Форма №24

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Комп'ютерних наук і технологій
(повне найменування факультету)

Комп'ютерні системи та мережі
(повне найменування кафедри)

Пояснювальна записка

до дипломного проєкту (роботи)
бакалаврський
(ступінь вищої освіти)

на тему: ПРОЄКТУВАННЯ РОЗПОДІЛЕНОЇ МЕРЕЖІ ПІДПРИЄМСТВА ІЗ ЗАСТОСУВАННЯМ ПРОТОКОЛУ RSTP

Виконав(ла): студент(ка) 4 курсу,
групи КНТ-512сп

Спеціальності
123 Комп'ютерна інженерія
(код і найменування спеціальності)

Освітня програма (спеціалізація)
Комп'ютерна інженерія
(назва освітньої програми (спеціалізації)

ПОПОВ М.А.
(ПРІЗВИЩЕ та ініціали)

Керівник КИРИЧЕК Г.Г
(ПРІЗВИЩЕ та ініціали)
Рецензент КОЗІНА Г.Л.
(ПРІЗВИЩЕ та ініціали)

2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»
(повне найменування закладу вищої освіти)

Факультет Комп'ютерних наук та технологій
Кафедра комп'ютерних систем та мереж
Ступінь вищої освіти бакалаврський
Спеціальність 123 Комп'ютерна інженерія
(код і найменування)
Освітня програма (спеціалізація) Комп'ютерна інженерія
(назва освітньої програми (спеціалізації)

ЗАТВЕРДЖУЮ
Завідувач кафедри КУДЕРМЕТОВ Р. К.

«14» квітня 2025 року

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА(КИ)

ПОПОВА Миколи Андрійовича
(прізвище, ім'я, по батькові)

1. Тема проєкту (роботи) «Проєктування розподіленої мережі підприємства із застосуванням протоколу RSTP»
керівник проєкту (роботи) доцент к.т.н КИРИЧЕК Галина Григоровна
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від « 08 » квітня 2025 року № 151
2. Строк подання студентом проєкту (роботи) 01.06.2025
3. Вихідні дані до проєкту (роботи) Проєктування розподіленої мережі підприємства із застосуванням протоколу RSTP, 4 філії, 117 кінцевих користувачів, VLAN, VTP, NTP, VPN (IPSec), RSTP, динамічна конфігурація IPv4 та статична маршрутизація, оптичний кабель, вита пара.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
Аналіз технічного завдання
Проєктування мережі та вибір технічних рішень
Налаштування додаткових технологій LAN мереж
Налаштування маршрутизації та додаткових технологій WAN мереж
Тестування мережі
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
слайди презентації

6. Консультанти розділів проєкту (роботи)

Розділ	ПРІЗВИЩЕ, ініціали та посада консультанта	Підпис, дата	
		завдання видав	Прийняв виконане завдання
1-5	КИРИЧЕК Г. Г., к. т. н., доцент		
нормоконтроль	ЩЕРБАК Н.В., ст. викл.		

7. Дата видачі завдання «___28___» ___лютого__2025__року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів курсового проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Примітка
1	Аналіз технічного завдання та оформлення ТЗ на проєктування	30.02.2025	
2	Проєктування мережі та вибір технічних рішень.	01.03.2025	
3	Розробка функціональної моделі, проєктованої мережі	11.03.2025	
4	Розробка структурної схеми проєктованої мережі підприємства	16.03.2025	
5	Налаштування додаткових технологій LAN мереж	21.04.2025	
6	Налаштування маршрутизації та додаткових технологій WAN мереж	30.04.2025	
7	Тестування мережі	01.05.2025	
8	Оформлення графічного матеріалу	16.05.2025	
9	Оформлення ПЗ	29.05.2025	
10			

Студент(ка) _____ Микола ПОПОВ
(підпис) (прізвище та ініціали)

Керівник проєкту (роботи) _____ Галина КИРИЧЕК
(підпис) (прізвище та ініціали)

Форма № 24

РЕФЕРАТ

Пояснювальна записка до дипломної кваліфікаційної роботи бакалавра: 94 с., 10 табл., 42 рис., 2 дод., 24 джерел.

1000BASE-BX10, 1000BASE-T, CISCO, DHCP, ETHERNET, IPSEC, NTP, RSTP, VLAN, VPN, VTP, МОДЕЛЮВАННЯ, ПРОЄКТУВАННЯ МЕРЕЖ

Метою роботи є проєктування розподіленої мережі підприємства із застосуванням протоколу зв'язуючого дерева та створення надійної, продуктивної інфраструктури, яка гарантує безперебійний зв'язок між усіма об'єктами та ефективне використання ресурсів. Об'єктом проєктування є процес створення мережі передачі даних для підприємства, що об’єднує філії в єдину інформаційну систему. Предметом є моделі, методи, програмні засоби, технології, стандарти та протоколи, які забезпечують стабільну роботу, безпеку, сегментацію трафіку й швидке відновлення з'єднань. Для досягнення мети впроваджено протокол RSTP, що вирішує проблему петель у мережі та значно скорочує час відновлення з'єднань у разі відмови обладнання або каналів.

Побудова мережі відбувалася з застосуванням стандартів 1000BASE-T для локальної мережі використовуючи виту пару (Cat 5e) та 1000BASE-BX10 для прокладення каналів між філіями.

Також застосовано такі технології й протоколи такі як VLAN для сегментації трафіку, VTP для централізованого управління VLAN, NTP для синхронізації часу, DHCP для автоматичної конфігурації хостів, статична маршрутизація для серверів і маршрутизаторів та IPsec VPN для захисту даних.

Проєкт реалізовано в Cisco Packet Tracer, що дозволяє змоделювати мережу, налаштувати обладнання, протестувати взаємодію пристроїв, оцінити ефективність технологій і виявити помилки до впровадження.

ABSTRACT

Explanatory note to the bachelor's thesis: 94 pages, 10 tables, 42 figures, 2 appendices, 24 sources.

1000BASE-BX10, 1000BASE-T, CISCO, DHCP, ETHERNET, IPSEC, NTP, RSTP, VLAN, VPN, VTP, MODELING, NETWORK DESIGN

The purpose of this work is to design a distributed enterprise network using the spanning tree protocol and to create a reliable, productive infrastructure that guarantees uninterrupted communication between all objects and efficient use of resources. The object of the design is the process of creating a data transmission network for an enterprise that unites branches into a single information system. The subject is models, methods, software tools, technologies, standards, and protocols that ensure stable operation, security, traffic segmentation, and fast connection recovery. To achieve this goal, the RSTP protocol was implemented, which solves the problem of loops in the network and significantly reduces the time to restore connections in the event of equipment or channel failure.

The network was built using 1000BASE-T standards for the local network using twisted pair (Cat 5e) and 1000BASE-BX10 for laying channels between branches.

Technologies and protocols such as VLAN for traffic segmentation, VTP for centralized VLAN management, NTP for time synchronization, DHCP for automatic host configuration, static routing for servers and routers, and IPsec VPN for data protection were also used.

The project was implemented in Cisco Packet Tracer, which allows you to simulate a network, configure equipment, test device interaction, evaluate the effectiveness of technologies, and identify errors before implementation.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

ЛКМ – Локальна комп’ютерна мережа;

ПК – Персональний комп’ютер;

BPDU – Bridge Protocol Data Unit, Блок даних протоколу мосту;

CIST – Common and Internal Spanning Tree Поширений і внутрішній сполучного дерева;

CLI – Command-line interface, Інтерфейс командного рядка;

CST – Common Spanning Tree, Поширене сполучне дерево;

DHCP – Dynamic Host Configuration Protocol Протокол динамічної конфігурації хостів;

ESP – Encapsulating Security Payload, Інкапсульоване корисне навантаження безпеки;

EHWIC – Enhanced High-Speed WAN Interface Card, Розширена високошвидкісна WAN-карта;

HWIC – High-Speed WAN Interface Card, Високошвидкісна WAN-карта;

ICV – Integrity Check Value, Значення перевірки цілісності;

IP – Internet Protocol address, Адреса Інтернет-протоколу;

IPSEC – IP Security, Безпека IP;

ISR – Integrated Services Router, Інтегровані послуги маршрутизатора;

LAN – Local Area Network, Локальна мережа;

MAC – Media Access Control, Управління доступом до середовища;

MITM – Man-in-the-middle, Атака типу людина посередині;

MSS – Maximum Segment Size, Максимальний розмір сегменту;

MSTI – Multiple Spanning Tree Instance, Екземпляр множинного дерева з’єднання;

MSTP – Multiple Spanning Tree Protocol, Протокол множинного сполучного дерева;

MTU – Maximum Transmission Unit, Максимальний розмір передаваного блока;

NTP – Network Time Protocol, Мережевий протокол часу;

OSI – Open Systems Interconnection, Модель взаємодії відкритих систем;

PC – Personal computer, Персональний комп’ютер;

PVDM – Packet voice/data module, Модуль голосових/даних пакетів;

RSTP – Rapid Spanning Tree Protocol Протокол швидкого сполучного дерева;

SA – Sequence Number, Порядковий номер;

SFP – Small Form-factor Pluggable, Малий форм-фактор підключення;

SST – Single Spanning Tree, Одинарне дерево з’єднання;

STP – Spanning Tree Protocol, Протокол сполучного дерева;

TCP – Transmission Control Protocol, Протокол керування передачею;

UDP – User Datagram Protocol, Протокол користувацьких дейтаграм;

VLAN – Virtual Local Area Network, Віртуальна локальна мережа;

VPN – Virtual private network, Віртуальна приватна мереж;а

VTP – VLAN Trunking Protocol, Протокол транкування VLAN;

VWIC – Voice and wan interface card, Карта інтерфейсу голосу та WAN;

WDM – Wavelength Division Multiplexing, Мультиплексування з поділом по довжині хвилі;

WAN – Wide area network, Глобальна мережа.

ВСТУП

Сучасні підприємства та організації залежать від комп'ютерних мереж як ключового інструменту для ефективного спілкування, обміну інформацією та керування ресурсами. З розвитком технологій та розширенням бізнесу, виникає необхідність у масштабованих та відмово стійких мережах, котрі здатні гарантувати безперебійну роботу бізнесу. Значною проблемою, з якою зіштовхуються корпоративні мережі, є петлі в топології, котрі можуть викликати збій, а це спричиняє низку наслідків, таких як втрата даних і повне відключення мережі.

Надійність мережі є важливим чинником для сучасних компаній з розкиданими офісами. Простої, тривалістю навіть в одну хвилину і більше, призводять до фінансових збитків, що негативно впливає на бізнес-процеси та шкодить репутації компанії.

Протокол RSTP зменшує час відновлення після того як відбувся збій у мережі та сприяє уникненню петель в мережі. Це важливо для компаній, що мають декілька офісів, оскільки дозволяє оптимізувати витрати на обладнання та інфраструктуру, адже протокол дозволяє ефективно використовувати наявні ресурси мережі, не потребуючи дорогих рішень. Одними з ключових вимог до мережі є стійкість і здатність швидко реагувати на зміни, що важливо при проєктуванні розподіленої мережі підприємств з використанням протоколу RSTP, який забезпечує мережі стабільність і продуктивність. У цій роботі розглядаються принципи функціонування RSTP, аналізуються вимоги до комп'ютерних мереж, створюється топологія. Ця робота демонструє ефективність використання RSTP для побудови сучасної розподіленої мережі, що є важливим кроком у забезпеченні стабільної роботи інформаційної інфраструктури підприємства.

1 АНАЛІЗ ТЕХНІЧНОГО ЗАВДАННЯ

1.1 Опис предметної області

Комп'ютерна система підприємства має включати корпоративну мережу, що гарантуватиме надання доступу користувачам, функціонування автоматизованих інформаційних систем та технічний захист інформації на об'єктах інформаційної діяльності України. Мережа дає змогу встановити системи безпеки та контролю доступу, що робить її більш захищеною від зовнішніх загроз. Окрім того, централізоване керування мережею дозволяє здійснювати моніторинг роботи пристроїв, контролювати трафік та оперативне реагування на можливі проблеми. Грамотне планування та розгортання комп’ютерної мережі на підприємстві дозволяє раціонально використовувати ресурси, задовольняти зростаючі потреби користувачів та забезпечувати масштабованість мережі для подальшого розвитку.

Спочатку необхідно проаналізувати протоколи сполучного дерева, їх принцип роботи, переваги та недоліки, щоб визначити найбільш підходящий варіант для конкретної мережевої топології. Це дозволить обрати оптимальний протокол залежно від масштабів мережі, вимог до швидкості конвергенції та необхідності балансування навантаження.

Наступним кроком необхідно визначити вимоги до мережі, беручи до уваги кількість користувачів, необхідну пропускну здатність, безпеку та резервування каналів зв'язку. Це дозволить розробити оптимальну топологію мережі та розподілити навантаження між пристроями.

Далі слід здійснити вибір та встановлення комутаторів, які є ключовими пристроями в локальній корпоративній мережі (ЛКМ). Вони забезпечують з'єднання комп'ютерів, серверів, принтерів та інших мережевих пристроїв, а також керування трафіком. Встановлення комутаторів на кожному поверсі будівлі дозволить створити ефективну мережеву інфраструктуру, що забезпечить швидке та стабільне підключення всіх користувачів. Для

забезпечення безпеки мережі потрібно розглянути використання мережевих брандмауерів, антивірусного програмного забезпечення та інших заходів безпеки, забезпечити спільний доступ до ресурсів, до мережі інтернет, даних, принтерів та потрібно встановити та налаштувати сервери.

Після того як завершили налаштування тестуємо ЛКМ та мережі перевіряється з'єднання і проводиться виявлення проблем які можуть виникти.

1.2 Протоколи сполучного дерева

Виходячи з мети проєктування розглянемо основні типи протоколів сполучного дерева, їх алгоритми роботи, принципи, відмінності, для визначення їх ефективності.

Для запобігання появі петель в комутованих мережах, використовуються протоколи сполучного дерева. Їхнє використання забезпечуватиме створенню ефективної топології шляхом блокування зайвих з’єднань які будуть використовуватися після виходу із строю основних з’єднань, та вибір оптимального маршруту для даних.

1.2.1 Протокол STP

Розгляньмо протокол STP, цей протокол другого рівня моделі OSI, який використовується у керованих комутаторах для усунення петель у мережах Ethernet. Він забезпечує створення резервованої топології, залишаючи лише один активний маршрут між будь-якими двома вузлами. Це запобігає штормам мовлення та зайвому дублюванню кадрів [1].

Протокол визначає який комутатор стане кореневим, що буде головною точкою для створення дерева. Для вибору кореневого комутатора використовується алгоритм, що аналізує унікальні ідентифікатори комутаторів та вартість зв’язків між ними [2]. При зміні топології STP використовує таймери перед переключенням портів у стан пересилання, щоб забезпечити поширення

нової інформації мережею.

Алгоритм роботи STP відбувається наступним чином, спочатку проводиться обмін BPDU-пакетами комутатори надсилають спеціальні пакети (Bridge Protocol Data Unit), що містять інформацію про пріоритет та ідентифікатор комутатора [2] (рис 1.1).

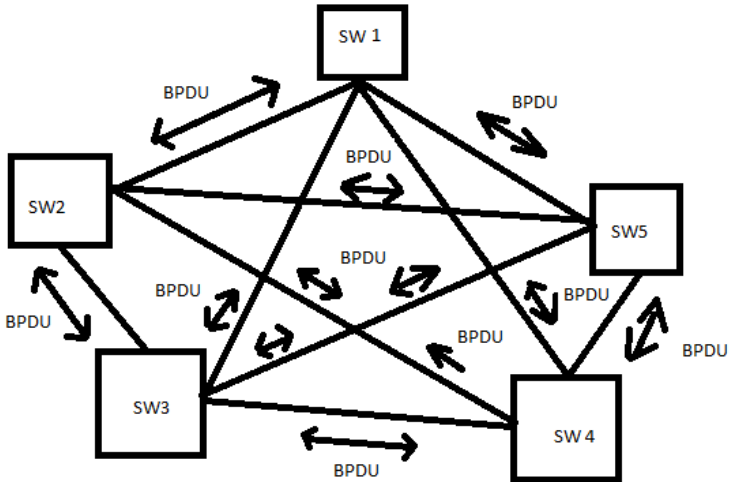


Рисунок 1.1 – Обмін BPDU-пакетами

Наступним кроком йде вибір кореневого комутатора (Root Bridge) комутатор з найменшим ідентифікатором (MAC-адреса + пріоритет) стає кореневим [2] (рис. 1.2).

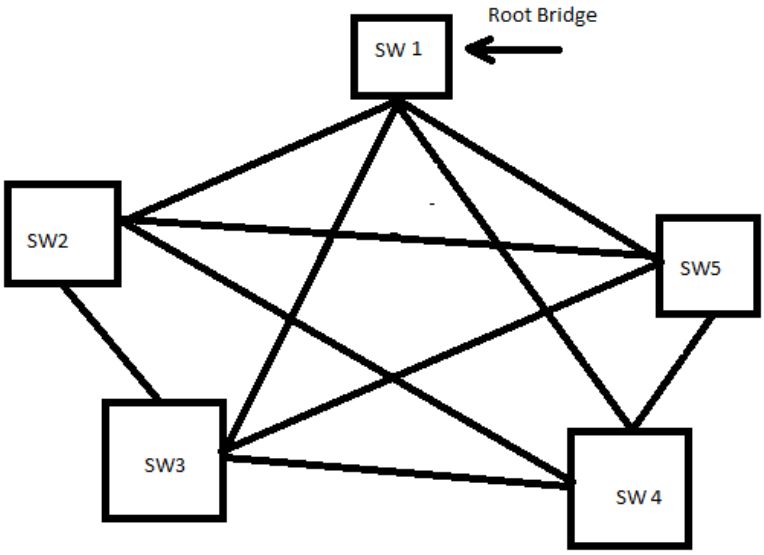


Рисунок 1.2 – Вибір кореневого комутатора

Після вибору кореневого комутатора, обчислюються найкоротші шляхи де кожен комутатор вибирає один оптимальний порт для зв’язку з коренем (Root Port) [1] (рис. 1.3).

Для визначення портів для пересилання (Designated Ports) визначаються активні порти, через які буде здійснюватися передача кадрів [1] (рис. 1.3).

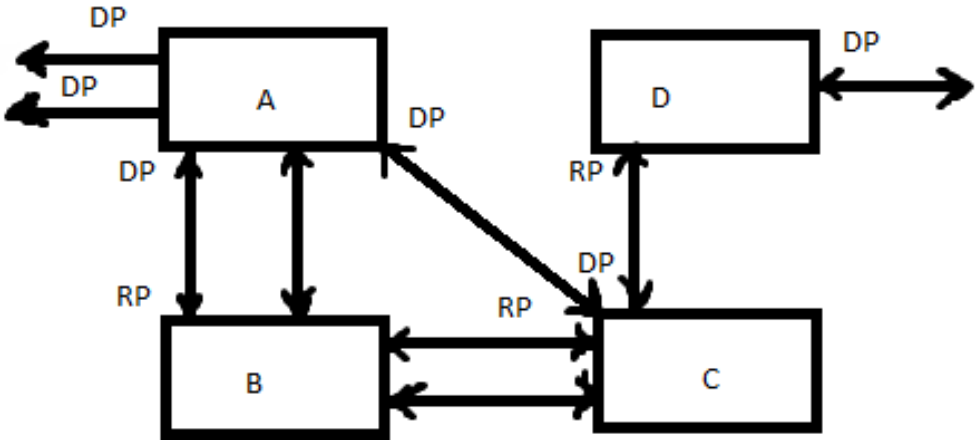


Рисунок 1.3 – Вибір оптимального та активного порту

Блокування зайвих портів порти, які можуть створити петлі, переходять у стан блокування (Blocking) [1] (рис. 1.4).

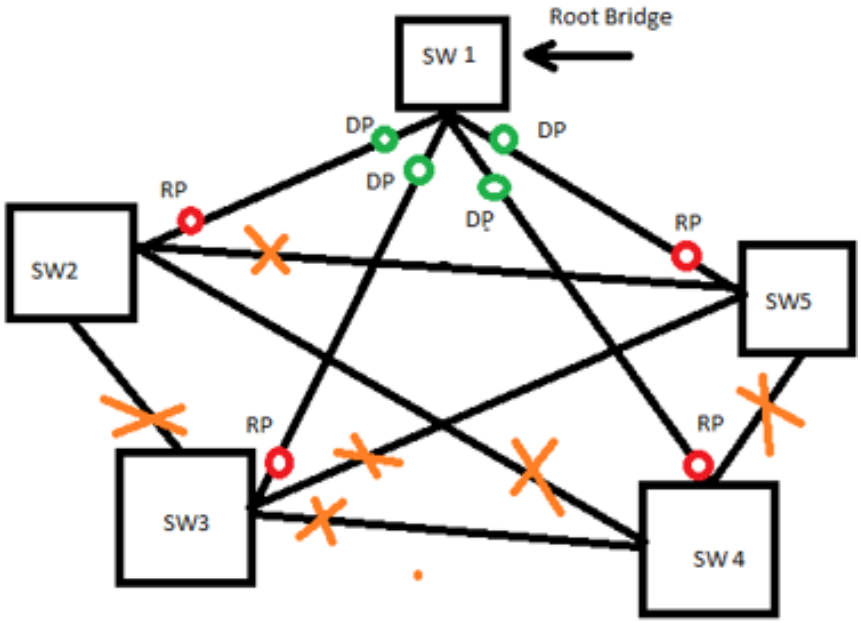


Рисунок 1.4 – Алгоритм блокування порту

Моніторинг та коригування топології STP постійно перевіряє стан мережі, реагуючи на зміни (наприклад, вихід з ладу активного каналу).

Статуси портів в STP:

– блокування (Blocking) порт блокує весь трафік, окрім BPDU;

– слухання (Listening) комутатор очікує BPDU для визначення топології;

– навчання (Learning) порт навчається MAC-адресам перед тим, як почати передавати кадри;

– переадресація (Forwarding) нормальний режим роботи, кадри передаються між сегментами мережі;

– відключений (Disabled) порт вимкнений адміністративно або через помилку

Порт може знаходитися в цих п’ятьох станах наступним чином (рис. 1.5).

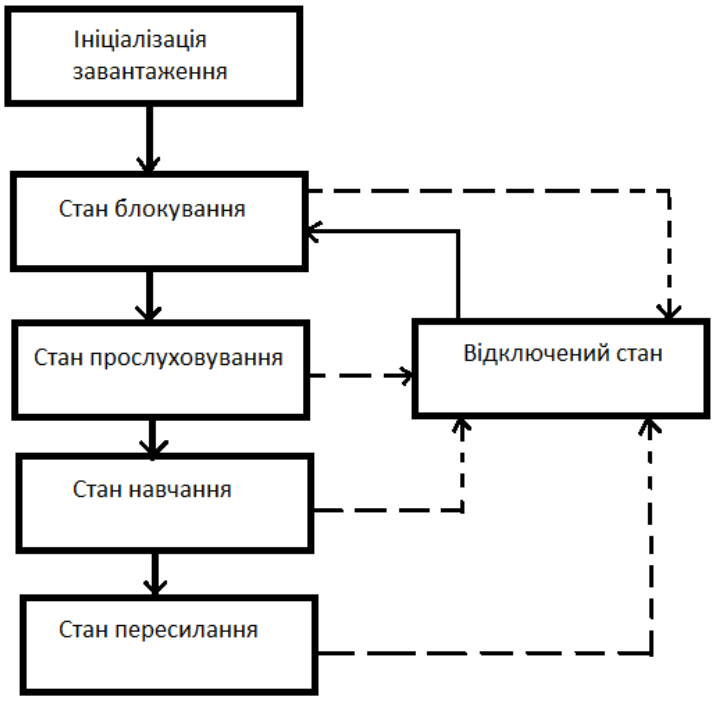


Рисунок 1.5 – Стани порту

Недоліками протоколу STP є те що коли вникає збій в мережі, відновлення маршруту займає приблизно до 30с [2]. Також якщо не справний зв’язок повертається до роботи то це може призвести до не працездатності частини мережі до 4с. Та навіть у випадку точкових підключень (наприклад, між

комутатором і ПК) нові з'єднання проходять етап навчання, що може спричинити додаткові затримки.

STP створює дерево з кореневим мостом і шляхом без петель до всіх пристроїв у мережі. Він переводить резервні шляхи в стан очікування (заблокований). У разі збою алгоритм STP перераховує топологію та активує резервний шлях.

1.2.2 Протокол RSTP

Розглянемо протокол RSTP (Rapid Spanning Tree Protocol), це вдосконалена версія класичного STP (IEEE 802.1D).

RSTP забезпечує швидшу конвергенцію мережі у разі змін топології, що дозволяє значно зменшити час відновлення з'єднань. Використання цього протоколу дозволяє усунути петлі у мережі, запобігаючи появі дублікатних маршрутів у середовищі Ethernet із резервними з’єднаннями.

Завдяки цьому протокол підвищує стійкість мережі до збоїв, оскільки відмова одного каналу не впливає на роботу альтернативних маршрутів.

Найпоширеніше початкове розгортання RSTP це в основі та розподіл шарів мережі перемикання рівня 2 моделі OSI [3]. Це розгортання забезпечує високодоступну мережу, необхідну в середовищі послуг-постачальника. RSTP вдосконалює експлуатацію дерева, що охоплює, зберігаючи сумісність з попереднім обладнанням, яке базується на (оригінальному) IEEE 802.1D, що охоплює дерево. RSTP використовує переваги point-to-point та забезпечує швидку конвергенцію дерева, що охоплює. Конфігурація дерева, може відбуватися менш ніж за 2 секунди (на відміну від 50 секунд із налаштуваннями за замовчуванням у дереві IEEE 802.1d), що є критичним для мереж, що несуть рух, що чутливий до затримки, наприклад, аудіо та відео [3]. Алгоритм роботи RSTP майже такий самий як у STP окрім станів портів та їх типів.

Обмін BPDU-пакетами передаються кожні 2 с. Кожен комутатор обробляє отриманні данні як показано на (рис. 1.6), та дозволяє комутатору ефективно обробляти BPDU, визначати зміни у топології та відповідно реагувати на них [4].

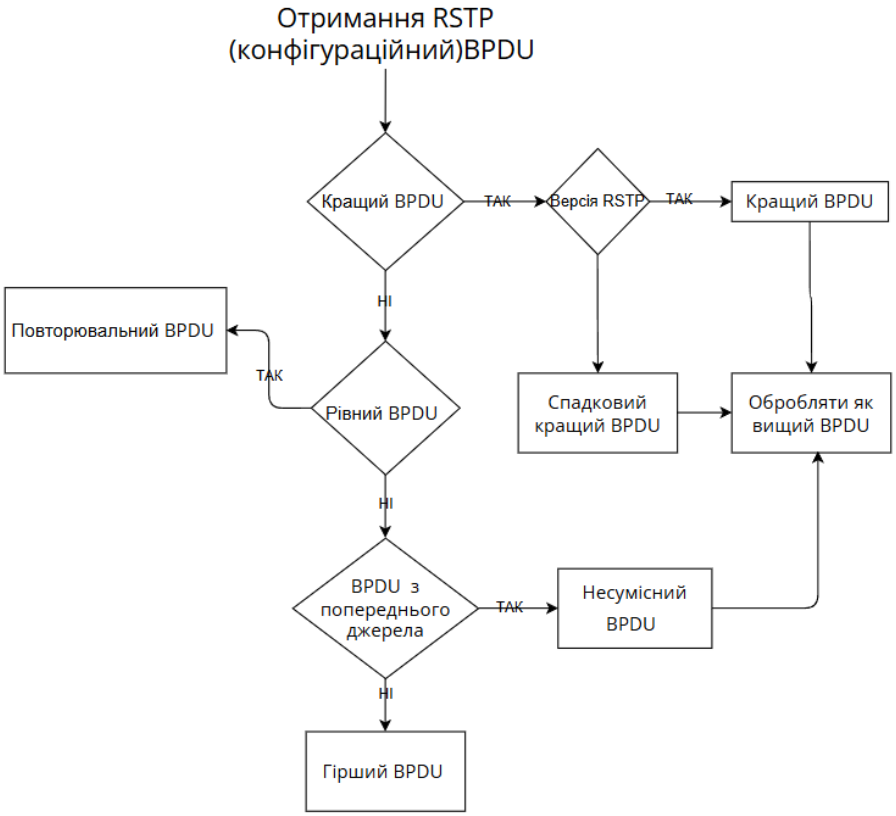


Рисунок 1.6 – Алгоритм обробки BPDU в RSTP

Вибір кореневого комутатора (Root Bridge) комутатор з найменшим ідентифікатором (MAC-адреса + пріоритет) стає кореневим.

Протокол RSTP визначає функції та обов'язки кожного порту в мережі

Кореневий порт (Root Port), через який передаються дані. Він служить найшвидшим способом до кореневого комутатора (рис. 1.7).

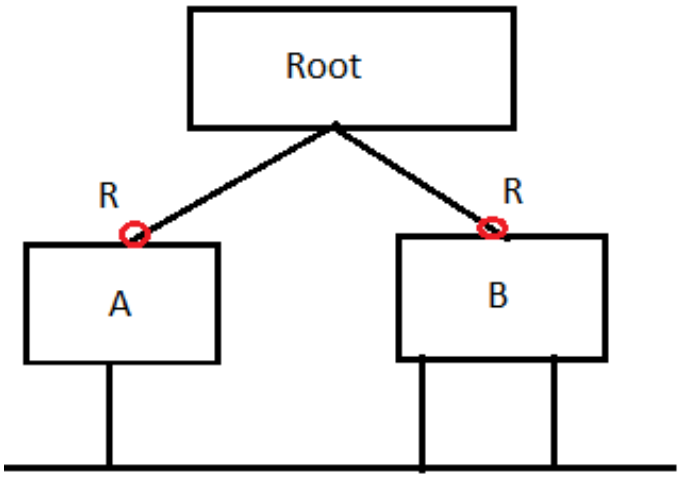


Рисунок 1.7 – Root Port

Призначений порт (Designated Port), через який передаються дані. Визначено для кожного сегмента локальної мережі (рис. 1.8) [4].

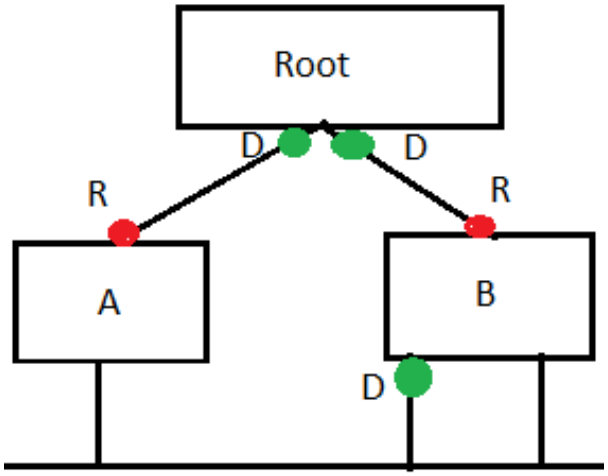


Рисунок 1.8 – Designated Port

Альтернативний порт (Alternate Port) через який не передаються данні (рис. 1.9). Блокований порт визначається як не призначений або кореневий порт та блокований порт отримує більш корисний BPDU, ніж той, який він надсилає на своєму сегменті і який миттєво активується при виникненні помилки в основного. І щоб залишатися заблокованим порт повинен отримати BPDU [4].

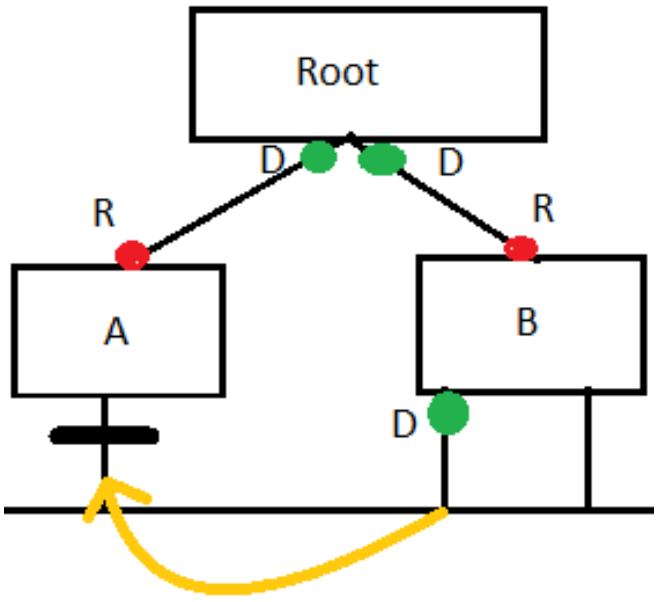


Рисунок 1.9 – Alternate Port

Резервний порт (Backup Port) це резервний порт для зв’язку в рамках одного комутатора (рис 1.10).

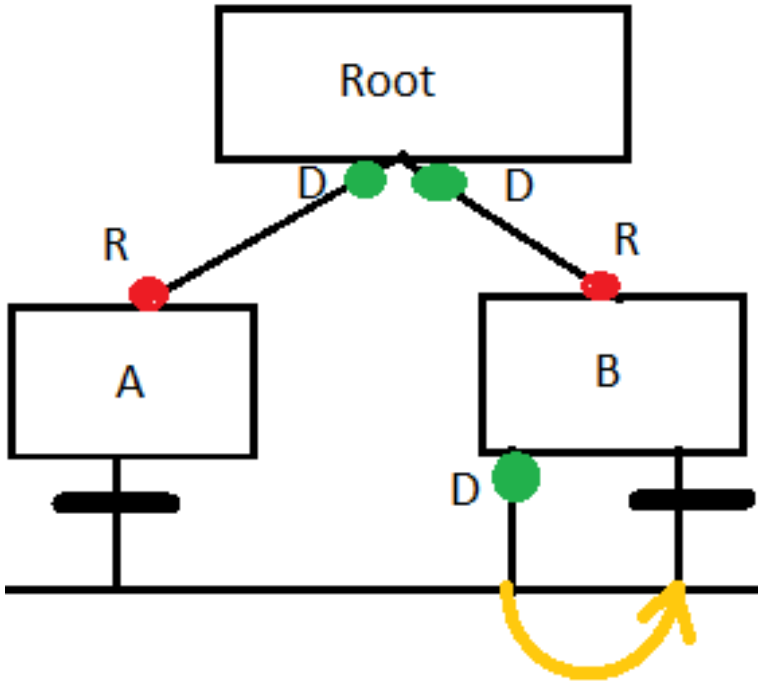


Рисунок 1.10 – Backup Port

Прискорений процес активації портів тепер замість по шагового переходу Blocking → Listening → Learning → Forwarding, RSTP порти можуть активуватись одразу після виявлення змін у топології [3]. У нього є три стани порту це:

– відкидання (Discarding) який поєднує в собі STP-статуси Blocking, Listening, Disabled та порт не пересилає трафік;

– навчання (Learning) комутатор навчається MAC-адресам, але не передає кадри;

– переадресація (Forwarding) нормальний режим роботи, передача та навчання MAC-адрес.

Перевагами цього протоколу є швидке відновлення зв’язку за 2 с. Швидке відновлення портів після збою та альтернативний порт забезпечує миттєвий перехід у разі відмови основного каналу. Та має зворотною сумісність а саме може працювати у гібридному режимі разом із STP.

До недоліків можна віднести залежність в апаратного забезпечення а саме потребує нового обладнання також цей протокол не сумісний з застарілими мережами. Немає балансування навантаження тому що він блокує резервні потри залишаючи тільки один основний порт. У масштабних мережах RSTP може бути недостатньо ефективним через централізований вибір кореневого комутатора і рекомендується використовувати не більше сими комутаторів [3].

1.2.3 Протокол MSTP

Розгляньмо протокол MSTP (Multiple Spanning Tree Protocol) він є покращеною версією RSTP, за допомогою якого можна створювати окремі дерева для груп VLAN, це балансує навантаження трафіку та оптимізує його.

MSTP розділяє мережу на регіони MST, кожен із яких може містити кілька зв’язуючих дерев (MST Instance, MSTI) з незалежною топологією (рис 1.11) [5].

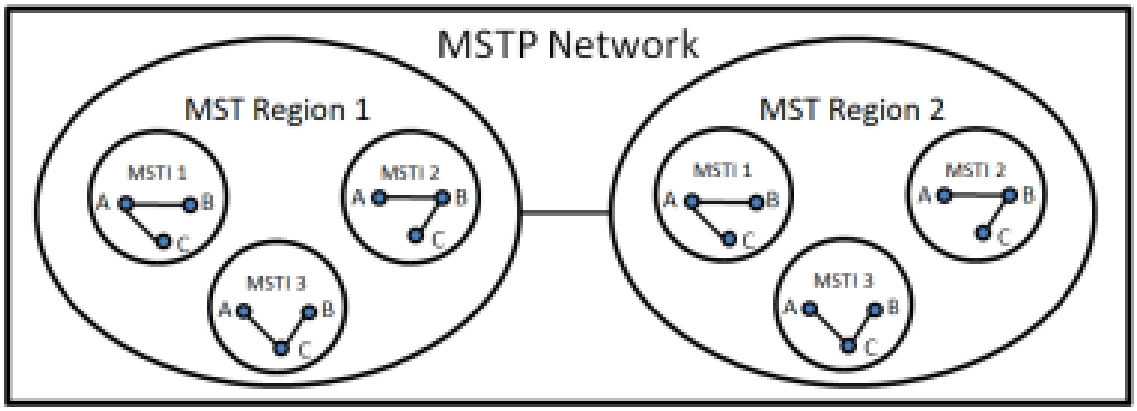


Рисунок 1.11 – Розділення мережі на регіони [5]

Щоб комутатори належали до одного регіону MST, їх конфігурація повинна збігатися за такими параметрами [5]:

– номер ревізії MSTP;

– назва регіону;

– відображення VLAN на MSTI.

У мережі може бути кілька MST-регіонів. MSTP визначає такі типи зв’язуючих дерев [6]:

– внутрішнє охоплення дерева (Common Spanning Tree) загальне дерево,

що з'єднує всі MST-регіони та мости SST;

– поширене та внутрішнє обертальне дерево (Common and Internal Spanning Tree) єдине дерево, що об'єднує CST кожного MST-регіону;

– одиничне сполучне дерево (Single Spanning Tree) bridge міст, що підтримує лише одне дерево (CST) через STP або RSTP.

Обчислення MSTP проходить невступним чином. Вибирається кореневий міст CIST Root це комутатор у якого найменший ідентифікатору мережі, далі у кожному MST-регіоні визначається регіональний кореневий міст CIST Region Root комутатор із найменшою вартістю шляху до CIST Root [6]. Після цього для кожного MSTI обирається регіональний кореневий міст MSTI Regional Root за найменшим ідентифікатором серед комутаторів MSTI і останнім кроком є використання алгоритму із стандарту IEEE 802.1D-2004 для визначення активної топології CIST та MSTI.

Недоліками цього протоколу є те цей протокол вимагає ретельного налаштування VLAN і регіонів і не всі комутатори підтримують MSTP що є значною проблемою в налаштуванні та при помилках в конфігурації буде нестабільна робота мережі.

Зазвичай MSTP використовується в мережах з великою кількістю комутаторів щоб зменшити кількість BPDU та уникнути перевантажень, наприклад в дата центрах в яких потрібно оптимізувати навантаження між VLAN.

1.2.4 Порівняння протоколів STP, RSTP, MSTP

Проаналізувавши роботу протоколів сполучного дерева та взявши до уваги їхні особливості переваги та недоліки тому вибір конкретного протоколу залежить від масштабів мережі, вимог до швидкості відновлення з’єднання та підтримки обладнання. STP підходить для простих мереж, тоді як RSTP та MSTP краще проявляють себе у складних і динамічних середовищах.

Щоб краще зрозуміти потрібно скористатися порівняльною таблицею (табл. 1.1).

Таблиця 1.1 – Порівняння характеристик протоколів

Характеристика	STP	RSTP	MSTP
Стандарт	IEEE 802.1D	IEEE 802.1w	IEEE 802.1s
Час збіжності	30-50 секунд	1-2 секунд	1-2 секунд
Типи портів	Root, Designated, Blocking	Root, Designated, Alternate, Backup	Root, Designated, Alternate, Backup
Кількість дерев	1	1	Декілька (для VLAN або їх груп)
Обробка топологічних змін	Використовує таймери	Використовує швидкі повідомлення BPDU	Аналогічно RSTP, але з підтримкою кількох дерев
Балансування навантаження	Немає	Немає	Є (через розподіл VLAN на MSTI)
Сумісність з попередніми версіями	Так	Так	Так
Область застосування	Невеликі та прості мережі	Середні за розміром мережі	Великі корпоративні та операторські мережі

Також ці протоколи підходять для різних типів топології залежно від їх складності, кількості комутаторів та необхідності швидкого відновлення після збоїв та для якої саме топології який протокол підходить найкраще, наведено в (табл. 1.2).

Таблиця 1.2 – Порівняння протоколів до топології [7]

Тип топології	STP	RSTP	MSTP
Шина	Рідко використовується, петлі малоймовірні	Аналогічно STP	Аналогічно STP
Зірка	Підходить, якщо є кілька шляхів	Кращий вибір через швидшу конвергенцію	Використовується у великих мережах
Кільце	Може викликати значні затримки через довгий час збіжності	Швидке перемикання між альтернативними шляхами	Гнучке керування маршрутами в VLAN-середовищі
Дерево	Основний сценарій використання	Покращений контроль маршрутів	Дозволяє створювати окремі дерева для VLAN
Сітка	Високі затримки, обмежене масштабування	Підходить для середніх мереж	Найкращий варіант для масштабованих мереж
Гібридна	Підходить для невеликих мереж	Оптимальний вибір для середніх мереж	Найкращий для великих мереж з VLAN

Розглянувши питання, отримав оптимальний вибір для побудови мережі, це протокол RSTP так як він краще підходить для середніх мереж та забезпечує швидке відновлення після змін у топології. Завдяки прискореній конвергенції, він мінімізує затримки та запобігає довготривалим перебоям у роботі мережі.

1.3 Основні вимоги до мережі

Виходячи з поставленої мети однією з основних вимог до мережі є мінімізація затримок у передачі даних, що особливо критично для середовищ, які працюють у реальному часі, таких як потокове передавання відео чи фінансові транзакції.

Для ефективного функціонування сучасних комп'ютерних мереж необхідно враховувати низку ключових вимог, які безпосередньо впливають на їх продуктивність, надійність та стійкість до збоїв. Одним із основних аспектів є забезпечення безперервності роботи мережі та швидке відновлення зв'язку в разі виходу з ладу окремих вузлів або каналів передачі даних.

Протокол Rapid Spanning Tree Protocol (RSTP) є ключовим елементом у цьому контексті, оскільки забезпечує суттєве скорочення часу відновлення мережі після змін її структури [3].

Також мережа повинна надавати користувачам можливість до ресурсів комп'ютерів які знаходяться в мережі, інші вимоги до мережі це [8]:

– захищеність;

– сумісність;

– розширюваність;

– продуктивність;

– надійність;

– масштабованість.

Високий рівень захисту мережі передбачає можливість швидкого

реагування на непередбачувані ситуації, такі як атаки типу «людина посередині» (MITM), атаки викликаючи петлі.

Також проблема безпеки полягає в тому що це можливе пошкодження даних зловмисником, конфіденційність, несанкціонований доступ, крадіжки та інше [8] (рис. 1.12).

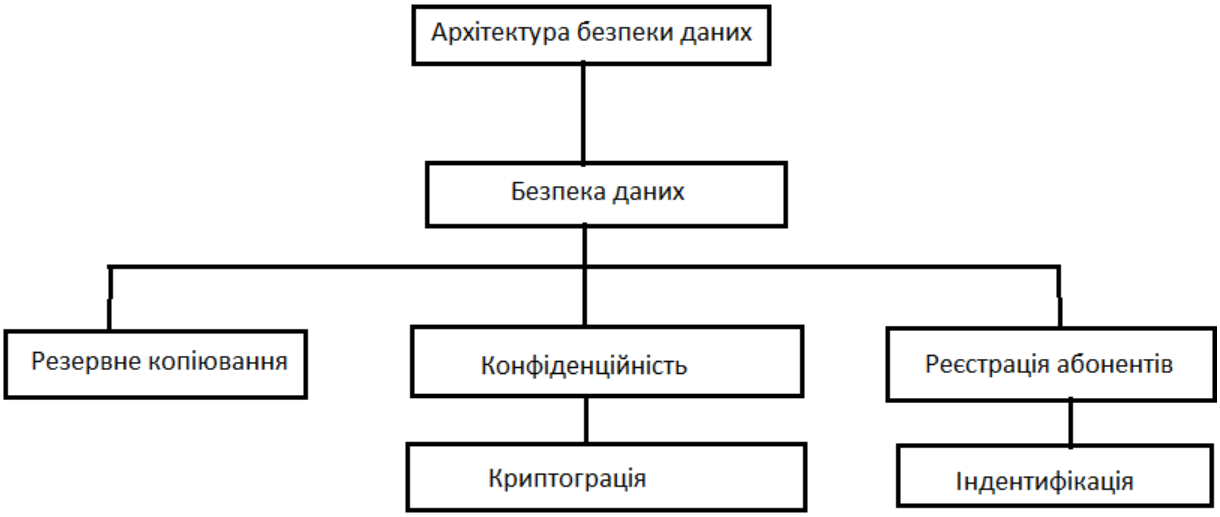


Рисунок 1.12 – Безпека даних

RSTP забезпечує миттєве визначення змін у топології мережі та мінімізує ризики, пов'язані з небажаними петлями, що виникають при фізичних змінах у структурі з’єднань. Основним інструментом залишається резервне копіювання (backup). Копія регулярно оновлюється, щоб забезпечити максимально швидкий і ефективний доступ до актуальних даних у разі втрати чи пошкодження основної інформації. Забезпечити надійний захист даних від різних загроз найзручніше у мережі з виділеним файловим сервером. Усі важливі файли зберігаються на серверах, що значно спрощує захист, адже забезпечити безпеку сервера набагато легше, ніж багатьох машин. Крім того, така централізація даних полегшує процес резервного копіювання, оскільки немає потреби збирати інформацію з усієї мережі.

Сумісність передбачає здатність мережі взаємодіяти з різноманітними апаратними та програмними компонентами, зокрема забезпечувати спільну роботу пристроїв і систем від різних виробників, що використовують різні

протоколи зв’язку та операційні середовища. [9]. Це означає, що пристрої, які підтримують лише STP, можуть працювати в тій самій мережі з пристроями, які підтримують RSTP.

Таким чином, при оновленні мережевих пристроїв не потрібно повністю змінювати всю інфраструктуру, що забезпечує плавний перехід до більш швидкого і ефективного протоколу.

Розширюваність дозволяє в мережу відносно просто додавати нові елементи, такі як користувачі, комп’ютери, додатки чи служби, збільшувати довжину сегментів та замінювати наявне обладнання на потужніше це дозволяє ефективно додавати нові пристрої в мережу без значних змін у топології або підвищення часу відновлення з'єднань [9].

Протокол здатен працювати в великих мережах з кількома комутаторами, автоматично знаходячи оптимальні шляхи передачі даних при кожній зміні конфігурації.

Продуктивність є однією з ключових характеристик розподілених систем, зокрема комп’ютерних мереж. Вона досягається завдяки можливості розподілу навантаження між кількома комп’ютерами в мережі. Однак реалізувати цей потенціал вдається не завжди.

Основними показниками продуктивності мережі є [10]:

– час реакції;

– пропускна спроможність;

– затримка передачі та варіація затримки.

За рахунок зменшеного часу відновлення з'єднань та зниженої потреби в обміні станами між комутаторами, RSTP значно покращує продуктивність мережі. Протокол використовує технологію швидкого переходу до робочих станів, що дозволяє мінімізувати час затримки і підвищує загальну швидкість обміну даними в мережі.

Пропускна спроможність показує обсяг даних, що передаються мережею за одиницю часу. Вона не є безпосередньо користувацьким показником, адже стосується внутрішніх процесів, таких як передача пакетів між вузлами через

комунікаційні пристрої. Однак саме вона визначає ефективність основної функції мережі транспортування інформації.

Пропускна спроможність вимірюється в бітах або пакетах за секунду та поділяється на:

– середню розраховується як відношення загального обсягу переданих даних до часу їх передачі за тривалий період (година, день, тиждень);

– миттєво визначається аналогічно, але за короткий проміжок часу (наприклад, 10 мс. або 1 с.);

– максимально фіксує найбільше значення миттєвої пропускної спроможності протягом періоду спостереження.

Пропускна спроможність і затримка передачі є незалежними характеристиками мережі. Це означає, що система може забезпечувати високу пропускну спроможність, але при цьому мати значні затримки в доставці пакетів тому пропускна спроможність і затримка передачі є незалежними характеристиками мережі [10]. Це означає, що система може забезпечувати високу пропускну спроможність, але при цьому мати значні затримки в доставці пакетів.

Надійність яка є однією з найважливіших характеристик обчислювальних мереж. Її підвищення ґрунтується на запобіганні несправностям, що досягається зменшенням частоти відмов і збоїв. Це можливо завдяки використанню електронних схем і компонентів із високим або надвисоким рівнем інтеграції, зниженню рівня перешкод, оптимізації режимів роботи схем, дотриманню теплових параметрів, а також удосконаленню технологій збирання апаратного забезпечення.

Масштабованість означає, що мережа здатна розширюватися, збільшуючи кількість вузлів і протяжність з’єднань у широких межах, без погіршення її продуктивності RSTP, будучи вдосконаленою версією STP, краще адаптується до динамічних змін у топології завдяки механізму швидкої конвергенції, що дає змогу без значних затримок інтегрувати нові сегменти мережі.

Було розглянуто основні вимоги до сучасних комп’ютерних мереж, серед

яких ключовими є мінімізація затримок, надійність, безпека, продуктивність, масштабованість, розширюваність і сумісність. Особливу увагу приділено протоколу RSTP як ефективному рішенню для підвищення швидкодії мережі, забезпечення відмовостійкості та адаптації до змін топології. Для досягнення високого рівня захищеності розглянуто методи резервного копіювання й централізації даних. Таким чином, дотримання цих вимог дозволяє створити стабільну, гнучку й ефективну мережеву інфраструктуру.

1.4 Постановка завдання

Виходячи із мети роботи сучасні компанії потребують надійної та безпечної комп’ютерної мережі, яка забезпечуватиме безперебійний обмін даними між усіма підрозділами, підтримуватиме роботу корпоративних інформаційних систем і відповідатиме актуальним вимогам щодо захисту інформації. Основна мета проєкту це створення розподіленої комп’ютерної мережі для підприємства, яка гарантуватиме стабільний та швидкий доступ користувачів до необхідних ресурсів.

У процесі виконання проєкту планується спочатку розглянути, як працюють протоколи сполучного дерева STP, RSTP та MSTP. Потрібно розібратися в їхніх алгоритмах, порівняти їх між собою та з’ясувати, в яких ситуаціях доцільніше використовувати той чи інший варіант. Після цього формуються загальні вимоги до майбутньої мережі, враховуючи ключові параметри: швидкодія, безпека, зручність у розширенні, стійкість до збоїв і сумісність з іншими технологіями.

Наступним кроком буде аналіз інформаційних потоків потрібно зрозуміти, які обсяги даних передаватимуться між підрозділами, які служби навантажують мережу найбільше, і на основі цього спрогнозувати навантаження на канали. Це дасть змогу розробити функціональну та структурну схему всієї мережі, де

будуть показані всі основні пристрої, їхні зв’язки та роль у мережевій топології.

Далі слід приділити увагу проблемі петель у мережі, яка може виникати при використанні комутаторів. Потрібно дослідити, як ця проблема вирішується на практиці за допомогою таких функцій, як RSTP, BPDU Guard, Root Guard тощо. Після того, як буде чітко сформульовано, які функції має виконувати мережа, необхідно обрати відповідні технології, протоколи та мережеве обладнання. У роботі будуть розглянуті такі протоколи, як VLAN, VTP, DHCP, NTP, IPSec та інші, які допомагають забезпечити ефективну та безпечну роботу мережі.

У підсумку проєкт повинен охоплювати все починаючи від аналізу вимог і розробки схеми до вибору обладнання та тестування мережевої моделі у віртуальному середовищі. Результати цієї роботи можуть бути основою для реального впровадження мережі на підприємстві або для подальшого вдосконалення мережевої інфраструктури.

2 ПРОЄКТУВАННЯ МЕРЕЖІ ТА ВИБІР ТЕХНІЧНИХ РІШЕНЬ

2.1 Аналіз інформаційних потоків

Виходячи з поставленого завдання та враховуючи необхідність забезпечення стабільної й ефективної роботи мережі, перед побудовою потрібно здійснити розрахунок навантаження для кожної філії підприємства, а також для всієї глобальної мережі. Цей крок дозволяє оцінити обсяг трафіку, потреби в пропускній здатності. На основі отриманих даних можна вибрати оптимальні стандарти та технології, які найкраще відповідають вимогам по продуктивності, надійності та масштабованості мережі.

Розрахуємо мінімальну швидкість каналів зв’язку для кожної філії для цього рахуємо кінцевих користувачів в кожній філії:

– перша філія = 45 користувачів;

– друга філія = 23 користувачів;

– третя філія = 18 користувачів;

– четверта філія = 30 користувачів.

Знайдемо загальний обсяг корисних даних для кожної філії, який потрібно передати за 10 хвилин та час у секундах:

– для першої філії Vк = 45 * 100 МБ = 4,5 ГБ обсяг корисних даних;

– для другої філії Vк = 23 * 100 МБ = 2,3 ГБ обсяг корисних даних;

– для третьої філії Vк = 18 * 100 МБ = 1,8 ГБ обсяг корисних даних;

– для четвертої філії Vк = 30 * 100 МБ = 3 ГБ обсяг корисних даних.

Далі визначмо MSS (Maximum Segment Size максимальний розмір сегмента) MSS = MTU - IP - TCP = 1500 - 20 - 20 = 1280 байт корисних даних.

Тепер розрахуємо кількість пакетів для кожної філії:

– кількість пакетів 4,5ГБ/1280 байт = 3 778 000 пакетів в першій філії;

– кількість пакетів 2,3ГБ/1280 байт = 1 796 875пакетів в другій філії;

– кількість пакетів 1,8ГБ/1280 байт = 1 509 949 пакетів в третій філії;

– кількість пакетів 3ГБ/1280 байт = 2 343 750 пакетів в четвертій філії.

Знаходим кількість заголовків в кожній філії:

– обсяг заголовків 3 778 000 * (20 + 20 + 20) байт = 226 680 000 байт;

– обсяг заголовків = 1 796 875 * (20 + 20 + 20) байт = 107 812 500 байт;

– обсяг заголовків = 1 509 949 * (20 + 20 + 20) байт = 90 596 940 байт;

– обсяг заголовків 2 343 750 * (20 + 20 + 20) байт = 140 625 000 байт.

Обчислимо загальний обсяг даних в бітах:

– перша філія V = 4,5 ГБ * 8 = 36 Гбіт;

– друга філія V = 2,3 ГБ * 8 = 18,4 ГБіт;

– третя філія V = 1,8 ГБ * 8 = 14,4 ГБіт;

– четверта філія V = 3 ГБ * 8 = 24 ГБіт.

Визначили загальний обсяг даних, який потрібно передати за 10 хвилин.

Наступним кроком буде визначення швидкості передачі даних:

– швидкість передачі даних в першій філії R1(t) = 36 ГБ / 600с = 60 Мб/с;

– швидкість передачі даних в другій філії R2(t) = 18,4 ГБ / 600с = 30 Мб/с;

– швидкість передачі даних в третій філії R3(t) = 14,4 ГБ / 600с = 24 Мб/с;

– швидкість передачі даних в четвертій філії R4(t) = 24 ГБ / 600с = 40 Мб/с.

Визначивши швидкість передачі даних в усіх філіях тепер визначмо швидкість передачі у глобальній мережі.

Знайдемо загальний обсяг корисних даних, який потрібно передати за 10 хвилин та час у секундах.

Vк = 117 * 100 МБ = 11,7 ГБ - загальний обсяг корисних даних.

T = 10 * 60 = 600 с - час у секундах.

Визначимо MSS (Maximum Segment Size) максимальний розмір сегмента для глобальної мережі. MSS = MTU - IP - TCP = 1500 - 20 - 20 = 1280 байт корисних даних. Далі рахуємо кількість пакетів = 11,7 ГБ / 960 байт = 12 187 500 пакетів. Проводимо розрахунок обсягу заголовків = 17 604 167 * (20 + 15 + 25) байт = 1 056 250 020 байт

Обчислимо загальний обсяг даних в бітах V = 11,7 ГБ * 8 = 93,6 ГБіт загальний обсяг даних, який потрібно передати за 10 хвилин.

Визначимо швидкість передачі даних у глобальній мережі R(t) = V / T = 93,6 ГБ / 600 с ≈ 156 Мб/с.

Отже, мінімальна швидкість каналу зв'язку, яку потрібно забезпечити у сегменті мережі з 117 користувачами, при одночасній передачі ними файлів обсягом по 100 МБайт за умови, що час передачі кожного користувача не перевищує 10 хвилин, складає приблизно 156 Мб/с.

Оскільки в реальних умовах присутня додаткове навантаження такий як фоновий трафік, відео конференції, веб серфінг тощо. Потрібно брати запас от 30% до 50% забезпечивши не менше 200 Мб/с для глобальної мережі також збільшивши швидкість і у локальних мережах.

Взявши до уваги розрахунки та необхідний запас швидкості мережі, для стабільної роботи буде використовуватися стандарт 1000BASE-T максимальна швидкість 1 Гб/с і використання витої пари стандарту Cat 5e для локальних мереж. А для глобальної мережі використовується 1000BASE-BX10 дає доступ до мережі через оптоволоконну лінію на швидкості до 1 Гбіт/с.

Розглянувши завдання з аналізу інформаційних потоків, було отримано повне уявлення про необхідну пропускну здатність каналів у локальних і глобальних сегментах мережі. Це дозволило обґрунтовано обрати відповідні технології та стандарти для подальшого проєктування мережі.

2.2 Розробка функціональної схеми

Згідно із завданням проєктування, визначено основні кроки створення комп’ютерної мережі для підприємства. Для побудови розподіленої мережі, яка об'єднує кілька віддалених філій, необхідно врахувати технічні вимоги, забезпечити високу надійність, захист від збоїв, безпеку даних, ефективну взаємодію між підрозділами, а також запобігти виникненню петель у мережевій топології.

Мережа базується на розподіленій інфраструктурі, де кожна філія має власну локальну інфраструктуру, інтегровану в загальну корпоративну мережу. У кожній філії встановлено від 2 до 4 комутаторів залежно від кількості користувачів. Один із комутаторів виконує роль центрального, до якого підключені інші комутатори що забезпечує правильне підключення комп'ютерів та інших пристроїв. Деякі комутатори розбиті на VLAN для сегментації трафіку та застосовується VTP, що спрощує управління та зменшує ризик конфігураційних помилок.

Для забезпечення надійності комутатори у філіях з'єднані між собою, і тим самим утворюють резервні лінії, та для запобігання петель і правильній роботі мережі використовується протокол RSTP. Для синхронізації часу між мережевими пристроями використовується NTP, що гарантує точність часових міток у логах та коректну роботу безпекових систем.

Для моделювання мережі обрано Cisco Packet Tracer. Функціональна схема мережі представлена на (рис. А.1).

Кожна філія має власний маршрутизатор, який забезпечує організацію локальної мережі та підключення до загальної корпоративної інфраструктури.

Дві філії обладнані серверами, доступними для всіх пристроїв у мережі.

Для підключення обладнання у філіях використовується кабель вита пара стандарту Cat 5e та з використанням мережевого стандарту 1000BASE-T для забезпечення високої швидкості передачі даних в середині філій до 1 Гбіт/с. Для WAN використовується мережевий стандарт 1000BASE-BX10 що забезпечить швидкість передачі даних до 1 Гбіт/с по одному волокну оптоволокна.

Захищене передавання даних між віддаленими сегментами забезпечується за допомогою IPsec, який використовує шифрування для запобігання несанкціонованому доступу до трафіку.

Після побудови мережі необхідно виконати її початкове налаштування, зокрема конфігурацію LAN та маршрутизацію WAN, а після цього впроваджувати додаткові технології. Завершальним етапом є тестування мережі, щоб уникнути можливих неполадок у майбутньому. Конфігурацію мережі наведено в (табл. 2.1)

Таблиця 2.1 – Конфігурація мережі

Пристроїв	Кількість мереж	Серверів	Стандарти локальних та глобальних мереж	Мережеве обладнання	Фізичне середовище	Маршрутизація
117	4	2	1000BASE-T 1000BASE-BX10	Switch Router	Вита пара, Оптичний кабель	Статична

На робочу область Cisco Packet Tracer, перенесено:

– 117 PC;

– 2 сервер Server;

– 16 комутаторів 2950-24;

– 4 маршрутизаторів 2901 (з встановленим модулем HWIC-2T).

Розглянувши завдання з побудови функціональної схеми, отримали проєкт розподіленої мережі, який відповідає вимогам до надійності, безпеки, керованості та продуктивності. Впроваджені технології VLAN, VTP, RSTP, NTP,

DHCP і IPsec дозволяють забезпечити стабільну взаємодію між усіма філіями підприємства.

2.3 Проблеми виникнення петель мережах та методи боротьби з ними

Розглянемо проблеми виникнення петель та їх вирішення в розподілених мережах, побудованих за технологією Ethernet які можуть призвести до серйозних збоїв у роботі мережі. Петлі виникають, коли існує більше одного шляху між двома вузлами мережі, що спричиняє безкінечне циклювання широкомовних (broadcast) або багатоадресних (multicast) кадрів між комутаторами.

Це може викликати ефект «шторму широкомовного трафіку» (broadcast storm), що перевантажує мережу і значно знижує її продуктивність [11].

Головною причиною утворення петель є особливості роботи комутаторів Ethernet, які не мають вбудованих механізмів виявлення дублікатів кадрів. Коли один і той самий кадр передається між комутаторами через кілька маршрутів, пристрої продовжують його обробляти і перенаправляти, оскільки не знають, що цей кадр вже був отриманий. Це створює надлишкове навантаження на мережу, споживаючи пропускну здатність каналів і ресурси комутаторів, що може призвести до повної втрати працездатності мережевої інфраструктури.

Ще однією проблемою, пов’язаною з петлями, є порушення нормального функціонування механізму навчання MAC-адрес комутаторами. Комутатори зберігають у своїх таблицях MAC-адреси пристроїв і відповідні порти, через які вони доступні, при утворенні петлі один і той самий пристрій може бути доступний через кілька портів комутатора, що призводить до постійного оновлення записів у таблиці MAC-адрес [12]. Це може викликати ситуацію, коли комутатор не зможе правильно визначити, через який порт слід передавати

кадри, і змушений буде їх широкомовно транслювати по всіх портах, що ще більше погіршує ситуацію.

Для боротьби з петлями у мережах Ethernet використовуються спеціальні механізми, основним з яких є протокол Spanning Tree Protocol (STP) та його покращені версії, такі як Rapid Spanning Tree Protocol (RSTP) і Multiple Spanning Tree Protocol (MSTP) [7]. Протоколи які описані вище створюють сполучне дерево в якому обирається один кореневий комутатор (Root Bridge), а інші комутатори повинні побудувати найкоротший шлях до кореневого комутатора.

Якщо комутатор виявляє надлишкові з'єднання, один із портів блокується, запобігаючи утворенню петлі. Під час відмови каналу який є активним тобто через нього передаються данні, тоді STP або RSTP автоматично змінюють топологію та переходять на резервний маршрут роблячи його активним.

Додатковим механізмом є використання функції BPDU Guard, яка запобігає підключенню несанкціонованих комутаторів до мережі, що може викликати зміну топології RSTP і створення петель [11]. Щоб не керовані пристрої не ставали кореневими використовується Root Guard що не дає спричинити нестабільність у мережі. Ще один ефективний спосіб боротьби з петлями це Loop Guard, який запобігає ситуаціям, коли порти комутатора переходять у некоректний стан через тимчасовий збій або втрату BPDU-пакетів [7]. Використання EtherChannel дозволяє з'єднати кілька фізичних каналів у єдиний логічний зв'язок, що зменшує ймовірність утворення петель, оскільки канали працюють як єдиний шлях передачі даних.

Для захисту від петель на рівні користувацьких портів можна застосовувати PortFast, що дозволяє кінцевим пристроям одразу переходити в активний стан без очікування конвергенції RSTP [3]. У поєднанні з BPDU Guard цей метод захищає мережу від випадкових змін у топології через неправильні підключення. Також важливою практикою є ретельне проєктування топології мережі, де використання резервних з'єднань має бути добре продуманим і контрольованим. Адміністратори повинні уникати довільного з'єднання комутаторів без застосування відповідних механізмів захисту від петель. Таким

чином, проблема петель у розподілених мережах Ethernet є серйозною загрозою для стабільності роботи мережі, оскільки може призвести до перевантаження трафіку, некоректного навчання MAC-адрес комутаторами до повного збою мережевих сервісів.

Для її вирішення застосовуються різні методи, серед яких ключову роль відіграють протоколи STP, RSTP, MSTP, а також механізми захисту BPDU Guard, Root Guard, Loop Guard, EtherChannel та PortFast. Комплексне використання цих технологій дозволяє забезпечити стабільну, надійну та безпечну роботу мережевої інфраструктури.

Розглянувши дане питання було отримане наступне, а саме що петлі в мережах Ethernet є критичною проблемою, яка може призвести до повної зупинки роботи мережі через перевантаження трафіком і порушення обміну даними. Щоб уникнути такої ситуації, потрібно використовувати механізми захисту, наприклад як Loop Guard, BPDU Guard, PortFast, Root Guard, EtherChannel та використовувати протоколи STP, RSTP, MSTP [14]. Правильне проєктування мережі та комплексне застосування цих засобів дозволяють забезпечити стабільну та надійну роботу інфраструктури.

2.4 Вибір технологій та протоколів

Спираючись на визначені вимоги до мережі, кількість обладнання та його розташування і проаналізувавши швидкість каналів будуть обрані наступні технології:

Gigabit Ethernet за стандартом 1000BASE-T (IEEE 802.3ab) цей стандарт дозволяє передавати дані зі швидкістю до 1 Гбіт/с на відстані до 100 метрів за допомогою звичайного мідного кабелю[13]. Важливою особливістю є підтримка повно дуплексного режиму, що означає можливість одночасної передачі та прийому даних без зниження загальної пропускної здатності мережі.

Для досягнення такої швидкості передача даних здійснюється через всі чотири пари витої пари зазвичай використовується кабель категорії Cat5e або Cat6. Що дозволяє ефективно використовувати наявну інфраструктуру, без необхідності встановлення дорогих оптоволоконних ліній для покриття типових офісних або корпоративних приміщень.

Ключовою перевагою 1000BASE-T є те що цей стандарт сумісний із мережевими інсталяціями які вже існують. Якщо в будівлі прокладено мідні кабелі категорії Cat5e або вище, їх можна використовувати для побудови гігабітної мережі без додаткових витрат на заміну кабельної системи.

Мережевий стандарт 1000base-bx10 (Gigabit Ethernet over Single Fiber) він дозволяє передавати данні на відстань до 10 км зі швидкістю 1 Гбіт/с по оптоволокну, використовуючи розділення по хвилі [15].

Це досягається завдяки використанню технології розділення за довжиною хвилі (Wavelength Division Multiplexing, WDM), що дозволяє одночасно здійснювати прийом і передачу даних по різних довжинах хвиль у межах одного волокна.

На відміну від класичних рішень, де для повно дуплексного з’єднання необхідно два оптичні волокна одне для передачі, інше для прийому BX10 дає змогу значно оптимізувати витрати на прокладення кабельної інфраструктури.

Що особливо актуально в умовах, коли прокладання додаткових волокон є технічно складним або надто дорогим, наприклад, у вже забудованих районах, підземних комунікаціях чи між будівлями. Для роботи за цим стандартом необхідна пара спеціалізованих трансиверів [15]:

– завантаження від клієнта BX10-U (Upstream) здійснює передачу даних на довжині хвилі 1310 нм і прийом на 1490 нм;

– завантаження до клієнта BX10-D (Downstream) навпаки, передає на 1490 нм і приймає на 1310 нм.

Така схема роботи дозволяє ефективно розподілити потоки трафіку, не заважаючи один одному, і водночас скоротити кількість фізичних з'єднань. При правильному налаштуванні ці трансивери забезпечують надійну, стабільну

комунікацію навіть на значних відстанях.

Однією з головних переваг 1000BASE-BX10 є його здатність передавати дані на великі відстані до 10 км без втрати якості з’єднання. Також варто відзначити високу стійкість оптичного сигналу до електромагнітних завад, що робить цю технологію ідеальною для промислових об’єктів, транспортної інфраструктури або місць з підвищеним рівнем електромагнітного шуму.

Крім технічних характеристик, значення має й економічний аспект: використання лише одного волокна значно знижує витрати на матеріали та монтаж. У випадку з великими об'єктами або довгими каналами зв'язку, це може призвести до суттєвого зменшення загальної вартості реалізації мережі.

Розглянувши питання можна дійти висновку, що використання цих стандартів дозволяє побудувати гнучку та ефективну мережеву інфраструктуру.

В одному випадку це дає можливість використовувати вже наявні мідні кабелі для організації швидкісного з’єднання всередині приміщень, в іншому забезпечити стабільну передачу даних на великі відстані при мінімальних витратах.

Такий підхід дозволяє не лише зменшити вартість розгортання мережі, а й забезпечити її надійну роботу відповідно до вимог конкретного об’єкта.

2.1.1 VTP протокол

Виходячи з завдання, для забезпечення зручного та централізованого управління віртуальними локальними мережами (VLAN) у корпоративному середовищі, було обрано протокол VTP (VLAN Trunking Protocol), розроблений компанією Cisco. Метою цього протоколу є автоматизація та обмін інформацією про VLAN між комутаторами та забезпечити узгодженість конфігурації в усій мережі. VTP може створювати, змінювати та видаляти VLAN та номер ревізії збільшується на +1. Після цього розсилаються оголошення, де вказаний номер ревізії [18]. Отримавши оголошення, клієнти роблять порівняння номеру ревізії з тим який їм надійшов. Та вони синхронізують свою базу, якщо номер співпадає з ревізією. Інакше оголошення ігнорується VTP має ролі. Роль комутатора за замовченням є сервер.

Існує три режими такі як:

– VTP Server створює, змінює, видаляє VLAN. Якщо отримує оголошення, в яких ревізія старша за нього, то синхронізується та розсилка оголошень робиться постійно яка ретранслюється від сусідів.

– VTP Client не може видаляти, створювати та якось змінювати VLAN.[18] Усі VLAN отримує та синхронізує від сервера. Періодично повідомляє сусідів про свою базу VLAN-ів.

– VTP Transparent має права до внесення змін та видалення VLAN у своїй базі. При отриманні будь-якого оголошення, передає далі, не синхронізуючи зі своєю базою. В порівнянні з іншими режимами у яких номер ревізії збільшується то в цьому режимі він дорівнює 0.

VTP був обраний у роботі через його здатність централізовано керувати VLAN у даній роботі для швидкого налаштування VLAN. Без нього довелося б вручну налаштовувати кожен комутатор окремо, що збільшує ризик помилок та потребує значних затрат часу. Оскільки VTP автоматично синхронізує конфігурацію VLAN між пристроями, він дозволяє швидко та ефективно впроваджувати зміни в мережі. Що особливо важливо в корпоративних середовищах, де регулярні оновлення мережевої інфраструктури є необхідністю.

Завдяки використанню цього протоколу можна значно скоротити час на налаштування мережі, уникнути помилок між комутаторами та забезпечити стабільну й ефективну роботу VLAN.

Розглянувши завдання щодо централізованого управління VLAN, отримали доцільне рішення у вигляді впровадження протоколу VTP, який забезпечує швидке, надійне та масштабоване адміністрування віртуальних мереж.

2.1.2 VLAN протокол

Виходячи із завдання проєктування, потрібно скористатися VLAN (Virtual Local Area Network) для забезпечення сегментування мережі підприємства що дозволяє розділити мережу створюючи ізольовані сегменти, це дозволяє сегментувати мережу без необхідності фізичної логічної сегментації

[17]. Мережі VLAN дуже гнучкі, і їх можна використовувати для забезпечення безпеки та підвищення продуктивності. VLAN інкапсулює Ethernet кадри разом з заголовком, та містить в собі ідентифікатор VLAN. Він використовує ідентифікатор щоб визначати, які саме пристрої знаходяться та до якої VLAN відносять.

Створення VLAN відбувається додаванням портів як окремих так і всіх до якоїсь VLAN.

Мережі VLAN в цьому проєкті використовуються для розділення трафіку що відокремлює різні відділи або групи таких як бухгалтерія, відділ кадрів, адміністрація чи технічна підтримка. Такий підхід підвищує безпеку, оскільки обмежує доступ до ресурсів між VLAN, а також дозволяє краще керувати трафіком, зменшуючи навантаження на мережу та підвищуючи її ефективність.

Що дозволяє робити VLAN:

− побудувати мережу з незалежною логічною структурою, побудова її топології не буде залежить від того, де фізично знаходяться компоненти мережі;

− розбити один такий домен на кілька, трафік широкомовного типу, який належить одному домену, не буде проходити через інший, це дозволяє менше навантажувати мережеве обладнання;

− захист мережі, ігнорування портом комутатора дає змогу відкидати кадри, які поступають з іншого VLAN;

− групувати ПК, та застосовувати політики які входять в одну підмережу;

− здійснювати маршрутизацію за допомогою використання віртуальних портів.

VLAN Trunking за допомогою одного фізичного з’єднання він надсилає трафік з декількох VLAN[17]. Що дає більш ефективне та гнучке налаштування пристроїв. Щоб забезпечити можливість відправки й приймання трафіку, який належить іншій підмережі, портом, його необхідно перевести в стан trunk або тегування.

Можна виділити три головні плюси застосування VLAN:

− можливість гнучкого угрупування девайсів (в тому числі й комп’ютерів,

які підключені до різних комутаторів) і створення таким чином ізольованої підмережі;

− зниження обсягу широкомовного трафіку він просто не транслюється між різними підмережами;

− можливість знизити кількість мережевих пристроїв і кабелів для використання, адже для створення нової віртуальної підмережі не потрібно купувати комутатор і прокладати кабель живлення.

Розглянувши завдання сегментування мережі, отримали оптимальне рішення у вигляді впровадження технології VLAN, яка забезпечує гнучке управління мережею, підвищення її безпеки, зменшення навантаження на обладнання і чітке розмежування трафіку між підрозділами підприємства.

2.1.3 RSTP протокол

Виходячи з теми проєктування для забезпечення надійного функціонування комутованої мережі з мінімальними затримками при зміні топології та уникнення петель, було обрано протокол Rapid spanning tree protocol (RSTP) це мережевий протокол, що використовується для запобігання циклів у мережах Ethernet, забезпечуючи резервний канал при блоку інших. Цей протокол э кращою версією протоколу, STP, так як RSTP він краще реакція на будь-які зміни топології, та сприяє швидшому відновленню мережі [14].

RSTP визначає кореневий міст у мережі, після чого всі комутатори розраховують найкоротший шлях до нього, вибираючи кореневий порт. Якщо якийсь порт веде до некореневого комутатора і використовується для передавання трафіку, він позначається як призначений порт. Інші порти, які можуть забезпечити резервний шлях у разі збою, отримують статус альтернативного або резервного порту. Завдяки цьому механізму RSTP може швидко реагувати на зміну в топології без необхідності чекати тривалих тайм-аутів, як це було в STP.

Однією з ключових особливостей RSTP є впровадження механізму швидкого переходу портів у робочий стан. Наприклад, порти, підключені до кінцевих пристроїв, можуть миттєво переходити в стан Forwarding, що дозволяє

уникнути затримок при активації нових підключень. Крім того, протокол підтримує зворотну сумісність із STP, що дозволяє поступово модернізувати існуючі мережі без ризику несумісності.

Крім швидкої конвергенції, RSTP має ще кілька важливих особливостей, які роблять його ефективним у сучасних мережах. Наприклад, він підтримує так звані «точки з'єднання» (Edge Ports), які використовуються для підключення кінцевих пристроїв, таких як комп'ютери чи сервери [19]. Ці порти одразу переходять у стан Forwarding, оминаючи проміжні стани Listening і Learning, що було обов'язковим у STP. Це дозволяє уникнути затримок при запуску або пере підключення пристроїв.

Ще однією перевагою RSTP є його гнучкість у визначенні альтернативних маршрутів. Якщо активний маршрут виходить з ладу, альтернативний порт може миттєво стати призначеним, що мінімізує час простою мережі. Крім того, механізм пропагування змін (Topology Change Notification) працює набагато швидше, оскільки зміни не потребують глобального оновлення всієї мережі, а лише стосуються безпосередньо пов'язаних вузлів. Інтеграція RSTP з VLAN є досить хорошою та добре інтегрується з іншими мережевими технологіями, це надає можливість збудувати масштабовані корпоративні мережі які будуть досить надійними. ефективно працює в поєднанні з MSTP (Multiple Spanning Tree Protocol), що дозволяє розподіляти навантаження між кількома VLAN, запобігаючи перевантаженню основного кореневого мосту.

Розглянувши завдання побудови стійкої комутованої мережі з мінімальним часом відновлення та запобіганням петель, отримали ефективне рішення у вигляді впровадження протоколу RSTP, що задовольняє вимоги продуктивності, надійності та масштабованості.

2.1.5 NTP протокол

Розглянемо мережевий протокол синхронізації часу NTP (Network Time Protocol) він потрібен для того щоб синхронізувати час комп'ютерів в мережі.

Традиційно NTP використовує для своєї роботи протокол UDP, NTP здатний працювати й поверх TCP [20]. NTP дуже стійкий до змін середовища

передачі. Основне завдання це підтримка точного часу на всіх пристроях у мережі, що є критично важливим для коректної роботи систем, журналу подій, безпеки, фінансових транзакцій та інших завдань, які потребують високої точності.

Протокол використовує складні алгоритми корекції, зокрема алгоритм Марзулло, який дозволяє обирати найточніше значення часу серед кількох джерел, враховуючи затримки передачі та можливі похибки. Також NTP компенсує коливання тактових генераторів на пристроях, використовуючи статистичні методи для обчислення відхилень.

У сучасних мережах NTP здатний досягати точності до 10 мілісекунд в Інтернеті та 200 мікросекунд у локальних мережах [20]. У версії NTPv4, яка є найновішою, покращено безпеку (наприклад, підтримка криптографічного захисту) та підвищено ефективність алгоритмів корекції.

Чому обрано NTP у роботі:

– висока точність і стабільність NTP забезпечує точну синхронізацію годинників у системі, що важливо для коректної роботи логів, баз даних та інших сервісів;

– стійкість до збоїв NTP використовує кілька джерел часу та алгоритми корекції, що дозволяє уникнути впливу одного несправного або неточного сервера;

– широка підтримка протокол підтримується всіма основними операційними системами та мережею Інтернет, що робить його стандартом для синхронізації часу;

– безпека нові версії підтримують аутентифікацію, що дозволяє уникнути підробки часу зловмисниками;

– гнучкість можливість використання як у глобальних мережах, так і в локальних середовищах.

Розглянувши завдання, можна зробити висновок, що протокол NTP є оптимальним рішенням для точної та надійної синхронізації часу в мережах

різного масштабу, забезпечуючи стабільність, безпеку та сумісність із сучасними системами.

2.1.6 DHCP протокол

Розглянемо DHCP (Dynamic Host Configuration Protocol) цей протокол потрібен для того, щоб автоматично видавати IP-адреси та працює на прикладному рівні моделі TCP/IP і також видає і інші мережеві налаштування пристроям у мережі. Завдяки цьому, адміністратору не потрібно вручну прописувати адресу для кожного пристрою, що особливо зручно, коли клієнтів багато. Процес видачі IP-адреси від DHCP-сервера проходить у кілька етапів (рис. 2.1), їх називають DORA, спочатку клієнт, який ще не має IP, розсилає запит (DHCP Discover). Сервер отримує запит і у відповідь надсилає пропозицію адреси (DHCP Offer). Потім клієнт погоджується (DHCP Request), і сервер підтверджує видачу (DHCP Acknowledgement)[21].

Коли сервер виділяє IP, він бере його з певного діапазону адрес, який задає адміністратор. Якщо потрібно, можна обмежити ці адреси, щоб деякі з них не призначалися клієнтам. Вся ця інформація зберігається на сервері так він знає, яка адреса вже видана і кому. IP видається не назавжди, а на певний час, який називають орендою (lease). Стандартно вона триває 24 години, але в налаштуваннях можна змінити цей період.

Рисунок 2.1 – Принцип роботи DHCP

Такий підхід дозволяє краще керувати IP-адресами, особливо коли клієнти можуть відключатись, переїжджати у мережі чи змінювати обладнання. Якщо

клієнт ще активний, але вже пройшла половина оренди (час T1), він пробує оновити свою адресу. Якщо сервер доступний, то він її підтверджує, і відлік оренди починається знову.

Якщо ж сервер не відповідає, клієнт пробує ще раз після певного часу, і так далі до моменту T2.

Якщо і тоді немає відповіді, запит надсилається вже до всіх серверів у мережі, щоб уникнути втрати зв’язку.

Є кілька способів, як сервер може призначати IP:

– статичну адресу прив’язують до MAC-адреси пристрою. Це зручно, коли потрібно, щоб пристрій завжди мав одну і ту саму IP-адресу;

– автоматичний сервер один раз видає IP клієнту і більше її не змінює;

– динамічний сервер видає IP на певний час, а потім повертає її в пул, якщо пристрій більше не підключений. Цей варіант найкраще підходить для ситуацій, коли кількість пристроїв може змінюватися.

У цьому проєкті DHCP налаштовано на сервері, і він автоматично видає IP-адреси всім пристроям у мережі. Для кожної VLAN створено окремий пул адрес, і задано, скільком користувачам можна видати адресу одночасно. Це дозволяє уникнути конфліктів і забезпечити стабільну роботу мережі навіть при великій кількості підключених пристроїв.

Розглянувши завдання, можна зробити висновок, що використання DHCP забезпечує зручне, ефективне та гнучке управління IP-адресами в мережі, що особливо важливо для великої інфраструктури з динамічною кількістю клієнтів.

2.1.7 IPSec протокол

Розгляньмо IPsec (Internet Protocol Security) цей протокол представляє з себе набір протоколів щоб забезпечити захист даних, що дозволяє здійснювати підтвердження справжності шифрування IP-пакетів які передаються за допомогою IP. Протоколи IPsec працюють на мережевому рівні (3 рівень OSI), що дозволяє їм захищати будь-які TCP чи UDP-протоколи. IPsec може використовуватись між двома вузлами, між шлюзами або між вузлом і шлюзом безпеки. IPsec забезпечує цілісність і конфіденційність даних.

До основних компонентів IPsec належать:

– заголовок автентифікації (Authentication Header) забезпечує аутентифікацію джерела та цілісність даних;

– інкапсуляція корисної навантаження безпеки (Encapsulating Security Payload) забезпечує шифрування, цілісність і аутентифікацію;

– асоціація безпеки (Security Association) набір параметрів, що визначають спосіб застосування AH або ESP. У транспортному режимі ESP інкапсулює лише дані в межах IP-пакета, у режимі тунелювання весь IP-пакет. Залежно від SA, IPsec-модуль визначає алгоритм шифрування (Triple-DES, AES, Blowfish) і секретний ключ [22]. Дані шифруються, доповнюються до потрібного розміру, і для них обчислюється контрольна сума. При отриманні ESP-пакета, приймальний модуль знаходить відповідне SA. Перевіряється номер послідовності (Sequence Number) і ICV, якщо все правильно дані розшифровуються, якщо ні пакет відкидається. Основне застосування IPsec створення VPN тунелі, де AH та ESP де вони працюють у режимі тунелювання [22]. Також IPsec можна використовувати для реалізації між мережевого екрану, фільтруючи пакети за заданими політиками безпеки. Що дає можливість, блокування усього трафіку, відокремлюючи певні порти 443 або 8 TCP.

Розглянувши завдання вибору технологій та протоколів, було визначено оптимальне поєднання сучасних рішень, що дозволяє створити стабільну, масштабовану й захищену корпоративну мережу, що відповідає усім поставленим технічним вимогам.

2.2 Вибір обладнання

Спираючись на тему проєктування, під час вибору мережевого обладнання важливо враховувати низку факторів, які можуть вплинути на ефективність та стабільність роботи всієї мережі. Зокрема, мова йде про площу будівлі, кількість

кабінетів, кількість користувачів та їхні потреби, а також про фінансові можливості підприємства. Усі ці параметри мають прямий вплив на пропускну здатність мережі та швидкість передачі даних.

Окрім цього, обладнання має підтримувати функції, які можуть знадобитися в майбутньому, зокрема розширення мережі або впровадження нових сервісів. З урахуванням проаналізованих параметрів таких як швидкість каналів, розташування обладнання, а також обрані мережеві технології та протоколи буде підібрано таке обладнання, яке найкраще відповідає поставленим вимогам, забезпечує безперебійну роботу мережі та дозволяє її масштабувати при необхідності. На (рис. А.2) наведена структурна схема мережі

До основних компонентів обладнання, які будуть потрібні у мережі багатоквартирного будинку можна віднести маршрутизатор Cisco 2901 стане гарним варіантом для побудови мережі адже Cisco 2900 серії обладнанні вбудованими сервісами другого покоління сімейства ISR G2 (Integrated Services Router Generation 2) [23]. Маршрутизатори Cisco ISR серії 2900 призначені для потреб малих і середніх організацій, яким необхідні сучасні мережеві рішення з високим рівнем надійності та продуктивності. Їх технічні можливості детально відображено на (рис. 2.2) та на (рис. 2.3.)

Manufacturer:	Cisco
Product ID:	CISCO2901/K9
Product Description:	Cisco 2901 with 2 onboard GE, 4 EHWIC slots, 2 DSP slots, 1 ISM slot, 256MB CF default ,512MB DRAM default, IP Base
Product Type:	Router
Interfaces/Ports	
Total Number of Ports:	2
USB:	Yes
Management Port:	Yes
Number of Broadband (RJ-45) Ports:	2
I/O Expansions	
Number of Total Expansion Slots:	9
Expansion Slot Type:	HWIC
	PVDM
Network & Communication	
Network Technology:	10/100/1000Base-T
Ethernet Technology:	Gigabit Ethernet
Management & Protocols	
Security Features:	• Cisco Security Manager • Cisco IOS Firewall • Cisco IOS Zone-Based Firewall • Cisco IOS IPS • Cisco IOS Content Filtering • Flexible Packet Matching (FPM) • AAA

Рисунок 2.2 – Технічні характеристики частина перша

До серії маршрутизаторів Cisco 2900 входять чотири базові моделі, кожна з яких має визначені технічні характеристики та підтримує можливість розширення функціональності за рахунок додаткових ліцензій і модулів.

Memory	
Standard Memory:	512 MB
Maximum Memory:	2.50 GB
Memory Technology:	SDRAM
Flash Memory:	256 MB
Memory Card Supported:	CompactFlash (CF) Card
Power Description	
Input Voltage:	110 V AC
	220 V AC
Power Source:	Power Supply
Redundant Power Supply:	Yes
Physical Characteristics	
Compatible Rack Unit:	1U
Form Factor:	Rack-mountable
Height:	1.8"
Width:	17.3"
Depth:	17.3"
Weight (Approximate):	13.45 lb
Miscellaneous	
Additional Information:	• IP Base • Cisco Unified SRST Sessions: 35 • Cisco Unified CCME Sessions: 35 **Expansion Slots:** • 1 x Internal Services Module (ISM)

Рисунок 2.3 – Технічні характеристики частина друга

Маршрутизатор Cisco 2901 має при собі два порти які підтримують гігабітну швидкість та може підключати оптичні модулі (SFP) також сумісний з попередніми модулями WIC, VWIC та має слоти розширення EHWIC, цей маршрутизатор оснащений 4 роз’єми HWIC. Також є підтримка модулів SM, що працюють із попередніми NM, NME, а внутрішній роз'єм під ISM замінює AIM.

Маршрутизатор легко розгортається, керується та підтримує мобільні сервіси, зокрема передачу даних, голосовий і відео зв’язок.

Маршрутизатори серії Cisco 2900 оснащуються цифровими сигнальними процесорами PVDM3, що зберігають зворотну сумісність із модулями попереднього покоління PVDM2. Крім того, у даних пристроях реалізована

технологія Services Ready Engine (SRE), яка забезпечує можливість гнучкого розгортання як програмних, так і апаратних сервісів. Пристрої мають вбудовану підтримку VPN-рішень, зокрема GETVPN, DMVPN та Enhanced Easy VPN, із апаратним прискоренням шифрування IPsec/SSL. Маршрутизатор Cisco 2901 завдяки своїй продуктивності та широкому функціоналу є доцільним вибором для використання в умовах середнього або малого бізнесу, що робить його вдалим рішенням у рамках цього проєкту.

Мережеві комутатори. Вибір комутаторів для проєкту буде базуватись на розрахованій кількості необхідних під'єднань для кожного поверху, що в свою чергу визначить потрібну кількість для всієї будівлі. Ключовими параметрами при виборі мережевого обладнання є кількість доступних портів, пропускна здатність, функції керування, а також засоби забезпечення безпеки даних.

Розміщуватися комутатори будуть в оптимальних для цього місцях, за для забезпечення стабільної мережі та потрібно технічно захистити обладнання від фізичного доступу в будинку.

Комутатор Cisco WS-C2960-24-S оснащений портами Fast Ethernet і Gigabit Ethernet, має розширені LAN сервіси для підприємств початкового рівня та мереж віддаленого офісу також підтримує передачу голосу, даних та відео, та безпечний доступ. Присутня підтримка Intelligent features (створення складних списків керування доступом, розширена безпека), комбіновані гігабітні лінки (мідний 10/100/1000BASE-T Ethernet або SFP-модуль для переходу в інше середовище Cisco 1000BASE-SX, 1000BASE-LX, 1000BASE-ZX, 100BASE-FX, 100BASE-LX, CWDM SFP) [24]. Крім того, комутатори підтримують технології QoS, обмеження швидкості (Rate Limiting) та списки контролю доступу (ACL) на основі MAC-адрес, IP-адрес і портів UDP/TCP. Є можливість гнучкого регулювання пропускної здатності на кожному порту з мінімальним кроком у 64 Кбіт/с. Присутня підтримка каналів для їх об'єднання (Link Aggregation) це забезпечує високошвидкісне з'єднання між комутаторами та серверами.

Реалізовано функціонал для налаштування транкових з'єднань із використанням тегів 802.1q, підтримка до 255 VLAN на один комутатор, до 4000

доступних VLAN ID, а також централізоване керування через Cisco Network Assistant. Вибір цього комутатора зумовлений тим що є великий спектр функцій, опцій та великою кількістю користувачів та присутній запас по портам на майбутнє збільшення користувачів також налаштування VLAN, QoS та безпеки портів. Після вибору необхідного обладнання потрібно його розмістити та з’єднати (рис. А.3). На плані приміщення схематично відображено розташування персональних комп’ютерів (PC), комутаторів (SW), сервера (SRV), маршрутизатора (R3), а також точку виходу до глобальної мережі (WAN).

З'єднання виконано із дотриманням оптимальних маршрутів між пристроями для прокладки кабельних ліній. Це забезпечує ефективну роботу локальної мережі.

Розглянувши завдання вибору мережевого обладнання, отримали оптимальну конфігурацію пристроїв маршрутизації та комутації, яка забезпечує баланс між функціональністю, надійністю та можливістю масштабування, повністю відповідає вимогам до побудови корпоративної мережі з високою продуктивністю та стабільністю роботи.

3 НАЛАШТУВАННЯ ДОДАТКОВИХ LAN МЕРЕЖ

3.1 Створення підмереж

Виходячи із мети роботи проєкту, щоб створити глобальну і локальну мережу необхідно використати адреси, 192.168.9.0/24 для локальної мережі та 201.1.98.0/27 глобальної мережі далі розбиваємо адреси IP-мережі за допомогою маски на дрібніші підмережі. Маска мережі визначає діапазон IP-адрес, які можуть використовуватися в межах однієї мережі. Її можна записати у десятковому або бінарному форматі. Для оптимізації мережевих ресурсів та ефективного управління мережею часто застосовується розподіл маски на підмережі. Мережа 192.168.9.0/24 має 256 адрес (0-255), де 192.168.9 це номер

мережі, а останній октет використовується для адресації хостів. Оскільки для кожної підмережі потрібно не менше 20 пристроїв, доцільно розділити цю мережу на 4 підмережі. Вихідна маска 11111111.11111111.11111111.00000000.

Далі потрібно змінити 2 додаткові біти для визначення підмережі, тобто маска зміниться на /26 11111111.11111111.11111111.11000000.

У десятковому форматі це буде 255.255.255.192, що дає по 64 адреси в кожній підмережі (включаючи адресу мережі та широкомовну адресу). Отримані підмережі:

– 192.168.9.0/26 (користувачі мають адресу від 192.168.9.1 до 192.168.9.62, широкомовна адреса 192.168.9.63);

– 192.168.9.64/26 (користувачі мають адресу від 192.168.9.65 до 192.168.9.126, широкомовна адреса 192.168.9.127);

– 192.168.9.128/26 (користувачі мають адресу від 192.168.9.129 до 192.168.9.190, широкомовна адреса 192.168.9.191);

– 192.168.9.192/26 (користувачі мають адресу від 192.168.9.193 до 192.168.9.254, широкомовна адреса 192.168.9.255).

Таким чином, поділ на підмережі забезпечує ефективне використання IP-адрес і дозволяє масштабувати мережу без втручання адміністратора (табл. 3.1).

Таблиця 3.1 – Розбиття LAN мережі

Мережа	Маска	Пул адрес	Можливі адреси	Максимальна кількість хостів
192.168.9.0	255.255.255.192	192.168.9.0 - 192.168.9.63	192.168.9.1 - 192.168.9.62	64
192.168.9.64	255.255.255.192	192.168.9.64 - 192.168.9.127	192.168.9.65 - 192.168.9.126	64
192.168.9.128	255.255.255.192	192.168.9.128 192.168.9.191	192.168.9.129 - 192.168.9.190	64
192.168.9.192	255.255.255.192	192.168.9.192 192.168.9.255	192.168.9.193 - 192.168.9.254	64

Далі розбиваємо адресу для глобальної мережі 201.1.98.0/27 так само розбиваємо на 4 підмережі змінюємо маску на \30 тим самим обмежуючи кількість хостів на 2 (табл. 3.2).

Таблиця 3.2 – Розбиття WAN мережі

Мережа	Маска	Пул адрес	Можливі адреси	Максимальна кількість хостів
201.1.98.0	255.255.255.252	201.1.98.0-201.1.98.3	201.1.98.1-201.1.98.2	2
201.1.98.4	255.255.255.252	201.1.98.4-201.1.98.7	201.1.98.5-201.1.98.6	2
201.1.98.8	255.255.255.252	201.1.98.8-201.1.98.11	201.1.98.9-201.1.98.10	2
201.1.98.12	255.255.255.252	201.1.98.12-201.1.98.15	201.1.98.13-201.1.98.14	2

В (табл. 3.3) наведено основні параметри конфігурації мережі, включаючи IP-адресацію філій, адреси між маршрутизаторами, типи адресації, а також використані технології рівня LAN та WAN.

Таблиця 3.3 – Конфігурація мережі

IP (адреси для філій)	IP (між маршрутизаторами (3-6 мереж))	Типи IP-адресації	LAN технології	WAN технології
192.168.9.0/24	201.1.98.0/27	Статична, Динамічна	VLAN, NTP,VTP,RSTP,DHCP	VPN (IPSec)

Розглянувши завдання, можна зробити висновок, що правильне планування IP-адресації та поділ мережі на підмережі забезпечує ефективне використання адресного простору, оптимізує мережеві ресурси та підвищує керованість і масштабованість як локальної, так і глобальної мережі.

3.2 Налаштування інтерфейсів

Виходячи із завдання, налаштування інтерфейсів на керуючих мережевих пристроях виконується через графічний інтерфейс, що значно спрощує процес конфігурації та взаємодію з обладнанням (рис. 3.1).

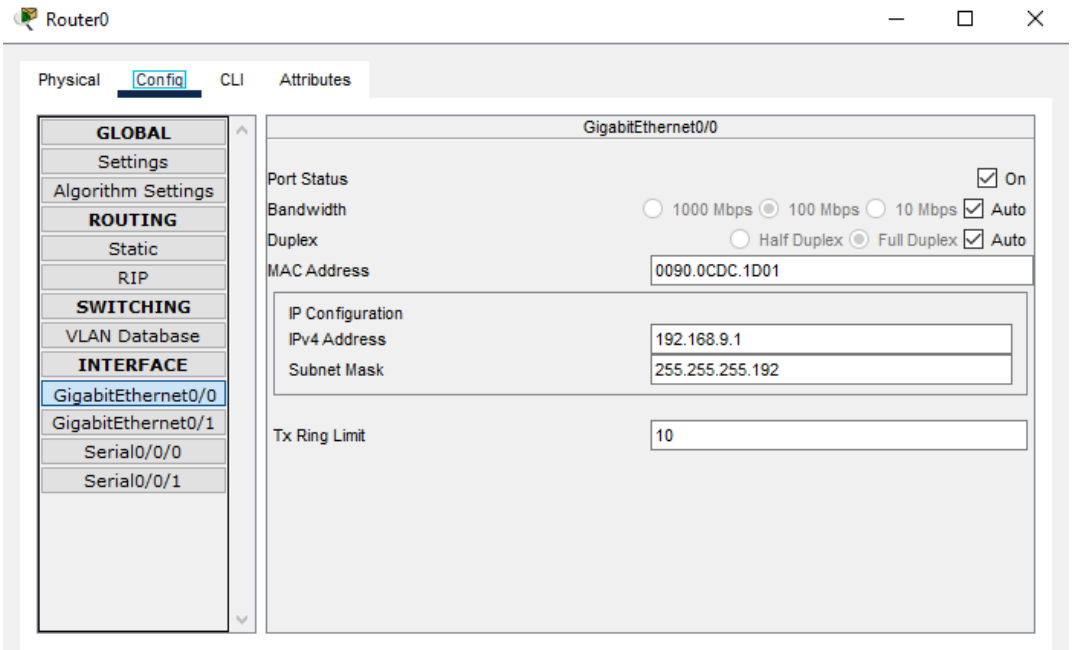


Рисунок 3.1 – Графічний інтерфейс router 0

Потрібно налаштувати інтерфейси на router 0 - router 3 щоб забезпечити роботу локальної та глобальної мережі потрібно скористатись інформацією IP-адрес з (табл. 3.4)

Таблиця 3.4 – IP адреси інтерфейсів маршрутизаторів

Пристрій	Інтерфейс	IP-адреса	Маска
Router0	Gig0/0	192.168.9.1	255.255.255.192
	Se0/0/0	201.1.98.1	255.255.255.252
	Se0/0/1	201.1.98.14	255.255.255.252
Router1	Gig0/0	192.168.9.65	255.255.255.192
	Se0/0/0	201.1.98.2	255.255.255.252
	Se0/0/1	201.1.98.5	255.255.255.252
Router2	Gig0/0	192.168.9.129	255.255.255.192
	Se0/0/0	201.1.98.9	255.255.255.252
	Se0/0/1	201.1.98.6	255.255.255.252
Router3	Gig0/0	192.168.12.193	255.255.255.192
	Se0/0/0	201.1.98.10	255.255.255.252
	Se0/0/1	201.1.98.13	255.255.255.252

Розглянувши завдання, отримали чітке розуміння структури мережі та необхідності налаштування інтерфейсів на кожному з маршрутизаторів.

Використовуючи графічний інтерфейс пристроїв, який значно спрощує конфігурування, забезпечується доступ як до локальних сегментів, так і до глобального з'єднання між маршрутизаторами.

3.3 Налаштування VTP та VLAN

Згідно з завданням спочатку потрібно створити VTP Server на Switch0 особливістю цього комутатора буде те що усі його порти будуть знаходиться в стані trunk та створюємо декілька VLAN один із них буде називатися VLAN70 який буде призначений для відокремлення однієї групи користувачів від інших та VLAN130 він потрібен буде для транкових портів комутаторів (рис. 3.2).

Послідовність дій наведена в лістингу 3.1.

Лістинг 3.1 – Налаштування VLAN на Router0

```
Router(config)#int gigabitEthernet 0/0.70
Router(config-subif)#encapsulation dot1Q 70
Router(config-subif)#ip ad
Router(config-subif)#ip address 192.168.18.1 255.255.255.0
```

А тепер після налаштування VLAN, переходимо до налаштування VTP Server на Switch0 лістинг 3.2

Лістинг 3.2 – Налаштування VTP Server

```
Switch(config)#vtp domain SW0
Changing VTP domain name from NULL to SW0
Switch(config)#vtp password 123
Setting device VLAN database password to 123
Switch(config)#do wr
```

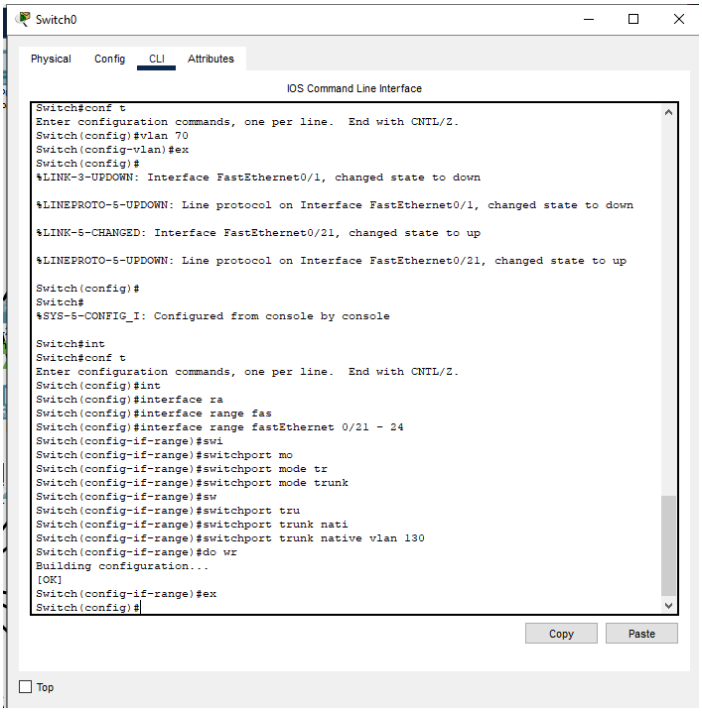


Рисунок 3.2 – Налаштування VLAN на Switch0

Далі потрібно налаштувати VTP Client (рис. 3.3) на інших комутаторах в підмережі і їх порти які з’єднанні з іншими комутаторами будуть знаходиться в стані trunk а на комутаторі Switch4 інші порти до яких під’єднані користувачі будуть знаходитися в VLAN70.

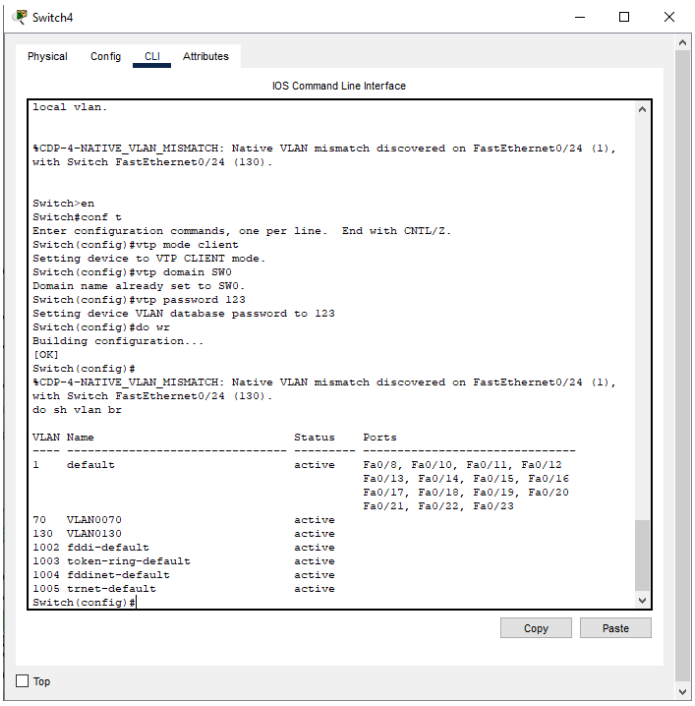


Рисунок 3.3 – Налаштування VTP Client на Switch4

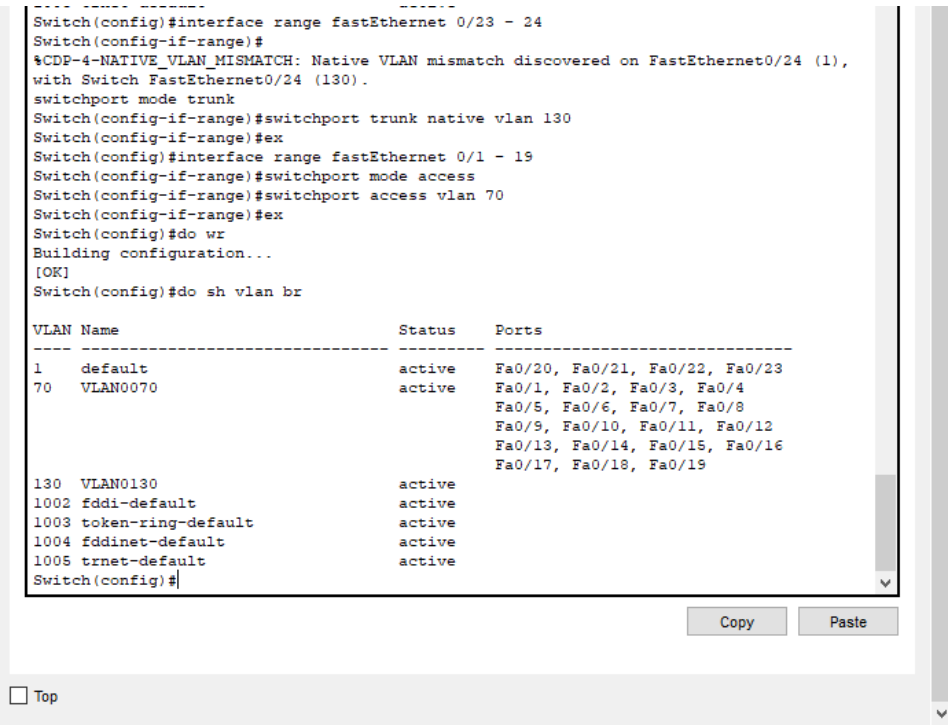


Рисунок 3.4 – Налаштування VLAN на Switch4

Такі самі операції проводимо на інших комутаторах за виключенням налаштування VLAN.

У результаті виконаних налаштувань було реалізовано централізоване управління VLAN за допомогою VTP, що дозволило спростити конфігурацію мережі, забезпечити її масштабованість і логічну сегментацію трафіку між користувачами.

3.4 Налаштування RSTP

Виходячи із мети роботи налаштування RSTP проходить наступним чином, перевіряємо налаштування протоколу на комутаторі (рис. 3.5) та показано таку строку Spanning tree enabled protocol ieee це означає що протокол RSTP ще не налаштований та потрібно його ввімкнути, для цього потрібно ввести в консоль комутатора наступні команду як показано на лістингу 3.3.

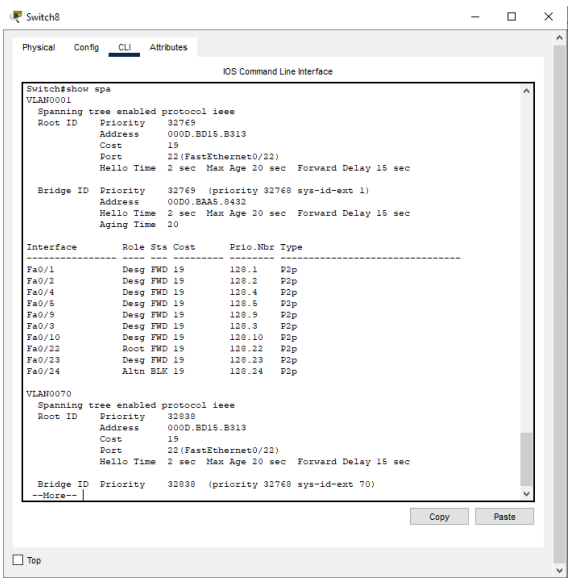


Рисунок 3.5 – Налаштування RSTP

Лістинг 3.3 – Налаштування RSTP

```
Switch# en
Switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#spanning-tree mode rapid-pvst
Switch(config)#ex
```

Далі перевіряємо налаштування за допомогою команди show spa (рис. 3.6) та як можна побачити в консолі Spanning tree enabled protocol rstp протокол налаштований і такі самі операції проводимо з іншими комутаторами.

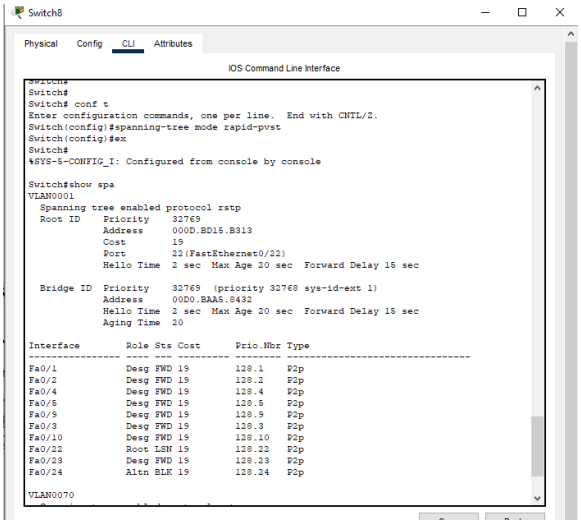


Рисунок 3.6 – Перевірка налаштування RSTP

Після введення необхідних команд, комутатор успішно перейшов на використання протоколу RSTP замість початкового стандарту IEEE Spanning Tree. Перевірка командою show spa показала, що тепер активним є саме протокол RSTP. Тепер якщо поглянути на робочу область (рис. 3.7).

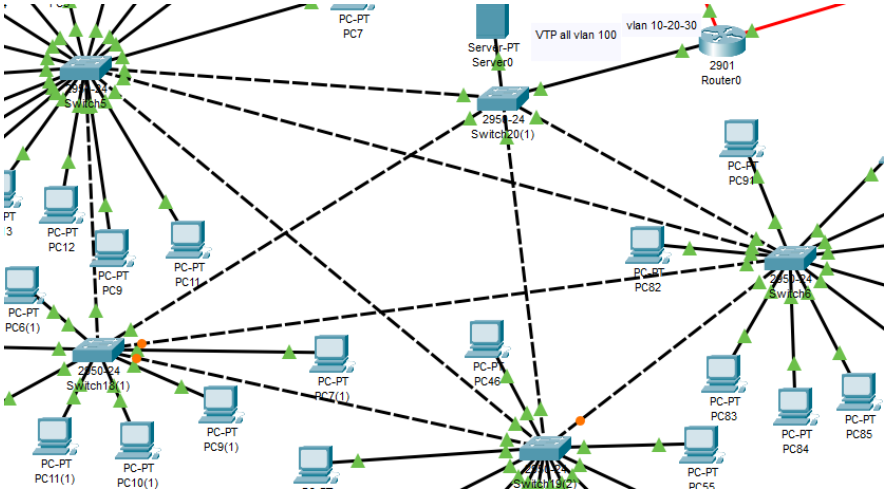


Рисунок 3.7 – Некоректна робота протоколу RSTP

Видно що на деяких комутаторах при роботі протоколу RSTP не резервуються деякі канали що свідчить про не коректну роботу протоколу, для початку потрібно знайти комутатор який став root, скориставшись командою show spanning-tree active, скорочена інформація наведена в лістингу 3.4.

Лістинг 3.4 – Перевірка кореневого комутатора для VLAN

```
SW0#show spanning-tree active
VLAN0001
Spanning tree enabled protocol rstp
Root ID Priority 32769
Address 0050.0F2B.B989
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

VLAN0010
Spanning tree enabled protocol rstp
Root ID Priority 32769
```

Продовження лістингу 3.4

```
Address 0050.0F2B.B989
Cost 57
Port 24(FastEthernet0/24)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

VLAN0020
Spanning tree enabled protocol rstp
Root ID Priority 32788
Address 0050.0F2B.B989
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

VLAN0030
Spanning tree enabled protocol rstp
Root ID Priority 32798
Address 0050.0F2B.B989
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

VLAN0100
Spanning tree enabled protocol rstp
Root ID Priority 32868
Address 0050.0F2B.B989
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

Рядок `This bridge is the root` говорить про те що цей комутатор є кореневим майже для кожного VLAN а саме якщо подивитися на `VLAN0010` і в нього описі є рядок `Port 24(FastEthernet0/24)` що свідчить про те що цей комутатор не є кореневим для цього VLAN.

Для того щоб зробити цей комутатор кореневим для усіх VLAN потрібно скористатися командою `spanning-tree vlan 1,10,20,30,100 priority 4096`.

Число 4096 це означає що цей комутатор є первинним коренем і має вищій пріоритет.

Далі необхідно ввести таку команду, `spanning-tree vlan 1,10,20,30,100 priority 8192` для інших комутаторів щоб зробити їх пріоритет нижчим за кореневий комутатор. Тепер для перевірки налаштування, на кореневому комутаторі скористуємося командою show spanning-tree summary яка виводить скорочену інформацію як показано на лістингу 3.5

Лістинг 3.5 – Перевірка налаштувань кореневого комутатора

```
SW0#show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: default VLAN10 VLAN20 VLAN30 VLAN100
Extended system ID is enabled
Portfast Default is disabled
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         6              6
VLAN0010 0            0          0         6              6
VLAN0020 0            0          0         6              6
VLAN0030 0            0          0         6              6
VLAN0100 0            0          0         6              6
---------------------- -------- --------- -------- ----------
5 vlans  0            0          0         30            30
```

Рядок `Root bridge for: default VLAN10 VLAN20 VLAN30 VLAN100` вказує на те що комутатор SW0 є кореневим для усіх VLAN у мережі та RSTP

працює штатно, тепер як можна побачити на (рис. 3.8) що комутатори заблокували резервні лінії для уникнення петель.

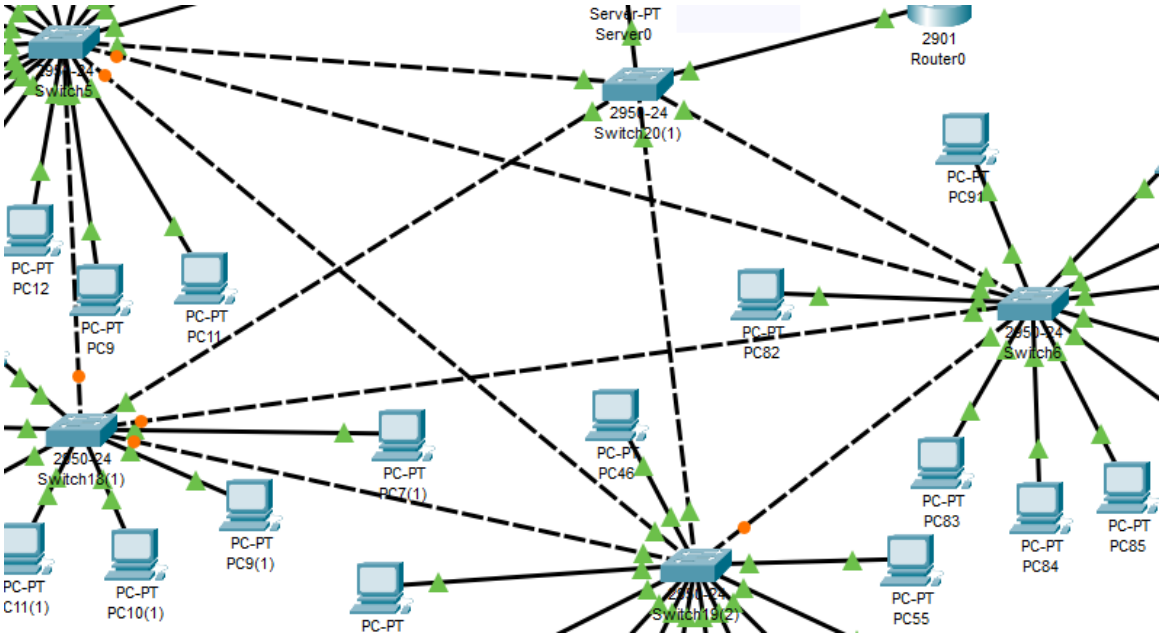


Рисунок 3.8 – Правильна робота протоколу RSTP

Налаштування RSTP на основних комутаторах завершено, при цьому забезпечено коректне визначення кореневого комутатора та блокування резервних ліній для запобігання петель.

Щоб протокол функціонував стабільно у всій мережі, аналогічні дії необхідно повторити на всіх інших комутаторах, в інших філіях. Це дозволить досягти узгодженої та безпечної роботи в мережі.

3.5 Налаштування NTP

Виходячи із завдання роботи потрібно виконати налаштування сервера для цього потрібно зайти в конфігурацію сервера перейти в вкладку Services і вибрати пункт NTP і його ввімкнути (рис. 3.9) на цьому налаштування сервера закінченні.

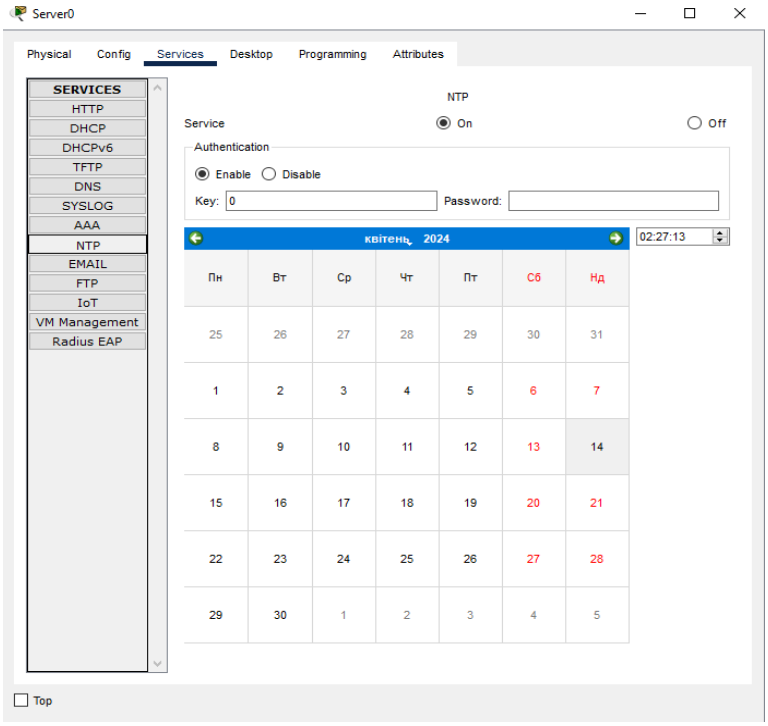


Рисунок 3.9 – Налаштування NTP сервера

Наступним кроком потрібно буде налаштувати пристрої Cisco таким чином, щоб вони зверталися до NTP-сервера для синхронізації свого годинника.

Це важливо для узгодження часу на всіх пристроях. Потрібно налаштувати маршрутизатори як NTP-клієнти для синхронізації їх годинника.

Маршрутизатори використовуватимуть сервер як NTP-сервер.

Щоб налаштувати маршрутизатори як NTP-клієнти потрібно спочатку перевірити поточні налаштування NTP та годинника (рис. 3.10)

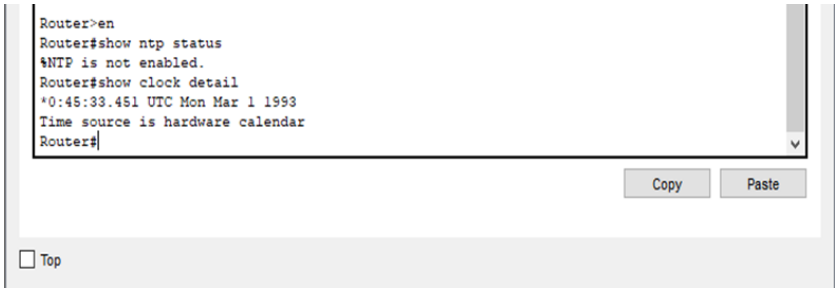


Рисунок 3.10 – Перевірка поточних налаштувань NTP та годинника

Потім потрібно виконати команду на всіх маршрутизаторах, NTP server

192.168.9.2 (Server0) (рис. 3.11).

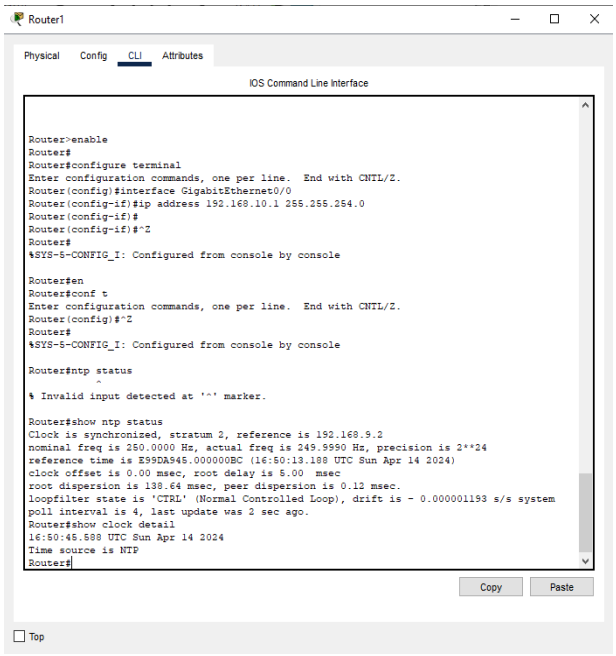


Рисунок 3.11 – Налаштування Router1 як NTP-клієнт

Отже, для синхронізації часу в мережі спочатку на сервері вмикається служба NTP. Потім на кожному маршрутизаторі вказується IP-адреса цього сервера за допомогою відповідної команди. Це дозволяє всім пристроям автоматично отримувати точний час з одного джерела.

3.6 Налаштування динамічної та статичної конфігурації

Виходячи із завдання потрібно налаштувати DHCP для цього заходимо в налаштування сервера переходимо в вкладку services і вибираємо пункт DHCP (рис. 3.12) натискаємо кнопку on щоб ввімкнути протокол потім вводимо в полі ім’я пулу наприклад serverPool10 що в даній роботі означає що це пул адрес для VLAN10 далі вводимо нижче шлюз за замовченням 192.168.11.1, далі пункт вводимо адресу 192.168.11.2 та маску підмережі 255.255.255.0 з якої сервер буде починати роздавати адреса кінцевим користувачам, та останнім кроком буде це

введення максимальної кількості користувачів яким будуть наданні адреси, в даному випадку ця кількість не перевищує 20 користувачів.

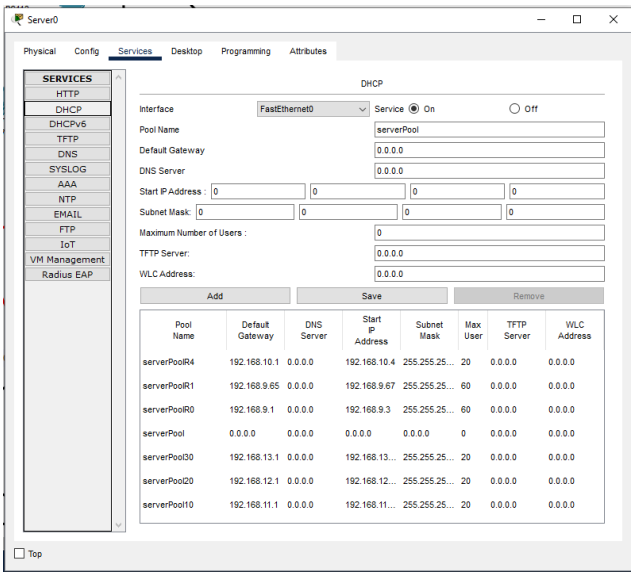


Рисунок 3.12 – Налаштування DHCP на сервері

Також потрібно зробити налаштування IP helper-адреса на маршрутизаторах, для того щоб DHCP-сервера правильно визначали які IP-адреси призначати для кожної підмережі (рис. 3.13).

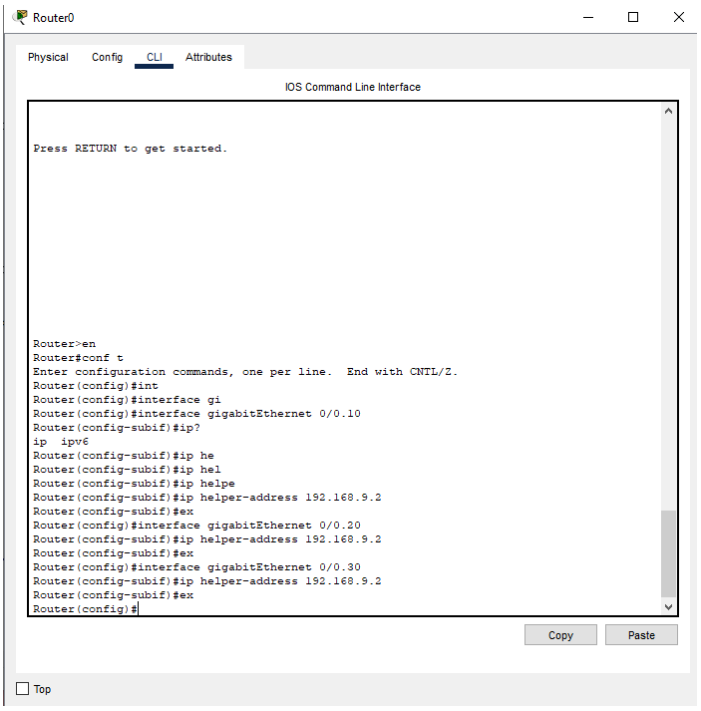


Рисунок 3.13 – Налаштування IP helper-адреса на маршрутизаторах

Для керуючих пристроїв потрібна статична маршрутизація для правильного та безперебійного функціонування мережі, адже до них постійно звертаються інші вузли. Вона дозволяє забезпечити стабільність і передбачуваність маршрутизації, зменшити затримки при передачі даних, а також мінімізувати навантаження на процесор маршрутизатора, оскільки відсутня необхідність у постійному перерахунку маршрутів.

Крім того, статична маршрутизація підвищує рівень безпеки, оскільки адміністратор самостійно визначає, які маршрути будуть доступні, що знижує ризик небажаних змін у мережевій топології (табл. 3.5).

Таблиця 3.5 – Статична конфігурація

Пристрій	Мережа	IP-адрес	Маска підмережі
Маршрутизатор Router 0	Філія 1	192.168.9.1	255.255.255.192
Маршрутизатор Router 1	Філія 2	192.168.9.65	255.255.255.192
Маршрутизатор Router 2	Філія 3	192.168.9.128	255.255.255.192
Маршрутизатор Router 3	Філія 4	192.168.9.193	255.255.255.192
Server1	Філія 1	192.168.9.2	255.255.255.0
Server2	Філія 4	192.168.9.194	255.255.255.0

Після налаштування динамічної та статичної конфігурації вказується пул адрес, шлюз за замовченням, початкова IP-адреса та маска підмережі, а також визначається максимальна кількість користувачів. Щоб DHCP-сервер міг коректно розподіляти адреси для різних підмереж, на маршрутизаторах налаштовується IP helper-адреса. Для керуючих пристроїв застосовується статична маршрутизація, що забезпечує стабільність, передбачуваність та безпеку передачі даних, а також знижує навантаження на маршрутизатори.

4 НАЛАШТУВАННЯ МАРШРУТИЗАЦІЇ ТА ДОДАТКОВИХ ТЕХНОЛОГІЙ WAN МЕРЕЖ

4.1 Налаштування статичної маршрутизації

Згідно з завданням, нижче наведено процес налаштування статичної маршрутизації для маршрутизатора.

За допомогою даних які наведені в (табл. 4.1.) була налаштована адресація приладів.

Ця таблиця містить інформацію про IP-адреси, інтерфейси та схеми підключення, що є основою для подальшого формування маршрутів.

Таблиця 4.1 – Параметри інтерфейсів пристроїв

Пристрій	Інтерфейс	IP-адреса	Підключення до пристрою	Підключення до інтерфейсу
Router0	Gig0/0	192.168.9.1	Switch2	Fa0/20
	Gig0/0.10	192.168.11.1	Switch2	Fa0/20
	Gig0/0.20	192.168.12.1	Switch2	Fa0/20
	Gig0/0.30	192.168.13.1	Switch2	Fa0/20
	Se0/0/0	201.1.98.1	Router1	Se0/0/0
	Se0/0/1	201.1.98.14	Router3	Se0/0/0
Router1	Gig0/0	192.168.9.65	Switch0	Fa0/1
	Gig0/0.70	192.168.18.1	Switch0	Fa0/1
	Se0/0/0	201.1.98.2	Router0	Se0/0/0
	Se0/0/1	201.1.98.5	Router2	Se0/0/1
Router2	Gig0/0	192.168.9.129	Switch12	Fa0/21
	Gig0/0.40	192.168.15.1	Switch12	Fa0/21
	Se0/0/0	201.1.98.9	Router3	Se0/0/0
	Se0/0/1	201.1.98.6	Router1	Se0/0/1
Router3	Gig0/0	192.168.9.193	Switch13	Fa0/21
	Gig0/0.50	192.168.16.1	Switch13	Fa0/21
	Gig0/0.60	192.168.17.1	Switch13	Fa0/21
	Se0/0/0	201.1.98.10	Router2	Se0/0/0
	Se0/0/1	201.1.98.13	Router4	Se0/0/1

Щоб далі налаштовувати маршрутизацію потрібно щоб кожен маршрутизатор визначив підмережі про яких є інформація відомих параметрів та не відомих.

Отримання інформації про мережі відбувається з інтерфейсів які вже налаштовані. А про невідомі мережі потрібно вже щоб адміністратор вручну прописати кожному маршрутизатору. Статична маршрутизація вимагає ручного заповнення таблиці маршрутизації на кожному маршрутизаторі де потрібно вказувати шлях до мережі які не є безпосередньо підключеними це потрібно для того щоб була правильна передача даних в ці напрямки (рис. 4.1).

Всі сформовані в лістингу Б.1 маршрути є напряму підключеними статичними маршрутами.

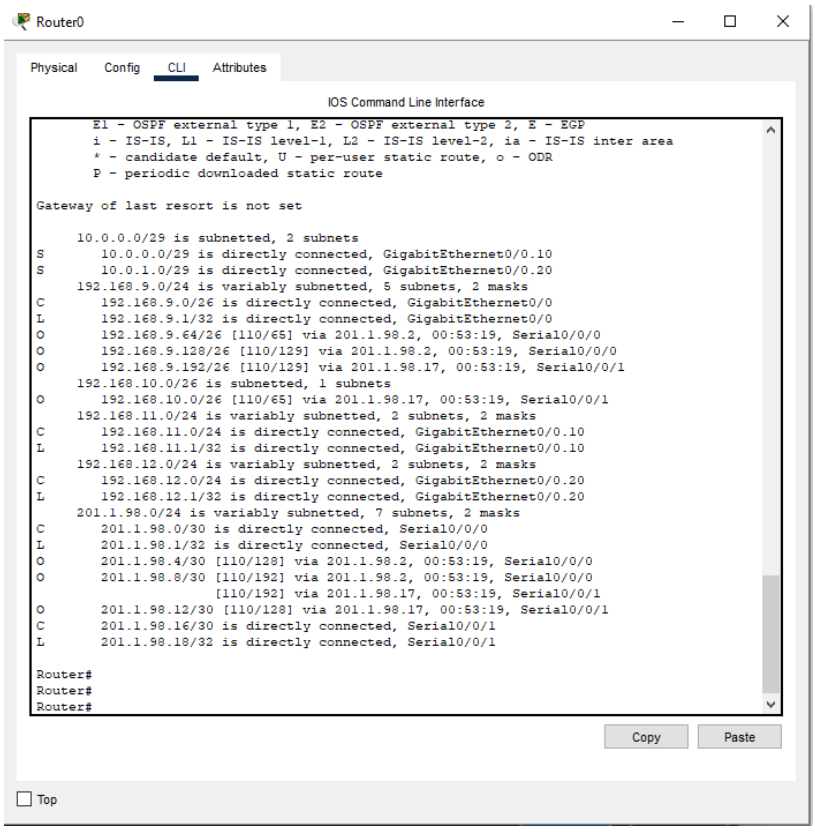


Рисунок 4.1 – Таблиця маршрутизації для Router0

Під час виконання завдання було налаштовано статичну маршрутизацію відповідно до заданих параметрів. Для кожного маршрутизатора визначено необхідні мережі та задано маршрути вручну. У результаті пристрої отримали

змогу обмінюватися даними між собою, що підтверджує правильність виконаної конфігурації.

4.2 Налаштування IPsec VPN

Згідно з завданням, налаштовуємо VPN IPsec між філіями підприємства, для початку налаштовуємо маршрутизатори на них VPN IPsec, та перевірити доступність пакету ліцензій Security Technology Package, тому що без нього, неможливо виконати деякі дії які забезпечують безпеку трафіку [15].

Тепер необхідно подивитися ліцензію, для цього потрібно написати команду Show version, та пролистати до низу, щоб переглянути ліцензії (рис. 4.2).

```
License UDI:

-------------------------------------------------
Device#   PID                   SN
-------------------------------------------------
*0        CISCO2901/K9          FTX1524F1OK-


Technology Package License Information for Module:'c2900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      disable       None          None
uc            disable       None          None
data          disable       None          None

Configuration register is 0x2102
```

Рисунок 4.2 – Перевірка ліцензії

Потрібно перевірити ліцензію Security Technology Package вона має бути доступною для подальшого налаштування. Після встановлення модуля c2900, пов’язаного з пакетом безпеки securityk9, наступним кроком потрібно активувати його за допомогою команди license boot module c2900 technology-package securityk9. Тепер необхідно зберегти конфігурацію яка зараз є поточною, використовуємо командою copy running-config startup-config. Потім необхідно виконати перезавантаження маршрутизатора, та потім перевіряємо що пакет

securityk9 активовано (Рис. 4.3).

```
249856K bytes of ATA System CompactFlash 0 (Read/Write)

License Info:

License UDI:

-------------------------------------------------
Device#   PID                   SN
-------------------------------------------------
*0        CISCO2901/K9          FTX15249H5V-


Technology Package License Information for Module:'c2900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      securityk9    Evaluation    securityk9
uc            disable       None          None
data          disable       None          None

Configuration register is 0x2102
```

Рисунок 4.3 – Securityk9

Налаштовуємо трафік між R1 та R2 як «особливий»: access-list 110 permit ip 192.168.9.0 0.0.0.63 192.168.9.128 0.0.0.63. Усі основні параметри, які пов'язані із налаштуваннями безпеки при передачі «особливого» трафіку наведено у (табл. 4.2).

Таблиця 4.2 – Параметри ISAKMP

Параметри		Router0	Router2	Router1	Router3
Спосіб розповсюдження ключа	Згідно інструкції чи ISAKMP	ISAKMP	ISAKMP	ISAKMP	ISAKMP
Алгоритм шифрування	DES, 3DES, or AES	AES	AES	AES	AES
Метод аутентифікації	Попередньо поширені ключі або RSA	Попередньо поширені ключі	Попередньо поширені ключі	Попередньо поширені ключі	Попередньо поширені ключі
Обмін ключами	Група DG 1, 2 або 5	DH 2	DH 2	DH 2	DH 2
Час життя IKE SA	88640 сек або менше	88640	88640	88640	88640
ISAKMP ключ		Cisco	Cisco	Cisco	Cisco

Налаштуємо політику криптографії ISAKMP 10 на маршрутизаторі Router1 с використанням ключа «cisco». Повернемося до таблиці ISAKMP (табл. 4.2) для вибору конкретних параметрів. Далі створюємо перетворювач VPN-SET для

можливості використання криптографічних алгоритмів шифрування esp-3des і esp-sha-hmac. Далі вже можна налаштувати мапу криптографії VPN-MAP, для пов'язування параметрів разом. Кінцевим налаштуванням мапи криптографії VPN-MAP є її прив'язка до вихідного інтерфейсу S0/0/0 на маршрутизаторі Router0 і всі ті самі дії робимо на Router2 (S0/0/1),

Лістинг 4.2 – VPN IPsec між Router 1 та Router2

```
Router#en
Router#conf t
Router(config)#access-list 100 permit ip 192.168.9.64 0.0.0.63
192.168.9.192 0.0.0.63
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#encryption aes 256
Router(config-isakmp)#group 5
Router(config)#crypto isakmp key Cisco address 201.1.98.10
Router(config)#crypto ipsec transform-set Router1-Router3 esp-aes
256 esp-sha-hmac
Router(config)#crypto map Router1Map 10 ipsec-isakmp
Router(config-crypto-map)#set peer 201.1.98.10
Router(config-crypto-map)#set pfs group5
Router(config-crypto-map)#set security-association lifetime seconds
80400
Router(config-crypto-map)#set transform-set Router1-Router3
Router(config-crypto-map)#match address 100
Router(config-crypto-map)#int serial 0/0/1
Router(config-if)#crypto map Router1Map

Router#en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 100 permit ip 192.168.9.192 0.0.0.63
192.168.9.64 0.0.0.63
Router(config)#do wr
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#encryption aes 256
Router(config-isakmp)#group 5
Router(config-isakmp)#ex
Router(config)#crypto isakmp key Cisco address 201.1.98.5
Router(config)#crypto ipsec transform-set Router3-Router1 esp-aes
256 esp-sha-hmac
Router(config)#crypto map Router3Map 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
Router(config-crypto-map)#set peer 201.1.98.5
Router(config-crypto-map)#set pfs group5
```

Продовження лістингу 4.2

```
Router(config-crypto-map)#set security-association lifetime
seconds 80400
Router(config-crypto-map)#set transform-set Router3-Router1
Router(config-crypto-map)#match address 100
Router(config-crypto-map)# int serial 0/0/0
Router(config-if)#crypto map Router3Map
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Далі перевіряємо налаштування за допомогою команди `show crypto ipsec sa` та бачимо на лістингу 4.3 налаштований VPN IPsec між двома філіями.

Лістинг 4.3 – Перевірка налаштування VPN IPsec

```
Router>en
Router#show crypto ipsec sa

interface: Serial0/0/0
Crypto map tag: VPN-MAP, local addr 201.1.98.1

protected vrf: (none)
local ident (addr/mask/prot/port):
(192.168.9.0/255.255.255.192/0/0)
remote ident (addr/mask/prot/port):
(192.168.9.128/255.255.255.192/0/0)
current_peer 201.1.98.6 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
```

У цьому завданні було реалізовано налаштування VPN IPsec між маршрутизаторами. Після перевірки та активації ліцензії securityk9 налаштовано політику ISAKMP, перетворювачі шифрування та карту криптографії. В результаті створено безпечний тунель для передачі трафіку між філіями, що забезпечує конфіденційність і цілісність даних.

5 ТЕСТУВАННЯ МЕРЕЖІ

5.1 Система моделювання

Згідно до мети проєктування, потрібно обрати необхідний інструмент моделювання в якому буде проводитися побудова та тестування проєктованої мережі для цього розглянемо такі інструменти як:

Cisco Packet Tracer це корисна програма за допомогою якої можна моделювати, налаштувати та тестувати мережі в віртуальному просторі з використовуючи різні пристрої такі як: ПК, маршрутизатори комутатори, сервери, хаби тощо. Пристрої розташовуються в віртуальному просторі що дозволяє працювати з будь-якими пристроями та будувати різного розміру мережі, при цьому не маючи фізичного доступу до обладнання.

Він добре підходить для навчання студентів щоб набути навичок та знать в роботі з мережевими протоколами, пристроями та з різними інструментами такими як: tracert, ssh, ping та іншими.

Плюси:

– інтуїтивно зрозумілий інтерфейс;

– має безкоштовний доступ для студентів та викладачів;

– створення віртуальних мереж з різними пристроями;

– моделювання в реальному часі;

– режим симуляції;

– тестування конфігурації мережі без фізичного обладнання;

– навчальні курси вже є в самому інструменті;

– дає змогу працювати на різних рівнях моделі OSI.

Мінусом є довге налаштування конфігурацій, особливо статичне налаштування.

GNS3 (Graphical Network Simulator 3) — це програмне забезпечення, яке дозволяє імітувати роботу мережі, об’єднуючи віртуальні пристрої з реальними для створення комплексних мережевих середовищ. Цей застосунок націлений на

побудову невеликих за розміром складних комп’ютерних мереж Cisco. Він написаний на Python з використанням бібліотеки Qt для використання графічного інтерфейсу також цей застосунок є корссплатформовим.

Плюси:

– повний функціонал емуляційних приладів що дозволяє створити модель комп’ютера, маршрутизатора чи іншого приладу та дає змогу працювати з оригінальними програмними засобами та емулює основні компоненти приладу як процесор, ОЗУ, і периферійні прилади;

– побудова гетерогенних мереж, наприклад схема де використовується Mikrotik, Cisco, Juniper тощо;

– можливість додавання реальних станцій, серверів, комп’ютерів і тд. також сам застосунок можна підключити вже існуючу комп’ютерну мережу;

– застосунок повністю безкоштовний.

Мінуси:

– неможливо емулювати комутатори із-за великої кількості ASIC мікросхем які використовуються в фізичних приладах;

– велика вимогливість програми до ресурсів комп’ютера;

– велика кількість багів.

NetSimm ця програма призначена для моделювання мереж для тестування протоколів та топології і їх аналізу, взаємодії з приладами які знаходяться в мережі такими як ПК, сервери, комутатори, маршрутизатори тощо. Присутня генерація різного виду трафіку та його відтворення також налаштування трафіку розмір пакетів та швидкість даних.

Присутні інструменти які дають змогу візуалізувати мережеві топології, та аналізувати данні результатів симуляції, тим самим визначати проблемні ділянки мережі.

Плюси:

– висока точність імітації мереж;

– присутня підтримка великої кількості мережевих протоколів.

– дозволяє створювати складні мережі з дуже великою кількістю вузлів;

– підтримує моделювання різних типів мереж, включаючи LAN, WAN, MAN, Wi-Fi, сенсорні мережі тощо;

– NetSim може інтегруватися з іншими програмами для аналізу даних, такими як MATLAB або Wireshark.

Мінуси:

– висока вартість;

– висока вимогливість до ресурсів комп'ютера;

– немає кроссплатформи;

– не підтримується NFV, SDN.

При виборі програмного засобу за допомогою якого буде побудована комп'ютерна мережа, були проаналізовані популярні програмні засоби, враховавши їх плюси та мінуси було обрано Cisco Packet Tracer, так як по перше наявність зрозумілого інтерфейсу а також є безкоштовний доступ для студентів, за допомогою цієї програми є можливість роботи з всіма рівнями моделі OSI. Це дає змогу проєктувати, моделювати та створювати віртуальні мережі підключати кінцеві та мережеві пристрої такі як ПК, сервери, принтери телефони, маршрутизатори, комутатори і тд. їх налаштування та взаємодію між собою.

Має обширний вибір пристроїв, що дає змогу для побудови реалістичних та великих мереж. Цей корисний інструмент надає користувачам можливість будувати мережу та імітувати її роботу та проводити аналіз даних що передаються приладами та аналізувати роботу різних протоколів DNS, HTTP, FTP тощо), і як взаємодіють різні компоненти мережі. Також є можливість створення складних мережевих сценаріїв, таких як налаштування віртуальних локальних мереж VLAN, маршрутизації між підмережами, Wi-Fi та роботи з IPv4/IPv6.

Розглянувши дане питання отримали Cisco Packet Tracer, чудово підходить для побудови мережі та навчання, маючи зрозумілий інтерфейс даючи можливість роботи з усіма рівнями моделі OSI. Та надає безкоштовний доступ для студентів.

5.2 Тестування LAN

Виходячи із мети роботи тестування мережі потрібно розбити на декілька пунктів щоб перевірити працездатність кожної із функція які були налаштовані в даній мережі. Мережа налаштована таким чином що не кожен пристрій має доступ до інших пристроїв в других підмережах але має доступ до всіх інших у своїй підмережі і до серверів мають доступ усі користувачі з усіх підмереж.

Працездатність мережі буде перевірятися на пристроях які мають доступ до всіх пристроїв і своєї та інших підмережах.

Для початку перевірятиметься доступ в середині філій, для цього потрібно скористатися утилітою ping, що надсилає ICMP запити на вказану адресу.

Всередині підмережі всі пристрої можуть взаємодіяти між собою.

Обравши пристрій який знаходиться в філії Router0 та має назву PC7(1) та якому присвоєний адрес 192.168.9.3 потрібно перейти до вкладки Desktop та обирати Command Prompt де прописуємо IP-адреси пристроїв PC11 який знаходиться в VLAN10 та має адрес 192.168.11.106, PC46 в VLAN20 192.168.12.100, та PC82 VLAN30 192.168.13.101. VLAN був встановлений, щоб створити внутрішню підмережу, яка застосовується для відокремлення деякої кількості комп'ютерів, та такі VLAN мають обмежений доступ тобто не до всіх філій він є. Наприклад PC11 який знаходиться в VLAN10 (Router0) не має доступу до другої філії Router 1.

Лістинг 5.1 – Результати виконання команди на PC7(1)

```
C:\>ping 192.168.11.106

Pinging 192.168.11.106 with 32 bytes of data:

Reply from 192.168.11.106: bytes=32 time=10ms TTL=127
Reply from 192.168.11.106: bytes=32 time=10ms TTL=127
Reply from 192.168.11.106: bytes=32 time=1ms TTL=127
Reply from 192.168.11.106: bytes=32 time<1ms TTL=127
Reply from 192.168.11.106: bytes=32 time<1ms TTL=127
```

Продовження лістингу 5.1

```
Ping statistics for 192.168.11.106:
Packets: Sent = 4, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 10ms, Average = 4ms

C:\>ping 192.168.12.100

Pinging 192.168.12.100 with 32 bytes of data:

Request timed out.
Reply from 192.168.12.100: bytes=32 time=2ms TTL=127
Reply from 192.168.12.100: bytes=32 time=10ms TTL=127
Reply from 192.168.12.100: bytes=32 time<1ms TTL=127
Reply from 192.168.12.100: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.12.100:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 10ms, Average = 3ms

C:\>ping 192.168.13.100

Pinging 192.168.13.100 with 32 bytes of data:

Request timed out.
Reply from 192.168.13.100: bytes=32 time<1ms TTL=127
Reply from 192.168.13.100: bytes=32 time<1ms TTL=127
Reply from 192.168.13.100: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.13.100:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

В інших філіях тестування зв’язку в локальних мережах було проведено аналогічним способом. Перевірка показала, що всередині кожної підмережі всі пристрої мають доступ один до одного відповідно до налаштувань VLAN і правил маршрутизації. Тепер перевіримо налаштування NTP сервера спочатку перевіряймо налаштування на Server0 відкриваємо Services та вибираємо пункт NTP (рис. 5.1)

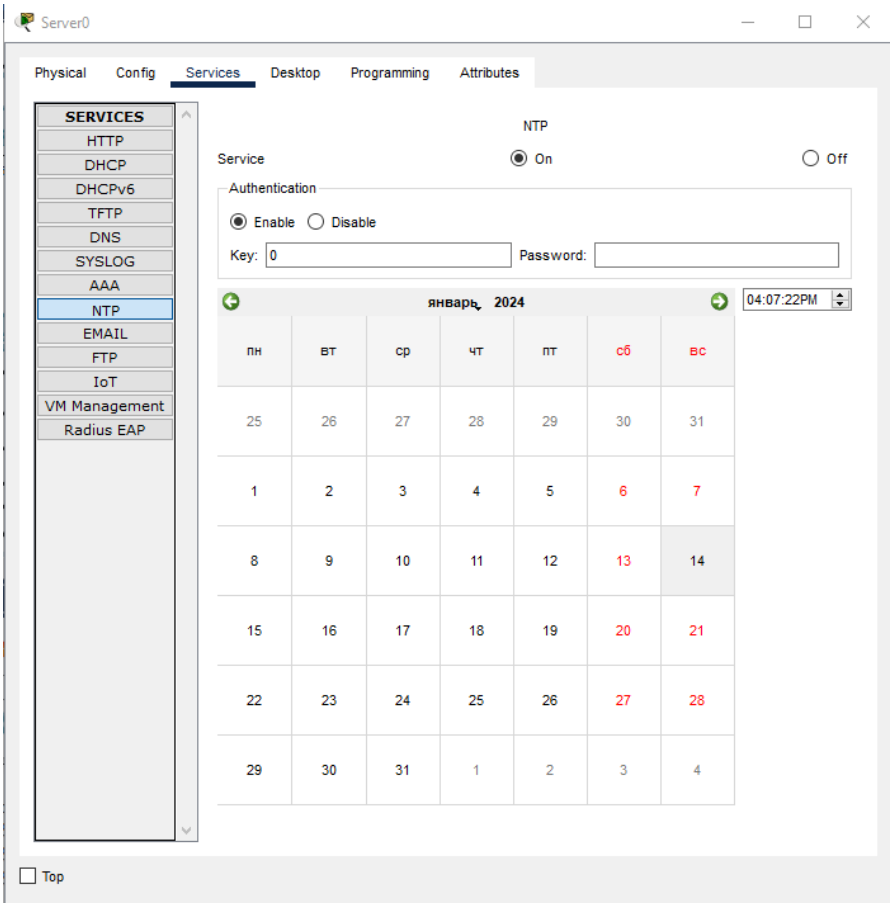


Рисунок 5.1 - NTP сервер

Тепер перевіряємо роботу NTP клієнтів це Router0, Router1, Router2, Router3. Щоб перевірити, потрібно зайти в маршрутизатор та перейти до вкладки CLI та прописати наступну команду `sh ntp status` вона виводить результат на лістингу Б.2

Як видно з лістингу 5.2 що Router0, Router1, Router2, Router3 є NTP клієнтами Server0 (192.168.9.2) та має актуальний час та дату. Наступним кроком буде перевірка працездатності протоколу RSTP. Для перевірки функціональності протоколу RSTP, який використовується для уникнення петель у комутованих мережах і забезпечує швидке перемикання у разі втрати зв'язку, було проведено тестування на прикладі однієї з філій. Тестування виконувалося у філії Router3 (рис. 5.2).

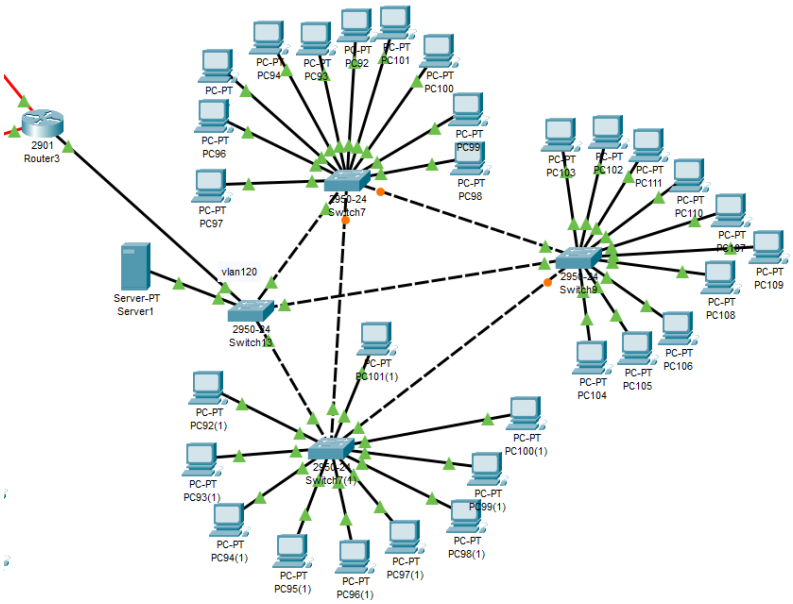


Рисунок 5.2 – Філія Router3

На схемі видно, що деякі з’єднання позначені помаранчевими індикаторами, це резервні канали, які неактивні, щоб уникнути утворення петель. Завдяки цьому формується топологія дерева.

У процесі тестування була змодельована ситуація, коли основний канал між Switch13 та Switch7 виходить з ладу. У такому випадку резервний шлях між Switch7 та Switch7(1) автоматично активується, забезпечуючи відновлення з’єднання без помітних затримок (рис. 5.3).

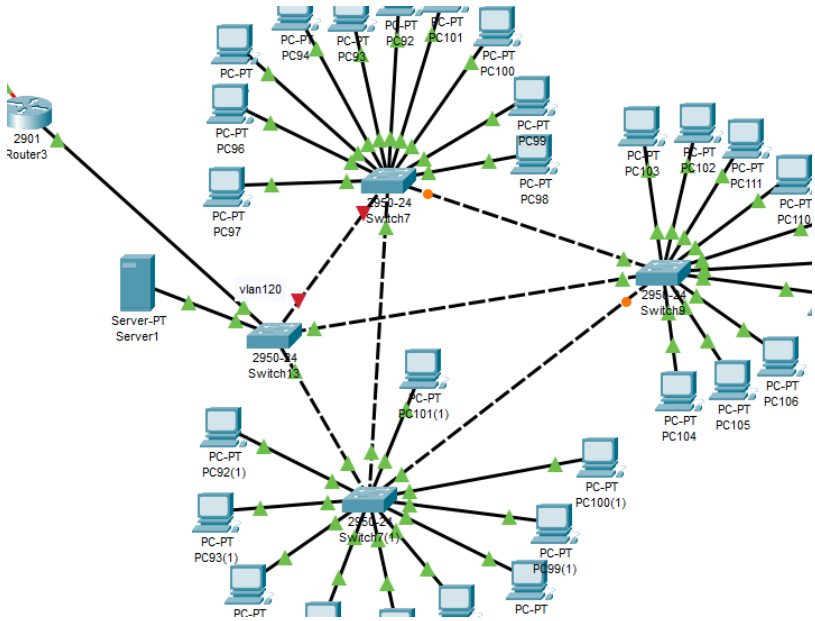


Рисунок 5.3 – Відновлення з’єднання

Також змодельована ситуація, коли декілька каналів вийшли з ладу. Як видно на (рис. 5.4), протокол RSTP автоматично перебудував топологію мережі, забезпечивши її безперервну роботу. Канал зв'язку між Switch7 та Switch7(1) став резервним, оскільки в умовах зміненої топології цей маршрут вже не є найоптимальнішим для передавання даних. Завдяки цьому вдалося уникнути утворення петель та забезпечити ефективний розподіл трафіку навіть при пошкодженні окремих ділянок мережі.

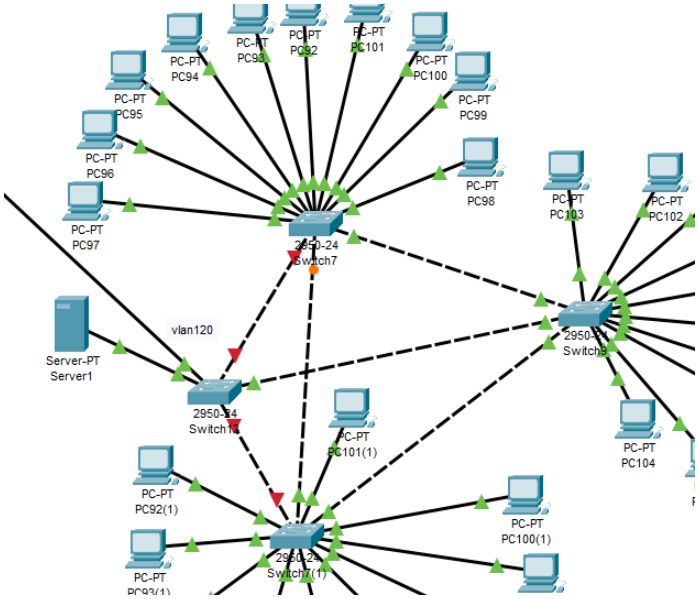


Рисунок 5.4 – Перебудована топологія мережі

Подібну поведінку мережі було зафіксовано і в інших філіях, що свідчить про правильну роботу RSTP та його здатність підтримувати стабільність мережевих з’єднань у разі несправностей.

Мережу протестовано поетапно, спершу всередині підмереж, потім між ними. Використання утиліти ping підтвердило доступність пристроїв згідно з політикою маршрутизації. NTP-клієнти успішно синхронізували час із сервером.

Перевірено роботу RSTP на прикладі філії Router3, при втраті основного каналу резервне з’єднання активується миттєво, що забезпечує відмовостійкість мережі. Загалом мережа працює стабільно та відповідає вимогам.

5.3 Тестування WAN

Тепер потрібно буде перевірити зв’язок між філіями, для цього будемо перевіряти зв’язок на пристроях які мають доступ до всіх пристроїв і своєї та інших підмережах.

Перевіримо зв’язок між філіями Router0 – Router1, Router0 – Router3, Router1 – Router2. Візьмемо PC7(1) (192.168.9.4) та використаємо утиліту ping, що надсилає ICMP запити в філію Router1 до PC0(1) (192.168.9.67). Результат показано на лістингу 5.2

Лістинг 5.2 – Перевірка з’єднання між філіями Router0 – Router1

```
C:\>ping 192.168.9.67

Pinging 192.168.9.67 with 32 bytes of data:

Reply from 192.168.9.67: bytes=32 time=2ms TTL=126
Reply from 192.168.9.67: bytes=32 time=1ms TTL=126
Reply from 192.168.9.67: bytes=32 time=8ms TTL=126
Reply from 192.168.9.67: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.9.67:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 8ms, Average = 3ms
```

Далі перевіримо з’єднання між філіями Router0 – Router2 PC7(1) (192.168.9.4) до PC104 (192.168.9.196) лістинг 5.3

Лістинг 5.3 – Перевірка з’єднання між філіями Router0 – Router3

```
C:\>ping 192.168.9.196

Pinging 192.168.9.196 with 32 bytes of data:

Reply from 192.168.9.196: bytes=32 time=2ms TTL=126
Reply from 192.168.9.196: bytes=32 time=1ms TTL=126
Reply from 192.168.9.196: bytes=32 time=8ms TTL=126
Reply from 192.168.9.196: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.9.196:
```

Продовження лістингу 5.3

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 8ms, Average = 3ms
```

На лістингу 5.4 показаний результат з’єднання між філіями Router1 – Router2 PC0(1) (192.168.9.67) до PC70 (192.168.9.130).

Лістинг 5.4 – Перевірка з’єднання між філіями Router1 – Router2

```
C:\>ping 192.168.9.130

Pinging 192.168.9.130 with 32 bytes of data:

Reply from 192.168.9.130: bytes=32 time=1ms TTL=126
Reply from 192.168.9.130: bytes=32 time=15ms TTL=126
Reply from 192.168.9.130: bytes=32 time=10ms TTL=126
Reply from 192.168.9.130: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.9.130:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 15ms, Average = 7ms
```

Та перевіряємо з’єднання між філіями Router3 – Router2, PC104 (192.168.9.196) до PC70 (192.168.9.130). Результат показано на лістингу 5.5

Лістинг 5.5 – Перевірка з’єднання між філіями Router3 – Router2

```
C:\>ping 192.168.9.130

Pinging 192.168.9.130 with 32 bytes of data:

Reply from 192.168.9.130: bytes=32 time=3ms TTL=126
Reply from 192.168.9.130: bytes=32 time=8ms TTL=126
Reply from 192.168.9.130: bytes=32 time=1ms TTL=126
Reply from 192.168.9.130: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.9.130:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 8ms, Average = 3ms
```

Наступним кроком іде перевірка з’єднання між філіями Router0 – Router2

та Router1 – Router3 так як між ними встановлений VPN IPsec для передачі зашифрованих даних нижче наведено данні о зашифрованих пакетах між Router0 – Router2 (рис. 5.5) та Router1 – Router3 (рис. 5.5).

На лістингу 5.6 командою Ping перевіряємо з'єднання між PC7 (192.168.9.5) який знаходиться у філії Router0 та PC70 (192.168.130) який знаходиться у філії Router2.

Лістинг 5.6 – перевірка з'єднання між філіями Router0 – Router2

```
C:\>ping 192.168.9.130

Pinging 192.168.9.130 with 32 bytes of data:

Reply from 192.168.9.130: bytes=32 time=4ms TTL=126
Reply from 192.168.9.130: bytes=32 time=5ms TTL=126
Reply from 192.168.9.130: bytes=32 time=4ms TTL=125
Reply from 192.168.9.130: bytes=32 time=4ms TTL=126

Ping statistics for 192.168.9.130:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 4ms, Maximum = 5ms, Average = 4ms
```

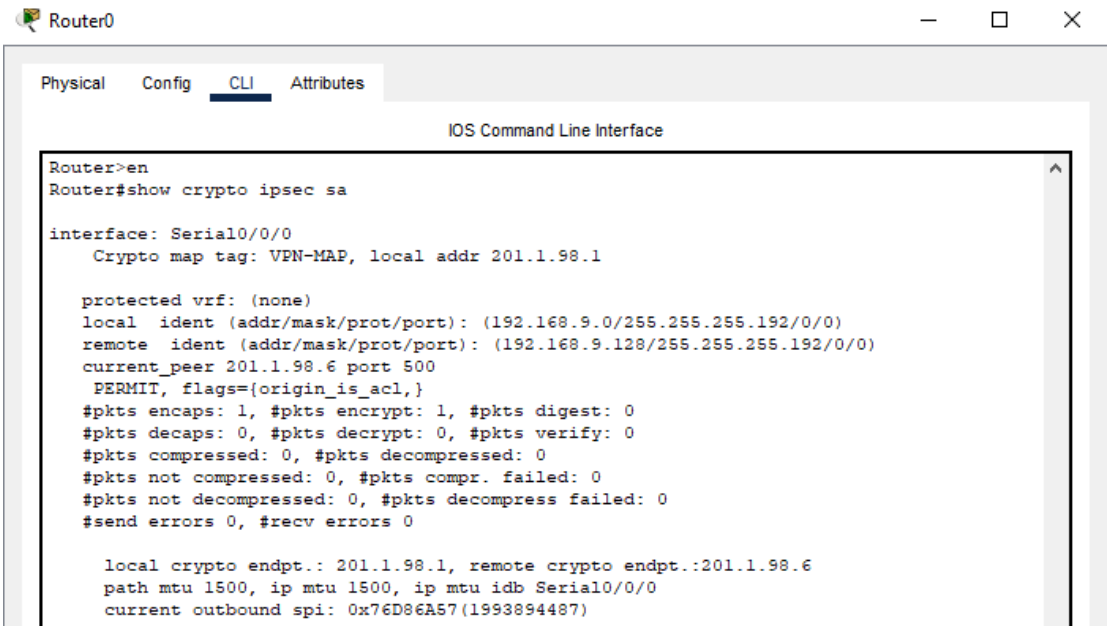


Рисунок 5.5 – Зашифровані пакети після передачі між Router0 – Router2

Аналогічно проводимо тестування з'єднання між Router1 – Router3,

PC0(192.168.9.65) Router1 та PC104(192.168.9.195), показано на лістингу 5.7.

Лістинг 5.7 – перевірка з’єднання між філіями Router1 – Router3

```
C:\>ping 192.168.9.195

Pinging 192.168.9.195 with 32 bytes of data:

Reply from 192.168.9.195: bytes=32 time=2ms TTL=125
Reply from 192.168.9.195: bytes=32 time=12ms TTL=126
Reply from 192.168.9.195: bytes=32 time=12ms TTL=125
Reply from 192.168.9.195: bytes=32 time=12ms TTL=126

Ping statistics for 192.168.9.195:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 12ms, Average = 9ms
```

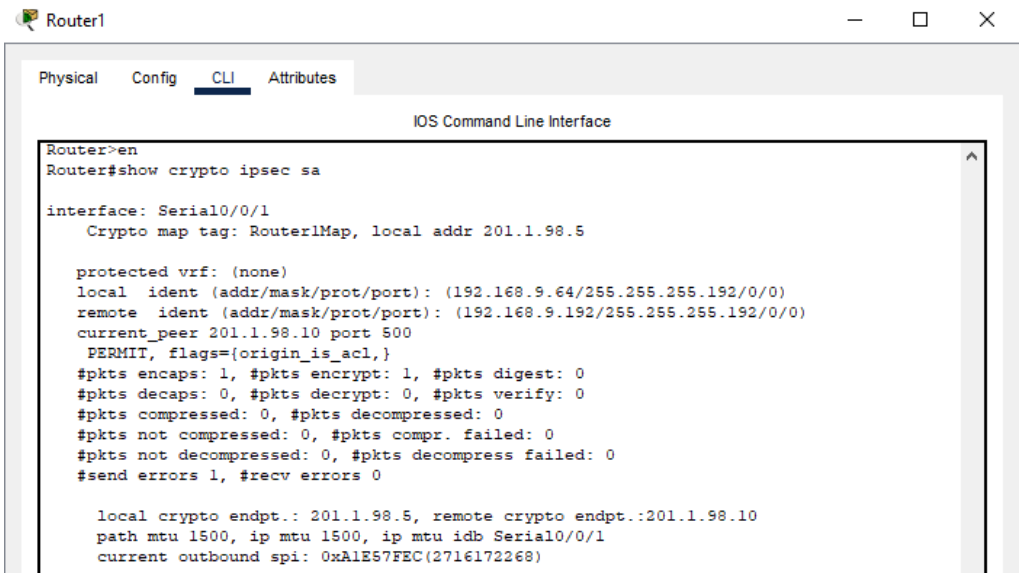


Рисунок 5.6 – Зашифровані пакети після передачі між Router1 – Router3

У результаті тестування IPsec VPN-з’єднань між філіями Router0 – Router2 та Router1 – Router3 підтверджено успішне встановлення захищених тунелів.

Команди show crypto ipsec sa показали, що зашифровані пакети передаються коректно, зафіксовано по 1 пакету, який було успішно зашифровано та відправлено без помилок. Це свідчить про працездатність VPN-з’єднань, правильність налаштувань шифрування та відповідність мережевої конфігурації вимогам безпеки.

ВИСНОВКИ

В процесі виконання даної роботи було успішно спроєктовано комп’ютерну мережу підприємства з використанням протоколу RSTP. Аналіз основних протоколів сімейства Spanning Tree засвідчив, що протокол RSTP є найдоцільнішим варіантом, оскільки забезпечує швидке відновлення мережевої топології після змін і ефективно усуває проблеми, пов’язані з утворенням петель.

При розробці проєкту були враховані основні вимоги до мережі, такі як масштабованість, надійність, безпека та продуктивність.

Для підвищення безпеки та керованості трафіком була здійснена сегментація мережі за допомогою технології VLAN. Щоб полегшити процес управління та пришвидшити налаштування VLAN, у мережі було впроваджено протокол VTP, який дозволяє централізовано керувати інформацією про віртуальні локальні мережі на всіх комутаторах. Для синхронізації часу на пристроях мережі було успішно використано протокол NTP. DHCP забезпечив автоматичну конфігурацію IP-адрес, що значно зменшило навантаження на адміністраторів. З метою захисту передачі даних між філіями було налаштовано VPN на основі протоколу IPsec.

Для побудови та моделювання мережі був обраний Cisco Packet Tracer. Це дозволило ретельно перевірити працездатність та ефективність прийнятих рішень. Результати тестування підтвердили, що спроєктована мережа повністю відповідає поставленим вимогам і готова до практичного впровадження.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1 Spanning Tree Protocols URL: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/154SY/config_guide/sup6T/15_3_sy_swcg_6T/spanning_tree.pdf? (дата звернення: 15.03.2025).

2 Huang, Wayne, Yining Chen, and Jarrad Hee. "STP technology: An overview and a conceptual framework." Information & management 43.3 (2006): 263-270.

3 Bernardino, Rodolfo C., et al. "Link redundancy in the process bus according to IEC 61850 ED. 2: experience with RSTP, PRP and HSR protocols." *IET Conference Proceedings CP800*. Vol. 2022. No. 2. Stevenage, UK: The Institution of Engineering and Technology, 2022.

4 Understand Rapid Spanning Tree Protocol (802.1w) URL: https://www-cisco-com.translate.goog/c/en/us/support/docs/lan-switching/spanning-tree-protocol/24062-146.html? (дата звернення: 20.03.2025).

5 Understand the Multiple Spanning Tree Protocol URL: https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/24248-147.html? (дата звернення: 01.04.2025).

6 ZHONG, Ming; XIE, Wenbo; YANG, Lei. The Optimization and Improvement of Campus Network Based on MSTP. In: 2023 4th International Conference on Computers and Artificial Intelligence Technology (CAIT). IEEE, 2023. p. 212-216.

7 Арсенюк І. Р., Яровий А. А. А85 Комп'ютерні мережі. Навчальний посібник. Частина 1. – Вінниця: ВНТУ, 2008. – 117 с

8 Swaid, Majed, et al. "Design of a uam ground infrastructure network with respect to maintenance capacity requirements." (2024).

9 Wu, Yulei, et al. "A survey of intelligent network slicing management for industrial IoT: Integrated approaches for smart transportation, smart energy, and smart factory." IEEE Communications Surveys & Tutorials 24.2 (2022): 1175-1211.

10 Комп’ютерні мережі : навчальний посібник / О. С. Городецька, В. А.

Гикавий, О. В. Онищук. − Вінниця : ВНТУ, 2017. − 129 с

11 Hengartner, U., Moon, S., Mortier, R., & Diot, C. (2002, November). Detection and analysis of routing loops in packet traces. In Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurment (pp. 107-112).

12 ITO, Hiro, et al. Avoiding routing loops on the internet. Theory of Computing Systems, 2003, 36: 597-609.

13 1000BASE-T (Gigabit Ethernet) URL: https://www.techtarget.com /searchnetworking/definition/1000BASE-T (дата звернення: 5.04.2025).

14 Попов М.А., Киричек Г.Г. Застосування протоколу RSTP. Тиждень науки-2025. Факультет комп'ютерних наук і технологій. Тези доповідей науково-практичної конференції, Запоріжжя, 14-18 квітня 2025 р. – Запоріжжя: НУ «Запорізька політехніка», 2025.

15 Cisco SFP Modules for Gigabit Ethernet Applications Data Sheet URL: https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/gigabit-ethernet-gbic-sfp-modules/datasheet-c78-366584.html (дата звернення: 15.04.2025).

16 Pestov O., Kyrychek H., Tiahunova M. Yggdrasil routing scheme as a basis for large-scale decentralized mesh networks. In Proceedings of the ICST-2024. CEUR Workshop. Vol. 3790. P. 110–122.

17 Understanding VLANs and VLAN Trunking | Transforming a Traditional Network into a VLAN-Based Network URL: https://www.rmtechcentral. com/understanding-vlans-and-vlan-trunking-transforming-a-traditional-network-into-a-vlan-based-network/ (дата звернення: 10.04.2025).

18 Salam, Rudi, and Jenih Jenih. "Perancangan dan Implementasi VLAN dengan VLAN Trunking Protocol (VTP) di PT. Citra Solusi Pratama." Jurnal Teknologi Informasi 8.2 (2022): 91-105.

19 Rudkovskyi O., Kirichek G. Interaction support system of network aplications, Proceedings of the 3rd Workshop forYoung Scientists in Computer Science & Software Engineering, CS&SE@SW 2020, Vol-2832, Kryvyi Rih, Ukraine, November 27, 2020, pp. 11-23.

20 Mills, David L. "A brief history of NTP time: Memoirs of an Internet

timekeeper." ACM SIGCOMM Computer Communication Review 33.2 (2003): 9-21.

21 Киричек Г.Г., Щетінін М.О. Управління конфігурацією серверів на основі Ansible. Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки, 2022. Том 33 (72) №1. С.109-114.

22 DHALL, Hitesh, et al. Implementation of IPSec protocol. In: 2012 Second International Conference on Advanced Computing & Communication Technologies. IEEE, 2012. p. 176-181.

23 Cisco 2900 Series Integrated Services Routers URL: https://www.cisco.com/c/en/us/support/routers/2900-series-integrated-services-routers-isr/series.html (дата звернення: 19.04.2025).

24 Комутатор Cisco WS-C2960-24-S URL: https://циско.com.ua/kommutator-cisco-ws-c2960-24-s (дата звернення: 19.04.2025).

ДОДАТОК А
СХЕМИ МЕРЕЖІ

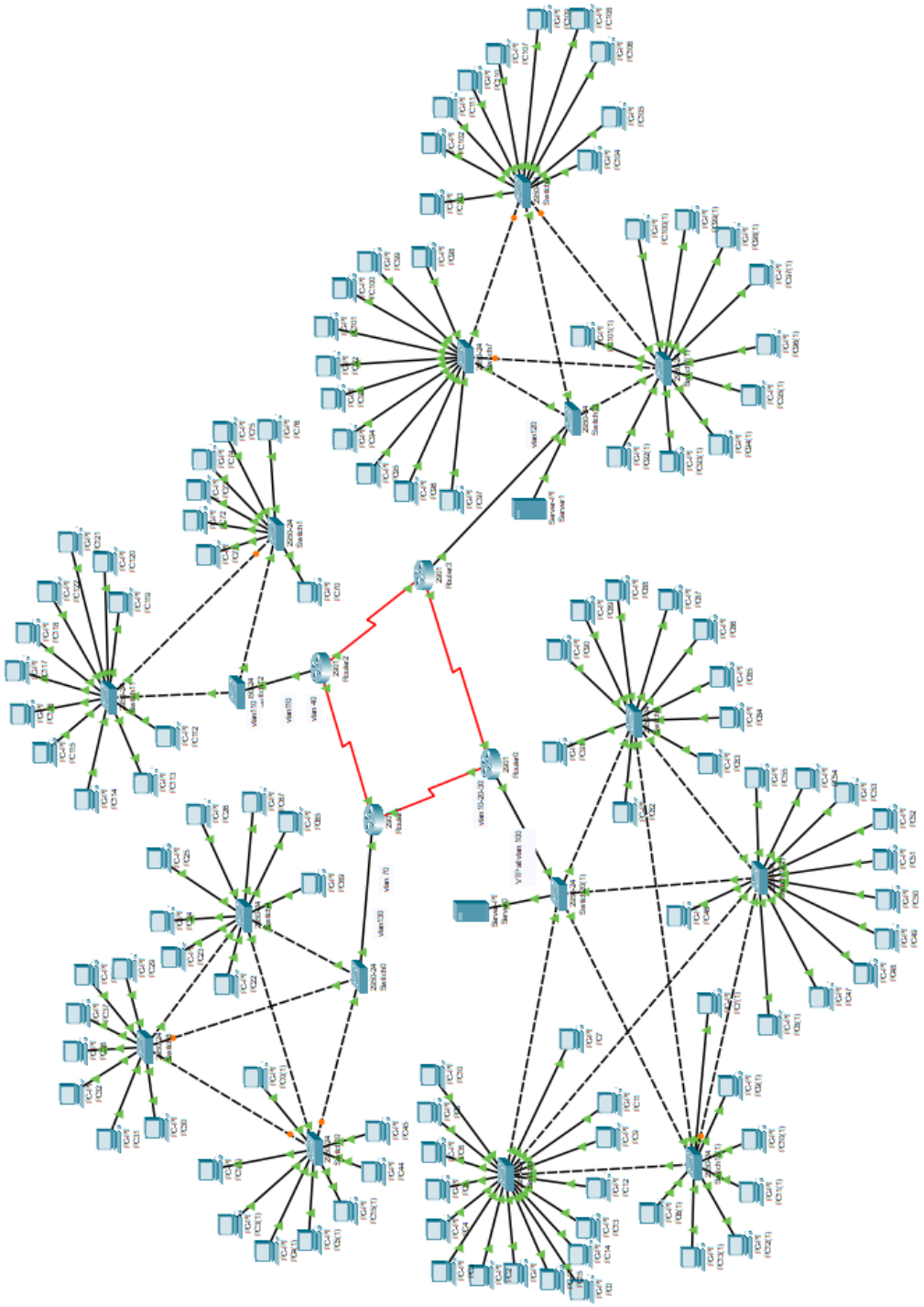


Рисунок А.1 – Функціональна схема

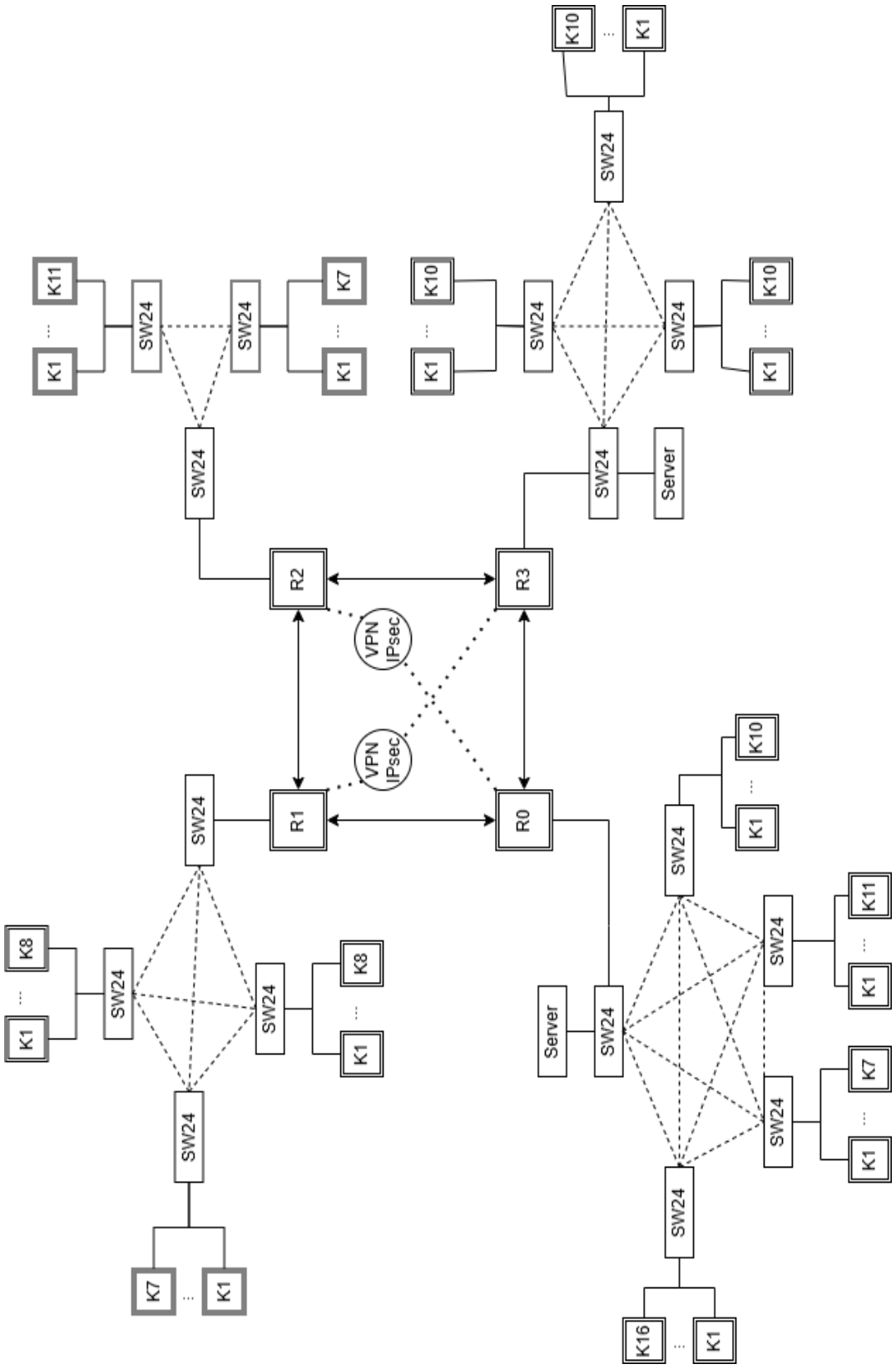


Рисунок А.2 – Структурна схема

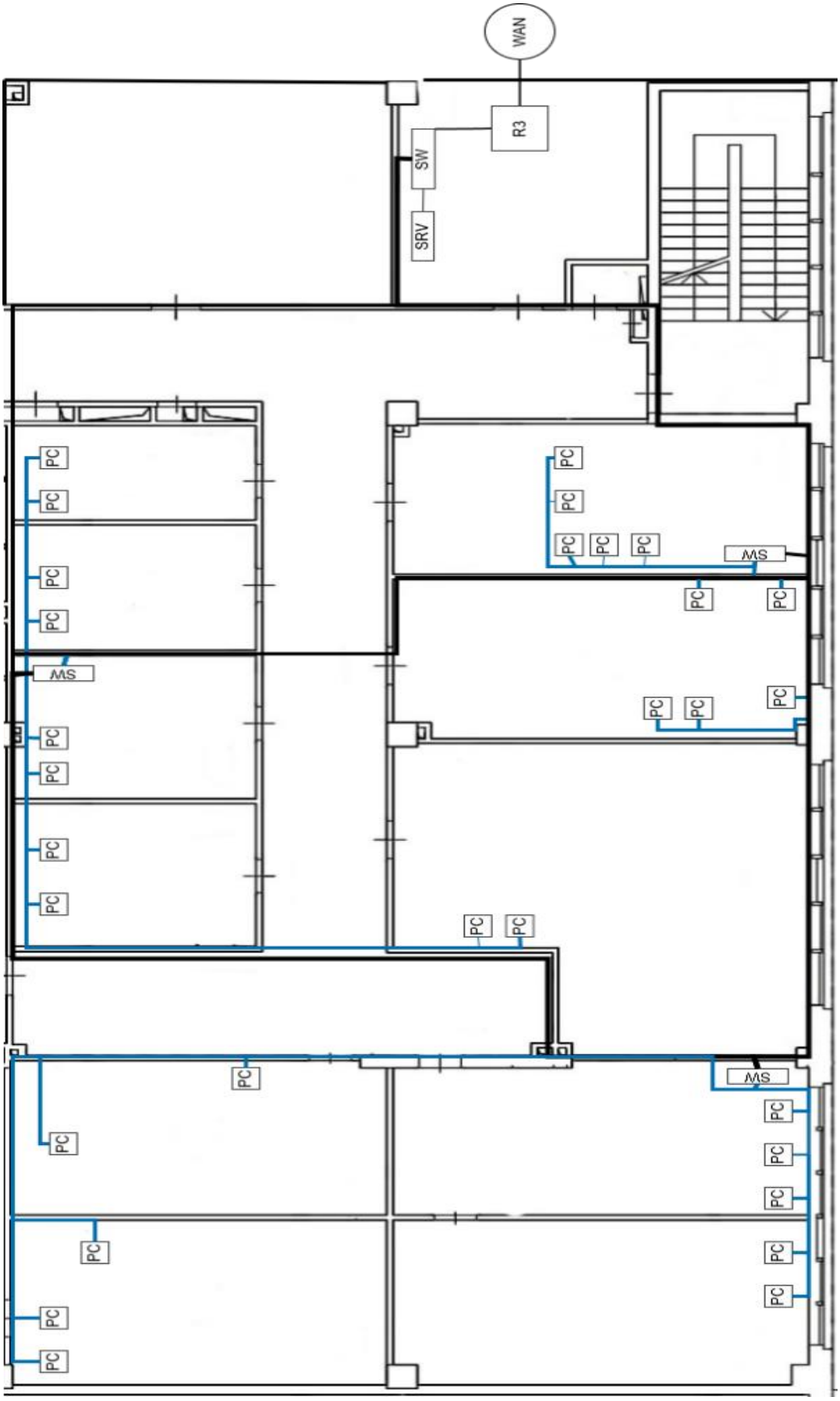


Рисунок А.3 – Монтажна схема

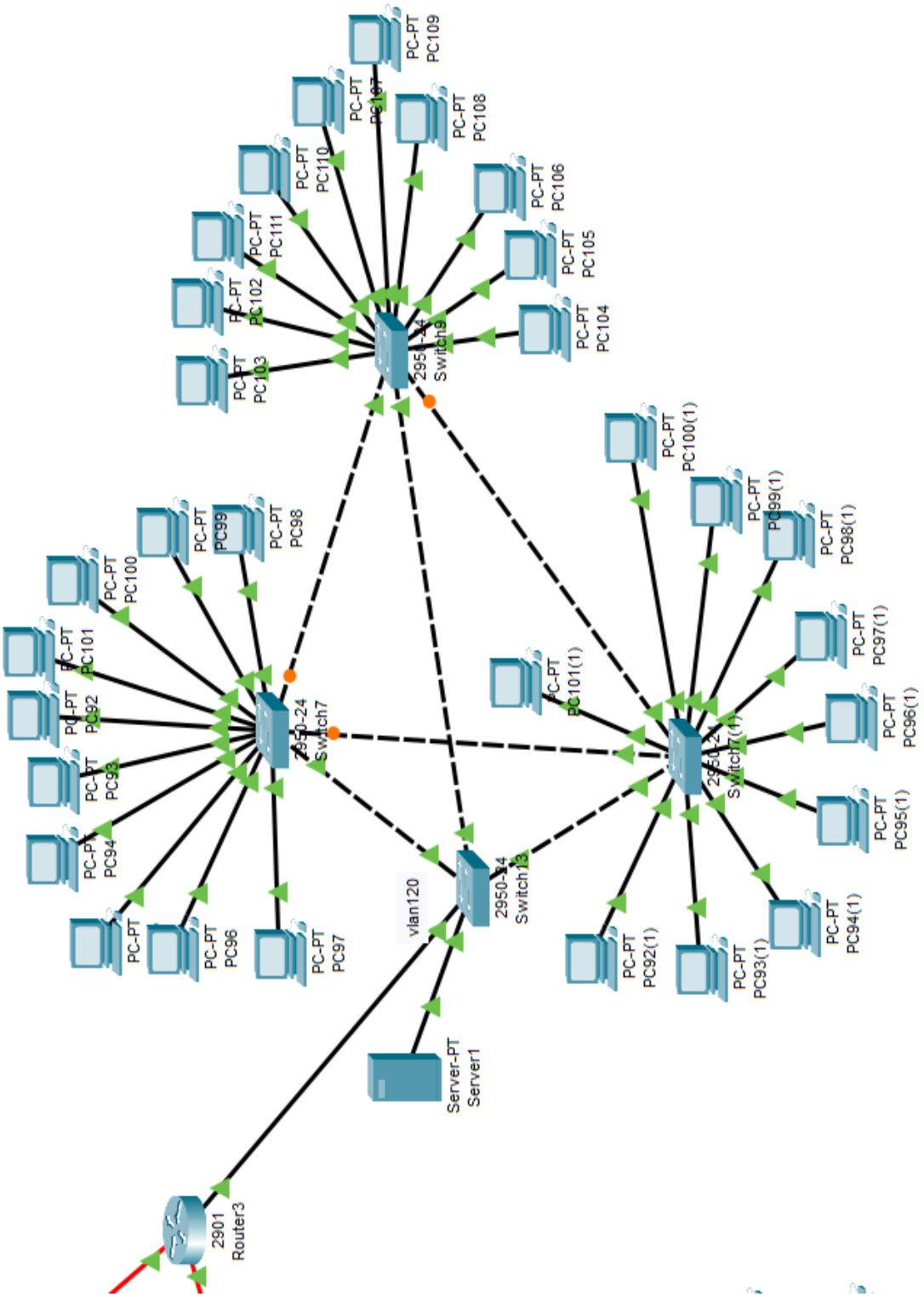


Рисунок А.4 – Філія router3

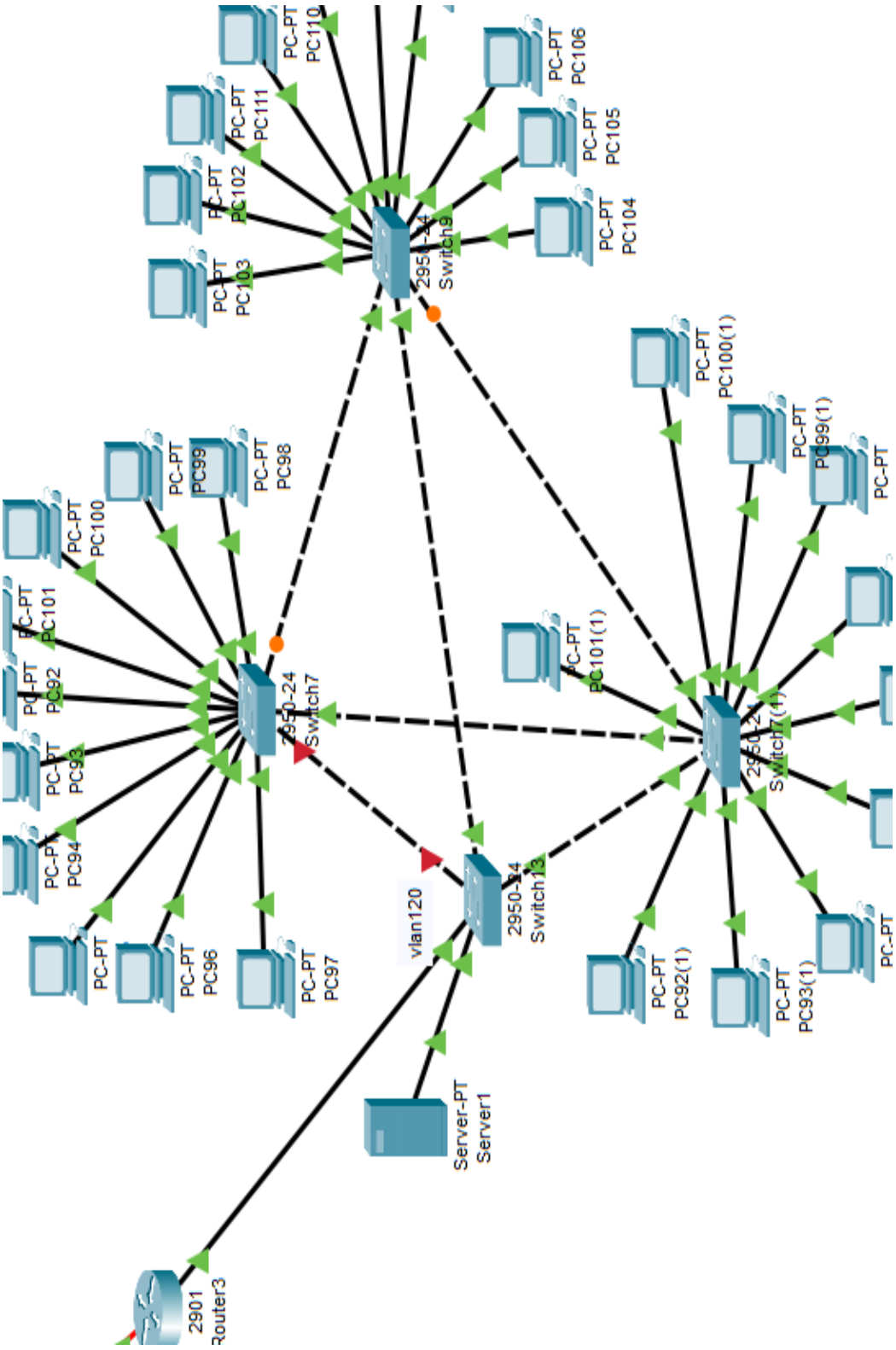


Рисунок А.5 – Перебудована топологія

ДОДАТОК Б
ЛІСТИНГИ ПРОГРАМ

Лістинг Б.1 - Налаштування статичної маршрутизації

```
Router0>en
Router0#conf t
Router0(config)ip route 192.168.9.64 255.255.255.192 201.1.98.2
Router0(config)ip route 192.168.9.128 255.255.255.192 201.1.98.2
Router0(config)ip route 192.168.9.128 255.255.255.192 201.1.98.13
Router0(config)ip route 192.168.18.0 255.255.255.0 201.1.98.2
Router0(config)ip route 192.168.9.192 255.255.255.192 201.1.98.13
Router0(config)ip route 201.1.98.4 255.255.255.252 201.1.98.2
Router0(config)ip route 201.1.98.8 255.255.255.252 201.1.98.13

Router1>en
Router1#conf t
Router1(config)ip route 192.168.9.0 255.255.255.192 201.1.98.1
Router1(config)ip route 192.168.9.128 255.255.255.192 201.1.98.6
Router1(config)ip route 192.168.9.192 255.255.255.192 201.1.98.1
Router1(config)ip route 192.168.9.192 255.255.255.192 201.1.98.6
Router1(config)ip route 201.1.98.8 255.255.255.252 201.1.98.6
Router1(config)ip route 201.1.98.12 255.255.255.252 201.1.98.1

Router2>en
Router2#conf t
Router2(config)ip route 192.168.9.0 255.255.255.192 201.1.98.5
Router2(config)ip route 192.168.9.0 255.255.255.192 201.1.98.10
Router2(config)ip route 192.168.9.64 255.255.255.192 201.1.98.5
Router2(config)ip route 192.168.9.192 255.255.255.192 201.1.98.10
Router2(config)ip route 201.1.98.0 255.255.255.252 201.1.98.5
Router2(config)ip route 201.1.98.12 255.255.255.252 201.1.98.10

Router3>en
Router3#conf t
```

Продовження лістингу Б.1

```
Router3(config)ip route 192.168.9.0 255.255.255.192 201.1.98.14
Router3(config)ip route 192.168.9.64 255.255.255.192 201.1.98.9
Router3(config)ip route 192.168.9.128 255.255.255.192 201.1.98.9
Router3(config)ip route 192.168.15.0 255.255.255.0 201.1.98.9
Router3(config)ip route 201.1.98.0 255.255.255.252 201.1.98.14
Router3(config)ip route 201.1.98.4 255.255.255.252 201.1.98.9
```

Лістинг Б.2 - NTP клієнти

```
Router0>en
Router0#sh ntp status
Clock is synchronized, stratum 2, reference is 192.168.9.2
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision
is 2**24
reference time is E926F93F.000001B7 (16:11:43.439 UTC Mon Apr 28
2025)
clock offset is 0.00 msec, root delay is 0.00 msec
root dispersion is 104.10 msec, peer dispersion is 0.11 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is -
0.000001193 s/s system poll interval is 4, last update was 12 sec
ago.
Router1>en
Router1#sh ntp status
Clock is synchronized, stratum 2, reference is 192.168.9.2
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision
is 2**24
reference time is E927123E.0000025A (17:58:22.602 UTC Mon Apr 28
2025)
clock offset is 0.00 msec, root delay is 5.00 msec
root dispersion is 107.76 msec, peer dispersion is 0.12 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is -
0.000001193 s/s system poll interval is 4, last update was 10 sec
ago.
Router2>en
Router2#sh ntp status
```

```
Clock is synchronized, stratum 2, reference is 192.168.9.2
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision
is 2**24
reference time is EB9164D2.0000016E (18:11:30.366 UTC Mon Apr 28
2025)
clock offset is 0.00 msec, root delay is 7.00 msec
root dispersion is 119.65 msec, peer dispersion is 0.00 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is -
0.000001193 s/s system poll interval is 4, last update was 5 sec
ago.
Router3>en
Router#sh ntp status
Clock is synchronized, stratum 16, reference is 192.168.9.2
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision
is 2**24
reference time is F1BB6854.0000032A (17:3:16.810 UTC Mon Apr 28 2025)
clock offset is -31536004880.00 msec, root delay is 3.00 msec
root dispersion is 122.82 msec, peer dispersion is 0.12 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is -
0.000001193 s/s system poll interval is 4, last update was 1 sec
ago.
```

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ “ЗАПОРІЗЬКА ПОЛІТЕХНІКА”

ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ НАУК І ТЕХНОЛОГІЙ

КАФЕДРА КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ

ПРОЄКТУВАННЯ РОЗПОДІЛЕНОЇ МЕРЕЖІ ПІДПРИЄМСТВА ІЗ ЗАСТОСУВАННЯМ ПРОТОКОЛУ RSTP

Виконавець:
ПОПОВ Микола Андрійович
студент групи КНТ-512сп

Керівник:
КИРИЧЕК Галина Григорівна
к. т. н., доцент кафедри
комп’ютерних систем та мереж

2

МЕТА РОБОТИ

Метою роботи є проектування розподіленої мережі підприємства із застосуванням протоколу RSTP та створення надійної, продуктивної інфраструктури, яка гарантує безперебійний зв'язок між усіма об'єктами.

Предметом дослідження є методи, засоби, технології, стандарти та протоколи, які забезпечують стабільну роботу, безпеку, сегментацію трафіку й швидке відновлення з'єднань.

АКТУАЛЬНІСТЬ

3

Сучасні підприємства потребують стабільного й безперебійного обміну даними між філіями.
Однією з критичних проблем у корпоративних мережах є утворення петель у топології, які можуть спричинити збої, втрату даних і навіть повне припинення роботи мережі.
Надійність інфраструктури ключовий чинник для компаній з розгалуженою структурою.
Навіть короткочасні простої призводять до фінансових втрат і негативно впливають на репутацію.
Протокол RSTP дозволяє значно зменшити час відновлення зв'язку після відмови та запобігає петлям, оптимізуючи роботу мережі без додаткових витрат на обладнання.

ПОРІВНЯННЯ ПРОТОКОЛІВ STP, RSTP, MSTP

4

Для забезпечення відмовостійкості та уникнення петель у мережевих топологіях використовуються протоколи родини Spanning Tree. Найбільш поширеними є STP, RSTP та MSTP.

У таблиці наведено основні характеристики та відмінності між ними. RSTP має значну перевагу у швидкості конвергенції, що є критично важливим для стабільної роботи сучасних мереж.

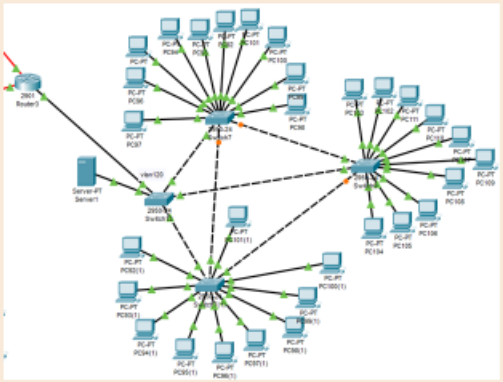
Хоча MSTP пропонує найкращу масштабованість і підтримку VLAN, для даного проєкту, де не потрібна складна сегментація VLAN, RSTP є оптимальним компромісом між швидкістю, простотою та ефективністю.

Характеристика	STP	RSTP	MSTP
Стандарт	IEEE 802.1D	IEEE 802.1w	IEEE 802.1s
Час збіжності	30-50 секунд	1-2 секунд	1-2 секунд
Типи портів	Root, Designated, Blocking	Root, Designated, Alternate, Backup	Root, Designated, Alternate, Backup
Кількість дерев	1	1	Декілька (для VLAN або їх груп)
Обробка топологічних змін	Використовує таймери	Використовує швидкі повідомлення BPDU	Аналогічно RSTP, але з підтримкою кількох дерев
Балансування навантаження	Немає	Немає	Є (через розподіл VLAN на MSTI)
Сумісність з попередніми версіями	Так	Так	Так
Область застосування	Невеликі та прості мережі	Середні за розміром мережі	Великі корпоративні та операторські мережі

5

ПРОТОКОЛ RSTP (RAPID SPANNING TREE PROTOCOL)

- RSTP це вдосконалена версія STP, яка забезпечує швидке відновлення мережевої топології після збоїв.
- Працює за стандартом IEEE 802.1w.
- Замість 30 – 50 секунд, як у STP, час конвергенції RSTP до 2 секунд.
- Забезпечує захист від петель, автоматично блокуючи резервні канали до моменту відмови основного.
- Підтримує стани портів Root, Designated, Alternate, Backup.
- Має зворотну сумісність зі стандартним STP.



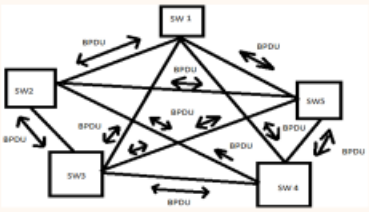
6

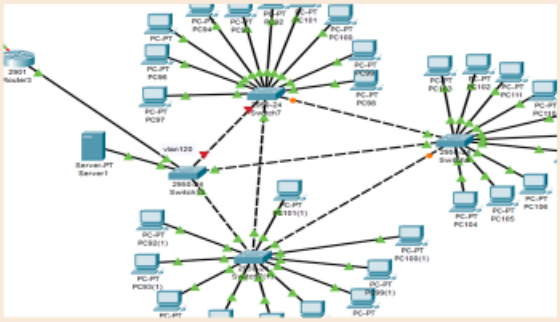
РОБОТА ПРОТОКОЛУ RSTP

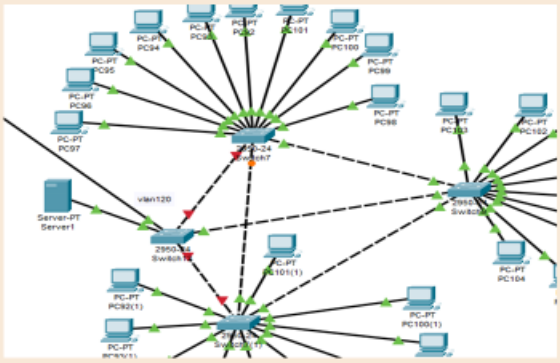
При виході із ладу одного або декількох каналів відбувається миттєве виявлення змін у топології та побудова нової активної структури мережі без необхідності ручного втручання.

RSTP переводить резервні (alternate або backup) порти в активний стан майже миттєво, що значно зменшує простої.

Протокол постійно обмінюється bpdu-повідомленнями (кожні 2 секунди), завдяки чому швидко реагує на зміни.







ПРОБЛЕМИ ВИНИКНЕННЯ ПЕТЕЛЬ МЕРЕЖАХ ТА МЕТОДИ БОРОТЬБИ З НИМИ

7

Петлі виникають при наявності кількох фізичних шляхів між комутаторами.
Це призводить до:
•Шторм широкомовного трафіку (Broadcast Storm) пакети безперервно циркулюють мережею, перевантажуючи її.
•Нестабільність таблиць MAC-адрес комутатори отримують суперечливу інформацію про розташування пристроїв.
•Дублювання кадрів одні й ті самі дані надсилаються кілька разів.
•Зростання затримок та втрати пакетів мережа стає повільною або недоступною.
•Повний вихід мережі з ладу у критичних випадках мережа перестає функціонувати.
Методи запобігання петлям
•RSTP (Rapid Spanning Tree Protocol) швидке виявлення та блокування петель.
•BPDU Guard захист від несанкціонованих підключень комутаторів.
•Root Guard запобігання зміні кореневого комутатора.
•Loop Guard виявлення "тихих" петель через втрату BPDU.
•PortFast швидке ввімкнення портів для кінцевих пристроїв.

ВИМОГИ ДО КОМП'ЮТЕРНОЇ МЕРЕЖІ

8

Захищеність
- Швидке реагування на загрози (наприклад, атаки типу MITM, петлі)
- Захист від несанкціонованого доступу, пошкодження, крадіжки даних
- Централізоване зберігання та резервне копіювання інформації

Сумісність
- Підтримка різного обладнання, ОС і протоколів
- Можливість співіснування STP, RSTP та інших протоколів

Розширюваність
- Просте додавання нових пристроїв, користувачів, служб
- Можливість заміни обладнання без зміни топології

Надійність
- Високий рівень відмовостійкості
- Якісне апаратне забезпечення, резервні лінії зв`язку

Масштабованість
- Розширення мережі без втрати продуктивності
- Гнучке реагування на зміни топології

Продуктивність
- Підвищена швидкодія за рахунок RSTP
- Мінімальні затримки, ефективне використання пропускної здатності

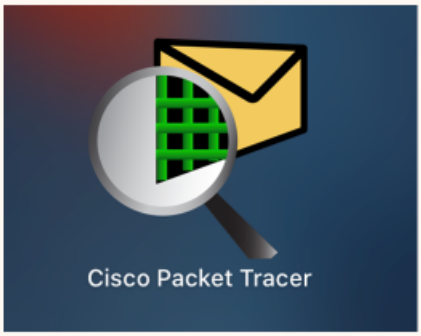
9

CISCO PACKET TRACER

Плюси:

- інтуїтивно зрозумілий інтерфейс;
- має безкоштовний доступ для студентів та викладачів;
- створення віртуальних мереж з різними пристроями;
- моделювання в реальному часі;
- режим симуляції;
- тестування конфігурації мережі без фізичного обладнання;
- навчальні курси вже є в самому інструменті;
- дає змогу працювати на різних рівнях моделі OSI.

Мінусом є довге налаштування конфігурацій, особливо статичне налаштування.

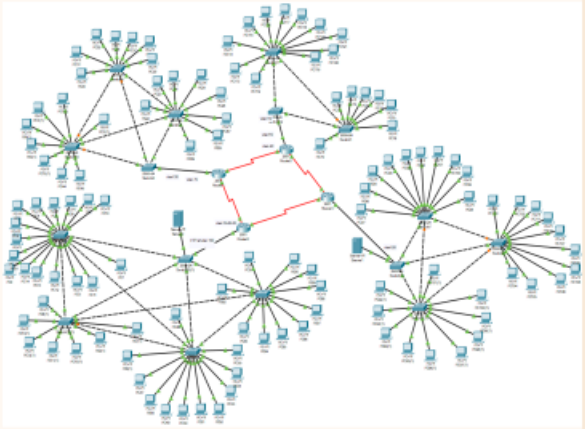


10

ПРОЄКТУВАННЯ МЕРЕЖІ

Розроблена мережа включає 4 філії, кожна з яких має власну локальну (LAN) мережу.
Всі філії об'єднані в єдину корпоративну інфраструктуру за допомогою WAN-з'єднань.
В основі кожної LAN кілька комутаторів, з яких один виконує роль центрального та під'єднаний до маршрутизатора.
У кожній локальній мережі налаштовані такі протоколи та технології:

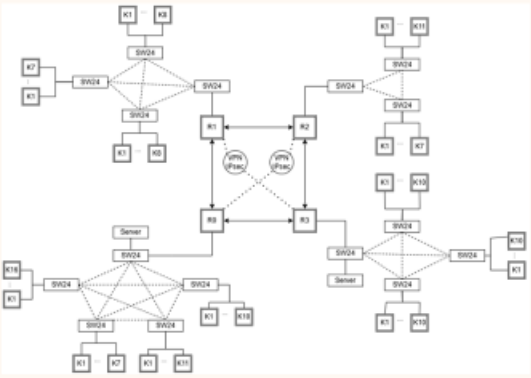
- VLAN логічне розділення мережевого трафіку між відділами
- VTP централізоване управління VLAN
- RSTP захист від петель та забезпечення відмовостійкості
- NTP синхронізація часу між мережевими пристроями
- DHCP автоматична видача IP-адрес кінцевим пристроям
- Статична маршрутизація для спрощеного адмініструваня
- IPsec VPN захищене з'єднання між філіями



11

СТРУКТУРА МЕРЕЖІ

Кожна філія має власний маршрутизатор, який забезпечує організацію локальної мережі та підключення до загальної корпоративної інфраструктури.
Дві філії обладнані серверами, доступними для всіх пристроїв.
Загалом мережа включає:
•2 сервери
•117 комп`ютерів
•16 комутаторів
•4 маршрутизатори
Для з`єднання використовується:
•1000BASE-T (витою парою Cat 5e) у локальних мережах зі швидкістю до 1 Гбіт/с
•1000BASE-BX10 – для міжфілійного з`єднання з оптичним кабелем до 1 Гбіт/с
Між філіями R0 – R2 та R1 – R3 реалізовано VPN-з'єднання з IPsec для забезпечення захищеної передачі даних.



12

ВИБІР МЕРЕЖЕВОГО ОБЛАДНАННЯ

Для побудови надійної та масштабованої корпоративної мережі обрано обладнання компанії Cisco, яке забезпечує високу продуктивність, підтримку сучасних протоколів і зручність налаштування.

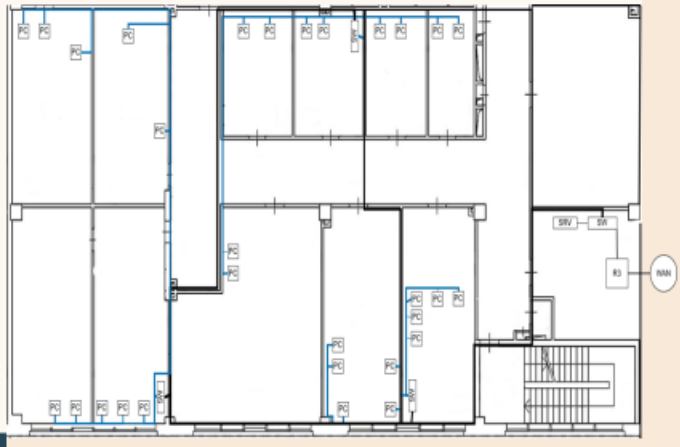
Маршрутизатор Cisco 2901
- Підтримка до 50 користувачів
- 2 вбудовані гігабітні Ethernet-порти
- Підтримка VPN, IPsec, NAT, QoS
- Сумісність з модулями HWIC, EHWIC
- Призначений для зв`язку філій у WAN-сегменті
- Використовується як міжфілійний шлюз

Комутатор Cisco WS-C2960-24TS-S
- 24 порти Ethernet 10/100/1000 Мбіт/с
- 2 порти SFP (оптичні модулі)
- Підтримка протоколів VLAN, VTP, RSTP
- Інтелектуальні функції рівня 2
- Ідеальний для побудови надійної LAN-мережі
- Просте керування через CLI

13

МОНТАЖНА СХЕМА

На ній представлені комутатори, маршрутизатори, сервери та робочі станції, а також кабельні з'єднання між ними. Розташування обладнання забезпечує зручність обслуговування, логічну побудову мережі та мінімізацію довжини кабелів. Також враховано резервування каналів для підвищення надійності мережевих з'єднань.



ВИСНОВКИ

14

• У ході виконання дипломної роботи було успішно спроєктовано розподілену комп'ютерну мережу підприємства з використанням протоколу RSTP. Проведений аналіз протоколів STP, RSTP та MSTP дозволив обґрунтувати вибір саме RSTP як оптимального рішення завдяки його здатності до швидкої конвергенції та ефективного уникнення петель.

• У проєкті враховано критично важливі характеристики мережі: масштабованість, продуктивність, надійність, безпека та сумісність. Для підвищення захищеності даних між філіями була реалізована VPN на базі IPsec, а централізоване зберігання інформації дозволило ефективно організувати процес резервного копіювання.

• Для логічного розподілу трафіку впроваджено технологію VLAN, а для спрощення адміністрування використано протокол VTP. DHCP забезпечив автоматичне призначення IP-адрес, а синхронізація часу була реалізована за допомогою NTP.

ПУБЛІКАЦІЇ

15

- Попов М.А., Киричек Г.Г. Застосування протоколу RSTP. Тиждень науки-2025. Факультет комп'ютерних наук і технологій. Тези доповідей науково-практичної конференції, Запоріжжя, 14-18 квітня 2025 р. – Запоріжжя: НУ «Запорізька політехніка», 2025