Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Навчально-науковий
інститут електроенергетики
(інститут)
Факультет інформаційних технологій
(факультет)
Кафедра інформаційних технологій та комп'ютерної інженерії
(повна назва)

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента Віхмана Євгенія Павловича
(ПІБ)
академічної групи 123-20зск-1
(шифр)
спеціальності 123 Комп'ютерна інженерія
(код і назва спеціальності)
за освітньо-професійною програмою 123 Комп'ютерна інженерія
(офіційна назва)
на тему «Комп'ютерна система IT-компанії "Servers.com" з реалізацією побудови дата-центру та налаштування та безпеки корпоративної мережі»
(назва за наказом ректора)

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	доц. Бешта Д.О.			
розділів:				
розробка апаратної частини	доц. Ткаченко С.М.			
розробка корпоративної мережі	ас. Бешта Л.В.			

Рецензент				

Нормоконтролер	проф. Цвіркун Л.І.			

Дніпро

2023

ЗАТВЕРДЖЕНО:
завідувач кафедри
інформаційних технологій
та комп'ютерної інженерії
(повна назва)
_____ Гнатушенко В.В.
(підпис) (прізвище, ініціали)

«_ __ »__ _____2023 року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавр

студента Віхмана Є.П. **академічної групи** 123-20зск-1
(прізвище та ініціали) (шифр)

спеціальності 123 Комп'ютерна інженерія

за освітньо-професійною програмою 123 Комп'ютерна інженерія
(офіційна назва)

на тему «Комп'ютерна система ІТ-компанії "Servers.com" з реалізацією побудови дата-центру та налаштування та безпеки корпоративної мережі»

затверджену наказом ректора НТУ «Дніпровська політехніка» від 11.04.2023 № 256-с

Розділ	Зміст	Термін виконання
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел конкретизується предмет та мету роботи та виконується постановка завдання	10.05.2023
Розробка апаратної частини	На основі аналізу підприємства формулюються технічні вимоги до комп'ютерної системи та розробляється апаратна частина системи	17.05.2023
Розробка корпоративної мережі	Виконується розрахунок налаштувань корпоративної мережі та перевірка роботи системи, розробляються методи та налаштування обладнання для захисту інформації в системі	24.05.2023
Розробка компонента системи	Виконується детальна розробка компонента системи	31.05.2023

Завдання видано _____ доц. Бешта Д.О.
(підпис керівника) (прізвище, ініціали)

Дата видачі 25.01.2023

Дата подання до екзаменаційної комісії 12.07.2023

Прийнято до виконання _____ Віхман Є.П.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 79 с., 39 рис., 8 табл., 3 дод., 9 джерел.

ДАТА-ЦЕНТР, МЕРЕЖА, ОФІС КЕРУВАННЯ, ПРОТОКОЛИ, ТОПОЛОГІЯ, LAN

Об’єкт: комп'ютерна система IT-компанії "Servers.com" з реалізацією побудови дата-центру та налаштування та безпеки корпоративної мережі.

Мета: створення мережевого проекту для реалізації та побудови IT-компанії "Servers.com".

Реалізована комп’ютерна система має можливість масштабування та переконфігурування мережі та орієнтована на побудову комплексних заходів щодо офісу та даца-центру компанії у м.Дніпро, а також впровадження виконаних заходів проекту для збільшення клієнтообігу та фінансової частини.

Мережева інфраструктура створена за всіма вимогами компанії та відподно до завдання кваліфікаційної роботи. Система вміщує в себе:

– запас робочих станцій в мережі;

– запас мережевих можливостей мережі;

– збільшення можливостей апаратної частини дата-центрів;

– контроль доступу між клієнтами та співробітниками.

Комп’ютерна мережа має організаційну структурну схему з описанням працездатності всіх підрозділів системи.

Моделювання проекту було реалізовано в додатку Cisco Packet Tracer.

IP-адресація була розроблена та винесена у вигляді таблиць. Також, було розроблена структурована кабельна система, всі дані винесені до таблиці.

Схеми розташування пристроїв та кабельних систем було розроблено та закріплено за розділами.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАК, ОДИНИЦЬ І ТЕРМІНІВ

ДЦ – дата-центр;

VLAN − віртуальна локальна комп'ютерна мережа;

WAN − глобальна мережа;

LAN − локальна мережа;

PUE – енергоефективність

POD – технологія з апаратною частиною ЦОД;

ЦОД – центр обробки даних;

RSA − криптографічний алгоритм з відкритим ключем;

CPN – приватна мережа клієнта;

GPN – глобальна приватна мережа;

iDRAC – модуль керування сервером;

ЦП – центральний процесор;

VPN − віртуальна локальна мережа.

ВСТУП

Метою створення кваліфікаційної роботи є вивчення реального підприємства і умов роботи на ньому, отримання прикладних навичок в розробці і супроводі програм, вивченні інформаційних потоків, способів зберігання і обробки інформації, збір матеріалів для створення проекту та звіту.

Після здобуття певних теоретичних навичок в навчальному закладі та практичних навичок на підприємстві, надається змога продемонструвати свої навички в кваліфікаційній роботі. В процесі створення використовуються основні системи інформаційних технологій, а саме використання комп'ютерних мереж – локальні та глобальні мережі.

Комп'ютерна мережа характеризує групу з декількох комп'ютерів, які з'єднані між собою за допомогою мережевого обладнання.

Комп'ютерна мережа забезпечує:

– централізований обмін даними;
– централізований доступ до файлів;
– безпечну передачу файлів;
– швидку передачу файлів.

Локальні мережи LAN (Local Area Networks) – створені для об'єднання пристроїв в мережі на невеликій відстані між один одним. В більш загальному вигляді, це мережа яка належить для однієї компанії.

Глобальні мережі WAN Wide Area Networks (Wide Area Networks) – створені для об'єднання пристроїв в мережі на великій відстані. Територіально мережі можуть знаходитися в різних куточках світу. Зв'язок між мережами забезпечують магістральні провайдери, які проводять шляхи через океани та ін. Для об'єднання двох локальних мереж в одному місті можна використовувати існуючі лінії зв'язку, замість того, щоб самостійно прокладати кабель, оскільки прокладка кабелю це дуже дорого.

В кваліфікаційній роботі вся увага зосереджена на цих двох базових системах мережі, повне налаштування взаємозв’язку між мережами та налаштування безпеки користування в мережі.

Мережі LAN та WAN будуть широко використовуватись для створення та обслуговування дата-центрів. Також при створення офісних приміщень для працездатності робочого персоналу.

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

1.1 Характеристика та аналіз діяльності компанії Servers.com

Компанія Servers.com – це хостингова компанія (HSP (Hosting Service Provider)), яка займається питанням щодо видачі фізичної спроможності серверів, та створення web-сайтів на своєму технічному обладнанні.

Надає наступні послуги:

- виділений сервер (dedicated servers);
- віртуальний виділений сервер (cloud servers);
- віртуальне сховище (cloud storage);
- балансувальник навантаження (load balancing);
- міжмережевий екран (firewall);
- приватна стійка (private racks);
- приватна хмара (private cloud);
- кластери Kubernetes (kubernetes clusters).

Дані послуги дуже необхідні в наш час інформаційних технологій, будь-яка платформа магазину, сайту, гри і так далі використовує обчислювальні ресурси.

В кваліфікаційній роботі розглядається власний досвід роботи в компанії Servers.com, а саме побудова дата-центру, налаштування та безпеки корпоративної мережі.

1.2 Сертифікація надійності і структура об’єкта

Під сертифікацією надійності ЦОД мають на увазі, що ЦОД підтвердив високий статус інформаційної безпеки, завдяки аудиту.

Для його проходження необхідно пройти перевірку безпеки компанії, налаштувати та захистити кожну інфраструктурну частину підприємства.

Більшість центрів обробки даних мають сертифікацію рівня 3 (доступність 99,982%) або 4 (доступність 99,995%), надану Uptime Institute.

Uptime Institute – один з найвідоміших міжнародних сертифікаційних інститутів, що користуються довірою, який розробив власний стандарт надійності центрів обробки даних.

Дані клієнтів добре захищені з погляду інформаційної безпеки. Всі центри обробки даних мають чинну сертифікацію ISO 27001:2013.

ISO/IEC 27001:2013 – це стандарт управління безпекою, що формулює рекомендації з управління безпекою та характеризує комплексні елементи контролю безпеки відповідно до посібника з дотримання рекомендацій ISO/IEC 27002. В основі цієї сертифікації лежить розробка та впровадження суворої програми забезпечення безпеки, яка включає у собі розробку та впровадження системи управління інформаційною безпекою (ISMS), що визначає безперервний, цілісний та всеосяжний процес управління безпекою в AWS. Цей широко визнаний міжнародний стандарт безпеки вимагає виконання AWS наступних умов:

– систематичної оцінки ризиків інформаційної безпеки з урахуванням впливу загроз та вразливостей;

– проектування та впровадження комплексного пакету інструментів управління інформаційною безпекою та інших форм управління ризиками, пов'язаними з ризиками безпеки компанії та архітектури систем;

– впровадження процесу управління, що гарантує постійну відповідність засобів управління інформаційною безпекою вимогам, що висуваються.

Більшість центрів обробки даних відповідають стандарту PCI DSS, що дозволяє обробляти платіжні картки.

Суворий контроль доступу, висока доступність та інформаційна безпека повинні доповнюватися ефективною системою керування.

Тому у всіх дата-центрах є сертифікат стандарту ISO 9001:2008.

Система управління якістю ISO 9001:2008 (система менеджменту якості) – це система управління всіма аспектами діяльності підприємства, які безпосередньо чи опосередковано впливають на якість продукції або послуг.

Організаційно-управлінська структура Servers.com складається з вищих рівнів управління та з відділів конкретизованих системи управління.

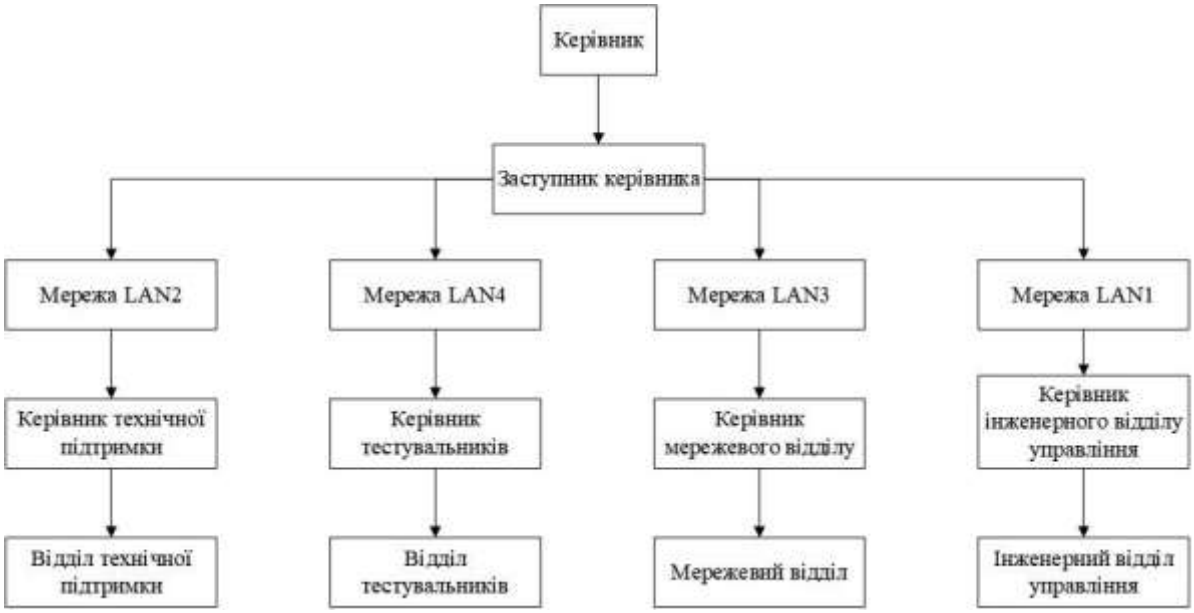

Рисунок 1.1 – Схема організаційної структури

Хостингова компанія Servers.com складається з:

– відділу технічної підтримки;
– відділу тестувальників;
– інженерного відділу управління;
– мережевого відділу.

Створення такого обсягу відділів дозволяє компанії завжди здобувати прогрес та розвиватися за всіма напрямками. В роботі кожний відділ працює та перетинається з іншим, та кожний співробітник перетинається з співробітниками інших відділів.

Відділ технічної підтримки обслуговує клієнтів компанії, займається налаштуванням серверів та розробкою модифікацій серверів під клієнтів.

Мережевий відділ допомагає реалізовувати безпеку в мережі та конструює адресацію клієнтів.

Відділ тестувальників займається впровадженням автоматизації багатьох систем задля уникнення технічних помилок людини.

Інженерний відділ управління знаходиться в дата-центрі та виконує завдання компанії на фізичному рівні, а саме підключення серверів в стійки, заміна комплектуючих і т.д.

1.3 Стислі відомості технологій дата-центру

В даній кваліфікаційній роботі було побудовано мережу дата-центру за всіма сучасними вимогами та стандартами. Були використані різноманітні мережеві пристрої, такі як – маршрутизатори, комутатори та технології їх використання.

Інфраструктура дата-центру:

– інженерна – усередині приміщень встановлюють кондиціонери і прокладають систему вентиляції, забезпечують безперебійне постачання електрики, створюють блок управління і контролю доступу;

– телекомунікаційна – мережеве обладнання, яке пов'язує компоненти центру обробки даних і забезпечує обмін інформацією між самим ДЦ і його користувачами;

– інформаційна – відповідає за обробку та зберігання великого обсягу даних.

Сучасний дата-центр схожий на фортецю, яка надійно захищена.

Рисунок 1.2 – Вигляд дата-центру

Дата-центри захищені від фізичного вторгнення й оснащені складними багаторівневими системами контролю доступу, включно з камерами відеоспостереження, біометричним доступом і системами перевірки документів.

Рисунок 1.3 – Вигляд всередині дата-центру

Щоб забезпечити стабільність POD у центрах обробки даних, забезпечується їхнє охолодження. Система кондиціонування сучасних ЦОД зазвичай будується за схемою N+1. Об’єкти оснащені резервними системами охолодження 2N.

Використовується схема охолодження гарячого і холодного коридору в центрах обробки даних. Вона забезпечує стабільно низьку температуру в холодному коридорі та низькі параметри PUE.

Тут приділено увагу кожному аспекту продуктивності центру обробки даних, включно з впливом на навколишнє середовище.

Сучасні дата-центри активно застосовують енергоефективні технології та використовують поновлювані джерела енергії. Ці дата-центри не є винятком, оскільки використовують зелену енергію, а середній рівень PUE знаходиться в межах 1,1-1,5.

Вигляд пропуску в дата-центрі представлений у (Додаток Б).

1.4 Георозміщення дата-центрів та офісів управління

Компанія надає доступ до рішень для хостингу серверів преміум-класу в центрах обробки даних. Вони розташовані у 5 континентах та 10 містах і мають 18 дата-центрів.

Рисунок 1.4 – Георозміщення дата-центрів на мапі

Розташування в багатьох точках планети дозволяє створити високу ефективність для всіх користувачів компанії. Кожен користувач має змогу вибрати сервер з найменшим часом відповіді(затримки) та с найпотужнішою пропускною здатністю.

Також, компанія має 5 офісів в Україні, Великобританії, Нідерландах, США та Кіпрі. Всі розташовані дата-центи, які зображені на мапі мають відстань від головного офісу в Україні. З нього виконуються основний об’єм роботи компанії. Весь досвід та практичні навички було отримано в офісі – Україна, місто Дніпро.

1.5 Аналітичний огляд офісу і дата-центру та безпеки функціонування

Управління серверами, налаштування мережі, заміна комплектуючих, встановлення серверів, заміна мережевого обладнання, оновлення та встановлення програмного забезпечення, комунікація з клієнтами та іншими відділами компанії і так далі, все це відбувається в офісі міста Дніпро.

Рисунок 1.5 – Вигляд офісу управління

Офіс в більшому обсязі відділу має технічну підтримку, яка виконує обслуговування всієї інфраструктури по всіх містах і дата-центрах.

Безпека офісу використовує найпопулярніше застосування технологіїї OpenVPN.

Головне, що до мережевих пристроїв та системи в цілому мають доступ обмежене коло осіб, які мають RSA-ключі.

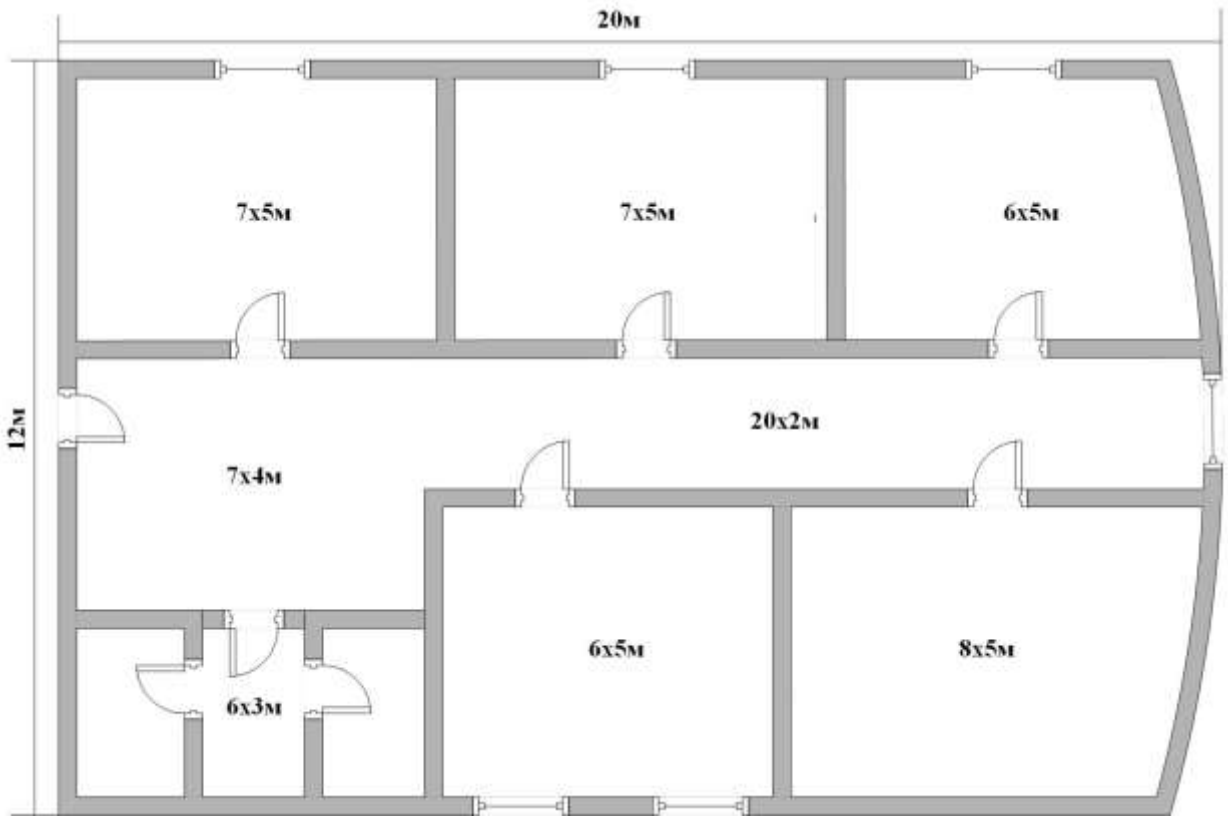

Рисунок 1.6 – Відображення розмірів офісного приміщення

Стіни будівлі офісу складаються з різних матеріалів, це залежить від дизайну, конструкції та вподобань забудовника. Будівля офісу складається з цегли та каменю. Цегляні та кам’яні стіни є одним із найтрадиційніших і найміцніших варіантів. Цегла в будівлі використовується як для зовнішніх, так і для внутрішніх стін.

Також, використовуються гіпсокартонні панелі. Вони є легкими і швидкими в установці. Вони складаються з гіпсового сердечника, покритого картононаплавленим листом. Гіпсокартонні стіни використовуються для внутрішнього оздоблення і перегородок в офісному приміщенні.

1.6 Завдання і мета роботи

Головним завданням при написанні кваліфікаційної роботи є побудова мережі дата-центру та розробка і встановлення апаратної частини серверної, що відповідає всім сучасним технологіям та вимогам працездатності дата-центрів.

При розробці проекту, були визначені наступні завдання виконання:

– зробити аналіз існуючих рішень мереж;
– зробити аналіз існуючих рішень апаратної частини;
– побудувати топологію мережі;
– побудувати апаратну частину;
– провести розрахунок інтенсивності трафіку;
– зробити підключення фізичного обладнання;
– налаштувати агрегування каналів PagP;
– налаштувати підмережі VLAN;
– виконати базове налаштування мережевих інтерфейсів;
– виконати розбиття IP-адресації за завданням;
– за допомогою технології інтернету речей створити систему охолодження дата-центру.

Проектування, моделювання та налаштування мережі повинно бути виконано в додатку Cisco Packet Tracer.

1.7 Визначення можливих напрямків рішення поставлених завдань

Для виконання практичної частини проекту було вирішено використовувати наступні методи налаштувань та безпеки:

– ACL списки для налаштування безпеки;
– розбиття мережі на підмережі VLAN;
– налаштування персональної безпеки кожного мережевого обладнання паролем;
– налаштування агрегування каналів для поліпшення відмовостійкості та підвищення швидкості передавання даних.

Зв’язок між вузлами забезпечує мережеве обладнання, комутатори та маршрутизатори. В якості моделювання та створення мережі було використано додаток Cisco Packet Tracer.

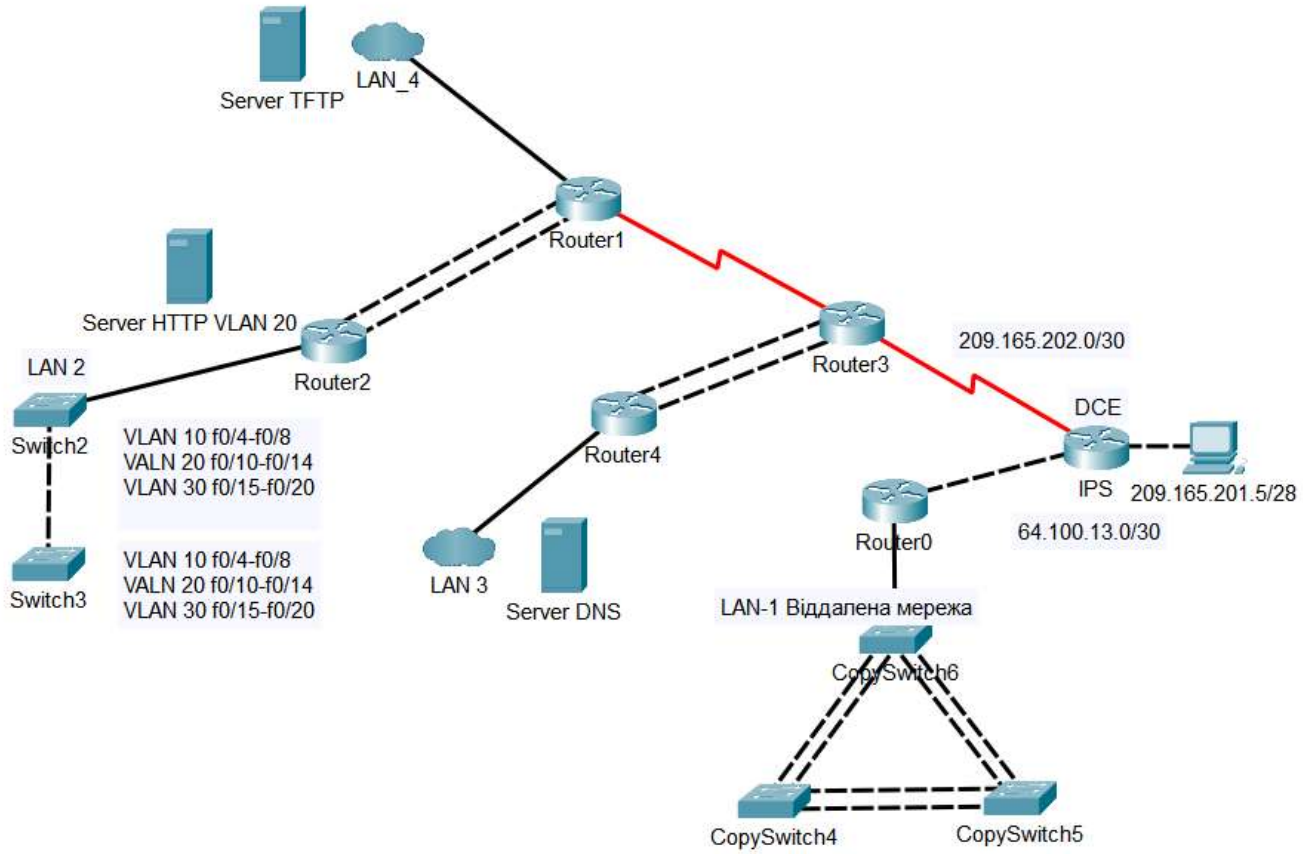

Рисунок 1.7 – Загальна топологія мережі Servers.com

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ

2.1 Технічні вимоги до системи

2.1.1 Вимоги до системи в цілому

2.1.1.1 Вимоги до структури і функціонування системи

2.1.1.1.1 Перелік підсистем, їхнє призначення й основні характеристики, вимоги до числа рівнів ієрархії та ступені централізації мережі

Система кваліфікаційної роботи представляє собою мережу компанії «servers.com». Дана система є корпоративною мережею компанії.

Підсистемами мережі є локальні мережі, в яких знаходяться підрозділи компанії та мають своє мережеве обладнання. Чисельність таких підмереж лімітована умовами завдання на кваліфікаційну роботу, що складає чотири локальних мережі.

Відповідно до схеми організаційної структури (рисунок 1.1) та загальної топології компанії (рисунок 1.7) в мережі знаходяться наступні підмережі:

– відділ технічної підтримки – LAN2;
– відділ тестувальників – LAN4;
– інженерний відділу управління – LAN1;
– мережевий відділу – LAN3.

Кожна підмережа повинна мати певну кількість користувачів, а саме:

– LAN1 – 28;
– LAN2 – 16;
– LAN3 – 45;
– LAN4 – 19.

При виконанні кваліфікаційної роботи повинні бути створені 4 підмережі. IP-адресація мереж повинна застосовуватись виключно із запропонованого завдання та відповідно до варіанту.

Підрозділи компанії призначені для обслуговування мережі в цілому та для обробки інформації клієнтів.

Головною характеристикою підрозділів є взаємна мета компанії, що працює на те, щоб видавати сервери клієнтам під різні задачі та проекти.

Система управління мережею являю собою єдину централізовану систему, від керівника компанії до працівників кожного підрозділу. Керівник компанії має заступника, в свою чергу вони приймають основні рішення щодо направлення роботи компанії. Керівники кожного підрозділу націлені на найвищий результат працездатності свого персоналу.

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

В системі повинна використовуватися мережева архітектура leaf-spine (архітектура центру обробки даних, що складається з двох рівнів комутації – стовбура і листа). Сервери повинні бути підключені до комутаторів нижнього рівня (листовий рівень). Кожен комутатор на листовому рівні повинен бути під'єднаний до кожного з комутаторів верхнього рівня (рівень хребта) у повнозв'язній топології, щоб забезпечувати з'єднання з трьома переходами між будь-якими двома серверами.

Кожен рівень – лист, хребет і ядро – повинен дублюватися як у приватних, так і в загальнодоступних мережах. Кожен сервер має бути оснащений як мінімум двома двопортовими мережевими картами. Один порт на кожній мережевій карті повинен використовуватися для підключення до приватної мережі, а інший – для загальнодоступної. Кожен порт має бути під'єднано до окремого комутатора, тобто кожен сервер під'єднано до двох загальнодоступних і двох приватних мережевих комутаторів. Потім кожен листовий комутатор повинен підключатися до двох хребетних комутаторів, кожен з яких підключається до одного з двох маршрутизаторів. Кожен маршрутизатор приватної мережі повинен мати два підключення до приватної мережі.

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

Створювана мережа повинна мати змогу на розширення мережі шляхом під’єднання суміжних мереж за допомогою фізичної спроможності мережевого обладнання.

2.1.1.1.4 Вимоги до режимів функціонування мережі

Підрозділи мережі повинні виконувати свої обов'язки цілодобово.

Відділ технічної підтримки повинен обслуговувати клієнтів компанії, займатися налаштуванням серверів та розробкою модифікацій серверів під клієнтів, виконувати налаштування апаратного та програмного забезпечення мережі.

Мережевий відділ повинен реалізувати безпеку в мережевій інфраструктурі компанії, конструювати IP-адресацію клієнтів, налаштовувати мережеве обладнання та мережеві адаптери серверів та пристроїв співробітників.

Відділ тестувальників повинен займатися впровадженням автоматизації багатьох систем задля уникнення технічних помилок від втручання рук людини, також перевіряти нові оновлення програмного забезпечення, прошивки серверів та тестувати працездатність нових операційних систем.

Інженерний відділ управління повинен знаходитися в дата-центрі та виконувати завдання компанії на фізичному рівні, а саме – підключення серверів в стійки, заміна комплектуючих, аналіз апаратного рівня в дата-центрі, перепідключення з’єднання мережевих адаптерів, обслуговування мережевого обладнання і т.д.

2.1.1.1.5 Вимоги до діагностування мережі

Діагностування працездатності мережі повинно виконуватися за допомогою двох складових:

– перевірка на програмному рівні;

– перевірка на фізичному рівні.

Співробітники технічної підтримки та мережевого відділу повинні застосовувати спроможність операційних систем та для діагностики мережі використовувати улитиліти командного рядку.

Співробітники інженерного відділу повинні здійснювати обхід усього обладнання дата-центру не менше 5 разів за робочий день. Співробітники повинні перевіряти індикацію на кожному пристрої, робоча індикація має жовте і зелене світло. Якщо співробітник побачив червону індикацію, він повинен повідомити в технічну підтримку номер і стійку обладнання.

2.1.1.1.6 Перспективи розвитку та модернізації мережі

Модернізація мережі повинна відбуватися за допомогою заміни комплектуючих серверів, заміни серверів на більш нові версії, заміна мережевого обладнання на нове покоління. Мережевий відділ та технічна підтримка мають слідкувати за обладнанням в мережі та робити модернізацію по можливості, або виконувати модернізацію за замовленням клієнта.

2.1.1.2 Вимоги до показників призначення

Корпоративна мережа служить для обслуговування інформаційних проєктів клієнтів, таких як сайти, ігри, магазини тощо. Мережа має відповідати всім заданим вимогам клієнта. Головною ідеєю мережі є видача фізичної потужності серверного обладнання клієнту.

2.1.1.3 Вимоги до експлуатації

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

Підмережі офісного приміщення не потребують додаткових умов експлуатації.

Дата-центр повинен мати спеціальні системи кондиціонування повітря побудовані шляхом впровадження технологій інтернет речей (IoT), для забезпечення оптимальних умов температури та вологості. Температура повинна знаходиться в діапазоні 18-27°C (64-80°F), а вологість повітря – в діапазоні 40-60%.

2.1.1.3.2 Вимоги до параметрів мереж енергопостачання

Дата-центри повинні працювати за стандартною напругою та частотою електромережі, а саме використання – 220-240V при частоті 50Гц або 60Гц.

Сервери повинні використовувати двофазні системи живлення.

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

Організаційне забезпечення мережі повинно включати навчання та розвиток персоналу, який відповідає за управління мережею.

Чисельність персоналу системи управління має бути 14 працівників, які займають посади у відділі технічної підтримки, відділі тестувальників та мережевому відділі.

Всі співробітники повинні мати вищу освіту за технічним напрямком з інформаційних систем. Також, має бути виключення для людей які ще навчаються у вищих навчальних закладах і мають змогу поєднувати роботу та навчання.

Кожного дня співробітники мають отримувати навички з англійської та української мови. Також, в певні періоди часу повинні відбуватися перевірки знань за пройдений час роботи.

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

Склад дата-центру повинен вміщувати різну кількість конфігурації серверів, мережевого обладнання та комплектуючих в залежності від навантаження роботою дата-центру.

У разі виникнення гарантійного випадку, товар має бути оформлений на повернення виробнику.

Умови збереження обладнання повинні відповідати таким самим як у пункті 2.1.1.3.1.

2.1.1.3.5 Вимоги до регламенту обслуговування мережі

Регламент обслуговування мережі повинен знаходитися у виді документів, в яких повинно бути вказаний графік проведення робіт та відповідальний за обслуговування. Обслуговування мережі дата-центру повинно відбуватися не менше ніж одного разу на день.

В обслуговування мережі входить:

– заміна серверів;
– побудова стійок;
– заміна комплектуючого обладнання в серверах;
– оновлення прошивок;
– заміна мережевого обладнання.

2.1.1.4 Вимоги до патентної чистоти

Мережа дата-центру призначена для роботи та знаходиться в країні США.

У випадку, коли можуть бути окремі технологічні рішення або інновації, які використовуються у зв'язку з дата-центрами або мережами, нові методи охолодження, енергозберігаючі рішення, програмні алгоритми тощо. У такому випадку, для отримання патенту на такі рішення, необхідно виконати вимоги до патентної чистоти країни, де знаходиться дата-центр, а саме – США.

Отримання патенту в США передбачає забезпечення новизни, непочатковості та неочевидності винаходу відносно публікацій та використання в США та світі. При поданні патентної заявки в США, заявник повинен провести дослідження на наявність подібних або аналогічних технологій, що можуть вплинути на патентну чистоту.

2.1.1.5 Додаткові вимоги

2.1.1.5.1 Вимоги до активного обладнання

Мережа повинна мати достатню пропускну здатність для передачі даних, а саме – 1000 Мбіт /с.

Комутатори повинні забезпечувати наступні вимоги:

– 24 порти гігабітної мережі;

– швидкість передачі даних до 10 Гбіт /с.;

– стандарт 100BASE-TX;

Маршрутизатори повинні забезпечувати наступні вимоги:

– технологія 100 мбіт/с;

– технологія 1 гбіт/с;

– технологія 10 гбіт/с

– протоколи Ethernet, Fast Ethernet, Gigabit Ethernet.

Мережеве обладнання мережі повинно мати запас невикористовуваних портів у співвідношені 10% від загальних портів.

Функціональність активного обладнання повинно включати:

– комутацію пакетів;

– маршрутизацію;

– балансування навантаження;

– фільтрацію трафіку;

– безпеку мережі.

Встановлення активного обладнання повинно виконуватися в стійку.

2.1.1.5.2 Вимоги до кабель каналів, інформаційним та електричним розеткам

Вимоги для обладнання кабельної системи офісів керування:

– кабель канал повинен мати настінне розміщення, розмір 15мм х 15мм та повинен бути пластиковим;

– інформаційні розетки повинні мати тип RJ-45, використовувати монтаж на стіні та забезпечувати розмір 86мм х 86мм.

Вимоги для обладнання кабельної системи дата-центру:

– кабель канал повинен мати настінне розміщення, розмір 15мм х 15мм та повинен бути пластиковим;

– інформаційні розетки повинні мати тип SC, використовувати монтаж на стіні та забезпечувати розмір 25мм х 15мм;

– горизонтальні кабельні організатори повинні мати розмір 40мм х 60мм, монтуватися у стійки та повинні бути пластиковими.

Електричні розетки в офісі та дата-центрі вже існують та не потребують розробки.

2.1.1.5.3 Вимоги до комунікаційного обладнання і його розташування

Комунікаційне обладнання повинно бути розташоване в спеціально призначених приміщеннях.

Тип шафи потрібно використовувати – стійки. Кабельні траси повинні бути правильно сплановані і встановлені, забезпечуючи належну організацію, захист і доступність кабелів. Тип підводу кабельних повинен включати використання кабельних каналів.

Розташування комунікаційного обладнання повинно бути правильно організоване і забезпечувати належну вентиляцію, а саме розташовувати так, щоб між кожним обладнанням в стійці було вільне місце в 1U.

2.1.1.5.4 Вимоги до однорідності

Тип кабелю структурованої кабельної системи офісів управління потрібно використовувати UTP cat5e з роз’ємом розеток RJ-45.

Тип кабелю структурованої кабельної системи дата-центру потрібно використовувати оптоволокно з роз’ємом розеток SC.

Електричні розетки в обох випадках потрібно використовувати типу C (розетка Europlug).

Кількість довжини кабелю, інформаційних та електричних розеток повинна забезпечувати підключення пристроїв в мережі згідно кількості користувачів в мережі. Для можливої майбутньої модернізації мережі потрібно використовувати запас всіх розеток у 10%.

Всі комп’ютери та сервери в офісі повинні бути підключені кабелем – вита пара. Сервери та мережеве обладнання в дата-центрі мають бути підключені за допомогою високошвидкісного оптоволоконного кабелю.

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

2.1.2.1 Вимоги до кожної підмережі та переліку їх функцій

Для працездатності мережевих пристроїв повинно бути проведено базове налаштування конфігурації пристроїв, а саме:

– повинно бути назначено назви пристроям за наступним правилом – прізвище студента_тип пристрою_номер пристрою, наприклад, Vihman_Router_1;

– на всіх пристроях повинно бути назначено пароль cisco до консолі і vty;

– на всіх пристроях повинно бути назначено пароль class до привілейованого режиму;

– усі паролі, що зберігаються у відкритому вигляді, під час налаштування моделі комп’ютерної системи повинні бути зашифровані;

– повинно бути розроблено банер MOTD;

– повинно бути назначено на усіх лініях vty використання протоколу ssh;

– повинно бути призначено на всіх пристроях користувача за правилом – група_прізвище, наприклад 123181_Vihman, з паролем admincisco;

– в якості імені домена повинно бути використно ім'я пристрою. Для шифрування даних повинно бути створено ключ RSA завдовжки 1024 біт;

– на DCE-інтерфейсах маршрутизаторів повинно бути призначено встановлення значення тактової частоти – 128000;

– повинно бути налаштувано аудит і відправку повідомлень про початок і завершення процесу exec, з використанням локальної бази.

Для налаштування протоколу маршрутизації повинно бути:

– оголошені безпосередньо підключені мережі і відключені поширення оновлень маршрутизації на інтерфейси в локальні мережі;

– для VLAN мереж налаштовано сумарний маршрут і оголошено його іншим маршрутизаторам;

– у разі реалізації в мережі протоколу OSPF змінено еталонну пропускну спроможність для обчислення вартості за умовчанням для дозволу інтерфейсів Gigabit на значення = 1000;

– задано пропускну спроможність на serial-інтерфейсах = 128 Кб/с, вартість метрики = 7500;

– налаштовано маршрут за замовчанням на маршрутизаторі з прямим підключенням до інтернет-провайдера (ISP) і розповсюджено його через оновлення маршрутизації;

– налаштувано на цьому маршруті ручне підсумовування (протокол маршрутизації підсумовує тільки підмережі організації), включено в таблицю приєднані мережі;

– додано статичні маршрути так, щоб будь-які два комп’ютера мережі могли взаємодіяти один з одним.

Налаштувати всі маршрутизатори на підтримку служби AAA необхідно таким чином:

– для перевірки підключень до VTY ліній на маршрутизаторі повинно бути використано локальну базу даних користувачів;

– для доступу до консолі повинно бути використано аутентифікацію на основі протоколу RADIUS і якщо немає − локальну базу даних;

– RADIUS-сервер повинен бути налаштований наступним чином – ключове слово – radius123; в якості облікового запису користувачів повинно бути використано ім’я пристрою з паролем admin123.

Для налаштування роботи Інтернет в системі повинні бути впроваджені технічні заходи.

Повинно бути встановлено одного провайдера послуг доступу до Інтернет (ISP).

Для виходу робочих станцій в Інтернет повинно бути налаштовано пограничний маршрутизатор з динамічним NAT за такими даними:

– ім’я пула: Internet;

– пул адресів: 209.165.200.5 по 209.165.200.30;

– номер списку доступу згідно номеру варіанта студента за списком у групі.

Повинно бути налаштовано сервер HTTP, щоб на вузлах при вводі в рядку браузера http://123.dnipro.ua (http://209.165.200.4) відкривався веб-сайт з відомостями про тему та завдання на кваліфікаційну роботу студента.

2.1.2.2 Часовий регламент і вимоги до якості реалізації кожної функції

Система повинна використовувати глобальну приватну мережу(GPN), яка буде поєднувати три континенти по 20 Гбіт/с з кожним виділеним сервером. Приватна мережа повинна бути захищена як на фізичному, так і на логічному рівні, щоб забезпечувати максимально швидку та безпечну передачу даних.

GPN повинна давати змогу клієнтам організувати взаємодію своїх серверів без використання додаткового тунелювання та VPN. Адресний простір приватної мережі клієнта (CPN) повинен виділятися клієнту під час першого замовлення виділеного сервера. Адресний простір CPN повинен видаватися з мережі 10.0.0.0/8. Потім приватна мережа, що маршрутизується, використовується для об'єднання всіх виділених серверів клієнта, хмарних серверів і хмарного сховища.

Всі сервери повинні бути підключені до трьох різних мереж – загальнодоступної мережі (Інтернет), приватної мережі та зовнішньої мережі. Ці мережі мають бути незалежними.

Залежно від моделі шасі та розташування сервера він може мати або не мати агрегацію каналів та резервування з'єднань, це все повинно відповідати специфікаціїї дата-центру.

Корпоративна мережа повинна мати локальний діапазон мереж – 192.168.7.0/24 з провадженням протоколу NAT з використанням мережі 209.165.202.0/30.

В маршрутизації віддаленної мережі повинна застосовуватися мережа 64.100.13.0/30.

Налаштування пристроїв в мережі повинно виконуватися за допомогою автоматизованого протоколу DHCP.

Для резервування конфігурацій мережевого обладнання потрібно використовувати TFTP сервер.

Безпека комп’ютерної мережі та мережевих пристроїв повинно забезпечуватись за допомогою сервера AAA.

Головною вимогою мережі та роботи сервера – є безперебійна робота та доступність його апаратних переваг в online часі. Так як сервер завжди має завдання для виконання від користувачів, то сервер не повинен знаходитися у статусі – без доступу. Тому мережі налаштовуються на рівні L3.

Як приватні, так і загальнодоступні мережі є рівнем мережі L3. Структурна архітектура рівні L3 між серверами не повинно мати прямого підключення L2.

Простіше кажучи, у сегменті L2 кожного сервера структури L3 є лише два хости – сам сервер та шлюз.

Оскільки між серверами в структурі L3 немає зв'язку L2, додаткові IP-адреси сервера є IP-псевдонімами, що маршрутизуються, і не можуть використовуватися спільно серверами.

Жодна помилка конфігурації ніколи не повинна призводити до витоку даних із приватної мережі в Інтернет. Приватні та загальнодоступні мережі повинні будуватися на різному обладнанні, тому жодна логічна помилка не призведе до того, що конфіденційні дані будуть не там де потрібно.

IP-мережа – єдиний спосіб досягти справжньої надмірності. Традиційні мережі L2, побудовані з використанням протоколу сполучного дерева, який використовує лише один «кращий шлях», вибраний з усіх доступних шляхів, означає, що існує активна/резервна надмірність. Проблема в тому, що в той момент, коли щось піде не так, ви не можете бути впевнені, що резервний шлях надійний. На відміну від цього, мережа L3, використовує всі доступні шляхи одночасно, залишаючись при цьому стабільною та уникаючи петель у мережі.

IP-мережа повинна бути захищена від комутаційних петель, тобто щоб було неможливо вивести з ладу всю мережу через помилку конфігурації. Він також має бути захищений від невідомого unicast-флуду, коли DoS-атака на одного клієнта може паралізувати всю мережу, помножену на мережеве обладнання.

Комутатори у мережі L3 повинні бути пов'язані між собою таким чином, щоб між будь-якими двома серверами можливе з'єднання з трьома переходами. Кожен сервер має бути підключений до чотирьох «кінцевих» комутаторів (так називається верхній комутатор L3), двох для загальнодоступної мережі та двох для приватної мережі. Кожен листовий комутатор має бути підключений до двох комутаторів хребта. Це забезпечить надмірність та буде гарантувати низьку затримку всередині POD: кожен сервер може зв'язатися з будь-яким іншим сервером не більше ніж за три переходи.

2.1.3 Вимоги до видів забезпечення комп’ютерної системи

2.1.3.1 Вимоги до математичного забезпечення

При розробці корпоративної мережі повинен бути виконаний розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі підприємства.

Вхідні дані наступні:

– найбільша кількість вузлів 45;
– середній показник інтенсивності трафіку: $\mu = 178$ (кадрів/с);
– розмір повідомлення в середньому: 650 байт;
– передача пакету не повинна перевищувати ≤ 6 мс;
– загальна кількість користувачів – 120

Також, маршрутизація мережі повинна застосовувати математичний алгоритм протоколу OSPF.

2.1.3.2 Вимоги до інформаційного забезпечення

2.1.3.2.1 Вимоги до складу, структури і способів організації даних у мережі

Дані в системі повинні бути організовані за допомогою певних структур, таких як таблиці, схеми або рисунки. Це дозволить зберігати та обробляти дані в впорядкованому форматі.

2.1.3.2.2 Вимоги до інформаційної сумісності із суміжними мережами

Вимоги до інформаційної сумісності повинні визначати, які протоколи зв'язку повинні підтримуватися для взаємодії з суміжними мережами. Це повинні бути стандартні мережеві протоколи, такі як TCP/IP та Ethernet.

Вимоги до інформаційної сумісності також повинні включати вимоги до стандартів безпеки, які повинні дотримуватися для забезпечення безпеки обміну даними з суміжними мережами. Це повинні бути стандарти шифрування, аутентифікації, авторизації та контролю доступу, які використовуються для захисту даних під час передачі.

2.1.3.2.3 Вимоги до структури процесу збору, обробки, передачі даних у мережі і представлення даних

Вимоги до структури процесу збору даних повинні визначати, які джерела даних будуть використовуватися і як ці дані будуть збиратися. Дані повинні збиратися за допомогою ручне введення з клавіатури.

Вимоги до структури процесу обробки даних повинні описувати, як дані будуть оброблятися після їх збору. Обробка даних після збору повинно включати в себе фільтрацію та аналіз даних.

Вимоги до структури процесу передачі даних повинні описувати, як дані будуть передаватися в мережі. Дані по мережі повинні передаватися за допомогою протоколів передачі даних.

Вимоги до структури процесу представлення даних повинні визначати, як дані будуть відображатися або представлятися користувачам або системам. Представлення даних користувачів повинно бути відображено в якості звітності або візуалізації даних.

2.1.3.2.4 Вимоги до контролю, збереження і відновлення даних

Для безпеки даних повинні використовуватися вимоги щодо аутентифікації, авторизації, шифрування даних, фізичної безпеки серверних приміщень та інших заходів, що забезпечують безпеку даних.

Резервне копіювання даних повинно включати вимоги до періоду копіювання, зберігання копій даних на віддалених серверах або хмарних платформах, а також процедури відновлення даних.

Моніторинг даних повинен включати вимоги до систем моніторингу, ведення журналів подій, аналізу логів та інших процедур, які допомагають виявити та відстежити незвичайну або несанкціоновану діяльність з даними.

2.1.3.3 Вимоги до лінгвістичного забезпечення

Мережа повинна підтримувати різні мови, що використовуються користувачами, і забезпечувати правильне відображення та обробку текстової інформації на різних мовах.

Вимоги до лінгвістичного забезпечення також повинні включати машинний переклад тексту з однієї мови на іншу.

Також, повинні включати можливість розпізнавання мовного вводу користувачів.

2.1.3.4 Вимоги до технічного забезпечення

2.1.3.4.1 Вимоги до технічних засобів, у тому числі до видів програмно-технічних комплексів

Робочі станції співробітників повинні відповідати мінімальним вимогам:

– ОЗП 6гб;

– SSD 256гб.

Операційні системи повинні мати різні версії для зручності користування співробітникам, а саме використовуватися:

– windows – 7/8/10/11;

– linux;

– cisco IOS.

Для обробки інформації та аналізу працездатності мережі повинно бути встановлене наступне програмне забезпечення:

– microsoft Office 365;

– slack;

– google chrome;

– networkMiner.

Комплектуючі серверів повинні відповідати вимогам жорстких дисків:

– 240/480/960 gb SSD;

– 1/2/4/8/16 TB HDD;

– 250/500/1000 gb NVMe SSD.

Кошики для жорстких дисків у сервери повинні відповідати наступним формакторам:

– 2.5”;

– 3.5”.

Технічні вимоги мережевого обладнання були розглянуті в пункті 2.1.1.5.1.

2.1.3.5 Вимоги до організаційного забезпечення

2.1.3.5.1 Вимоги до структури і функцій підрозділів, що беруть участь у функціонуванні мережі

Вимоги до керування змінами повинні визначати процедури та вимоги до впровадження змін у мережевому середовищі. Це повинні бути вимоги до затвердження змін, тестування, документування, забезпечення сумісності та інших аспектів, що забезпечують контрольовану та безпечну впровадження змін.

Вимоги до чисельності та якості персоналу було розглянуто в пункті 2.1.1.3.3.

Функціонування підрозділів мережі більш детально було описано в пункті 2.1.1.1.4.

2.1.3.5.2 Вимоги до захисту від помилкових дій персоналу мережі

Зберігання і передавання приватної інформації повинно виконуватися надійно з застосуванням алгоритму шифрування даних, який матиме відповідну сертифікацію.

Вимоги повинні включати використання сильних паролів, багаторівневу авторизацію та обмеження прав доступу в залежності від ролі користувача.

Вимоги повинні включати ведення журналів дій користувачів, виявлення підозрілих активностей та системи сповіщень про незвичайні події.

2.1.3.6 Вимоги до методичного забезпечення

Методичне забезпечення мережі повинно включати документацію, яка описує архітектуру мережі, конфігураційні налаштування, процедури установки та налагодження, політики безпеки, зразки схем мережі та іншу важливу інформацію.

Дана документація мережі повинна слугувати як навчальні матеріали для співробітників, вони повинні допомагати адміністраторам та користувачам отримувати необхідні навички для управління та використання мережі.

Також, методичне забезпечення повинно містити методики відладки мережевих проблем та усунення неполадок. Це включає опис загальних проблем, їх можливі причини та кроки для їх виявлення і вирішення. Така документація повинна допомагати забезпечити швидке та ефективне відновлення роботи мережі в разі виникнення проблем.

Забезпечення повинно включати опис політик безпеки, резервного копіювання даних, моніторингу мережі, управління ресурсами та інші важливі процедури.

2.2 Розробка апаратної частини системи

2.2.1 Розробка та моделювання структурної схеми комплексу технічних засобів комп’ютерної системи з урахуванням структури георозміщення об’єкту

За аналізом поставлених завдань та технічних вимог створюємо схему комплексу технічних засобів, яка складається з мереж та підмереж компанії Servers.com. Вона містить в собі 3 офіси управління та обробки інформацією, а також дата-центр, який містить в собі сервери для надання послуг клієнтам під хостингову систему.

Апаратне забезпечення мережі має маршрутизатори, комутатори, сервери та комп'ютери.

Схема складається з:

– першого рівня – провайдера інтернету;
– другого рівня – ядра компанії та її маршрутизації;
– третього рівня – доступу та комутації;
– четвертого рівня – користувачів, кінцевих пристроїв співробітників.

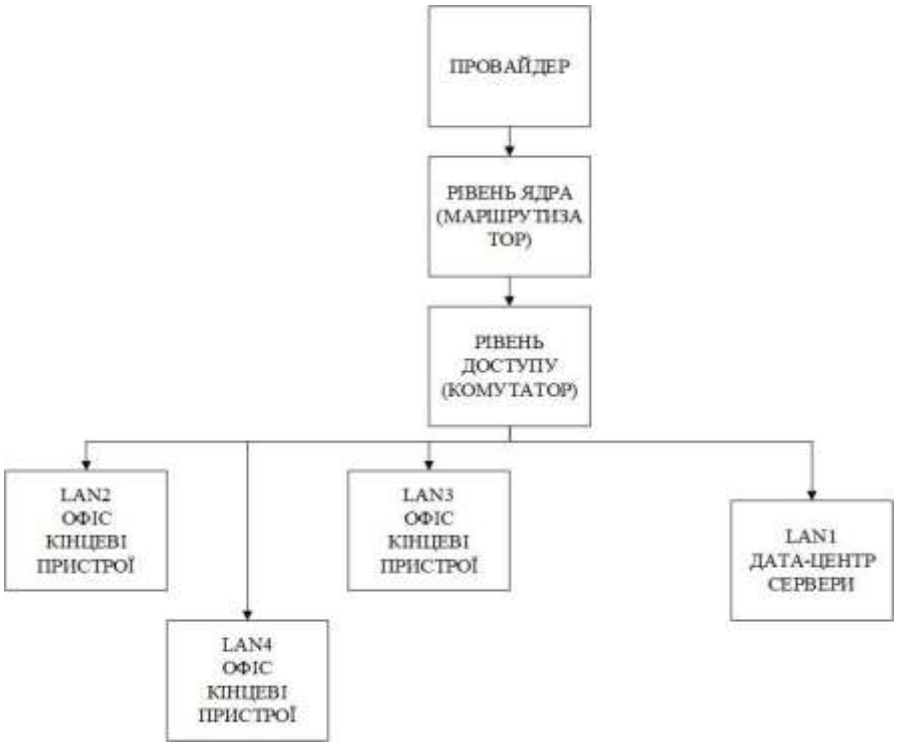

Рисунок 2.1 – Структурна схема комплексу технічних засобів

На основі структурної схеми (рисунок 2.1) створюємо таблицю де вказана кількість кінцевих пристроїв в кожному офісі, а також серверів в дата-центрі. Таблиця розроблена відповідно проекту створеному в програмі Cisco Packet Tracer.

Таблиця 2.1 – Кількість кінцевих пристроїв

Мережа	Призначення	Ідентифікатор	Тип	Кількість
LAN1	Дата-центр	Server_7-15	Server	9
LAN2	Офіс управління	PC1_10-3_10	PC	3
		PC1_20-2_20	PC	2
		Server HTTP VLAN 10	Server	1
		PC1_30-3_30	PC	3
LAN3	Офіс управління	PC13-14	PC	2
		Server DNS	Server	1
LAN4	Офіс управління	PC1-4	PC	4
		Server TFTP	Server	1

Моделювання підключення вузлів дата-центру відбувається за вимогами проєкту. Схема складається з офісу керування та дата-центру.

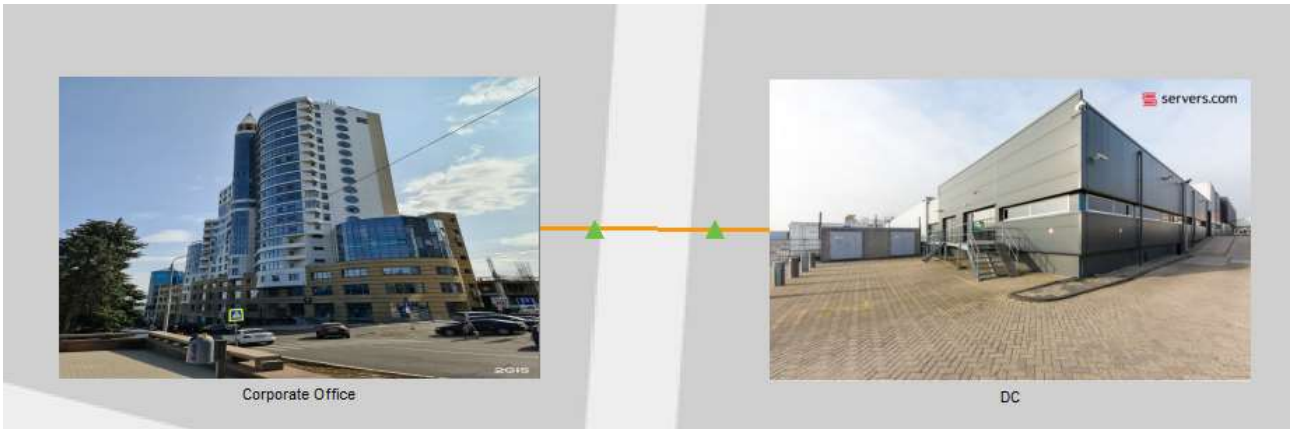

Рисунок 2.2 – Схематичне зображення вузлів мережі

Підключення здійснюється за допомогою оптоволоконного кабелю з використанням прикордонних інтернет-провайдерів.

Рисунок 2.3 – Підключення кінцевих пристроїв

Сервери, комутатори та маршрутизатори підключаються оптоволоконним кабелем в самому дата-центрі, за (рисунок 2.3). К кожному комутатору підключені певні сервери. Об’єднує всі комутатори в одну мережу – маршрутизатор.

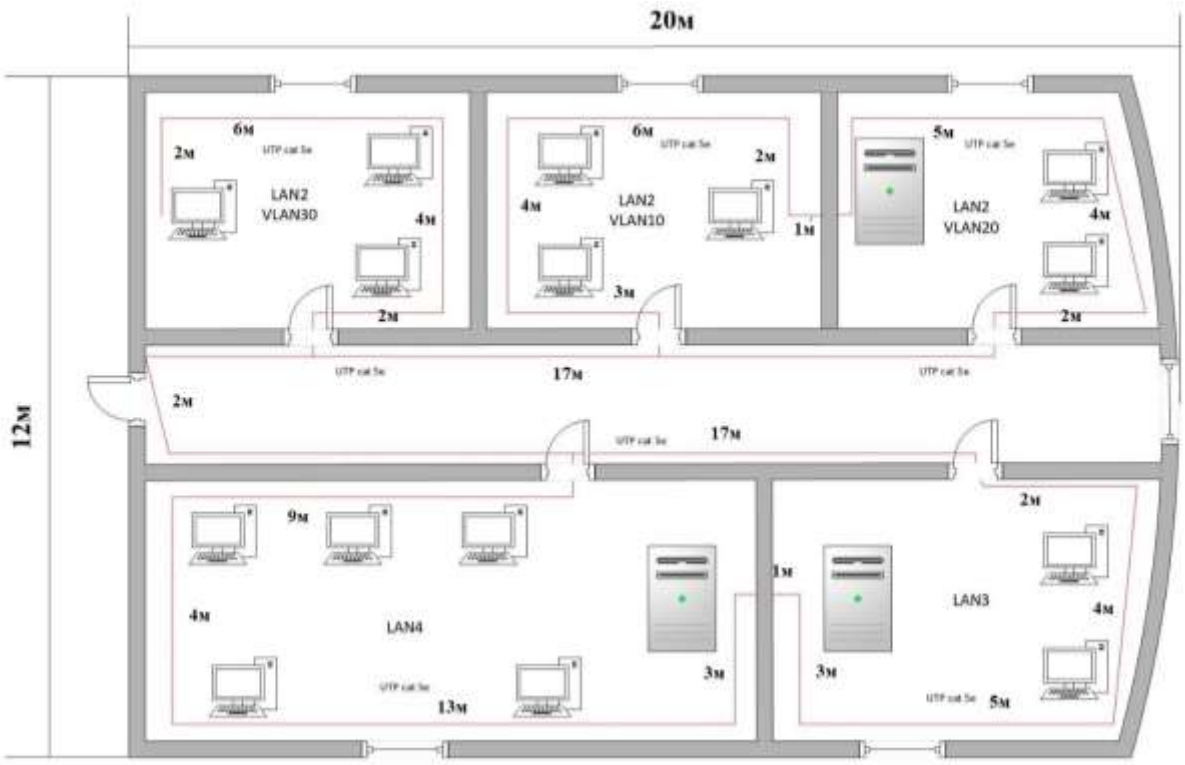

Рисунок 2.4 – Вигляд фізичного підключення вузлів в офісі

Офіс має другий поверх на якому знаходяться три підмережі.

Остання одна підмережа є центром обробки даних. Вона складається з серверів та мережевого обладнання, та має підключення всіх пристроїв за допомогою оптоволоконного кабелю.

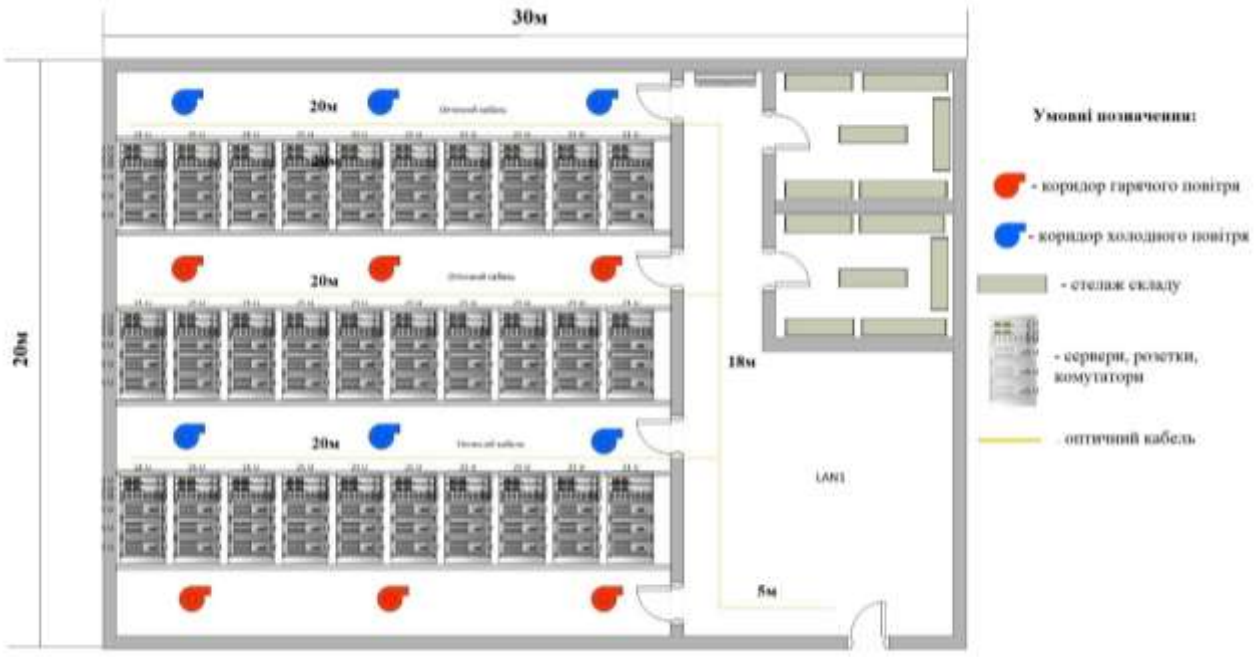

Рисунок 2.5 – Вигляд відключення вузлів дата-центру

Відповідно до (рисунок 2.4) та (рисунок 2.5) була створена специфікація структурованих кабельних систем і відображена у таблиці 2.2.

Відповідно до схематичних розрахунків для прокладання мережевого кабелю в офісі управління потрібно 150м кабелю вита пара.

Відповідно до схематичних розрахунків для прокладання мережевого кабелю в дата-центрі потрібно 150м оптоволоконного кабелю. По розрахункам ми отримуємо 83м, але для підключення пристроїв в стійках ми використовуємо залишкова 67м.

Таблиця 2.2 – Специфікація структурованих кабельних систем

Позиція	Найменування і технічна характеристика	Тип, марка, позначення документа	Одиниці виміру	Кількість	Примітка
1	Кабельний канал 15мм х 15мм, 2м	Sokol	од	70	За проектом офісу

Кінець таблиці – 2.2

2	Розетка інтерфейсу RJ-45 UTP cat5e 86мм х 86мм	Vinga	од	20	За проектом офісу
3	Кабель вита пара UTP cat5e	Одескабель	м	150	За проектом офісу
4	Конектор RJ-45	Cablexpert	од	20	За проектом офісу
5	Стійка настінна 9U 280мм х 480мм	CMS-WB9U-480V-GR 19"	од	1	За проектом офісу
6	Кабельний канал 15мм х 15мм	Sokol	од	50	За проектом дата-центру
7	Розетка інтерфейсу SC 25мм х 15мм	Vinga	од	10	За проектом дата-центру
8	Горизонтальний кабельний організатор 40мм х 60мм	W&T	од	10	За проектом дата-центру
9	Оптоволоконний кабель SC	Одескабель	м	150	За проектом дата-центру
10	Конектор оптоволокна SC	Cablexpert	м	10	За проектом дата-центру
11	Стійка підлогова 24U 550мм х 1160мм	OF42DBK	од	3	За проектом дата-центру

2.2.2 Розробка специфікації апаратних засобів комп’ютерної системи

Дивлячись на поставлені вимоги проекту були обрані апаратні рішення, які повністю задовольняють потреби.

Також, дані рішення конфігурують в розробці проекту програми Cisco Packet Tracer та в налаштуванні мережі компанії Servers.com. Комутатори використовуємо для з'єднання всіх вузлів в одну мережу та маршрутизатори для з'єднання всіх підмереж в мережу.

З мережевого обладнання були використані комутатори Catalyst 2960 та маршрутизатори Cisco 2911.

Комутатор Catalyst 2960 – це мережевий пристрій комутації мережі, що має змогу підключити 24 користувача та надати максимальну швидкість передачі даних.

Рисунок 2.6 – Вигляд комутаторів Catalyst 2960

Технічні характеристики:

– 24 порти гігабітної мережі Ethernet;
– 64 Мб флеш-пам'яті;
– швидкість передачі даних до 10 Гбіт / с.;
– стандарт 100BASE-TX;
– універсальний порт Ethernet 2 x SFP.

Маршрутизатор Cisco 2911 – це мережевий пристрій маршрутизації мережі, який має функцію об’єднання комутаторів до загальної корпоративної мережі компанії.

Рисунок 2.7 – Вигляд маршрутизаторів Cisco 2911

До технічних характеристик відносять:

– 3 x інтерфейс Ethernet 10Base-T / 100Base-TX / 1000Base-T, роз'єм RJ-45;
– 1 x гігабітний WAN (RJ-45);
– 1 x гігабітний DMZ (RJ-45);
– швидкість передачі 1 Гбіт / с.;
– протокол Ethernet, Fast Ethernet, Gigabit Ethernet.

Таблиця 2.3 – Специфікація мережевого обладнання

Позиція	Найменування і технічна характеристика	Тип, марка, позначення документа	Одиниці виміру	Кількість	Примітка
1	Комутатор Catalyst 2960 TC-L 24 x 10BaseT/100Base-TX - RJ45; 2 x Gigabit Ethernet Uplink	Catalyst 2960 TC-L	од.	7	За проектом у СРТ: Vihman_CopySw4 Vihman_CopySw5 Vihman_CopySw6 Vihman_Sw2,Vihman_Sw3 Vihman_Sw5, Vihman_Sw6
2	Маршрутизатор Cisco 2911 3 x GE RJ-45, 4 x EHWIC, 2 x DSP, 1 x ISM, 1 x SM	Cisco 2911	од.	6	За проектом у СРТ: Vihman_R0,Vihman_R1 Vihman_R2,Vihman_R3 Vihman_R4,Vihman_IPS

За вимогами по вибору серверів було узгоджено використовувати компанію Dell, яка буде повність покривати всі запроси.

Досвід доводить надійність серверів Dell і їхню цінність, зокрема низькі вимоги до обслуговування.

Сервери Dell постачаються з автономною підсистемою, що забезпечує можливості керування та моніторингу – iDRAC. iDRAC – це частина обладнання, яка розміщена на материнській платі сервера і дає змогу керувати сервером, навіть коли сервер вимкнений. iDRAC надає як веб-інтерфейс, так і інтерфейс командного рядка.

Будемо використовувати такі шасі: R220, R230, R240, R330, R340, R430, R440, R530, R540, R730xd, R740xd і T630.

Найменування моделей серверів зазвичай складається з літери, за якою йдуть три цифри (наприклад, PowerEdge R240). Угода про імена наступна:

– R – Форм-фактор (R – стійковий, T – баштовий)
– 2 – клас (1-3 для 1-процесорних систем, 4-7 для 2-процесорних систем)
– 4 – покоління платформи (з 4 для 14-го покоління)

– 0 – ЦП (0 для Intel і 5 для AMD)

Сервери R2xx. Система з одним сокетом (один ЦП) і одним блоком живлення в розмірі 1U. Встановлюються в серверні стійки, обладнані автоматичним введенням резерву

Рисунок 2.8 – Вигляд серверів R2xx

Сервери R3xx. Практично такий самий, як R2xx, але має два блоки живлення (БЖ).

Рисунок 2.9 – Вигляд серверів R3xx

Сервери R4xx. Двогніздова система 1U. Два процесори дають змогу використовувати більше оперативної пам'яті, більше ліній PCI тощо.

Рисунок 2.10 – Вигляд серверів R4xx

Сервери R5xx. Двогніздова система 2U. Має більше слотів для зберігання, слотів розширення і ліній PCI, ніж R4xx.

Рисунок 2.11 – Вигляд серверів R5xx

Сервери R7xx. Система з двома сокетами 2U для робочих навантажень зберігання та обробки даних. До 26 дисків 2,5 дюйма на сервер.

Рисунок 2.12 – Вигляд серверів R7xx

Сервери T6xx. Вони явно використовуються для серверів GPU. Незважаючи на те, що це корпус типу "вежа", його можна встановити в серверну стійку як блок висотою 5U.

Рисунок 2.13 – Вигляд серверів T6xx

Для комфортного осблуговування мережі та зручної роботи всіх співробітників з урахуванням вимог були обрані комп'ютер-моноблоки Acer Aspire C24-1600 (DQ.BHRME.001) Silver.

Рисунок 2.14 – Вигляд комп'ютер-моноблока

Він повністю задовольняє поставлені вимоги та має наступні характеристики:

– процесор Pentium Silver N6005(4 ядра – 2,0 (3,3) ГГц);
– ОЗП 6гб DDR4 3200МГц;
– SSD 256гб;
– діагональ екрану 23,8";
– роздільна здатність екрана 1920x1080 Full HD.

Всі користувачі офісного приміщення з’єднанні витою парою UTP cat. 5e.

UTP cat. 5e – це тип кабелю для передачі сигналу, що складається з чотирьох кручених пар.

Таблиця 2.4 – Специфікація офісного обладнання

Позиція	Найменування і технічна характеристика	Тип, марка, позначення документа	Одиниці виміру	Кількість	Примітка
1	Моноблок Acer Aspire процесор Pentium (4 ядра – 2,0 (3,3) ГГц) ОЗП 6гб DDR4 3200МГц SSD 256гб діагональ екрану 23,8" 1920x1080 Full HD	Acer Aspire C24-1600 (DQ.BHRME.001)	од.	14	За проектом у СРТ: PC_0(1-14)

Схема підключення пристроїв наведена у (рисунок 2.4 і рисунок 2.5).

Мережеве обладнання та сервери з’єднанні оптоволоконним кабелем.

Оптоволоконний кабель – кабель мережі, який розрахований використовуватися на великі відстані і забезпечувати високу швидкість передачі даних, створений із скла.

2.2.3 Розробка специфікації програмних засобів комп’ютерної системи

Відповідно вимогам проекту було обрано наступне програмне забезпечення:

– Microsoft Office 365;
– slack;
– google chrome;
– networkMiner.

Microsoft Office 365 – це сервіс від Microsoft, який надає доступ до пакета офісних продуктів і застосунків, таких як – Microsoft Word, Excel, PowerPoint, Outlook, OneNote, Publisher, Access та інших популярних застосунків, а також до сервісів спільної роботи й хмарного зберігання – Microsoft Teams, SharePoint і OneDrive.

Slack – це додаток корпоративної мережі, який застосовується для робочого спілкування і підходить під розміри великих компаній.

Google chrome – це додаток веббраузеру, для вирішення питань в мережі інтернет.

NetworkMiner – додаток, що слугує для дослідження та аналізу великих мережевих даних, при цьому надає повну візуалізацію мережі.

2.2.4 Розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі підприємства

Для розрахунку ключових характеристик вихідного трафіку, треба щоб мережа компанії Servers.com була завантажена на 100%.

Вхідні дані наступні:

– найбільша кількість вузлів 45;

– середній показник інтенсивності трафіку: μ = 178 (кадрів/с);

– розмір повідомлення в середньому: 650 байт;

– передача пакету не повинна перевищувати ≤6 мс;

– загальна кількість користувачів – 120

Вихідний трафік перенаправляється на маршрутизатор по лінії з пропускною здатністю 1000 Мбіт/с.

Пропускна здатність всієї мережі розраховується з урахуванням того, що мережею одночасно користується 100% користувачів. Пропускна здатність мережі обчислюється наступним чином:

Пропускна здатність мережі на рівні доступу:

$$Pp.д= \mu*l*n*8=178*650*24*8= 22,21 \text{ Мбіт/с}, \quad (2.1)$$

де n – кількість портів в комутаторі рівня доступу.

Пропускна здатність мережі на рівні розподілу обчислюється наступним чином:

З комутаторами рівня доступу, придатними для одного комутатора рівня розподілу та загалом 45 користувачів, пропускна здатність мережі на рівні розподілу така:

$$Pp.p = \mu * l * N * 8 = 178 * 650 * 45 * 8= 416,52 \text{ Мбіт/с}, \quad (2.2)$$

де N – кількість вузлів в найбільшій мережі.

Результати, отримані під час розрахунку, не перевищують зазначених параметрів мережі. Тому обране обладнання не буде перевантаженим.

Перемикач рівня розподілу перенаправляє трафік до маршрутизатора через вихідну лінію з пропускною здатністю 1000 Мбіт / с.

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

Кожне джерело виробляє в середньому 178 пакетів на секунду, що обмежує його до підключення до максимального розподілу на рівні комутації.

$$N = 192\,310 / 178 = 1080 \text{ джерел}. \quad (2.4)$$

Він заповнює мережу з 45 ПК. Кожен з 45 ПК посилає потік заявок з інтенсивністю 178 кадрів/с.

Інтенсивність вихідного трафіку від всіх користувачів:

$$\lambda = N \cdot \mu = 45 * 178 = 8010 \text{ (пакетів/с).} \quad (2.5)$$

Коефіцієнт затримки на рівні розподілу, показник навантаження на вихідний канал зв'язку, що впливає на затримку черги.

$$\rho = \lambda / \mu\text{вих} = 8010 / 192\,310 = 0{,}04 \quad (2.6)$$

Коефіцієнт зайнятості комутатора рівня розподілу:

$$r = \rho / (1 - \rho) = 0{,}04 / (1 - 0{,}04) = 0{,}038 \quad (2.7)$$

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

$$T=1/((\mu-\lambda))=1/(192\,310-8010)=18{,}4 \text{ мкс} \quad (2.8)$$

Середня довжина черги:

$$L\_чер=\rho^2/(1-\rho)=(0{,}04)^2/(1-0{,}04)=0{,}001 \quad (2.9)$$

Ця цифра корисна під час черги пристрою. В апаратному забезпеченні можна вказати максимальний розмір черги пакетів.

Середній час пакетів у черзі:

$$T\_оч=L\_чер/\lambda=0{,}001/8010=1{,}24 \text{ мкс} \quad (2.10)$$

Це значення менше необхідного значення ≤ 6 мс, що відповідає вимогам.

Пропускна здатність каналу:

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

$$b=\lambda*l=8010*650*8=41\,652\,000 \text{біт/с}=41{,}6 \text{ Мбіт/с} \quad (2.11)$$

Середнє значення пропускної здатності каналу розраховано та відповідає пропускній здатності вихідного каналу 1000 Мбіт /с.

Висновок до розділу

В ході написання розділу було розроблено структуровану кабельну систему мережі, апаратну складову компанії та структуровану схему комплексу технічних засобів. Розділ вміщує в собі схеми підключення вузлів мережі та прокладання кабелю. Дані апаратної частини занесені до таблиць. Також, був виконаний розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі підприємства.

3 РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Розрахунок налаштувань корпоративної мережі

3.1.1 Розробка архітектури мережі підприємства

Архітектура мережі підприємства створюється на основі головних вимог з поставлених завдань проекту.

Мережева архітектура компанії Servers.com з повним резервуванням є економічно ефективною, і на це є кілька причин. Однією з них є інтелектуальна кабельна система – рішення, яке дозволило довести використання портів на комутаторах до 100%, і, таким чином, знизити витрати.

Інша причина – розумний диспетчер трафіку, який дозволяє використовувати з'єднання з декількома операторами зв'язку.

Проектна мережа будується на основі вимоги IP-адресації, а саме використання мережі 192.168.7.0./24. За цією мережею були сформовані чотири IP-підмережі з урахуванням кількості користувачів у кожній. Дві підмережі LAN3 та LAN4 мають стандартний вигляд мережі, підмережа LAN2 має розподіл на три віртуальні підмережі та має налаштування мережі VLAN для безпеки даних в системі. Підмережа LAN1 є віддаленою мережею з серверами та використовує технологію агрегування каналів на комутаторах для підвищення швидкості передачі даних і забезпечення відмовостікойсті.

По завданню підмережі мають змогу вміщати в собі певну кількість користувачів (кінцевих вузлів).

Підмережа LAN1 – 28, LAN2 – 16, LAN3 – 45, LAN4 – 19. Всього мережа повинна витримувати 108 хостів.

Також по завданню проекту була з’ясована середня інтенсивність вихідного трафіку в найбільшій мережі, вона дорівнює 178(кадрів/с).

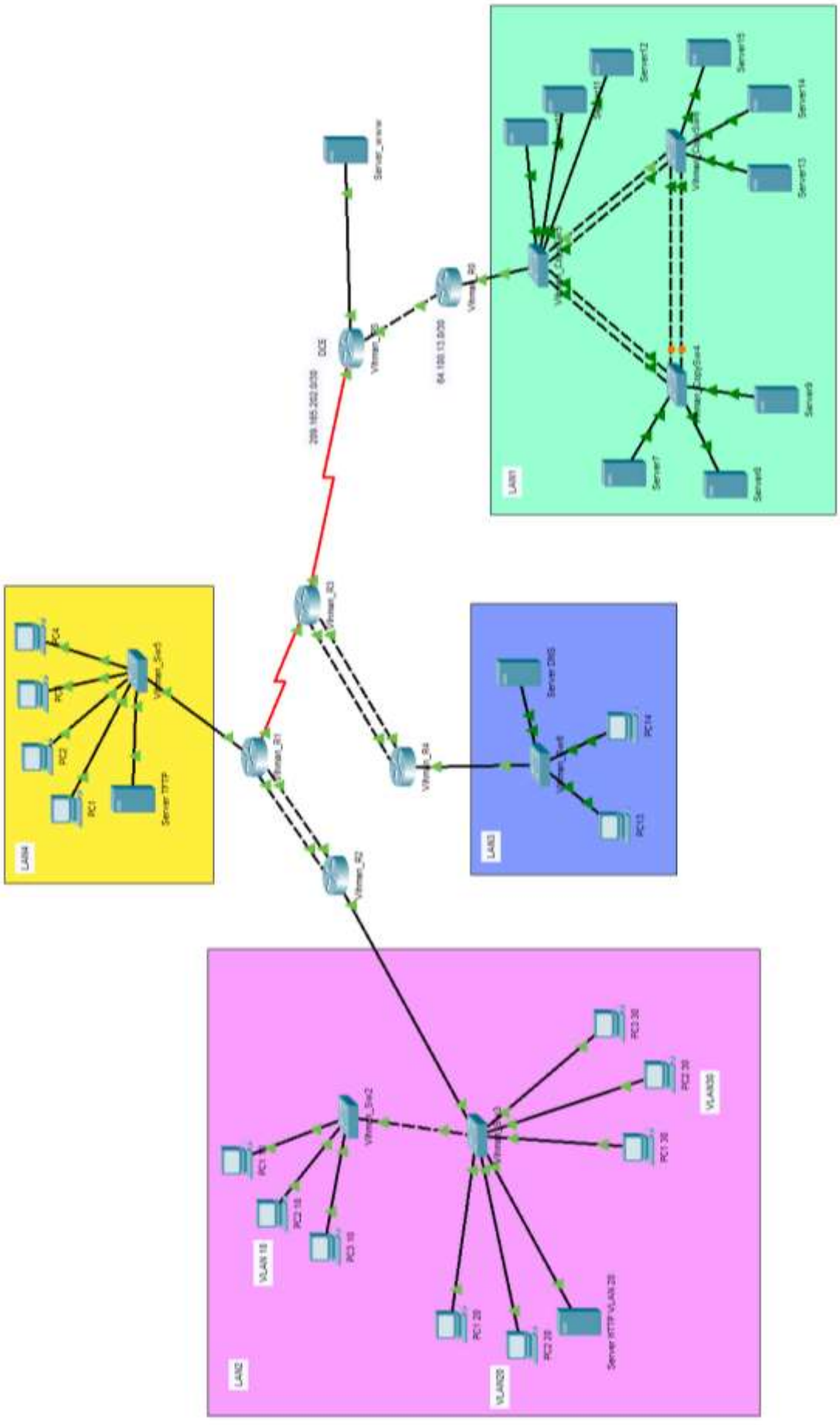

Рисунок 3.1 - Архітектура мережі компанії Servers.com

3.1.2 Розрахунок схеми адресації корпоративної мережі

При виконанні проекту був використаний адресний простір 192.168.7.0/24.

Даний простір має 254 кінцевих вузлів, від 192.168.7.1 до 192.168.7.254.

Так як, мережевий простір не великий, підмережі будемо створювати з хост частини IP-адреси.

Підмережа – це технологія, яка дозволяє зменшити складність мережі і дає більшу продуктивність, ніж одна велика мережа. Головною перевагою підмережі є легкість в управлінні та виявленні конфліктів. За економічним показником розподілення мережі на підмережі є дуже ефективним. На підмережі використовується мережеве обладнання середнього рівня, в той час коли на великій мережі середнього рівня буде не достатньо.

Зі свого боку мережа – це технологія більшого об'єму, яка створюється на певній топології мережі.

Таблиця 3.1 – Кількість вузлів в підмережі

Адреса	LAN1	LAN2	LAN3	LAN4
192.168.7.0/24	28	16	45	19

Тому, адресний простір 192.168.7.0/24 треба розподілити на 4 підмережі.

IP-адреса завжди логічно розділяється на дві частини: адреса підмережі та адреса конкретного вузла у підмережі. Маска підмережі використовується для визначення того, які біти вказують на мережу, а які – на хост.

Маска підмережі є числом, яке використовується поряд з IP-адресою, вона може бати два вигляди, наприклад 255.255.255.0 або /24.

Октети маски порівнюються з октетами IP-адреси, і отримане значення використовується для визначення адреси мережі та адреси хоста.

Наприклад, стандартна маска корпоративної мережі – 255.255.255.0, де перші три октети (або 24 біти) представляють мережу, а останній октет (8 біт) – хост. Застосовуючи цю маску до IP-адреси 192.168.7.100, ми бачимо, що це вузол під номером 100 у підмережі 192.168.7.0.

Розрахуємо адресу мережі та адресу вузла для підмережі LAN1, яка має адресу 192.168.7.160 з маско. 255.255.255.224 або /27. Початкова адреса цієї мережі – 192.168.7.161, кінцева – 192.168.7.190.

Маска також має двійковий вигляд – 11111111.11111111.11111111.111 | 00000.

Лінія | демонструє межу між адресою мережі та адресою вузла.

Дана підмережа має 30 доступних вузлів, починаючи з 11000000.10101000.00000111.101|00001 та закінчуючи 11000000.10101000.00000111.101 | 11110.

Таким чином розподіляється кожна підмережа з мережі 192.168.7.0/24.

Таблиця 3.2 – Параметри адрес підмережі центрального офісу

Назва підмережі	Кіл.вузлів	Адреса підмережі	Маска підмережі у десятк. форматі	Діапазон допустимих IP-адресів вузлів	
LAN3	45	192.168.7.0	255.255.255.192	192.168.7.1	192.168.7.62
LAN1	28	192.168.7.160	255.255.255.224	192.168.7.161	192.168.7.190
LAN4	19	192.168.7.128	255.255.255.224	192.168.7.129	192.168.7.158
LAN2	16	192.168.7.64	255.255.255.192	192.168.7.65	192.168.7.126
VLAN10	5	192.168.7.80	255.255.255.240	192.168.7.81	192.168.7.94
VLAN20	5	192.168.7.96	255.255.255.240	192.168.7.97	192.168.7.110
VLAN30	6	192.168.7.112	255.255.255.240	192.168.7.113	192.168.7.126
WAN1	2	10.0.3.0	255.255.255.252	10.0.3.1	10.0.3.2
WAN2	2	10.0.3.4	255.255.255.252	10.0.3.5	10.0.3.6
WAN3	2	10.0.3.8	255.255.255.252	10.0.3.9	10.0.3.10
WAN4	2	10.0.3.12	255.255.255.252	10.0.3.13	10.0.3.14
WAN5	2	10.0.3.16	255.255.255.252	10.0.3.17	10.0.3.18
WAN IPS	2	209.165.202.0	255.255.255.252	209.165.202.1	209.165.202.2
WAN Remote Network	2	64.100.13.0	255.255.255.252	64.100.13.1	64.100.13.2

3.1.3 Розрахунок схеми адресації пристроїв

За нашим адресним простором ми маємо 254 вільні IP-адреси. Тому завдання потребує від мережі 120 користувачів в підмережах та додаткові адреси на мережеве обладнання.

В залежності від вимог мережі підприємства Servers.com, мережа повинна створюватись з певними пунктами:

– перші доступні IP-адреси знаходяться на інтерфейсі маршрутизатора та нижче інтерфейсу LAN;

– другу можливу IP-адресу присвоюємо кожному комутатору локальній мережі;

– сервер зазвичай налаштовуються і їм присвоюються IP-адреси. IPадреса така ж, як і перша можлива адреса у мережі;

– остання використана IP-адреса буде призначена останньою;

– VLAN використовують адресацію кінцевих пристроїв через DHCP.

Адресація всіх пристроїв мережі топології наведено у таблиці 3.3.

Таблиця 3.3 – Схема адресації пристроїв мережі

Ім’я пристрою	Інтерфейс	IP-адреса	Маска	Шлюз	VLAN	Інтерфейс підключеного пристрою
Мережа IPS						
Vihman_IPS	S0/3/0	209.165.202.2	/30	–	–	S0/3/0
	G0/1	64.100.13.2	/30	–	–	G0/1
Host_IPS	NIC	209.165.201.5	/28	–	–	Fa0/1
Vihman_R3	G0/0	10.0.3.1	/30	–	–	G0/0
	G0/1	10.0.3.5	/30	–	–	G0/1
	S0/3/0	209.165.202.1	/30	–	–	S0/3/0
	S0/3/1	10.0.3.9	/30	–	–	S0/3/1
Мережа LAN4						
Vihman_R1	G0/0	10.0.3.13	/30	–	–	G0/0
	G0/1	10.0.3.17	/30	–	–	G0/1
	G0/2	192.168.7.129	/26	–	–	G0/2

Кінець таблиці 3.3

	S0/3/1	10.0.3.10	/30	–	–	S0/3/1
PC_1-4	NIC	192.168.7.132-192.168.7.135	/26	192.168.7.129	–	Fa0/2-5
Server_TFTP	NIC	192.168.7.131	/26	192.168.7.129	–	Fa0/1
Мережа LAN1						
Vihman_R0	G0/0	192.168.7.161	/27	–	–	G0/0
	G0/1	64.100.13.1	/30	–	–	G0/1
Server_7-15	NIC	192.168.7.162-192.168.7.170	/27	192.168.7.161	–	Fa0/1 – 0/3
Vihman_CopySw4	Vlan1	192.168.7.162	/27	192.168.7.161	–	Fa0/1
Vihman_CopySw5	Vlan1	192.168.7.163	/27	192.168.7.161	–	Fa0/2
Vihman_CopySw6	Vlan1	192.168.7.164	/27	192.168.7.161	–	Fa0/3
Мережа LAN3						
Vihman_R4	G0/0	10.0.3.2	/30	–	–	G0/0
	G0/1	10.0.3.6	/30	–	–	G0/1
	G0/2	192.168.7.1	/26	–	–	G0/2
Vihman_Sw6	Vlan1	192.168.7.2	/26	192.168.7.1	–	G0/2
PC_13-14	NIC	192.168.7.3-192.168.7.4	/26	192.168.7.1	–	Fa0/1-0/2
Server_DNS	NIC	192.168.7.5	/26	192.168.7.1	–	Fa0/3
Мережа LAN2						
Vihman_R2	G0/0	10.0.3.14	/30	–	–	G0/0
	G0/1	10.0.3.18	/30	–	–	G0/1
	G0/2	192.168.7.65	/28	–	–	G0/2
Vihman_Sw2	Vlan1	192.168.7.66	/28	192.168.7.65	–	G0/2
Vihman_Sw3	Vlan1	192.168.7.67	/28	192.168.7.65	–	G0/1
PC1.10-PC3.10	NIC	192.168.7.82-192.168.7.84	/28	192.168.7.81	10	Fa0/1-3 – Sw2
PC1.10-PC2.10	NIC	192.168.7.98-192.168.7.99	/28	192.168.7.97	20	Fa0/1-2 – Sw3
Server HTTP	NIC	192.168.7.100	/28	192.168.7.97	20	Fa0/3
PC1.10-PC3.10	NIC	192.168.7.114-192.168.7.116	/28	192.168.7.113	30	Fa0/15-17 – Sw3

3.1.4 Розробка схеми фізичної топології корпоративної мережі

У комп'ютерній мережі компанії використовується топологія «дерево».

Дерево – це топологія мережі, у якій кожен головний вузол з'єднаний зі своїми нижчими вузлами за принципом зірки, утворюючи комбінацію зірок. Дерева так само називають ієрархічними зірками.

Назва «дерево» прийшла з теорії графів. Перший вузол у дереві називається коренем, наступні вищі вузли називаються головними вузлами та меншого рівня нижчими. Отже, усі нижчі вузли, сполучені зі своїми головними вузлами, вони є батьками цих вузлів.

Таким чином, ця топологія поєднує в собі властивості двох інших топологій – шини і зірки.

Переваги цієї топології полягають у тому, що мережі з такою топологією легко розширюються та легко контролюються (виявлення несправностей і збоїв). Недоліки полягають у тому, що при відмові батьківського вузла відключають усі дочірні вузли (при відмові кореневого вузла відключає усю мережу), а пропускна спроможність обмежена (доступ до мережі може бути важким).

Детальне графічне зображення підключення пристроїв відображено у розділі 2.

Стандартна POD складається з 40 стійок по 36 серверів у кожній. Кожен сервер має дві мережеві карти Intel X540 або Intel I350. Кожна карта має два інтерфейси: один для приватної мережі та один для публічної.

У цій схемі немає єдиної точки відмови (SPOF).

Кабельна система між серверами і комутаторами, а також система комутаторів між стійками дозволили використовувати 100% портів. Таким чином, скоротивши витрати на мережеве обладнання приблизно на 25%.

Сервери встановлені в стійках. Кабелі приєднані повністю і ґрунтовно, після чого до кабелів ніхто не торкається.

Множинні повторні підключення збільшують імовірність людської помилки. Було вирішено повністю виключити цей фактор. Знизивши ризики клієнтів за допомогою технології Zero Touch, скоротили час підготовки сервера.

Технологія Smart Traffic Dispatcher допомагає оптимізувати розподіл трафіку по основних каналах і збільшити швидкість роботи. Система стежить за навантаженням на основні канали та намагається використовувати їх максимально ефективно. Крім того, Smart Traffic Dispatcher автоматично перенаправляє з'єднання для зменшення затримки.

3.2 Перевірка роботи комп’ютерної системи компанії

3.2.1 Базове налаштування конфігурації пристроїв

Після моделювання та створення мережі було виконано налаштування конфігурації мережевих пристроїв. А саме:

– налаштувати паролі для приватного режиму, консолі і vty;

– усі відкриті паролі зашифровані;

– встановлено банер MOTD;

– налаштований на усіх лініях vty використання протоколу ssh;

– для шифрування даних створено ключ RSA завдовжки 1024 біт;

– на DCE-інтерфейсах маршрутизаторів значення тактової частоти – 128000;

– в якості імені домена використовув ім'я пристрою.

Приклад налаштування на Vihman_R1:

Vihman_R1(config)#service password-encryption

Пароль для входу в привілейований режим:

Vihman_R1(config)#enable secret class

Встановлено парою на вхід до консольної лінії:

Vihman_R1 (config)#line console 0

Vihman_R1 (config-line)#password cisco

Налаштування запиту пароля при вході:

Vihman_R1 (config-line)#login

Vihman_R1 (config-line)#exit

Налаштування банера MOTD:

Vihman_R1 (config)#banner motd #123-20zck Vihman authorization PASSWORD#

Налаштування протоколу SSH, створення користувача 12320zck_Vihman з паролем cisco.

Vihman_R1 (config)#username 12320zck_Vihman password cisco;

Створення домену:

Vihman_R1 (config)#ip domain-name Vihman_R1

Для шифрування даних створено ключ RSA довжиною 1024 біт:

Vihman_R1 (config)#crypto key generate rsa

How many bits in the modulus [512]: 1024

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

Налаштування лінії VTY:

Vihman_R1 (config)#line vty 0 4

Встановлення необхідності введення логіну та пароля для входу лінії:

Vihman_R1 (config-line)#login local

Встановлення входу на лінію тільки по протоколу SSH:

Vihman_R1 (config-line)#transport input ssh

3.2.2 Налаштування маршрутизації корпоративної мережі

Відповідно до технічних вимог в компанії Servers.com використовується протокол динамічної маршрутизації OSPF.

Протокол OSPF – це проткол динамічної маршрутизації, який розрахований на автоматизований режим збереження та побудови таблиць маршрутів, для майбутнього використання для передачі файлів.

У мережах OSPF маршрутизатори або системи з однієї області підтримують одну й ту саму базу даних виявлених маршрутів, що описує топологію області. Кожен маршрутизатор або система в області створює свою базу даних інформації про стан каналів, яка складається з оголошень маршрутів (LSAs), отриманих від усіх маршрутизаторів або систем в області, а також від LSA, що генеруються самостійно. LSA – це пакет, що містить відомості про сусідів і оцінку шляху.

Використовуючи бази даних із виявленням маршрутів за станом зв'язку, кожен маршрутизатор або сервер за допомогою алгоритму пошуку найкоротшого шляху (SPF) будує дерево шляхів, у якому коренем є сам маршрутизатор або сервер.

Після того, як маршрутизатори або сервери мережі OSPF налаштовують інтерфейси, вони відправляють через інтерфейси OSPF пакети Hello за допомогою протоколу привітання Hello, для пошуку сусідів. Сусідами є маршрутизатори або сервери, що мають інтерфейси в загальній мережі. Потім вони обмінюються власними базами даних маршрутів для встановлення зв'язку.

Приклад налаштування на маршрутизаторі Vihman_R1:

Включити протокол OSPF на маршрутизаторі командою:

Vihman_R3 (config)#router ospf 1

Протоколу потрібно об’явити мережі, підключені до маршрутизатора.

Vihman_R3 (config-router)#network 10.0.3.0 0.0.0.3 area 0

Vihman_R3 (config-router)#network 10.0.3.4 0.0.0.3 area 0

Vihman_R3 (config-router)#network 10.0.3.8 0.0.0.3 area 0

Маршрут за замовчуванням на Vihman_IPS:

ip route 0.0.0.0 0.0.0.0 209.165.202.2

Для роботи протоколу по всій мережі треба об’явити мережі на всіх маршрутизаторах:

Vihman_R1 (config-router)#network 10.0.3.8 0.0.0.3 area 0

Vihman_R1 (config-router)#network 10.0.3.12 0.0.0.3 area 0

Vihman_R1 (config-router)#network 10.0.3.16 0.0.0.3 area 0

Vihman_R1 (config-router)#network 192.168.7.128 0.0.0.63 area 0

Vihman_R4 (config-router)#network 10.0.3.0 0.0.0.3 area 0

Vihman_R4 (config-router)#network 10.0.3.4 0.0.0.3 area 0

Vihman_R4 (config-router)#network 192.168.7.0 0.0.0.63 area 0

Vihman_R2 (config-router)#network 10.0.3.12 0.0.0.3 area 0

Vihman_R2 (config-router)#network 10.0.3.16 0.0.0.3 area 0

Vihman_R2 (config-router)#network 192.168.7.64 0.0.0.15 area 0

Vihman_R2 (config-router)#network 192.168.7.80 0.0.0.15 area 0

Vihman_R2 (config-router)#network 192.168.7.96 0.0.0.15 area 0

Vihman_R2 (config-router)#network 192.168.7.112 0.0.0.15 area 0

На serial-інтерфейсах відповідно до технічних умов задано пропускну спроможність = 128 Кб/с та визначим швидкість каналу 128000, та вартість метрики = 7500.

Vihman_R3 (config)#interface s0/3/0

Vihman_R3 (config-if)#bandwidth 128

Vihman_R3 (config-if)# clock rate 128000

Vihman_R3 (config-if)# ip ospf cost 7500

```
Vihman_R3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.165.202.2 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
S       10.0.1.8/30 is directly connected, Serial0/3/1
C       10.0.3.0/30 is directly connected, GigabitEthernet0/0
L       10.0.3.1/32 is directly connected, GigabitEthernet0/0
C       10.0.3.4/30 is directly connected, GigabitEthernet0/1
L       10.0.3.5/32 is directly connected, GigabitEthernet0/1
C       10.0.3.8/30 is directly connected, Serial0/3/1
L       10.0.3.9/32 is directly connected, Serial0/3/1
O       10.0.3.12/30 [110/65] via 10.0.3.10, 00:34:36, Serial0/3/1
O       10.0.3.16/30 [110/65] via 10.0.3.10, 00:34:26, Serial0/3/1
     192.168.7.0/24 is variably subnetted, 6 subnets, 2 masks
O       192.168.7.0/26 [110/2] via 10.0.3.2, 00:40:57, GigabitEthernet0/0
                       [110/2] via 10.0.3.6, 00:40:57, GigabitEthernet0/1
O       192.168.7.64/28 [110/66] via 10.0.3.10, 00:09:45, Serial0/3/1
O       192.168.7.80/28 [110/66] via 10.0.3.10, 00:08:47, Serial0/3/1
O       192.168.7.96/28 [110/66] via 10.0.3.10, 00:07:55, Serial0/3/1
O       192.168.7.112/28 [110/66] via 10.0.3.10, 00:07:55, Serial0/3/1
O       192.168.7.128/26 [110/65] via 10.0.3.10, 00:36:23, Serial0/3/1
     209.165.202.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.202.0/30 is directly connected, Serial0/3/0
L       209.165.202.1/32 is directly connected, Serial0/3/0
S*   0.0.0.0/0 [1/0] via 209.165.202.2
```

Рисунок 3.2 – Таблиця маршрутизації на Vihman_R3

3.2.3 Налаштування трансляції мережевих адрес

Корпоративна мережа налаштована на блок приватних IP-адрес, для того щоб вузли мали маршрутизацію поза межі локальної мережі ми використовуємо технологію NAT.

Наша IT-компанія серверів має виділений діапазон публічних IP-адрес, також в мережі існує безліч пристроїв, які мають локальні IP-адреси. Вони потребують доступ до мережі Інтернет. Локальні мережі не можуть виходити у зовнішній світ за допомогою своїх локальних IP-адрес, тому для вирішення даного питання було використано технологію трансляції мережевих адрес. Вона дає змогу комп'ютерам у локальній мережі взаємодіяти з Інтернетом, використовуючи діапазон публічних IP-адрес.

Після того, як пристрій з локальної мережі намагається отриматі доступ у глобальну мережу, адреса вузла надходить на маршрутизатор і там відбувається заміна локальної адреси на виданий пул публічних адрес. Після цього користувач може користуватися мережею Інтернет.

Для виходу робочих станцій в Інтернет необхідно настроїти пограничний маршрутизатор з динамічним NAT за такими даними:

– ім’я пула: Internet;
– пограничний маршрутизатор Vihman_3 з інтерфейсом outside s0/3/0;
– номер списку доступу 5.

Vihman_R3 (config)# access-list 5 permit 192.168.7.0 0.0.0.255// Список контролю доступу для внутрішніх адрес;

Заміна адреси Інтернету на адреси внутрішньої мережі відповідно до порта маршрутизатора:

Vihman_R3 (config)#ip nat inside source list 5 interface s0/3/0

Vihman_R3 (config)#interface Serial0/3/0

Vihman_R3 (config-if)#ip nat outside

Vihman_R3 (config-if)#interface Serial0/3/1

Vihman_R3 (config-if)#ip nat inside

Щоб перевірити роботу NAT, переглянемо таблицю перекладів

```
Vihman_R3#sh ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.202.1:10  192.168.7.83:10    209.165.201.5:10   209.165.201.5:10
icmp 209.165.202.1:11  192.168.7.83:11    209.165.201.5:11   209.165.201.5:11
icmp 209.165.202.1:12  192.168.7.83:12    209.165.201.5:12   209.165.201.5:12
icmp 209.165.202.1:9   192.168.7.83:9     209.165.201.5:9    209.165.201.5:9
```

Рисунок 3.3 – Таблиця перекладів NAT

3.2.4 Налаштування протоколу агрегування каналів

Агрегація каналів PAgP (Port Aggregation Protocol) – це технологія, яка об'єднує дротове підключення мережевих пристроїв в один сегмент інформаційного каналу, завдяки цьому система є більш резервованою та має високий рівень відмовостійкості.

Головною перевагою агрегації каналів в єдиний інформаційний канал, це збільшення пропускної спроможності, при об’єднанні декількох каналів зв’язку в один, їх пропускна спроможність сумується.

Ще однією перевагою є резервування каналів в процесі працездатності. Якщо один із каналів агрегації виходить з ладу, трафік передається каналами, що залишилися, все це відбувається без вимикання системи в цілому, або ж перезапуску мережевого обладнання. Після того як канал знову запрацює, він автоматично під’єднається назад.

Налаштування EtherChannel на Vihman _CopySw4:

Vihman _CopySw4 (config)#int range fa0/1-2

Vihman _CopySw4(config-if-range)#shutdown

Vihman _CopySw4 (config-if-range)#channel-group 1 mode active

Creating a port-channel interface Port-channel 1

Vihman _CopySw4 (config-if-range)#no shutdown

Vihman _CopySw4 (config-if-range)#exit

Vihman _CopySw4 (config)#int port-channel 1 B

Vihman _CopySw4 (config-if)#switchport mode trunk

Vihman _CopySw4 (config)#int range f0/3-4

Vihman _CopySw4 (config-if-range)#channel-group 2 mode passive

Creating a port-channel interface Port-channel 2

Vihman _CopySw4 (config-if-range)#no shutdown

Vihman _CopySw4 (config)#int port-channel 2

Vihman _CopySw4 (config-if)#switchport mode trunk

Налаштування EtherChannel на Vihman _CopySw5:

Vihman _CopySw5(config)#int range fa0/1-2

Vihman _CopySw5 (config-if-range)#shutdown

Vihman _CopySw5 (config-if-range)#channel-group 1 mode active

Creating a port-channel interface Port-channel 1

Vihman _CopySw5 (config-if-range)#no shutdown

Vihman _CopySw5 (config-if-range)#exit

Vihman _CopySw5 (config)#int port-channel 1

Vihman _CopySw5 (config-if)#switchport mode trunk

Vihman _CopySw5 (config)#int range f0/3-4

Vihman _CopySw5 (config-if-range)#channel-group 2 mode passive

Creating a port-channel interface Port-channel 2

Vihman _CopySw5 (config-if-range)#no shutdown

Vihman _CopySw5 (config)#int port-channel 2

Vihman _CopySw5 (config-if)#switchport mode trunk

Налаштування EtherChannel на Vihman _CopySw6:

Vihman _CopySw6 (config)#int range fa0/1-2

Vihman _CopySw6 (config-if-range)#shutdown

Vihman _CopySw6 (config-if-range)#channel-group 1 mode passive

Creating a port-channel interface Port-channel 1

Vihman _CopySw6 (config-if-range)#no shutdown

Vihman _CopySw6 (config-if-range)#exit

Vihman _CopySw6 (config)#int port-channel 1

Vihman _CopySw6 (config-if)#switchport mode trunk

Vihman _CopySw6 (config)#int range f0/3-4

Vihman _CopySw6 (config-if-range)#channel-group 2 mode active

Creating a port-channel interface Port-channel 2

Vihman _CopySw6 (config-if-range)#no shutdown

Vihman _CopySw6 (config)#int port-channel 2

Vihman _CopySw6 (config-if)#switchport mode trunk

Перевірка налаштувань проводиться командою: sh etherchannel summary

```
Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------

1      Po1(SU)           LACP    Fa0/1(P) Fa0/2(P)
2      Po2(SD)           LACP    Fa0/3(I) Fa0/4(I)
Vihman_CopySw5#
```

Рисунок 3.4 – Вигляд налаштованого агрегування

3.2.5 Перевірка роботи комп'ютерної системи

Для перевірки працездатності мережі будемо перевіряти доступність вузлів в мережі та певні налаштування пристроїв.

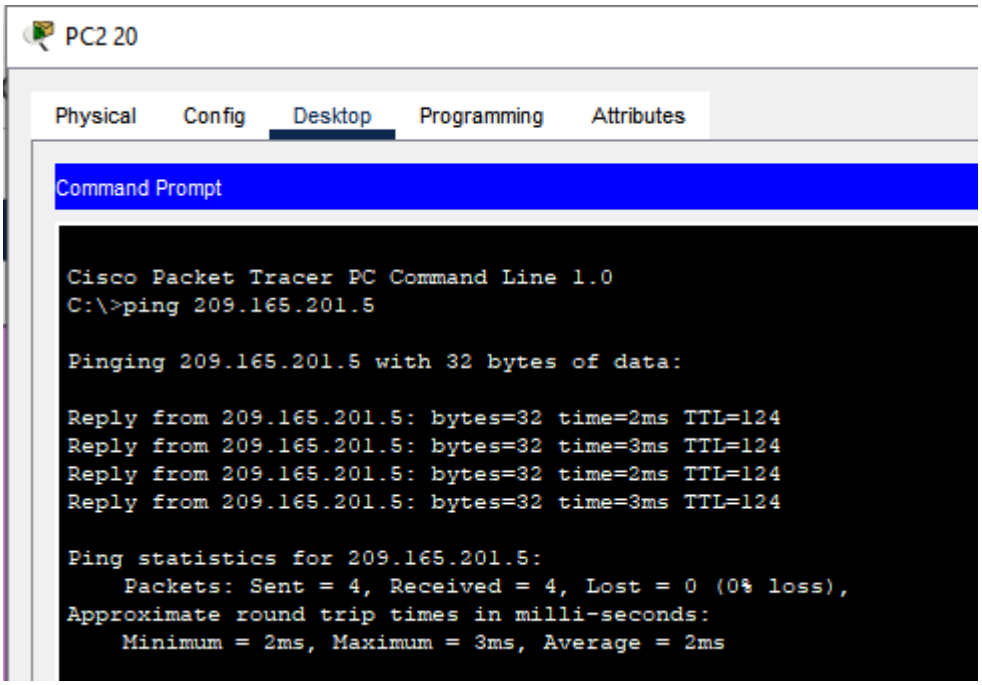

Рисунок 3.5 – Перевірка з'єднання вузлів

Доступність вузлів будемо перевіряти командою – ping.

Утиліта ping – це функція в мережах, яка за певний час відправляє пакет і повертається назад з відповіддю, в якій демонструється доступність вузла, затримка і т.д.

Тут ми перевірили зв'язок між ПК який знаходиться у 23 VLAN та з віддаленим DNS сервером.

Також, було налаштовано сервер HTTP, щоб на вузлах при вводі в рядку браузера http://123.dnipro.ua (http://209.165.201.5) відкривався веб-сайт з відомостями про тему та завдання на кваліфікаційну роботу студента.

0	123.dnipro.ua	A Record	209.165.201.5
1	http://123.dnipro.ua	CNAME	123.dnipro.ua

Рисунок 3.6 – Записи DNS

На (рисунок 3.6) зображені записи DNS-сервера, а сама запис A та CNAME. Записи встановлюють відповідність між IP-адресою та ім'ям(сайт).

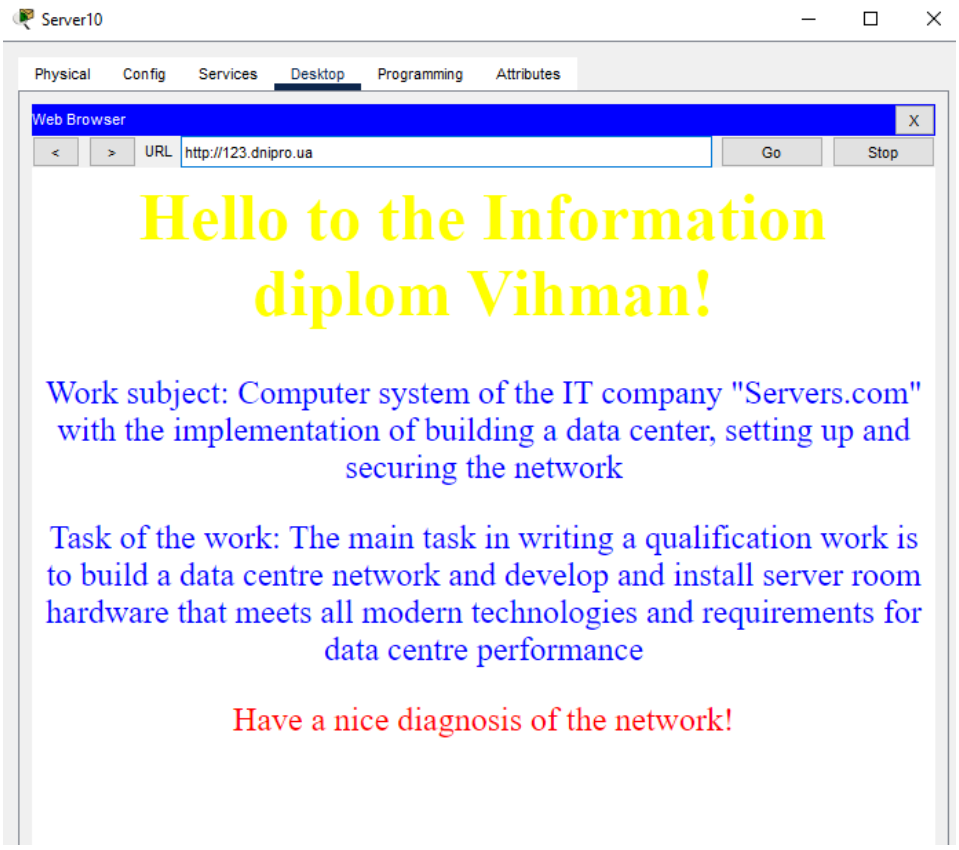

Рисунок 3.7 – Перевірка роботи серверів HTTP та DNS

По завданню було налаштовано протокол SSH.

SSH – це протокол управління через відділений доступ, який має захищений канал передачі даних.

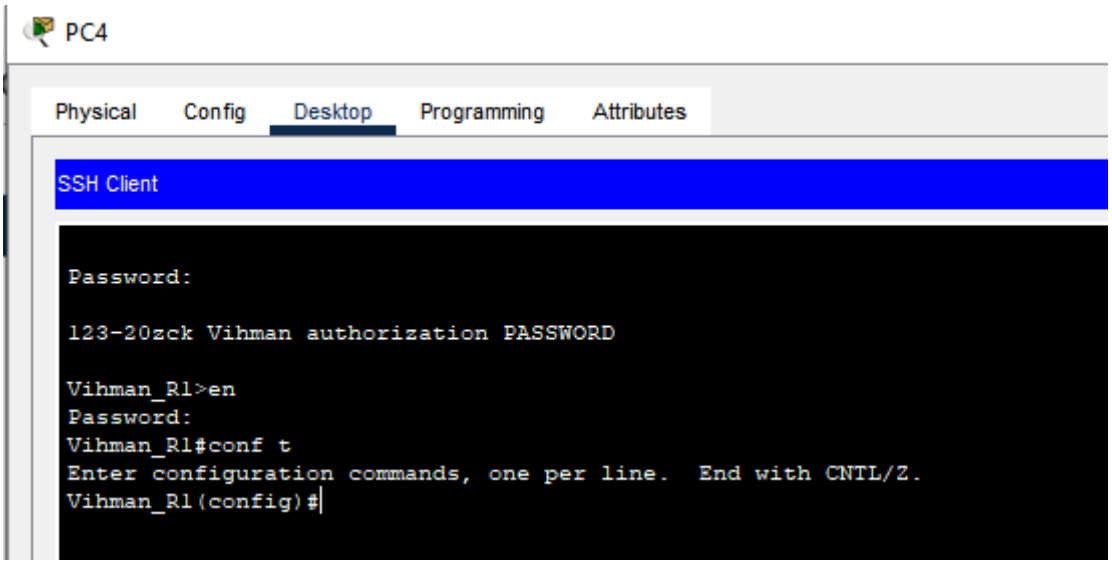

Рисунок 3.8 – Перевірка налаштування протоколу SSH

Для кожної мережі VLAN було перевірено коректність роботи протоколу DHCP.

```
Vihman_R2#show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
192.168.7.83     0001.42B9.7E37          --                      Automatic
192.168.7.84     0001.C737.C109          --                      Automatic
192.168.7.82     0004.9A93.630B          --                      Automatic
192.168.7.98     0050.0F3E.ED15          --                      Automatic
192.168.7.99     0001.97AC.E592          --                      Automatic
192.168.7.100    00E0.A3E7.69CC          --                      Automatic
192.168.7.115    0090.21B3.4A06          --                      Automatic
192.168.7.114    0005.5E83.6136          --                      Automatic
192.168.7.116    0007.ECA0.16E6          --                      Automatic
Vihman_R2#
```

Рисунок 3.9 – Перевірка налаштування протоколу DHCP

3.3 Захист інформації в комп’ютерній системі від несанкціонованого доступу

3.3.1 Розробка методів для захисту інформації в комп’ютерній системі

Захист інформації – це заходи, які повинні утримувати зловмисників від несанкціонованого доступу в корпоративну мережу та забезпечувати надійне користування мережею.

У ході роботи були розроблені та впроваджені методи захисту від несанкціонованого доступу в мережі, а саме:

– налаштування VLAN та маршрутизація між ними;
– функція захисту портів на комутаторі, які підключені до сервера;
– налаштування маршрутизаторів для підтримки протоколу AAA.

3.3.2 Налаштування віртуальних локальних мереж

За вимогами проекту були налаштовані віртуальні локальні мережі.

Під час адміністрування локальної мережі виникає потреба про необхідність фізичного перенесення співробітника в інший відділ, для об'єднання вузлів в одну підмережу. Цей спосіб є дуже важким в реалізації і коли в компанії знаходяться сотні вузлів, варіант з перенесенням стає майже неможливим. Віртуальні мережі ділять вузли на логічному рівні, і не застосовують методи з фізичним втручанням.

Також, локальні віртуальні мережі забезпечують високий рівень безпеки в мережі. Співробітники одної віртуальної мережі не можуть отримувати доступ до іншого віртуальної мережа та навпаки. Технологія може створювати велику кількість логічних підмереж на одному фізичному пристрої.

Відповідно до завдання було створені 3 мережі VLAN, які не повинні мати доступу одна до одної.

Таблиця 3.4 – VLAN мережі і порти призначення

Номер VLAN	Ім'я VLAN	Порт
13	Otdel-1	Sw2-Fa0/1-8
23	Otdel-2	Sw3-Fa0/1-8
33	Otdel-3	Sw3-Fa0/15-20

Об'ява VLAN13 та задання ім'я:

Vihman_Sw3 (config)#vlan 13

Vihman_Sw3 (config-vlan)#name Otdel-1

Об'ява VLAN23 та задання ім'я:

Vihman_Sw3 (config-vlan)# vlan 23

Vihman_Sw3 (config-vlan)#name Otdel-2

Об’ява VLAN33 та задання ім’я:

Vihman_Sw3 (config-vlan)#vlan 33

Vihman_Sw3 (config-vlan)#name Otdel-3

Налаштування транкових каналів:

Vihman_Sw3(config)#interface range g0/1-2

Vihman_Sw3 (config-if)#switchport trunk allowed vlan 13,23,33

Vihman_Sw3 (config-if)#switchport mode trunk

Налаштування портів доступу:

Vihman_Sw3 (config)#interface range f0/1-8

Vihman_Sw3 (config-if)#switchport mode access

Vihman_Sw3 (config-if)# switchport access vlan 23

Vihman_Sw3 (config)#interface range f0/15-20

Vihman_Sw3 (config-if)#switchport mode access

Vihman_Sw3 (config-if)# switchport access vlan 33

Vihman_Sw2 (config)#interface range f0/1-8

Vihman_Sw2 (config-if)#switchport mode access

Vihman_Sw2 (config-if)# switchport access vlan 13

Після налаштування в командному рядку, ми будемо мати 3 незалежні віртуальні локальні підмережі.

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24
13   otdel-1                          active
23   otdel-2                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
33   otdel-3                          active    Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20
```

Рисунок 3.10 – Налаштовані VLAN

3.3.3 Налаштування протоколу перевірки користувачів

Забезпечення безпеки мережевих пристроїв полягає в протоколі AAA. Цей протокол забезпечує контроль доступу з боку користувачів. Він виконує роботу за сценаріями аутентифікації, авторизації та обліку.

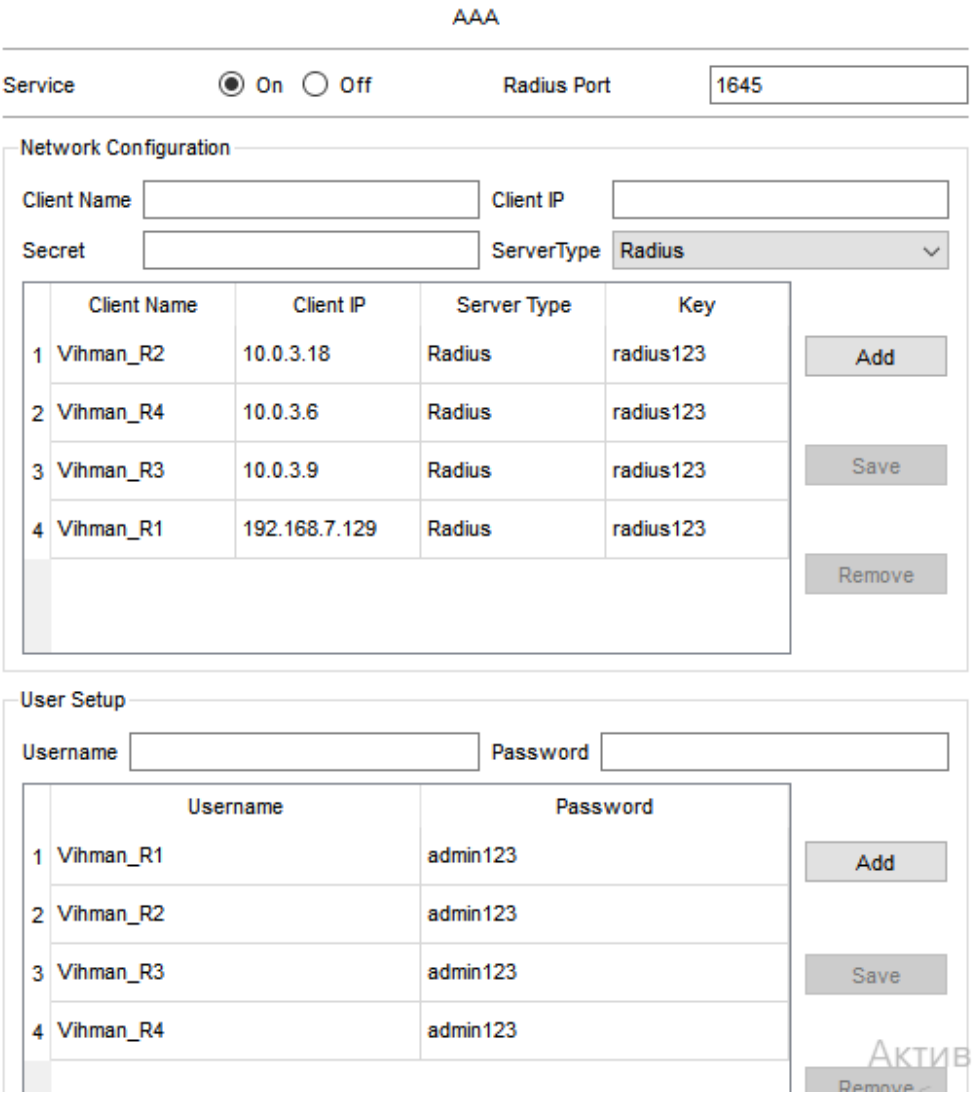

Рисунок 3.11 – Налаштування серверу AAA

Протокол працює за наступним алгоритмом:

– авторизація;
– аутентифікація;
– облік.

Авторизація – процес надання прав користувачу, які заздалегідь записані в системі, та дозволяють управляти мережею.

Аутентифікація – процес перевірки з загальною базою логіна та пароля користувача.

Облік – процес моніторингу споживання мережевих ресурсів та запис спроб аутентифікації до мережевих пристроїв.

Для того щоб запустити протокол на маршрутизаторах, треба спочатку налаштувати сервер AAA, а саме:

– включити сервіс AAA – режим on;
– задаємо порт 1645;
– вводимо ім’я, IP-адресу маршрутизатора та ключ доступу;
– створюємо користувачів ім’я та пароль.

Налаштування маршрутизаторів здійснюється наступним чином:

Vihman_R1(config) aaa new-model

Vihman_R1(config) radius-server host 192.168.7.130

Vihman_R1(config) radius-server key radius123

Vihman_R1(config) aaa authentication login default group radius local

Командами ми включаємо протокол AAA, вказуємо IP-адресу серверу, ключ доступу між сервером і маршрутизатором та правила авторизації в систему.

В системі завжди буде виконуватись авторизація за протоколом AAA, якщо виникне збій в системі, маршрутизатори мають локальних користувачів за якими можна буде потрапити у налаштування маршрутизатора.

3.3.4 Налаштування копіювання мережевих конфігурацій

Резервування мережевих конфігурацій виконується шляхом збереження конфігурацій на сервер TFTP.

```
Vihman_R0#copy running-config tftp:
Address or name of remote host []? 192.168.7.99
Destination filename [Vihman_R0-confg]?

Writing running-config.....!!
[OK - 1121 bytes]

1121 bytes copied in 7.068 secs (158 bytes/sec)
```

Рисунок 3.12 – Запис конфігурації до серверу

TFTP сервер використовується для передачі файлів конфігурації між мережевими пристроями. Сервер дає можливість записувати в нього конфігурації мережевих пристроїв, для резервування даних. У разі виникнення якихось причин або поломок із мережевим пристроєм, завжди можна відновити налаштування.

Запис мережевої конфігурації на сервер відбувається командою – copy running-config tftp. Після цього можна вказати назву збереженого файлу та після цього вказується IP-адреса серверу.

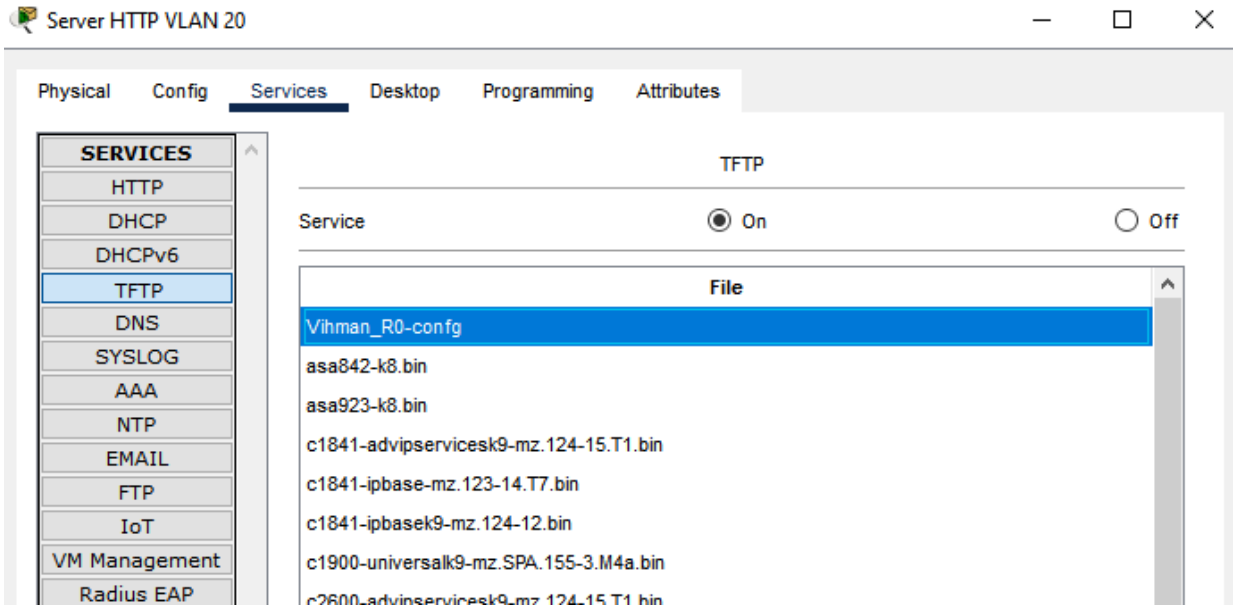

Рисунок 3.13 – Перевірка записаної конфігурації

3.3.5 Налаштування доступу мережам VLAN

Доступ мережам VLAN надається за допомогою списків доступу ACL (Access Control List).

ACL – це списки контролю доступу або правила, які впроваджуються мережевому обладнанню, вони вказують за яким алгоритмом треба приймати або відправляти пакети в мережах.

Обробка інформації може відбуватися тільки після того, як мереже обладнання зробить перевірку самого пакету та списку доступу, на основі цього користувач мережі отримає відповідь, буде прийнято пакет чи ні.

Створення списків доступу включає в собі заборону або дозвіл мережевим пристроям на певні дії.

Після створення списку доступу потрібно обов’язково під'єднати його на потрібні нам інтерфейси мережевого обладнання. Це може бути як фізичний так і логічний інтерфейс.

Для даної мережі що розробляється, були надані такі вимоги:

– VLAN 13 немає доступу до мереж VLAN23,33;

– VLAN 23 немає доступу до мереж VLAN13,33;

– VLAN 33 немає доступу до мереж VLAN13,23.

Приклад налаштування мережі:

```
Vihman_R2(config)#ip access-list extended network2
Vihman_R2(config-ext-nacl)#deny ip 192.168.7.80 0.0.0.15 192.168.7.96 0.0.0.15
Vihman_R2(config-ext-nacl)#deny ip 192.168.7.80 0.0.0.15 192.168.7.112 0.0.0.15
Vihman_R2(config-ext-nacl)#deny ip 192.168.7.96 0.0.0.15 192.168.7.112 0.0.0.15
Vihman_R2(config-ext-nacl)#deny ip 192.168.7.96 0.0.0.15 192.168.7.80 0.0.0.15
Vihman_R2(config-ext-nacl)#deny ip 192.168.7.112 0.0.0.15 192.168.7.80 0.0.0.15
Vihman_R2(config-ext-nacl)#deny ip 192.168.7.112 0.0.0.15 192.168.7.96 0.0.0.15
Vihman_R2(config-ext-nacl)#permit ip any any
```

Далі кожному інтерфейсу VLAN підключаємо список доступу ACL:

```
Vihman_R2(config)#interface gigabitEthernet 0/2.13
Vihman_R2(config-subif)#ip access-group network2 in
Vihman_R2(config-subif)#interface gigabitEthernet 0/2.23
Vihman_R2(config-subif)#ip access-group network2 in
Vihman_R2(config-subif)#interface gigabitEthernet 0/2.33
Vihman_R2(config-subif)#ip access-group network2 in
```

Спочатку ми створюємо стандартний список доступу. Команда deny забороняє проходження трафіку з вказаної IP-адреси, permit дозволяє.

Для перевірки списку доступу треба виконати команди ping з різних хостів мереж VLAN.

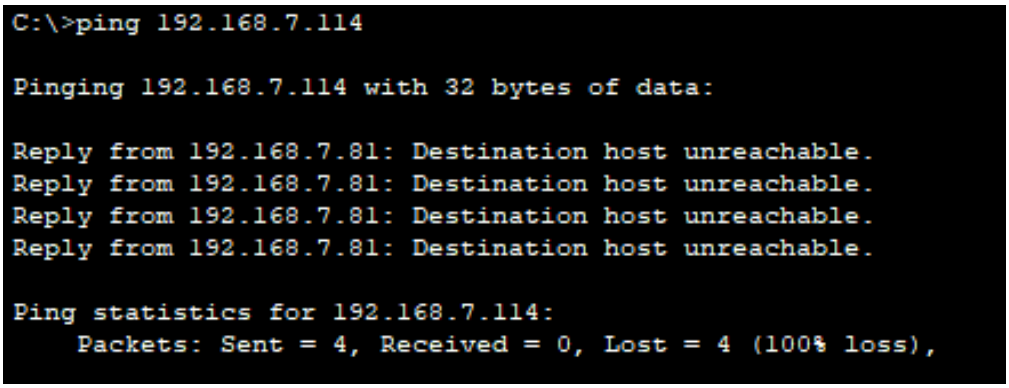

Рисунок 3.14 – Перевірка командою ping

Нашим списком доступу ми заблокували доступність між мережами VLAN.

3.3.6 Налаштування параметрів безпеки комутаторів

Для налаштування безпеки комутатора на портах комутатора були прописані параметри безпеки. Технологія безпеки називається Port-sequrity.

Port-sequrity – це функціонал комутатора, в якому ми можемо записувати алгоритм, через який порти будуть дозволяти подачу трафіку або забороняти.

Цей функціонал розрахований на спроби взлому від шахраїв або до атак різного роду, таких як – направлення на завантаження таблиць MAC-адрес.

Port-sequrity має Звиди налаштування:

– статичні MAC-адреси;

– динамічні MAC-адреси;

– sticky MAC-адреси.

Статичні MAC-адреси – це ті адреси, які налаштовуються на порту вручну.

Динамічні MAC-адреси – адреси, які виявляються динамічно і зберігаються в таблиці адрес.

Sticky MAC-адреси – адреси, які можуть бути як динамічно, так і вручну, водночас зберігатися в таблицю адрес. Ми будемо використовувати Sticky MAC-адреси.

Для цього командою switchport port-security mac-address sticky увімкнено вивчення конфігурацій.

Vihman_Sw5(config)#interface fa0/24

Vihman _Sw5(config)#switchport mode access

Vihman_Sw5(config)#switchport port-security

Vihman _Sw5(config)#switchport port-security maximum 1

Vihman _Sw5(config)#switchport port-security mac-address sticky

Vihman _Sw5(config)# switchport port-security violation shutdown

Налаштування приводять к безпеці на портах, дає змогу підключення тільки одного користувача і має запам’ятовування MAC-адреси. Якщо в системі будуть виявлені порушення безпеки порту, то це призведе до негайного вимкнення інтерфейсу.

Висновок до розділу

При написанні розділу була розроблена архітектура мережі компанії, схема та розрахунок IP-адресації пристроїв в мережі та схема фізичної топології мережі.

Також, було налаштовано базові конфігурації пристроїв, маршрутизацію в мережі, трансляцію мережевих адрес, протокол агрегування каналів, віртуальні локальні мережі, протокол перевірки доступу користувачів, протокол копіювання мережевих конфігурацій, списки доступу та параметри безпеки комутаторів.

За допомогою мережевих утиліт було перевірено роботу комп’ютерної системи компанії.

4 РОЗРОБКА КОМПОНЕНТА СИСТЕМИ ОХОЛОДЖЕННЯ IoT

4.1 Розробка системи IoT в цілому

При виконанні кваліфікаційної роботи було додатково спроектовано систему охолодження в дата-центрі за допомогою технології IoT.

Завдяки технологіям IoT управління системою охолодження можна проводити навіть зі смартфону, планшету, тощо.

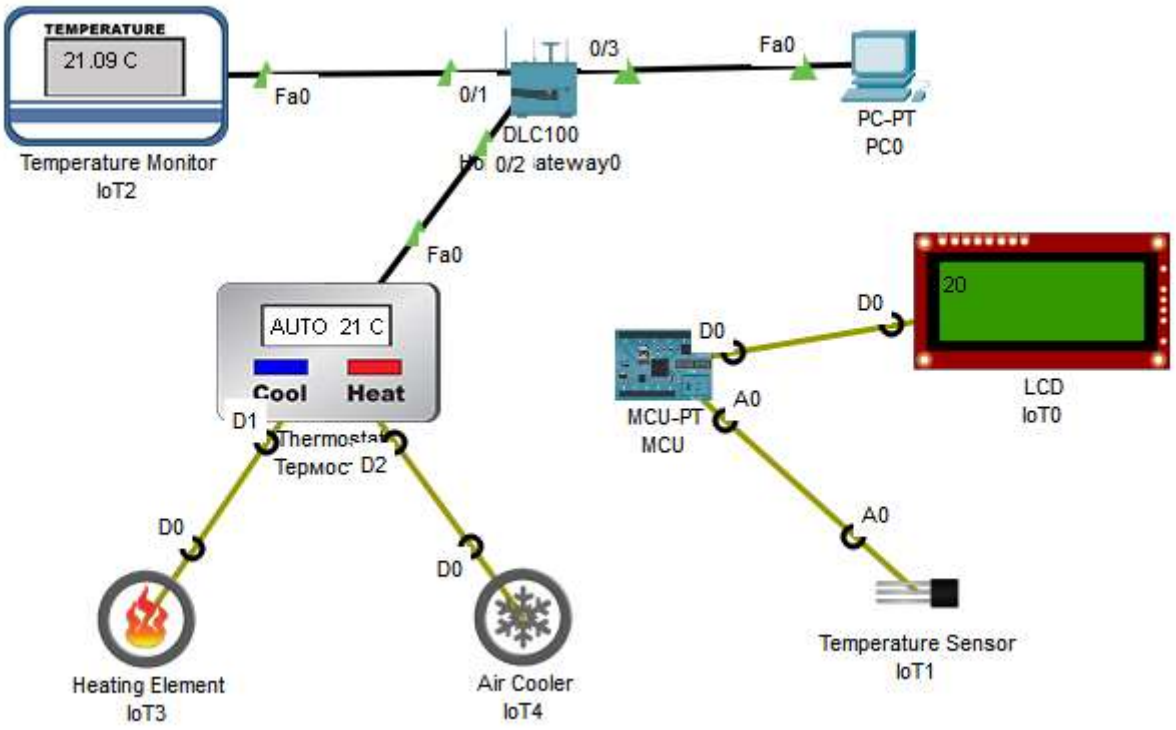

Рисунок 4.1 – Вигляд системи охолодження IoT

Система має нагрівальний та охолоджувальний елементи, які підключаються за допомогою термостату. Термостат має як фізичне налаштування так і за допомогою мережі. Термостат підключений до шлюзу системи, з іншої сторони шлюза також підключений монітор температури, який в реальному часі відображає температуру яка налаштовується в термостаті.

Шлюз налаштований на IP-адресу – 192.168.25.1 з маскою 255.255.255.0.

Для налаштування температури за допомогою мережі підключаємося к шлюзу за IP-адресою та використовуємо логін та пароль – admin/admin.

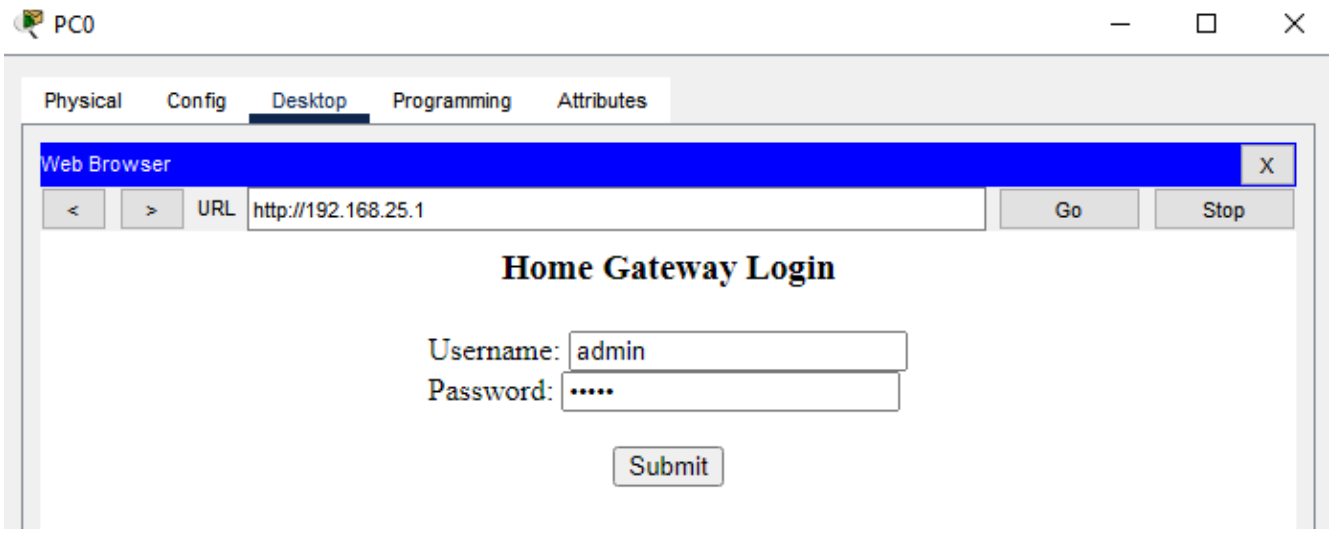

Рисунок 4.2 – Вигляд авторизації в систему охолодження

При вході в систему ми бачимо два елементи – монітор та термостат. При натисканні на термостат ми бачимо певні налаштування, а саме режими управління охолодженням. Ми можемо виключити систему, включити тільки охолодження або нагрів температури та головне налаштування яким буде користуватися дата-центр це регулювання за певною температурою. Включаємо авто режим охолодження та вибираємо мінімальну та максимальну температуру, яка буде підтримуватись весь час.

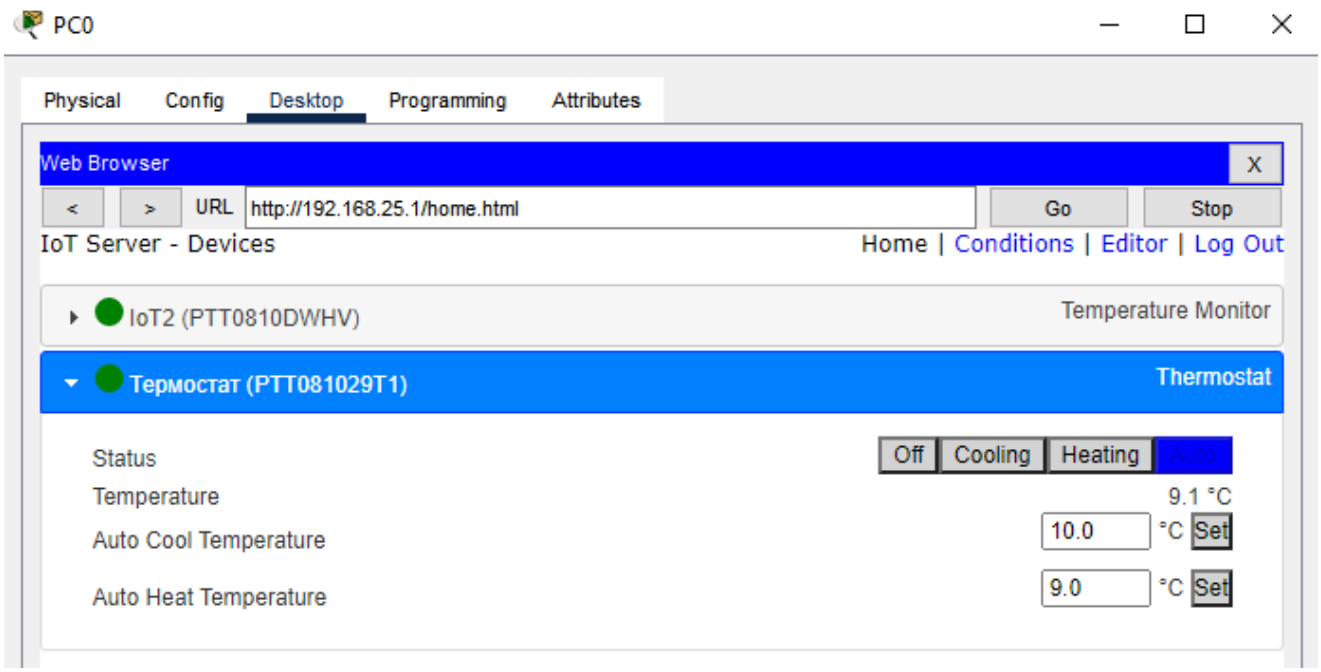

Рисунок 4.3 – Вигляд налаштування температури

4.2 Відображення працездатності системи та код управління

Після налаштування потрібного температурного режиму в дата-центрі буде додатково налаштований датчик температури, який буде відображувати температуру дата-центру в реальному часі.

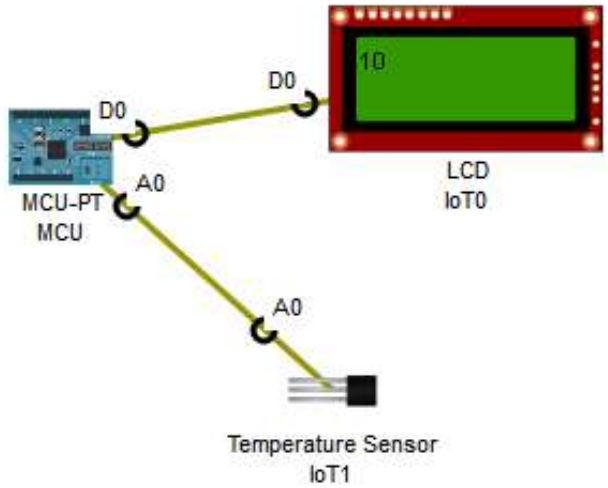

Рисунок 4.4 – Вигляд системи контролю температури

За управління між дисплеєм та датчиком температури відповідає контролер–MCU. В ньому записаний код, який зчитує інформацію з датчика та виводить дані на дисплей. Код управління наступний:

```
from gpio import *
from time import *
# Зворотний виклик, який використовується для визначення, коли датчик температури, приєднаний до mcu, надсилає дані.
def inputHandler():
        # Перетворення зі старого діапазону в новий діапазон.
        value =  (((analogRead(A0) - 0) * (100 - -100)) / (1023 - 0)) + -100
        customWrite(0, value)
# Налаштування події зворотного виклику для обробки значення у слоті A0.
def main():
    add_event_detect(A0, inputHandler)
```

```
while True:
                delay(1000)
if __name__ == "__main__":
        main()
```

Висновок до розділу

При написанні розділу було розроблено систему охолодження дата-центру за допомогою технологій інтернет-речей IoT. Для відображення температурного режиму була налаштована взаємодія термостату з монітором. Також, було впроваджено систему управління температурою с будь-якого пристрою, який має доступ до мережі Інтернет.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи була розроблена корпоративна мережа, що складається з чотирьох підмереж. В процесі проектування мережі набув стійкі навички і вміння самостійно працювати з навчальною, науковою літературою та використовувати сучасні інформаційні технології, програмні продукти та засоби навчання.

Мета завдання проектування виконана та основа структури об’єкту розрахована з урахуванням географічного розташування.

Розробку інформаційної системи підприємства було реалізовано засобами додатку Cisco Packet Tracer. Мережеве обладнання при проектуванні використовував компанії Cisco. Схема IP-адресації розроблена для активного мережевого обладнання на основі технічних вимог та завдані проекту. Було повністю перевірено роботу комп’ютерної мережі.

У цій кваліфікаційній роботі були виконані ключові технічні розрахунки трафіку та продуктивності мережі. Вони продемонстрували, що мережа відповідає всім сучасним стандартам та задовольняє потреби компанії.

В проекті були реалізовані всі сучасні протоколи мережевих технологій, які відповідають вимогам безпеки та безперебійності роботи мережі.

За вимогами кваліфікаційної роботи були використані сучасні протоколу TCP/IP з урахуванням безпеки та масштабування мережі.

Кваліфікаційна робота може бути використана як повний опис та алгоритм дій створення комп’ютерних мереж.

ПЕРЕЛІК ПОСИЛАНЬ

1. ДСТУ «3008-2015». Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлювання. – К.: Держстандарт, 1998. – 37 с.

2. Положення про організацію атестації здобувачів вищої освіти НТУ «Дніпровська політехніка» / М-во освіти і науки України, Нац. техн. ун-т. – Д. : НТУ «ДП», 2018. – 40 с

3. ДСТУ «ГОСТ 19.701-90. ЄСПД». Єдина система програмної документації. Схема алгоритмів, програм, даних і систем. Позначення умовні та правила виконання. – М.: Держстандарт, 1990. – 128 с.

4. Воробйова Н.І., Корнійчук В.І., Савчук О.В. Надійність комп'ютерних систем. – К.: "Корнійчук", 2002. - 144 с.

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

6. Шаблон базового налаштування маршрутизатора Cisco за стандартами [Електронний ресурс] – https://habr.com/ru/articles/87680/

7. Технології налаштування агрегування каналів, налаштування списків доступу, створення аутентифікації та адресація локальних та глобальних мереж [Електронний ресурс] – https://www.cisco.com/c/ru_ua/index.html

8. Офісний пакет Microsoft Office [Електронний ресурс] – https://www.microsoft.com/ru-ru/microsoft-365/products-apps-services

9. Діагностика мережевого підключення [Електронний ресурс] – https://wiki.lan.ua/doku.php?id=diagnostics

Додаток А

Текст програми налаштування мережі комп’ютерної системи

Міністерство освіти і науки України
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
“ДНІПРОВСЬКА ПОЛІТЕХНІКА”

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Текст програми
804.02070743.23003-01 12 01

Листів 14

2023

АННОТАЦІЯ

Програма складається с частини програмного коду для налаштування конфігурацій мережевих інтерфейсів корпоративної мережі. Цей код призначений для впровадження протоколів DHCP, AAA, NAT, для налаштування консолей та ліній VTY та для створення комп'ютерних систем VPN, домену та SSH доступу.

ЗМІСТ

Конфігурація Vihman_R2:

```
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
//Шифрування паролів
service password-encryption
!
//Ім’я пристрою
hostname Vihman_R2
!
//Пароль до привілейованого режиму
enable secret 5
$1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
//Налаштування DHCP
ip dhcp pool Vlan13
 network 192.168.7.80 255.255.255.240
 default-router 192.168.7.81
 dns-server 192.168.7.4
ip dhcp pool Vlan23
 network 192.168.7.96 255.255.255.240
 default-router 192.168.7.97
 dns-server 192.168.7.4
ip dhcp pool Vlan33
 network 192.168.7.112 255.255.255.240
 default-router 192.168.7.113
 dns-server 192.168.7.4
ip dhcp pool Vlan99
ip dhcp pool comutation
 network 192.168.7.64 255.255.255.240
```

```
 default-router 192.168.7.65
!
// Налаштування протоколу AAA
aaa new-model
!
aaa authentication login default group radius local
!
ip cef
no ipv6 cef
!
//Створення користувача
username 12320zck_Vihman password 7 0822455D0A16
!
license udi pid CISCO2911/K9 sn FTX15247LQF-
!
//Створення домену
ip domain-name Vihman_R2
!
spanning-tree mode pvst
!
//Налаштування інтерфейсів та VLAN
interface GigabitEthernet0/0
 ip address 10.0.3.14 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 10.0.3.18 255.255.255.252
 duplex auto
 speed auto
```

```
!
interface GigabitEthernet0/2
 ip address 192.168.7.65 255.255.255.240
 duplex auto
 speed auto
!
interface GigabitEthernet0/2.13
 description otdel-1
 encapsulation dot1Q 13
 ip address 192.168.7.81 255.255.255.240
 ip access-group network2 in
!
interface GigabitEthernet0/2.23
 description otdel-2
 encapsulation dot1Q 23
 ip address 192.168.7.97 255.255.255.240
 ip access-group network2 in
!
interface GigabitEthernet0/2.33
 description otdel-3
 encapsulation dot1Q 33
 ip address 192.168.7.113 255.255.255.240
 ip access-group network2 in
!
interface Vlan1
 no ip address
 shutdown
!
```

```
//Налаштування OSPF
router ospf 1
 log-adjacency-changes
 network 10.0.3.12 0.0.0.3 area 0
 network 10.0.3.16 0.0.0.3 area 0
 network 192.168.7.64 0.0.0.15 area 0
 network 192.168.7.80 0.0.0.15 area 0
 network 192.168.7.96 0.0.0.15 area 0
 network 192.168.7.112 0.0.0.15 area 0
!
ip classless
!
ip flow-export version 9
!
//Налаштування списку доступу ACL
ip access-list standard lan2
ip access-list extended network2
 deny ip 192.168.7.80 0.0.0.15 192.168.7.96 0.0.0.15
 deny ip 192.168.7.80 0.0.0.15 192.168.7.112 0.0.0.15
 deny ip 192.168.7.96 0.0.0.15 192.168.7.112 0.0.0.15
 deny ip 192.168.7.96 0.0.0.15 192.168.7.80 0.0.0.15
 deny ip 192.168.7.112 0.0.0.15 192.168.7.80 0.0.0.15
 deny ip 192.168.7.112 0.0.0.15 192.168.7.96 0.0.0.15
 permit ip any any
!
//Створення банеру
banner motd #123-20zck Vihman authorization PASSWORD#
!
```

```
//Налаштування сервера протоколу AAA
radius server 192.168.7.130
 address ipv4 192.168.7.130 auth-port 1645
!
//Створення пароля на консоль
line con 0
 password 7 0822455D0A16
!
line aux 0
!
line vty 0 4
Створення ssh
 transport input ssh
!
End
```

Налаштування маршрутизатора IPS:

```
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
//Шифрування паролів
service password-encryption
!
//Ім’я пристрою
hostname Vihman_IPS
!
//Встановлення паролю на режим enable
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
no ip cef
```

```
no ipv6 cef
!
//Створення користувача
username 12320zck_Vihman password 7 0822455D0A16
!
license udi pid CISCO2911/K9 sn FTX1524P242-
!
//Створення домену
ip domain-name Vihman_IPS
!
spanning-tree mode pvst
!
//Налаштування інтерфейсів
interface GigabitEthernet0/0
 ip address 209.165.201.1 255.255.255.240
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 64.100.13.2 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
!
interface Serial0/3/0
 ip address 209.165.202.2 255.255.255.252
```

```
 clock rate 9600
!
interface Serial0/3/1
 no ip address
 clock rate 2000000
!
interface Vlan1
 no ip address
 shutdown
!
//Налаштування протоколу NAT
ip nat pool Internet 209.165.202.5 209.165.202.30 netmask 255.255.255.224
ip nat inside source list 5 pool Internet
ip classless
ip route 192.168.7.160 255.255.255.224 GigabitEthernet0/1
ip route 192.168.7.0 255.255.255.192 209.165.202.1
ip route 192.168.7.64 255.255.255.224 209.165.202.1
ip route 192.168.7.96 255.255.255.224 209.165.202.1
ip route 192.168.7.128 255.255.255.224 209.165.202.1
!
ip flow-export version 9
!
access-list 5 permit 192.168.7.0 0.0.0.255
!
//Створення банеру
banner motd #123-20zck_Vihman authorization PASSWORD#
!
//Встановлення паролю на консоль
line con 0
 password 7 0822455D0A16
```

```
 login
!
line aux 0
!
line vty 0 4
 login local
//Впровадження протоколу SSH
 transport input ssh
!
End
```

Налаштування комутатора Vihman_Sw3:

```
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
//Шифрування паролів
no service password-encryption
!
//Ім’я пристрою
hostname Vihman_Sw3
!
spanning-tree mode pvst
spanning-tree extend system-id
!
//Налаштування інтерфейсів
interface FastEthernet0/1
 switchport access vlan 23
 switchport trunk allowed vlan 23
 switchport mode access
```

```
!
interface FastEthernet0/2
 switchport access vlan 23
 switchport trunk allowed vlan 23
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 23
 switchport trunk allowed vlan 23
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 23
 switchport trunk allowed vlan 23
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 23
 switchport trunk allowed vlan 23
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 23
 switchport trunk allowed vlan 23
 switchport mode access
!
interface FastEthernet0/7
 switchport access vlan 23
 switchport trunk allowed vlan 23
 switchport mode access
```

```
!
interface FastEthernet0/8
 switchport access vlan 23
 switchport trunk allowed vlan 23
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 33
 switchport mode access
!
interface FastEthernet0/16
 switchport access vlan 33
 switchport mode access
!
interface FastEthernet0/17
 switchport access vlan 33
 switchport mode access
!
interface FastEthernet0/18
 switchport access vlan 33
 switchport mode access
!
interface FastEthernet0/19
 switchport access vlan 33
 switchport mode access
!
interface FastEthernet0/20
 switchport access vlan 33
 switchport mode access
!
```

```
interface GigabitEthernet0/1
 switchport trunk allowed vlan 13,23,33
 switchport mode trunk
!
interface GigabitEthernet0/2
 switchport trunk allowed vlan 13,23,33
 switchport mode trunk
!
interface Vlan1
 no ip address
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
end
```

ДОДАТОК Б

Точка пропуску в дата-центрі

Рисунок Б.1 – Точка пропуску в дата-центрі

ДОДАТОК В

Схема підключення серверів до мережі

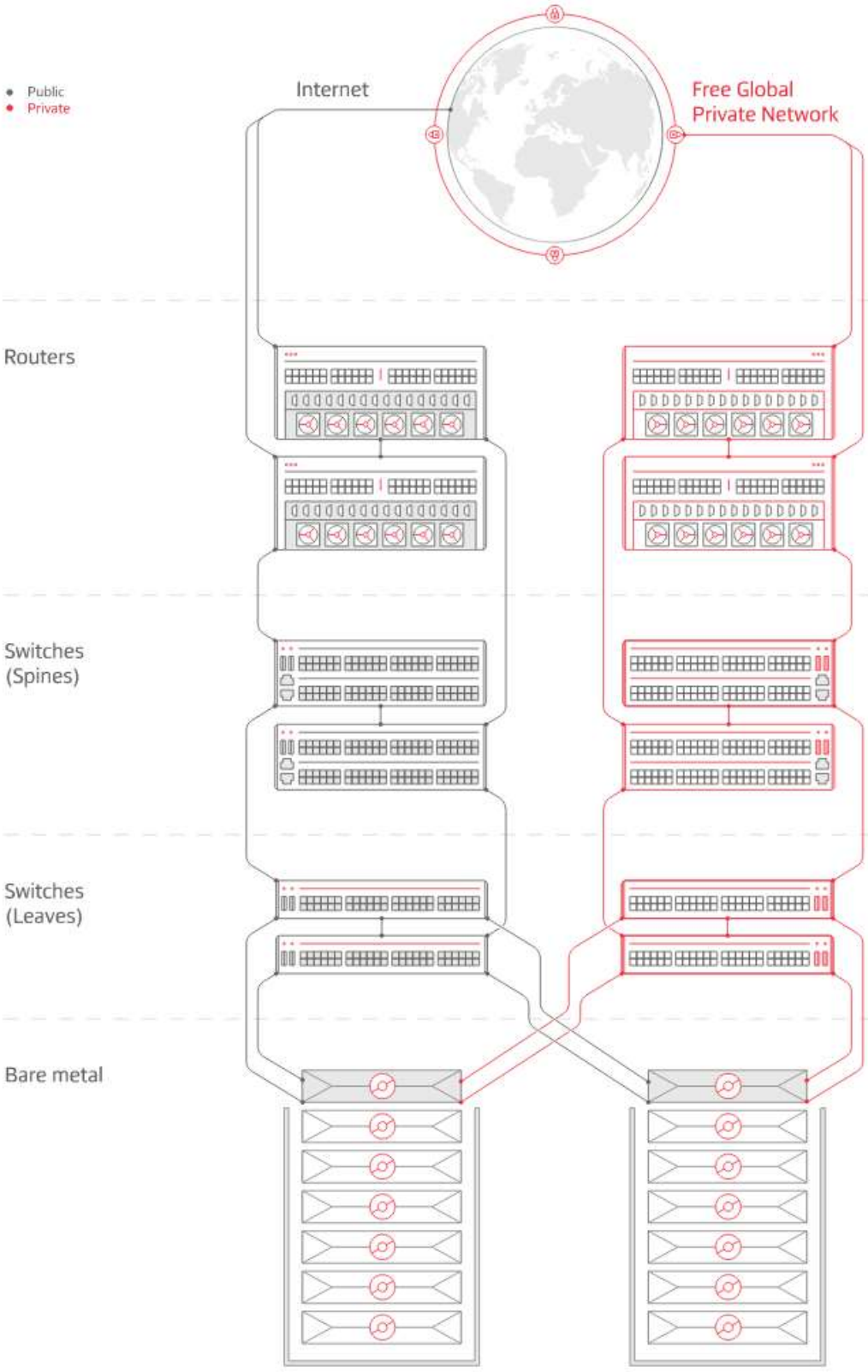

Рисунок В.1 – Схема підключення серверів до мережі