

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 Маленкової Марії Костянтинівни  
(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 "КНП "Центральна лікарня" Криничанської селищної ради з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі»  
(назва за наказом ректора)

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	доц. Шедловський І.А.			
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 Маленкової М.К. 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 "КНП "Центральна лікарня" Криничанської селищної ради з детальним опрацюванням побудови, 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 \_\_\_\_\_  
(підпис керівника)

доц. Шедловський І.А.  
(прізвище, ініціали)

Дата видачі 25.01.2023

Дата подання до екзаменаційної комісії 12.07.2023

Прийнято до виконання \_\_\_\_\_  
(підпис студента)

Маленкова М.К.  
(прізвище, ініціали)

## РЕФЕРАТ

Пояснювальна записка: 64 с., 40 рис., 6 табл., 2 дод., 12 джерел.

CDP, VTP, РЕЄСТРАЦІЙНИЙ ПІДРОЗДІЛ, ПІДМЕРЕЖА, VLAN, AAA

Об'єкт: комп'ютерна система "КНП "Центральна лікарня" Криничанської селищної ради з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі.

Мета: побудова та моделювання комп'ютерної інфраструктури підприємства з налаштуванням пристроїв та безпеки мережі.

У вступі кваліфікаційної роботи обґрунтована актуальність мети роботи та конкретизовані завдання, які необхідно вирішити.

Комп'ютерна інфраструктура підприємства розрахована на розподілення мережі на підмережі для реєстрації хворих, для внесення інформації щодо хвороб та обслуговування людей. Вона розташована в Україні, м.Кринички яке знаходиться біля м.Дніпро.

Моделювання мережі виконується згідно за завданням кваліфікаційної роботи та за планом і вимогами замовника.

Мережа має великий запас спроможності мережевих пристроїв та їх налаштувань, для майбутньої модернізації або масштабованості.

В даній роботі був створений повний перелік графічної частини мережі та її налаштувань. З мережевого обладнання використовується компанія Cisco.

Налаштування мережі відбувається за сучасними протоколами стеку TCP/IP.

Відображення комп'ютерної мережі здійснюється за допомогою додатку Cisco Packet Tracer.

## ЗМІСТ

Перелік скорочень, умовних позначок, одиниць і термінів	7
Вступ	8
1 Стан питання і постановка завдання	10
1.1 Стисла характеристика умов сфери проектування	10
1.2 Опис та оцінка діяльності «Криничанської центральної районної лікарні»	11
1.3 Детальний аналіз організації управління лікарні	12
1.4 Планова схема розташування лікарні	13
1.5 Принципи компонування системи лікарні	14
1.6 Завдання і мета роботи	15
1.7 Визначення можливих напрямків рішення поставлених завдань	15
2 Розробка апаратної частини комп'ютерної системи	17
2.1 Технічні вимоги до системи	17
2.1.1 Вимоги до системи в цілому	17
2.1.1.1 Вимоги до структури і функціонування системи	17
2.1.1.1.1 Перелік підсистем, їхнє призначення й основні характеристики, вимоги до числа рівнів ієрархії та ступені централізації мережі	17
2.1.1.1.2 Вимоги до способів і засобів зв'язку для обміну інформації між підмережами	18
2.1.1.1.3 Вимоги до характеристик взаємозв'язків створюваної мережі із суміжними мережами	18
2.1.1.1.4 Вимоги до режимів функціонування мережі	19
2.1.1.1.5 Вимоги до діагностування мережі	19
2.1.1.1.6 Перспективи розвитку та модернізації мережі	20
2.1.1.2 Вимоги до показників призначення	20
2.1.1.3 Вимоги до експлуатації	20
2.1.1.3.1 Умови і регламент експлуатації, що повинні забезпечувати використання технічних засобів мережі	20
2.1.1.3.2 Вимоги до параметрів мереж енергопостачання	20

2.1.1.3.3	Вимоги до кількості, кваліфікації обслуговуючого персоналу і режимам його роботи	21
2.1.1.3.4	Вимоги до складу, розміщенню й умовам збереження комплекту запасних віrobів і приладів	21
2.1.1.3.5	Вимоги до регламенту обслуговування мережі	21
2.1.1.4	Вимоги до патентної чистоти	22
2.1.1.5	Додаткові вимоги	22
2.1.1.5.1	Вимоги до активного обладнання	22
2.1.1.5.2	Вимоги до кабель каналів, інформаційним та електричним розеткам	22
2.1.1.5.3	Вимоги до комунікаційного обладнання і його розташування	22
2.1.1.5.4	Вимоги до однорідності	23
2.1.2	Вимоги до задач, які виконуються у комп'ютерній системи	23
2.1.2.1	Вимоги до кожної підмережі та переліку їх функцій	23
2.1.2.2	Часовий регламент і вимоги до якості реалізації кожної функції	25
2.1.3	Вимоги до видів забезпечення комп'ютерної системи	26
2.1.3.1	Вимоги до математичного забезпечення	26
2.1.3.2	Вимоги до інформаційного забезпечення	26
2.1.3.3	Вимоги до лінгвістичного забезпечення	27
2.1.3.4	Вимоги до технічного забезпечення	27
2.1.3.5	Вимоги до організаційного забезпечення	27
2.1.3.6	Вимоги до методичного забезпечення	28
2.2	Розробка апаратної частини системи лікарні	28
2.2.1	Розробка та моделювання структурної схеми комплексу технічних засобів комп'ютерної системи відповідно до планової схеми розташування	28
2.2.2	Розробка специфікації фізичних параметрів комп'ютерної мережі	29
2.2.3	Розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі підприємства	33
3	Розробка мережевої інфраструктури підприємства	35
3.1	Розробка логічної схеми підключення компонентів комп'ютерної мережі	35

3.2	Конфігурація параметрів мережевого обладнання корпоративної мережі	38
3.3	Конфігурація маршрутизаторів для забезпечення доступу до мережі	
	Інтернет	41
3.3.1	Базове конфігурування пристроїв мережі	41
3.3.2	Налаштування маршрутних протоколів у корпоративній мережі	42
3.3.3	Параметризація технології NAT	44
3.3.4	Конфігурація автоматичного налаштування IP-адреси	45
3.4	Налаштування технологій віртуальних комутаційних груп	45
3.4.1	Налаштування технології на маршрутизаторі	45
3.4.2	Налаштування технології на комутаторах	46
3.4.3	Параметризація ACL для керування мережевим трафіком	47
3.4.4	Налаштування протоколу синхронізації VTP	48
3.5	Налаштування безпеки даних в комп'ютерній системі	49
3.5.1	Налаштування політик безпеки AAA	49
3.5.2	Налаштування резервного зберігання конфігурацій	50
3.5.3	Налаштування протоколу CDP та безпеки комутаторів	50
3.6	Перевірка сполучення та комунікації мережевих компонентів	52
4	Розробка компонента системи з організації підключення пристроїв мережі	57
4.1	Розробка організаційних компонентів	57
4.2	Результат з організації підключення	61
	Висновки	65
	Перелік посилань	66
	Додаток А. Загальна схема комп'ютерної системи "КНП "Центральна лікарня" Криничанської селищної ради	67
	Додаток Б. Текст програми налаштування мережі комп'ютерної системи	68

## **ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАК, ОДИНИЦЬ І ТЕРМІНІВ**

VLAN – віртуальні комутаційні групи;

DHCP – протокол конфігурації автоматичного налаштування IP-адреси;

OSPF – маршрутний протокол у корпоративній мережі;

ACL – керування мережевим трафіком

AAA – протокол політик безпеки маршрутизаторів;

HTTP – сервер веб-сайту кваліфікаційної роботи;

TFTP – сервер резервного зберігання конфігурацій;

DNS – сервер, для налаштування адреси веб-сайту;

CDP – протокол взаємодії та обміну інформацією між пристроями;

VTP – протокол комутації VLAN;

ЦУМ – центр управління мережею.

## ВСТУП

Інформаційні технології охопили весь сучасний світ, як у роботі так і в навчанні. Майже кожна компанія або виробництво має мережеву інфраструктуру, для забезпечення більшої продуктивності системи. У кваліфікаційній роботі було розроблено мережеву інфраструктуру лікарні. Лікарня має великий потік хворих людей, але мережеві технології дають змогу оперативніше вирішувати організаційні питання щодо прийому хворих до лікаря, призначення лікування та ведення обліку хворого.

У кваліфікаційній роботі були вирішені всі питання щодо організації мережевої інфраструктури та впровадження обчислювальних технологій майже в кожен кабінет лікарні. Кожен лікар має доступ до загальних інформаційних ресурсів лікарні, таких як історії хвороб, лікарняні довідки, облік хворих тощо. Усе це тепер доступно кожному лікарю у своєму кабінеті, що спрощує і прискорює прийом людей, знижує чергу і ймовірність зараження інших.

Мережа побудована за сучасними технологіями та стандартами. Вона має підтримку сучасних протоколів TCP/IP. В мережі використовуються віртуальні локальні мережі, агрегування каналів, мережева трансляція адрес, списки доступу, динамічна та статична маршрутизація, протоколи безпеки та технології локальних та глобальних мереж.

В ході роботи було розроблено апаратну та програмну складову мережевої інфраструктури.

Виконання кваліфікаційної роботи дає можливість закріпити всі навички, які було придбано на шляху навчання. Проект великого обсягу дозволяє відчутти та запам'ятати всі моменти створення та налаштування мережі. Кожний крок виконання кваліфікаційної роботи підвищує та укріплює знання на практиці.

Моделювання корпоративної мережі виконано в додатку Cisco Packet Tracer.

Кваліфікаційна робота може використовуватися як повний перелік всіх налаштувань мережі для створення або модернізації мереж.



## 1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

### 1.1 Стисла характеристика умов сфери проектування

В якості сфери проектування було використано – медичну сферу діяльності.

Головною задачею медичної сфери є лікування хворих людей, тому комп'ютерна мережа буде відігравати важливу роль для підвищення швидкості лікування та обслуговування хворих.

Для побудови комп'ютерної інфраструктури лікарні використовуються всі сучасні технології локальних та глобальних комп'ютерних мереж.

Для організації локальної мережі кожен кінцевий пристрій повинен мати мережевий адаптер або мережеву картку, яка має бути інтегрована в материнську плату.

Важливою характеристикою локальних комп'ютерних мереж є швидкість передачі даних по мережі, яка залежить від кількох факторів:

- спроможність мережевих адаптерів;
- продуктивність мережевих пристроїв;
- якість кабелів;
- принцип побудови локальної мережі.

Глобальна мережа – це взаємодія локальних підмереж лікарні між собою на незалежній відстані.

Головним принципом побудови мережевої інфраструктури лікарні є забезпечення безпеки діяльності та якісне обслуговування мережевих пристроїв мережі.

Безпека мережі виконується шляхом впровадження стеку протоколів безпеки TCP/IP та певних налаштувань мережевих пристроїв.

Важливим аспектом мережевого проекту є топологія мережі. Від неї залежить рівень безпеки та доступність вузлів між собою.

Після налаштування топології, мережа лікарні повинна мати високу швидкість передачі даних.

## 1.2 Опис та оцінка діяльності «Криничанської центральної районної лікарні»

Комунальний заклад «Криничанська центральна районна лікарня» Дніпровської обласної ради – заклад, перевірений часом. У лікарні працює 251 співробітник, з них 46 лікарів та 95 осіб середнього медичного персоналу. Медична допомога населенню надається за 22 лікарськими спеціальностями. У лікарні розміщено 120 ліжок, що становить 34,1 ліжка на 100 тисяч населення.



Рисунок 1.1 – Криничанська центральна районна лікарня

У консультативній поліклініці ведеться прийом за 19 лікарськими спеціальностями. В середньому за рік лікарі поліклініки приймають більше 80 тисяч пацієнтів. Із них з приводу захворювань – 52 тисячі, з приводу профілактичних медичних оглядів – 28 тисяч. Щорічно план амбулаторно поліклінічних відвідувань виконується на 140-145%. Одним з перших серед сільських районів Дніпропетровської області в лікарні впроваджено телемедичне консультування хворих за результатами їх досліджень через мережу Інтернет у лікарів третинного рівня медичного обслуговування.

Через кабінет телемедицини проводиться попередній запис хворих на консультацію, обстеження, корекцію лікування, госпіталізацію, отримання висновків для МСЕК до лікарів-консультантів обласної лікарні ім. Мечнікова.

Все вищевказане скорочує терміни консультування хворих сільського населення Криничанського району, прискорює діагностування та призначення

лікування хвороб, пацієнти отримують висококваліфіковану медичну допомогу на третинному рівні медобслуговування у зручний для них час.

З 2012 року лікарня плідно співпрацює з фахівцями обласної лікарні ім. Мечнікова в частині наближення висококваліфікованої медичної допомоги стаціонарним та амбулаторним хворим із відділених сіл Криничанського району.

### 1.3 Детальний аналіз організації управління лікарні

Аналіз організації управління лікарні включає детальне вивчення структури, процесів та систем, які забезпечують ефективне функціонування лікарні. Основною метою аналізу є ідентифікація сильних та слабких сторін управління, а також виявлення можливостей для їх поліпшення.

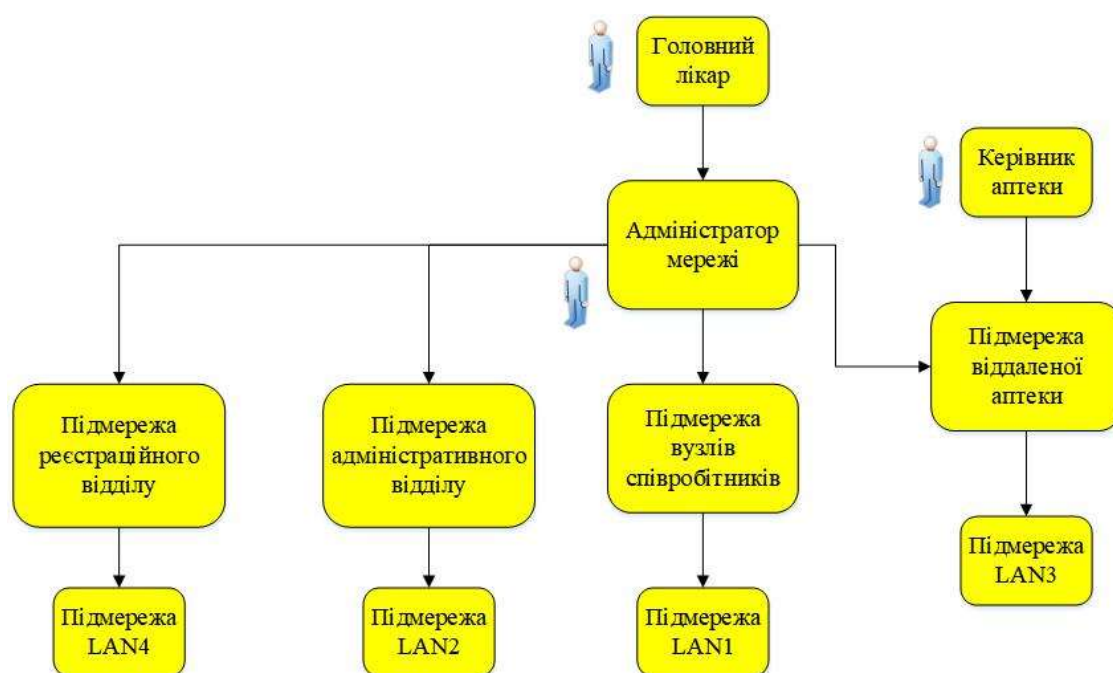


Рисунок 1.2 – Організація управління мережею лікарні

Головною ідеєю структури управління є процес управління кожної ланки мережі та між кожними користувачами цих підмереж. Також, процес управління передбачає повну відповідальність за будь-які наказові дії.

Структура мережі лікарні будується на головному лікарі та керівнику аптекою. Управління мережею відбувається в центрі управління мережею.

Центр управління мережею (ЦУМ) – це централізоване середовище, яке вирішує поточні завдання функціонування мережі. В якості ЦУМ лікарні є адміністративний підрозділ.

Адміністративний підрозділ займається моніторингом мережі, забезпечує працездатність кінцевих пристроїв таких як – маршрутизатори, комутатори, комп'ютери, принтери, сервери і т.д. Також підрозділ відповідає за якісне програмне забезпечення, в якому працюють лікарі.

Реєстраційний відділ – займається реєстрацією хворих на запис до лікаря, створює медичні картки, в яких відображається повна історія хвороб людини. Після створення та запису даних, мають змогу роздрукувати картку для видачі хворому.

Відділ вузлів співробітників – в цьому відділі вміщуються всі комп'ютери лікарів різних напрямків, в яких вони мають певну інформацію хвороб, а також передану базу людей з реєстраційного відділу.

Підмережа віддаленої аптеки – підмережа, в якій знаходяться комп'ютери для обслуговування клієнтів, розрахунку покупок та для створення обліку всіх препаратів в аптеці.

#### **1.4 Планова схема розташування лікарні**

Підрозділи "Криничанської центральної районної лікарні" Дніпровської обласної ради знаходяться в місті Кринички, Україна. Розташовані вони в трьох різних будівлях, які забезпечують функціонування різних медичних служб та підрозділів.

Кожна з цих будівель обладнана для виконання специфічних медичних процедур та надання необхідної медичної допомоги пацієнтам. Вони розташовані на вулиці Героїв Чорнобиля, 22.

Ці підрозділи мають взаємний доступ один до одного, що забезпечує зручну та швидку комунікацію між медичним персоналом та обмін необхідною інформацією. Це важливо для забезпечення координації дій та ефективного функціонування лікарні в цілому.

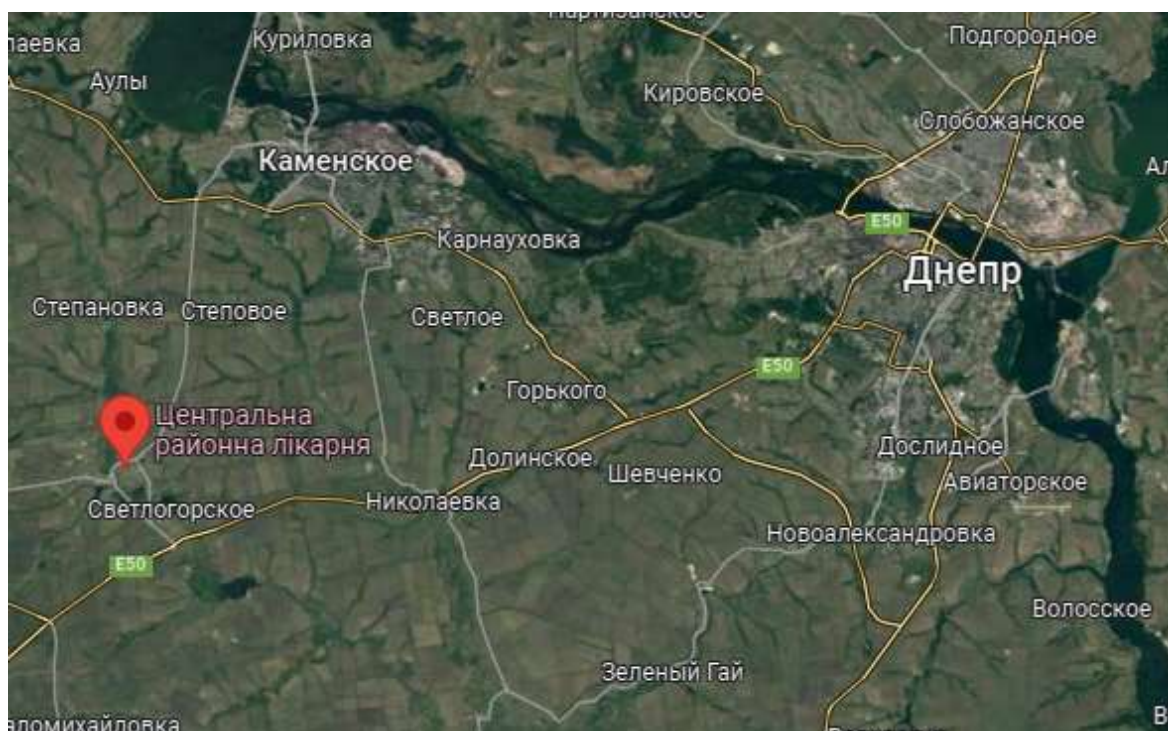


Рисунок 1.3 – Схема розташування лікарні

### 1.5 Принципи компонування системи лікарні

Комп'ютерна мережа – це система контакту між двома або більше комп'ютерами чи комп'ютерними пристроями, яка призначена для передачі інформації між комп'ютерами, спільного доступу до програм і даних та спільного використання обладнання.

Мережа лікарні побудована на принципі централізованого управління даних що свідчить про те, що дані обробляються на центральному вузлі мережі.

Використання методу центрального управління надає наступні переваги:

- централізована система надає велику спроможність швидкості обробки інформації;
- сприяє зручності моніторингу, керуванню або виправленню проблем з однієї точки управління, що не передбачає фізичне втручання;
- адміністратор мережі з легкістю може встановлювати або видаляти правила доступу на керування або зчитування інформації в мережі;
- масштабованість мережі в такому випадку виконується без додаткових зусиль, а тільки додаванням користувача в єдиній точці управління

## **1.6 Завдання і мета роботи**

Завдання кваліфікаційної роботи полягає в створенні мережі та інфраструктури зв'язку, яка забезпечить ефективний обмін інформацією між різними підрозділами та працівниками лікарні.

Головною метою цієї роботи є покращення якості та швидкості комунікації, забезпечення надійності передачі даних та підтримання безпеки і конфіденційності інформації.

Розробка складається з списку завдань, в яких необхідно:

1. Створити вимоги до працездатності мережі;
2. Розробити логічну схему підключення компонентів;
3. Розробити конфігурації мережевого обладнання в тому числі IP-адресацію;
4. Провести базове конфігурування пристроїв;
5. Налаштувати маршрутний протокол;
6. Виконати параметризацію технології NAT;
7. Розробити конфігурації автоматичного налаштування IP-адрес;
8. Налаштувати технології віртуальних комутаційних груп;
9. Налаштувати безпеку даних;
10. Перевірити сполучення та комунікації мережевих компонентів;
11. Розробити компонент системи з організації підключення пристроїв мережі.

## **1.7 Визначення можливих напрямків рішення поставлених завдань**

Для побудови логічної схеми підключення компонентів можна використовувати наступні топології:

- зіркова топологія;
- лінійна топологія;
- кільцева топологія;
- деревоподібна топологія.

Налаштування мережевих компонентів може включати:

- встановлення основних параметрів мережевого обладнання, таких як IP-адреса, маска підмережі, шлюз за замовчуванням, DNS-сервери і т.д.;
- встановлення правил фільтрації трафіку, налаштування віддаленого доступу з обмеженнями;
- конфігурування маршрутів між різними мережами, налаштування протоколів маршрутизації (наприклад, OSPF, BGP) і оптимізація шляхів маршрутизації для ефективного руху даних в мережі;
- конфігурування параметрів бездротової мережі, встановлення безпеки;
- включення і налаштування додаткових мережевих сервісів, таких як DHCP-сервер, DNS-сервер, сервери файрволу, сервери проксі і т.д.;
- встановлення налаштувань моніторингу та журналювання, щоб відстежувати стан мережі;
- налаштування резервного копіювання конфігурацій мережевого обладнання та відновлення після випадку відмови або неправильної конфігурації.

## **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**

"Криничанська центральна районна лікарня" Дніпровської обласної ради повинна бути розділена на чотири частини для більш ефективного та організованого функціонування.

Перша частина мережі повинна бути призначена – реєстраційному відділу.

Реєстраційний відділ повинен бути відповідальним за реєстрацію та обробку інформації пацієнтів

Друга частина мережі повинна бути призначена – адміністративному відділу.

Адміністративний відділ повинен займатися організацією та керуванням різними аспектами діяльності.

Третя частина мережі повинна бути призначена – відділу вузлів співробітників. Вона повинна забезпечуватися пристроями для лікарів.

Та остання частина мережі повинна бути призначена для віддаленої мережі аптеки.

Кожна з цих частин повинна мати визначене значення або обсяг завдань, щоб забезпечити ефективну організацію та функціонування лікарні.

Також, кожна з цих частин повинна підтримувати чітку кількість вузлів в мережі – 49, 30, 38 та 33, відповідно до частин мережі.

Отримані частини лікувальних установ повинні використовуватися для організації мережевої інфраструктури та забезпечення ефективного управління мережею.

Використання окремих частин загальної мережі повинно давати змогу розділити трафік між різними лікувальними приміщеннями.



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

Методи комунікації для обміну інформацією в мережі повинні відповідати нормам мережі:

- пристрої в мережі повинні підтримувати CDP, щоб брати участь в обміні інформацією;
- CDP має бути увімкнений на мережевих пристроях, які повинні обмінюватися інформацією;
- пристрої, які взаємодіють через CDP, повинні знаходитися в одному і тому ж мережевому сегменті;
- CDP повинен надавати інформацію про сусідні пристрої, включно з їхніми моделями та версіями програмного забезпечення;
- CDP повинен бути використаний для моніторингу та управління мережевою інфраструктурою, оскільки надає інформацію про топологію мережі та сусідні пристрої.

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

Мережа повинна мати взаємодію з суміжними підмережами за протоколом VTP, та відповідати вимогам:

- пристрої в мережі повинні підтримувати VTP, щоб використовувати його функціональність;
- VTP має бути увімкнений на комутаторах, які братимуть участь у синхронізації інформації;
- усі комутатори в мережі повинні використовувати одну й ту саму версію протоколу VTP;
- комутатори мають бути налаштовані в одному і тому ж VTP-доміні, щоб обмінюватися інформацією;
- у мережі мають бути призначені відповідні ролі комутаторів у контексті VTP. Один комутатор має бути налаштований у режимі сервера (VTP

server), який керуватиме інформацією, а решта комутаторів - у режимі клієнта (VTP client), щоб отримувати оновлення від сервера;

- необхідно використовувати відповідні паролі для VTP-домену;
- необхідно налаштувати комутатори в режимі прозорого (VTP transparent), щоб запобігти несанкціонованим змінам.

#### **2.1.1.1.4 Вимоги до режимів функціонування мережі**

Управління мережею відбувається в центрі управління мережею.

Центр управління мережею (ЦУМ) – це централізоване середовище, яке вирішує поточні завдання функціонування мережі. В якості ЦУМ лікарні є адміністративний підрозділ.

Адміністративний підрозділ повинен займатися моніторингом мережі, забезпечувати працездатність кінцевих пристроїв таких як – маршрутизатори, комутатори, комп'ютери, принтери, сервери і т.д. Також підрозділ повинен відповідати за якісне програмне забезпечення, в якому працюють лікарі.

Реєстраційний відділ – повинен займатися реєстрацією хворих на запис до лікаря, створювати медичні картки, в яких відображається повна історія хвороб людини. Після створення та запису даних, мають змогу роздрукувати картку для видачі хворому.

Відділ вузлів співробітників – в цьому відділі вміщуються всі комп'ютери лікарів різних напрямків, в яких вони мають певну інформацію хвороб, а також передану базу людей з реєстраційного відділу.

Підмережа віддаленої аптеки – підмережа, в якій знаходяться комп'ютери для обслуговування клієнтів, розрахунку покупок та для створення обліку всіх препаратів в аптеці.

#### **2.1.1.1.5 Вимоги до діагностування мережі**

Діагностика мережі в лікарні повинна бути виконана з використанням декількох простих способів:

- перевірка фізичного підключення;

- перевірка наявності сигналу;
- перевірка IP-адрес;
- використання інструментів перевірки мережі;
- перевірка наявності оновлень.

#### **2.1.1.1.6 Перспективи розвитку та модернізації мережі**

Перспективи розвитку мережі лікарні у майбутньому, визначені, та мають наступні аспекти:

- впровадження бездротових технологій;
- розширення системи віддаленого доступу;
- інтеграція Інтернету речей (IoT).

#### **2.1.1.2 Вимоги до показників призначення**

Мережа повинна підтримувати механізми управління трафіком, що дають змогу пріоритизувати медичний трафік перед іншими видами трафіку. Це гарантує, що медичні дані будуть передаватися з найвищим пріоритетом і мінімальною затримкою.

#### **2.1.1.3 Вимоги до експлуатації**

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

Умови не передбачені та не включаються в загальні вимоги до мережі в лікарні.

##### **2.1.1.3.2 Вимоги до параметрів мереж енергопостачання**

Енергопостачання має відповідати стандартним напругам і частотам для електрообладнання в лікарні – 220-240 В. Генератори або безперебійні джерела живлення не передбачені.

Важливо мати системи фільтрації та згладжування електричних перешкод, щоб запобігти пошкодженню медичного обладнання та забезпечити стабільне електропостачання.

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

В мережі лікарні повинна бути достатня кількість обслуговуючого персоналу, щоб забезпечити безперервність роботи та ефективне функціонування мережі лікарні. У лікарні в наявності повинно бути декілька мережевих адміністраторів.

Обслуговуючий персонал повинен мати досвід роботи з мережевими технологіями.

Персонал лікарні працює позмінно:

- денна зміна: 8:00-16:00;
- вечірня зміна: 16:00-24:00;
- нічна зміна: 24:00-8:00.

#### **2.1.1.3.4 Вимоги до складу, розміщенню й умовам збереження комплекту запасних віrobів і приладів**

Склад мережі не вимагає додаткових заходів обслуговування. Ремонт або заміна комплектуючих проводяться тільки в разі виникнення поломки або несправності.

#### **2.1.1.3.5 Вимоги до регламенту обслуговування мережі**

Регламент обслуговування вимагає тільки оновлення програмного забезпечення пристроїв мережі.

Обслуговування, діагностика, ремонт або заміна несправної деталі проводиться тільки тоді, коли елемент системи виходить з ладу або перестає функціонувати належним чином.

#### **2.1.1.4 Вимоги до патентної чистоти**

Мережа лікарні повинна відповідати вимогам законодавства України у сфері захисту персональних даних, конфіденційності медичної інформації та кібербезпеки. Найважливішими нормативно-правовими актами є Закон України "Про захист персональних даних" та норми, визначені Міністерством охорони здоров'я України.

#### **2.1.1.5 Додаткові вимоги**

##### **2.1.1.5.1 Вимоги до активного обладнання**

До вимог активного обладнання мережі лікарні відноситься мінімальна характеристика швидкості передачі даних, що задовольняє основні потреби медичного закладу.

Швидкість передачі даних повинна бути від 100 Мбіт/с до 1 Гбіт/с, що буде достатньою для більшості мережевих зв'язків в медичному середовищі.

##### **2.1.1.5.2 Вимоги до кабель каналів, інформаційним та електричним розеткам**

Кабель-канали, інформаційні та електричні розетки повинні відповідати наступним стандартам:

- EN 50575;
- ISO/IEC 11801;
- IEC 60364.

##### **2.1.1.5.3 Вимоги до комунікаційного обладнання і його розташування**

Комунікаційне обладнання повинно відповідати вимогам електромагнітної сумісності. Так як в лікарні знаходяться медичні прилади, обладнання повинно відповідати ЕМС-стандартам. Обладнання повинно розташовуватися в окремих приміщеннях лікарні, для того щоб бути впевненим що пристрої не створюють електромагнітних перешкод для роботи медичних приладів.

#### 2.1.1.5.4 Вимоги до однорідності

Власні мережі лікарні використовують технологію VLAN для підтримки сегментації мережі та забезпечення безпеки та ефективності передачі даних, тому для ефективного керування та розширення VLANs в мережі лікарні необхідно використовувати протокол VTP (VLAN Trunking Protocol).

VTP повинен дозволити централізовано керувати інформацією про VLANs, що знаходяться на різних комутаторах у мережі.

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

#### 2.1.2.1 Вимоги до кожної підмережі та переліку їх функцій

Застосування мережевого обладнання можливе тільки після проведення на ньому конкретних налаштувань:

- маркування мережевого обладнання повинно здійснюватися за стандартом: *Студента\_Тип пристрою\_Номер пристрою*, на прикладі кваліфікаційної роботи це виглядає – *Malienkova\_Router\_4*;
- консолі та лінії керування vty повинні забезпечуватися безпекою, шляхом встановлення паролю – *cisco*;
- привілейованого режиму також повинен забезпечуватися безпекою, шляхом встановлення паролю – *class*;
- дані безпеки, а саме паролі, повинні мати вигляд формату шифрування даних;
- для покращення візуального вигляду авторизації повинен бути створений банер MOTD;
- лінії керування vty повинні забезпечуватися додатковою безпекою використання протоколу ssh;
- профіль в системі повинен створюватися за стандартом: *група\_прізвище*, на прикладі кваліфікаційної роботи це виглядає – *123-20zck\_Malienkova* та забезпечуватися безпекою паролю – *admincisco*;
- маркування мережевого обладнання повинно відповідати значенню імені домена;

- для використання формату шифрування даних необхідно створити RSA ключ довжиною 1024 біт;
- значення тактової частоти повинно дорівнювати 128000 та використовуватися на DCE-інтерфейсах маршрутизаторів;
- на початку та після завершення процесу *EXEC* повинні надходити сповіщення, використовуючи персональну базу.

Налаштування маршрутного протокол повинно відбуватися за певними вимогами:

- мережі безпосереднього підключення оголошені, і оновлення маршрутизації на інтерфейси в локальні мережі вимкнені;
- мережі віртуальних комутаційних груп повинні бути оголошені за допомогою протоколу VTP;
- застосування маршрутного протоколу OSPF вимагає зміни спроможності дозволів для розрахунку вартості на портах інтерфейсу Gigabit на значення = 1000;
- для serial інтерфейсів необхідно застосувати значення пропускну спроможності 128 Кб/с, а ціновий показник метрики = 7500;
- отримання функціоналу глобальної мережі необхідно від інтернет-провайдера, для цього на головному маршрутизаторі потрібно встановити маршрут за замовчуванням, та після отримання трафіку необхідно оголосити про нього в локальну мережу засобами маршрутизації;
- так як сумування мереж виконується тільки в маршрутизації для локальних мереж, оголошення маршруту потребує ручного введення та запису у таблицю;
- мережа аптеки може застосовувати статичний маршрут до корпоративної мережі для отримання спільних даних.

Застосування технології безпеки AAA повинно супроводитися налаштуваннями:

- процес перевірки даних до ліній управління VTU на мережевому обладнанні повинен використовувати базу локальних користувачів в корпоративній мережі;

- база локальних користувачів повинна мати другий рівень доступу, в свою чергу перший рівень доступу повинен отримуватися за допомогою протоколу RADIUS;

- протокол RADIUS повинен мати налаштування с секретного кодового слова – radius123;

- База локальних користувачів повинні застосовувати назву маркування мережевого обладнання та пароль *admin123*.

Доступ до мережі Інтернет повинен отримуватися від місцевого Інтернет-провайдера з застосуванням технології NAT. При використанні технології NAT, Інтернет-провайдер повинен надавати користувачам публічну IP-адресу, яка використовується для зв'язку з Інтернетом. Користувачі у свою чергу повинні використовувати приватні IP-адреси в своїх локальних мережах.

В налаштування повинно входити:

- назва адресації networkNAT;
- адресація публічного діапазону 209.165.200.5-209.165.200.30;
- номер публічного пулу має бути – 9.

Після налаштування мережевих технологій, необхідно створити веб-сторінку серверу НТТР для демонстрації інформації щодо кваліфікаційної роботи. Для цього повинна бути налаштована взаємодія між назвою сторінки <http://123.dnipro.ua> та адресою 209.165.202.2.

### **2.1.2.2 Часовий регламент і вимоги до якості реалізації кожної функції**

Кожна підмережа повинна відповідати конкретному налаштуванню та відповідати вимогам:

- адресація корпоративної мережі повинна конфігуруватися на протоколі версії IPv4;



- для маршрутизації між маршрутизаторами необхідно застосовувати адресний простір 10.0.13.0/24;
- при розподіленні адресного простору необхідно врахувати кількість вузлів в кожній підмережі;
- перші отриманні адреси необхідно призначати мережевим інтерфейсам маршрутизаторів;
- другі отриманні адреси необхідно призначати мережевим інтерфейсам комутаторів;
- наступні адреси призначати серверам у довільному порядку, за необхідністю;
- адреси які залишаються у вільному простору необхідно призначати вузлам мережі;
- в корпоративній мережі для налаштування адресації необхідно використовувати протокол DHCP.

## **2.1.3 Вимоги до видів забезпечення комп'ютерної системи**

### **2.1.3.1 Вимоги до математичного забезпечення**

В мережі лікарні необхідно провести математичний розрахунок, який буде служити аналізом можливостей мережевого обладнання. Розрахунок будується на основі інтенсивності вихідного трафіку та пропускнуої здатності для найбільшої частини мережі.

### **2.1.3.2 Вимоги до інформаційного забезпечення**

Інформаційне забезпечення повинно надавати варіанти збереження даних пацієнтів до загальної бази, яка повинна знаходитися у мережі Інтернет та надавати доступ користування всім співробітникам(лікарям, тощо).

За вимогами лікарні повинно бути встановлене наступне програмне забезпечення:

- Healthroad EHR;

- USU;
- BAS Медицина.

### **2.1.3.3 Вимоги до лінгвістичного забезпечення**

В лікарні повинні бути в наявності письмові матеріали, такі як інформаційні брошури та друковані засоби комунікації, перекладені на різні мови. Це буде допомагати пацієнтам зрозуміти свої права, процедури лікування та іншу важливу інформацію.

Також, сімейні лікарі повинні мати системи відеозв'язку з можливістю перекладу або субтитрування мовного контенту, що дозволить персоналу та пацієнтам спілкуватися на різних мовах.

### **2.1.3.4 Вимоги до технічного забезпечення**

Технічні вимоги потребують належного розташування серверних кімнат, комунікаційного обладнання та пунктів розподілу по різних ділянках лікарні, включаючи лікарські кабінети, операційні блоки, інтенсивну терапію та інші кабінети.

Серверні кімнати повинні бути достатнього простору для розміщення комунікаційного обладнання та інфраструктури кабельних систем.

В кожній серверній кімнаті повинен бути наявний вогнегасник.

### **2.1.3.5 Вимоги до організаційного забезпечення**

Лікарня повинна ефективно керувати медичними ресурсами, такими як медикаменти, обладнання, медичні засоби та інші матеріали, щоб забезпечити необхідність відповідного рівня медичної допомоги для пацієнтів. Це включає планування запасів, контроль якості, підтримку обладнання та його технічне обслуговування.

### **2.1.3.6 Вимоги до методичного забезпечення**

Лікарня повинна включати впровадження електронної медичної документації, систем управління пацієнтами, систем телемедицини та інших інструментів для підтримки надання медичних послуг.

Методичне забезпечення повинно включати рекомендації та інструкції з використання інформаційної системи мережі лікарні. Це дозволить лікарям та медичному персоналу ефективно використовувати комп'ютерні системи для ведення медичної документації, обміну інформацією та планування роботи.

## **2.2 Розробка апаратної частини системи лікарні**

### **2.2.1 Розробка та моделювання структурної схеми комплексу технічних засобів комп'ютерної системи відповідно до планової схеми розташування**

Мережа лікарні починається з фізичного розташування у місті. Лікарня є центральним медичним закладом та відповідно і центральним вузлом мережі лікарні, який забезпечує керування та координацію всією мережею. В місті також розташована віддалена мережа аптеки, яка не входить в медичний заклад.

У кожній частині лікарні існує локальна мережа, яка об'єднує різні пристрої та системи всередині цієї лікарні. Ця мережа включає в себе комп'ютери, медичні пристрої, сервери, маршрутизатори, комутатори та принтери. Локальна мережа забезпечує обмін даними та комунікацію між різними системами та пристроями всередині лікарні.

Локальні мережі кожної частини лікарні пов'язані через зовнішню мережу. Вони підключені за лініями зв'язку оптоволоконного кабелю, що забезпечує підключення між різними частинами лікарнями та місцевого інтернет-провайдера. Зовнішня мережа також включає основні мережеві пристрої, такі як маршрутизатори та комутатори, які забезпечують маршрутизацію, фільтрацію та безпеку даних.

Отже, структура мережі лікарні починається з міста, включає в себе локальні мережі в кожній частині лікарні, зовнішню мережу для з'єднання частин мережі та

провайдера, а також різноманітні пристрої, що сприяють наданню якісних медичних послуг.

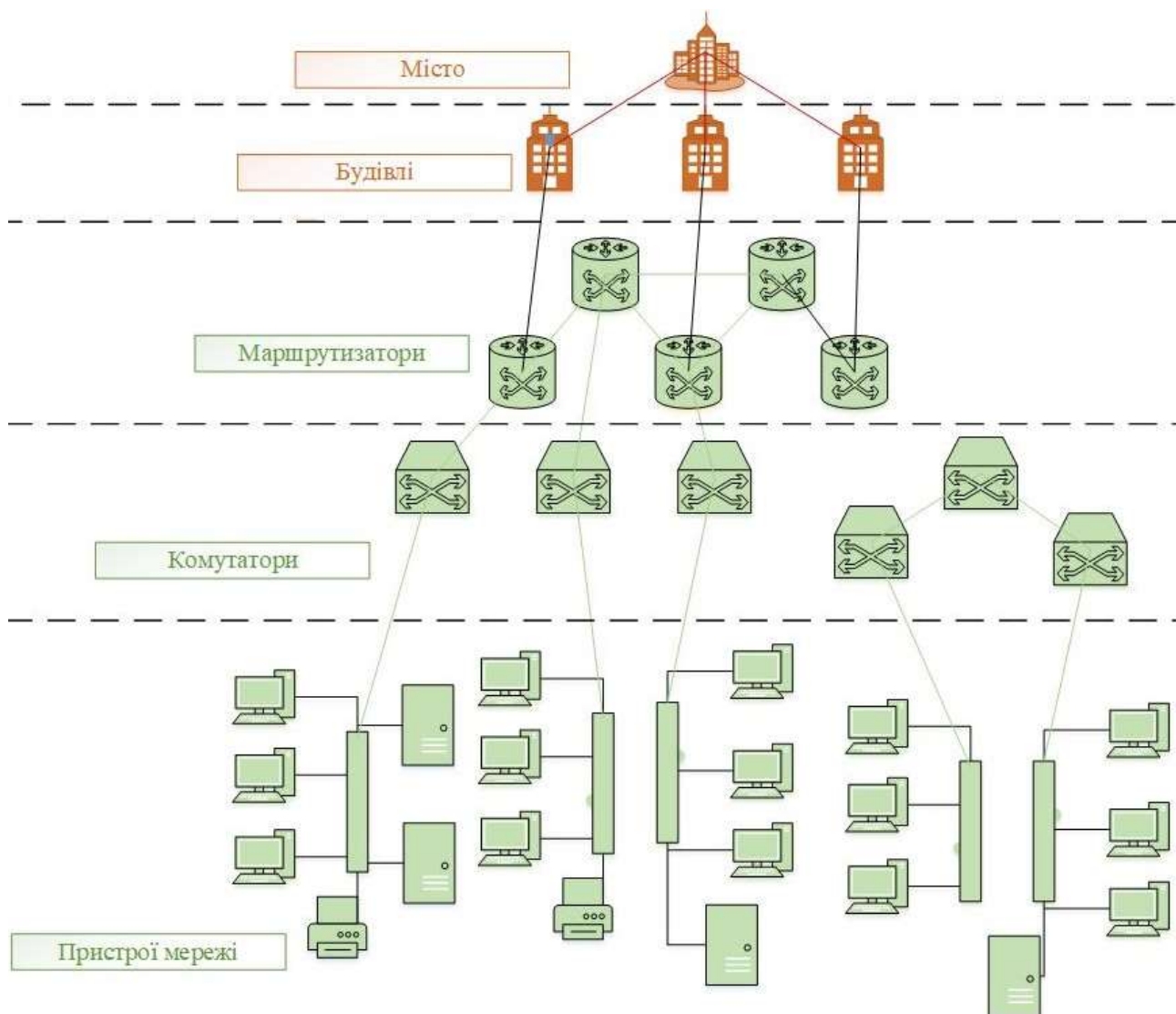


Рисунок 2.1 – Структурна схема засобів побудови мережі лікарні

Розуміння структури мережі допомагає забезпечити ефективну роботу всіх компонентів та забезпечити потрібний обмін даними та комунікацію між ними.

### 2.2.2 Розробка специфікації фізичних параметрів комп'ютерної мережі

Розробка специфікації фізичних параметрів комп'ютерної мережі для потреб медичної установи, зокрема, лікарні, включає вибір обладнання Cisco на основі конкретних вимог та потреб медичного закладу.

Наше завдання - розробити специфікацію фізичних параметрів комп'ютерної мережі для лікарні з використанням обладнання Cisco.

Обладнання Cisco може легко інтегруватися з іншими системами, такими як система електронних медичних записів (EMR) чи система моніторингу пацієнтів. Це дозволяє покращити ефективність роботи, спростити процеси та забезпечити більш точну інформацію про пацієнтів.

Таблиця 2.1 – Специфікація апаратного забезпечення лікарні

Номер пристрою	Ім'я з технічною характеристикою	Тип, марка, позначення	Одиниці виміру	Кількість
1	Комутатори Пропускна здатність комутатора може сягати до 10 ГБ Мають 24 порти для підключення вузлів Використання комутації на основі MAC-адрес	Cisco Catalyst 4500 Series	шт	6
2	Маршрутизатори оперативна пам'ять DDR4 DIMM до 16 ГБ Gigabit Ethernet (10/100/1000 Mbps) Порти WAN (Wide Area Network) з різними варіантами швидкості передачі даних, включаючи 1 Gbps, 2 Gbps, 10 Gbps	Cisco ISR 4000 Series	шт	6

## Кінець таблиці 2.1

3	ПК Intel Core i3-6300 Skylake 3800 MHz Intel / AMD DDR3 8 Гб SSD 480gb PowerColor R7 360 2 Гб AcBel iPower85H 550W	GA-H110M	шт	14
---	---	----------	----	----

Метою цієї розробки є встановлення та фізичне підключення нового обладнання до наявної системи. У межах цього проєкту ми маємо провести необхідні схеми проводки та здійснити встановлення обладнання для забезпечення його коректної роботи.

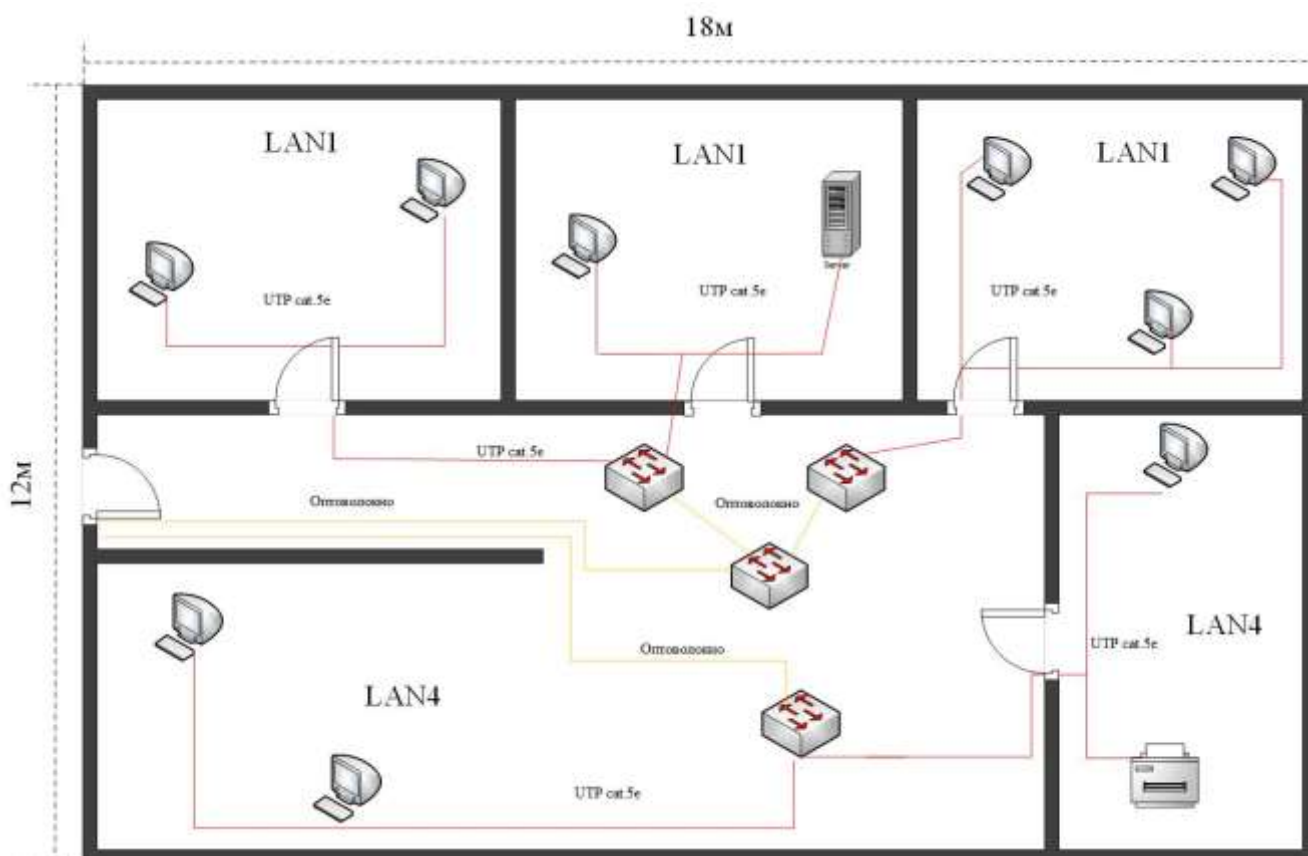


Рисунок 2.2 – Схема проводки кабелів та розташування обладнання в одній будівлі

Схема проводки кабелів і розташування обладнання дає змогу використовувати доступний простір максимально ефективно.

Попереднє планування схеми проводки і розташування обладнання допомагає знизити складність процесу встановлення та обслуговування.

Дотримуючись схеми проводки і розташування обладнання, ми створили структуроване середовище, для полегшення обслуговування і налагодження мережі.

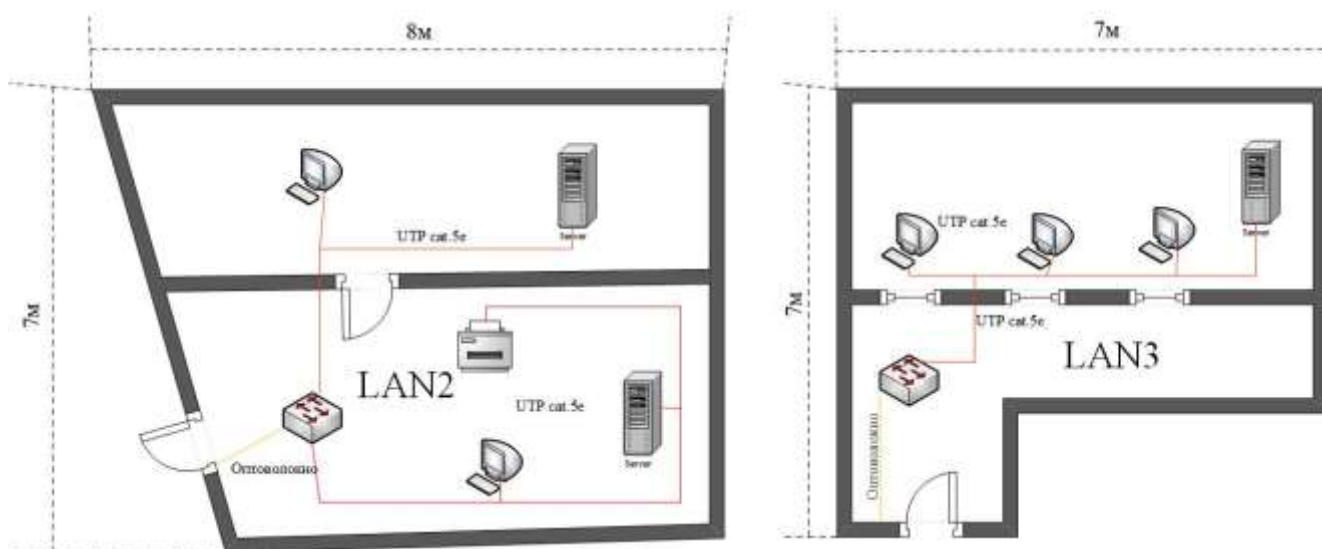


Рисунок 2.3 – Схема проводки кабелів та розташування обладнання в двох будівлях

На кінцеві пристрої лікарів було встановлене програмне забезпечення відповідно до поставлених вимог лікарні.

Healthroad EHR – це додаток, який виконує функції по створенню та обслуговуванню електронних медичних карток.

USU – додаток, який є універсальною системою обліку. Програмне забезпечення допомагає проводити аналітичні обліки за хворобами, медичними препаратами та ін.

BAS Медицина – додаток, що дозволяє створити загальний інформаційний простір лікарні і є ефективним інструментом для побудови сучасної системи управління медичної організації.

### 2.2.3 Розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі підприємства

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

Поставлені вимоги лікарні повинні забезпечувати розрахунок інтенсивності вихідного трафіку для найбільшої частини мереж. Це виконується для розуміння ефективного чи не ефективного мережевого обладнання.

Найбільша частина мережі має 49 вузлів, що становить 37% від загальної кількості співробітників. Середній показник інтенсивності трафіку лікарні складає 161 (кадрів/с). Для розрахунку будемо використовувати середнє значення ваги повідомлення у 650 байт. Додатковою умовою розрахунку є перевірка часу затримки для передачі пакетів, вона не повинна бути більшою за 6 мс.

Для початку розрахуємо пропускну здатність мережі на комутаційному обладнанні. Розрахунок потрібно здійснювати при максимальній завантаженості мережі.

Розрахунок пропускну здатності мережі на комутаційному обладнанні:

$$P_{p.d} = \mu * l * n * 8 = 161 * 650 * 24 * 8 = 20,10 \text{ Мбіт/с}, \quad (2.1)$$

де  $n$  – цифра кількості портів, які застосовуються на комутаторі.

Далі розрахуємо пропускну здатність мережі на маршрутизаційному обладнанні. Отримане значення не повинно перевищувати 1000 Мбіт/с.

Розрахунок:

$$P_{p.p} = \mu * l * N * 8 = 161 * 650 * 49 * 8 = 410,02 \text{ Мбіт/с}, \quad (2.2)$$

де  $N$  – кількість вузлів в найбільшій частині мережі.

Мережа має пропускну здатність в 410,02 Мбіт/с що дозволяє створити запас потужностей мережевого обладнання.

Балансувальник навантаження перенаправляє трафік до маршрутизатора через вихідну лінію з пропускну здатністю 1000 Мбіт /с.

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

Кожний пристрій виробляє 161 пакетів на секунду, тому розрахуємо потенційне значення джерел в мережі:



$$N = 192\,310 / 161 = 1194 \text{ джерел.} \quad (2.4)$$

Запас джерел також надає можливість для резервування можливостей мережі.

Розрахуємо інтенсивність вихідного трафіку від всіх користувачів, якщо кожен вузол генерує 161 кадрів/с:

$$\lambda = N \cdot \mu = 49 * 161 = 7889 \text{ (пакетів/с).} \quad (2.5)$$

Розрахуємо коефіцієнт затримки на рівні маршрутизаторів, для цього показник навантаження в системи ділимо на вихідний канал зв'язку:

$$\rho = \lambda / \mu_{\text{вих}} = 7889 / 192\,310 = 0,041 \quad (2.6)$$

Коефіцієнт навантаженості комутатора рівня розподілу:

$$r = \rho / (1 - \rho) = 0,041 / (1 - 0,041) = 0,043 \quad (2.7)$$

Розрахуємо значення затримки кадру, відповідно до черги M/M/1:

$$T = 1 / ((\mu - \lambda)) = 1 / (192\,310 - 7889) = 5,42 \text{ мкс} \quad (2.8)$$

Розрахуємо середню довжину черги:

$$L_{\text{чер}} = \rho^2 / (1 - \rho) = (0,041)^2 / (1 - 0,041) = 0,0017 \quad (2.9)$$

Розрахуємо середній час існування пакетів у черзі:

$$T_{\text{оч}} = L_{\text{чер}} / \lambda = 0,0017 / 7889 = 2,22 \text{ мкс} \quad (2.10)$$

Затримка не перевищує 6мс що підтверджує якість обладнання;

Розрахуємо пропускну здатність каналу:

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

$$b = \lambda * l = 7889 * 650 * 8 = 41\,022\,800 \text{ Мбіт/с} = 41,02 \text{ Мбіт/с} \quad (2.11)$$

Пропускна здатність каналу дорівнює 41,02 Мбіт/с, це значення повністю задовольняє потреби.

## 3 РОЗРОБКА МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ПІДПРИЄМСТВА

### 3.1 Розробка логічної схеми підключення компонентів комп'ютерної мережі

Мережа LAN1 складається з 6 персональних комп'ютерів і TFTP сервера.

На рівні комутатора мережі LAN1 будуть налаштовані VLAN для розділення мережі на логічні групи. Кожен VLAN матиме свій ідентифікатор і визначений діапазон IP-адрес. Це дозволить обмежити доступ до ресурсів мережі між різними групами користувачів.

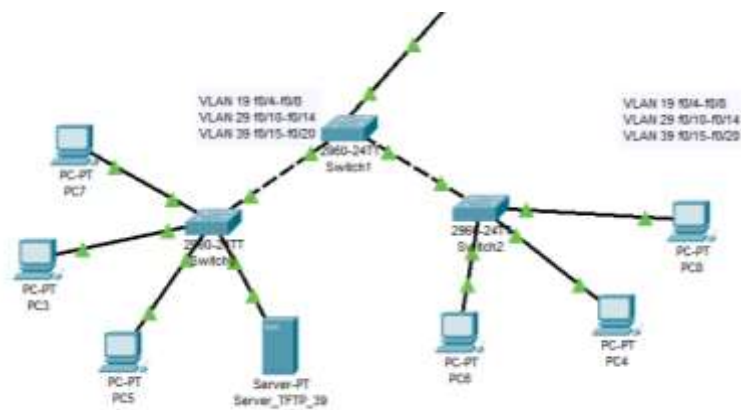


Рисунок 3.1 – Вигляд підмережі LAN1

Частина мережі LAN2 складається з двох персональних комп'ютерів, принтера та серверів DNS і AAA

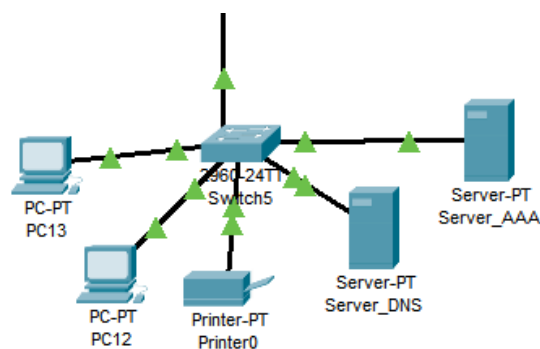


Рисунок 3.2 – Вигляд підмережі LAN2

Підрозділ LAN3 складається з трьох персональних комп'ютерів та сервера HTTP.

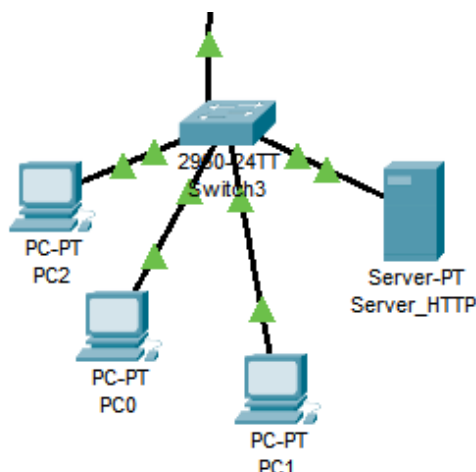


Рисунок 3.3 – Вигляд підмережі LAN3

Підрозділ LAN4 складається з трьох персональних комп'ютерів та принтера.

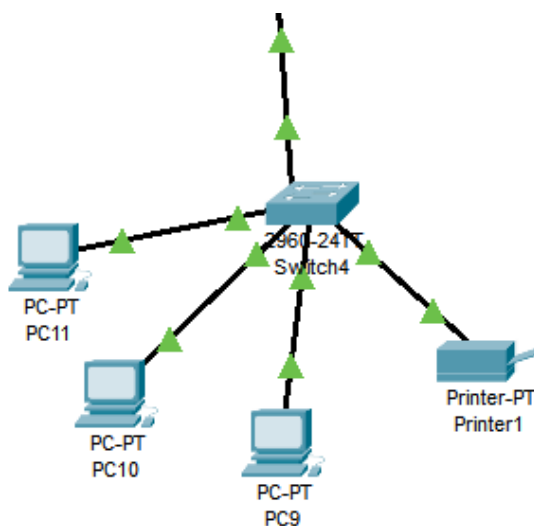


Рисунок 3.4 – Вигляд підмережі LAN4

В рамках організації лікарні була створена логічна схема, яка поєднує всі підмережі в єдину мережу.

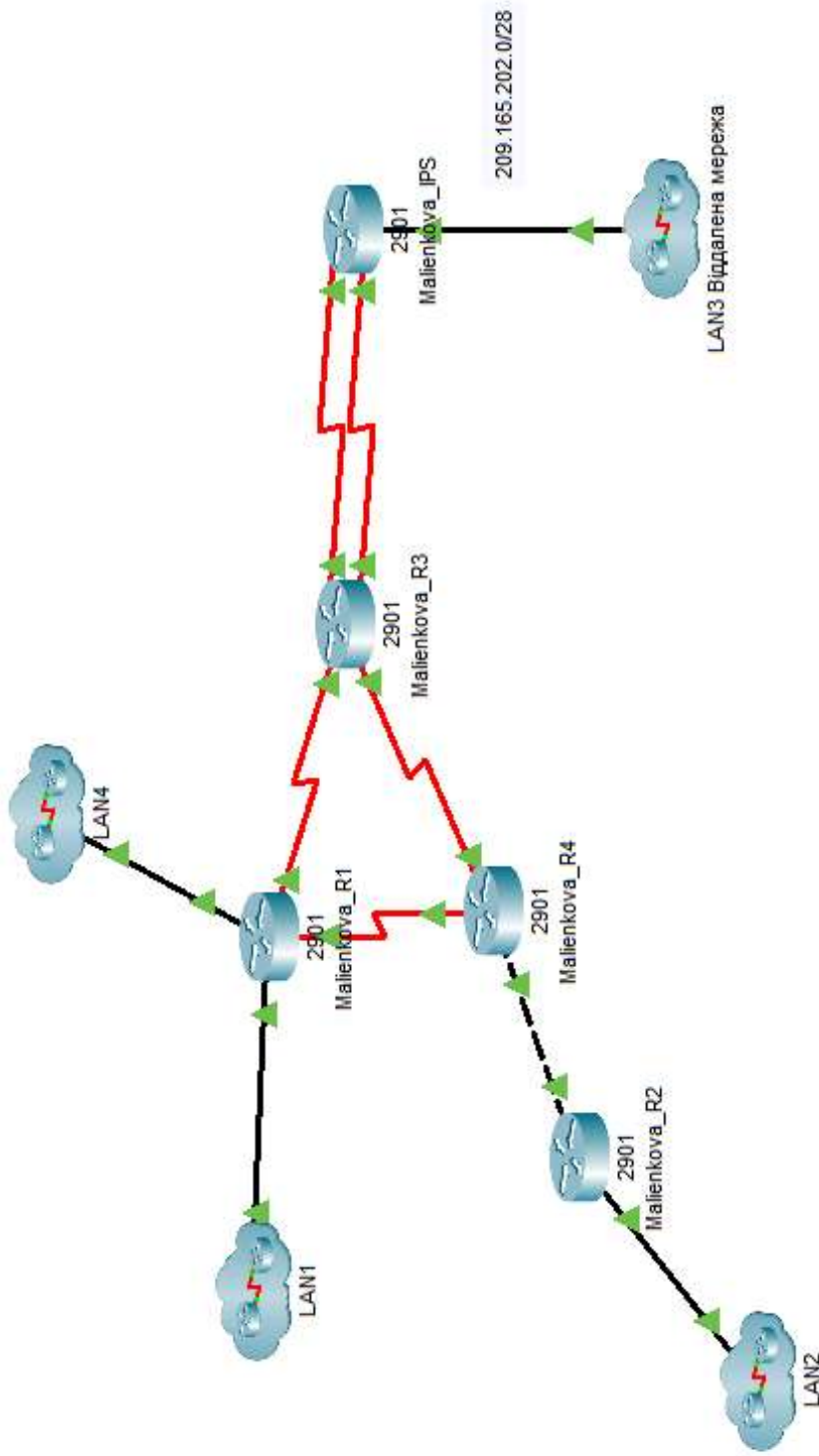


Рисунок 3.5 – Логічна схема підключення компонентів комп'ютерної мережі  
Криничанської лікарні

### 3.2 Конфігурація параметрів мережевого обладнання корпоративної мережі

Мережа лікрані отримала вимоги з IP-адресного діапазону, а саме – 192.168.13.0/24. Це означає, що мережа складається з 256 IP-адрес, починаючи з 192.168.13.1 і закінчуючи 192.168.13.254.

IP-адреса складається з 32 розрядів сумарно або ж з 4 октетів по 8 розрядів та є показником унікальності в мережі. Адреса служить для конкретної відправки або отримки пакетів певному користувачу, якому заздалегіть вона призначена.

Октет який має 8 розрядів може мати значення від 1 до 254, кожний октет при цьому відокремлений крапками.

Маска мережі допомагає ділити її на невеликі частини та використовує двійкові розряди.

Наприклад, значення адреси 192.168.13.20/24 означає, що адреса 192.168.13.20 має перші 3 значення відповідно до маски, вона буде 255.255.255.0, тоді адреса мережі – 192.168.13.0, адреса вузла 0.0.0.20.

IP-адреса може бути представлена в різних форматах, наприклад:

- десяткова: 192.168.13.0;
- двійкова: 11000000.10101000.00001101.0000 | 0000;
- шістнадцяткова: C0.A8.0D.00.

Таблиця 3.1 – Кількість необхідних адрес для мереж

Адреса	LAN1		LAN2		LAN3		LAN4
192.168.13.0/24	49		20		28		33
Адреса	WAN1	WAN2	WAN3	WAN4	WAN5	WAN6	
10.0.13.0/24	2	2	2	2	2	2	

Без налаштування WAN інтерфейсів маршрутизаторів немає сенсу налаштовувати LAN інтерфейси, так як взаємодія між частинами мережі працювати не буде.

Для цього визначимо всі необхідні значення та відобразимо до таблиці.

Таблиця 3.2 – Мережеві значення обладнання

Номер мережі	Вузлів в мережі	Адреса підмережі	Маска мережі	Адреса початку пулу	Адреса кінця пулу
VLAN19	5	192.168.13.16	/28	192.168.13.17	192.168.13.31
VLAN29	5	192.168.13.32	/28	192.168.13.33	192.168.13.46
VLAN39	6	192.168.13.48	/28	192.168.13.49	192.168.13.62
LAN1	49	192.168.13.0	/26	192.168.13.1	192.168.13.62
LAN2	20	192.168.13.128	/26	192.168.13.129	192.168.13.190
LAN3	28	209.165.202.0	/28	209.165.202.1	209.165.202.14
LAN4	33	192.168.13.64	/26	192.168.13.65	192.168.13.126
WAN IPS	2	209.165.202.0	/30	209.165.202.1	209.165.202.1
WAN1	2	10.0.13.0	/30	10.0.13.1	10.0.13.2
WAN2	2	10.0.13.4	/30	10.0.13.5	10.0.13.6
WAN3	2	10.0.13.8	/30	10.0.13.9	10.0.13.10
WAN4	2	10.0.13.12	/30	10.0.13.13	10.0.13.14
WAN5	2	10.0.13.16	/30	10.0.13.17	10.0.13.18
WAN6	2	10.0.13.20	/30	10.0.13.21	10.0.13.22

Після визначення адресації мережі для сетевого обладнання, наступним кроком є розподіл IP-адрес кожному пристрою в цих мережах.

Таблиця 3.3 – Схема адресації пристроїв мережі

Назва пристрою	Порт пристрою	IP-адреса	Маска	Шлюз	№ VLAN	Порт вузла
Інтернет провайдер						
Malienkova_IPS	S0/3/0	10.0.13.10	/30	–	–	S0/3/0
	S0/3/1	10.0.13.14	/30	–	–	S0/3/1
	G0/1	209.165.202.1	/28	–	–	G0/1
Malienkova_Router3	S0/2/0	10.0.13.5	/30	–	–	S0/2/0
	S0/2/1	10.0.13.1	/30	–	–	S0/2/1
	S0/3/0	10.0.13.9	/30	–	–	S0/3/0
	S0/3/1	10.0.13.13	/30	–	–	S0/3/1
Malienkova_Router4	S0/3/0	10.0.13.2	/30	–	–	S0/3/0
	S0/3/1	10.0.13.17	/30	–	–	S0/3/1
	G0/1	10.0.13.21	/30	–	–	G0/1

## Продовження таблиці

Вузли співробітників						
Malienkova_Router1	G0/0	192.168.13.65	/26	–	–	G0/0
	G0/1	192.168.13.1	/28	–	–	G0/1
	S0/3/0	10.0.13.18	/30	–	–	S0/3/0
	S0/3/1	10.0.13.6	/30	–	–	S0/3/1
Malienkova_Switch0	Vlan1	192.168.13.2	/28	192.168.13.65	–	G0/1
Malienkova_Switch1	Vlan1	192.168.13.3	/28	192.168.13.65	–	G0/1
Malienkova_Switch2	Vlan1	192.168.13.4	/28	192.168.13.65	–	Fa0/1
PC19_5-6	NIC	192.168.13.18- 192.168.13.19	/28	192.168.13.17	19	Fa0/4- 0/8
PC29_3-4	NIC	192.168.13.34- 192.168.13.35	/28	192.168.13.33	29	Fa0/10- 0/14
PC39_7-8	NIC	192.168.13.50- 192.168.13.51	/28	192.168.13.49	39	Fa0/15- 0/20
Server TFTP_39	NIC	192.168.13.52	/28	192.168.13.49	39	Fa0/17
Адміністративний відділ						
Malienkova_Router2	G0/0	10.0.13.22	/30	–	–	G0/0
	G0/1	192.168.13.129	/26	–	–	G0/1
Malienkova_Switch4	Vlan1	192.168.13.131	/26	192.168.13.129	–	G0/1
Server DNS	NIC	192.168.13.130	/26	192.168.13.129	–	Fa0/1
Server AAA	NIC	192.168.13.135	/26	192.168.13.129	–	Fa0/2
PC12-13	NIC	192.168.13.130- 192.168.13.133	/26	192.168.13.129	–	Fa0/3- 0/4
Printer0	NIC	192.168.13.134	/26	192.168.13.129	–	Fa0/5
Віддалена аптека						
Malienkova_IPS	S0/3/0	10.0.13.10	/30	–	–	S0/3/0
	S0/3/1	10.0.13.14	/30	–	–	S0/3/1
	G0/1	209.165.202.1	/28	–	–	G0/1
Switch3	Vlan1	209.165.202.3	/28	209.165.202.1	–	G0/1
PC0-2	NIC	209.165.202.4- 209.165.202.6	/28	209.165.202.1	–	Fa0/1-3
Server HTTP	NIC	209.165.202.2	/28	209.165.202.1	–	Fa0/4

Кінець таблиці 3.3

Реєстраційний відділ						
Malienkova_Router1	G0/0	192.168.13.65	/26	–	–	G0/0
	G0/1	192.168.13.1	/28	–	–	G0/1
	S0/3/0	10.0.13.18	/30	–	–	S0/3/0
	S0/3/1	10.0.13.6	/30	–	–	S0/3/1
PC9-11	NIC	192.168.13.67- 192.168.13.69	/26	192.168.13.65	–	Fa0/1- 0/3
Malienkova_Switch4	Vlan1	192.168.13.66	/26	192.168.13.65	–	G0/1
Printer1	NIC	192.168.13.70	/26	192.168.13.65	–	Fa0/4

### 3.3 Конфігурація маршрутизаторів для забезпечення доступу до мережі Інтернет

#### 3.3.1 Базове конфігурування пристроїв мережі

Для належного функціонування мережі і мережевого обладнання потрібно здійснити базове конфігурування пристроїв в мережі.

Для прикладу будемо використовувати маршрутизатор мережі вузлів співробітників.

Спочатку потрібно підключити комп'ютер до консольного порту маршрутизатора за допомогою консольного кабелю та запустити термінальну програму.

```
enable // переходимо в режим доступу
configure terminal // переходимо в режим налаштування
hostname Malienkova_R1 // вказуємо hostname маршрутизатора
Malienkova_R1 (config)#enable secret class // для режиму доступу призначаємо
пароль class
```

```
Malienkova_R1 (config)#line console 0 // консоль керування номер 0
```

```
Malienkova_R1 (config-line)#password cisco // призначаємо пароль cisco
```

```
Malienkova_R1 (config-line)#login // призначаємо запит пароллю на постійній
основі
```



Malienkova\_R1 (config)#banner motd #123-20zck Malienkova authorization  
PASSWORD# // відповідно до пункту 2.1.2.1 призначаємо налаштування для банеру

Malienkova\_R1 (config)#username 12320zck\_Malienkova password cisco  
призначаємо дані користувача в мережі *12320zck\_Malienkova* з паролем *cisco*

Malienkova\_R1 (config)#ip domain-name Malienkova\_R1 // за вимогами  
призначаємо домен

Malienkova\_R1 (config)#service password-encryption // призначаємо  
шифрування паролів

Malienkova\_R1 (config)#crypto key generate rsa // створюємо ключ безпеки

How many bits in the modulus [512]: 1024 // розмір ключа

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

Malienkova\_R1 (config)#line vty 0 4 // консоль керування номер 0, 1, 2, 3, та 4,  
в загальні 5 ліній

Malienkova\_R1 (config-line)#login local // призначаємо запит паролю на  
постійній основі

Malienkova\_R1 (config-line)#transport input ssh // призначаємо доступ до ліній  
через ssh

### 3.3.2 Налаштування маршрутних протоколів у корпоративній мережі

Входимо в маршрутизатор, використовуючи правильні облікові дані доступу та за вимогами пункту 2.1.2.1 налаштуємо маршрутний протокол OSPF.

router ospf 1 // призначаємо роботу протоколу

network 192.168.13.0 0.0.0.63 area 0 анонсуємо мережу 192.168.13.0 яка підключена до маршрутизатора, при цьому вказуємо зворотню маску мережі 0.0.0.63, та призначаємо область роботи протоколу 0

network 192.168.13.64 0.0.0.63 area 0

network 10.0.13.6 0.0.0.3 area 0

network 10.0.13.18 0.0.0.3 area 0

ip route 0.0.0.0 0.0.0.0 10.0.13.10 // призначаємо статичний маршрут до маршрутизатора, який підключений до інтернет-провайдера. В свою чергу маршрутизатор в мережі з адресою 10.0.13.10 має свій статичний маршрут до мережі Інтернет.

```
ip route 0.0.0.0 0.0.0.0 10.0.13.14
```

Отримуємо список маршрутів, які налагоджені на маршрутизаторі за допомогою статичних та динамічних налаштувань:

```

10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
C    10.0.13.0/30 is directly connected, Serial0/2/1
L    10.0.13.1/32 is directly connected, Serial0/2/1
C    10.0.13.4/30 is directly connected, Serial0/2/0
L    10.0.13.5/32 is directly connected, Serial0/2/0
C    10.0.13.8/30 is directly connected, Serial0/3/0
L    10.0.13.9/32 is directly connected, Serial0/3/0
C    10.0.13.12/30 is directly connected, Serial0/3/1
L    10.0.13.13/32 is directly connected, Serial0/3/1
O    10.0.13.16/30 [110/128] via 10.0.13.6, 03:13:36, Serial0/2/0
192.168.13.0/24 is variably subnetted, 6 subnets, 2 masks
O    192.168.13.0/28 [110/65] via 10.0.13.6, 03:13:36, Serial0/2/0
O    192.168.13.16/28 [110/65] via 10.0.13.6, 03:13:36, Serial0/2/0
O    192.168.13.32/28 [110/65] via 10.0.13.6, 03:13:36, Serial0/2/0
O    192.168.13.48/28 [110/65] via 10.0.13.6, 03:13:36, Serial0/2/0
O    192.168.13.64/26 [110/65] via 10.0.13.6, 03:13:36, Serial0/2/0
S    192.168.13.128/26 [1/0] via 10.0.13.2
209.165.202.0/28 is subnetted, 1 subnets
S    209.165.202.0/28 [1/0] via 10.0.13.10
      [1/0] via 10.0.13.14

```

Рисунок 3.6 – Список маршрутів різних видів налаштувань

На (рисунок 3.6) конструкція [110/65] означає адміністративну відстань, а «via» означає, що перехід у підмережу відбуватиметься через цього сусіда.

Види пакетів протоколу:

- hello – цей пакет схожий на команду ping, він перевіряє таким чином, чи є хтось на тому кінці каналу зв'язку;
- dbd – пакет надання короткої інформації про всі маршрути, щоб перевірити, якої інформації не вистачає сусідові;
- lsr – це відповідь на запитання пакета dbd, маршрутизатор відповідає якої саме інформації у нього немає;
- lsu – це пакет відповіді на пакет lsr, усередині цього пакета вже надсилається запитувана інформація сусідом;
- lsack – пакет підтвердження, заміщає протокол TCP.

Цей протокол не застосовується в глобальній маршрутизації, оскільки у маршрутизаторів не вистачить обчислювальної потужності, щоб прорахувати всі маршрути в інтернеті.

### 3.3.3 Параметризація технології NAT

Параметризація технології NAT потрібна для налагодження доступу локальної мережі у мережу Інтернет.

`access-list 9 permit 192.168.13.0 0.0.0.255` // розробляємо список дозволів за номером 9 та надаємо право мережі 192.168.13.0 виходити к загальну мережу

Призначаємо кожному вхідному інтерфейсу маршрутизатора створений список дозволу:

```
ip nat inside source list 9 interface s0/3/1
```

```
ip nat inside source list 9 interface s0/3/0
```

Використовуємо діапазон адрес та назву діапазону відповідно до вимог пункту 2.1.2.1

```
ip nat pool networkNAT 209.165.200.5 209.165.200.30 netmask 255.255.255.224
interface Serial0/3/0
```

```
ip nat outside // призначаємо порт як вихідний
```

```
interface Serial0/3/1
```

```
ip nat outside // призначаємо порт як вихідний
```

```
interface Serial0/2/0
```

```
ip nat inside // призначаємо порт як вхідний
```

```
interface Serial0/2/1
```

```
ip nat inside // призначаємо порт як вхідний
```

```
Malienkova_R3 (config)#interface s0/3/0
```

```
Malienkova_R3 (config-if)#bandwidth 128 // пропускна спроможність
```

```
Malienkova_R3 (config-if)# clock rate 128000 // швидкість каналу
```

```
Malienkova_R3 (config-if)# ip ospf cost 7500 // вага метрики
```

### 3.3.4 Конфігурація автоматичного налаштування IP-адреси

Конфігурація автоматичного налаштування IP-адреси призначається за допомогою протоколу динамічного конфігурування DHCP.

Призначимо налаштування:

```
ip dhcp pool Vlan19 // призначаємо пул та номер пулу
network 192.168.13.16 255.255.255.240 // призначаємо мережу та маску мережі
default-router 192.168.13.17 // призначаємо шлюз заданої мережі
dns-server 192.168.13.130 // призначаємо адресу серверу dns

ip dhcp pool Vlan29
network 192.168.13.32 255.255.255.240
default-router 192.168.13.33
dns-server 192.168.13.130

ip dhcp pool Vlan39
network 192.168.13.48 255.255.255.240
default-router 192.168.13.49
dns-server 192.168.13.130
```

Приклад налаштування побудований на призначені пулів адрес для віртуальних комутаційних груп.

## 3.4 Налаштування технологій віртуальних комутаційних груп

### 3.4.1 Налаштування технології на маршрутизаторі

Технології віртуальних комутаційних груп забезпечують розширення комутаційної архітектури мережі. Вона застосовується в комутаторах Cisco для створення віртуального комутатора з декількох фізичних комутаторів, які працюють як єдиний логічний пристрій.

Таблиця 3.4 – Дані призначення мережам

Номер суб-інтерфейсу	Назва підмережі	Фізичний порт комутатора
19	work1	Sw0-2 - f0/4-f0/8
29	work2	Sw0-2 - f0/10-f0/14
39	work3	Sw0-2 - f0/15-f0/20

Проведемо налаштування на маршрутизаторі:

```
int gi0/0.19 // призначаємо САБ-інтерфейси та їх номер
```

```
encapsulation dot1Q 19 // призначаємо номер мережі тільки для певного інтерфейсу
```

```
ip address 192.168.13.17 255.255.255.240 // призначаємо адресу та маску інтерфейсу на маршрутизаторі
```

Налаштування призначаємо на всі інтерфейси відповідно до таблиці 3.4.

```
int gi0/0.29
```

```
encapsulation dot1Q 29
```

```
ip address 192.168.13.33 255.255.255.240
```

```
int gi0/0.39
```

```
encapsulation dot1Q 39
```

```
ip address 192.168.13.49 255.255.255.240
```

### 3.4.2 Налаштування технології на комутаторах

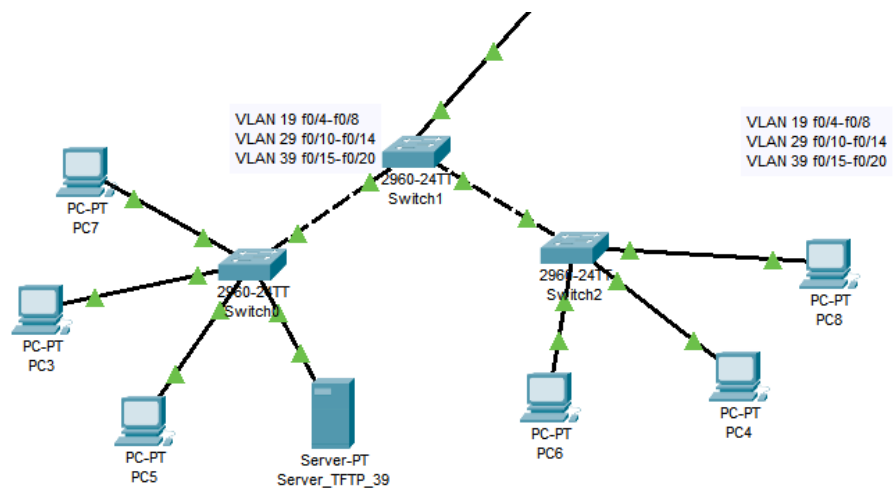


Рисунок 3.7 – Підмережа технологій віртуальних комутаційних груп

Проведемо налаштування на комутаторах:

```
vlan 19 // призначаємо групу та номер групи
```

```
name work1 // призначаємо назву групи
```

```
vlan 29
```

```
name work2
```

```

vlan 39
name work3
interface g0/1 // призначаємо налаштування інтерфейсам які сполучають
підключення комутаторів між собою
switchport trunk allowed vlan 19,29,39 // призначаємо дозвіл використання
портів для заданих підмереж
switchport mode trunk // переводимо роботу порту в режим транк
interface range f0/4-8 // обираємо інтерфейси для підмережі 19
switchport mode access // призначаємо режим роботи access
switchport access vlan 19 // для режиму роботи вказуємо номер підмережі 19
Налаштування повторюємо для підмереж 29 та 39:
interface range f0/10-14 // обираємо інтерфейси для підмережі 29
switchport mode access // призначаємо режим роботи access
switchport access vlan 29 // для режиму роботи вказуємо номер підмережі 29
interface range f0/15-20 // обираємо інтерфейси для підмережі 39
switchport mode access // призначаємо режим роботи access
switchport access vlan 39 // для режиму роботи вказуємо номер підмережі 39

```

### 3.4.3 Параметризація ACL для керування мережевим трафіком

Для керування мережевим трафіком налаштуємо дозволи ACL. За вимогами трафік між частинами мережі проходити не повинен.

```
ip access-list extended 9 // створюємо список керування трафіком 9
```

Призначимо правила використання мережевого трафіку, де команда `deny` – забороняє проходження. Необхідно звернути увагу, що при написанні адреси необхідно використовувати зеркальну маску `wildcard`.

```

deny ip 192.168.13.16 0.0.0.15 192.168.13.32 0.0.0.15 // заборона трафіку
deny ip 192.168.13.16 0.0.0.15 192.168.13.48 0.0.0.15
deny ip 192.168.13.32 0.0.0.15 192.168.13.16 0.0.0.15
deny ip 192.168.13.32 0.0.0.15 192.168.13.48 0.0.0.15
deny ip 192.168.13.48 0.0.0.15 192.168.13.16 0.0.0.15

```

```
deny ip 192.168.13.48 0.0.0.15 192.168.13.32 0.0.0.15
permit ip any any // всім іншим мережам даємо повний дозвіл
```

Повертаючись до саб-інтерфейсів маршрутизатора необхідно призначити список кожному інтерфейсу

```
interface gigabitEthernet 0/1.19 // обираємо саб-інтерфейс для підмережі 19
ip access-group 9 in // призначення списку
interface gigabitEthernet 0/1.29 // обираємо саб-інтерфейс для підмережі 29
ip access-group 9 in // призначення списку
interface gigabitEthernet 0/1.39 // обираємо саб-інтерфейс для підмережі 39
ip access-group 9 in // призначення списку
```

### 3.4.4 Налаштування протоколу синхронізації VTP

VTP – це протокол комутації VLAN, який використовується в мережах Cisco для автоматичного розподілу інформації про VLAN між комутаторами. Вона дозволяє спростити адміністрування VLAN, оновлення конфігурації та додавання нових VLAN в мережі.

Налаштуємо головний комутатор системи, обираємо будь-який для зручності конфігурування:

```
enable
```

```
configure terminal
```

`vtp mode server` // вмикаємо протокол та вказуємо режим роботи протоколу, в нашому випадку режим *server*, тобто даний комутатор є відповідальним за працездатність системи. В налаштуванні є ще два режими це *client* та *transparent*. *Client* налаштовується на всіх інших комутаторах, на яких потрібна робота протоколу. Щоб комутатор не використовував правила протоколу необхідно вказати режим *transparent* і система не буде його бачити.

`vtp domain VLAN` // призначаємо назву домену, спільного ім'я за яким буде працювати протокол

```
vtp password cisco // призначаємо загальний пароль для роботи протоколу
```

Ці кроки потрібно повторити для кожного комутатора, до якого ви хочете застосувати налаштування VTP, але вказати режим роботи client.

### 3.5 Налаштування безпеки даних в комп'ютерній системі

#### 3.5.1 Налаштування політик безпеки AAA

Виконаємо налаштування безпеки даних мережевого обладнання в комп'ютерній системі за протоколом політик безпеки AAA:

aaa new-model // призначаємо роботу протоколу

radius-server host 192.168.13.135 // призначаємо адресу сервера, на якому записані налаштування

radius -server key radius123 // використовуємо загальний ключ для потрапляння в систему

aaa authentication login default group radius local // призначаємо вхід за протоколом або за локальним записом мережі

Конфігурування RADIUS-серверу наступне:

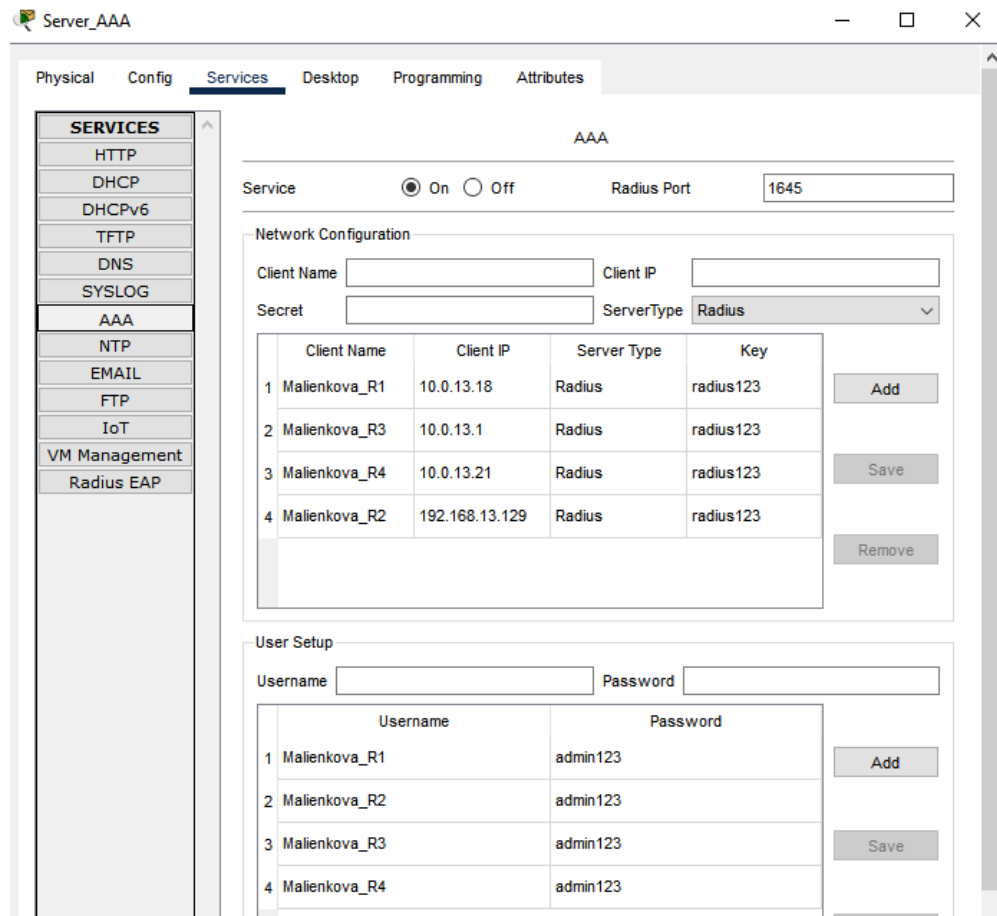


Рисунок 3.8 – Конфігурування політик безпеки



### 3.5.2 Налаштування резервного зберігання конфігурацій

Резервне зберігання конфігурацій відноситься до використання серверу TFTP.

Зберігання конфігурацій необхідно за правилом:

```
copy running-config tftp://<IP_адреса_TFTP_сервера>/<назва_файлу>
```

```
copy running-config tftp://192.168.13.51/Malienkova_R1-config
```

```
Malienkova_R1#copy running-config tftp
Address or name of remote host []? 192.168.13.51
Destination filename [Malienkova_R1-config]?

Writing running-config...!!
[OK - 2523 bytes]

2523 bytes copied in 3.061 secs (824 bytes/sec)
```

Рисунок 3.9 – Працездатність виконання команди

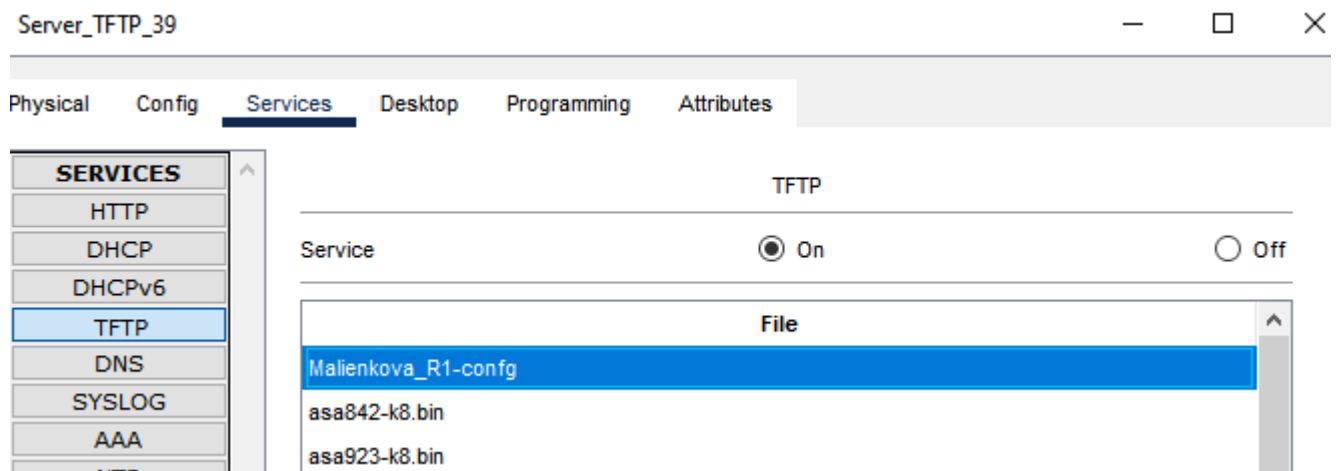


Рисунок 3.10 – Відображення файлів у сервері

### 3.5.3 Налаштування протоколу CDP та безпеки комутаторів

CDP (Cisco Discovery Protocol) - це протокол, розроблений компанією Cisco, який дозволяє мережним пристроям взаємодіяти та обмінюватися інформацією про себе. В Cisco Packet Tracer, CDP використовується для виявлення та взаємодії між пристроями Cisco в мережі.

CDP дозволяє пристроям автоматично визначати та відобразити інформацію про сусідні пристрої, таку як їхні імена, типи інтерфейсів та IP-адреси. Це значно полегшує адміністрування мережі, оскільки операторам не потрібно ручно налаштовувати або вводити інформацію про кожен пристрій.

```

Malienkova_Switch1#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID      Local Intrfce  Holdtme   Capability   Platform   Port ID
Malienkova_R1
  Gig 0/1      149         R         C2900        Gig 0/1
Malienkova_R1
  Gig 0/1      149         R         C2900        Gig 0/1.19
Malienkova_R1
  Gig 0/1      149         R         C2900        Gig 0/1.29
Malienkova_R1
  Gig 0/1      149         R         C2900        Gig 0/1.39
Malienkova_Switch0
  Gig 0/2      148         S         2960         Gig 0/1
Malienkova_Switch2
  Fas 0/1      148         S         2960         Gig 0/1

```

Рисунок 3.11 – Загальні інтерфейси

```

Malienkova_Switch0#show cdp interface
FastEthernet0/1 is down, line protocol is down
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
FastEthernet0/2 is down, line protocol is down
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
FastEthernet0/3 is down, line protocol is down
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
FastEthernet0/4 is up, line protocol is up
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
FastEthernet0/5 is down, line protocol is down
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds

```

Рисунок 3.12 – Статус роботи портів

Після оптимізації роботи протоколу CDP, налаштуємо безпеку портів на комутаторах:

```

interface fa0/1 // обираємо потрібний інтерфейс
switchport mode access // переводимо режим порту в access
switchport port-security maximum 1 // призначаємо кількість доступних сесій
на порту 1
switchport port-security mac-address sticky // використовується для
автоматичного закріплення MAC-адресів підключених пристроїв до захищеного
порту на комутаторі Cisco

```

switchport port-security violation shutdown // використовується для налаштування режиму порушення безпеки порту на комутаторі Cisco, при якому порт переходить в стан "shutdown" (вимкнений), якщо виявляється порушення.

### 3.6 Перевірка сполучення та комунікації мережевих компонентів

Останнім кроком налаштування є повна перевірка всіх систем в корпоративній мережі.

При виконанні команди ping використовується URL-адреса або IP-адреса вузла призначення. Протокол надсилає декілька ICMP пакетів вузлу призначення, після цього очікує відповідь. Якщо відповіді немає – вузол призначення не має доступу в мережі. Наявність відповіді свідчить про те, що вузол призначення правильно налаштований та має доступ до маршрутизації мережі.

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::2D0:FFFF:FE05:52DE
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 192.168.13.133
    Subnet Mask . . . . .: 255.255.255.192
    Default Gateway . . . . .: ::
                                     192.168.13.129

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: ::
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .: ::
                                     0.0.0.0

C:\>ping 209.165.202.6

Pinging 209.165.202.6 with 32 bytes of data:

Reply from 209.165.202.6: bytes=32 time=3ms TTL=124
Reply from 209.165.202.6: bytes=32 time=4ms TTL=124
Reply from 209.165.202.6: bytes=32 time=4ms TTL=124
Reply from 209.165.202.6: bytes=32 time=4ms TTL=124

Ping statistics for 209.165.202.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 4ms, Average = 3ms
```

Рисунок 3.13 – Здійснення діагностики працездатності вузла

```

Malienkova_Switch1#show vtp status
VTP Version capable      : 1 to 2
VTP version running      : 1
VTP Domain Name          : VLAN
VTP Pruning Mode         : Disabled
VTP Traps Generation     : Disabled
Device ID                 : 0001.4389.7200
Configuration last modified by 192.168.13.2 at 3-1-93 00:22:24

Feature VLAN :
-----
VTP Operating Mode       : Client
Maximum VLANs supported locally : 255
Number of existing VLANs : 8
Configuration Revision   : 0
MD5 digest               : 0xFB 0x20 0x76 0x96 0x5A 0xE7 0x55 0x9A
                        : 0x85 0x1E 0xFB 0x59 0x53 0x8E 0x39 0x9D

```

Рисунок 3.14 – Перевірка статусу VTP клієнту

```

Malienkova_Switch0#show vtp status
VTP Version capable      : 1 to 2
VTP version running      : 1
VTP Domain Name          : VLAN
VTP Pruning Mode         : Disabled
VTP Traps Generation     : Disabled
Device ID                 : 0090.0C39.D500
Configuration last modified by 192.168.13.2 at 3-1-93 00:22:24
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN :
-----
VTP Operating Mode       : Server
Maximum VLANs supported locally : 255
Number of existing VLANs : 8
Configuration Revision   : 0
MD5 digest               : 0xFB 0x20 0x76 0x96 0x5A 0xE7 0x55 0x9A
                        : 0x85 0x1E 0xFB 0x59 0x53 0x8E 0x39 0x9D

```

Рисунок 3.15 – Перевірка статусу VTP серверу

```

Malienkova_Switch0#show vtp counters
VTP statistics:
Summary advertisements received : 5
Subset advertisements received  : 4
Request advertisements received  : 2
Summary advertisements transmitted : 2
Subset advertisements transmitted : 2
Request advertisements transmitted : 2
Number of config revision errors  : 1
Number of config digest errors    : 0
Number of V1 summary errors       : 0

```

Рисунок 3.16 – Перевірка статистики використання VTP серверу

Pro	Inside global	Inside local	Outside local	Outside global
icmp	10.0.13.1:10	192.168.13.49:10	209.165.202.4:10	209.165.202.4:10
icmp	10.0.13.1:11	192.168.13.49:11	209.165.202.4:11	209.165.202.4:11
icmp	10.0.13.1:12	192.168.13.49:12	209.165.202.4:12	209.165.202.4:12
icmp	10.0.13.1:9	192.168.13.49:9	209.165.202.4:9	209.165.202.4:9

Рисунок 3.17 – Перевірка таблиці параметризації NAT

```
Malienkova_R1#show access-lists
Extended IP access list VLANS
 10 deny ip 192.168.13.16 0.0.0.15 192.168.13.32 0.0.0.15
 20 deny ip 192.168.13.16 0.0.0.15 192.168.13.48 0.0.0.15
 30 deny ip 192.168.13.32 0.0.0.15 192.168.13.16 0.0.0.15
 40 deny ip 192.168.13.32 0.0.0.15 192.168.13.48 0.0.0.15
 50 deny ip 192.168.13.48 0.0.0.15 192.168.13.16 0.0.0.15
 60 deny ip 192.168.13.48 0.0.0.15 192.168.13.32 0.0.0.15
 70 permit ip any any (14 match(es))
```

Рисунок 3.18 – Перевірка заданих значень параметризації ACL для керування мережевим трафіком

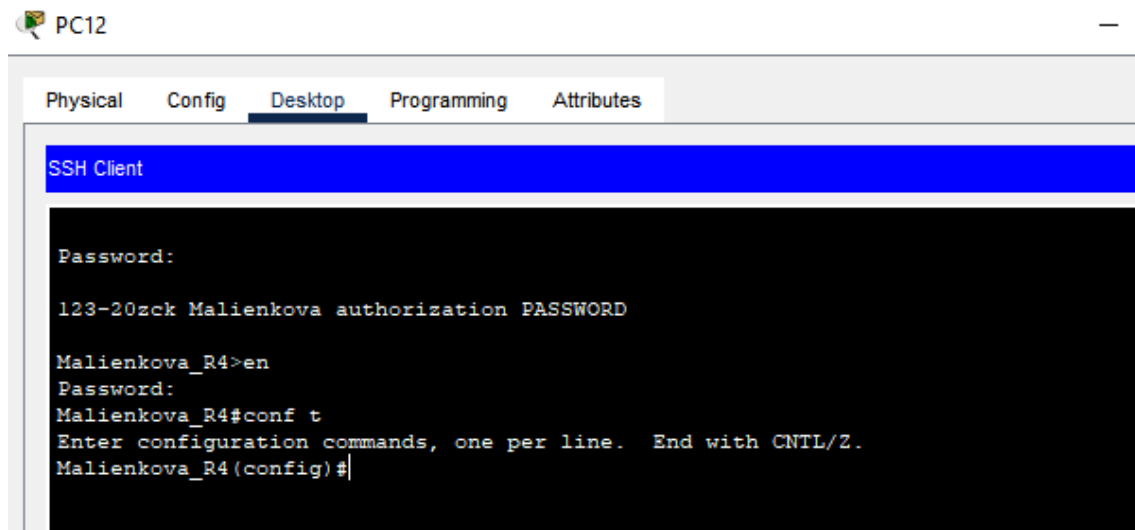


Рисунок 3.19 – Перевірка призначення налаштувань віддаленого доступу

```

Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.13.35

Pinging 192.168.13.35 with 32 bytes of data:

Request timed out.
Reply from 192.168.13.35: bytes=32 time=31ms TTL=127
Reply from 192.168.13.35: bytes=32 time<1ms TTL=127
Reply from 192.168.13.35: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.13.35:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 31ms, Average = 10ms

C:\>ping 192.168.13.35

Pinging 192.168.13.35 with 32 bytes of data:

Reply from 192.168.13.49: Destination host unreachable.
Reply from 192.168.13.49: Destination host unreachable.
Reply from 192.168.13.49: Destination host unreachable.
Reply from 192.168.13.49: Destination host unreachable.

Ping statistics for 192.168.13.35:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

```

Рисунок 3.20 – Перевірка роботи параметризації ACL для керування мережевим трафіком

```

Malienkova_R1#show ip dhcp binding

```

IP address	Client-ID/ Hardware address	Lease expiration	Type
192.168.13.70	0001.4357.8509	--	Automatic
192.168.13.67	0004.9AA7.6992	--	Automatic
192.168.13.69	0007.EC99.AE38	--	Automatic
192.168.13.68	0002.17B8.A805	--	Automatic
192.168.13.71	0060.2F65.B336	--	Automatic
192.168.13.18	0004.9A27.8113	--	Automatic
192.168.13.19	0007.ECE0.3DDC	--	Automatic
192.168.13.34	0030.A395.9C61	--	Automatic
192.168.13.35	0030.A32C.DC43	--	Automatic
192.168.13.51	0001.63C4.26C0	--	Automatic
192.168.13.52	0007.ECD3.0352	--	Automatic
192.168.13.50	0001.63A9.CCB3	--	Automatic

```

Malienkova_R1#

```

Рисунок 3.21 – Таблиця конфігурації автоматичного налаштування IP-адреси

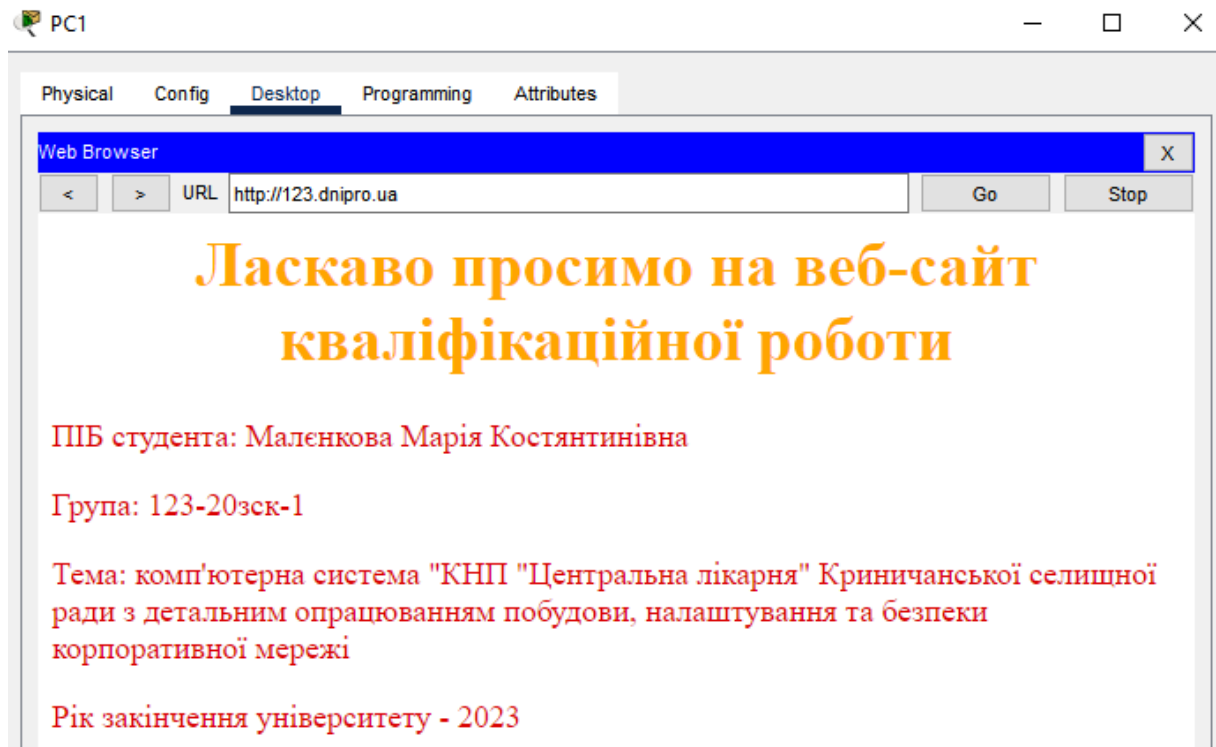


Рисунок 3.22 – Перевірка працездатності персонального веб-сайту кваліфікаційної роботи

VLAN	Name	Status	Ports
1	default	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24
19	work1	active	
29	work2	active	
39	work3	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Рисунок 3.23 – Налаштування технологій віртуальних комутаційних груп

## 4 РОЗРОБКА КОМПОНЕНТА СИСТЕМИ З ОРГАНІЗАЦІЇ ПІДКЛЮЧЕННЯ ПРИСТРОЇВ МЕРЕЖІ

### 4.1 Розробка організаційних компонентів

Для створення фізичної частини мережі використовується не лише активне мережеве обладнання, а і пасивне. Розробка компонента системи включає створення структурованої кабельної системи мережі лікарні.

При моделюванні інфраструктури було використано наступне пасивне мережеве обладнання:

- кабелі (кручена пара) – це найбільша й основоположна частина пасивного обладнання. Для підключення всіх вузлів в підмережах було використано 200м кабелю – вита пара, та 50м – оптоволокна.;

- кабельні органайзери, зроблені з металу або пластику. Використовуються для впорядкування кабелів і захисту їх від зовнішніх пошкоджень. Було обрано кабельний органайзер Cablexpert 19C-CM2;



Рисунок 4.1 – Вигляд кабельних органайзерів Cablexpert 19C-CM2

- кабель-канали – це короби, необхідні для захисту проводів, але водночас мають більш непомітний зовнішній вигляд. Було використано кабель канал LHD 21\*19\_FD;



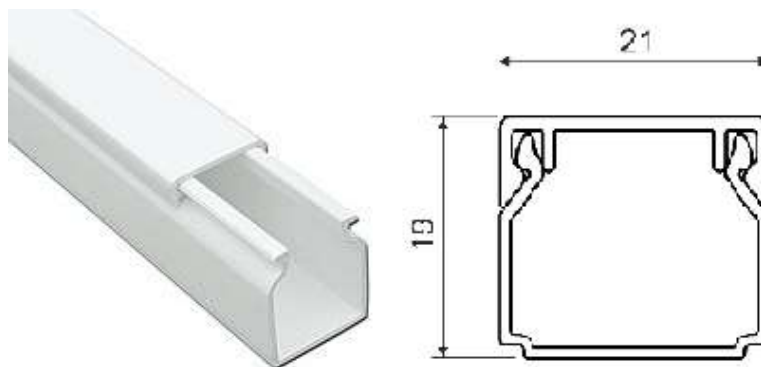


Рисунок 4.2 – Вигляд кабельних каналів LHD 21\*19\_FD

– розетки. Розміщуються на перегородках і надійно тримають приєднані до них кабелі. Вони створені для кріплення мережевих кабелів у приміщенні. Розетки використовуємо UTP 8P8C Atcom;



Рисунок 4.3 – Вигляд розетки UTP 8P8C Atcom

– патч-корди – це кабелі для комутації активного мережевого обладнання, що під'єднується, між собою або до дротової мережі, використовуємо Ugreen NW102;



Рисунок 4.4 – Вигляд патч-корда Ugreen NW102

- конектор – роз'єм, який знаходиться на кінцях патч-корду Merlion RJ-45 8P8C;



Рисунок 4.5 – Вигляд конектора Merlion RJ-45 8P8C

- серверні стійки – це шафи без стінок призначені для розміщення обладнання. Було обрано стійки MGS UA-OF24-D-BK.



Рисунок 4.6 – Вигляд стійки MGS UA-OF24-D-BK

Відповідно до (рисунок 2.2-2.3) створимо таблицю фізичних компонентів системи з описом необхідних особливостей, та опишемо кількість та довжину елементів.

Таблиця 4.1 – Специфікація структурованих кабельних систем

Номер компоненту	Ім'я з технічною характеристикою	Тип, марка, позначення	Одиниці виміру	Кількість
1	Кабельний канал Розмір: 21 мм x 19 мм Довжина 1.5м	Kopos	од	80
2	Кабель-органайзер Розмір: 1рівень	IP2HOUSE	од	2
3	Інформаційна розетка RJ-45	Schneider Electric	од	10
4	Кабель вита пара Тип: UTP cat5e	AMP	м	200
5	Конектор RJ-45	Eserver	од	40
6	Стійка Розмір: 9рівнів	Conteg	од	2
7	Оптоволоконний кабель	AMP	м	50
8	Конектор оптоволокна	Eserver	м	25

Відповідно до схем прокладки кабельної системи, для мережі потрібно 200м кабелю вита пара та 50м оптоволоконного кабелю. Мережеві пристрої вбудовуються в стійки, які мають монтаж на стіні. Для компактності організації кабельної системи були розраховані кабельні органайзери. Для всіх співробітників лікарні були розраховані мережеві розетки інтерфейсу RJ-45 UTP cat5e.

Для встановлення стійок на стіну потрібен перфоратор, оскільки стіни мають бетонну основу.

## 4.2 Результат з організації підключення

В результаті використання пасивного та активного мережевого обладнання, ми отримали 4 стійки на кожну підмережу.

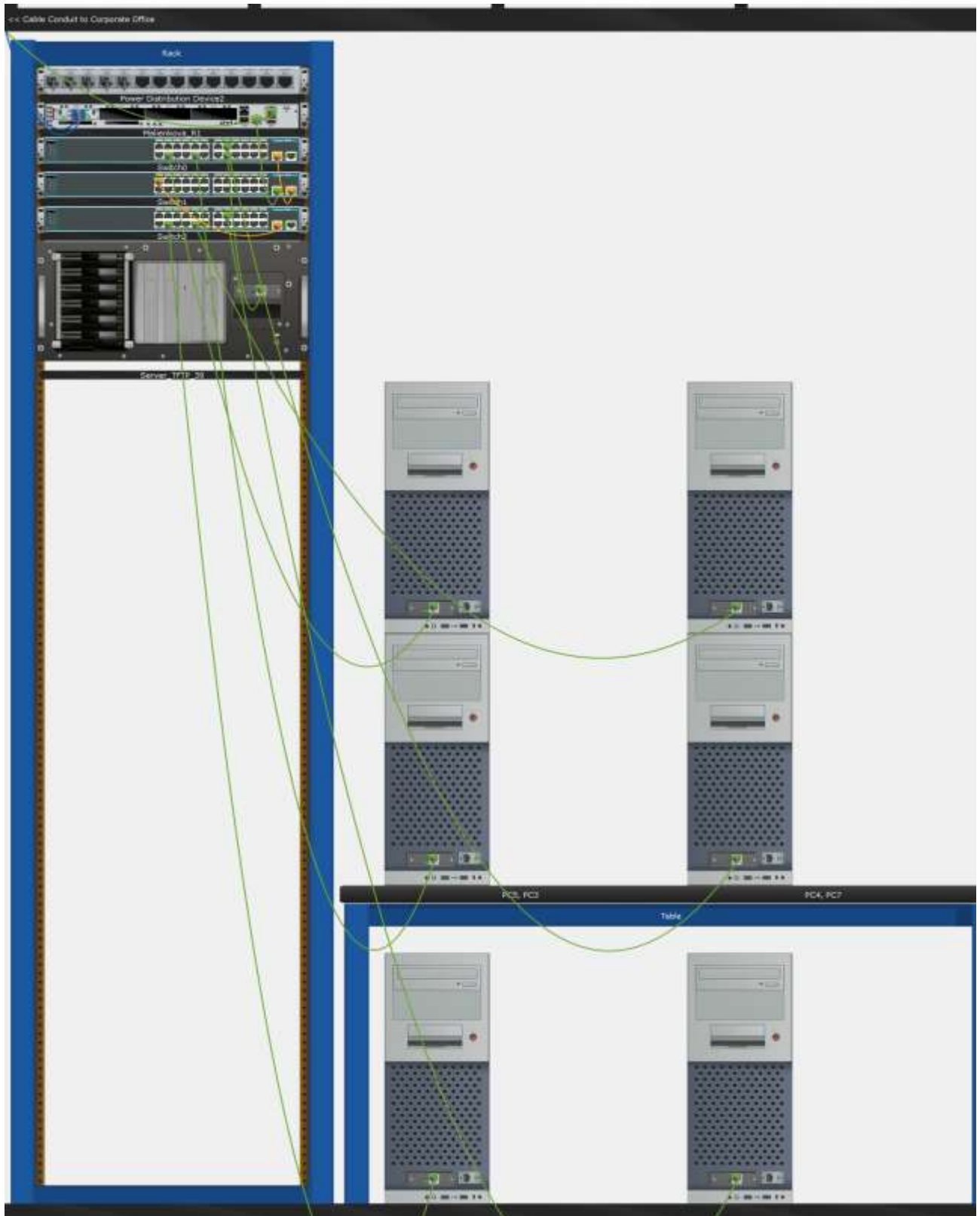


Рисунок 4.7 – Вигляд фізичного підключення підмережі LAN1

В них знаходяться мережеве обладнання, сервери та з'єднання з кінцевими пристроями.

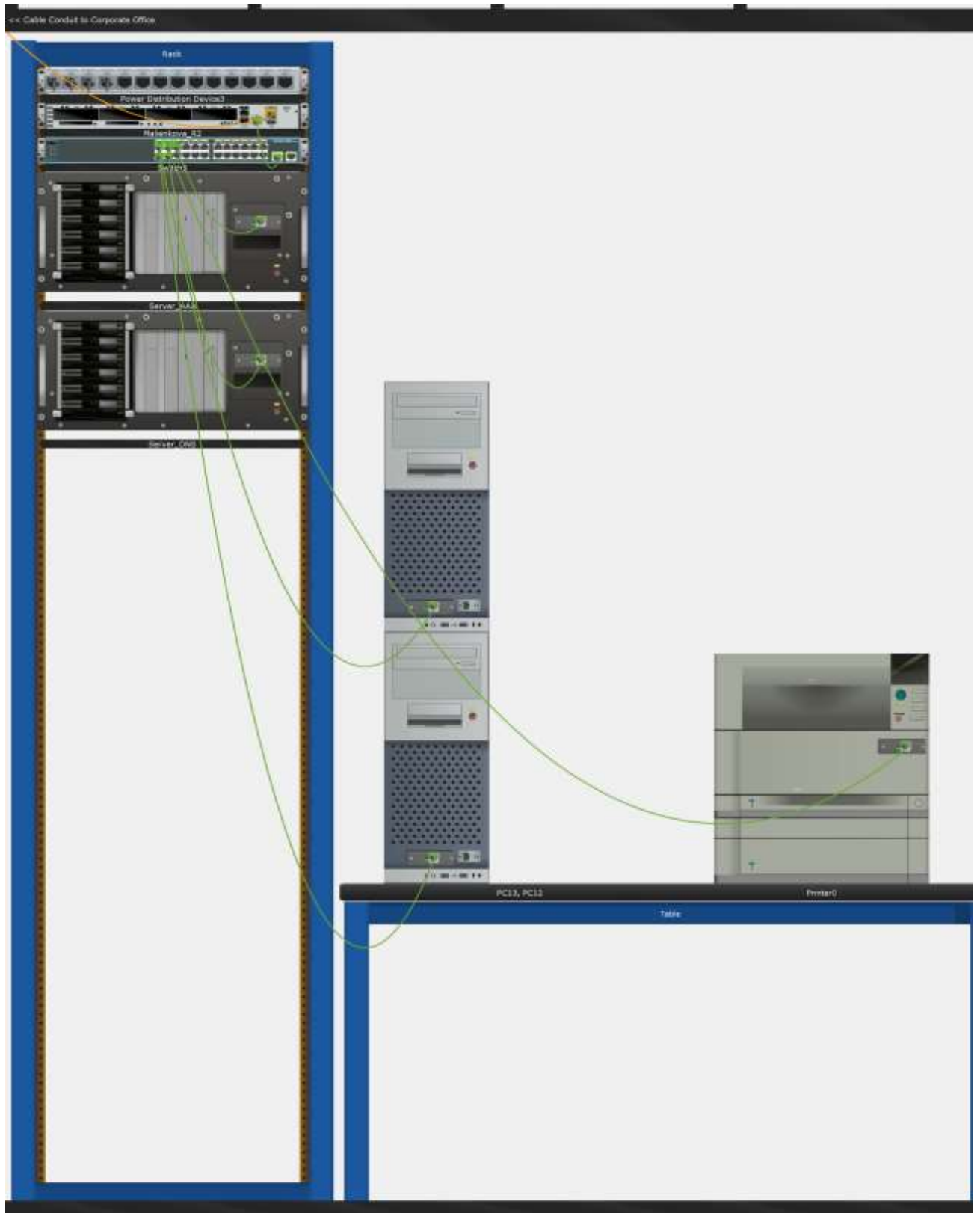


Рисунок 4.8 – Вигляд фізичного підключення підмережі LAN2

Розташування кінцевих пристроїв на рисунках потрібно знехтувати, так як вони виконують функцію моделювання.



Рисунок 4.9 – Вигляд фізичного підключення підмережі LAN3

Кожна стійка має спроможність к масштабуванню кількості мережевого обладнання або серверів.

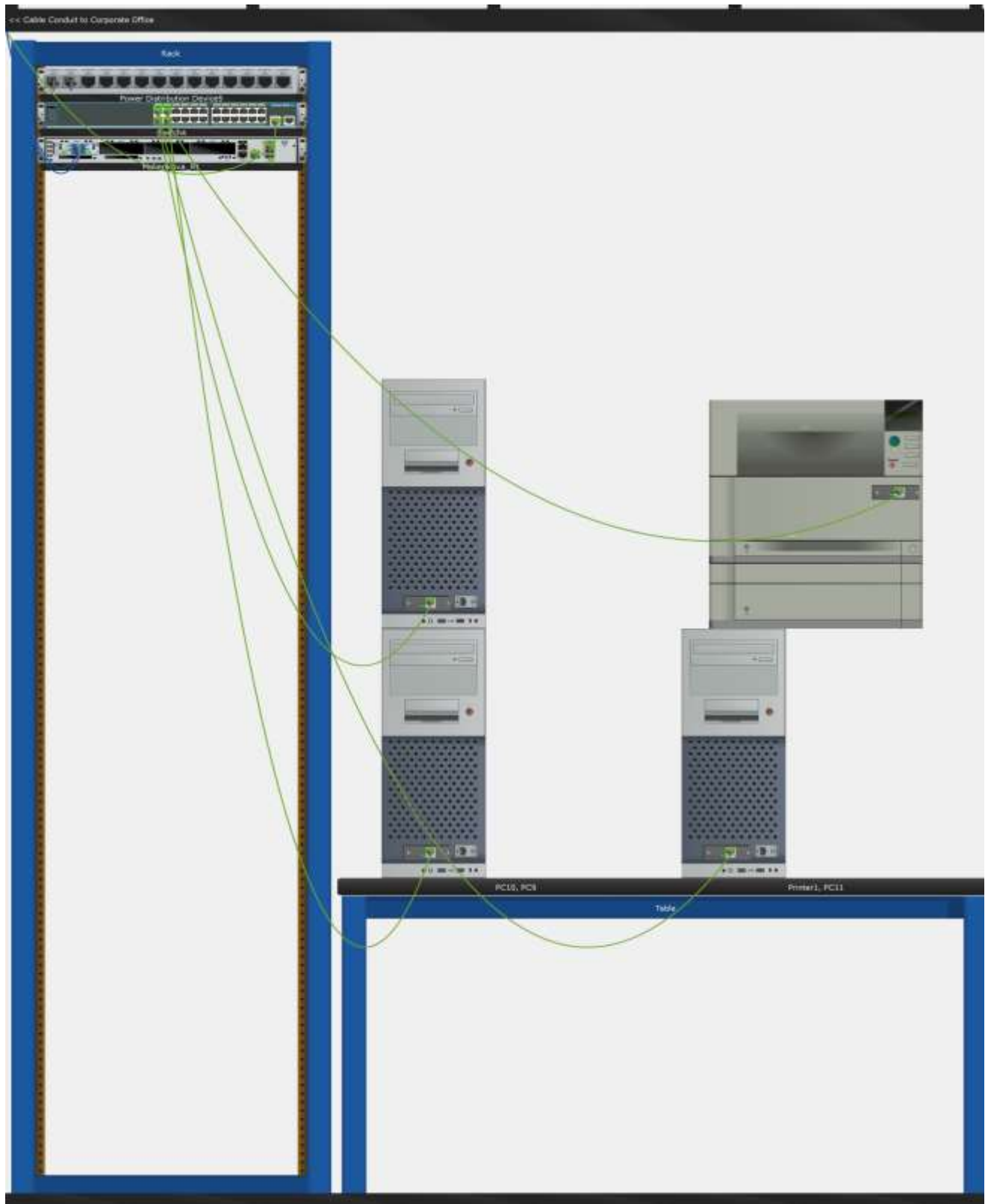


Рисунок 4.10 – Вигляд фізичного підключення підмережі LAN4

## ВИСНОВКИ

Результатом кваліфікаційної роботи є повністю змодульована та налаштована корпоративна мережа комунального закладу «Криничанська центральна районна лікарня».

Мережа має великий потенціал та масштабованість, як з апаратної частини, так і з програмної. Діапазон IP-адрес розрахований на майбутній розвиток персоналу, та при збільшенні робочих станцій не викличе труднощів.

В наш час інформаційних технологій, мережа побудована на сучасних стандартах та вимогах. Вона задовольняє високу швидкість передачі даних та високий рівень безпеки.

Кваліфікаційна робота має повний перелік схем розташування пристроїв мережі, таблиць налаштування мережі та технічний код програмування мережевого обладнання.

Також, була розроблена апаратна та програмна частина мережі. Мережа лікарні має сучасне програмне та апаратне забезпечення, а саме – сучасне мережеве обладнання та сучасні персональні комп'ютери. Для організації підключення апаратної частини був розроблений компонент системи. Він вміщує в собі повну розробку структурованої кабельної системи лікарні.

В мережі використовуються всі сучасні мережеві протоколи стеку протоколів TCP/IP.

Моделювання проекту було виконано в програмному додатку Cisco Packet Tracer.



## ПЕРЕЛІК ПОСИЛАНЬ

1. ДСТУ 3008-2015. Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлювання. – К.: Держстандарт, 2015. – 37 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. 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.
4. Цвіркун Л.І. Комп'ютерні мережі. Методичні рекомендації до виконання лабораторних робіт студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія: у 2 ч. / Л.І. Цвіркун, Я.В. Панферова ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2018. – Ч. 2. – 39 с
5. Налаштування локальних пристроїв для користувачів Cisco [Електронний ресурс] – <https://collaborationhelp.cisco.com/uk-ua/article/poqjhk/Cisco-Webex-Teams>
6. Списки контролю доступу [Електронний ресурс] – [https://bstudy.net/982506/tehnika/spiski\\_kontrolya\\_dostupa](https://bstudy.net/982506/tehnika/spiski_kontrolya_dostupa)
7. Глобальні мережі. Загальні принципи організації. [Електронний ресурс] – <http://um.co.ua/6/6-15/6-15800.html>
8. Пасивне мережеве обладнання [Електронний ресурс] – <https://comtrade.ua/passivnoe-setevoe-oborudovanie/>
9. Монтаж локальної мережі [Електронний ресурс] – <https://my.kpi.ua/syllabus/4390?trainform=1>
10. Трансляція мережевих адрес (NAT) [Електронний ресурс] – <https://techukraine.net/>

## Додаток А

Загальна схема комп'ютерної системи "КНП "Центральна лікарня" Криничанської селищної ради

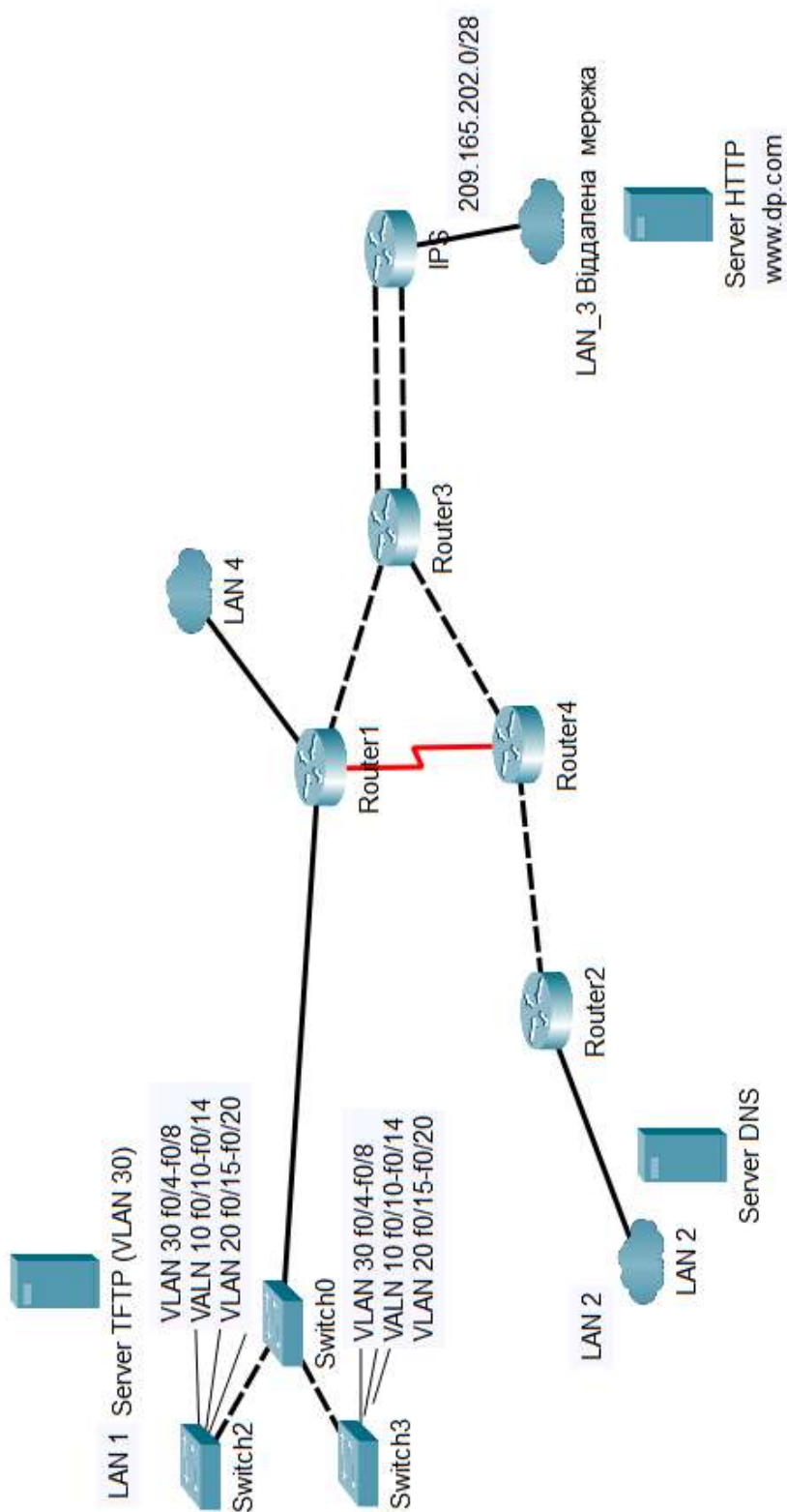


Рисунок А.1 – Загальна схема комп'ютерної системи "КНП "Центральна лікарня" Криничанської селищної ради

## 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  
804.02070743.23009-01 12 01

Листів 13

2023

## АННОТАЦІЯ

Програма складається з частини програмного коду для налаштування конфігурацій мережевих інтерфейсів мережі. Код призначений для працездатності протоколів DHCP, AAA, NAT, для налаштування консолей та ліній VTY та для створення комп'ютерних підмереж VLAN, домену та SSH доступу. Також, для налаштування списків доступу ACL.

**ЗМІСТ**

	Стор.
1.Налаштування маршрутизатора Malienkova_R4	4
2.Налаштування маршрутизатора Malienkova_R1	6
3.Налаштування комутатора Switch0	10

**Конфігурація Malienkova\_R4:**

```
!  
version 15.1  
no service timestamps log datetime msec  
no service timestamps debug datetime msec  
service password-encryption  
!  
hostname Malienkova_R4  
!  
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1  
!  
no ip cef  
no ipv6 cef  
!  
username 12320zck_Malienkova password 7 0822455D0A16  
!  
license udi pid CISCO2901/K9 sn FTX15247FPJ-  
!  
ip domain-name Malienkova_R4  
!  
spanning-tree mode pvst  
!  
interface GigabitEthernet0/0  
no ip address  
duplex auto  
speed auto  
!  
interface GigabitEthernet0/1  
ip address 10.0.13.21 255.255.255.252  
duplex auto
```

```
speed auto
!
interface Serial0/3/0
ip address 10.0.13.2 255.255.255.252
!
interface Serial0/3/1
ip address 10.0.13.17 255.255.255.252
clock rate 2000000
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
network 10.0.13.20 0.0.0.3 area 0
network 10.0.13.0 0.0.0.3 area 0
network 10.0.13.16 0.0.0.3 area 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.0.13.5
ip route 0.0.0.0 0.0.0.0 10.0.13.1
!
ip flow-export version 9
!
banner motd #123-20zck Malienkova authorization PASSWORD#
!
line con 0
password 7 0822455D0A16
login
```



```
!  
line aux 0  
!  
line vty 0 4  
login local  
transport input ssh  
!  
end
```

### **Налаштування маршрутизатора Malienkova\_R1:**

```
!  
version 15.1  
no service timestamps log datetime msec  
no service timestamps debug datetime msec  
no service password-encryption  
!  
hostname Malienkova_R1  
!  
ip dhcp pool LAN4  
network 192.168.13.64 255.255.255.192  
default-router 192.168.13.65  
dns-server 192.168.13.130  
ip dhcp pool Vlan19  
network 192.168.13.16 255.255.255.240  
default-router 192.168.13.17  
dns-server 192.168.13.130  
ip dhcp pool LAN1  
network 192.168.13.0 255.255.255.240  
default-router 192.168.13.1  
dns-server 192.168.13.130
```

```
ip dhcp pool Vlan29
network 192.168.13.32 255.255.255.240
default-router 192.168.13.33
dns-server 192.168.13.130
ip dhcp pool Vlan39
network 192.168.13.48 255.255.255.240
default-router 192.168.13.49
dns-server 192.168.13.130
!
no ip cef
no ipv6 cef
!
license udi pid CISCO2901/K9 sn FTX1524ANOL-
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
ip address 192.168.13.65 255.255.255.192
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 192.168.13.1 255.255.255.240
duplex auto
speed auto
!
interface GigabitEthernet0/1.19
encapsulation dot1Q 19
ip address 192.168.13.17 255.255.255.240
ip access-group VLANS in
```

```
!  
interface GigabitEthernet0/1.29  
  encapsulation dot1Q 29  
  ip address 192.168.13.33 255.255.255.240  
  ip access-group VLANS in  
!  
interface GigabitEthernet0/1.39  
  encapsulation dot1Q 39  
  ip address 192.168.13.49 255.255.255.240  
  ip access-group VLANS in  
!  
interface Serial0/3/0  
  ip address 10.0.13.18 255.255.255.252  
  clock rate 2000000  
!  
interface Serial0/3/1  
  ip address 10.0.13.6 255.255.255.252  
  clock rate 2000000  
!  
interface Vlan1  
  no ip address  
  shutdown  
!  
router ospf 1  
  log-adjacency-changes  
  network 192.168.13.0 0.0.0.63 area 0  
  network 10.0.13.4 0.0.0.3 area 0  
  network 10.0.13.16 0.0.0.3 area 0  
  network 192.168.13.64 0.0.0.63 area 0  
  network 192.168.13.16 0.0.0.15 area 0
```

```
network 192.168.13.32 0.0.0.15 area 0
network 192.168.13.48 0.0.0.15 area 0
network 192.168.13.0 0.0.0.15 area 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.0.13.5
!
ip flow-export version 9
!
ip access-list extended VLANS
deny ip 192.168.13.16 0.0.0.15 192.168.13.32 0.0.0.15
deny ip 192.168.13.16 0.0.0.15 192.168.13.48 0.0.0.15
deny ip 192.168.13.32 0.0.0.15 192.168.13.16 0.0.0.15
deny ip 192.168.13.32 0.0.0.15 192.168.13.48 0.0.0.15
deny ip 192.168.13.48 0.0.0.15 192.168.13.16 0.0.0.15
deny ip 192.168.13.48 0.0.0.15 192.168.13.32 0.0.0.15
permit ip any any
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
End

Налаштування комутатора Switch0:
!
version 15.0
```

```
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
  switchport access vlan 19
  switchport mode access
!
interface FastEthernet0/5
  switchport access vlan 19
  switchport mode access
!
interface FastEthernet0/6
  switchport access vlan 19
  switchport mode access
!
interface FastEthernet0/7
  switchport access vlan 19
  switchport mode access
```

```
!  
interface FastEthernet0/8  
  switchport access vlan 19  
  switchport mode access  
!  
interface FastEthernet0/9  
!  
interface FastEthernet0/10  
  switchport access vlan 29  
  switchport mode access  
!  
interface FastEthernet0/11  
  switchport access vlan 29  
  switchport mode access  
!  
interface FastEthernet0/12  
  switchport access vlan 29  
  switchport mode access  
!  
interface FastEthernet0/13  
  switchport access vlan 29  
  switchport mode access  
!  
interface FastEthernet0/14  
  switchport access vlan 29  
  switchport mode access  
!  
interface FastEthernet0/15  
  switchport access vlan 39  
  switchport mode access
```

```
!  
interface FastEthernet0/16  
  switchport access vlan 39  
  switchport mode access  
!  
interface FastEthernet0/17  
  switchport access vlan 39  
  switchport mode access  
!  
interface FastEthernet0/18  
  switchport access vlan 39  
  switchport mode access  
!  
interface FastEthernet0/19  
  switchport access vlan 39  
  switchport mode access  
!  
interface FastEthernet0/20  
  switchport access vlan 39  
  switchport mode access  
!  
interface FastEthernet0/21  
!  
interface FastEthernet0/22  
!  
interface FastEthernet0/23  
!  
interface FastEthernet0/24  
!  
interface GigabitEthernet0/1
```

```
switchport trunk allowed vlan 19,29,39
switchport mode trunk
!
interface GigabitEthernet0/2
!
interface Vlan1
  no ip address
!
line con 0
!
line vty 0 4
  login
line vty 5 15
  login
!
end
```