервера на вкладці Global Settings

На контролері MCU реалізував роботу системи, яка виконує поставленні задачі. А саме при реагуванні датчика вогню буде спрацьовувати сирена та ввімкнеться оприскувач води.

Налаштування роботи контролера MCU на мові Python:

```
from gpio import *
from time import *


# Callback used to detect when the temperature sensor attached to
the mcu sends data.
def inputHandler():
     # Convert from the old range to the new range.
     value =  (((analogRead(A0) - 0) * (100 - -100)) / (1023 - 0))
+ -100
     customWrite(0, value  )

     if (value > +25):
          customWrite(1, '1')
          customWrite(2, '1')
          customWrite(3, '1')

     else:
          customWrite(1, '0')
          customWrite(2, '0')
          customWrite(3, '0')


# Setup the callback event to handle a value on the A0 slot.

def main():
     add_event_detect(A0, inputHandler);

def handleSensorData():
     value = digitalRead(0)
     if value == 0:

          customWrite(1, '0')
          digitalWrite(2, LOW)
     else:

          customWrite(1, '1')
          digitalWrite(2, HIGH)

def handleSensorData1():
     value = digitalRead(1)
     if value == 0:

          customWrite(1, '0')
          digitalWrite(2, LOW)
```

```
        else:

                customWrite(1, '1')
                digitalWrite(2, HIGH)

def main():
        add_event_detect(0, handleSensorData)
        add_event_detect(3, handleSensorData1)

        while True:
                delay(1000)


if __name__ == "__main__":
        main()
```

4.2.5 Реалізація хмарних обчислень

Хмарні обчислення виконані за допомогою віддаленого сервера IoT, до якого підключені усі розумні пристрої в системі за допомогою керуючого шлюзу. Сервер отримує інформацію про стан пристроїв, зберігає їх данні, а також надає можливість керувати пристроями з мобільних телефонів, планшета чи комп'ютера. Принцип роботи наведе на рисунках 4.16 – 4.17.

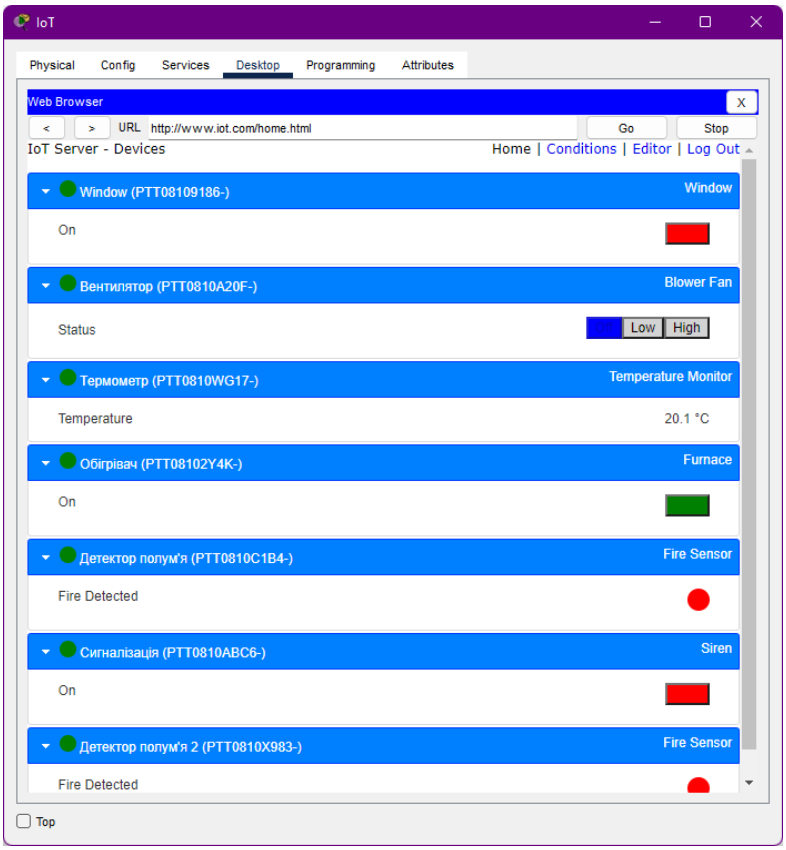

Рисунок 4.16 – Відображення пристроїв на віддаленому сервері

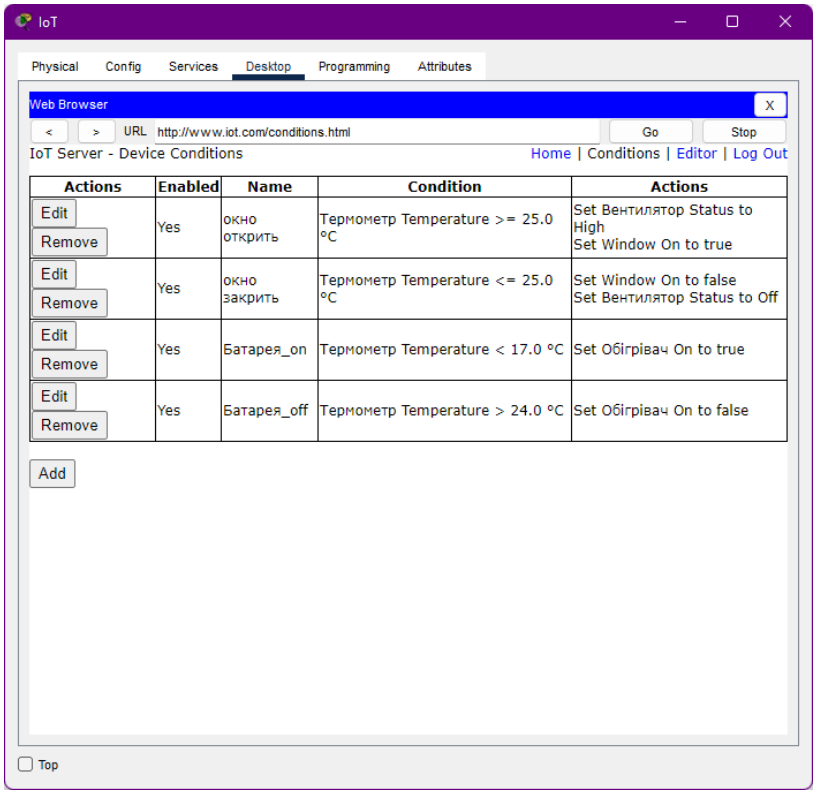

Рисунок 4.17 – Сценарій керування розумних пристроїв

4.3 Перевірка роботи комп’ютерної системи

Налаштувавши комп’ютерну системи з використанням Інтернет речей, отримали наступний результат:

– при температурі навколишнього середовища більше 25 градусів, то автоматично відчиняється вікно та вмикається вентелятор;

– при температурі навколишнього середовища менеш ніж 25 градусів, то автоматично зачиняється вікно та вимикається вентелятор;

– при температурі навколишнього середовища менеше 17 градусів, то вмикається обігрівач;

– при температурі навколишнього середовища більше 24 градусів, то обігрівач вимикається;

– при спрацюванні дедектора вогню, сигнал тривоги передається на сирену та вмикається оприскувач;

– можливість керувати системою з мобільного телефона за допомогою 3G/4G технологією.

Приклад роботи комп'ютерної системи наведено на рисунках 4.18 – 4.21

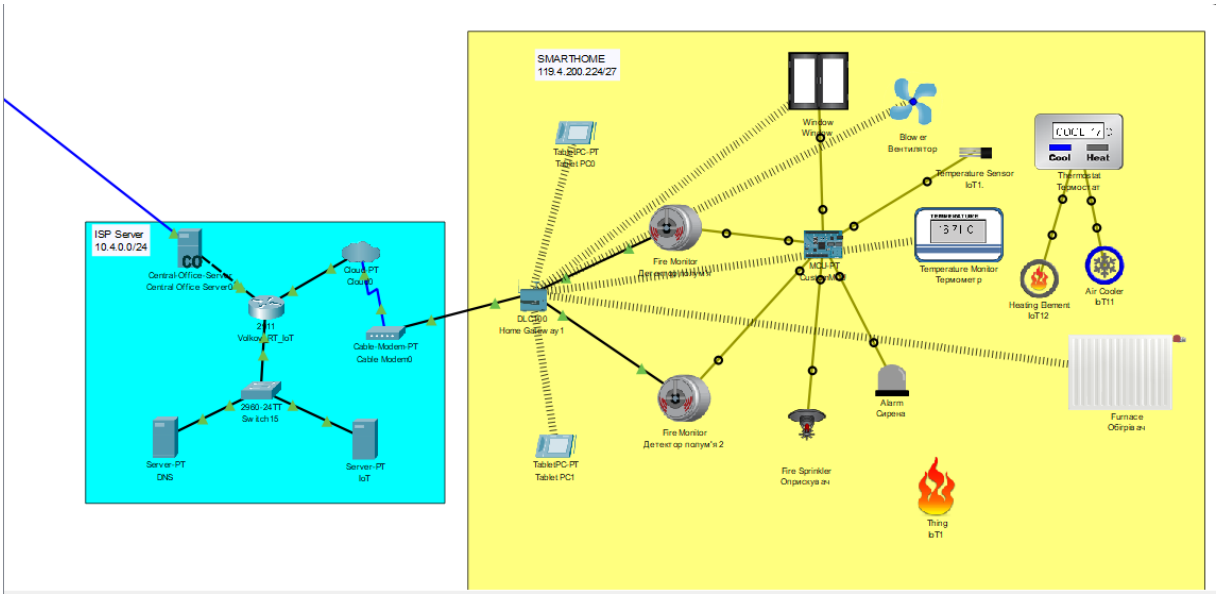

Рисунок 4.18 – Спрацювання обігрівачі при досягненні мінімальної температури в кімнаті

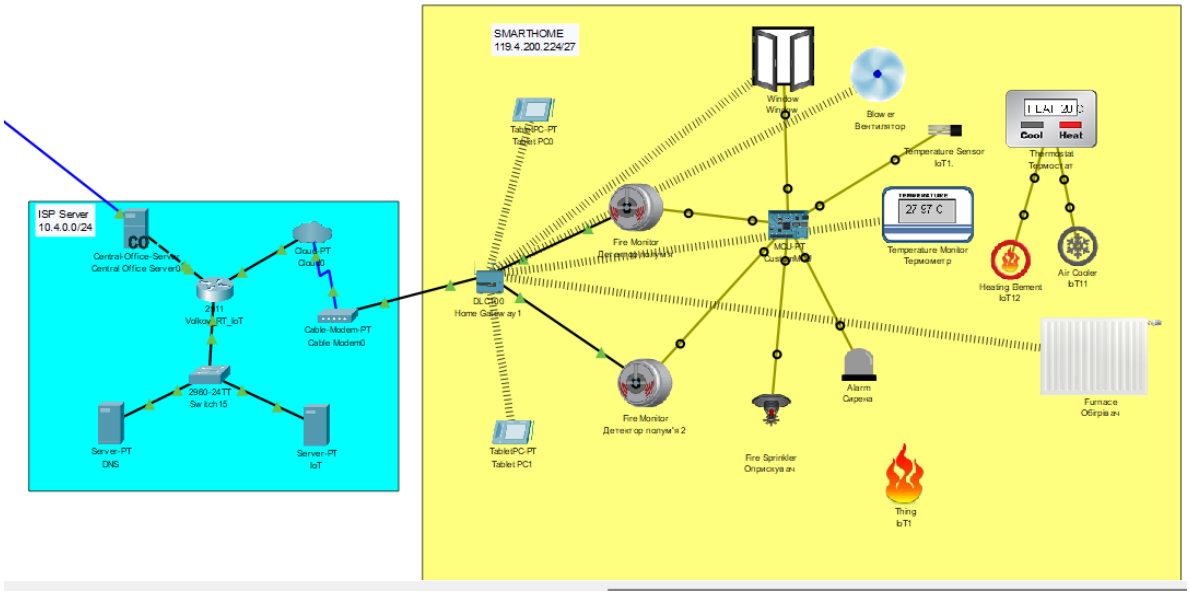

Рисунок 4.19 – Спрацювання датчика вікна та вентелятора при досягненні максимальної температури

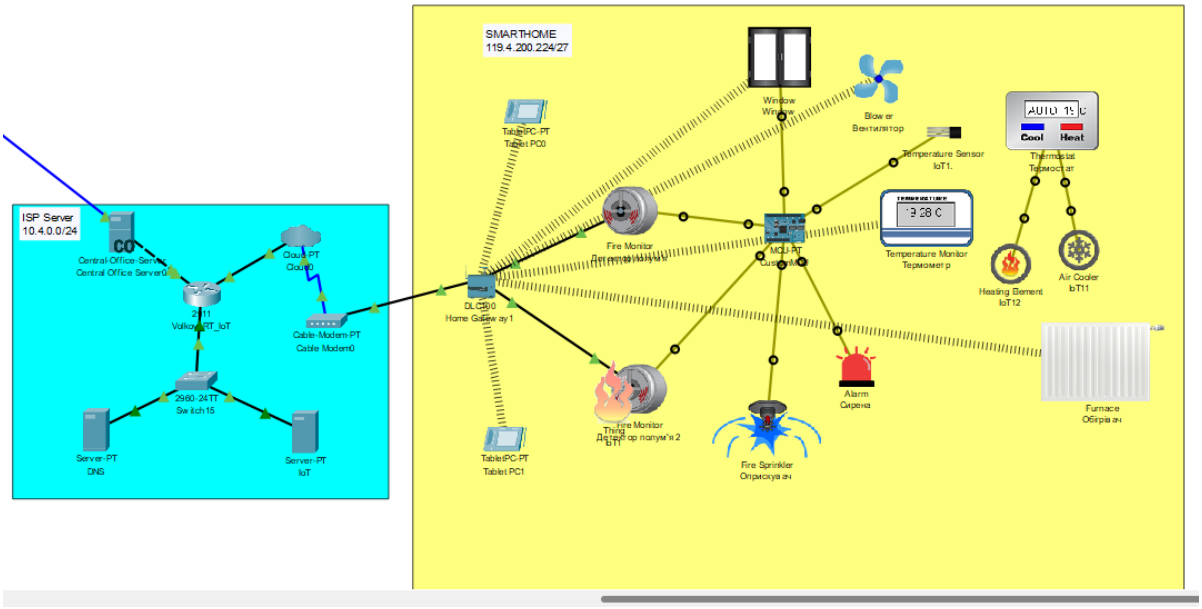

Рисунок 4.20 – Спрацювання датчика вогню

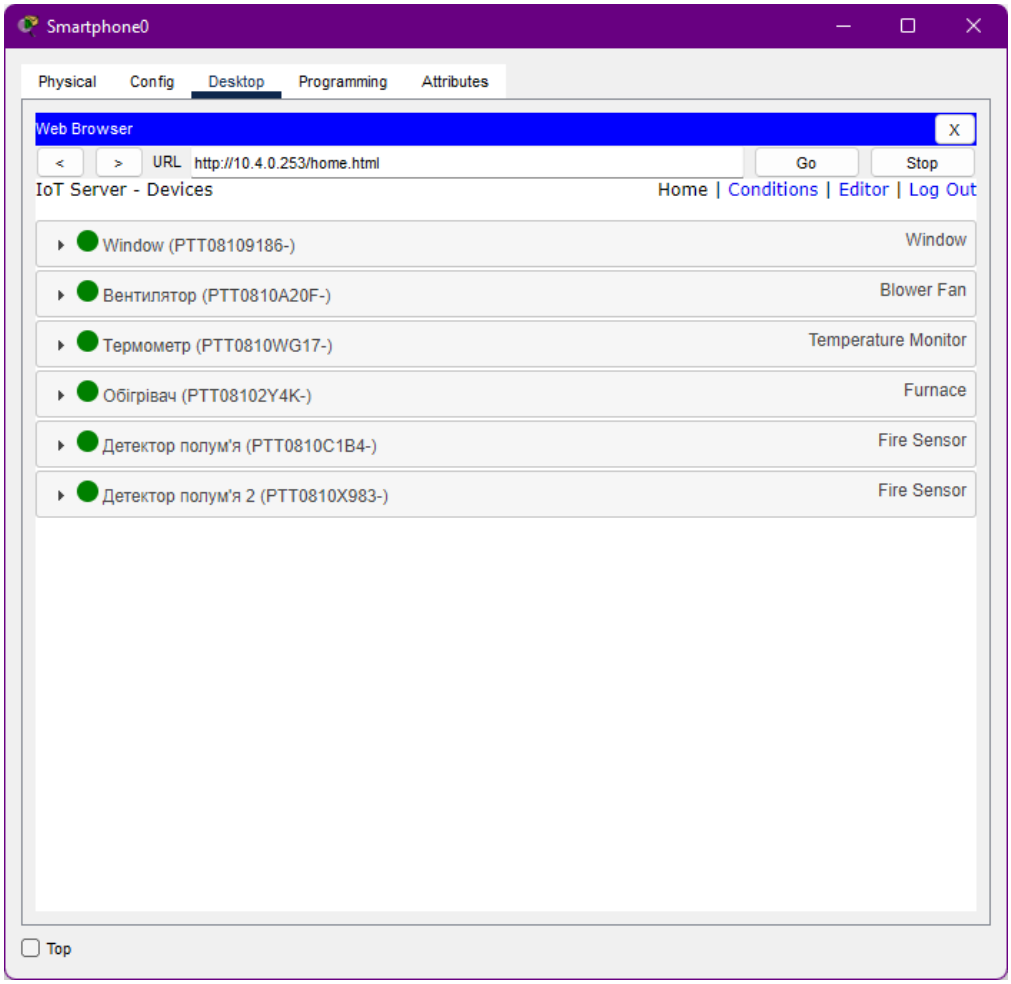

Рисунок 4.21 – Перевірка підключеня до системи через мобільний телефон

ВИСНОВОК

Під час виконання кваліфікаційної роботи, розглянута комп'ютерна система мережі кінотеатрів «Планета кіно» місто Дніпро, з детальним опрацюванням побудови, налаштування та беспеки корпоротивної мережі, яка спецілізується на показі фільмів. Також розглянуті вимоги для проектування мережі, вибрано мережеве обладнання, яке відповідає всім поставленним вимогам.

Для комп'ютерної мережі здійснено розрахунок налаштувань маршрутизації, базове налаштування пристроїв, забезпечення маршрутизаціїї за допомогою протоколу OSPF, налаштування параметрів безпеки, а саме захист від несанкціонованого доступу, налаштовано VPN канал між віддаленими підмережами, надано доступ до мережі Інтернет.

Під час розробки системи було створив модель системи IoT SMARTHOME, що має можливість передавати данні стану системи на смартфон, планшет та ноутбук користувача, обробляти та зберігати дані розумних пристроїв на віддаленому сервері IoT. Запрограмував MCU контролер, який за допомогою термостату то датчика температури відстежує температуру навколишнього середовища, які в свою чергу дають сигнал для коректної роботи IoT пристроїв, також становлено детектор вогню, який при виявлені вогню передає сигнал на сирену та вмикається оприскувач водм. В мережі STRIT реалізовано налаштування DNS та IoT серверів для віддаленого підключення, налаштовано DHCP сервіс.

Перевірка працездатності роботи виконана методом моделювання комп'ютерної системи у багатофункціональній програмі Cisco Packet Tracer.

Кваліфікаційна робота виконанна відповідно теми а завдання, оформлена відповідно до нормативних документів і методичного керівництва.

ПЕРЕЛІК ПОСИЛАНЬ

1. Офіційний сайт мережі кінотеатрів «Планета кіно». [електронний ресурс] — Режим доступу: URL https://planetakino.ua/res/storage/ pkzvitproupra vlinnakompanieuza2020rik.pdf

2. Оглад мережевого обладнання Cisco: [електронний ресурс] — Режим доступу: URLhttps://gta.group/cisco–equipment–overview/

3. Методичні рекомендації до виконання кваліфікаційної роботи ступеня бакалавр студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія /Л.І. Цвіркун, Я.В. Панферова, Л.В. Бешта. – Д.: НТУ «Дніпровська політехніка», 2018. – 32 с.

4. Вимоги до комп'ютерної мережі:[електронний ресурс] — Режим доступу: URL https://studfile.net/preview/5484683/

5. Мережева академія Cisco курс IOT, CCNA1, 2, 3: [Електронний ресурс] – Режим доступа:URL: https://www.netacad.com/ru.

6. Національна бібліотека ім. Н.Е.Баумана: [електронний ресурс] – Режим доступу: URL: https://ru.bmstu.wiki/NAT_(Network_Address_ Translation)

7. Мережа для самих маленьких. Агрегація каналів: [електронний ресурс] – Режим доступу: URL: https://linkmeup.gitbook.io/sdsm/4.-stp/05-link-aggregation

8. LanMarket. Енциклопедія: [електронний ресурс] – Режим доступу: URL: https://lanmarket.ua/entsiklopediya/telekommunikatsionnye-tekhnologii/vlan.html

Додаток А

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Міністерство освіти і науки України
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ДНІПРОВСЬКА ПОЛІТЕХНІКА»

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП'ЮТЕРНОЇ СИСТЕМИ

Текст програми

804.02070743.22004–01 12 01

Листів 6

2022

АНОТАЦІЯ

Дана програма містить в собі частину програмного коду для програмування налаштування компонентів корпоративної мережі комп’ютерної системи. Програма призначена для забезпечення налаштування DHCP, AAA, інтерфейсів, протоколу маршрутизації NAT, консольних і vty ліній та створення мереж VPN, домену и ssh комп’ютерної системи.

ЗМІСТ

1 Налаштування маршрутизатора Volkov_RT0 4

1.1 Налаштування DHCP 4

1.2 Налаштування AAA 4

1.3 Створення користувача с паролем 4

1.4 Створення домену 4

1.5 Налаштування інтерфейсів 4

1.6 Налаштування віртуального інтерфейсу VLAN 5

1.7 Налаштування протоколу маршрутизації 5

1.8 Налаштування банеру 5

1.9 Налаштування RADIUS 5

1.10 Налаштування консольних та vty ліній 5

```
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
```

Шифрування паролів

```
service password-encryption
!
```

Ім’я пристрою

```
hostname Volkov_RT0
```

Пароль для привілейованого режиму

```
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
```

Виключення адрес з пулу DHCP

```
ip dhcp excluded-address 172.22.66.1 172.22.66.10
ip dhcp excluded-address 172.22.66.33 172.22.66.42
ip dhcp excluded-address 172.22.66.65 172.22.66.75
```

1.1 Налаштування DHCP

```
ip dhcp pool poolvvlan14
network 172.22.66.0 255.255.255.224
default-router 172.22.66.1
```

1.2 Налаштування AAA

```
aaa new-model
!
aaa authentication login Volkov_RT0 group radius local
aaa authentication login default local
!
!
no ip cef
no ipv6 cef
```

1.3 Створення користувача с паролем

```
username Volkov_RT0 password 7 082048430017544541
!
license udi pid CISCO2911/K9 sn FTX15246RK3-
```

1.4 Створення домену

```
no ip domain-lookup
ip domain-name Volkov_RT0
```

1.5 Налаштування інтерфейсів

```
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
```

1.6 Налаштування віртуального інтерфейсу VLAN

```
interface GigabitEthernet0/0.14
encapsulation dot1Q 14
ip address 172.22.66.1 255.255.255.224
```

1.7 Налаштування протоколу маршрутизації

```
router ospf 1
log-adjacency-changes
network 172.22.66.0 0.0.0.31 area 0
network 172.22.66.32 0.0.0.31 area 0
network 172.22.66.64 0.0.0.31 area 0
network 172.22.66.96 0.0.0.31 area 0
network 172.22.66.0 0.0.0.127 area 0
network 172.22.66.128 0.0.0.127 area 0
network 10.0.4.0 0.0.0.3 area 0
network 10.0.4.4 0.0.0.3 area 0
network 10.0.4.12 0.0.0.3 area 0
network 172.22.64.0 0.0.0.255 area 0
network 172.22.65.0 0.0.0.255 area 0
network 209.165.202.0 0.0.0.15 area 0
network 10.0.4.16 0.0.0.3 area 0
network 209.165.202.0 0.0.0.31 area 0
```

1.8 Налаштування банеру

```
banner motd ^C123-19ck1 Volkov access only with password^C
```

1.9 Налаштування RADIUS

```
radius-server host 172.22.64.1 auth-port 1645
radius-server host 172.22.64.5 auth-port 1645
radius-server key radius123
!
radius server 172.22.64.1
address ipv4 172.22.64.1 auth-port 1645
radius server 172.22.64.5
address ipv4 172.22.64.5 auth-port 1645
```

1.10 Налаштування консольних та vty ліній

```
login authentication Volkov_RT0
!
line aux 0
!
line vty 0 4
login authentication default
transport input ssh
line vty 5 15
```