

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 Гриви Данила Юрійовича
(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 компанії "Воля" з реалізацією налаштування, безпеки та підключень будинків до мереж»
(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 Гриви Д.Ю. 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 компанії "Воля" з реалізацією налаштування, безпеки та підключень будинків до мереж»

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 _____
(підпис керівника)

доц.Бешта Д.О.
(прізвище, ініціали)

Дата видачі 25.01.2023

Дата подання до екзаменаційної комісії 12.07.2023

Прийнято до виконання _____
(підпис студента)

Грива Д.Ю.
(прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 62 с., 28 рис., 7 табл., 1 дод., 9 джерел.

ІНТЕРНЕТ, ПРОВАЙДЕР, ВИТА ПАРА, ОПТОВОЛОКНО, WAN, LAN

Об'єкт впровадження: комп'ютерна система компанії "Воля" з реалізацією підключення будинку до мережі, налаштування та безпеки мережі.

Мета: моделювання мережевого проекту для реалізації відділів управління та системи підключення будинків до мережі.

Проектування мережі інтернет-провайдера розрахована на підключення абонентів до мережі інтернет. Система вміщує в собі технічну підтримку користувачів, підрозділів управління та обслуговування мережі. Надання послуг виконується в підрозділах технічної підтримки.

Відділи інтернет провайдера розраховані на збір інформації від користувачів, для подальшого індивідуального налаштування мережі абонента. У зв'язку з цим були впроваджені сучасні апаратні та програмні технології.

Компанія інтернет-провайдера є шлюзом для своїх користувачів і забезпечує працездатність мережі від магістрального провайдера. Мережа має змогу на постійну масштабованість, модернізацію та вдосконалення системи.

Налаштування протоколів мережевого рівня має відображення у вигляді коду, який має повний опис функціонування кожної команди для кожного протоколу.

Моделювання мережевої інфраструктури виконувалось в додатку Cisco Packet Tracer.

IP-адресація вузлів мережі зображена у вигляді таблиці та графічної частини і відповідає поставленому завданню.

ЗМІСТ

Перелік скорочень, умовних позначок, одиниць і термінів	8
Вступ	9
1 Стан питання і постановка завдання	11
1.1 Характеристика сфери обслуговування мережі інтернет-провайдера	11
1.2 Характеристика діяльності компанії інтернет-провайдера «Воля»	12
1.3 Організаційна структура підрозділів мережі компанії	14
1.4 Розміщення офісів інтернет провайдера	15
1.5 Опис відділів та принцип підключення вузлів до мережі Інтернет	15
1.6 Завдання і мета роботи	17
1.7 Визначення можливих напрямків рішення поставлених завдань	17
2 Розробка апаратної частини комп'ютерної системи	19
2.1 Технічні вимоги до системи	19
2.1.1 Вимоги до системи в цілому	19
2.1.1.1 Вимоги до структури і функціонування системи	19
2.1.1.1.1 Перелік підсистем, їхнє призначення й основні характеристики, вимоги до числа рівнів ієрархії та ступені централізації мережі	19
2.1.1.1.2 Вимоги до способів і засобів зв'язку для обміну інформації між підмережами	20
2.1.1.1.3 Вимоги до характеристик взаємозв'язків створюваної мережі із суміжними мережами	20
2.1.1.1.4 Вимоги до режимів функціонування мережі	20
2.1.1.1.5 Вимоги до діагностування мережі	21
2.1.1.1.6 Перспективи розвитку та модернізації мережі	21
2.1.1.2 Вимоги до показників призначення	22

2.1.1.3	Вимоги до експлуатації	22
2.1.1.3.1	Умови і регламент режиму експлуатації, що повинні забезпечувати використання технічних засобів мережі	22
2.1.1.3.2	Вимоги до параметрів мереж енергопостачання	22
2.1.1.3.3	Вимоги до кількості, кваліфікації обслуговуючого персоналу і режимам його роботи	22
2.1.1.3.4	Вимоги до складу, розміщенню й умовам збереження комплекту запасних виробів і приладів	23
2.1.1.3.5	Вимоги до регламенту обслуговування мережі	23
2.1.1.4	Вимоги до патентної чистоти	23
2.1.1.5	Додаткові вимоги	24
2.1.1.5.1	Вимоги до активного обладнання	24
2.1.1.5.2	Вимоги до кабель каналів, інформаційним та електричним розеткам	24
2.1.1.5.3	Вимоги до комунікаційного обладнання і його розташування	25
2.1.1.5.4	Вимоги до однорідності	25
2.1.2	Вимоги до задач, які виконуються у комп'ютерній системи	25
2.1.2.1	Вимоги до кожної підмережі та переліку їх функцій	25
2.1.2.2	Часовий регламент і вимоги до якості реалізації кожної функції	28
2.1.3	Вимоги до видів забезпечення комп'ютерної системи	28
2.1.3.1	Вимоги до математичного забезпечення	28
2.1.3.2	Вимоги до інформаційного забезпечення	28
2.1.3.2.1	Вимоги до складу, структури і способів організації даних у мережі	28
2.1.3.2.2	Вимоги до інформаційної сумісності із суміжними мережами	29

2.1.3.2.3	Вимоги до структури процесу збору, обробки, передачі даних у мережі і представлення даних	29
2.1.3.3	Вимоги до лінгвістичного забезпечення	29
2.1.3.4	Вимоги до технічного забезпечення	29
2.1.3.4.1	Вимоги до технічних засобів, у тому числі до видів програмно-технічних комплексів	29
2.1.3.5	Вимоги до організаційного забезпечення	30
2.1.3.5.1	Вимоги до структури і функцій підрозділів, що беруть участь у функціонуванні мережі	30
2.1.3.5.2	Вимоги до захисту від помилкових дій персоналу мережі	30
2.1.3.6	Вимоги до методичного забезпечення	30
2.2	Розробка апаратної частини мережі інтернет-провайдера	31
2.2.1	Розробка схеми комплексу технічних засобів мережевої інфраструктури	31
2.2.2	Реалізація фізичного підключення будинка до мережі	34
2.2.3	Розробка апаратного забезпечення мережі	36
2.2.4	Розробка програмного забезпечення мережі	38
2.2.5	Розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі компанії	39
3	Розробка корпоративної мережі	41
3.1	Розрахунок та розробка схем корпоративної мережі компанії	41
3.1.1	Розробка логічної топології системи	41
3.1.2	Розрахунок схеми адресного простору підмереж та маршрутизаторів	43
3.1.3	Розрахунок схеми адресного простору вузлів мережі	44
3.1.4	Розробка фізичної топології та обґрунтування використання кабельних систем	47

3.2 Налаштування сегментів мережі та перевірка працездатності мережі в цілому	47
3.2.1 Базове налаштування конфігурації пристроїв	47
3.2.2 Налаштування динамічного протоколу маршрутизації в мережі	48
3.2.3 Налаштування динамічного NAT	50
3.2.4 Налаштування списків доступу ACL	51
3.2.5 Налаштування агрегування каналів PAgP	53
3.2.6 Перевірка працездатності налаштувань в мережі	55
3.3 Налаштування безпеки мережевого обладнання	56
3.3.1 Налаштування мереж VLAN	56
3.3.2 Налаштування маршрутизаторів на підтримку служби AAA	57
3.3.3 Налаштування та перевірка роботи сервера TFTP	59
3.3.4 Налаштування безпеки на портах комутаторів	60
4 Розробка компонента системи пожежогасіння	61
4.1 Розробка системи та налаштування	61
Висновки	63
Перелік посилань	64
Додаток А. Схема загальної топології інтернет-провайдера «Воля»	65
Додаток Б. Текст програми налаштування мережі комп'ютерної системи	66

ПЕРЕЛІК СКОРОЧЕНЬ, УМНОВНИХ ПОЗНАК, ОДИНИЦЬ І ТЕРМІНІВ

HDD – жорсткий диск;

SSD – твердотілий накопичувач;

FTTB – підключення до будинку;

FTTH – підключення до квартири;

VLAN – віртуальна локальна мережа;

WAN – глобальна мережа;

LAN – локальна мережа;

NAT – технологія виходу в глобальну мережу за певним діапазоном адрес;

OSPF – протокол маршрутизації мережі;

RAgP – протокол агрегування каналів;

HTTP – протокол передачі гіпертексту;

SSH – технологія безпечного з'єднання з пристроями;

AAA – протокол перевірки даних з погляду безпеки системи;

DNS – протокол перетворення адреси в ім'я сайту та навпаки;

TFTP – протокол передачі файлів.

ВСТУП

Головною задачею кваліфікаційної роботи є розбір довершеності системи масштабування та створення нових комп'ютерних мереж. Для об'єднання всіх мереж та підмереж або інакше кажучи міст, сіл, країн прийнято користуватися послугами інтернет-провайдерів.

Інтернет-провайдер зазвичай є точкою доступу або шлюзом, який надає користувачеві доступ до всього доступного в Інтернеті. Наше сучасне життя неможливо уявити без інтернету. Інформаційні технології охоплюють весь світ і мають неймовірну швидкість в розвитку.

За допомогою мережевих технологій ми можемо робити покупки різних товарів в мережі Інтернет. Кошти можуть мати цифровий формат, при цьому мати безпечне зберігання. Тепер, замість того щоб люди носили і використовували гроші в паперовому представленні, вони використовують пластикові картки, які мають менший розмір не залежно від суми та пов'язані із рахунком у банку.

Якщо ознайомитися зі списком існуючих сьогодні професій, ми побачимо багато нових назв, про яких люди не знали ще близько 30 років тому. Це можуть бути – СММ-щики, програмісти, розробники мобільних додатків, SEO-фахівці, UI/UX-дизайнери і так далі. Дуже очевидно, що надалі цей список продовжуватиме поповнюватись.

ІТ-інфраструктура також дозволяє нам користуватись віддаленою роботою.

Це дає можливість не використовувати оренду офісного приміщення, а виконувати робочий план сидячі вдома.

Всі ці переваги та технології ми отримуємо в онлайн часі та не маємо уяви що такого може не бути. Завдяки інтернет-провайдерам ми маємо змогу працювати майже в будь-якій точці світу та бути впевненими, що в нас є доступ у мережу інтернет.

Основна функція постачальника послуг інтернет – це забезпечити надійне з'єднання комп'ютера користувача(шлюз, тощо) з будь-яким запитуваним ним сервером, де розміщується потрібний йому сайт.

Інтернет являє собою складну структуру дротових і бездротових мереж, що об'єднують сумісні сервери і пристрої. Сушею, дном океанів і морів проходять кабелі, які з'єднують усі континенти. Це робить інтернет справді глобальною мережею.

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

1.1 Характеристика сфери обслуговування мережі інтернет-провайдера

Інтернет – це те, без чого складно уявити життя сучасної людини, роботу глобальних систем і організацію передачі даних.

Для організації мережі в світі були реалізовані компанії, які є постачальникам та надають послуги інтернет в кожний будинок та кожній людині.

Інтернет-провайдер – це посередник, який надає своїм абонентам доступ до глобальної мережі. Провайдер отримує інтернет від компанії-оператора, яка володіє власною телекомунікаційною мережею. Оператор має право надавати доступ до інтернету, а також відповідає за обслуговування та експлуатацію магістральних мереж. Своєю чергою, провайдер укладає договір з оператором і використовує ресурси мережі без права її технічного обслуговування.

Глобальна мережа має наступні рівні:

- tier-1;
- tier-2;
- tier-3.

Провайдери першого рівня tier-1 займаються обслуговуванням та передачею ліній зв'язку між континентами. Таких компаній налічується близько 10 по всьому світу. До них належать Level3, Global Crossing, Telefonica та інші корпорації, що надають послуги зв'язку. Провайдер першого рівня не надають послуги кінцевому споживачеві, але вони продають інтернет-трафік компаніям другого рівня (tier-2), якими найчастіше є національні оператори. Третій рівень (tier-3) – регіональні та міські провайдери, які закупають інтернет-трафік у компанії другого рівня.

Користувачі отримують інтернет-трафік від провайдерів другого і третього рівня. Останні надають доступ до потужностей серверів, що мають постійний канал зв'язку з глобальною мережею.

Від параметрів серверів залежить якість послуг, що надаються та максимальна кількість одночасних підключень.

Також провайдери відповідають за:

- якість трафіку;
- швидкість з'єднання;
- модернізацію використовуваних мереж, їхній ремонт і обслуговування.

Ці та інші обов'язки продиктовані вимогами ліцензій, які потрібні провайдерам для надання послуг зв'язку, зокрема телефонії та телебачення.

За будь-якого зі сценаріїв використання інтернету взаємодія відбувається за таким алгоритмом:

- користувацький запит надходить на сервер провайдера;
- запит проходить обробку і переходить на потрібний сервер в інтернеті;
- дані з інтернет-сервера надходять на обладнання провайдера;
- від провайдера дані надходять користувачеві.

Цей алгоритм передавання даних можна вважати константою під час виконання будь-яких завдань у режимі онлайн: від пошуку сайту до скачування файлів.

1.2 Характеристика діяльності компанії інтернет-провайдера «Воля»

Компанія «Воля» є одна із провідних загальнонаціональних українських телекомунікаційних компаній. Вона надає послуги аналогового та цифрового телебачення, а головною послугою є – високошвидкісне з'єднання з мережею Інтернет.

Компанія пропонує до 200 програм українських і кращих міжнародних телекомпаній, дотримуючись усіх міжнародних норм у галузі авторських і суміжних прав.

Чисельність персоналу інтернет провайдера Volia налічується біля 3000 чоловік.

Стабільна та швидка передача даних – основна перевага доступу до всесвітньої павутини від Volia. Тут можна замовити бездротове або провідне підключення на швидкості до 1 Гбіт/с. При цьому, незалежно від розташування багатоквартирного будинку в Дніпрі, погоди за вікном та навантажень на мережу у вихідні та свята, можна бути впевненим у безперебійній роботі інтернету.

Для цього компанія використовує якісне обладнання та сучасні технології. Оптиковолоконний кабель забезпечує блискавичну передачу сигналу без спотворень навіть на великі відстані.

Також компанія надає послуги дата-центру. Дата-центр надає в користування хмарні та фізичні сервери, пропонує розміщення, colocation серверів клієнтів, хмарну інфраструктуру IaaS та великий перелік супутніх сервісів.

Дата-центри мають наступні переваги:

- відмовостійкий технічний майданчик, еталонний uptime 99,98%;
- персональний менеджер та цілодобовий Support;
- автоматизація CLOUDSERVER та хмарна інфраструктура від VMWare;
- більше 14 років роботи та професійна команда IT-спеціалістів;
- тарифні плани для проєктів будь-якого рівня.

Послуга CLOUDSERVER – служить для тих, хто запускає роботу невеликого віртуального офісу, відкриває інтернет-магазин, розміщує сайти клієнтів або має потребу в тестовому середовищі.

Послуга Dedicated – надає можливість використання персональних виділених серверів, для більшості важких проєктів нашого часу. Компанія надає різні моделі апаратної частини під різні запити клієнтів. Апаратна спроможність може бути застосована під важкі вимоги, а саме – онлайн ігри, мережу сайтів, соціальні мережа та ін.

Послуга Colocation – надає можливість клієнтам використовувати своє апаратне забезпечення в дата-центрах компанії, при цьому отримувати найдійне електропостачання та безпеку від зовнішнього середовища. За невелику плату людина може мати майже свій дата-центр.

Послуга CLOUD IaaS – надає послуги по віртуальній взаємодії з мережею. Дана послуга імітує послугу «Dedicated», але на рівні віртуальних спроможностей. Можна сказати, що це віртуальний дата-центр кожного клієнта, який може модернізувати та масштабувати мережу.

1.3 Організаційна структура підрозділів мережі компанії

Організаційна структура компанії «Воля» вміщує в собі керівників та посередників компанії, а також виробничі підрозділи за індивідуальним напрямом.

Організаційна структура компанії розрахована на налаштування та підтримку користувачів в онлайн часі.

Кожен рівень в структурі компанії є важливим та виконує свої певні функції для працездатності системи.

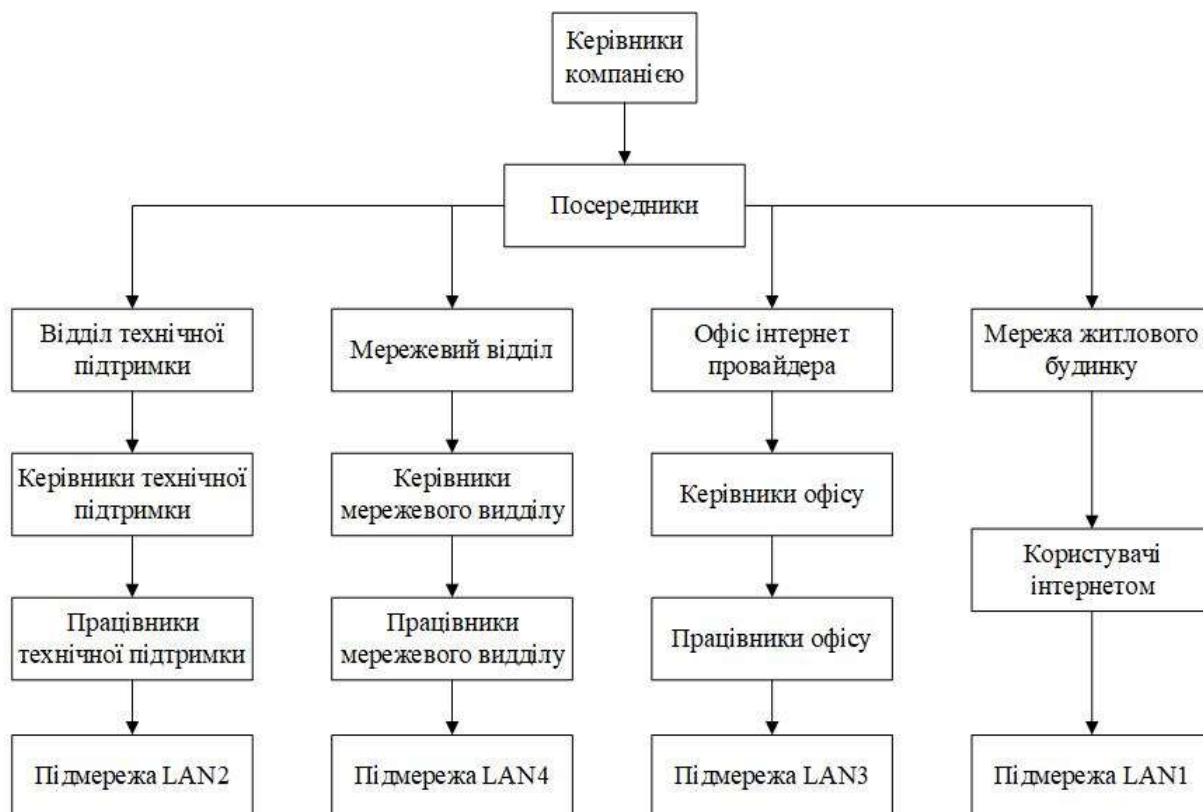


Рисунок 1.1 – Організаційна схема компанії

Мережевий відділ – займається проектуванням, створенням і налаштуванням комп'ютерних мереж, встановленням і налагодженням обладнання, розподіленням IP-адресації в мережі.

Технічна підтримка – обробляє всі запити клієнтів, а саме підключення або відключення послуг, вирішення питань щодо доступу до мережі, регулюванням швидкості передачі даних на вузлах, вирішення індивідуальних пропозицій клієнтів, тощо.

Офіс інтернет провайдера – має фізичний прийом клієнтів, приймає оплату за тарифами клієнтів, продає мережеве обладнання, консультує користувачів за

тарифами та базовими налаштуванням мережевого обладнання. Здійснює записи клієнтів для виїзду мережевого відділу на адрес користувачів, які налаштовують мережу.

Мережа будинків(вузлів) – це є кінцеві вузли компанії, які використовують надані послуги та формують локальну мережу в глобальну мережу.

1.4 Розміщення офісів інтернет-провайдера

У центрі продажу та обслуговування виконується основна робота з клієнтами, тому для зручності були створені офіси у м. Дніпро, які мають зручну геопозицію для всіх точок міста.

Центри обслуговування розташовані наступним чином:



Рисунок 1.2 – Розташування офісів на мапі міста

Офіси розташовані на обох берегах міста, що додає зручності всім користувачам міста. Відстань між офісами займає майже 8км. Кожен користувач може відвідувати оптимальну для нього точку.

1.5 Опис відділів та принцип підключення вузлів до мережі Інтернет

Обслуговування клієнтів на фізичному рівні відбувається в офісі або центрі продажу та обслуговування.

В ньому знаходяться – 2 ПК, один сервер DNS та принтер.

Вирішенням організаційних питань займається технічна підтримка, яка має приміщення в якому знаходяться – 9 ПК та один сервер HTTP. Комп'ютери розподілені на підмережі по 3 ПК і не мають доступу один до одного.

Здійснення мережевого обліку, налаштування та виправлення помилок на мережевому обладнанні виконує мережевий відділ. В ньому знаходяться – 5 ПК та 2 сервери.

Підключення житлового будинку до мережі виконується на базі наступних технологій – FTTB та FTTH.

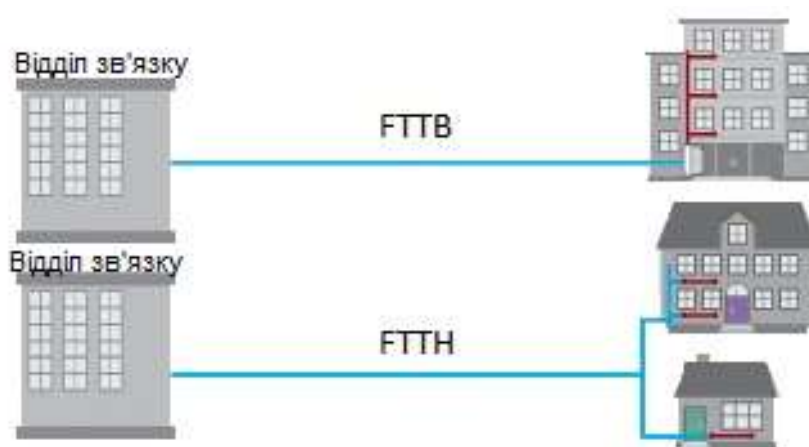


Рисунок 1.3 – Вигляд технології підключення будинків

FTTB (Fiber To The Building) – це технологія, що дає змогу надати інтернет абонентам у багатоквартирні будинки. Вона підходить для офісних будівель, готелів, бізнес-центрів, промислових підприємств та інших комерційних об'єктів. Головна особливість технології FTTB полягає в тому, що в будівлю заводиться оптоволоконний кабель, а фінішне підключення користувачів здійснюється за допомогою мідного дроту (кручена пара).

FTTH (Fiber To The Home) – це тип мережевої архітектури, в якій оптоволокно безпосередньо сягає житлового приміщення. У більшості випадків вона використовується для налаштування домашнього широкосмугового доступу. Оптоволоконна мережа розповсюджується від центральних офісів до житлових приміщень. Волоконно-оптичні кабелі закінчуються межі житлового приміщення.

Таким чином, окремі будинки та офіси можуть ефективніше використовувати мережу.

1.6 Завдання і мета роботи

Завданням кваліфікаційної роботи виступає моделювання та побудова мережі житлового будинку, розробка апаратної частини та конфігурування IP-адресації кінцевих вузлів мережі.

Проект має перелік завдань, за яким буде налаштовуватися мережа, а саме:

- проаналізувати систему впровадження;
- визначити вимоги щодо технічного забезпечення мережі;
- обрати топологію проектування мережі;
- за технічними вимогами створити таблицю специфікації мережевого обладнання;
- за технічними вимогами створити таблицю структурованих кабельних систем;
- за технічними вимогами створити таблицю IP-адресації компанії;
- за технічними вимогами виконати налаштування пристроїв;
- за інформаційними вимогами налаштувати програмне забезпечення;
- налаштувати всі мережеві протоколи;
- налаштувати систему безпеки на мережевому обладнанні;
- розробити компонент системи пожежогасіння в офісному приміщенні, шляхом впровадження технологій інтернету речей;
- відобразити налаштування в додатку Cisco Packet Tracer.

1.7 Визначення можливих напрямків рішення поставлених завдань

Для моделювання комп'ютерної системи компанії "Воля" з реалізацією налаштування, безпеки та підключень будинків до мереж, потрібно здійснити наступні рішення:

- топологію проектування мережі слід обирати за принципом зручності управління мережею та відповідно до кількості користувачів в мережі, що сприяє складності побудови;
- мережеве обладнання обирати за доцільністю фінансової частини та відповідністю до масштабування системи;
- структуровані кабельні системи використовувати за сучасними стандартами, та відповідно до необхідності використання витої пари чи оптоволоконного кабелю;
- для побудови IP-адресації компанії в локальній мережі, можна застосовувати діапазон локальних адрес за вимогами проекту;
- для побудови IP-адресації компанії в глобальній мережі, можна використати певний пул адресів за протоколом NAT;
- для розподілу мережі на підмережі можна застосовувати технологію віртуальних локальних мереж;
- для забезпечення мережевого резервування, можна впровадити агрегування каналів, що дозволить мережевому обладнанню завжди мати доступ до мережі.

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

Компанія інтернет-провайдера «Воля» надає послуги з доступу до мережі інтернет. Для функціонування організаційної мережі та для надання послуг, повинні бути створені підрозділи управління компанії.

Компанія інтернет-провайдера «Воля» складається з наступних підмереж:

1. підмережа технічної підтримки;
2. підмережа мережевого відділу;
3. підмережа офісу управління;
4. підмережа житлового будинку.

Мережа компанії повинна вміщувати в собі 118 співробітників та надавати доступ до локальної та глобальної мережі.

Характеристикою підрозділів компанії є бажання підключити якомога більше абонентів до мережі Інтернет.

Компанія має централізовану схему управління, яка має – керівника, посередників, керівників підрозділів та співробітників в цих підрозділах. Організаційні питання вирішуються на рівні керівника. Підмережі житлових будинків знаходяться на нижчому рівні в мережі.

Для компанії інтернет-провайдера «Воля» необхідно створити систему пожежогасіння в відділах управління за допомогою технологій IoT.

Система повинна мати вогняний датчик, який проводить аналіз пожежі, та пожежний сповіщувач, який подає воду при пожежі.

Всі ці механізми повинні працювати на основі коду та мікроконтролеру MCU.

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

Підмережі інтернет-провайдера повинні забезпечуватися комп'ютерами для кожного співробітника, з яких буде виконуватися зв'язок між підмережами для обміну інформацією.

Підмережі компанії повинні мати локальну адресацію, яка має автоматичне налаштування. Зв'язок між підмережами повинен забезпечуватися за допомогою протоколу OSPF.

Відносно фізичного способу зв'язку повинні використовуватися мережеві кабелі за сучасними стандартами. Підтримку та працездатність ліній зв'язку повинні забезпечувати мережеві протоколи.

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

Для забезпечення взаємозв'язку створюваної мережі із суміжними мережами або ж підмереж компанії та мереж підключених будинків необхідно мати глобальну адресацію, яка застосовується за протоколом NAT.

Для підключення будинків до мережі інтернет-провайдера потрібно використовувати статичний маршрут на загальний маршрутизатор в кожному будинку.

2.1.1.1.4 Вимоги до режимів функціонування мережі

Кожен рівень в структурі компанії є важливим та повинен виконувати свої певні функції для працездатності системи.

Мережевий відділ – повинен займатися проектуванням, створенням і налаштуванням комп'ютерних мереж, встановленням і налагодженням обладнання, розподіленням IP-адресації в мережі.

Технічна підтримка – повинна обробляти всі запити клієнтів, а саме підключення або відключення послуг, вирішенням питань щодо доступу до мережі,

регулюванням швидкості передачі даних на вузлах, вирішення індивідуальних пропозицій клієнтів, тощо.

Офіс інтернет провайдера – повинен мати фізичний прийом клієнтів, приймати оплату за тарифами клієнтів, продавати мережеве обладнання, консультувати користувачів за тарифами та базовими налаштуванням мережевого обладнання. Здійснювати записи клієнтів для виїзду мережевого відділу на адрес користувачів, які налаштовують мережу.

Мережа будинків(вузлів) - це є кінцеві вузли компанії, які використовують надані послуги та формують корпоративну мережу в глобальну мережу.

2.1.1.1.5 Вимоги до діагностування мережі

Забезпечення діагностування мережі інтернет-провайдера є головною вимогою компанії. Вирішення питань не стабільного зв'язку та доступності до мережі інтернет повинно виконуватися цілодобово.

Відповідальні за доступність мережі повинні організувати перевірку налаштувань мережевого обладнання за для виявлення помилок чи випадкового скидання налаштувань.

2.1.1.1.6 Перспективи розвитку та модернізації мережі

Обслуговування великої кількості абонентів повинно забезпечувати постійний розвиток та модернізацію мережевого обладнання.

Кожного дня відбувається підключення нових сегментів мережі, при цьому кожного разу повинен бути зроблений аналіз мережевої спроможності будинку, в якому додається підключення. Якщо мережева спроможність низька, необхідно замінити мережеве обладнання на більш вдосконалене. Також, повинна перевірятися таблиця IP-адресації на кількість доступних адрес в мережі, при цьому мати резервування адрес, на випадок великого замовлення на послуги інтернет-провайдера.

2.1.1.2 Вимоги до показників призначення

Мережева інфраструктура інтернет-провайдера повинна забезпечувати підключення абонентів міста до мережі Інтернет, з повним обслуговуванням мережевого обладнання та забезпечувати високу швидкість передачі даних та надійне підключення до мережі.

2.1.1.3 Вимоги до експлуатації

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

Відділи управління компанії та підмережі будинків не мають потреби в особливих умовах зберігання мережевого обладнання. Середнє значення температурного режиму навколишнього середовища повинна дорівнювати 15-20 градусів.

2.1.1.3.2 Вимоги до параметрів мереж енергопостачання

Кожний пристрій в мережі повинен забезпечуватися напругою 220 Вольт для однофазних систем, при частоті 50Гц.

Мережеве обладнання компанії не потребує додаткового резервного енергопостачання.

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

Для обслуговування та підтримки працездатності мережі повинні бути 5 працівників мережевого відділу.

Для обслуговування клієнтів та обробки їх запитів повинні бути 9 працівників технічної підтримки.

Також, для обслуговування клієнтів на фізичному рівні безпосередньо у відділені необхідні 2 людини.

Графік роботи повинен передбачувати цілодобову підтримку ліній зв'язку.

Всі співробітники повинні мати щонайменше освіту молодшого спеціаліста в галузі ІТ-технологій та володіти навичками діагностики мережі та виправлення помилок.

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

Складне приміщення інтернет-провайдера повинно забезпечувати мінімальні вимоги для підключення абонентів к мережі Інтернет, а саме мати в наявності – кабель вита пара та оптоволокно, конектори під кожний вид кабелю, резервне мережеве обладнання комутаторів та маршрутизаторів, а також прилади для монтажу в стійках.

Всі елементи резервного призначення повинні забезпечувати надійність та відповідати гарантії виробника.

2.1.1.3.5 Вимоги до регламенту обслуговування мережі

Апаратне обслуговування мережі повинно здійснюватися за викликом клієнта або за встановленим попередньо графіком. Графік проведення робіт повинен бути узгоджений с абонентами мережі.

Графік обслуговування мережі повинен бути створений з урахуванням тимчасового простою мережі та недоступності до мережі Інтернет. Графік повинен виконуватися в ASAP режимі та здійснюватися відповідно від навантаження, але не рідше чим 1 раз на 10 днів.

2.1.1.4 Вимоги до патентної чистоти

В Україні діє законодавство, що регулює патентну чистоту для інтернет-провайдерів. Основні правила патентної чистоти такі:

- інтернет-провайдер не повинен надавати доступ до контенту, який порушує авторські права;
- інтернет-провайдер повинен використовувати захисні технології, щоб уникнути несанкціонованого доступу до інформації клієнтів;

– інтернет-провайдер повинен використовувати тільки ліцензійне забезпечення.

2.1.1.5 Додаткові вимоги

2.1.1.5.1 Вимоги до активного обладнання

Активне обладнання, а саме – маршрутизатори та комутатори повинні відповідати запиту від мережі та використовувати сучасні технології мережевого обладнання.

Швидкість передачі даних всередині мережі (комутаторах) повинна відповідати значенню від 100 Мбіт/с до 1000 Мбіт/с, тоді швидкість передачі даних на маршрутизаторах повинна бути забезпечена в 10 Гбіт/с.

Підключення активного мережевого обладнання повинно здійснюватися через оптоволоконний кабель.

Мережеві картки пристроїв співробітників повинні використовувати формат підключення RJ-45.

2.1.1.5.2 Вимоги до кабель каналів, інформаційним та електричним розеткам

Кабель-канал повинен мати достатню ширину, щоб забезпечити передачу всіх необхідних кабелів та проводів та бути захищений від зовнішніх впливів, таких як фізичні пошкодження, пил, волога і електромагнітні перешкоди.

Інформаційні розетки повинні забезпечувати підключення пристроїв в мережі та мати формат розетки RJ-45.

Електричні розетки потрібно використовувати відносно кількості пристроїв в мережі та мати формат європейського типу з напругою 220 Вольт.

2.1.1.5.3 Вимоги до комунікаційного обладнання і його розташування

Комунікаційне обладнання повинно мати вбудовані механізми безпеки для захисту мережі від несанкціонованого доступу та бути енергоефективним для зниження споживання електроенергії та теплових викидів.

Розташування комунікаційного обладнання повинно забезпечувати належну вентиляцію і охолодження.

Для монтажу мережевого обладнання в відділах та житлових будинках потрібно використовувати стійки, які мають формат розміщення на стіні.

Обладнання повинно мати можливість масштабування для врахування зростаючих потреб мережі.

Підключення мережевого обладнання повинно бути структуровано відведено від стійки та закріплені хомутами.

2.1.1.5.4 Вимоги до однорідності

Також, повинна бути розроблена спрощена система налаштування конфігурацій різних пристроїв мережі шляхом автоматизованих протоколів, таких як – DHCP.

2.1.2 Вимоги до задач, які виконуються у комп'ютерній системі

2.1.2.1 Вимоги до кожної підмережі та переліку їх функцій

Кожна підмережа в кваліфікаційній роботі повинна виконувати функції забезпечення персоналу доступом до мережі інтернет та передачі даних між собою.

При цьому мережеве обладнання та пристрої мережі повинні відповідати вимогам щодо базового налаштування. Вимоги наступні:

- пристрої та мережеве обладнання повинні мати назву відповідно до прикладу *Hryva_Router_1*, а саме мати – прізвище, тип пристрою та номер;
- мережеве обладнання повинно мати пароль за замовчування – *cisco*, який повинен встановлюватися до консолі та до лінії *vty*;
- мережеве обладнання повинно мати пароль привілейованого режиму – *class*;

- налаштування пристроїв та мережевого обладнання повинно виконуватися виключно в зашифрованому вигляді;
- для відображення інформації студента повинен бути створений банер MOTD;
- використання ліній vty повинно бути забезпечено за допомогою протоколу безпечного управління – *ssh*;
- облікові записи для доступу до мережевого обладнання повинні мати формат – *123-20zck-1_Hryva*, де *123-20zck-1* – це група студента, *Hryva* – прізвище студента;
- в налаштуванні пристроїв повинно бути налаштовано доменне ім'я, яке повинно відповідати назві пристрою та мати шифрування даних за допомогою RSA-ключа з довжиною 1024 біт;
- маршрутизатори які містять DCE-інтерфейси повинні мати тактову частоту 128000;
- повідомлення процесу *exec* про початок та кінець повинно мати аудит за допомогою локальної бази.

Після базового налаштування пристроїв, потрібно налаштувати протокол маршрутизації на мережевому обладнанні за наступними вимогами:

- інтерфейси мережевого обладнання повинні бути відключені від розповсюдження таблиць маршрутизації та мати оголошення мереж, які підключення фізично до обладнання;
- віртуальні локальні мережі повинні мати єдиний маршрут та повинні бути розповсюджені між мережевим обладнанням;
- пропускна спроможність, яка використовується для обчислення вартості маршруту за протоколом OSPF повинна мати значення – 1000 на gigabit інтерфейсах;
- на інтерфейсах *serial* вартість метрики повинна дорівнювати 7500, в свою чергу пропускна спроможність повинна дорівнювати 128 кб/с;

- на маршрутизаторах повинен бути налаштований маршрут за замовчуванням до інтернет-провайдера, в свою чергу розповсюдження таблиці маршрутизації від провайдера повинно здійснюватися за протоколом OSPF;

- протокол OSPF повинен об'єднувати тільки підмережі компанії. Мережі які підключені до провайдера не повинні застосовуватися в таблицях маршрутизації протоколу;

- при необхідності розгортанні невеликої підмережі потрібно використовувати статичні маршрути.

Мережеве обладнання повинно мати захист від зловмисників за допомогою протоколу AAA та відповідати наступним вимогам:

- перевірка даних за протоколом повинна мати локальну базу облікових записів про користувачів мережі;

- доступ до мережевого обладнання повинен виконуватися за допомогою аутентифікації за протоколом RADIUS. При непрацездатності серверу, аутентифікація повинна виконуватися за допомогою локальних облікових записів;

- в якості секретного слова в сервері потрібно використовувати – radius123;

- облікові записи співробітників повинні містити ім'я пристроїв та використовувати пароль – admin123.

Доступ до мережі Інтернет повинен відбуватися за допомогою підключення до інтернет-провайдера. Корпоративна мережа повинна використовувати локальну IP-адресацію в мережі та для виходу в глобальну мережу використовувати IP-адресацію за протоколом NAT.

Налаштування протоколу NAT повинно відповідати наступним вимогам:

- мати назву – *Internet*;

- IP-адресація повинна застосовуватися з початкової адреси 209.165.200.5 по кінцеву 209.165.200.30;

- повинен бути створений список доступу відповідно до номеру варіанта завдання.

Для збереження та відображення інформації щодо кваліфікаційної роботи потрібно налаштувати сервер НТТР, який повинен мати взаємодію між доменним ім'ям та IP-адресою. Ім'я «http://123.dnipro.ua» повинно відповідати IP-адресі 209.165.200.4.

2.1.2.2 Часовий регламент і вимоги до якості реалізації кожної функції

Корпоративна мережа повинна мати чіткий часовий регламент, який визначає, коли і як швидко повинні бути виконані певні функції, одна з яких входить та визначає, за який час повинна передаватися інформація з однієї точки мережі в іншу.

Мережеві адміністратори повинні мати зручні інструменти для налаштування, моніторингу та управління мережевими ресурсами.

2.1.3 Вимоги до видів забезпечення комп'ютерної системи

2.1.3.1 Вимоги до математичного забезпечення

У вигляді математичного забезпечення мережі є розрахунок, який повинен відображати швидкість передачі даних каналу та середній час затримки.

Розрахунок повинен відбуватися в мережі, яка має найбільший об'єм користувачів та найбільше потенціальне навантаження в мережі.

2.1.3.2 Вимоги до інформаційного забезпечення

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

Система повинна мати записи щодо налаштування мережевого обладнання, а саме – код налаштування з описом дій, для подальшого використання іншими співробітниками компанії.

2.1.3.2.2 Вимоги до інформаційної сумісності із суміжними мережами

Програмне забезпечення повинно відповідати стандартам використання програм в інших галузях та використовувати додатки редагування та збору інформації постачальника Microsoft.

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

Мережа повинна мати механізми для збору даних з різних джерел, які можуть бути розташовані в різних частинах мережі. Повинні використовуватися пристрої для збору даних, такі як – сервери. Також, повинно бути надійне підключення до цих джерел і передачу даних до місця обробки.

2.1.3.3 Вимоги до лінгвістичного забезпечення

Пристрої в мережі повинні забезпечувати обробку та отримання інформації на зручних мовах для співробітників, які повинні легко налаштовуватися індивідуально під кожну людину.

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

Технічні засоби корпоративної мережі повинні підтримувати програмні додатки microsoft office та team viewer, які є ключовим програмним забезпеченням для налаштування та відображення інформації.

Комутатори повинні забезпечувати 24 підключення кінцевих вузлів мережі, при цьому мати резервовану кількість портів під модернізацію мережі або для непередбачених випадків у зв'язку з перебоями портів.

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

Підрозділи мережі повинні мати відповідну інфраструктуру для забезпечення надійного і безперебійного функціонування мережі. Робота кожного підрозділу повинна бути чітко визначена за для уникнення дублювання роботи.

Відділи мережі повинні бути забезпечені засобами комунікації та зв'язку для ефективного обміну інформацією та спілкування один між одним.

2.1.3.5.2 Вимоги до захисту від помилкових дій персоналу мережі

Кожен член персоналу, який має доступ до мережі, повинен пройти процедуру автентифікації, щоб підтвердити свою ідентичність.

Після автентифікації персонал повинен бути авторизований із відповідними рівнями доступу до мережевих ресурсів. Це повинно обмежити доступ до критичних систем.

2.1.3.6 Вимоги до методичного забезпечення

Кваліфікаційна робота повинна мати відповідну інструкцію та документацію з кожного аспекту проекту, а саме повинна мати:

- схему організації персоналу;
- схему організації пристроїв в мережі;
- таблиці апаратної частини мережі;
- таблиці IP-адресації пристроїв;
- схема початкового варіанту топології мережі;
- схема кінцевого варіанту топології мережі;
- розрахунок швидкості передачі даних каналу;
- графічний матеріал налаштування мережі;
- графічний матеріал перевірки налаштувань мережі;
- код налаштування мережевого обладнання.

2.2 Розробка апаратної частини мережі інтернет-провайдера

2.2.1 Розробка схеми комплексу технічних засобів мережевої інфраструктури

Структурна схема комп'ютерної системи включає в себе комплекс технічних засобів, які взаємодіють між собою для забезпечення функціонування та працездатності системи.

Інтернет провайдер «Воля» знаходиться в двох точках міста та має три приміщення. Комплекс структурних засобів полягає в поєднанні всіх частин мережі в єдину корпоративну мережу.

Локальна мережа компанії складається з початкових елементів – активного мережевого обладнання. Маршрутизатор має головний рівень управління та виконує маршрутизацію вузлів своєї мережі. Після побудови маршрутизації діє рівень комутації, де здійснюється підключення вузлів мережі в єдину контрольовану систему. Таким чином, кожна підмережа отримує вихід до глобальної мережі інтернет.

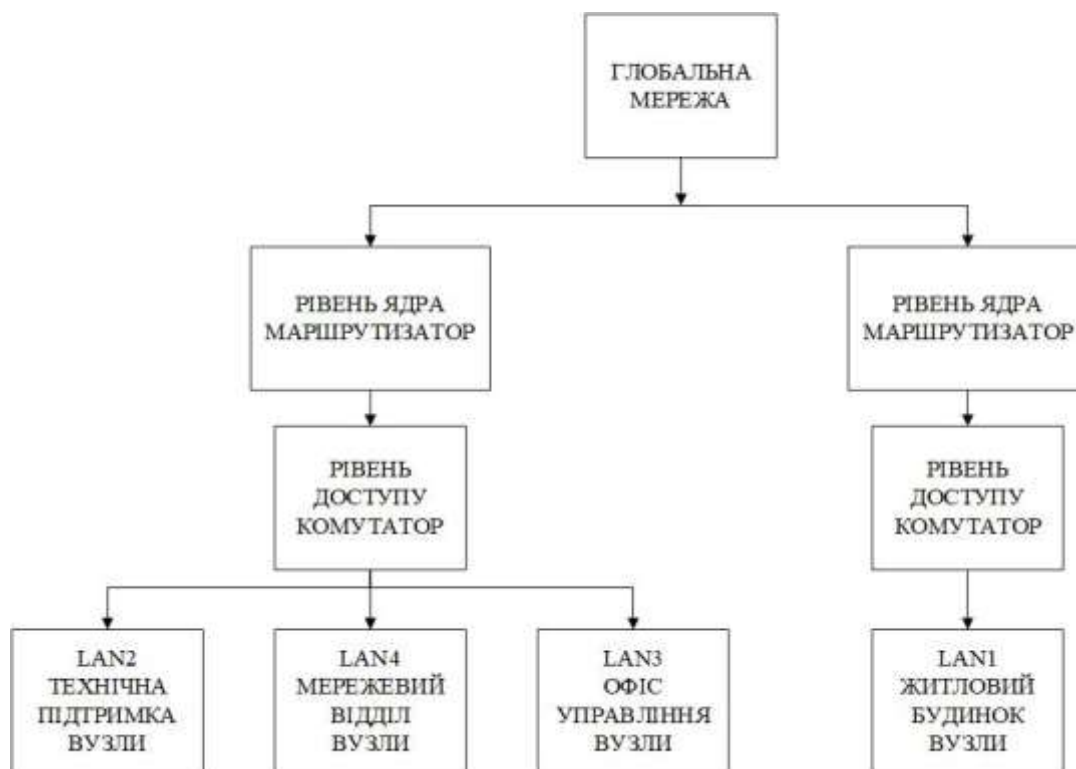


Рисунок 2.1 – Структурна схема комплексу технічних засобів мережевої інфраструктури компанії «Воля»

В свою чергу, будинки які підключаються до мережі інтернет-провайдера мають таку саму структуру як і в локальній мережі відділів компанії, при цьому будинок має безпосередній фізичний канал підключення від інтернет-провайдера «Воля».

Маршрутизація в мережі працює на протоколі OSPF, а також має статичні маршрути до магістральних маршрутизаторів. Для обробки або отримання інформації між мережами та будинками використовується глобальна мережа. Вихід в глобальну мережу забезпечує протокол NAT.

Для зрозумілості масштабу структурної схеми (рисунок 2.1) були створені топологічні схеми кожного відділу компанії з урахуванням проведення кабелю та його довжини. Підключення вузлів в мережі виконується кабелем – вита пара cat.5e.

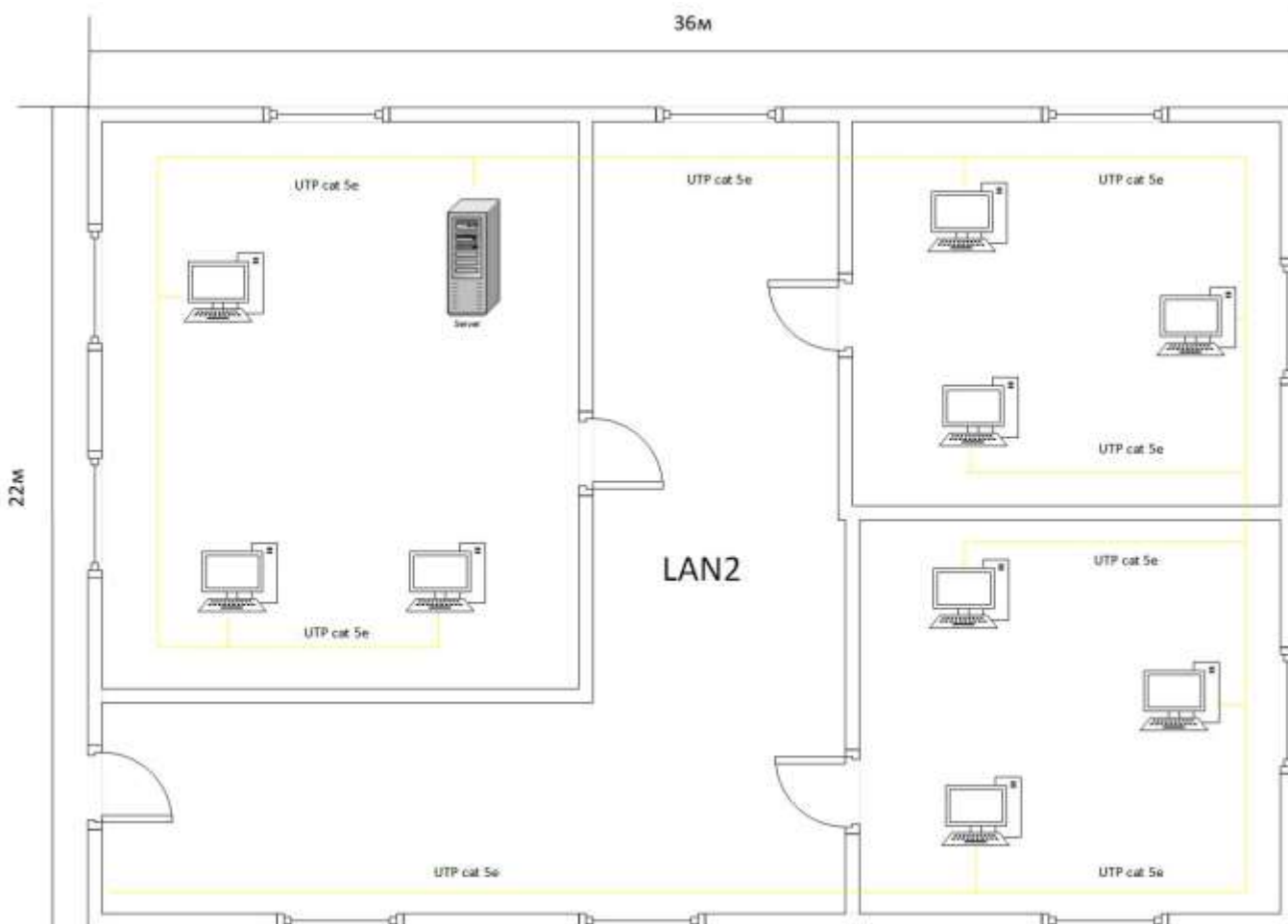


Рисунок 2.2 – Топологічна схема відділу технічної підтримки

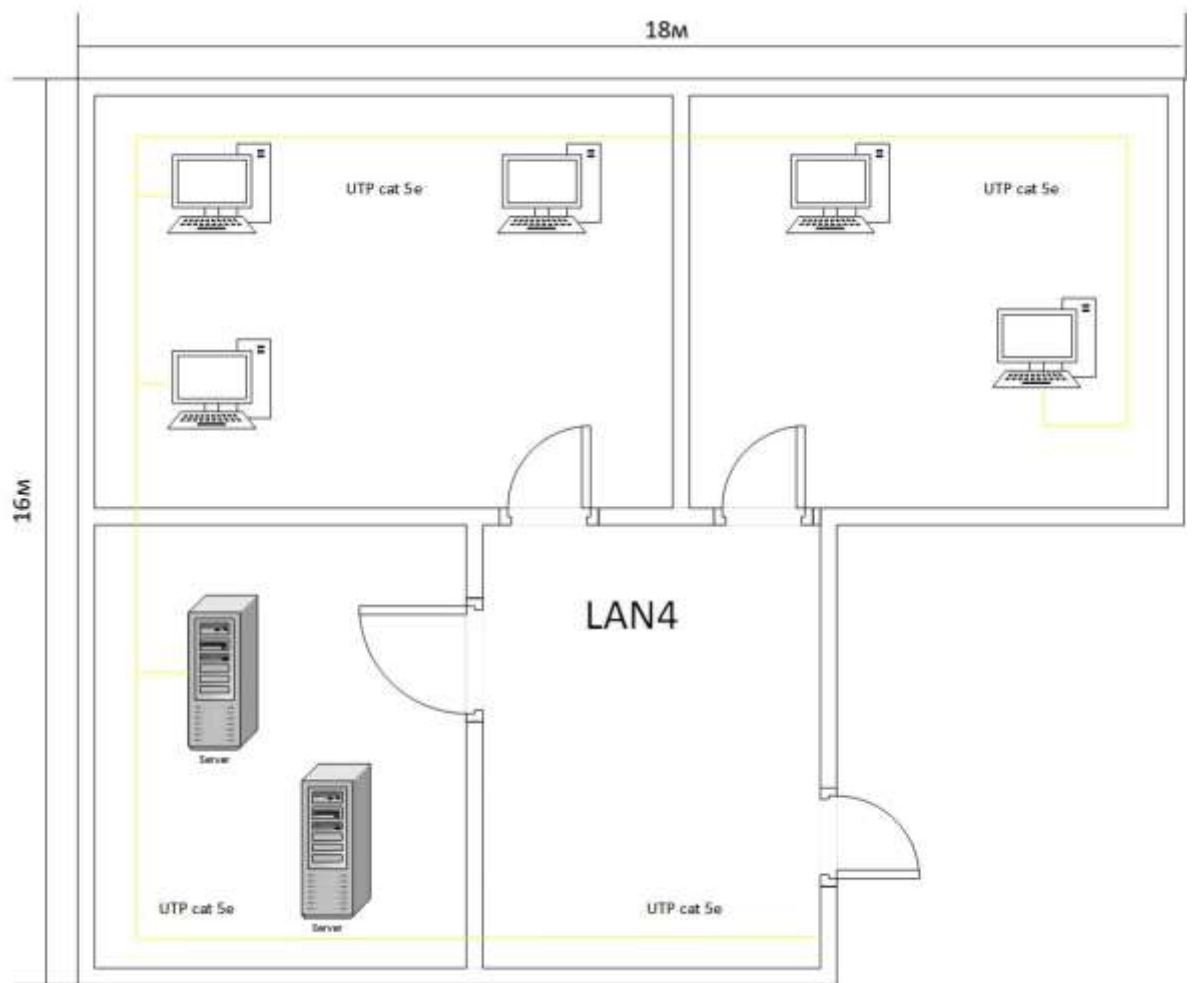


Рисунок 2.3 – Топологічна схема мережевого відділу

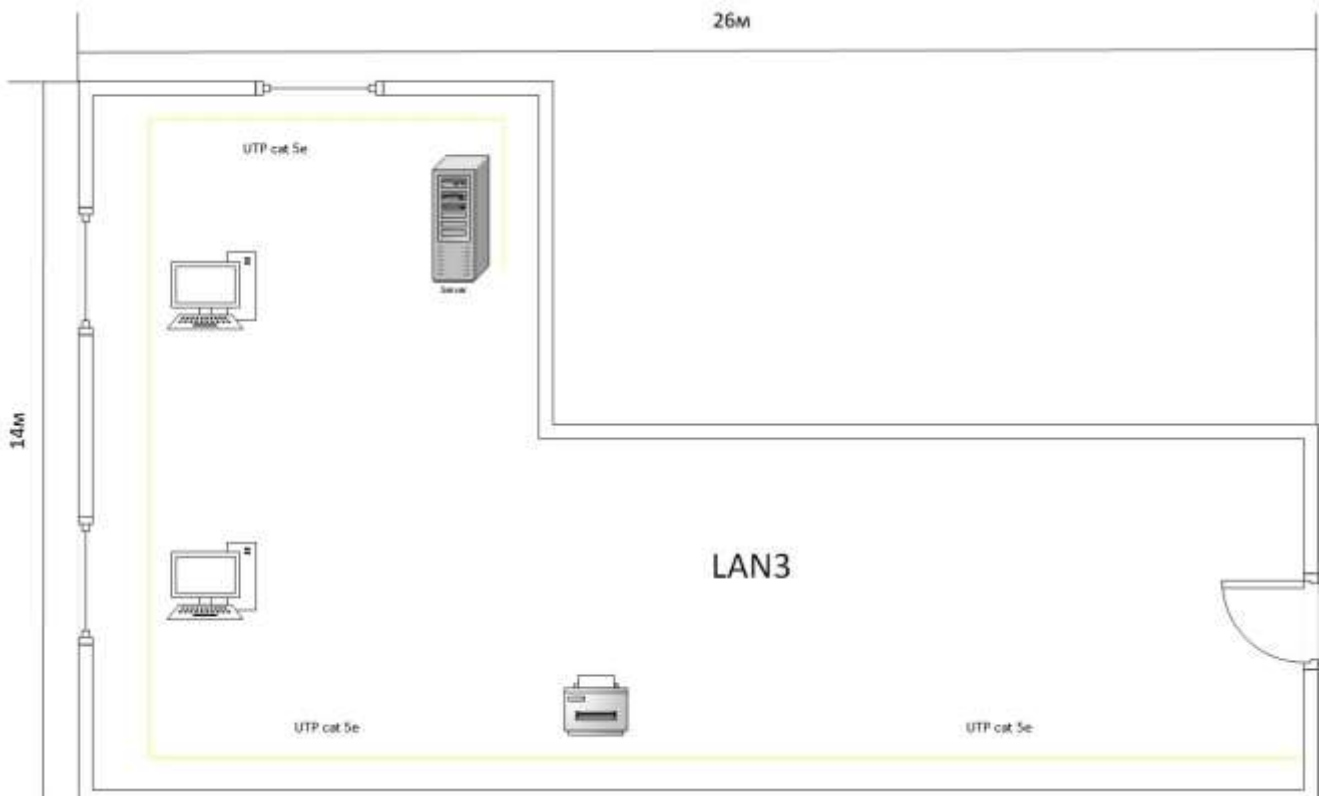


Рисунок 2.4 – Топологічна схема офісного приміщення

2.2.2 Реалізація фізичного підключення будинка до мережі

Для детального відображення фізичного підключення будинку до мережі провайдера було змодельовано схему в додатку Cisco Packet Tracer.

В ній демонструється офіс провайдера та будинок, який підключається до офісу.



Рисунок 2.5 – Схема розташування підключення в місті

Офіс та будинок підключається за допомогою оптоволоконного кабелю.



Рисунок 2.6 – Схематичне зображення будинку

Будинок має під'їзд (subway) в якому в свою чергу знаходяться комутатори та кінцеві пристрої користувачів (квартири).

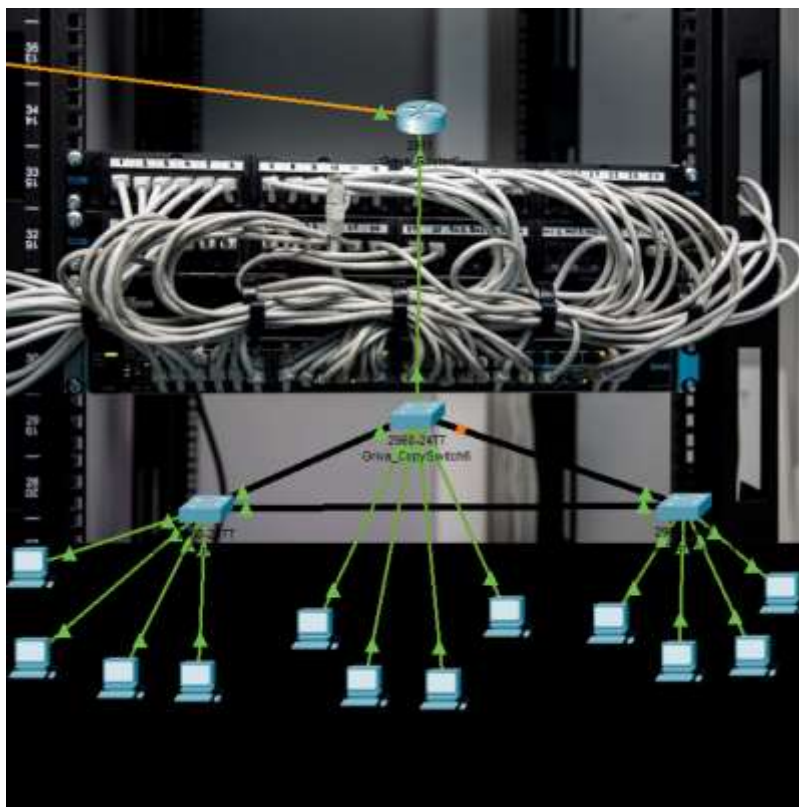


Рисунок 2.7 – Фізичне підключення під'їзду

В під'їзді використовуються 3 комутатори які мають 12 вузлів. Комутатори під'єднані до загального маршрутизатора, який в свою чергу вже підключений до мережі провайдера.

Всі вузли в мережі з'єднуються кабелем – вита пара та використовують систему структурованих кабельних систем зв'язку.

Для детального проектування підключення було побудовано таблицю специфікацій структурованої кабельної системи мережі.

Таблиця 2.1 – Специфікація структурованої кабельної системи мережі

Позиція	Тип, марка, найменування	Технічна характеристика	Одиниці виміру	Кількість
1.	Кабельний канал, монтаж на підлозі	Розмір – 40 мм x 40 мм Довжина – 2 м	од	30

Кінець таблиці – 2.1

2.	Кабельний канал, монтаж на стіні	Розмір – 20 мм х 20 мм Довжина – 2 м	од	60
3.	Інформаційна розетка	Тип – RJ-45 Категорія – UTP cat5e Портів – 2шт	од	12
4.	Блок електричних розеток	Напруга – 220В Входів – 8	од	7
5.	Кабель вита пара	Тип – RJ-45 Категорія – UTP cat5e	м	250
6.	Оптоволоконний кабель	Тип – SC	м	100
7.	Конектор	Тип – RJ-45	од	30
8.	Конектор	Тип – SC	од	20
9.	Стійка	Формат – на стіні Розмір – 6U	од	7
10.	Патч-панель	Формат – в стійку	од	7

2.2.3 Розробка апаратного забезпечення мережі

За схематичними умовами та вимогами Системи в цілому була розроблена та відображена специфікація мережевого обладнання у вигляді таблиці 2.2 з повними характеристиками та кількістю.

Таблиця 2.2 – Специфікація мережевого обладнання

Позиція	Тип, марка, найменування	Технічна характеристика	Одиниц і виміру	Кількі сть
1.	Комутатор Catalyst 2960	Портів – 24; Тип портів – RJ-45, SC; Швидкість інтерфейсів – 10/100/1000 Мбіт; Управління – CLI.	од.	7

Кінець таблиці – 2.2

2.	Маршрутизатор Cisco 2911	Портів – 3 RJ-45, 4 – SC; Швидкість інтерфейсів – до кількох сотень мегабіт або гігабіт на секунду	од.	7
----	-----------------------------	---	-----	---

Також, була розрахована та відображена специфікація пристроїв мережі, яка містить детальні технічні вимоги до пристроїв, які будуть використовуватися в офісному середовищі. Все компоненти наведені у таблиці 2.3.

Таблиця 2.3 – Специфікація пристроїв мережі

Позиція	Тип, марка, найменування	Технічна характеристика	Одиниц і виміру	Кількість
1	Блок ПК – DTOP Business	Intel Core i5-3470 3.4 ГГц ОЗП 8 ГБ DDR4 3200МГц SSD 240гб відеоадаптер Intel HD Graphics БЖ 400Вт	од.	16
2	Монітор Acer Nitro	діагональ дисплея 23.8 дюймів частота 75 Гц роздільна здатність дисплея 1920x1080 (FullHD) інтерфейси 2 x HDMI та 1 x VGA	од.	16
3	Клавіатура Gembird	KB-UML3-01-UA USB (EN/RU/UA)	од.	16
4	Миша A4Tech	N-70FX-1 USB Black	од.	16

2.2.4 Розробка програмного забезпечення мережі

Для забезпечення програмної підтримки мережі Інтернет провайдера «Воля» були встановлені додатки.

Microsoft Access – це інструмент для збору і структурування інформації.



Рисунок 2.8 – Логотип програми MS Access

У базі можуть зберігатися дані про людей, а саме – особисті дані, термін оплати тарифного плану та сам тарифний план, також зберігається індивідуальне налаштування кожного користувача.

TeamViewer – це програмне забезпечення віддаленого доступу управління комп'ютера, яке також забезпечує обмін інформацією між вузлами.

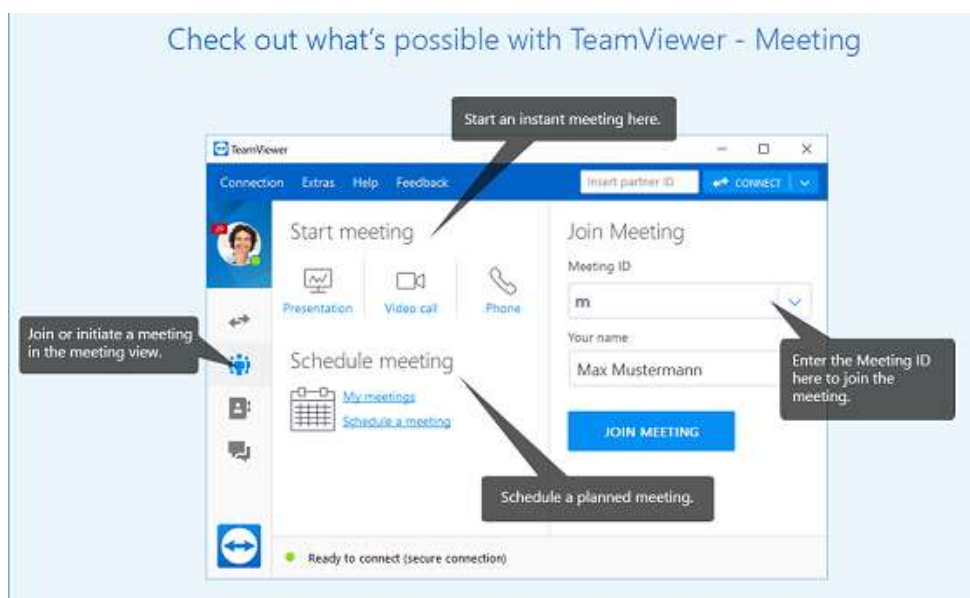


Рисунок 2.9 – Функціонал програми TeamViewer

Рішення для віддаленого доступу дозволяє:

- організовувати спеціальний віддалений доступ до комп'ютерів колег або клієнтів;

- встановлювати з'єднання між комп'ютерами з різними операційними системами;
- адмініструвати сервера і робочі станції Windows;
- підключатися з мобільних пристроїв до комп'ютерів;
- підключатися до пристроїв Android та iOS для надання технічної підтримки;
- виконувати моніторинг системи з інтегрованими перевітками стану для віддаленого моніторингу та відстеження ресурсів.

2.2.5 Розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі компанії

Головною умовою розрахунку інтенсивності вихідного трафіку є те, що кінцеве значення мережі повинно задовольняти пропускну здатність каналу у 1000 Мбіт/с або 1Гбіт/с.

Найбільша локальна підмережа має – 48 вузлів, при цьому інтенсивність трафіку дорівнює 126 кадрів/с. В якості розміру повідомлень в мережі візьмемо середнє значення – 650 байт. Загальна кількість вузлів в мережі дорівнює – 118.

Також, після розрахунку необхідно, щоб мережа не перевищувала затримку передачі пакетів у значенні бмс.

Розрахунок можливий за умови представлення мережі в максимальному навантаженні. Розрахуємо пропускну спроможність мережі на рівні доступу:

$$P_{p,d} = \mu * 1 * n * 8 = 126 * 650 * 24 * 8 = 15,72 \text{ Мбіт/с}, \quad (2.1)$$

де n – кількість портів в комутаторі.

Розрахуємо пропускну здатність мережі на рівні розподілу:

$$P_{p,r} = \mu * 1 * N * 8 = 126 * 650 * 48 * 8 = 314,49 \text{ Мбіт/с}, \quad (2.2)$$

де N – кількість вузлів в найбільшій мережі.

Відповідь розрахунку входить у норму пропускну здатності каналу у 1000 Мбіт/с, що свідчить на неперевантаження обладнання.

При передачі трафіку з комутатора на маршрутизатор зі швидкістю 1000 Мбіт/с, навантаження на комутатор не повинно перевищувати значення:

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

Кожний вузол в мережі виробляє 126 кадрів/с, тоді розрахуємо максимальне значення доступних вузлів в мережі:

$$N = 192\ 310 / 126 = 1526 \text{ джерел} \quad (2.4)$$

Найбільша мережа в 48 вузлів входить в це значення, та мережа має великий потенціал для масштабування.

Інтенсивність вихідного трафіку користувачів найбільшої мережі:

$$\lambda = N * \mu = 48 * 126 = 6048 \text{ пакетів/с} \quad (2.5)$$

Коефіцієнт затримки:

$$\rho = \lambda / \mu_{\text{вих}} = 6048 / 192\ 310 = 0,031 \quad (2.6)$$

Коефіцієнт навантаження комутатора рівня доступу:

$$r = \rho / (1 - \rho) = 0,031 / (1 - 0,031) = 0,031 \quad (2.7)$$

Середня затримка кадру, пов'язана з чергою М/М/1, становить:

$$T = 1 / ((\mu - \lambda)) = 1 / (192\ 310 - 6048) = 5,36 \text{ мкс} \quad (2.8)$$

Середня довжина черги:

$$L_{\text{чер}} = \rho^2 / (1 - \rho) = (0,031)^2 / (1 - 0,031) = 0,00099 \quad (2.9)$$

Середній час знаходження пакетів у черзі:

$$T_{\text{оч}} = L_{\text{чер}} / \lambda = 0,00099 / 6048 = 1,63 \text{ мкс} \quad (2.10)$$

Отримане значення є меншим за ≤ 6 мс.

Пропускна здатність каналу:

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

$$b = \lambda * l = 6048 * 650 * 8 = 31\ 449\ 600 \text{ біт/с} = 31,44 \text{ Мбіт/с} \quad (2.11)$$

Значення пропускної здатності каналу відповідає швидкості 1000 Мбіт /с.

3 РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Розрахунок та розробка схем корпоративної мережі компанії

3.1.1 Розробка логічної топології системи

Архітектура мережі створюється на базових принципах та вимогах до кваліфікаційної роботи. В якості розподілення адресації IPv4 для кожного сегмента мережі використовувалася мережа 192.168.8.0 з маскою /24.

З використанням на комутаторах технології віртуальних локальних мереж для розподілу на сегменти, мережа є захищеною та дозволяє використання механізмів брандмауерів, систем виявлення вторгнень та шифруванням даних, для підвищення безпеки архітектурної частини мережі.

Мережа забезпечує регулярне резервне копіювання мережевих конфігурацій та даних на централізоване серверне сховище, яке має назву – TFTP.

Доступ до мережі Інтернет(WAN) застосовується завдяки використанню маршрутизаторів, які здатні керувати трафіком та забезпечувати безпеку зовнішніх з'єднань.

В якості безпеки використовується технологія AAA для централізованої аутентифікації та керування користувачами.

Для ефективної працездатності мережі використано сучасне мережеве обладнання з високою пропускнуною спроможністю, а саме до 100 Мбіт/с на робочу станцію та до 10 Гбіт/с на мережевому обладнанні.

Кожний крок побудови архітектури мережі включає в собі тести та перевірку перед кожним етапом.

При розробці схеми мережі, включаючи фізичну було побудовано і логічну топологію мережі.

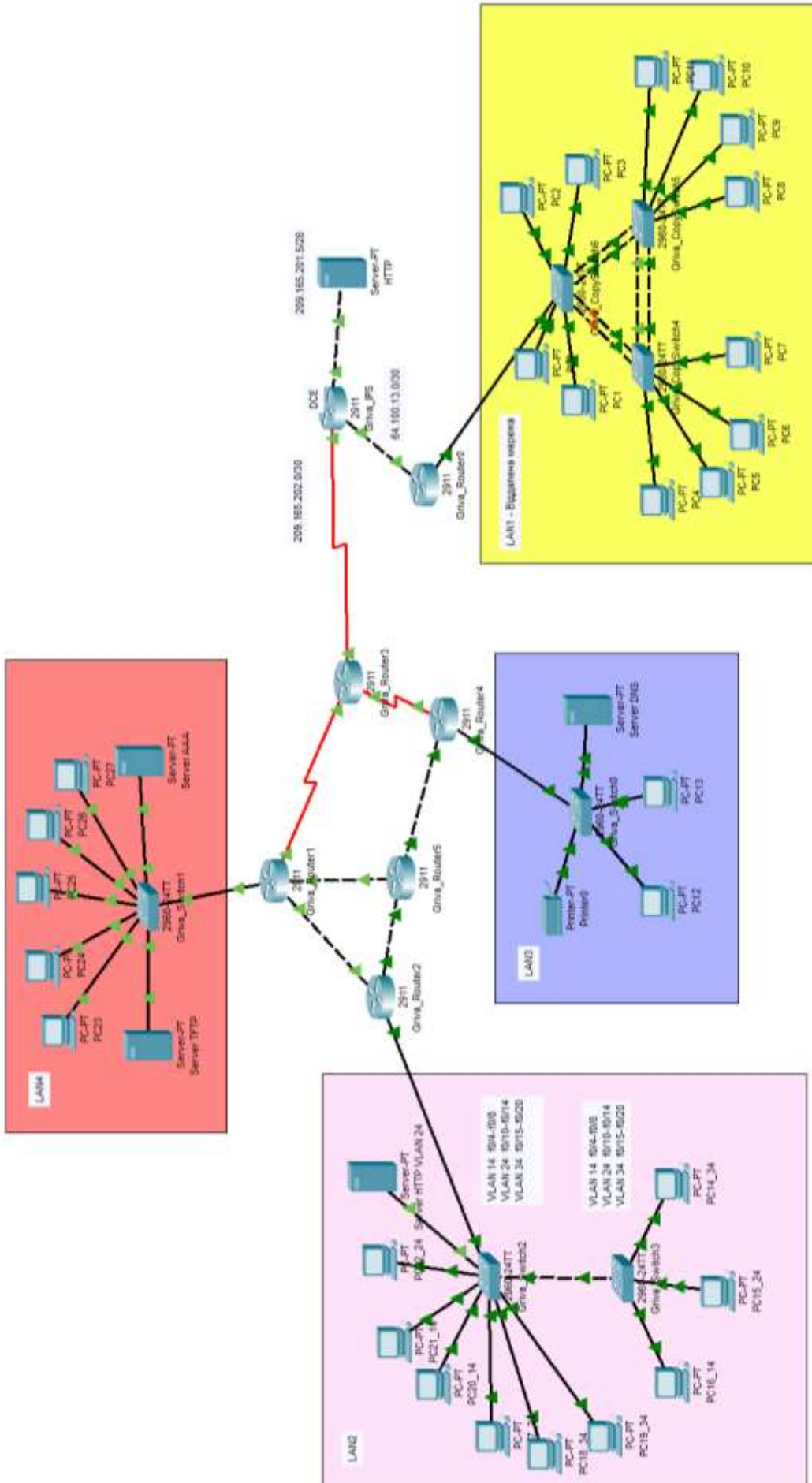


Рисунок 3.1 – Логічна топологія системи компанії «Воля»

3.1.2 Розрахунок схеми адресного простору підмереж та маршрутизаторів

Розрахунок адресації вузлів в кожній підмережі виконується виключно до вимог компанії та поставлених завдань до кваліфікаційної роботи.

Початкові дані для розрахунку відображені в таблиці 3.1.

Також, для маршрутизації мережевого обладнання були виділені адреси 10.0.4.0 за маскою – /30.

Таблиця 3.1 – Адреса мережі та кількість вузлів в кожній підмережі

Адреса	LAN1	LAN2	LAN3	LAN4
192.168.8.0/24	48	41	7	22

Маска підмережі визначає кінцеві точки діапазону IP-адрес підмережі. У будь-якій мережі дві адреси завжди резервуються для спеціальних цілей. Адреса "0" – це мережева адреса та ідентифікатор мережі, а адреса "255" виділена як ширококомовна адреса. Вони не можуть бути виділені пристроям в мережі та мережевому обладнанню.

Розмір адресного простору: IPv4 використовує 32-бітові адреси і може підтримувати приблизно 4,3 мільярда (2^{32}) унікальних адрес. Зі збільшенням кількості пристроїв, під'єднаних до Інтернету, адресного простору IPv4 стане недостатньо. IPv6 використовує 128-бітові адреси і може забезпечити приблизно $3,4 \times 10^{38}$ (2^{128}) унікальних адрес. Це дуже велика кількість адрес, і кожному пристрою у світі може бути виділена унікальна адреса IPv6.

Ми знаходимося на початковому рівні переходу протоколів від IPv4 до IPv6, з кожним роком протокол IPv6 буде набирати обертів.

Розрахуємо адресацію для підмережі LAN1, при умові що в мережі знаходяться 48 користувачів:

– маска 255.255.255.224 або /27 забезпечує 30 вузлів, та не підходить для вирішення. Маска 255.255.255.192 або /26 забезпечує 62 вузли, яке забезпечує наше число та надає гнучкості в підмережі.

– тоді, використовуємо адресу 192.168.8.0 з маскою /26 та маємо доступні вузли з 192.168.8.1 по 192.168.8.62.

Таблиця 3.2 – Адресний простір підмереж та маршрутизаторів мережі

Назва підмережі	Кількість вуз.	Адреса підмережі	Маска підмережі	Діапазон допустимих IP-адрес	
LAN1	48	192.168.8.0	255.255.255.192	192.168.8.1	192.168.8.62
LAN2	41	192.168.8.64	255.255.255.192	192.168.8.65	192.168.8.126
LAN4	22	192.168.8.128	255.255.255.224	192.168.8.129	192.168.8.158
LAN3	7	192.168.8.160	255.255.255.224	192.168.8.161	192.168.8.190
VLAN14	5	192.168.8.80	255.255.255.240	192.168.8.81	192.168.8.94
VLAN24	5	192.168.8.96	255.255.255.240	192.168.8.97	192.168.8.110
VLAN34	6	192.168.8.112	255.255.255.240	192.168.8.113	192.168.8.126
WAN1	2	10.0.4.0	255.255.255.252	10.0.4.1	10.0.4.2
WAN2	2	10.0.4.4	255.255.255.252	10.0.4.5	10.0.4.6
WAN3	2	10.0.4.8	255.255.255.252	10.0.4.9	10.0.4.10
WAN4	2	10.0.4.12	255.255.255.252	10.0.4.13	10.0.4.14
WAN5	2	10.0.4.16	255.255.255.252	10.0.4.17	10.0.4.18
WAN6	2	10.0.4.20	255.255.255.252	10.0.4.21	10.0.4.22
WAN IPS	2	209.165.202.0	255.255.255.252	209.165.202.1	209.165.202.2
WAN віддалена мережа	2	64.100.13.0	255.255.255.252	64.100.13.1	64.100.13.2

3.1.3 Розрахунок схеми адресного простору вузлів підмереж

За принципом розрахунку адресного простору підмереж та маршрутизаторів мережі зробимо розрахунок адресного простору всіх вузлів в мережі. За вимогами компанії «Воля» та для зручності налаштування та використання мережевого обладнання перші вільні адреси потрібно призначити маршрутизаторам.

Наступні адреси використовуються для комутаторів та серверів, які розташовані безпосередньо в мережі.

Після розрахунку адресації кожної підмережі потрібно задіяти протокол DHCP. для підвищення швидкості налаштування та для прибирання чиннику помилки від людини.

Таблиця 3.3 – Адресний простір вузлів мережі

Ім'я пристрою	Інтерфейс	IP-адреса	Маска	Шлюз	VLAN	Інтерфейс пристрою
Мережа IPS						
Hryva_IPS	S0/3/0	209.165.202.1	/30	–	–	S0/3/0
	G0/0	64.100.13.1	/30	–	–	G0/0
Host_IPS	NIC	209.165.201.5	/28	–	–	Fa0/1
Мережа LAN4						
Hryva_Router3	S0/2/0	10.0.4.22	/30	–	–	S0/2/0
	S0/3/0	209.165.202.2	/30	–	–	S0/3/0
	S0/3/1	10.0.4.18	/30	–	–	S0/3/1
Hryva_Router1	G0/0	10.0.4.9	/30	–	–	G0/0
	G0/1	10.0.4.6	/30	–	–	G0/1
	G0/2	192.168.8.129	/26	–	–	G0/2
	S0/3/0	10.0.4.21	/30	–	–	S0/3/0
Hryva_Switch1	Vlan1	192.168.8.130	/27	192.168.8.129	–	G0/2
PC23-27	NIC	192.168.8.131 -192.168.8.135	/27	192.168.8.129	–	Fa0/2-0/6
Server TFTP	NIC	192.168.8.132	/27	192.168.8.129	–	Fa0/1
Server AAA	NIC	192.168.8.138	/27	192.168.8.129	–	Fa0/7
Мережа LAN3						
Hryva_Router4	G0/0	10.0.4.14	/30	–	–	G0/0
	G0/1	192.168.8.161	/27	–	–	G0/1
	S0/3/1	10.0.4.17	/30	–	–	S0/3/0
Hryva_Switch0	Vlan1	192.168.8.163	/27	192.168.8.161	–	G0/1
PC12-13	NIC	192.168.8.164 - 192.168.8.165	/27	192.168.8.161	–	Fa0/2-0/3
Server DNS	NIC	192.168.8.162	/27	192.168.8.161	–	Fa0/1

Кінець таблиці 3.3

Printer	NIC	192.168.8.166	/27	192.168.8.161	–	Fa0/4
Мережа LAN2						
Hryva_Router2	G0/0	10.0.4.1	/30	–	–	G0/0
	G0/1	10.0.4.5	/30	–	–	G0/1
	G0/2	192.168.8.65	/26	–	–	G0/2
Hryva_Switch2	Vlan1	192.168.8.67	/28	192.168.8.65	–	G0/2
Hryva_Switch3	Vlan1	192.168.8.68	/28	192.168.8.65	–	G0/2
PC20_14-21_14	NIC	192.168.8.82- 192.168.8.83	/28	192.168.8.81	14	Fa0/4-0/5 Sw2
PC16_14	NIC	192.168.8.84	/28	192.168.8.81	14	Fa0/4 - Sw3
PC15_24	NIC	192.168.8.100	/28	192.168.8.97	24	Fa0/10 - Sw3
PC22_24	NIC	192.168.8.98	/28	192.168.8.97	24	Fa0/11 – Sw2
PC17_34-19_34	NIC	192.168.8.114 192.168.8.115 192.168.8.117	/28	192.168.8.113	34	Fa0/15 - 0/17 - Sw2
PC14_34	NIC	192.168.8.116	/28	192.168.8.113	34	Fa0/15 - Sw3
Server HTTP	NIC	192.168.8.99	/28	192.168.8.97	24	Fa0/10 - Sw2
Мережа LAN1						
Hryva_Router0	G0/0	64.100.13.2	/30	–	–	G0/0
	G0/1	192.168.8.1	/26	–	–	G0/1
Hryva_CopySwitch 4-6	Vlan1	192.168.8.2- 192.168.8.4	/26	192.168.8.1	–	Fa0/1-0/4
PC0-3	NIC	192.168.8.5- 192.168.8.8	/26	192.168.8.1	–	Fa0/5-0/8 Sw-1
PC4-7	NIC	192.168.8.9- 192.168.8.12	/26	192.168.8.1	–	Fa0/5-0/8 Sw-2
PC8-11	NIC	192.168.8.13 192.168.8.16	/26	192.168.8.1	–	Fa0/5-0/8 Sw-3

3.1.4 Розробка фізичної топології та обґрунтування використання кабельних систем

Від вибору фізичної топології мережі залежить дуже багато факторів безпеки та швидкості передачі даних.

Топологія комп'ютерної мережі – це схема з'єднання і фізичне розташування мережевих пристроїв, включно з комп'ютерами, по відношенню один до одного.

Топологія комп'ютерної мережі дає змогу побачити всю мережу, точніше її структуру, а також проаналізувати зв'язок усіх пристроїв, щодо підключення до мережі.

При створенні проекту було використано топологію «дерево», це топологія яка вміщує в себе об'єднання декількох топологій «зірка».

Топологія виду дерево забезпечує підключення вузлів с самого низу до самої поверхні мережі – мережі Інтернет, проходячи комутаційний та маршрутизаційний рівні.

В даній топології застосовані структуровані кабельні системи зв'язку.

Структуровані кабельні системи зв'язку – це фізичне середовище для організації передавання даних у будівлі або в групі будівель. Під час побудови мережі застосовуються стандартні елементи (кабелі, комутатори та інше спеціалізоване обладнання, елементи роз'ємів). У проектуванні систем застосовуються загальноприйняті правила і стандарти. Під час приймання обладнання мереж має відповідати певним нормам. Завдяки стандартизації побудови мереж досягається необхідний рівень типових параметрів (швидкість передавання даних, захист від втрат інформації), проводиться адміністрування мереж і вирішення інших завдань з управління мережі.

3.2 Налаштування сегментів мережі та перевірка працездатності мережі в цілому

3.2.1 Базове налаштування конфігурації пристроїв

Для подальшого налаштування пристроїв в мережі необхідно виконати базове налаштування маршрутизаторів.

Налаштуємо конфігурацію маршрутизатора за базовими вимогами:

```
Router1(config)#hostname Hryva_Router1 // даємо назву пристрою
```

```
Hryva_Router1(config)#service password-encryption // застосовуємо шифрування введених паролів
```

```
Hryva_Router1 (config)#enable secret class // вказуємо пароль у привілейований режим
```

```
Hryva_Router1 (config)#line console 0 // входимо до налаштувань лінії консолі
```

```
Hryva_Router1 (config-line)#password cisco // вказуємо пароль до ліній консолі
```

```
Hryva_Router1 (config-line)#login // вказуємо запит паролю назавжди
```

```
Hryva_Router1 (config)#banner motd #123-20zck Hryva authorization PASSWORD# // вказуємо текст відображення при авторизації в консолі
```

```
Hryva_Router1 (config)#username 12320zck_Hryva password cisco; // створення користувача з ім'ям 12320zck_Hryva та паролем cisco
```

```
Hryva_Router1 (config)#ip domain-name Hryva_Router1 // створення домену
```

```
Hryva_Router1 (config)#crypto key generate rsa // вказуємо шифрування паролів за принципом RSA
```

```
How many bits in the modulus [512]: 1024 // система пропонує 512біт для складності шифрування, але ми використовуємо 1024біти
```

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

```
Hryva_Router1 (config)#line vty 0 4
```

```
Hryva_Router1 (config-line)#login local // вказуємо умову, щоб при вході до лінії вказували логін та пароль
```

```
Hryva_Router1 (config-line)#transport input ssh // вказуємо протокол, за яким можна підключитися к маршрутизатору за допомогою віддаленого доступу
```

3.2.2 Налаштування динамічного протоколу маршрутизації в мережі

Після налаштування адресації пристроїв та мережевого обладнання потрібно налаштувати протокол, який зможе обмінюватися інформацією про адреси з іншими мережами, тобто маршрутизувати мережу за протоколом динамічної маршрутизації OSPF.

Для початку виконаємо налаштування на маршрутизаторі Hryva_Router3, який є магістральним:

```
Hryva_Router3 (config)#router ospf 1 // вмикаємо протокол
```

```
Hryva_Router3 (config-router)#network 10.0.4.16 0.0.0.3 area 0 // робимо об'яву мережі 10.0.4.16, яка підключена до маршрутизатора
```

```
Hryva_Router3 (config-router)#network 10.0.4.20 0.0.0.3 area 0 // робимо об'яву мережі 10.0.4.20, яка підключена до маршрутизатора
```

Маршрут за замовчуванням на Hryva__IPS:

```
ip route 0.0.0.0 0.0.0.0 209.165.202.1 // вказуємо статичний маршрут на інший магістральний маршрутизатор
```

Тепер робимо такі налаштування на всіх маршрутизаторах, які потребують цей протокол:

```
Hryva_Router1 (config-router)#network 10.0.4.4 0.0.0.3 area 0
```

```
Hryva_Router1 (config-router)#network 10.0.4.8 0.0.0.3 area 0
```

```
Hryva_Router1 (config-router)#network 10.0.4.20 0.0.0.3 area 0
```

```
Hryva_Router1 (config-router)#network 192.168.8.128 0.0.0.31 area 0
```

```
Hryva_Router4(config-router)#network 10.0.4.12 0.0.0.3 area 0
```

```
Hryva_Router4 (config-router)#network 10.0.4.16 0.0.0.3 area 0
```

```
Hryva_Router4 (config-router)#network 192.168.8.160 0.0.0.31 area 0
```

```
Hryva_Router2(config-router)#network 10.0.4.0 0.0.0.3 area 0
```

```
Hryva_Router2 (config-router)#network 10.0.4.4 0.0.0.3 area 0
```

```
Hryva_Router2 (config-router)#network 192.168.8.64 0.0.0.15 area 0
```

```
Hryva_Router2 (config-router)#network 192.168.8.80 0.0.0.15 area 0
```

```
Hryva_Router2 (config-router)#network 192.168.8.96 0.0.0.15 area 0
```

```
Hryva_Router2 (config-router)#network 192.168.8.112 0.0.0.15 area 0
```

```
Hryva_Router5 (config-router)#network 10.0.4.0 0.0.0.3 area 0
```

```
Hryva_Router5 (config-router)#network 10.0.4.8 0.0.0.3 area 0
```

```
Hryva_Router5 (config-router)#network 10.0.4.12 0.0.0.3 area 0
```

Після виконання об'яв всі мережі будуть автоматично знати про існування кожної.

За вимогами компанії виконуємо налаштування на serial-інтерфейсах:

Hryva_Router3 (config)#interface s0/3/0 // використовуємо serial-інтерфейс

Hryva_Router3 (config-if)#bandwidth 128 // вказуємо пропускну спроможність

Hryva_Router3 (config-if)# clock rate 128000 // вказуємо швидкість каналу

Hryva_Router3 (config-if)# ip ospf cost 7500 // вказуємо вартість метрики

```

Gateway of last resort is 209.165.202.1 to network 0.0.0.0

    10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
O       10.0.4.0/30 [110/66] via 10.0.4.17, 4294967276:4294967257:4294967255, Serial0/3/1
        [110/66] via 10.0.4.21, 4294967276:4294967257:4294967255, Serial0/2/0
O       10.0.4.4/30 [110/65] via 10.0.4.21, 4294967276:4294967257:4294967255, Serial0/2/0
O       10.0.4.8/30 [110/65] via 10.0.4.21, 4294967276:4294967257:4294967255, Serial0/2/0
O       10.0.4.12/30 [110/65] via 10.0.4.17, 4294967276:4294967257:4294967255,
Serial0/3/1
C       10.0.4.16/30 is directly connected, Serial0/3/1
L       10.0.4.18/32 is directly connected, Serial0/3/1
C       10.0.4.20/30 is directly connected, Serial0/2/0
L       10.0.4.22/32 is directly connected, Serial0/2/0
    192.168.8.0/24 is variably subnetted, 6 subnets, 2 masks
O       192.168.8.64/28 [110/66] via 10.0.4.21, 4294967276:4294967257:4294967255,
Serial0/2/0
O       192.168.8.80/28 [110/66] via 10.0.4.21, 4294967276:4294967257:4294967255,
Serial0/2/0
O       192.168.8.96/28 [110/66] via 10.0.4.21, 4294967276:4294967257:4294967255,
Serial0/2/0
O       192.168.8.112/28 [110/66] via 10.0.4.21, 4294967276:4294967257:4294967255,
Serial0/2/0
O       192.168.8.128/27 [110/65] via 10.0.4.21, 4294967276:4294967257:4294967255,
Serial0/2/0
O       192.168.8.160/27 [110/65] via 10.0.4.17, 4294967276:4294967257:4294967255,
Serial0/3/1
    209.165.201.0/28 is subnetted, 1 subnets
S       209.165.201.0/28 [1/0] via 209.165.202.1
    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       209.165.202.2/32 is directly connected, Serial0/3/0
S*    0.0.0.0/0 [1/0] via 209.165.202.1

```

Рисунок 3.2 – Схема адресації за протоколом OSPF

3.2.3 Налаштування динамічного NAT

NAT – Network Address Translation, що на перекладі – метод трансляції мережевих адрес.

Комп'ютер може бути під'єднаний до Інтернету безпосередньо (біла IP-адреса), або через NAT – тоді комп'ютер має локальну IP-адресу, з Інтернету недоступну (приватна, сіра).

Налаштування здійснюються на магістральному маршрутизаторі, який має діапазон публічних адрес з 209.165.200.5 по 209.165.200.30.

Налаштуємо магістральний маршрутизатор:

Hryva_Router3(config)# access-list 4 permit 192.168.8.0 0.0.0.255// створюємо список доступу для надходження локальних адрес до протоколу

Hryva_Router3 (config)#ip nat inside source list 4 interface s0/3/0 // використовуємо створений список доступу до вхідного інтерфейсу маршрутизатора

Hryva_Router3 (config)#interface Serial0/3/0 // вибираємо інтерфейс

Hryva_Router3 (config-if)#ip nat outside // назначаємо його в режим виходу

Hryva_Router3 (config-if)#interface Serial0/3/1 // вибираємо інтерфейс

Hryva_Router3 (config-if)#ip nat inside // назначаємо його в режим входу

Hryva_Router3 (config-if)#ip nat pool Internet 209.165.200.5 209.165.200.30 netmask 255.255.255.224 // створюємо пул адрес перетворення

Hryva_Router3 (config-if)#ip nat inside source list NAT pool Internet // підключаємо пул адрес перетворення

Після налаштування, при передачі файлів між віддаленими мережами з'являються записи щодо перетворення адрес.

Pro	Inside global	Inside local	Outside local	Outside global
icmp	209.165.202.2:2	192.168.8.165:2	192.168.8.2:2	192.168.8.2:2
icmp	209.165.202.2:3	192.168.8.165:3	192.168.8.2:3	192.168.8.2:3
icmp	209.165.202.2:4	192.168.8.165:4	192.168.8.2:4	192.168.8.2:4
icmp	209.165.202.2:5	192.168.8.165:5	192.168.8.2:5	192.168.8.2:5
icmp	209.165.202.2:6	192.168.8.165:6	192.168.8.2:6	192.168.8.2:6
icmp	209.165.202.2:7	192.168.8.165:7	192.168.8.2:7	192.168.8.2:7
icmp	209.165.202.2:8	192.168.8.165:8	192.168.8.2:8	192.168.8.2:8

Рисунок 3.3 – Схема перетворення мережевих адрес

3.2.4 Налаштування списків доступу ACL

Для віртуальних локальних мереж потрібно створити правила, за якими буде виконуватися маршрутизація між підмережами. Це можна зробити шляхом створення списків доступу ACL. В проекті були створені підмережі VLAN за номерами 14,24 та 34, ці підмережі не повинні мати доступу одна між одною.

Створимо правила для підмереж:

Hryva_Router2 (config)#ip access-list extended network2 // створюємо список з ім'ям *network2*

Hryva_Router2 (config-ext-nacl)#deny ip 192.168.8.80 0.0.0.15 192.168.8.96 0.0.0.15 // командою deny забороняємо проходження трафіку з мережі 192.168.8.80 у мережу 192.168.8.96

Hryva_Router2 (config-ext-nacl)#deny ip 192.168.8.80 0.0.0.15 192.168.8.112 0.0.0.15 // командою deny забороняємо проходження трафіку з мережі 192.168.8.80 у мережу 192.168.8.112

Hryva_Router2 (config-ext-nacl)#deny ip 192.168.8.96 0.0.0.15 192.168.8.112 0.0.0.15 // командою deny забороняємо проходження трафіку з мережі 192.168.8.96 у мережу 192.168.8.112

Hryva_Router2 (config-ext-nacl)#deny ip 192.168.8.96 0.0.0.15 192.168.8.80 0.0.0.15 // командою deny забороняємо проходження трафіку з мережі 192.168.8.96 у мережу 192.168.8.80

Hryva_Router2 (config-ext-nacl)#deny ip 192.168.8.112 0.0.0.15 192.168.8.80 0.0.0.15 // командою deny забороняємо проходження трафіку з мережі 192.168.8.112 у мережу 192.168.8.80

Hryva_Router2 (config-ext-nacl)#deny ip 192.168.8.112 0.0.0.15 192.168.8.96 0.0.0.15 // командою deny забороняємо проходження трафіку з мережі 192.168.8.112 у мережу 192.168.8.96

Hryva_Router2 (config-ext-nacl)#permit ip any any // всі інші адреси мають повну маршрутизацію

Hryva_Router2 (config)#interface gigabitEthernet 0/2.14 // обираємо інтерфейс

Hryva_Router2 (config-subif)#ip access-group network2 in // підключаємо до інтерфейсу список доступу

Hryva_Router2 (config-subif)#interface gigabitEthernet 0/2.24 // обираємо інтерфейс

Hryva_Router2 (config-subif)#ip access-group network2 in // підключаємо до інтерфейсу список доступу

Hryva_Router2 (config-subif)#interface gigabitEthernet 0/2.34 // обираємо інтерфейс

Hryva_Router2 (config-subif)#ip access-group network2 in // підключаємо до інтерфейсу список доступу

Після повного налаштування виконаємо перевірку з мережі 192.168.8.96 у мережу 192.168.8.80 та побачимо що вузли не мають доступу один до одного, що і є умовою створення.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.8.84

Pinging 192.168.8.84 with 32 bytes of data:

Reply from 192.168.8.97: Destination host unreachable.
Reply from 192.168.8.97: Destination host unreachable.
Reply from 192.168.8.97: Destination host unreachable.
Reply from 192.168.8.97: Destination host unreachable.

Ping statistics for 192.168.8.84:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Рисунок 3.4 – Перевірка працездатності списків доступу

3.2.5 Налаштування агрегування каналів PAgP

Агрегація каналів PAgP (Port Aggregation Protocol) – це протокол, який використовується для комбінування кількох фізичних мережевих портів в один логічний канал.

Це дозволяє підвищити пропускну здатність, надійність та ефективність мережі шляхом розподілу трафіку між кількома фізичними портами.

Для працездатності протоколу потрібно виконати налаштування на трьох
Налаштування EtherChannel на Hryva_CopySwitch4:

Hryva_CopySwitch4 (config)#int range fa0/1-2 // обираємо два інтерфейси

Hryva_CopySwitch4 (config-if-range)#shutdown // вимикаємо порт

Hryva_CopySwitch4 (config-if-range)#channel-group 1 mode active // номер 1 вказує на номер групи агрегованих каналів, до якої додається фізичний порт, *active* вказує на режим активної роботи для агрегованого каналу

Creating a port-channel interface Port-channel 1

Hryva_CopySwitch4 (config-if-range)#no shutdown // включаємо порт

Hryva_CopySwitch4 (config-if-range)#exit

Hryva_CopySwitch4 (config)#int port-channel 1 // обираємо групу агрегації

Hryva_CopySwitch4 (config-if)#switchport mode trunk // встановлюємо режим порта на комутаторі як *trunk*

Hryva_CopySwitch4 (config)#int range f0/3-4 // обираємо два інтерфейси

Hryva_CopySwitch4 (config-if-range)#channel-group 2 mode passive // номер 2 вказує на номер групи агрегованих каналів, до якої додається фізичний порт, *passive* вказує на режим пасивної роботи для агрегованого каналу

Creating a port-channel interface Port-channel 2

Hryva_CopySwitch4 (config-if-range)#no shutdown // включаємо порт

Hryva_CopySwitch4 (config)#int port-channel 2 // обираємо групу агрегації

Hryva_CopySwitch4 (config-if)#switchport mode trunk // встановлюємо режим порта на комутаторі як *trunk*

Такі самі налаштування потрібно виконати на комутаторах Hryva_CopySwitch5 та Hryva_CopySwitch6.

Після налаштування перевіримо агрегацію на комутаторах.

```

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)

```

Рисунок 3.5 – Агреговані канали на комутаторах

3.2.6 Перевірка працездатності налаштувань в мережі

Діагностика мережі в цілому починається з перевірки доступу вузлів за допомогою команди ping, яка в свою чергу надсилає ехо-запити або повідомлення кінцевому пристрою та очікує відповідь.

```
C:\>ping 192.168.8.138

Pinging 192.168.8.138 with 32 bytes of data:

Reply from 192.168.8.138: bytes=32 time<1ms TTL=126
Reply from 192.168.8.138: bytes=32 time<1ms TTL=126
Reply from 192.168.8.138: bytes=32 time<1ms TTL=126
Reply from 192.168.8.138: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.8.138:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Рисунок 3.6 – Приклад застосування команди

Для збереження та відображення інформації щодо кваліфікаційної роботи потрібно налаштувати сервер НТТР, який повинен мати взаємодію між доменним ім'ям та IP-адресою. Ім'я «http://123.dnipro.ua» повинно відповідати IP-адресі 209.165.200.4.

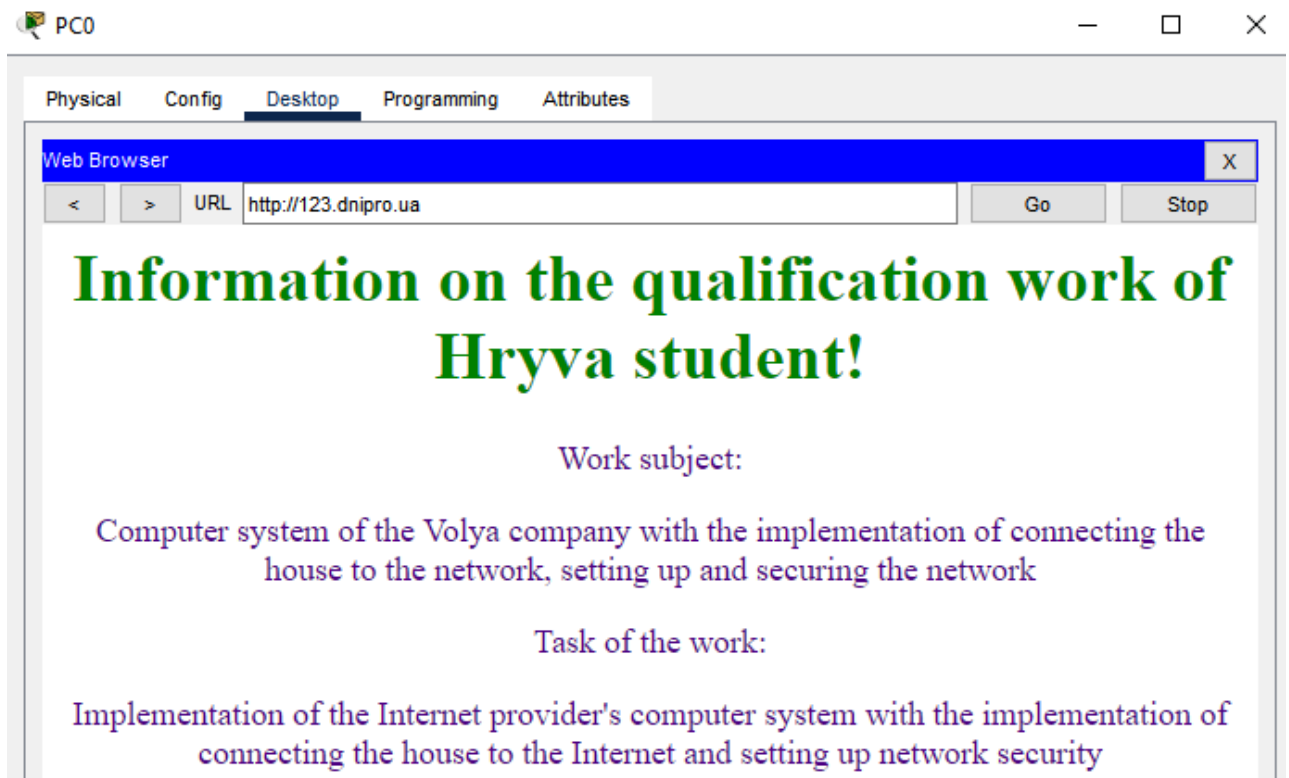


Рисунок 3.7 – Перевірка доступності веб-сайту та роботи серверу

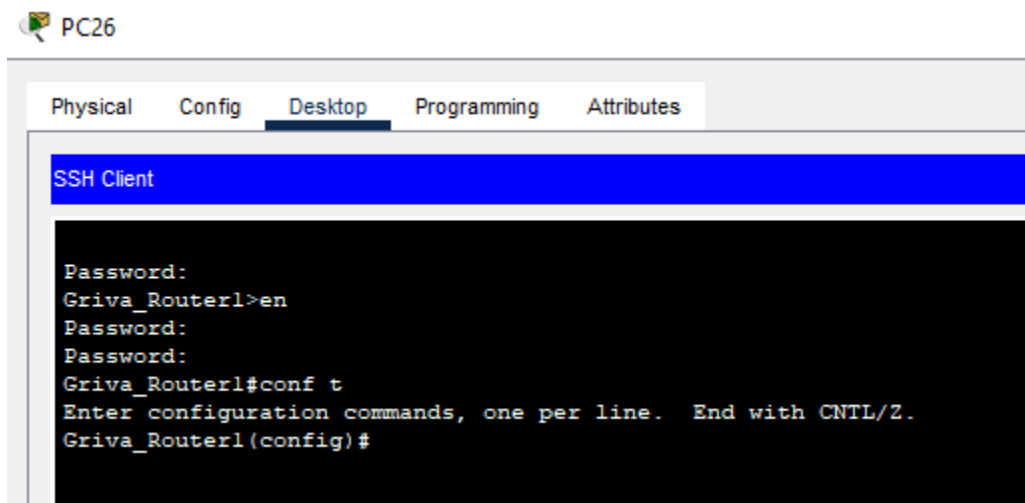


Рисунок 3.8 – Працездатність протоколу віддаленого доступу SSH

3.3 Налаштування безпеки мережевого обладнання

3.3.1 Налаштування мереж VLAN

Технології VLAN дають змогу побудувати мережу на логічному рівні, та не бути залежним від фізичного рівня. При цьому, технологія покращує безпеку мережі та надає централізоване управління.

В пункті 3.2.4 розробили списки доступу для мереж VLAN.

Таблиця 3.4 – Структура віртуальних локальних мереж

Номер	Ім'я	Порт
14	Part-1	Sw2-3 - f0/4-f0/8
24	Part-2	Sw2-3 - f0/10-f0/14
34	Part-3	Sw2-3 - f0/15-f0/20

Налаштуємо мережі VLAN на комутаторах та маршрутизаторі:

Hryva _Switch2(config)#vlan 14 // створюємо *vlan14*

Hryva _Switch2 (config-vlan)#name Part-1 // задаємо ім'я *Part-1*

Hryva _Switch2 (config-vlan)# vlan 24 // створюємо *vlan24*

Hryva _Switch2 (config-vlan)#name Part-2 // задаємо ім'я *Part-2*

Hryva _Switch2 (config-vlan)#vlan 34 // створюємо *vlan34*

Hryva _Switch2 (config-vlan)#name Part-3 // задаємо ім'я *Part-3*

Hryva _Switch2 (config)#interface range g0/1-2 // обираємо інтерфейси

Hryva _Switch2 (config-if)#switchport trunk allowed vlan 14,24,34 // дозволяємо проходження трафіку тільки для VLAN 14,24,34

Hryva _Switch2 (config-if)#switchport mode trunk // вказуємо режим роботи транк

Hryva _Switch2 (config)#interface range f0/4-8 // обираємо інтерфейси

Hryva _Switch2 (config-if)#switchport mode access // встановлюємо режим доступу *access*

Hryva _Switch2 (config-if)# switchport access vlan 14 // призначення VLAN 14 порту комутатора

Hryva _Switch2 (config)#interface range f0/10-14

Hryva _Switch2 (config-if)#switchport mode access

Hryva _Switch2 (config-if)# switchport access vlan 24 // призначення VLAN 24 порту комутатора

Hryva _Switch2 (config)#interface range f0/15-20

Hryva _Switch2 (config-if)#switchport mode access

Hryva _Switch2 (config-if)# switchport access vlan 34// призначення VLAN 34 порту комутатора

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/9 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1
14 part1	active	Fa0/4, Fa0/5, Fa0/6, Fa0/7 Fa0/8
24 part2	active	Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14
34 part3	active	Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20

Рисунок 3.10 – Список віртуальних локальних підмереж

3.3.2 Налаштування маршрутизаторів на підтримку служби AAA

Протокол перевіряє доступ всіх користувачів мережі та при проходженні перевірки надає права доступу.

Налаштуємо маршрутизатори на підтримку протоколу:

Hryva_Router1(config) aaa new-model // включимо роботу протоколу на маршрутизаторі

Hryva_Router1 (config) radius-server host 192.168.8.138 // вказуємо адресу серверу

Hryva_Router1 (config) radius –server key radius123 // вказуємо налаштований ключ на сервері

Hryva_Router1 (config) aaa authentication login default group radius local // задаємо умови авторизації в систему за сервером або за локальним обліковим записом

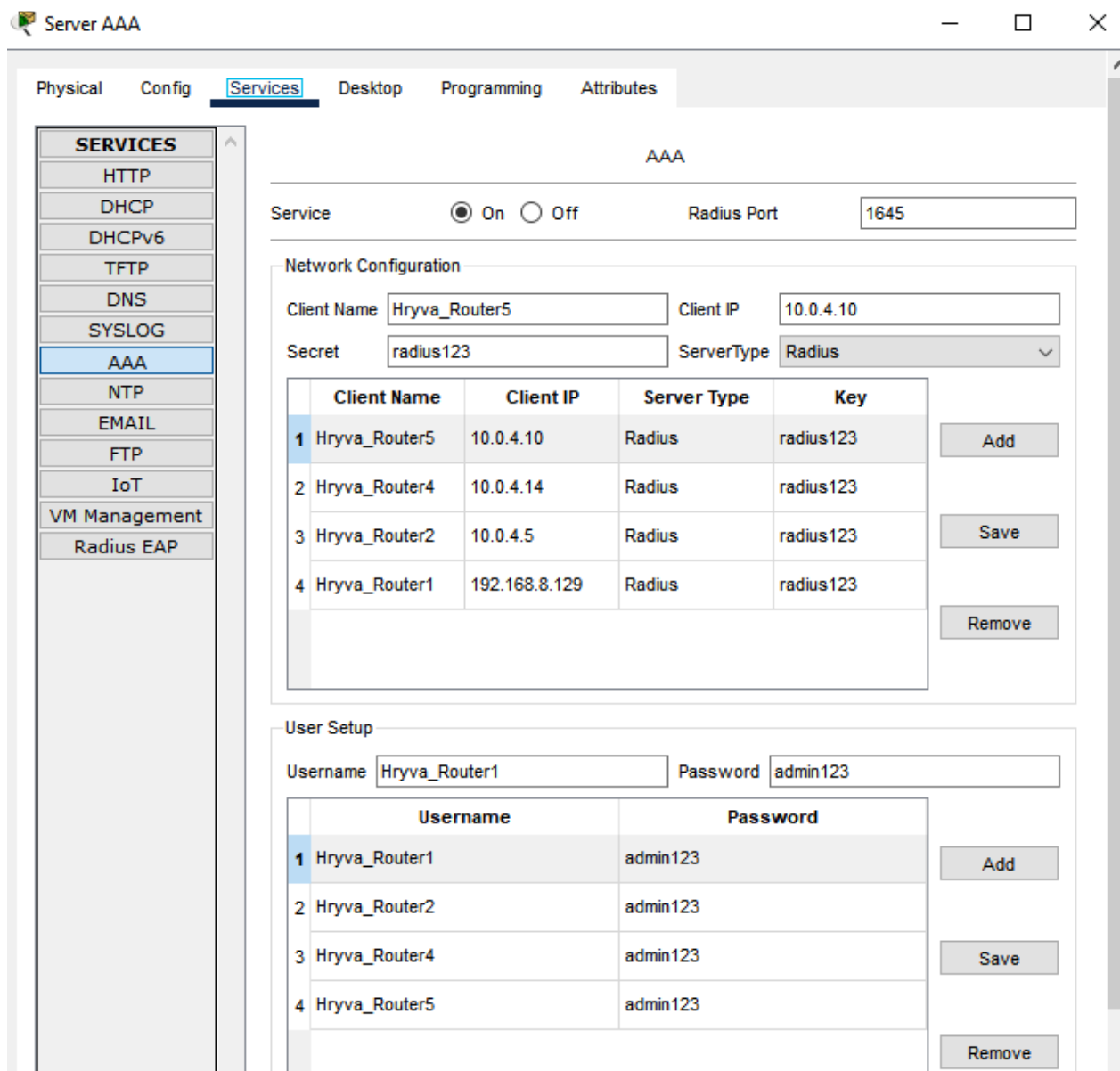


Рисунок 3.11 – Створені облікові записи на сервері

3.3.3 Налаштування та перевірка роботи сервера TFTP

TFTP (Trivial File Transfer Protocol) – це простий протокол передавання файлів, який зазвичай використовується для передавання конфігурацій або файлів завантаження, коли не потрібна аутентифікація.

Увімкнення служби TFTP дає змогу мережевим пристроям передавати завантажувачі на клієнтські пристрої.

Для перевірки роботи сервера збережемо в нього стартову конфігурацію маршрутизатора:

```
Hryva_Router1#copy running-config tftp:
Address or name of remote host []? 192.168.8.132
Destination filename [Hryva_Router1-config]?

Writing running-config...!!
[OK - 1567 bytes]

1567 bytes copied in 0.017 secs (92176 bytes/sec)
Hryva_Router1#
```

Рисунок 3.12 – Процес збереження мережевої конфігурації

На випадок коли щось може статися с мережевим обладнанням, завжди будуть збережені копії конфігурації пристроїв для швидкого відновлення працездатності мережі.

Зайдемо в сервер і перевіримо збережену конфігурацію:

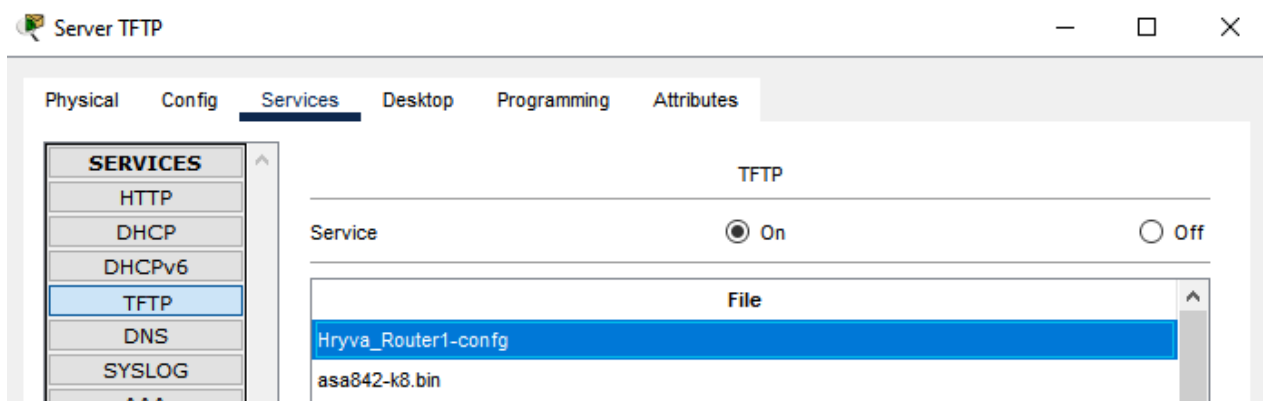


Рисунок 3.13 – Збережена мережева конфігурація в сервер

Як бачимо конфігурація була збережена до серверу.

3.3.4 Налаштування безпеки на портах комутаторів

Налаштуємо безпеку комутаторів в роботі:

```
Hryva_Switch5(config)#interface fa0/18 // обираємо інтерфейс
```

```
Hryva_Switch5 (config)#switchport mode access // обираємо режим роботи  
access
```

```
Hryva_Switch5 (config)#switchport port-security // включаємо функцію, яка дає  
змогу комутатору запам'ятовувати MAC-адреси
```

```
Hryva_Switch5 (config)#switchport port-security maximum 1 // вказуємо число  
MAC-адрес, які будуть збережені 1
```

```
Hryva_Switch5 (config)#switchport port-security mac-address sticky //  
встановлюємо режим sticky для того, щоб комутатор автоматично додавав MAC-  
адреси пристроїв, які відправляють трафік через цей порт, до таблиці MAC-адрес
```

```
Hryva_Switch5 (config)# switchport port-security violation shutdown //  
включаємо функцію за якою комутатор, при виявленні на порту під'єданого  
несанкціонованого пристрою, відключить порт в автоматичному режимі
```

4 РОЗРОБКА КОМПОНЕНТА СИСТЕМИ ПОЖЕЖОГАСІННЯ

4.1 Розробка системи та налаштування

При створенні проекту в кваліфікаційній роботі було впроваджено систему пожежогасіння в відділах управління, за допомогою технології IoT.

Інтернет речей – це технологія, яка дає змогу використовувати розумні елементи мережі та мати до них доступ через будь-які сучасні пристрої.

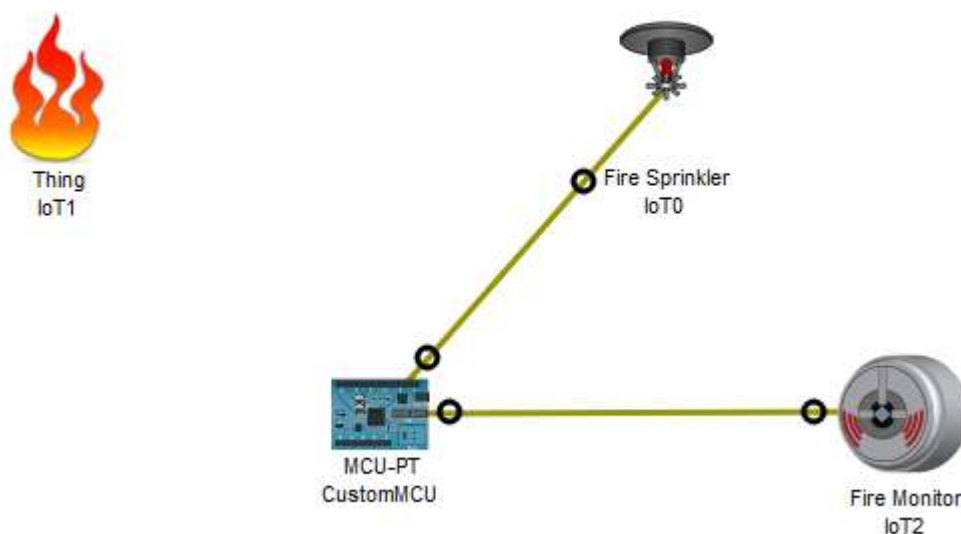


Рисунок 4.1 – Вигляд системи пожежогасіння IoT

Система має вогняний датчик який проводить аналіз пожежі та пожежний сповіщувач який подає воду при пожежі. Всі ці механізми працюють на основі коду та мікроконтролеру MCU.

Мікроконтролер – це прилад, який розрахований на програмування мовами Python чи Java, та відіграє важливу роль у конструювання систем інтернет речей, для побудови великих проектів.

Переглянемо працездатність системи:

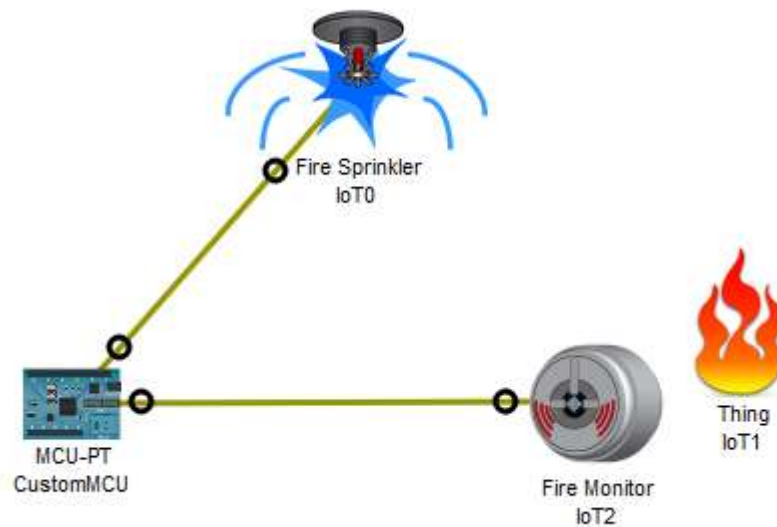


Рисунок 4.2 – Працездатність системи

Код який використовується:

```

from gpio import *
from time import *

def handleSensorData(): // Команда handleSensorData() використовується для
обробки даних з сенсорів
    value = digitalRead(0) // використовується для зчитування цифрового
значення з певного піна
    if value == 0:
        customWrite(1, '0') // використовується для передачі даних на
певний пристрій
    else:
        customWrite(1, '1')

def main():
    add_event_detect(0, handleSensorData) // використовується для виклику
функції, що додає виявлення подій для певного піна
    while True:
        delay(1000)

if __name__ == "__main__":
    main()

```

ВИСНОВКИ

Проектування та написання кваліфікаційної роботи було виконано відповідно до всіх вимогам та стандартів сучасних технологій. Моделювання комп'ютерної мережі інтернет-провайдера було розроблено відповідно до структурної схеми об'єкта впровадження. Розташування всіх підмереж було зображено на карті певного міста.

Розробка специфікації апаратних та програмних засобів комп'ютерних систем відповідають вимогам заказчика. Дивлячись на розрахунок інтенсивності вихідного трафіку мережі, можна сказати що мережа повністю відповідає стандартам інформаційних технологій.

Для всієї мережі було розроблено схему адресації мережі, схему адресації пристроїв та схему фізичної топології мережі. IP-адресація налаштовувалась за протоколом IPv4.

В мережі використано технологію розподілу мережі на підмережі – VLAN. Маршрутизатор мають налаштування на підтримку протоколу AAA. Всі користувачі отримують IP-адресу в мережі за протоколом DHCP. Також, було впроваджено налаштування роботи сервера TFTP.

Дана кваліфікаційна робота може використовуватись в майбутньому як інструкція з налаштування мережі інтернет-провайдера в сучасному світі.

Моделювання мережі виконувалось у додатку Cisco Packet Tracer.

ПЕРЕЛІК ПОСИЛАНЬ

1. Цвіркун Л.І. Комп'ютерні мережі. Методичні рекомендації до виконання курсового проекту студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія / Л.І. Цвіркун, Я.В. Панферова, Л.В. Бешта ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2018. – 28 с
2. Дипломування. Методичні вказівки для бакалаврів галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія / Л.І. Цвіркун, С.М. Ткаченко, Я.В. Панферова ; М-во освіти і науки України, Нац. гірн. ун-т. – Дніпро: НГУ, 2016. – 56 с.
3. Цвіркун Л.І. Інженерна та комп'ютерна графіка. AutoCAD : навч. посіб. / Л.І. Цвіркун, Л.В. Бешта ; під. заг. ред. Л.І. Цвіркуна ; М-во освіти і науки України, НТУ «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2018. – 209 с. – ISBN 978-966-350-663-0.
4. Воробйова Н.І., Корнійчук В.І., Савчук О.В. Надійність комп'ютерних систем. – К.: "Корнійчук", 2002. – 144 с.
5. Цвіркун Л.І. Глобальні комп'ютерні мережі. Програмування мовою PHP: навч. посібник / Л.І. Цвіркун, Р.В. Липовий, під заг. ред. Л.І. Цвіркуна. – Д.: Національний гірничий університет, 2013. – 239 с. – ISBN 978-966-350-417-9.
6. Комутатор Cisco 2960: налаштування підключення, конфігурації, установка [Електронний ресурс] - <https://what.com.ua/komytator-cisco-2960-nalashty/>
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. Базова діагностика пристроїв Cisco: команди для виявлення та виправлення неполадок [Електронний ресурс] - <https://blog.sedicomm.com/2016/11/30/komandy-bazovoj-diagnostiki-ustrojstv-cisco-dlya-vyyavleniya-i-ispravleniya-nepoladok/>
9. Маршрутизатор Cisco 2911: Базове налаштування [Електронний ресурс] – <https://habr.com/ru/articles/87680/>

Додаток А

Схема загальної топології інтернет-провайдера «Воля»

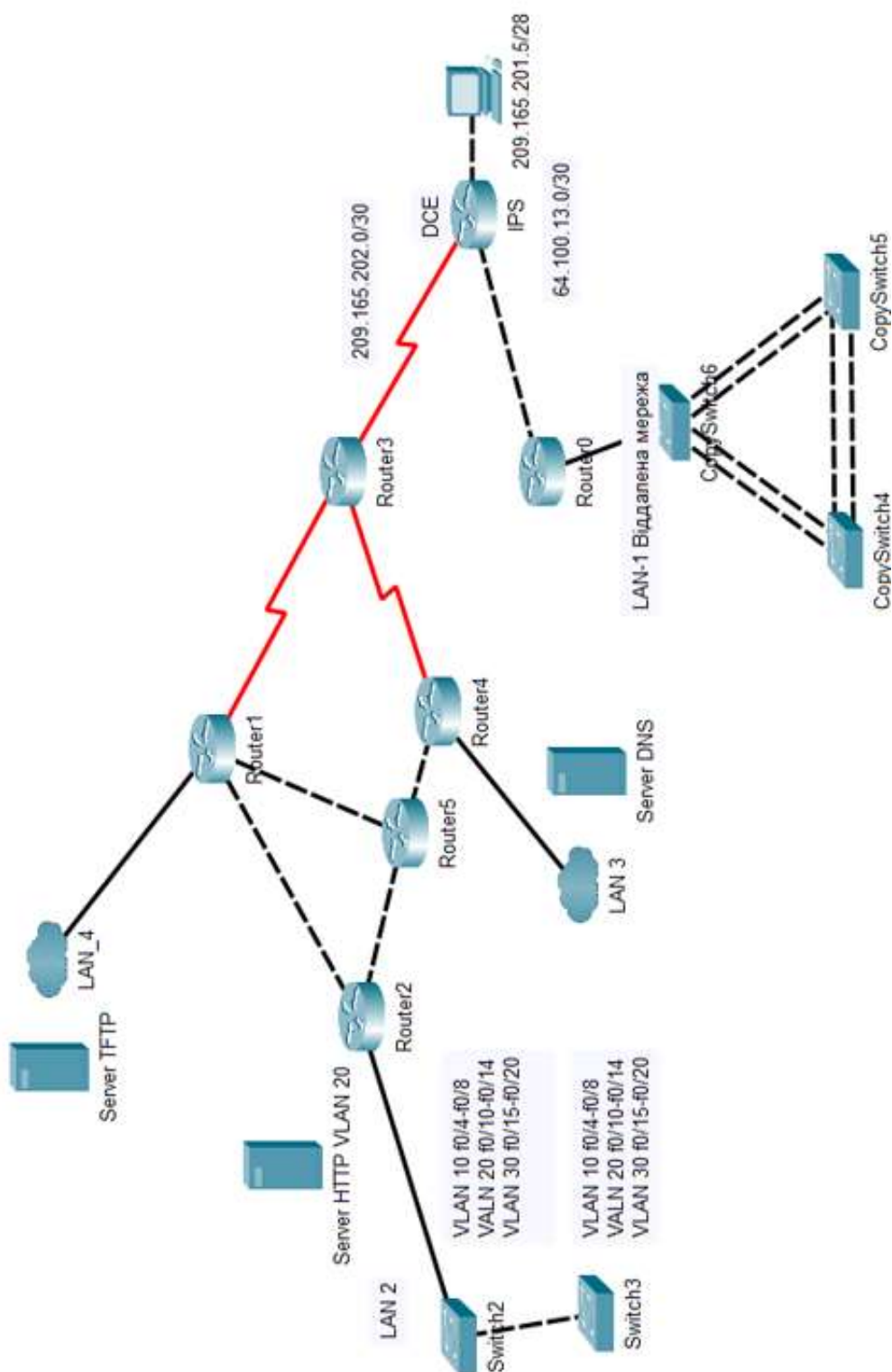


Рисунок А.1 – Схема загальної топології інтернет-провайдера «Воля»

Додаток Б

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
804.02070743.23004-01 12 01

Листів 10

2023

АННОТАЦІЯ

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

ЗМІСТ

	Стор.
1.Налаштування маршрутизатора Hryva_Router1	4
2.Налаштування маршрутизатора Hryva_IPS	6
3.Налаштування комутатора Hryva_CopySwitch6	8

Конфігурація Hryva_Router1:

```
!  
version 15.1  
no service timestamps log datetime msec  
no service timestamps debug datetime msec  
service password-encryption  
!  
hostname Hryva_Router1  
!  
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1  
!  
ip dhcp pool LAN4  
network 192.168.8.128 255.255.255.224  
default-router 192.168.8.129  
dns-server 192.168.8.162  
!  
aaa new-model  
!  
aaa authentication login default group radius local  
!  
no ip cef  
no ipv6 cef  
!  
username 12320zck_Hryva password 7 0822455D0A16  
!  
license udi pid CISCO2911/K9 sn FTX1524Z31V-  
!  
ip domain-name Hryva_Router1  
!  
spanning-tree mode pvst
```

```
!  
interface GigabitEthernet0/0  
  ip address 10.0.4.9 255.255.255.252  
  duplex auto  
  speed auto  
!  
interface GigabitEthernet0/1  
  ip address 10.0.4.6 255.255.255.252  
  duplex auto  
  speed auto  
!  
interface GigabitEthernet0/2  
  ip address 192.168.8.129 255.255.255.224  
  duplex auto  
  speed auto  
!  
interface Serial0/3/0  
  ip address 10.0.4.21 255.255.255.252  
!  
interface Serial0/3/1  
  no ip address  
  clock rate 2000000  
  shutdown  
!  
interface Vlan1  
  no ip address  
  shutdown  
!  
router ospf 1  
  log-adjacency-changes
```

```
network 10.0.4.4 0.0.0.3 area 0
network 10.0.4.8 0.0.0.3 area 0
network 10.0.4.20 0.0.0.3 area 0
network 192.168.8.128 0.0.0.31 area 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.0.4.22
!
ip flow-export version 9
!
banner motd #123-20zck Hryva authorization PASSWORD#
!
radius server 192.168.8.138
  address ipv4 192.168.8.138 auth-port 1645
!
line con 0
  password 7 0822455D0A16
!
line aux 0
!
line vty 0 4
  transport input ssh
!
end
```

Налаштування маршрутизатора Hryva_IPS:

```
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
```



```
no service password-encryption
!
hostname IPS
!
no ip cef
no ipv6 cef
!
license udi pid CISCO2911/K9 sn FTX1524QEB0-
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
ip address 64.100.13.1 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 209.165.201.1 255.255.255.240
duplex auto
speed auto
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/3/0
ip address 209.165.202.1 255.255.255.252
clock rate 2000000
```

```
!  
interface Serial0/3/1  
  no ip address  
  clock rate 2000000  
  shutdown  
!  
interface Vlan1  
  no ip address  
  shutdown  
!  
ip classless  
ip route 0.0.0.0 0.0.0.0 209.165.202.2  
ip route 192.168.8.0 255.255.255.192 64.100.13.2  
!  
ip flow-export version 9  
!  
line con 0  
!  
line aux 0  
!  
line vty 0 4  
  login  
!  
end
```

Налаштування комутатора Hryva_CopySwitch6:

```
!  
version 15.0  
no service timestamps log datetime msec  
no service timestamps debug datetime msec
```

```
no service password-encryption
!
hostname Hryva_CopySwitch6
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface Port-channel1
  switchport mode trunk
!
interface Port-channel2
  switchport mode trunk
!
interface FastEthernet0/1
  switchport mode trunk
  channel-group 1 mode active
!
interface FastEthernet0/2
  switchport mode trunk
  channel-group 1 mode active
!
interface FastEthernet0/3
  switchport mode trunk
  channel-group 2 mode passive
!
interface FastEthernet0/4
  switchport mode trunk
  channel-group 2 mode passive
!
!
```

```
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address dhcp
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
end
```