Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра обчислювальної техніки

БАКАЛАВРСЬКА ДИПЛОМНА РОБОТА

на тему:

Комп'ютерна мережа центрального офісу компанії «Vodafone»

ПОЯСНЮВАЛЬНА ЗАПИСКА

Виконав: студент 4 курсу, групи 1КІ-18б
Спеціальності
123 — «Комп'ютернаінженерія»
Мазуренко В.В.
Керівник к.т.н., проф.
Захарченко С.М.
Рецензент к.т.н., доц.
Карпінець В.В.

Допущено до захисту
д.т.н., проф. Азаров О.Д.

"21" 06 2022 р.

ВНТУ 2022

ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра обчислювальної техніки
Освітній рівень — бакалавр
Спеціальність — 123 Комп'ютерна інженерія

ЗАТВЕРДЖУЮ
Завідувач кафедри ОТ
д.т.н., проф. О.Д. Азаров
(підпис)
«9» лютого 2022 р.

З А В Д А Н Н Я
НА БАКАЛАВРСЬКУ ДИПЛОМНУ РОБОТУ

студенту **Мазуренку Владиславу Володимировичу**

1 Тема роботи «Комп'ютерна мережа центрального офісу компанії Vodafone» керівник роботи Захарченко Сергій Михайлович к.т.н., професор, затверджено наказом вищого навчального закладу від "24" березня 2022 року №66.

2 Строк подання студентом роботи 21.06.2022.

3 Вихідні дані до роботи: структура компанії, структура будівлі, де розташована компанія, перелік мережевих сервісів, вимоги до пропускної спроможності, кількість кінцевих пристроїв.

4 Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити): вступ, аналіз сучасних принципів розробки ком'ютерних мереж, проектування спеціалізованої ком'ютерної мережі, реалізація проекту в симуляторі Cisco Packet Tracer.

5 Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень): схема компанії, схема поверхів.

6 Консультанти розділів роботи приведені в таблиці 1.

Таблиця 1— Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1-3	Захарченко Сергій Михайлович, к.т.н., професор кафедри ОТ	16.05	27.05

7 Дата видачі завдання

8 Календарний план виконання БКР приведений в таблиці 2.

Таблиця 2 — Календарний план

№ з/п	Назва етапів БДР	Строк виконання	Підпис
1	Постановка задачі роботи	16.05	
2	Аналіз сучасних технологій побудови комп'ютерних мереж	17.05	
3	Аналіз та вибір апаратних засобів комп'ютерної мережі	18.08	
4	Розробка структури комп'ютерної мережі	19.05	
5	Реалізація проекту в симуляторі Cisco Packet Tracer	20.05-21.05	
6	Підготовка матеріалів та опис розробки комп'ютерної мережі	22.05-23.05	
7	Оформлення пояснювальної записки та ілюстративного матеріалу	24.05-25.05	
8	Аналіз виконання роботи, висновки, додатки	26.05	
9	Перевірка якості виконання бакалаврської роботи та усунення недоліків	27.05	

Студент Мазуренко Владислав Володимирович

Керівник Захарченко Сергій Михайлович

АНОТАЦІЯ

Бакалаврська робота містить 66 сторінок пояснюючої записки, 33 рисунки, 7 таблиць та 13 лістингів.

У ході виконання даної бакалаврської роботи було розроблено комп’ютерну мережу центрального офісу компанії «Vodafone», що була промодельована в симуляторі Cisco Packet Tracer. Розроблена комп’ютерна мережа забезпечує швидкий обмін даними, забезпечує надійний захист інформації, та надає доступ користувачам до сервера. Також реалізовано безпечний вихід в зовнішню мережу та вжито заходи з покращення продуктивності мережі.

Ключові слова: комп’ютерна мережа.

Студент групи 1КІ-18б спеціальності 123 — «Комп’ютерна інженерія»

Мазуренко Владислав Володимирович

Керівник Захарченко С.М.

ABSTRACT

The bachelor's thesis contains 66 pages of explanatory notes, 33 figures, 7 tables, and 13 listings.

In the course of this bachelor's thesis a computer network of Vodafone central office was developed and simulated in Cisco Packet Tracer simulator. The developed computer network provides fast data exchange, provides reliable information protection and gives users access to the server. Secure access to the outside network is also implemented and measures are taken to improve network performance.

Keywords: computer network.

Студент групи 1КІ-18б спеціальності 123 — «Комп’ютерна інженерія»
Мазуренко Владислав Володимирович
Керівник Захарченко С.М.

ЗМІСТ

ВСТУП

Актуальність теми дослідження полягає в тому, сьогодні важко уявити світ без комп'ютерних мереж. Це пов’язано з тим, що комп'ютерні мережі сприяють обміну інформацією на високій швидкості і на великі відстані. Наприклад, організація з великою кількістю офісів по всьому світу може миттєво отримати інформацію про стан віддалених офісів одним натисканням кнопки.

Комп'ютерні мережі — це спосіб обміну інформацією між двома або більше комп'ютерами. Мережі бувають різних розмірів, форм та конфігурацій. Зазвичай, вони з'єднані в одну велику мережу, найвідомішим прикладом якої є Інтернет.

Об’єктом дослідження даної дипломної роботи є процеси, що протікають в комп’ютерних мережах, які експлуатуються в компанії.

Предмет дослідження даної дипломної роботи є створення та налаштування комп’ютерної мережі компанії “Vodafone”.

Метою роботи є розробка локальної комп’ютерної мережі для компанії “Vodafone”.

Відповідно до мети дослідження висуваються такі **задачі**:

— огляд можливостей сучасних протоколів передачі даних;

— аналіз тенденцій розвитку сучасних мережевих технологій;

— розробити фізичну та логічну структуру мережі;

— спроектувати локальну мережу.

Методи дослідження. Дослідження, виконані під час роботи над бакалаврською роботою, ґрунтуються на використанні чималого функціоналу мережевих технологій, які в свою чергу являються основними при побудові мережі.

Практичне значення роботи полягає в застосуванні розробленої комп’ютерної мережі центральним офісом для забезпечення збільшення продуктивності компанії.

1 СУЧАСНІ ПРИНЦИПИ РОЗРОБКИ КОМП'ЮТЕРНИХ МЕРЕЖ

1.1 Локальні та глобальні комп'ютерні мережі

Локальна мережа (LAN) — це кластер комп'ютерів і пов'язаних пристроїв, які спільно використовують стандартну лінію зв'язку або бездротове з'єднання із сервером. Зазвичай локальна мережа охоплює комп'ютери та периферійні пристрої, під'єднані до сервера в певному географічному регіоні, як-от робоче місце або установа з рекламними щитами. Комп'ютери та різні мобільні пристрої використовують приналежність до локальної мережі для спільного використання ресурсів, як-от принтер або мережеве сховище.

Локальна мережа може функціонувати лише з 2 або 3 користувачами (наприклад, у мережі дуже маленького офісу) або з багатьма сотнями користувачів на дуже великому робочому місці. Комп'ютерна мережа містить кабелі, комутатори, маршрутизатори та різні частини, які дозволяють користувачам підключатися до внутрішніх серверів, веб-сайтів та різних локальних мереж через глобальні мережі.

Міська мережа (MAN) — це мережа, що об'єднує користувачів із ресурсами ПК у географічному просторі або регіоні, що перевищує розміри навіть великої локальної мережі (LAN), але менший, ніж простір, що охоплюється глобальною мережею (WAN). Термін застосовується до об'єднання мереж у великому місті в одну велику мережу. Він також використовується для поєднання багатьох місцевих мереж шляхом з'єднання їх магістральними лініями.

Глобальна мережа (WAN) може бути телекомунікаційною мережею або мережею, яка тягнеться на величезну географічну відстань. Широкозонні мережі зазвичай створюються за допомогою найманих телекомунікаційних каналів. Бізнес, освітні та урядові організації використовують глобальні мережі для передачі інформації співробітникам, студентам, клієнтам, покупцям та постачальникам з багатьох точок планети.

По суті, цей спосіб телекомунікацій дозволяє підприємству ефективно виконувати свої щоденні завдання, незалежно від його місцезнаходження. Близькі терміни для альтернативних типів мереж - персональні мережі (PANs), локальні мережі (LANs), кампусні мережі (CANs) або міські мережі (MANs).

1.2 Віртуальна локальна мережа (VLAN)

VLAN (віртуальна локальна мережа) – це логічне угруповання пристроїв в одному широкомовному домені. VLAN зазвичай налаштовуються на комутаторах шляхом розміщення деяких інтерфейсів в один широкомовний домен, а деяких інтерфейсів - в інший.

VLAN можуть розповсюджуватися на кілька комутаторів, при цьому кожна VLAN розглядається як власна підмережа або широкомовний домен. Це означає, що кадри, що передаються в мережу, комутуватимуться лише між портами однієї віртуальної мережі.

VLAN діє як фізична локальна мережа, але дозволяє об'єднувати хости в один широкомовний домен, навіть якщо вони не підключені до одного комутатора. Ось основні причини, через які використовуються віртуальні локальні мережі:

— VLAN збільшує кількість широкомовних доменів при зменшенні їх розміру;

— VLAN знижують ризики безпеки за рахунок зменшення кількості хостів, які отримують копії кадрів, що передаються комутаторами;

— ви можете утримувати хости, що зберігають конфіденційні дані, окремій мережі VLAN для підвищення безпеки;

— ви можете створювати гнучкіші мережеві схеми, які групують користувачів по відділах, а не за фізичним розташуванням;

— зміни мережі легко досягаються простим конфігуруванням порту у відповідну VLAN.

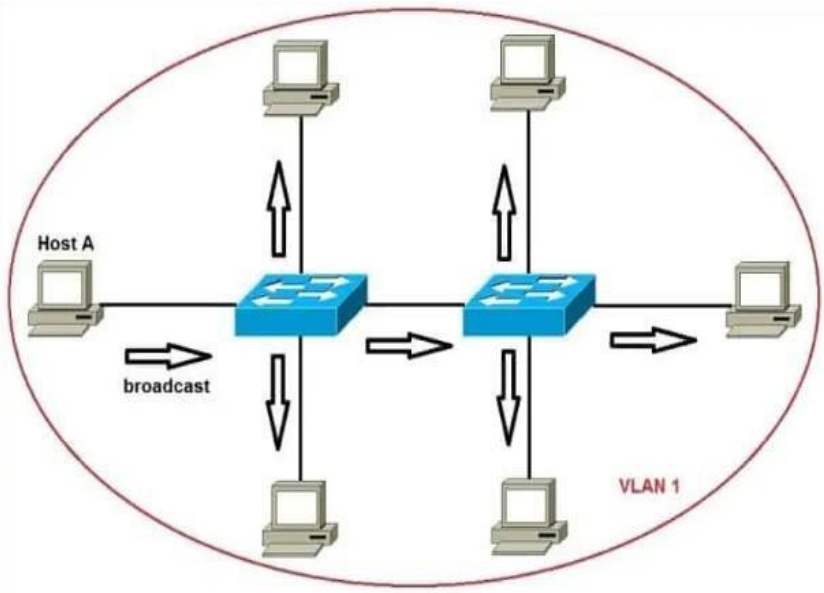

Рисунок 1.1 — Мережа, де всі хости знаходяться в одній віртуальній локальній мережі

Без різних VLAN'ів широкомовна передача, відправлена з хоста A, досягла всіх пристроїв у мережі. Кожен пристрій отримуватиме та оброблятиме широкомовні кадри, збільшуючи навантаження на процесор кожного пристрою та знижуючи загальну безпеку мережі.

Якщо помістити інтерфейси обох комутаторів в окрему VLAN, широкомовна передача від хоста A досягатиме лише пристроїв у тій же VLAN, оскільки кожна VLAN є окремим широкомовним доменом. Це показано на рисунку 1.2.

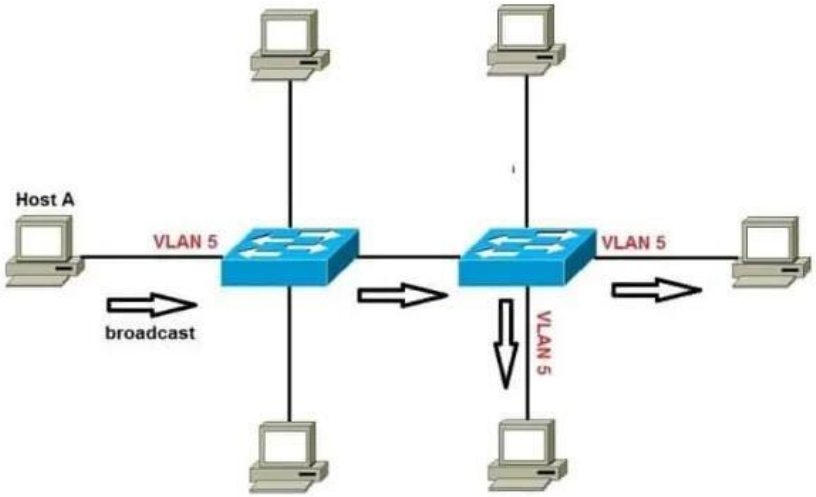

Рисунок 1.2 — Мережа з інтерфейсами обох комутаторів в окремому VLAN

1.3 Технології маршрутизації

Маршрутизація мережі — це процес вибору шляху через одну абокілька мереж. Принципи маршрутизації можуть бути застосовані до будь- якого типу мереж, від телефонних мереж до громадського транспорту. У мережах з комутацією пакетів, таких як Інтернет, маршрутизація вибирає шляхи, якими пакети Інтернет-протоколу (IP) будуть рухатися від місця відправлення до місця призначення. Рішення про маршрутизацію в Інтернеті приймаються спеціалізованими частинами мережного обладнання, які називають маршрутизаторами.

Маршрутизатор — це частина мережного обладнання, що відповідає за пересилання пакетів за призначенням. Маршрутизатори підключаються до двох або більше IP-мереж або підмереж і передають пакети даних між ними при необхідності. Маршрутизатори використовуються в будинках та офісах для налаштування локальних мережних з'єднань. Більш потужні маршрутизатори працюють у всьому Інтернеті, допомагаючи пакетам даних досягати своїх пунктів призначення.

Є два види маршрутизації:

— статичнамаршрути задаються вручну адміністратором.

— динамічнамаршрути обчислюються автоматично за допомогою протоколів динамічної маршрутизації —RIP, OSPF, EIGRP, IS-IS, BGP, HSRP та ін, які отримують інформацію про топологію і стан каналів зв'язку від інших маршрутизаторів у мережі.

1.3.1 Статична маршрутизація

Статична маршрутизація — це форма маршрутизації, коли маршрутизатор використовує налаштований вручну запис маршрутизації, а не інформацію з динамічного трафіку маршрутизації. У багатьох випадках статичні маршрути налаштовуються вручну адміністратором мережі шляхом додавання записів у таблицю маршрутизації, хоча це не завжди так. На відміну від динамічної маршрутизації статичні маршрути фіксовані і не змінюються

при зміні або переконфігурації мережі. Статична маршрутизація і динамічна маршрутизація є взаємовиключними.

Як динамічна, так і статична маршрутизація зазвичай використовуються на маршрутизаторі для максимізації ефективності маршрутизації і для забезпечення резервного копіювання у разі, якщо обмін інформацією при динамічній маршрутизації відсутній. Статична маршрутизація також може бути використана в мережах-заглушках або для забезпечення шлюзу останньої інстанції.

1.3.2 Динамічна маршрутизація

Протоколи динамічної маршрутизації — це один із типів протоколів маршрутизації, що має вирішальне значення для сучасних корпоративних мереж. Протоколи динамічної маршрутизації дозволяють маршрутизаторам автоматично додавати інформацію до своїх таблиць маршрутизації від підключених маршрутизаторів. За допомогою цих протоколівмаршрутизатори відправляють оновлення топології щоразу, коли топологічна структура мережі змінюється. Це означає, що користувачеві не потрібно турбуватися про підтримку мережевих маршрутів у актуальному стані.

Однією з основних переваг протоколів динамічної маршрутизації і те, що вони знижують необхідність управління конфігурацією. Недоліком є те, що це відбувається за рахунок виділення ресурсів, для підтримки їхньої роботи на постійній основі. OSPF, EIGRP та RIP вважаються протоколами динамічної маршрутизації.

1.3.3 Протоколи динамічної маршрутизації

Протокол маршрутної інформації або RIP — один із перших створених протоколів маршрутизації. RIP використовується як у локальних (LAN), такі глобальних (WAN) мережах, а також працює на прикладному рівні моделі OSI. Існує кілька версій RIP, включаючи RIPv1 та RIPv2. Оригінальна версіяабо RIPv1 визначає мережеві шляхи на основі IP-адреси призначення та кількості

хопів у дорозі.

RIPv1 взаємодіє з мережею, транслюючи свою IP-таблицю всім маршрутизаторам, підключеним до мережі. RIPv2 трохи складніше інадсилає свою таблицю маршрутизації на багатоадресне розсилання. RIPv2 також використовує автентифікацію для забезпечення більшої безпеки даних та вибирає маску підмережі та шлюз для майбутнього трафіку. Основне обмеження RIP полягає в тому, що максимальна кількість хопів становить 15, що робить його непридатним для великих мереж.

Протокол внутрішнього шлюзу (IGP) — це метод, що дозволяє мережним адміністраторам керувати маршрутизацією трафіку комп'ютерної мережі з однієї частини контрольованої мережі до іншої. Протокол внутрішнього шлюзу потрібен лише за наявності кількох маршрутизаторів, які необхідно долати, щоб трафік проходив мережею. Якщо IGP необхідний, мережа називається автономною системою (AC). IGP відповідає за те, щоб усі маршрутизатори в AC знали, як передавати трафік один через одного до пунктів призначення. Це відрізняється від протоколу зовнішнього шлюзу, який відповідає за напрямок трафіку, що виходить або входить до певної AC.

Протокол внутрішнього шлюзу вважається динамічним протоколом маршрутизації через його здатність автоматично оновлювати інформацію про маршрутизацію кожного маршрутизатора. У порівнянні зі статичним методом, при якому адміністратор повинен вручну оновлювати кожен маршрутизатор, IGP значно корисніший для великих мереж маршрутизаторів, статичний метод найкраще підходить для невеликих мереж із одним маршрутизатором. Існує кілька типів протоколів внутрішніх шлюзів, які поділяються на кілька загальних класифікацій.

Протокол маршрутизації з вектором відстані заснований на алгоритмі,в якому кожен маршрутизатор AC розраховує найкоротший шлях до пункту призначення шляхом підрахунку кількості інших маршрутизаторів, через які повинні пройти дані, щоб досягти пункту призначення. Маршрутизатори надсилають один одному повідомлення, щоб прокласти шлях, де кожен

зустрінутий маршрутизатор вважається одним "стрибком" на шляху. Шляхіз найменшою кількістю переходів маршрутизатор називає кращим маршрутом для пакетів даних. Якщо один із маршрутизаторів на цьомушляху виходить з ладу, маршрутизатор шукає наступний маршрут з найменшою кількістю хопів.

Один із недоліків полягає в тому, що протоколи внутрішніх шлюзів, засновані на маршрутизації вектором відстані, можуть мати проблеми з тимчасовою затримкою. Щоразу, коли до АС додається або видаляється новий маршрутизатор, всі маршрутизатори повинні знову сходитися визначення найкоротшого шляху. Затримка часу виникає тому, що маршрутизатори чекають три хвилини, перш ніж відмовитися від кращого шляху та почати процес збіжності з пошуку нового шляху. Дистанційно- векторна IGP-маршрутизація також не знає, чи є з'єднання з конкретним маршрутизатором швидше, ніж з іншим, і покладається лише на кількість переходів між маршрутизаторами як ідеальний шлях.

Інший тип протоколу внутрішнього шлюзу — це метод стану каналів. У протоколі зі станом з'єднання кожен маршрутизатор АС ділиться трохи більшою інформацією. У міру того, як кожен маршрутизатор спілкується з іншим, вони створюють базу даних, що містить інформацію про інші маршрутизатори АС, включаючи швидкість, з якою відбувається обмін даними між маршрутизаторами. Потім база даних обробляється в кожному маршрутизаторі і створюються таблиці маршрутизації. При використанні протоколу IGP зі станом зв'язків АС здатна зазнавати швидких змін і швидко переходити до інших маршрутизаторів, якщо один маршрут стає недоступним. Збіжність у протоколі маршрутизації зі станом зв'язків відбувається за секунди, а не за хвилини.

Протокол OSPF (Open Shortest Path First) є одним із сімейства протоколів IP-маршрутизації і є протоколом внутрішнього шлюзу (IGP) для Інтернету, що використовується для поширення інформації IP- маршрутизації в рамках однієї автономної системи в IP-мережі.

Enhanced Interior Gateway Routing Protocol — це вдосконалений

протокол маршрутизації за вектором відстані, заснований на принципах протоколу маршрутизації внутрішнього шлюзу (IGRP). Він має унікальну характеристику, яка покращує експлуатаційні можливості та швидкість конвергенції. Він може визначати найкоротший шлях вектора відстані та працює за принципом Interior Gateway Routing Protocol, безкласового протоколу маршрутизації. Він використовує такі метрики, як пропускна здатність, навантаження та затримку для розрахунку найкоротшого оптимального мережного маршруту. Це технологічно досконаліший протокол маршрутизації на основі вектора відстані. Для обміну інформацією за допомогою EIGRP, насамперед, маршрутизатори повинні стати сусідами EIGRP, потім EIGRP використовує багатоадресне розсилання для обміну інформацією.

В основі логіки Enhanced Interior Gateway Routing Protocol є концепція автономної системи. У системі, де кожен маршрутизатор повинен стати сусідом EIGRP, і кожна система, позначена як сусіди в рамках Enhanced Interior, Gateway Routing Protocol, матиме той самий налаштований номер системи.

Enhanced Interior Gateway Routing Protocol (EIGRP) — це протокол динамічної маршрутизації, який використовується для прийняття рішень та налаштування маршрутизаторів. EIGRP посилає тільки інкрементні оновлення, що в результаті знижує навантаження на маршрутизатори і кількість інформації, що передається. EIGRP — це класичний гібридний протокол, що підтримує безкласову маршрутизацію, він підтримує автоматичне та ручне підсумовування на інтерфейсі з підтримкою EIGRP. Він підтримує MD5-аутентифікацію на маршрутизаторах, що працюють під керуванням EIGRP, а також має максимальну кількість хопів, близьку до 255. EIGRP виконує балансування навантаження на шляху з рівною вартістю та шляху з нерівною вартістю.

Для виконання функцій EIGRP створюється три таблиці, а саме:

— таблиця сусідів;

— таблиця топології;

— таблиця маршрутизації.

Border Gateway Protocol або BGP — це протокол маршрутизації в Інтернеті, який класифікується як протокол вектора шляху відстані. BGP був розроблений для заміни EGP із децентралізованим підходом до маршрутизації. Алгоритм вибору кращого шляху BGP використовується для вибору кращих маршрутів передачі пакетів даних. Якщо у вас немає жодних налаштувань користувача, то BGP буде вибирати маршрути з найкоротшим шляхом до місця призначення.

Однак багато адміністраторів бажають змінювати рішення щодо маршрутизації відповідно до своїх потреб. Алгоритм вибору кращого шляху маршрутизації може бути налаштований за допомогою зміни атрибута BGP cost community.

BGP надсилає оновлені дані таблиці маршрутизаторів лише тоді, коли щось змінюється. В результаті відсутнє автоматичне виявлення змінтопології, що означає, що користувач має налаштовувати BGP вручну. З точки зору безпеки, протокол BGP може бути автентифікований, тому лишеавторизовані маршрутизатори можуть обмінюватися даними один з одним.

Intermediate System-to-Intermediate System (IS-IS) — це протокол IP-маршрутизації зі станом каналу та протокол IGPP, що використовується в Інтернеті для передачі інформації IP-маршрутизації. IS-IS використовує модифіковану версію алгоритму Дейкстри. Мережа IS-IS складається з низки компонентів, включаючи кінцеві системи (пристрої користувача), проміжні системи (маршрутизатори), області та домени.

У IS-IS маршрутизатори організовані в групи, названі областями, а кілька областей об'єднуються в домен. Маршрутизатори всередині області відносяться до рівня 1, а маршрутизатори, що з'єднують сегменти разом, класифікуються як рівень 2. В IS-IS використовуються два типи мережевих адрес: точка доступу до мережевої служби (NSAP) і назва мережевої організації (NET).

1.4 Віртуальна приватна мережа VPN

Віртуальна приватна мережа, більш відома як VPN, забезпечує конфіденційність та анонімність в Інтернеті, створюючи приватну мережу з публічного інтернет-з'єднання. VPN маскує вашу адресу інтернет-протоколу (IP), тому ваші дії в мережі практично неможливо відстежити. Найголовніше, VPN-сервіси встановлюють безпечні та зашифровані з'єднання, що забезпечують більшу конфіденційність, ніж навіть захищена точка доступу Wi-Fi.

Віртуальна приватна мережа — це ключовий інструмент забезпечення конфіденційності, який слід використовувати, під час виходу в Інтернет із громадського місця, наприклад, з кав'ярні, холу готелю або будь-якого іншого місця, де є доступ до безкоштовного публічного Wi-Fi.

VPN створює тунель, який приховує ваші дії в Інтернеті, включаючи посилання, за якими ви переходите, або файли, які ви завантажуєте, щоб кіберзлочинці, компанії, урядові установи або інші шпигуни не могли їх побачити.

VPN створює тунель даних між вашою локальною мережею івихідним вузлом в іншому місці, яке може знаходитися за тисячі кілометрів,створюючи враження, що ви знаходитесь в іншому місці. Ця перевага забезпечує свободу в Інтернеті або можливість доступу до улюблених програм та веб-сайтів у дорозі.

VPN використовує шифрування для скремблювання даних під час їх передачі через мережу Wi-Fi. Шифрування робить дані не можливими для читання. Безпека даних особливо важлива під час використання публічної мережі Wi-Fi, оскільки вона не дозволяє іншим користувачам мережі підслуховувати вашу інтернет-активність.

У конфіденційності є й інша сторона. Без VPN ваш інтернет- провайдер може знати всю історію ваших відвідувань. З VPN ваша історія пошуку прихована. Це тому, що ваша веб-активність буде пов'язана з IP-адресою сервера VPN, а не з вашою. У постачальника послуг VPN можуть бути сервери

по всьому світу. Це означає, що ваша пошукова активність може здатися, що відбувається на будь-якому з них. Пам'ятайте, що пошукові системи також відстежують історію ваших пошуків, але вони будуть пов'язувати цю інформацію з IP-адресою, яка не є вашою. Знову ж таки, VPN забезпечить конфіденційність вашої діяльності в Інтернеті.

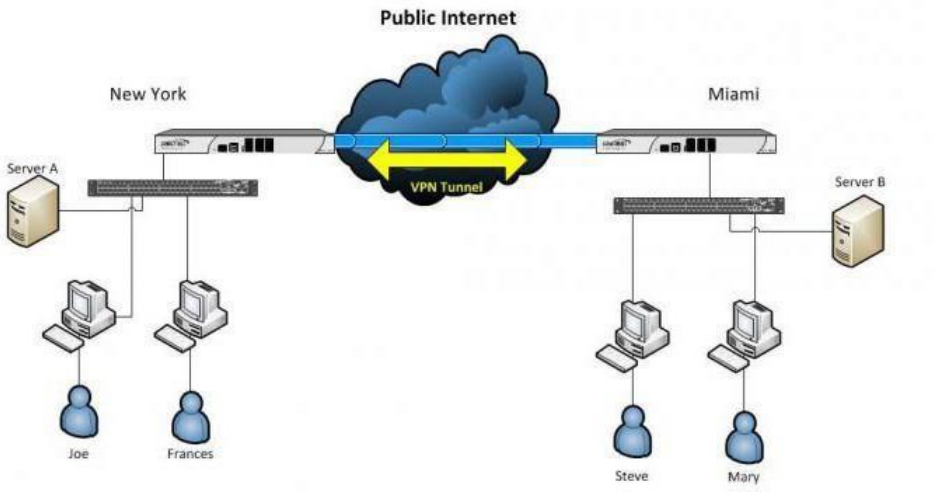

Рисунок 1.3 — Базовий вигляд використання VPN

1.5 Мережева технологія Ethernet

Ethernet — це насамперед стандартний протокол зв'язку, який використовується для створення локальних мереж. Він передає та приймає дані по кабелях. Це полегшує мережевий зв'язок між двома або більше різними типами мережевих кабелів, наприклад, з мідного на оптоволоконний та навпаки. Медіаконвертер Ethernet — це пристрій, здатний підтримувати зв'язок між двома різними типами мережевих середовищ. Медіаконвертер складається із плати в корпусі. Карта зазвичай має два порти для підключення двох різних типів мережевих кабелів.

Мережа Ethernet використовується для створення локальної мережі та підключення кількох комп'ютерів або інших пристроїв, таких як принтери, сканери тощо. У провідній мережі це робиться за допомогою оптоволоконних кабелів, а в бездротовій мережі — за допомогою бездротової мережевої технології. У мережі Ethernet використовуються різні топології, такі як зірка,

шина, кільце та інші.

Опто-волоконні медіаконвертори з'єднують Ethernet-пристрій із мідними кабелями CAT5/CAT6 з опто-волоконним кабелем. Мережа Ethernet зазвичай діє у 10-кілометровій периферії. Перехід на оптоволоконний кабель значно збільшує відстань, що покривається мережею. Ось деякі типи мереж Ethernet:

— Fast Ethernet досить високошвидкісний інтернет, він може передавати або приймати дані зі швидкістю близько 100 Мбіт/с. Цей тип мережі зазвичай підтримується витою парою або кабелем CAT5. Якщо до мережіпідключено ноутбук, камеру або будь-який інший пристрій, вони працюють на швидкості 10/100Base Ethernet і 100Base на стороні оптоволоконного з'єднання.

— Gigabit Ethernet передає дані з вищою швидкістю — близько 1000 Мбіт/с або 1 Гбіт/с. Гігабітна швидкість є удосконаленням Fast Ethernet, який поступово виводиться із вживання. У мережах цього типу всі чотири парив кабелі витої пари роблять свій внесок у швидкість передачі даних. Цей тип мережі знаходить широке застосування у системах відеодзвінків, у яких використовуються кабелі CAT5e чи інші сучасні кабелі. Для протяжних мереж на відстань до 500 м можуть використовуватися оптоволоконні кабелі 1000Base SX для багатомодових, а також 1000Base LX для одномодових систем.

— 10-Gigabit Ethernet — це ще більш досконалий та високошвидкісний тип мережі зі швидкістю передачі даних 10 гігабіт/сек. Він підтримується кабелями крученої пари CAT6a або CAT7, а також оптоволоконними кабелями. При використанні оптоволоконного кабелю область дії мережі може бути розширена приблизно до 10000 метрів.

— Switch Ethernet потребує комутатора або концентратора. Крім того, замість крученої пари в цьому випадку використовується звичайний мережний кабель. Мережеві комутатори використовуються для передачі даних від одного пристрою до іншого, не перериваючи роботу інших пристроїв в мережі.

2 ПРОЕКТУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ

2.1 Огляд компанії та її приміщень

Vodafone — оператор мобільного зв'язку у Німеччині зі штаб-квартирою в Дюссельдорфі. Він надає послуги мобільного зв'язку, LTE, 5G, кабельного інтернету, стаціонарних телефонів, кабельного телебачення та IPTV. За даними на третій квартал 2021 року, Vodafone GmbH обслуговує понад 31 мільйон клієнтів мобільного зв'язку в Україні.

Мережа Vodafone Germany обслуговує клієнтів у мережах GSM та LTE (Long Term Evolution). У липні 2019 року Vodafone почав надавати послуги 5G.

Центральний офіс — офіс в якому знаходиться керівництво підприємства, місце перебування центрального апарату компанії або підприємства, де розміщуються топ-менеджмент, дирекція, секретаріат та інші важливі адміністративні підрозділи. Місце розташування головного офісу вказується під час реєстрації фірми. Деякі надання важливості називають свій головний офіс штаб-квартирою. [1]

Центральний офіс компанії знаходиться в місті Києві. Він розміщується на двох поверхах.

Дана комп'ютерна мережа спроектована згідно з усіма потребами компанії.

2.1.1 Перший поверх

На першому поверсі розміщені: відділ бухгалтерії, відділ кадрів, приймальня, кабінет директора фірми, кабінет заступника директора,кабінет для нарад, кабінет головного інженера.

План першого поверху наведено на рисунку 2.1.

Рисунок 2.1 — План першого поверху

Під відповідними номерами розташовані відповідні відділи:

1) кабінет для нарад;
2) відділ кадрів;
3) відділ бухгалтерії;
4) приймальня;
5) кабінет головного інженера;
6) кабінет заступника директора;
7) кабінет директора фірми.

Бухгалтерія — структурний підрозділ суб'єкта господарювання, що призначений для ведення бухгалтерського обліку. Бухгалтерія забезпечує відповідних користувачів, в першу чергу керівництво, повною та неупередженою інформацією про фінансове становище, результатидіяльності та грошових коштів підприємства.[2]

У відділі бухгалтерії розміщено три персональних комп’ютерів, два принтери та два IP-телефони.

Відділення кадрів компанії займається навчанням і розвитком своїх працівників, які вважаються одними з найбільш важливих ресурсів компанії.

Відділ кадрів призваний слідкувати за тим, щоб співробітникикомпанії отримували відповідне управління, відповідну компенсацію та ефективне

навчання. Відділ також відповідає за підбір персоналу, прийом на роботу, звільнення та надання льгот.

У відділі кадрів розміщено три персональних комп’ютери, двапринтери та один IP-телефони.

У приймальні розміщено один персональний комп’ютер, один IP-телефон та один принтер.

Кабінет для нарад- це приміщення, зазвичай призначене для того, щоб люди збиралися разом, часто неформально, для проведення нарад, обговорення питань, визначення пріоритетів і прийняття рішень.

Переговорні кімнати бувають різних розмірів вони можуть бути невеликими, щоб розмістити двох людей, які проводять співбесіду, або велику кількість людей для колективного обговорення.

У кабінеті для нарад розміщено один переснальний комп’ютер.

Кабінетом директора називається приміщення, створене спеціально до ухвалення відповідних рішень. Кабінет продуманий до дрібниць, адже місце директора має бути максимально комфортним та зручним, а також сприяти зміцненню образу компанії серед колег та конкурентів.

У кабінеті директора розміщено один переснальний комп’ютер та IP-телефон.

У кабінеті заступника директора розміщено один переснальний комп’ютер та IP–телефон.

Головниий інженеер — це один з керівників компанії, що відповідаєза технічну політику і напрями технічного розвитку підприємства в умовах ринкової економіки.

У кабінеті головного інженера розміщено один переснальний комп’ютер та IP-телефон.

2.1.2 Другий поверх

На другому поверсі розміщені: серверна кімната, центр обробки викликів, кімната відпочинку, кабінет головного економіста та відділ охорони

праці. План другого поверху наведено на рисунку 2.2.

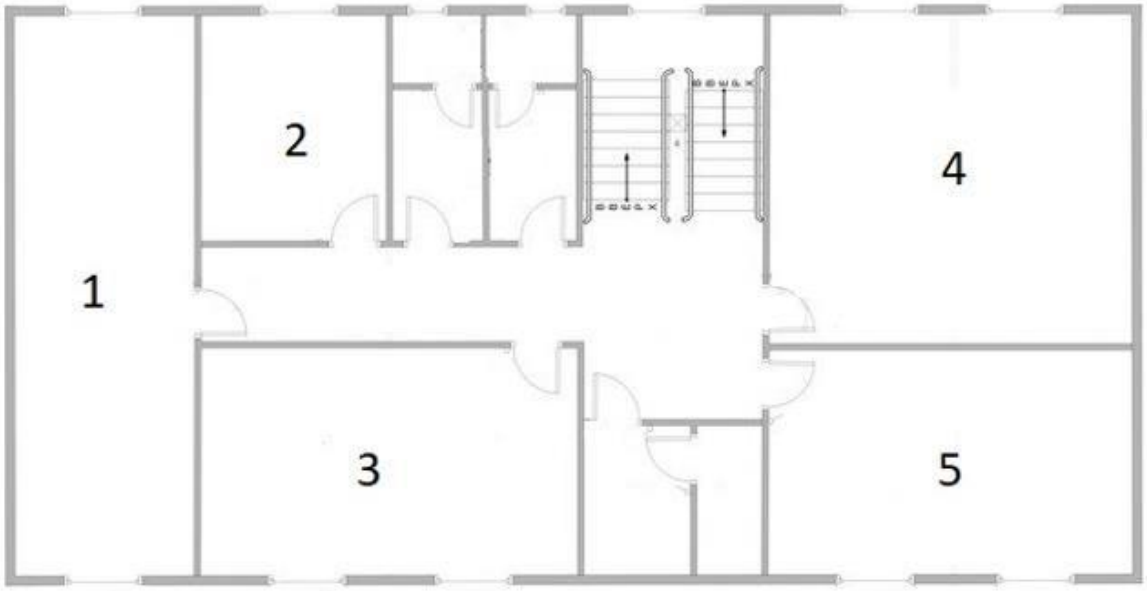

Рисунок 2.2– План другого поверху

Під відповідними номерами розташовані відповідні відділи:

1) кімната відпочинку;
2) кабінет головного економіста;
3) відділ охорони праці;
4) центр обробки викликів;
5) серверна кімната.

Центр обробки викликів — це централізований відділ, який обробляє вхідні та вихідні дзвінки від існуючих та потенційних клієнтів. Центри обробки викликів розташовуються або всередині організації, або передаються аутсорсинг інший компанії, що спеціалізується на обробці викликів.

Контакт-центри орієнтовані на один канал зв'язку — телефон. Контакт-центри надають підтримку за додатковими каналами, такими як електронна пошта, чат, веб-сайти та програми. Контакт-центр може містити один або кілька центрів обробки дзвінків.

У центрі обробки викликів розміщено п’ять персональних комп'ютерів, п'ять IP–телефонів та три принтери.

Кімнати відпочинку зазвичай діляться на два типи: ті, де можна розмовляти, і ті, де потрібно поводитися тихо. У кімнатах зазвичай є крісла,

шезлонги, бобові мішки, а в деяких випадках — підвісні капсули або гамаки, щоб ви могли прилягти, покласти ноги та розслабитися. Кімната релаксації - це місце, де можна або зануритися в спокійний стан духу перед роботою, або насолодитися ефектом прекрасного відпочинку.

У кімнаті відпочинку розміщено один персональний комп’ютер та IP-телефон.

У кабінеті головного економіста розміщено один персональний комп’ютер та IP-телефон.

Відділ охорони праці керується федеральними законами про працю, що гарантують справедливі права працівників, безпечні та здорові умови праці, включаючи мінімальну погодинну оплату праці та оплату понаднормових, захист від дискримінації у сфері зайнятості та страхування по безробіттю.

У відділі охорони праці розміщено два персональних комп’ютери, два IP–телефони та один принтер.

Серверна кімната — це приміщення, призначене для безперервної роботи комп'ютерних серверів.Комп'ютери в серверних кімнатах зазвичай є безголовими системами, якими можна керувати віддалено за допомогою перемикача KVM або програм віддаленого адміністрування, таких як Secure Shell, VNC. У серверній кімнаті розміщено один персональний комп’ютер та сервер.

2.2 Розробка логічної структури мережі

Логічна структуризація мережі — це розбиття мережі на окремі частини з локалізованим трафіком. Логічні зв’язки являють собою шляхи проходження інформації по мережі; вони створюються завдяки конфігуруванню комунікаційного обладнання. На рисунку 2.3 зображена логічна структура компанії.

Рисунок 2.3 — Логічна структура компанії

Призначення адрес компонентам мережі відбувається за допомогою сервісу DHCP, на центральному маршрутизаторі. Також мережа буде розбита на підмережі та Vlan у відповідності з фізичним та логічним розсташуванням її елементів.

Розрахунок адрес відбудеться починаючи з адреси 178.95.1.0. Оскільки дана WAN проектується з прямим виходом до мережі Інтернет , то адреси повинні бути публічними. Для більш гнучкого виконування адміністрування використано маски змінної довжини.

Таблиця 2.1 — Розбиття адресного простору на підмережі

Назва підрозділу	Кількість необхідних IP–адрес	128	64	32	16	8	4	2	1	Префікс
Персональні комп’ютери	21	1	1	1	0	0	0	0	0	27
IP-телефони	15	1	1	1	1	0	0	0	0	28
Принтери	9	1	1	1	1	0	0	0	0	28
Сервер	1	1	1	1	1	1	1	0	0	30

У таблиці 2.1 наведена кількість необхідних IP–адрес та маски які для них будуть використовуватися.

Таблиця 2.2 — Розподіл адрес по підмережах

	Мережа	Перша	Остання	Широкомовна	Маска
Персональні комп’ютери	178.95.1.0	178.95.1.1	178.95.1.30	178.95.1.31	255.255.255.224
IP-телефони	178.95.2.0	178.95.2.1	178.95.2.14	178.95.2.15	255.255.255.240
Принтери	178.95.3.0	178.95.3.1	178.95.3.14	178.95.3.15	255.255.255.240
Сервер	178.95.4.0	178.95.4.1	178.95.4.2	178.95.4.3	255.255.255.252

У таблиці 2.2 наведено адреси підмереж, доступні адреси що використовуватимуться та маски.

2.3 Реалізація VLAN до мережного обладнання

Відповідно до поставленого завдання того чи іншого мережного обладнання було створено таблицю 2.3, з відповідністю VLAN до певного типу обладнання.

Таблиця 2.3 — Відповідність VLAN до певного обладнання

Обладнання:	Відповідність VLAN до мережного обладнання	
	Назва VLAN	Номер VLAN
Персональні комп’ютери	PC	10
IP-телефони	Telephone	20
Принтери	Printer	30
Сервер	Server	40

VLAN (віртуальна локальна мережа) — це логічне угрупування пристроїв в одному широкомовному домені. VLAN зазвичай налаштовуються на комутаторах шляхом розміщення деяких інтерфейсів в один широкомовний

домен, а деяких інтерфейсів — в інший.

VLAN можуть розповсюджуватися на кілька комутаторів, при цьому кожна VLAN розглядається як власна підмережа або широкомовний домен. Це означає, що кадри, що передаються в мережу, комутуватимуться лише між портами однієї віртуальної мережі.

VLAN діє як фізична локальна мережа, але дозволяє об'єднувати хости в один широкомовний домен, навіть якщо вони не підключені до одного комутатора. Ось основні причини, через які було використано віртуальні локальні мережі:

— VLAN збільшує кількість широкомовних доменів при зменшенні їх розміру;

— VLAN знижують ризики безпеки за рахунок зменшення кількості хостів, які отримують копії кадрів, що передаються комутаторами;

— можливість утримувати хости, що зберігають конфіденційні дані, в окремій мережі VLAN для підвищення безпеки;

— можливість створювати гнучкіші мережеві схеми, які групують користувачів по відділах, а не за фізичним розташуванням.

2.4 Вибір та порівняння мережевого обладнання

Мережеве обладнання використовується для об'єднання, поділу, перемикання, посилення або направлення пакетів інформації через комп'ютерну або телекомунікаційну мережу. У цю область продукції входять концентратори, комутатори, маршрутизатори, мости, шлюзи, мультиплексори, трансівери та брандмауери. Крім типу пристрою, мережеве обладнання визначається протоколом (наприклад, Ethernet) та типом порту або інтерфейсу (наприклад, T1).

Мережне обладнання з'єднує пристрої так, щоб між ними можна було обмінюватись даними. До поширених топологій комп'ютерних мереж відносяться шина, кільце, зірка, дерево та сітка. Також використовуються гібридні топології.

Комп'ютерні мережі обробляють дані відповідно до протоколів, які є основними механізмами мережевих комунікацій. Мережеві протоколи визначають програмні атрибути передачі даних, включаючи структуру пакетів і інформацію, що міститься в них. Залежно від типу мережі, пакети можуть називатися блоками, осередками, кадрами або сегментами. Мережеві протоколи можуть також вказувати деякі або всі експлуатаційні характеристики мережного обладнання, на якому вони працюють.

2.4.1 Комутатори

Комутатор з'єднує пристрої в мережі і пересилає пакети даних на ці пристрої і назад. На відміну від маршрутизатора, комутатор надсилає дані лише на один пристрій, для якого він призначений (це може бути інший комутатор, маршрутизатор або комп'ютер користувача), а не в мережу з декількох пристроїв.

Для порівняння було обрано чотири моделі комутаторів.

EdgeSwitch - це повністю керований гігабітний комутатор з підтримкою PoE+, що забезпечує надійну продуктивність та інтелектуальну комутацію для зростаючих мереж. EdgeSwitch пропонує широкий набір передових функцій та протоколів комутації другого рівня, а також забезпечує можливість маршрутизації третього рівня.

Рисунок 2.4 — Комутатор EdgeSwitch PoE+ 48

Особливості:

— 48 гігабітних портів RJ45;

— 2 порти SFP+;

— 2 порти SFP;

— послідовний консольний порт;

— пропускна спроможність без блокування 70 Гбіт/с;

— комутаційна спроможність 140 Гбіт/с;

— швидкість переадресації 104,16 Mpps;

— максимальне енергоспоживання 500W;

— підтримує POE+ IEEE 802.3at/af та пасивне PoE 24 В;

— монтований у стійку.

Cisco 350X — це нова лінійка керованих комунаторів Ethernet, які забезпечують широкі можливості, необхідні для підтримки більш вимогливого мережевого середовища, за дуже доступною ціною.

Моделі SG350X забезпечують 24 або 48 портів Gigabit і Multigigabit Ethernet з 10-гігабітними вихідними каналами. Моделі Cisco 350XG надають 12, 24 або 48 портів 10 Gigabit Ethernet, забезпечуючи надійну основу для поточних бізнес-програм, а також тих, які ви плануються в майбутньому. Крім того, ці комутатори легко розгорнути та керувати ними без залучення великого штату IT-фахівців.

Рисунок 2.5 — Комутатор L3 Gigabit Ethernet PoE Cisco SG350X-24MP-K9-EU

Основні характеристики:

Пам'ять

— Flash 256 Мб;

— ОЗУ пам'ять 512 Мб;

— Пакетний буфер 1,5 Мб;

— CPU 800 MHz (dual-core) ARM.

Продуктивність

— Матриця комутації 128 Гбіт/с;

— Таблиця MAC адрес до 16000 MAC адрес;

— Jumbo frames до 9K (9216) bytes supported;

— Комутація Мпакет/с 95,23 MPPS.

Комутатор L3 Gigabit Ethernet HP 3800-24G-2SFP+ (J9575A) є керованим комутатором третього рівня від компанії HP з можливістю установки в стійку. Обладнаний великою кількістю різних інтерфейсів, до яких входять: основні 24 гігабітні LAN-порти, 2 десяти-гігабітні порти SFP+, 2 порти з роз'ємом RJ-45 (один послідовний і один для зовнішнього управління), 1 слот для роботи у фізичному стеку, а також 2 додаткові слоти для портів. Облаштований двома видами пам'яті – ОЗУ на 2048 МБ та Флеш на 4096 МБ. Має таблицю адрес MAC на 10 тисяч записів. Технологія комутаційної матриці портів дозволяє забезпечити швидкість передачі в 88 Гбіт/с. Також порти підтримують технологію автовизначення типу кабелю (звичайний/кросоверний) Auto-MDI/MDI(X). Як засоби управління присутні WEB-інтерфейс з доступом до налаштувань через браузер, доступ по Telnet (локальний/віддалений), протокол SNMP.

Рисунок 2.6 — Комутатор L3 Gigabit Ethernet HP 3800-24G-2SFP+ (J9575A)

Комутатор Smart Fast Ethernet D-Link DES-1100-26 з металевим корпусом та можливістю установки в 19-дюймову стійку оснащений 26 портами. 24 порти 10/100 Ethernet/Fast Ethernet Base-Tx та два комбінованих порти 10/100/1000 Base-T/SFP. Підтримують стандарти 802.3/u/ab/x, функцію MDI/MDI-X (автовизначення кабелю + можливість підключати будь-який кабель до порту), а також автоматичне узгодження швидкості. Комутатор має індикатори на кожен із портів та окремий індикатор, що показує стан його живлення.

Оснащений великим функціоналом та програмним забезпеченням другого рівня управління, функціоналом VLAN (віртуальна локальна мережа) для її проведення та управління, а також функцією QoS для пріоритезації різних видів трафіку. Керувати мережею та комутатором можливо через WEB-інтерфейс (за підтримки протоколу IPv4) та через утиліту SmartConsole. Також другий рівень управління дозволяє встановлювати швидкість, один з двох режимів дуплексу та керувати потоком даних. Для надійності можна резервувати та відновлювати конфігураційний файл мережі через протокол HTTP.

Рисунок 2.7 — Комутатор Smart Fast Ethernet D-Link DES-1100-26

Для даної комп’ютерної мережі було прийнято рішення взяти комутатори L3 Gigabit Ethernet HP 3800-24G-2SFP+ (J9575A) та Smart Fast Ethernet D-Link DES-1100-26.

В порівнянні зі своїми аналогами вони показали себе більш багатофункціональними, простими в управлінні та конфігуруванні, мають високий рівень безпеки.

Таблиця 2.4 — Основні характеристики комутаторів

	EdgeSwitch PoE+ 48	Cisco SG350X-24MP-K9-EU	HP 3800-24G-2SFP+ (J9575A)	Smart Fast Ethernet D-Link DES-1100-26
Пропускна здатність, Гбит/с	70	128	88	80
Об’єм ОЗП, Мб	512	512	2048	1024
Объем flash–пам’яті, Мб	256	256	4096	1024
Таблица MAC адрес	8000	16000	10240	4000
Комутаційна матриця Гбит/с	16	32	128	8.8

2.4.2 Маршрутизатор

В якості основного активного мережного обладнання використовуємо маршутизатори. Працюють на мережевому рівні мережевих протоколів. Використовується для зовнішнього світу і для локальної мережі. У локальній мережі основний роутер може роздавати IP–адреси по DHCP, контролювати допустимі IP-адреси.

Маршрутизатор — це пристрій, що з'єднує дві або більше мереж або підмереж з комутацією пакетів. Він виконує дві основні функції: керування трафіком між цими мережами шляхом пересилання пакетів даних за призначеними IP-адресами та забезпечення можливості використання одного інтернет-з'єднання декількома пристроями.

Існує кілька типів маршрутизаторів, але більшість маршрутизаторів передають дані між локальними та глобальними мережами (LAN). Локальна мережа — це група підключених пристроїв, обмежена певною географічною зоною. Для локальної мережі зазвичай потрібний один маршрутизатор.

WAN, навпаки, являє собою велику мережу, поширену на широкій географічній території. Наприклад, великі організації та компанії, які працюють у кількох місцях по всій країні, потребують окремих локальних мереж для кожного місця, які потім підключаються до інших локальних мереж, утворюючи WAN. Оскільки глобальна мережа розподілена великою територією, часто потрібно кілька маршрутизаторів і комутаторів.

Для порівняння характеристик було обрано два маршрутизатори MikroTik RB1100Dx4 та Cisco ISR4331/K9. В таблиці 2.5 наведено характеристики маршрутизатора MikroTik RB1100Dx4.

Таблиця 2.5 — Характеристики маршрутизатора MikroTik RB1100Dx4

Характеристики	Опис
Тип пристрою	Маршрутизатор
Форм–фактор	Настільний– modular – 1U
Операційна система	RouterOS
Ширина	444 мм
Довжина	148 мм
Висота	47 мм
Матеріал корпуса	Метал
Об'єм RAM	1024 MB
Об'єм ROM	128 MB
Частота процесора	1400 MHz
Максимальна споживана потужність	25 W
Мінімальна робоча температура	-40 ° C

Продовження таблиці 2.5

Максимальна робоча температура	+70 ° C
Інтерфейси	13 × 10/100/1000 Mbit/s Ethernet RJ45 Auto-MDI/X 1 × microSD slot 1 × DB9 RS232C
Підтримувані стандарти	UL 60950–1, CAN/CSA–C22.2 No. 60950–1, IEC 60950–1, EN 60950–1, FCC Part 15.247, 15.407, EN 300.328
Вага	1500 г

Рисунок 2.8 — Маршрутизатор MikroTik RB1100Dx4

В таблиці 2.6 Наведено характеристики маршрутизатора Cisco ISR4331/K9.

Таблиця 2.6 — Характеристики маршрутизатора Cisco ISR4331/K9.

Характеристики	Опис
Тип пристрою	Маршрутизатор
Форм–фактор	Настільний– modular – 1U
Операційна система	RouterOS
Ширина	445 мм
Довжина	438 мм
Висота	44 мм
Матеріал корпуса	Метал

Продовження таблиці 2.6

Об'єм RAM	4 ГБ (Установлено) / 16 ГБ (максимально)
Частота процесора	47-63 Гц
Споживаний струм	3-3.1 А
Максимальна споживана потужність	250 W
Мережева технологія	10/100/1000Base-T
Технологія Ethernet	Gigabit Ethernet
Слоти розширення	Модуль мережевого інтерфейсу (NIM), картка інтегрованих послуг (ISC), SFP
Технологія пам'яті	DDR3 SDRAM
Функції безпеки	IPsec, VPN, рівень безпечного сокета (SSL), розширена перевірка додатків, контроль додатків, Secure Shell (SSH), контроль доступу до мережі (NAC), VPN із підтримкою голосового та відеозв’язку, GET, Flex VPN, IOS XE, NBAR, AAA, PKI, ACL
Мінімальна робоча температура	-40 ° C
Максимальна робоча температура	+70 ° C
Вага	2100 г

Рисунок 2.9 — Маршрутизатор Cisco ISR4331/K9

Характеристики даних маршрутизаторів цілком задовольняють наші вимоги щодо побудови корпоративної мережі. Однак порівнявши характеристики маршрутизаторів, пристрій компанії Cisco краще відповідає потребам компанії, для якої проектується дана комп'ютерна мережа.

2.4.3 Серверне обладнання

Сервера — це "комп'ютер, який надає послуги, ресурси та дані іншим комп'ютерам".

Сервери більше схожі на "суперкомп'ютери", призначені для цілодобової роботи. Надаючи інформацію іншим комп'ютерам або пристроям, відомим як "клієнти" у глобальній або локальній мережі, сервери можуть виконувати програми. Функції серверів різні, але в кінцевому підсумку вони є постачальником контенту або проміжною ланкою, що дозволяє виконувати більшість завдань на комп'ютері, таких як спілкування з людьми, відвідування веб-сторінок або доступ до мережних дисків.

Хоча більшість людей рідко вступає в безпосередній контакт із серверами, майже всі тією чи іншою мірою покладаються на них. Вони грають надзвичайно важливу роль у нашому повсякденному житті, будь то робота, навчання або розваги. Більша частина Інтернету залежить від серверів, оскільки вони надають більшість послуг або інформації, які ми запитуємо з настільних комп'ютерів, планшетів та мобільних пристроїв.

Сервер налаштований на отримання завдань та запитів від "клієнтів" у межах свого мережевого з'єднання та відповідає відповідними даними. Сервери знають, що запит є справжнім завдяки IP-адресі, числовій адресі, яка відповідає комп'ютеру, призначеному в мережі. Потім інформація доставляється користувачам за допомогою IT-обладнання, наприклад мережевих кабелів.

Усередині сервера компоненти складаються з різних елементів IT-обладнання, які працюють разом для забезпечення функціональних можливостей. У кожного підприємства свої вимоги до IT. Наприклад, центр

обробки даних великого підприємства потребує набагато більше енергії, ніж серверу в офісі. Компоненти сервера можуть бути оптимізовані або налаштовані для задоволення цих специфічних потреб.

В якості серверного обладнання було обрано сервер Dell EMC PowerEdge R740. Зовнішній вигляд сервера зображено на рисунку 2.10.

Рисунок 2.10 — Сервер Dell EMC PowerEdge R740

Сервер Dell R740 представляє архітектуру Dell з оновленим інтегрованим контролером віддаленого доступу Dell 9.0 (iDRAC9) для покращеного локального та віддаленого керування системою. Нові опції постійної пам'яті також дозволяють збільшити продуктивність у десять разів. Ідеальні робочі навантаження для цієї платформи включають:

— інфраструктура віртуальних робочих столів (VDI);

— приватна хмара;

— штучний інтелект;

— машинне навчання.

У цій системі підтримуються один або два процесори Intel Xeon Scalable першого або другого покоління, які забезпечують збільшення кількості обчислювальних ядер на 27% та пропускну здатність на 50%. Вибрати можна один процесор Bronze, Silver, Gold або Platinum із 28 ядрами на процесор та 56 загальними ядрами у двопроцесорній конфігурації. У цій системі підтримуються високопродуктивні графічні процесори Nvidia чи FPGA.

Сервер Dell EMC R740 підтримує модулі пам'яті з реєстрацією (RDIMM), зменшенням навантаження (LRDIMM) та незалежні модулі пам'яті

(NVDIMM-N). Він підтримує 24 слоти пам'яті у двопроцесорній конфігурації і лише 12 — в однопроцесорній.

У двопроцесорній конфігурації із завантаженням усіх 24 слотів модулями RDIMM або LRDIMM об'ємом 128 ГБ система підтримуватиме максимум 3 ТБ. Модулі NVMe DIMM не підтримуються з одним процесором і обмежені лише 12 слотами для модулів пам'яті максимальним об'ємом 192 ГБ. Однак модулі NVDIMM можуть працювати в парі тільки з модулями Registered DIMM в слотах, що залишилися. Залежно від вибраного процесора Intel Xeon Scalable 1-го або 2-го покоління максимальна швидкість пам'яті становитиме 2666 МГц або 2933 МГц відповідно.

Існує дві конфігурації шасі: одна з 16 х 2,5-дюймовими дисками, інша з 8 х 3,5-дюймовими дисками, що підтримують максимум 60 ТБ або 80 ТБ відповідно. Підтримуються жорсткі та твердотільні диски SAS, SATA та Nearline SAS. Змішування різних типів дисків не підтримується. Є кілька додаткових пристроїв зберігання, які можна встановити, включаючи тонкий оптичний диск SATA та модуль Dual SD Card/vFlash з двома трьома картами micro SD – двома для IDSDM та однією vFlash для підтримки відмовостійкого гіпервізора. У стандартну комплектацію системи входить програмний RAID-контролер S140, але знову ж таки у вас є опції, що підтримують більше конфігурацій RAID і збільшену пропускну здатність. Для підтримки зовнішніх жорстких дисків рекомендує Dell PERC H840.

На сервері Dell R740 підтримується підсистема зберігання даних Dell PowerEdge Boot Optimized Storage Subsystem або BOSS. BOSS використовує один або два оптимізовані для завантаження накопичувача M.2 на карті PCIe, які можуть бути налаштовані на режим "pass-thru" або за наявності двох встановлених пристроїв можуть бути налаштовані на апаратний RAID 1 у дзеркальному режимі для відмови від завантаження. Це обладнання є особливо привабливим для адміністраторів, які використовують Hyper-Converged Infrastructure (HCI) або Software Defined Storage (SDS), що дозволяють відокремити ОС від сховища. Конфігурація BOSS здійснюється через системний BIOS (F2), а також інтегрована із Dell OpenManage.

Рисунок 2.11 — Зображення задньої частини системи сервера Dell PowerEdge R740

У Dell PowerEdge R740 підтримується вісім слотів розширення PCIe Gen 3.0, що на один більше, ніж у попередньому поколінні R730. Залежно від потреб, можна вибрати кілька різних варіантів стояків, які підтримуватимуть додаткові мережеві карти, HBA, зовнішні контролери HD/RAID та графічні процесори. Фактично система підтримує шість карт потужністю 150 Вт або три карти прискорювача потужністю 300 Вт. Оснащена трьома GPU подвійною шириною, система буде підтримувати на 50 більше розгортань VDI, ніж R730. Опції дочірніх мережевих плат (NDC) включають швидкості підключення 1GbE, 10GbE та 25GbE з двома та чотирма портами. Щоб забезпечити додаткову пропускну здатність, адміністратори можуть встановлювати окремі карти PCIe.

Система має кіберстійку архітектуру та поставляється у стандартній комплектації з iDRAC9 з LifeCycle Controller Express, який пропонує покращені функції автоматизації та безпеки. OpenManage також забезпечує легку інтеграцію з VMware vSphere, Microsoft System Center та Nagios. Також є покращена рамка Quick Sync 2 з вбудованою комунікацією ближнього поля (NFC), яку можна використовувати зі смартфонами та планшетами на базі Android та iOS з можливостями NFC для отримання оперативної інформації про стан сервера та мережі. Нові та покращені функції безпеки включають блокування конфігурації, автентифікацію вбудованої прошивки, безпечне завантаження та стирання системи.

Таблиця 2.7 — Характеристики сервера Dell PowerEdge R740

Характеристики	Опис
Доступні типи ядра процесора	28 або 56
Максимальна пам'ять	3 ТБ
Слоти для пам'яті	24 слоти DIMM
Пам'ять	DDR4 DIMM
Порти	4 x 1GE, 2 x 10GE + 2 x 1GE, 4 x 10GE або 2 x 25GE
Мережевий контролер	PERC H330, H730p, H740p, HBA330, програмний RAID
Відсіки для дисководів	До 16 накопичувачів 2,5" SAS/SATA/SSD, максимум 60 Тб До 8 накопичувачів 3,5" SAS/SATA, максимум 80 Тб
Живлення	Titanium 750 Вт

2.4.4 IP-АТС

Для телефонної мережі обрано Zycoo CooVox U20 A202.

Zycoo CooVox U20 A202 — міні IP АТС, оптимізована для малого та середнього бізнесу. Ця телефонна система дозволяє здійснити до 30 реєстрацій користувача і має два вбудовані аналогові телефонні порти - FXO. Крім традиційних функцій, міні-АТС надає багато передових функцій, таких як доступ до голосової та електронної пошти, зручний веб-інтерфейс керування та багато іншого. Міні-АТС зроблена в невеликому акуратному корпусі і займає мінімум місця. При цьому станція вкрай ефективна та проста у налаштуванні.

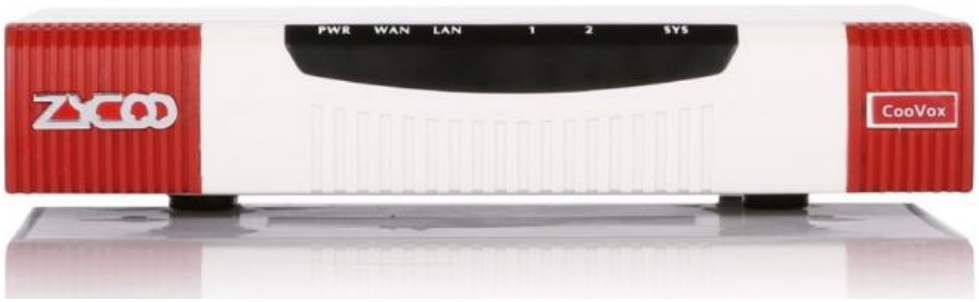

Рисунок 2.12 — Zycoo CooVox U20 A202

Основні характеристики:

— кількість FXO-портів 2;

— кількість Ethernet-портів 1;

— максимальна кількість одночасних розмов 10;

— вбудований інтерфейс UMTS для 3G;

— SDRAM 128M DDR2;

— підтримувані VoIP-протоколи SIP, IAX2;

— підтримка відео.

VoIP:

— протоколи SIP 2.0, IAX2;

— підтримка аудіокодеків G.711a\u, G.726, G.729A\B, GSM, Speex;

— підтримка відеокодеків H.261, H.263, H.263+, H.264;

— підтримка проходження факсів T.38 FAX (Pass-through);

— підтримка DTFM RFC2833, SIP INFO, In-band;

— підтримка безпечних протоколів SRTP, TLS, HTTPS, SSH, Syslog.

Мережеві функції:

— Ethernet-порт 10/100 Мбіт/с;

— мережеві протоколи TCP/UDP/IP, RTP/RTCP, ICMP, ARP/RARP, DNS, DDNS, DHCP, NTP, TFTP, SSH, HTTP/HTTPS, PPPoE, STUN, SRTP, TLS/SIP, LDAP, NAT, Support N2N/L2TP.

3 НАЛАШТУВАННЯ АКТИВНОГО МЕРЕЖЕВОГО ОБЛАДНАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ

В данному підрозділі буде розглянуто налаштування мережеаого обладнання.

3.1 Налаштування VLAN

В даній локальній мережі використано один маршрутизатор та три комутатори.

На комутаторах потрібно налаштувати інтерфейси до відповідних VLAN. На лістингу 3.1 показано приклад додавання інтерфейса до VLAN.

Лістинг 3.1 — Додавання інтерфейса до VLAN

```
Switch(config)#int range f0/1-12
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
```

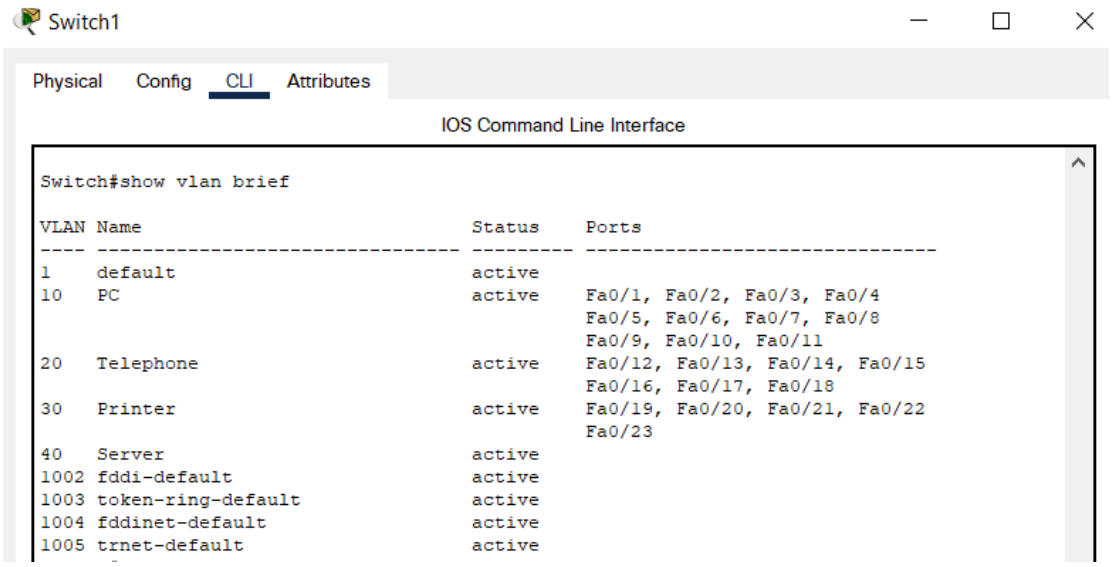

Рисунок 3.1 — Розподіл інтерфейсів на Switch1

Оскільки всі VLAN підключені до одного фізичного порта маршрутизатора, то налаштовуємо маршрутизацію між ними. Налаштування маршрутизації наведено на лістингу 3.2.

Лістинг 3.2 — Налаштування маршрутизації

```
Router>en
Router# configure terminal
Router(config)#int fa0/0.10
Router (config–subif) # encapsulation dot1Q 10
Router (config–subif) # ip address 178.95.1.30 255.255.255.224
Router(config)#ip dhcp pool vl10
Router(dhcp-config)#network 178.95.1.0 255.255.255.224
Router(dhcp-config)#default-router 178.95.1.30
Router(config)#int fa0/0.30
Router(config–subif) # encapsulation dot1Q 30
Router(config–subif) # ip address 178.95.3.14 255.255.255.240
Router(config)# ip dhcp pool vl10
Router(dhcp-config)#network 178.95.3.0 255.255.255.240
Router(dhcp-config)#default-router 178.95.3.14
```

Команда int fa0/0.10 відповідає за створення логічного підінтерфейсу, вказуючи його номер.

Налаштовуємо інкапсуляцію за допомогою команди encapsulation dot1Q10.

Ip address відповідає за призначення ip–адреси підінтерфейсу.

Ip dhcp pool vl10 — створення пулів адрес dhcp.

Default-router — задання адреси шлюза.

Лістинг 3.3 — Виключення з пулу адресів інтерфейсів комутатора

```
Router(config)#ip dhcp excluded-address 178.95.1.30
Router(config)#ip dhcp excluded-address 178.95.2.14
Router(config)#ip dhcp excluded-address 178.95.3.14
Router(config)#ip dhcp excluded-address 178.95.4.2
```

При підключенні до мережі пристрої отримують IP-адреси за протоколом DHCP, відповідно до VLAN в яких вони знаходяться.

3.2 Налаштування VoIP

VoIP — це технологія для передачі медіа-даних до мережі в режимі реального часу.

Нульовим пунктом вважається налаштування dhcp-сервера на маршрутизаторі, так як практично всі стандартні телефони налаштовані на отримання IP-адреси саме таким способом. На лістингу 3.4 наведено налаштування dhcp-сервера.

Лістинг 3.4 — Налаштування dhcp-сервера

```
Router(config)#ip dhcp pool v20
Router(dhcp-config)#network 178.95.2.0 255.255.255.240
Router(dhcp-config)#default-router 178.95.2.14
Router(dhcp-config)#option 150 ip 178.95.2.14
Router(dhcp-config)#ex
```

Наступним кроком буде налаштування для роботи з SCCP. Всі налаштування для роботи протоколу SCCP проводяться в розділі telephony-service. На лістингу 3.5 наведено налаштування номерів телефонів.

Лістинг 3.5 — Налаштування номерів телефонів

```
Router(config)#telephony-service
Router (config-telephony) #max-ephones 30
Router (config-telephony) #max-dn 30
Router (config-telephony) #ip source-address 178.95.2.14 port 2000
Router(config–telephony)#auto assign 1 to 30
Router(config)#ephone–dn 1
Router(config– ephone–dn)#number 322
```

Параметр max-ephones відповідає за те, яка кількість телефонів може бути зареєстрована в даній мережі.

Dn (directory number) — символізує собою телефонний номер. Max-dn відповідає за те, яка кількість номерів може бути зареєстрована в мережі.

Ip source-address задає IP-адресу та порт, на якому будуть слухатися запити від телефонів.

Auto assign слугує для автоматичного призначення номерів телефонам.

3.3 Налаштування VPN

ISAKMP та IPSec необхідні для побудови та шифрування VPN-тунелю. ISAKMP, також званий IKE (Internet Key Exchange), є протоколом, який дозволяє двом хостам домовлятися про те, як створити зіставлення безпеки IPsec. ISAKMP складається з двох етапів: фаза 1 та фаза 2.

Під час фази 1 створюється перший тунель, який захищає наступні повідомлення ISAKMP. Під час другої фази створюється тунель, який захищає дані. Далі в дію вступає IPSec для шифрування даних з використанням алгоритмів шифрування і надає аутентифікацію, шифрування та захист від повторного відтворення.

Для початку проведемо налаштування першого маршрутизатора. Першим кроком є налаштування політики ISAKMP Phase 1.

Лістинг 3.6 — Налаштування політики ISAKMP

```
Router1(config)#  crypto isakmp policy 1
Router1(config-isakmp)# encr 3des
Router1(config-isakmp)# hash md5
Router1(config-isakmp)# authentication pre-share
Router1(config-isakmp)# group 2
Router1(config-isakmp)# lifetime 9999
```

Наведені вище команди означають :

3DES — метод шифрування, який використовуватиметься на етапі 1

MD5 — алгоритм хешування

Pre-Share — використання попереднього загального ключа (PSK) як метод автентифікації

Group 2 — група, яка використовуватиметься

lifetime 9999 — час життя ключа сеансу. Виражається або в кілобайтах (скільки трафіку має пройти до зміни ключа), або за секунди.

Далі за допосогою команди Router1(config)# crypto isakmp key merionet address 1.1.1.3 визначаємо Pre-Shared.

Pre-Shared ключ партнера встановлений на merionet, а його публічна IP-адреса — 1.1.1.3. Кожний раз, коли R1 намагається встановити VPN-тунель із R2 (1.1.1.3), буде використовуватись цей ключ.

Для налаштування IPSec нам потрібно зробити наступне:

— створити розширений ACL;

— створити криптографічну карту (Crypto Map);

— застосувати криптографічну карту до загальнодоступного інтерфейсу.

Нам потрібно створити розширений access-list і в ньому визначити, який трафік ми хочемо пропускати через VPN-тунель.

Наступним кроком є створення набору перетворення (Transform Set), що використовується для захисту даних. Це відбувається за допомогою команди Router1(config)# crypto ipsec transform-set TS esp-3des esp-md5-hmac.

Створення Crypto Map є останнім етапом настройки та поєднує раніше задані конфігурації ISAKMP та IPSec. На лістингу 3.7 наведено створення Crypto Map.

Лістинг 3.7 — Створення Crypto Map

```
Router1(config)# crypto map CMAP 10 ipsec-isakmp
Router1(config-crypto-map)# set peer 1.1.1.2
Router1(config-crypto-map)# set transform-set TS
Router1(config-crypto-map)# match address VPN-TRAFFIC
```

Останній крок — застосувати криптографічну карту до інтерфейсу маршрутизатора, через який виходить трафік. На лістингу 3.8 наведно застосування криптографічної карти.

Лістинг 3.8 — Застосування криптографічної карти

```
Router1(config)# interface fa0/1
Router1(config- if)# crypto map CMAP
```

Як тільки ми застосуємо криптографічну карту до інтерфейсу, ми отримуємо повідомлення від маршрутизатора, що підтверджує, що isakmp увімкнено: “ISAKMP is ON”.

На цьому етапі ми завершили налаштування IPSec VPN на маршрутизаторі 1.

Налаштування для маршрутизатора 2 ідентичні, з відмінностями лише в IP-адресах та ACL.

3.4 Налаштування NAT

NAT дозволяє приватним IP-мережам, які використовують незареєстровані IP-адреси, підключатися до Інтернету. NAT працює на пристрої, який зазвичай з'єднує дві мережі. Перед пересиланням пакетів в іншу мережу NAT перетворює приватні адреси у внутрішній мережі на легальні адреси. NAT може бути настроєний так, щоб рекламувати у зовнішньому світі лише одну адресу для всієї мережі. Ця можливість забезпечує велику безпеку, ефективно приховуючи всю внутрішню мережу за однією адресою.

Існує три типи NAT:

— статична адресна трансляція (static NAT), передбачає зіставлення між глобальними та локальними адресами, як «один до одного»;

— динамічна адресна трансляція (dynamic NAT), зіставлення адрес здійснюється за приницпом «багато до багатьох»;

— адресна трансляція з використанням портів (overload NAT), де передбачається багатоадресне зіставлення.

Статична NAT використовується для зіставлення внутрішньої та зовнішньої адреси один до одного. Статична NAT також дозволяє з'єднуватися із зовнішнього вузла на внутрішній. Зазвичай статична NAT використовується

для серверів всередині мережі. Наприклад, може бути веб-сервер з внутрішньою IP-адресою 178.95.4.1, і ви хочете, щоб він був доступний, коли віддалений вузол робить запит на 209.165.200.10. Щоб це спрацювало, потрібно зробити статичне NAT-порівняння між цими IP-адресами.

Статична NAT забезпечує постійне зіставлення між внутрішньою та публічною IP-адресою. У лістингу 3.7 наведено приклад, де приватна IP-адреса 178.95.4.1 завжди буде відповідати публічній IP-адресі 209.165.200.10.

Лістинг 3.9 — Налаштування статичної NAT

```
Router(config)#ip nat inside source static 178.95.4.1 209.165.200.10
Router(config)#interface FastEthernet 0/1
Router(config-if)#ip nat inside
Router(config-if)#interface Serial 0/0/0
Router(config-if)#ip nat outside
```

Динамічна NAT використовується, коли у вас є пул публічних IP-адрес, які ви хочете динамічно призначати своїм внутрішнім вузлам.

У лістингу 3.8 наведено приклад, коли внутрішня мережа як 192.168.0.0/24. Також є пул публічних IP-адрес від 209.165.200.226 до 209.165.200.240, а призначена нами маска мережі – 255.255.255.224. При налаштувані динамічної NAT, потрібно визначити ACL, щоб дозволити тільки адреси, які дозволено транслювати.

Лістинг 3.10 — Налаштування динамічної NAT

```
Router(config)#ip nat pool NAT-POOL 209.165.200.226 209.165.200.240 netmask 255.255.255.224
Router(config)#access-list 1 permit 192.168.0.0 0.255.255.255
Router(config)#ip nat inside source list 1 pool NAT-POOL
Router(config)#interface FastEthernet 0/1
Router(config-if)#ip nat inside
Router(config-if)#interface Serial 0/0/0
Router(config-if)#ip nat outside
```

Overload NAT, іноді також зване PAT, ймовірно, є найбільш використовуваним типом NAT. Налаштувати навантаження NAT можна двома способами, залежно від того, скільки є публічних IP-адрес.

Лістинг 3.11 — Налаштування Overload NAT

```
Router(config)#access list 1 permit 192.168.0.0 0.255.255.255
Router(config)#ip nat inside source list 1 interface serial 0/0/0 overload
Router(config)#interface FastEthernet 0/1
Router(config-if)#ip nat inside
Router(config-if)#interface Serial 0/0/0
Router(config-if)#ip nat outside
```

Визначення команд:

— ip access-list 1 permit 10.0.0.0 0.255.255.255 надає доступ до режиму глобальної конфігурації іменованого ACL. При першому введені також створює ACL з обраним іменованим ідентифікатором;

— ip nat inside source list 1 interface serial 0/0/0 overload налаштовує перетворення адреси відправника (внутрішня IP-адреса) на IP-адресу інтерфейсу serial 0/0/0;

— ip nat outside позначає зовнішній інтерфейс;

— ip nat inside позначає внутрішній інтерфейс.

3.5 Налаштування обмеженого доступу

Для запобігання вільного доступу до керування пристроєм сторонніми особам, на маршрутизаторі було встановлено пароль на привілейований режим за допомогою команди enable password 2222.

При наступній спробі входу у привілейований режим, буде запитаний пароль.

```
Router>en
Password:
Router#
```

Рисунок 3.2 — Запит пароля при вході у привілейований режим

Для можливості віддаленого доступу з кінцевого пристрою до центрального маршрутизатора було налаштовано Telnet. Налаштування маршрутизатора наведене у лістингу 3.12. Результат входу на маршрутизатор з комп’ютера 1 з використанням Telnet наведено на рисунку 3.3.

Лістинг 3.12 — Налаштування Telnet

```
Router#conf t
Router(config)#line vty 0 4
Router(config-line)#password 1111
Router(config-line)#cdp run
Router(config)#service password-encryption
```

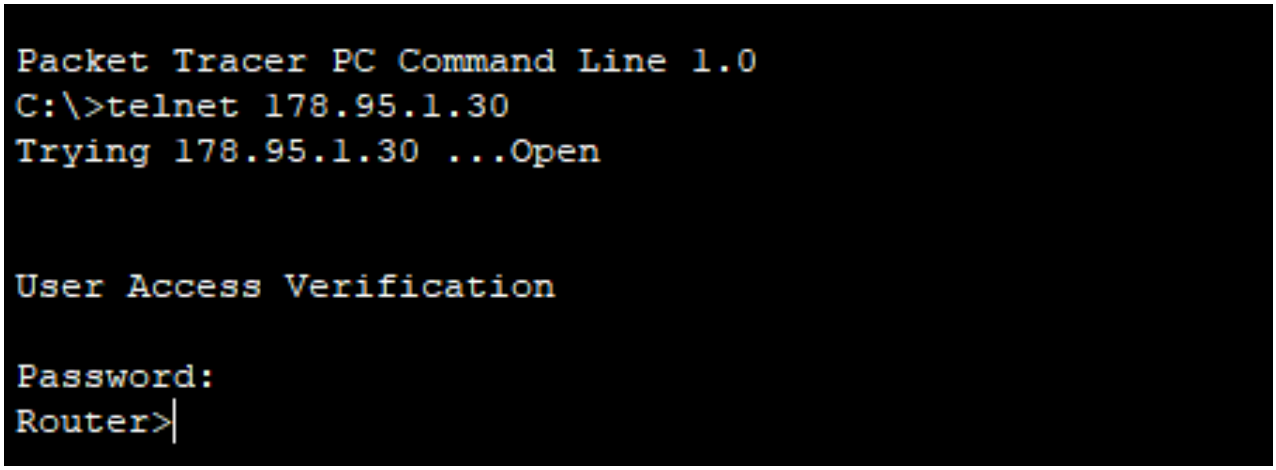

Рисунок 3.3 — Результат входу на маршрутизатор з використанням Telnet

В лістингу 3.13 наведено встановлення секретного паролю. Секретний ключ «перекриває» дію звичайного паролю на привілейований режим доступу.

Лістинг 3.13 — Налаштування секретного паролю

```
Router>en
Router#conf t
Router(config)#enable secret 3333
```

3.6 Перевірка працездатності мережі

Для проектування та перевірки працездатності мережі було обрано програмний пакет CiscoPacketTracer. Схема моделювання мережі приведена на рисунку 3.4.

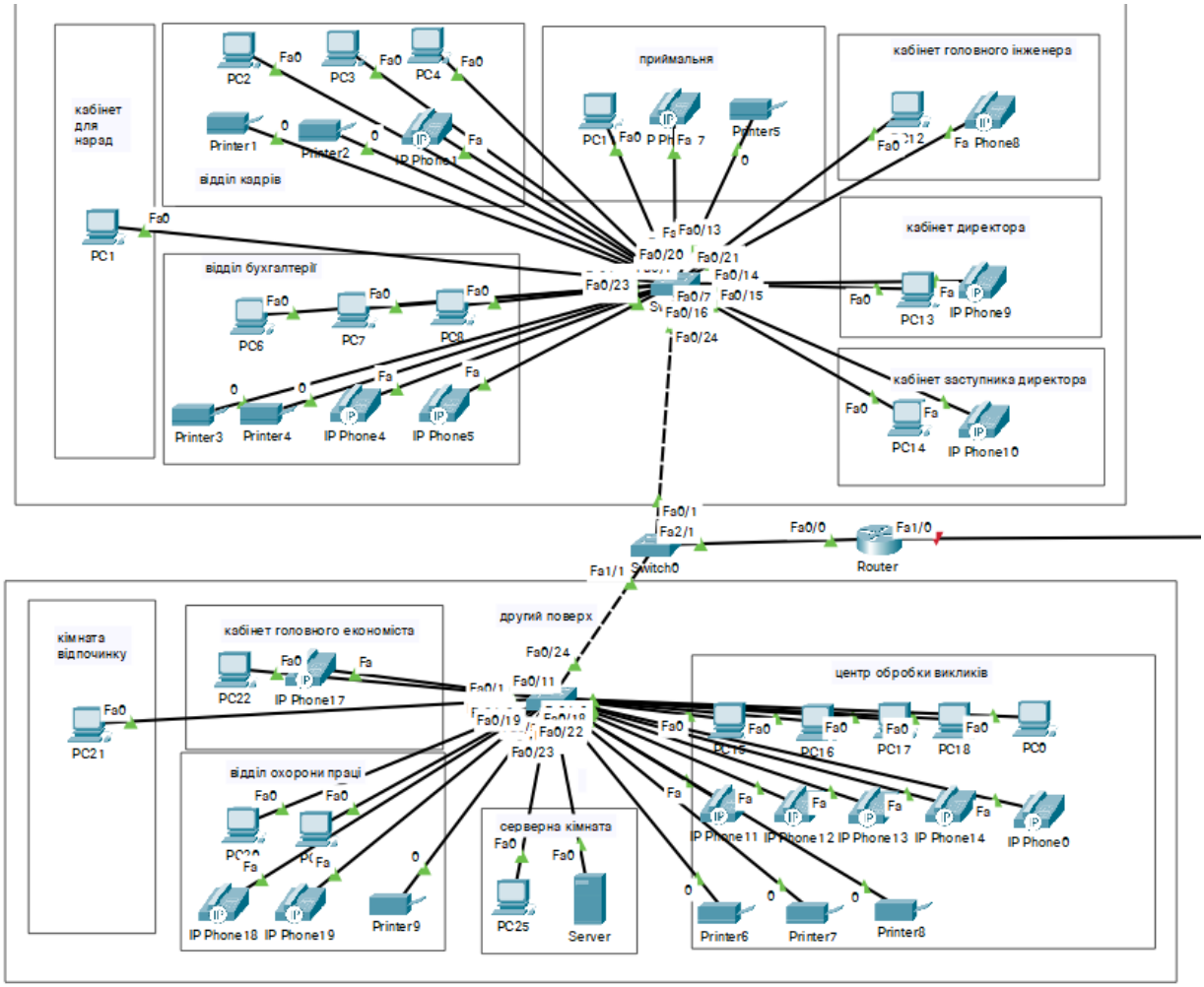

Рисунок 3.4 — Схема моделювання мережі

Cisco Packet Tracer — це програмне забезпечення Cisco для моделювання. Воно може використовуватися для створення складних типологій мереж, а також для тестування та моделювання абстрактних мережевих концепцій. Він діє як ігровий майданчик для вивчення мережевих технологій, а досвід дуже близький до того, що ви бачите у комп'ютерних мережах.

Перевірка працездатності відбувається за допомогою команд ping та tracert. Для перевірки з’єднання обрано комп’ютер з кабінета “Відділ кадрів” (178.95.1.20). Від даного комп’ютера була використана комадна ping для перевірки з’єднання з сервером(178.95.4.1).

```
Packet Tracer PC Command Line 1.0
C:\>ping 178.95.4.1

Pinging 178.95.4.1 with 32 bytes of data:

Reply from 178.95.4.1: bytes=32 time=16ms TTL=127
Reply from 178.95.4.1: bytes=32 time=1ms TTL=127
Reply from 178.95.4.1: bytes=32 time<1ms TTL=127
Reply from 178.95.4.1: bytes=32 time<1ms TTL=127

Ping statistics for 178.95.4.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 16ms, Average = 4ms
```

Рисунок 3.5 — Перевірка з’єднання з сервером

Перевірка проходження пакета від комп’ютера, що знаходиться в приймальні до сервера наведено в рисунку 3.5.

```
C:\>tracert 178.95.4.1

Tracing route to 178.95.4.1 over a maximum of 30 hops:

  1    0 ms      1 ms      0 ms      178.95.1.30
  2    0 ms      0 ms      1 ms      178.95.4.1

Trace complete.
```

Рисунок 3.6 — Перевірка шляху проходження пакету

ВИСНОВКИ

Бакалаврська робота присвячена розробці комп’ютерної мережі центрального офісу компанії «Vodafone». Проаналізовано розташування кабінетів та їх призначення та обрано оптимальний набір мережевого обладнання.

Був проведений детальний огляд принципів побудови сучасних локальних комп’ютерних мереж.

Розроблено фізичну та логічну структуру мережі компанії, поділено на віртуальні локальні мережі та використано DHCP-сервер для динамічного присвоєння ip-адрес.

Реалізовано технології безпеки мережі у вигляді: налаштовано VPN для безпечного виходу в Internet, на маршрутизаторі встановлено паролі на привілейований режим та консольне з’єднання, налаштовано технологію NAT.

Для реалізації системи IP-телефонії була розглянута та використана технологія VoIP.

Моделювання, налаштування обладнання та перевірка працездатності мережі проведено в середовищі Cisco Packet Tracer.

Отже, розроблена мережа відповідає всім мережевим стандартам та задовільняє всім поставленим вимогам. Використання сучасного обладнання дозволить мережі стабільно працювати протягом всього строку експлуатації та виконувати поставлені завдання.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Комп’ютерні мережі / Азаров О.Д., Захарченко С.М. та інш. Вінниця, ВНТУ, 2013. – 370 с.

2. Комп’ютерні мережі / Азаров О.Д., Захарченко С.М. та інш. Вінниця, ВНТУ, 2020. – 377 с.

3. Офіс [Електронний ресурс] – Режим доступу до ресурсу: https://calvarybaptisthsv.org/wiki/Головний_офіс

4. Бухгалтерія [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki /Бухгалтерія_(підрозділ)

5. Погорілий С. Д. Комп'ютерні мережі. Апаратні засоби та протоколи передачі даних: підручник для студентів вищ. навч. закладів / С. Д. Погорілий, Д. М. Калита ; за ред. О. В. Третяка. - К. : ВПЦ "Київський університет", 2007. - 455 с.

6. Антонов В. М. Сучасні комп'ютерні мережі. — К.: "МК-Прес", 2005. – 480 с.

7. В.Оліфер. та Н.Оліфер,Комп’ютерні мережі. Принципи, технології, протоколи: Посібник для вузів.Пітер, Росія:3-е вид.,2009. – 958 с.

8. Бернерс-Лі Тім,Фічетті Марк, Заснування павутини. З чого починалася і до чого прийде всесвітня мережа. Київ, Україна: Києво-Могилянська академія, 2007. – 150 с.

9. Боднар К.О., Захарченко С.М. - Аналіз пристроїв Internet of Things, використовуючи середовище моделювання Cisco Packet Tracer, XLIX Науково-технічна конференція факультету інформаційних технологій та комп'ютерної інженерії — ВНТУ, 2020.

ДОДАТОК А

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

ЗАТВЕРДЖУЮ
Завідувач кафедри ОТ
____ д.т.н., проф. О.Д. Азаров
(підпис)
«28» квітня 2022 р.

ТЕХНІЧНЕ ЗАВДАННЯ

на виконання бакалаврської дипломної роботи

Комп'ютерна мережа центрального офісу компанії «Vodafone»
08–23.БДР.010.00.000.ТЗ

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

Студент групи 1КІ – 18б
_____Мазуренко В.В.

ВНТУ 2022

1 Підстава для виконання бакалаврської дипломної роботи (БДР)

1.1 Актуальність розробки обумовлена тим, що постає необхідність у створенні локальних мереж для компаній для задоволення їхніх потреб у обчислювальній потужності та зв’язку між структурними підрозділами;

1.2 Наказ про затвердження теми БДР.

2 Мета БДР і призначення розробки

2.1 Мета полягає у розробці комп’ютерної мережі центрального офісу компанії «Vodafone», для забезпечення продуктивності компанії;

2.2 Призначення розробки — покращення управління персоналом, збільшення продуктивності компанії та організація централізованого доступу до електронних ресурсів компанії.

3 Вихідні дані для виконання БДР

3.1 Проведення аналізу існуючих принципів та технологій побудови комп’ютерних мереж;

3.2 Розробка структури та функціональної схеми приміщень;

3.3 Виконання розрахунків для доведення доцільності нової розробки з економічної точки зору.

4 Вимоги до виконання БДР

Головна вимога — побудова комп’ютерної мережі для компанії.

5 Етапи МКР та очікувані результати

Етапи роботи та очікувані результати приведено в Таблиці А.1.

Таблиця А.1 — Етапи МКР

№ етапу	Назва етапу	Термін виконання		Очікувані результати
		Початок	Кінець	
1	Аналіз завдання. Вступ	16.05	17.05	Вступ
2	Аналіз сучасних технологій побудови комп’ютерних мереж	18.05	19.05	Розділ 1
3	Огляд приміщень та потреб компанії	20.05	21.05	Розділ 2
4	Розробка логічної топології мережі	22.05	23.05	Розділ 2
5	Практична реалізація, результати	24.05	25.05	Розділ 3
6	Оформлення пояснювальної записки	26.05	27.05	ПЗ, презентація

6 Матеріали, що подаються до захисту БДР

До захисту подаються: пояснювальна записка БДР, графічні і ілюстративні матеріали, протокол попереднього захисту БДР на кафедрі, відзив наукового керівника, відзив опонента, анотації до БДР українською та іноземною мовами, нормоконтроль про відповідність оформлення БДР діючим вимогам.

7 Порядок контролю виконання та захисту МКР

Виконання етапів графічної та розрахункової документації БДР контролюється науковим керівником згідно зі встановленими термінами. Захист БДР відбувається на засіданні Екзаменаційної комісії, затвердженої наказом ректора.

8 Вимоги до оформлювання та порядок виконання БДР

8.1 При оформлюванні БДР використовуються:

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

— ДСТУ 8302 : 2015 «Бібліографічні посилання. Загальні положення та

правила складання»;

— ГОСТ 2.104-2006 «Єдина система конструкторської документації. Основні написи»;

— Методичні вказівки. Кафедра обчислювальної техніки 2022;

— Документами на які посилаються у вище вказаних.

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

Технічне завдання до виконання отримав _____Мазуренко В.В.

ДОДАТОК Б

Структурна схема комп’ютерної мережі

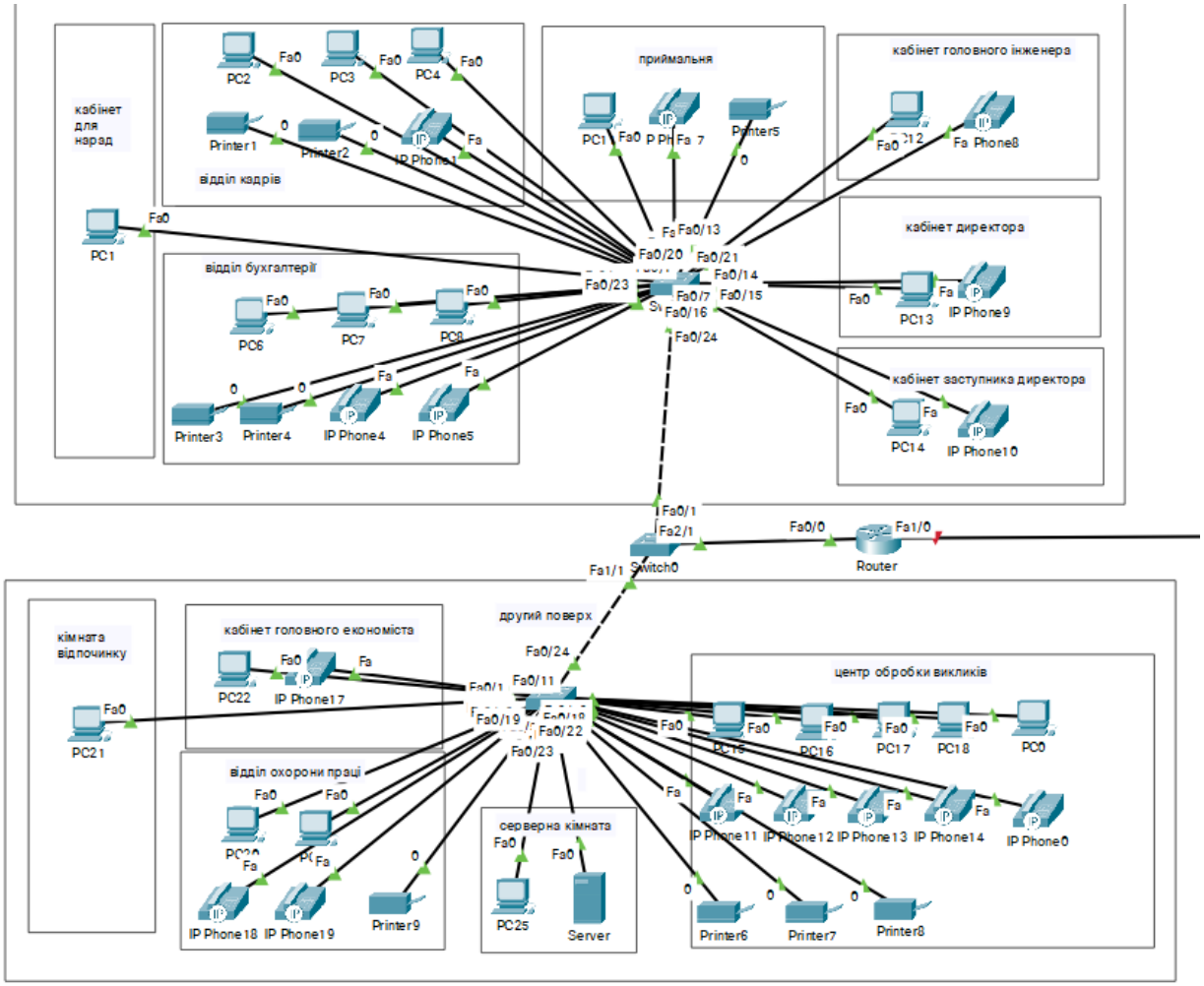

Рисунок Б.1— структурна схема комп’ютерної мережі

ДОДАТОК В

Конфігураційний файл маршрутизатора

```
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname Router
enable secret 5 $1$mERr$DAmA1LM8ekW8fVPyihECO1
enable password 2222
ip dhcp pool vl10
network 178.95.2.0 255.255.255.240
default-router 178.95.2.14
no ip cef
no ipv6 cef
interface FastEthernet0/0
no ip address
duplex auto
speed auto
shutdown
interface FastEthernet0/0.10
encapsulation dot1Q 10
ip address 178.95.1.30 255.255.255.224
interface FastEthernet0/0.20
encapsulation dot1Q 20
ip address 178.95.2.14 255.255.255.240
interface FastEthernet0/0.30
encapsulation dot1Q 30
ip address 178.95.3.14 255.255.255.240
interface FastEthernet0/0.40
encapsulation dot1Q 40
ip address 178.95.4.2 255.255.255.252
interface FastEthernet1/0
no ip address
duplex auto
speed auto
shutdown
interface Serial2/0
no ip address
shutdown
interface Serial3/0
no ip address
shutdown
interface FastEthernet4/0
```

```
no ip address
duplex auto
speed auto
shutdown
interface FastEthernet5/0
no ip address
duplex auto
speed auto
shutdown
interface FastEthernet6/0
no ip address
duplex auto
speed auto
shutdown
interface FastEthernet7/0
no ip address
duplex auto
speed auto
shutdown
ip classless
ip flow-export version 9
line con 0
line aux 0
line vty 0 4
password 1111
login
end
```

ДОДАТОК Г

Конфігураційні файли комутаторів

```
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname Switch
spanning-tree mode pvst
spanning-tree extend system-id
interface FastEthernet0/1
switchport access vlan 10
interface FastEthernet0/2
switchport access vlan 10
interface FastEthernet0/3
switchport access vlan 10
interface FastEthernet0/4
switchport access vlan 10
interface FastEthernet0/5
switchport access vlan 10
interface FastEthernet0/6
switchport access vlan 10
interface FastEthernet0/7
switchport access vlan 10
interface FastEthernet0/8
switchport access vlan 10
interface FastEthernet0/9
switchport access vlan 10
switchport mode access
interface FastEthernet0/10
switchport access vlan 10
interface FastEthernet0/11
switchport access vlan 10
interface FastEthernet0/12
switchport access vlan 20
switchport voice vlan 20
interface FastEthernet0/13
switchport access vlan 20
switchport voice vlan 20
interface FastEthernet0/14
switchport access vlan 20
switchport voice vlan 20
interface FastEthernet0/15
switchport access vlan 20
switchport voice vlan 20
```

```
interface FastEthernet0/16
switchport access vlan 20
switchport voice vlan 20
interface FastEthernet0/17
switchport access vlan 20
switchport voice vlan 20
interface FastEthernet0/18
switchport access vlan 20
switchport voice vlan 20
interface FastEthernet0/19
switchport access vlan 30
interface FastEthernet0/20
switchport access vlan 30
interface FastEthernet0/21
switchport access vlan 30
interface FastEthernet0/22
switchport access vlan 30
interface FastEthernet0/23
switchport access vlan 30
interface FastEthernet0/24
switchport mode trunk
interface Vlan1
no ip address
shutdown
line con 0
line vty 0 4
login
line vty 5 15
login
end

version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname Switch
spanning-tree mode pvst
spanning-tree extend system-id
interface FastEthernet0/1
switchport access vlan 10
interface FastEthernet0/2
switchport access vlan 10
interface FastEthernet0/3
switchport access vlan 10
interface FastEthernet0/4
switchport access vlan 10
```

```
interface FastEthernet0/5
switchport access vlan 10
interface FastEthernet0/6
switchport access vlan 10
interface FastEthernet0/7
switchport access vlan 10
interface FastEthernet0/8
switchport access vlan 10
interface FastEthernet0/9
switchport access vlan 10
interface FastEthernet0/10
switchport access vlan 10
interface FastEthernet0/11
switchport access vlan 20
switchport voice vlan 20
interface FastEthernet0/12
switchport access vlan 20
switchport voice vlan 20
interface FastEthernet0/13
switchport access vlan 20
switchport voice vlan 20
interface FastEthernet0/14
switchport access vlan 20
switchport voice vlan 20
interface FastEthernet0/15
switchport access vlan 20
switchport voice vlan 20
interface FastEthernet0/16
switchport access vlan 20
switchport voice vlan 20
interface FastEthernet0/17
switchport access vlan 20
switchport voice vlan 20
interface FastEthernet0/18
switchport access vlan 20
switchport voice vlan 20
interface FastEthernet0/19
switchport access vlan 30
interface FastEthernet0/20
switchport access vlan 30
interface FastEthernet0/21
switchport access vlan 30
interface FastEthernet0/22
switchport access vlan 30
interface FastEthernet0/23
switchport access vlan 40
```

```
interface FastEthernet0/24
switchport mode trunk
interface Vlan1
no ip address
shutdown
line con 0
line vty 0 4
login
line vty 5 15
login
end
```

ДОДАТОК Д

ПРОТОКОЛ
ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ
НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: Комп'ютерна мережа центрального офісу компанії "Vodafone".

Тип роботи: бакалаврська дипломна робота
(БДР, МКР)

Підрозділ кафедра обчислювальної техніки
(кафедра, факультет)

Показники звіту подібності
Unicheck

Оригінальність 89,8% Схожість 10,2%

Аналіз звіту подібності (відмітити потрібне):

- ✓ Запозичення, виявлення у роботі, оформлені коректно і не містять ознак плагіату.
- ☐ Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.
- ☐ Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

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

Ознайомлені з повним звітом подібності, який був згенерований системою Unicheck щодо роботи.

Автор роботи _____ Мазуренко В.В.
(підпис) (прізвище, ініціали)

Керівник роботи _____ Захарченко С.М.
(підпис) (прізвище, ініціали)