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 Квятковської Діани Миколаївни
(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 АТ "Універсал банк" з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі»
(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	проф. Цвіркун Л.І.			
розділів:				
розробка апаратної частини	доц. 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 Квятковської Д.М. **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 АТ "Універсал банк" 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 _____ проф. Цвіркун Л.І.
(підпис керівника) (прізвище, ініціали)

Дата видачі 25.01.2023

Дата подання до екзаменаційної комісії 12.07.2023

Прийнято до виконання _____ Квятковська Д.М.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 63 с., 31 рис., 8 табл., 2 дод., 10 джерел.

LAN, WAN, VLAN, SSH, Wi-Fi, IoT, HTTP, DNS, ОБЛІК ДАНИХ

Об’єкт: комп'ютерна система АТ “Універсал банк” з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі.

Мета: створення мережевої системи управління банку з моделюванням проекту, налаштуванням безпеки системи в цілому.

Основна мета створення комп'ютерної мережі в банку полягає в забезпеченні ефективного та безпечного обміну інформацією, управлінні даними та наданні високоякісних послуг клієнтам.

Комп'ютерна мережа дає змогу зв'язати різні відділи банку, забезпечуючи оперативний обмін інформацією. Це дає змогу банку ефективно управляти клієнтськими даними, фінансовими операціями, транзакціями та іншою важливою інформацією.

Також дає змогу банку зберігати й управляти великим обсягом даних про клієнтів, рахунки, транзакції, кредити та інші фінансові операції. Централізоване зберігання даних забезпечує доступність і цілісність інформації, а також полегшує виконання аналізу даних і створення звітів.

Основні технологічні характеристики які забезпечує комп'ютерна мережа:

– топологія - зірку(дерево);
– протоколи зв'язку – TCP/IP;
– висока пропускна спроможність;
– масштабованість;
– безпека;
– резервування і відмовостійкість.

Моделювання мережевої системи банку було відображено в додатку Cisco Packet Tracer.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАК, ОДИНИЦЬ І ТЕРМІНІВ

Wi-Fi – бездротовий доступ в Інтернет;

VLAN – сегментована мережа;

DHCP – протокол автоматичного розподілу конфігурацій;

OSPF – протокол маршрутизації;

NAT – протокол маскування IP-адрес;

EtherChannel – технологія паралельного з’єднання;

ACL – списки дозволених операцій;

AAA – протокол моделі доступу та управління;

HTTP – протокол передачі інформації;

DNS – сервер доменних імен;

SBC – програмований мікроконтролер;

TFTP – протокол передачі та збереження файлів;

SSH – протокол захищеної оболонки.

ВСТУП

У наш час комп'ютерні мережі в банках відіграють ключову роль у їхній діяльності. Мережі дають змогу банкам ефективно управляти інформацією, забезпечувати безпеку даних і надавати високоякісні послуги клієнтам.

В Україні існує кілька дротових компаній, які надають послуги доступу до інтернету. Деякі з них включають:

– «Укртелеком» – найбільший національний оператор зв'язку в Україні, що надає широкий спектр послуг, включно з DSL і оптоволоконним інтернетом під брендом «VOLIA»;

– «Vodafone Україна» – великий оператор мобільного зв'язку, що пропонує також послуги фіксованого доступу до інтернету через DSL і оптоволокно.

– «Kyivstar» – оператор мобільного зв'язку, який надає послуги доступу в мережу інтернет через DSL;

– «Lanet Network» – провайдер широкосмугового інтернету і телекомунікаційних послуг, що надає високошвидкісний доступ в інтернет за технологіями DSL і оптоволокно;

– «Triolan» – провайдер послуг кабельного та оптоволоконного інтернету, що надає послуги в різних регіонах України.

У наш час існує кілька способів побудови локальної мережі (Local Area Network, LAN) з використанням різних технологій. Ось деякі з найпоширеніших способів:

– провідна мережа Ethernet є одним із найпоширеніших способів побудови локальної мережі. Вона використовує мережеві кабелі (зазвичай кручена пара) для з'єднання комп'ютерів, серверів, принтерів та інших мережевих пристроїв. Ethernet підтримує різні швидкості передачі даних, такі як 10/100/1000 Mbps і більше;

– бездротова мережа Wi-Fi дає змогу пристроям підключатися до мережі без використання дротів. Wi-Fi використовує радіохвилі для передачі даних між

пристроями. Для побудови Wi-Fi мережі потрібен Wi-Fi маршрутизатор, який забезпечує бездротове з'єднання між пристроями та доступ в Інтернет;

– провідна мережа оптоволокно на основі оптоволоконних кабелів (fiber-optic network) надає високу швидкість передавання даних і велику пропускну здатність. Оптоволокно дає змогу передавати дані з використанням світлових сигналів замість електричних сигналів, що забезпечує більш стабільне і швидке з'єднання.

Кваліфікаційна записка є документом, який подає інформацію про навички, знання та досвід роботи.

Вона може бути корисною в кількох аспектах:

– працевлаштуванні;
– просуванні кар'єрними сходами;
– освіті та навчанні;
– професійній акредитації;
– участі у проєктах і конкурсах.

Загалом, кваліфікаційна записка з комп'ютерної інженерії допомагає документувати професійні знання та досвід у даній галузі, що може бути корисним під час пошуку роботи, кар'єрного розвитку та подальшого навчання.

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

1.1 Стисла характеристика мережі проектування

Для проектування мережі було обрано сферу банківської діяльності.

Мережа банківської системи призначена для обслуговування клієнтів, введення обліку та передачі даних між співробітниками.

Проектування комп'ютерної мережі – це процес планування, створення та організації мережевої інфраструктури. Ось деякі основні характеристики проектування комп'ютерної мережі:

Архітектура мережі – включає вибір відповідної архітектури мережі відповідно до вимог і потреб організації. Це може бути централізована, децентралізована або комбінована архітектура.

Топологія мережі – вибір оптимальної топології мережі (наприклад, зірка, кільце, шина, дерево) залежить від вимог мережі, кількості вузлів і очікуваного трафіку.

Технології, що використовуються – вибір відповідних технологій для мережі включає вибір мережевих протоколів, стандартів зв'язку (наприклад, Ethernet, Wi-Fi), типів кабелів і обладнання (комутатори, маршрутизатори тощо).

Безпека – проєктування мережі має включати заходи безпеки, щоб захистити дані та ресурси мережі від несанкціонованого доступу та шкідливих атак. Це може включати фаєрволи, шифрування даних, аутентифікацію та інші заходи безпеки.

Пропускна здатність і масштабованість – під час проєктування мережі необхідно враховувати необхідну пропускну здатність мережі, а також її масштабованість, тобто здатність мережі розширюватися і підтримувати зростаючий обсяг трафіку і кількість пристроїв.

Керування та моніторинг – мережа має бути проєктована з урахуванням можливості керування та моніторингу її стану, продуктивності, навантаження і проблем.

1.2 Характеристика та аналіз діяльності АТ «Універсал Банк»

«Універсал Банк» – це універсальний банк, що займає 12 сходинку в рейтингу життєздатності системи Mind.

Банк працює з 1994 року. З грудня 2016 року «Універсал Банк» є частиною групи «ТАС» Сергія Тігіпка. В 2017 році на базі «Універсал Банк» команда Дмитра Дубілєта створила проєкт Monobank, який цьогоріч відсвяткував 5 років.

«Універсал Банк» входить в десятку українських банків за розмірами активів.

Рисунок 1.1 – Вигляд відділення АТ «Універсал Банк»

Сьогодні основна маса традиційних стандартних послуг, що надаються банком, – таких, наприклад, як приймання грошей, проведення платежів і короткострокове кредитування – здійснюється банкоматами, а також автоматизованими філіями, що працюють цілодобово. Це дає змогу значно збільшити обсяг операцій, які здійснюються електронними банківськими системами. Водночас це позитивним чином позначається на подальшому розвитку

банківської сфери, оскільки дає змогу скоротити витрати на персонал, до обов'язків якого раніше входило консультування та обслуговування клієнтів, і спрямувати зекономлені кошти на подальший розвиток банківської сфери та впровадження IT-технологій.

Застосування IT-технологій, спрямованих на створення стандартизованого профілю, що відповідає всім міжнародним стандартам, дасть змогу клієнтам не відчувати різниці між філією банку, розташованою в центрі міста і на його околиці.

1.3 Організаційна структура об’єкта впровадження

Організаційна структура управління включає в себе розподіл функцій та відповідальностей між різними рівнями та підрозділами організації. Вона визначає, як приймаються рішення, комунікується і виконується робота в межах організації. Організаційна структура управління може змінюватися в залежності від типу організації, розміру, діяльності та стратегії.

Організаційна структура АТ «Універсал Банк» має ієрархічну структуру. Ієрархічна структура передбачає рівні управління, включаючи верхній рівень (наприклад, керівництво) та нижчі рівні (наприклад, відділи, підрозділи).

Керівники на вищих рівнях приймають стратегічні рішення, тоді як керівники на нижчих рівнях відповідають за оперативне виконання завдань.

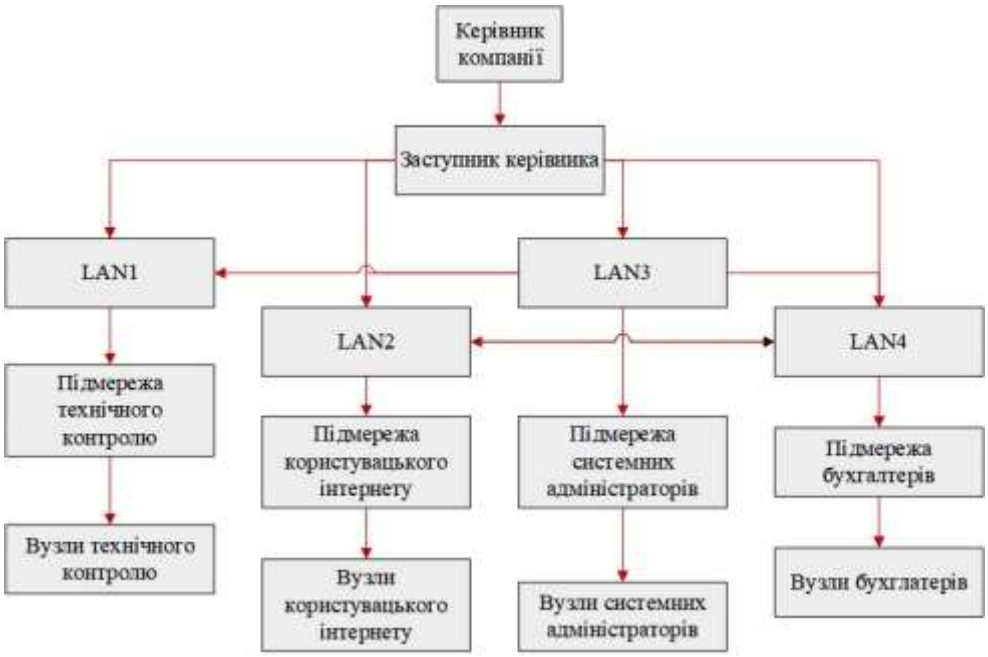

Рисунок 1.2 – Організаційна структура банку відповідно до мережі

За структурною схемою (рисунок 1.2) видно, що компанія має централізоване управління.

Централізоване управління – це підхід до управління організацією або системою, за якого ухвалення рішень і контроль над діяльністю зосереджені в одному центральному органі або управлінському органі. У такій моделі центральне керівництво має широкий спектр повноважень і ухвалює ключові стратегічні й тактичні рішення, а потім передає їх для виконання та реалізації на нижчі рівні.

Підрозділ технічного контролю виконує важливі функції щодо забезпечення відповідності поданих документів та інформації встановленим вимогам і правилам.

Підмережа користувацького інтернету розрахована на точку доступу Wi-Fi, а саме для безкоштовного виходу в інтернет клієнтам та співробітникам.

Підрозділ системних адміністраторів відповідає за управління, підтримку та забезпечення надійної роботи інформаційних систем і мережевої інфраструктури банку. Вони виконують низку завдань і обов'язків для забезпечення ефективного функціонування технологічного середовища банку.

Підрозділ бухгалтерів відповідає за ведення фінансової звітності, обробку фінансової інформації та виконання інших завдань, пов'язаних із фінансовим обліком та аналізом.

Всі сфери відіграють важливу роль і взаємопов'язані між собою для забезпечення ефективного функціонування банківської діяльності.

1.4 Топологічна схема розміщення структурних підрозділів

Топографічна схема банку – це графічне зображення структури та розташування різних відділів і приміщень усередині банківських будівель.

Метою топографічної схеми є забезпечення чіткого уявлення про внутрішню організацію банку, включно з трьома будівлями. Топографічна схема банку розроблена з урахуванням зручності та безпеки.

Схема має 3 різні будівлі з різними підрозділами, але підмережа бухгалтерів та підмережа користувацького інтернету знаходяться в одній будівлі.

Всі будівлі проекту кваліфікаційної роботи знаходяться в Україні, м. Дніпро.

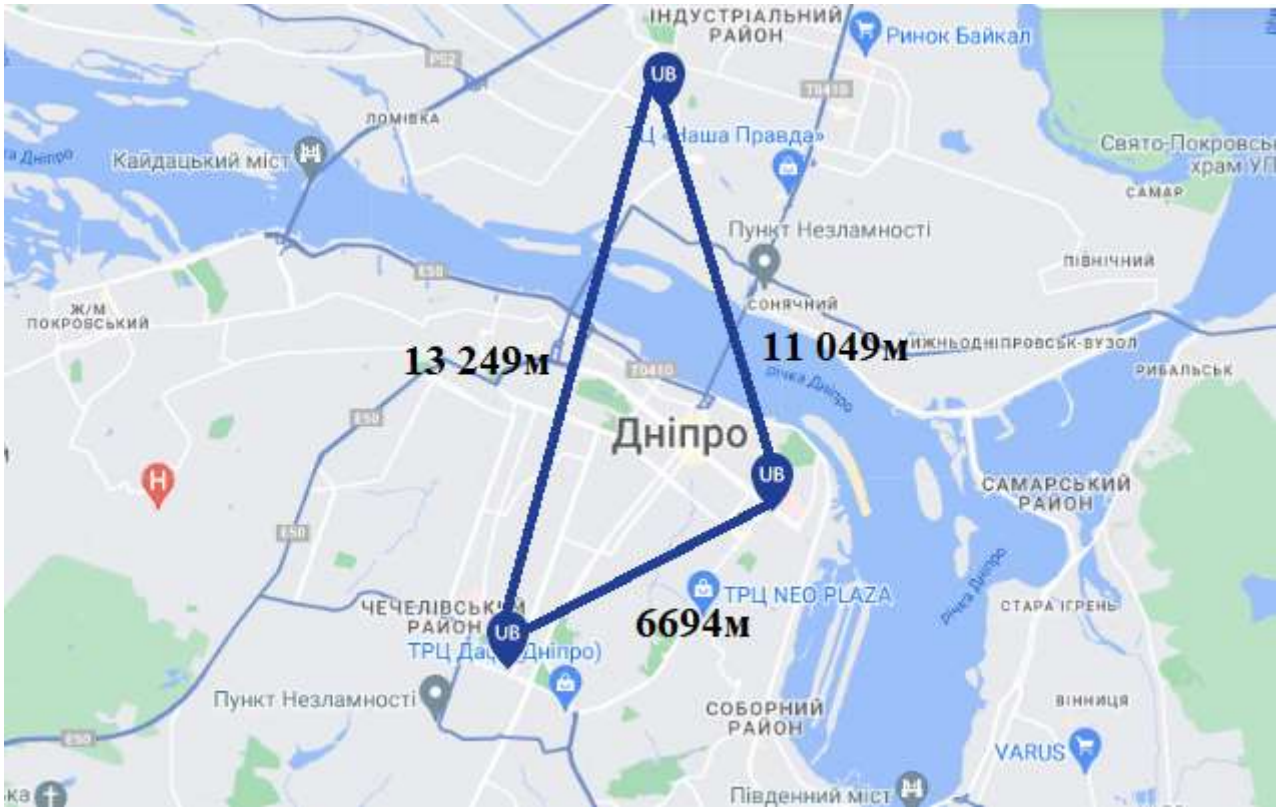

Рисунок 1.3 – Топографічна схема банку

1.5 Принцип побудови об’єкта проектування

Для розуміння принципу побудову мережі потрібно визначити варіанти організації передачі даних. Існує багато способів обробки та передачі інформації в корпоративних мережах, наприклад:

– комутація пакетів (Packet Switching): цей спосіб передачі даних має широке застосування. Інформація розбивається на пакети, які незалежно передаються по мережі до призначення. Кожен пакет може обходити різні шляхи та приземлятися у різних частинах мережі перед доставкою.

– комутація каналів (Circuit Switching): цей спосіб використовується у традиційних телефонних мережах і деяких корпоративних системах. При встановленні з'єднання між двома вузлами мережі створюється постійний фізичний канал для передачі даних. Цей канал залишається відкритим протягом усього з'єднання. Використання комутації каналів дає гарантованість пропускної здатності.

– використання бездротових технологій: зростання популярності бездротових мереж, таких як Wi-Fi і Bluetooth, дозволяє безпроводово підключати пристрої до корпоративної мережі. Це надає мобільність і гнучкість спілкування, дозволяючи працівникам працювати з будь-якого місця в офісі або поза ним.

– використання віртуальних приватних мереж (VPN): VPN-підключення дозволяють забезпечити безпечну передачу даних через незахищені мережі, такі як Інтернет. Вони створюють зашифрований тунель між вузлами мережі, що дозволяє працівникам здійснювати віддалений доступ до ресурсів компанії без ризику проникнення незаконних осіб.

– використання облачних технологій: облачні сервіси дозволяють зберігати, обробляти та передавати інформацію через віддалені сервери, що доступні через Інтернет. Це дає змогу підприємствам зосередитися на своїй основній діяльності, перекладаючи частину обчислювального навантаження та зберігання даних на зовнішніх постачальників хмарних послуг.

При моделюванні проекту корпоративної мережі банку ми використовуємо комутація пакетів та бездротові технології.

1.6 Завдання і мета роботи

Метою кваліфікаційної роботи є створення функціональної і надійної мережі, яка забезпечує ефективну комунікацію та обмін даними в межах організації, і буде використовуватися кожного дня, для забезпечення прибутку фінансової діяльності банку.

В завдання входять наступні розділи:

– створити фізичну інфраструктуру мережі банку;

– для використання мережевого обладнання необхідно використовувати протокол захищеної віддаленої оболонки;

– при розробці безпеки мережі необхідно використати протокол моделі доступу та управління;

– для виходу в мережу інтернет застосовувати протокол маскування IP-адрес;

– для пристроїв в мережі застосувати протокол динамічної видачі мережевих налаштувань;

– для архівації мережевих конфігурацій необхідно використовувати протокол файлового збереження та передавання;

– при необхідності в кожній системи використовувати списки дозволених операцій;

– в мережі з трьома комутаторами налаштувати паралельне з'єднання каналів;

– налаштувати та перевірити роботу сегментованих мереж;

– в якості реалізації користувацього Інтернету налаштувати бездротовий зв’язок Wi-Fi;

– розробити систему безпеки та сигналізації засобами інтернет-речей.

1.7 Визначення можливих напрямків рішення поставлених завдань

Для побудови фізичної частини мережі можна використовувати проводові мережі. Напрямок передбачає використання проводів для підключення пристроїв до мережі. Це звичайний підхід, який забезпечує стабільність і високу швидкість передачі даних. При цьому можна використовувати різні типи кабелів, такі як вита пара, оптичний кабель або коаксіальний кабель та інші.

Безпровідні мережі здійснюються за допомогою безпровідних технологій, таких як Wi-Fi. Цей напрямок дозволяє створити гнучку та мобільну мережу, але швидкість передачі даних може бути обмеженою та залежати від фізичних перешкод.

В якості використання протоколів мережі, можна використати TCP/IP. Цей набір протоколів є основним стандартом для Інтернету і використовується для передачі даних в мережах. TCP/IP забезпечує надійну передачу даних шляхом розбиття їх на пакети і керування потоком даних між відправником і отримувачем.

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 мережі

Мережа банку повинна складатися з чотирьох логічно відокремлених сегментів. Кожний з цих сегментів повинен мати свою власну адресацію IP і використовуватися для підключення різних груп пристроїв та забезпечення відповідних функцій.

Кожному мережевому сегменту повинна відповідати певна кількість людей:

1. технічний контроль повинен мати 23 вузли;
2. користувацький інтернет повинен мати 47 вузлів;
3. системні адміністратори повинні мати 10 вузлів;
4. бухгалтери повинні мати 47 вузлів.

Головне завдання роботи мережі в банку полягає в забезпеченні безпечного, ефективного та надійного функціонування банківських операцій і послуг.

Мережа повинна передбачувати:

– обробку транзакції клієнтів;
– зберігання та управління інформацією про клієнтів;
– надання зв'язку між різними філіями та відділеннями банку.

Мережа банку повинна мати систему безпеки та сигналізації за технологіями сучасності інтернет речей IoT.

В компоненти інтернет речей повинно входити – вебкамери, освітлення, оптичні датчики, сирена, кнопка та програмуючий мікроконтролер SBC

2.1.1.1.2 Вимоги до способів і засобів зв’язку для обміну інформації між підмережами

Обмін інформацією між підмережами повинно виконуватися шляхом апаратного та програмного забезпечення.

Апаратне забезпечення повинно забезпечувати безперебійну роботу фізичних каналів та забезпечувати високу швидкість передачі даних. Фізичні канали повинні бути налаштовані за допомогою кабелю вита пара та оптоволокно.

Програмне забезпечення повинно забезпечувати логічну взаємодію фізичного рівня з запитами до мережі від співробітників.

2.1.1.1.3 Вимоги до характеристик взаємозв’язків створюваної мережі із суміжними мережами

Взаємозв’язок між суміжними мережами повинен забезпечуватися при умові, що мережа буде здатна передавати документи з високим рівнем надійності. Мережа банку повинна взаємодіяти з іншими фінансовими установами, такими як інвестиційні фонди, страхові компанії, пенсійні фонди та інші банки, при цьому мати список документів:

– фінансове становище організації;
– доходи, витрати і чистий прибуток;
– притоки і відтоки грошових коштів усередині організації;
– зміни в капіталі;
– звітність про оподаткування;
– фінансові прогнози та бюджети.

2.1.1.1.4 Вимоги до режимів функціонування мережі

Підрозділ технічного контролю повинен виконувати важливі функції щодо забезпечення відповідності поданих документів та інформації встановленим вимогам і правилам.

Підмережа користувацького інтернету повинна бути розрахована на точку доступу Wi-Fi, а саме для безкоштовного виходу в інтернет клієнтам та співробітникам.

Підрозділ системних адміністраторів повинен відповідати за управління, підтримку та забезпечення надійної роботи інформаційних систем і мережевої інфраструктури банку. Вони повинні виконувати низку завдання і обов'язки для забезпечення ефективного функціонування технологічного середовища банку.

Підрозділ бухгалтерів повинен відповідати за ведення фінансової звітності, обробку фінансової інформації та виконання інших завдань, пов'язаних із фінансовим обліком та аналізом.

2.1.1.1.5 Вимоги до діагностування мережі

Спеціалісти відділу системних адміністраторів банку повинні виконувати діагностику мережі.

Діагностика повинна відбуватися за допомогою програмного забезпечення та фізичного перегляду компонентів мережі. Діагностика повинна передбачувати тестування швидкості та стабільності з'єднання між різними вузлами мережі банку. Потрібно використовувати інструменти для вимірювання затримки, втрати пакетів і пропускної здатності.

2.1.1.1.6 Перспективи розвитку та модернізації мережі

Компанія банку має великі перспективи до розвитку мережевої інфраструктури в майбутньому. Цілі компанії - досягти високих потужностей своїх дата-центрів для відмови у послугах приватних компаній і самостійного регулювання обчислювальних ресурсів.

Створювана мережева інфраструктура повинна забезпечувати початкове налаштування серверів у дата-центрі, а також мати на перший час запас адрес для налаштування мережі.

Після налаштування корпоративної мережі ця інструкція з налаштування має послужити для майбутніх проектів банку.

2.1.1.2 Вимоги до показників призначення

Показники призначення банку повинні бути розраховані на:

– забезпечення ефективної комунікацію між різними відділами, філіями та співробітниками банку;

– здатність обробки великих обсягів фінансових транзакцій у режимі реального часу;

– вимоги віддаленого доступу до мережі;

– надійні та безпечні засоби для зберігання даних.

2.1.1.3 Вимоги до експлуатації

2.1.1.3.1 Умови і регламент експлуатації, що повинні забезпечувати використання технічних засобів мережі

Пристрої мережі, які використовуються в мережевій інфраструктурі, не потребують спеціальної підтримки або оточення для своєї нормальної роботи. Вони розроблені та спроектовані для роботи у звичайних робочих умовах.

2.1.1.3.2 Вимоги до параметрів мереж енергопостачання

Пристрої в мережі повинні функціонувати при стандартній напрузі в 220 Вольт змінного струму.

Пристрої в мережі мають бути належним чином заземлені для запобігання електричних розрядів і захисту від статичної електрики.

Банк має бути забезпечений генератором для забезпечення надійності та безпеки своєї операційної діяльності. Генератор є важливим джерелом електроенергії, яке забезпечує безперебійну роботу банківських систем і обладнання під час війни.

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

Співробітники банку, які працюють з комп'ютерами (ПК), повинні мати базову освіту та навички, що дають їм змогу ефективно використовувати комп'ютерні технології та програмне забезпечення.

Для роботи відділу адміністраторів мережі банку потрібна вища освіта і спеціалізація в галузі інформаційних технологій або комп'ютерних наук.

Графік роботи відділень банку:

1. Понеділок: 9:00 - 17:00;
2. Вівторок: 9:00 - 17:00;
3. Середа: 9:00 - 17:00;
4. Четвер: 9:00 - 17:00;
5. П'ятниця: 9:00 - 17:00;
6. Субота: 10:00 - 14:00.

У проектованій мережі необхідно мати команду з 28 осіб.

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

На складі мережевої інфраструктури банку повинні знаходитися такі резервні компоненти та обладнання:

– комутатори – 3шт.;
– маршрутизатори – 1шт.;
– бездротові точки доступу (Wi-Fi) – 1шт.;
– кабель вита пара – 100м;
– оптичний кабель – 50м;
– комп’ютери – 1шт.;
– клавіатура та миш – 3шт.

2.1.1.3.5 Вимоги до регламенту обслуговування мережі

У рамках регламенту обслуговування мережі банку повинен проводитися регулярний моніторинг стану мережі.

У регламенті повинно бути передбачено планове обслуговування та оновлення мережі та повинно включати розробку графіка планового обслуговування та проведення регулярних оновлень програмного та апаратного забезпечення мережевих пристроїв.

Регламент також повинен визначати процедури управління мережевими пристроями, включаючи конфігурування, встановлення та налаштування мережевого обладнання. Крім того, повинен забезпечує технічну підтримку користувачів щодо мережевих проблем та запитів.

Кожного понеділка адміністративний відділ повинен дотримуватися встановленого графіку регламентованих робіт:

– 9:00-10:00 – Перевірка доступності та оновлення програмного забезпечення на робочих станціях працівників;

– 10:00-11:00 – Резервне копіювання конфігураційних файлів маршрутизаторів;

– 11:00-12:00 – Перевірка пропускної здатності бездротових точок доступу та оптимізація налаштувань;

– 12:00-14:00 – Проведення аналізу мережевої активності для виявлення потенційних загроз безпеці;

– 15:00-17:00 – Перевірка та оновлення програмного забезпечення серверів.

2.1.1.4 Вимоги до патентної чистоти

Для забезпечення патентної чистоти, банк повинен виконувати такі кроки:

– повинен виконати детальний пошук та аналіз патентних баз даних, щоб переконатися, що використовувані ним технології та інновації не порушують чужих патентних прав;

– повинен перевірити, чи має він угоди про ліцензування з іншими суб'єктами інтелектуальної власності, які дозволяють йому використовувати патентовані технології або винаходи;

– повинен прийняти необхідні заходи для запобігання порушенню патентних прав інших осіб. Це може включати встановлення процедур внутрішнього контролю, навчання персоналу щодо патентної чистоти, а також залучення юридичних консультантів для порад і контролю за патентною ситуацією.

2.1.1.5 Додаткові вимоги

2.1.1.5.1 Вимоги до активного обладнання

Маршрутизатор повинен мати пропускну здатність не менше 1 Гбіт для забезпечення швидкого обміну даними між різними мережевими сегментами банку.

Комутатор повинен мати не менше 24 портів Ethernet для підключення різних пристроїв, таких як комп'ютери, сервери, принтери і т.д.

Комутатор повинен мати підтримку створення віртуальних мереж (VLAN) для сегментації мережі.

Обладнання повинно підтримувати основні мережеві протоколи, такі як TCP/IP, VLAN, OSPF, BGP, і можливість налаштування та розподіл IP-адрес для підключених пристроїв.

Обладнання повинно мати можливість централізованого управління і моніторингу, включаючи підтримку протоколів управління мережею.

2.1.1.5.2 Вимоги до кабель каналів, інформаційним та електричним розеткам

До організаційних вимог кабельних систем входять наступні пункти:

– категорія кабелю вита пара повинна забезпечувати швидкість передачі даних від 100Мбіт/с до 1Гбіт/с;

– довжина кабелю повинна забезпечувати підключення всього обладнання в мережі та мати запас на кожному кінці у 5м;

– кількість інформаційних розеток повинна бути встановлена до 20шт;

– тип інформаційних розеток повинен забезпечувати підключення RJ-45;

– кількість електричних розеток повинна бути встановлена до 50шт;

– тип електричних розеток повинен мат номінальну потужність 10А або 16А.

2.1.1.5.3 Вимоги до комунікаційного обладнання і його розташування

Комунікаційне обладнання банку повинно знаходитися в серверній кімнати, при цьому кімната повинна відповідати вимогам:

– рекомендована температура в приміщенні повинна бути в межах 20-24 градусів Цельсія;

– вологість повітря повинна знаходитися в межах 40-60%;

– щодо запобігання випадкового відключення серверів та збереження даних система повинна мати наявність резервного живлення – генератора;

– кімнати повинні бути обладнані системами вентиляції та охолодження, які забезпечать циркуляцію повітря та відведення тепла.

В пункті 2.1.1.3.2 були визначені вимоги щодо необхідності використання генератора.

2.1.1.5.4 Вимоги до однорідності

Мережа банку повинна застосовувати єдиний стандарт безпеки в усій мережі, а саме – протокол моделі доступу та управління.

Всі відділи компанії повинні мати резервне живлення від генератора.

2.1.2 Вимоги до задач, які виконуються у комп’ютерній системи

2.1.2.1 Вимоги до кожної підмережі та переліку їх функцій

Перед початком налаштування сегментів мережі, необхідно виконати початкове налаштування мережевого обладнання:

– ім’я обладнанню повинно надаватися за правилом – *Студента_Тип пристрою_Номер пристрою*, на прикладі – Kviatkovska_Switch_5;

– віртуальний термінал мережевого обладнання необхідно захистити паролем – cisco;

– мережеве обладнання повинно мати захист паролем *class* до режиму – enable mode;

– створені паролі для будь-яких систем повинні зберігатися у зашифрованому форматі;

– для відображення інформації при авторизації необхідно створити привітальний банер MOTD;

– всі віртуальні термінал від 0 до 4 повинні використовувати протокол безпечної оболонки SSH;

– мережеве обладнання повинно містити облікові записи адміністраторів мережі за структурою – Група_Прізвище, на прикладі – 12320zck_Kviatkovska, та використовувати пароль – admincisco;

– для забезпечення безпеки, імена доменів повинні використовувати імена мережевого обладнання. Для забезпечення захисту даних потрібно створити RSA-ключ розміром 1024 біти, який буде використовуватися для шифрування і розшифрування даних;

– DCE-інтерфейси мережевого обладнання повинні застосовувати тактову частоту у 128000;

– процес взаємодії віртуального терміналу повинен мати налаштування з нотифікації сповіщень про початок та кінець роботи, з використанням локальної бази.

Протокол маршрутизації повинен налаштовуватися відповідно до вказаних вимог:

– конфігурування прямо підключених мереж та відключення розсилки маршрутизаційних оновлень на інтерфейсах локальних мереж;

– сегментовані мережі повинні мати єдиний маршрут, та повинні бути оголошені всім маршрутизаторам в мережі;

– для використання протоколу маршрутизації OSPF потрібно змінити пропускну спроможність для розрахунку ваги за замовчуванням на Gigabit інтерфейсах на 1000;

– пропускна спроможність мережевого обладнання на serial портах повинна дорівнювати 128 Кб/с, розрахунок ваги 7500;

– маршрутизатор, який розташований на кордоні між мережами, повинен мати статичний маршрут за замовчуванням до мережі ISP або інтернет-провайдера, отриманий доступ у глобальну мережу, прикордонний маршрутизатор повинен розповсюджувати за протоколом маршрутизації;

– на отриманому маршруті необхідно налаштувати додавання маршруту вручну, так як протокол маршрутизації сумує тільки локальні мережі, та додати в таблицю приєднання мережі;

– в мережі LAN4 налаштувати статичний маршрут до мережі серверу AAA.

Мереже обладнання повинно мати захист та використовувати протокол AAA за наступними вимогами:

– для діагностики працездатності ліній віртуального термінала на маршрутизаторі необхідно створити локальну базу облікових записів співробітників адміністративного відділу;

– доступ до віртуального терміналу повинен отримуватися за допомогою протоколу RADIUS. При недоступності протоколу та перевірки з'єднання необхідно використовувати локальну базу облікових записів співробітників;

– протокол RADIUS повинен мати слово доступу з'єднання – radius123;

– база облікових записів співробітників повинна використовувати ім'я мережевого обладнання та пароль – *admin123*.

Прикордонний маршрутизатор мережі повинен мати одне підключення до інтернет-провайдера. Співробітники повинні отримувати доступ у мережу Інтернет за допомогою прикордонного маршрутизатора з налаштуванням протоколу NAT за наступними даними:

– ім'я пула: poolNAT;

– пул адресів: починаючи з 209.165.200.5 та закічнуючи 209.165.200.30;

– номер списку доступу повинен мати номер – 6.

Також, у ході налаштування повинен бути створений веб-сайт на сервері HTTP, та мати доменне ім’я http://123.dnipro.ua (http://209.165.200.4). Дані на веб-сайті повинні містити інформацію щодо кваліфікаційної роботи студента.

Розрахунок адресації мережевого обладнання та пристроїв повинен відповідати наступним вимогам:

– діапазон адрес повинен використовувати версію IPv4;

– маршрутизація мережевого обладнання повинна здійснюватися за мережею *10.0.№.0/24*, де *№ = 10*;

– необхідно врахувати кількість вузлів в кожній мережі;

– перші адреси з діапазону IP потрібно призначати мережевим інтерфейсам маршрутизаторів;

– другі адреси з діапазону IP потрібно призначати мережевим інтерфейсам комутаторів;

– треті адреси з діапазону IP потрібно призначати мережевим інтерфейсам серверів;

– останні адреси з діапазону IP потрібно призначати вузлам мережі;

– сегментовані мережі повинні використовувати протокол динамічного налаштування адрес DHCP.

2.1.3 Вимоги до видів забезпечення комп’ютерної системи

2.1.3.1 Вимоги до математичного забезпечення

У вимогах компанії до мережі передбачено проведення математичного розрахунку, що дозволить оцінити інтенсивність вихідного трафіку найбільшої локальної мережі компанії. Цей розрахунок відіграє важливу роль у визначенні потреб мережі, розмірів каналів зв'язку та загальної пропускної здатності.

Математичний розрахунок ґрунтується на аналізі обсягу даних, що передаються через мережу, та розрахунку середньої інтенсивності цього трафіку.

Для цього використовуються методи теорії черг, статистичного аналізу або спеціалізовані інструменти моделювання мережевого трафіку.

Результати розрахунку допоможуть визначити оптимальну пропускну здатність каналів зв'язку, розподілити трафік на мережевих пристроях та планувати майбутні розширення мережі.

2.1.3.2 Вимоги до інформаційного забезпечення

Інформаційне забезпечення мережі банку повинно містити:

– SolarWinds Network Performance Monitor, програмне забезпечення моніторингу мережі, яке надає детальну інформацію про стан мережевих пристроїв, пропускну здатність, завантаження та інші метрики продуктивності;

– IBM Security QRadar, програмне забезпечення системи інформаційної безпеки, яке забезпечує моніторинг, виявлення та реагування на потенційні загрози безпеки в мережі.

2.1.3.3 Вимоги до лінгвістичного забезпечення

До вимог лінгвістичного забезпечення мережі банку входять:

– необхідно щоб веб-сайт банку мав можливість відображати контент у різних мовах, таких як англійська, іспанська, французька тощо. Це повинно включати локалізацію і переклад інтерфейсу користувача, текстів, повідомлень про помилки та іншого вмісту, що відображається на веб-сайті;

– наявність системи або програмного забезпечення, яке може автоматично перекладати документи, такі як заявки на кредит, контракти або фінансові звіти, з однієї мови на іншу.

2.1.3.4 Вимоги до технічного забезпечення

Оптоволоконні кабелі повинні відповідати технічним вимогам:

– тип оптоволоконного кабелю повинен застосовуватися формату одномодового (OS2) та багатомодового (OM2, OM3, OM4);

– конектори повинні використовуватися такі як LC та SC, для з'єднання оптоволоконних кабелів;

– повинна застосовуватися максимальна довжина передачі оптоволоконного кабелю до 50м від мережевого обладнання мережі до мережевого обладнання інтернет-провайдера;

– повинні бути дотримані встановлені параметри загинів та радіусів кривизни оптоволоконних кабелів для забезпечення оптимальної передачі сигналу.

Комп'ютери співробітників мають відповідати звичайним вимогам до офісних комп'ютерів, та не потребують додаткових технічних вимог.

2.1.3.5 Вимоги до організаційного забезпечення

Мережа банку повинна підтримувати встановлені стандарти та процедури для різних операцій, включаючи відкриття рахунків, кредитування, обмін валют, зняття готівки та інші банківські операції.

Комунікація між співробітниками повинна забезпечуватися за допомогою електронної пошти, телефонної системи та системи відеоконференцій.

2.1.3.6 Вимоги до методичного забезпечення

Методичне забезпечення має містити в собі навчальні матеріали, такі як презентації та відеоуроки. Інформація повинна оновлюватися щонеділі. Також, співробітники повинні обов'язково ознайомитися з отриманою інформацією, для актуалізації знань з надання послуг банку.

2.2 Розробка апаратної частини мережі банку

2.2.1 Розробка структурної схеми комплексу технічних засобів комп’ютерної системи відповідно до заданої топології мережі

Для передачі даних між компонентами мережі використовується мережеве з'єднання. Для цього використовуються технології локальних мереж (LAN), глобальних мереж (WAN) та безпровідних мереж (Wi-Fi).

Для зберігання та організації отриманих даних використовуэться база даних на серверах компанії. Вона дозволяє ефективно зберігати, впорядковувати та отримувати доступ до великого обсягу інформації. Сервери отримують дані від пристроїв збору даних та виконують їх обробку і аналіз.

За пристрої збору даних відповідають комп'ютери, або інакше кажучи – кінцеві вузли мережі.

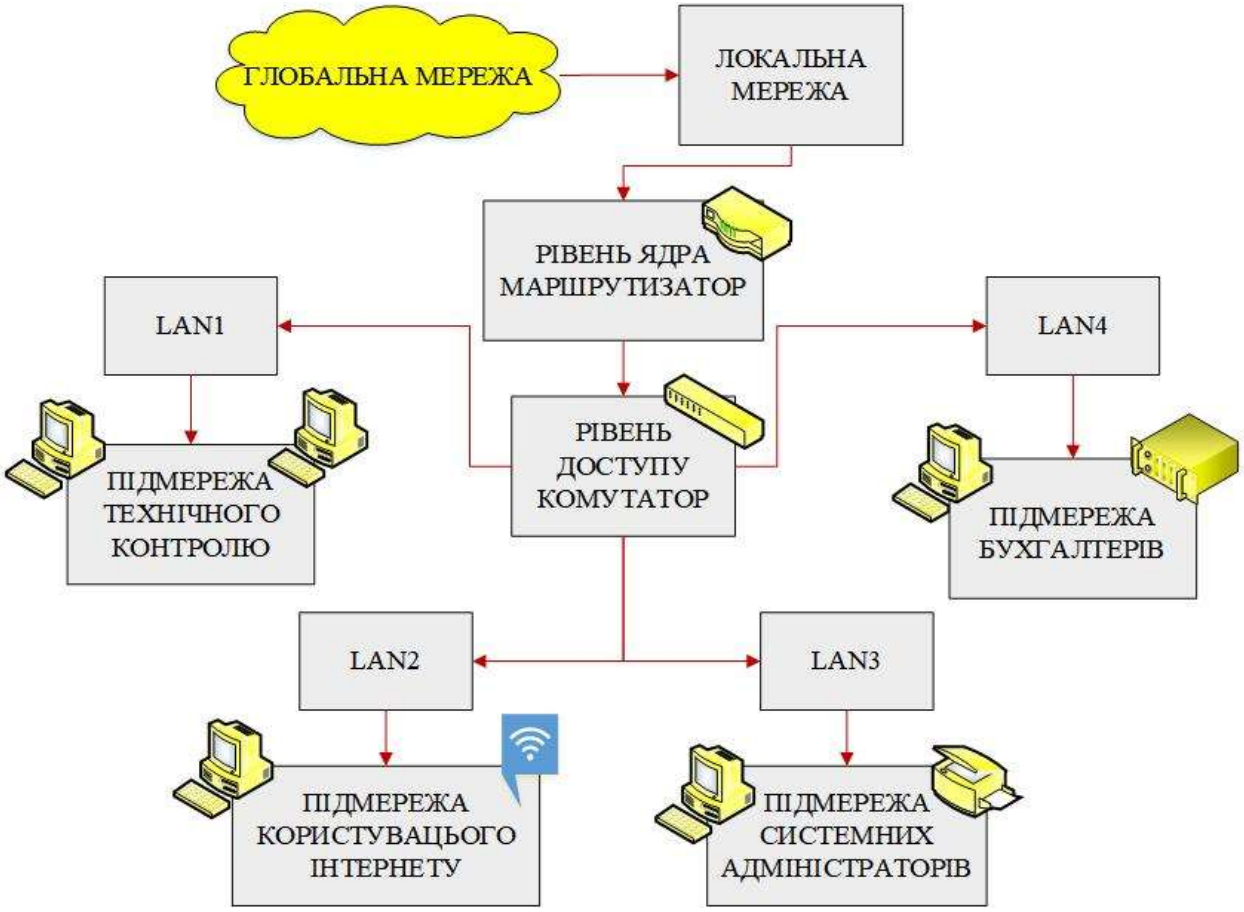

Рисунок 2.1 – Структурна схема комплексу технічних засобів

На схемі (рисунок 2.1) ми бачимо 4 LAN мережі які мають мережеві комутатори, які підключені між собою оптоволоконними кабелями. Кожен комутатор має свої входи та виходи, через які він з'єднаний з іншими комутаторами. Оптоволоконні кабелі забезпечують швидке та надійне передавання даних між комутаторами.

В свою чергу, мережа має маршрутизатори, які також підключені між собою оптоволоконними кабелями та об'єднують мережі комутаторів в єдиний сегмент мережі.

Окрім цього, на схемі відображені комп'ютери, принтери та сервери, підключені до окремих комутаторів використовуючи виту пару категорії Ethernet Cat5e.

Також, в мережі LAN2 існує маршрутизатор, який надає доступ до мережі за бездротовими лініями зв'язку Wi-Fi. Кількість кінцевих пристроїв завжди буде змінюватися, оскільки в кожен проміжок часу бездротовим інтернетом користуватиметься різна кількість людей.

2.2.2 Розробка специфікації апаратних засобів комп’ютерної мережі

Для проектування мережі та визначення необхідного технічного обладнання було розроблено таблицю 2.3, в якій вказані основні характеристики та вимоги до кожного пристрою.

У програмі Cisco Packet Tracer відображається технічне обладнання, що використовується в мережах.

Таблиця 2.1 – Специфікація технічного обладнання банку

№ в списку	Назва та технічна характеристика	Тип, марка, позначення	Одиниці виміру	Кількість	Позначення у додатку СРТ
1	Комутатор Швидкість передачі даних: 10/100/1000 Мбіт/с Кількість портів: 24 Тип портів: Ethernet Підтримка VLAN: до 255 віртуальних локальних мереж (VLAN) Підтримка керування швидкістю портів ідтримка стандартів Ethernet: IEEE 802.3, IEEE 802.3u, IEEE 802.3ab	Catalyst 2960	од.	7	Kviatkovska_Switch0 Kviatkovska_Switch1 Kviatkovska_Switch2 Kviatkovska_Switch3 Kviatkovska_Switch4 Kviatkovska_Switch5 Kviatkovska_Switch6

Продовження таблиці

2	Маршрутизатор Операційна система: Cisco IOS Процесор: 1.2 GHz одноядерний процесор Ethernet-інтерфейси: 2 x 10/100/1000 Gigabit Ethernet (RJ-45) 4 x 10/100 Fast Ethernet (RJ-45) Оперативна пам'ять (RAM): 512 МБ Мережеві протоколи: IPv4, IPv6, OSPF, BGP, RIP, EIGRP	Cisco 2911	од.	6	Kviatkovska_Router0 Kviatkovska_Router1 Kviatkovska_Router2 Kviatkovska_Router3 Kviatkovska_Router4 Kviatkovska_IPS
3	Wi-Fi маршрутизатор Стандарт бездротового зв'язку: IEEE 802.11n: До 300 Мбіт/с Ethernet-порти: 4 x 10/100 Fast Ethernet портів (RJ-45) USB-порт: 1 x USB 2.0 порт Бездротові протоколи: WEP, WPA, WPA2 Мережеві протоколи: IPv4, IPv6	Linksys WRT-300N	од.	1	Wireless Router0
4	Комп’ютери Intel Xeon E5-2670 2.6-3.3 GHz, 8 ядер ОЗП 16 Гб; E5-VG3 LGA2011 mATX SSD 240gb GeForce 210	Asus TRLineX	од.	28	PC_0-27

Кінець таблиці 2.1

5	Монітор діагональ екрану 21.5 дюймів максимальне розширення екрану 1920x1080 підтримка інтерфейсів VGA та HDMI.	Acer V226HQLGbi	од.	28	PC_0-27
6	Клавіатура Frime	Frime FKBS-002 USB	од.	28	PC_0-27
7	Миша W110	Gemix W110	од.	28	PC_0-27
8	Принтер Epson	Epson L132	од.	1	Printer_0

Для візуального представлення інформації розглянемо схеми розподілу обладнання. На схемах розподілу обладнання в мережі зображені всі пристрої та компоненти, які були в розроблені для конфігурування мережі банку.

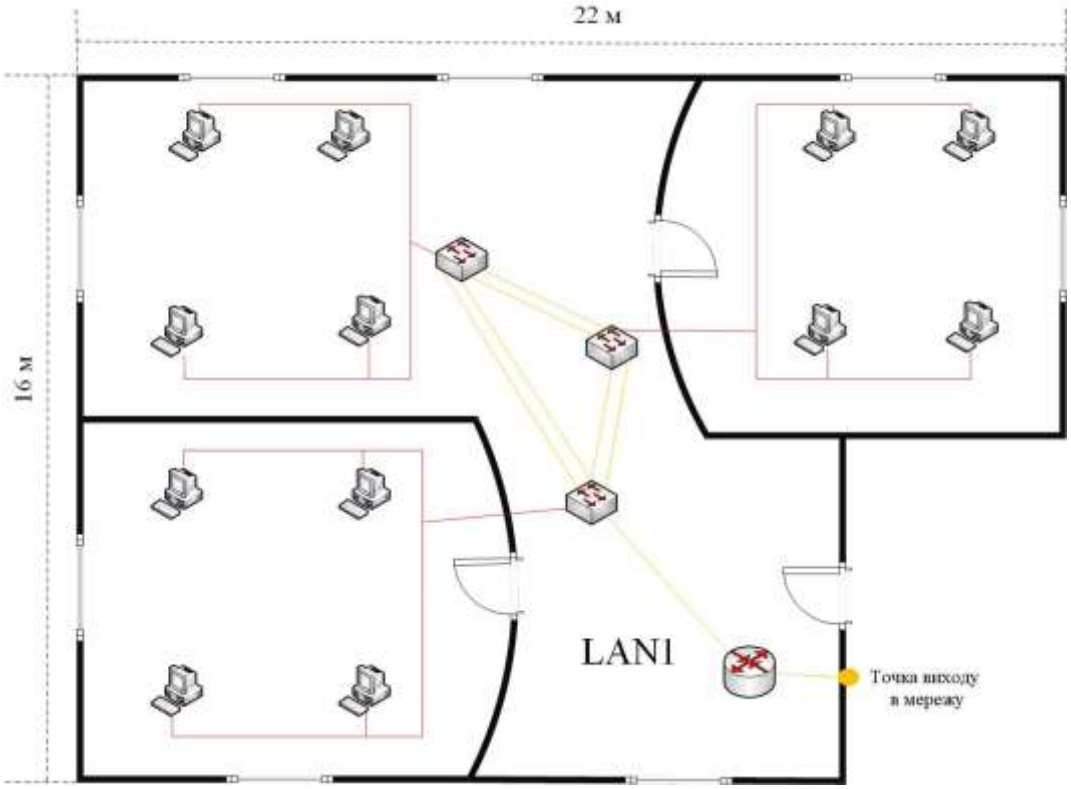

Рисунок 2.2 – Схема розподілу компонентів сегменту мережі LAN1

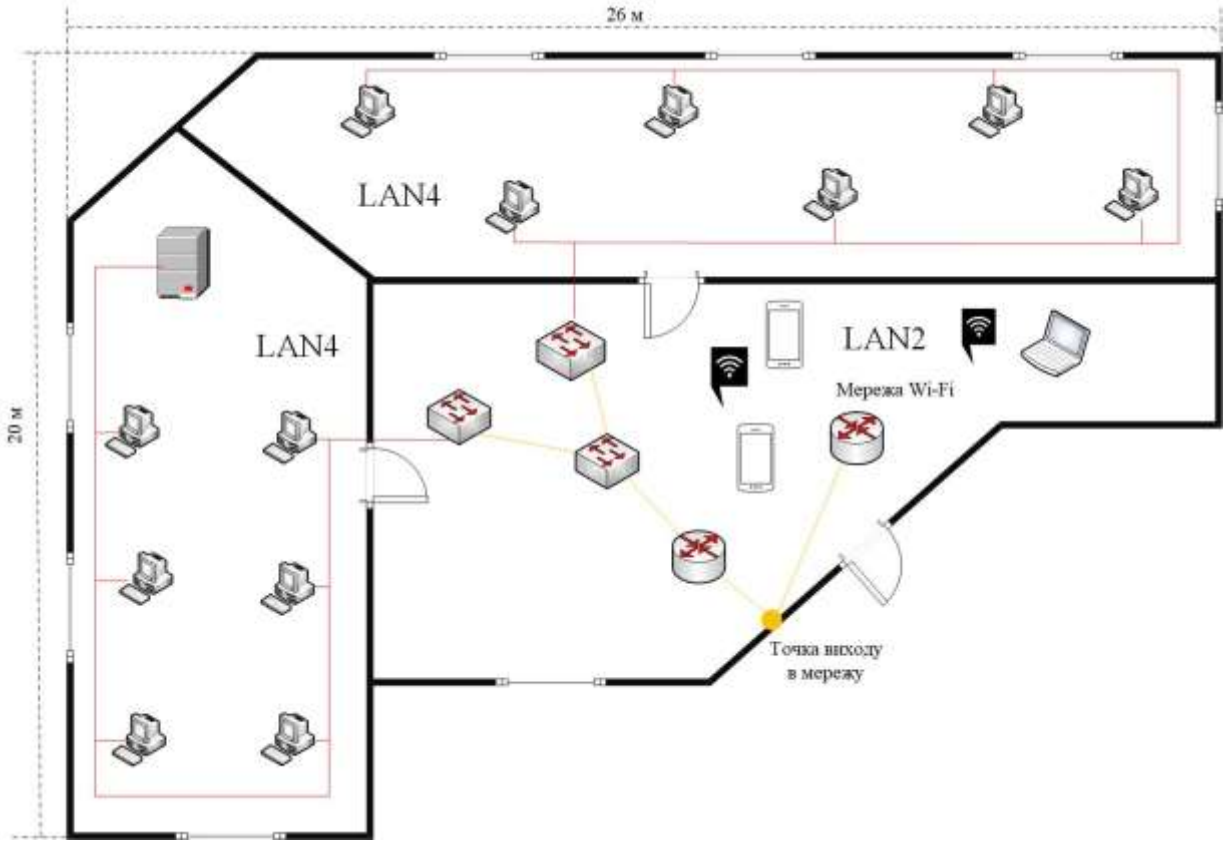

Рисунок 2.3 – Схема розподілу компонентів сегменту мережі LAN2 та LAN4

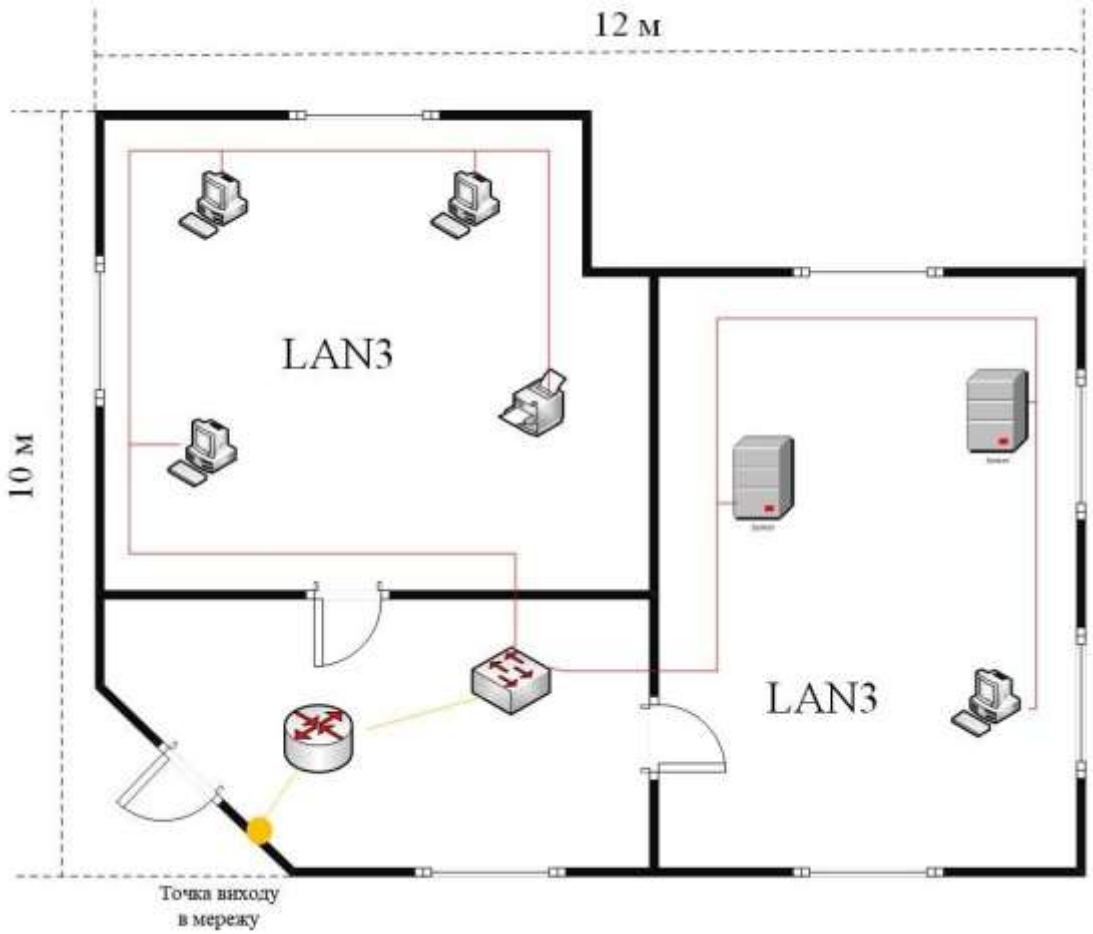

Рисунок 2.4 – Схема розподілу компонентів сегменту мережі LAN3

Для розуміння і опису властивостей та характеристик кожного компонента, які використовуються в мережі є необхідним створити таблицю технічного опису компонентів структурованих кабельних систем.

Цей опис допоможе забезпечити правильне планування, розгортання та управління мережею з високоякісною передачею даних.

Таблиця 2.2 – Технічний опис компонентів структурованих кабельних систем

№ в списку	Назва та технічна характеристика	Тип, марка, позначення	Одиниці виміру	Кількість
1	Кабельний канал Розмір: 40 мм х 40 мм Довжина одиниці: 2м	КАМа	од	90
2	Кабель-органайзер Розмір: 1 юніт стійки	Hypernet CM-5P	од	3
3	Інформаційна розетка Інтерфейс: RJ-45 UTP cat5e	Asfora	од	18
4	Кабель вита пара Тип: UTP cat5e	Dialan	м	250
5	Конектор витої пари Тип: RJ-45	W&T	од	50
6	Стійка Розмір: 8 юнітів Монтаж: на стіні	CSV CSV-8U 400	од	3
7	Оптоволоконний кабель Тип: SC	Dialan	м	70
8	Конектор оптоволокна Тип: SC	W&T	м	35

2.2.3 Розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі підприємства банку

Суттєвої частиною кваліфікаційної роботи є виконання розрахунку інтенсивності вихідного трафіку. Розрахунок вважається дійсним, якщо будуть використані значення пікового навантаження мережі банку та всі співробітники одночасно почнуть користуватися мережею.

При найбільшій кількості вузлів в мережі – 47 та середньому розмірі даних у 650 байт, необхідно застосувати показник інтенсивності трафіку у 216 кадрів/секунду. При цьому, час передачі пакетів не повинен перевищувати 6 мс.

Вихідний трафік з мережі на маршрутизатор не повинен перевищувати 1000 Мбіт/с.

Розрахуємо пропускна здатність мережі на рівні комутаторів:

$$Рр.д= \mu*l*n*8=216*650*24*8= 26,95 \text{ Мбіт/с}, \quad (2.1)$$

де n – кількість портів на комутаторі.

Розрахуємо пропускну здатність мережі на маршрутизаторах:

$$Рр.р = \mu * l * N *8 = 216*650*47*8= 527,90 \text{ Мбіт/с}, \quad (2.2)$$

де N – кількість вузлів в найбільшій мережі.

Швидкість передачі даних на рівні маршрутизаторів не перевищує значення у 1000 Мбіт/с, тому обладнання не буде перенавантажене.

Балансувальник навантаження перенаправляє трафік до маршрутизатора через вихідну лінію з пропускною здатністю 1000 Мбіт / с.

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

Розрахуємо максимальну кількість можливих вузлів в мережі на рівні комутаторів при тому, що кожне джерело виробляє 216 пакетів на секунду

$$N = 192\,310 / 216 = 890 \text{ джерел}. \quad (2.4)$$

Отже, 47 вузлів входять в отримане значення.

Кожен з 47 ПК відправляє інформацію з інтенсивністю 216 кадрів/с, тому розрахуємо інтенсивність вихідного трафіку від всіх користувачів підмережі:

$$\lambda = N * \mu = 47 * 216 = 10152 \text{ (пакетів/с)}. \quad (2.5)$$

Розрахуємо коефіцієнт затримки на рівні маршрутизатора, показник навантаження поділимо на вихідний канал зв'язку та отримаємо затримку черги:

$$\rho = \lambda / \mu_{вих} = 10152 / 192\,310 = 0{,}052 \quad (2.6)$$

Коефіцієнт завантаженості комутатора рівня розподілу:

$$r = \rho / (1 - \rho) = 0{,}052 / (1 - 0{,}052) = 0{,}0548 \quad (2.7)$$

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

$$T = 1/((\mu-\lambda)) = 1/(192\,310-10152) = 5{,}489 \text{ мкс} \quad (2.8)$$

Середня довжина черги:

$$L_{чер} = \rho^2/(1-\rho) = (0{,}052)^2/(1-0{,}052) = 0{,}00285 \quad (2.9)$$

Середній час пакетів у черзі:

$$T_{оч} = L_{чер}/\lambda = 0{,}00285/10152 = 2{,}8 \text{ мс} \quad (2.10)$$

Отримане значення менше ніж 6мс, тому вимоги розрахунку задовільні.

Пропускна здатність каналу:

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

$$b = \lambda * l = 10152 * 650 * 8 = 52\,790\,400 \text{біт/с} = 52{,}79 \text{ Мбіт/с} \quad (2.11)$$

Середнє значення пропускної спроможності підмережі не перевищує 1000 Мбіт/с, що задовольняє розрахунок в цілому.

3 РОЗРОБКА КОМПЮ’ТЕРНОЇ МЕРЕЖІ З РОЗРАХУНКОМ НАЛАШТУВАНЬ

3.1 Розрахунок адресації для підмереж

За завданням до кваліфікаційної роботи був використаний адресний простір 192.168.10.0/24 – для локальних мереж, та 10.0.10.0/24 – для глобальних мереж.

Мережа складається з 254 вільних IP-адрес, та має діапазоні адрес від 192.168.10.1 до 192.168.10.254.

Таблиця 3.1 – Загальна кількість хостів кожного сегменту мережі

Задана адреса	LAN1	LAN2	LAN3	LAN4	Загалом
192.168.10.0/24	23	47	10	47	127

IP-адреса – це унікальна послідовність цифр, що присвоюється пристрою під час під'єднання до мережі на основі протоколів TCP/IP.

IP-адреса – це послідовність із чотирьох цифр, розділених крапками, наприклад 192.168.10.33, яка використовується для ідентифікації та зв'язку з учасниками мережі. Простіше кажучи, IP-адреса – це певна послідовність цифр, привласнена конкретному пристрою в Інтернеті або локальній мережі (LAN), щоб інші пристрої в цій мережі могли його розпізнати та ідентифікувати.

Запис IP-адреси здійснюється у форматі '0.0.0.0', де кожне з чотирьох чисел повинно бути значенням від 0 до 255, тобто '255.255.255.255' – це максимально можлива послідовність. Крім десяткової нотації, для реєстрації IP можна використовувати і двійкову нотацію. У цьому випадку діапазон значень буде від 00000000 до 11111111.

Для розподілення IP-адреси на логічні сегменти використовується маска підмережі, яка дозволяє здійснювати адресацію та маршрутизацію в мережах Інтернету,. Вона також використовується для обчислення діапазону доступних IP-адрес у певній мережі або підмережі.

Наприклад, якщо маска підмережі складається з перших 24 бітів, це означає, що перші 24 біти IP-адреси використовуються для ідентифікації мережі чи підмережі, а останні 8 бітів - для ідентифікації конкретного пристрою.

Таблиця 3.2 – Внутрішня адресація сегментів мережі

Номер мережі	Кількість вузлів	Адреса підмережі	Маска підмережі	Перша адреса	Остання адреса
LAN1	23	192.168.10.128	255.255.255.224	192.168.10.129	192.168.10.158
LAN2	47	192.168.10.0	255.255.255.192	192.168.10.1	192.168.10.62
LAN3	10	192.168.10.64	255.255.255.192	192.168.10.65	192.168.10.126
LAN4	47	192.168.10.160	255.255.255.240	192.168.10.161	192.168.10.174

Для розбиття мережі 10.0.10.0/24 на 5 необхідних підмереж, необідно створити пули з маскою /30.

Маска /30 використовує 30 бітів, з яких 2 біти будуть використовуватися для ідентифікації мережі, а решта 2 біти залишаються для ідентифікації конкретних пристроїв у підмережі.

Отже, ми можемо виділити 2^2 = 4 підмережі з маскою /30, кожна з яких буде мати 2 доступних IP-адреси: одну для мережі та одну для широкомовного адресу.

Для підключення прикордонного маршрутизатора с інтернет-провайдером необхідно використовувати адреси: 209.165.202.1 та 209.165.202.2 з маскою /30.

Віддалена мережа повинна використовувати адреси: 64.100.13.1 та 64.100.13.2 з маскою /30.

Таблиця 3.3 – Зовнішня адресація сегментів мережі

Номер мережі	Кількість вузлів	Адреса підмережі	Маска підмережі	Перша адреса	Остання адреса
WAN1	2	10.0.10.0	255.255.255.252	10.0.10.1	10.0.10.2
WAN2	2	10.0.10.4	255.255.255.252	10.0.10.5	10.0.10.6
WAN3	2	10.0.10.8	255.255.255.252	10.0.10.9	10.0.10.10
WAN4	2	10.0.10.12	255.255.255.252	10.0.10.13	10.0.10.14
WAN5	2	10.0.10.16	255.255.255.252	10.0.10.17	10.0.10.18
WAN IPS	2	209.165.202.0	255.255.255.252	209.165.202.1	209.165.202.1
WAN–R0	2	64.100.13.0	255.255.255.252	64.100.13.1	64.100.13.2

3.2 Розрахунок адресації для пристроїв в мережі

На принципах побудови та розрахунку таблиці 3.1 та таблиці 3.2 створимо таблицю адресацію пристроїв в кожному сегменті мережі відповідно до зазначених діапазонів мереж.

Таблиця 3.3 – Адресація пристроїв кожного сегменту мережі

Назва пристрою	Мережевий інтерфейс	IP-адреса	Маска	Шлюз	VLAN	Інтерфейс пристрою
Мережа IPS						
Kviatkovska_IPS	S0/3/0	209.165.202.2	/30	–	–	S0/3/0
	G0/0	64.100.13.2	/30	–	–	G0/0
	G0/1	209.165.201.1	/28	–	–	G0/1
Kviatkovska_Router3	S0/2/0	10.0.10.1	/30	–	–	S0/2/0
	S0/3/0	209.165.202.1	/30	–	–	S0/3/0
	S0/3/1	10.0.10.5	/30	–	–	S0/3/1
Server_AAA	Fa0	209.165.201.5	/28	–	–	Fa0
Мережа технічного контролю						
Kviatkovska_Router0	G0/0	64.100.13.1	/30	–	–	G0/0
	G0/1	192.168.10.129	/27	–	–	G0/1
Kviatkovska_Switch4	Vlan1	192.168.10.130	/27	192.168.10.129	–	Fa0/1-0/4
Kviatkovska_Switch5	Vlan1	192.168.10.131	/27	192.168.10.129	–	Fa0/1-0/4
Kviatkovska_Switch6	Vlan1	192.168.10.132	/27	192.168.10.129	–	Fa0/1-0/4
PC_17-20	NIC	192.168.10.18-192.168.10.19	/27	192.168.10.129	–	Fa0/5-0/8_sw4
PC_21-24	NIC	192.168.10.34-192.168.10.35	/27	192.168.10.129	–	Fa0/5-0/8_sw5
PC_25-28	NIC	192.168.10.50-192.168.10.51	/27	192.168.10.129	–	Fa0/5-0/8_sw6

Кінець таблиці 3.3

Мережа користувацього інтернету						
Kviatkovska_Router1	S0/3/0	10.0.10.13	/30	–	–	S0/3/0
	S0/3/1	10.0.10.17	/30	–	–	S0/3/1
	G0/0	10.0.10.1	/30	–	–	G0/0
	G0/1	192.168.10.1	/26	–	–	G0/1
Wireless Router0	LAN	192.168.10.2	/26	192.168.10.1	–	LAN
Smartphone0	NIC	192.168.10.4-192.168.10.5	/26	192.168.10.2	–	Wi-Fi
Laptop0	NIC	192.168.10.6	/26	192.168.10.2	–	Wi-Fi
Мережа системних адміністраторів						
Kviatkovska_Router4	G0/0	10.0.10.9	/30	–	–	G0/0
	G0/1	192.168.10.161	/28	–	–	G0/1
	S0/3/1	10.0.10.6	/30	–	–	S0/3/1
Kviatkovska_Switch3	Vlan1	192.168.10.164	/28	192.168.10.161	–	G0/1
PC1-4	NIC	192.168.10.165 192.168.10.168	/28	192.168.10.161	–	Fa0/1-4
Printer1	NIC	192.168.13.70	/28	192.168.10.161	–	Fa0/5
Server DNS	NIC	192.168.10.162	/28	192.168.10.161	–	Fa0/6
Server HTTP	NIC	192.168.10.163	/28	192.168.10.161	–	Fa0/7
Мережа бухгалтерів						
Kviatkovska_Router2	G0/0	192.168.10.65	/28	–	–	G0/0
	S0/2/0	10.0.10.2	/30	–	–	S0/2/0
	S0/3/0	10.0.10.14	/30	–	–	S0/3/0
	S0/3/1	10.0.10.18	/30	–	–	S0/3/1
PC16_9-12	NIC	192.168.10.82-192.168.10.85	/28	192.168.10.81	19	Fa0/5-0/9
PC26_7,8,13,14	NIC	192.168.10.98-192.168.10.101	/28	192.168.10.97	29	Fa0/10-0/14
PC36_5,6,15,16	NIC	192.168.10.114 192.168.10.117	/28	192.168.10.113	39	Fa0/15-0/24
Server_TFTP_16	NIC	192.168.10.86	/28	192.168.10.81	-	Fa0/1

3.3 Розробка та моделювання топологічної схеми мережі банку

Розробка топологічної схеми надає розуміння які компоненти мережі (сервери, комутатори, маршрутизатори) будуть використовуватись та як вони будуть пов'язані між собою.

Цей крок включає визначення логічного розташування пристроїв у відділеннях банку.

Топологічна схема мережі банку, створена на базі топології "дерево", передбачає ієрархічну організацію мережі з головним комутатором або маршрутизатором, від якого виходять гілки до підключених відділень та підмереж.

У такій схемі, головний комутатор або маршрутизатор знаходиться в центрі мережі, і він виконує функцію централізованого вузла для обміну даними між всіма підмережами та відділеннями банку. Він також відповідає за маршрутизацію трафіку між підмережами та зовнішніми мережами.

Кожне відділення або підмережа підключається до головного комутатора або маршрутизатора через свій власний комутатор або маршрутизатор.

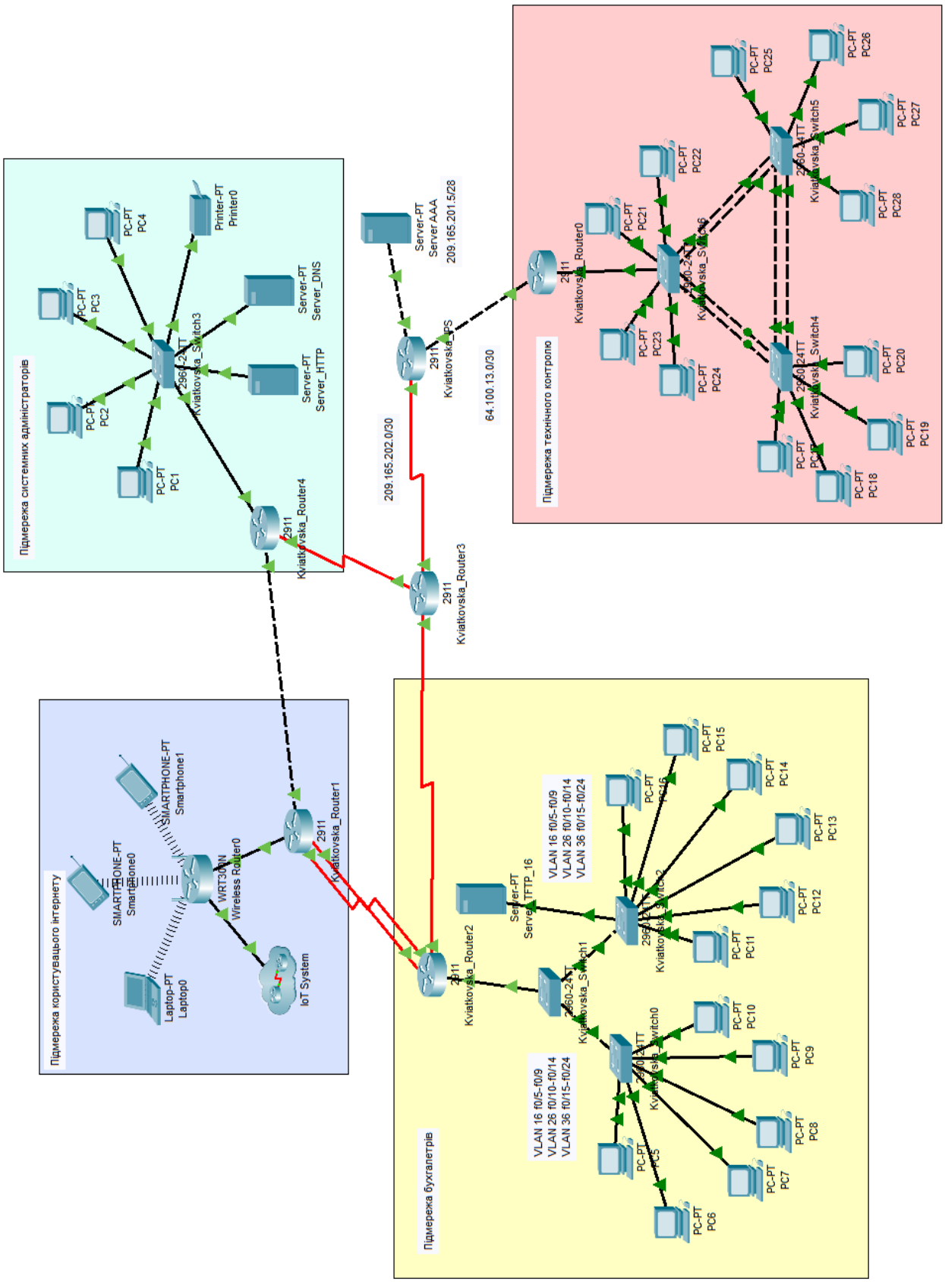

Рисунок 3.1 – Топологічна схема підприємства АТ «Універсал Банк»

3.4 Налаштування мережевих комунікацій та перевірка роботи застосувань в мережі

3.4.1 Базове налаштування конфігураційних файлів пристроїв в мережі

Налаштування мережі передбачає налагодження роботи протоколів та технологій за різними напрямами. Щоб виконати налаштування протоколів, потрібно здійснити базове налаштування пристроїв за замовчуванням на всьому мережевому обладнанні мережі.

Для прикладу візьмемо маршрутизатор Kviatkovska_Router3 та налаштуємо його:

en // входимо до EXEC режиму

conft t // входимо до терміналу конфігурування

hostname Kviatkovska_Router3 // назначимо назву маршрутизатора

enable secret class // задаємо пароль до EXEC режиму

line console 0 // входимо до консолі 0

password cisco // задаємо пароль

login // вказуємо функцію авторизації

banner motd #123-20zck Kviatkovska authorization PASSWORD# // задаємо стандартний банер за вимогами

username 12320zck_Kviatkovska password cisco // створюємо користувача

service password-encryption // вказуємо функцію шифрування паролів

ip domain-name Kviatkovska_Router3 // для домену використовуємо назву маршрутизатора

crypto key generate rsa // робимо генерацію ключа

How many bits in the modulus [512]: // система запитує в якому обсязі потрібно створити ключ, за стандартом пропонує 512

1024 // вписуємо значення 1024 відповідно до вимог

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK] // ключ згенеровано

line vty 0 4 // входимо до консолей від 0 до 4

login local // використовуємо авторизацію за створеними даними користувача

transport input ssh // задаємо використання протоколу віддаленого доступу

3.4.2 Налаштування мережевих конфігурацій маршрутизаторів

Налаштуємо маршрутизатор бездротового зв’язку корпоративної мережі.

Бездротовий зв’язок (Wi-Fi) – це технологія передавання даних бездротовим каналом, іншими словами, це локальна мережа, яка складається з пристроїв, під'єднаних за бездротовою технологією.

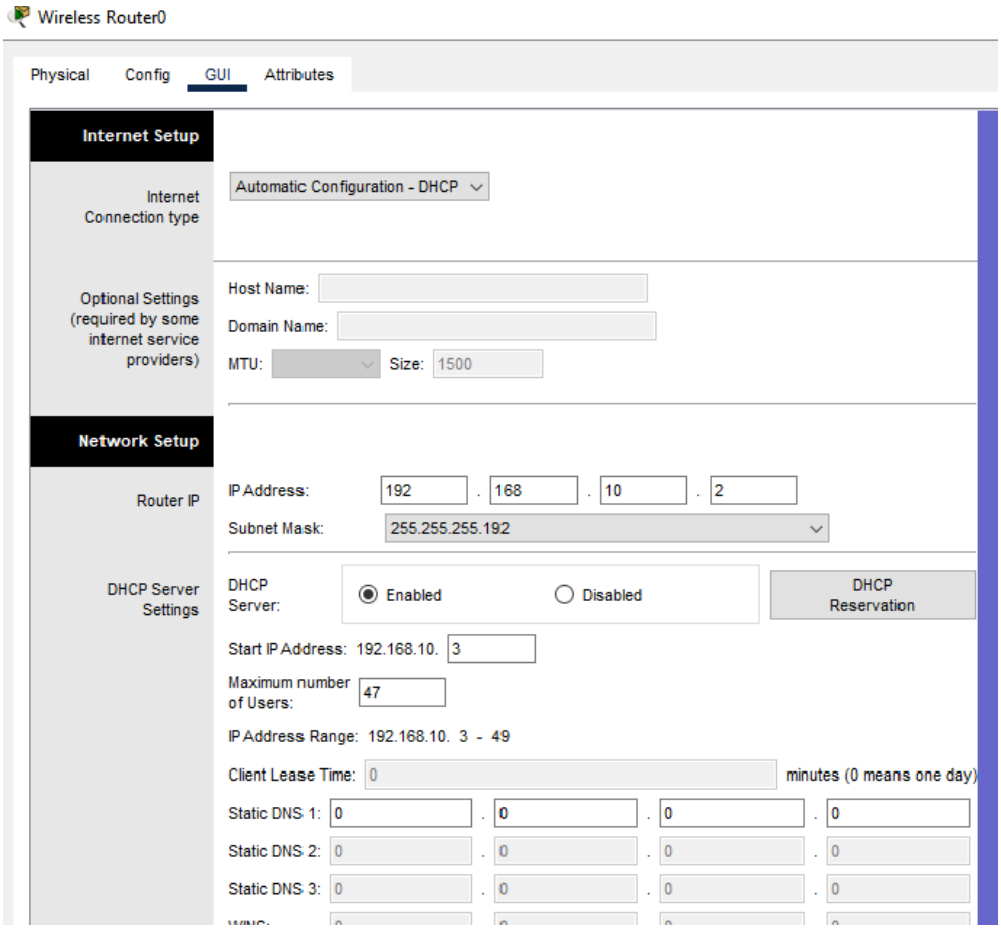

Рисунок 3.2 – Вигляд налаштування мережі Wi-Fi

Спочатку це абсолюнто локальна мережа, але після підключення до маршрутизатора інтернету дана мережа має вихід у загальний доступ.

Підмережа LAN2 повинна мати таку технологію, для цього виконаємо налаштування на маршрутизаторі Wireless Router0.

Для початку потрібно вказати діапазон допустимих IP-адрес, які будуть використовуватися для пристроїв мережі. За вимогами проекту підмережа повинна обслуговувати 47 користувачів. Адресний простір будемо використовувати 192.168.10.3-192.168.10.49.

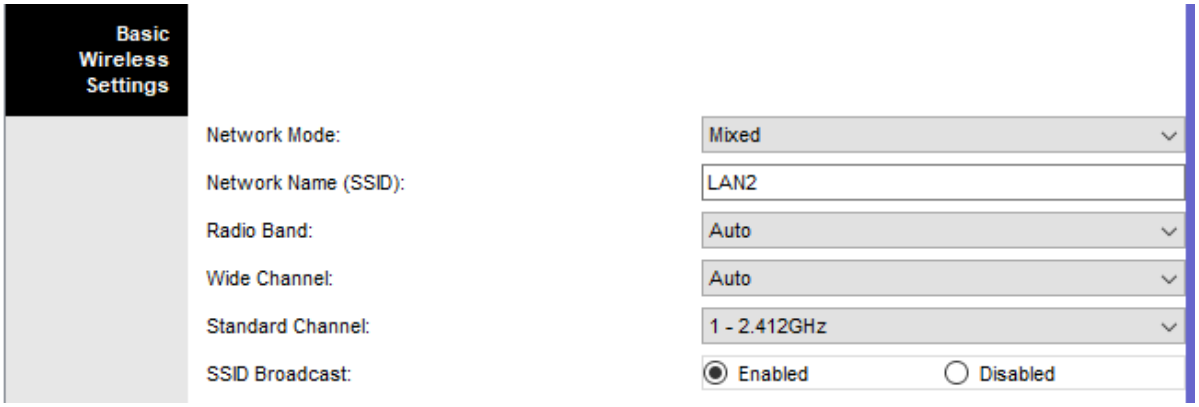

Рисунок 3.3 – Вигляд базового налаштування Wi-Fi

В базових налаштуваннях маршрутизатора назначимо ім’я мережі.

Рисунок 3.4 – Вигляд налаштування безпеки Wi-Fi

В налаштуваннях безпеки мережі Wi-Fi вибираємо режим роботи безпеки та вказуємо пароль мережі.

Після заданих налаштувань мережа має захист – паролем, та виконує всі вимоги до чисельності IP-адрес мережі.

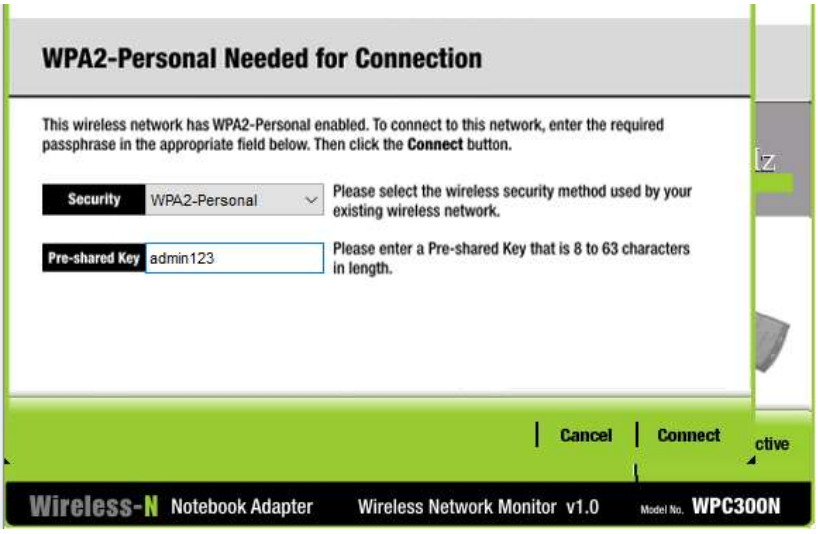

Рисунок 3.5 – Підключення ноутбуку к мережі Wi-Fi

Мережа з’явилась в загальному доступі, після цього виконали підключення за паролем

Налаштуємо протокол динамічної видачі налаштувань для мережевих інтерфейсів, а саме DHCP.

ip dhcp pool LAN1 // створюємо та вказуємо назву пулу

network 192.168.10.128 255.255.255.224 // вказуємо мережу та маску пулу

default-router 192.168.10.129 // вказуємо шлюз мережі

dns-server 192.168.10.162 // вказуємо dns сервер мережі

Після цього на пристроях мережі необхідно включити можливість отримання налаштувань за протоколом DHCP.

Налаштуємо маршрутизацію мережі на прикладі маршрутизатора Kviatkovska_R1:

router ospf 1 // вмикаємо протокол маршрутизації

network 192.168.10.0 0.0.0.63 area 0 // оголошуємо мережу *192.168.10.0*

network 10.0.10.8 0.0.0.3 area 0 // оголошуємо мережу 10.0.10.8

network 10.0.10.12 0.0.0.3 area 0 // оголошуємо мережу 10.0.10.12

network 10.0.10.16 0.0.0.3 area 0 // оголошуємо мережу 10.0.10.16

ip route 0.0.0.0 0.0.0.0 209.165.201.1 // вказуємо маршрут за замовчуванням до прикордонного маршрутизатора, який підключено до інтернет-провайдера

На прикладі маршрутизатора Kviatkovska_R3 налаштуємо порти, відповідно до вимог:

interface s0/3/0 // заходимо до налаштувань інтерфейсу

bandwidth 128 // встановлюємо значення пропускної здатності

clock rate 128000 // встановлюємо значення швидкості передачі даних

ip ospf cost 7500 // встановлюємо значення вартості маршруту

За поставленими завданнями налаштуємо роботу сегментованих мереж технологій VLAN.

Технології сегментації мережі підвищують рівень безпеки в мережі та розподіляють загальну мережу на частини.

Таблиця 3.4 – Таблиця сегментованих мереж

№ мережі	Назва мережі	Порти комутатора
16	team1	f0/5-f0/9
26	team 2	f0/10-f0/14
36	team 3	f0/15-f0/24

Налаштуємо мережеві інтерфейси на маршрутизаторі:

int gi0/0.16 // створюємо підінтерфейс для сегментованої мережі 16

encapsulation dot1Q 16 // налаштовуємо маркування на підінтерфейсі

ip address 192.168.10.81 255.255.255.240 // вказуємо адресу шлюзу мережі та маску

int gi0/0.26

encapsulation dot1Q 26

ip address 192.168.10.97 255.255.255.240

int gi0/0.36

encapsulation dot1Q 36

ip address 192.168.10.113 255.255.255.240

do wr // зберігаємо налаштування

Далі, створимо пул адресів за протоколом DHCP:

ip dhcp pool Vlan16 // створюємо пул під певний сегмент мережі

network 192.168.10.80 255.255.255.240 // вказуємо мережу та маску

default-router 192.168.10.81 // вказуємо раніше визначений шлюз

dns-server 192.168.10.162 // вказуємо dns сервер мережі

ip dhcp pool Vlan26

network 192.168.10.96 255.255.255.240

default-router 192.168.10.97

dns-server 192.168.10.162

ip dhcp pool Vlan36

network 192.168.10.112 255.255.255.240

default-router 192.168.10.113

dns-server 192.168.10.162

На основі налаштувань отримуємо адресацію сегментованих мереж банку у вигляді таблиці 3.5.

Таблиця 3.5 – Адресація сегментованих мереж банку

Номер мережі	Кількість вузлів	Адреса підмережі	Маска підмережі	Перша адреса	Остання адреса
VLAN16	4	192.168.10.80	255.255.255.240	192.168.10.81	192.168.10.94
VLAN26	4	192.168.10.96	255.255.255.240	192.168.10.97	192.168.10.110
VLAN36	5	192.168.10.112	255.255.255.240	192.168.10.113	192.168.10.126

Налаштуємо сегментовані мережі на комутаторах:

vlan 16 // створюємо сегментовану мережу

name team1 // надаємо їй ім’я

vlan 26

name team2

vlan 36

name team3

interface g0/1

switchport trunk allowed vlan 16,26,36 // визначаємо список дозволених мереж на транк-порту комутатора

switchport mode trunk // включаємо режим транк

interface range f0/5-9

switchport mode access // порт комутатора переводимо в режим access, трафік по ньому буде йти лише за заданою сегментованою мережею

switchport access vlan 16 // задаємо значення мережі

interface range f0/10-14

switchport mode access

switchport access vlan 26

interface range f0/15-24

switchport mode access

switchport access vlan 36

3.4.3 Налаштування взаємозв'язку з глобальною мережею

Між прикордонним маршрутизатором та маршрутизатором інтерне-провайдера налаштуємо протокол маскування IP-адрес NAT.

За його допомогою локальні адреси будуть маскуватися в глобальній мережі, та будуть використовувати заданий діапазон адрес, і навпаки, люди в глобальній мережі не будуть бачити локальну адресу користувача, а лише адресу глобального використання.

Налаштуємо протокол на прикладі маршрутизатора Kviatkovska_Router3

access-list 6 permit 192.168.10.0 0.0.0.255 // створюємо лист доступу з інформацією використання протоколу мережі *192.168.10.0*

ip nat pool poolNAT 209.165.200.5 209.165.200.30 netmask 255.255.255.224 // використання заданого пулу адрес за завданням

ip nat inside source list 6 interface s0/3/0 // підключення створеного списку доступу до порту маршрутизатора

interface Serial0/3/0

ip nat outside // вказуємо роботу інтерфейсу в режимі *outside*

interface Serial0/3/1

ip nat inside вказуємо роботу інтерфейсу в режимі *inside*

interface Serial0/2/0

ip nat inside вказуємо роботу інтерфейсу в режимі *inside*

Після налаштування можна отримати доступ в глобальну мережу та отримувати будь-яку інформацію.

В консолі маршрутизатора ми бачимо налаштування портів та трафік, який здійснюють вузли в мережі (рисунок 3.6).

```
Kviatkovska_Router3#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/3/0
Inside Interfaces: Serial0/2/0 , Serial0/3/1
Hits: 0  Misses: 0
Expired translations: 0
Dynamic mappings:
Kviatkovska_Router3#show ip nat t
Kviatkovska_Router3#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.202.1:3   192.168.10.82:3    192.168.10.130:3   192.168.10.130:3
icmp 209.165.202.1:4   192.168.10.82:4    192.168.10.130:4   192.168.10.130:4
icmp 209.165.202.1:5   192.168.10.82:5    192.168.10.130:5   192.168.10.130:5
icmp 209.165.202.1:6   192.168.10.82:6    192.168.10.130:6   192.168.10.130:6
icmp 209.165.202.1:7   192.168.10.82:7    192.168.10.130:7   192.168.10.130:7
icmp 209.165.202.1:8   192.168.10.82:8    192.168.10.130:8   192.168.10.130:8
```

Рисунок 3.6 – Робота протоколу маскування IP-адрес

3.4.4 Система захисту мережевої інфраструктури від різних загроз

Для управління захистом в мережі налаштуємо мережеві списки дозволених операцій ACL.

Сегментована мережа 16 не повинна мати взаємозв’язок з мережами 26 та 36. Тоді, мережа 26 не повинна мати взаємозв’язок з мережею 16, але повинна мати з 36. Мережа 36 повинна мати відповідні налаштування.

Налаштуємо списки:

ip access-list extended 6 // створюємо списки

deny ip 192.168.10.80 0.0.0.15 192.168.10.96 0.0.0.15 // забороняємо мережі *192.168.10.80* взаємодіяти з мережею *192.168.10.96*

deny ip 192.168.10.96 0.0.0.15 192.168.10.80 0.0.0.15

deny ip 192.168.10.80 0.0.0.15 192.168.10.112 0.0.0.15

deny ip 192.168.10.112 0.0.0.15 192.168.10.80 0.0.0.15

permit ip any any // останні мережі мають повні права доступу

interface gigabitEthernet 0/0.16

ip access-group 6 in // на кожному підінтерфейсі підключаємо створений список

interface gigabitEthernet 0/0.26

ip access-group 6 in

interface gigabitEthernet 0/0.36

ip access-group 6 in

Для резервування передачі інформацію налаштуємо паралельне з'єднання каналів, а саме – EtherChannel:

int range fa0/1-2 // обираємо інтерфейси для налаштування

channel-group 1 mode active // створюємо активний канал

Creating a port-channel interface Port-channel 1

int port-channel 1 // переходимо в його налаштування

switchport mode trunk // вмикаємо режим портів в транк

int range f0/3-4 // обираємо інтерфейси для налаштування

channel-group 2 mode passive // створюємо пасивний канал

Creating a port-channel interface Port-channel 2

int port-channel 2 // переходимо в його налаштування

switchport mode trunk // вмикаємо режим портів в транк

Резервування буде працювати лише тоді, коли налаштування будуть прописані на кожному з комутаторів цієї системи.

Налаштуємо протокол моделі доступу та управління мережевого обладнання мережі:

aaa new-model // вмикаємо протокол

radius-server host 209.165.201.5 // додаємо адресу сервера, на якому працює протокол

radius–server key radius123 // вводимо секретне слово протоколу *radius123*

aaa authentication login default group radius local // створюємо умови для отримання доступу до протоколу, а саме використання перш за все можливості протоколу, при інших випадках потрібно використовувати дані, які були створені в локальній мережі.

3.4.5 Перевірка налаштувань комп’ютерної мережі

Для перевірки налаштувань мережі будемо використовувати командний рядок мережевого обладнання Cisco та можливості операційної системи Windows, з детальним графічним матеріалом.

Перевіримо доступність вузлів з пристрою 192.168.10.166 до вузла 192.168.10.134.

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::202:17FF:FE41:2DEB
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.10.166
   Subnet Mask.....: 255.255.255.240
   Default Gateway.....: ::
                                 192.168.10.161

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0

C:\>ping 192.168.10.134

Pinging 192.168.10.134 with 32 bytes of data:

Reply from 192.168.10.134: bytes=32 time=4ms TTL=124
Reply from 192.168.10.134: bytes=32 time=4ms TTL=124
Reply from 192.168.10.134: bytes=32 time=4ms TTL=124
Reply from 192.168.10.134: bytes=32 time=3ms TTL=124

Ping statistics for 192.168.10.134:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 4ms, Average = 3ms
```

Рисунок 3.7 – Перевірка доступності вузлів

Перевіримо паралельне з’єднання каналів EtherChannel.

```
Kviatkovska_Switch6>sh etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


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 3.8 – Перевірка паралельного з’єднання каналів

Перевіримо роботу сегментованих мереж, з мережі 26 відправимо ехо-запит у мережу 16 та 36. Одна мережа повинна відповідати, інша повинна бути заблокована програмним чином.

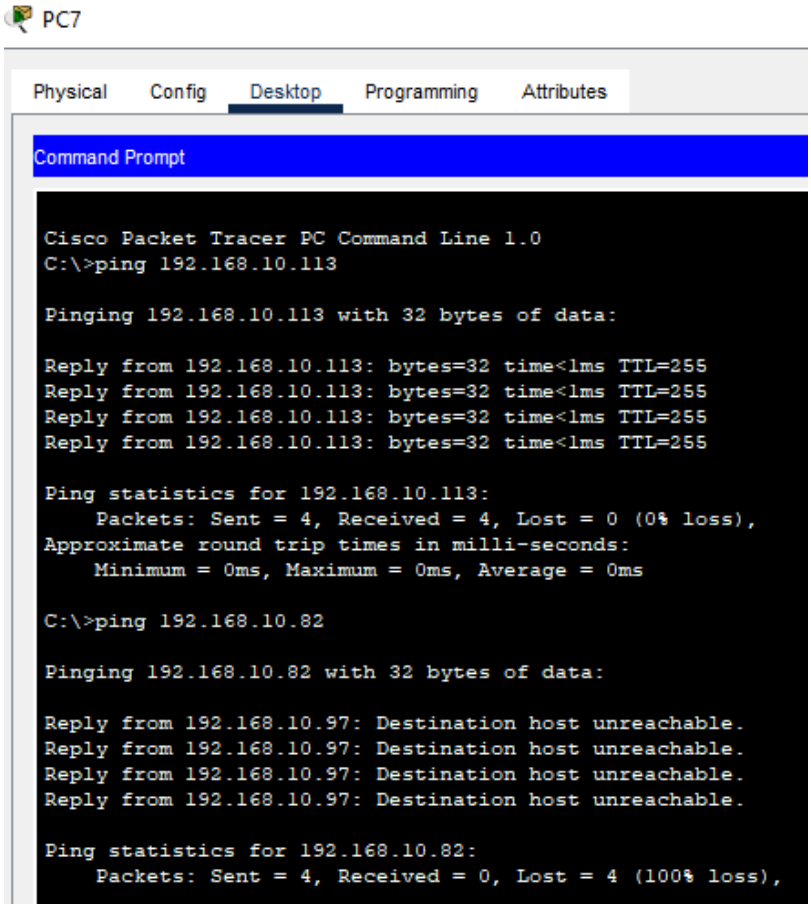

Рисунок 3.9 – Перевірка сегментованих мереж

Перевіримо налаштування протоколу віддаленого управління безпечної оболонки.

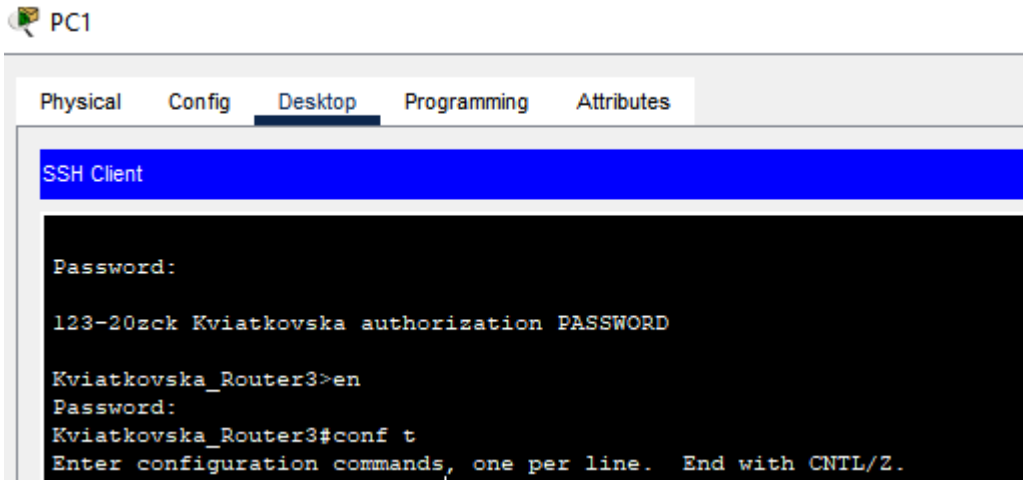

Рисунок 3.10 – Перевірка протоколу безпечної оболонки

Перевіримо таблицю налаштувань автоматичних мережевих налаштувань за протоколом DHCP на маршрутизаторі віддаленої мережі LAN1.

```
Kviatkovska_Router0#show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
192.168.10.133   0090.210C.53A4           --                     Automatic
192.168.10.132   000D.BD73.08A9           --                     Automatic
192.168.10.131   00D0.D3A2.B7C9           --                     Automatic
192.168.10.130   0060.5C64.C4A2           --                     Automatic
192.168.10.134   0009.7CD3.AA28           --                     Automatic
192.168.10.140   0060.5C7D.7B21           --                     Automatic
192.168.10.137   00E0.A363.ACC1           --                     Automatic
192.168.10.139   0004.9A8A.91EC           --                     Automatic
192.168.10.141   00D0.FF5C.E711           --                     Automatic
192.168.10.136   0001.9665.D273           --                     Automatic
192.168.10.135   00D0.BCE4.B30A           --                     Automatic
192.168.10.138   0060.7063.B313           --                     Automatic
192.168.10.142   00E0.F723.2796           --                     Automatic
192.168.10.144   0060.479E.4265           --                     Automatic
192.168.10.143   0010.11E9.9AB4           --                     Automatic
```

Рисунок 3.11 – Перевірка автоматичних мережевих налаштувань

На комутаторах мережі перевіримо співвідношення налаштувань портів до сегментованих мереж.

```
Kviatkovska_Switch0>show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Gig0/1
16   teaml                            active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9
26   team2                            active    Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14
36   team3                            active    Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Рисунок 3.12 – Перевірка сегментованих мереж

Перевіримо облікові записи, які були налаштовані на RADIUS сервері та конфігурують в роботі протоколу AAA.

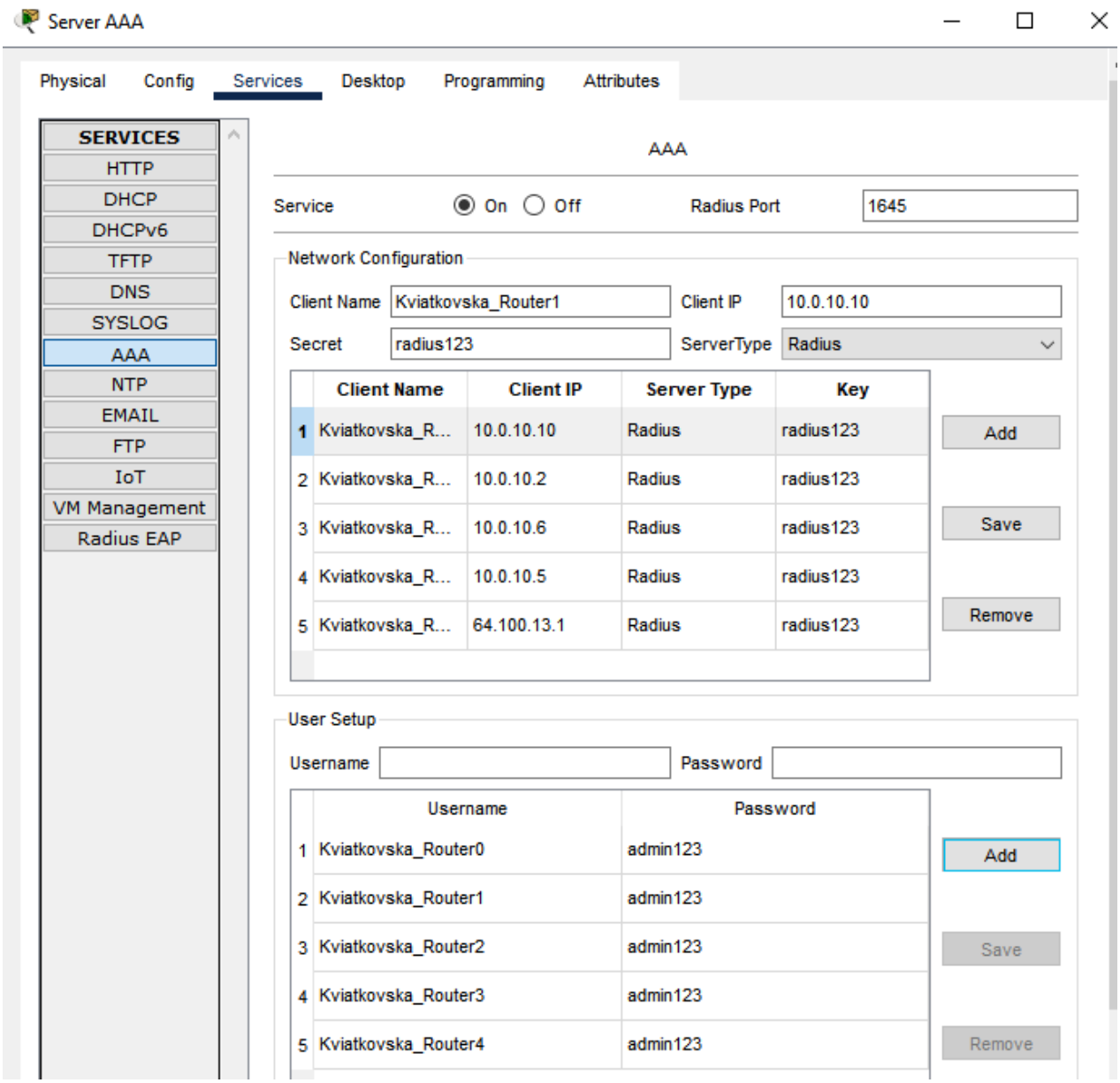

Рисунок 3.13 – Перевірка налаштувань RADIUS серверу

Перевіримо налаштування резервування мережевих конфігурацій, які виконуються за допомогою серверу TFTP.

```
Kviatkovska_Router2#copy running-config tftp
Address or name of remote host []? 192.168.10.84
Destination filename [Kviatkovska_Router2-confg]?

Writing running-config...!!
[OK - 2513 bytes]

2513 bytes copied in 0 secs
Kviatkovska_Router2#
```

Рисунок 3.14 – Перевірка запису конфігурацій

Перевіримо збережену конфігурацію на TFTP сервері.

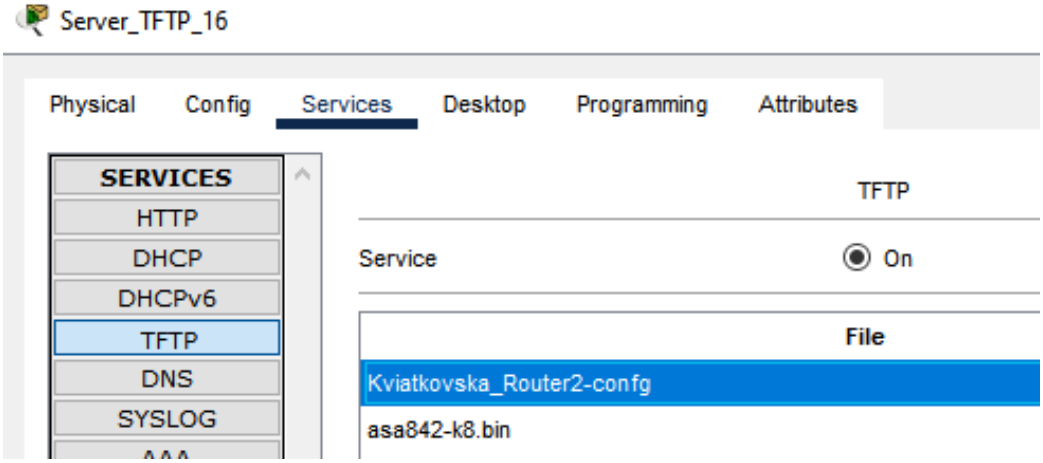

Рисунок 3.15 – Перевірка роботи сервера TFTP

Перевіримо роботу веб-сайту, для відображення інформація студента, та роботу DNS серверу.

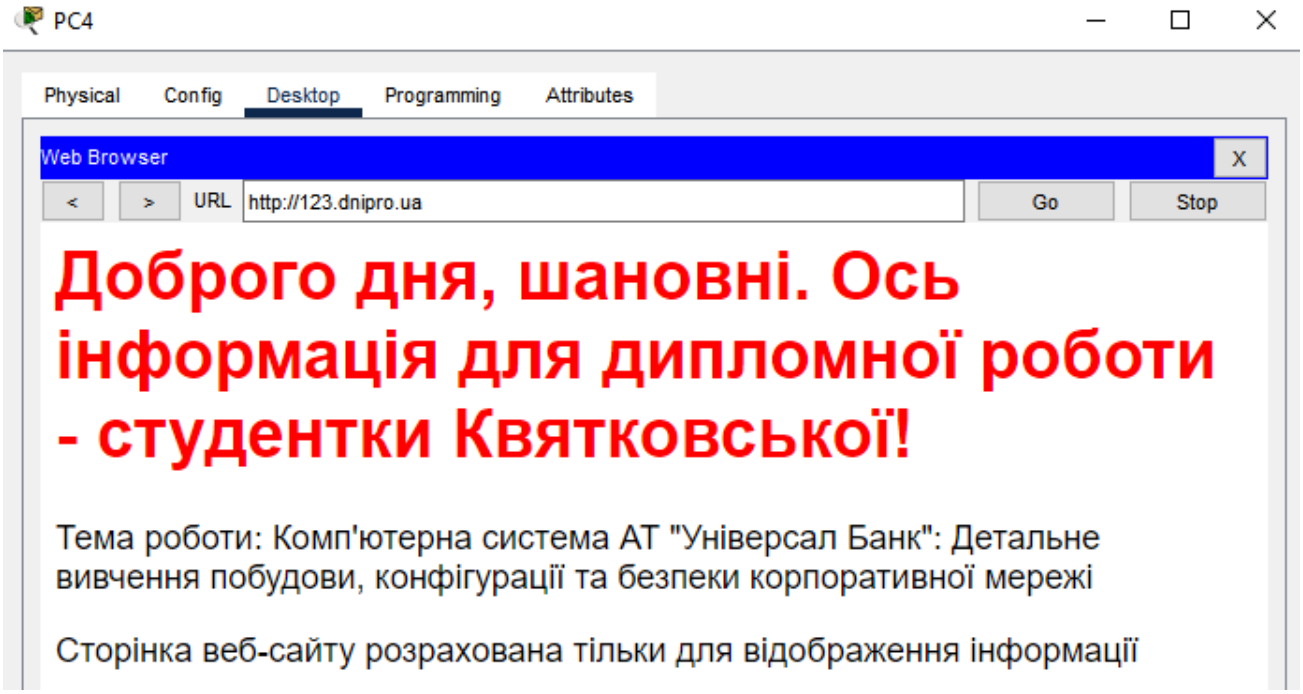

Рисунок 3.16 – Перевірка роботи веб-сайту

Перевіримо працездатність роутеру Wi-Fi та конфігурації пристроїв після підключення.

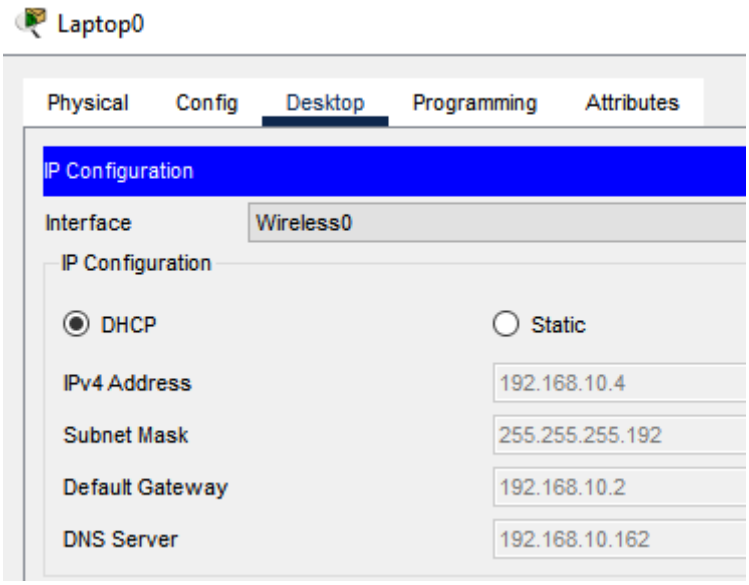

Рисунок 3.17 – Перевірка конфігурації ноутбуку від мережі Wi-Fi

Переглянемо html код, який записаний у HTTP сервері та відпрацьовує для відображення інформації веб-сайту компанії банку.

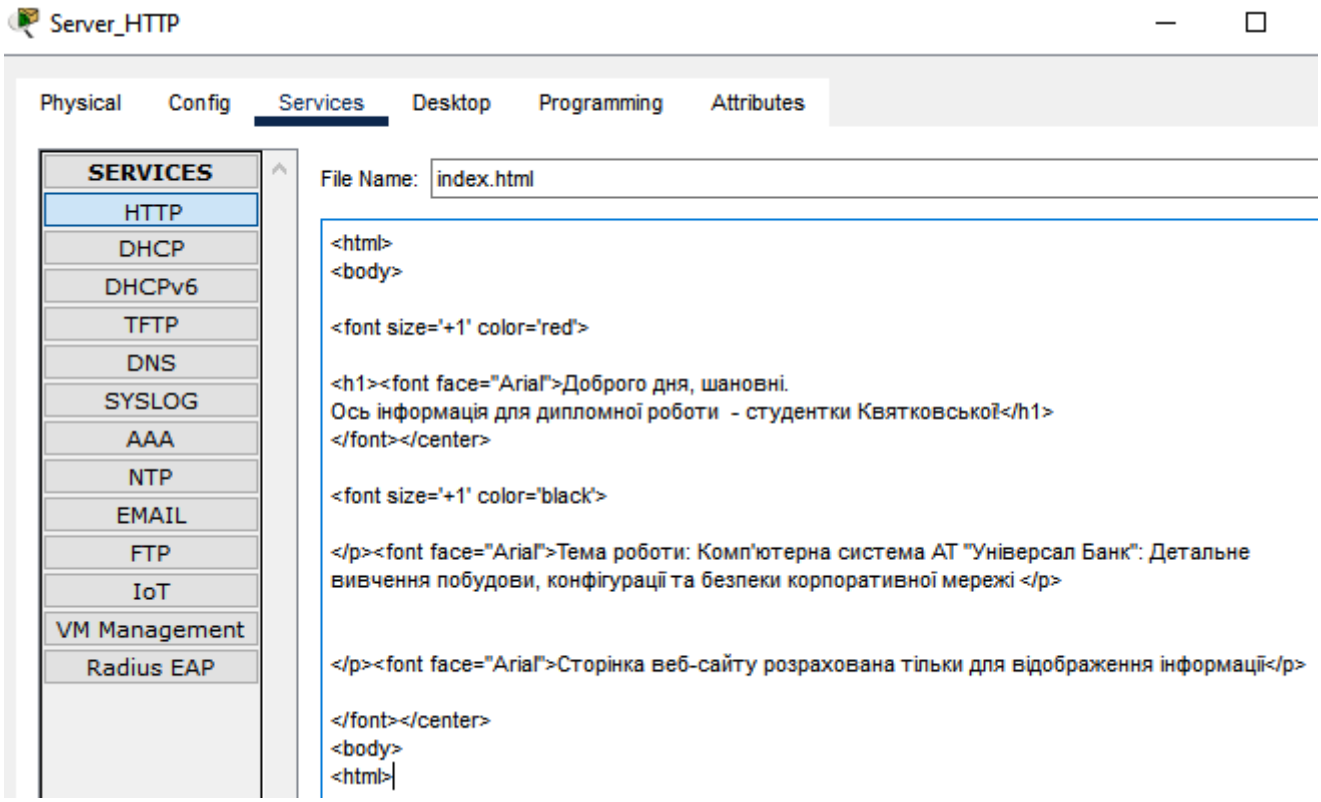

Рисунок 3.18 – Перевірка html коду

4 РОЗРОБКА КОМПОНЕНТА СИСТЕМИ БЕЗПЕКИ ТА СИГНАЛІЗАЦІЇ АТ "УНІВЕРСАЛ БАНКУ"

4.1 Розробка компонентів інтернет-речей

За вимогами кваліфікаційної роботи було створено систему безпеки підмережі LAN2, за технологією IoT – інтернет речей.

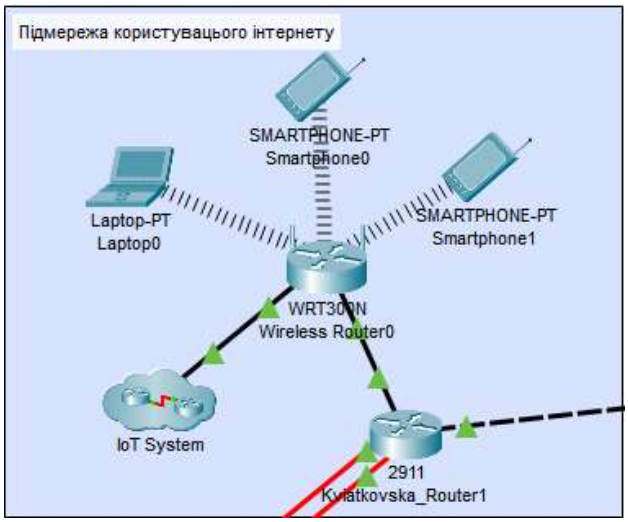

Рисунок 4.1 – Інтегрована система IoT

Головним аспектом банку є безпека.

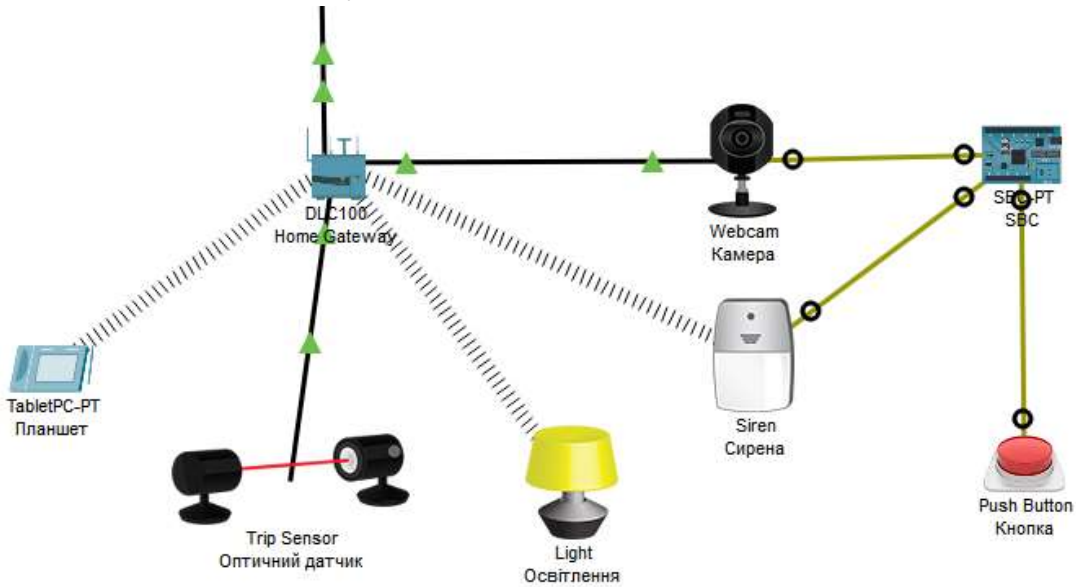

Рисунок 4.2 – Система безпеки IoT

Система розрахована на запис інформації по веб-камері, якщо хтось зайде в офіс без перепустки. При цьому увімкнеться сирена та світло.

В будівлі офісу впроваджені оптичні датчики, які визначають рух у приміщенні. Якщо система безпеки не була вимкнена співробітниками, оптичний датчик спрацьовуватиме для відпрацювання безпеки.

Таблиця 4.1 – Вихідні дані

Webcam	End Devices → Home
Siren	End Devices → Home
Lamp	End Devices → Home
Trip Sensor	End Devices → Industrial
Push Button	Components → Sensors
SBC	Components → Boards

4.2 Налаштування системи безпеки

Налаштування системи відбувається в домашньому шлюзі – Home Gateway. Адреса шлюза – 192.168.25.1, на цій адресі розташований сервер системи IoT.

Рисунок 4.3 – Авторизація в систему безпеки IoT

Налаштування виконуємо з планшету, який підключений до мережі. Для авторизації до серверу використовуємо логін та пароль – admin/admin.

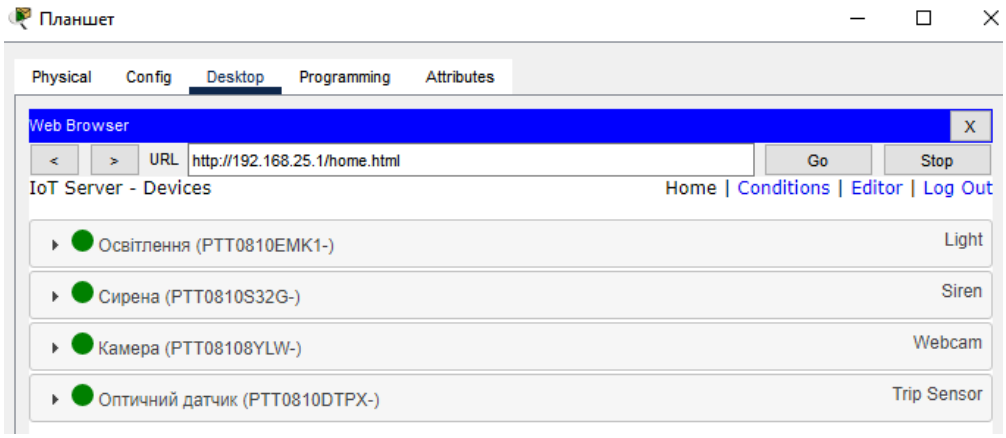

Рисунок 4.4 – Пристрої в системі безпеки IoT

В IoT севері ми бачимо всі пристрої, які підключені до – Home Gateway.

Для підключення к серверу в кожному пристрої треба вказати дані Remote server, а саме – IP-адресу та логін/пароль.

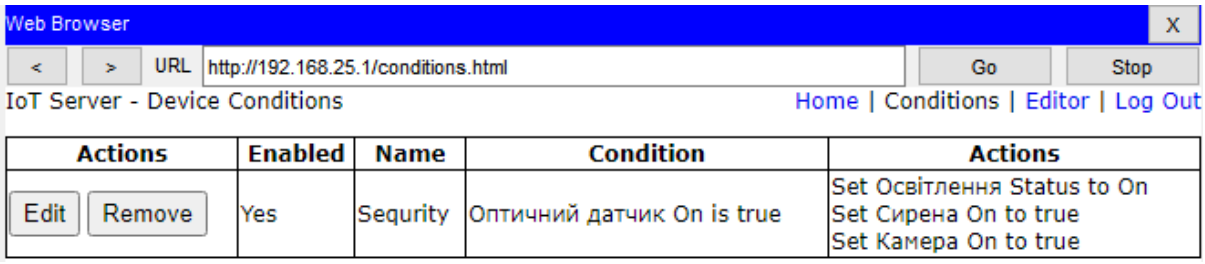

Рисунок 4.5 – Створення сценарію в системі безпеки IoT

В сервері у вкладці Conditions записуємо сценарій роботи пристроїв. Коли оптичний датчик спрацьовує, освітлення, сирена та камера повинні включатися.

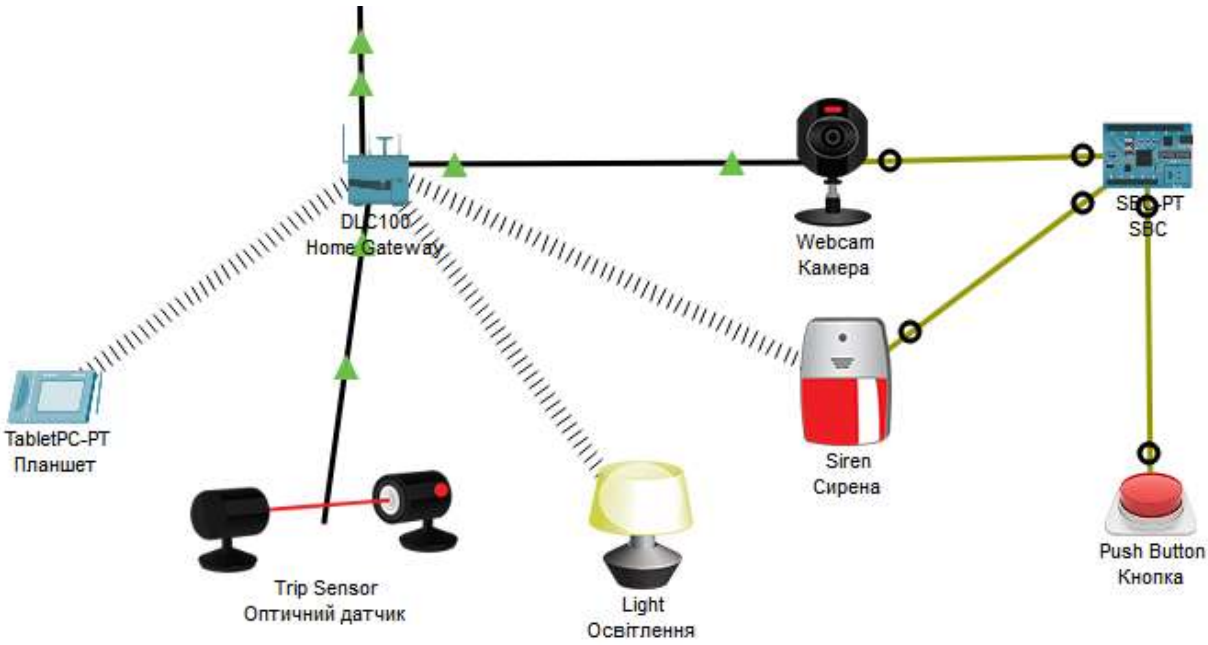

Рисунок 4.6 – Працездатність системи безпеки IoT

Головною вимогою системи є фізичне виключення сирени та камери за допомогою кнопки. За цією вимого було використано програмуючий мікроконтролер SBC.

Програмування мікроконтролеру SBC відбувається на мові програмування Python, код програми може бути як невеликими скриптами, так і складними системами.

Код мікроконтролеру SBC:

```
from gpio import *
from time import *

def main():
	pinMode(0, IN)
	pinMode(1, OUT)
	pinMode(2, OUT)

	print("Starting program")
	while True:

		PButton = digitalRead(0)

		if (PButton == HIGH):
			customWrite(2, 1)
			customWrite(1, 1)
		else:
			customWrite(2, 0)
			customWrite(1, 0)

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

ВИСНОВКИ

При створені кваліфікаційної роботи було досліджено та проаналізовано різні аспекти комп'ютерних мереж з метою поліпшення їхньої продуктивності та надійності.

Результатом моделювання було обрано топологію дерево, вона є найбільш поширеною і зручною для управління, та пропонує вищу відмовостійкість і ефективніше використання ресурсів.

В ході роботи були використані протоколи комунікації, зокрема стек протоколів TCP/IP. Було встановлено, що TCP/IP є найпоширенішим і найнадійнішим протоколом для передавання даних у комп'ютерних мережах.

Також було обрано метод маршрутизації, включно зі статичною та динамічною маршрутизацією за протоколом. Динамічна маршрутизація, заснована на протоколі маршрутизації OSPF, який надає більш гнучкі та автоматизовані способи управління маршрутами в мережі.

Моделювання мережі виконано в додатку Cisco Packet Tracer.

Були розглянуті питання мережевої безпеки і впроваджені різні заходи, які можна вжити для захисту комп'ютерних мереж від загроз і несанкціонованого доступу. Це включає в себе використання протоколів SSH, ACL, AAA, VLAN та використання певних налаштувань на комутаторах та маршрутизаторах.

Для безпечної працездатності банку було впроваджено технологію інтернет речей (IoT) та визначено вплив технологій на сучасну мережеву інфраструктуру.

ПЕРЕЛІК ПОСИЛАНЬ

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

2. 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.

3. Цвіркун, Л.І. Розробка програмного забезпечення комп'ютерних систем. Програмування: навч. посібник / Л.І. Цвіркун, А.А. Євстігнєєва, Я.В. Панферова, під заг. ред. Л.І. Цвіркуна. – 3-є вид., випр. – Д.: Національний гірничий університет, 2016. – 223 с. – ISBN 978-966-350-595-4.

4. 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. 1. – 60 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 маршрутизатора Cisco [Електронний ресурс] – https://creativnost.com.ua/yak-samostijno-nalashtuvati-marshrutizator-cisco/

7. Основні поняття агрегування каналів [Електронний ресурс] – https://cisco.nitaet.com/ccna-3-sn-ru/course/module3/3.1.2.2/3.1.2.2.html

8. Локальні мережі. Загальні принципи організації. [Електронний ресурс] – https://www.briz.ua/blog/article/cto-takoe-lokalnaya-set

9. Вибір активного мережевого обладнання [Електронний ресурс] – https://klaster.ua/ua/stati-i-obzory/chto-takoe-aktivnoe-setevoe-oborudovanie/

10. Інтернет речей і розумний дім у cisco packet tracer [Електронний ресурс] – http://arekusander.blogspot.com/2017/12/cisco-packet-tracer-7.html

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
804.02070743.23006-01 12 01

Листів 12

2023

АННОТАЦІЯ

Програма складається з частини програмного коду для налаштування конфігурацій мережевих інтерфейсів мережі. Код призначений для працездатності протоколів DHCP, AAA, NAT, PAgP для налаштування консолей та ліній VTY та для створення комп'ютерних підмереж VLAN, домену та SSH доступу. Також, для налаштування списків доступу ACL.

ЗМІСТ

Конфігурація Kviatkovska_Router2:

```
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Kviatkovska_Router2
!
ip dhcp pool Vlan16
 network 192.168.10.80 255.255.255.240
 default-router 192.168.10.81
 dns-server 192.168.10.162
ip dhcp pool Vlan26
 network 192.168.10.96 255.255.255.240
 default-router 192.168.10.97
 dns-server 192.168.10.162
ip dhcp pool Vlan36
 network 192.168.10.112 255.255.255.240
 default-router 192.168.10.113
 dns-server 192.168.10.162
ip dhcp pool LAN4
 network 192.168.10.64 255.255.255.240
 default-router 192.168.10.65
 dns-server 192.168.10.162
!
no ip cef
no ipv6 cef
!
license udi pid CISCO2911/K9 sn FTX1524E66K-
```

```
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
 ip address 192.168.10.65 255.255.255.240
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.16
 encapsulation dot1Q 16
 ip address 192.168.10.81 255.255.255.240
 ip access-group CLOSED in
!
interface GigabitEthernet0/0.26
 encapsulation dot1Q 26
 ip address 192.168.10.97 255.255.255.240
 ip access-group CLOSED in
!
interface GigabitEthernet0/0.36
 encapsulation dot1Q 36
 ip address 192.168.10.113 255.255.255.240
 ip access-group CLOSED in
!
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 10.0.10.2 255.255.255.252
!
interface Serial0/2/1
 no ip address
 clock rate 2000000
 shutdown
!
interface Serial0/3/0
 ip address 10.0.10.14 255.255.255.252
 clock rate 2000000
!
interface Serial0/3/1
 ip address 10.0.10.18 255.255.255.252
 clock rate 2000000
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 network 10.0.10.0 0.0.0.3 area 0
 network 10.0.10.12 0.0.0.3 area 0
 network 10.0.10.16 0.0.0.3 area 0
```

```
 network 192.168.10.64 0.0.0.15 area 0
 network 192.168.10.80 0.0.0.15 area 0
 network 192.168.10.96 0.0.0.15 area 0
 network 192.168.10.112 0.0.0.15 area 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.202.1
ip route 0.0.0.0 0.0.0.0 10.0.10.1
!
ip flow-export version 9
!
ip access-list extended CLOSED
 deny ip 192.168.10.80 0.0.0.15 192.168.10.96 0.0.0.15
 deny ip 192.168.10.96 0.0.0.15 192.168.10.80 0.0.0.15
 deny ip 192.168.10.112 0.0.0.15 192.168.10.80 0.0.0.15
 deny ip 192.168.10.80 0.0.0.15 192.168.10.112 0.0.0.15
 permit ip any any
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
end
```

Налаштування маршрутизатора Kviatkovska_Router3:

```
!
version 15.1
```

```
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Kviatkovska_Router3
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
no ip cef
no ipv6 cef
!
username 12320zck_Kviatkovska password 7 0822455D0A16
!
license udi pid CISCO2911/K9 sn FTX1524Y86V-
!
ip domain-name Kviatkovska_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 10.0.10.1 255.255.255.252
 ip nat inside
 clock rate 2000000
!
interface Serial0/2/1
 no ip address
 clock rate 2000000
 shutdown
!
interface Serial0/3/0
 ip address 209.165.202.1 255.255.255.252
 ip nat outside
!
interface Serial0/3/1
 ip address 10.0.10.5 255.255.255.252
 ip nat inside
 clock rate 2000000
!
interface Vlan1
 no ip address
 shutdown
!
```

```
router ospf 1
 log-adjacency-changes
 network 10.0.10.0 0.0.0.3 area 0
 network 10.0.10.4 0.0.0.3 area 0
!
ip nat inside source list 5 interface Serial0/3/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.202.2
!
ip flow-export version 9
!
access-list 5 permit 192.168.10.0 0.0.0.255
!
banner motd #123-20zck Kviatkovska authorization PASSWORD#
!
line con 0
 password 7 0822455D0A16
 login
!
line aux 0
!
line vty 0 4
 login local
 transport input ssh
!
end
```

Налаштування комутатора Kviatkovska_Switch6:

```
!
version 15.0
```

```
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Kviatkovska_Switch6
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface Port-channel1
 switchport mode trunk
!
interface Port-channel2
 switchport mode trunk
!
interface FastEthernet0/1
 switchport mode trunk
 channel-group 1 mode active
!
interface FastEthernet0/2
 switchport mode trunk
 channel-group 1 mode active
!
interface FastEthernet0/3
 switchport mode trunk
 channel-group 2 mode passive
!
interface FastEthernet0/4
 switchport mode trunk
 channel-group 2 mode passive
```

```
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address dhcp
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
End
```

Додаток Б

Схема загальної топології банку

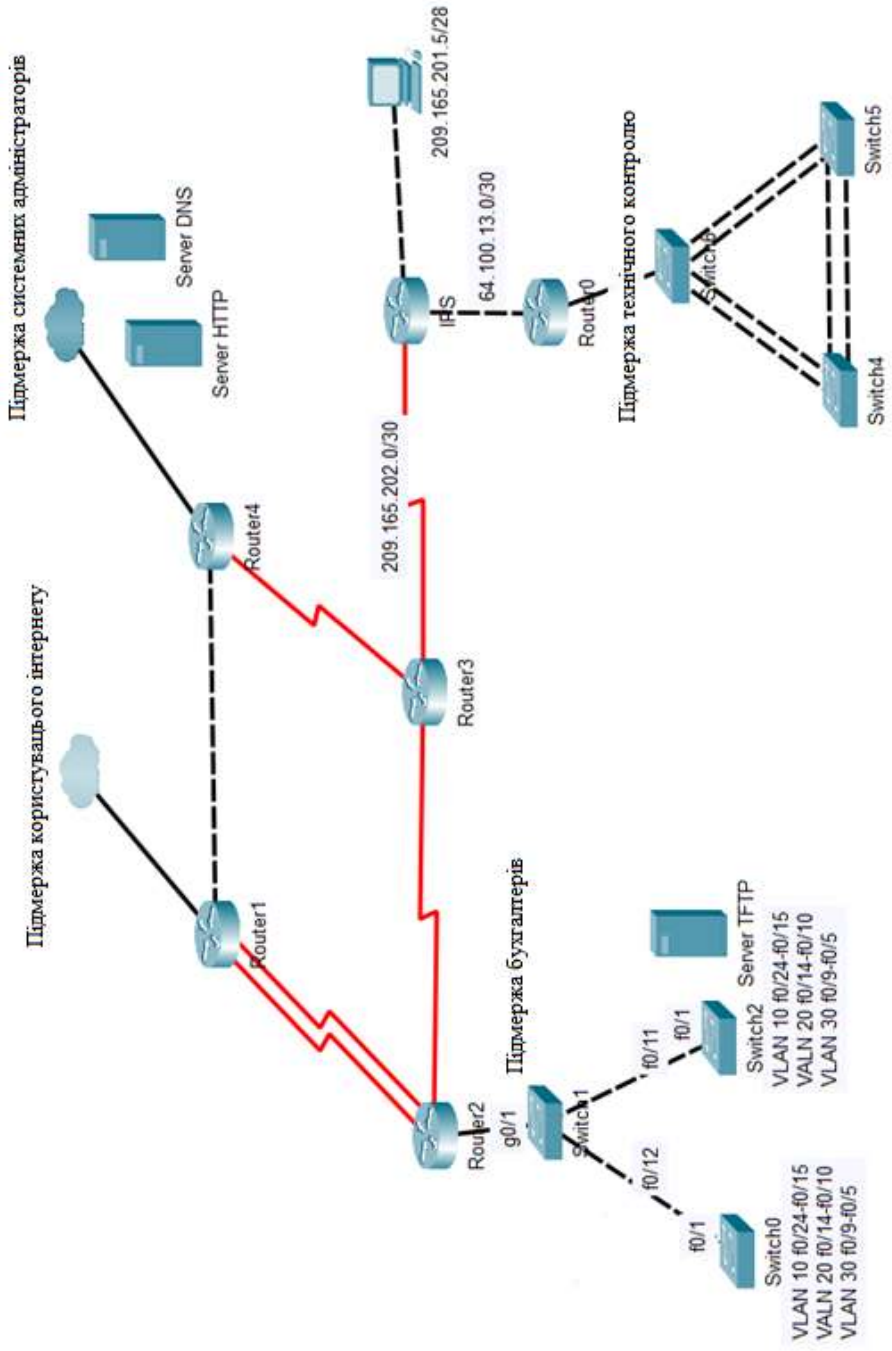

Рисунок Б.1 – Схема загальної топології банку