Міністерство освіти і науки України

Національний технічний університет

«Дніпровська політехніка»

Інститут електроенергетики
(інститут)
Факультет інформаційних технологій
(факультет)
Кафедра інформаційних систем та технологій
(повна назва)

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи ступеня бакалавра

(бакалавра, спеціаліста, магістра)

Студента Кириченко Микити Олеговича
(ПІБ)
академічної групи 123-18-1
(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 туристичної компанії ТОВ «Круїз» з опрацюванням побудови та налаштування корпоративної мережі»
(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
Кваліфікаційної роботи	Доц. Шедловський І.А.			
Розробка апаратної частини	Доц. Ткаченко С.М.			
Проектування корпоративної мережі	Ас. Бешта Л.В.			
Рецензент Нормоконтролер	Проф. Цвіркун Л.І.			

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 Кириченко М.О. **академічної групи** 123-18-1
(прізвище та ініціали) (шифр)
спеціальності 123 «Комп'ютерна інженерія»
за освітньо-професійною програмою 123 «Комп'ютерна інженерія»
(офіційна назва)
на тему "Комп'ютерна система туристичної компанії ТОВ «Круїз» з опрацюванням побудови та налаштування корпоративної мережі"
затверджену наказом ректора НТУ «Дніпровська політехніка» від 10.05.2022 № 771-л

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 задачі	
Розробка апаратної частини	На основі аналізу підприємства формується технічні вимоги до комп'ютерної мережі та розробляється апаратна частина мережі	
Розробка корпоративної мережі	Виконується розрахунок налаштувань корпоративної мережі та перевірка роботи системи, розробляється методи та налаштування обладнання для захисту системи	
Розробка компонента системи	Виконується детальна розробка компонентів системи	

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

Дата видачі _____
Дата подання до екзаменаційної комісії _____
Прийнято до виконання _____ Кириченко М.О.

РЕФЕРАТ

Пояснювальна записка: 20стр; 28 рис; 7 таб; 13 джерел; додатки.

Об’єкт розробки - комп’ютерна система Туристичної Агенції Круїз з детальним опрацюванням побудови та налаштуванням мережі, безпеки мережі.

Мета роботи − створення комп’ютерної системи для туристичної агенції.

Орієнтована на обслуговування клієнтів, сбір даних про клієнтів, співробітників та туристичні подорожі, зберігання конфіденціальної інформації про клієнтів та співробітників агенції, активний пошук інформації в глобальній мережі інтернет.

Мережа дозволяє користатись, відкрито входити до мережі інтернет, зберігати інформацію, користатись віддаленими філіями. Це підвищує ефективність роботи співробітників, облегшує комунікацію між ними. Мережа дуже безпечна до схоронності інформації в ній, безпечна до загроз.

Також налаштована система IoT облегшує роботу працівників компанії та обслуговування клієнтів, а також підвищує рівень безпеки у приміщені.

Розробка комп’ютерної мережі виконана відповідно до завдання на кваліфікаційну роботу бакалавра.

Розроблена схема мережі реалізована у вигляді моделі на симуляторі Cisco Packet Tracer і перевірена її робота.

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

ТУРИСТИЧНА АГЕНЦІЯ, МЕРЕЖА, ТОПОЛОГІЯ, VPN, NAT, EIGRP, DHCP, IOT, VLAN, WAN

ЗМІСТ

РЕФЕРАТ 3
ЗМІСТ 4
ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАК, ОДИНИЦЬ І ТЕРМІНІВ 6
ВСТУП 7
1 СТАН ПИТАННЯ ТА ПОСТАНОВКА ЗАВДАННЯ 9
1.1 Характеристика та аналіз діяльності Туристичного Агентства 9
1.2 Характеристика і структура об’єкта впровадження 9
1.3 Стислі відомості про технології збору та передачі інформації для об’єкта впровадження 12
1.4 Принципи, технічні способи та математичні методи інформаційного забезпечення для об’єкта впровадження 14
1.5 Огляд існуючих інженерних рішень для об’єкта впровадження у цій галузі 15
1.6 Завдання і мета роботи 17
1.7 Визначення можливих напрямків рішення поставлених завдань 17
2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП’ЮТЕРНОЇ СИСТЕМИ 20
2.1 ТЕХНІЧНІ ВИМОГИ ДО СИСТЕМИ 20
2.1.1 Вимоги до системи в цілому 20
2.1.2 Вимоги до функцій яка зобов'язана виконувати комп'ютерна система 22
2.1.3 Вимоги до видів забезпечення 23
2.2 Розробка апаратної частини комп’ютерної системи 26
2.2.1 Вибір і обґрунтування структурної схеми комплексу технічних засобів комп’ютерної системи 26
2.2.2 Розробка специфікації апаратних засобів КС 30
2.2.3 Розробка фізичної топологічної схеми корпоративної мережі 31
2.2.4 Розрахунок інтенсивності трафіку вихідного трафіку найбільшої локальної мережі підприємства 34
3 РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ 37
3.1 Розрахунок схеми адресації корпоративної мережі 37

3.2 Розробка топологічної схеми корпоративної мережі 39
3.3 Розрахунок налаштувань маршрутизації корпоративної мережі 41
3.4 Налаштування та перевірка роботи комп'ютерної системи 44
3.4.1 Базове налаштування конфігурації пристроїв 44
3.4.2 Налаштування маршрутизаторів корпоративної мережі 46
3.4.3 Налаштування роботи Інтернет 48
3.4.4 – Налаштування протоколу NAT 52
3.4.5 – Агрегування каналів 54
3.4.6 - Перевірка роботи комп'ютерної системи 57
3.5 Захист інформації в комп'ютерній системі від несанкціонованого доступу 62
3.5.1 Розробка методів для захисту інформації в комп'ютерній системі. 62
3.5.2 Налаштування мереж VLAN 62
3.5.3 Налаштування мережі VPN 68
3.5.4 Налаштування параметрів безпеки комутаторів 70
4 РОЗРОБКА СИСТЕМИ ІНТЕРНЕТУ РЕЧЕЙ 72
4.1 Аналіз засобів реалізації функцій пожежної системи засобами IoT 72
4.2 Аналіз засобів реалізації функцій автоматичного відкриття дверей засобами IoT 74
4.3 Аналіз засобів реалізації функцій регулювання температурою у кімнаті засобами IoT 75
4.4 Налаштування обладнання та сервісів системи IoT 77
ВИСНОВОК 82
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 84

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАК, ОДИНИЦЬ І ТЕРМІНІВ

КС - Комп'ютерна система

КМ - Комп'ютерна мережа

DHCP - Dynamic Host Configuration Protocol (англ) протокол динамічної конфігурації вузла

VLAN - Virtual Local Area Network (англ) віртуальна локальна комп'ютерна мережа

VPN - virtual private network (англ) віртуальна приватна мережа

IP-адреса - унікальний ідентифікатор комп'ютера локальної мережі

WAN - Wide Area Network (англ) глобальна мережа

SSH - Secure SHell (англ) безпечна оболонка мережевий протокол рівня застосунків віддаленого адміністрування

IoT - Internet of Things (англ) Інтернет речей, концепція мережі, що складається із взаємозв'язаних фізичних пристроїв

Cisco Packet Tracer - багатофункціональна програма моделювання мереж

Мережевий комутатор (свіч) - пристрій, призначений для з'єднання декількох вузлів комп'ютерної мережі в межах одного сегмента

Маршрутизатор (роутер) - електронний пристрій, що використовується для поєднання двох або більше мереж і керує процесом маршрутизації

NAT - Network Address Translation (англ) протокол перетворення мережевих адрес

EIGRP - Enhanced Interior Gateway Routing Protocol (англ) протокол маршрутизації, розроблений фірмою Cisco

ВСТУП

Впровадження та розвиток комп'ютерних систем в Україні розпочалося з 1990-х років. Вони впроваджувалися повсюдно як і державні підприємства, міністерства і у приватний сектор, малий, середній і крупний бізнес. Такий розвиток не міг не вплинути на туристичний бізнес. Більшість операцій в туристичному бізнесі здійснюється за допомогою інтернету: онлайн покупка квитків, оренда житла для відпочинку, автоматизація обслуговування клієнтів і так далі.

До 2010 було не так помітно впровадження комп'ютерних систем і повсюдної цифровізації, але з розвитком технологій і здешевленням виробництва на обладнання зробило доступним цифрові технології для всіх. Зараз практично будь-який бізнес чи державне підприємство не може обійтися без комп'ютерної мережі, додатку чи бази даних. Все, що зараз оточує людину, складається з комп'ютерних мереж, деякі міста регулюються мережами, навіть перемикання світлофорів у місті з урахуванням кількості автомобілів на дорозі може відбуватися за допомогою комп'ютерної мережі.

Комп'ютерна мережа це мережа підключених між собою комп'ютерів, комутаторів та маршрутизаторів. Вона дозволяє виходити у світовий інтернет, обмінюватися файлами, шукати співробітників, надсилати повідомлення та повідомлення. Комп'ютерна мережа збільшує продуктивність праці в десятки разів, без навичок поводження з комп'ютером зараз практично не можна влаштуватися на роботу.

Одне з основних завдань туристичної компанії – це запропонувати своїм клієнтам місця для відпочинку, покупка квитків, надання комфортного та дешевого житла на місці. Все це в наш час робиться за допомогою інтернету. Для цього туристичним компаніям часто потрібен IT персонал, а також розвинена комп'ютерна мережа. Найчастіше найрозвиненіші туристичні

компанії вдаються до автоматизації багатьох сфер своєї діяльності. Також можливе створення бази даних для обслуговування фірми, ведення бізнес-аналітики, економічних розрахунків, ведення звітів про роботу та розвиток фірми. За допомогою комп'ютерної мережі туристична компанія може знайти кваліфікований персонал, без чого створення та обслуговування мережі неможливе. Клієнти можуть відсилати відгуки про фірму, рекомендувати її у соціальних мережах.

Сучасні технології дозволяють навіть побудову топології, налаштування комп'ютерної мережі та її обслуговування оптимізувати та автоматизувати. Технічному персоналу тепер потрібно менше часу для налаштування мережі, з чого випливає, що їх можна розподілити в інші області бізнесу або скоротити.

У цій кваліфікаційній роботі розглядається проектування та розробка комп'ютерної мережі для туристичної фірми "Круїз".

1 СТАН ПИТАННЯ ТА ПОСТАНОВКА ЗАВДАННЯ

1.1 Характеристика та аналіз діяльності Туристичного Агентства

Туристичні компанії надають клієнтам послуги з внутрішнього та зовнішнього туризму. Клієнту допомагають вибрати спосіб переміщення до місця призначення і назад, вибрати житло у місці відпочинку, а також допомагають з необхідними документами та законами в зоні відпочинку, якщо це закордонний туризм.

Основні завдання перед Туристичним агентством:

- Надання клієнтам оптимальних путівок за матеріальними можливостями клієнта
- Допомога клієнту з переміщенням у місце відпочинку та назад
- Рекомендація щодо дозвілля клієнта у місці відпочинку
- Допомога з орендою житла у місці відпочинку
- Пояснення правил та заборон у місці проведення відпочинку
- Допомога у збиранні необхідних документів

В наш час туристичні агенції є дуже важливими для надання клієнтам послуг у сфері дозвілля та відпочинку. Люди можуть і самі відвідувати інші країни та дивитися пам'ятки, але за допомогою кваліфікованого персоналу туристичної агенції можна значно скоротити бюрократичний аспект відпочинку, у плані заповнення та отримання необхідних документів, що вкрай складно та важливо у всьому світі. Скоротити витрати на дозвілля та відпочинок, а також знайти цікавіші види рекреації, для оздоровлення або інших видів розваг у місці відпочинку.

1.2 Характеристика і структура об’єкта впровадження

Туристичне агентство круїз поділяється на кілька відділів із чіткою ієрархією. Частина відділів знаходиться у вигляді філій по всьому місту.

Філії це відділення агентства для надання послуг клієнтам, вони маю лише технічних фахівців, а також менеджера та співробітників для роботи з клієнтами.

Головний офіс має всі відділи, у вигляді відділу для роботи з фінансами та бухгалтерією, відділу кадрів, відділу охорони праці. Також у головному офісі є відділ технічних фахівців, що створюють, налаштовують та обслуговують комп'ютерну мережу та відділ для роботи з клієнтами.

Ієрархія Туристичного Агентства Круїз поділяється на: Директора компанії, який керує основними напрямками розвитку агенції, а також передає основне управління заступнику директора. Заступник директора також керує відділами у вигляді: відділу фінансів та бухгалтерії, відділу технічних фахівців та відділу для роботи з клієнтами.

Відділ фінансів та бухгалтерії ділиться на відділ кадрів та відділ охорони праці. Цим відділом керує завідувач відділу фінансів та бухгалтерії. Відділ займається прийомом працювати, дотриманням робочих норм, аналізом ринку праці, аналізом туристичного ринку, шукає спонсорів і акціонерів.

Відділом технічних спеціалістів управляє Головний Системний Інженер, який керує системними адміністраторами. Відділ займається створенням, налаштуванням та обслуговуванням комп'ютерної мережі, а також допомогою співробітникам для обслуговування клієнтів з роботою за комп'ютером та іншими системами.

Відділом роботи з клієнтами керує менеджер по роботі з клієнтами. Відділ обслуговує клієнтів, заповнює звіти щодо роботи та обслуговування клієнтів.

Організаційна структура агенції має лінійну структуру (рис. 1.1). Це багаторівнева система з чіткою ієрархією де керівну посаду займає Директор, а нижчі посади підпорядковуються своїм завідувачами відділів, які у свою чергу підпорядковуються заступнику директора, який підпорядкований директору компанії.

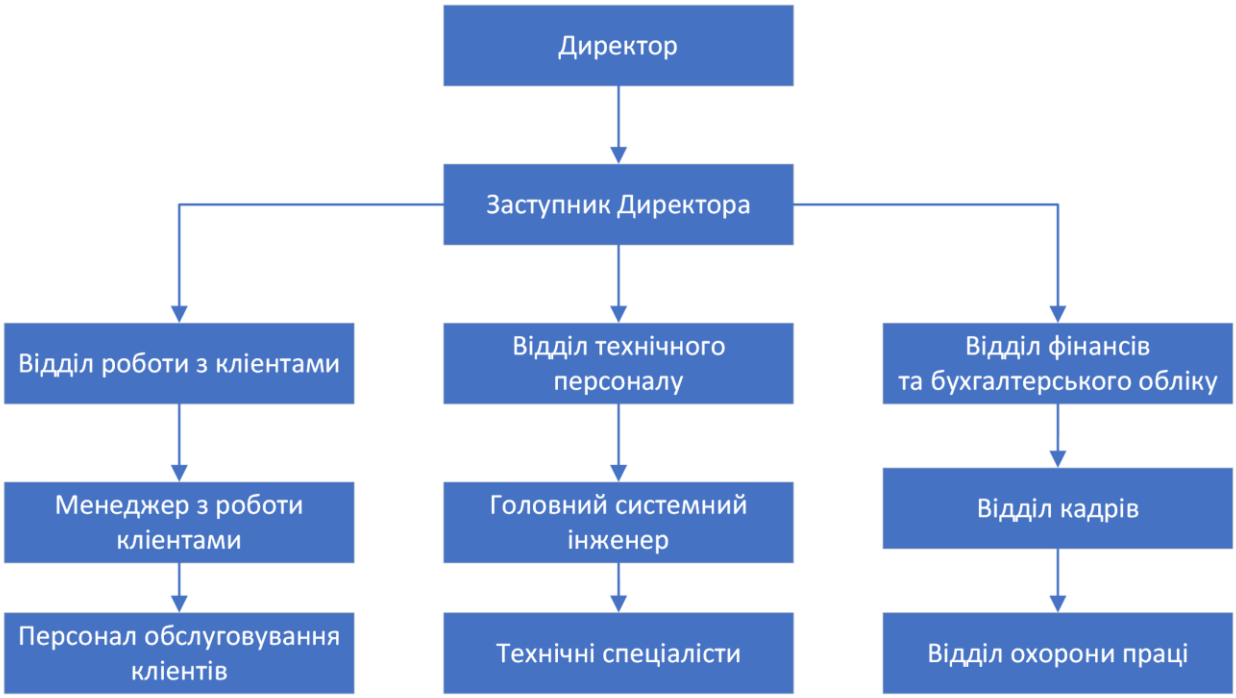

Рисунок 1.1 - Організаційна структура Туристичної Агенції Круїз

Послуги клієнтам компанії:

- Туризм по Україні
- Екскурсії по Україні
- Туризм у різні країни
- Оренда житла на певний термін у країні призначення
- Оренда житла на певний термін по Україні
- Купівля квитків до дивного призначення
- Купівля квитків для пересування по Україні

Для розробки проекту комп'ютерної системи для туристичної компанії "Круїз" з використанням сучасних мережевих технологій потрібно проаналізувати структурні підрозділи компанії, які будуть об'єднані в комп'ютерну мережу. Комп'ютерна мережа розробляється з реальними потребами компанії, для оптимізації роботи відділів та поліпшення робочих умов співробітників та клієнтів.

1.3 Стислі відомості про технології збору та передачі інформації для об’єкта впровадження

У цій кваліфікаційній роботі була побудована сучасна комп'ютерна мережа, яка включає великий перелік обгородження. Серед них: комп'ютери, маршрутизатори, комутатори, сервери, кабелі. Обладнання мешкає цілям структурування та обміну інформації в даній комп'ютерній мережі. Все обладнання відповідає усім вимогам інформаційної безпеки.

До обов'язку від співробітників агентства лежить збір інформації про клієнтів і роботу компанії. Вся отримана інформація структурується у побудованій комп'ютерній мережі. Це полегшує роботу багатьох відділів та оптимізує їхню роботу.

Збір інформації здійснюється за допомогою спеціалізованих для цього інструментів, таких як клавіатура та сканер. Вся інформація, що збирається цими способами, далі обробляється технічними фахівцями у форму зручної для комп'ютерної обробки.

Для конфіденційної інформації про клієнтів та співробітників компанії вживаються всі заходи безпеки, щоб не допустити її витоку. У роботі з конфіденційною інформацією про клієнтів дуже важливо забезпечити її безпеку. І тому здійснюється різні способи обмеження доступу до даних.

Головний офіс туристичної агенції Круїз знаходиться за адресою: м.Дніпро, вул.Пушкіна 15б. (Рис. 1.2)

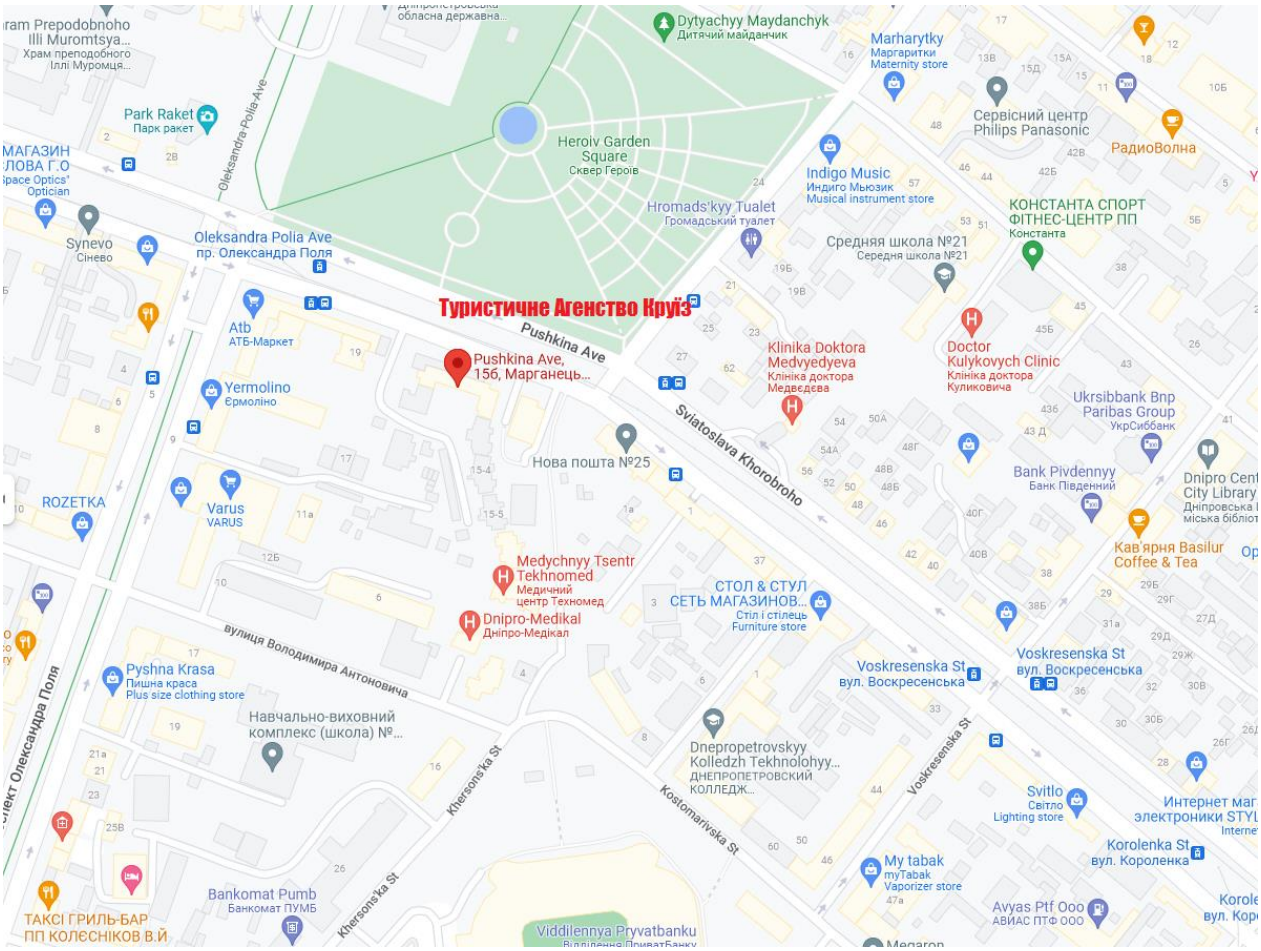

Рисунок 1.2 − Топографічна схема об’єкта впровадження

У цій локальній мережі об'єднано безліч комп'ютерів та периферійних пристроїв. Це дозволяє робити такі речі як:

- Мати доступ до інтернету
- Працювати із спільними корпоративними файлами
- Обмінюватися файлами
- Мати більш простий доступ до периферійних пристроїв, таких як принтер
- Надавати клієнтам наочні приклади для туризму

Усі комп'ютери та периферійні пристрої об'єднані у загальну комп'ютерну мережу розташовану у фізичному місці. Це дозволяє полегшити створення та підтримку такої мережі для системних адміністраторів.

1.4 Принципи, технічні способи та математичні методи інформаційного забезпечення для об’єкта впровадження

Хорошим фундаментом для стабільного утримування ринку, хорошого функціонування компанії і якісного обслуговування клієнтів є надійна мережева інфраструктура.

Для цього використовується серверне обладнання, маршрутизатори, комутатори та кабелі, що з'єднують все обладнання. Види кабелів бувають різні, для різних цілей, з різними показниками пропускної спроможності.

Для підключення внутрішніх пристроїв до комп'ютерної мережі використовуються кабелі типу Fast Ethernet, ще він називається вита пара. Ці кабелі з'єднують комп'ютери та серверне обладнання співробітників агенції та проходять усередині захищеної пластикової оболонки, яка захищає кабель від зовнішніх загроз у вигляді сонячного світла, фізичних ушкоджень тощо. Максимальна швидкість такого способу підключення становить 100 мегабайт на секунду.

Також використовується кабель типу оптоволокна. Він має більш високі показники пропускної спроможності кабелю, від 1 гігабайта на секунду до 40-50 гігабайт на секунду. Такий тип підключення використовується для з'єднання філій компанії, далеких офісів. Через особливості даного виду кабелю та іншої структури передачі даних, кабель може мати більшу довжину, що і дозволяє його використовувати як спосіб підключення ззовні комп'ютерної мережі.

1.5 Огляд існуючих інженерних рішень для об’єкта впровадження у цій галузі

Наприклад, використання існуючих рішень є мережа для невеликого офісу від компанії Computer Success[2]. Компанія створює комп'ютерні мережі для невеликих офісів, компаній, а також маленьких приватних підприємств.

Звичайний приклад побудови сучасної комп'ютерної мережі складається з маршрутизатора з доступу у світову мережу інтернет, маршрутизаторів підключений до основного маршрутизатора з доступу в інтернет, комутаторів, які підключені до маршрутизатора і периферійне, серверне обладнання з підключенням до комутатора(рис. 1.3).

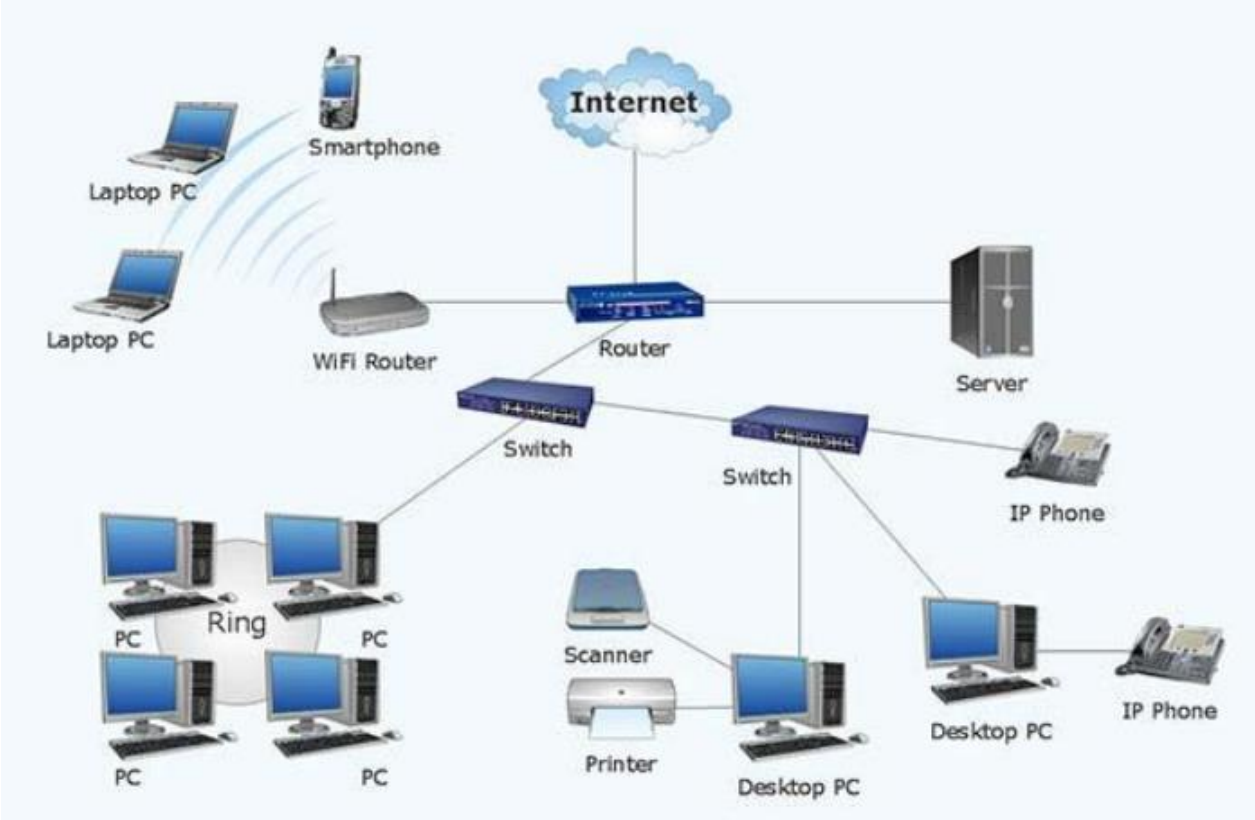

Рисунок 1.3 – Приклад побудови мережі від компанії Computer Success

Такий спосіб побудови комп'ютерної мережі дозволяє скоротити витрати на створення обслуговування мережі, а так само полегшити її налаштування.

Комп'ютерні мережі подібних видів легко настроюються і масштабуються. Вони підходять як для великих корпорацій з великою кількістю комп'ютерів, серверів та інших периферійних пристроїв, так і дрібним фірмам з малою кількістю обладнання.

Такий спосіб побудови мережі дозволяє зробити таку мережу безпечною, за допомогою налаштування доступу до комутаторів і маршрутизаторів можна повністю виключити зовнішнє втручання в роботу мережі, а також забезпечити безпеку конфіденційних даних як клієнтів так і співробітників компанії.

У прикладі інженерного рішення можна взяти туристичну компанію у місті Дніпро на вулиці Короленка 18 – Туристична Агенція "ДаріТур" (рис. 1.4). Воно складається із одноповерхової будівлі з коридором, 4 кімнатами. У 3-х кімнатах розташована велика кількість комп'ютерів та серверів для ведення фінансів, бухгалтерії та планування. У центральному залі розташовані місця обслуговування клієнтів і точкою бездротового підключення до інтернет мережі.

Така мережа зберігає високу пропускну здатність, легко масштабована, а також надійно захищена.

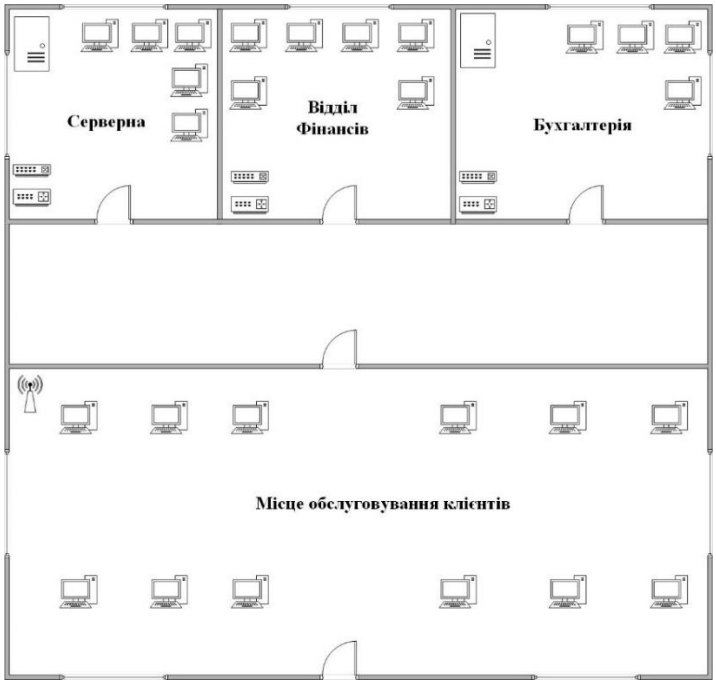

Рисунок 1.4 - Схема розведення мережі Туристичної Агенції "ДаріТур"

1.6 Завдання і мета роботи

У цій кваліфікаційній роботі основне завдання складається із побудови локальної комп'ютерної мережі для Туристичної Агенції Круїз.

За допомогою головного завдання кваліфікаційної роботи з метою його виконання були поставлені завдання, такі як:

- аналіз сучасних методів побудови мережі
- проектування комп'ютерної мережі відповідно до завдання кваліфікаційної роботи
- розрахунок адресацій за допомогою методу VLSM
- базове налаштування мережевого обладнання, таких як маршрутизатор та комутатор
- настроєна автоматична видача IP адрес для комп'ютерів у локальних мережах за допомогою технології DHCP
- налаштовано NAT підключення
- налаштовано безпечне VPN підключення між локальною мережею та віддаленою мережею
- налаштовані HTML та DNS сервери

Все проектування, налаштування та перевірка комп'ютерної мережі було вироблено у програмі Cisco Packet Tracer з обладнання доступним у цій програмі.

1.7 Визначення можливих напрямків рішення поставлених завдань

Най логічне для вирішення поставленого завдання це використовувати рішення від компанії Cisco. Ця компанія є світовим лідером на ринку мережевого обладнання та їх рішень.

Для швидкого переходу туристичної компанії "Круїз" на нові технології можна використовувати рішення Cisco DNA[11]. Ця технологія комплексне рішення, яке дозволяє переводити дані мережевого трафіку, в аналітику. Вона допомагає оперативне приймати бізнес-рішення, мінімізувати загрози, а так само швидко і легко керувати великою кількістю підключених пристроїв і серверів.

Основні особливості цього рішення:

- Прискорення роботи – Ініціалізація кількох тисяч пристроїв у корпоративному середовищі. Централізоване керування для оперативних дій. Автоматизація розгортання пристроїв.
- Зниження витрат - Скорочення числа помилок за рахунок автоматизації. Розгортання та адаптація на основі політик збільшують час безвідмовної роботи та підвищують безпеку.
- Зниження ризиків – завчасне прогнозування проблем. Використання цінної аналітичної інформації для забезпечення оптимальної продуктивності мережі, пристроїв та програм.

Для кожного відділу та їх підмережі логічна використати технологію віртуальної локальної мережі VLAN. Оскільки до цих підрозділів входять різні відділення та співробітники.

Для захисту комп'ютерної мережі між сайтами та співробітниками можна використовувати технологію VPN. Мережа з цією технологією буде приватною оскільки кожен трафік у ній буде шифруватися для конфіденційності даних при передачі їх через основну мережу.

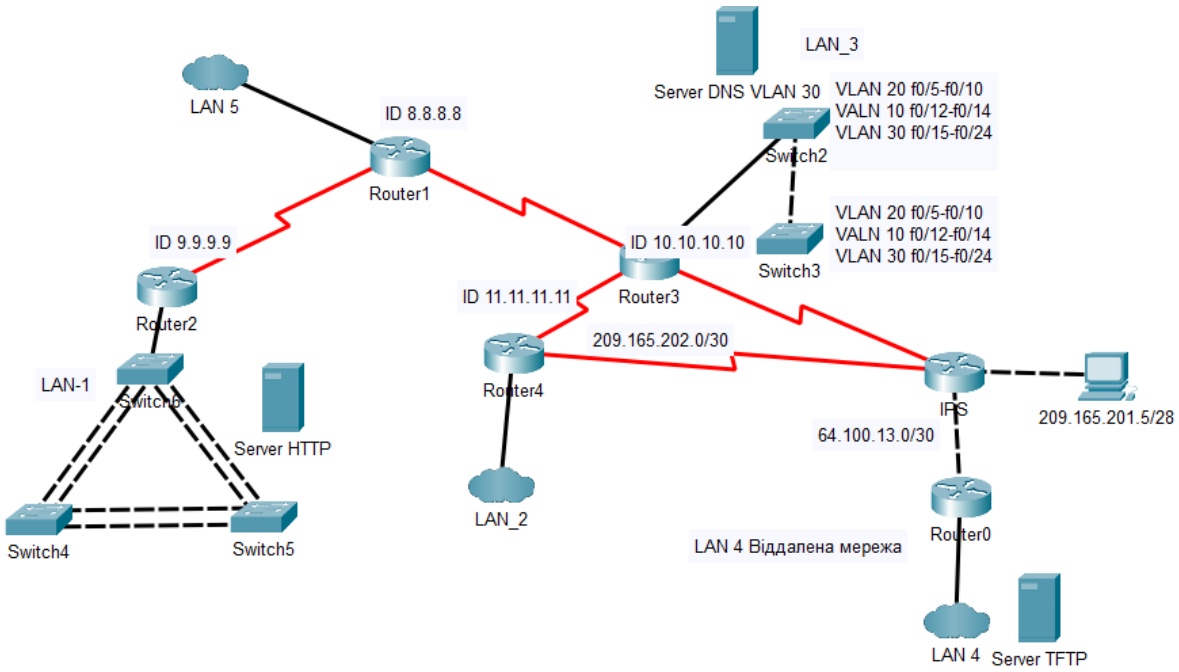

Рисунок 1.5 - − Загальна топологія мережі Туристичного Агентства Круїз

Для виконання кваліфікаційної роботи було використано програму Cisco Packet Tracer. Вона дозволяє проектувати та розробляти комп'ютерні мережі та проводити їх тестування.

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП’ЮТЕРНОЇ СИСТЕМИ

2.1 ТЕХНІЧНІ ВИМОГИ ДО СИСТЕМИ

2.1.1 Вимоги до системи в цілому

2.1.1.1 Вимоги до структури і функціонування системи

Для створення сучасної комп'ютерної мережі, мережа повинна виконувати безліч функцій, такі як обмін файлами, створення баз даних, вихід в інтернеті, архівація робота з голосовими помічниками, тощо у розмірах глобальної та локальної мережі.

Згідно з ієрархічною та організаційною структурою компанії, комп'ютерна мережа буде створена на базі п'яти локальних підсистем:

- локальна підсистема для технічного персоналу та серверного обладнання
- локальна підсистема для обслуговування клієнтів
- локальна підсистема для відділу фінансів та бухгалтерії
- локальна підсистема для відділу кадрів
- локальна підсистема для відділу охорони праці
- віддалена локальна підсистема для філій

Кожна з цих локальних підсистем повинна мати зв'язок між усіма іншими підсистемами, а також мати можливість виходу до міжнародної мережі інтернет. Відповідно до завдання кваліфікаційної роботи підсистеми повинні мати задану кількість доступних IP адрес: LAN1 – 74 IP адрес, LAN2 – 17 IP адрес, LAN3 – 90 IP адрес, LAN4 – 241 IP адрес, LAN5 – 99 IP адрес.

Для локальної підсистеми відділу фінансів та бухгалтерії розумно буде розбиття системи на кілька VLAN, щоб створити як більш захищену систему, так і відокремити одні відділи від інших.

2.1.1.2 Показники призначення

Все обладнання в комп'ютерній мережі має відповідати всім вимогам щодо безпеки, продуктивності та ліцензійної угоди. Обладнання має бути надійним при використанні та мати ККД відповідно до їх технічних характеристик, які були вказані виробником.

2.1.1.3 Вимоги до патентної чистоти

Патентна чистота - це юридична особливість, яка дозволяє вільно користуватися об'єктом інтелектуальної власності в країні знаходження цього об'єкта без порушення місцевих законів про інтелектуальну власність[12].

Кожне обладнання або програмне забезпечення комп'ютерної мережі має відповідати всім вимогам патентної чистоти, щоб компанія не зазнала збитків у випадку, якщо було порушено інтелектуальну власність або місцеві закони.

Для цього слід купувати обладнання в зареєстрованих та спеціалізованих магазинах які або я є представниками або безпосередньо мають відношення до виробника мережевого обладнання. Все програмне забезпечення має бути представлене як ліцензійне забезпечення, для дрібних компаній або просто для зниження витрат на програмне забезпечення можна використовувати програмні системи з відкритим вихідним кодом і ліцензії GNU або MIT.

Для комп'ютерних систем слід за основу патентної чистоти брати закони інтелектуальної власності США та країни Європейського Союзу та Китаю.

2.1.1.4 Додаткові вимоги

До додаткових вимог до побудови комп'ютерної системи слід віднести такі речі як:

- Знаходження кабелів у спеціальних кабель-каналах, які захищають їх від сонячного випромінювання, вологи та фізичних пошкоджень
- Сервери повинні розташовуватися в приміщенні, яке має рівень вологості відповідно до технічних вимог від виробника, а так само приміщення має бути обладнане кондиціонерами для запобігання перегріву обладнання.
- Кабелі повинні з'єднатися в спеціальних коробах, що дозволяє запобігти незапланованому розриву мережі
- Все обладнання повинно мати на 10 відсотків більше запасних портів для можливості підтримки та розширення мережі без додаткових витрат на нове мережне обладнання

2.1.2 Вимоги до функцій яка зобов'язана виконувати комп'ютерна система

При розробці комп'ютерної системи необхідно враховувати всі вимоги до функцій, які повинна виконувати система.

Основні вимоги до працездатності комп'ютерної мережі:

- швидкість відгуку на запити користувача
- швидкість передачі даних
- конфіденційність
- надійність

Основні вимоги до функціоналу комп'ютерної мережі:

- збір даних про клієнтів
- збір даних про співробітників
- зберігання баз даних
- доступ до міжнародної мережі інтернет

– обмін даними між співробітниками
– доступ до спільних файлів

Комп'ютерна система повинна працювати безперебійно та надати всі необхідні функції для компанії. Система має бути оснащена необхідним для функціонування програмним забезпеченням, платним або вільним вихідним кодом.

2.1.3 Вимоги до видів забезпечення

2.1.3.1 Вимоги до інформаційного забезпечення

Комп'ютерна система дозволяє користувачам без перешкод обмінюватися файлами, спільно їх редагувати та переглядати. Для цього використовуються сервери, які можуть бути розташовані як в одному місці, так і в декількох місцях однієї і тієї ж локальної комп'ютерної мережі. Так само для співробітників туристичного агентства важливий вихід у глобальну мережу інтернет, для обслуговування клієнтів.

Система яка була зроблена в кваліфікаційній роботі складається з локальної комп'ютерної мережі, з декількома підсистемами, а так само віддаленої локальної мережі, яка виконує функцію філії.

Головний офіс туристичної агенції розташований за адресою м.Дніпро вул.Пушкіна 15б. А філія розташована за адресою м.Дніпро вул.Набережна Перемоги 61а. Між головним офісом і філією також має бути вільний обмін файлами, конфіденційність переданої та отриманої інформації, а також вихід в інтернет.

Для забезпечення безпеки системи зазвичай можна використовувати вбудовані в деякі операційні системи функції захисту або ж перейти до тих операційних систем, що менш схильні до зламів такі як Linux та FreeBSD. Так

само ці системи більш надійні з погляду працездатності, вони безкоштовні і позбавлені багатьох вразливостей як у Windows. Їх головним недоліком є відсутність багато важливого програмного забезпечення.

2.1.3.2 Вимоги до програмного забезпечення

Для роботи в туристичній агенції співробітникам які обслуговують клієнтів необхідно мати програмне забезпечення, яке дозволяє виходити в інтернет, писати текстові документи, а так само інше програмне забезпечення, яке необхідно туристичній агенції.

Для забезпечення безпеки конфіденційної інформації клієнтів та співробітників у кожному устаткуванні повинна стояти система, що запобігає несанаційному доступу. Це можна досягти шляхом призначення введення логіну та пароля на пристрій. Логін повинен відповідати імені та прізвища співробітника, а також його спеціальність та відділ у даній компанії, пароль має бути виданий технічним фахівцем.

Доступ до серверів, комутаторів та маршрутизаторів повинен бути жорстко контролювати, мати привілей суперкористувача повинні лише системні адміністратори та інший технічний персонал для обслуговування системи.

Доступ до файлів, баз даних повинні мати лише співробітники, яким необхідно мати доступ до такої інформації і лише вони і технічний персонал повинні мати можливість її змінювати.

Для роботи з текстовими документами, основним завданням будь-якого відділу, можна використовувати пакет офісних програм від Microsoft – Microsoft Office. Також можна використовувати безкоштовний аналог з вільним вихідним кодом, такий як Libre Office, його головна перевага, це

кроссплатформенність і безкоштовність, що дозволяє його використовувати на будь-яких системах з будь-якою операційною системою.

Кожен комп'ютер у цій системі має бути забезпечений даними програмами, що наведені нижче у таблиці 2.1.

Таблиця 2.1 - Програмне забезпечення Туристичного Агентства Круїз

Тип програмного забезпечення	Назва
Операційна система	Fedora Linux
ПЗ для роботи з документами	Libre Office
ПЗ для роботи з базами даних	OpenOffice Linux
ПЗ для роботи з pdf-файлами	Mozila Firefox
ПЗ для роботи з веб-сторінками	Mozilla Firefox
Інше Програмне забезпечення	Python

Операційна система для маршрутизаторів та комутаторів це Cisco IOS. Вона забезпечує як безпеку системи, так і можливість зручного її налаштування. Вона дозволяє створити та забезпечувати комп'ютерну мережу, що відповідатиме всім вимогам для її функціонування. Усі команди для налаштування цієї операційної системи можна знайти на сайті виробника з детальним описом. Також вона дозволяє створювати рівні доступу до налаштувань для користувача, що забезпечує безпеку.

2.1.3.3 Вимоги до надійності системи

Комп'ютерна система повинна мати можливість створення, зберігання та відновлення за допомогою резервних копій. Для збереження конфіденційних даних клієнтів та співробітників слід забезпечувати все обладнання запасними

джерелами електроенергії, такими як безперебійне джерело живлення, що дозволяє у разі стрибків напруги або відключення підтримати роботу системи до моменту збереження та безпечного вимкнення.

Для окремих локальних підсистем можуть бути свої вимоги для надійності системи.

2.1.3.4 Вимоги до чисельності та кваліфікації персоналу

Головний офіс Туристичної Агенції Круїз має забезпечувати безперебійну роботу від 50 до 100 працівників. Технічний персонал повинен мати всі навички для створення та підтримки комп'ютерної системи, повинен мати вищу професійну освіту за спеціальністю комп'ютерна інженерія. Чисельність технічного персоналу становить 10 осіб.

2.2 Розробка апаратної частини комп’ютерної системи

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

Комп'ютерна система для Туристичного Агентства Круїз представлена у вигляді хостів у локальних підсистемах, які сусіди між собою комутаторами та маршрутизаторами. Система характеризує собою мережеве обладнання, яке є функціональною комп'ютерною мережею для Туристичного Агентства Круїз. Система спеціально спроектована та розроблена для функціонування Туристичної Агенції.

Центральна частина комп'ютерної мережі це маршрутизатори, які пов'язані між собою. Маршрутизатори Kyrychenko_RT1-4 є точки для зв'язку локальних підсистем, а також як маршрутизатори для надання хостам IP адрес.

Маршрутизатор Kyrychenko_IPS є як вихід в інтернет мережу. Маршрутизатор Kyrychenko_RT5 це точка доступу до віддаленої локальної мережі.

Зв'язок між маршрутизаторами здійснюється за допомогою Serial протоколу. Він дозволяє швидко передавати велику кількість даних між роутерами.

Зв'язок між маршрутизатором та комутатором здійснюється за допомогою Gigabit Ethernet протоколу. Він дозволяє передавати велику кількість даних між двома або більшими пристроями без втрати даних.

Зв'язок між хостом та комутатором здійснюється за допомогою Fast Ethernet протоколу. Цей протокол має обмеження в 100 мегабайт на секунду, але цього достатньо для користування комп'ютерною системою, обміну файлами, а також для виходу в інтернет.

Звичайна локальна підсистема містить один маршрутизатор як точку доступу та спосіб видачі IP адрес за допомогою технології DHCP, один комутатор для підключення до нього кінцевих хостів.

Локальна підсистема LAN1 має три комутатори, пов'язані між собою за допомогою технології агрегування каналів, що дозволяє забезпечити мережу від виходу з ладу одного з кабелів, що з'єднують між собою комутатори.

Локальна підсистема LAN3 має два комутатори, які пов'язані між собою, а також вони розділені на окремі VLAN, для забезпечення безпеки, а також для апаратного поділу підсистеми на ще менші підсистеми для функціонування різних відділів компанії.

На рисунку 2.1 наведена структурна схема комплексу технічних засобів комп’ютерної системи Туристичного Агентства Круїз.

На рисунку(Рис. 2.2) показана схема першого поверху будівлі в якому розташовується Туристичне Агентство Круїз, на ньому також зображено схематичне розташування обладнання комп'ютерної системи такі як

комп'ютери, сервери, комутатори і маршрутизатори, а також назва приміщення і відділів розташованих в них. Кабінет директора та заступника директора розташований у відділі бухгалтерії та фінансів, а відділ охорони праці не має виходу в коридор і до нього потрібно заходити з відділу бухгалтерії та фінансів.

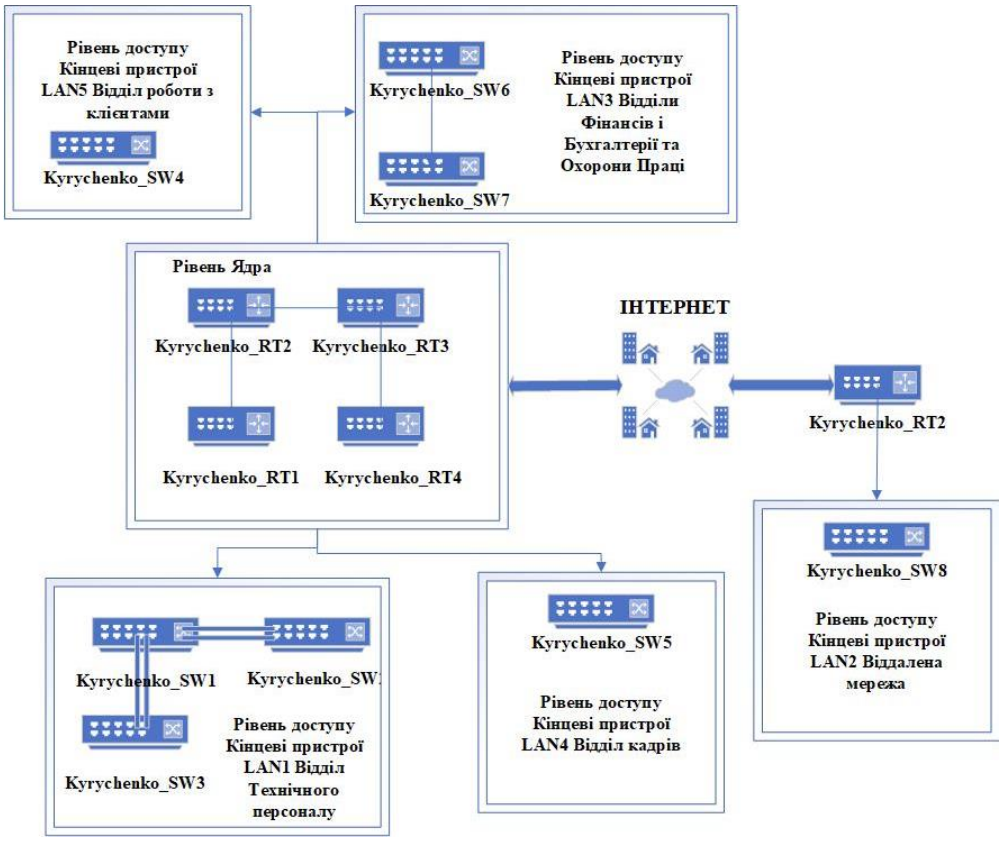

Рисунок 2.1 - Структурна схема комплексу технічних засобів комп’ютерної системи

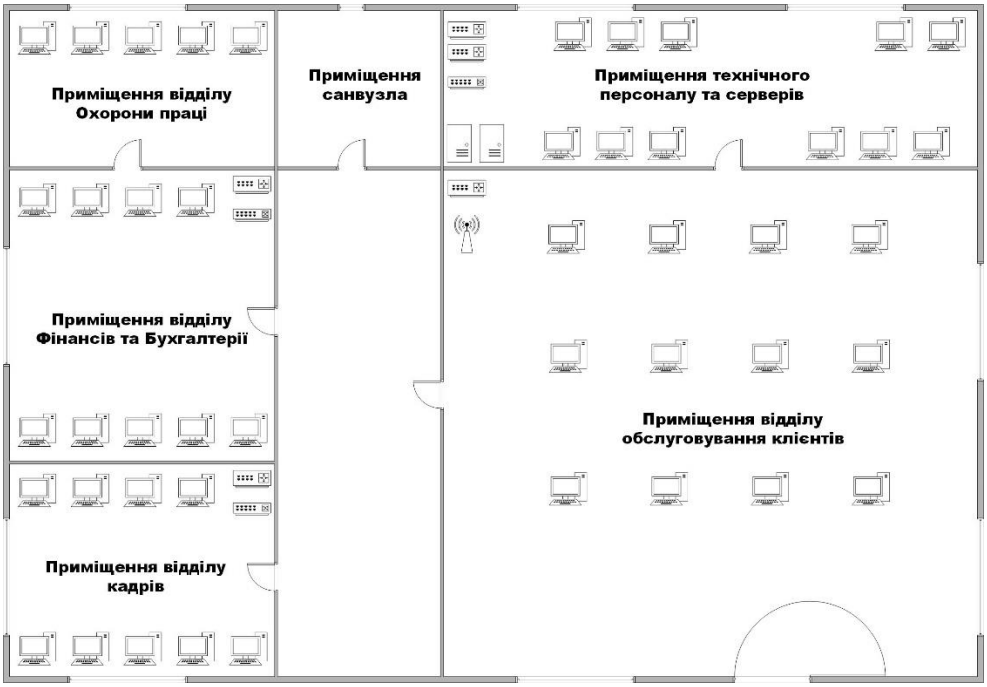

Рисунок 2.2 - Схема будівлі в якому розташована туристична агенція круїз з елементами комп'ютерної мережі

У таблиці 2.2 представлено обладнання та його кількість згідно з ієрархічною та організаційною структурою Туристичної Агенції Круїз. Воно узгодить між собою робочі місця співробітників та технічного персоналу компанії.

Таблиця 2.2 - Типи пристроїв та їх кількості згідно з організаційною структурою підприємства

Відділ	Ідентифікатор	Тип	Посада	Кількість
Відділ фінансів та бухгалтерії	PC0	PC	Директор	1
	PC34	PC	Заступник директора	1
	PC1	PC	Начальник відділу фінансів та бухгалтерії	1
	PC35-40	PC	Бухгалтера	5
	PC40-45	PC	Фінансисти	5
	Server_DNS	Server	---	1
Відділ охорони праці	PC53	PC	Начальник відділу охорони праці	1

	PC54-57	PC	Співробітники відділу охорони праці	4
Відділ кадрів	PC28	PC	Начальник відділу кадрів	1
	PC29-33	PC	Співробітники відділу кадрів	4
Відділ технічного персоналу	PC19	PC	Головний інженер відділу технічного персоналу	1
	PC12-22	PC	Системні адміністратори	10
	Server_HTTP	Server	---	1
Відділ роботи з клієнтами	PC8	PC	Головний менеджер відділу роботи з клієнтами	1
	PC10-60	PC	Менеджери для роботи з клієнтами	50

Продовження таблиці 2.1

Філія	PC31	PC	Начальник філії	1
	PC32-52	PC	Менеджери для роботи з клієнтами	20

2.2.2 Розробка специфікації апаратних засобів КС

Згідно з технологіями для створення комп'ютерної мережі та її функціонування потрібно мати комутатор для надання виходу в комп'ютерну мережу для кінцевих хостів, і маршрутизатор для об'єднання локальних мереж в комп'ютерну мережу.

Пристрої які були використані та їх технічні характеристики наведені нижче:

Комутатор Cisco 2960 - комутатори даної лінійки дозволяють легко масштабувати корінну мережу відповідно до потреб бізнесу, вони хороші для невеликих компаній, а також для віддалених локальних підсистем. Вони

дозволяють убезпечити комп'ютерну мережу за допомогою створення списку доступу, для поліпшення продуктивності мережі у них є можливість регулювання швидкості передачі, так само вони підтримують можливість створення транкових з'єднань. Загальна кількість портів – 24 на технології Fast Ethernet[3].

Маршрутизатор Cisco 4331 - це лінійка маршрутизаторів Cisco з модулями NIM, що розширюються, що дозволяє легко збільшити необхідну кількість портів. Стандартна вбудована кількість портів 3 з технологією Gigabit Ethernet від 50 мегабайт на секунду до 2 гігабайт на секунду дозволяє легко користуватися комп'ютерною мережею без втрати даних. Вбудована прошивка від Cisco дозволяє легко налаштовувати роботу маршрутизатора та загалом комп'ютерної мережі, що прискорює розгортання мережі у бізнесі[4].

Таблиця 2.2 - Специфікація обладнання

Позиція	**Найменування і тех. характеристика**	**Тип, марка, позначення документа**	**Одиниці виміру**	**Кількість**
1	Cisco WS-C2960-24-S, 24 Ethernet 10/100 ports, LAN Lite Software	Kyrychenko_SW1 Kyrychenko_SW2 Kyrychenko_SW3 Kyrychenko_SW4 Kyrychenko_SW5 Kyrychenko_SW6 Kyrychenko_SW7 Kyrychenko_SW8	Шт.	8
2	ISR4331-AX/K9, 3 x Gigabit Ethernet, NIM, 10/100/1000Base-T, 1000Base-X	Kyrychenko_RT1 Kyrychenko_RT2 Kyrychenko_RT3 Kyrychenko_RT4 Kyrychenko_RT5 Kyrychenko_RT6	Шт.	6

2.2.3 Розробка фізичної топологічної схеми корпоративної мережі

Система представлена в даній кваліфікаційній роботі досить мала, так що був використаний ієрархічний спосіб побудови комп'ютерної мережі з двома рівнями. Рівнем кінцевих пристроїв – хостів, та рівнем мережевого обладнання – маршрутизаторів та комутаторів.

При розробці моделі архітектури мережі необхідно враховувати деякі важливі моменти побудови, такі як:

- топологія комп'ютерної мережі
- мережеве та серверне обладнання
- мережеві технології та протоколи
- кабельні маршрути

В ядрі комп'ютерної мережі стоять 6 маршрутизаторів, один з яких відповідає за вихід в інтернет і зв'язок з віддаленою локальною підсистемою, і ще один є точкою доступу в віддалену підсистему. У проекті кваліфікаційної роботи використовується технологія IP адресації четвертої вертії. Комп'ютерна система розділена на 5 окремих локальних підсистем, одна з яких є віддаленою філією. Всі підсистеми пов'язані між собою за допомогою комутаторів та маршрутизаторів. Для цього адреса IP:10.22.192.0/21 розбивається за допомогою технології розбиття адреси IP на окремі підсистеми VLSM. Для виходу в інтернет на кінцевих маршрутизаторах було застосовано технологію NAT.

Маршрутизатор Kyrychenko_RT3 що знаходиться у відділі бухгалтерії та фінансів використовує технологію інкапсуляції dot 802 1Q для надання IP адрес за допомогою технології DHCP кінцевим пристроям, які були розділені VLAN, це дозволяє кожному окремому VLAN використовувати власний блок IP адрес. Для зв'язку між маршрутизаторами було використано технологію EGRP що дозволяє проводити динамічну маршрутизацію між пристроями без

ручного налаштування кожного окремого маршруту. Маршрутизатор Kyrychenko_IPS розташований у відділі технічних фахівців дозволяє виходити комп'ютерній системі в глобальну мережу інтернет. Для цього в кінцевих маршрутизаторах Kyrychenko_RT3 -–Kyrychenko_RT4, пов'язаних з ним, були налаштовані на використанні технології NAT.

Комп'ютерна система поділена на п'ять локальних повдсистем згідно з ієрахічною та організаційною структурою підприємства та заданою функцією цього підприємства.

Локальна підсистема LAN1 для відділу технічного персоналу складається з пов'язаних між собою комп'ютерів за допомогою технології агрегування каналів для надання безпеки підключення у разі втрати одного з портів або кабелю, а також для високої швидкості передачі даних, має при собі сервер для надання сайту клієнтам. Також у цій підсистемі є комп'ютери для технічного персоналу, в ній присутні маршрутизатори для зв'язку з іншими підсистемами і маршрутизатори для виходу в інтернет.

Локальна підсистема LAN2 для відділу кадрів має комп'ютери пов'язані між собою комутатором, а так само маршрутизатор налаштований з використанням технології VPN для надання доповненої безпеки для зв'язку з локальною підсистемою LAN4.

Локальна підсистема LAN3 для відділу бухгалтерії та фінансів, а також для відділу охорони праці представлена двома комутаторами, маршрутизатором та комп'ютерами. У цій підсистемі налаштована технологія VLAN для виділення підсистеми на окремі мережі для розмежування та безпеки. Також у цій підсистемі є сервер DNS, який відповідає за зміни IP адреси сайту на посилання. На маршрутезаторі була налаштована технологія - dot 802 1Q для взаємопов'язаного виділення адрес між підсистемами VLAN.

Також між комутаторами цієї підсистеми було налаштовано транковий канал для правильного функціонування технології DHCP.

Локальна підсистема LAN44 є підсистемою для віддаленої мережі філії компанії, з комутатором і маршрутизатором на якому налаштована технологія VPN для безпечної передачі даних біжу цією підсистемою і LAN2. Також у цій підсистемі є кінцеві хости у вигляді комп'ютерів та інших периферійних пристроїв.

Локальна підсистема 5 для відділу роботи з клієнтами має велику кількість налаштованих кінцевих хостів комп'ютерів, а також великий ліміт вільних IP адрес для клієнтів.

2.2.4 Розрахунок інтенсивності трафіку вихідного трафіку найбільшої локальної мережі підприємства

Під час розрахунку характеристик вхідного трафіку потрібно, щоб комп'ютерна мережа Туристичної Агенції та її підсистем була завантажена на всі 100%. Після цього ми маємо такі значення як:

- найбільша кількість вузлів – 241
- середній показник інтенсивності трафіку: $\mu = 117$(кадрів/с)
- розмір повідомлення в середньому: 650 байт
- передача пакету не повинна перевищувати ≤ 5 мс

Для такої кількості вузлів було взято маршрутизатори Cisco ISR4331 і комутатори Cisco 2960. Після того як трафік виходить з комп'ютера користувача від перенаправляється на маршрутизатор зі швидкістю 1000 Мбіт/с.

Під час розрахунків пропускна здатність комп'ютерної мережі враховується, що зараз використовуються всі 100% пристроїв користувачів.

Пропускна здатність комп'ютерної мережі на рівні доступу обчислюється таким чином:

$$Рр.д=\mu*l*n*8=117*650*24*8=\ 14{,}6\ Мбіт/с$$

де n- кількість портів в комутаторі рівня доступу.

На рівні розподілу пропускна спроможність мережі розраховується так, потрібно порахувати максимальну кількість комутаторів на рівні розподілу та загальну чисельність користувачів. Після цього можна обчислити пропускну здатність за допомогою формули нижче:

$$P_{р.р}=\ \mu*l*N*8=117*650*241*8=\ 146{,}6\ Мбіт/с$$

N – кількість вузлів в найбільшій мережі.

Після обчислень видно, що результати не переважують параметри комп'ютерної мережі, з чого випливає, що навантаження на обраній ділянці мережі не буде.

Загальне навантаження на комутатор не повинно перевищувати:

$$\mu_{вих}=1\ 000\ 000\ 000/(650*8)=\ 192\ 307\ пакетів/с.$$

Кожне джерело генерує десь 117 пакетів/с, то обмеження на приєднанням до комутатора рівня розподілу становить:

$$N=192\ 307\ /\ 117=1643\ джерел$$

Це заповнює мережу з 241 ПК.

Далі кожен з 241 ПК посилає потік пакетів з інтенсивністю до 117 кадрів/с.

Інтенсивність вихідного трафіку всіх співробітників становить:

$$\lambda = N * \ \mu = 241*117=28197\ (пакетів/с);$$

Далі потрібно розрахувати коефіцієнт затримки на рівні розподілу, це показник того як завантажене вихід каналу зв’язку, який впливає на час очікування в черзі, це можна зробити за формулою нижче:

$$\rho = \frac{\lambda}{\mu_{вих}} = \frac{28197}{192307} = 0.15$$

Коефіцієнт зайнятості комутатора рівня розподілу розраховується за формулою нижче:

$$r = \frac{\rho}{1-\rho} = \frac{0,15}{1-0,15} = 0.18$$

Середня затримка кадру, пов'язана з чергою M/M/1, розраховується за формулою нижче:

$$T = \frac{1}{(\mu - \lambda)} = \frac{1}{192\,307\ - 28197} = 6.09 \text{ мкс}$$

Середня довжина черги розраховується за формулою нижче:

$$\mathcal{L}_{чер} = \frac{\rho^2}{1-\rho} = \frac{0,15^2}{1-0,15} = 0.026$$

З цього слідує, що середня довжина черзі працює менше ніж 1 пакету, це означає що система працює з запасом по продуктивності мережі.

Середній час перебування пакета в черзі розраховується за формулою нижче:

$$T_{чер} = \frac{\mathcal{L}_{чер}}{\lambda} = \frac{0,026}{28197} = 0,9 \text{ мкс}$$

Поставлені вимоги до системи становлять ≤5 мс, а значення отримане висче менше цього, з чого свідчить що система задовольняє всім поставленим вимогам.

Пропускна здатність каналу розраховується за формулою нижче:

$$b = \lambda \times l = 28197 * 650 * 8 = 146,6 \text{ Мбіт/с}$$

Що задовольняє пропускній здатності вихідного каналу в 1000 Мбіт/с.

3 РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Розрахунок схеми адресації корпоративної мережі

За основу для створення комп'ютерної мережі було взято IP адресу: 10.22.192.0/21 і за допомогою організаційної структури підприємства Туристична Агенція Круїз IP адреса була розбита на підмережі.

Розбити адресу IP на підмережі можна за допомогою методу VLSM. Він дозволяє легко і грамотно розбити існуючу IP адресу на локальні підмережі. Завдяки цьому роутери зможуть отримати інформацію про IP адреси підмереж та їх маску, це здійснюється за допомогою зчитування байтів з яких і складається адреса IP.

Таблиця 3.1 – Кількість вузлів в підмережах

Адреса	LAN1	LAN2	LAN3	LAN4	LAN5
10.22.192.0/21	74	17	90	241	99

У завданні кваліфікаційної роботи є дві задані підмережі, які відокремлені від інших підмереж, це WAN5 - 209.165.202.0/30 та WAN6 - 64.100.13.0/30. Один з них являє собою підключення кінцевого маршрутизатора до маршрутизатора для виходу в Інтернет, а другий це підключення маршрутизатора віддаленої підмережі до маршрутизатора для виходу в інтернет. Таблиця, зазначена вище(таб. 3.1), демонструє розбиття комп'ютерної мережі на локальні підмережі, усі п'ять підмереж пов'язані між собою комутаторами та маршрутизаторами.

Також між маршрутизаторами була проведена розбивка іншого IP адреси 10.0.8.0/24 на окремі ВЛАН, на побудову маршрутизації між ними. Розбиття проводилося згідно з таблицею нижче (табл. 3.2).

Таблиця 3.2 – Кількість вузлів між маршрутизаторами

Адреса	WAN1	WAN2	WAN3	WAN4
10.0.8.0/24	2	2	2	2

Розбиття методом VLSM здійснюється наступним способом. Кожна мережна IP адреса, яка містить діапазон допустимих адресних вузлів. Пристрої, що підключені до однієї і тієї ж мережі, має при собі IPv4 вузла цієї мережі, а також маску підмережі та префікс тієї мережі. Ці вузли між собою обмінюються трафіком безпосередньо, без використання маршрутизатора, але для визначення є трафік локальним або виходить з віддаленого пристрою використовується маска підмережі, яку зчитує маршрутизатор. Створення підмереж на основі IPv4 ми використовуємо один або кілька бітів з вузлової частини для створення біта мережної частини. На визначення блоку IP адрес за допомогою маски підмережі впливають два фактори[5].

- кількість необхідних підмереж
- максимальна кількість вузлів у підмережі

Між цими важливими факторами існує зворотна сумісність, чим більше біт запозичено для створення підмереж, тим менше біт залишиться в вузловій частині, це сприяє тому, що менше вузлів буде доступно в кожній підмережі.

Розрахунок кількості адресів, доступних для кожної підмережі розпадається за допомогою формули 2^n. Де н - це кількість бітів вузлової частини, що залишилися. Але потрібно враховувати, що в такому поданні не доступні діапазони мережної адреси та широкомовної адреси. Тому правильна формула для розрахунку становить 2^n-2.

Таблиця в якій розписані параметри адресацій підмереж згідно з організаційною структурою організації наведено нижче (таб. 3.3). Вона була створена за допомогою методу VLSM.

Таблиця 3.3 - Параметри адрес підмережі центрального офісу

Назва підмережі	**Кіл. вузлів**	**Номер мережі**	**Адреса підмережі**	**Маска підмережі**	**Початкове значення діапазону можливих адрес вузлів у підмереж**	**Кінцеве значення діапазону можливих адрес вузлів у підмережі**
LAN1	74	1	10.22.194.0	255.255.255.128	10.22.194.1	10.22.194.126
LAN2	17	2	10.22.194.128	255.255.255.224	10.22.194.129	10.22.194.158
LAN3	90	3	10.22.193.128	255.255.255.128	10.22.193.129	10.22.194.254
LAN4	241	4	10.22.192.0	255.255.255.0	10.22.192.1	10.22.192.254
LAN5	99	5	10.22.193.0	255.255.255.128	10.22.193.1	10.22.193.126
WAN1	2	1	10.0.8.0	255.255.255.252	10.0.8.1	10.0.8.2
WAN2	2	2	10.0.8.4	255.255.255.252	10.0.8.5	10.0.8.6
WAN3	2	3	10.0.8.8	255.255.255.252	10.0.8.9	10.0.8.10
WAN4	2	4	10.0.8.12	255.255.255.252	10.0.8.13	10.0.8.14
WAN5	2	5	10.0.8.16	255.255.255.252	10.0.8.17	10.0.8.18
WAN6	2	6	10.0.8.20	255.255.255.252	10.0.8.21	10.0.8.22
VLAN18	30	18	10.22.193.192	255.255.255.224	10.22.193.193	10.22.193.222
VLAN28	30	28	10.22.193.224	255.255.255.224	10.22.193.225	10.22.193.254
VLAN38	60	38	10.22.193.128	255.255.255.192	10.22.193.129	10.22.193.190

3.2 Розробка топологічної схеми корпоративної мережі

Для побудови моделі системи було використано програму Cisco Packet Tracer. У ній присутня безліч пристроїв, у тому числі і комутатори та маршрутизатори. Система має бути побудована відповідно до завдання кваліфікаційної роботи, а також організаційної структури підприємства.

Насамперед для побудови комп'ютерної мережі потрібно вибрати основне мережеве обладнання, такі як комутатори та маршрутизатори.

У цьому проекті були використані маршрутизатори Cisco 4331 та комутатори Cisco 2560. Топологія, яка була спроектована згідно з завданням роботи, показана нижче (рис. 3.1). У ній присутні 5 локальних підсистем, пов'язаних між собою комутаторами і маршрутизаторами, які були налаштовані відповідним чином.

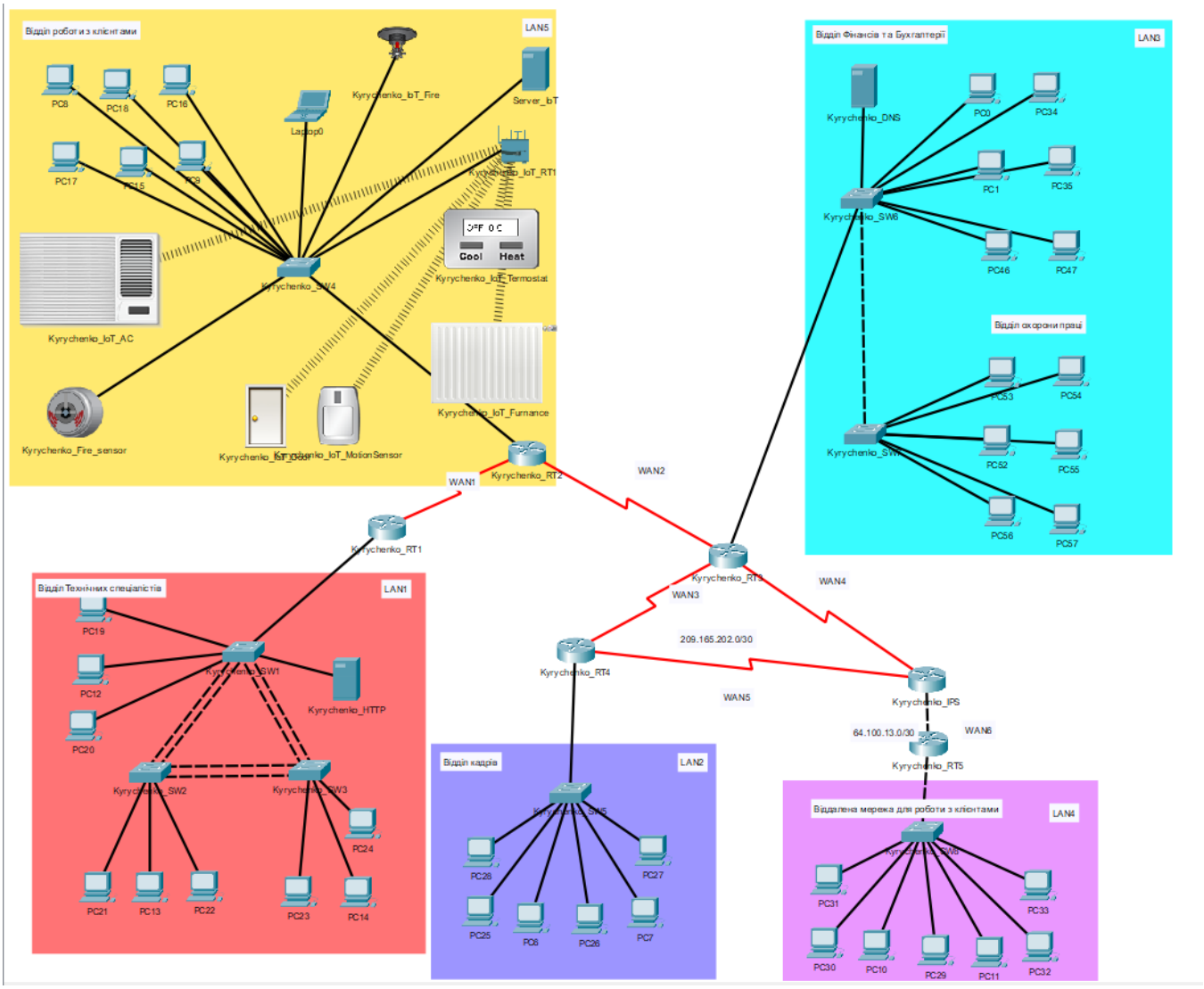

Рисунок 3.1 − Архітектура мережі обласної служби зайнятості

3.3 Розрахунок налаштувань маршрутизації корпоративної мережі

Відповідно до вимог кваліфікаційної роботи, а також вимог організаційної структури Туристичної Агенції Круїз необхідно створити топологічне адресне розбиття комп'ютерної мережі для мережевих пристроїв. Але при цьому потрібно враховувати такі пункти як:

- перший з доступних IP адрес мережі призначається для маршрутизатора і використовується ним
- другий з доступних IP адрес призначається для комутатора підмережі

- так само з виділеного пулу адрес потрібно залишити статичний IP адрес для серверів
- адреси, що залишилися, використовуються для пулу DHCP і використовуються кінцевими хостами
- VLAN використовують теж DHCP адреси кінцевих пристроїв але з урахуванням розбиття мережі на VLAN

У наведеній нижче(таб. 3.4) таблиці представлена схема адресації між пристроями мережі в центральному офісі Туристичної Агенції Круїз, а також у віддаленій філії мережі. Ця таблиця була створена відповідно до вимог кваліфікаційної та організаційної структури організації.

Таблиця 3.4 - Схема адресації пристроїв

Пристрій	**Інтерфейс**	**IP-адреса**	**Маска**	**Шлюз**	**VLAN**	**Інтерфейс підключеного пристрою**
Відділ Технічних спеціалістів						
Kyrychenko_RT1	G0/0/0	10.22.194.1	/25	-	-	G0/1
	S0/1/0	10.0.8.1	/30	-	-	S0/1/0
Kyrychenko_SW1	VLan1	10.22.194.2	/25	10.22.194.1	-	G0/1
	F0/1	-	-	-	-	F0/3
	F0/2	-	-	-	-	F0/2
	F0/3	-	-	-	-	F0/1
	F0/4	-	-	-	-	F0/2

Продовження таблиці 3.4

Kyrychenko_SW2	F0/1	-	-	-	-	F0/1
	F0/2	-	-	-	-	F0/2
	F0/3	-	-	-	-	F0/3
	F0/4	-	-	-	-	F0/4
Kyrychenko_SW3	F0/1	-	-	-	-	F0/3
	F0/2	-	-	-	-	F0/4

	F0/3	-	-	-	-	F0/3
	F0/4	-	-	-	-	F0/4
PC-PT 1-74	F0/1	10.0.8.6-126	/25	10.22.194.1	-	F05-24
Відділ кадрів						
Kyrychenko_RT4	G0/0/1	10.22.194.129	/27	-	-	G0/1
	S0/1/0	10.0.8.10	/30			S0/1/1
	S0/1/1	209.165.202.1	/30	-	-	S0/1/1
Kyrychenko_SW5	VLan1	10.22.194.130	/30	10.22.194.129	-	G0/0/1
PC-PT 1-17	F0/1	10.22.194.131-158	/27	10.22.194.129	-	F05-24
Відділ Фінансів та Бухгалтерії та охорони праці						
Kyrychenko_RT3	G0/0/0.18	10.22.193.129	/28	-	-	G0/1
	G0/0/0.28	10.22.193.145	/28	-	-	G0/1
	G0/0/0.38	10.22.193.193	/28	-	-	G0/1
	S0/1/0	10.0.8.6	/30	-	-	S0/1/1
	S0/1/1	10.0.8.9	/30	-	-	S0/1/1
	S0/2/0	10.0.8.13	/30	-	-	S0/1/0
Kyrychenko_SW6	VLan1	10.22.193.130	/25	10.22.193.129	-	G0/0/0
	F12-14	-	/25	-	18	F01
	F5-10	-	/25	-	28	F01
	F15-24	-	/25	-	38	F01
Kyrychenko_SW7	F12-14	-	/25	-	18	F01
	F5-10	-	/25	-	28	F01
	F15-24	-	/25	-	38	F01
PC-PT 1-3	F01	10.22.193.129-158	/27	10.22.193.129	18	F12-14
PC-PT 1-5	F01	10.22.193.161-190	/27	10.22.193.129	28	F5-10

Продовження таблиці 3.4

PC-PT 1-9	F01	10.22.193.193-222	/27	10.22.193.129	30	F15-24
Віддалена мережа для роботи з клієнтами						
Kyrychenko_RT5	G0/0/0	10.22.192.1	/24	-	-	G0/1
	G0/0/1	64.100.13.2	/30	-	-	G0/0/0

Kyrychenko_SW8	VLan1	10.22.192.2	/24	10.22.192.1	-	G0/0/0
PC-PT 1-241	F01	10.22.192.3 -254	/24	10.22.192.1	-	F01-24
Відділ роботи з клієнтами						
Kyrychenko_RT2	G0/0/0	10.22.193.1	/25	-	-	G0/1
	S0/1/0	10.0.8.2	/30	-	-	S0/1/0
	S0/1/1	10.0.8.5	/30	-	-	S0/1/0
Kyrychenko_SW4	VLan1	10.22.193.2	/25	10.22.193.1	-	G0/0/0
PC-PT 1-99	F01	10.22.193.3 -126	/25	10.22.193.1	-	F01-24
Маршрутизатор виходу в Інтернет						
Kyrychenko_IPS	S0/1/0	10.0.8.14	/30	-	-	S0/2/0
	S0/1/1	209.165.20 2.2	/30	-	-	S0/1/0
	G0/0/0	64.100.13.1	/30	-	-	G0/0/1

3.4 Налаштування та перевірка роботи комп’ютерної системи

3.4.1 Базове налаштування конфігурації пристроїв

Базове налаштування конфігурацій пристроїв це перелік дій для створення початкового налаштування маршрутизаторів, щоб отримати в результаті початковий функціонал мережі.

Налаштування виконуються суворо вимогам кваліфікаційної роботи, такі як:

- налаштування унікальної назви пристрою
- встановлення шифрування для пристрою
- налаштування привілейованого доступу до пристрою
- налаштування пароля для в ходу в консоль пристрою
- налаштування банеру MOTD
- налаштування протоколу SSH для входу до пристрою користувача
- налаштування домену

Приклад базового налаштування для пристрою Kyrychenko_RT1:

Присвоєння імені пристрою:

Router#enable

Router#conf t

Router(config)#hostname Kyrychenko_RT1

Встановлення IPv4 згідно таблиці 3.4:

Kyrychenko_RT1#conf t

Kyrychenko_RT1(config)#interface G0/0/0

Kyrychenko_RT1(config-if)#ip address 10.22.194.1 255.255.255.128

Kyrychenko_RT1(config-if)#no shutdown

Шифрування відкритих паролів:

Kyrychenko_RT1(config)#service password-encryption

Встановлено парою на вхід до консольної лінії:

Kyrychenko_RT1(config)#line console 0

Kyrychenko_RT1(config-line)#password cisco

Настроювання запиту пароля під час входу в пристрій:

Kyrychenko_RT1(config-line)#login

Kyrychenko_RT1(config-line)#exit

Налаштування банера MOTD:

Kyrychenko_RT1(config)#banner motd Kyrychenko M.O. 123-18-1

Створення пароля під час входу в привілейований режим:

Kyrychenko_RT1(config)#enable secret class

Створення користувача, а також настроювання протоколу SSH:

Kyrychenko_RT1(config)#username 123181_Kyrychenko privilege 15 password cisco

Створення домену:

Kyrychenko_RT1(config)#ip domain-name Kyrychenko_RT1

Шифрування даних за допомогою ключа RSA довжина якого 1024 біт:

Kyrychenko_RT1(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:

Kyrychenko_RT1(config)#line vty 0 4

Встановлення необхідності введення логіну та пароля для входу лінії:

Kyrychenko_RT1(config-line)#login local

Встановлення входу на лінію тільки по протоколу SSH:

Kyrychenko_RT1 (config-line)#transport input ssh

3.4.2 Налаштування маршрутизаторів корпоративної мережі

Згідно з вимогами кваліфікаційної роботи, а також особливостями організаційної структури Туристичної Агенції Круїз, маршрутизатори повинні бути пов'язані між собою, для передачі даних між підмережами, а також для виходу в інтерент. Для цього використовується технологи ---, яка надає здійснювати динамічну маршрутизацію без ручного налаштування кожного маршруту.

EIGRP - це протокол динамічної маршрутизації, заснований на векторі відстані який використовується в комп'ютерних мережах. Протокол був розроблений Cisco для своїх собі як власний протокол маршрутизації у 2013 році. EIGRP використовується в маршрутизаторі в тій же комп'ютерній мережі, що знаходяться інші маршрутизатори, тому що цей протокол відправляє іншим роутерам лише пакети оновлень, він зменшує навантаження на комп'ютерну мережу та обсяги даних, які необхідно передати для побудови таблиці маршрутизації[13].

EIGRP не працює в мережах з протоколами TCP і UDP, з чого слід, що він не використовує номер порту для індифікації трафіку.

Приклад створення зв'язків між двома маршрутизаторами Kyrychenko_RT1 та Kyrychenko_RT2 у кваліфікаційній роботі:

Щоб увімкнути протокол EIGRP слід на маршрутизаторі ввести команди:

Kyrychenko_RT1#enable

Kyrychenko_RT1#conf t

Kyrychenko_RT1(config)#router eigrp 100

Далі потрібно оголосити локальну підмережу до якої прив'язаний маршрутизатор, а також наступний підключений маршрутизатор:

Kyrychenko_RT1(config-router)# network 10.22.194.0 0.0.0.127

Kyrychenko_RT1(config-router)# network 10.0.8.0 0.0.0.3

Також згідно з вимогами кваліфікаційної роботи слід встановити на кожному Serial-port швидкість каналу 128000.

Kyrychenko_RT1#conf t

Kyrychenko_RT1(config)#interface S0/0/0

Kyrychenko_RT1(config-if)# clock rate 128000

Такі ж установки слід зробити на іншому маршрутизаторі і через деякий час роутери зможуть обмінятися пакетами даних для побудови таблиці маршрутизації, яка показана нижче(Рис. 3.2). Відповідно до неї, всі маршрути крім цього роутера мають приставку D що позначає їх доступність завдяки протоколу EIGRP. З цього випливає, що вони пов'язані між собою і можуть обмінюватися даними вільно.

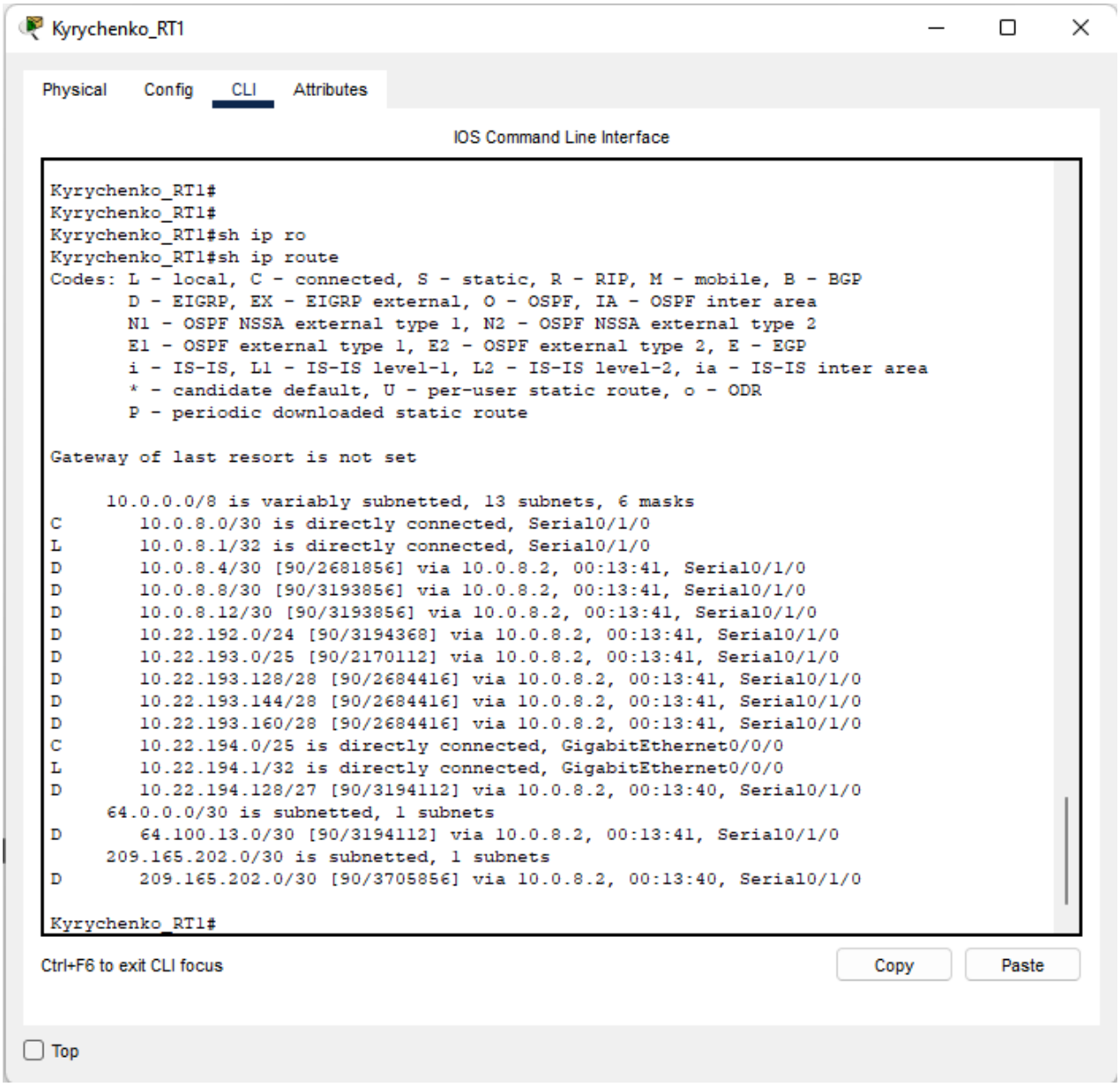

Рисунок 3.2 - Таблиця маршрутизації на маршрутизаторі Kyrychenko_RT1 після налаштування протоколу EIGRP

3.4.3 Налаштування роботи Інтернет

Після того як була влаштована базова конфігурація пристроїв, а так само завдяки протоколу EIGRP була проведена маршрутизація між маршрутизаторами, можна здійснити налаштування сервера HTTP для надання доступу до інтернет сторінці. Для цього потрібно встановити два сервери, це

HTTP сервер який виконуватиме функцію зберігання та роздачі HTML сторінки, а також DNS сервер для заміни IP адреси HTTP сервера, на посилання на ресурс сайту.

Насамперед потрібно налаштувати статичний айпі адресу для двох серверів. Для цього потрібно перейти в налаштування сервера та призначити йому статичну адресу, як зазначено на скріншоті нижче(Рис. 3.3).

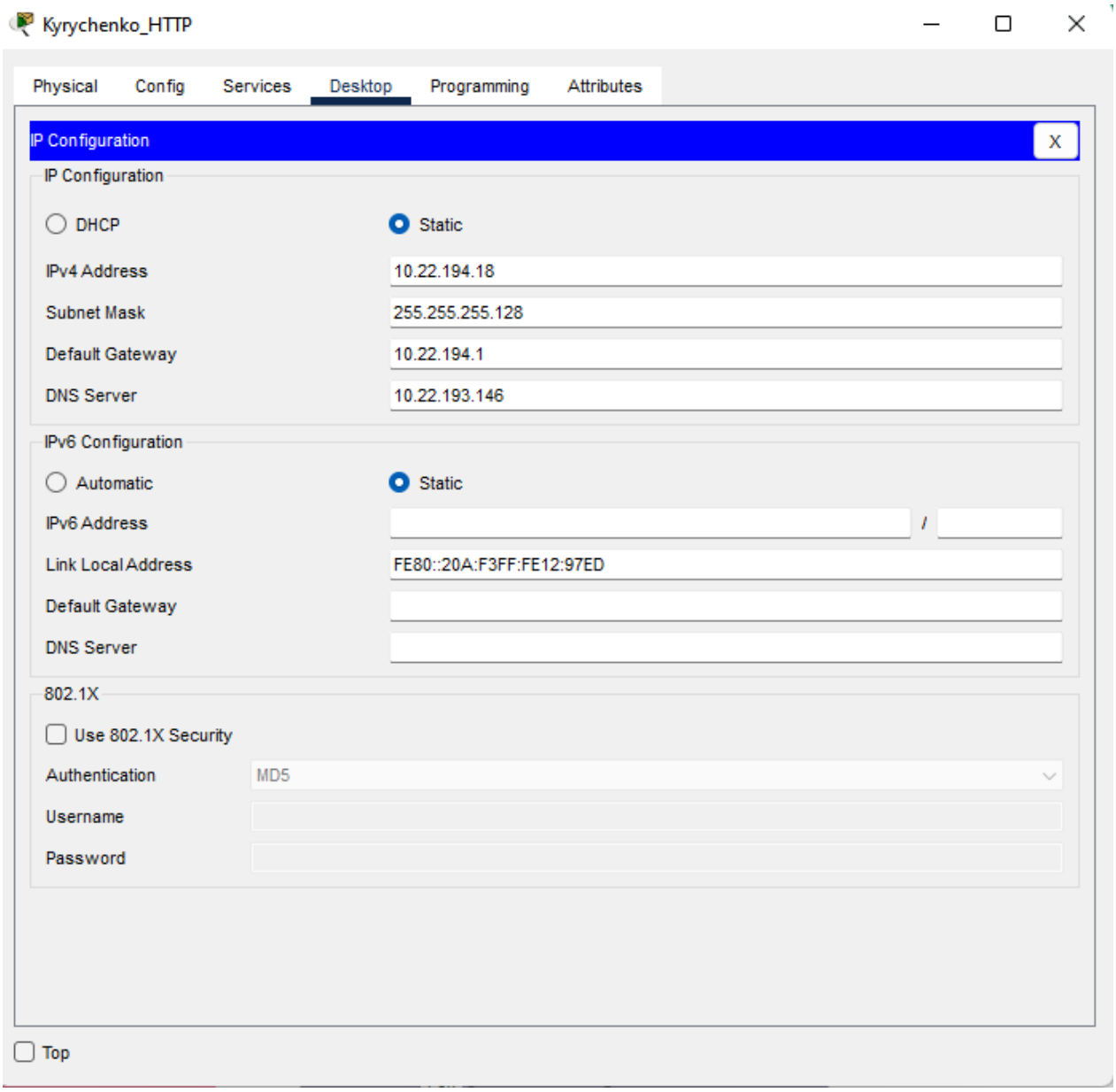

Рисунок 3.3 - Налаштований статичний IP та маски мережі HTTP серверу.

Після цього слід налаштувати роздачу HTTP сторінки на сервері з її редагуванням під завдання кваліфікаційної роботи. Приклад такого налаштування вказано на скріншоті нижче (Рис. 3.4).

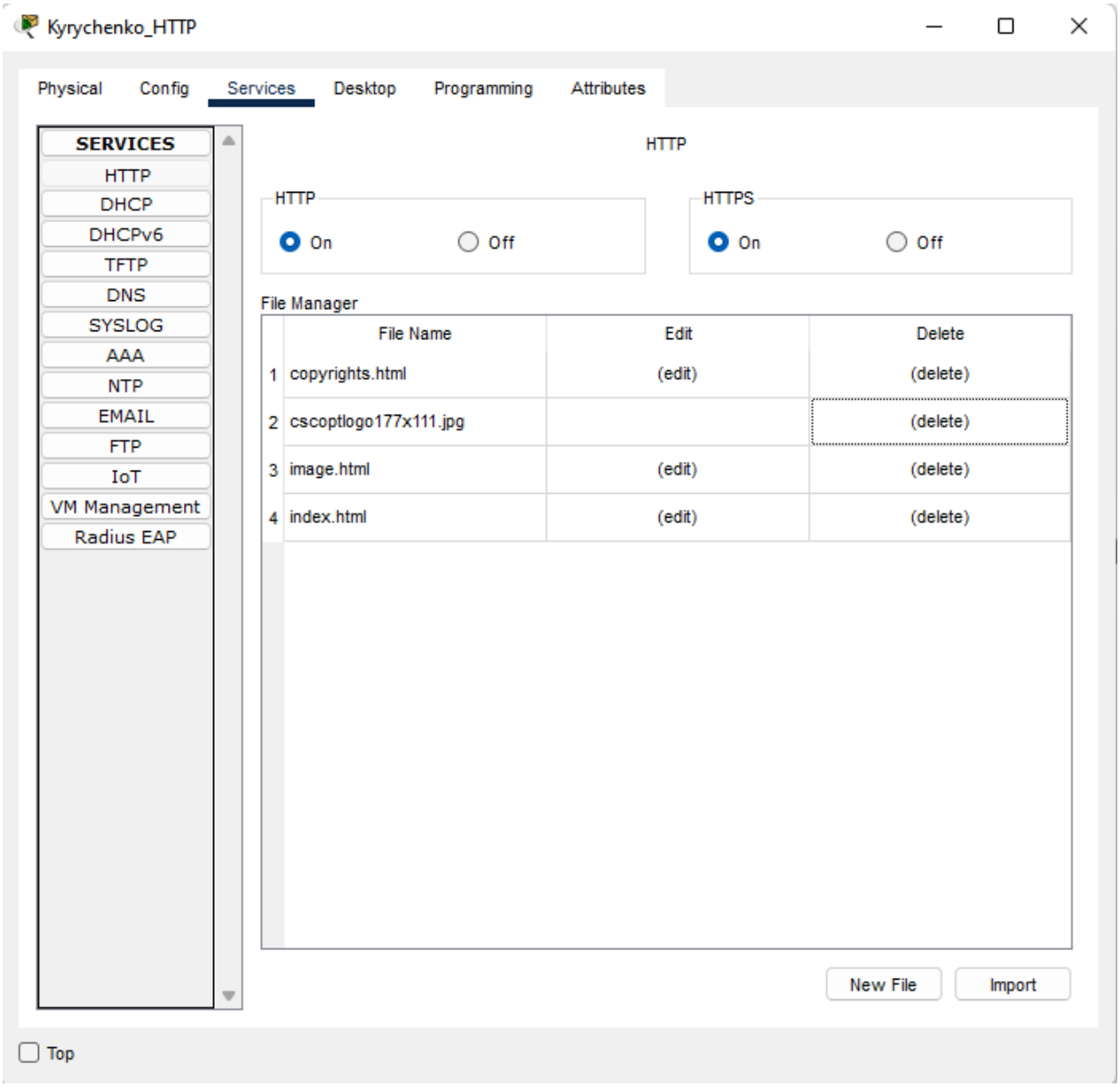

Рисунок 3.4 – Налаштування HTML сторінки на сервері

Далі слід зробити подібне DNS налаштування як на сервері HTTP для отримання статичного IP, а так само маски підмережі. Після цього потрібно включити службу заміни адреси DNS. Це було продемонстровано на скріншоті

нижче(Рис. 3.5), як видно(Рис. 3.6) відбувається заміна адреси на посилання сторінки, яку можна ввести в браузер пристрою, після чого проводиться перехід на сторінку HTML.

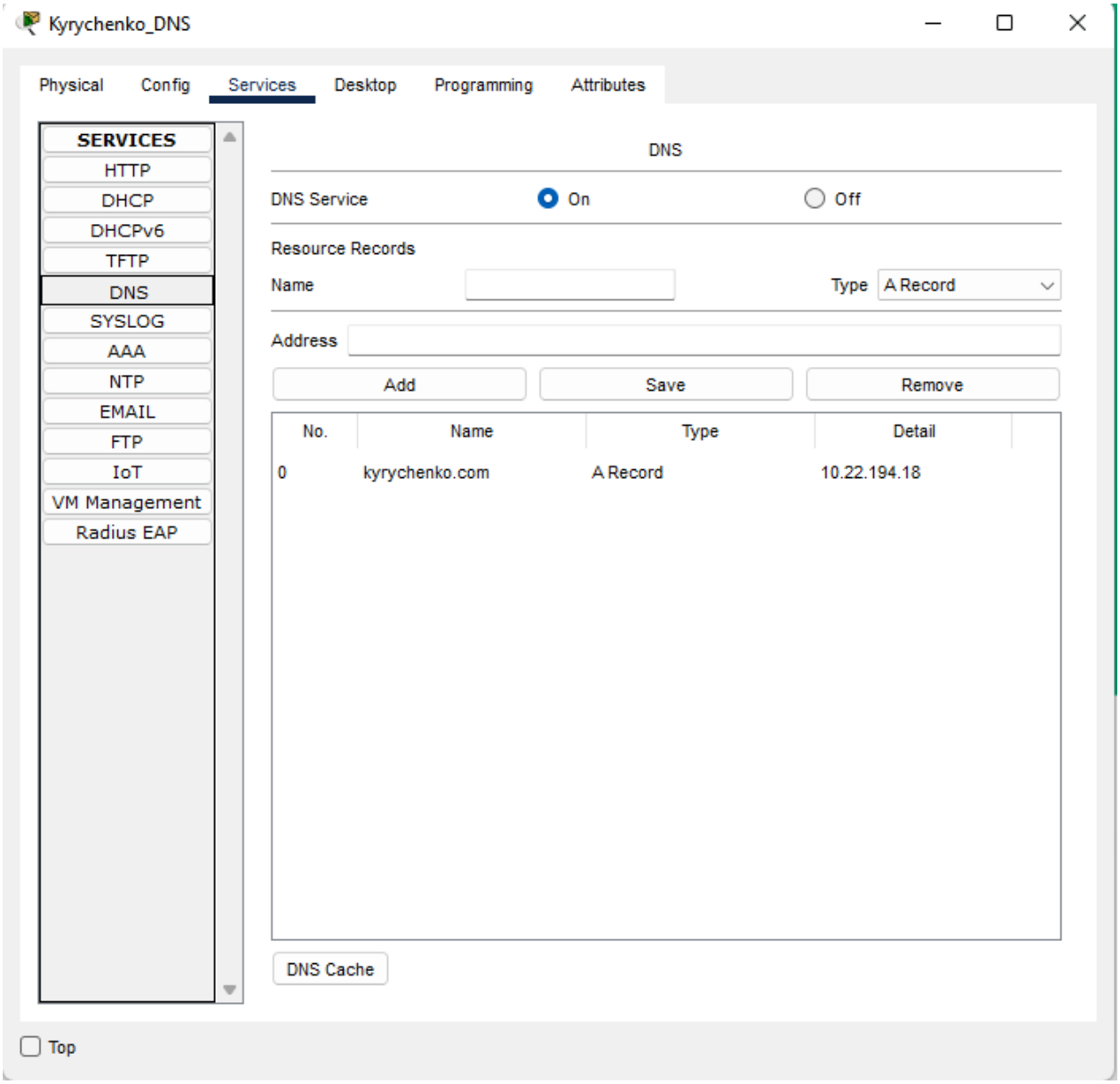

Рисунок 3.5 – Налаштування протоколу DNS

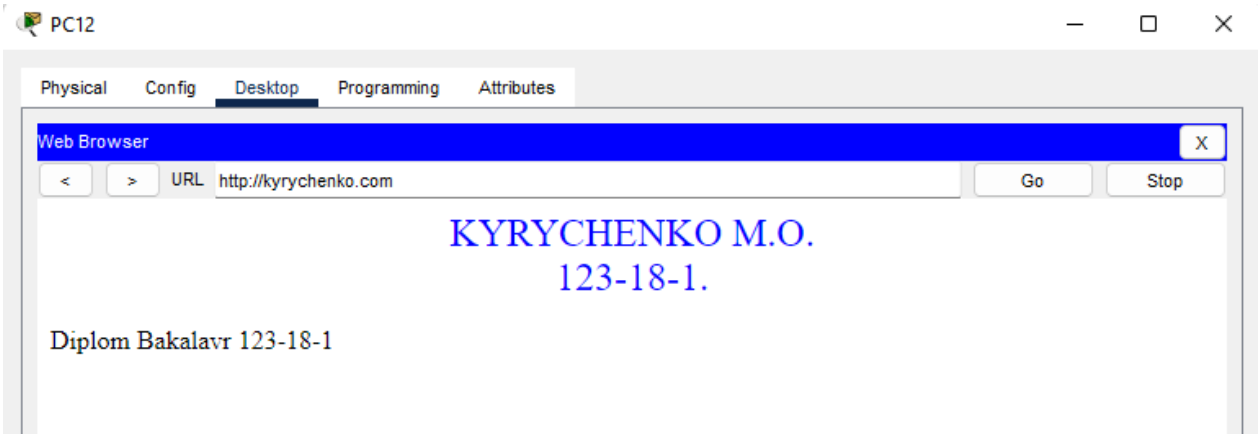

Рисунок 3.5 – Приклад роботи HTML сторінки

3.4.4 – Налаштування протоколу NAT

NAT використовується для того, щоб уникнути необхідності призначати нову адресу кожному хосту при переміщенні мережі або заміні інтернет-провайдера який стоїть на вищому рівні. Для цього один простір IP адрес перетворюється на інший шляхом зміни інформації про мережну адресу в заголовку IP пакета, під час проходу через маршрутизатор[6].

У цій кваліфікаційній роботі необхідно створити перетворення NAT на кінцевих зі джерелом інтернету маршрутизаторах мережі. Для цього потрібно створити пул адрес, які зможе використовувати NAT протокол, а також позначити вихідні та вхідні порти.

Далі показано налаштування NAT на маршрутизаторі Kyrychenko_RT3. Описані команди, завдяки яким можна налаштувати цей протокол:

Спочатку потрібно задати список айпі адрес, які будуть використовуватися для всіх внутрішніх мереж:

Kyrychenko_RT1#enable

Kyrychenko_RT1#conf t

Kyrychenko_RT1(config)# access-list 14 permit 10.22.192.0 0.0.7.255

Далі потрібно позначити пул адрес для підміни:

Kyrychenko_RT1(config)# ip nat pool Internet 10.0.8.13 10.0.8.14 netmask 255.255.255.252

І тепер можна ввести команду, яка замінятиме внутрішню мережу пулом адрес для протоколу NAT:

Kyrychenko_RT1(config)# ip nat inside source list 14 pool Internet

Далі потрібно позначити порти, які повинні приймати пакети з внутрішньої мережі, а також позначити порт, який буде виходити з внутрішньої мережі:

Kyrychenko_RT1(config)# interface Serial0/1/0

Kyrychenko_RT1(config-if)# ip nat inside

Kyrychenko_RT1(config)# interface Serial0/2/0

Kyrychenko_RT1(config-if)# ip nat outside

Kyrychenko_RT1(config)# interface Serial0/1/1

Kyrychenko_RT1(config-if)# ip nat inside

Kyrychenko_RT1(config)# interface G0/0/0

Kyrychenko_RT1(config-if)# ip nat inside

Після цих налаштувань кінцеві маршрутизатори можуть вводити вихідні та вихідні адреси IP для надання доступу до інтернет мережі, таблицю перетворень можна переглянути нижче(Рис. 3.6).

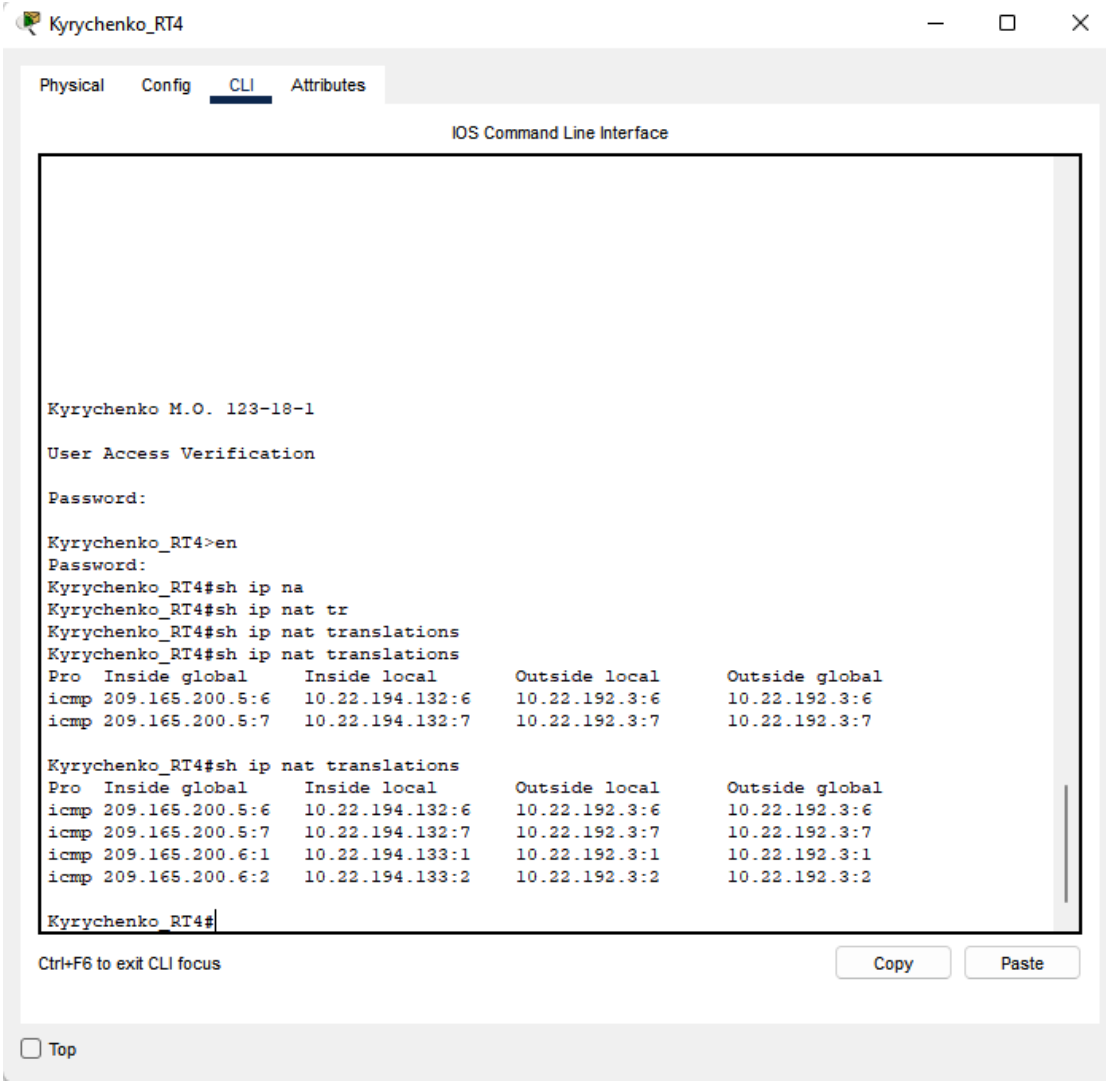

Рисунок 3.6 – Таблиця перетворювань NAT

3.4.5 – Агрегування каналів

Агрегування каналів у комп'ютерних мережах це об'єднання кількох мережевих підключень в одне логічне з метою підвищення надійності та пропускної спроможності мережі.

Для цього можна налаштувати агрегацію каналів між двома комутаторами, комутатором та маршрутизатором тощо. Приклад налаштування агрегації каналів між трьома комутаторами наведено нижче:

Налаштування агрегування на комутаторі Kyrychenko_SW1:

Kyrychenko_SW1#enable

Kyrychenko_SW1#conf t

Kyrychenko_SW1(config)#int range fa0/1-2

Kyrychenko_SW1(config-if-range)# no shutdown

Kyrychenko_SW1(config-if-range)# channel-protocol lacp

Kyrychenko_SW1(config-if-range)# channel-group 1 mode active

Kyrychenko_SW1(config-if-range)#exit

Kyrychenko_SW1(config)#int range fa0/3-4

Kyrychenko_SW1(config-if-range)# channel-protocol lacp

Kyrychenko_SW1(config-if-range)# channel-group 2 mode active

Налаштування агрегування на комутаторі Kyrychenko_SW2:

Kyrychenko_SW2#enable

Kyrychenko_SW2#conf t

Kyrychenko_SW2(config)#int range fa0/1-2

Kyrychenko_SW1(config-if-range)# no shutdown

Kyrychenko_SW2(config-if-range)# channel-protocol lacp

Kyrychenko_SW2(config-if-range)# channel-group 1 mode active

Kyrychenko_SW2(config-if-range)#exit

Kyrychenko_SW2(config)#int range fa0/3-4

Kyrychenko_SW2(config-if-range)# channel-protocol lacp

Kyrychenko_SW2(config-if-range)# channel-group 3 mode active

Налаштування агрегування на комутаторі Kyrychenko_SW3:

Kyrychenko_SW3#enable

Kyrychenko_SW3#conf t

Kyrychenko_SW3(config)#int range fa0/1-2

Kyrychenko_SW1(config-if-range)# no shutdown

Kyrychenko_SW3(config-if-range)# channel-protocol lacp

Kyrychenko_SW3(config-if-range)# channel-group 2 mode active

Kyrychenko_SW3(config-if-range)#exit

Kyrychenko_SW3(config)#int range fa0/3-4

Kyrychenko_SW3(config-if-range)# channel-protocol lacp

Kyrychenko_SW3(config-if-range)# channel-group 3 mode active

Щоб перевірити працездатність технології агрегування каналів можна вказати команду нижче, це виводить інформацію щодо функціювання протоколу(Рис. 3.7):

Kyrychenko_SW3# show etherchannel summary

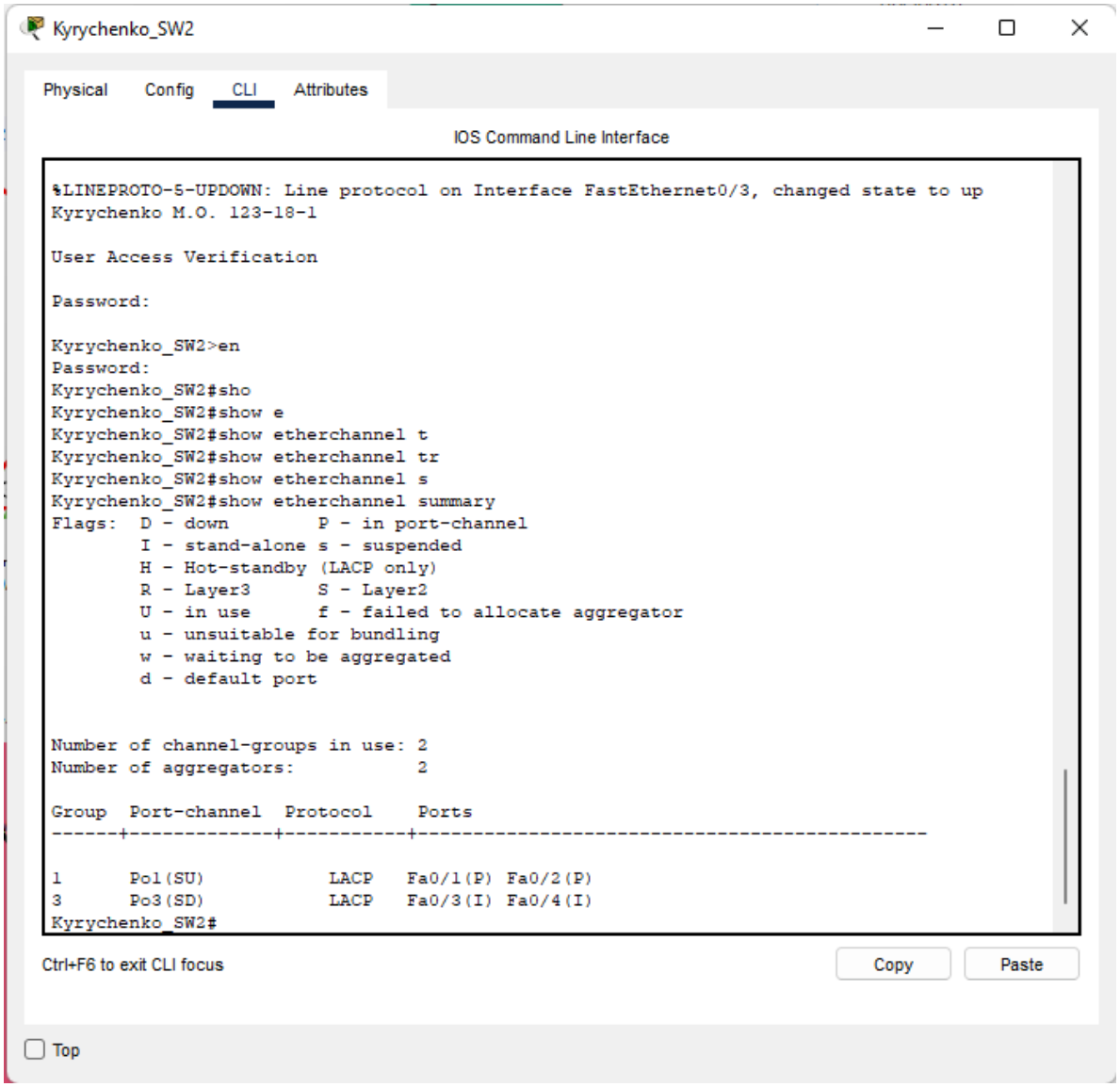

Рисунок 3.7 – Перевірка роботи протоколу агрегування каналів

Як видно, агрегація каналів відбувається за допомогою протоколу LACP. Цей протокол функціонує за допомогою створення груп агрегацій з однаковими налаштуваннями швидкості та дуплексу. Він використовує мережеві інтерфейси в активній групі агрегування згідно з технологією.

Основні переваги такого методу полягає в тому, що аварійне перемикання відбувається автоматично, якщо відбувається проміжний збій то однорангова система може не виявити жодних проблем з підключенням, так само це динамічна конфігурація завдяки чому пристрій може зрозуміти, що конфігурація на іншому кінці мережі підтримує агрегацію.

LACP працює за принципом відправлення кадрів за всіма посиланнями, яких підключений протокол. Коли він знаходить пристрій, до якого підключений цей же протокол, то цей пристрій зможе незалежно відправляти кадри по цих же каналах у протилежному напрямку, що дозволяє іншим пристроям виявити кілька каналів між собою і потім об'єднати їх в один логічний. Протокол працює у двох режимах, пасивному та активному. Пасивний режим не відправляє кадри до тих пір, поки один з них не отримає з іншого боку, а активний відправляє кадри один раз в секунду налаштованими каналами.

3.4.6 - Перевірка роботи комп’ютерної системи

Для перевірки працездатності комп'ютерної мережі, слід перевірити доступність мережних вузлів, так само слід здійснити підключення по безпечному віддаленому доступу, а також настроїти автоматичне присвоєння адрес IP для кінцевих хостів в підмережах і VLAN.

Насамперед слід налаштувати автоматичне присвоєння IP адреси та маски для підсистем та VLAN. Для підсистем та для VLAN у підсистемі налаштування дещо відрізняються, що буде показано нижче при налаштуванні маршрутизаторів Kyrychenko_RT2 та Kyrychenko_RT3.

DHCP - це протокол, який дозволяє керувати мережею і використовується при підключенні до мережі інтернет, він виконує функцію автоматичного присвоєння IP та маски підмережі. Така технологія позбавляє співробітника компанії від індивідуального налаштування мережевих пристроїв вручну, для цього потрібно наявність центрального встановленого сервера DHCP і клієнтських екземплярів стека протоколів на кожному комп'ютері або іншому іншому пристрої. Під час підключення до мережі та ще через деякий час клієнт запитує набір параметрів у DHCP сервера з використанням протоколу DHCP[9].

Така мережа може бути реалізована будь-де, від маленьких житлових мереж або ж у великих корпораціях на кілька тисяч пристроїв. Багато маршрутизаторів інтернет-провайдерів використовують цю технологію для автоматичного присвоєння IP. Наприклад домашні маршрутизатори поєднують можливості як технології DHCP так і сервера для роздачі IP та маски підмережі.

Приклад налаштування протоколу DHCP для підмережі:

Налаштування протоколу DHCP на маршрутизаторі Kyrychenko_RT2:

Вимкнення айпі адрес з пулу --- для присвоєння їх значень для комутатора та маршрутизатора.

Kyrychenko_RT2#enable

Kyrychenko_RT2#conf t

Kyrychenko_RT2(config)# ip dhcp excluded-address 10.22.193.1 10.22.193.2

Далі необхідно написати ім'я пула DHCO, присвоїти йому IP адресу, маску, а також DNS сервер за замовчуванням.

Kyrychenko_RT2(config)# ip dhcp pool NET5

Kyrychenko_RT2(config)# network 10.22.193.0 255.255.255.128

Kyrychenko_RT2(config)# default-router 10.22.193.1

Kyrychenko_RT2(config)# dns-server 10.22.193.146

Kyrychenko_RT2(config)# domain-name kyrychenko.com

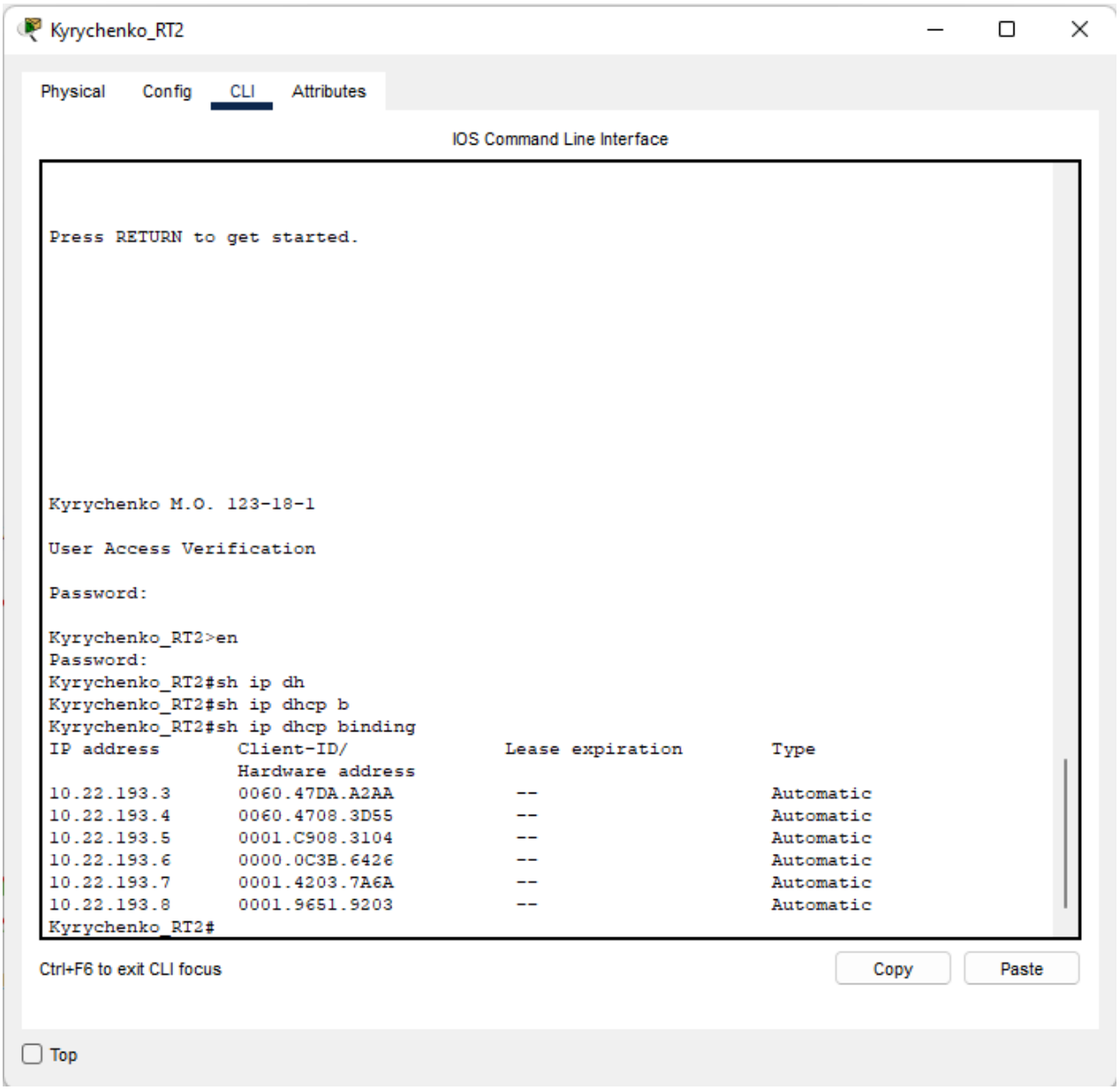

Рисунок 3.8 – Таблиця роздачі IP адрес за протоколом DHCP

Як ми бачимо за допомогою протоколу DHCP можна автоматично роздати кінцевим хостам адреси IP, це можна переглянути в таблиці зазначеної вище(Рис. 3.8).

Тепер можна перевірити доступність маршрутів мережі. Для цього можна виконати команду ping у консолі комп'ютера у напрямку комп'ютера іншої підмережі. Виконання такої команди показано на малюнку нижче(Рис. 3.9).

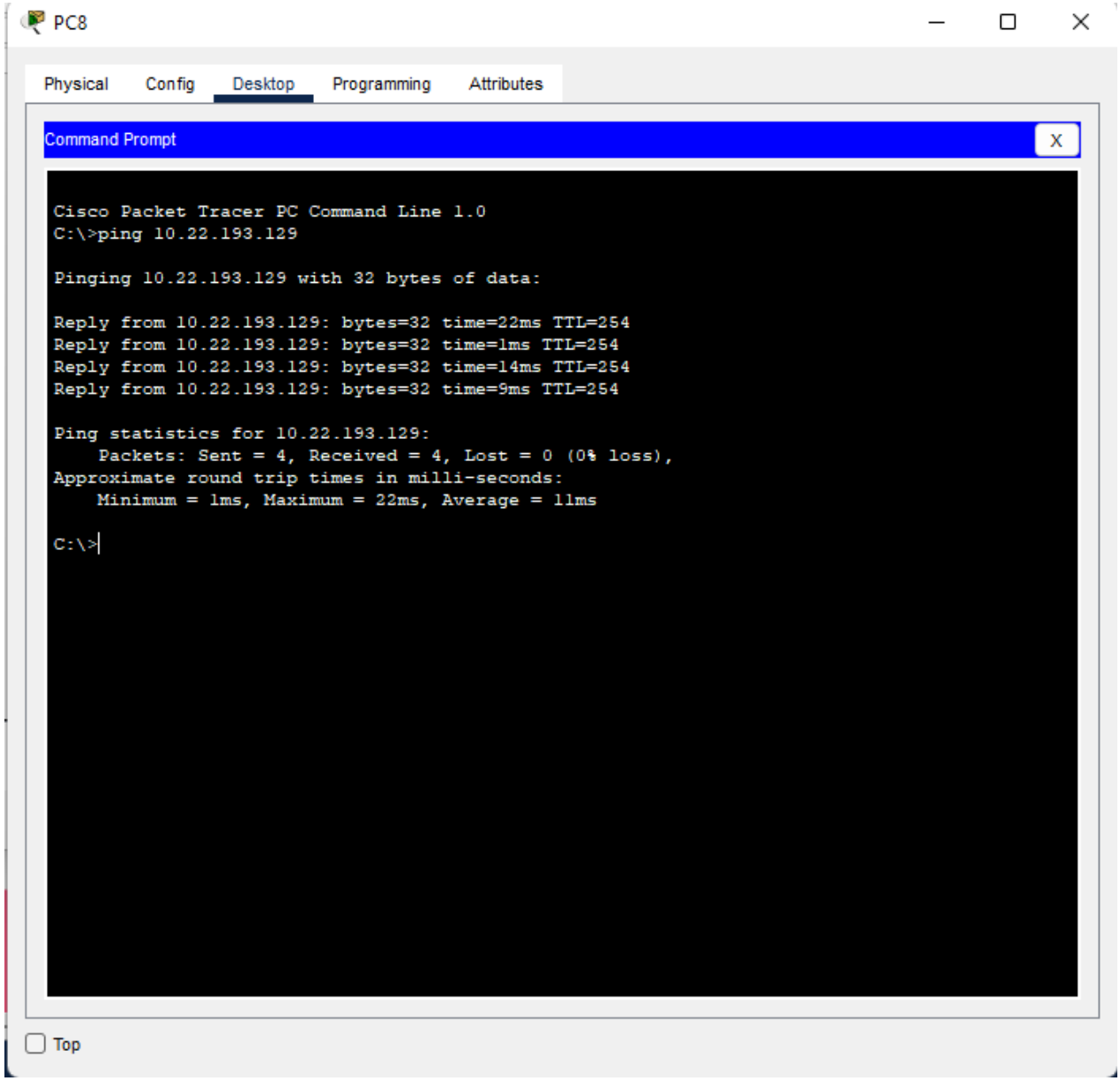

Рисунок 3.9 – Перевірка роботи маршрутів між підмережами

Далі ми перевіримо працездатність підключення до віддаленого маршрутизатора або комутатора за допомогою протоколу SSH. Це можна зробити за допомогою команди, наведеної нижче.

C:\ssh -l [login name] [ip address]

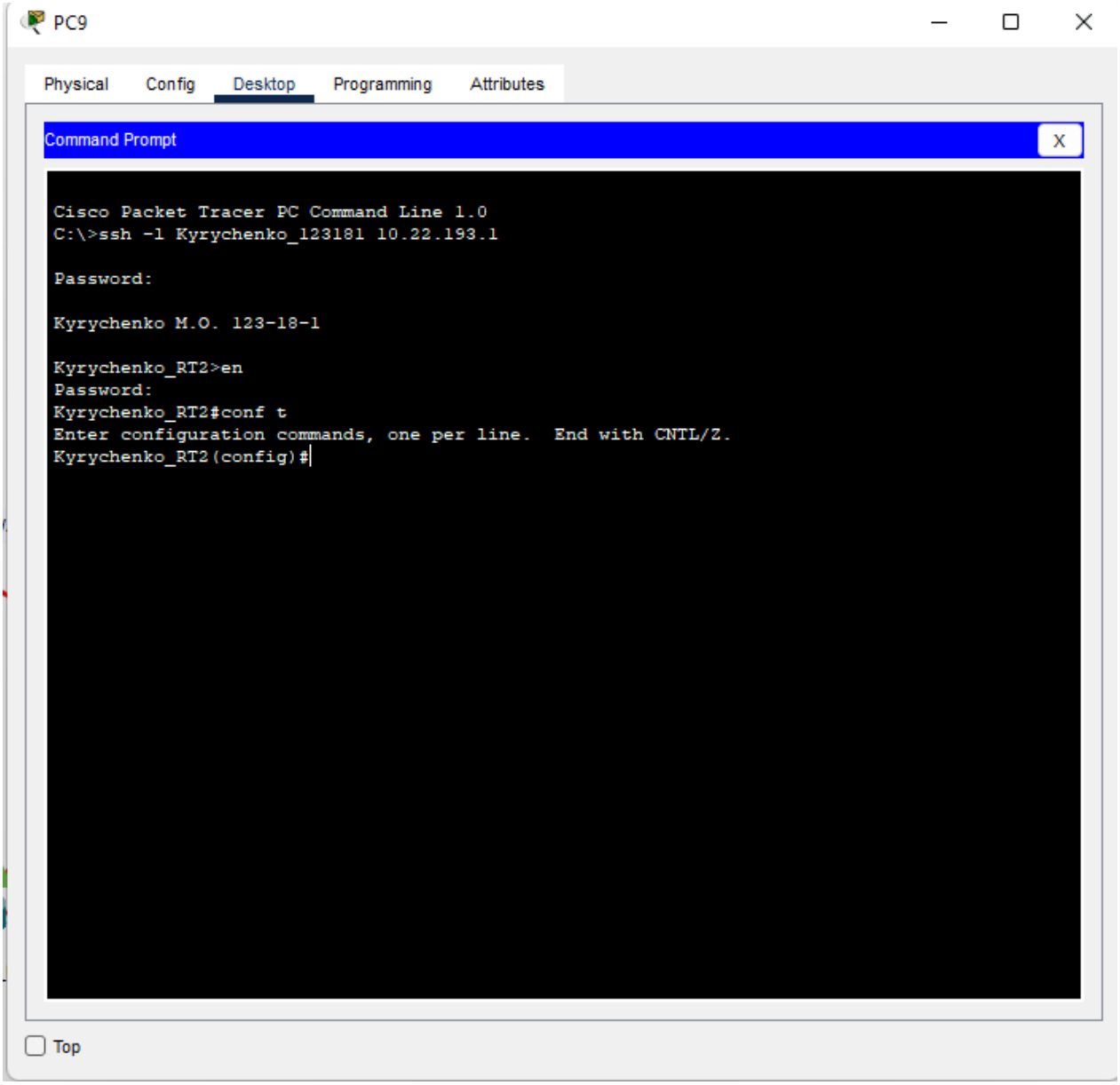

Рисунок 3.10 – Перевірка роботи підключення до маршрутизатора через протокол SSH

Як показано на малюнку вище(Рис. 3.10), ми можемо вільно підключитися до віддаленого маршрутизатора завдяки цьому протоколу. Але для подальшої взаємодії з ним потрібно буде ввести пароль.

3.5 Захист інформації в комп’ютерній системі від несанкціонованого доступу

3.5.1 Розробка методів для захисту інформації в комп’ютерній системі

Для забезпечення безпеки від несанкціонованого доступу до комп'ютерної мережі необхідно забезпечити систему рядом функцій. Список налаштувань до комп'ютерної мережі, для забезпечення безпеки мережі:

- налаштування VLAN в окремій локальній підмережі
- налаштування VPN між підсистемою, а також філією віддаленої локальної підсистемою

3.5.2 Налаштування мереж VLAN

VLAN це спосіб розбиття підсистеми на сегменти, але при цьому потрібно враховувати, що порти з протоколами IPv4 та IPv6 на комутаторах другого рівня сильно обмежена у функціональності. Також слід запам'ятати що статичної маршрутизації, на побудову VLAN великого розміру, не вистачить, але й комутатора другого рівня досить хороші при перемиканні, але так само недостатні в динамічній маршрутизації.

VLAN - це розділений та ізольований широкомовний домен комп'ютерної мережі на другому канальному рівні. VLAN працює застосовуючи теги до мережевих кадрам, обробляючи їх так, що створюється

зовнішній вигляд мережного трафіку, який фактично знаходиться в одній мережі, але на практиці розділений на кілька підмереж. Таким чином віртуальні локальні мережі, можуть розділяти мережеві програми, незважаючи, що вони знаходяться в одній і тій же фізичній комп'ютерній підсистемі[10].

Відповідно до організаційної структури Туристичного Агентства Круїз, а також для відповідальних вимог Відділу Бухгалтерії та Фінансів, а також відділу Охорони праці була створена таблиця поділу підсистеми на сегменти VLAN. Таблиця вказана нижче(Таб. 3.5).

Таблиця 3.5 – Схема розподілення підмережі на сегменти VLAN

Номер VLAN	**Ім’я VLAN**	**Примітка**
1	default	Не використовується
18	Accounting	Для бухгалтерії та фінансів
28	Resources Department	Для відділу охорони праці
38	Guest	Для гостей
99	Management	Для управління пристроями
100	Native	Власна мережа

Нижче розписано по пунктах налаштування комутаторів Kyrychenko_SW6 та Kyrychenko_SW7, для поділу підмережі на сегменти, а також установка на маршрутизаторі Kyrychenko_RT3 мережі DHCP для роздачі їх кінцевих хостів підмережі.

Налаштування на Boboshko_Sw1.1:

Задання імені хосту:

Switch#enable

Switch#conf t

Switch (config)# hostname Kyrychenko_SW6

Об’ява VLAN18:

Kyrychenko_SW6(config)# vlan 18

Задання опису для VLAN18 для відділу бухгалтерії та фінансів:

Kyrychenko_SW6(config-vlan)#name Accounting

Об’ява VLAN28:

Kyrychenko_SW6(config)# vlan 28

Задання опису для VLAN28 для відділу охорони праці:

Kyrychenko_SW6(config-vlan)#name ResourcesDep

Об’ява VLAN38:

Kyrychenko_SW6(config)# vlan 38

Задання опису для VLAN38 для відділу охорони праці:

Kyrychenko_SW6(config-vlan)#name Guest

Об’ява VLAN99:

Kyrychenko_SW6(config)# vlan 99

Задання опису для VLAN99 для управління пристроями:

Kyrychenko_SW6(config-vlan)#name Management

Об’ява VLAN100:

Kyrychenko_SW6(config)# vlan 100

Задання опису для VLAN100 для управління пристроями:

Kyrychenko_SW6(config-vlan)#name Native

Kyrychenko_SW6(config-vlan)#exit

Налаштування транкових каналів:

Kyrychenko_SW6(config)#interface range g0/1-2

Kyrychenko_SW6(config-if-range)# switchport trunk native vlan 100

Kyrychenko_SW6(config-if-range)# switchport mode trunk

Налаштування портів доступу:

Kyrychenko_SW6(config)#interface range f0/12-14

Kyrychenko_SW6(config-if-range)# switchport mode access

Kyrychenko_SW6(config-if-range)# switchport access vlan 18

Kyrychenko_SW6(config)#interface range f0/5-10

Kyrychenko_SW6(config-if-range)# switchport mode access

Kyrychenko_SW6(config-if-range)# switchport access vlan 28

Kyrychenko_SW6(config)#interface range f0/15-24

Kyrychenko_SW6(config-if-range)# switchport mode access

Kyrychenko_SW6(config-if-range)# switchport access vlan 38

Налаштування SVI-интерфейсу:

Kyrychenko_SW6(config)# interface Vlan1

Kyrychenko_SW6(config-if)# ip address 10.22.193.130 255.255.255.128

Після цього потрібно зробити схожі установки на другому комп'ютері. Коли все це зроблено можна перевірити працездатність мережі ---. Для цього можна ввести команду, вказану нижче.

Kyrychenko_SW6#show vlan

Після цього з'явиться таблиця, яка показана нижче(Рис. 3.11). У ній видно які VLAN створені взагалі і який порт прив'язаний до того чи іншого VLAN.

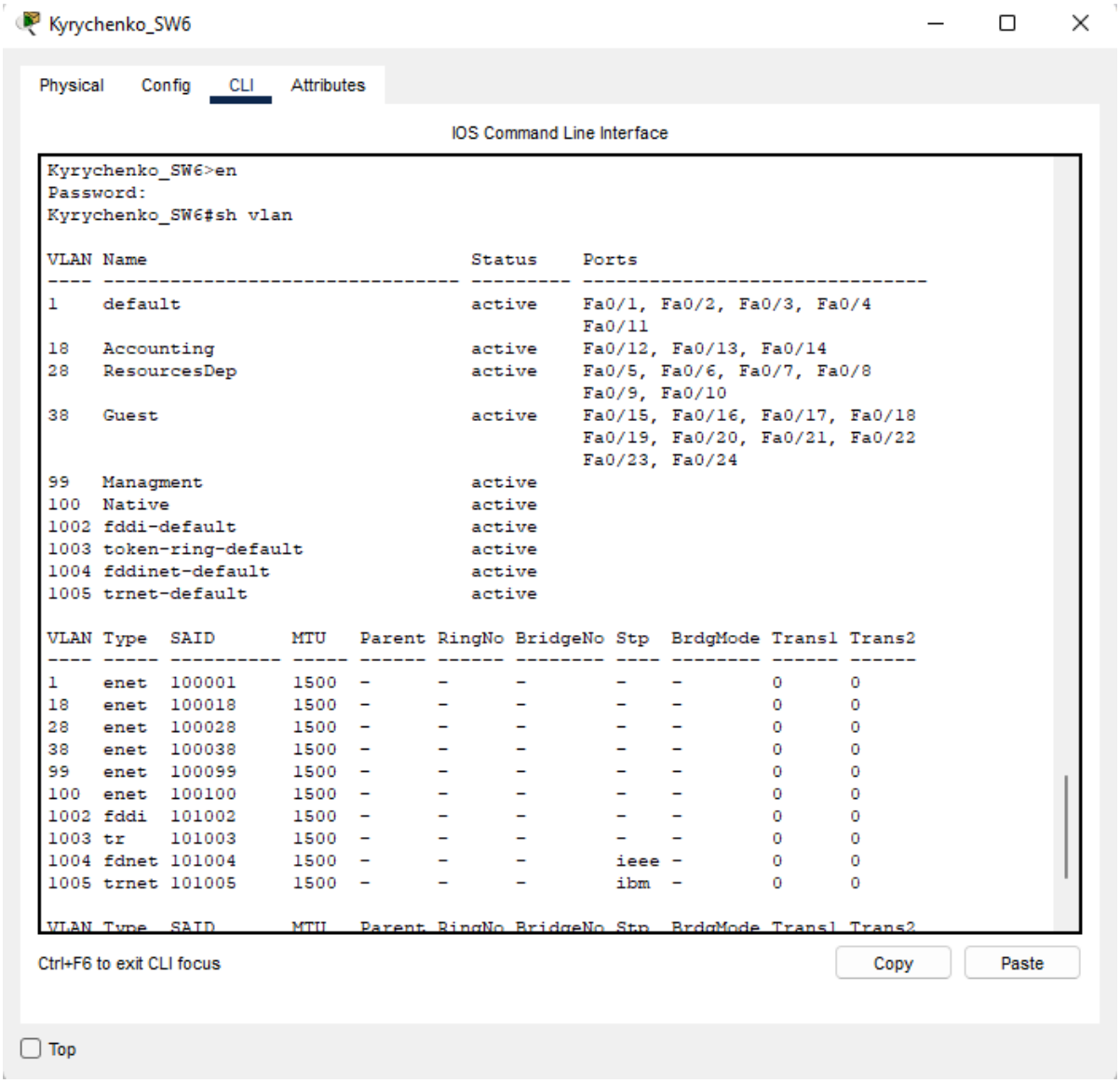

Рисунок 3.11 – Таблиця сегментів VLAN

Для повноцінного функціонування VLAN необхідно призначити кожному сегменту VLAN власний пул адрес DHCP. Цей метод мало чим відрізняється від стандартної установки протоколу DHCP для автоматичної роздачі, але має деякі відмінності які показані нижче.

Насамперед потрібно створити пул адрес для кожного сегмента лан. Для цього ми вводимо такі команди:

Kyrychenko_RT3#enable

```
Kyrychenko_RT3#conf t
Kyrychenko_RT3(config)#ip dhcp pool VLAN18
Kyrychenko_RT3(config)# network 10.22.193.128 255.255.255.240
Kyrychenko_RT3(config)# default-router 10.22.193.129
Kyrychenko_RT3(config)# dns-server 10.22.193.146
Kyrychenko_RT3(config)# domain-name kyrychenko.com
Kyrychenko_RT3(config)#ip dhcp pool VLAN28
Kyrychenko_RT3(config)# network 10.22.193.144 255.255.255.240
Kyrychenko_RT3(config)# default-router 10.22.193.129
Kyrychenko_RT3(config)# dns-server 10.22.193.146
Kyrychenko_RT3(config)# domain-name kyrychenko.com
Kyrychenko_RT3(config)#ip dhcp pool VLAN38
Kyrychenko_RT3(config)# network 10.22.193.160 255.255.255.240
Kyrychenko_RT3(config)# default-router 10.22.193.129
Kyrychenko_RT3(config)# dns-server 10.22.193.146
Kyrychenko_RT3(config)# domain-name kyrychenko.com
```

Далі потрібно створити віртуальні порти та присвоїти їм адреси та маски, також потрібно для них вказати інкапсуляцію dot1Q N8:

```
Kyrychenko_RT3(config)# interface GigabitEthernet0/0/0.18
Kyrychenko_RT3(config-if)# encapsulation dot1Q 18
Kyrychenko_RT3(config-if)# ip address 10.22.193.129 255.255.255.240
Kyrychenko_RT3(config)# interface GigabitEthernet0/0/0.28
Kyrychenko_RT3(config-if)# encapsulation dot1Q 28
Kyrychenko_RT3(config-if)# ip address 10.22.193.145 255.255.255.240
Kyrychenko_RT3(config)# interface GigabitEthernet0/0/0.38
Kyrychenko_RT3(config-if)# encapsulation dot1Q 38
Kyrychenko_RT3(config-if)# ip address 10.22.193.161 255.255.255.240
```

3.5.3 Налаштування мережі VPN

Протокол VPN дозволяє користувачам відправляти та отримувати дані розширення загальнодоступної мережі через інші доступні мережі, начебто їх мережі були підключені безпосередньо. Такий тип безпеки дозволяє збільшити функціональність, а так само безпеку управління приватною мережею, забезпечує доступ до ресурсів, які раніше були недоступними без VPN[8].

VPN створюється шляхом накладання віртуального з'єднання точка-точка, при використанні виділених каналів і протоколів тунелювання у вже існуючих мережах. Всі мережі VPN доступні з загальнодоступного інтернету, що може забезпечити переваги у використанні глобальної мережі WAN.

Нижче записано точне настроювання протоколу на маршрутизаторі Kyrychenko_RT4 в підмережі LAN2 для безперервного відправлення пакетів між цією підсистемою до віддаленої локальної мережі філії LAN4.

Створення ACL таблиці у тому, щоб зазначити протоколу VPN із якими підмережами йому працювати:

Kyrychenko_RT4#enable

Kyrychenko_RT4#conf t

Kyrychenko_RT4(config)# access-list 110 permit ip 10.22.194.128 0.0.0.31 10.22.192.0 0.0.0.255

Налаштування шифрування політики isakmp:

Kyrychenko_RT4(config)# crypto isakmp policy 10

Kyrychenko_RT4(config)# encr aes 256

Kyrychenko_RT4(config)# authentication pre-share

Kyrychenko_RT4(config)# group 5

Kyrychenko_RT4(config)# crypto isakmp key vpnpa address 64.100.13.2

Налаштування закриття пакетів шляхом трансформації:

Kyrychenko_RT4(config)# crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac

Налаштування шляху з'єднання мапи VPN:

Kyrychenko_RT4(config)# crypto map VPN-MAP 10 ipsec-isakmp

Kyrychenko_RT4(config)# description VPN to LAN4

Kyrychenko_RT4(config)# set peer 64.100.13.2

Kyrychenko_RT4(config)# set transform-set VPN-SET

Kyrychenko_RT4(config)# match address 110

Підключення VPN шифрування до порту:

Kyrychenko_RT4(config)# interface Serial0/1/1

Kyrychenko_RT4(config)# crypto map VPN-MAP

Після цього ми надішлемо кілька пакетів між цими підмережами та відобразимо таблицю ВПН перетворень за допомогою команди нижче:

Kyrychenko_RT4# show crypto ipsec sa

У цій таблиці (Рис. 3.12) ми побачимо, як відбувається перетворення пакетів між цими мережами, було розшифровано 6 пакетів. З чого випливає, що мережа з протоколом VPN повністю налаштована і функціонує правильно забезпечуючи ці дві підмережі безпечною передачею даних.

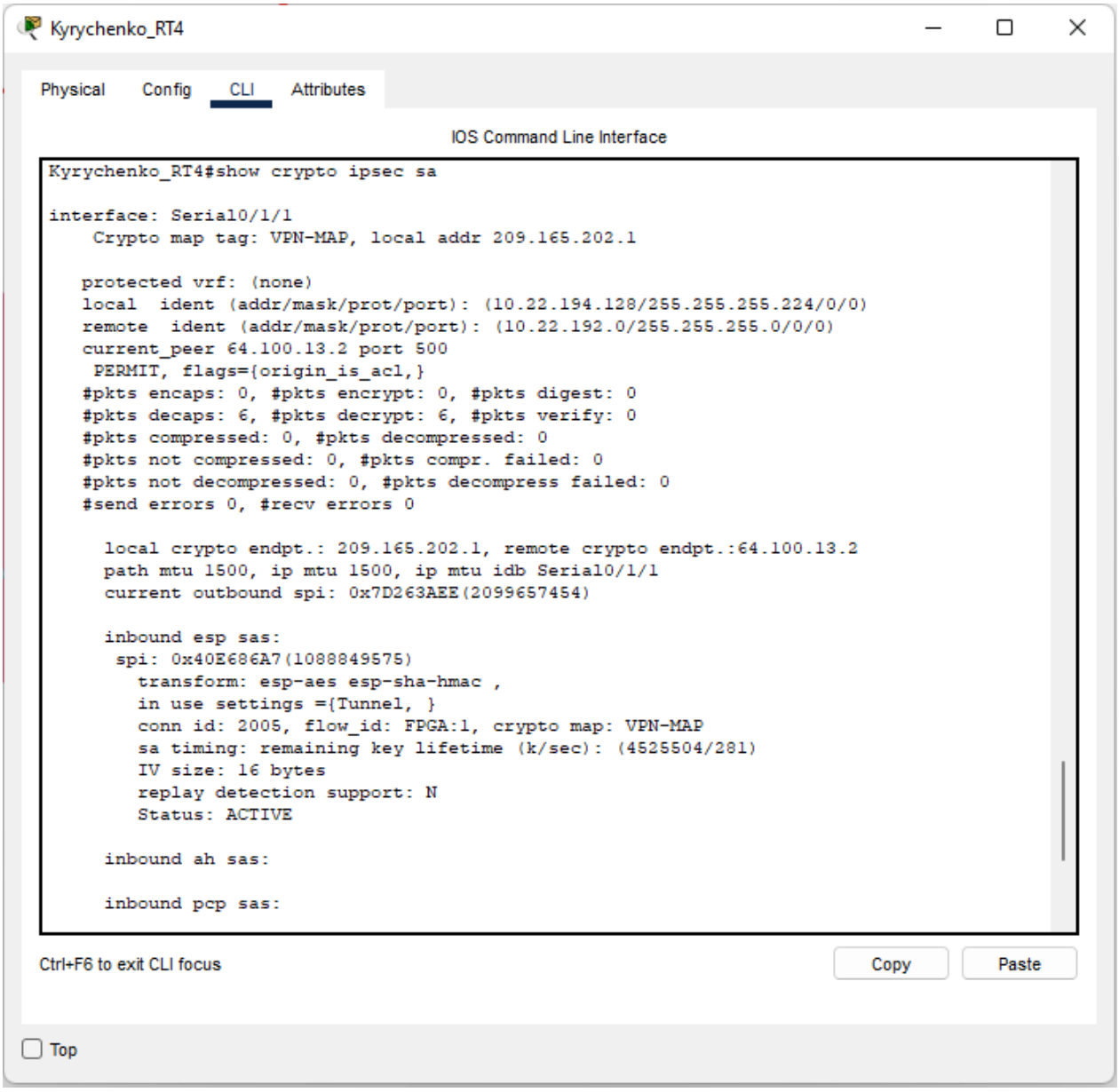

Рисунок 3.12 – Таблиця перетворень протоколу VPN

3.5.4 Налаштування параметрів безпеки комутаторів

Для забезпечення безпеки комутатора можна обмежити кількість мак адрес, які можуть мати доступ до порту. За основу ми візьмемо комутатор Kyrychenko_SW6 та введемо такі команди для забезпечення безпеки порту:

Забезпечимо функцію захисту порту на комутаторі, підключені на сервер:

Kyrychenko_SW6#enable

Kyrychenko_SW6#conf t

Kyrychenko_SW6(config)# interface FastEthernet0/5

Kyrychenko_SW6(config)# switchport mode access

Початок налаштування захисту:

Kyrychenko_SW6(config)#switchport port-security

Дозволити тільки двум вузлам доступ до порту:

Kyrychenko_SW6(config)# switchport port-security maximum 2

Увімкнення запам’ятовування MAC-адрес:

Kyrychenko_SW6(config)# switchport port-security mac-address sticky

Тепер якщо підключити порти і після перегляду таблиці конфігурації комутатора, то можна побачити(Рис. 3.13) які саме мак адреси отримували доступ до порта.

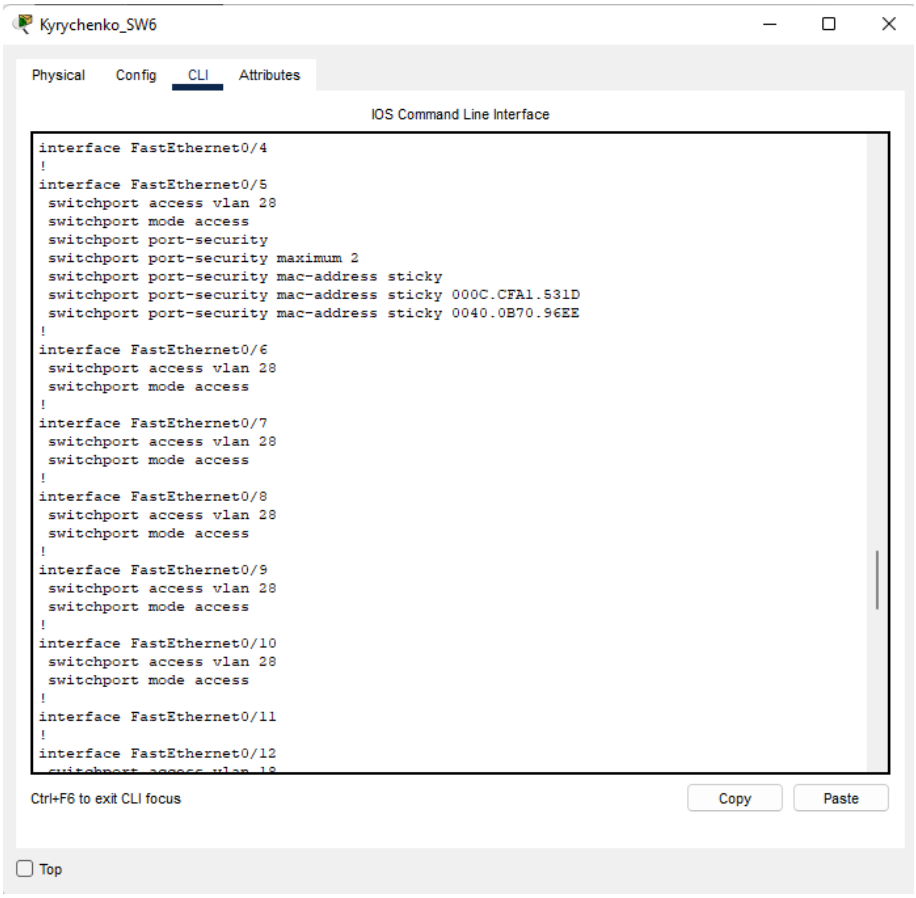

Рисунок 3.13 – Таблиця конфігурації комутатора

4 РОЗРОБКА СИСТЕМИ ІНТЕРНЕТУ РЕЧЕЙ

4.1 Аналіз засобів реалізації функцій пожежної системи засобами IoT

Інтернет речі - це сукупність фізичних об'єктів або груп об'єктів з датчиками та можливостями обробки даних, програмним забезпеченням та іншими технологіями, які з'єднаються в одну комп'ютерну мережу та обмінюються даними між іншими пристроями системи через інтернет або інші засоби зв'язку. Це дозволяє створити оптимізацію та автоматизацію багатьох речей, такі як автоматичне відкриття дверей, зволоження повітря під час читання вологості в кімнаті[7].

Ця область розвивалася за допомогою злиття кількох технологій, які працюють незалежно один від одного і колективно з'єднуються між собою в одну спільну мережу інтернет речей.

У цьому пункті йтиметься про розробку пожежної системи в кімнаті відділу обслуговування клієнтів Туристичної Компанії Круїз. Для цього потрібно поставити три речі:

- Датчик наявності вогню
- Роздавач води під час пожежі
- Точка доступу в інтернет для датчиків та пристроїв
- Сервер для реєстрації та управління інтернет речами

Схема підключення цих датчиків, а також їх розташування показано на скріншоті нижче (Рис. 4.1).

Для функціонування цієї системи потрібно буде створити умови, за яких роздавач води пожежної системи спрацьовуватиме після дачі сигналу від датчика вогню. Все це можна зробити всередині сервера IoT, до якого буде через інтернет підключено інший пристрій.

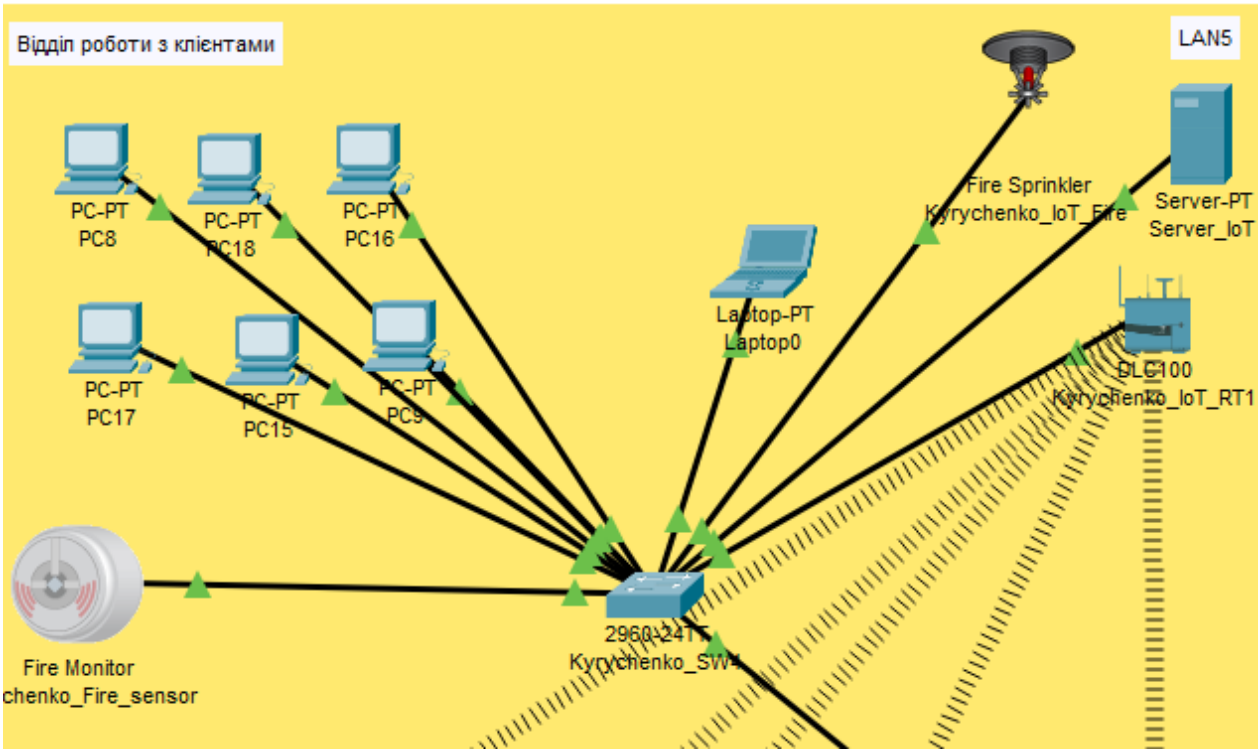

Рисунок 4.1 – Схема розміщення Інтернет речей для пожежної системи

4.2 Аналіз засобів реалізації функцій автоматичного відкриття дверей засобами IoT

Для того, щоб клієнтам не довелося вручну відчиняти двері в приміщення була створена і розроблена система завдяки якому двері автоматично відкриваються при спрацьовуванні датчика руху, для цього потрібно в комп'ютерній мережі інтернет речей розташувати такі речі як:

- двері з функцією автоматичного відчинення за умов
- датчик руху

Схема підключення цих датчиків, а також решта IoT інфраструктура показана на скріншоті нижче(Рис. 4.2).

Для того, щоб двері автоматично відчинялися, потрібно додати умови, при яких функція автоматичного відкривання буде працювати тільки після того, як пройде сигнал від датчика руху, а так само після того, як сигнал перестане йти, двері будуть автоматично зачинятися.

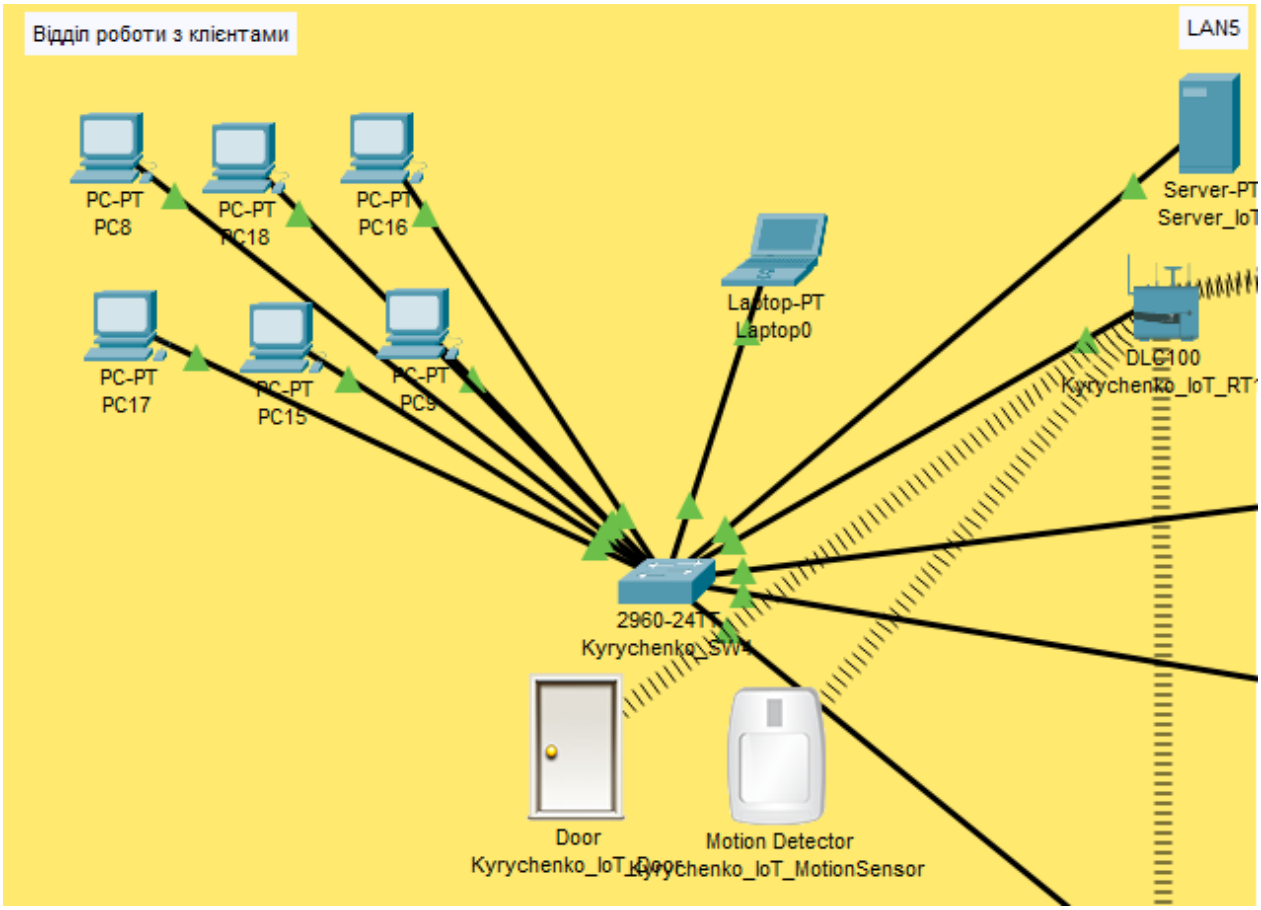

Рисунок 4.2 – Схема розміщення Інтернет речей для автоматичного відкриття дверей

4.3 Аналіз засобів реалізації функцій регулювання температурою у кімнаті засобами IoT

Для покращення робочих умов співробітників агентства, а також для зручності клієнтів була розроблена система, яка дозволяє регулювати температуру в приміщенні за допомогою панелі керування. У разі встановлення температури та включення кнопки на подачі холоду включається кондиціонер, а якщо кнопка встановлена на подачу тепла то кондиціонер відключається та вмикається обігрівач, якщо панель управління не виставлена всі системи відключаються автоматично. Для реалізації цієї системи нам знадобиться:

– панель керування температурою
– розумний кондиціонер
– розумний обігрівач

Схему розміщення цієї системи показано нижче, також показано зв'язок між іншими системами управління IoT.

Для функціонування цієї системи потрібно встановити умови при якій натискання кнопки на позицію холод включається кондиціонер і відключається обігрівач, а при натисканні кнопки на позиції тепло включався обігрівач але відключався вже кондиціонер. Інакше всі функції обігрівача та кондиціонера відключалися.

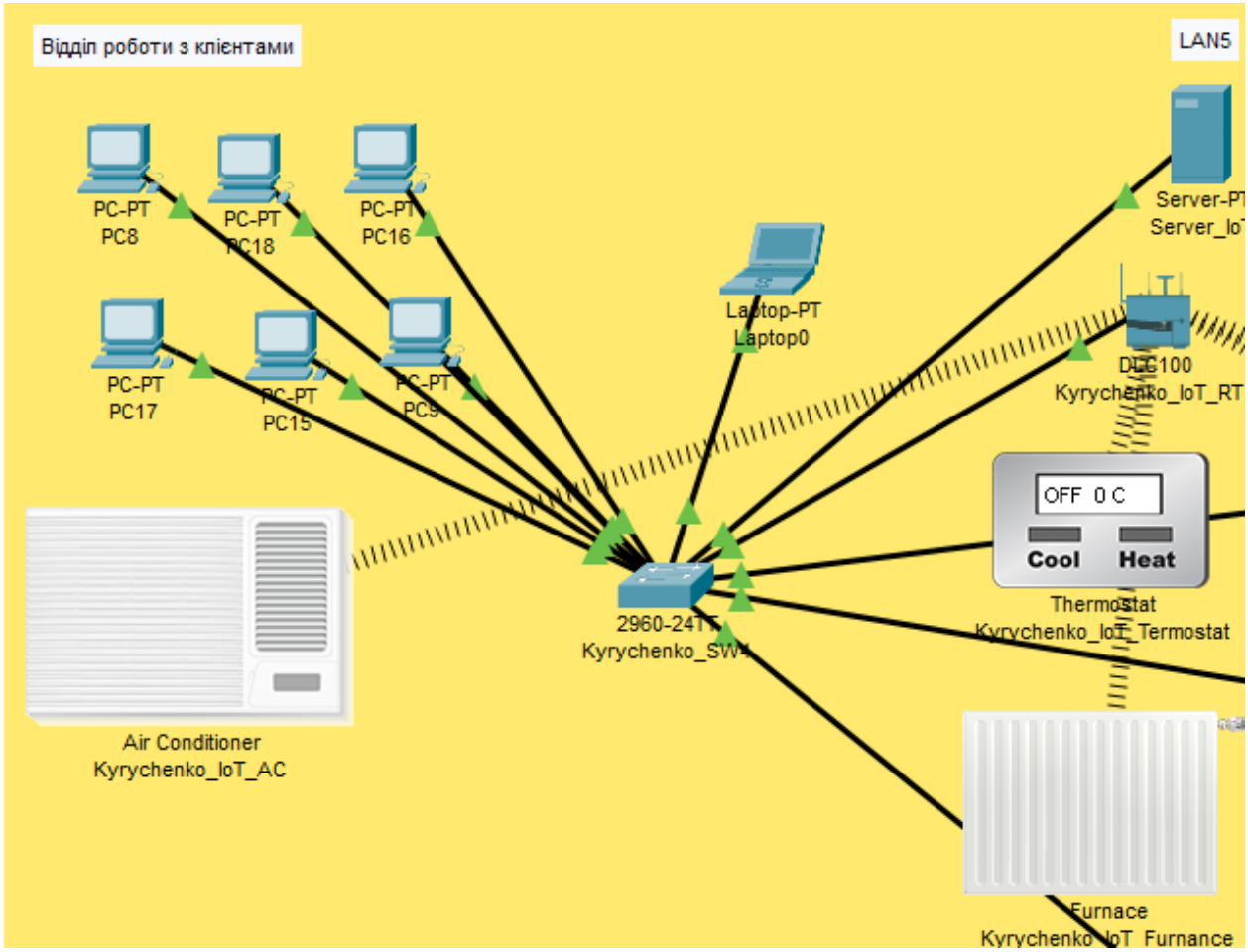

Рисунок 4.3 – Схема розміщення Інтернет речей для роботи системи обігріву та кондиціювання

4.4 Налаштування обладнання та сервісів системи IoT

Спочатку потрібно встановити сервер і маршрутизатор для підключення IoT, а також зробити їх базове налаштування. Для початку ми поставимо сервер і підключимо до нього функцію IoT(Рис. 4.4), а також дамо йому динамічний IP адрес.

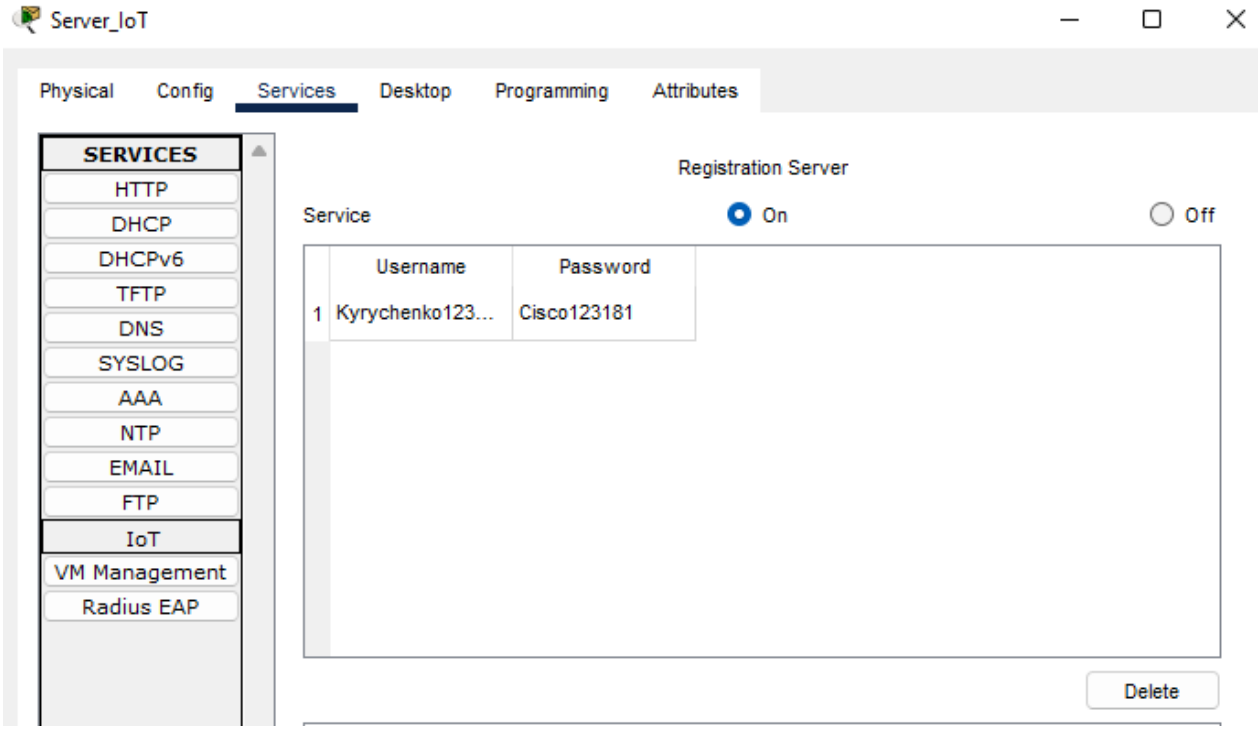

Рисунок 4.4 – Налаштування функції IoT на сервері

Далі потрібно поставити та налаштувати маршрутизатор для роздачі бездротової мережі та задати йому пул IP адрес, які будуть призначені для датчиків та пристроїв IoT. Для цього потрібно увійти в налаштування маршрутизатора і ввести ім'я та пароль для бездротової мережі як показано нижче(Рис. 4.5).

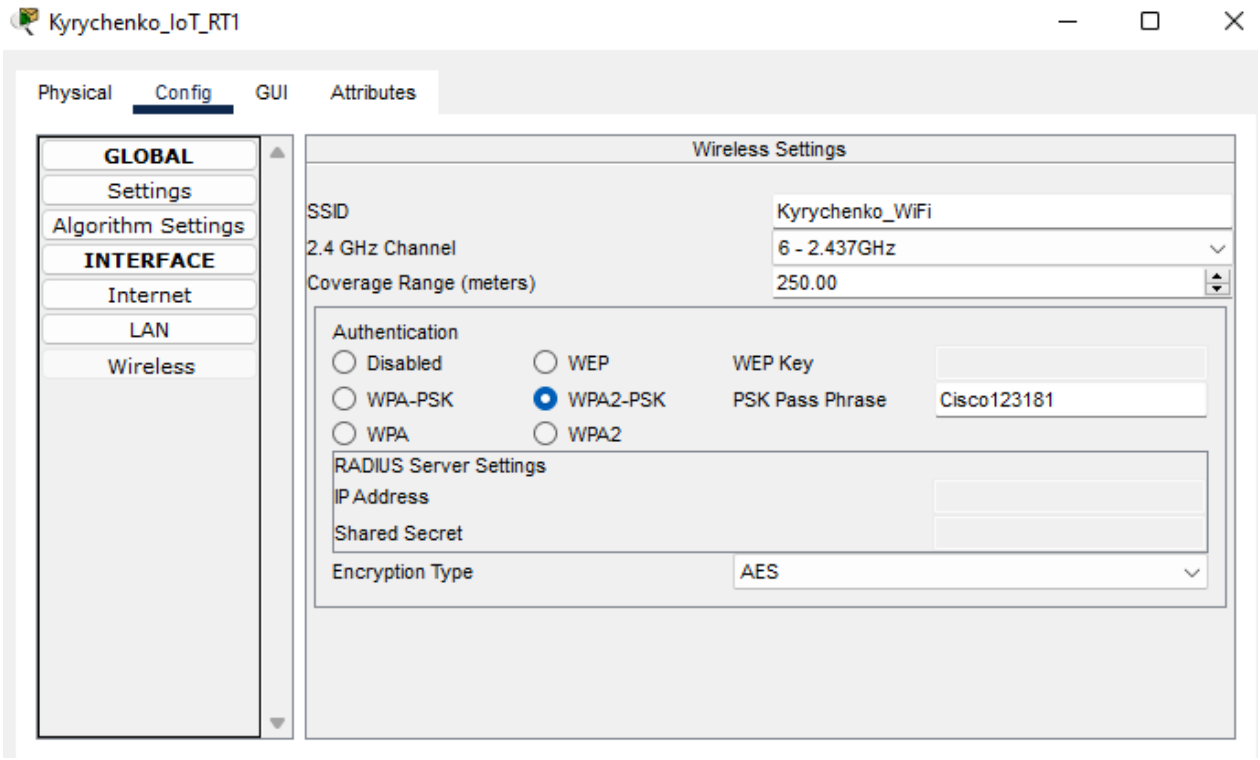

Рисунок 4.5 – Налаштування бездротової мережі

Після налаштування сервера та маршрутизатора для IoT потрібно підключитися пристроєм до сервера для подальших налаштувань функціоналу системи. Далі показаний приклад для налаштування автоматичного відкриття та закриття дверей за умови роботи датчика руху.

Насамперед потрібно встановити датчик руху, а також двері з автоматичним відчиненням і підключити ці пристрої до бездротового маршрутизатора для отримання IP адреси це показано нижче(Рис. 4.6), а також підключиться до сервера IoT як показано нижче(Рис. 4.7).

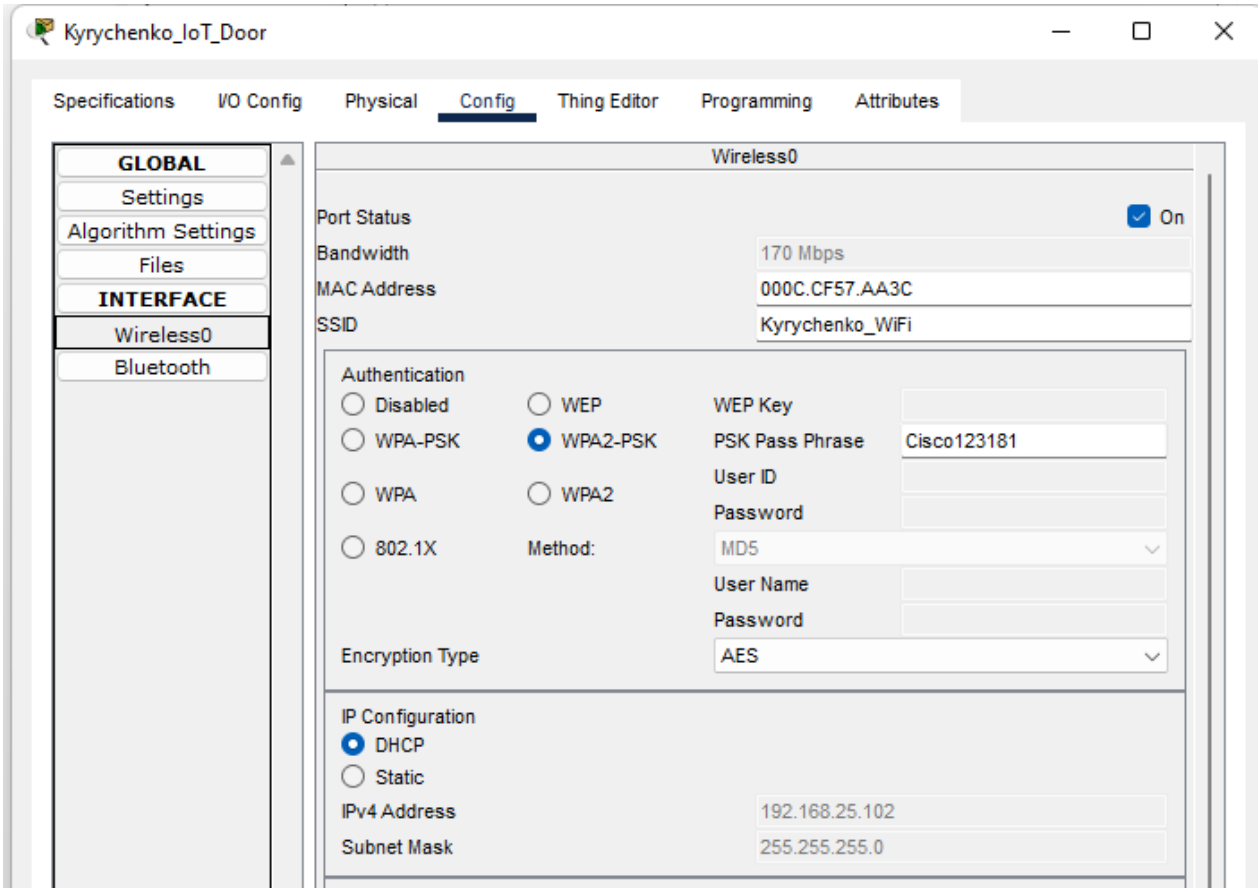

Рисунок 4.6 – Підключення двері до бездротової мережі

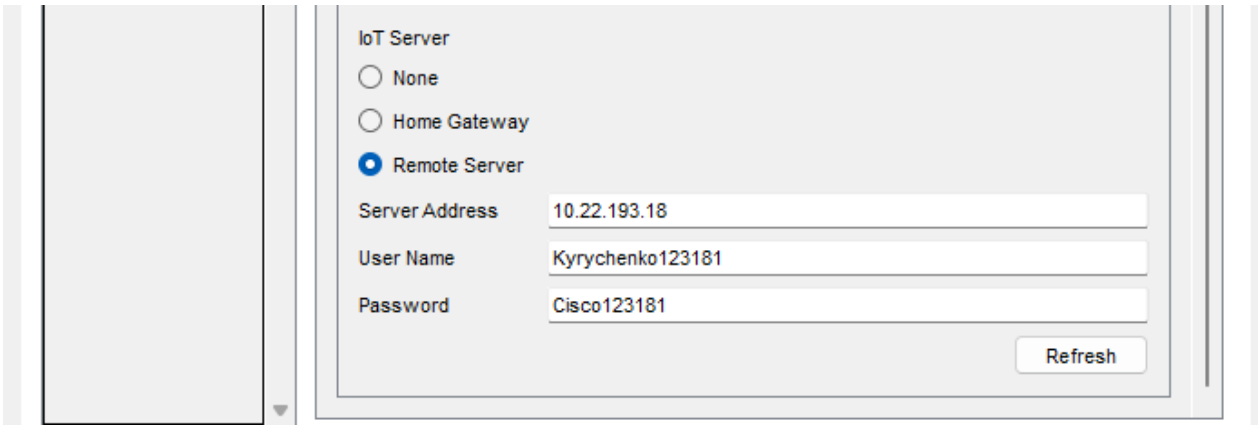

Рисунок 4.7 – Підключення двері до серверу IoT

Далі ми входимо в управління функціями девайсів IoT через будь-який пристрій що підключено до мережі та вводимо IP адресу сервера, логін та пароль від облікового запису IoT. Ми бачимо всі підключення до мережі пристрою і нам потрібно увійти до управління умовами та діями.

Ми створюємо нову дію, як показано нижче(Рис. 4.8), і встановлюємо умову, що при виклики датчика руху двері в полі активації будуть відчинені.

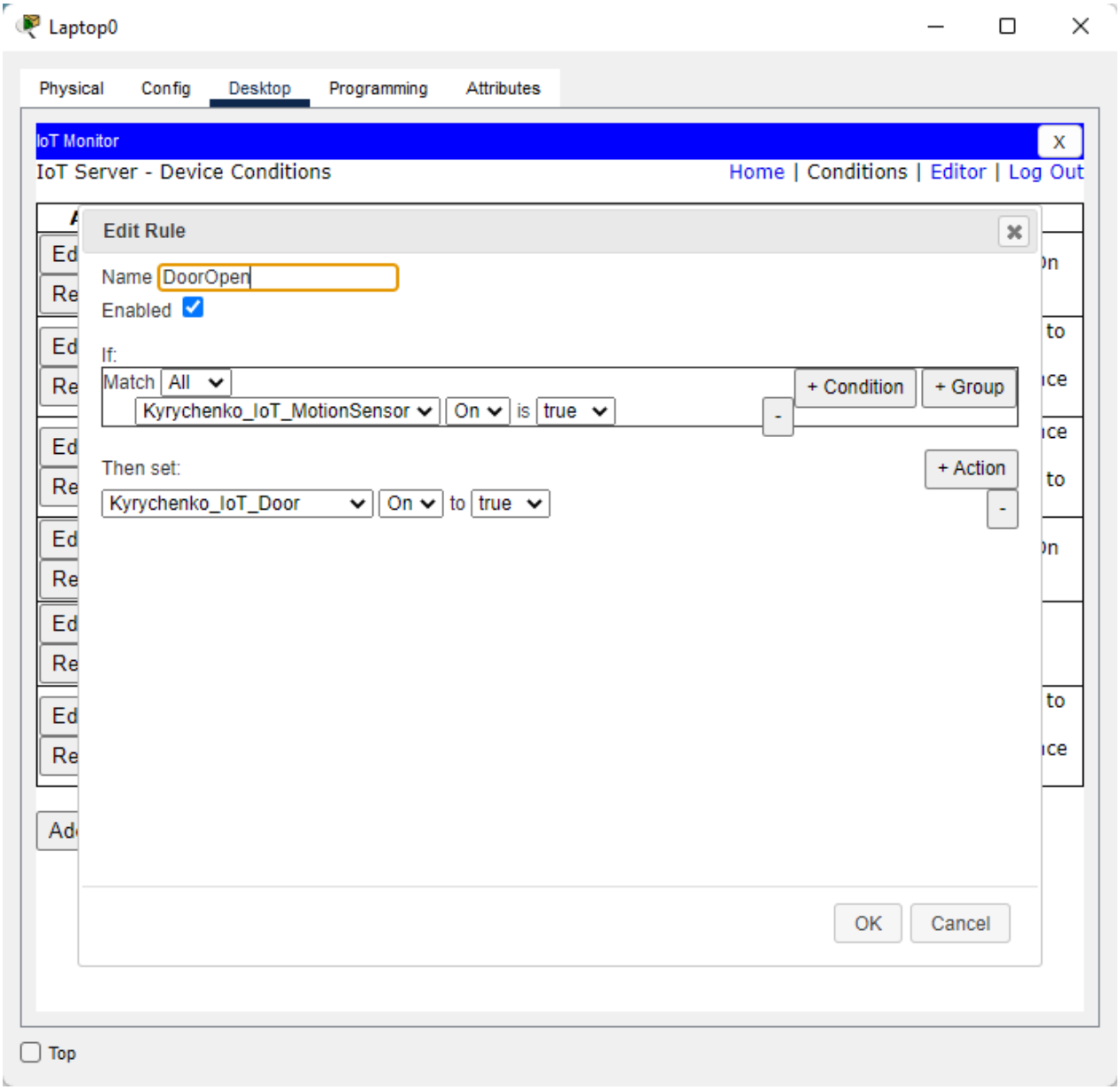

Рисунок 4.8 - Налаштування умов відкриття дверей

Далі ми проводимо подібні налаштування на закриття дверей, а також на інших пристроях для функціонування системи обігріву і кондиціювання, а також системи пожежогасіння. Після цього система IoT вважатиметься налаштованою та функціональною.

ВИСНОВОК

У цій кваліфікаційній роботі було розроблено комп'ютерну модель системи мережі для Туристичної Агенції Круїз. Комп'ютерна мережа була розроблена відповідно до технічних завдань кваліфікаційної роботи, а також ієрархічної та організаційної структури підприємства.

Підприємство було розділено на підмережі, які відповідали тим чи іншим відділам компанії, а також на VLAN для економії мережевого обладнання. Кожної підмережі був доданий маршрутизатор, комутатор або комутатор, і комп'ютери. Підмережі були налаштовані так, щоб мати спосіб взаємодії між собою, а також мати загальний вихід у мережу інтернет. Для таких налаштувань заздалегідь було зроблено розрахунки пропускної спроможності та розрахунки адресацій мережі за допомогою методу розбиття мережі на підмережі VLSM. Корпоративна мережа складається з п'яти підмереж, одна з яких виконує функцію віддаленої локальної підмережі.

Так само при проведенні розрахунків пропускної спроможності цієї комп'ютерної мережі було з'ясовано, що дана мережа відповідає всім вимогам, які були поставлені, а так само в ній є достатній запас для подальшого розширення мережі. З цього випливає, що під час функціонування працівники підприємства не зіштовхнуться із затримками, зупинками та іншими проблемами комп'ютерної мережі, які можуть призвести до небезпечних наслідків.

Так само мережа володіє функціоналом який дозволяє убезпечити мережу від несанкціонованого доступу, для цього деякі порти які знаходяться на комутаторах мають обмеження на кількість підключених до них пристроїв за mac адресою. У мережі налаштована технологія NAT, що дозволяє співробітникам та клієнтам Туристичної Агенції Круїз виходити в глобальну

мережу інтернет, а також VPN, що дозволяє між двома підсистемами безпечно передавати дані.

Після цього в цій комп'ютерній мережі, у підсистемі відділу для роботи з клієнтами було налагоджено технологію інтернет речей. Це було реалізовано шляхом додавання сервера, а також маршрутизатора IoT, що дозволяє за допомогою датчика руху відкривати автоматично двері, а при появі пожежі включати систему пожежогасіння. Також була реалізована функція обігріву та кондиціювання, яка керується шляхом перемикання кнопок на контролері управління.

З усього цього випливає, що комп'ютерна система, що була створена, розрахована і налаштована в цій кваліфікаційній роботі, охоплює всі поставлені вимоги і може повноцінно функціонувати в рамках Туристичної Агенції Круїз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Методичні рекомендації до виконання кваліфікаційної роботи бакалавра студентами галузі знань 12 інформаційні технології спеціальності 123 комп'ютерна інженерія.
2. Computer Success Since 2004: https://computersuccess.com/
3. Характеристики комутатора Cisco Catalyst 2960 Series Switches: https://www.cisco.com/c/en/us/support/switches/catalyst-2960-series-switches/series.html
4. Характеристики маршрутизатора Cisco 4331 Integrated Services Router: https://www.cisco.com/c/en/us/support/routers/4331-integrated-services-router-isr/model.html
5. Маска підмережі змінної довжини, розрахунок за методом VLSM: https://www.techtarget.com/searchnetworking/definition/variable-length-subnet-mask
6. Перетворення мережевих адрес (NAT) та налаштовування протоколу NAT: https://uk.wikipedia.org/wiki/NAT
7. Інтернет речей (IoT) та налаштовування технології IoT: https://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/iot_fnd/guide/4_8/b-iot-fnd-user-guide-48.html
8. Віртуальна приватна мережа(VPN) та налаштування VPN: https://www.cisco.com/c/en/us/td/docs/security/vpn_modules/6342/vpn_cg/6342site3.html
9. Протокол динамічної конфігурації вузла (DHCP) та його налаштування: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/xe-3se/3850/dhcp-xe-3se-3850-book/config-dhcp-server.html

10. Віртуальна локальна комп'ютерна мережа (VLAN) та налаштування VLAN:https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst1000/software/releases/15_2_7_e/configuration_guides/vlan/b_1527e_vlan_c1000_cg/configuring_vlan.html
11. Cisco DNA архітектура на основі контролера: https://www.secureitstore.com/DNA.asp#:~:text=Cisco%20DNA%20is%20a%20controller,protect%20against%20degradation%20and%20threats.
12. Вимоги до патентної чистоти: https://www.msp-patent.com.ua/ua/8-chto-takoe-patentnaya-chistota.html
13. Enhanced Interior Gateway Routing Protocol (EIGRP) та його налаштування: https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html

ДОДАТОК А

Текст програми налаштування мережі комп’ютерної системи

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

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ КОМП'ЮТЕРНОЇ СИСТЕМИ ТУРИСТИЧНОЇ АГЕНЦІЇ КРУЇЗ

Текст програми

804.02070743.22028-01 12 01

Листів 8

2022

87

АНОТАЦІЯ

Ця програма містить конфігураційні установки маршрутизаторів і комутаторів для комп'ютерної системи Туристичної Компанії Круїз. У ній налаштовані протоколи DHCP, NAT та маршрутизація між маршрутизаторами, у конфігураційному файлі комутатора містяться налаштування VLAN.

ЗМІСТ

1. Конфігураційне налаштування Kyrychenko_RT4
2. Конфігураційне налаштування Kyrychenko_SW6

Kyrychenko_RT4

```
Current configuration : 2053 bytes
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
hostname Kyrychenko_RT4
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
ip dhcp excluded-address 10.22.194.129 10.22.194.130
ip dhcp pool NET2
 network 10.22.194.128 255.255.255.224
 default-router 10.22.194.129
 dns-server 10.22.193.242
 domain-name kyrychenko.com
no ip cef
no ipv6 cef
username 123181_Kyrychenko privilege 15 password 7
082048430017061E010803
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
crypto isakmp key vpnpa address 64.100.13.2
crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
crypto map VPN-MAP 10 ipsec-isakmp
 description VPN to LAN4
 set peer 64.100.13.2
```

```
 set transform-set VPN-SET
 match address 110
ip ssh version 1
ip domain-name Kyrychenko_RT4
spanning-tree mode pvst
interface GigabitEthernet0/0/0
 no ip address
 duplex auto
 speed auto
 shutdown
interface GigabitEthernet0/0/1
 ip address 10.22.194.129 255.255.255.224
 ip nat inside
 duplex auto
 speed auto
interface GigabitEthernet0/0/2
 no ip address
 duplex auto
 speed auto
 shutdown
interface Serial0/1/0
 ip address 10.0.8.10 255.255.255.252
 ip nat inside
 clock rate 128000
interface Serial0/1/1
 ip address 209.165.202.1 255.255.255.252
 ip nat outside
```

```
 crypto map VPN-MAP
interface Vlan1
 no ip address
 shutdown
router eigrp 100
 network 10.22.194.128 0.0.0.31
 network 209.165.202.0 0.0.0.3
 network 10.0.8.8 0.0.0.3
ip nat pool Internet 209.165.200.5 209.165.200.30 netmask 255.255.255.224
ip nat inside source list 8 pool Internet
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/1/1
ip flow-export version 9
access-list 8 permit 10.22.194.128 0.0.0.31
access-list 110 permit ip 10.22.194.128 0.0.0.31 10.22.192.0 0.0.0.255
banner motd ^CKyrychenko M.O. 123-18-1^C
line con 0
 password 7 0822455D0A16
 login
line aux 0
line vty 0 4
 password 7 0822455D0A16
 login
 transport input ssh
end
```

Kyrychenko_SW6

Current configuration : 2634 bytes

version 15.0

no service timestamps log datetime msec

no service timestamps debug datetime msec

service password-encryption

hostname Kyrychenko_SW6

enable secret 5 1mERr$9cTjUIEqNGurQiFU.ZeCi1

ip ssh version 1

ip domain-name Kyrychenko_SW6

username 123181_Kyrychenko privilege 15 password 7

082048430017061E010803

spanning-tree mode pvst

spanning-tree extend system-id

interface FastEthernet0/1

interface FastEthernet0/2

interface FastEthernet0/3

interface FastEthernet0/4

interface FastEthernet0/5

 switchport access vlan 28

 switchport mode access

 switchport port-security

 switchport port-security maximum 2

 switchport port-security mac-address sticky

 switchport port-security mac-address sticky 000C.CFA1.531D

 switchport port-security mac-address sticky 0040.0B70.96EE

interface FastEthernet0/6

```
 switchport access vlan 28
 switchport mode access
interface FastEthernet0/7
 switchport access vlan 28
 switchport mode access
interface FastEthernet0/8
 switchport access vlan 28
 switchport mode access
interface FastEthernet0/9
 switchport access vlan 28
 switchport mode access
interface FastEthernet0/10
 switchport access vlan 28
 switchport mode access
interface FastEthernet0/11
interface FastEthernet0/12
 switchport access vlan 18
 switchport mode access
interface FastEthernet0/13
 switchport access vlan 18
 switchport mode access
interface FastEthernet0/14
 switchport access vlan 18
 switchport mode access
interface FastEthernet0/15
 switchport access vlan 38
 switchport mode access
```

```
interface FastEthernet0/16
 switchport access vlan 38
 switchport mode access
interface FastEthernet0/17
 switchport access vlan 38
 switchport mode access
interface FastEthernet0/18
 switchport access vlan 38
 switchport mode access
interface FastEthernet0/19
 switchport access vlan 38
 switchport mode access
interface FastEthernet0/20
 switchport access vlan 38
 switchport mode access
interface FastEthernet0/21
 switchport access vlan 38
 switchport mode access
interface FastEthernet0/22
 switchport access vlan 38
 switchport mode access
interface FastEthernet0/23
 switchport access vlan 38
 switchport mode access
interface FastEthernet0/24
 switchport access vlan 38
 switchport mode access
```

```
interface GigabitEthernet0/1
 switchport mode trunk
interface GigabitEthernet0/2
 switchport mode trunk
interface Vlan1
 ip address 10.22.193.130 255.255.255.128
banner motd ^CKyrychenko M.O. 123-18-1^C
line con 0
 password 7 0822455D0A16
 login
line vty 0 4
 password 7 0822455D0A16
 login
 transport input ssh
line vty 5 15
 login
end
```