Вінницький національний технічний університет
*(повне найменування вищого навчального закладу)*

Факультет інформаційних технологій та комп'ютерної інженерії
*(повне найменування інституту, назва факультету (відділення))*

Кафедра обчислювальної техніки
*(повна назва кафедри (предметної, циклової комісії))*

# БАКАЛАВРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Комп'ютерна мережа кафе "O'CAKE"»

08-54.БКР.034.00.000 ПЗ

Виконав: студент 4 курсу, групи 2КІ-21б

спеціальності 123 — Комп'ютерна інженерія
*(шифр і назва напряму підготовки, спеціальності)*

_____ Шестопал А.Р.
*(підпис)*

Керівник: к.т.н., проф. каф. ОТ

_____ Захарченко С. М.
*(підпис)*

«_____» _____ 2025 р.

Рецензент: доктор філософії, доцент каф. МБІС

_____ Салієва О. В.
*(підпис)*

«_____» _____ 2025 р.

Допущено до захисту

Завідувач кафедри ОТ

д.т.н., проф. Азаров О. Д.

«17» 06 2025 р.

Вінниця ВНТУ — 2025 рік

**ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ**

Факультет інформаційних технологій та комп'ютерної інженерії

Кафедра обчислювальної техніки

Освітньо-кваліфікаційний рівень бакалавр

Галузь знань — 12 «Інформаційні технології»

Спеціальність — 123 «Комп'ютерна інженерія»

Освітньо-професійна програма «Комп'ютерна інженерія»

**ЗАТВЕРДЖУЮ**

**Завідувач кафедри ОТ**

д.т.н., проф. Азаров О. Д.

«21» березня 2025 р.

**З А В Д А Н Н Я**

**НА БАКАЛАВРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ**

Шестопалу Андрію Руслановичу

1 Тема роботи: «Комп'ютерна мережа кафе "О'САКЕ"», керівник роботи к.т.н., проф. каф. ОТ Захарченко С.М., затверджена наказом вищого навчального закладу від 20 березня 2025 р. №97.

2 Термін подання студентом роботи 13 травня 2025 р.

3 Вихідні дані до роботи: основні підтримувані функції — проєктування комп'ютерної мережі для кафе з кількома філіями; організація зв'язку між віддаленими підрозділами; забезпечення безпечного обміну даними; централізованого доступу до сервісів і можливості адміністрування мережі.

4 Зміст розрахунково-пояснювальної записки: вступ, аналіз сучасних мережевих технологій, обґрунтування проєктних рішень, вибір топології та обладнання, налаштування і тестування мережі, реалізація захищених з'єднань між філіями, налаштування серверної частини та бази даних.

5 Перелік ілюстративної частини: логічна топологія мережі кафе «О'САКЕ».

6 Консультанти розділів роботи приведені в таблиці 1.

Таблиця 1 — Консультанти роботи

| Розділ | Прізвище, ініціали та посада консультанта | Підпис, дата | |
|---|---|---|---|
| | | завдання видав | завдан прийн |
| 1-3 | к.т.н., проф. каф. ОТ Захарченко С. М. | 21.03.25 | 13.05. |
| Нормоконтроль | ас. каф. ОТ Швець С. І. | 13.05.25 | 30.05. |

7 Дата видачі завдання 21 березня 2025 р.

8 Календарний план виконання БКР приведений в таблиці 2.

Таблиця 2 — Календарний план виконання БКР

| № | Назва етапу | Термін виконання | Підпис |
|---|---|---|---|
| 1 | Постановка задачі | 21.03.25 | вик. |
| 2 | Аналіз технологій для створення комп'ютерних мереж | 21.03.25— 30.03.25 | вик. |
| 3 | Аналіз та обґрунтування вибору технологій | 21.03.25— 30.03.25 | вик. |
| 4 | Реалізація комп'ютерної мережі | 31.03.25— 13.04.25 | вик. |
| 5 | Тестування комп'ютерної мережі | 14.04.25— 27.04.25 | вик. |
| 6 | Підготовка тезових матеріалів для публікації | 21.04.25— 28.04.25 | вик. |
| 7 | Оформлення пояснювальної записки та презентації для доповіді | 29.04.25— 12.05.25 | вик. |
| 8 | Підготовка супровідної документації, перевірка відповідності нормам та проходження тесту на плагіат | 13.05.25 | вик. |

**Студент** Андрій ШЕСТОПАЛ

**Керівник роботи** к.т.н., проф. Сергій ЗАХАРЧЕНКО

# АНОТАЦІЯ

УДК 004.7

Шестопал А. Р. Проєктування корпоративної мережі для мережі кафе «О'САКЕ». Бакалаврська кваліфікаційна робота зі спеціальності 123 «Комп'ютерна інженерія», освітня програма «Комп'ютерна інженерія». Вінниця: ВНТУ, 2025. 81 с.

На укр. мові. Бібліогр.: 19 назв, рис.: 29, табл.: 23.

У роботі проведено комплексний аналіз сучасних технологій комп'ютерних мереж, зокрема моделей OSI та TCP/IP, IP-адресації (IPv4), технологій Ethernet та Wi-Fi. Обґрунтовано вибір динамічного маршрутизувального протоколу OSPF для побудови внутрішньої маршрутизації між філіями. Запропоновано топологію з'єднання на основі технології Frame Relay для організації міжфілійної WAN-мережі.

Реалізовано захищене з'єднання між філіями на базі GRE over IPsec VPN. Розгорнуто сервер на ОС Debian із встановленими службами DNS, MariaDB та phpMyAdmin, який виконує роль централізованого сервера бази даних для всієї мережі. Запроваджено служби DHCP та NAT для автоматизації конфігурації клієнтів, а також безпечне адміністрування з використанням SSH та обмеження доступу через ACL. Передбачено підключення бездротових клієнтів до Wi-Fi точок доступу у філіях.

Роботу реалізовано у симуляційному середовищі Cisco Packet Tracer. Проведено тестування функціональності мережевих сервісів та міжфілійної взаємодії. Результати підтвердили працездатність та масштабованість запропонованої архітектури.

Ключові слова: комп'ютерна мережа, Frame Relay, IP-адресація, OSPF, VPN, GRE, IPsec, DHCP, NAT, SSH, ACL, DNS, MariaDB, phpMyAdmin, Wi-Fi.

## ABSTRACT

Shestopal A. R. Design of a Corporate Network for the «O'CAKE» Café Chain. Bachelor's qualification work in specialty 123 "Computer Engineering", educational program "Computer Engineering". Vinnytsia: VNTU, 2025. 81 p.

In Ukrainian. Bibliography: 19 sources, illustrations: 29, tables: 23.

This work presents a comprehensive analysis of modern computer network technologies, including OSI and TCP/IP models, IP addressing (IPv4), Ethernet, and Wi-Fi technologies. The OSPF dynamic routing protocol was selected and justified for building internal routing between branches. A network topology based on Frame Relay technology was proposed for organizing inter-branch WAN connections.

A secure connection between branches was implemented using GRE over IPsec VPN. A server running the Debian operating system was deployed, featuring DNS, MariaDB, and phpMyAdmin services, serving as a centralized database server for the entire network. DHCP and NAT services were introduced for automated client configuration, along with secure administration via SSH and access restrictions using ACLs. Wireless client connectivity was also provided through Wi-Fi access points at each branch.

The project was implemented in the Cisco Packet Tracer simulation environment. Functional testing of network services and inter-branch communication was carried out. The results confirmed the operability and scalability of the proposed architecture.



Keywords: computer network, Frame Relay, IP addressing, OSPF, VPN, GRE, IPsec, DHCP, NAT, SSH, ACL, DNS, MariaDB, phpMyAdmin, Wi-Fi

# ЗМІСТ

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ, ТЕРМІНІВ

TCP/IP — Transmission Control Protocol/Internet Protocol

IPv4 — Internet Protocol Version 4

IPv6 — Internet Protocol Version 6

NAT — Network Address Translation

EIGRP — Enhanced Interior Gateway Routing Protocol

RIP — Routing Information Protocol

ACL — Access Control List

DHCP — Dynamic Host Configuration Protocol

DNS — Domain Name System

Ethernet — Ethernet Technology

Frame Relay — Frame Switching Technology

GRE — Generic Routing Encapsulation

IPsec — Internet Protocol Security

IPv4 — Internet Protocol version 4

MariaDB — Relational Database Management System

OSPF — Open Shortest Path First

phpMyAdmin — Web Interface for MariaDB Administration

SSH — Secure Shell

VPN — Virtual Private Network

Wi-Fi — Wireless Fidelit

# ВСТУП

Сучасні інформаційні технології та комп'ютерні мережі є ключовим елементом інформаційної інфраструктури підприємств, забезпечуючи ефективну комунікацію, управління та захист даних. Ця тема є актуальною для фахівців із комп'ютерних мереж через постійний розвиток технологій, що відкриває нові можливості та ставить завдання підвищення продуктивності та безпеки мережевих систем.

**Актуальність** роботи полягає у необхідності впровадження надійних мережевих рішень для корпоративної мережі мережі кафе O'CAKE, що дозволить ефективно обробляти зростаючі обсяги даних та кількість мережевих операцій. Розробка інтегрованої мережевої системи дасть змогу оптимізувати комунікацію між філіями, спростити управління та забезпечити високий рівень інформаційної безпеки.

У наукових дослідженнях підкреслюється важливість використання сучасних технологій, таких як динамічна маршрутизація, NAT, VPN, а також засобів захисту мережевої інфраструктури. Попередні роботи демонструють ефективність застосування існуючих протоколів маршрутизації та методів організації мережевих сегментів для підвищення надійності та безпеки.

**Метою** роботи є розробка безпечної та масштабованої архітектури комп'ютерної мережі для мережі кафе «O'CAKE» з використанням сучасних технологій: Frame Relay для WAN-з'єднань, динамічного маршрутизування OSPF, VPN на базі GRE over IPsec, служб DHCP, а також захищеного віддаленого адміністрування через SSH.

Для досягнення поставленої мети необхідно виконати такі **задачі**:

— провести аналіз сучасних технологій проєктування комп'ютерних мереж;

— визначити оптимальну топологію мережі з урахуванням специфіки корпоративної структури кафе;

— обґрунтувати вибір протоколів маршрутизації та заходів безпеки;

— спланувати IP-адресацію та підібрати відповідне мережеве обладнання;

— реалізувати та протестувати мережеве рішення у симуляційному середовищі для підтвердження його працездатності та масштабованості.

**Об’єкт дослідження** — процес проєктування та експлуатації корпоративної комп’ютерної мережі мережі кафе «O’CAKE».

**Предметом дослідження** є технології та методи проєктування, налаштування і забезпечення безпеки мереж із застосуванням сучасних протоколів маршрутизації, VPN і мережевих сервісів.

**Новизна** результатів полягає у комплексному підході до побудови багатофіліальної мережевої інфраструктури, що відповідає сучасним вимогам безпеки та забезпечує надійну роботу мережі кафе.

**Апробація** отриманих результатів відбулася під час виступу на LIV Всеукраїнській науково-технічній конференції факультету інформаційних технологій та комп'ютерної інженерії [1].

**Публікації**: Розвиток технологій 5G та їх вплив на побудову сучасних локальних мереж. / А. Р. Шестопал, С. М. Захарченко // Матеріали конференції LIV Всеукраїнської науково-технічної конференції підрозділів ВНТУ, 2025 р. Режим доступу:https://conferences.vntu.edu.ua/index.php
/all-fitki/all-fitki2025/paper/view/23658/19529.

# 1 АНАЛІЗ ТЕХНОЛОГІЙ ДЛЯ СТВОРЕННЯ КОМП'ЮТЕРНИХ МЕРЕЖ

## 1.1 Моделі OSI та TCP/IP: принципи побудови мереж

У процесі проєктування сучасних комп'ютерних мереж важливо керуватись усталеними теоретичними моделями, які описують принципи взаємодії між окремими компонентами мережі. Найбільш поширеними і загальноприйнятими є дві моделі: еталонна модель OSI (Open Systems Interconnection) та мережева модель TCP/IP (Transmission Control Protocol/Internet Protocol) [2].

Ці моделі виконують декілька ключових функцій:

— визначають стандарти взаємодії між різнорідними пристроями і програмним забезпеченням;

— дозволяють розділити складний процес передачі даних на логічні етапи;

— служать основою для проєктування, діагностики та розвитку комп'ютерних мереж.

Модель OSI була запропонована в 1984 році міжнародною організацією зі стандартизації (ISO) для створення універсального підходу до побудови мереж. Вона розділяє комунікаційний процес між двома пристроями на сім ієрархічних рівнів, кожен з яких виконує визначений набір функцій [3].

Ключовою перевагою моделі OSI є її модульність: кожен рівень працює незалежно, використовуючи послуги нижчого рівня та надаючи сервіси вищому. Це дозволяє ефективно впроваджувати нові технології без радикальної перебудови мережевої архітектури. Наприклад, коли користувач надсилає листа через електронну пошту:

— на рівні 7 використовується SMTP-протокол;

— рівень 4 забезпечує доставку за допомогою TCP;

— рівень 3 відповідає за маршрутизацію пакетів до отримувача;

— на рівні 2 виконується локальна передача через MAC-адресу;

— рівень 1 транслює інформацію у фізичні сигнали.

На рисунку 1.1 наведено рівні еталонної моделі OSI.


Рисунок 1.1 — Рівні еталонної моделі OSI

На відміну від теоретичної OSI, TCP/IP — це модель, що виникла з реальних потреб побудови розподіленої мережі (Інтернет) ще в 1970-х роках. Вона отримала широке розповсюдження завдяки гнучкості, відкритості та підтримці з боку урядових структур і приватних компаній. З часом TCP/IP стала основою всіх мережевих взаємодій в Інтернеті та корпоративних середовищах.

Модель TCP/IP включає чотири рівні, що охоплюють основні функції OSI, але більш компактно. Складові TCP/IP, такі як IP-протокол для адресації та маршрутизації, TCP для надійної передачі, UDP для передачі в реальному часі, а також ICMP для діагностики (ping, traceroute), утворюють набір механізмів, які реалізуються у кожному пристрої, підключеному до Інтернету. Рівні моделі TCP/IP та їх відповідність OSI показано у таблиці 1.1. Обидві моделі мають спільну мету

— структурувати процес взаємодії між мережевими компонентами, проте між ними існують суттєві відмінності. Порівняння моделей OSI та TCP/IP описано у таблиці 1.1.

Таблиця 1.1 — Рівні моделі TCP/IP та їх відповідність OSI

| Рівень TCP/IP | Відповідність OSI | Функції |
|---|---|---|
| Прикладний | 7, 6, 5 | Робота з протоколами прикладного рівня: HTTP, FTP, DNS |
| Транспортний | 4 | Надійна/ненадійна передача (TCP/UDP) |
| Мережевий (Інтернет) | 3 | IP-адресація, маршрутизація |
| Канальний (Мережевий інтерфейс) | 2, 1 | Передача даних у локальній мережі (Ethernet, Wi-Fi) |

Таблиця 1.2 — Порівняння моделей OSI та TCP/IP

| Критерій | OSI | TCP/IP |
|---|---|---|
| Кількість рівнів | 7 | 4 |
| Тип моделі | Теоретична | Практична, реалізована |
| Принцип побудови | Строго розмежовані рівні | Інтегровані, менш чіткі межі |
| Протоколи | Не визначені | Чітко задані (TCP, IP, ICMP тощо) |
| Основне застосування | Навчальні та концептуальні цілі | Інтернет та локальні мережі |

У межах проєкту з побудови комп’ютерної мережі для мережі кафе «O’CAKE», обидві моделі відіграють важливу роль:

— модель OSI використовується для логічного поділу функціональності обладнання;

— модель TCP/IP реалізується на практиці: кожен вузол мережі має IP-

адресу, використовує TCP/UDP для передачі, застосовує DHCP, SSH, NAT — усе в межах TCP/IP-стеку.

Таким чином, розуміння та застосування обох моделей є ключовим етапом у проєктуванні надійної, масштабованої та сумісної мережі.

## 1.2 IP-адресація: IPv4 та IPv6

IP-адресація є фундаментальною складовою будь-якої комп'ютерної мережі, адже саме вона дозволяє ідентифікувати кожен пристрій та забезпечувати доставку даних від відправника до отримувача. Існують дві основні версії Інтернет-протоколу, які використовуються в сучасних мережах — IPv4 та IPv6 [4]. Порівняння форматів IPv4 та IPv6-адрес відображено на рисунку 1.2.


Рисунок 1.2 — Порівняння форматів IPv4 та IPv6-адрес

IPv4 (Internet Protocol version 4) є найбільш поширеною версією і використовує 32-бітну адресацію. Це дозволяє створити приблизно 4,3 мільярда унікальних адрес. Формат IPv4-адреси складається з чотирьох октетів (байтів), записаних у десятковій формі й розділених крапками, наприклад: 192.168.1.1. Адреси розподіляються на публічні та приватні, останні використовуються всередині локальних мереж і не маршрутизуються через Інтернет. Зокрема, приватні діапазони — 192.168.0.0/16, 10.0.0.0/8, 172.16.0.0/12 — широко

застосовуються в бізнес-середовищі, у тому числі й у даному проєкті.

Незважаючи на свою популярність, IPv4 має низку обмежень, основне з яких — вичерпання адресного простору. Зі стрімким розвитком Інтернету речей, мобільних технологій та глобальних мереж попит на IP-адреси значно перевищив можливості протоколу IPv4. У зв'язку з цим було розроблено нову версію — IPv6.

IPv6 використовує 128-бітну адресацію, що теоретично дозволяє створити до $3.4 \times 10^{38}$ унікальних адрес — кількість, що майже необмежена з погляду сучасних потреб. На відміну від IPv4, адреси IPv6 записуються у шістнадцятковому форматі, наприклад: 2001:0db8:85a3:0000:0000:8a2e:0370:7334. Крім збільшеного адресного простору, IPv6 має інші переваги: спрощену маршрутизацію, відсутність необхідності у NAT, розширені можливості для безпеки (вбудована підтримка IPsec), автоконфігурацію пристроїв у мережі тощо [15].Порівняння характеристик протоколів IPv4 та IPv6 описано у таблиці 1.3.

Таблиця 1.3 — Порівняння характеристик протоколів IPv4 та IPv6

| Характеристика | IPv4 | IPv6 |
|---|---|---|
| Розмір адреси | 32 біти | 128 біт |
| Формат запису | Десятковий | Шістнадцятковий |
| Кількість унікальних адрес | ~4,3 мільярда | ~$3.4 \times 10^{38}$ |
| Автоматична конфігурація | Обмежена (через DHCP) | Підтримується (SLAAC, DHCPv6) |
| Підтримка NAT | Необхідна для приватних мереж | Необов'язкова |
| Безпека (IPsec) | Необов'язкова | Обов'язкова за стандартом |
| Простота маршрутизації | Відносно складна | Спрощена |
| Сумісність | Підтримується всіма пристроями | Поступове впровадження |

Попри переваги IPv6, його впровадження відбувається поступово, і багато організацій, включно з тими, що мають розгалужену філійну структуру, продовжують використовувати IPv4 як основний протокол через простоту налаштування, сумісність з існуючим обладнанням та зручність у керуванні. Саме тому у даному дипломному проєкті реалізовано систему адресації на основі IPv4, що є виправданим рішенням в умовах побудови мережі малого бізнесу.

Особливу увагу також слід приділити концепції підмережування (subnetting), яка дозволяє ефективно розподіляти IP-адреси між філіями компанії, групами користувачів або типами пристроїв. Застосування правильної маски підмережі забезпечує зменшення широкомовного трафіку, підвищення безпеки та оптимізацію маршрутизації. У проєкті для кожної філії виділено окрему підмережу з урахуванням кількості пристроїв, що дозволяє масштабувати мережу без необхідності глобального перепланування.

## 1.3 Технології побудови локальних мереж

Локальна мережа (LAN) є основою для об’єднання комп’ютерів, серверів, мережевого обладнання та інших пристроїв у межах обмеженої географічної області — наприклад, офісу, кафе чи навчального закладу. Основна мета LAN — забезпечити швидкий, надійний і безпечний обмін даними між пристроями без необхідності звертатися до глобальної мережі. Така мережа дозволяє централізовано зберігати дані, адмініструвати ресурси та оптимізувати взаємодію між працівниками чи клієнтами [5].

Сучасні локальні мережі можуть включати як дротові, так і бездротові компоненти. Поєднання обох типів дозволяє досягти гнучкості, мобільності користувачів і високої пропускної здатності. Для дротових мереж найчастіше використовується технологія Ethernet, яка забезпечує просту топологію, високу швидкість передавання даних (до 1 Гбіт/с і більше) та зручне масштабування. У випадках, коли дротове підключення ускладнене або неможливе застосовуються бездротові технології, передусім Wi-Fi, які забезпечують зручність підключення без фізичної інфраструктури.

### 1.3.1 Ethernet як основа дротової інфраструктури

Ethernet — це базовий стандарт побудови дротових локальних мереж, який підтримує передачу даних за допомогою крученої пари або оптичного кабелю. У рамках проєктування корпоративної мережі Ethernet застосовується для з'єднання комп'ютерів персоналу, POS-систем, принтерів, а також для підключення до маршрутизаторів та серверів [14].

Сучасні комутатори Ethernet підтримують автоузгодження швидкості, VLAN, QoS і PoE, що дозволяє організувати ефективну та структуровану мережу з централізованим управлінням. Завдяки підтримці VLAN забезпечується логічне розділення мережі на ізольовані сегменти, що підвищує рівень безпеки та оптимізує трафік. Механізми QoS дають змогу пріоритезувати важливі типи даних, зокрема голосовий або відеотрафік, а функція PoE дозволяє підключати IP-телефони, точки доступу та камери спостереження без потреби у додаткових блоках живлення, що значно спрощує інфраструктур. У рисунку 1.3 представлено загальну модель побудови дротової LAN з використанням технології Ethernet.


Рисунок 1.3 — Структурна схема Ethernet-підключення в межах локальної мережі

### 1.3.2 Бездротові мережі (Wi-Fi) у сфері обслуговування

Бездротові технології, зокрема Wi-Fi (Wireless Fidelity), стали невід'ємною частиною мереж у закладах громадського харчування, таких як кафе чи ресторани. Вони дозволяють забезпечити підключення мобільних пристроїв відвідувачів (смартфонів, планшетів, ноутбуків), а також внутрішнього обладнання — наприклад, портативних терміналів, замовлень або камер відеоспостереження.

Wi-Fi працює за стандартами IEEE 802.11 і підтримує різні діапазони частот (2.4 ГГц та 5 ГГц). При правильному налаштуванні точок доступу можна досягти стабільного покриття у всіх функціональних зонах кафе. Окрім цього, реалізується сегментація трафіку між гостьовою мережею та службовою мережею персоналу для підвищення безпеки.

У таблиці 1.4 представлено порівняння основних характеристик технологій Ethernet і Wi-Fi, які застосовуються при побудові локальних мереж.

Таблиця 1.4 — Порівняння дротової та бездротової технології

| Характеристика | Ethernet | WiFi |
|---|---|---|
| Тип підключення | Дротове | Бездротове |
| Середовище передачі | Кручена пара, оптика | Радіохвилі |
| Швидкість | До 10 Гбіт/с | До 1.2 Гбіт/с (WiFi 6) |
| Надійність | Висока | Середня |
| Безпека | Вища (фізичний доступ) | Залежить від налаштувань WPA |
| Мобільність | Низька | Висока |
| Вартість інфраструктури | Вища | Нижча |

## 1.4 Технології маршрутизації

Маршрутизація — це процес передавання даних між різними мережами через спеціальні пристрої — маршрутизатори. Основна функція маршрутизатора полягає в аналізі IP-адреси призначення кожного пакета та визначенні найкращого маршруту для його доставки. У корпоративних, зокрема мультифілійних, мережах

правильно налаштована маршрутизація гарантує безперебійний обмін даними між сегментами мережі, серверами та користувачами.

Усі методи маршрутизації можна поділити на два основні типи: статична маршрутизація, коли всі шляхи задаються вручну, і динамічна маршрутизація, яка здійснюється автоматично за допомогою спеціальних протоколів. Залежно від складності, розміру та очікуваного зростання мережі, в реальних системах можуть використовуватись обидва підходи одночасно.

### 1.4.1 Статична маршрутизація

Статична маршрутизація полягає у ручному додаванні маршрутів до таблиці маршрутизації на кожному маршрутизаторі. Такий підхід зазвичай використовується в простих або стабільних мережах, де топологія рідко змінюється. У рисунку 1.4 зображено базову схему, у якій маршрутизатор пов’язує підмережі через статичні записи, додані вручну [8].

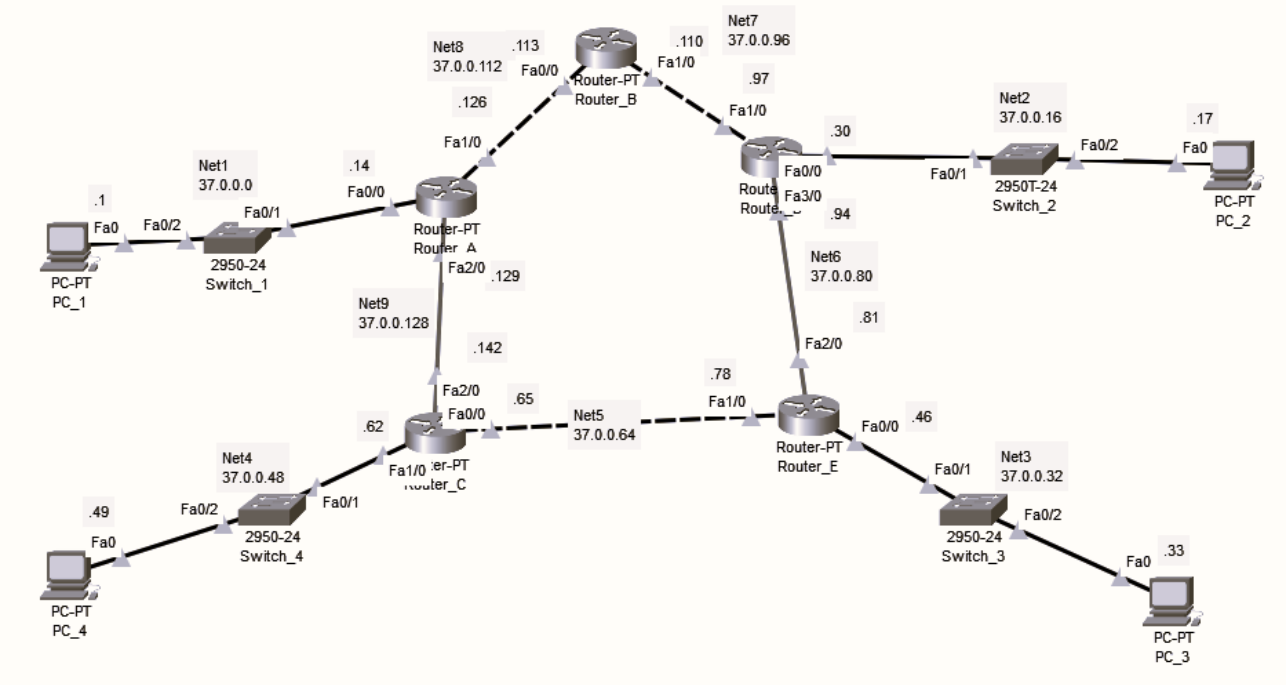


Рисунок 1.4 — Приклад маршрутизації між підмережами з використанням статичних маршрутів

Перевагою цього методу є повний контроль адміністратора над маршрутизацією, висока стабільність, передбачуваність роботи. Проте при збої

одного з вузлів або зміні структури мережі маршрути потрібно оновлювати вручну, що може ускладнювати адміністрування в масштабних проєктах.

### 1.4.2 Динамічна маршрутизація

Динамічна маршрутизація дозволяє пристроям самостійно обмінюватися маршрутною інформацією та будувати таблиці маршрутизації в автоматичному режимі. Цей підхід суттєво спрощує адміністрування великих мереж, дозволяє швидко реагувати на зміни топології, збої та появу нових сегментів. Найбільш відомими динамічними протоколами є RIP, EIGRP та OSPF.

RIP (Routing Information Protocol) — найпростіший протокол, що базується на кількості переходів (hops). Він підтримує до 15 переходів і підходить лише для невеликих мереж. Його основний недолік — повільна конвергенція та обмежена масштабованість.

EIGRP (Enhanced Interior Gateway Routing Protocol) — гібридний протокол, який використовує складніші метрики (затримку, пропускну здатність, надійність) для вибору маршруту. Він поєднує швидку конвергенцію та можливість тонкого налаштування маршрутів. EIGRP є власністю компанії Cisco, тому підтримується лише на пристроях Cisco.

OSPF (Open Shortest Path First) — протокол внутрішньої маршрутизації, який використовує алгоритм Дейкстри для визначення найкоротших шляхів. Його переваги — підтримка зон (area), швидка конвергенція, гнучкість та відкритий стандарт. OSPF дозволяє масштабувати маршрутизовану мережу завдяки ієрархічній побудові [7].

Кожен із протоколів динамічної маршрутизації має власні особливості застосування, залежно від типу мережі, її масштабів і вимог до швидкості реагування на зміни. Наприклад, RIP залишається простим у налаштуванні, проте поступається сучасним протоколам у продуктивності. EIGRP забезпечує кращу ефективність і гнучкість, особливо в мережах Cisco, однак є пропрієтарним. OSPF, навпаки, є відкритим стандартом і найчастіше використовується у корпоративних мережах завдяки швидкій конвергенції, підтримці ієрархічної структури та

широкій масштабованості.

Вибір протоколу маршрутизації завжди залежить від конкретних вимог: кількості маршрутизаторів, наявності кількох підмереж, необхідності балансування навантаження або резервування. Саме динамічні протоколи дозволяють зробити мережу не лише більш адаптивною до змін, а й стійкою до збоїв, що є критично важливим для забезпечення безперервної роботи сучасних інформаційних систем.. У таблиці 1.5 представлено ключові характеристики трьох найпоширеніших протоколів динамічної маршрутизації.

Таблиця 1.5 — Порівняння основних динамічних протоколів маршрутизації

| Протокол | Тип алгоритму | Максимальна кількість хопів | Швидкість конвергенції | Стандартизація | Підтримка зон |
|---|---|---|---|---|---|
| RIP | Вектор відстані | 15 | Повільна | Відкритий | Ні |
| EIGRP | Гібридний (DUAL) | 224 | Висока | Пропрієтарний | Частково |
| OSPF | Стан зв’язку | Без обмежень | Висока | Відкритий | Так |

## 1.5 Технологія VPN

У сучасних комп’ютерних мережах технологія VPN (Virtual Private Network) широко застосовується для побудови захищених з’єднань через загальнодоступні або ненадійні мережі, такі як Інтернет. Вона дозволяє створити логічно ізольовану мережу, у якій вузли можуть взаємодіяти так, наче вони підключені до єдиної локальної мережі. Основною перевагою VPN є забезпечення конфіденційності, цілісності та автентичності переданих даних.

Функціональність VPN базується на інкапсуляції пакетів у нові пакети з

додатковими заголовками, які дозволяють передавати інформацію у зашифрованому вигляді. Утворюється так званий тунель між двома або більше пристроями, що проходить поверх Інтернету або іншої відкритої мережі. Завдяки цьому організації можуть безпечно поєднувати віддалені офіси, філії або користувачів із головною інфраструктурою. У рисунку 1.5 представлено принцип роботи VPN.

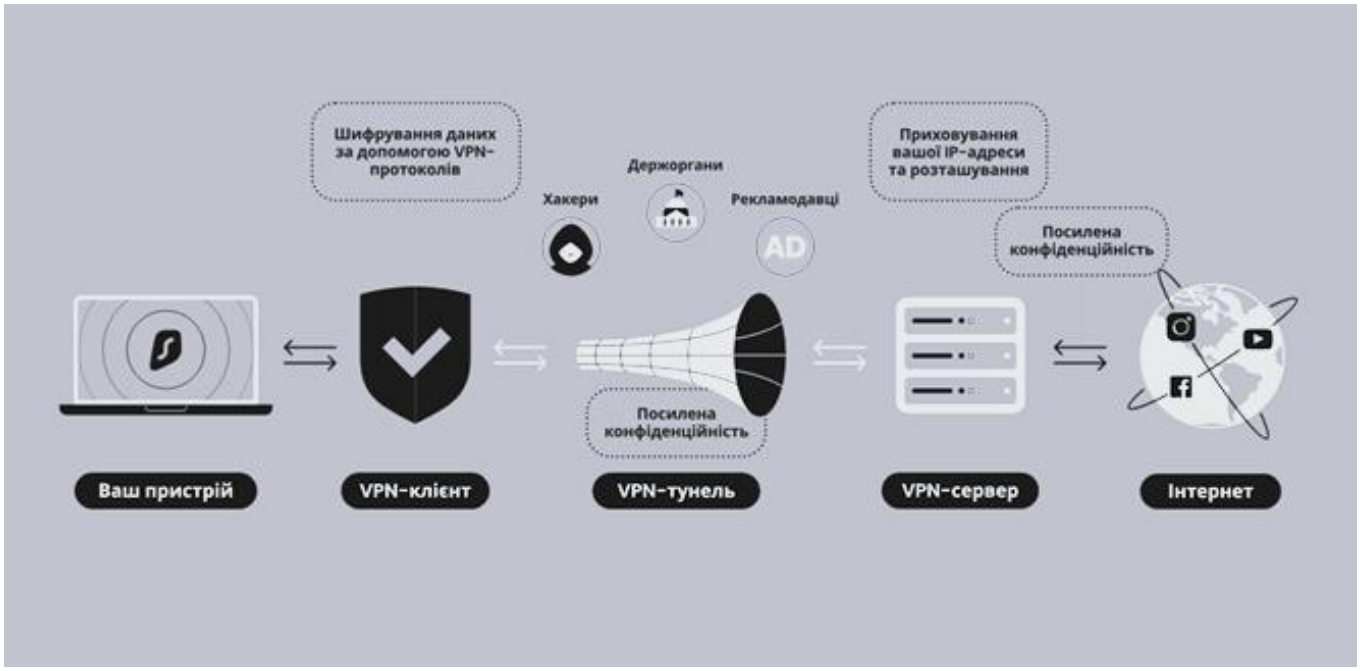


Рисунок 1.5 — Принцип роботи VPN

Серед найпоширеніших рішень VPN слід згадати GRE, який забезпечує логічне інкапсульоване з’єднання між пристроями. Він підтримує передавання різних типів трафіку, включаючи динамічні протоколи маршрутизації, але сам по собі не забезпечує шифрування. Саме тому GRE часто використовується в комбінації з IPsec, який додає шифрування та автентифікацію. Таке поєднання — GRE over IPsec — дозволяє забезпечити одночасно захист і функціональність. Ще одним популярним типом VPN є SSL/TLS-рішення, яке функціонує на рівні прикладного шару і дозволяє користувачам отримувати захищений доступ до веб-інтерфейсів внутрішніх сервісів через браузер [6].

Також широкого поширення набули такі рішення, як OpenVPN та WireGuard. Перший є гнучким і кросплатформним, активно використовується в багатьох

системах, тоді як другий — новіше рішення, оптимізоване для високої продуктивності та простоти налаштування. У певних випадках ще зустрічається L2TP або PPTP, проте вони поступово втрачають актуальність через обмежену безпеку. У таблиці 1.6 відображено порівняння найбільш поширених VPN-технологій за критеріями безпеки, продуктивності, сумісності з NAT та підтримки маршрутизації.

Таблиця 1.6 — Порівняння основних VPN-протоколів

| Протокол | Шифрування | Динамічна маршрутизація | Сумісність із NAT | Продуктивність | Коментарі |
|---|---|---|---|---|---|
| GRE | Немає | Так | Так | Висока | Потрібен додатковий захист |
| IPsec | Так | Ні (без GRE) | Обмежена | Висока | Забезпечує шифрування, але не підтримує маршрутизацію |
| GRE over IPsec | Так | Так | Так | Висока | Комбінує гнучкість GRE та IPsec |
| SSL VPN | Так | Ні | Так | Середня | Працює через HTTPS, зручний для користувачів |
| OpenVPN | Так | Обмежена | Так | Середня | Гнучкий, зручний у налаштуванні |
| WireGuard | Так | Обмежена | Так | Дуже висока | Новітній протокол із фокусом на продуктивність |

Загалом, технологія VPN стала основним інструментом для безпечної

організації міжмережевої взаємодії. Вона дозволяє не лише об’єднувати географічно розподілені структури, а й захищати доступ до корпоративних даних, зменшуючи ризики перехоплення чи втручання в трафік з боку третіх осіб [17].

## 1.6 NAT та DHCP: автоматизація налаштування мережі

Автоматизація процесів у комп’ютерних мережах є важливим кроком до спрощення адміністрування, зменшення кількості помилок при налаштуванні, а також до ефективного використання обмежених ресурсів. У цьому контексті ключову роль відіграють дві технології: NAT (Network Address Translation) і DHCP (Dynamic Host Configuration Protocol).

DHCP призначений для автоматичного надання IP-адрес клієнтам у мережі. Коли новий пристрій підключається до локальної мережі, він може автоматично отримати IP-адресу, маску підмережі, шлюз за замовчуванням та інші параметри без втручання адміністратора. Це дозволяє значно зменшити час на налаштування великих мереж і мінімізувати помилки при конфігурації вручну. DHCP також зручно використовувати в мережах, де пристрої часто змінюються або підключаються тимчасово, наприклад у готелях, кафе, навчальних закладах або офісах з гнучкими робочими місцями.

NAT, у свою чергу, дає змогу комп’ютерам внутрішньої приватної мережі взаємодіяти з публічною мережею Інтернет, навіть якщо у них немає глобально унікальних IP-адрес. Найпоширенішим варіантом NAT є PAT (Port Address Translation), який дозволяє багатьом внутрішнім пристроям одночасно використовувати одну публічну IP-адресу завдяки трансляції портів. Це особливо важливо в умовах обмеженого пулу публічних адрес. NAT також виконує функцію додаткового бар’єра безпеки, приховуючи структуру внутрішньої мережі від зовнішнього світу. Ці дві технології є фундаментальними для будь-якої сучасної мережі, особливо коли йдеться про оптимальне використання ресурсів та підвищення гнучкості адміністрування. На рисунку 1.6 відображено принцип роботи NAT.

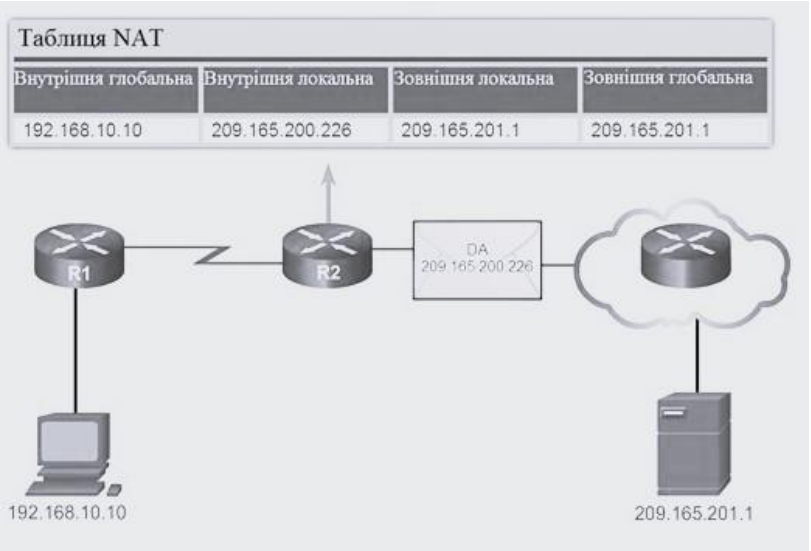


Рисунок 1.6 — Принцип роботи NAT

Вони часто працюють разом: NAT на межі мережі забезпечує вихід у глобальну мережу, тоді як DHCP забезпечує правильну роботу локальних хостів без ручного налаштування. У таблиці 1.7 наведено порівняльну характеристику DHCP і NAT за ключовими параметрами функціональності, призначення, рівня роботи в моделі OSI та основних переваг.

Таблиця 1.7 — Порівняння DHCP і NAT

| Параметр | DHCP | NAT |
|---|---|---|
| Призначення | Автоматичне надання IP-адрес та інших параметрів | Трансляція адрес для доступу до зовнішніх мереж |
| Рівень моделі OSI | Рівень прикладний (Application layer) | Рівень мережевий (Network layer) |
| Тип дії | Динамічне конфігурування клієнтів | Зміна IP-адреси в заголовках пакетів |
| Основна перевага | Спрощення адміністрування, гнучкість налаштування | Можливість економії публічних IP-адрес |

Продовження таблиці 1.7

| | | |
|---|---|---|
| Приклади застосування | Локальні мережі у підприємствах і організаціях | Вихід у Інтернет через один публічний інтерфейс |
| Взаємодія з клієнтами | Пряме: клієнт отримує параметри автоматично | Опосередкована: клієнти “не бачать” зовнішню мережу |

Завдяки використанню NAT і DHCP адміністратор мережі отримує ефективний інструмент для управління IP-адресами та маршрутизацією трафіку, що забезпечує стабільну та безпечну роботу як внутрішньої, так і зовнішньої мережевої взаємодії.

## 1.7 Захист мережевого обладнання: SSH, ACL, керування доступом

У сучасному цифровому середовищі, де комп’ютерні мережі є основою для обміну даними, надання послуг і комунікації, безпека мережевого обладнання посідає провідне місце. Навіть найефективніше налаштована інфраструктура може стати вразливою, якщо не захищено маршрутизатори, комутатори та сервери — ключові точки управління мережею. Саме тому впровадження комплексного підходу до безпеки на рівні обладнання є обов’язковою умовою стабільної роботи інформаційної системи [19].

Одним із основних засобів безпечного адміністрування мережевого обладнання є протокол SSH (Secure Shell).

Його призначення — забезпечити конфіденційне, цілісне та автентифіковане з’єднання між адміністратором і пристроєм. SSH використовує шифрування даних і методи криптографічної перевірки, що дозволяє уникнути таких загроз, як перехоплення паролів, підміна команд або несанкціоноване втручання в процес налаштування. На рисунку 1.7 відображено схему взаємодії адміністратора з мережевим обладнанням через SSH.


Рисунок 1.7 — Приклад реалізації SSH-доступу

Протокол SSH повністю замінює застарілий Telnet, який передавав дані відкритим текстом і був вкрай вразливим до атак типу “Man-in-the-Middle”. Сьогодні SSH є стандартом безпечного віддаленого керування маршрутизаторами Cisco, Mikrotik, серверними платформами Linux, BSD, а також обладнанням, що підтримує інтерфейси командного рядка.

Ще одним фундаментальним інструментом безпеки є ACL (Access Control List) — списки контролю доступу, які дозволяють задавати правила фільтрації трафіку. ACL можуть бути налаштовані як на вхідному, так і на вихідному інтерфейсі, визначаючи, які пакети дозволено або заборонено передавати далі. Наприклад, за допомогою ACL можна:

— обмежити доступ до маршрутизатора лише з певних IP-адрес або підмереж;

— заблокувати небажаний трафік ззовні;

— дозволити лише певні сервіси (наприклад, HTTP, DNS, SSH);

— заборонити пінг або доступ до керуючих портів з інтернету.

ACL бувають стандартні і розширені (можуть фільтрувати за IP-адресою призначення, портами, протоколами тощо). Цей механізм дозволяє реалізувати гнучку політику безпеки на маршрутизаторі [13].

Для забезпечення внутрішнього захисту важливо також правильно налаштувати аутентифікацію користувачів, які мають доступ до обладнання. У Cisco IOS та інших платформах можливо:

— створити окремі облікові записи для різних адміністраторів;

— призначити рівні привілеїв (наприклад, лише читання або повний доступ);

— обмежити вхід лише через певні інтерфейси (наприклад, тільки з локальної мережі).

Також для критичних змін у конфігурації рекомендовано використовувати аутентифікацію за паролем Enable або зовнішні сервери автентифікації (RADIUS, TACACS+), які дозволяють централізовано керувати правами доступу до обладнання.У таблиці 1.8 наведено характеристику основних механізмів захисту мережевого обладнання, їх призначення та область застосування.

Таблиця 1.8 — Основні засоби захисту мережевого обладнання

| Засіб захисту | Призначення | Приклад використання |
|---|---|---|
| SSH | Безпечне віддалене адміністрування | Підключення до маршрутизатора для конфігурації |
| ACL | Фільтрація вхідного/вихідного трафіку | Заборона доступу до внутрішньої мережі ззовні |
| Рівні доступу | Обмеження прав користувачів | Видача лише читання логів, без права змінювати налаштування |
| Фізичний захист | Запобігання несанкціонованому доступу до обладнання | Замикання комутаційної шафи |

Окрім основних механізмів, до практик безпеки на рівні мережевого обладнання також відносяться:

— фізичний захист, а саме обмеження фізичного доступу до маршрутизаторів і комутаторів (розміщення у закритих комутаційних шафах або серверних кімнатах);

— вимкнення невикористовуваних портів на комутаторах для запобігання несанкціонованого підключення;

— журналювання (logging), а саме збереження логів подій та дій користувачів з метою моніторингу та аудиту;

— регулярне оновлення прошивок маршрутизаторів і комутаторів для усунення вразливостей.

Комплексне застосування зазначених заходів дозволяє суттєво підвищити рівень безпеки мережевої інфраструктури та запобігти як внутрішнім, так і зовнішнім загрозам.

## 1.8 Технологія Frame Relay

Frame Relay — це технологія широкосмугової комутації пакетів, яка призначалася для передавання даних у мережах з середнім та високим навантаженням. Вона була особливо популярною в 1990-х і на початку 2000-х років як альтернатива дорогим виділеним лініям та складним протоколам, таким як X.25. Frame Relay дозволяла передавати дані з високою ефективністю та з мінімальними затримками, що зробило її однією з основних технологій для побудови корпоративних WAN-мереж того часу [5].

Технологія працює на другому рівні моделі OSI — канальному, де відбувається комутація кадрів (frame switching). Усі дані передаються у вигляді фреймів (кадрів), які містять заголовок з ідентифікатором з’єднання — DLCI (Data Link Connection Identifier). DLCI визначає логічний канал між двома пристроями у мережі Frame Relay. Саме через використання логічних, а не фізичних каналів, Frame Relay дає змогу встановлювати декілька віртуальних з’єднань (PVC — Permanent Virtual Circuits) на одному фізичному інтерфейсі. Frame Relay підтримує дві основні моделі з’єднання:

— Point-to-point (коли два пристрої з’єднані прямим віртуальним каналом,

що використовується для трафіку тільки між цими двома вузлами);

— Multipoint (коли декілька пристроїв розділяють один логічний сегмент мережі, що знижує потребу в окремих фізичних каналах для кожного з’єднання, але ускладнює маршрутизацію).

У Cisco-мережах (зокрема, в емуляторі Cisco Packet Tracer) Frame Relay часто реалізовується через маршрутизатор типу Cloud, до якого підключаються інші маршрутизатори через послідовні інтерфейси.

Frame Relay підтримує створення підінтерфейсів — окремих логічних інтерфейсів на базі одного фізичного, кожен з яких обробляє конкретне з’єднання. Це особливо зручно для реалізації точка-точка з’єднань із різними вузлами через єдиний фізичний порт.

Frame Relay не має вбудованого механізму перевірки доставки даних або повторної передачі, як це реалізовано в TCP або X.25. Ці функції покладаються на вищі рівні OSI-моделі. Через це технологія не забезпечує високий рівень надійності, але значно зменшує затримки передачі. На рисунку 1.8 представлено базову схему Frame Relay.

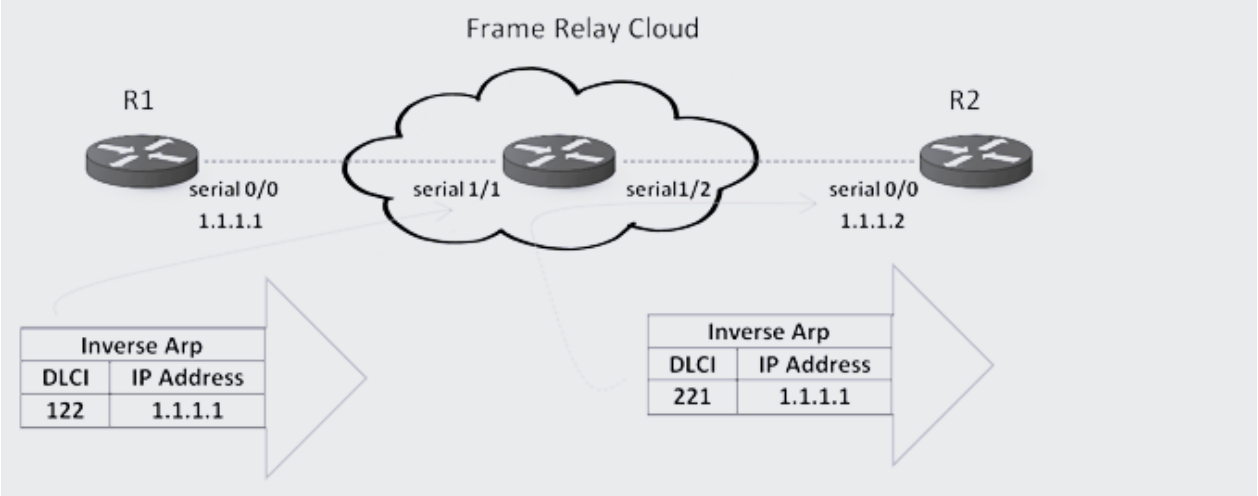


Рисунок 1.8 — Приклад реалізації технології Frame Relay

Однією з головних переваг технології є її масштабованість, адже завдяки підтримці мультиплексування логічних каналів на одному фізичному інтерфейсі, провайдер або корпоративна структура може об’єднувати десятки і сотні вузлів із мінімальними витратами. Frame Relay також дає змогу гнучко управляти

маршрутизацією та інтегруватися з протоколами рівня 3 (IP, IPX тощо).

Попри свою ефективність, Frame Relay має і недоліки: відсутність шифрування, відносно низький рівень безпеки, обмежена підтримка QoS і повна залежність від провайдера. З розвитком VPN, MPLS та оптоволоконних технологій Frame Relay поступово вийшла з ужитку, однак її моделювання залишається корисним у навчальних цілях. У таблиці 1.9 наведено ключові характеристики Frame Relay, MPLS і VPN, що дає змогу оцінити ефективність та актуальність кожної з технологій у різних сценаріях застосування.

Таблиця 1.9 — Порівняння Frame Relay з іншими WAN-технологіями

| Технологія | Рівень OSI | Тип з’єднання | Надійність | Гнучкість | Сфера застосування |
|---|---|---|---|---|---|
| Frame Relay | Канальний | PVC (точка-точка, багатоточкове) | Середня | Висока | Навчальні мережі, старі WAN-мережі |
| MPLS | Мережевий | Комутація за мітками (labels) | Висока | Висока | Великі підприємства, провайдери |
| VPN | Транспортний /Мережний | Тунелювання через публічну мережу | Висока | Дуже висока | Сучасні корпоративні з’єднання |

# 2 АНАЛІЗ ТА ОБҐРУНТУВАННЯ ВИБОРУ РІШЕНЬ

## 2.1 Топологія та характеристика мережі кафе «O'CAKE»

Комп'ютерна мережа, розроблена для потреб мережі кафе «O'CAKE», має на меті забезпечити централізоване управління усіма філіями, стабільний обмін інформацією між ними, безпечний доступ до внутрішніх ресурсів і ефективну роботу клієнтських пристроїв. Усього проєкт охоплює чотири філії, три з яких є віддаленими точками обслуговування клієнтів, а перша філія виконує роль головного офісу з сервером, маршрутизатором центрального рівня та єдиною точкою обміну з усіма іншими закладами.

Мережева архітектура має ієрархічну структуру, де головна філія (філія 1) виконує роль центру керування, обліку та баз даних, а решта філій функціонують як клієнтські вузли в системі. Зв'язок між філіями реалізовано за допомогою технології Frame Relay, яка дозволяє побудувати логічно розділену, проте централізовано керовану WAN-мережу з точкою доступу в центрі (hub-and-spoke).

Для захисту даних при передаванні між філіями використовуються GRE-тунелі, захищені протоколом IPsec. Це дозволяє організувати логічні VPN-з'єднання між головною філією та кожною з інших трьох, що дає змогу створити ізольований та безпечний канал для службової інформації. Використання GRE дозволяє інкапсулювати маршрутизований трафік (зокрема OSPF), що не підтримується нативно в IPsec.

Локальна мережа кожної філії побудована на основі Ethernet-технології, що дозволяє зручно сегментувати внутрішній трафік. У кожному закладі встановлено комутатор, який з'єднує всі стаціонарні пристрої: POS-термінали, офісні ПК, принтери, сервери. Також реалізовано бездротову інфраструктуру Wi-Fi для підключення ноутбуків персоналу, мобільних пристроїв, а за потреби — й гостей закладу. Для ізоляції гостьового та службового трафіку в точках доступу передбачено використання окремих VLAN або списків контролю доступу (ACL).

Сервери відіграють важливу роль у забезпеченні послуг та централізованого зберігання даних. У головній філії встановлено сервер із операційною системою Debian, на якому працює служба MariaDB, а також інструмент адміністрування

phpMyAdmin, що дозволяє централізовано зберігати й опрацьовувати інформацію з усіх закладів. Окремо в схемі Cisco Packet Tracer передбачено сервер, який виконує роль DNS-сервера, забезпечуючи розпізнавання доменних імен у межах всієї мережі. DHCP-сервери реалізовано безпосередньо на маршрутизаторах, що забезпечує динамічне надання IP-адрес у кожній філії. Також маршрутизатори забезпечують SSH-доступ, що дозволяє адміністраторам віддалено підключатись до пристроїв для конфігурації та моніторингу.

Кожна філія має свою унікальну IP-підмережу, що дозволяє ефективно маршрутизувати трафік, уникати конфліктів і забезпечувати ізоляцію. Для маршрутизації між підмережами використовується протокол OSPF, що автоматично оновлює маршрути при зміні структури мережі або відмові окремих вузлів. На рисунку 2.1 зображено загальну топологію комп'ютерної мережі кафе «O'CAKE», включаючи головну філію, три віддалені філії, хмару Frame Relay, VPN-тунелі та мережеві пристрої.

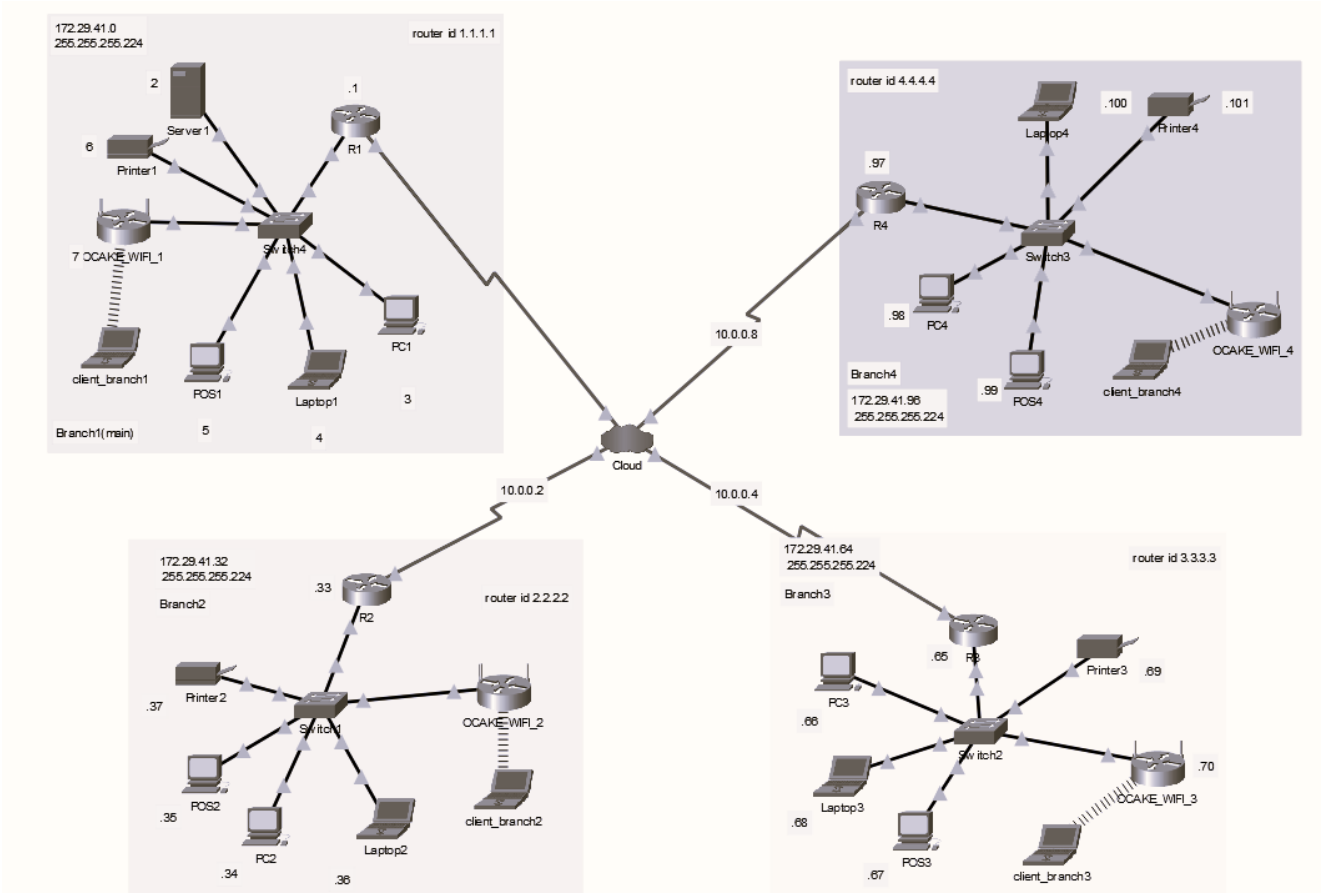


Рисунок 2.1 – Загальна топологія мережі кафе «O'CAKE»

## 2.2 Вимоги до мережі та обґрунтування обраної архітектури

Мережева інфраструктура для мережі закладів «O’CAKE» повинна відповідати сучасним вимогам надійності, масштабованості, безпеки та зручності в адмініструванні. Усі філії кафе мають бути з’єднані в єдину логічну мережу, що дозволить централізовано керувати сервісами, забезпечити захищений обмін даними, організувати стабільний міжфілійний зв’язок, а також надати клієнтам доступ до локального Wi-Fi.

Усі пристрої в межах філій отримують статичні IP-адреси, що дозволяє точно контролювати адресний простір, зменшує ризики конфліктів IP та спрощує керування політиками доступу (наприклад, через списки доступу ACL). Разом із цим, DHCP-сервери реалізовані на маршрутизаторах, однак їхня роль обмежується динамічною видачею IP-адрес лише для клієнтів Wi-Fi — наприклад, для ноутбуків користувачів, які підключаються через точки доступу у залі обслуговування.

Мережева архітектура передбачає чіткий розподіл між локальними (LAN) і глобальними (WAN) сегментами. Для зв’язку між філіями використовується технологія Frame Relay, що моделює реальне середовище WAN-з’єднань через хмарну інфраструктуру. Для забезпечення безпечного обміну даними між філіями реалізовано тунелювання за допомогою GRE over IPsec, що забезпечує як інкапсуляцію маршрутів, так і шифрування даних.

Передбачено виділення окремого DNS-сервера, розміщеного на сервері у головній філії. Він відповідає за трансляцію доменних імен у локальній мережі. Протокол SSH використовується для захищеного віддаленого керування маршрутизаторами.

Обрана архітектура побудована на динамічному маршрутизуванні з використанням OSPF, що забезпечує ефективне й адаптивне оновлення маршрутів між філіями. Такий підхід дозволяє масштабувати мережу, автоматично враховувати зміни в топології та зменшувати затримки при маршрутизації трафіку.

Таким чином, архітектура відповідає ключовим вимогам:

— захищеність і стабільність з’єднань між філіями;

— ефективне управління IP-адресним простором;

— підтримка мобільних пристроїв клієнтів;

— централізоване управління сервісами та політиками доступу;

— простота масштабування в разі відкриття нових філій.

У таблиці 2.1 наведено основні технічні вимоги, яким має відповідати проєктована мережева інфраструктура кафе «O’CAKE» для забезпечення стабільної роботи сервісів та безпечного обміну даними між філіями.

Таблиця 2.1 — Технічні вимоги до мережі кафе «O’CAKE»

| № | Вимога | Обґрунтування |
|---|---|---|
| 1 | Надійний міжфілійний зв’язок | Забезпечення стабільної роботи бізнес-процесів |
| 2 | Захищене передавання даних | Реалізація VPN-тунелів з шифруванням IPsec |
| 3 | Статична IP-адресація для ключових вузлів | Спрощення адміністрування та безпеки |
| 4 | DHCP лише для Wi-Fi-клієнтів | Автоматична видача IP-адрес ноутбукам клієнтів |
| 5 | Централізоване керування доменними іменами | DNS-сервер на головному сервері |
| 6 | Захищене адміністрування обладнання | Підключення по SSH до маршрутизаторів |
| 7 | Масштабованість архітектури | Можливість підключення нових філій без порушення логіки мережі |

## 2.3 Розподіл IP-адресного простору між філіями

Для організації мережевої інфраструктури мережі кафе «O’CAKE» було зарезервовано адресний простір із приватного діапазону класу B — 172.29.0.0/16, що забезпечує значний запас підмереж та дозволяє гнучко масштабувати архітектуру у майбутньому. В рамках проєкту реалізовано чіткий ієрархічний розподіл IP-адресного простору залежно від типу мережі: локальні мережі філій

(LAN), глобальні з’єднання між маршрутизаторами (WAN), та захищені VPN-тунелі (VPN).Такий поділ дозволяє:

— централізовано керувати адресами у великих мережах;

— легко фільтрувати трафік за мережевими діапазонами;

— спрощувати маршрутизацію через агрегування підмереж;

— передбачити резерв на майбутнє розширення або інтеграцію додаткових філій.

У кожній філії реалізовано окрему внутрішню підмережу для підключення робочих пристроїв — POS-систем, офісних ноутбуків, принтерів, точок доступу Wi-Fi тощо. Для цих цілей використано підмережі з префіксом /27, які надають по 30 корисних IP-адрес. Такої кількості достатньо для поточних потреб філій, при цьому зберігається певний резерв для розширення.У таблиці 2.2 представлено розподіл IP-підмереж між філіями для локального трафіку. Зазначено обраний префікс, кількість доступних IP-адрес у кожній підмережі та кількість фактично задіяних адрес.

Таблиця 2.2 — Розподіл IP-адрес у локальних мережах

| Філія | Підмережа | Префікс | Кількість корисних IP | Задіяно IP |
|---|---|---|---|---|
| 1 | 172.29.41.0 | /27 | 30 | 8 |
| 2 | 172.29.41.32 | /27 | 30 | 7 |
| 3 | 172.29.41.64 | /27 | 30 | 7 |
| 4 | 172.29.41.96 | /27 | 30 | 7 |

Для забезпечення взаємодії між філіями використовуються point-to-point з’єднання через технологію Frame Relay, реалізовану між маршрутизаторами. У таких типах з’єднань доцільно використовувати підмережі з префіксом /30, що надають 2 корисні IP-адреси — по одній для кожного кінця лінку. Це мінімізує витрати адресного простору та унеможливлює широкомовні запити.У таблиці 2.3 наведено підмережі, зарезервовані для WAN-з’єднань між філіями. Показано кількість доступних адрес і їх фактичне використання.

Таблиця 2.3 — Розподіл IP-адрес у глобальних з’єднаннях

| Підмережа | Префікс | Кількість корисних IP | Задіяно IP |
|---|---|---|---|
| 10.0.0.0 | /30 | 2 | 2 |
| 10.0.0.4 | /30 | 2 | 2 |
| 10.0.0.8 | /30 | 2 | 2 |

Для захищеного обміну даними між філіями реалізовано VPN-з’єднання GRE over IPsec. Для тунелів використано окремі підмережі, також із префіксом /30, які дозволяють адресувати кінцеві точки тунелю з мінімальними витратами простору. Окреме виділення VPN-підмереж дозволяє легко фільтрувати тунельний трафік, контролювати безпеку та спростити діагностику. У таблиці 2.4 представлено підмережі, зарезервовані для тунельних VPN-з’єднань між філіями. Для кожної підмережі зазначено обсяг доступних IP-адрес та кількість фактично задіяних.

Таблиця 2.4 — Розподіл IP-адрес у VPN-з’єднаннях

| Підмережа | Префікс | Кількість корисних IP | Задіяно IP |
|---|---|---|---|
| 192.168.1.0 | /30 | 2 | 2 |
| 192.168.2.0 | /30 | 2 | 2 |
| 192.168.3.0 | /30 | 2 | 2 |

## 2.4 Обґрунтування вибору логічної топології та VPN-рішення

Для забезпечення гнучкої та надійної маршрутизації між філіями мережі кафе «O’CAKE» було прийнято рішення використати логічну топологію «зірка», у якій головна філія (Філія 1) виконує роль центрального вузла. Саме через неї проходить весь трафік між філіями, що значно спрощує адміністрування, моніторинг та

контроль доступу.

На наступному рисунку зображено VPN-схему логічних тунелів між маршрутизаторами. Стрілками позначено напрямок GRE over IPsec тунелів, а також відповідні IP-адреси. На рисунку 2.4.1 зображено логічну схему VPN-з’єднань типу GRE over IPsec між головним маршрутизатором (R1) та віддаленими філіями (R2, R3, R4). Підписано інтерфейси Tunnel1–Tunnel3, їхні IP-адреси, а також фізичні адреси інтерфейсів Frame Relay (Serial0/1/0.x).

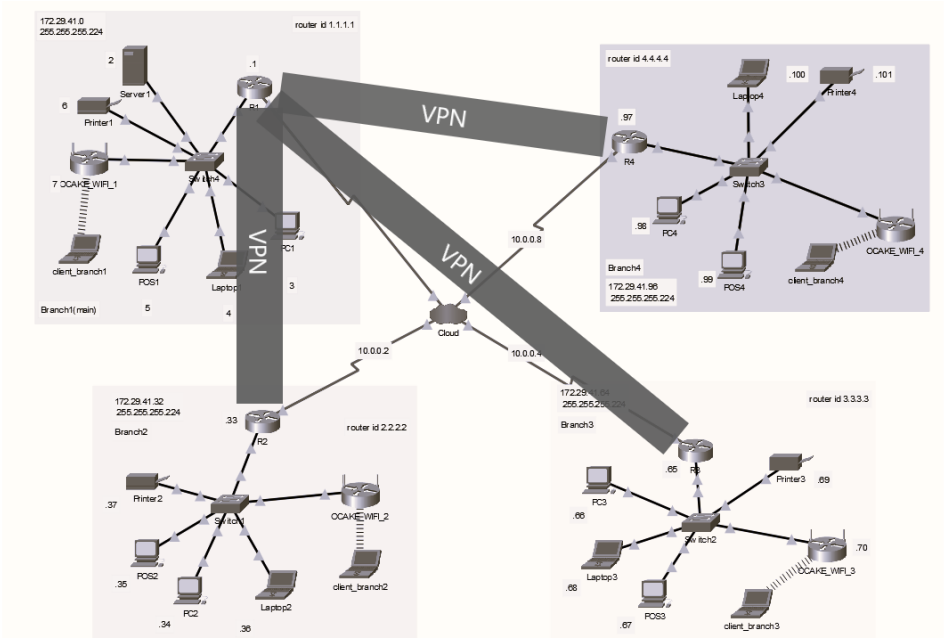


Рисунок 2.2 — VPN-з’єднання між філіями через GRE over IPsec

Логічні з’єднання між філіями реалізовані через інкапсульовані VPN-тунелі поверх каналу Frame Relay, налаштованого через Cloud-модуль у середовищі Cisco Packet Tracer.

Для реалізації захищеного обміну даними між філіями було обрано технологію GRE over IPsec. Таке рішення дозволяє:

— інкапсулювати пакети будь-якого протоколу (через GRE);

— забезпечити конфіденційність, цілісність та автентичність даних (через IPsec);

— передавати динамічні маршрути протоколу OSPF між філіями в зашифрованому тунелі.

На кожному маршрутизаторі створено окремий GRE-тунель для з’єднання з центральним вузлом:

— Tunnel1 між R1 і R2 через підмережу 192.168.1.0/30;

— Tunnel2 між R1 і R3 через підмережу 192.168.2.0/30;

— Tunnel3 між R1 і R4 через підмережу 192.168.3.0/30.

Щоб продемонструвати принцип конфігурування GRE over IPsec, нижче наведено фрагмент налаштування VPN-тунелю Tunnel1 між маршрутизаторами R1 та R2. Повна конфігурація включає визначення політик ISAKMP, створення ACL, GRE-тунель та прив’язку IPsec. У лістингу 2.1 показано фрагмент конфігурації VPN між R1 і R2. Зокрема, наведено створення GRE-тунелю Tunnel1 з IP-адресою 192.168.1.1/30 та налаштування IPsec з ACL, що дозволяє лише GRE-трафік.

Лістинг 2.1 — Фрагмент налаштування GRE over IPsec між R1 і R2

```
crypto isakmp policy 10
encr aes
authentication pre-share
group 2
crypto isakmp key VPNKEY address 10.0.0.2
access-list 100 permit gre host 10.0.0.1 host 10.0.0.2
interface Tunnel1
ip address 192.168.1.1 255.255.255.252
tunnel source Serial0/1/0.101
tunnel destination 10.0.0.2
crypto map VPNMAP 10 ipsec-isakmp
set peer 10.0.0.2
set transform-set TS
match address 100
interface Serial0/1/0
crypto map VPNMAP
```

Подібним чином реалізовано тунелі Tunnel2 (до R3) та Tunnel3 (до R4), з окремими підмережами 192.168.2.0/30 та 192.168.3.0/30 відповідно.

## 2.5 Вибір мережевого обладнання

Для побудови корпоративної мережі кафе «O’CAKE» було підібрано мережеве обладнання, що відповідає функціональним вимогам і масштабу мережі. Усі пристрої моделюються в середовищі Cisco Packet Tracer на основі підтримуваних моделей маршрутизаторів, комутаторів, бездротових точок

доступу, серверів та робочих станцій.

### 2.5.1 Комутатори та маршрутизатори

У кожній філії використано один маршрутизатор Cisco, який виконує роль основного шлюзу, реалізує функції маршрутизації, NAT, ACL, VPN, DHCP та SSH-доступу. Головна філія (філія 1) має маршрутизатор Cisco 1841, оскільки саме до нього підключаються всі інші філії через GRE over IPsec VPN. В інших філіях використано також маршрутизатори серії Cisco, сумісні з IPsec та Frame Relay.

Кожна філія також обладнана одним керованим комутатором рівня 2 для підключення локальних пристроїв. У таблиці 2.5 представлено перелік маршрутизаторів та комутаторів які використовуються у філіях.

Таблиця 2.5 — Маршрутизатори та комутатори у філіях

| Філія | Маршрутизатор | Комутатор |
|---|---|---|
| 1 | Cisco 1841 | Cisco 2960 |
| 2 | Cisco 1841 | Cisco 2960 |
| 3 | Cisco 1841 | Cisco 2960 |
| 4 | Cisco 1841 | Cisco 2960 |

Маршрутизатори філій підключено через Frame Relay до Cloud-мережі, а тунелі VPN реалізовано за допомогою GRE over IPsec, що забезпечує захищену передачу даних та підтримку динамічної маршрутизації OSPF.

### 2.5.2 POS-системи, ноутбуки, комп’ютери, точки доступу

У кожній філії використовуються типові користувацькі пристрої, які забезпечують обслуговування клієнтів та адміністративні функції. Зокрема, передбачено:

— 1 POS-термінал;

— 1 ноутбук;

— 1 принтер;

— 1 звичайний ПК;

— 1 точка доступу Wi-Fi.

Клієнтські Wi-Fi-пристрої, що змінюються, у таблиці не враховуються, оскільки вони отримують IP-адреси динамічно через DHCP і не є частиною фіксованої інфраструктури.

Основні пристрої мають статичні IP-адреси й працюють у межах локальних підмереж філій. Вони також використовуються для адміністративних завдань, зокрема для доступу до серверів, перевірки з'єднань по SSH або тестування VPN-тунелів.

### 2.5.3 Сервер на Debian для бази даних

Для зберігання інформації про замовлення, меню, клієнтів тощо використовується сервер на базі Debian GNU/Linux, розташований у головній філії (філія 1). Він розгорнутий у окремому серверному сегменті та працює з СУБД MariaDB з веб-інтерфейсом phpMyAdmin, що полегшує адміністрування. У таблиці 2.6 вказано основні характеристики сервера бази даних.

Таблиця 2.6 — Основні характеристики сервера бази даних

| Параметр | Значення |
|---|---|
| ОС | Debian GNU/Linux |
| СУБД | MariaDB |
| Інтерфейс адміністрування | phpMyAdmin |
| Розташування | Філія 1 |
| IP-адреса | 172.29.41.2 |

Сервер має статичну IP-адресу й розміщується в захищеному сегменті головної LAN. Доступ до нього обмежується лише пристроями з інших філій через тунель VPN, а також контролюється ACL і NAT

Сервер виконує лише функції бази даних і не дублює DHCP або DNS-служби.

Останні реалізовано відповідно на маршрутизаторах (DHCP) і окремому сервері в Cisco Packet Tracer (DNS).

## 2.6 Проєктування логічної схеми мережі

Логічна схема корпоративної мережі кафе «O'CAKE» розроблена з урахуванням потреб масштабованості, централізованого управління, захисту каналів зв'язку та розподілу ролей між філіями. Уся мережа побудована за принципом ієрархічної топології з центральною філією, яка виконує роль головного вузла зв'язку та центру обробки даних.У головній філії розміщено:

— сервер бази даних (на базі Debian з встановленими MariaDB та phpMyAdmin);

— DNS-сервер, який забезпечує локальну трансляцію імен;

— маршутизатор головної філії, що має інтерфейси для підключення до мережі Frame Relay через Cloud;

— VPN-тунелі GRE over IPsec, які встановлюються до кожної з філій (R2, R3, R4);

— статичну IP-адресацію всіх стаціонарних пристроїв (POS, ноутбук, комп'ютер).

Централізація критичних служб (DNS, база даних) дозволяє спростити резервне копіювання, адміністрування та оновлення.

Для побудови захищених каналів між головною філією та віддаленими філіями використано технологію GRE over IPsec поверх Frame Relay. Кожен тунель має власну підмережу:

— R1 ↔ R2: 192.168.1.0/30;

— R1 ↔ R3: 192.168.2.0/30;

— R1 ↔ R4: 192.168.3.0/30.

Через ці тунелі передається не лише дані користувачів, а й OSPF-маршрути, що дає змогу кожному маршрутизатору мати актуальні дані про всі LAN-підмережі.

Кожна з чотирьох філій має власну підмережу класу /27 для підключення

внутрішніх пристроїв. У кожній філії є:

— POS-термінал;

— ноутбук адміністратора;

— персональний комп’ютер;

— точка доступу Wi-Fi, яка обслуговує клієнтські пристрої.

Загалом, IP-адреси для цих пристроїв надаються статично, за винятком Wi-Fi-клієнтів, для яких маршрутизатори виконують роль DHCP-серверів. Уся адресація в мережі продумана з урахуванням ієрархії:

— LAN-підмережі мають чітке розмежування між філіями (172.29.41.0/27 і далі);

— VPN- і WAN-підключення мають окремі діапазони (192.168.x.0/30 для VPN, 10.0.0.x/30 для Frame Relay).

Завдяки такій побудові логічної схеми забезпечено:

— ізоляцію та безпеку між філіями;

— можливість масштабування без зміни основної структури;

— зручне адміністрування через SSH і DNS;

— централізований доступ до бази даних і можливість легко реалізувати політику доступу.

# 3 РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ МЕРЕЖІ

## 3.1 Налаштування мережі головної філії

У головній філії розташовано центральний маршрутизатор R1, який відповідає за маршрутизацію, VPN-підключення до інших філій, DHCP, DNS-настройку для локальних клієнтів та захищене адміністрування. У цьому підпункті розглянуто налаштування основних мережевих функцій. До маршрутизатора R1 підключено кілька інтерфейсів:

— FastEthernet0/1;

— Loopback0;

— Serial0/1/0.101,Serial0/1/0.102, Serial0/1/0.103;

— Tunnel1, Tunnel2, Tunnel3.

У рисунку 3.1 показано підключення маршрутизатора R1 до локальної мережі та WAN

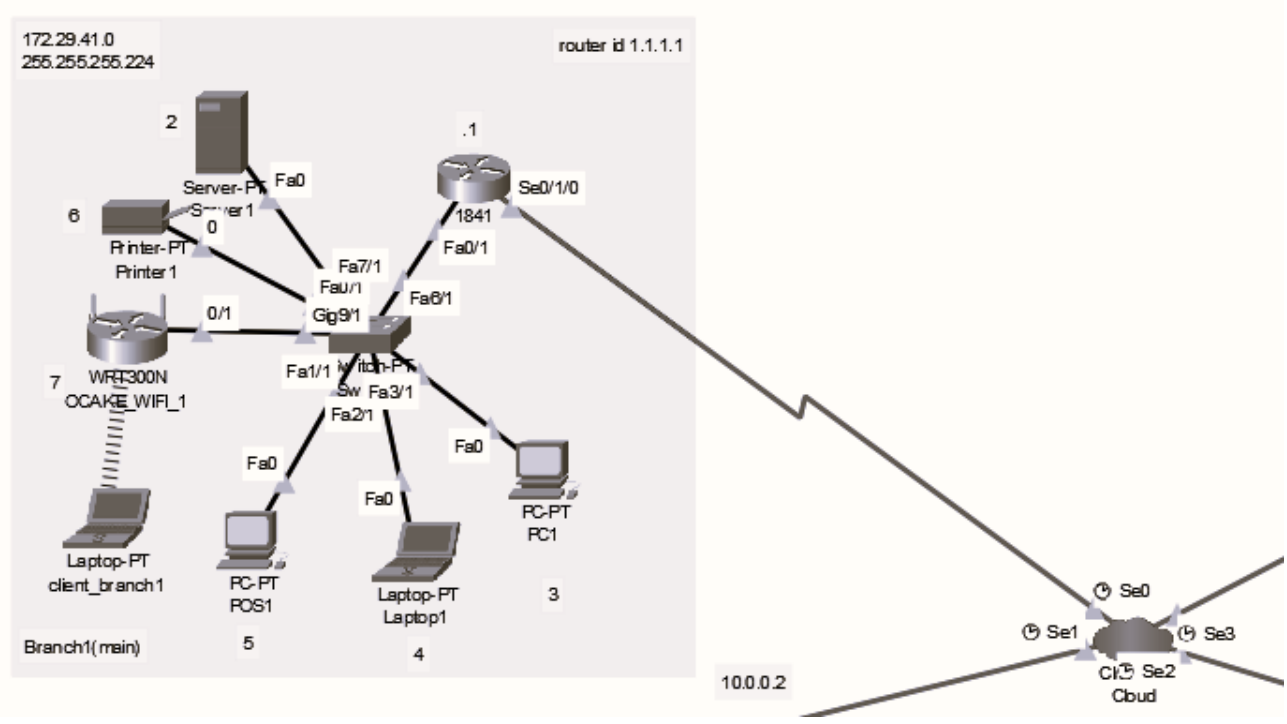


Рисунок 3.1 — Підключення маршрутизатора R1 до локальної мережі та WAN

Для маршрутизації між філіями використовується протокол OSPF. Ідентифікатором маршрутизатора встановлено адресу Loopback0 — 1.1.1.1. У

лістингу 3.1 представлено конфігурацію протоколу OSPF на маршрутизаторі R1.

Лістинг 3.1 — Налаштування OSPF на R1

```
router ospf 1
 router-id 1.1.1.1
 log-adjacency-changes
 network 172.29.41.0 0.0.0.31 area 0
 network 10.0.0.0 0.0.0.3 area 0
 network 10.0.0.4 0.0.0.3 area 0
 network 10.0.0.8 0.0.0.3 area 0
```

DHCP використовується лише для клієнтів Wi-Fi, які підключаються до головної філії. У діапазоні 172.29.41.0/27 частина адрес зарезервована, решта — видається автоматично. У лістингу 3.2 показано налаштування DHCP-сервера на R1.

Лістинг 3.2 — Налаштування DHCP на R1

```
ip dhcp excluded-address 172.29.41.1 172.29.41.10
ip dhcp pool LAN1
 network 172.29.41.0 255.255.255.224
 default-router 172.29.41.1
 dns-server 172.29.41.2
```

У головній філії встановлено сервер DNS з IP-адресою 172.29.41.2, що обслуговує домен ocake.com.vn. Маршрутизатор R1 направляє всі DNS-запити на цю адресу.

Між маршрутизатором R1 і філіями створено три GRE-тунелі. Tunnel1 — до R2, Tunnel2 — до R3, Tunnel3 — до R4. Тунелі мають власні IP-адреси в окремих VPN-підмережах. У лістингу 3.3 наведено приклад налаштування GRE-тунелю Tunnel1 до маршрутизатора R2.

Лістинг 3.4 — Налаштування GRE-тунелю Tunnel1

```
interface Tunnel1
 ip address 192.168.1.1 255.255.255.252
 mtu 1476
 tunnel source Serial0/1/0.101
 tunnel destination 10.0.0.2
```

Кожен тунель захищено IPsec-трафіком з використанням ISAKMP, шифрування AES та попередньо встановленого ключа VPNKEY. Для кожного тунелю використовується окремий peer. У лістингу 3.4 представлено конфігурацію

ISAKMP та IPsec transform set.

Лістинг 3.5 — Налаштування IPsec на R1

```
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
crypto isakmp key VPNKEY address 10.0.0.2
crypto isakmp key VPNKEY address 10.0.0.6
crypto isakmp key VPNKEY address 10.0.0.10
crypto ipsec transform-set TS esp-aes esp-sha-hmac
```

Для захищеного адміністрування активовано SSH-доступ. Створено локального адміністратора adminr1, обмежено час сесії та дозволено лише SSH-підключення. У лістингу 3.6 наведено налаштування доступу по SSH.

Лістинг 3.6 — Налаштування SSH-доступу до R1

```
username adminr1 privilege 15 secret <admin1>
line vty 0 4
 exec-timeout 5 0
 login local
 transport input ssh
```

У рисунку 3.2 показано вікно CLI з демонстрацією SSH-доступу до R1.

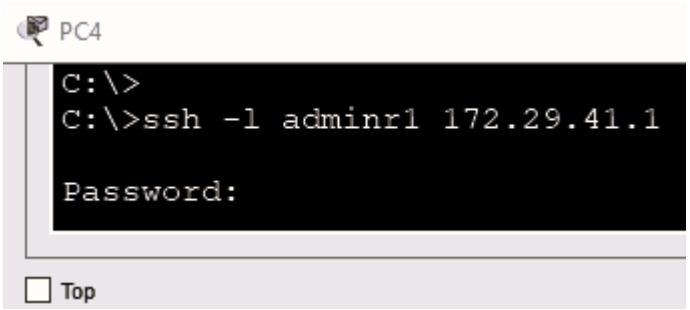


Рисунок 3.2 — Вікно CLI з демонстрацією SSH-доступу до R1

## 3.2 Розгортання мережі інших філій

Кожна з філій мережі кафе «O’CAKE» (R2, R3, R4) реалізована з типовою структурою. Основу архітектури складають маршрутизатор Cisco 1841, комутатор, точка доступу Wi-Fi, принтер, POS-термінал, стаціонарний ПК персоналу та ноутбук клієнта, підключений через точку доступу. Такий набір обладнання забезпечує виконання щоденних завдань філії: обслуговування клієнтів, друк чеків,

касове обслуговування, адміністрування та клієнтський Wi-Fi-доступ.

Усі філії мають підключення до головної філії через VPN-тунелі GRE over IPsec, які проходять поверх мережі Frame Relay. У межах кожної філії реалізовано окрему LAN-підмережу, а також одна WAN-підмережа між філією та головним офісом. Для маршрутизації використовується OSPF із налаштованими loopback-інтерфейсами як router-id.

DNS-запити в усіх філіях скеровуються на центральний DNS-сервер у головному офісі за адресою 172.29.41.2, де обслуговується доменне ім’я ocake.com.vn. DHCP-сервер на маршрутизаторі кожної філії забезпечує автоматичне налаштування клієнтських пристроїв, зокрема ноутбуків, що підключаються через Wi-Fi. Нижче у таблиці 3.1 подано поділ WAN- і LAN-мереж між філіями:

Таблиця 3.1 — WAN- і LAN-мережі філій 2,3,4

| Філія | WAN-підмережа | IP на маршрутизаторі | LAN-підмережа | IP шлюзу |
|---|---|---|---|---|
| 2 | 10.0.0.0/30 | 10.0.0.2 | 172.29.41.0/27 | 172.29.41.1 |
| 3 | 10.0.0.4/30 | 10.0.0.6 | 172.29.41.64/27 | 172.29.41.65 |
| 4 | 10.0.0.8/30 | 10.0.0.10 | 172.29.41.96/27 | 172.29.41.97 |

Для кожної філії реалізовано налаштування loopback-інтерфейсу з унікальною IP-адресою для використання як router-id у OSPF. П Налаштування Loopback0 на маршрутизаторі R3 показано у лістингу 3.7.

Лістинг 3.7 — Налаштування Loopback0 на маршрутизаторі R3

```
interface Loopback0
 ip address 3.3.3.3 255.255.255.255
```

Далі на маршрутизаторі вмикається протокол OSPF, додаються відповідні LAN- та WAN-мережі. У лістингу 3.8 відображено налаштування OSPF на маршрутизаторі R3

Лістинг 3.6 — Налаштування OSPF на маршрутизаторі R3

```
router ospf 1
 router-id 3.3.3.3
 network 172.29.41.64 0.0.0.31 area 0
 network 10.0.0.4 0.0.0.3 area 0
```

На рисунку 3.3 зображено локальну топологію мережі філії R3. У ній реалізовано типовий набір пристроїв: маршрутизатор, комутатор, POS-термінал, принтер, персональний комп'ютер персоналу, точка доступу Wi-Fi, а також ноутбук клієнта, що під'єднується через бездротову мережу. Уся локальна мережа філії працює в межах підмережі 172.29.41.64/27. Підключення до головного офісу реалізовано через VPN-тунель GRE over IPsec поверх Frame Relay у WAN-підмережі 10.0.0.4/30.

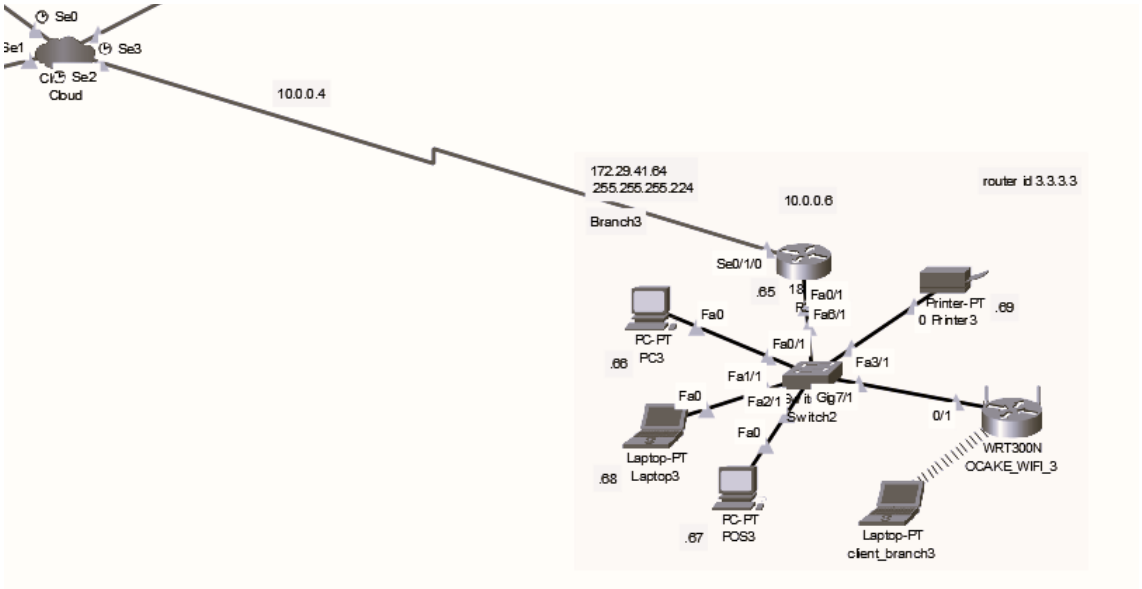


Рисунок 3.3 — Топологія локальної мережі філії R3

## 3.3 Організація WAN-з'єднань за допомогою Frame Relay

Для реалізації міжфілійного зв'язку у мережі кафе «O'CAKE» використано технологію Frame Relay з топологією типу "зірка". Центральна філія відіграє роль хабу, а маршрутизатори інших філій — спиць. Всі маршрутизатори підключаються до Cloud, який емулює провайдера Frame Relay у середовищі Cisco Packet Tracer

На R1 використовується інтерфейс Serial0/1/0, на якому створено три підінтерфейси типу point-to-point — по одному для кожної філії. Кожен

підінтерфейс має власну IP-адресу та відповідний номер DLCI. У таблиці 3.2 наведено конфігурацію WAN-інтерфейсів маршрутизаторів та їхнє призначення.

Таблиця 3.2 — Налаштування WAN-інтерфейсів Frame Relay

| Філія | Інтерфейс на R1 | IP-адреса R1 | Інтерфейс на філії | IP-адреса філії | DLCI |
|---|---|---|---|---|---|
| 2 | Serial0/1/0.101 | 10.0.0.1 | Serial0/1/0.201 | 10.0.0.2 | 101 |
| 3 | Serial0/1/0.102 | 10.0.0.5 | Serial0/1/0.301 | 10.0.0.6 | 102 |
| 4 | Serial0/1/0.103 | 10.0.0.9 | Serial0/1/0.401 | 10.0.0.10 | 103 |

У лістингу 3.5 показано приклад налаштування головного інтерфейсу та підінтерфейсів на маршрутизаторі R1.

Лістинг 3.5 — Налаштування інтерфейсу Frame Relay на маршрутизаторі R1

```
interface Serial0/1/0
 no ip address
 encapsulation frame-relay
 crypto map VPNMAP
interface Serial0/1/0.101 point-to-point
 ip address 10.0.0.1 255.255.255.252
 frame-relay interface-dlci 101
 clock rate 2000000
interface Serial0/1/0.102 point-to-point
 ip address 10.0.0.5 255.255.255.252
 frame-relay interface-dlci 102
 clock rate 2000000
interface Serial0/1/0.103 point-to-point
 ip address 10.0.0.9 255.255.255.252
 frame-relay interface-dlci 103
 clock rate 2000000
```

На рисунку 3.4 подано логічну схему з’єднань філій за допомогою Frame Relay, яка відображає організацію віртуальних каналів зв’язку між головним маршрутизатором та маршрутизаторами філій, а також використання підінтерфейсів для розділення трафіку до кожної з філій.

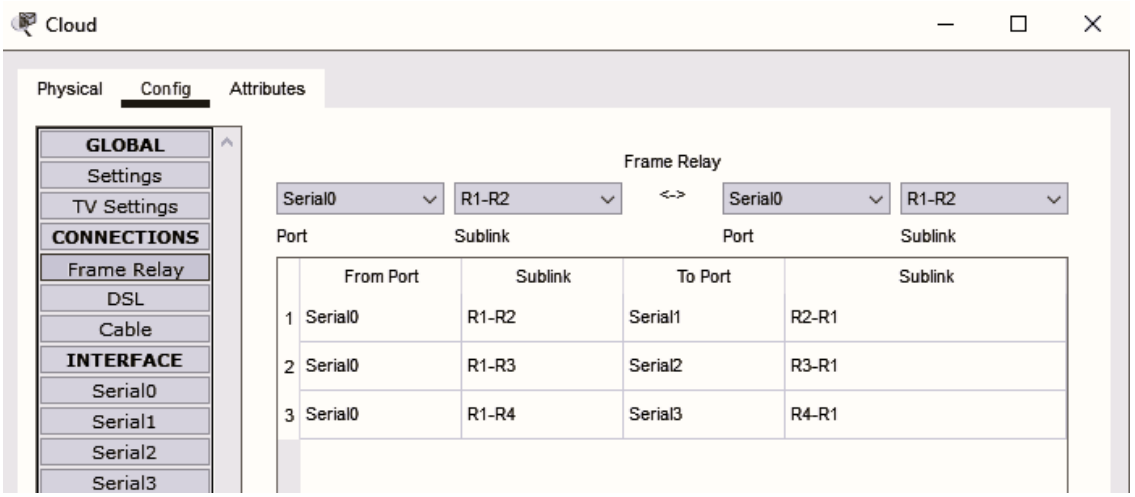


Рисунок 3.4 — WAN-зв’язок між філіями через Cloud у середовищі Cisco Packet Tracer

## 3.4 VPN-з’єднання між філіями

Для забезпечення захищеного передавання даних між філіями мережі «O’CAKE» було реалізовано VPN-з’єднання з інкапсуляцією GRE поверх IPsec. Такий підхід дозволяє передавати маршрутизовані пакети різних протоколів через захищений тунель, використовуючи публічну мережу провайдера.

Між кожною філією та головною реалізовано окремий тунель GRE, який захищено за допомогою IPsec у режимі crypto map. Усі тунелі побудовані між підінтерфейсами Frame Relay. Тунелі логічно організовані в окремі point-to-point підмережі.У таблиці 3.3 наведено інформацію про VPN-тунелі між головним маршрутизатором R1 і віддаленими філіями.

Таблиця 3.3 — VPN-тунелі GRE over IPsec між філіями

| Тунель | Маршрутизатори | Інтерфейси WAN | IP-адреси тунелів | Підмережа тунелю |
|---|---|---|---|---|
| Tunnel1 | R1 ↔ R2 | 10.0.0.1 ↔ 10.0.0.2 | 192.168.1.1 ↔ 192.168.1.2 | 192.168.1.0/30 |
| Tunnel2 | R1 ↔ R3 | 10.0.0.5 ↔ 10.0.0.6 | 192.168.2.1 ↔ 192.168.2.2 | 192.168.2.0/30 |
| Tunnel3 | R1 ↔ R4 | 10.0.0.9 ↔ 10.0.0.10 | 192.168.3.1 ↔ 192.168.3.2 | 192.168.3.0/30 |

На рисунку 3.5 зображено логічну схему побудови GRE-тунелів між філіями

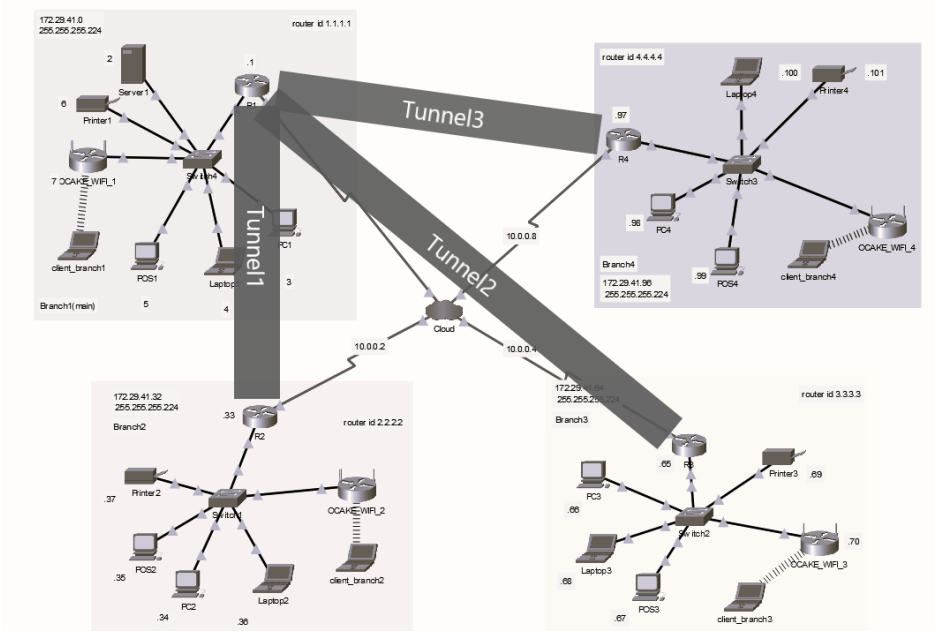


Рисунок 3.5 — Побудова тунелів GRE між філіями через Frame Relay Cloud

У лістингу 3.5 показано приклад налаштування тунелю та IPsec-захисту для з’єднання між R1 і R2.

Лістинг 3.5 — Налаштування тунелю GRE та IPsec на маршрутизаторі R1

```
interface Tunnel1
 ip address 192.168.1.1 255.255.255.252
 tunnel source Serial0/1/0.101
 tunnel destination 10.0.0.2
 tunnel mode gre ip
crypto isakmp policy 10
 encryption aes
 authentication pre-share
 group 2
 lifetime 86400
crypto isakmp key cisco address 10.0.0.2
crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
 mode transport
access-list 100 permit gre host 192.168.1.1 host 192.168.1.2
crypto map VPNMAP 10 ipsec-isakmp
 set peer 10.0.0.2
 set transform-set VPN-SET
 match address 110
interface Serial0/1/0
 crypto map VPNMAP
```

Аналогічне налаштування реалізується на маршрутизаторі R2, лише з

дзеркальними IP-адресами тунелю та заміною місця призначення показано у лістингу 3.6.

Лістинг 3.6 — Налаштування тунелю GRE та IPsec на маршрутизаторі R2

```
interface Tunnel1
 ip address 192.168.1.2 255.255.255.252
 tunnel source Serial0/1/0.201
 tunnel destination 10.0.0.1
 tunnel mode gre ip
crypto isakmp policy 10
 encryption aes
 authentication pre-share
 group 2
 lifetime 86400
crypto isakmp key cisco address 10.0.0.1
crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
 mode transport
access-list 100 permit gre host 192.168.1.2 host 192.168.1.1
crypto map VPNMAP 10 ipsec-isakmp
 set peer 10.0.0.1
 set transform-set VPN-SET
 match address 11
interface Serial0/1/0
 crypto map VPNMAP
```

## 3.5 Налаштування локальної мережі Wi-Fi у філіях

Для забезпечення бездротового доступу клієнтів та персоналу до Інтернету у кожній філії встановлено точку доступу, яка підключена до внутрішнього комутатора в режимі моста (Bridge mode). Це дозволяє інтегрувати бездротових клієнтів до загальної мережі філії без необхідності додаткової маршрутизації.

Для кожної філії створено окрему Wi-Fi мережу з унікальним SSID. Для безпеки використовується WPA2-PSK з паролем 12345678. Точки доступу працюють у закритому режимі, з обмеженим доступом: Wi-Fi клієнти можуть виходити лише в Інтернет, не маючи доступу до внутрішніх серверів та обладнання філії. Обмеження реалізовано через списки контролю доступу (ACL), які розглядаються у підпункті 3.8.

DHCP-сервер на маршрутизаторі кожної філії видає IP-адреси лише для бездротових клієнтів. Всі інші пристрої філії мають статично налаштовані IP-адреси. Частина адрес у підмережі філії зарезервована для цих пристроїв (POS-термінали, ПК, принтери, ноутбуки адміністраторів, самі точки доступу).

DNS-запити як з дротових, так і бездротових клієнтів обробляються внутрішнім DNS-сервером у головній філії. Його IP-адреса — 172.29.41.2, доменне ім’я — ocake.com.vn.

Таблиця 3.4 – Параметри Wi-Fi у філіях компанії «O’CAKE»

| Філія | SSID | DHCP-пул для Wi-Fi | Зарезервовані IP-адреси | DNS-сервер |
|---|---|---|---|---|
| 1 | ocake_branch1 | 172.29.41.11–172.29.41.30 | 172.29.41.1–172.29.41.10 | 172.29.41.2 |
| 2 | ocake_branch2 | 172.29.41.41–172.29.41.62 | 172.29.41.33–172.29.41.40 | 172.29.41.2 |
| 3 | ocake_branch3 | 172.29.41.76–172.29.41.94 | 172.29.41.65–172.29.41.75 | 172.29.41.2 |
| 4 | ocake_branch4 | 172.29.41.111–172.29.41.126 | 172.29.41.95–172.29.41.110 | 172.29.41.2 |

На рисунку 3.5 зображено реалізацію бездротової мережі у філії.

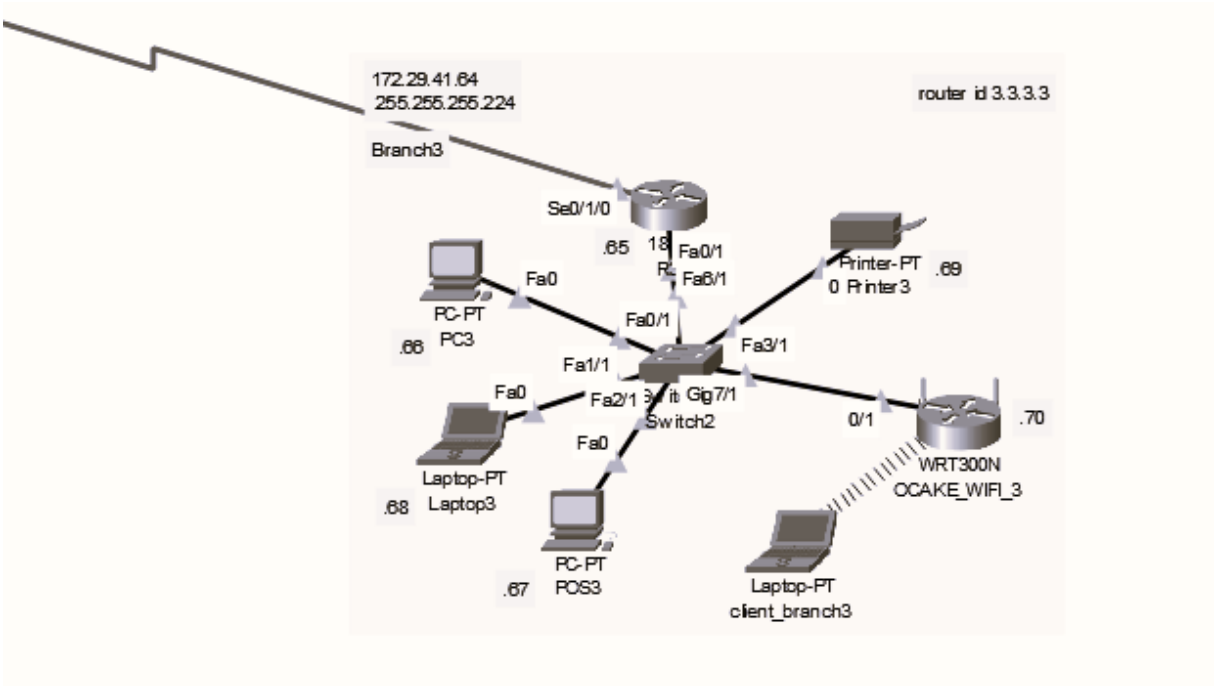


Рисунок 3.5 — Топологія Wi-Fi у філії 3

## 3.6 Налаштування маршрутизації за допомогою OSPF

У корпоративній мережі «O’CAKE» реалізовано динамічну маршрутизацію за допомогою протоколу OSPF (Open Shortest Path First). Це дозволяє забезпечити

автоматичне оновлення таблиць маршрутизації між усіма філіями без ручного налаштування статичних маршрутів.

Усі маршрутизатори об’єднані в одну загальну зону — area 0, а як ідентифікатори маршрутизаторів (router ID) використано інтерфейси Loopback0. До OSPF додаються лише LAN- та WAN-мережі кожної філії. VPN-тунелі на базі GRE over IPsec не беруть участі в OSPF і використовуються лише як транспорт для міжфілійного з’єднання.У таблиці 3.4 подано короткий огляд маршрутизованих мереж, що беруть участь у OSPF, та ідентифікаторів маршрутизаторів.

Таблиця 3.4 — LAN- і WAN-мережі

| Маршрутизатор | WAN-мережа | LAN-мережа | Router ID | Маршрутизатор |
|---|---|---|---|---|
| R1 | 10.0.0.0/30 | 172.29.41.0/28 | 1.1.1.1 | R1 |
| R2 | 10.0.0.0/30 | 172.29.41.32/28 | 2.2.2.2 | R2 |
| R3 | 10.0.0.4/30 | 172.29.41.64/28 | 3.3.3.3 | R3 |

У лістингу 3.6 наведено приклад конфігурації OSPF на маршрутизаторі R3. У ній додаються до OSPF його LAN- і WAN-мережі, а також призначається унікальний ідентифікатор маршрутизатора через loopback-інтерфейс, що забезпечує стабільність роботи маршрутизації незалежно від стану фізичних інтерфейсі.

Лістинг 3.6 — Конфігурація OSPF на маршрутизаторі R3

```
interface Loopback0
 ip address 3.3.3.3 255.255.255.255
router ospf 1
 router-id 3.3.3.3
 network 10.0.0.4 0.0.0.3 area 0
 network 172.29.41.64 0.0.0.31 area 0
```

У рисунку 3.6 відображено результат команди show ip ospf interface brief, що демонструє активні OSPF-інтерфейси, їхні стани, ролі в процесі маршрутизації, а також підтверджує успішне включення необхідних інтерфейсів до OSPF.

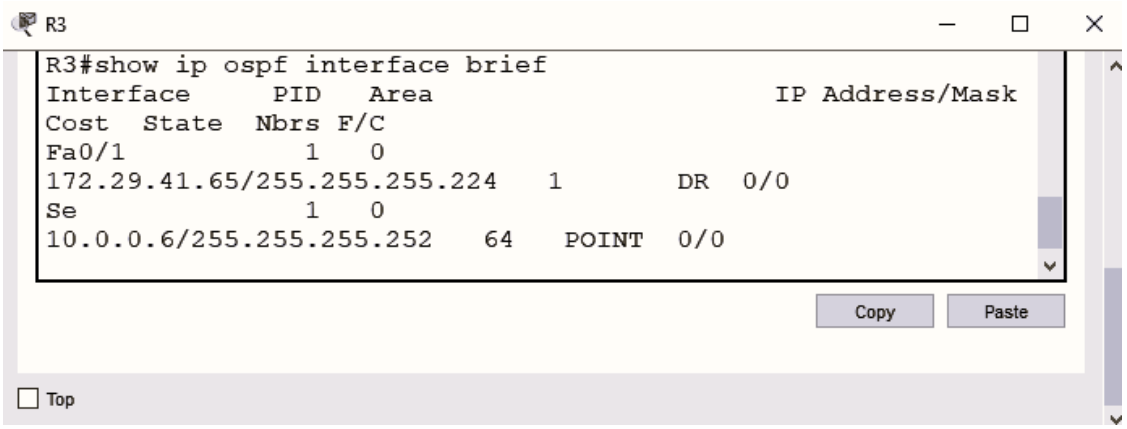


Рисунок 3.10 — Вивід активних інтерфейсів OSPF на R3

## 3.7 Центральний сервер на Debian: налаштування Apache, MariaDB, phpMyAdmin

У головній філії на окремому сервері, розгорнутому під керуванням операційної системи Debian, реалізовано функціонал бази даних для всієї мережі «O'CAKE». Сервер забезпечує централізоване зберігання даних, зручне адміністрування через веб-інтерфейс та надає віддалений доступ до інформації для працівників мережі.

Перед початком конфігурування було встановлено всі необхідні компоненти LAMP-стека. На сервері встановлено наступне:

— Apache;

— MariaDB;

— phpMyAdmin.

Для встановлення та налаштування компонентів було виконано низку команд, наведено у лістингу 3.7.

Лістинг 3.7 — Встановлення Apache, MariaDB і phpMyAdmin у Debian

```
sudo apt update
sudo apt install apache2 mariadb-server php php-mysql libapache2-mod-php
phpmyadmin
sudo systemctl enable apache2
sudo systemctl enable mariadb
```

Після інсталяції MariaDB було створено окрему базу даних ocake_db, яка містить основну інформацію про філії, працівників та продукцію. Структуру наведено у таблиці 3.5.

Таблиця 3.5 — Таблиці бази даних ocake_db

| Назва таблиці | Опис |
|---|---|
| products | Дані про продукцію кафе |
| employees | Інформація про персонал |
| branches | Адреси та дані про філії |

Користувачі бази даних мають розмежовані привілеї доступу залежно від ролі. Розмежування наведено у таблиці 3.4.

Таблиця 3.4 — Користувачі БД та їхні права

| Ім’я користувача | Привілеї |
|---|---|
| admin_user | Повний доступ до всіх таблиць, створення, зміна, видалення даних |
| manager_user | Читання всіх таблиць, редагування таблиць employees, products |
| staff_user | Лише читання всіх таблиць |

Процес створення бази даних і користувачів представлено в лістингу 3.8.

Лістинг 3.8 — Створення бази даних ocake_db та користувачів у MariaDB

```
CREATE DATABASE ocake_db;
CREATE USER 'admin_user'@'localhost' IDENTIFIED BY 'admin';
CREATE USER 'manager_user'@'localhost' IDENTIFIED BY 'manager';
CREATE USER 'staff_user'@'localhost' IDENTIFIED BY 'staff';
GRANT ALL PRIVILEGES ON ocake_db.* TO 'admin_user'@'localhost';
GRANT SELECT, UPDATE ON ocake_db.products TO 'manager_user'@'localhost';
GRANT SELECT, UPDATE ON ocake_db.employees TO 'manager_user'@'localhost';
GRANT SELECT ON ocake_db.* TO 'staff_user'@'localhost';
FLUSH PRIVILEGES;
```

Для доступу до БД через браузер було налаштовано phpMyAdmin, який доступний у внутрішній мережі за IP-адресою сервера. На рисунку 3.10 показано головну сторінку phpMyAdmin після авторизації.

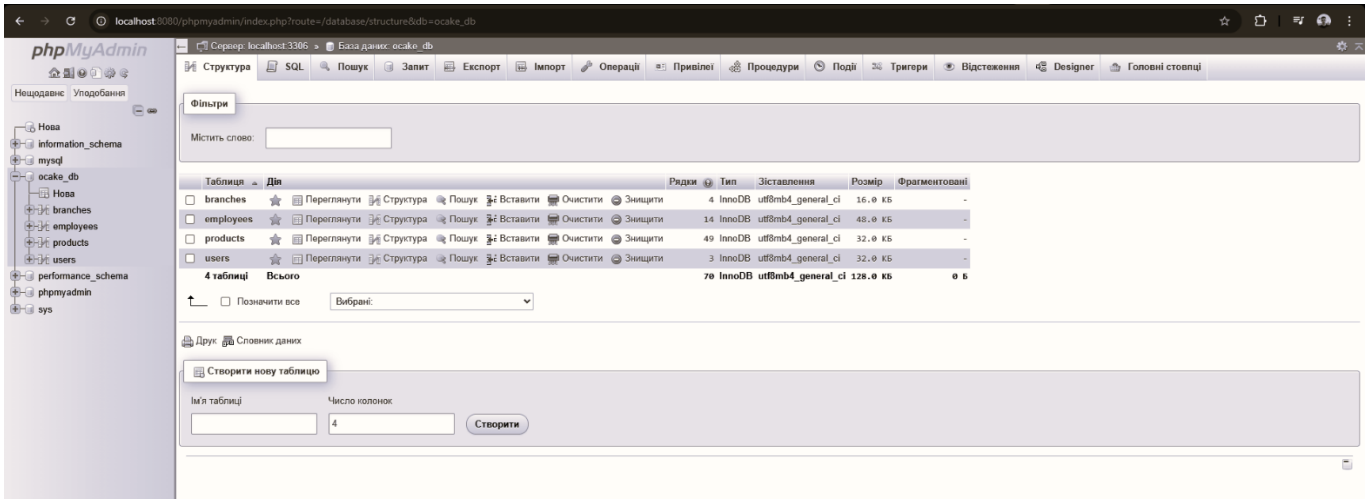


Рисунок 3.10 — Головна сторінка phpMyAdmin із базою ocake_db

## 3.8 Захист мережі: SSH, ACL, обмеження доступу

Для забезпечення базового рівня безпеки всі маршрутизатори у філіях налаштовані на використання SSH для дистанційного адміністрування. Доступ до пристроїв здійснюється тільки через протокол SSH, тоді як Telnet повністю вимкнено. Це дозволяє уникнути передавання паролів у відкритому вигляді. На маршрутизаторах створено локальні облікові записи з рівнем привілеїв 15, що дає адміністраторам повний доступ до системи. Приклад налаштування SSH на маршрутизаторі R1 подано в лістингу 3.9.

Лістинг 3.9 – Налаштування SSH на маршрутизаторі R1

```
ip domain-name ocake.com.vn
username adminr1 privilege 15 secret <admin1>
ip ssh version 2
line vty 0 4
 login local
 transport input ssh
```

Усі зовнішні з’єднання між філіями реалізовано через тунелі GRE поверх IPsec, захищені шифруванням AES та аутентифікацією за попередньо узгодженим ключем. Їх детальна реалізація вже була розглянута раніше, тому в цьому пункті зосередимося на засобах фільтрації трафіку за допомогою списків доступу.

На маршрутизаторах R1 та R3 реалізовано ACL, які дозволяють трафік GRE лише між IP-адресами тунелів. Це мінімізує ризики атаки або небажаного трафіку на рівні тунельного інтерфейсу. У лістингу 3.10 наведено відповідні рядки

конфігурації ACL на R1.

Лістинг 3.10 – ACL на маршрутизаторі R1 для GRE

```
access-list 100 permit gre host 192.168.1.1 host 192.168.1.2
access-list 110 permit gre host 192.168.2.1 host 192.168.2.2
access-list 120 permit gre host 192.168.3.1 host 192.168.3.2
```

На маршрутизаторі R3 присутній лише один тунель, відповідно й ACL лише один, що дозволяє GRE-трафік між R1 і R3. Відповідне налаштування подано в лістингу 3.11.

Лістинг 3.11 – ACL на маршрутизаторі R3 для GRE

```
access-list 110 permit gre host 192.168.2.2 host 192.168.2.1
```

Таким чином, трафік через VPN-тунелі обмежено лише необхідними IP-адресами, що унеможливлює доступ сторонніх вузлів до логічних каналів зв’язку між філіями.

Окрім маршрутизаторів, відповідно до вимог безпеки, було вжито заходів і на стороні сервера. Центральний сервер з базою даних ocake_db, розташований у головній філії, доступний лише через внутрішню мережу. Адміністрування сервера відбувається виключно через SSH.

phpMyAdmin також обмежено — доступ до нього надано лише з внутрішніх IP-адрес. Було створено кілька облікових записів користувачів бази даних із розмежованими правами доступу:

— admin_user має повний доступ;

— manager_user може переглядати всі таблиці і редагувати employees та products;

— staff_user має лише права на перегляд даних.

Таке розмежування дозволяє уникнути несанкціонованих змін у базі даних, зменшити ризики витоку чи пошкодження інформації та забезпечити контрольовану взаємодію з нею відповідно до ролей користувачів.

Загалом реалізовані заходи забезпечують базову сегментацію, шифрування даних та контроль доступу до всіх ресурсів як на рівні мережі, так і на прикладному рівні.

## 3.9 Тестування роботи мережі: міжфілійний зв’язок, сервіси, VPN, Wi-Fi

Після завершення налаштування мережі було проведено тестування її основних компонентів. Метою тестування є перевірка працездатності LAN і WAN-з’єднань, коректної маршрутизації, доступності сервісів, наявності міжфілійного зв’язку через VPN, функціонування DHCP, DNS, ACL, Wi-Fi, доступу через SSH, а також перевірка роботи сервера з Debian.

Для перевірки локальної мережі в кожній філії було виконано пінг між стаціонарними ПК, POS-терміналом та принтером. Зокрема, у філії 2 ПК успішно пінгує POS-термінал і принтер, що свідчить про стабільну LAN-комунікацію. У рисунку 3.11 показано результат пінгу між пристроями локальної мережі філії 2.

PDU List Window

| Fire | Last Status | Source | Destination | Type | Color | Time(sec) | Periodic | Num | Edit | Delete |
|---|---|---|---|---|---|---|---|---|---|---|
| | Successful | Laptop2 | PC2 | ICMP | | 0.000 | N | 0 | (edit) | |
| | Successful | POS2 | Printer2 | ICMP | | 0.000 | N | 1 | (edit) | |
| | Successful | client_br... | POS2 | ICMP | | 0.000 | N | 2 | (edit) | |
| | Successful | POS2 | R2 | ICMP | | 0.000 | N | 3 | (edit) | |

Рисунок 3.11 — Результат пінгу між пристроями локальної мережі філії 2

Для тестування WAN-зв’язку виконано пінг між маршрутизаторами через зовнішні WAN-інтерфейси. На рисунку 3.12 відображено виконання пінгу з маршрутизатора R1 до IP-адрес 10.0.0.6 та 10.0.0.10. Результат підтверджує функціональність з’єднань через Frame Relay.

```
R1#ping 10.0.0.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.6, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
4/17/24 ms

R1#ping 10.0.0.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.10, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
7/20/33 ms
```

Рисунок 3.12 — Виконання пінгу WAN-зв’язків

Для перевірки VPN-тунелів виконано пінг між тунельними інтерфейсами.

Наприклад, з тунельного інтерфейсу R1 192.168.2.1 виконано пінг до 192.168.2.2 на R3. Зв’язок стабільний, затримки мінімальні. Це свідчить про правильну інкапсуляцію трафіку GRE-тунелем. У рисунку 3.13 наведено результат пінгу між тунельними інтерфейсами маршрутизаторів R1 і R3.

```
R1#ping 192.168.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.2, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
21/26/34 ms

R1#
```

Рисунок 3.13 — Пінг тунельного інтерфейсу

Для перевірки правил доступу, заданих через ACL, здійснено пінг з Wi-Fi-клієнта до внутрішніх IP-адрес філії. Пінг проходить успішно, що свідчить про те, що на поточному етапі ACL не обмежують цей трафік. Це дозволяє виявити потенційну зону для посилення безпеки в майбутньому — шляхом створення додаткових ACL для блокування доступу з Wi-Fi до локальних пристроїв. У рисунку 3.14 показано результат пінгу з клієнтського ноутбука до внутрішньої мережі філії.

PDU List Window

| Fire | Last Status | Source | Destination | Type | Color | Time(sec) | Periodic | Num | Edit | Delete |
|---|---|---|---|---|---|---|---|---|---|---|
| | Successful | client_branch3 | PC3 | ICMP | | 0.000 | N | 0 | (edit) | |
| | Successful | client_branch3 | R3 | ICMP | | 0.000 | N | 1 | (edit) | |
| | Successful | client_branch3 | POS3 | ICMP | | 0.000 | N | 2 | (edit) | |

Рисунок 3.14 — Перевірка правил доступу

Роботу DHCP перевірено шляхом підключення клієнтського ноутбука до точки доступу Wi-Fi. Усі клієнти отримують IP-адреси автоматично. Наприклад, у філії 3 ноутбук отримав IP-адресу з відповідного пулу DHCP. У рисунку 3.15 наведено результат автоматичного отримання IP-адреси ноутбуком у філії 3.

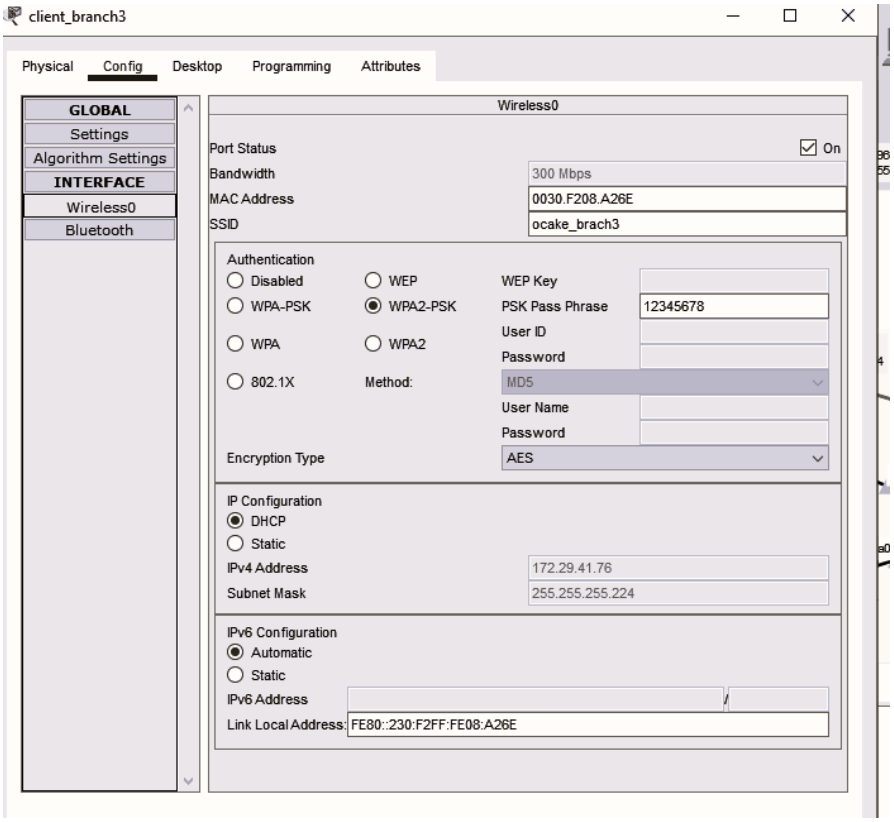


Рисунок 3.15 — Результат автоматичного отримання IP-адреси ноутбуком у філії 3

DNS-сервер протестовано з ПК користувача. Виконано запит nslookup ocake.com.vn Відповідь з IP-адресою 172.29.41.2 підтверджує працездатність DNS. У рисунку 3.16 наведено результат виконання запиту до DNS-сервера з ПК.

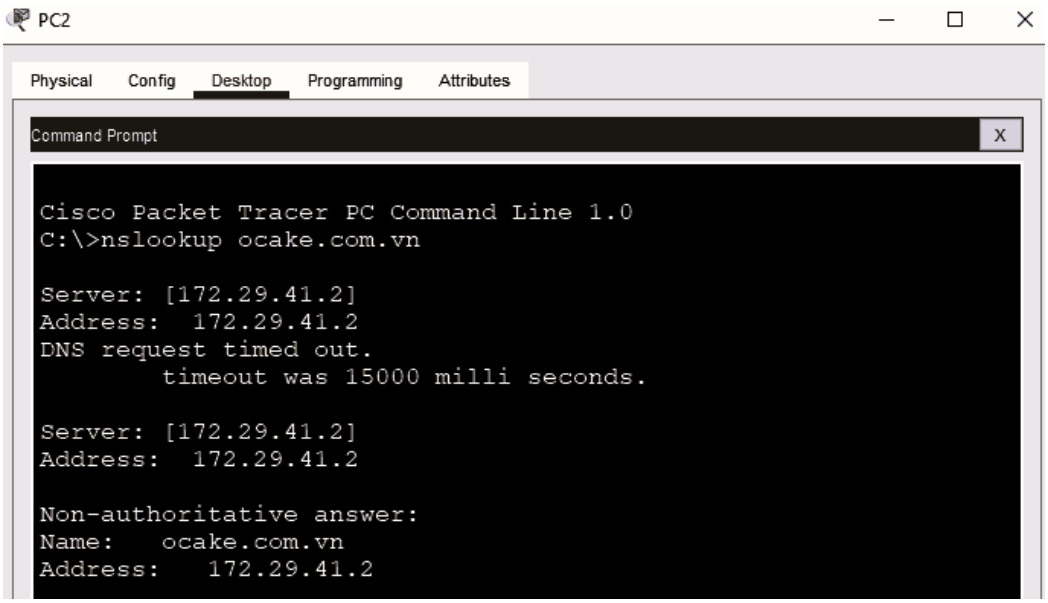


Рисунок 3.16 — Тестування DNS

SSH-доступ до маршрутизаторів перевірено з адміністративного ПК. З ПК адміністратора виконано команду ssh -l adminr1 172.29.41.1. З'єднання встановлено успішно, що свідчить про правильну реалізацію SSH-сервісу та політик безпеки. У рисунку 3.17 показано вхід на маршрутизатор R1 через SSH.

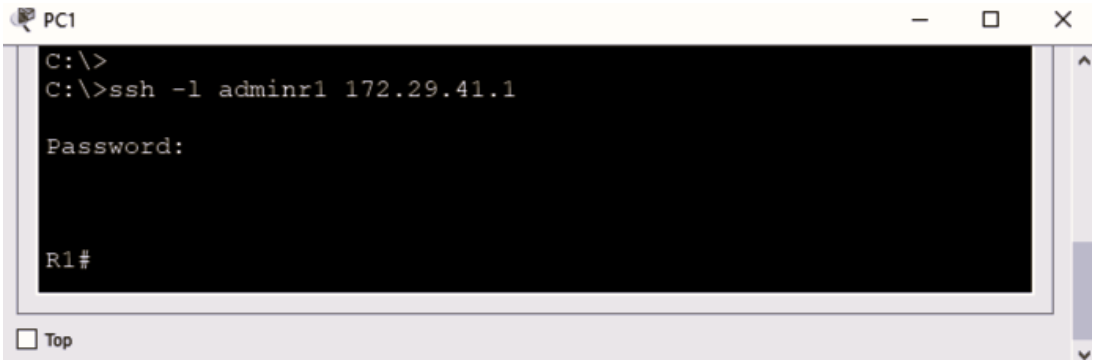


Рисунок 3.17 — Тестування SSH

Сервер з Debian протестовано з доступом до phpMyAdmin. З ПК адміністратора відкрито вебінтерфейс phpMyAdmin, успішно авторизовано користувача admin_user. Відкрито базу даних ocake_db і здійснено перегляд таблиць products, employees та branches. Сервер працює стабільно. У рисунку 3.18 зображено доступ до бази даних ocake_db через phpMyAdmin.

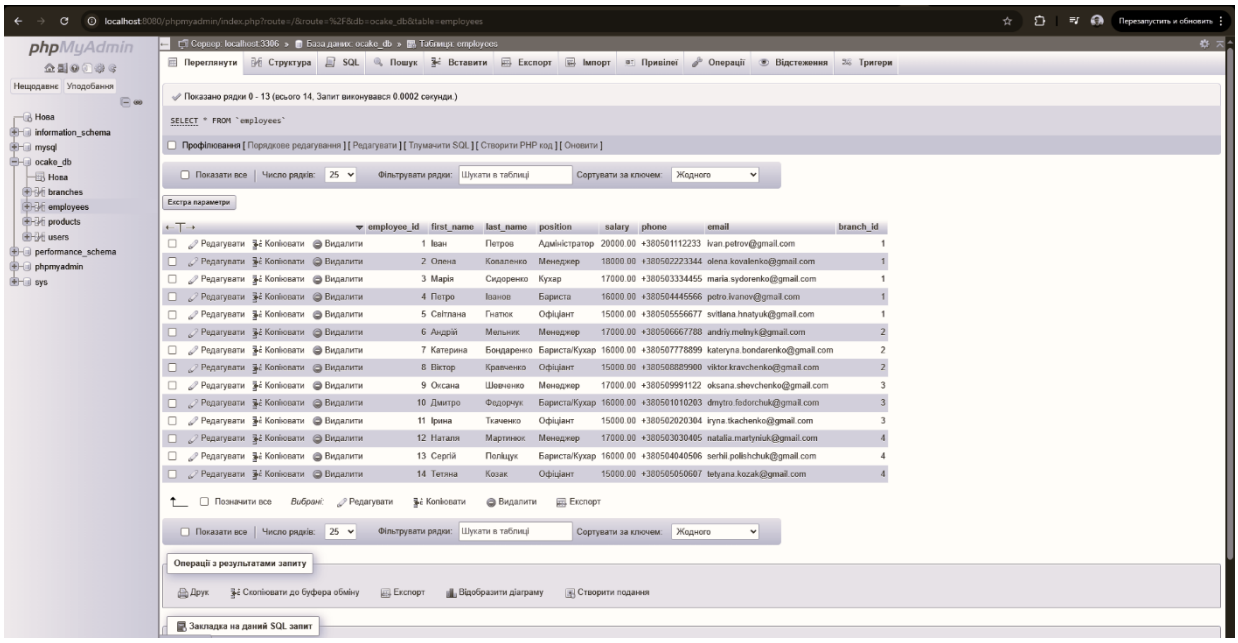


Рисунок 3.18 — Доступ до бази даних ocake_db через phpMyAdmin під користувачем admin_user

Далі виконано вихід із phpMyAdmin і вхід під обліковим записом staff_user. Користувач успішно авторизується, має доступ до перегляду таблиць, однак при спробі змінити запис у таблиці products з’являється повідомлення про недостатні привілеї. У рисунку 3.19 зображено повідомлення про помилку при редагуванні запису в таблиці products користувачем staff_user.

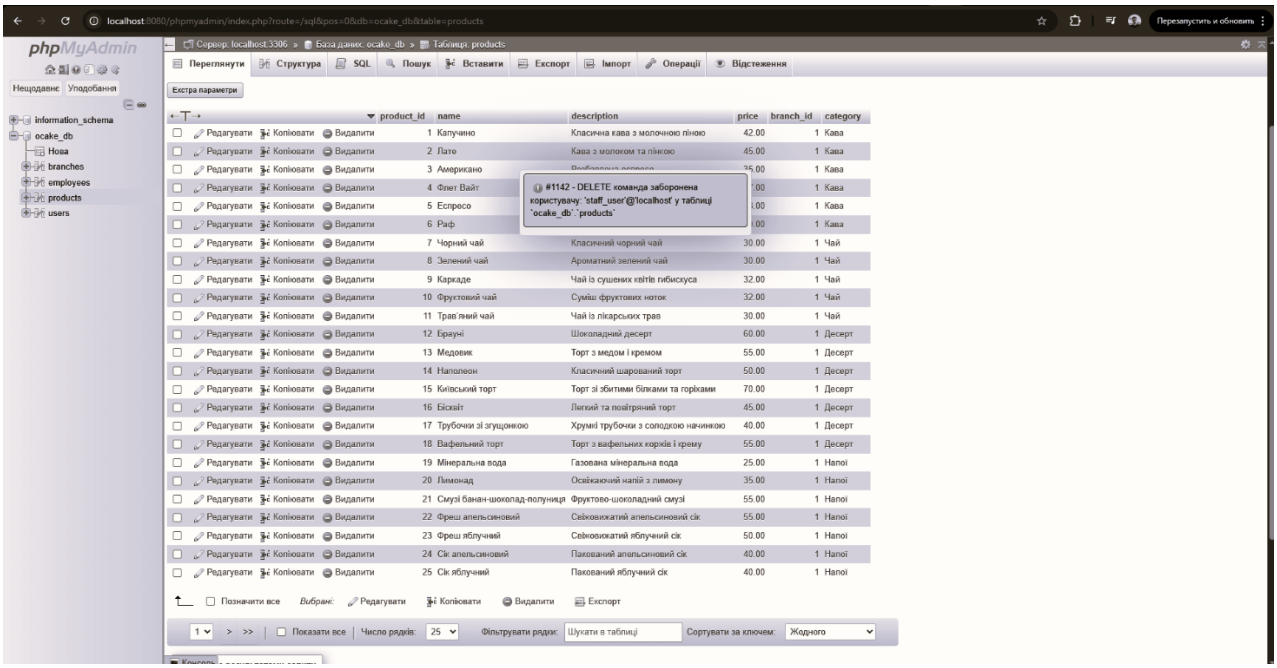


Рисунок 3.19 — Повідомлення про помилку при редагуванні запису в таблиці products користувачем staff_user

Таким чином, підтверджено коректну реалізацію розмежування прав доступу до бази даних згідно з заданими обліковими записами, що дозволяє обмежити дії користувачів відповідно до їхніх повноважень.

Wi-Fi-з’єднання перевірено в усіх філіях. Кожен ноутбук успішно підключається до відповідної точки доступу з унікальним SSID формату ocake_branchX, що відповідає номеру філії. Після підключення пристрій автоматично отримує IP-адресу через DHCP, коректно визначає адресу DNS-сервера, має стабільний доступ до внутрішніх ресурсів філії, а також вихід до зовнішньої мережі Інтернет. Це підтверджує правильність налаштування точок доступу, IP-адресації та роботи DHCP-сервісу. У рисунку 3.20 показано підключення ноутбука до Wi-Fi у філії 1.


Рисунок 3.20 — Підключення ноутбука до Wi-Fi у філії 1

У рисунку 3.21 показано результат роботи глобального з’єднання

У результаті тестування встановлено, що всі компоненти мережі працюють коректно, з’єднання між філіями стабільне, сервіси функціонують відповідно до налаштувань, а безпека доступу може бути посилена шляхом додаткового обмеження доступу з бездротових клієнтів.

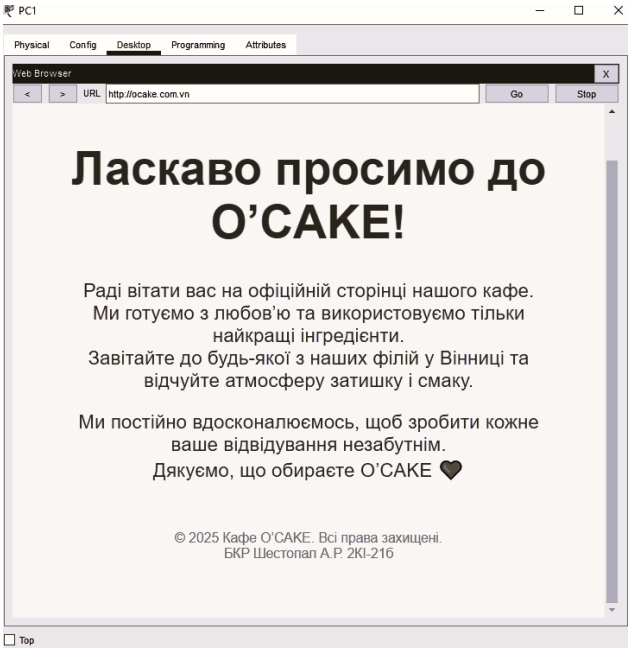


Рисунок 3.20 — Робота глобального з’єднання

## 3.10 Аналіз результатів тестування та оптимізація налаштувань

Проведене тестування підтвердило стабільну роботу побудованої мережі для всіх філій компанії. У результаті виконаних перевірок встановлено, що всі основні компоненти функціонують згідно з вимогами проєкту.

Локальні мережі кожної філії забезпечують надійний зв’язок між пристроями, пінг проходить з мінімальною затримкою, що свідчить про відсутність проблем на рівні комутації або IP-адресації.

WAN-з’єднання через Frame Relay працюють стабільно. Пінг між зовнішніми інтерфейсами маршрутизаторів підтвердив коректну роботу фізичних та канальних з’єднань у глобальній мережі.

VPN-тунелі GRE over IPsec між філіями функціонують без збоїв. Пакети інкапсулюються та деінкапсулюються належним чином, трафік шифрується, що забезпечує конфіденційність даних під час передачі між офісами.

DHCP-сервери на маршрутизаторах правильно роздають IP-адреси клієнтам Wi-Fi. Це підтверджено на практиці через отримання адрес ноутбуками в кожній філії.

Сервер DNS успішно обробляє запити з клієнтських пристроїв. Отримання правильної IP-адреси у відповідь на доменне ім’я свідчить про функціональність локального іменного сервера.

SSH-доступ до маршрутизаторів здійснюється лише для авторизованих адміністраторів, з’єднання встановлюється через безпечний канал, що підвищує рівень керованості й безпеки мережі.

Wi-Fi у кожній філії дозволяє клієнтам підключатися лише до Інтернету. Клієнтські ноутбуки успішно підключаються до точки доступу через WPA2-PSK, отримують IP-адресу, однак виявлено, що пінг до внутрішніх пристроїв все ще проходить. Це свідчить про необхідність посилити обмеження через додаткові ACL, які блокуватимуть трафік від бездротових клієнтів до внутрішньої інфраструктури філії.

Сервер на базі Debian з MariaDB і phpMyAdmin працює стабільно. Перевірка прав доступу до бази даних підтвердила реалізацію політик безпеки: admin_user

має повний доступ, manger_user частковий доступ, а staff_user обмежений лише переглядом даних, без можливості редагування критичних таблиць.

Аналіз виявив такі рекомендації для оптимізації:

— налаштувати журналювання з’єднань SSH для додаткового аудиту доступу адміністраторів;

— розглянути запровадження VLAN у філіях для логічного розділення внутрішніх пристроїв (наприклад, POS, принтери, клієнти);

— забезпечити періодичне резервне копіювання бази даних на сервері Debian;

— розширити набір прав користувачів бази даних відповідно до ролей персоналу, якщо передбачається подальше зростання системи.

У цілому, побудована мережева інфраструктура відповідає поставленим вимогам і демонструє високий рівень доступності, безпеки та керованості.

# ВИСНОВКИ

У результаті виконання бакалаврської кваліфікаційної роботи було спроєктовано, налаштовано та протестовано корпоративну комп'ютерну мережу для кафе «O'CAKE» з головною філією та трьома віддаленими філіями. Проєкт реалізовано з урахуванням сучасних вимог до безпеки, масштабованості та надійності мережевих інфраструктур.

У процесі виконання роботи були досягнуті всі поставлені завдання. Проведено аналіз архітектури комп'ютерних мереж та визначено доцільність використання топології з центральною філією-сервером і трьома підключеними філіями.

Запропоновано ефективну IP-адресацію з поділом на підмережі для локальних сегментів, VPN-тунелів та WAN-з'єднань, що забезпечило зручність маршрутизації;

Впроваджено протокол динамічної маршрутизації OSPF з унікальними router ID для кожного маршрутизатора, що дозволило реалізувати адаптивну маршрутизацію між філіями;

Реалізовано WAN-з'єднання за допомогою технології Frame Relay з логічними підінтерфейсами, що імітують телекомунікаційного провайдера;

Налаштовано VPN-тунелі GRE over IPsec між головною філією та всіма іншими філіями з метою шифрування та інкапсуляції міжфілійного трафіку;

Налаштовано локальні Wi-Fi мережі в кожній філії з використанням WPA2-PSK, що забезпечує захищений доступ для клієнтських ноутбуків;

Налаштовано DHCP-сервери на маршрутизаторах для автоматичної видачі адрес клієнтам Wi-Fi, що забезпечує зручність підключення;

Реалізовано обмеження доступу до внутрішньої інфраструктури з бездротового сегменту за допомогою ACL;

Встановлено центральний сервер на Debian з базою даних MariaDB та phpMyAdmin, який забезпечує централізоване зберігання даних філій;

Налаштовано користувачів бази даних із різними правами доступу (admin_user, staff_user, manager_user), що реалізує політику мінімальних

привілеїв;

Забезпечено безпечний доступ до маршрутизаторів за допомогою SSH;

Проведено комплексне тестування роботи мережі, що підтвердило стабільність з’єднання між філіями, працездатність VPN, функціональність серверів DHCP, DNS, бази даних та правильність налаштувань безпеки.

Розроблена мережева інфраструктура відповідає сучасним вимогам до корпоративних мереж малого бізнесу. Вона забезпечує захищене міжфілійне з’єднання з шифруванням трафіку через VPN, безпечне підключення клієнтських пристроїв через захищені Wi-Fi мережі, надійну маршрутизацію через OSPF з підтримкою масштабованості, зручність адміністрування через SSH та централізований сервер бази даних, гнучкий контроль доступу через ACL та налаштування прав у БД.

Новизна проєкту полягає в комплексному підході до проєктування розподіленої мережі для філійного бізнесу з акцентом на безпеку, централізованість зберігання даних та автономність кожного підрозділу. Обрані технології (Frame Relay, GRE over IPsec, OSPF, DHCP, ACL, SSH) дозволили реалізувати надійне і гнучке рішення для компанії.

Практична цінність проєкту підтверджується результатами тестування — усі сервіси функціонують коректно, з’єднання між філіями є стабільним, VPN-тунелі шифрують трафік, клієнти мають доступ до мережі відповідно до політик доступу, а адміністратор має централізований контроль над усіма компонентами.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Розвиток технологій 5G та їх вплив на побудову сучасних локальних мереж. / А. Р. Шестопал, С. М. Захарченко // Матеріали конференції LIV Всеукраїнської науково-технічної конференції факультету інформаційних технологій та комп'ютерної інженерії. Вінниця 2025 р. [Електронний ресурс]. Режим доступу: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2025/paper/view/23658/19529.

2. Комп’ютерні мережі: підручник / Азаров О. Д., Захарченко С. М., Кадук О. В., Орлова М. М., Тарасенко В. П. — Вінниця: ВНТУ, 2020. 378 с.

3. Коробейнікова Т. І., Захарченко С. М. Комп’ютерні мережі. — Львів: Видавництво Львівської політехніки, 2022. 228 с.

4. Таненбаум А. С., Уезеролл Д. Дж. Комп’ютерні мережі. К. : Діалектика, 2021. 960 с.

5. Cisco Systems. Introduction to Frame Relay Configuration [Електронний ресурс]. Режим доступу: https://www.cisco.com/c/en/us/support/docs/wan/frame-relay/10378-10.html

6. Cisco Systems. GRE over IPsec Design and Implementation Guide [Електронний ресурс]. Режим доступу: https://www.cisco.com/c/en/us/support/docs /ip/generic-routing-encapsulationgre/118370-technote-gre-00.html

7. Cisco Systems. OSPF Design Guide [Електронний ресурс]. Режим доступу: https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html

8. Городецька О. С., Гикавий В. А., Онищук О. В. Комп’ютерні мережі: навчальний посібник. — Вінниця: ВНТУ, 2017. 129 с.

9. Захист інформації в комп’ютерних системах та мережах / О. І. Гуцулай, А. О. Паламарчук — Львів: ЛНУ імені Івана Франка, 2021. 212 с.

10. Debian 11 Installation Manual [Електронний ресурс]. Режим доступу: https://www.debian.org/releases/bullseye/amd64/index.en.html

11. MariaDB Foundation. MariaDB Documentation [Електронний ресурс]. Режим доступу: https://mariadb.com/kb/en/documentation/

12. phpMyAdmin Official Documentation [Електронний ресурс]. Режим доступу: https://docs.phpmyadmin.net/

13. Натхненна модель безпеки комп’ютерних мереж / С. М. Захарченко, О. В. Кадук // Матеріали конференції ВНТУ. — Вінниця, 2023. [Електронний ресурс]. Режим доступу: https://conf.vntu.edu.ua/index.php/all-fitki/all-fitki2023/paper/view/18204

14. IEEE Std 802.11-2020: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Computer Society, 2020.

15. RFC 1918: Address Allocation for Private Internets [Електронний ресурс]. Режим доступу: https://tools.ietf.org/html/rfc1918

16. Cisco Packet Tracer – Cisco Networking Academy [Електронний ресурс]. Режим доступу: https://www.netacad.com/courses/packet-tracer

17. Віртуальні приватні мережі (VPN): принципи побудови та засоби реалізації / А. В. Задоя. Харків: НТУ “ХПІ”, 2021. 144 с.

18. Операційні системи та сервери: Linux, Windows, FreeBSD / І. В. Мельничук. Київ: КНУ, 2022. 276 с.

19. Безпека комп’ютерних мереж: навчальний посібник / Ю. А. Коваль. Київ: Ліра-К, 2020. 198 с.

# ДОДАТОК А

Технічне завдання

Міністерство освіти і науки України
Вінницький національний технічний університет
Факультет інформаційних технологій та комп’ютерної інженерії
Кафедра обчислювальної техніки

ЗАТВЕРДЖУЮ
Завідувач кафедри ОТ
д.т.н., проф. Азаров О.Д.
21 березня 2025 р.

ТЕХНІЧНЕ ЗАВДАННЯ
на виконання бакалаврської кваліфікаційної роботи
«Комп'ютерна мережа кафе "O’CAKE"»

08-54.БКР.034.00.000 ТЗ

Науковий керівник: к.т.н., проф. каф. ОТ
_____Захарченко С. М.

Студент групи 2КІ-21б
_____Шестопал А. Р.

м. Вінниця — 2025

1 Підстава для виконання бакалаврської кваліфікаційної роботи (БКР)

1.1 Актуальність проєкту полягає в необхідності побудови безпечної та масштабованої комп'ютерної мережі для приватної мережі кафе «O'CAKE», що включає головний офіс із сервером і декілька філій. Забезпечення надійного міжфілійного зв'язку, централізованого доступу до бази даних, гнучкої IP-адресації та високої доступності сервісів є ключовими потребами сучасного малого бізнесу у сфері громадського харчування.

1.2 Завданням розробки є проєктування корпоративної мережі з використанням технологій WAN-з'єднань (Frame Relay), VPN-тунелів (GRE over IPsec), протоколу маршрутизації OSPF, сервісів DHCP, DNS, NAT, а також впровадження засобів інформаційної безпеки (ACL, SSH).

1.3 Наказ про затвердження теми бакалаврської дипломної роботи від 21 березня 2025 р. №97.

2 Мета і призначення БКР

2.1 Метою роботи є побудова логічно структурованої, захищеної та масштабованої комп'ютерної мережі для організації «O'CAKE», яка забезпечує міжфілійний зв'язок, централізований доступ до бази даних, підтримку Wi-Fi клієнтів, а також високий рівень інформаційної безпеки.

2.2 Призначення розробки полягає у створенні технічного рішення для впровадження інформаційної інфраструктури, що охоплює декілька філій, для подальшого практичного використання та адміністрування мережею організації.

3 Вихідні дані для виконання БКР

3.1 Модель бізнес-інфраструктури мережі кафе «O'CAKE», яка складається з головного офісу та трьох філій, що з'єднуються за допомогою технології Frame Relay.

3.2 Аналіз сучасних протоколів маршрутизації (OSPF), механізмів тунелювання (GRE over IPsec), бездротового доступу (Wi-Fi WPA2-PSK), сервісів

адресації (DHCP), трансляції адрес (NAT), іменування (DNS), а також методів адміністрування (SSH, ACL).

3.3 Вибір маршрутизаторів Cisco, комутаторів, точок доступу Wi-Fi, серверного обладнання та програмного забезпечення (Debian, MariaDB, phpMyAdmin).

3.4 Побудова логічної схеми мережі, топології підмереж, VPN-тунелів, реалізація OSPF з призначенням router ID через loopback-інтерфейси.

3.5 Організація безпечного підключення клієнтів Wi-Fi у кожній філії та забезпечення доступу до локальної мережі філії і Інтернету..

3.6 Створення централізованої бази даних ocake_db, адміністрованої через phpMyAdmin, доступ до якої мають співробітники організації відповідно до ролей.

## 4 Вимоги до виконання БКР

Для успішного виконання бакалаврської кваліфікаційної роботи з проєктування комп'ютерної мережі для мережі кафе «O'CAKE» висуваються такі технічні та функціональні вимоги:

— Мережа має забезпечувати надійне з'єднання головного офісу та трьох філій з використанням технології Frame Relay і захищених VPN-тунелів GRE over IPsec;

— Усі пристрої в мережі повинні бути правильно маршрутизовані за допомогою протоколу OSPF, з призначенням router ID через loopback-інтерфейси.

— Повинна бути реалізована автоматична адресація клієнтських пристроїв через DHCP, з чітким розмежуванням LAN- та WAN-сегментів;

— Необхідно забезпечити бездротовий доступ для клієнтів кафе через Wi-Fi точки доступу з використанням WPA2-PSK;

— Вся мережа повинна бути захищена: адміністрування здійснюється через SSH, а доступ до служб і серверів обмежено за допомогою ACL;

— На сервері Debian має бути розгорнута база даних ocake_db, з доступом до неї через phpMyAdmin згідно з рольовою моделлю доступу;

— Необхідно здійснити тестування мережі: перевірити з’єднання між філіями, функціональність VPN, доступ до DNS, DHCP, Wi-Fi та Інтернету.

5 Етапи БКР та очікувані результати

Етапи розробки БКР та очікувані результати наведено у Таблиці А.1

Таблиця А.1 — Етапи БКР

| № етапу | Назва етапу | Термін виконання | | Очікувані результати |
|---|---|---|---|---|
| | | Початок | Кінець | |
| 1 | Постановка задачі | 21.03.25 | 21.03.25 | Розділ 1 |
| 2 | Аналіз технологій для створення комп’ютерних мереж | 21.03.25 | 30.03.25 | Розділ 1 |
| 3 | Аналіз та обґрунтування вибору технологій | 21.03.25 | 30.04.25 | Розділ 2 |
| 4 | Реалізація комп’ютерної мережі | 31.03.25 | 13.04.25 | Розділ 3 |
| 5 | Тестування комп’ютерної мережі | 14.04.25 | 27.04.25 | Розділ 4 |
| 6 | Підготовка тезових матеріалів для публікації | 21.04.25 | 28.04.25 | Тези |
| 7 | Оформлення пояснювальної записки та демонстраційної презентації для доповіді | 29.04.25 | 12.05.25 | ПЗ, презентація |
| 8 | Підготовка супровідної документації, перевірка відповідності нормам та проходження тесту на плагіат | 13.05.25 | 13.05.25 | ПЗ, презентація |

6 Матеріали, що подаються до захисту БКР

До захисту подаються: пояснювальна записка БКР, ілюстративні матеріали, протокол попереднього захисту БКР на кафедрі, відгук наукового керівника, анотації до БКР українською та іноземною мовами, довідка про відповідність оформлення БКР чинним вимогам.

7 Порядок контролю виконання та захисту БКР

Виконання етапів графічної та розрахункової документації БКР

контролюється науковим керівником к.т.н., проф. каф. ОТ Захарченком С. М. згідно зі встановленими термінами. Захист БКР відбувається на засіданні Екзаменаційної комісії, затвердженої наказом ректора ВНТУ.

## 8 Вимоги до оформлювання та порядок виконання БКР

8.1 При оформлюванні БКР використовуються:

8.1.1 ДСТУ 3008 : 2015 «Звіти в сфері науки і техніки. Структура та правила оформлювання»;

8.1.2 ДСТУ 8302 : 2015 «Бібліографічні посилання. Загальні положення та правила складання»;

8.1.3 методичні вказівки до виконання бакалаврських кваліфікаційних робіт для студентів спеціальності 123 «Комп'ютерна інженерія» (освітня програма «Комп'ютерна інженерія») — кафедра обчислювальної техніки, ВНТУ 2023.

8.2 Порядок виконання БКР викладено в «Положення про кваліфікаційні роботи на першому (бакалаврському) рівні вищої освіти СУЯ ВНТУ-03.02.02-П.001.01:21»

# ДОДАТОК Б

## ПРОТОКОЛ ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Назва роботи: _____«Комп'ютерна мережа кафе "О’САКЕ"»_____

Тип роботи: _____бакалаврська кваліфікаційна робота_____
(бакалаврська кваліфікаційна робота / магістерська кваліфікаційна робота)

Підрозділ _____кафедра обчислювальної техніки_____
(кафедра, факультет, навчальна група)

Коефіцієнт подібності текстових запозичень, виявлених у роботі системою StrikePlagiarism __10__%

Висновок щодо перевірки кваліфікаційної роботи (відмітити потрібне)

✓ Запозичення, виявлені у роботі, є законними і не містять ознак плагіату, фабрикації, фальсифікації. Роботу прийняти до захисту

☐ У роботі не виявлено ознак плагіату, фабрикації, фальсифікації, але надмірна кількість текстових запозичень та/або наявність типових розрахунків не дозволяють прийняти рішення про оригінальність та самостійність її виконання. Роботу направити на доопрацювання.

☐ У роботі виявлено ознаки плагіату та/або текстових маніпуляцій як спроб укриття плагіату, фабрикації, фальсифікації, що суперечить вимогам законодавства та нормам академічної доброчесності. Робота до захисту не приймається.

Експертна комісія:

_____Азаров О.Д., зав. каф. ОТ_____ _____
(прізвище, ініціали, посада) (підпис)

____Крупельницький Л.В., доц. каф ОТ_____ _____
(прізвище, ініціали, посада) (підпис)

Особа, відповідальна за перевірку _____ ___Захарченко С.М.____
(підпис) (прізвище, ініціали)

З висновком експертної комісії ознайомлений(-на)

Керівник _____ _____Захарченко С.М._проф.каф. ОТ_____
(підпис) (прізвище, ініціали, посада)

Здобувач _____ _____Шестопал А.Р._____
(підпис) (прізвище, ініціали)

# ДОДАТОК В

## ІЛЮСТРАТИВНА ЧАСТИНА

КОМП'ЮТЕРНА МЕРЕЖА КАФЕ «О’САКЕ»

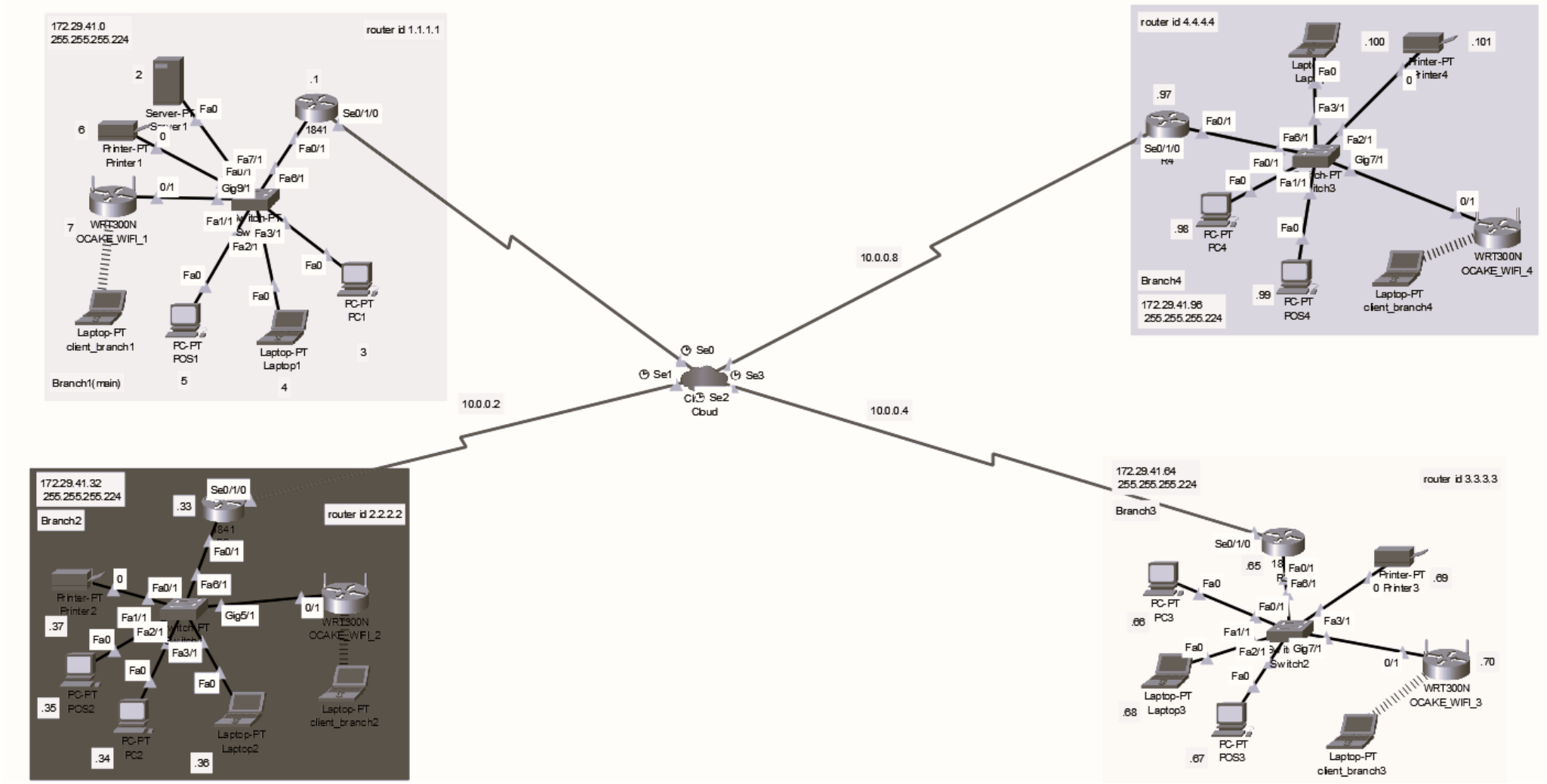


Рисунок В.1 – Логічна топологія мережі кафе «O’CAKE»

# ДОДАТОК Г

## Лістинги конфігураційних файлів

Лістинг Г.1 – Конфігурація маршрутизатора головної філії

```
R1#sh r
Building configuration...
Current configuration : 2840 bytes
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname R1
ip dhcp excluded-address 172.29.41.1 172.29.41.10
ip dhcp pool LAN1
network 172.29.41.0 255.255.255.224
default-router 172.29.41.1
dns-server 172.29.41.2
no ip cef
no ipv6 cef
username adminr1 privilege 15 secret 5 $1$mERr$7n6je7c9FKvO.o.40Rj1Q0
crypto isakmp policy 10
encr aes
authentication pre-share
group 2
crypto isakmp key VPNKEY address 10.0.0.2
crypto isakmp key VPNKEY address 10.0.0.6
crypto isakmp key VPNKEY address 10.0.0.10
crypto ipsec transform-set TS esp-aes esp-sha-hmac
crypto map VPNMAP 10 ipsec-isakmp
set peer 10.0.0.2
set transform-set TS
match address 100
crypto map VPNMAP 20 ipsec-isakmp
set peer 10.0.0.6
set transform-set TS
match address 110
crypto map VPNMAP 30 ipsec-isakmp
set peer 10.0.0.10
set transform-set TS
match address 120
ip ssh version 2
ip domain-name ocake.local
ip name-server 172.29.41.2
spanning-tree mode pvst
interface Loopback0
ip address 1.1.1.1 255.255.255.255
interface Tunnel1
ip address 192.168.1.1 255.255.255.252
mtu 1476
tunnel source Serial0/1/0.101
tunnel destination 10.0.0.2
interface Tunnel2
ip address 192.168.2.1 255.255.255.252
mtu 1476
```

```
tunnel source Serial0/1/0.102
tunnel destination 10.0.0.6
interface Tunnel3
ip address 192.168.3.1 255.255.255.252
mtu 1476
tunnel source Serial0/1/0.103
tunnel destination 10.0.0.10
interface FastEthernet0/0
no ip address
duplex auto
speed auto
shutdown
interface FastEthernet0/1
ip address 172.29.41.1 255.255.255.224
duplex auto
speed auto
interface Serial0/1/0
no ip address
encapsulation frame-relay
crypto map VPNMAP
interface Serial0/1/0.101 point-to-point
ip address 10.0.0.1 255.255.255.252
frame-relay interface-dlci 101
clock rate 2000000
interface Serial0/1/0.102 point-to-point
ip address 10.0.0.5 255.255.255.252
frame-relay interface-dlci 102
clock rate 2000000
interface Serial0/1/0.103 point-to-point
ip address 10.0.0.9 255.255.255.252
frame-relay interface-dlci 103
clock rate 2000000
interface Serial0/1/1
no ip address
clock rate 2000000
shutdown
interface Vlan1
no ip address
shutdown
router ospf 1
router-id 1.1.1.1
log-adjacency-changes
network 172.29.41.0 0.0.0.31 area 0
network 10.0.0.0 0.0.0.3 area 0
network 10.0.0.4 0.0.0.3 area 0
network 10.0.0.8 0.0.0.3 area 0
ip classless
ip flow-export version 9
access-list 100 permit gre host 192.168.1.1 host 192.168.1.2
access-list 110 permit gre host 192.168.2.1 host 192.168.2.2
access-list 120 permit gre host 192.168.3.1 host 192.168.3.2
line con 0
line aux 0
line vty 0 4
exec-timeout 5 0
login local
```

```
transport input ssh
end
```

Лістинг Г.2 – Конфігурація маршрутизатора філії 2

```
R2#sh r
Building configuration...
Current configuration : 1819 bytes
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname R2
ip dhcp excluded-address 172.29.41.33 172.29.41.40
ip dhcp pool LAN2
network 172.29.41.32 255.255.255.224
default-router 172.29.41.33
dns-server 172.29.41.2
no ip cef
no ipv6 cef
username adminr2 privilege 15 secret 5 $1$mERr$4CFVt/60iQmc.ia/CrCAa/
crypto isakmp policy 10
encr aes
authentication pre-share
group 2
crypto isakmp key VPNKEY address 10.0.0.1
crypto ipsec transform-set TS esp-aes esp-sha-hmac
crypto map VPNMAP 10 ipsec-isakmp
set peer 10.0.0.1
set transform-set TS
match address 100
ip ssh version 2
ip domain-name ocake.local
spanning-tree mode pvst
interface Loopback0
ip address 2.2.2.2 255.255.255.255
interface Tunnel1
ip address 192.168.1.2 255.255.255.252
mtu 1476
tunnel source Serial0/1/0.201
tunnel destination 10.0.0.1
interface FastEthernet0/0
no ip address
duplex auto
speed auto
shutdown
interface FastEthernet0/1
ip address 172.29.41.33 255.255.255.224
duplex auto
speed auto
interface Serial0/1/0
no ip address
encapsulation frame-relay
crypto map VPNMAP
interface Serial0/1/0.201 point-to-point
ip address 10.0.0.2 255.255.255.252
```

```
frame-relay interface-dlci 201
clock rate 2000000
interface Serial0/1/1
no ip address
clock rate 2000000
shutdown
interface Vlan1
no ip address
shutdown
router ospf 1
router-id 2.2.2.2
log-adjacency-changes
network 172.29.41.32 0.0.0.31 area 0
network 10.0.0.0 0.0.0.3 area 0
ip classless
ip flow-export version 9
access-list 100 permit gre host 192.168.1.2 host 192.168.1.1
line con 0
line aux 0
line vty 0 4
exec-timeout 5 0
login local
transport input ssh
end
```

Лістинг Г.3 – Конфігурація маршрутизатора філії 3

```
R3#sh r
Building configuration...
Current configuration : 1832 bytes
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname R3
ip dhcp excluded-address 172.29.41.65 172.29.41.75
ip dhcp pool LAN3
network 172.29.41.64 255.255.255.224
default-router 172.29.41.65
dns-server 172.29.41.2
no ip cef
no ipv6 cef
username adminr3 privilege 15 secret 5 $1$mERr$JpU75fgWPP7c43kksZEKc1
crypto isakmp policy 10
encr aes
authentication pre-share
group 2
crypto isakmp key VPNKEY address 10.0.0.1
crypto ipsec transform-set TS esp-aes esp-sha-hmac
crypto map VPNMAP 20 ipsec-isakmp
set peer 10.0.0.1
set transform-set TS
match address 110
ip ssh version 2
ip domain-name ocake.local
spanning-tree mode pvst
```

```
interface Loopback0
ip address 3.3.3.3 255.255.255.255
interface Tunnel2
ip address 192.168.2.2 255.255.255.252
mtu 1476
tunnel source Serial0/1/0.301
tunnel destination 10.0.0.5
interface FastEthernet0/0
no ip address
duplex auto
speed auto
shutdown
interface FastEthernet0/1
ip address 172.29.41.65 255.255.255.224
duplex auto
speed auto
interface Serial0/1/0
no ip address
encapsulation frame-relay
crypto map VPNMAP
interface Serial0/1/0.301 point-to-point
ip address 10.0.0.6 255.255.255.252
frame-relay interface-dlci 301
clock rate 2000000
interface Serial0/1/1
no ip address
clock rate 2000000
shutdown
interface Vlan1
no ip address
shutdown
router ospf 1
router-id 3.3.3.3
log-adjacency-changes
network 172.29.41.64 0.0.0.31 area 0
network 10.0.0.4 0.0.0.3 area 0
router rip
ip classless
ip flow-export version 9
access-list 110 permit gre host 192.168.2.2 host 192.168.2.1
line con 0
line aux 0
line vty 0 4
exec-timeout 5 0
login local
transport input ssh
end
```

Лістинг Г.4 – Конфігурація маршрутизатора філії 4

```
R4#sh r
Building configuration...
Current configuration : 1872 bytes
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
```

```
no service password-encryption
hostname R4
ip dhcp excluded-address 172.29.41.97 172.29.41.11
ip dhcp excluded-address 172.29.41.97 172.29.41.110
ip dhcp pool LAN4
network 172.29.41.96 255.255.255.224
default-router 172.29.41.97
dns-server 172.29.41.2
no ip cef
no ipv6 cef
username adminr4 privilege 15 secret 5 $1$mERr$heBMQP4AWM.Ive/aCWSY30
crypto isakmp policy 10
encr aes
authentication pre-share
group 2
crypto isakmp key VPNKEY address 10.0.0.1
crypto ipsec transform-set TS esp-aes esp-sha-hmac
crypto map VPNMAP 30 ipsec-isakmp
set peer 10.0.0.1
set transform-set TS
match address 120
ip ssh version 2
ip domain-name ocake.local
spanning-tree mode pvst
interface Loopback0
ip address 4.4.4.4 255.255.255.255
interface Tunnel3
ip address 192.168.3.2 255.255.255.252
mtu 1476
tunnel source Serial0/1/0.401
tunnel destination 10.0.0.9
interface FastEthernet0/0
no ip address
duplex auto
speed auto
shutdown
interface FastEthernet0/1
ip address 172.29.41.97 255.255.255.224
duplex auto
speed auto
interface Serial0/1/0
no ip address
encapsulation frame-relay
crypto map VPNMAP
interface Serial0/1/0.401 point-to-point
ip address 10.0.0.10 255.255.255.252
frame-relay interface-dlci 401
clock rate 2000000
interface Serial0/1/1
no ip address
clock rate 2000000
shutdown
interface Vlan1
no ip address
shutdown
router ospf 1
```

```
router-id 4.4.4.4
log-adjacency-changes
network 172.29.41.96 0.0.0.31 area 0
network 10.0.0.8 0.0.0.3 area 0
ip classless
ip flow-export version 9
access-list 120 permit gre host 192.168.3.2 host 192.168.3.1
line con 0
line aux 0
line vty 0 4
exec-timeout 5 0
login local
transport input ssh
end
```