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

Навчально-науковий
інститут електроенергетики
(інститут)
Факультет інформаційних технологій
(факультет)
Кафедра інформаційних технологій та комп'ютерної інженерії
(повна назва)

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента Буряченка Салтана Дмитровича
(ПІБ)
академічної групи 123-20зск-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 компанії "Lifecell" з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі»
(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	доц. Бешта Д.О.			
розділів:				
розробка апаратної частини	доц. Ткаченко С.М.			
розробка корпоративної мережі	ас. Бешта Л.В.			

Рецензент				

Нормоконтролер	проф. Цвіркун Л.І.			

Дніпро

2023

ЗАТВЕРДЖЕНО:
завідувач кафедри
інформаційних технологій
та комп'ютерної інженерії
(повна назва)
_____ Гнатушенко В.В.
(підпис) (прізвище, ініціали)

«__»_____2023 року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавр

студента Буряченка С.Д. **академічної групи** 123-20зск-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 компанії "Lifecell" з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі»

затверджену наказом ректора НТУ «Дніпровська політехніка» від 11.04.2023 № 256-с

Розділ	Зміст	Термін виконання
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел конкретизується предмет та мету роботи та виконується постановка завдання	10.05.2023
Розробка апаратної частини	На основі аналізу підприємства формулюються технічні вимоги до комп'ютерної системи та розробляється апаратна частина системи	17.05.2023
Розробка корпоративної мережі	Виконується розрахунок налаштувань корпоративної мережі та перевірка роботи системи, розробляються методи та налаштування обладнання для захисту інформації в системі	24.05.2023
Розробка компонента системи	Виконується детальна розробка компонента системи	31.05.2023

Завдання видано _____ доц. Бешта Д.О.
(підпис керівника) (прізвище, ініціали)

Дата видачі 25.01.2023

Дата подання до екзаменаційної комісії 12.07.2023

Прийнято до виконання _____ Буряченко С.Д.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 62 с., 28 рис., 9 табл., 1 дод., 10 джерел.

ВІДДІЛ ЗВ’ЯЗКУ, ПІДМЕРЕЖА, АДМІНІСТРАТИВНИЙ ПДРОЗДІЛ, WAN, LAN

Об’єкт: комп'ютерна система компанії "Lifecell" з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі.

Мета: розробка та проектування мережі компаніїї з використанням сучасних технологій для реалізації безпеки та функціонування.

Комп’ютерна мережа спрямована на створення підрозділів мережі для обслуговування клієнтів та наданню послуг телефонного зв’язку. Мережа має розташовуватись в Україні, м.Дніпро. Налаштування мережі виконується виключно за допомогою стеку протоколів TCP/IP.

Налаштування мережі відбувається за планом роботи замовника та моделюється в додатку Cisco Packet Tracer. До проекту були розроблені схеми підключення мережевих пристроїв, схеми IP-адресації пристроїв та схеми розташування всіх підрозділів.

Пояснювальна записка містить в собі повний перелік таблиць та графічної частини і має перевірку працездатності мережі.

Мережа підтримує можливу майбутню модернізацію та масштабованість без глобального переналаштування або заміни мережевих компонентів корпоративної мережі.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАК, ОДИНИЦЬ І ТЕРМІНІВ

СКС – структуровані кабельні системи;

LACP – агрегування портів комутаторів;

IoT – технології інтернету речей або автоматизованих систем;

OSPF – мережевий протокол, який забезпечує обмін даними між підмережами;

DHCP – протокол автоматизованого налаштування адресації пристроїв;

VLAN – технологія розподілу мережі на підмережі;

ACL – правила керування мережею;

AAA – протокол безпеки мережевого обладнання;

SC – оптоволокно.

ВСТУП

Проблемою та ідеєю написання кваліфікаційної роботи є зростання людини як професійного фахівця в своїй сфері діяльності. Найбільша кількість представників інших професійних галузей прагнуть перейти саме в ІТ-сферу. Сучасні інформаційні технології мають тенденцію досить швидкого розвитку. Завдяки інтернету, нам стає доступна майже будь-яка інформація. Майже кожна компанія в будь-якій галузі праці має свою локальну мережу та свій ІТ-відділ.

Завданням проєкту є створення корпоративної мережі компанії з повним описом, обгрунтуванням та налаштуванням мережі. Для виконання повного об'єму роботи повинні бути виявлені вимоги проєкту, його структура та аналіз актуальності системи у наш час.

Кожна компанія, яка має цілі високого зростання – має свою корпоративну мережу.

Корпоративна мережа – це локальна мережа, яка служить для підключення співробітників до централізованого інформаційного вузла компанії. Всі вузли мережі мають зв'язок між собою.

Для початку реалізації проєкту потрібно обрати певну топологію мережі.

Топологія мережі – це система, за якою будуть налаштовані вузли мережі та виставлений рівень безпеки кожного вузла та мережевого обладнання, таких як – маршрутизатор та комутатор.

При налаштуванні мережі будуть використовуватися протоколи стеку TCP/IP.

Стек протоколів TCP/IP – це набір мережевих протоколів або, інакше кажучи, набір правил обміну інформацією, за якими працює сучасна корпоративна мережа компанії.

Застосовувати технології кваліфікаційної роботи можна в різних галузях та підприємствах. Мережева інфраструктура описує кожний шлях налаштування мережевих пристроїв та персональних пристроїв всіх користувачів мережею. Фізична розробка структурованих кабельних систем та впровадження робочих

станцій – є інженерним рішенням, яке побудовано на вимогах та завданні кваліфікаційної роботи.

У зв'язку з частим використанням комп'ютерних мереж у побутовій роботі, кваліфікаційна робота слугуватиме інструкцією для побудови мережі.

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

1.1 Опис умов застосування корпоративної мережі компанії

Комп’ютерна мережа компанії – це система об'єднання комп'ютерів, серверів та інших пристроїв в межах компанії. Вона забезпечує обмін даними, спільний доступ до ресурсів, комунікацію та роботу між співробітниками. Мережа включає в себе локальну мережу (Local Area Network, LAN), яка охоплює декілька будівель, а також об'єднує розподілені мережі, які з'єднують віддалені офіси компанії.

Мережа використовується для надання технічної підтримки клієнтам або користувачам певних продуктів або послуг. Це може включати вирішення технічних проблем, відповіді на запитання, консультації та інші форми підтримки.

Використовується для керування заявками та тикетами, що стосуються технічної підтримки. Це включає прийом, реєстрацію, відстеження та вирішення заявок від клієнтів.

Дозволяє забезпечити зв'язок між технічними спеціалістами та клієнтами для обміну інформацією, вирішення проблем та надання підтримки. Це може бути здійснено через телефонні дзвінки, електронну пошту, чат або інші засоби комунікації.

Також, використовується для зберігання і обміну інформацією, пов'язаною з технічною підтримкою. Це може включати базу знань, документацію, посібники, відео-інструкції та інші ресурси, які допомагають технічним спеціалістам вирішувати проблеми.

Мережа може включати інструменти моніторингу та аналізу, які допомагають відстежувати продуктивність технічної підтримки, виявляти тренди, ідентифікувати проблемні зони та приймати відповідні заходи.

Мережа повинна мати механізми безпеки для захисту конфіденційної інформації клієнтів, а також для запобігання несанкціонованому доступу до систем та ресурсів технічної підтримки.

1.2 Діяльність та процеси роботи компанії «Lifecell»

Lifecell – це компанія, яка надає послуги мобільного зв’язку та передачі даних. Компанія Lifecell належить компанії Turkcell, в свою чергу Turkcell це – найбільший турецький постачальник телекомунікаційних послуг.

Компанія має великий розвиток в мережвій інфраструктурі світу. Дана компанія одна з перших представила технологію мобільного інтернету в Україні 3G та 4G.

Головною розробкою проєкту є створення кол-центрів для обробки клієнтів.

Ключові відділи компанії – це центри, в яких виконуються дзвінки своїм абонентам з метою покращення зв’язку.

Кол-центр – це підрозділ компанії, співробітники якого обробляють дзвінки.

Робота кол-центру зводиться до розвантаження інших відділів від рутинних розмов. Вона ділиться на:

– первинні консультації – оператори відповідають на базові запитання;

– актуалізація лідів – якщо потрібно обдзвонити базу клієнтів і нагадати про співпрацю;

– маршрутизація звернень – якщо менеджер не може відповісти на специфічне запитання клієнта, він допомагає зв'язатися з тим, хто достатньо компетентний для відповіді.

1.3 Структура організації відділів мережі

Організаційна структура компанії – це концепція, яка представляється у вигляді схеми, що відображає відносини між керівництвом і персоналом, розподіляє і закріплює функціонал кожної посади.

Структура відповідає всім вимогам та принципам стратегічного планування, оскільки за рахунок своєї гнучкості здатна масштабувати або переконфігуровувати мережі.

Організаційна структура компанії «Lifecell» складається з адміністративних підрозділів(вищих) та підрозділів обробки клієнтів(нижніх).

Рисунок 1.1 – Схема організаційної структури компанії «Lifecell»

У даній структурі зберігається централізоване управління, що виключає взаємовідносини між підрозділами та багато ієрархічних рівнів.

Адміністративний підрозділ – виконує задачі щодо підтримки своїх користувачів в мережі та надання їм безперешкодного застосування пристроїв.

В обов'язки мережевого адміністратора входить:

– заміна комплектуючих;
– ремонт апаратного забезпечення по можливості;
– аналіз апаратної частини;
– аналіз помилок в системі;
– діагностика мережевих каналів;
– перевірка затримки в мережі.

Вихідна лінія кол-центру – забезпечує потік інформації для клієнтів компанії, задля продажів продуктів сфери діяльності компанії та проводить опитування щодо актуальності продукції.

Вихідна лінія кол-центру(іншомовні) – має всі ті самі обов'язки що і звичайна вихідна лінія, але вони ведуть розмову іноземними мовами.

Вхідна лінія кол-центру використовується як гаряча лінія, технічна підтримка, інформаційна підтримка.

Компонентами організаційної структури є ланки та рівні управління.

ІТ-відділ контролює встановлення та обслуговування комп'ютерної мережі всередині компанії.

Якщо мережева система виходить з ладу, наслідки можуть бути дорогими. Не лише для компанії, а й для зовнішніх організацій, які потребують продуктів чи послуг компанії.

Завдяки сучасним технологіям, структура компанії дозволяє вести безперебійну роботу в кол-центрах.

1.4 Схема фізичного розташування відділів компанії

Оскільки підрозділи не призначені для ведення роботи з співробітниками, а також організації зустрічей з клієнтами, то приміщення можуть бути розташовані на умовах зручності для співробітників.

Всі підрозділи розташовані в 4 різних будівлях, але мають доступ один до одного і мають спільну локальну мережу та знаходяться в Україні, м.Дніпро.

Відстань між підмережами наступна:

– підмережа 1 та підмережа 2 має відстань 8193м;
– підмережа 1 та підмережа 3 має відстань 7230м;
– підмережа 1 та підмережа 4 має відстань 6340м;
– підмережа 3 та підмережа 2 має відстань 2353м;
– підмережа 4 та підмережа 2 має відстань 4865м.

Детальне опрацювання та графічне зображення кожного відділу в середині виконаємо в інших розділах.

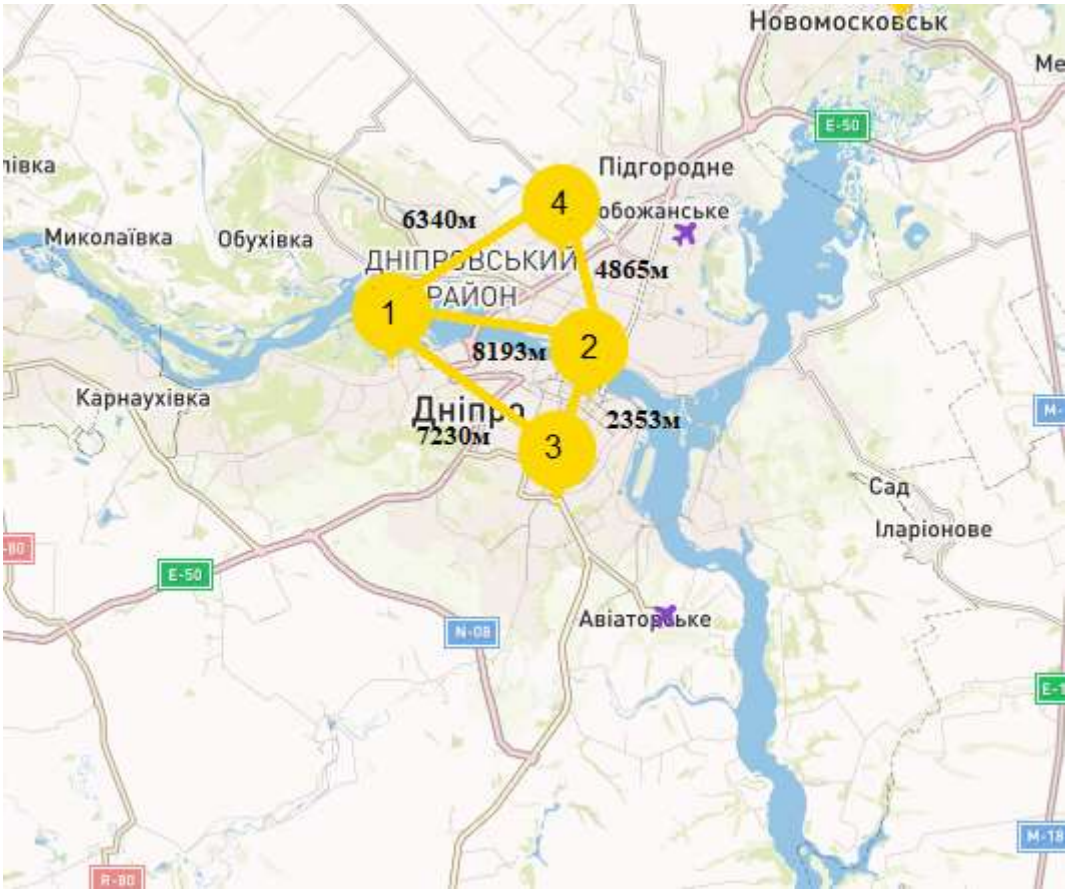

Рисунок 1.2 – Схематичне розташування компанії «Lifecell» у місті

1.5 Огляд відомих рішень щодо способів обробки інформації

Огляд відомих рішень щодо способів обробки інформації в мережі може включати наступні елементи:

1. Централізована обробка, у цьому підході всі дані обробляються на центральному сервері або вузлі мережі. Це може бути вигідно для обробки великого обсягу даних або забезпечення єдиної точки керування. Програмне забезпечення, таке як бази даних, аналітичні інструменти та системи керування, можуть використовуватися для централізованої обробки.

2. Розподілена обробка, у цьому підході обробка даних розподіляється між різними вузлами мережі або обчислювальними пристроями. Кожен вузол може мати обмежені обчислювальні ресурси, але в сукупності вони забезпечують широкі можливості обробки. Розподілені системи, такі як кластери або обчислювальні сітки, можуть використовуватися для розподіленої обробки.

3. Обробка на краю мережі, цей підхід передбачає обробку даних на вузлах мережі, ближчих до джерела збору даних. Це зменшує затримку і обсяг трафіку в мережі, оскільки лише відфільтровані або важливі дані передаються до центральних систем. Вбудовані пристрої або шлюзи можуть використовуватися для обробки на краю мережі.

4. Обчислення в реальному часі, вимоги до обробки даних в реальному часі можуть вимагати спеціалізованих рішень. Системи обробки подій (event processing systems) або потокові аналітичні системи (stream analytics systems) можуть використовуватися для обробки неперервного потоку даних у реальному часі.

5. Обробка у бортових системах, у випадку мобільних або вбудованих систем обробка даних може здійснюватися безпосередньо на пристрої. Це може бути вигідно для забезпечення швидкості обробки та збереження приватності даних.

6. Гібридні рішення, часто реалістичним підходом є використання комбінації різних способів обробки в мережі. Наприклад, можна поєднувати централізовану та розподілену обробку, використовувати обчислення на краю мережі для передобробки даних та обчислення в реальному часі для важливих подій.

1.6 Завдання і мета роботи

Мета роботи полягає у вивченні практичних навичок на підприємстві та демонстрації навичок при налаштуванні компонентів мережі. У завдання кваліфікаційної роботи входять методичні вказівки та вимоги від замовника до побудови корпоративної мережі.

Перелік поставлених завдань для виконання:

1. Розробити архітектуру корпоративної мережі, що задовольняє потребам компанії у швидкісному та надійному обміні даними;

2. Вибрати та налаштувати оптимальні мережеві пристрої для побудови мережної інфраструктури;

3. Визначити необхідну пропускну здатність мережі для забезпечення ефективного обміну даними;

4. Розробити заходи безпеки мережі з урахуванням потреб компанії та застосування відповідних заходів безпеки;

5. Провести тестування та оптимізацію мережі для забезпечення її ефективності та надійності;

6. Налагодити маршрутизації між підмережами та встановити вихід локальної мережі у мережу Інтернет;

7. За заданою топологією (рисунок 1.3) розробити апаратну складову кожної підмережі для обробки інформації;

8. За технологіями IoT розробити систему безпеки доступу в офісне приміщення.

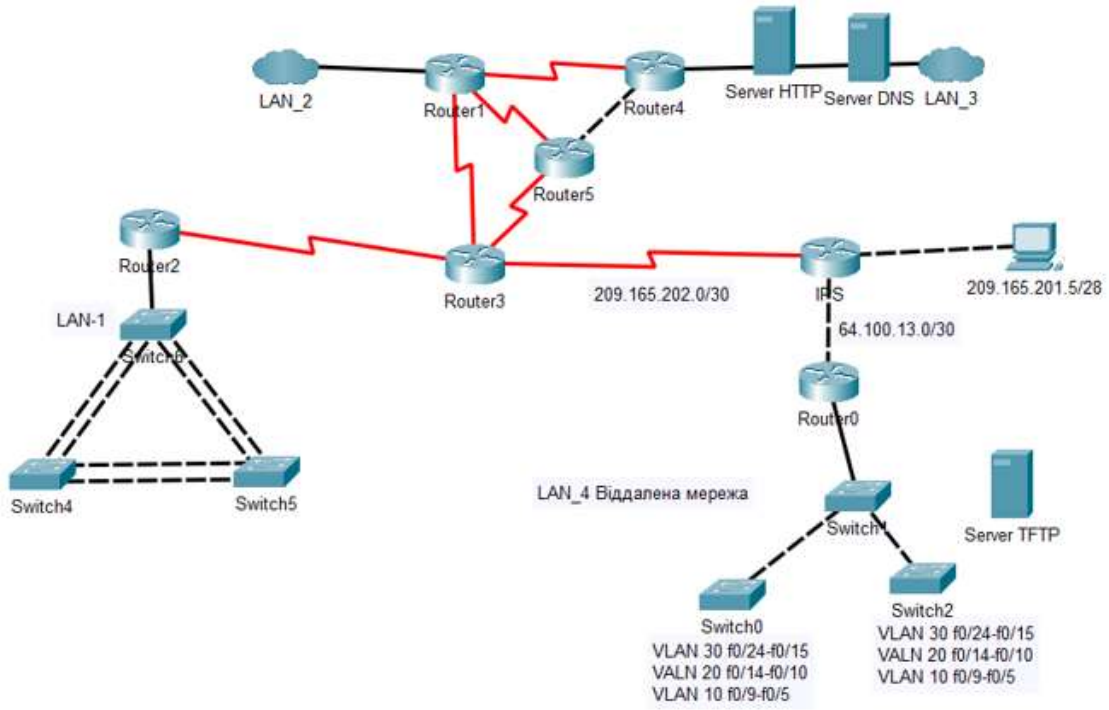

Рисунок 1.3 – Загальна топологія мережі компанії «Lifecell»

1.7 Визначення можливих напрямків рішення поставлених завдань

Для вирішення поставлених завдань у пункті 1.6 необхідно розробити мережеву систему з повним переліком налаштувань.

Для вирішення завдання з працездатністю фізичного обладнання мережі потрібно розробити специфікацію апаратних та програмних засобів.

Після побудови апаратної складової для кожної підмережі необхідно розробити структурну схему комплексу технічних засобів та кінцевий варіант графічного зображення топології мережі компанії «Lifecell».

Підтвердити апаратну та програмну спроможність мережі можна за допомогою розрахунку інтенсивності вихідного трафіку. При цьому, значення потрібно використовувати для найбільшої локальної мережі підприємства.

Для топології мережі зробити розрахунок налаштувань та скласти список необхідних рішень.

Побудова мережі на фізичному рівні потребує розрахунку схеми адресації підмереж та схеми адресації пристроїв в підмережах.

Після розрахунку IP-адресації необхідно виконати наступні налаштування в мережі:

– базове налаштування конфігурації пристроїв;
– сегментації ip-адрес;
– протоколу рівня маршрутизації;
– правил віртуальної мережі;
– резервування дротового підключення в мережі;
– підмереж корпоративної мережі;
– параметрів безпеки маршрутизаторів.

На завершення проекту необхідно виконати перевірку роботи комп’ютерної мережі.

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

2.1.1.1.1 Перелік підсистем, їхнє призначення й основні характеристики, вимоги до числа рівнів ієрархії та ступені централізації мережевої інфраструктури

Розробка апаратної частини повинна залежати від кількості напрямків діяльності компанії «Lifecell» Вона надає послуги мобільного зв'язку, тому згідно топології мережі, корпоративна мережа повинна поділятися на окремі локальні мережі, але при цьому повинні мати доступ до загальної точки інформації.

Отримані локальні мережі:

– адміністративний підрозділ;
– вихідна лінія зв'язку;
– вихідна лінія зв'язку(іншомовні);
– вхідна лінія зв'язку.

Дані мережі не мають між собою ієрархії управління, вони мають рівні права в мережі, але працюють за різними напрямами. Керуючим органом компанії є директор та заступник директора, згідно організації мереж (рисунок 1.1).

Головною характеристикою мережі є – централізоване обслуговування задач клієнтів щодо налаштування мобільного зв'язку. Так як це одна компанія, необхідно реалізувати зв'язок між підмережами.

Мережа повинна мати спроможність мережевого обладнання для підключення пристроїв, в залежності від кількості людей в кожній мережі.

Спроможність мережевого обладнання повинна забезпечувати:

– кількість людей в 1 мережі – 34;
– кількість людей в 2 мережі – 29;
– кількість людей в 3 мережі – 6;
– кількість людей в 4 мережі – 42.

Тобто, загальна кількість людей, яку повинно підтримувати мережеве обладнання мережі складає – 111 осіб.

Безпека офісного приміщення повинна бути розроблена за допомогою інтернет речей. До складу системи повинно входити:

– 2 RFID-зчитувача;
– 4 RFID-мітки;
– 2 IoT-двері;
– 2 IoT-web-камери.

2.1.1.1.2 Вимоги до способів і засобів зв’язку для обміну інформації між компонентами мережевих пристроїв

Обмін інформацією між мережами повинен здійснюватися за допомогою маршрутизаторів. Щоб виконати умову – отримання пакетів даних з однієї мережі та направити їх до призначення через іншу мережу потрібно використати протокол маршрутизації. Визначення найкоротшого шляху для передачі даних між мережами повинен виконувати протокол динамічної маршрутизації OSPF.

Для передачі інформації також потрібно використовувати кабельні з'єднання та використовувати мідні та оптоволоконні кабелі.

Отримані мережі в пункті 2.1.1.1.1 повинні застосовувати наступні технології:

– логічну ізоляція за технологією VLAN;
– резервування дротового підключення за допомогою агрегації;
– безпечне управління пристроями по протоколу SSH з використанням протоколу транспортного рівня TCP.

2.1.1.1.3 Вимоги до режимів функціонування кожної підмережі

Вихідна лінія кол-центру – повинна працювати як підтримка організації прямих продажів і телефонних продажів, проводити соціологічні та маркетингові опитування, у тому числі, допомагати визначити, чи задоволений клієнт обслуговуванням, чи дозволяє зібрати будь-яку іншу важливу інформацію.

Вихідна лінія кол-центру(іншомовні) – повинна мати всі ті самі обов'язки що і звичайна вихідна лінія кол-центру, але вони повинні вести розмову на іноземних мовах.

Вхідна лінія кол-центру повинна використовуватися як гаряча лінія, технічна підтримка, інформаційна підтримка.

ІТ-відділ або адміністративний відділ повинен контролювати працездатність мережі, обслуговувати комп'ютерну мережу всередині компанії, проводити аналіз апаратного забезпечення та відповідати за працездатність програмного та апаратного забезпечення.

2.1.1.1.4 Вимоги до діагностування мережі

Діагностування мережі повинно виконуватися адміністративним відділом.

Діагностика повинна передбачувати спеціальне програмне забезпечення для пошуку та аналізу помилок, які виникають у корпоративній мережі.

Діагностика мережі повинна застосовувати чіткий алгоритм дій, а саме виконання:

- перевірки фізичного з'єднання;
- перевірки світлових індикаторів на мережевих пристроях;
- виконання ping-тесту;
- використання тесту traceroute;
- перевірки журналів подій мережевих пристроїв.

2.1.1.1.5 Перспективи розвитку, модернізація мережі

При постійному працевлаштуванні нових співробітників необхідно забезпечувати модернізацію мережевого обладнання, а саме комутаційного рівня.

Мобільний зв’язок є необхідним в наш час, тому робота повинна збільшуватися, в свою чергу модернізація мережевого обладнання та персональних пристроїв співробітників повинна виконуватися також.

Мережа повинна передбачувати перспективу розвитку при додаванні нових відділів кол-центрів, для прискорення обробки клієнтської бази. Мережеве

обладнання має бути сумісними на довгий час, та при необхідності використовуватися в нових сегментах мережі.

2.1.1.2 Вимоги до показників призначення

Показники призначення мережевої інфраструктури кол-центрам:

– кол-центри повинні обробляти великий обсяг даних, включно з інформацією про клієнтів, історію взаємодії, запити та іншу важливу інформацію. Комп'ютерні мережі повинні давати змогу передавати ці дані між різними системами та додатками всередині кол-центру, забезпечуючи швидке та надійне передавання інформації;

– комп'ютерні мережі повинні давати змогу маршрутизувати вхідні дзвінки між операторами кол-центру та забезпечувати ефективний розподіл дзвінків на вільних операторів, враховуючи їхнє навантаження, навички та доступність;

– комп'ютерні мережі повинні давати змогу операторам кол-центру швидко отримувати доступ до інформації про клієнтів за допомогою баз даних та інших систем, що допомагають надавати персоналізоване обслуговування та ефективно відповідати на запити клієнтів;

– комп'ютерні мережі повинні давати змогу операторам кол-центру обмінюватися інформацією та співпрацювати один з одним та використовувати електронні системи обміну повідомленнями, внутрішні чати для розв'язання питань клієнтів, обміну знаннями та координації роботи;

– комп'ютерні мережі повинні давати змогу кол-центрам підтримувати віддалену роботу і гнучкість у географічному розміщенні співробітників.

2.1.1.3 Вимоги до експлуатації, технічного обслуговування, ремонту і збереженню

2.1.1.3.1 Умови і режим експлуатації, що повинні забезпечувати використання технічних засобів мережі з заданими технічними показниками

Для експлуатації пристроїв в мережі та мережевого обладнання додаткових умов не передбачено.

2.1.1.3.2 Вимоги до параметрів мереж енергопостачання, живлення та заземлення

Мережа енергопостачання повинна забезпечувати стабільне та безперебійне електроживлення всіх пристроїв і обладнання.

Пристрої і обладнання в мережі повинні працювати в межах допустимих значень напруги, а саме – 220В.

Вимоги до заземлення включають належне з'єднання всіх металевих елементів мережі з землею, забезпечення низького опору заземлення та відповідність стандартам електробезпеки.

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

Персонал, який працює в кол-центрі, не зобов'язаний мати вищу освіту, але повинен володіти навичками комунікації, умінням працювати з клієнтами, а також знанням продуктів або послуг, які надає компанія.

Оператори мають бути організованими, здатними ефективно розподіляти свій час між дзвінками, опрацюванням запитів і веденням записів.

Співробітники кол-центру повинні суворо дотримуватися конфіденційності та етики щодо даних клієнтів.

Кол-центр має надавати можливості для навчання та розвитку персоналу.

Кол-центр вимагає гнучкого графіка роботи, включно з роботою у вихідні дні, пізні години або змінну роботу.

Загальна кількість робочого персоналу дорівнює – 36 чоловік.

2.1.1.3.4 Вимоги до складу, розміщенню й умовам збереження комплекту запасних виробів і приладів

Для складу необхідно мати окреме приміщення щоб зберігати запасні вироби та прилади. Також, необхідно мати систему інвентаризації, яка дає змогу відстежувати кількість і стан запасних частин, а також своєчасно поповнювати запаси, за потреби.

Із запасних компонентів кол-центру завжди мають бути навушники і мікрофони, запасні компоненти комп'ютерних блоків, монітори, клавіатури і миші.

Обладнання потрібно зберігати за температури від 10 до 35 градусів Цельсія.

2.1.1.3.5 Вимоги до регламенту обслуговування мережі

Регулярне обстеження та технічне обслуговування повинно відбуватися кожного дня. Обслуговування повинно охоплювати перевірку й оновлення програмного забезпечення мережевих пристроїв, маршрутизаторів та комутаторів. Також повинно включати заміну зношених компонентів та оновлення апаратної частини.

Заплановані роботи повинні включати в себе створення резервних копій даних і налаштування процедур відновлення в разі збою або втрати даних. Відповідні роботи потрібно виконувати за командами системних адміністраторів.

2.1.1.4 Вимоги до патентної чистоти

Патентна чистота кол-центру в Україні означає, що кол-центр не використовує інтелектуальну власність (патенти, товарні знаки, авторські права тощо), що порушує законодавство про інтелектуальну власність.

2.1.1.5 Додаткові вимоги

2.1.1.5.1 Вимоги до активного обладнання

Вимоги до маршрутизаторів включають високу продуктивність, підтримку різних мережевих протоколів, можливість резервування та відновлення з'єднань, а також механізми безпеки, такі як віртуальні приватні мережі.

Вимоги до комутаторів включають високу пропускну здатність, підтримку різних швидкостей підключення, розширені можливості управління мережею.

Комутатори та маршрутизатори повинні підтримувати технологію Gigabit Ethernet.

Комп’ютери, сервери та комутатори повинні мати мережеві порти RJ-45 та забезпечувати швидкість до 100Мбіт/с.

Комутатори та маршрутизатори повинні підтримувати швидкості до 1Гбіт/с для розподілення між абонентами мережі.

2.1.1.5.2 Вимоги до кабель-каналів, інформаційним та електричним розеткам(тип, розмір, варіант розміщення)

Кабель-канали повинні мати достатню ємність для розміщення всіх необхідних кабелів з резервом на майбутнє розширення мережі. Вони повинні бути виготовлені з якісних матеріалів, що забезпечують високу механічну міцність та стійкість до зовнішніх впливів.

Кабель-канали повинні мати відповідні кришки або захисні елементи, щоб забезпечити безпеку кабелів та легкий доступ для обслуговування та заміни.

Розетки повинні відповідати стандартам, які визначаються відповідно до регіональних норм та нормативних документів. Тип розеток повинен бути стандартним та використовувати тип RJ-45.

Розташування розеток повинно бути логічним і зручним для підключення комп'ютерів та серверів.

Варіант розміщення розеток повинен включати встановлення їх у підлогу та на стіні.

2.1.1.5.3 Вимоги до комунікаційного обладнання і його розташування (розташування у приміщенні)

Розташування обладнання повинно забезпечувати доступність для обслуговування і заміни компонентів без перерви в роботі мережі. Побудова системи комунікації повинна виконуватися у стійках.

Розташування обладнання повинно передбачати наявність ефективної системи вентиляції та кондиціонування повітря для забезпечення оптимальних умов роботи обладнання.

Комунікаційне обладнання повинно бути підключене до надійного джерела електропостачання, що забезпечує безперебійне живлення.

Кабелі повинні бути професійно прокладені і маркуватися для легкої ідентифікації.

Повинно виконуватися роздільне кабелювання для різних типів мереж, наприклад ПК, мережеве обладнання та сервери, для забезпечення максимальної ефективності та уникнення перешкод.

2.1.1.5.4 Вимоги до однорідності в мережі

Мережа повинна використовувати уніфіковані методи управління на всьому мережевому обладнанні. Управління повинно здійснюватися виключно з командного рядка обладнання за допомогою прямого фізичного розташування біля пристрою або застосовувати безпечне віддалене управління за протоколом SSH.

Для зручної уніфікації та легкості налаштування потрібно обрати мережеве обладнання Cisco.

2.1.2 Вимоги до функцій та задач, які виконує мережа

2.1.2.1 Вимоги до функцій та задач в кожному відділі мережі

Для того, щоб мережеве обладнання працювало належним чином, необхідно виконати базові налаштування конфігурації обладнання, тобто:

– імена пристроїв в мережі повинні формуватися за прикладом – Buriachenko_Router_1, де «Buriachenko» – прізвище, «Router» – тип пристою, «1» – номер пристрою;

– пароль *Cisco* має бути призначений для консолі та vty у всіх налаштуваннях;

– пароль class має бути призначений до привілейованого режиму у всіх налаштуваннях;

– при налаштуванні обладнання всі паролі повинні мати зашифрований вигляд;

– перед проходженням процесу *логіна* та *пароля* необхідно створити привітання MOTD;

– для ліній vty потрібно використовувати протокол віддаленого доступу ssh;

– на всьому обладнанні повинні бути назви користувачів за прикладом – «123-20-zck-1_Buriachenko» – група_прізвище, «admincisco» – пароль;

– назва обладнання повинна фігурувати як доменне ім'я та при цьому використовувати шифрування даних силою в 1024-біт ключа RSA;

– мережеве обладнання з DCE інтерфейсами повинні використовувати частоту – 128000;

– потрібно налаштувати перевірку та надсилання повідомлення при виконанні та завершені процесу exes, з локальної бази даних.

Щоб здійснити працездатність маршрутизації в мережі необхідно:

– всі мережі які підключені одна до одної повинні бути оголошені, при цьому оновлення таблиць не повинні відправлятися на мережеві інтерфейси в локальній мережі;

– мережі VLAN повинні мати загальний шлях, який буде розповсюджено по всій мережі;

– при використанні протоколу OSPF має бути виставлена здатність калькуляції для гігабітного інтерфейсу Gigabit та мати значення = 1000;

– serial-інтерфейси повинні мати пропускну здатність у 128 Кб/с, а вартість шляху = 7500;

– магістральний маршрутизатор, який підключається до мережі Інтернет повинен мати маршрут за замовчуванням та при цьому передавати його всім членам мережі за допомогою протоколу маршрутизації;

– на магістральному маршрутизаторі також повинно бути налаштовано об’єднання мереж локальної та глобальної мережі в ручному режимі та додано до таблиці маршрутизатора;

– статичні маршрути мають використовуватись при необхідності не використанні протоколу динамічної маршрутизації.

Для забезпечення індивідуального використання мережевого обладнання співробітниками потрібно виконати налаштування протоколу безпеки AAA за наступними вимогами:

– перевірка даних на лініях VTY у маршрутизаторі повинна здійснюватися за допомого локальних облікових записів щодо робітників в компанії;

– здійснення входу до маршрутизатору потрібно налаштувати за протоколом *RADIUS*, якщо виникає помилки при проходженні входу, потрібно використовувати локальні записи;

– в протоколі *RADIUS-серверу* необхідно використовувати серкретний ключ, за замовчуванням він повинен бути – *radius123;*

– облікові записи у сервері повинні складатися з ім'я маршрутизатора та мати пароль за замовчуванням *admin123.*

Щоб налагодити Інтернет, мережа повинна мати вихід до глобальної мережі за допомогою використання спроможності інтернет-провайдера.

Магістральний маршрутизатор повинен перетворювати локальні адреси в глобальні, і навпаки, за допомогою протоколу NAT.

Налаштування протоколу NAT на маршрутизаторі повинні відповідати глобальному діапазону адрес *з 209.165.200.5 по 209.165.200.30*, мати назву в мережі – *Internet* та використовувати список доступу для роботи за номером завдання в мережі.

Після отримання виходу в мережу Інтернет, потрібно налаштувати веб-сайт серверу HTTP за адресою *http://209.165.200.4* щоб доменне ім'я відповідало значенню – *http://123.dnipro.ua.* Веб-сайт повинен мати дані про тему та мету кваліфікаційної роботи.

2.1.2.2 Часовий регламент і вимоги до якості реалізації кожної функції, форми представлення вихідної інформації

Кожний відділ корпоративної мережі повинен відповідати наступим вимогам:

- для побудови адресації в мережі необхідно використовувати IP-адресу версії *v4*;
- для маршрутизації мережевого обладнання необхідно використовувати пул адрес за замовчуванням – *10.0.№.0* з маскою */24*, при цьому *№* повинен відповідати номеру студента у групі;
- початкові вільні IP-адреси потрібно назначати інтерфейсам та саб-інтерфейсам маршрутизаторів незалежно від підмережі;
- наступні вільні IP-адреси потрібно назначати інтерфейсам комутаторів незалежно від підмережі;
- після налаштування адресації мережевого обладнання наступні адреси потрібно видавати серверам;
- кінцеві вільні IP-адреси потрібно назначати безпосередньо пристроям в мережі;
- пристрої в віртуальних локальних мережах повинні бути налаштовані на динамічне отримання адрес за протоколом *DHCP*.

2.1.3 Вимоги до видів забезпечення мережі

2.1.3.1 Вимоги до математичного забезпечення

Для отримання даних про якісний вибір апаратного та програмного забезпечення та підтвердження працездатності мережі за поставленими задачами необхідно провести розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі компанії, з повним розрахунком пропускної здатності мережі.

2.1.3.2 Вимоги до інформаційного забезпечення

У мережу повинно бути впроваджено моніторингову систему активності на будь-якому комп'ютері, підключеному до мережі. Програма повинна надавати

змогу виявити діяльність, що не має стосунку до роботи, наскільки раціонально співробітники використовують робочий час.

Також, повинно бути встановлене програмне забезпечення для керування вхідними дзвінками, для розподілу їх між операторами та забезпечання належного контролю якості обслуговування.

2.1.3.3 Вимоги до лінгвістичного забезпечення

Головною вимогою до персоналу колл-центру є вільне володіння мовними навичками, включаючи добре знання мови клієнтів або мов, з якими вони спілкуються. Це включає володіння граматикою, правильним вимовлянням, належним розумінням мовних нюансів та ефективними комунікаційними навичками.

Вимога поширюється не тільки для україномного відділу, але і для іншомовного.

2.1.3.4 Вимоги до технічного забезпечення

Головними технічними вимогами є представлення сучасних комп’ютерів, які повинні відповідати вимогам:

– мати мінімум двоядерний процесор з достатньою швидкістю, щоб ефективно обробляти завантаження від програмного забезпечення колл-центру;

– мати мінімум 4 ГБ оперативної пам'яті для плавної роботи програм та запобігання затримок у відповідях;

– мінімум 250 ГБ для забезпечення достатнього простору для зберігання програм та даних, при цьому використовувати диски SSD;

– повинен бути монітор з достатньою роздільною здатністю та розміром екрану для зручної роботи з інтерфейсом програм та відображенням даних;

– повинна бути надійна клавіатура та миша, які дозволять операторам швидко та точно вводити інформацію та взаємодіяти з програмами.

Також, для побудови якісної безпеки офісного приміщення, були враховані вимоги до RFID-карток:

– RFID картки повинні бути сумісні з читачами RFID, які будуть використовуватися в кол-центрі;

– картки повинні мати механізми захисту від несанкціонованого доступу та підробки, а саме – захищені елементи пам'яті або криптографічні протоколи;

– RFID картки повинні бути витривалими і здатними витримувати повсякденні умови використання;

– залежно від вимог ідентифікації та контролю доступу в колл-центрі, RFID картки повинні мати унікальні індивідуальні характеристики, такі як унікальні ідентифікатори або додаткові дані, що відображають статус або дозволені права доступу.

2.1.3.5 Вимоги до організаційного забезпечення

Всі співробітники, а також директори компанії повинні застосовувати RFID картки для отримання фізичного доступу в офісні приміщення компанії.

Якщо співробітник загубив картку, потрібно оформити протокол втрати і деактивувати номер картки, яка була прикріплена за співробітником.

2.1.3.6 Вимоги до методичного забезпечення

Після налагодження всіх елементів мережі необхідно створити звіт із виконаної роботи. Звіт повинен містити текстові та графічні матеріали з:

– конфігурації мережі;

– фізичного розташування обладнання;

– схеми з'єднань підмереж;

– налаштування мережевого обладнання;

– усунення несправностей мережевого обладнання;

– IP-схем;

– процедури безпеки;

– розрахунку швидкості каналу;

– стану працездатності обладнання.

2.2 Розробка апаратної частини мережі

2.2.1 Вибір і обґрунтування структурної схеми комплексу технічних засобів комп'ютерної мережі шляхом узгодження структури з топологічними особливостями розташування відділів

Структурна схема комплексу технічних засобів комп'ютерної мережі колл-центру визначає організацію та взаємозв'язок дій між різними компонентами мережі.

Основне обґрунтування такої структурної схеми базується на ефективності, надійності та масштабованості мережевого середовища колл-центру.

Структура технічного забезпечення мережі знаходиться в чотирьох різних куточках міста, що надає варіації для підключення кожного відділу до мережі міського інтернет-провайдера.

Відділи не мають прямого підключення один між одними, а вузли в мережі підключені кабелем – вита пара.

Графічне представлення схеми дає змогу наочно відобразити структуру й організацію технічних засобів кол-центру.

За допомогою графічного представлення можна легко визначити місце розташування проблеми в структурі мережі. Це спрощує процес діагностики та усунення несправностей, оскільки можна швидко виділити відповідний компонент.

Для зручного створення структурної схеми комплексу технічних засобів була відображена інформація, щодо кількості технічних засобів в кожній підмережі компанії у таблиці 2.1.

Таблиця 2.1 – Кількість технічних засобів в кожній підмережі

Номер підмережі	Назва підмережі	Тип пристрою	Кількість
LAN1	Вихідна лінія зв'язку	PC	12
LAN2	Вихідна лінія зв'язку(іншомовні)	PC	5
LAN3	Адміністративний підрозділ	PC	1
		Server	2
LAN4	Вхідна лінія зв'язку	PC	18
		Server	1

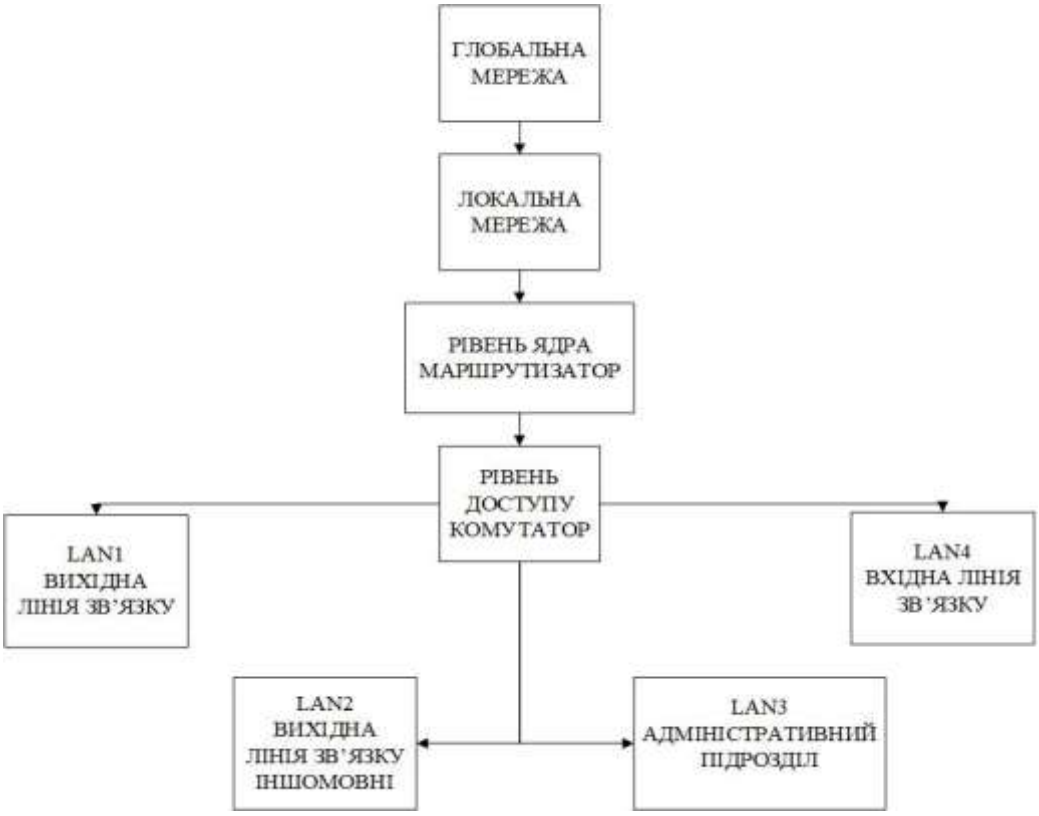

Рисунок 2.1 – Структурна схема комплексу технічних засобів комп'ютерної мережі компанії «Lifecell»

2.2.2 Розробка специфікації апаратних та програмних засобів комп'ютерної системи

Розробка специфікації апаратних та програмних засобів комп'ютерної системи включає в себе розробку детального опису необхідних апаратних компонентів та програмного забезпечення, що будуть використовуватися в системі компанії.

На основі проведеного аналізу вимог до кваліфікаційної роботи були створені схеми фізичного розташування пристроїв кожного відділу корпоративної мережі.

Схеми мають детальне опрацювання СКС з відображенням розмірів довжини кабелю.

Габаритні розміри кожної будівлі зазначенні та відповідають стандартам технічного креслення.

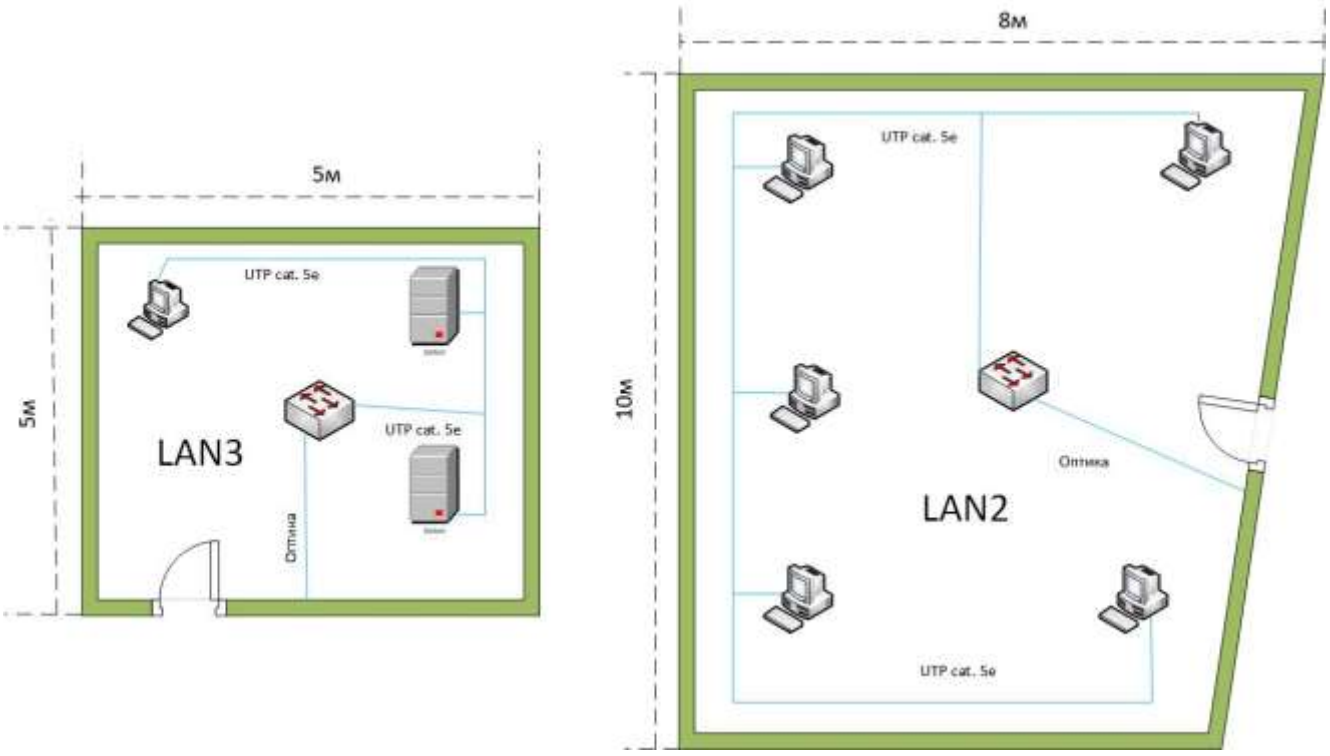

Рисунок 2.2 – Схема фізичного розташування пристроїв адміністративного відділу та відділу кол-центру

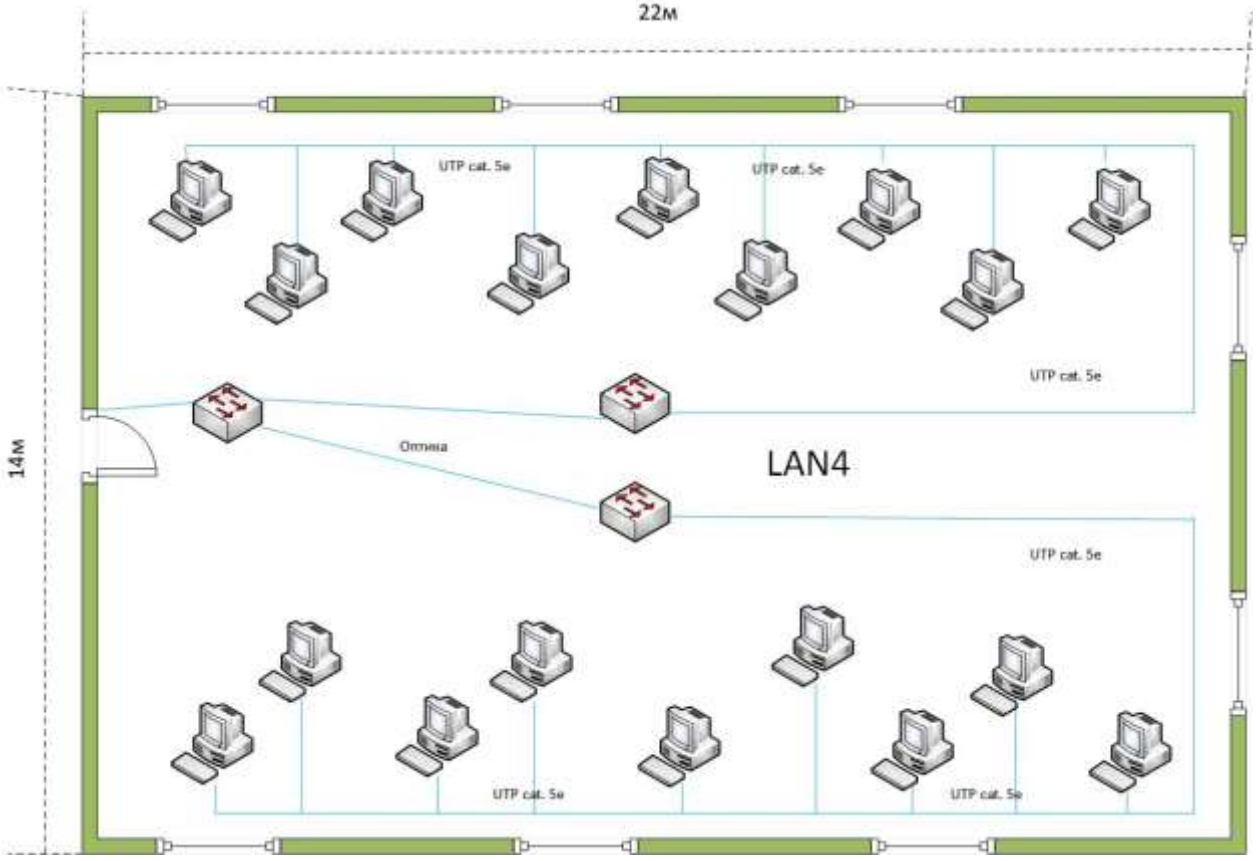

Рисунок 2.3 – Схема фізичного розташування пристроїв кол-центру вхідного зв’язку

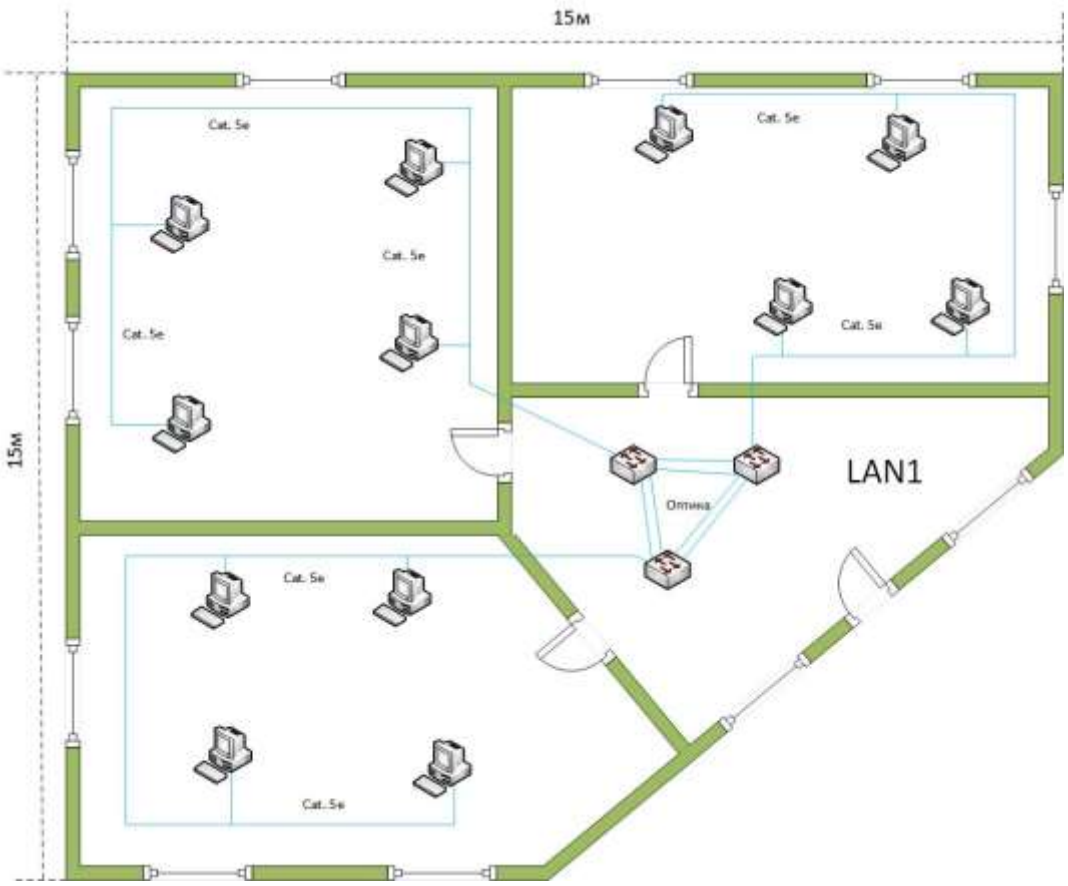

Рисунок 2.4 – Схема фізичного розташування пристроїв кол-центру вихідного зв’язку

Для побудови фізичного забезпечення мережі розробляється таблиця елементів СКС.

СКС відноситься до фізичної інфраструктури комп'ютерної мережі та включає в себе кабелі, роз'єми, патч-панелі, розподільні коробки та інші компоненти для передачі даних і забезпечення комунікації між пристроями в мережі.

На основі проекту СКС вибираються необхідні компоненти, такі як, активне мережеве обладнання.

Після вибору компонентів проводяться монтажні роботи.

Важливим кроком є створення документації, яка описує структуру СКС, схеми підключення, топологію, типи кабелів, роз'єми і зв'язки між компонентами.

Документація СКС занесена до таблиці 2.2.

Таблиця 2.2 – Елементи побудови СКС

Позиція елементу	Назва та технічна характеристика	Тип та позначення	Одиниця виміру	Кількість
1	Кабельний канал 30 мм х 30 мм, 2м	Vinga	од	100
2	Інформаційна розетка інтерфейсу RJ-45 UTP cat5e	ASFORA	од	20
3	Кабель вита пара Тип – UTP cat5e	OK-Net	м	240
4	Конектор Тип – RJ-45	Patron	од	40
5	Стійка настінна Розмір – 6U	CMS-WB6U-480V-BK	од	3
6	Оптоволоконний кабель	OK-Net	м	60
7	Конектор оптоволокна Тип – SC	Patron	м	30

За вимогами в пункті 2.1.3.4 було обрано офісне апаратне забезпечення робочих станцій користувачів мережі, при цьому вся інформація з технічного погляду відображена у таблиці.

Рисунок 2.5 – Обраний ПК для користувачів мережі

Рисунок 2.6 – Обраний монітор для користувачів мережі

Апаратне забезпечення користувачів мережі включає в себе фізичні пристрої, які використовуються користувачами для підключення до мережі та здійснення різних операцій.

Таблиця 2.3 – Апаратне забезпечення користувачів мережі

Позиція	Назва та технічна характеристика	Тип та позначення	Одиниці виміру	Кількість
1	Блок ПК: ARTLINE, Процесор: 4700S (3.6 - 4.0 ГГц), ОЗП: 16гб, SSD: 250гб, Відеокартка: nVidia GeForce GT 710, Блок живленн: 400 Вт.	ARTLINE Business B48v07	од.	36
2	Монітор: MSI діагональ 23.8 165Гц, роздільна здатність дисплея 1920x1080 (FullHD), інтерфейси 2 x HDMI	MSI G2412	од.	36
3	Клавіатура Logitech K120 USB UKR OEM	Logitech	од.	36
4	Миша Logitech M185 Wireless Blue	Logitech	од.	36

Апаратне забезпечення мережевого рівня включає в себе пристрої, які забезпечують комутацію, маршрутизацію та передачу даних у мережі.

Таблиця 2.4 – Апаратне забезпечення мережевого рівня

Позиція	Назва та технічна характеристика	Тип та позначення	Одиниці виміру	Кількість	Примітка
1	Пристрій: Комутатор Портів: 24, Швидкість:10/100/1000 Мбіт/с, VLAN-підтримка, Стандарт: Ethernet (IEEE 802.3, 802.3u, 802.3ab)	Catalyst 2960	од.	8	За проектом у CPT: Buriachenko_Switch0 Buriachenko_Switch1 Buriachenko_Switch2 Buriachenko_Switch3 Buriachenko_Switch4 Buriachenko_Switch5 Buriachenko_Switch6 Buriachenko_Switch7
2	Пристрій: Маршрутизатор, Продуктивність: 180000 пакетів за секунду, Швидкість: до 10Гбіт/с ОЗП: 2Гб ОС: Cisco IOS	Cisco 2911	од.	7	За проектом у CPT: Buriachenko_Router0 Buriachenko_Router1 Buriachenko_Router2 Buriachenko_Router3 Buriachenko_Router4 Buriachenko_Router5 Buriachenko_IPS

Програмне забезпечення мережі включає набір програмних компонентів, які використовуються для керування, моніторингу та оптимізації мережевих ресурсів мережі.

В програмне забезпечення компанії було інстальовано програму Microsoft Office, яка слугуватиме для збору та обробки інформації та створення графіків щодо змін праці.

Також було інстальовано додаток LanAgent, це програмний додаток для контроля дій користувачів в мережі та аналізу вихідного трафіку.

Він служить для проведення вхідних та вихідних ліній зв’язку кол центру.

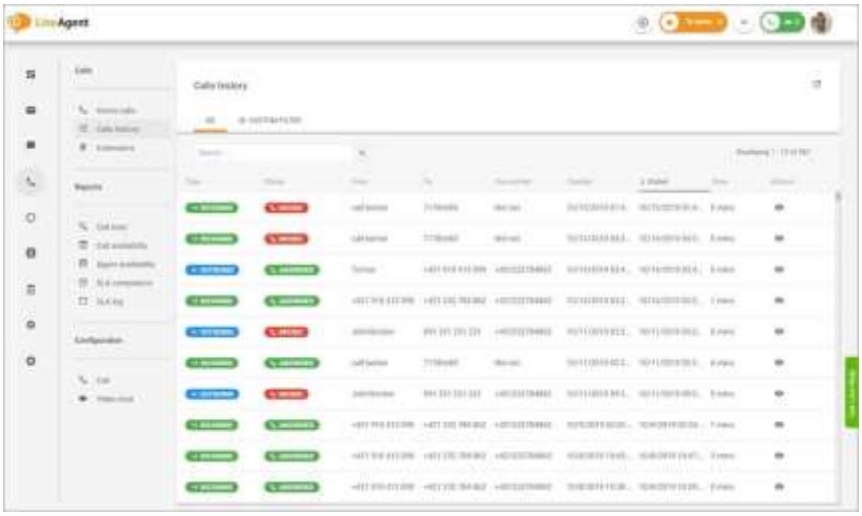

Рисунок 2.7 – Обраний додаток LiveAgent

2.2.3 Розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі підприємства

Розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі компанії «Lifecell» виконується на основі аналізу різних факторів, таких як кількість користувачів, типи додатків, обсяг передаваних даних та характер їх використання.

У найбільшій системі існує 42 вузли. Середнє навантаження трафіку складає $\mu = 111$ кадрів на секунду. Розмір повідомлення становить 650 байтів у середньому. Максимальний час передачі пакету не повинна перевищувати 6 мілісекунд. Загальна кількість користувачів системи складає 111 осіб.

Проведення розрахунків ключових характеристик вихідного трафіку, можлива при умові максимального завантаження мережі або досягнення 100% своєї потужності.

Трафік, що виходить, спрямовується до маршрутизатора та повинен мати пропускну здатність не більше значення у 1000 Мбіт/с.

Пропускна здатність мережі визначається з урахуванням максимального навантаження, коли всі користувачі використовують мережу на повну потужність

одночасно. Це означає, що пропускна здатність мережі враховує загальну швидкість передачі даних всіма користувачами в цей момент часу.

Швидкість передачі даних в даній мережі на рівні доступу:

$$Рр.д= \mu * l*n * 8=111 * 650 * 24 * 8= 13,85 \text{ Мбіт/с}, \quad (2.1)$$

де n – в даному контексті відповідає кількості портів, доступних в комутаторі на рівні доступу.

Пропускна здатність мережі на рівні розподілу визначається шляхом обчислення сумарної пропускної здатності для всіх 42 користувачів:

$$Рр.р = \mu * l * N *8 = 111 * 650 * 42 * 8= 242,42 \text{ Мбіт/с}, \quad (2.2)$$

де N – є числом кількості користувачів найбільшої мережі.

Розрахунки показали, що обладнання, яке було обрано, відповідає параметрам мережі і не буде надмірно навантажене.

Трафік з комутатора рівня розподілу передається до маршрутизатора через вихідну лінію, яка має максимальну пропускну здатність 1000 Мбіт/с.

$$\mu вих = 1000\,000\,000 / (650 * 8) = 192\,310 \text{ пакетів/с}. \quad (2.3)$$

Середнє число пакетів, що генерується кожним джерелом, становить 111 пакетів на секунду, що межує його здатність підключитися до максимального рівня комутації.

$$N = 192\,310 / 111 = 1732 \text{ джерел}. \quad (2.4)$$

1742 джерела повністю вистачають для обслуговування 42 осіб, що означає повне покриття кількості користувачів.

Інтенсивність генерації заявок на кожному з 42 ПК складає 111 кадрів на секунду в середньому.

Сумарна інтенсивність вихідного трафіку від усіх користувачів складає:

$$\lambda = N * \mu = 42 * 111 = 4662 \text{ (пакетів/с)}. \quad (2.5)$$

У розподільній частині мережі, присутній коефіцієнт затримки і показник завантаження вихідного каналу зв'язку, які мають вплив на затримку у черзі.

$$\rho= \lambda / \mu вих = 4662 / 192\,310= 0,024 \quad (2.6)$$

Показник використання комутатора на рівні розподілу:

$$r = \rho / (1 – \rho) = 0,024 / (1 – 0,024) = 0,024 \quad (2.7)$$

Середня часова затримка передачі кадру що виникає внаслідок черги M/M/1, дорівнює:

$$T=1/((\mu-\lambda))=1/(192\ 310-4662)=5{,}32 \text{ мкс} \quad (2.8)$$

Середня довжина черги:

$$L\_чер=\rho^2/(1-\rho)=(0{,}024)^2/(1-0{,}024)=0{,}00059 \quad (2.9)$$

Ця величина має велике значення для керування чергою пристрою. В апаратному рішенні можна вказати максимальний обсяг черги пакетів.

Середній час пакетів у черзі:

$$T\_оч=L\_чер/\lambda=0{,}00059/4662=1{,}26 \text{ мкс} \quad (2.10)$$

Ця величина відповідає встановленим вимогам, оскільки вона менша за необхідне значення ≤ 6 мс.

Пропускна здатність каналу:

$$\lambda=(\text{пропускна здатність})/(\text{довжина кадру})=b/l \quad (2.11)$$

$$b=\lambda*l=4662*650*8=24\ 242\ 400 \text{біт/с}=24{,}2 \text{Мбіт/с}$$

Розраховане середнє значення пропускної здатності каналу дорівнює 24Мбіт/с що відповідає пропускній здатності вихідного каналу, яка становить 1000 Мбіт/с.

3 МОДЕЛЮВАННЯ ТА НАЛАШТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Розрахунок налаштувань для заданої топології мережі

Під час розрахунку IP-адрес для мережі необхідно врахувати кілька важливих аспектів. Насамперед, визначимо необхідний розмір мережі та необхідну кількість вузлів. Розмір мережі повинен відповідати заданому пулу адрес – 192.168.6.0 з маскою 255.255.255.0. Необхідна кількість вузлів повинна розраховуватися відповідно до кількості кінцевих пристроїв в відділах мережі, які були визначені в пункті 2.1.1.1.1.

Далі проводиться розбивка діапазону IP-адрес мережі на підмережі.

Мережа складається з семи маршрутизаторів та восьми комутаторів, усього підключено 15 мережевих пристроїв.

Відповідно від заданих даних створимо таблицю адресації та об’єм підмереж локальної мережі.

Таблиця 3.1 – Завдання адресації та об’єм підмереж локальної мережі

Адресація	Розмір LAN1	Розмір LAN2	Розмір LAN3	Розмір LAN4
192.168.6.0/24	34	29	6	42

Після успішного розбиття IP-адрес та підмереж у нашій мережі, наступним кроком є налаштування маршрутизації між різними підмережами та пристроями.

Кожен маршрутизатор повинен знати про підмережі, які знаходяться в системі та мати уявлення щодо найкоротшого шляху до цих підмереж. Для цього ми встановимо таблиці маршрутизації на кожному маршрутизаторі, вказуючи мережеві адреси та шляхи до них.

Наступним кроком є обмін маршрутною інформацією між маршрутизаторами, цей процес здійснимо за допомогою протоколу маршрутизації OSPF, який автоматично обмінюється інформацією про маршрути.

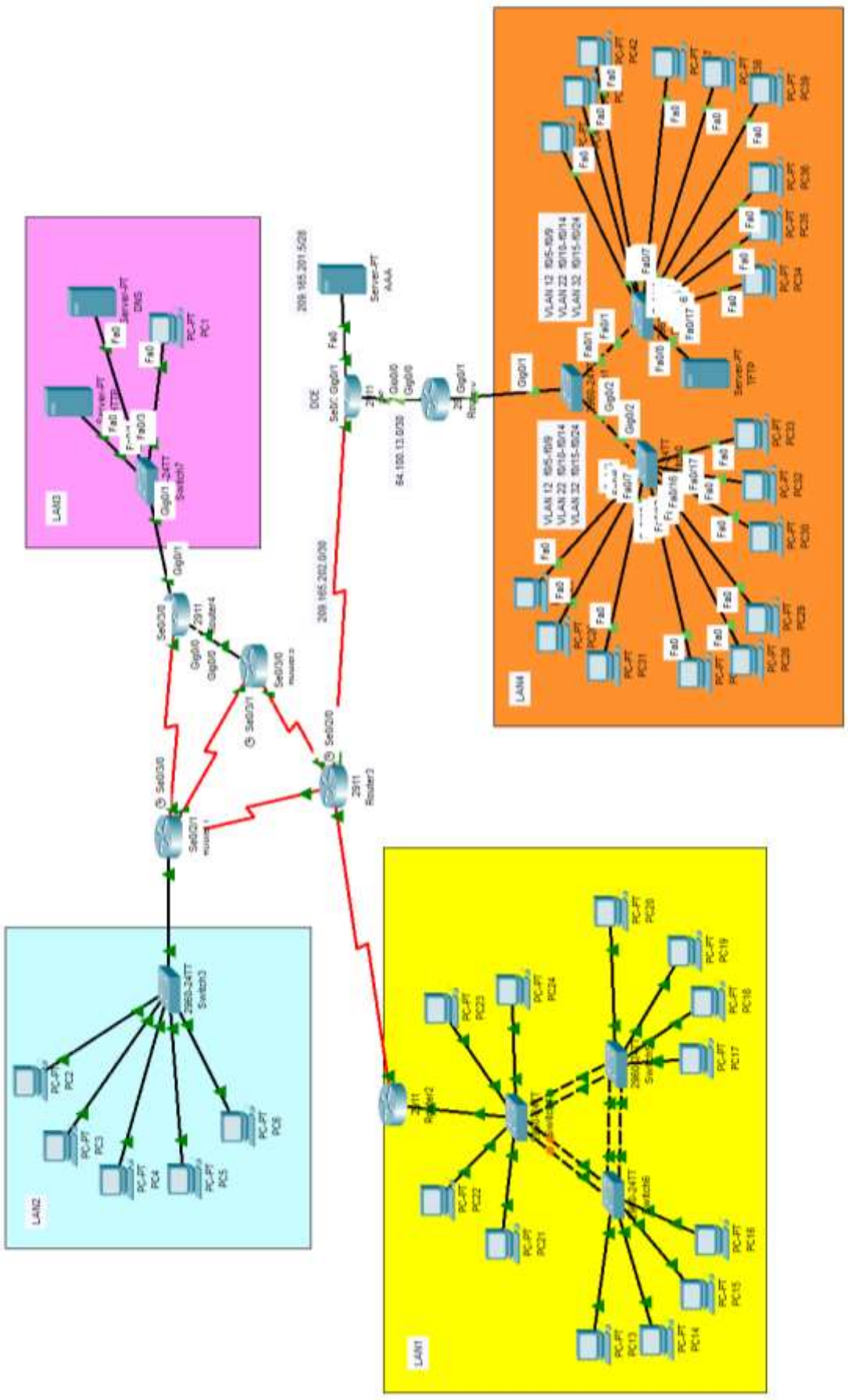

Рисунок 3.1 – Топологічне представлення пристроїв компанії «Lifecell»

3.2 Розрахунок схеми адресації підмереж компанії

Проведемо розбиття мережі 192.168.6.0/24 на чотири підмережі з метою ефективного використання доступних IP-адрес та оптимізації ресурсів мережі. Цей процес дозволить нам створити окремі сегменти мережі з власними IP-адресами, що допоможе в управлінні та розподілі трафіку.

За допомогою маски підмережі /24 (або 255.255.255.0), ми маємо початковий діапазон IP-адрес від 192.168.6.1 до 192.168.6.254. Тепер розбиваємо цей діапазон на чотири рівні локальні підмережі, кожна з яких матиме свій власний діапазон IP-адрес.

1. Перша підмережа: 192.168.6.0/26;
   - IP-адреси: 192.168.6.1 - 192.168.6.62;
   - кількість доступних адрес – 62;
   - маска підмережі: 255.255.255.192 (/26);
2. Друга підмережа: 192.168.6.64/26;
   - IP-адреси: 192.168.6.65 - 192.168.6.126;
   - кількість доступних адрес – 62;
   - маска підмережі: 255.255.255.192 (/26);
3. Третя підмережа: 192.168.6.128/28;
   - IP-адреси: 192.168.6.129 - 192.168.6.142;
   - кількість доступних адрес – 14;
   - маска підмережі: 255.255.255.240 (/28);
4. Четверта підмережа: 192.168.6.192/26;
   - IP-адреси: 192.168.6.193 - 192.168.6.254;
   - кількість доступних адрес – 62;
   - маска підмережі: 255.255.255.192 (/26).

Кожна з цих підмереж має свою власну маску підмережі, яка визначає кількість доступних IP-адрес у кожній підмережі.

Після цього розрахуємо адреси для маршрутизаторів. Вихідний діапазон IP-адрес у мережі 10.0.2.0/24 з маскою 255.255.255.0 охоплює адреси від 10.0.2.1 до 10.0.2.254. Тепер розбиваємо цей діапазон на шість підмереж з маскою /30, що

дозволяє нам мати по чотири адреси в кожній підмережі, з виключенням адреси мережі та широкомовної адреси.

1. Перша підмережа: 10.0.2.0/30;
   - IP-адреси: 10.0.2.1 - 10.0.2.2;
   - кількість доступних адрес – 2;
   - маска підмережі: 255.255.255.252 (/30)
2. Друга підмережа: 10.0.2.4/30;
   - IP-адреси: 10.0.2.5 - 10.0.2.6;
   - кількість доступних адрес – 2;
   - маска підмережі: 255.255.255.252 (/30)
3. Третя підмережа: 10.0.2.8/30;
   - IP-адреси: 10.0.2.9 - 10.0.2.10;
   - кількість доступних адрес – 2;
   - маска підмережі: 255.255.255.252 (/30)
4. Четверта підмережа: 10.0.2.12/30;
   - IP-адреси: 10.0.2.13 - 10.0.2.14;
   - кількість доступних адрес – 2;
   - маска підмережі: 255.255.255.252 (/30)
5. П'ята підмережа: 10.0.2.16/30;
   - IP-адреси: 10.0.2.17 - 10.0.2.18;
   - кількість доступних адрес – 2;
   - маска підмережі: 255.255.255.252 (/30)
6. Шоста підмережа: 10.0.2.20/30;
   - IP-адреси: 10.0.2.21 - 10.0.2.22;
   - кількість доступних адрес – 2;
   - маска підмережі: 255.255.255.252 (/30)

Кожна з цих шести підмереж має свій власний діапазон IP-адрес що гарантує ефективне використання доступних адрес і забезпечує ізольованість трафіку між сегментами мережі.

Занесемо отримані значення до таблиці.

Таблиця 3.2 – Параметри адрес підмереж відділів управління

Підмережа	Кількість кінцевих пристроїв	Адреса підмережі	Маска підмережі	Адресація кінцевих пристроїв	
LAN1	34	192.168.6.0	255.255.255.192	192.168.6.1	192.168.6.62
LAN2	29	192.168.6.64	255.255.255.192	192.168.6.65	192.168.6.126
LAN3	6	192.168.6.128	255.255.255.240	192.168.6.129	192.168.6.142
LAN4	42	192.168.6.192	255.255.255.192	192.168.6.193	192.168.6.254
VLAN12	5	192.168.6.208	255.255.255.240	192.168.6.209	192.168.6.222
VLAN22	5	192.168.6.224	255.255.255.240	192.168.6.225	192.168.6.238
VLAN32	6	192.168.8.240	255.255.255.240	192.168.6.241	192.168.6.254
WAN1	2	10.0.2.0	255.255.255.252	10.0.2.1	10.0.2.2
WAN2	2	10.0.2.4	255.255.255.252	10.0.2.5	10.0.2.6
WAN3	2	10.0.2.8	255.255.255.252	10.0.2.9	10.0.2.10
WAN4	2	10.0.2.12	255.255.255.252	10.0.2.13	10.0.2.14
WAN5	2	10.0.2.16	255.255.255.252	10.0.2.17	10.0.2.18
WAN6	2	10.0.2.20	255.255.255.252	10.0.2.21	10.0.2.22
WAN IPS	2	209.165.202.0	255.255.255.252	209.165.202.1	209.165.202.2
WAN Global	2	64.100.13.0	255.255.255.252	64.100.13.1	64.100.13.2

3.3 Розрахунок схеми адресації пристроїв в підмережах

Після отримання мереж і визначення доступних адрес у пункті 3.2, ми приступимо до призначення IP-адрес для кожного мережевого інтерфейсу пристроїв у нашій мережі. Це включає ПК, сервери, принтери, комутатори та маршрутизатори, які використовуються в нашій інфраструктурі.

Ми будемо призначати IP-адреси відповідно до визначених підмереж та їхніх IP-діапазонів. Кожен пристрій отримає унікальний IP-адрес, який буде відповідати відповідній підмережі.

Таким чином, ми забезпечимо належне функціонування і взаємодію всієї мережевої інфраструктури.

Таблиця 3.3 – Схема адресації мережевих інтерфейсів в мережах

Ім’я пристрою	Інтерфейс	IP-адреса	Маска	Шлюз	VLAN	Інтерфейс підключеного пристрою
Мережа IPS						
IPS	S0/3/1	209.165.202.2	/30	–	–	S0/3/1
	G0/0	64.100.13.1	/30	–	–	G0/0
AAA_IPS	NIC	209.165.201.5	/28	–	–	Fa0/1
Router3	S0/3/1	209.165.202.1	/30	–	–	S0/3/1
	S0/2/0	10.0.2.13	/30	–	–	S0/2/0
	S0/2/1	10.0.2.10	/30	–	–	S0/2/1
	S0/3/0	10.0.2.21	/30	–	–	S0/3/0
Router5	S0/3/0	10.0.2.14	/30	–	–	S0/3/0
	S0/3/1	10.0.2.6	/30	–	–	S0/3/1
	G0/0	10.0.2.17	/30	–	–	G0/0
Мережа LAN1						
Router2	G0/1	192.168.6.1	/26	–	–	G0/1
	S0/3/0	10.0.2.22	/30	–	–	S0/3/0
Switch4	Vlan1	192.168.6.2	/26	192.168.6.1	–	Fa0/1-0/4
Switch5	Vlan1	192.168.6.3	/26	192.168.6.1	–	Fa0/1-0/4
Switch6	Vlan1	192.168.6.4	/26	192.168.6.1	–	Fa0/1-0/4
PC13-24	NIC	192.168.6.5-192.168.6.16	/26	192.168.6.1	–	Fa0/5-0/8
Мережа LAN2						
Router1	G0/1	192.168.6.65	/26	–	–	G0/1
	S0/2/1	10.0.2.5	/30	–	–	S0/2/1
	S0/3/0	10.0.2.1	/30	–	–	S0/3/0
	S0/3/1	10.0.2.9	/30	–	–	S0/3/1
Switch3	Vlan1	192.168.6.66	/26	192.168.6.65	–	G0/1
PC2-6	NIC	192.168.6.67-192.168.6.71	/26	192.168.6.65	–	Fa0/1-0/5
Мережа LAN3						
Router4	G0/0	10.0.2.18	/30	–	–	G0/0
	G0/1	192.168.6.129	/28	–	–	G0/1
	S0/3/1	10.0.2.2	/30	–	–	S0/3/1

Кінець таблиці 3.3

Switch7	Vlan1	192.168.6.133	/28	192.168.6.129	–	G0/1
Server DNS	NIC	192.168.6.131	/28	192.168.6.129	–	Fa0/1
Server DNS	NIC	192.168.6.132	/28	192.168.6.129	–	Fa0/1
PC1	NIC	192.168.6.130	/28	192.168.6.129	–	Fa0/1
Мережа LAN4						
Router0	G0/0	64.100.13.1	/30	–	–	G0/0
	G0/1	192.168.6.193	/28	–	–	G0/1
Switch0	Vlan1	192.168.6.194	/28	192.168.6.129	–	G0/1
Switch1	Vlan1	192.168.6.195	/28	192.168.6.129	–	G0/2
Switch2	Vlan1	192.168.6.196	/28	192.168.6.129	–	Fa0/1
PC25,26,31, 40,41,42_12	NIC	192.168.6.210-192.168.6.222	/28	192.168.6.209	12	Fa0/5-0/9
PC27-29, 37-39_22	NIC	192.168.6.227-192.168.6.238	/28	192.168.6.226	22	Fa0/10-0/14
PC30,32-36_32	NIC	192.168.6.243-192.168.6.254	/28	192.168.6.242	32	Fa0/15-0/24
Server TFTP	NIC	192.168.6.215	/28	192.168.6.209	12	Fa0/8

3.4 Налаштування елементів корпоративної мережі

3.4.1 Базове налаштування конфігурації пристроїв

Для успішного налаштування протоколів мережевої безпеки, маршрутизації та інших параметрів, необхідно виконати базову конфігурацію маршрутизаторів.

Цей процес включає створення облікових записів, паролів та ін.

Налаштуємо маршрутизатор – Router1:

Router1 (config)# hostname Buriachenko_Router1 // вказуємо ім’я маршрутизатора

Buriachenko_Router1 (config)#enable secret class // встановлюємо пароль *class* до привілейованого режиму

Buriachenko_Router1 (config)#line console 0 // отримуємо доступ до консолі

Buriachenko_Router1 (config-line)#password cisco // задаємо значення до паролю

Buriachenko_Router1 (config)#service password-encryption // вмикаємо шифрування паролів

Buriachenko_Router1 (config-line)#login // встановлюємо правило авторизації

Buriachenko_Router1 (config-line)#exit

Buriachenko_Router1 (config)#banner motd #123-20zck Buriachenko authorization PASSWORD# // встановлюємо текст, який буде фігурувати при авторизації в систему

Buriachenko_Router1 (config)#username 12320zck_ Buriachenko password cisco // створюємо обліковий запис за логіном – *12320zck_ Buriachenko* і паролем *cisco*

Buriachenko_Router1 (config)#ip domain-name Buriachenko_Router1 // встановлюємо співвідношення ім’я пристрою до доменного ім’я

Buriachenko_Router1 (config)#crypto key generate rsa // створюємо ключ шифрування

How many bits in the modulus [512]: 1024 // кількість бітів обираємо за завданням – *1024*

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK] // генерація ключа успішна

Buriachenko_Router1 (config)#line vty 0 4 // отримуємо доступ до консолі

Buriachenko_Router1 (config-line)#login local // вмикаємо обов’язкову авторизацію

Buriachenko_Router1 (config-line)#transport input ssh // керування лініями доступу за протоколом

3.4.2 Налаштування сегментації IP-адрес

Ми використовуємо технологію Network Address Translation (NAT) для кількох цілей в нашій мережі.

По-перше, NAT дозволяє нам заощадити публічні IP-адреси. Оскільки доступні публічні IP-адреси обмежені завданням, ми можемо використовувати NAT для перетворення наших приватних IP-адрес у публічні IP-адреси. Це дозволяє нам підключати більше пристроїв до Інтернету, навіть якщо у нас обмежена кількість публічних IP-адрес.

По-друге, NAT забезпечує безпеку мережі, ховаючи приватні IP-адреси внутрішніх пристроїв. Зовнішні пристрої, які підключені до Інтернету, бачать тільки публічну IP-адресу маршрутизатора NAT, а не окремих пристроїв у нашій мережі.

NAT дає негайне, але тимчасове вирішення проблеми дефіциту адрес IPv4, яка рано чи пізно відпаде сама собою з появою протоколу IPv6.

(config)# access-list 7 permit 192.168.6.0 0.0.0.255 // встановлюємо правило проходження мережі *192.168.6.0* у протокол, та вказуємо номер списку *7*

(config-if)#ip nat pool IPNAT 209.165.200.5 209.165.200.30 netmask 255.255.255.224 // встановлюємо заданий діапазон адрес за завданням та даємо ім’я *IPNAT*

(config-if)#ip nat inside source list 7 pool IPNAT // застосовуємо діапазон *IPNAT* для віхдної лінії маршрутизатора

(config)#ip nat inside source list 7 interface s0/3/1 // також, застосовуємо список номеру *7* на вихідної лініїї маршрутизатора з інтерфейсом *s0/3/1*

Налаштовуємо Serial інтерфейси на прийом та відправку пакет, відповідно за функціонуванням – *inside / outside:*

(config)#interface Serial0/3/0

(config-if)#ip nat inside

(config)#interface Serial0/2/1

(config-if)#ip nat inside

(config)#interface Serial0/2/0

(config-if)#ip nat inside

(config-if)#interface Serial0/3/1

(config-if)#ip nat outside

(config)#interface s0/3/0

(config-if)#bandwidth 128 // встановлюємо значення *128 Кб* для пропускної спроможності

(config-if)# clock rate 128000 // встановлюємо значення *128000* для швидкості каналу

(config-if)# ip ospf cost 7500 // встановлюємо значення *7500* для числового значення шляху

Застосування технології можна побачити у таблиці дій користувачів з запитами до глобальної мережі.

```
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.202.1:10  192.168.6.6:10     192.168.6.211:10   192.168.6.211:10
icmp 209.165.202.1:11  192.168.6.6:11     192.168.6.211:11   192.168.6.211:11
icmp 209.165.202.1:12  192.168.6.6:12     192.168.6.211:12   192.168.6.211:12
icmp 209.165.202.1:9   192.168.6.6:9      192.168.6.211:9    192.168.6.211:9
```

Рисунок 3.2 – Таблиця працездатності роботи протоколу

3.4.3 Налаштування протоколу рівня маршрутизації

Протоколи маршрутизації є головною частиною забезпечення мережі для її працездатності.

Вони грають важливу роль в ефективному функціонуванні мережі, дозволяючи маршрутизаторам приймати рішення про найоптимальніший шлях передачі даних.

Протокол маршрутизації дозволяє маршрутизаторам обмінюватися інформацією про стан мережі, доступні маршрути та вартість кожного маршруту. В результаті, маршрутизатори можуть встановлювати маршрути до різних мереж та пересилати пакети даних відправникам до призначень.

Налаштуємо протокол OSPF на всіх маршрутизаторах локальної мережі:

Buriachenko_Router3 (config)#router ospf 1 // процес запуску роботи протоколу

Buriachenko_Router3 (config-router)#network 10.0.2.8 0.0.0.3 area 0 // передаємо інформацію протоколу за підключення мережі *10.0.2.8*

Buriachenko_Router3 (config-router)#network 10.0.2.12 0.0.0.3 area 0 // передаємо інформацію протоколу за підключення мережі *10.0.2.12*

Buriachenko_Router3 (config-router)#network 10.0.2.20 0.0.0.3 area 0 // передаємо інформацію протоколу за підключення мережі *10.0.2.20*

Buriachenko_Router3 (config-router)#ip route 0.0.0.0 0.0.0.0 209.165.202.1 // встановлюємо статичний маршрут для обміну інформації локальної мережі в глобальну мережу

Процедуру налаштування слід застосувати на всіх маршрутизаторах мережі, окрім магістрального.

На кожному маршрутизаторі з’явиться таблиця маршрутизації, де записи з символом – O, будуть вказувати на маршрут з протоколу OSPF.

```
     10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
O       10.0.2.0/30 [110/128] via 10.0.2.9, 04:39:38, Serial0/2/1
O       10.0.2.4/30 [110/128] via 10.0.2.9, 04:39:38, Serial0/2/1
                    [110/128] via 10.0.2.14, 04:39:38, Serial0/2/0
C       10.0.2.8/30 is directly connected, Serial0/2/1
L       10.0.2.10/32 is directly connected, Serial0/2/1
C       10.0.2.12/30 is directly connected, Serial0/2/0
L       10.0.2.13/32 is directly connected, Serial0/2/0
O       10.0.2.16/30 [110/65] via 10.0.2.14, 04:39:08, Serial0/2/0
C       10.0.2.20/30 is directly connected, Serial0/3/0
L       10.0.2.21/32 is directly connected, Serial0/3/0
     192.168.6.0/24 is variably subnetted, 3 subnets, 2 masks
O       192.168.6.0/26 [110/65] via 10.0.2.22, 04:39:38, Serial0/3/0
O       192.168.6.64/26 [110/65] via 10.0.2.9, 04:39:38, Serial0/2/1
O       192.168.6.128/28 [110/66] via 10.0.2.14, 04:39:08, Serial0/2/0
     209.165.202.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.202.0/30 is directly connected, Serial0/3/1
L       209.165.202.1/32 is directly connected, Serial0/3/1
S*   0.0.0.0/0 [1/0] via 209.165.202.2
```

Рисунок 3.3 – Побудовані маршрути на маршрутизаторах

3.4.4 Налаштування правил віртуальної мережі

ACL – це система побудови списків контролю доступу та правил, які розраховані для мережевого обладнання, та використовується як інструкція, за якою треба прцювати мережевому обладнанню, а саме приймати або відправляти пакети в мережах.

Згідно до варіанту поставлених завдань будуть створені мережі за номерами 12,22 та 32, які не повинні мати доступ одна між одною.

Налаштування проводимо на маршрутизаторі Buriachenko_Router2:

ip access-list extended vlan // налаштуємо мережі у списку з назвою vlan

deny ip 192.168.6.208 0.0.0.15 192.168.6.224 0.0.0.15 // забороняємо мережі *192.168.6.208* потрапляти у мережу *192.168.6.224*

deny ip 192.168.6.208 0.0.0.15 192.168.6.240 0.0.0.15 // забороняємо мережі *192.168.6.208* потрапляти у мережу *192.168.6.240*

deny ip 192.168.6.224 0.0.0.15 192.168.6.208 0.0.0.15 // забороняємо мережі *192.168.6.224* потрапляти у мережу *192.168.6.208*

deny ip 192.168.6.224 0.0.0.15 192.168.6.240 0.0.0.15 // забороняємо мережі *192.168.6.224* потрапляти у мережу *192.168.6.240*

deny ip 192.168.6.240 0.0.0.15 192.168.6.224 0.0.0.15 // забороняємо мережі *192.168.6.240* потрапляти у мережу *192.168.6.224*

deny ip 192.168.6.240 0.0.0.15 192.168.6.208 0.0.0.15 // забороняємо мережі *192.168.6.240* потрапляти у мережу *192.168.6.208*

permit ip any any // встановлюємо правило, що всі інші мережі маршрутизуються без умов

interface gigabitEthernet 0/1.12 // налаштовуємо саб-інтерфейс *gigabitEthernet 0/1.12*

ip access-group vlan in // встановлюємо створений раніше список до роботи

interface gigabitEthernet 0/1.22 // налаштовуємо саб-інтерфейс *gigabitEthernet 0/1.12*

ip access-group vlan in // встановлюємо створений раніше список до роботи

interface gigabitEthernet 0/1.32// налаштовуємо саб-інтерфейс *gigabitEthernet 0/1.12*

ip access-group vlan in // встановлюємо створений раніше список до роботи

Якщо ми виконаємо ехо-запит між мережами, то побачимо, що доступ між ними заблокований.

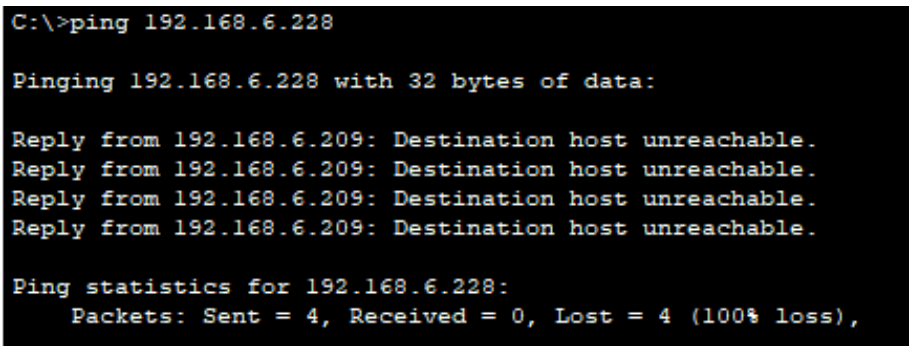

Рисунок 3.4 – Перевірка роботи встановлених налаштувань

3.4.5 Налаштування резервування дротового підключення в мережі

Резервування дротового підключення в мережі виконується за допомогою протоколу агрегації портів – LACP.

Налаштуємо протокол LACP на комутаторі Buriachenko_Switch4:

int range fa0/1-2 // використовуємо порти, які будуть залучені у агрегацію системи

channel-group 1 mode active // створюємо першу групу портів у режими *active*

Creating a port-channel interface Port-channel 1 // група створена

int port-channel 1 // використовуємо створену групу

switchport mode trunk // встановлюємо режим роботи групи у *trunk* режимі

int range f0/3-4 // використовуємо порти, які будуть залучені у агрегацію системи

channel-group 2 mode passive // створюємо другу групу портів у режими passive

Creating a port-channel interface Port-channel 2 // група створена

int port-channel 2 // використовуємо створену групу

switchport mode trunk // встановлюємо режим роботи групи у *trunk* режимі

Тепер, якщо один із фізичних портів вийде із ладу, трафік автоматично перенаправиться на порти, що залишилися в порт-агрегаті.

LACP підтримує два режими роботи - активний (active) і пасивний (passive). В активному режимі він ініціює процес агрегації портів, а в пасивному режимі - відповідає на запити агрегації.

```
Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------

1      Po1(SU)           LACP   Fa0/1(P) Fa0/2(P)
2      Po2(SD)           LACP   Fa0/3(I) Fa0/4(I)
```

Рисунок 3.5 – Встановлений протокол LACP

3.4.6 Налаштування підмереж корпоративної мережі

Для відокремлення певних відділ компанії між собою на одному мережевому обладнанні було використано технології VLAN, розподілення повинно забезпечувати три незалежні підмережі.

Дані розподілення мережі занесені у таблицю 3.4.

Таблиця 3.4 – Ідентифікація підмереж розподілення

№ VLAN	Назва VLAN	№ портів
12	group1	F0/5-f0/9
22	group2	F0/10-f0/14
32	group3	F0/15-f0/24

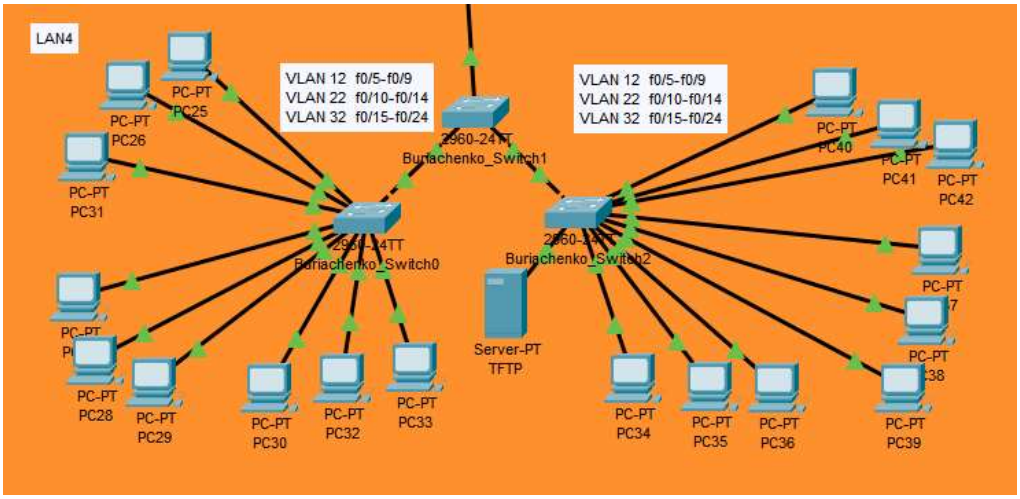

Рисунок 3.6 – Графічне зображення віртуальних мереж

Встановимо налаштування на комутаторах Buriachenko_Switch0 та Buriachenko_Switch2

(config)#vlan 12 // налаштовуємо vlan під номером 12

(config-vlan)#name group1 // встановлюємо назву *group1*

(config)#vlan 22 // налаштовуємо vlan під номером 22

(config-vlan)#name group2 // встановлюємо назву *group2*

(config)#vlan 32 // налаштовуємо vlan під номером 32

(config-vlan)#name group3 // встановлюємо назву *group3*

(config)#interface range g0/1-2 // заходимо у інтерфейси комутатора, які виходять з нього для взаємодії з іншими комутаторами

(config-if)#switchport trunk allowed vlan 12,22,32 // встановлюємо правила передачі інформацію лише для виділених номерів vlan

(config-if)#switchport mode trunk // встановлюємо роботу порту в режимі *trunk*

(config)#interface range f0/5-9

(config-if)#switchport mode access

(config-if)# switchport access vlan 12 // до портів *f0/5-9* відносимо *vlan 12*

(config)#interface range f0/10-14

(config-if)#switchport mode access

(config-if)# switchport access vlan 22 // до портів *f0/10-14* відносимо *vlan 22*

(config)#interface range f0/15-24

(config-if)#switchport mode access

(config-if)# switchport access vlan 32// до портів *f0/15-24* відносимо *vlan 32*

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24
12   group1                           active
22   group2                           active
32   group3                           active
```

Рисунок 3.7 – Запис підмереж на комутаторі

3.4.7 Налаштування параметрів безпеки маршрутизаторів

Параметри безпеки маршрутизаторів налаштовуються відповідно до заходів авторизації в систему.

Налаштування маршрутизаторів здійснюється наступним чином:

(config) aaa new-model // на кожному маршрутизаторі вмикаємо роботу протоколу

(config) radius-server host *IP-адреса серверу AAA* // встановлюємо значення адреси серверу AAA відповідно до адресації мережі

(config) radius–server key radius123 // встановлюємо захисний ключ з'єднання r*adius123*

(config) aaa authentication login default group radius local // використовуємо авторизацію пріорітету, спочатку сервер, потом локальні облікові записи

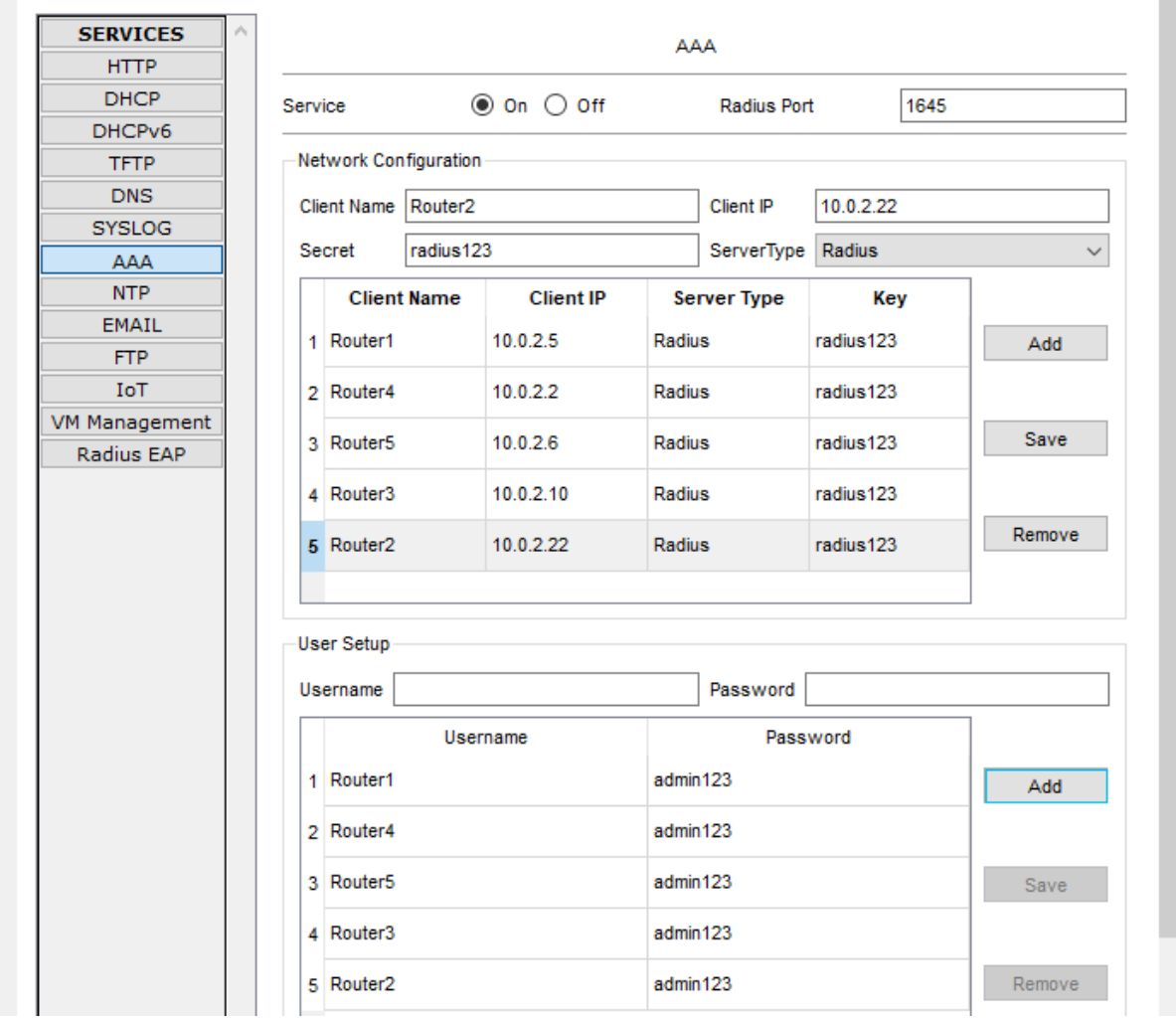

Рисунок 3.8 – Сценарії створення даних

3.5 Перевірка роботи комп’ютерної системи компанії

Для підтвердження працездатності мережевої інфраструктури компанії «Lifecell» необхідно провести перевірку роботи з урахуванням проведених налаштувань.

```
Router#show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
192.168.6.67     0002.4A4E.5454          --                      Automatic
192.168.6.69     0090.21BD.001E          --                      Automatic
192.168.6.68     00E0.F933.A271          --                      Automatic
192.168.6.70     0002.17D4.284D          --                      Automatic
192.168.6.71     00D0.FFCC.6217          --                      Automatic
192.168.6.72     0001.4244.2944          --                      Automatic
```

Рисунок 3.9 – Автоматичне налаштування адресації пристроїв

0	123.dnipro.ua	A Record	192.168.6.132
1	http://123.dnipro.ua	CNAME	123.dnipro.ua

Рисунок 3.10 – Перенаправлення адреси в назву та навпаки для роботи веб-сайту

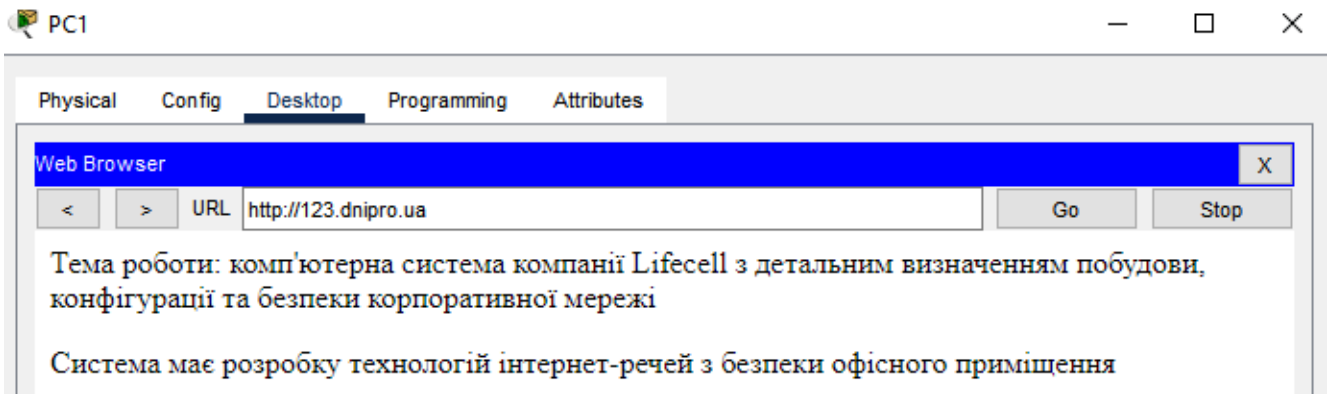

Рисунок 3.11 – Інформація закладена на веб-сайті

```
C:\>ping 192.168.6.6

Pinging 192.168.6.6 with 32 bytes of data:

Reply from 209.165.202.1: bytes=32 time=2ms TTL=124
Reply from 209.165.202.1: bytes=32 time=2ms TTL=124
Reply from 209.165.202.1: bytes=32 time=2ms TTL=124
Reply from 209.165.202.1: bytes=32 time=2ms TTL=124

Ping statistics for 192.168.6.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

Рисунок 3.12 – Працездатність вузлів між різними підмережами

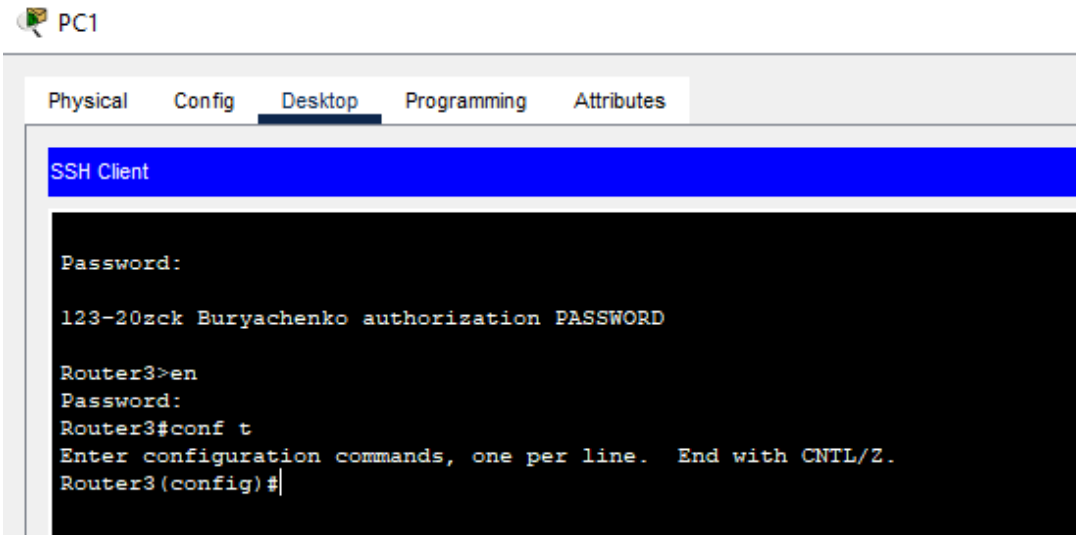

Рисунок 3.13 – Здійснення авторизації за протоколом віддаленого доступу

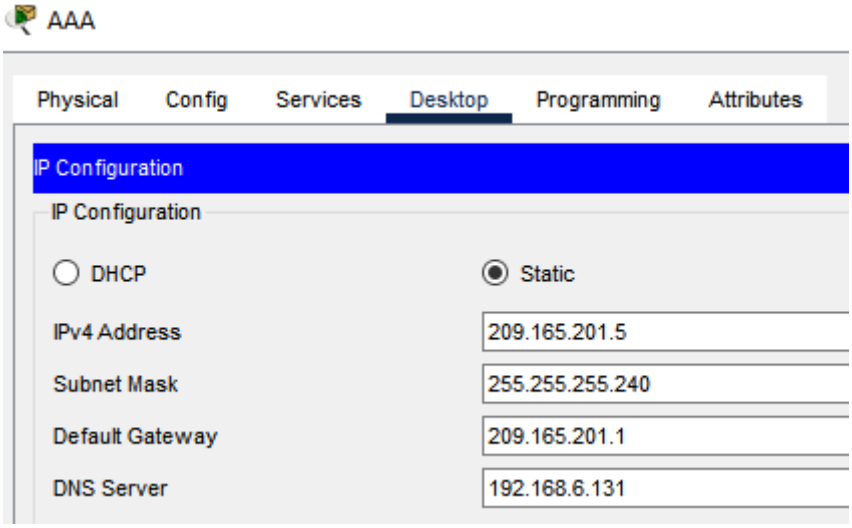

Рисунок 3.14 – Налаштування мережевого інтерфейсу серверу безпеки

```
Extended IP access list VLANS
    10 deny ip 192.168.6.208 0.0.0.15 192.168.6.224 0.0.0.15
    20 deny ip 192.168.6.208 0.0.0.15 192.168.6.240 0.0.0.15
    30 deny ip 192.168.6.224 0.0.0.15 192.168.6.208 0.0.0.15
    40 deny ip 192.168.6.224 0.0.0.15 192.168.6.240 0.0.0.15
    50 deny ip 192.168.6.240 0.0.0.15 192.168.6.208 0.0.0.15
    60 deny ip 192.168.6.240 0.0.0.15 192.168.6.224 0.0.0.15
    70 permit ip any any (38 match(es))
```

Рисунок 3.15 – Налаштовані списки доступів для віртуальних локальних мереж

4 РОЗРОБКА КОМПОНЕНТА СИСТЕМИ БЕЗПЕКИ ОФІСНОГО ПРИМІЩЕННЯ

4.1 Розробка системи в цілому та створення сценаріїв

При розробці компонента мережі було спроектовано рішення щодо безпеки персоналу, які мають доступ підрозділів мережі.

Система спроектована за допомогою IoT технологій.

До складу системи входять: 2 RFID-зчитувача, 4 RFID-мітки (2 valid та 2 novalid), 2 IoT-двері, 2 IoT-web-камери. Всі співробітники отримують доступ до підрозділів за допомогою наявності RFID-мітки та сигналу від зчитувачів. За сигналом кожного зі зчитувачів відбувається відчинення відповідних дверей та ввімкнення web-камери.

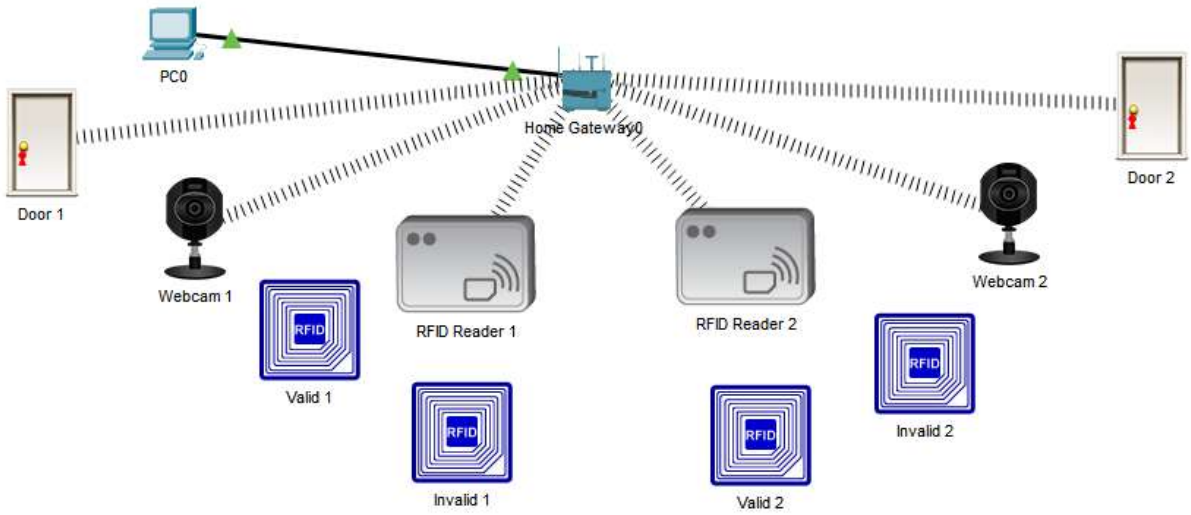

Рисунок 4.1 – Логічна топологія мережі

В системі у кожного RFID зчитувача є по дві мітки, одна valid та одна invalid.

Таблиця 4.1 – Вихідні дані

Door	End Devices → Home
Webcam	End Devices → Home
RFID Reader	End Devices → Power Meter
RFID Card	End Devices → Power Meter

Після створення логічної мережі усі елменти були налаштовані к реєстраційному сервері.

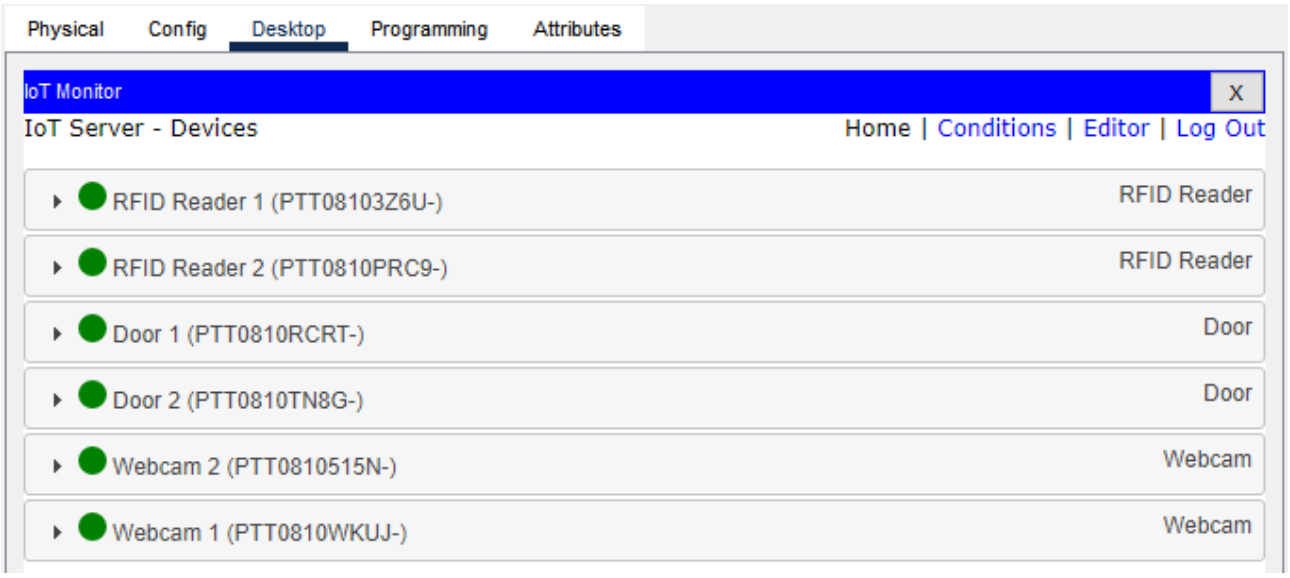

Рисунок 4.2 – Елементи мережі в сервері

Також були налоштовані наступні сценарії на сервері:

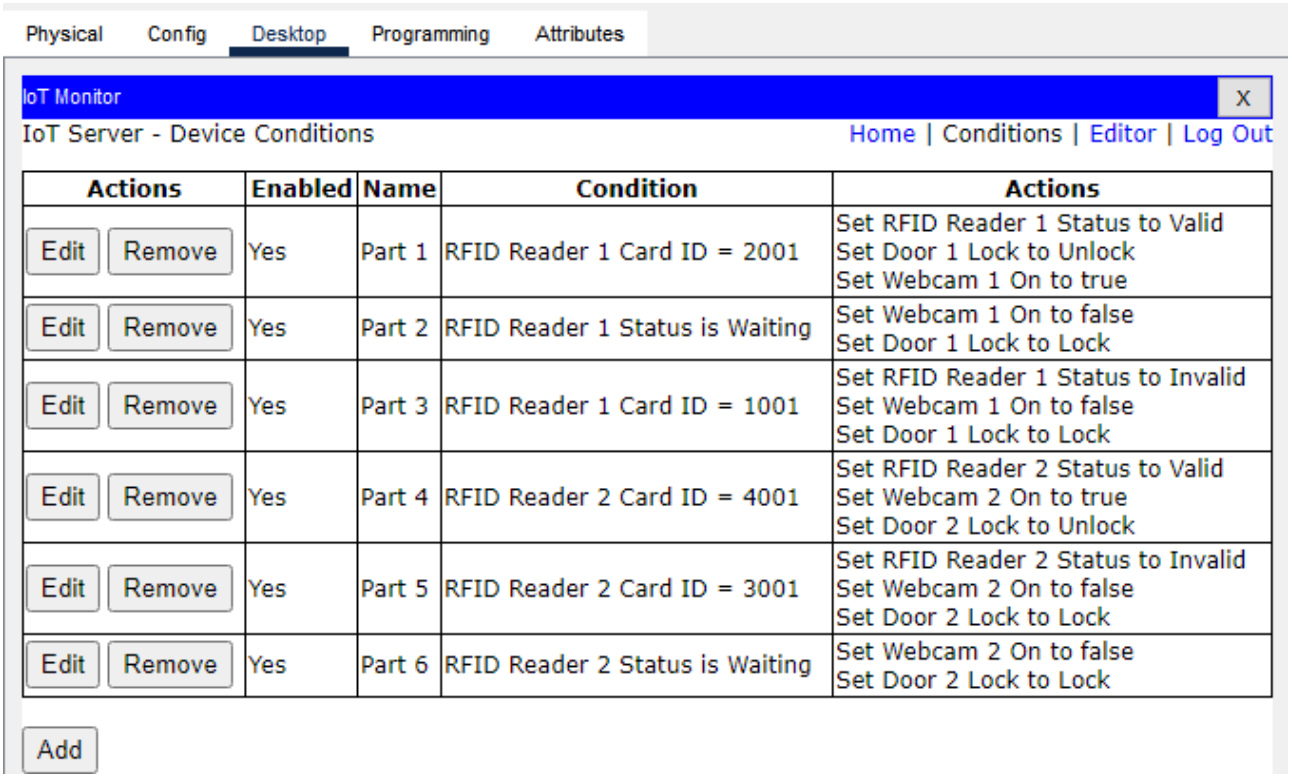

Рисунок 4.3 – Сценарії на сервері

В даній реалізації проєкту RFID картки мають певне значення до яких RFID зчитувач заздалегідь готовий. Вони мають значення 1001, 2001, 3001, 4001, де 2001

та 4001 мають статус valid у своїх певних зчитувачах. Об’єм значень не має меж, тому система має змогу зареєструвати безліч співробітників. Всі значення та налаштування знаходяться в адміністративному підрозділі.

В будь-який момент часу завжди можна активувати або деактивувати RFID картку і людина отримає або не отримає доступ в підздрозділ.

ВИСНОВКИ

Виконання кваліфікаційної роботи призвело до повної розробки комп’ютерної мережі об’єкта впровадження. Мережа складається с детального опрацювання систем функціонування, безпеки та управління. Моделювання мережі виконано в додату Cisco Packet Tracer.

Мережа складається с чотирьох підмереж, водповідно до вимог та структурної схеми компанії. Завдяки технології VLSM мережа має зручну конфігурацію налатшувань з IP-адресації. Всі адреси вузлів мережі були зображені в таблиці адресації пристроїв.

Мережеве обладнання налаштоване за вимогами безпеки та підтримує управління пристроєм за допомогою протоколу SSH. Маршрутизація в мережі виконано за технологією OSPF.

Для виходу робочих станцій співробітників з локальної мережі в глобальну мережу, було налаштовано протокол NAT. В мережі існує розподіл на підмережі за протоколом VLAN, який в свою чергу використовує списки доступу ACL.

Мережа має власні DNS та HTTP сервери, до яких під’єднані всі користувачі мережі.

В наш час мережа має сучасні апаратні та програмні технології. Завдяки якісному мережевому обладнанню, мережа має великий запас щодо додавання нових користувачів в мережу.

Інформацію з кваліфікаційної роботи можна застосовувати при налаштуванні великих мереж з поділами на підмережі та використовувати як алгоритм функціонування мереж.

ПЕРЕЛІК ПОСИЛАНЬ

1. Цвіркун Л.І. Глобальні комп’ютерні мережі. Програмування мовою PHP: навч. посібник / Л.І. Цвіркун, Р.В. Липовий, під заг. ред. Л.І. Цвіркуна. – Д.: Національний гірничий університет, 2013. – 239 с. – ISBN 978-966-350-417-9.

2. Цвіркун Л.І. Комп’ютерні мережі. Методичні рекомендації до виконання лабораторних робіт студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп’ютерна інженерія: у 2 ч. / Л.І. Цвіркун, Я.В. Панферова ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2018. – Ч. 2. – 39 с.

3. ДСТУ 3008-2015. Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлювання. – К.: Держстандарт, 2015. – 37 с.

4. ДСТУ ГОСТ 7.1:2006. Бібліографічний запис, бібліографічний опис. Загальні вимоги та правила складання: метод. рекомендації з впровадження / Уклали: Галевич О. К., Штогрин І. М. – Львів, 2008. – 20 с.

5. Дипломування. Методичні вказівки для бакалаврів галузі знань 12 Інформаційні технології спеціальності 123 Комп’ютерна інженерія / Л.І. Цвіркун, С.М. Ткаченко, Я.В. Панферова ; М-во освіти і науки України, Нац. гірн. ун-т. – Дніпро: НГУ, 2016. – 56 с.

6. Налаштування локальних пристроїв для користувачів Cisco [Електронний ресурс] – https://collaborationhelp.cisco.com/uk-ua/article/poqjhk/Cisco-Webex-Teams

7. Cisco. Агрегування каналів. [Електронний ресурс] – http://steinkafer.blogspot.com/2016/01/cisco.html

8. Cisco VLAN - налаштування vlan на комутаторі Cisco [Електронний ресурс] – https://www.skleroznik.in.ua/2015/08/03/cisco-vlan-nastrojka-vlan-na-kommutatore-cisco/

9. Що таке NAT. Як налаштовується мережева трансляція адрес. Технічні нюанси [Електронний ресурс] – https://techprofi.com/network/nastroyka-nat/

10. Комп'ютерні мережі та безпека за технологіями CISCO [Електронний ресурс] – https://my.kpi.ua/syllabus/4390?trainform=1

Додаток А

Текст програми налаштування мережі комп’ютерної системи

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

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Текст програми
804.02070743.23002-01 12 01

Листів 13

2023

АННОТАЦІЯ

Програма складається с частини програмного коду для налаштування конфігурацій мережевих інтерфейсів мережі. Код призначений для впровадження протоколів DHCP, AAA, NAT, для налаштування консолей та ліній VTY та для створення комп'ютерних систем VPN, домену та SSH доступу. Також налаштовується агрегування каналів – PagP.

ЗМІСТ

Конфігурація R0:

```
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
ip dhcp pool Vlan12
 network 192.168.6.208 255.255.255.240
 default-router 192.168.6.209
 dns-server 192.168.6.131
ip dhcp pool Vlan22
 network 192.168.6.224 255.255.255.240
 default-router 192.168.6.225
 dns-server 192.168.6.131
ip dhcp pool Vlan32
 network 192.168.6.240 255.255.255.240
 default-router 192.168.6.241
 dns-server 192.168.6.131
ip dhcp pool LAN4
 network 192.168.6.192 255.255.255.240
 default-router 192.168.6.193
 dns-server 192.168.6.131
!
ip cef
no ipv6 cef
!
license udi pid CISCO2911/K9 sn FTX1524C17G-
```

```
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
 ip address 64.100.13.1 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.6.193 255.255.255.240
 duplex auto
 speed auto
!
interface GigabitEthernet0/1.12
 encapsulation dot1Q 12
 ip address 192.168.6.209 255.255.255.240
 ip access-group VLANS in
!
interface GigabitEthernet0/1.22
 encapsulation dot1Q 22
 ip address 192.168.6.225 255.255.255.240
 ip access-group VLANS in
!
interface GigabitEthernet0/1.32
 encapsulation dot1Q 32
 ip address 192.168.6.241 255.255.255.240
 ip access-group VLANS in
!
interface GigabitEthernet0/2
 no ip address
```

```
 duplex auto
 speed auto
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 64.100.13.2
!
ip flow-export version 9
!
!
ip access-list extended VLANS
 deny ip 192.168.6.208 0.0.0.15 192.168.6.224 0.0.0.15
 deny ip 192.168.6.208 0.0.0.15 192.168.6.240 0.0.0.15
 deny ip 192.168.6.224 0.0.0.15 192.168.6.208 0.0.0.15
 deny ip 192.168.6.224 0.0.0.15 192.168.6.240 0.0.0.15
 deny ip 192.168.6.240 0.0.0.15 192.168.6.208 0.0.0.15
 deny ip 192.168.6.240 0.0.0.15 192.168.6.224 0.0.0.15
 permit ip any any
!
line con 0
line aux 0
!
line vty 0 4
 login
end
```

Налаштування маршрутизатора R3:

```
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Router3
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
no ip cef
no ipv6 cef
!
username 12320zck_Buriachenko password 7 0822455D0A16
!
license udi pid CISCO2911/K9 sn FTX1524O608-
!
ip domain-name Router3
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
```

```
 speed auto
 shutdown
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/2/0
 ip address 10.0.2.13 255.255.255.252
 ip nat inside
 clock rate 2000000
!
interface Serial0/2/1
 ip address 10.0.2.10 255.255.255.252
 ip nat inside
 clock rate 2000000
!
interface Serial0/3/0
 ip address 10.0.2.21 255.255.255.252
 ip nat inside
!
interface Serial0/3/1
 ip address 209.165.202.1 255.255.255.252
 ip nat outside
 clock rate 2000000
!
interface Vlan1
 no ip address
```

```
 shutdown
!
router ospf 1
 log-adjacency-changes
 network 10.0.2.8 0.0.0.3 area 0
 network 10.0.2.12 0.0.0.3 area 0
 network 10.0.2.20 0.0.0.3 area 0
 network 209.165.202.0 0.0.0.3 area 0
!
ip nat inside source list 7 interface Serial0/3/1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.202.2
!
ip flow-export version 9
!
access-list 7 permit 192.168.6.0 0.0.0.255
!
banner motd #123-20zck Buriachenko authorization PASSWORD#
!
line con 0
 password 7 0822455D0A16
 login
!
line aux 0
!
line vty 0 4
 login local
 transport input ssh
end
```

Налаштування комутатора Sw0:

```
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
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 12
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 12
 switchport mode access
!
interface FastEthernet0/7
 switchport access vlan 12
```

```
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 12
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 12
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 22
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 22
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 22
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 22
 switchport mode access
!
interface FastEthernet0/14
 switchport access vlan 22
 switchport mode access
!
```

```
interface FastEthernet0/15
 switchport access vlan 32
 switchport mode access
!
interface FastEthernet0/16
 switchport access vlan 32
 switchport mode access
!
interface FastEthernet0/17
 switchport access vlan 32
 switchport mode access
!
interface FastEthernet0/18
 switchport access vlan 32
 switchport mode access
!
interface FastEthernet0/19
 switchport access vlan 32
 switchport mode access
!
interface FastEthernet0/20
 switchport access vlan 32
 switchport mode access
!
interface FastEthernet0/21
 switchport access vlan 32
 switchport mode access
!
interface FastEthernet0/22
 switchport access vlan 32
```

```
 switchport mode access
!
interface FastEthernet0/23
 switchport access vlan 32
 switchport mode access
!
interface FastEthernet0/24
 switchport access vlan 32
 switchport mode access
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
 switchport trunk allowed vlan 12,22,32
 switchport mode trunk
!
interface Vlan1
 no ip address
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
end
```