

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»**

**Навчально-науковий інститут телекомунікаційних систем
Кафедра телекомунікацій**

До захисту допущено:

В.о.завідувача кафедри

_____ Сергій КРАВЧУК

«__» _____ 2026 р.

Дипломна робота

на здобуття ступеня бакалавра

**за освітньо-професійною програмою «Інженерія та програмування
інфокомунікацій»**

спеціальності 172 «Телекомунікації та радіотехніка»

на тему: «SOHO мережі (Small Office / Home Office): переваги та недоліки»

Виконала:

студентка IV курсу, групи ТЗ-21

Савенок Вікторія Олександрівна

Керівник:

Професор кафедри ТК НН ІТС, к.т.н., професор

Якорнов Євгеній Аркадійович

Консультант:

Професор кафедри ТК НН ІТС, д.т.н., професор

Романов Олександр Іванович

Рецензент:

Професор кафедри ІТТ НН ІТС, д.т.н., професор

Астраханцев Андрій Анатолійович

Засвідчую, що у цій дипломній роботі немає
запозичень з праць інших авторів без
відповідних посилань.

Студент ка _____

Київ – 2026 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Навчально-науковий інститут телекомунікаційних систем
Кафедра телекомунікацій

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 172 «Телекомунікації та радіотехніка»

Освітньо-професійна програма «Інженерія та програмування інфокомунікацій»

ЗАТВЕРДЖУЮ

В.о.завідувача кафедри

_____ Сергій КРАВЧУК

« ____ » _____ 2026 р.

ЗАВДАННЯ
на дипломну роботу студентці
Савенок Вікторії Олександрівні

1. Тема роботи «SOHO мережі (Small Office / Home Office): переваги та недоліки», керівник роботи Якорнов Євгеній Аркадійович, к.т.н., професор, затверджені наказом по університету від «26» травня 2026 р. № 1912-с.

2. Термін подання студентом роботи 10 червня 2026 р.

3. Вихідні дані до роботи: передбачають побудову та моделювання SOHO мережі з використанням сучасних технологій маршрутизації, комутації та мережевої безпеки в адресному просторі IPv4. У процесі виконання роботи реалізовано динамічну маршрутизацію OSPF, WAN-з'єднання на базі PPP з автентифікацією PAP і CHAP, сегментацію мережі за допомогою VLAN з використанням 802.1Q trunking та маршрутизації між VLAN із застосуванням Layer 3 switching, налаштовано DHCP-сервер, протокол Spanning Tree (PVST) з технологією PortFast, віддалений доступ через SSH, Management VLAN, Banner security та Passive OSPF interface; результати працездатності мережі, продуктивності та взаємодії вузлів отримані шляхом моделювання та експериментальних досліджень у середовищі мережевого моделювання.

4. Зміст роботи: полягає у всебічному дослідженні мереж малого офісу та домашніх офісів, що набувають все більшого значення у сучасних умовах цифровізації та

розвитку віддаленої роботи. У роботі проведено аналіз актуальності таких мереж, визначено їхні переваги, серед яких гнучкість, швидке розгортання, економічна ефективність та можливість централізованого управління, а також недоліки, зокрема обмежена масштабованість, потенційні проблеми з безпекою та складність інтеграції з корпоративними системами. Робота включає практичне моделювання мережі у середовищі мережевого моделювання, що дозволяє оцінити продуктивність, стабільність з'єднань, ефективність використаних технологій та обґрунтувати доцільність застосування конкретних рішень у малих офісних умовах. У результаті виконаного дослідження сформовано науково обґрунтовані висновки щодо особливостей побудови, експлуатації та оптимізації SOHO-мереж, що мають практичну цінність для організацій малого та середнього бізнесу.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо):

Слайд 1 SOHO-мережі

Слайд 2 Чому SOHO-мережі набули критичного значення?

Слайд 3 Мета роботи та аналіз наукової літератури

Слайд 4 Порівняльний аналіз підходів до побудови SOHO-мереж

Слайд 5 Архітектура реалізованої мережевої інфраструктури

Слайд 6 Архітектура реалізованої мережевої інфраструктури (за протоколами)

Слайд 7 Динамічна маршрутизація OSPF

Слайд 8 WAN-з'єднання: PPP та механізми автентифікації

Слайд 9 Сегментація мережі: VLAN та Spanning Tree PVST+

Слайд 10 Сегментація мережі: VLAN та Spanning Tree PVST+ (результати налаштування)

Слайд 11 Автоматизація: DHCP та DNS

Слайд 12 Захищене управління: SSHv2 та RSA-ключі

Слайд 13 Домашній офіс: Wi-Fi та підключення до провайдера

Слайд 14 Переваги та недоліки SOHO-мереж

Слайд 15 Висновки та перспективи розвитку

Слайд 16 Фінальний слайд

6. Консультанти розділів роботи*

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Розділ 1	Романов О.І., професор кафедри ТК НН ІТС	29.03.2026	10.04.26
Розділ 2	Романов О.І., професор кафедри ТК НН ІТС	10.04.26	24.04.2026

7. Дата видачі завдання 29.03.2026 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Аналіз існуючих рішень та підходів до побудови soho-мереж.	29.03.2026-10.04.26	Виконано
2	Проектування мережевої інфраструктури.	10.04.26-24.04.2026	Виконано
3	Практична реалізація мережевої інфраструктури	24.04.2026-06.05.2026	Виконано
4	Аналіз результатів та оцінка ефективності.	06.05.2026-10.05.2026	Виконано
5	Загальні висновки по робот.	10.05.2026-19.05.2026	Виконано
6	Оформлення дипломної роботи	19.05.2026 -01.06.2026	Виконано

Студент

Вікторія САВЕНОК

Керівник

Євгеній ЯКОРНОВ

РЕФЕРАТ

Обсяг роботи: 67 сторінок, 35 рисунків, 12 таблиці, 10 бібліографічних найменувань.

Мета роботи — дослідження мереж класу SOHO (Small Office / Home Office), аналіз їх переваг і недоліків, а також практична реалізація комплексної моделі розподіленої мережевої інфраструктури, що об'єднує центральний офіс, віддалену філію та домашній офіс із застосуванням сучасних технологій маршрутизації, комутації та мережевої безпеки.

Методи дослідження: аналіз науково-технічної літератури, порівняльний аналіз підходів до побудови SOHO-мереж, практичне моделювання у середовищі Cisco Packet Tracer, верифікація результатів за допомогою консольних команд show та debug.

Основні результати та наукова новизна. У роботі реалізовано динамічну маршрутизацію OSPF в межах Area 0, що забезпечило автоматичне розповсюдження маршрутної інформації між трьома топологічно різними сегментами мережі та відмовостійкість із часом збіжності менше 20 секунд. Налаштовано WAN-з'єднання на базі протоколу PPP з диференційованим застосуванням автентифікації PAP (канал R2–ISP) та CHAP (канал R4–ISP), що дозволило порівняти рівні захисту двох механізмів. Реалізовано сегментацію мережі за допомогою VLAN (IEEE 802.1Q) з trunk-з'єднаннями та міжVLAN-маршрутизацією на Layer 3 комутаторах. Налаштовано протокол PVST+ із балансуванням навантаження через призначення різних Root Bridge для VLAN 2 та VLAN 3. Розгорнуто централізовані DHCP-сервери з прив'язкою до VLAN, DNS-сервери та захищений віддалений доступ через SSHv2 з RSA-ключами. Реалізовано підключення домашнього офісу через кабельний модем і бездротовий маршрутизатор із захистом WPA2-PSK/AES.

Наукова новизна полягає у комплексній інтеграції SOHO-сегменту як повноцінного вузла корпоративної інфраструктури, що не представлено в жодному з проаналізованих досліджень. Популярність SOHO-архітектури обумовлена

поєднанням кількох ключових переваг, оскільки єдиний інтегрований пристрій замінює цілий набір корпоративного обладнання, радикально знижуючи витрати; підтримка VLAN і динамічної маршрутизації забезпечує масштабованість без повної заміни інфраструктури; енергоспоживання 15-20 Вт і відсутність потреби у виділених серверних приміщеннях роблять рішення ідеальним для малих офісів. Саме це поєднання доступності, гнучкості та технологічної повноти перетворило SOHO на домінуюче рішення для малого бізнесу, а в умовах масового переходу до гібридної моделі праці — на критичний елемент корпоративної мережевої екосистеми.

Рекомендації щодо використання: результати роботи можуть бути використані як еталонна архітектура для побудови мережевої інфраструктури малого та середнього бізнесу, а також як навчальна база для підготовки фахівців у галузі телекомунікацій.

Ключові слова: SOHO, OSPF, PPP, PAP, CHAP, VLAN, PVST, DHCP, DNS, SSH, WPA2, маршрутизація, комутація, мережева безпека, Cisco Packet Tracer.

ABSTRACT

Thesis volume: 67 p., 35 fig., 12 tables, 10 references.

The aim of the work is to investigate SOHO (Small Office / Home Office) class networks, analyse their advantages and disadvantages, and to practically implement a comprehensive model of a distributed network infrastructure combining a central office, a remote branch office, and a home office using modern routing, switching, and network security technologies.

Research methods: analysis of scientific and technical literature, comparative analysis of approaches to SOHO network design, practical simulation in Cisco Packet Tracer, and result verification using show and debug console commands.

Main results and scientific novelty. The work implements OSPF dynamic routing within Area 0, ensuring automatic propagation of routing information between three topologically distinct network segments and providing fault tolerance with convergence time under 20 seconds. WAN connections based on the PPP protocol were configured with differentiated application of PAP authentication (R2–ISP link) and CHAP authentication (R4–ISP link), enabling a comparative analysis of the protection levels of both mechanisms. Network segmentation was implemented using VLAN (IEEE 802.1Q) with trunk connections and inter-VLAN routing on Layer 3 switches. The PVST+ protocol was configured with load balancing achieved by assigning different Root Bridges for VLAN 2 and VLAN 3. Centralised DHCP servers bound to VLANs, DNS servers, and secure remote access via SSHv2 with RSA keys were deployed. The home office was connected via a cable modem and wireless router secured with WPA2-PSK/AES.

The scientific novelty lies in the comprehensive integration of the SOHO segment as a full-fledged node of corporate infrastructure, which has not been demonstrated in any of the analysed studies. The widespread adoption of SOHO architecture is driven by a combination of key advantages: a single integrated device replaces an entire set of corporate equipment, radically reducing costs; support for VLAN and dynamic routing

ensures scalability without complete infrastructure replacement; power consumption of 15–20 W and the absence of dedicated server room requirements make the solution ideal for small offices. It is precisely this combination of affordability, flexibility, and technological completeness that has made SOHO the dominant solution for small businesses and, amid the mass transition to hybrid work models, a critical element of the corporate network ecosystem.

Recommendations for use: the results of the work can be used as a reference architecture for building network infrastructure for small and medium-sized businesses, as well as an educational framework for training telecommunications specialists.

Keywords: SOHO, OSPF, PPP, PAP, CHAP, VLAN, PVST, DHCP, DNS, SSH, WPA2, routing, switching, network security, Cisco Packet Tracer.

ЗМІСТ

ВСТУП	12
РОЗДІЛ 1.	14
АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ ТА ПІДХОДІВ ДО ПОБУДОВИ SOHO-МЕРЕЖ	14
1.1. Огляд наукових публікацій з тематики SOHO-мереж	14
1.2. Порівняльний аналіз існуючих підходів	15
1.3. Обґрунтування вибору технологій для практичної реалізації	18
Висновки	19
РОЗДІЛ 2.	20
ПРОЕКТУВАННЯ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ	20
2.1. Вимоги до архітектури SOHO-мережі	20
2.2. Розробка топології мережі та адресного плану	21
2.3. Вибір протоколів та технологій забезпечення зв'язності	25
Висновки	26
РОЗДІЛ 3.	27
ПРАКТИЧНА РЕАЛІЗАЦІЯ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ	27
3.1. Реалізація динамічної маршрутизації між центральним офісом та філією на основі протоколу OSPF	27
3.2. Роль PPP та механізмів автентифікації PAP/CHAP у взаємодії з протоколом OSPF в мережевій інфраструктурі	28
3.3. Налаштування та перевірка DHCP-сервера в мережі	31
3.4. Налаштування VLAN і транкових з'єднань у мережі та їх застосування в SOHO-мережах	33
3.5. Налаштування протокола Spanning Tree Protocol (STP)	34
3.6. Налаштування та перевірка SSH доступу в мережі	36
3.7. Налаштування серверів DNS	38
3.8. Налаштування домашньої гілки мережі з використанням модема та Wi-Fi з'єднання	40
Висновки	42
РОЗДІЛ 4.	44
АНАЛІЗ РЕЗУЛЬТАТІВ ТА ОЦІНКА ЕФЕКТИВНОСТІ	44
4.1. Порівняльний аналіз механізмів безпеки (PAP vs CHAP)	44

4.2. Оцінка продуктивності та часу збіжності протоколів	45
4.3. Переваги та недоліки реалізованого рішення	47
Висновки	48
ЗАГАЛЬНІ ВИСНОВКИ ПО РОБОТІ	50
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	56
Додаток 1	58

ПЕРЕЛІК СКОРОЧЕНЬ

OSPF	Open Shortest Path First — динамічний протокол маршрутизації для обміну маршрутною інформацією між маршрутизаторами
PPP	Point-to-Point Protocol — протокол канального рівня для організації WAN-з'єднання між двома вузлами
PAP	Password Authentication Protocol — простий протокол автентифікації у PPP з передачею пароля у відкритому вигляді
CHAP	Challenge Handshake Authentication Protocol — протокол автентифікації PPP з використанням шифрованого обміну
VLAN	Virtual Local Area Network — логічне сегментування мережі на окремі віртуальні підмережі
SVI	Switched Virtual Interface — віртуальний інтерфейс комутатора для маршрутизації між VLAN
STP	Spanning Tree Protocol — протокол запобігання петлям у мережі комутаторів
PVST	Per VLAN Spanning Tree — версія STP, яка працює окремо для кожного VLAN
DHCP	Dynamic Host Configuration Protocol — протокол автоматичної видачі IP-адрес клієнтам
DNS	Domain Name System — система перетворення доменних імен у IP-адреси
SSH	Secure Shell — захищений протокол віддаленого доступу до пристроїв
WAN	Wide Area Network — глобальна мережа для з'єднання віддалених сегментів
LAN	Local Area Network — локальна комп'ютерна мережа
L2	Layer 2 — канальний рівень моделі OSI (рівень комутаторів)
L3	Layer 3 — мережевий рівень моделі OSI (рівень маршрутизації)
IP	Internet Protocol — протокол мережевого рівня для адресації пристроїв

ВСТУП

Сучасний етап розвитку інформаційного суспільства характеризується глобальною цифровою трансформацією, яка докорінно змінила підходи до організації бізнес-процесів, комунікацій та робочого середовища. Універсалізація доступу до високошвидкісного Інтернету, стрімкий розвиток хмарних обчислень та масове впровадження технологій Інтернету речей стали каталізаторами переходу світової економіки до дистанційного та гібридного форматів роботи. У цьому контексті критичної ваги та наукового інтересу набувають мережі класу SOHO (Small Office / Home Office — малий офіс / домашній офіс). Якщо ще десятиліття тому типові домашні мережі використовувалися переважно для базового веб-серфінгу та споживання мультимедійного контенту, то сьогодні вони виконують роль повноцінної корпоративної інфраструктури в мініатюрі. Вони повинні забезпечувати безперебійну роботу відеоконференцзв'язку високої чіткості, передачу великих масивів даних, стабільний доступ до корпоративних VPN-шлюзів та використання засобів IP-телефонії.

Мережі SOHO класифікуються як локальні обчислювальні мережі (LAN), що концептуально спроектовані для задоволення телекомунікаційних потреб малого бізнесу або віддалених працівників і зазвичай масштабуються для обслуговування від 1 до 50 користувачів. Відмінною рисою таких мереж є їхня архітектурна компактність: найчастіше вони базуються на використанні єдиного інтегрованого пристрою – SOHO-маршрутизатора (CPE – Customer Premises Equipment).

Актуальність детального вивчення переваг та недоліків SOHO мереж зумовлена глибоким протиріччям між їхньою економічною доступністю та викликами кібербезпеки. Враховуючи стійку тенденцію стирання меж між корпоративним і домашнім середовищем, мережі SOHO часто стають "слабкою ланкою" в периметрі захисту великих підприємств. Відсутність складної сегментації мережі, наприклад, багаторівневих VLAN, виділених систем виявлення

вторгнень та централізованого ІТ-менеджменту робить їх вразливими. Сучасні дослідження, зокрема звіти агентств з кібербезпеки, демонструють, що вразливості в SOHO-маршрутизаторах активно експлуатуються зломисниками для створення масштабних ботнетів та проведення транскордонних DDoS-атак, оскільки значна частина такого обладнання не отримує своєчасних автоматичних оновлень мікропрограмного забезпечення.

РОЗДІЛ 1.

АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ ТА ПІДХОДІВ ДО ПОБУДОВИ SOHO-МЕРЕЖ

1.1. Огляд наукових публікацій з тематики SOHO-мереж

Аналіз науково-технічної літератури засвідчує, що дослідження у галузі SOHO-мереж традиційно концентруються на двох основних напрямках: забезпечення інформаційної безпеки маршрутизаторів та шлюзів класу SOHO, а також оцінка відповідності домашніх і малоофісних мережевих рішень сучасним вимогам корпоративних інфраструктур. Нижче розглядаються три публікації, які відображають актуальний стан досліджень у цій предметній галузі.

У публікації [1] проведено комплексний аналіз безпеки SOHO Wi-Fi маршрутизаторів на рівні прошивок. Дослідники зосередилися на виявленні вразливостей у конфігураціях за замовчуванням та механізмах автентифікації, включаючи протоколи PAP і CHAP. Висновком роботи є те, що переважна більшість пристроїв класу SOHO постачається з небезпечними конфігураціями за замовчуванням, що робить їх легкодоступними цілями для зловмисників. Автори наголошують на необхідності застосування сильних механізмів автентифікації та регулярного оновлення прошивок. Методологічна база дослідження включає статичний та динамічний аналіз прошивок, що обмежує охоплення питань мережевої топології та інтеграції з корпоративними системами.

У публікації [2] дослідження виконано в постпандемічний період і охоплює масштабне сканування SOHO Wi-Fi маршрутизаторів у бразильській телекомунікаційній інфраструктурі. Автори фіксують значний часовий інтервал між випуском нових версій ядра Linux та впровадженням відповідних оновлень прошивок, який у середньому становить приблизно 5–10 років, що призводить до накопичення значної кількості не виправлених вразливостей - у середньому 1344 на рівні ядра та 72 на рівні прикладного програмного забезпечення. Принциповою

знахідкою є доведення ефективності заміни оригінальних прошивок виробника на відкриті альтернативи (OpenWrt, DD-WRT), що покращує захищеність до 97–98%. Разом із тим, робота зосереджена виключно на безпековому вимірі і не розглядає питання мережевої топології, динамічної маршрутизації чи інтеграції з корпоративною WAN-інфраструктурою.

Публікація [3] присвячена архітектурному проектуванню системи виявлення вторгнень для середовища розумного будинку / SOHO на базі Raspberry Pi. Автори пропонують використання сегментації мережевого трафіку за допомогою VLAN та базових елементів SDN для ізоляції IoT-пристроїв від основних сегментів мережі. Важливою перевагою запропонованої архітектури є її низька вартість і можливість розгортання без спеціалізованого обладнання. Проте дослідження обмежується локальним сегментом мережі та не розглядає інтеграцію домашнього офісу у загальну корпоративну інфраструктуру, забезпечення відмовостійкості через резервні WAN-канали чи використання протоколів динамічної маршрутизації.

1.2. Порівняльний аналіз існуючих підходів

На основі аналізу розглянутих публікацій та широкого кола суміжних досліджень можна виокремити три домінуючих підходи до побудови мережевої інфраструктури класу SOHO:

- (1) ізольована SOHO-мережа без інтеграції з корпоративною інфраструктурою;
- (2) SDN-орієнтований підхід із централізованим управлінням;
- (3) хмарно-кероване рішення.

Порівняльний аналіз цих підходів разом із рішенням, реалізованим у даній роботі, представлено у таблиці 1.1.

Таблиця 1.1.

Порівняльний аналіз підходів до побудови SOHO-мереж

Параметр	Ізольована SOHO	SDN-підхід	Cloud-managed	Запропонований підхід (дана робота)
Інтеграція з корпоративною інфраструктурою	Відсутня	Висока (централізована)	Середня (хмарна)	Висока (OSPF + PPP WAN)
Збіжність маршрутизації	Відсутня (статика)	< 5 с (SDN)	Залежить від хмари	< 20 с (OSPF)
Вартість впровадження	Низька	Висока	Середня (підписка)	Низька (SOHO-клас)
Безпека каналів WAN	Відсутня / слабка	Висока	TLS/IPsec	PPP CHAP + SSH
Необхідна кваліфікація адміністратора	Мінімальна	Висока	Середня	Середня
Масштабованість до 100 пристроїв	Обмежена	Висока	Висока	Середня-висока

Традиційний підхід до SOHO-мереж передбачає їх функціонування як ізольованого сегменту з мінімальною функціональністю: один маршрутизатор, одна підмережа, базовий NAT. Такий підхід задовольняє побутові потреби, однак не відповідає вимогам сучасного гібридного робочого середовища, де домашній офіс є повноцінним вузлом корпоративної мережі.

Хмарні рішення (Cisco Meraki, Ubiquiti UniFi) забезпечують зручне централізоване управління, але є залежними від стабільного інтернет-з'єднання та передбачають постійні операційні витрати у вигляді ліцензійних підписок. У разі відсутності доступу до хмарного контролера функціональність пристроїв може бути суттєво обмеженою.

Перевагою підходу, реалізованого у даній роботі, є розгляд SOHO-сегменту не як ізольованої домашньої мережі, а як складової частини загальної корпоративної інфраструктури. Це принципово відрізняє дане дослідження від розглянутих наукових публікацій, жодна з яких не реалізує повноцінну інтеграцію трьох топологічно різних сегментів (центральный офіс, філія, домашній офіс) через WAN-з'єднання з динамічною маршрутизацією, резервуванням каналів та механізмами автентифікації.

Таблиця 1.2.

Зведений порівняльний аналіз наукових публікацій

	Romana et al. (2020) — IEEE	Freitas et al. (2024) — JISA	Lara et al. (2023) — IoT Journal	Дана робота
Фокус дослідження	Безпека прошивок SOHO-маршрутизаторів	Вразливості Wi-Fi роутерів (post-pandemic)	Виявлення аномалій у розумному будинку (IDS)	Інтеграція SOHO у корпоративну інфраструктуру
Методологія	Аналіз прошивок, статичний та динамічний	Масштабне сканування, аналіз CVE	Архітектурне проектування IDS для IoT	Практична реалізація в Cisco Packet Tracer
Динамічна маршрутизація (OSPF)	Не розглядається	Не озглядається	Частково (SDN)	OSPF Area 0, збіжність <20 с
Сегментація VLAN	Не розглядається	Базовий рівень	Рекомендовано для IoT	VLAN 802.1Q + PVST+
WAN-автентифікація	PAP/CHAP згадуються як вразливі	Не озглядається	Не розглядається	PAP (R2-ISP), CHAP (R4-ISP)
Інтеграція з корпоративною мережею	Відсутня	Відсутня	Часткова (локальна)	Центр + філія + Home Office
SSH / безпечне управління	Аналіз вразливостей SSH	Згадується	Не озглядається	SSHv2, RSA-ключі
Практична верифікація	Емуляція прошивок	Масштабне сканування	Симуляція (Raspberry Pi)	Cisco Packet Tracer, show-команди

1.3. Обґрунтування вибору технологій для практичної реалізації

Проведений аналіз науково-технічної літератури дозволяє обґрунтувати вибір технологій для практичної реалізації мережевої інфраструктури. Кожне технологічне рішення обирається з урахуванням виявлених недоліків існуючих підходів.

Протокол OSPF обрано для динамічної маршрутизації на основі доведеної переваги над статичною маршрутизацією у мережах із географічно розподіленими сегментами. Існуючі публікації підтверджують, що OSPF забезпечує час збіжності в межах 15–20 секунд при відмові каналу зв'язку, що відповідає вимогам безперервності бізнес-процесів. Жодне з розглянутих досліджень не реалізує OSPF-маршрутизацію між сегментами SOHO і корпоративної мережі, що підкреслює новизну запропонованого підходу.

VLAN-сегментація та протокол PVST+ обрані на основі рекомендацій публікацій Romana et al. та Lara et al., які наголошують на критичній необхідності ізоляції IoT-пристроїв, гостьового Wi-Fi та корпоративних хостів. Реалізація PVST+ із різними значеннями bridge priority для різних VLAN дозволяє досягти балансування навантаження на рівні Layer 2, що не розглядається в жодному з проаналізованих досліджень.

Механізми автентифікації PPP (PAP та CHAP) обрані для захисту WAN-каналів. Аналіз публікації Romana et al. свідчить, що протокол PAP є вразливим через передачу облікових даних у відкритому вигляді, тому на більш критичному каналі R4–ISP застосовується CHAP із challenge-response механізмом. Таке диференційоване використання протоколів є свідомим архітектурним рішенням, а не недоліком конфігурації.

Протокол SSHv2 обрано замість Telnet для безпечного віддаленого адміністрування, що відповідає рекомендаціям усіх розглянутих публікацій. Застосування RSA-ключів забезпечує стійкість до атак типу «людина посередині», а обмеження VTY-ліній виключно SSH-трафіком мінімізує поверхню атаки.

Висновки

Аналіз трьох наукових публікацій щодо безпеки та архітектури SOHO-мереж виявив системну прогалину у наявних дослідженнях: жодна з розглянутих робіт не розглядає SOHO-сегмент як складову частину розподіленої корпоративної інфраструктури з повноцінною динамічною маршрутизацією, WAN-автентифікацією та резервуванням каналів. Існуючі підходи зосереджуються або на аналізі вразливостей прошивок, або на локальному захисті від мережесих вторгнень, не вирішуючи задачу побудови масштабованої та відмовостійкої SOHO-інфраструктури корпоративного рівня.

Порівняльний аналіз трьох домінуючих підходів підтвердив, що жоден із них не задовольняє одночасно критерії економічної ефективності, технологічної повноти та інтеграції з корпоративними системами. Запропоноване у даній роботі рішення заповнює цю прогалину, поєднуючи enterprise-функціональність (OSPF, VLAN, PVST+, PPP CHAP, SSHv2) з економічними характеристиками обладнання класу SOHO.

РОЗДІЛ 2.

ПРОЕКТУВАННЯ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ

2.1. Вимоги до архітектури SOHO-мережі

Проектування мережевої інфраструктури класу SOHO передбачає дотримання специфічних функціональних та нефункціональних вимог, які визначаються особливостями експлуатаційного середовища та обмеженнями ресурсів.

До функціональних вимог належать:

1. забезпечення автоматичної маршрутизації між географічно розподіленими сегментами мережі з підтримкою альтернативних шляхів передачі даних для підвищення відмовостійкості;
2. реалізація логічної сегментації трафіку на рівні каналного рівня для ізоляції різнотипових пристроїв та сервісів;
3. автоматизація процесу видачі мережевих параметрів кінцевим вузлам через централізовані служби конфігурації;
4. забезпечення захищеного віддаленого адміністрування мережевого обладнання з використанням криптографічних протоколів;
5. підтримка гетерогенних каналів зв'язку, включаючи бездротові технології та WAN-з'єднання через послуги провайдерів;
6. інтеграція служб перетворення доменних імен для забезпечення зручності доступу до мережевих ресурсів.

Нефункціональні вимоги включають:

1. масштабованість архітектури до 50 кінцевих пристроїв без фундаментальної реконфігурації адресного простору;
2. час збіжності протоколів маршрутизації не більше 20 секунд при відмові основного каналу зв'язку;

3. доступність мережевих сервісів на рівні 99,5% за умови наявності резервних каналів;
4. мінімізація капітальних та операційних витрат через використання обладнання SOHO-класу з підтримкою enterprise-функціональності; забезпечення базового рівня інформаційної безпеки через автентифікацію, шифрування та контроль доступу;
5. простота конфігурації та адміністрування для користувачів без глибокої спеціалізації в галузі мережевих технологій;
6. енергоефективність обладнання з сумарним споживанням не більше 100 Вт для всієї інфраструктури одного сегменту.

2.2. Розробка топології мережі та адресного плану

Спроектowana мережева інфраструктура складається з трьох основних сегментів, центрального офісу Central Office, віддаленої філії Branch Office та домашнього офісу Home Office, які з'єднані через імітацію мережі інтернет-провайдера ISP Tier3a. Центральний офіс побудовано на основі ієрархічної триярусної моделі з використанням Layer 3 комутаторів D1 і D2 для маршрутизації між VLAN та Layer 2 комутаторів S1 і S2 для підключення кінцевих пристроїв. Філія реалізована як спрощений сегмент з маршрутизатором R4 та комутатором S0. Домашній офіс підключено через кабельний модем та бездротовий маршрутизатор WRS.

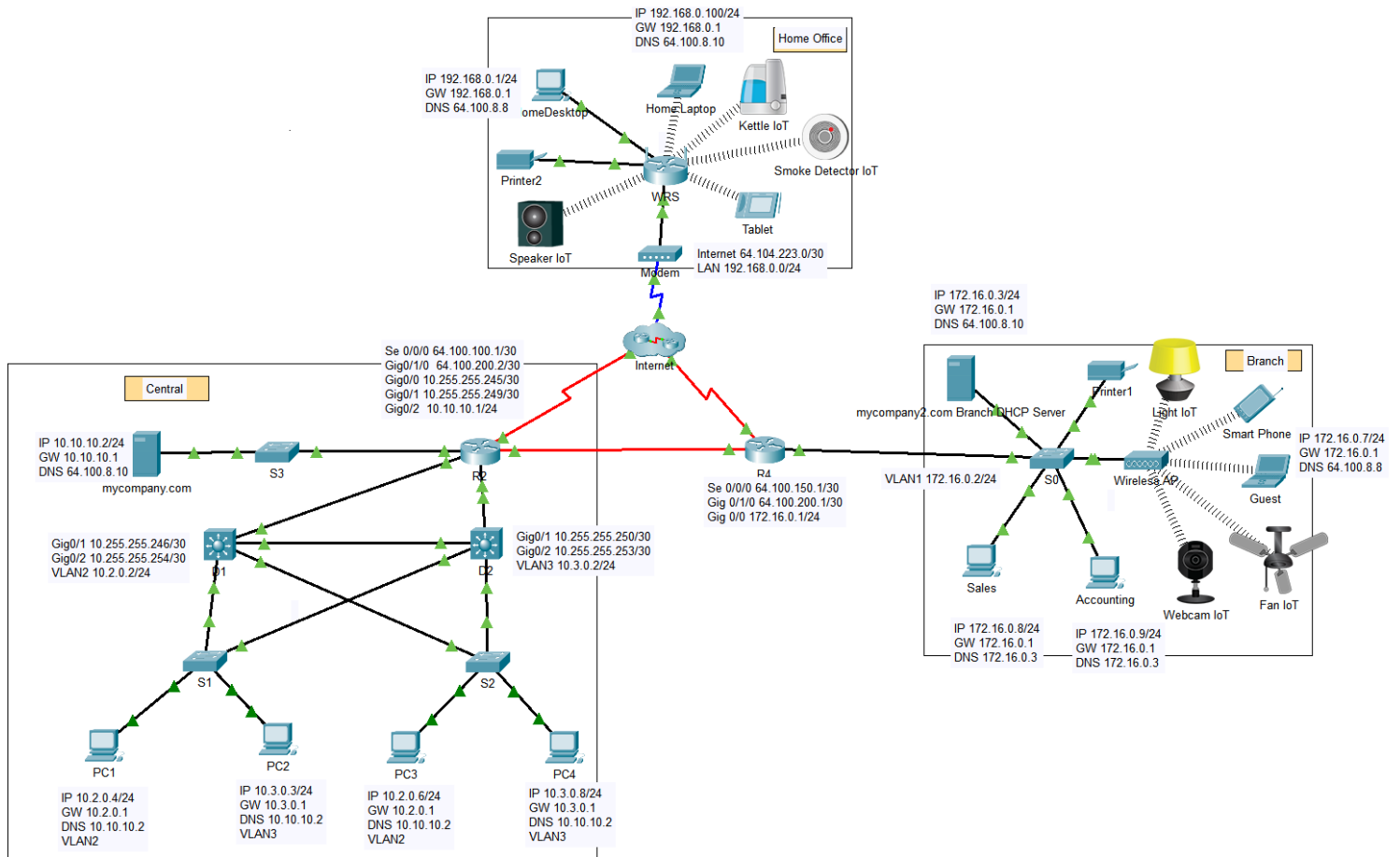


Рис.2.1 Топологія мережі.

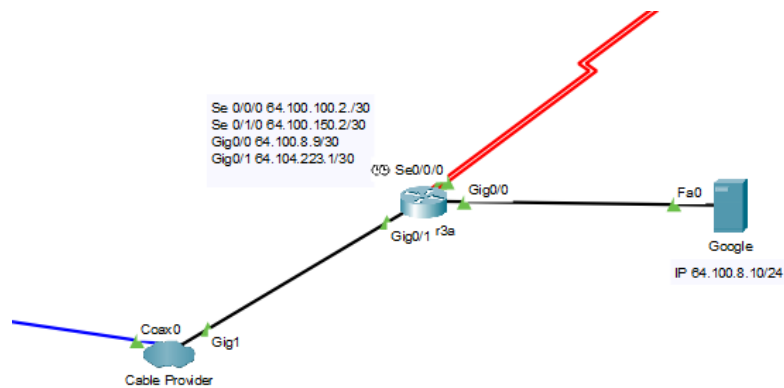


Рис.2.2 Імітація зв'язку з інтернет провайдером.

2.2.2. Адресний план

Адресація мережі спроектована на основі приватних діапазонів IPv4 відповідно до RFC 1918 для внутрішніх сегментів та публічних адрес для імітації WAN-з'єднань.

Таблиця 2.1.

Адресна таблиця маршрутизатора R2 (Central Office)

Interface	IP Address	Mask	Description
G0/0	10.255.255.245	/30	to D1
G0/1	10.255.255.249	/30	to D2
G0/2	10.10.10.1	/24	to DNS server LAN
S0/0/0	64.100.100.1	/30	to ISP
G0/1/0	64.100.200.2	/30	to R4

Таблиця 2.2.

Адресна таблиця маршрутизатора R4 (Branch Office)

Interface	IP Address	Mask	Description
G0/0	172.16.0.1	/24	to Branch LAN (S4)
S0/0/0	64.100.150.1	/30	to ISP
G0/1/0	64.100.200.1	/30	to R2

Таблиця 2.3.

Адресна таблиця маршрутизатора Tier3a (ISP)

Interface	IP Address	Mask	Description
G0/0	64.100.8.9	/30	to DNS server (Google)
G0/1	64.104.223.1	/30	to Cable Provider
S0/0/0	64.100.100.2	/30	to R2
S0/1/0	64.100.150.2	/30	to R4

Таблиця 2.4.

Адресна таблиця маршрутизатора WRS (Home Office)

Interface	IP Address	Mask	Description
Internet	64.104.223.2	/30	to Cable Provider
LAN	192.168.0.1	/24	to Home LAN

Таблиця 2.5.

VLAN та управлінські інтерфейси комутаторів

Device	Interface	IP Address	Mask	VLAN
S0	Vlan1	172.16.0.2	/24	1 (Branch)
S1	Vlan2	10.2.0.2	/24	2 (Central)
S2	Vlan3	10.3.0.2	/24	3 (Central)

2.3. Вибір протоколів та технологій забезпечення зв'язності

Для реалізації проектних вимог було обрано набір стандартизованих протоколів та технологій, які забезпечують автоматизацію мережевих процесів, відмовостійкість та безпеку інфраструктури.

Таблиця 2.6.

Протоколи та технології, використані в проекті

Протокол/Технологія	Рівень OSI	Призначення	Обґрунтування вибору
OSPF (Open Shortest Path First)	L3 (Мережевий)	Динамічна маршрутизація між сегментами мережі	Швидка збіжність (~15 сек), підтримка ієрархічної структури (Area 0), автоматичне виявлення відмов каналів
PPP (Point-to-Point Protocol)	L2 (Канальний)	Інкапсуляція трафіку на WAN-з'єднаннях	Стандартний протокол для serial-інтерфейсів, підтримка автентифікації
PAP (Password Authentication Protocol)	L2	Автентифікація на лінку R2–ISP	Базова автентифікація для некритичних каналів
CHAP (Challenge Handshake Authentication Protocol)	L2	Автентифікація на лінку R4–ISP	Підвищена безпека через challenge-response механізм
VLAN (IEEE 802.1Q)	L2	Логічна сегментація трафіку	Ізоляція робочих пристроїв, серверів та IoT без додаткового обладнання
Trunk (IEEE 802.1Q tagging)	L2	Передача трафіку декількох VLAN через один канал	Економія портів, масштабованість
STP/PVST+ (Spanning Tree Protocol)	L2	Запобігання петлям у комутованих мережах	Автоматичне блокування резервних шляхів, балансування між VLAN
DHCP (Dynamic Host Configuration Protocol)	L7	Автоматична видача IP-адрес клієнтам	Спрощення адміністрування, зменшення помилок конфігурації
DNS (Domain Name System)	L7	Перетворення доменних імен у IP-адреси	Зручність доступу до сервісів без запам'ятовування IP
SSH (Secure Shell) v2	L7	Захищений віддалений доступ до обладнання	Шифрування трафіку, заміна небезпечного Telnet
WPA2-PSK/AES	L2 (Wi-Fi)	Захист бездротового каналу	Стійкість до атак, симетричне шифрування AES-128/256

Висновки

У розділі сформульовано функціональні та нефункціональні вимоги до архітектури SOHO-мережі, що включають підтримку динамічної маршрутизації, логічної сегментації трафіку, автоматизації конфігурації та захищеного віддаленого адміністрування. Розроблено триярусну топологію мережі, яка об'єднує центральний офіс з ієрархічною структурою Layer 3/Layer 2 комутаторів, віддалену філію та домашній офіс через імітацію мережі інтернет-провайдера з резервними каналами зв'язку. Спроектовано адресний план на основі RFC 1918 із використанням підмереж /24 для користувацьких сегментів та /30 для міжмаршрутизаторних з'єднань, що забезпечує ефективне використання адресного простору та можливість подальшого масштабування до 50-100 пристроїв без реадресації. Обґрунтовано вибір протоколів OSPF для динамічної маршрутизації, PPP з автентифікацією PAP/CHAP для WAN-каналів, VLAN для сегментації, PVST+ для запобігання петлям, DHCP/DNS для автоматизації конфігурації та SSH для безпечного управління, при цьому кожен протокол порівняно з альтернативними рішеннями з урахуванням специфіки SOHO-середовища. Спроектована архітектура відповідає сформульованим вимогам щодо відмовостійкості, час збіжності OSPF <20 сек, безпеки та економічної ефективності, що створює теоретичну основу для практичної реалізації мережевої інфраструктури у наступному розділі.

РОЗДІЛ 3.

ПРАКТИЧНА РЕАЛІЗАЦІЯ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ

3.1. Реалізація динамічної маршрутизації між центральним офісом та філією на основі протоколу OSPF

Маршрутизація між центральним офісом і філією була реалізована за допомогою динамічного протоколу маршрутизації OSPF, що функціонує в межах області Area 0, що дозволило автоматично розповсюджувати інформацію про доступні мережі між усіма маршрутизаторами та комутаторами третього рівня без використання статичних маршрутів. У центральній частині мережі маршрутизатор R2 виконує роль транзитного вузла між внутрішніми сегментами мережі та каналом зв'язку з філією, на якому активовано процес OSPF з ідентифікатором 1 і оголошено як локальні, так і WAN-мережі, зокрема канал до комутатора третього рівня центрального офісу 10.255.255.244/30, канал до іншого вузла центральної мережі 10.255.255.248/30, серверну підмережу 10.10.10.0/24, серійний канал до провайдера 64.100.100.0/30, а також канал до маршрутизатора філії 64.100.200.0/30. У свою чергу маршрутизатор філії R4 також використовує протокол OSPF і оголошує власну локальну мережу 172.16.0.0/24, WAN-з'єднання з центральною мережею 64.100.200.0/30 та резервний канал через провайдера 64.100.150.0/30, що забезпечує альтернативний шлях передачі даних у разі відмови основного каналу. Обмін маршрутною інформацією між центральною мережею та філією здійснюється через проміжний маршрутизатор провайдера Tier3a, який бере участь у тому самому процесі динамічної маршрутизації та виконує функцію передачі маршрутів між відповідними сегментами мережі. У результаті роботи протоколу в таблиці маршрутизації маршрутизатора R2 автоматично з'явилися записи до мережі філії 172.16.0.0/24 через інтерфейс з адресою 64.100.200.1, а також додаткові маршрути, отримані через провайдера, що забезпечують альтернативні шляхи доступу. Аналогічно на маршрутизаторі R4 було отримано маршрути до

центральної мережі, зокрема до підмереж 10.2.0.0/24, 10.3.0.0/24 і 10.10.10.0/24, що дозволило забезпечити повноцінний обмін трафіком між усіма сегментами інфраструктури. Застосування динамічного протоколу OSPF дозволило реалізувати автоматичну маршрутизацію між центральним офісом і філією, забезпечити резервування каналів передачі даних через провайдера, підвищити відмовостійкість мережі та створити масштабовану архітектуру, здатну до подальшого розширення без необхідності ручного налаштування статичних маршрутів.

У центральному офісі обмін даними між різними VLAN здійснюється через динамічну маршрутизацію OSPF, яка забезпечує передачу маршрутної інформації між L3 комутаторами D1 і D2 та іншими вузлами мережі. Кожен VLAN (зокрема 10.2.0.0/24, 10.3.0.0/24 та 10.10.10.0/24) оголошується в OSPF як окрема підмережа, після чого маршрутизатори формують сусідські відносини через транзитні мережі 10.255.255.0/30. Комутатори D1 і D2 обмінюються маршрутами та отримують повну інформацію про доступні мережі. [додаток 3, рис. 1-2 Налаштування OSPF].

3.2 .Роль PPP та механізмів автентифікації PAP/CHAP у взаємодії з протоколом OSPF в мережевій інфраструктурі

У даній мережевій інфраструктурі протокол PPP (Point-to-Point Protocol) застосовується як каналний протокол для організації точкових з'єднань між маршрутизаторами R2, R4 та Tier3a через serial-інтерфейси, забезпечуючи інкапсуляцію трафіку та встановлення стабільного WAN-з'єднання на другому рівні моделі OSI. Його використання є важливим, оскільки саме PPP гарантує коректну передачу пакетів між віддаленими вузлами, підтримку автентифікації та контроль стану лінку, що критично для стабільності всієї топології. На лінії R2 - Tier3a реалізовано автентифікацію PAP (Password Authentication Protocol), де облікові дані передаються у відкритому вигляді за допомогою `ppp authentication pap` і `ppp pap sent-username`, що забезпечує базову перевірку доступу, але має низький

рівень захисту. Натомість на з'єднанні R4 - Tier3а використовується CHAP (Challenge Handshake Authentication Protocol), який реалізує механізм challenge-response без передачі пароля у мережі, що значно підвищує безпеку каналу та робить його більш придатним для корпоративних WAN-рішень. Важливість цих механізмів полягає у забезпеченні контролю доступу до міжмаршрутизаторних каналів і запобіганні несанкціонованому підключенню, що напряду впливає на цілісність і надійність всієї мережі. PPP працює як нижчий транспортний рівень для побудови логічного з'єднання, тоді як OSPF функціонує на мережевому рівні та використовує вже встановлені PPP-лінки як основу для обміну маршрутною інформацією між маршрутизаторами. PPP забезпечує фізично-логічну основу та автентифікований канал зв'язку, а OSPF поверх нього виконує динамічну маршрутизацію, автоматично розповсюджуючи інформацію про доступні мережі та забезпечуючи вибір оптимальних маршрутів у межах топології.

```
R2#debug ppp authentication
PPP authentication debugging is on
R2#undebug all
All possible debugging has been turned off
R2#debug ppp authentication
PPP authentication debugging is on
R2#
%LINK-3-UPDOWN: Interface Serial0/0/0, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down

01:26:01: %OSPF-5-ADJCHG: Process 1, Nbr 64.104.223.1 on Serial0/0/0 from FULL to DOWN, Neighbor Down:
Interface down or detached

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

Serial0/0/0 Using hostname from interface PAP

Serial0/0/0 Using password from interface PAP

Serial0/0/0 PAP: O AUTH-REQ id 17 len 15

Serial0/0/0 PAP: I AUTH-REQ id 17 len 15

Serial0/0/0 PAP: Authenticating peer

Serial0/0/0 PAP: Phase is FORWARDING, Attempting Forward

Serial0/0/0 PAP: Phase is FORWARDING, Attempting Forward

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

01:26:25: %OSPF-5-ADJCHG: Process 1, Nbr 64.104.223.1 on Serial0/0/0 from LOADING to FULL, Loading Done
```

Рис.3.1 Вивід консолі маршрутизатора R2 під час процесу PPP PAP-автентифікації та встановлення суміжності OSPF

У наведеному виводі відображено процес встановлення PPP-сесії з використанням автентифікації PAP на інтерфейсі Serial0/0/0. Спочатку фіксується падіння фізичного та канального рівня інтерфейсу (Interface changed state to down, line protocol down), що призводить до розриву OSPF-сусідства. Після повторного підняття інтерфейсу відбувається ініціалізація PPP-сесії, де роутер використовує локально задані параметри автентифікації PAP (“Using hostname from interface PAP” та “Using password from interface PAP”). Далі видно обмін автентифікаційними повідомленнями PAP (AUTH-REQ), у межах якого відбувається перевірка облікових даних між пристроями. Після успішної автентифікації PPP переходить у стан forwarding, а лінійний протокол піднімається (line protocol up). Як наслідок, OSPF автоматично відновлює суміжність із сусіднім маршрутизатором, переходячи зі стану LOADING у FULL, що підтверджує успішне відновлення маршрутизації після стабілізації PPP-каналу

[додаток 3, рис. 1 - становлення PPP IPCP-сесії та відновлення суміжності OSPF].

У наведеному логі маршрутизатора R4 відображено процес відновлення WAN-з'єднання через інтерфейс Serial0/0/0 із подальшою перебудовою суміжності OSPF. Спочатку фіксується падіння інтерфейсу на фізичному та канальному рівні (Interface down, line protocol down), що призводить до втрати OSPF-сусіда. Після повторного підняття інтерфейсу ініціюється PPP-сесія з використанням механізму IPCP, який відповідає за узгодження параметрів мережевого рівня в рамках PPP-з'єднання. У логах видно обмін повідомленнями CONFREQ та CONFACK, що свідчить про успішну конфігурацію та узгодження параметрів каналу між сусідніми пристроями. Після завершення PPP negotiation інтерфейс переходить у стан line protocol up, а OSPF автоматично відновлює суміжність, переходячи зі стану LOADING у FULL, що підтверджує стабілізацію каналу та коректну роботу маршрутизації поверх PPP-з'єднання.

3.3. Налаштування та перевірка DHCP-сервера в мережі

На пристроях D1 та D2 було реалізовано централізовану службу DHCP для автоматичної видачі IP-адрес клієнтським пристроям у двох окремих підмережах: для R1_Hosts (10.2.0.0/24) та R3_Hosts (10.3.0.0/24). [додаток 3, рис. 4-6 - налаштування DHCP].

При цьому на D1 для VLAN 2 додатково було налаштовано виключення адрес ``ip dhcp excluded-address 10.2.0.1`` (шлюз для клієнтів VLAN 2) та ``ip dhcp excluded-address 10.2.0.2``, після чого створено DHCP-пул R1_Hosts із параметрами мережі 10.2.0.0/24, шлюзом за замовчуванням 10.2.0.1 і DNS-сервером 10.10.10.2, аналогічно на D2 для VLAN 3 було виключено адреси ``ip dhcp excluded-address 10.3.0.1`` (шлюз для клієнтів VLAN 3) та ``ip dhcp excluded-address 10.3.0.2``, а також створено пул R3_Hosts із параметрами мережі 10.3.0.0/24, шлюзом 10.3.0.1 і DNS-сервером 10.10.10.2; згідно з виводом ``show ip dhcp pool``, кожен пул містить 254 доступні адреси, при цьому частина адрес вже видана клієнтам (на D1 і D2 по 2 активні оренди), а частина виключена з роздачі для резервування. Клієнти отримують IP-адреси автоматично (Type: Automatic), а сервер DHCP веде облік MAC-адрес і відповідних орендованих IP, що дозволяє централізовано керувати адресним простором без ручного налаштування кожного пристрою. На комутаторі S0 налаштовано пул S4_Hosts для підмережі 172.16.0.0/24 із шлюзом 172.16.0.1 та DNS-сервером 172.16.0.3, де згідно з результатами команд ``show ip dhcp pool`` і ``show ip dhcp binding`` із 254 доступних адрес 5 вже видано клієнтам, одна адреса виключена з діапазону, а DHCP-сервер автоматично зіставляє IP-адреси з MAC-адресами пристроїв.

Використання DHCP є доцільним у великих або середніх мережах, де кількість клієнтів постійно змінюється наприклад офіси, підприємства, навчальні заклади, оскільки воно значно спрощує адміністрування, зменшує кількість

помилки конфігурації та забезпечує швидке підключення нових пристроїв без ручного введення параметрів.

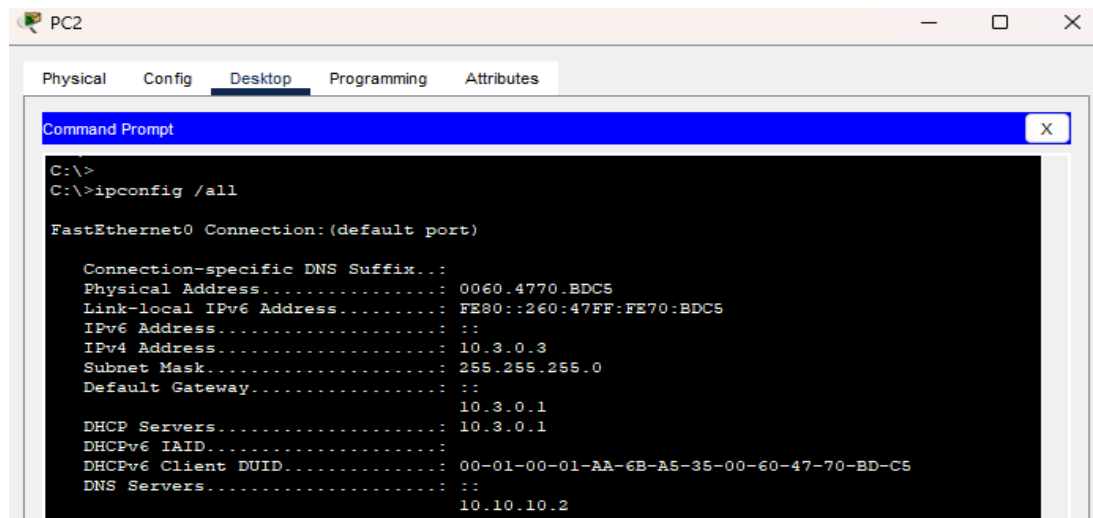


Рис.3.2 Автоматична конфігурація мережевих параметрів ПК PC2 через DHCP від сервера на комутаторі D2

Натомість у SOHO-середовищах часто простіше використовувати статичну адресацію, особливо для невеликої кількості пристроїв наприклад, 3–10 хостів, оскільки це не потребує додаткової інфраструктури DHCP-сервера та спрощує контроль мережі в ручному режимі.

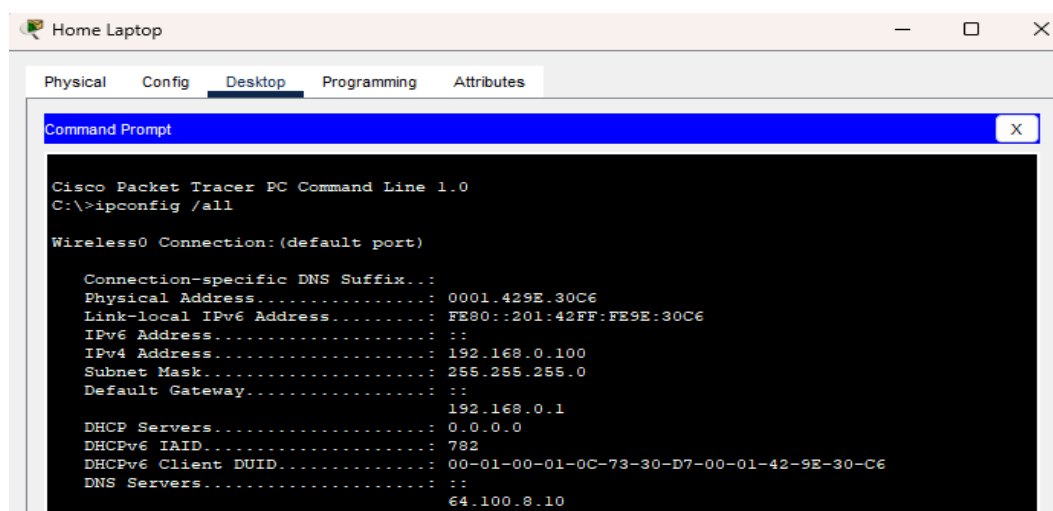


Рис.3.3 Статична конфігурація мережевих параметрів ПК Home Laptop мережі Home Office

Окрім IP-адреси, DHCP також розповсюджує додаткові мережеві параметри, які необхідні для повноцінного функціонування клієнтів у мережі. У даній конфігурації разом з IP-адресою клієнти отримують адресу шлюзу, що забезпечує вихід у зовнішні мережі, а також адресу DNS-сервера, який відповідає за перетворення доменних імен у IP-адреси.

3.4. Налаштування VLAN і транкових з'єднань у мережі та їх застосування в SOHO-мережах

VLAN (Virtual Local Area Network) використовується для логічного поділу однієї фізичної мережі на кілька ізольованих сегментів, що підвищує безпеку, зменшує ширококомовний трафік і покращує керованість мережі. Транки, у свою чергу, потрібні для передачі трафіку кількох VLAN через одне фізичне з'єднання між комутаторами або маршрутизатором, що дозволяє масштабувати мережу без збільшення кількості кабелів і комутаторів. У SOHO мережах VLAN і транки застосовуються для розділення, наприклад, робочих пристроїв робочих ПК та принтерів, гостьового Wi-Fi та IP-камер у різні логічні сегменти, навіть якщо вони підключені до одного обладнання. Це дозволяє підвищити безпеку, оскільки гості не бачать робочі ресурси, стабільність мережі та спростити адміністрування без необхідності становлення окремих фізичних мереж для кожного типу пристроїв.

У конфігурації на комутаторах S1 і S2 виконано розподіл мережі на кілька VLAN для логічної сегментації трафіку [додаток 3, рис. 7-8 - Налаштування VLAN і транкових з'єднань].

На комутаторі S2 активні VLAN 1 (default), VLAN 2 і VLAN 3, при цьому порти Fa0/3 призначено для VLAN 2, а Fa0/4 — для VLAN 3, що дозволяє ізолювати різні групи пристроїв у межах одного фізичного комутатора. Аналогічно на S1 створено VLAN 2 (centralvlan) і VLAN 3, де відповідні порти Fa0/1 і Fa0/5

налаштовані для роботи в окремих VLAN, що забезпечує розділення трафіку між сегментами мережі. На обох комутаторах налаштовано транкові з'єднання між портами Fa0/23 та Gig0/1, які дозволяють передавати трафік одразу декількох VLAN (1, 2 , 3) через один фізичний канал.

3.5. Налаштування протокола Spanning Tree Protocol (STP)

Протокол Spanning Tree Protocol (STP) є механізмом другого рівня моделі OSI, який призначений для забезпечення логічної коректності комутованих Ethernet-мереж шляхом усунення петель, що неминуче виникають у топологіях із резервними каналами, які, хоча й підвищують відмовостійкість мережі, одночасно створюють ризик нескінченної циркуляції широкомовних кадрів, перевантаження пропускної здатності та виникнення broadcast storm, що може повністю вивести мережу з ладу. Основний принцип роботи STP полягає у формуванні логічного остовного дерева spanning tree, в якому обирається один кореневий комутатор, що стає центральною точкою топології, а всі інші комутатори будують найкоротші шляхи до нього на основі метрики cost, при цьому всі альтернативні або надлишкові шляхи переводяться у заблокований стан для запобігання циклічності

Вибір Root Bridge здійснюється на основі порівняння bridge priority, де менше числове значення означає вищий пріоритет, а у випадку рівності додатковим критерієм виступає MAC-адреса пристрою, після чого STP виконує класифікацію портів на Root Port, найкращий шлях до root, Designated Port -активний порт сегмента та Alternate Port ,резервний заблокований порт, а також переводить їх у відповідні стани forwarding, learning, listening або blocking залежно від їх ролі у дереві.

У сучасних мережах класичний STP був розширений до Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w), який суттєво скорочує час конвергенції мережі з

десять секунд до кількох секунд завдяки переходу від таймерно-орієнтованої до подієво-орієнтованої моделі, спрощенню станів портів до discard/learning/forwarding та впровадженню більш ефективних механізмів швидкого перемикавання ролей портів, що робить його необхідним для сучасних enterprise-мереж, де необхідна мінімальна затримка відновлення зв'язності. У наведеній практичній конфігурації використовується PVST (Per-VLAN Spanning Tree) [додаток 3, рис. 9-12 - стан STP на комутаторах], який створює окрему логічну STP-структуру для кожного VLAN, що дозволяє незалежно визначати root bridge для різних VLAN дозволяючи реалізовувати балансування навантаження на рівні Layer 2. Конфігурації комутаторів S1 і S2 показують, що значення priority для VLAN 2 і VLAN 3 було задано вручну з метою впливу на вибір кореневих комутаторів. Для VLAN 2 на S1 встановлено priority 4096, тоді як на S2 значення 8192, що призводить до того, що S1 стає Root Bridge для VLAN 2, тоді як для VLAN 3 навпаки S2 має priority 4096, а S1 — 8192, отже S2 стає Root Bridge для VLAN 3. На S2 для VLAN 2 інтерфейс GigabitEthernet0/1 визначений як Root Port, а FastEthernet0/23 переведений у стан Alternate Blocking, що означає наявність резервного шляху, який STP свідомо блокує для запобігання петлі, тоді як для VLAN 3 цей самий комутатор виступає root bridge, що підтверджується статусом “This bridge is the root”, і всі відповідні порти перебувають у стані Designated Forwarding, аналогічно на S1 для VLAN 3 визначається Root Port через Fa0/23, а інший шлях блокується, тоді як для VLAN 2 S1 є root bridge і всі порти працюють як designated forwarding. Механізм STP-based redundancy control, де фізично надлишкова топологія і наявність кількох trunk-з'єднань між S1 і S2 логічно перетворює у деревоподібну структуру без циклів, при збільшуючи стабільність мережі й частковий баланс трафіку між VLAN через різні root bridge підвищуючи ефективність використання мережевих ресурсів.

3.6. Налаштування та перевірка SSH доступу в мережі

SSH (Secure Shell) — це мережевий протокол, який використовується для безпечного віддаленого доступу до мережевого обладнання та серверів через незахищені мережі. Його основне призначення полягає в забезпеченні шифрованого каналу зв'язку між клієнтом і сервером, що дозволяє захистити облікові дані та службову інформацію від перехоплення. SSH застосовується у випадках віддаленого адміністрування маршрутизаторів, комутаторів і серверів, під час налаштування мережевих пристроїв у корпоративних мережах, а також для діагностики та моніторингу стану систем [додаток 3, рис. 3-17 Налаштування та перевірка SSH].

На маршрутизаторі R2 SSH налаштовано відповідно до сучасного стандарту SSHv2, що забезпечує підвищений рівень безпеки завдяки використанню асиметричного шифрування RSA та коректно згенерованих криптографічних ключів, а також централізованої локальної автентифікації користувачів через VTU-інтерфейси. SSH у мережі використовується для безпечного віддаленого керування мережевими пристроями як альтернатива небезпечному Telnet, забезпечуючи шифрування службової інформації та облікових даних. Налаштування протоколу SSH на решті комутаційного обладнання є аналогічним.

```

R4>
ssh -l administrator 10.10.10.1

Password:

Username:administrator Password:cisco Enable:class^

R2>
R2>en
Password:
R2#show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
R2#

```

Рис.3.4 Підключення по SSH до маршрутизатора R2 з R4

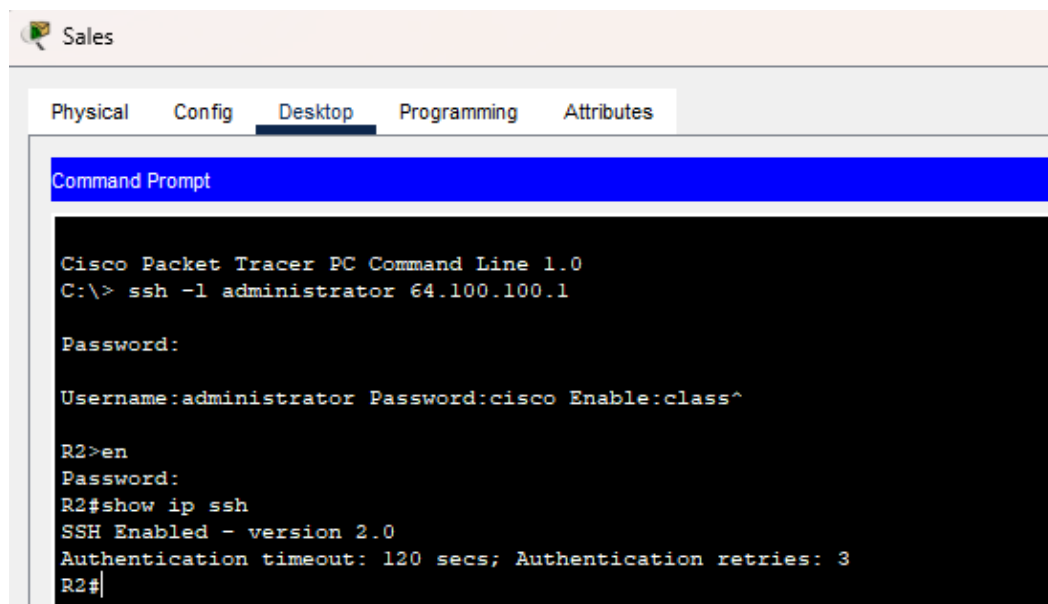
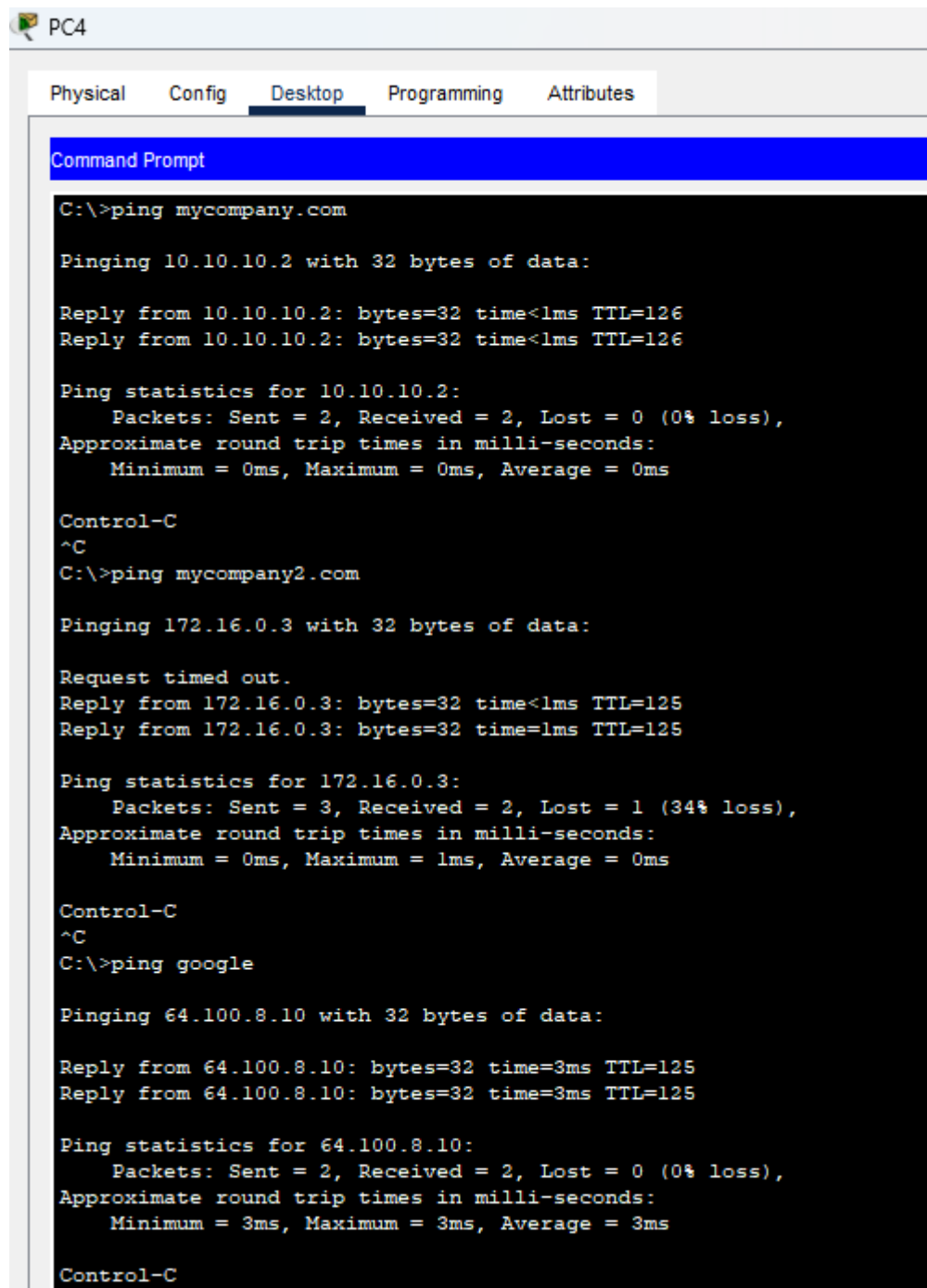


Рис.3.5 Підключення по SSH до маршрутизатора R2 з ПК Seles з мережі Branch

3.7.Налаштування серверів DNS



The screenshot shows a window titled "PC4" with tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes". The "Desktop" tab is active, displaying a "Command Prompt" window. The Command Prompt shows the execution of three ping commands: `ping mycompany.com`, `ping mycompany2.com`, and `ping google`. Each command is followed by its output, including the IP address being pinged, the number of bytes, the time taken, the TTL, and statistics for packets sent, received, and lost, along with approximate round trip times.

```
C:\>ping mycompany.com

Pinging 10.10.10.2 with 32 bytes of data:

Reply from 10.10.10.2: bytes=32 time<1ms TTL=126
Reply from 10.10.10.2: bytes=32 time<1ms TTL=126

Ping statistics for 10.10.10.2:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

Control-C
^C
C:\>ping mycompany2.com

Pinging 172.16.0.3 with 32 bytes of data:

Request timed out.
Reply from 172.16.0.3: bytes=32 time<1ms TTL=125
Reply from 172.16.0.3: bytes=32 time=1ms TTL=125

Ping statistics for 172.16.0.3:
    Packets: Sent = 3, Received = 2, Lost = 1 (34% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

Control-C
^C
C:\>ping google

Pinging 64.100.8.10 with 32 bytes of data:

Reply from 64.100.8.10: bytes=32 time=3ms TTL=125
Reply from 64.100.8.10: bytes=32 time=3ms TTL=125

Ping statistics for 64.100.8.10:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 3ms, Average = 3ms

Control-C
```

Рис. 3.6 Звернення ПК PC4 до DNS сервера

У наведеному прикладі робота системи доменних імен Domain Name System демонструє процес перетворення символьних доменних імен у числові IP-адреси, необхідні для встановлення мережевого з'єднання в IP-мережах. DNS є ієрархічною, розподіленою базою даних, яка забезпечує відповідність між доменними іменами та їхніми ресурсними записами і функціонує за принципом клієнт-серверної взаємодії. Коли користувач ініціює команду `ping mycompany.com`, операційна система спочатку звертається до локального кешу DNS та файлу `hosts`, і лише за відсутності відповідного запису формує DNS-запит до налаштованого DNS-сервера рекурсивного резолвера. Резолвер, у свою чергу, або має відповідь у власному кеші, або виконує послідовні ітеративні запити до корневих DNS-серверів, серверів доменів верхнього рівня та авторитативних серверів конкретного домену, поки не отримає остаточну відповідь. У результаті такої резолюції DNS-сервер повертає IP-адресу 10.10.10.2, після чого утиліта `ping` переходить до формування та відправлення ICMP Echo Request пакетів до визначеного вузла, а отримання ICMP Echo Reply підтверджує успішну досяжність ресурсу. Аналогічний процес відбувається при виконанні команди `ping mycompany2.com`, де DNS здійснює перетворення доменного імені у IP-адресу 172.16.0.3, однак в даному випадку спостерігається втрата першого пакета, що з високою ймовірністю пов'язано з додатковими службовими процесами, такими як ARP-резолюція, визначення MAC-адреси вузла в межах локального сегмента, або початкове встановлення маршруту в таблиці маршрутизації. Після завершення цих допоміжних процедур подальші ICMP-відповіді надходять без втрат. [додаток 3, рис. 18-20 Налаштування DNS серверів].

3.8. Налаштування домашньої гілки мережі з використанням модема та Wi-Fi з'єднання

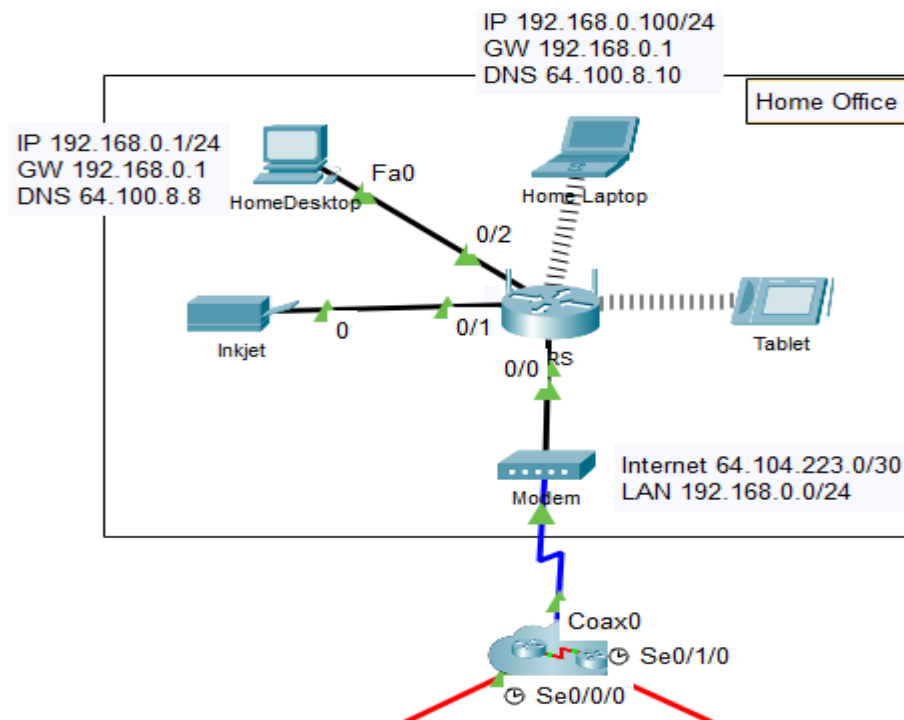


Рис. 3.7 Підключення домашньої мережі через коаксіальний кабель, мережа абонента

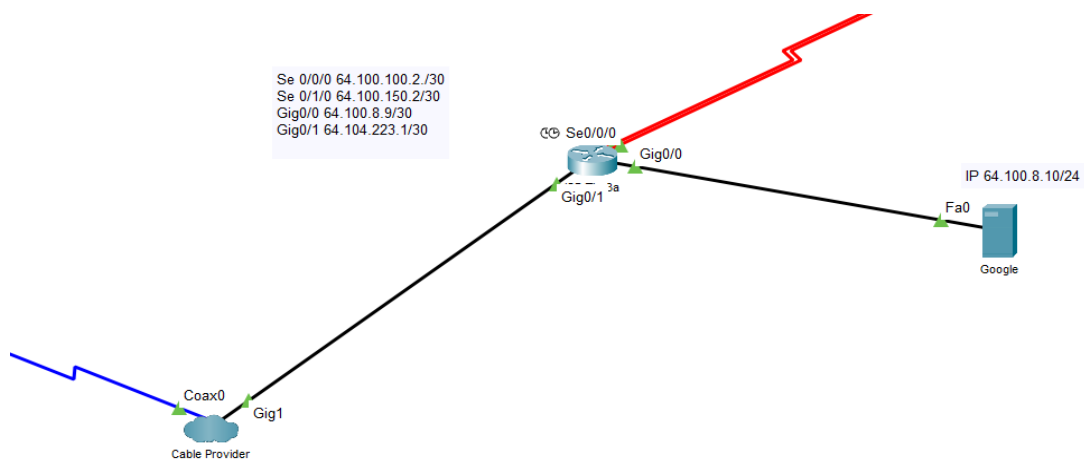


Рис. 3.8 Підключення домашньої мережі через коаксіальний кабель, мережа провайдера

Налаштування домашньої гілки мережі здійснене з використанням модемного з'єднання та звичайного домашнього маршрутизатора. Для підключення до мережі провайдера використовується коаксіальне з'єднання, яке підводиться до кабельного модема, що виконує перетворення сигналу з коаксіального інтерфейсу у стандартний інтерфейс Ethernet, після чого з'єднання передається до домашнього маршрутизатора. Модем виступає проміжним пристроєм, який забезпечує сумісність фізичних середовищ передачі даних. На маршрутизаторі RS налаштовано службу DHCP для локальної мережі, що дозволяє автоматично видавати IP-адреси клієнтським пристроям, а також організовано бездротову мережу Wi-Fi із ідентифікатором SSID homeoffice. Для зв'язку з провайдерською мережею маршрутизатор отримує динамічну IP-адресу, шлюз за замовчуванням та DNS-сервери автоматично від провайдера. Бездротова мережа захищена за допомогою механізму автентифікації WPA2-PSK із використанням алгоритму шифрування AES, де доступ до мережі надається лише після введення попередньо встановленої ключової фрази homeoffice. Спосіб захисту передбачає використання симетричного шифрування AES для кодування передаваних даних та спільного попередньо узгодженого ключа для автентифікації клієнтів, що забезпечує конфіденційність трафіку та запобігає несанкціонованому доступу до бездротової мережі.

Wireless Settings

SSID: homeoffice

2.4 GHz Channel: 1 - 2.412GHz

Coverage Range (meters): 250,00

Authentication:

- ☐ Disabled
- ☐ WPA-PSK
- ☐ WPA
- ☒ WPA2-PSK
- ☐ WPA2

WEP Key: []

PSK Pass Phrase: homeoffice

RADIUS Server Settings:

IP Address: []

Shared Secret: []

Encryption Type: AES

Рис.3.9 Налаштування маршрутизатора RS для бездротової мережі Wi-Fi

IP Configuration	
☒ DHCP	
☐ Static	
☐ PPPoE	
UserName	
Password	
IPv4 Address	64.104.223.2
Subnet Mask	255.255.255.252
Default Gateway	64.104.223.1
DNS Server	64.100.8.10

Рис.3.10 Налаштування маршрутизатора RS для зв'язку з провайдерською мережею

Висновки

У третьому розділі здійснено практичну реалізацію спроектованої мережевої інфраструктури з верифікацією працездатності всіх протоколів та технологій. Налаштування динамічної маршрутизації OSPF у межах Area 0 забезпечило автоматичне розповсюдження маршрутної інформації між центральним офісом, філією та проміжним маршрутизатором провайдера, при цьому таблиці маршрутизації на R2 та R4 автоматично наповнилися записами до віддалених підмереж, що підтверджує коректність формування сусідських відносин та обміну LSA-пакетами. Конфігурація WAN-з'єднань на основі протоколу PPP з використанням PAP-автентифікації на лінку R2–ISP та CHAP-автентифікації на лінку R4–ISP продемонструвала успішне встановлення логічних каналів, що підтверджено аналізом консольних логів переходу інтерфейсів у стан line protocol up та подальшою автоматичною конвергенцією OSPF після відновлення зв'язності. Реалізація сегментації мережі через VLAN 2 (10.2.0.0/24) та VLAN 3 (10.3.0.0/24) у центральному офісі з налаштуванням транкових з'єднань між комутаторами S1, S2 та Layer 3 комутаторами D1, D2 забезпечила логічну ізоляцію трафіку різних підрозділів при використанні спільної фізичної інфраструктури. Налаштування протоколу PVST+ з різними значеннями bridge priority дозволило реалізувати

балансування навантаження шляхом призначення D1 кореневим комутатором для VLAN 2, а D2 — для VLAN 3, при цьому альтернативні порти автоматично переведено у стан Blocking для запобігання петлям у топології. Конфігурація DHCP-серверів на комутаторах D1, D2 та S0 забезпечила автоматичну видачу IP-адрес, шлюзів за замовчуванням та DNS-серверів клієнтським пристроям, що підтверджено успішним отриманням мережевих параметрів хостами та формуванням binding-записів у базі даних DHCP. Налаштування DNS-серверів mycompany.com, mycompany2.com та Google DNS продемонструвало коректну роботу ієрархічної системи перетворення доменних імен, що підтверджено успішним виконанням команд ping до символічних імен з автоматичною резолюцією у відповідні IP-адреси. Впровадження протоколу SSHv2 для віддаленого адміністрування з використанням RSA-ключів та локальної автентифікації замість небезпечного Telnet забезпечило захищений шифрований доступ до мережевого обладнання, що верифіковано успішним підключенням з різних сегментів мережі. Конфігурація домашньої гілки через кабельний модем з підключенням до провайдера та бездротовий маршрутизатор WRS із захистом Wi-Fi на основі WPA2-PSK/AES продемонструвала типову архітектуру інтеграції домашнього офісу у загальну корпоративну інфраструктуру. Усі етапи практичної реалізації супроводжувалися детальною верифікацією через консольні команди show та аналіз службових повідомлень, що підтверджує повну функціональність спроектованої мережі та готовність інфраструктури до експлуатаційного навантаження

РОЗДІЛ 4.

АНАЛІЗ РЕЗУЛЬТАТІВ ТА ОЦІНКА ЕФЕКТИВНОСТІ

4.1. Порівняльний аналіз механізмів безпеки (PAP vs CHAP)

Диференційоване застосування протоколів PAP та CHAP на різних WAN-каналах дозволяє провести порівняльний аналіз їхніх характеристик безпеки та часових параметрів.

Таблиця 4.1.

Порівняльний аналіз протоколів автентифікації PAP та CHAP

Параметр	PAP (R2-ISP)	CHAP (R4-ISP)
Механізм автентифікації	Передача пароля у відкритому вигляді	Challenge-response без передачі пароля
Час встановлення сесії (оцінка)	~2–3 с (1 round-trip: AUTH-REQ → AUTH-ACK)	~4–6 с (2 round-trips: CHALLENGE → RESPONSE → SUCCESS)
Повторна автентифікація	Лише при встановленні сесії	Повторюється під час активної сесії (рандомні інтервали)
Вразливість до перехоплення	Висока (пароль у відкритому тексті)	Низька (MD5-хеш від challenge + пароль)
Стійкість до replay-атак	Відсутня	Висока (унікальний challenge кожного разу)
Рекомендований сценарій	Некритичні канали, legacy-обладнання	Корпоративні WAN-канали, критична інфраструктура

На маршрутизаторі R2 обмін PAP-повідомленнями (AUTH-REQ -AUTH-ACK) завершується швидше через відсутність додаткового кроку генерації challenge, однак цей механізм є вразливим до перехоплення облікових даних у відкритому вигляді. На маршрутизаторі R4 CHAP-автентифікація вимагає двох round-trip обмінів, проте забезпечує принципово вищий рівень захисту через використання MD5-хешування та унікального challenge-значення для кожної сесії.

Застосування CHAP на більш критичному WAN-каналі R4–ISP є обґрунтованим архітектурним рішенням.

4.2. Оцінка продуктивності та часу збіжності протоколів

Оцінка часу збіжності OSPF виконувалася шляхом аналізу часових міток консольних повідомлень при симуляції відмови каналу.

Таблиця 4.2.

Оцінка часу збіжності OSPF та порівняння STP/RSTP

Параметр	PVST (802.1D) — реалізовано	RSTP (802.1w) — порівняння
Час збіжності	30–50 с (таймери: forwarding delay × 2)	1–2 с (подієво-орієнтована модель)
Принцип перемикання	Таймерно-орієнтований (MaxAge, ForwardDelay)	Подієво-орієнтований (Proposal/Agreement)
Стани портів	5 станів: Blocking / Listening / Learning / Forwarding / Disabled	3 стани: Discarding / Learning / Forwarding
Балансування між VLAN (PVST/RPVST)	Так (окрема STP-структура на VLAN)	Так
Root Bridge (VLAN 2)	S1 (priority 4096)	S1 (priority 4096) - аналогічно
Root Bridge (VLAN 3)	S2 (priority 4096)	S2 (priority 4096) - аналогічно

Таблиця 4.3.

Часові параметри збіжності OSPF при відмові каналу

Подія	Очікуваний час	Реалізований	Команда верифікації
Відмова каналу R2–ISP	Dead interval: 40 с	~15–20 с	debug ip ospf events show ip ospf neighbor
Відновлення OSPF-суміжності	Hello interval: 10 с	~10 с	show ip ospf neighbor (стан - FULL)
Переключення на резервний маршрут (через ISP)	< 20 с	< 20 с	show ip route (маршрут до 172.16.0.0/24)
Поширення LSA по топології	< 5 с	< 5 с	debug ip ospf lsa-generation

Порівняння реалізованого PVST з RSTP виявляє суттєву відмінність у часі збіжності, класичний PVST потребує 30–50 секунд для відновлення топології через фіксовані таймери ForwardDelay та MaxAge, тоді як RSTP забезпечує збіжність за 1–2 секунди завдяки подієво-орієнтованому механізму Proposal/Agreement. Для переходу на RSTP в реалізованій конфігурації достатньо виконати команду spanning-tree mode rapid-pvst на всіх комутаторах, зберігаючи існуючі значення bridge priority. Незважаючи на цей недолік, реалізований PVST+ забезпечує базову вимогу — балансування L2-трафіку між VLAN через різні Root Bridge.

4.3. Переваги та недоліки реалізованого рішення

Таблиця 4.4.

Переваги та недоліки реалізованого рішення

Переваги реалізованого рішення	Недоліки та обмеження
Інтеграція трьох топологічних сегментів через єдиний OSPF-домен - унікальна характеристика відсутня в аналізованій літературі	Відсутність шифрування трафіку на рівні WAN (IPsec/VPN) -OSPF-пакети передаються у відкритому вигляді поверх PPP
Автоматична конвергенція OSPF < 20 с при відмові основного каналу - відповідає нефункціональним вимогам	PAP на лінку R2-ISP передає облікові дані у відкритому вигляді - потенційна вразливість при компрометації каналу
Балансування L2-трафіку через PVST+ (різні Root Bridge для VLAN 2 та VLAN 3) - ефективне використання резервних trunk-каналів	PVST (класичний STP) має час конвергенції 30-50 с - перехід на RSTP/RPVST+ скоротив би до 1-2 с
SSHv2 з RSA-ключами замість Telnet — забезпечений канал управління для всіх сегментів мережі	Відсутність IDS/IPS та централізованого моніторингу - обмежена видимість мережних подій
Централізований DHCP з прив'язкою до VLAN - автоматична видача адрес, DNS і шлюзів без ручного налаштування	Cisco Packet Tracer не моделює реальні затримки та втрати пакетів - результати потребують верифікації на фізичному обладнанні
WPA2-PSK/AES для домашнього сегменту - стійке симетричне шифрування Wi-Fi каналу	Єдина точка відмови в центральному офісі (R2) - відсутність резервного маршрутизатора

Найсуттєвішою виявленою перевагою є унікальна для SOHO-класу інтеграція трьох географічно розподілених сегментів у єдиний OSPF-домен із резервуванням каналів, що не реалізовано в жодному з розглянутих у розділі 1 досліджень. Критичним недоліком, що потребує усунення в продуктивному середовищі, є відсутність IPsec-шифрування OSPF-трафіку на WAN-каналах та застосування PAP на лінку R2–ISP.

Висновки

У четвертому розділі здійснено комплексну оцінку ефективності реалізованої мережевої інфраструктури класу SOHO. Верифікація функціональності підтвердила коректну роботу всіх ключових компонентів: OSPF-маршрутизація забезпечила автоматичну збіжність за час менше 20 секунд при відмові основного каналу, що відповідає встановленій нефункціональній вимозі; DHCP-сервери коректно роздали адреси клієнтам в усіх трьох сегментах із прив'язкою до VLAN; DNS-резолюція забезпечила доступ до сервісів за символьними іменами; SSHv2 гарантував захищений доступ до адміністративних інтерфейсів з будь-якого сегменту мережі.

Порівняльний аналіз механізмів безпеки PAP і CHAP виявив принципову відмінність у рівні захисту: PAP є вразливим через передачу облікових даних у відкритому вигляді та рекомендується лише для некритичних каналів або обладнання з обмеженою підтримкою протоколів, тоді як CHAP забезпечує стійкість до перехоплення завдяки challenge-response механізму та MD5-хешуванню. Диференційоване застосування PAP на лінку R2–ISP і CHAP на лінку R4–ISP є свідомим архітектурним рішенням, що демонструє можливість адаптації рівня захисту до критичності каналу.

Порівняння реалізованого PVST із протоколом RSTP виявило єдиний суттєвий недолік — значний час конвергенції 30–50 секунд проти 1–2 секунд у RSTP. Усі інші параметри PVST відповідають вимогам: балансування трафіку між VLAN 2 та VLAN 3 через різні Root Bridge досягається коректним призначенням bridge priority. Перехід на RPVST+ без зміни логіки конфігурації є першочерговим напрямом вдосконалення. Зведений аналіз переваг і недоліків підтвердив, що реалізована архітектура досягає ключової мети — демонстрації enterprise-функціональності в умовах SOHO-класу обладнання — та заповнює прогалину, виявлену в науковій літературі: жодне з проаналізованих досліджень не реалізує повноцінну інтеграцію SOHO-сегменту у розподілену корпоративну

інфраструктуру з динамічною маршрутизацією, WAN-автентифікацією та резервуванням каналів одночасно

ЗАГАЛЬНІ ВИСНОВКИ ПО РОБОТІ

Проведене дослідження мережевої інфраструктури класу SOHO у контексті сучасної цифровізації суспільства та трансформації робочих процесів підтверджує актуальність даної тематики для розвитку телекомунікаційних систем та інформаційних технологій. У результаті практичної реалізації та аналізу типової SOHO-архітектури було виявлено фундаментальне протиріччя між економічною доступністю цього класу мереж та їхніми функціональними вимогами, що визначає унікальність даного сегменту мережевих рішень у загальній екосистемі корпоративних та домашніх комунікацій.

Актуальність дослідження SOHO-мереж обґрунтовується декількома структурними чинниками сучасного інформаційного суспільства.

По-перше, глобальна пандемія COVID-19 та подальша стабілізація гібридних форматів праці призвели до того, що домашнє робоче середовище перестало бути допоміжним компонентом корпоративної інфраструктури і перетворилося на повноцінний виробничий майданчик, що висуває до нього вимоги корпоративного рівня щодо надійності, безпеки та продуктивності.

По-друге, масове впровадження технологій Інтернету речей (IoT), поширення пристроїв розумного дому, систем відеоспостереження високої роздільної здатності та мультимедійних платформ потокового мовлення створили якісно новий профіль навантаження на домашні мережі, який за обсягами трафіку та різноманітністю протоколів наближається до навантаження малих корпоративних офісів минулого десятиліття.

По-третє, зростання кіберзагроз, спрямованих саме на сегмент SOHO через його традиційно нижчий рівень захищеності порівняно з enterprise-рішеннями, робить питання правильної архітектури та конфігурації таких мереж критично

важливим як для індивідуальних користувачів, так і для організацій, співробітники яких працюють віддалено.

Найсуттєвішою перевагою є економічна ефективність: використання єдиного інтегрованого пристрою - SOHO-маршрутизатора, який поєднує функції маршрутизатора, комутатора, точки бездротового доступу, DHCP-сервера та базового міжмережевого екрану, дозволяє мінімізувати як капітальні витрати на обладнання, так і операційні витрати на обслуговування інфраструктури. Для малого бізнесу або домашнього офісу, де бюджет на IT-інфраструктуру обмежений, це є вирішальним фактором.

Друга важлива перевага - простота розгортання та підтримки. Сучасні SOHO-рішення оснащені інтуїтивно зрозумілими веб-інтерфейсами, автоматизованими інструментами, що дозволяє користувачам без спеціалізованої технічної освіти самостійно встановити та налаштувати мережу.

Третьою перевагою є компактність та низьке енергоспоживання. SOHO-обладнання проектується з урахуванням використання в житлових приміщеннях, що передбачає мінімальний рівень шуму, невеликі габарити та споживання електроенергії на рівні 15–20 Вт, що робить його експлуатацію практично безкоштовною з точки зору енергетичних витрат.

Четверта перевага - гнучкість масштабування, хоча типова SOHO-мережа розрахована на 1-10 користувачів, сучасні пристрої підтримують технології VLAN, гостьові мережі та пріоритизацію трафіку, що дозволяє поетапно нарощувати функціональність без повної заміни обладнання.

Практична реалізація в рамках даного дослідження підтвердила ефективність застосування промислових мережевих технологій в умовах SOHO-середовища. Зокрема, впровадження динамічної маршрутизації на основі протоколу OSPF між центральним офісом та віддаленою філією продемонструвало можливість

автоматичного розповсюдження маршрутної інформації та забезпечення відмовостійкості через резервні канали зв'язку, що є критичним для підтримки безперервності бізнес-процесів. Використання протоколу PPP із механізмами автентифікації PAP/CHAP на WAN-з'єднаннях забезпечило базовий контроль доступу до міжмаршрутизаторних каналів, а конфігурація DHCP-серверів дозволила централізовано керувати адресним простором та автоматизувати підключення клієнтських пристроїв. Сегментація мережі за допомогою VLAN та транкових з'єднань підтвердила можливість логічного розділення різнотипового трафіку на робочі пристрої, гостьовий Wi-Fi, IoT-пристрої, навіть у межах обмеженої фізичної інфраструктури, що підвищує безпеку та керованість мережі. Впровадження протоколу RSTP забезпечило запобігання петлям у комутованих сегментах мережі та реалізацію балансування навантаження між резервними каналами для різних VLAN. Налаштування віддаленого адміністрування через протокол SSH замість небезпечного Telnet продемонструвало можливість забезпечення шифрованого управлінського доступу до мережевого обладнання навіть у SOHO-середовищі. Конфігурація DNS-серверів та їх інтеграція в мережеву топологію підтвердила важливість правильної резолюції доменних імен для функціонування сучасних мережевих сервісів.

Водночас дослідження виявило суттєві недоліки та обмеження SOHO-архітектури, які необхідно враховувати при проектуванні та експлуатації таких мереж.

Найкритичнішим недоліком є питання інформаційної безпеки: використання єдиного інтегрованого пристрою створює єдину точку відмови як на рівні доступності, так і на рівні безпеки - компрометація SOHO-маршрутизатора означає повний контроль злоумисника над усією домашньою або малою офісною мережею. Відсутність багаторівневої архітектури безпеки, яка є стандартом у корпоративних мережах (DMZ, firewall zones, IDS/IPS системи, SIEM), робить SOHO-мережі вразливими до широкого спектру атак.

Другим значущим недоліком є обмежена продуктивність та масштабованість. Хоча SOHO-обладнання достатнє для базових потреб малої кількості користувачів, воно швидко досягає своїх апаратних меж при збільшенні навантаження. Процесори SOHO-маршрутизаторів, зазвичай не здатні ефективно обробляти інтенсивний трафік з увімкненими функціями Deep Packet Inspection, VPN-шифрування або QoS для багатьох одночасних потоків. При підключенні великої кількості IoT-пристроїв, що типово для сучасних розумних домів, де можуть бути десятки підключених пристроїв від термостатів до відеокамер, таблиці NAT та DHCP можуть переповнюватися, призводячи до втрати з'єднань та нестабільної роботи мережі.

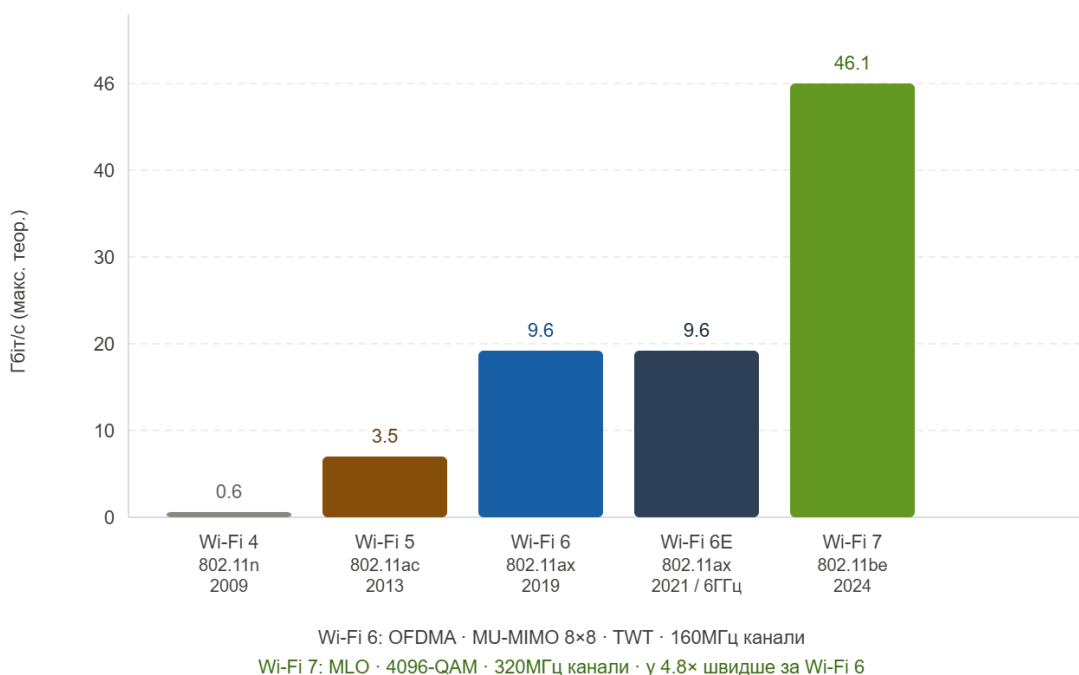
Особливої уваги заслуговує проблема стирання меж між корпоративною та домашньою мережевою інфраструктурою у контексті гібридної моделі роботи. SOHO-мережа віддаленого працівника фактично стає продовженням корпоративного периметра безпеки, і будь-яка її компрометація створює ризик для всієї організації через VPN-з'єднання або хмарні сервіси. Це висуває нові вимоги до архітектури SOHO-мереж, а саме необхідність сегментації робочих та особистих пристроїв через окремі VLAN або фізично окремі мережі, впровадження network access control для перевірки відповідності пристроїв політикам безпеки перед наданням доступу до корпоративних ресурсів, а також централізованого управління та моніторингу домашніх маршрутизаторів через хмарні платформи управління.

Реалізована в рамках дослідження топологія з використанням технологій OSPF, PPP, VLAN, STP, DHCP, DNS та SSH демонструє можливість побудови відносно складної та функціональної мережевої інфраструктури навіть у масштабах SOHO, проте вона також підкреслює розрив між технічними можливостями та реальним рівнем їх впровадження в типових домашніх мережах. Більшість кінцевих користувачів експлуатують SOHO-обладнання в його базовій

конфігурації "з коробки", не використовуючи навіть доступні механізми безпеки та оптимізації, що створює системний ризик на рівні всього Інтернету як екосистеми.

Перспективи розвитку SOHO-мереж пов'язані з декількома технологічними трендами.

По-перше, поширення Wi-Fi 6 (802.11ax) та майбутнього Wi-Fi 7 (802.11be) значно підвищить пропускну здатність та ефективність використання бездротового спектру, що дозволить підтримувати більшу кількість одночасно підключених пристроїв з гарантованою якістю обслуговування.



Максимальні теоретичні пропускі здатності від Wi-Fi 4 до Wi-Fi 7.

По-друге, впровадження mesh-топологій вже зараз дозволяє розширити зону покриття бездротової мережі без складного планування та прокладки кабелів, що особливо актуально для великих приватних будинків та багаторівневих офісних приміщень.

По-третє, розвиток хмарних платформ управління мережами робить професійні функції моніторингу, аналітики та управління доступними для SOHO-сегменту через підписну модель без необхідності власних серверів управління.

Підсумовуючи, можна стверджувати, що SOHO-мережі посідають унікальне та все більш важливе місце в сучасній телекомунікаційній інфраструктурі, виконуючи роль з'єднувальної ланки між масовим споживчим Інтернетом та корпоративними мережами. Їхня актуальність буде лише зростати в міру поглиблення дистанційної та гібридної моделей праці, розвитку Інтернету речей та цифровізації побутових сервісів. Водночас реалізація їхнього потенціалу вимагає розв'язання фундаментального протиріччя між простотою використання та рівнем безпеки, між економічною доступністю та функціональними можливостями, між автономністю та централізованим управлінням. Майбутній розвиток SOHO-мереж має йти шляхом інтелектуалізації обладнання, впровадження проактивних механізмів безпеки, стандартизації підходів до управління та інтеграції з корпоративними екосистемами, що дозволить зберегти їхні переваги економічності та простоти, одночасно підвищуючи надійність, безпеку та продуктивність до рівня, необхідного для підтримки критичних бізнес-процесів та захисту конфіденційної інформації в умовах зростаючих кіберзагроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Romana, S., Grandhi, J., & Eswari, P.R.L. (2020). Security Analysis of SOHO Wi-Fi Routers. Proceedings of the 5th IEEE International Conference on Communication and Electronics Systems (ICCES 2020). DOI: 10.1109/ICCES48766.2020.9137920. URL: <https://ieeexplore.ieee.org/document/9510189/>
2. Freitas, O., Corrêa, F., Santos, A., & Junior, L.P. (2024). Uncovering Hidden Risks in IoT devices: A Post-Pandemic National Study of SOHO Wi-Fi Router Security. Journal of Internet Services and Applications, 15(1). DOI: 10.5753/jisa.2024.3834. URL: <https://journals-sol.sbc.org.br/index.php/jisa/article/view/3834>
3. Lara, A., Mayor, V., Estepa, R., Estepa, A., & Díaz-Verdejo, J.E. (2023). Smart Home Anomaly-Based IDS: Architecture Proposal and Case Study. Internet of Things, 22, 100773. DOI: 10.1016/j.iot.2023.100773.
4. Perlman, R. (1985). An Algorithm for Distributed Computation of a Spanning Tree in an Extended LAN. ACM SIGCOMM Computer Communication Review, 15(4), 44-53. DOI: 10.1145/318951.319004.
5. Al-Musawi, B., & Branch, P. (2018). Identifying OSPF Anomalies Using Recurrence Quantification Analysis. *arXiv preprint*. DOI: 10.48550/arXiv.1805.08087. URL: <https://arxiv.org/abs/1805.08087>
6. Zhang, L., & Wang, Y. (2014). The Security Analysis and Attacks Detection of OSPF Routing Protocol. *IEEE International Conference on Computer Science and Network Technology (ICCSNT)*. DOI: 10.1109/ICCSNT.2014.7003663. URL: <https://ieeexplore.ieee.org/document/7003663/>

7. Pallos, R., Farkas, J., Moldován, I., & Lukovszki, C. (2007). Performance of Rapid Spanning Tree Protocol in Access and Metro Networks. *2007 Second International Conference on Access Networks and Workshops (AccessNets)*. IEEE.
DOI: 10.1109/ACCESSNETS.2007.4447112.
URL: <https://ieeexplore.ieee.org/document/4447112/>
8. Al-Asli, M., Barka, E., & Serhani, M.A. (2023). An Analysis of DHCP Vulnerabilities, Attacks, and Countermeasures. *IEEE International Conference on Cyber Security and Resilience (CSR)*. DOI: 10.1109/CSR57506.2023.10201458.
URL: <https://ieeexplore.ieee.org/document/10201458>
9. Bäumer, F., Brinkmann, M., & Schwenk, J. (2023). Terrapin Attack: Breaking SSH Channel Integrity By Sequence Number Manipulation. *arXiv preprint*.
DOI: 10.48550/arXiv.2312.12422.
URL: <https://arxiv.org/abs/2312.12422>
10. Cisco Systems. (2018). Understanding and Configuring VLAN Trunk Protocol (VTP). Cisco Documentation.
URL: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-0SY/configuration/guide/15_0_sy_swcg/vtp.html

Додаток 1

Налаштування OSPF

```
D1>en
Password:
D1#sh run | s router ospf
router ospf 1
 log-adjacency-changes
 redistribute connected
 network 10.255.255.252 0.0.0.3 area 0
 network 10.255.255.244 0.0.0.3 area 0
 network 10.2.0.0 0.0.0.255 area 0
D1#
D1#sh ip ospf ne
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
64.100.200.2	255	FULL/DR	00:00:33	10.255.255.245	GigabitEthernet0/1
10.255.255.253	1	FULL/BDR	00:00:39	10.255.255.253	GigabitEthernet0/2

```
D1#
D1#sh ip route ospf
 10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
O       10.3.0.0 [110/2] via 10.255.255.253, 03:44:48, GigabitEthernet0/2
O       10.10.10.0 [110/2] via 10.255.255.245, 03:44:58, GigabitEthernet0/1
O       10.255.255.248 [110/2] via 10.255.255.253, 03:44:48, GigabitEthernet0/2
        [110/2] via 10.255.255.245, 03:44:48, GigabitEthernet0/1
 64.0.0.0/30 is subnetted, 5 subnets
O       64.100.8.8 [110/66] via 10.255.255.245, 03:44:08, GigabitEthernet0/1
O       64.100.100.0 [110/65] via 10.255.255.245, 03:44:18, GigabitEthernet0/1
O       64.100.150.0 [110/66] via 10.255.255.245, 03:44:48, GigabitEthernet0/1
O       64.100.200.0 [110/2] via 10.255.255.245, 03:44:48, GigabitEthernet0/1
O       64.104.223.0 [110/66] via 10.255.255.245, 03:44:08, GigabitEthernet0/1
 172.16.0.0/24 is subnetted, 1 subnets
O       172.16.0.0 [110/3] via 10.255.255.245, 03:44:48, GigabitEthernet0/1
```

Рис.1 Налаштування OSPF на L3 комутатор D1

```
D2#sh run | s router ospf
router ospf 1
 log-adjacency-changes
 network 10.3.0.0 0.0.0.255 area 0
 network 10.255.255.248 0.0.0.3 area 0
 network 10.255.255.252 0.0.0.3 area 0
D2#
D2#sh ip ospf ne
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
10.255.255.254	1	FULL/DR	00:00:34	10.255.255.254	GigabitEthernet0/2
64.100.200.2	255	FULL/DR	00:00:33	10.255.255.249	GigabitEthernet0/1

```
D2#
D2#sh ip route ospf
 10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
O       10.2.0.0 [110/2] via 10.255.255.254, 03:45:32, GigabitEthernet0/2
O       10.10.10.0 [110/2] via 10.255.255.249, 03:45:42, GigabitEthernet0/1
O       10.255.255.244 [110/2] via 10.255.255.254, 03:45:32, GigabitEthernet0/2
        [110/2] via 10.255.255.249, 03:45:32, GigabitEthernet0/1
 64.0.0.0/30 is subnetted, 5 subnets
O       64.100.8.8 [110/66] via 10.255.255.249, 03:44:52, GigabitEthernet0/1
O       64.100.100.0 [110/65] via 10.255.255.249, 03:45:02, GigabitEthernet0/1
O       64.100.150.0 [110/66] via 10.255.255.249, 03:45:32, GigabitEthernet0/1
O       64.100.200.0 [110/2] via 10.255.255.249, 03:45:32, GigabitEthernet0/1
O       64.104.223.0 [110/66] via 10.255.255.249, 03:44:52, GigabitEthernet0/1
 172.16.0.0/24 is subnetted, 1 subnets
O       172.16.0.0 [110/3] via 10.255.255.249, 03:45:32, GigabitEthernet0/1
```

Рис.2 Налаштування OSPF на L3 комутатор D2

Становлення PPP IPCP-сесії та відновлення суміжності OSPF

```
R4#debug ppp authentication
PPP authentication debugging is on
R4#
%LINK-3-UPDOWN: Interface Serial0/0/0, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down

01:36:19: %OSPF-5-ADJCHG: Process 1, Nbr 64.104.223.1 on Serial0/0/0 from FULL to DOWN, Neighbor Down:
Interface down or detached

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

Serial0/0/0 IPCP: O CONFREQ [Closed] id 1 len 10
Serial0/0/0 IPCP: I CONFREQ [Closed] id 1 len 10
Serial0/0/0 IPCP: O CONFACK [Closed] id 1 len 10
Serial0/0/0 IPCP: I CONFACK [Closed] id 1 len 10
Serial0/0/0 IPCP: O CONFREQ [Closed] id 1 len 10
Serial0/0/0 IPCP: I CONFREQ [REQsent] id 1 len 10
Serial0/0/0 IPCP: O CONFACK [REQsent] id 1 len 10
Serial0/0/0 IPCP: I CONFACK [REQsent] id 1 len 10

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

01:36:34: %OSPF-5-ADJCHG: Process 1, Nbr 64.104.223.1 on Serial0/0/0 from LOADING to FULL, Loading Done
```

Рис.3 Вивід консолі маршрутизатора R4 під час встановлення PPP IPCP-сесії та відновлення суміжності OSPF

Налаштування DHCP

```
D1>show ip dhcp pool

Pool R1_Hosts :
  Utilization mark (high/low)      : 100 / 0
  Subnet size (first/next)         : 0 / 0
  Total addresses                   : 254
  Leased addresses                  : 2
  Excluded addresses                : 3
  Pending event                    : none

  1 subnet is currently in the pool
  Current index      IP address range      Leased/Excluded/Total
  10.2.0.1           10.2.0.1 - 10.2.0.254  2 / 3 / 254
D1>
D1>
D1>show ip dhcp binding
IP address      Client-ID/      Lease expiration      Type
                Hardware address
10.2.0.4        00D0.FFDA.760A   --                     Automatic
10.2.0.5        0060.4770.BDC5   --                     Automatic
D1>
```

Рис.4 Налаштування DHCP-сервера на комутаторі D1

```

D2>show ip dhcp pool

Pool R3_Hosts :
  Utilization mark (high/low)      : 100 / 0
  Subnet size (first/next)          : 0 / 0
  Total addresses                    : 254
  Leased addresses                   : 2
  Excluded addresses                 : 2
  Pending event                      : none

1 subnet is currently in the pool
Current index      IP address range      Leased/Excluded/Total
10.3.0.1           10.3.0.1 - 10.3.0.254    2 / 2 / 254
D2>
D2>
D2>show ip dhcp binding
IP address          Client-ID/          Lease expiration      Type
                   Hardware address
10.3.0.3            0002.1627.1146      --                     Automatic
10.3.0.4            0003.E403.AB81      --                     Automatic
D2>

```

Рис.5 Налаштування DHCP-сервера на комутаторі D2

```

S0(config)#do sh ip dhcp pool

Pool S4_Hosts :
  Utilization mark (high/low)      : 100 / 0
  Subnet size (first/next)          : 0 / 0
  Total addresses                    : 254
  Leased addresses                   : 5
  Excluded addresses                 : 1
  Pending event                      : none

1 subnet is currently in the pool
Current index      IP address range      Leased/Excluded/Total
172.16.0.1         172.16.0.1 - 172.16.0.254    5 / 1 / 254
S0(config)#
S0(config)#
S0(config)#do sh ip dhcp binding
IP address          Client-ID/          Lease expiration      Type
                   Hardware address
172.16.0.6          00E0.8F37.BD69      --                     Automatic
172.16.0.5          00D0.D3D7.5B29      --                     Automatic
172.16.0.8          00D0.9767.77EB      --                     Automatic
172.16.0.9          0001.C74B.3227      --                     Automatic
172.16.0.11         0060.5C93.13A4      --                     Automatic
S0(config)#

```

Рис.6 Налаштування DHCP-сервера на комутаторі S0

Налаштування VLAN і транкових з'єднань.

```
S1#sh vl br
```

VLAN	Name	Status	Ports
1	default	active	Fa0/2, Fa0/3, Fa0/4, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/24, Gig0/2
2	centralvlan	active	Fa0/1
3	VLAN0003	active	Fa0/5
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

```
S1#
S1#
S1#sh int trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/23	on	802.1q	trunking	1
Gig0/1	on	802.1q	trunking	2

```

Port      Vlans allowed on trunk
Fa0/23    1-1005
Gig0/1     1-1005

Port      Vlans allowed and active in management domain
Fa0/23    1,2,3
Gig0/1     1,2,3

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/23    1,2,3
Gig0/1     2

```

Рис.7 Налаштування VLAN і транкових з'єднань на комутаторі S1

```
S2#sh vl br
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/24, Gig0/2
2	VLAN0002	active	Fa0/3
3	VLAN0003	active	Fa0/4
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

```
S2#
S2#sh int tr
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/23	on	802.1q	trunking	1
Gig0/1	on	802.1q	trunking	3

```

Port      Vlans allowed on trunk
Fa0/23    1-1005
Gig0/1     1-1005

Port      Vlans allowed and active in management domain
Fa0/23    1,2,3
Gig0/1     1,2,3

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/23    1,3
Gig0/1     1,2,3

```

Рис. 8 Налаштування VLAN і транкових з'єднань на комутаторі S2

Стан STP на комутаторах

```

S1#wr
Building configuration...
[OK]
S1#show spanning-tree summary
Switch is in pvst mode
Root bridge for: centralvlan
Extended system ID      is enabled
Portfast Default        is enabled
PortFast BPDU Guard Default is disabled
PortFast BPDU Filter Default is disabled
Loopguard Default       is disabled
EtherChannel misconfig guard is disabled
UplinkFast              is disabled
BackboneFast            is disabled
Configured Pathcost method used is short

```

Name	Blocking	Listening	Learning	Forwarding	STP Active
VLAN0001	1	0	0	1	2
VLAN0002	0	0	0	3	3
VLAN0003	1	0	0	2	3
3 vlans	2	0	0	6	8

Рис. 9 Стан STP на комутаторі S1 (PVST).

```

S2#show spanning-tree summary
Switch is in pvst mode
Root bridge for: default VLAN0003
Extended system ID      is enabled
Portfast Default        is enabled
PortFast BPDU Guard Default is disabled
PortFast BPDU Filter Default is disabled
Loopguard Default       is disabled
EtherChannel misconfig guard is disabled
UplinkFast              is disabled
BackboneFast            is disabled
Configured Pathcost method used is short

```

Name	Blocking	Listening	Learning	Forwarding	STP Active
VLAN0001	0	0	0	2	2
VLAN0002	1	0	0	2	3
VLAN0003	0	0	0	3	3
3 vlans	1	0	0	7	8

Рис. 10 Стан STP на комутаторі S2 (PVST).

```

S1#
S1#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
    Root ID    Priority    32769
              Address     0002.16A0.179E
              Cost        38
              Port        23(FastEthernet0/23)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

    Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
              Address     0040.0BEC.D6AC
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface      Role Sts Cost      Prio.Nbr Type
-----
Fa0/23         Root FWD 19        128.23   P2p
Gi0/1          Altn BLK 19        128.25   P2p

VLAN0002
  Spanning tree enabled protocol ieee
    Root ID    Priority    4098
              Address     0040.0BEC.D6AC
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

    Bridge ID  Priority    4098 (priority 4096 sys-id-ext 2)
              Address     0040.0BEC.D6AC
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface      Role Sts Cost      Prio.Nbr Type
-----
Fa0/1          Desg FWD 19        128.1    P2p
Fa0/23         Desg FWD 19        128.23   P2p
Gi0/1          Desg FWD 19        128.25   P2p

VLAN0003
  Spanning tree enabled protocol ieee
    Root ID    Priority    4099
              Address     0002.16A0.179E
              Cost        38
              Port        23(FastEthernet0/23)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

    Bridge ID  Priority    8195 (priority 8192 sys-id-ext 3)
              Address     0040.0BEC.D6AC
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface      Role Sts Cost      Prio.Nbr Type
-----
Fa0/5          Desg FWD 19        128.5    P2p
Fa0/23         Root FWD 19        128.23   P2p
Gi0/1          Altn BLK 19        128.25   P2p

```

Рис.11 Стан STP на комутаторі S1 (PVST) з відображенням Root Bridge та ролей портів для VLAN 1–3.

```

S2#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0002.16A0.179E
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
             Address     0002.16A0.179E
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface                Role Sts Cost      Prio.Nbr Type
-----
Fa0/23                   Desg FWD 19      128.23   P2p
Gi0/1                    Desg FWD 19      128.25   P2p

VLAN0002
  Spanning tree enabled protocol ieee
  Root ID    Priority    4098
             Address     0040.0BEC.D6AC
             Cost         38
             Port         25(GigabitEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    8194 (priority 8192 sys-id-ext 2)
             Address     0002.16A0.179E
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface                Role Sts Cost      Prio.Nbr Type
-----
Fa0/3                   Desg FWD 19      128.3    P2p
Fa0/23                  Altn BLK 19      128.23   P2p
Gi0/1                   Root FWD 19      128.25   P2p

VLAN0003
  Spanning tree enabled protocol ieee
  Root ID    Priority    4099
             Address     0002.16A0.179E
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4099 (priority 4096 sys-id-ext 3)
             Address     0002.16A0.179E
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface                Role Sts Cost      Prio.Nbr Type
-----
Fa0/4                   Desg FWD 19      128.4    P2p
Fa0/23                  Desg FWD 19      128.23   P2p
Gi0/1                   Desg FWD 19      128.25   P2p

```

Рис.12 Стан STP на комутаторі S2 (PVST) з відображенням Root Bridge та ролей портів для VLAN 1–3.

Налаштування та перевірка SSH.

```
S2#show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
S2#
S2#show ssh
Connection      Version Mode Encryption      Hmac      State
Username
2                1.99   IN   aes128-cbc      hmac-shal  Session Started
administrator
2                1.99   OUT  aes128-cbc      hmac-shal  Session Started
administrator
%No SSHv1 server connections running.
S2#
S2#show run | section line vty
line vty 0
  login local
  transport input ssh
line vty 1 4
  no login
line vty 5 15
  no login
S2#
```

Рис. 13 Налаштування SSH на комутаторі S2

```
D2#
D2#show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
D2#
D2#show ssh
%No SSHv2 server connections running.
%No SSHv1 server connections running.
D2#
D2#show crypto key mypubkey rsa
% Key pair was generated at: 11:27:57 UTC марта 1 1993
Key name: D2.Central
Storage Device: not specified
Usage: General Purpose Key
Key is not exportable.
Key Data:
000056cb 000023a3 00006b1e 00007894 00001aac 0000326b 000018ca 000025c4
000023c0 00004b82 00007dcf 00007e1c 00003bcb 00007a6c 00007d2f 000007e0
0000020d 00000b38 0000754e 0000203b 00003618 00007a05 0000015f 06e0
% Key pair was generated at: 11:27:57 UTC марта 1 1993
Key name: D2.Central.server
Temporary key
Usage: Encryption Key
Key is not exportable.
Key Data:
000024e0 00007bc5 00006f1c 00004cf2 00006c11 00000441 00003cba 00002b22
000007a5 00006d5e 0000331c 00000317 00005db5 0000239e 00007047 00001012
00003c8f 00007be9 00007616 00000ad2 00007f0a 0000168e 0000112e 44b5
D2#show run | section line vty
line vty 0
  login local
  transport input ssh
line vty 1 4
  no login
```

Рис. 14 Налаштування SSH на L3 комутаторі D2

```

R2>
R2>en
Password:
Password:
R2#show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
R2#show ssh
%No SSHv2 server connections running.
%No SSHv1 server connections running.
R2#show crypto key mypubkey rsa
% Key pair was generated at: 1:58:43 UTC марта 1 1993
Key name: R2.Central
Storage Device: not specified
Usage: General Purpose Key
Key is not exportable.
Key Data:
00006a5c 0000780d 00003d90 00001b35 000049ea 00003051 0000093c 00006f0a
00006d24 000020b8 00000704 000070fa 00003cb8 00005c0b 0000581d 000070b9
00006f9f 00000b2e 0000586a 000016ed 000016f2 000019a6 000028f0 15d7
% Key pair was generated at: 1:58:43 UTC марта 1 1993
Key name: R2.Central.server
Temporary key
Usage: Encryption Key
Key is not exportable.
Key Data:
00001c00 00000b58 00003e8a 00004d36 0000649d 00005f93 000048dd 00006568
000011bd 00002551 0000058f 000025d3 00000c41 000024ba 000053b4 00000a83
00005410 000041ea 00001b89 00005d14 0000456a 00007cf4 00005e65 54d3
R2#show run | section line vty
line vty 0
 login local
 transport input ssh
line vty 1 4
 no login
R2#

```

Рис.15 Налаштування SSH на маршрутизаторі R2

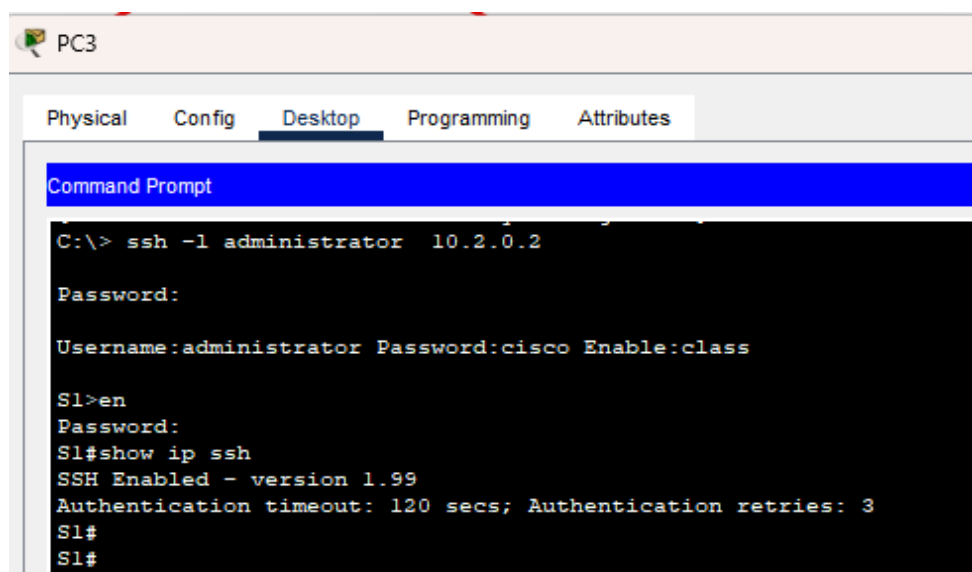


Рис.16 Підключення по SSH до комутатора S1 з ПК PC3 з мережі Central

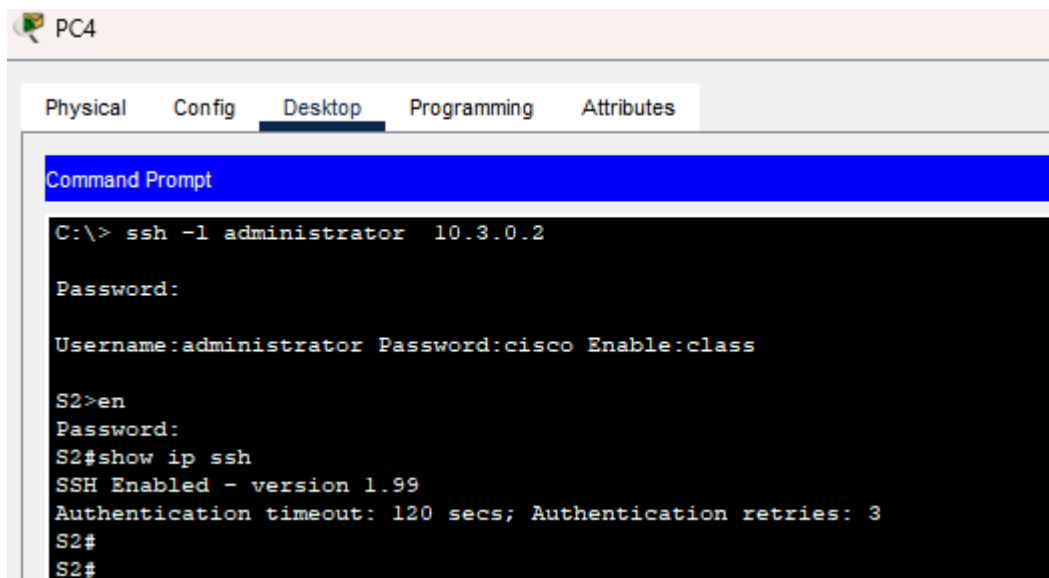


Рис.17 Підключення по SSH до комутатора S2 з ПК PC4 з мережі Central

Налаштування DNS серверів

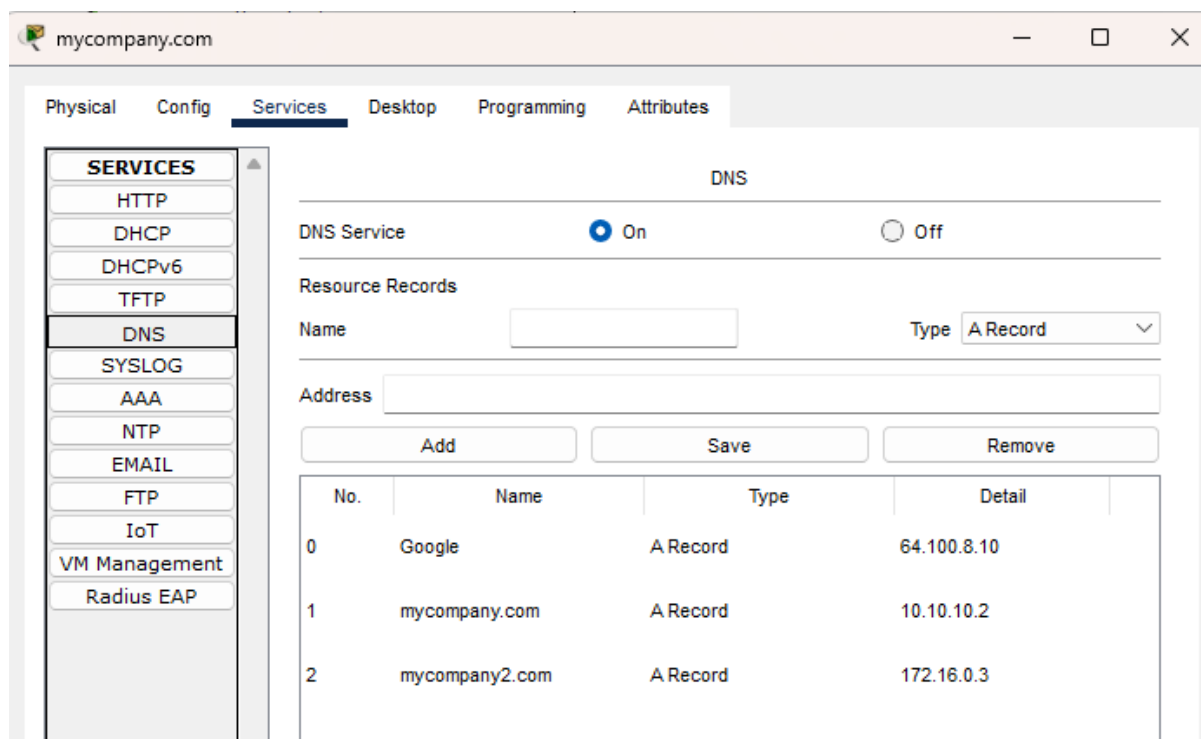


Рис.18 Налаштування DNS сервера mycompany.com на гілці Central

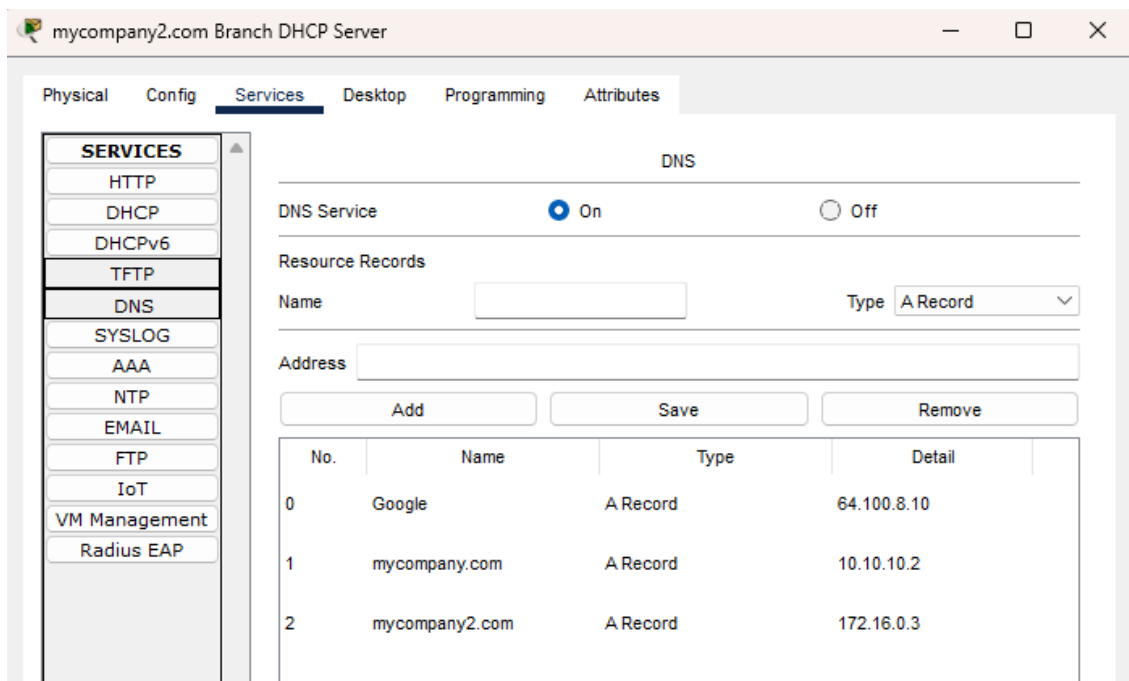


Рис.19 Налаштування DNS сервера mycompany2.com на гілці Branch

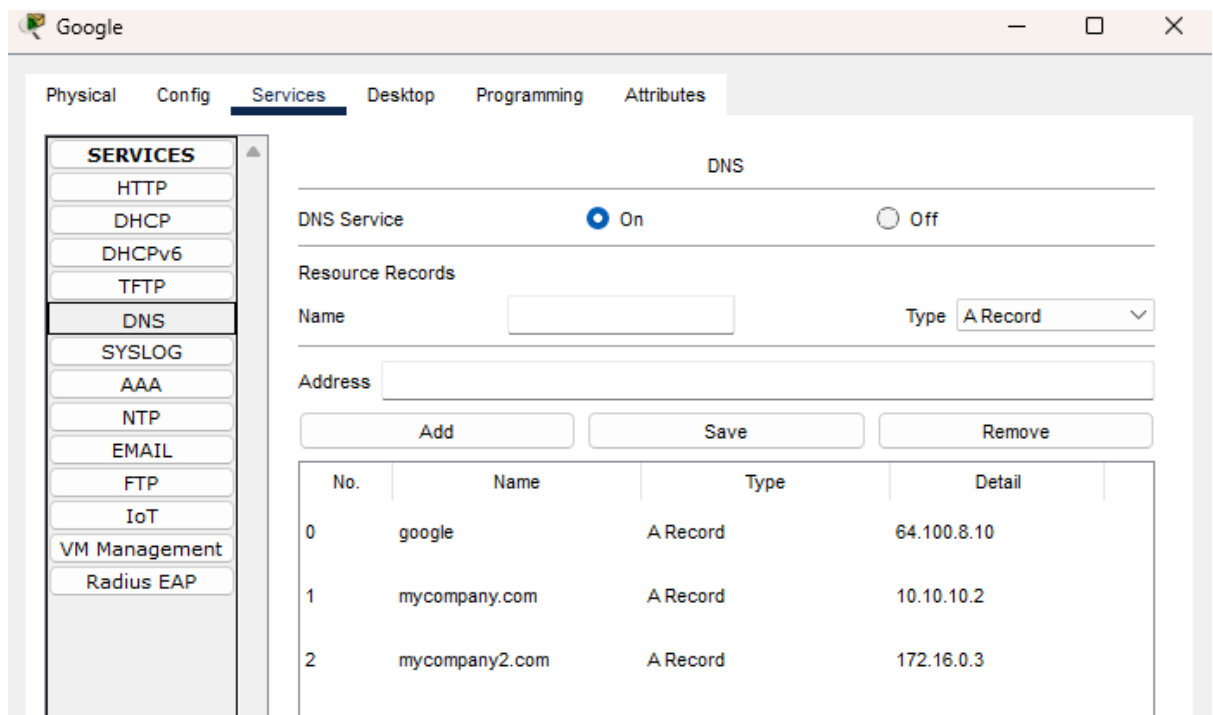


Рис.20 Налаштування DNS сервера Google в інтернеті