Міністерство освіти і науки України
Луцький національний технічний університет
(повне найменування закладу вищої освіти)

Факультет комп'ютерних та інформаційних технологій
(повне найменування факультету)

Кафедра комп'ютерної інженерії та охоронних систем
(повне найменування кафедри)

КВАЛІФІКАЦІЙНА РОБОТА ЗА СТУПЕНЕМ ВИЩОЇ ОСВІТИ «БАКАЛАВР»

КОМП'ЮТЕРНА МЕРЕЖА МЕДИЧНОГО ЦЕНТРУ «КЛІНІКА ЗДОРОВ'Я»

COMPUTER NETWORK OF THE MEDICAL CENTER "KLINIKA ZDOROV'YA"

спеціальність 123 Комп'ютерна інженерія
(шифр і назва спеціальності)

освітня програма Комп'ютерна інженерія
(назва освітньої програми)

Виконав: здобувач вищої освіти
групи КІ-41
Вікторова Яна Андріївна

(підпис)

Керівник:
к.т.н., доцент
Багнюк Наталія Володимирівна

(підпис)

Кваліфікаційну роботу
допущено до захисту
«_____» червня 2026 р.
Гарант освітньої програми:
к.т.н., доцент
Лавренчук Світлана Василівна

(підпис)

Луцьк – 2026 року

ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Факультет *комп'ютерних та інформаційних технологій*
Кафедра *комп'ютерної інженерії та безпеки*
Ступінь вищої освіти: *бакалавр*
Галузь знань: *12 Інформаційні технології*
Спеціальність: *123 Комп'ютерна інженерія*
Освітня програма: *«Комп'ютерна інженерія»*

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ доц. Т. Терлецький
«__23__» _____12_____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ВИЩОЇ ОСВІТИ

Вікторовій Яні Андріївні
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи *Комп'ютерна мережа медичного центру «Клініка здоров'я»*

Керівник роботи *к.т.н., доцент Багнюк Наталія Володимирівна*

затверджені наказом закладу вищої освіти від «20» грудня 2025 року № 536/01-02
2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 28.05.2026 р.

3. Вихідні дані до роботи *Джерелом розробки є науково-технічна література та публікації в періодичних виданнях з даного питання, опубліковані зарубіжні та вітчизняні роботи в даній області, різні інтернет-ресурси технічного спрямування*

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити):
Вступ
Аналіз вимог та інфраструктури комп'ютерної мережі медичного закладу
Техніко-економічне обґрунтування та вибір засобів побудови мережі
Проєктування, розгортання та тестування комп'ютерної мережі
Висновки

5. Перелік графічного (ілюстративного) матеріалу:
Логічна структура комп'ютерної мережі медичного закладу
Схема VLAN-сегментування та IP-адресації мережі
Принципова схема підключення активного мережевого обладнання
Моделювання та перевірка працездатності мережі в Cisco Packet Tracer

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис	
		завдання видав	завдання прийняв
Аналіз вимог та інфраструктури комп'ютерної мережі медичного закладу	*Багнюк Н.В., доцент*		
Техніко-економічне обґрунтування та вибір засобів побудови мережі	*Багнюк Н.В., доцент*		
Проєктування, розгортання та тестування комп'ютерної мережі	*Багнюк Н.В., доцент*		
Нормоконтроль	*Багнюк Н. В., доцент*		
Гарант ОП	*Лавренчук С. В., доцент*		
Показник запозичень тексту	***___%***		
Академічна доброчесність	*Міскевич О. І., ст. викладач*		

7. Дата видачі завдання 23.12.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	*Огляд літератури із досліджуваної проблеми, аналіз предметної області та наявних рішень*	до 10.02.2026 р.	
2.	*Аналіз вимог та інфраструктури комп'ютерної мережі медичного закладу*	до 02.03.2026 р.	
3.	*Техніко-економічне обґрунтування та вибір засобів побудови мережі*	до 02.04.2026 р.	
4.	*Проєктування, розгортання та тестування комп'ютерної мережі*	до 10.04.2026 р.	
5.	*Представлення остаточного варіанту кваліфікаційної роботи керівникові*	до 01.05.2026 р.	
6.	*Нормоконтроль*	до 23.05.2026 р.	
7.	*Інструментальна перевірка на академічний плагіат*	до 25.05.2026 р.	
8.	*Здача кваліфікаційної роботи та всіх супровідних документів на кафедру*	до 28.05.2026 р.	

Здобувач вищої освіти _____ Яна ВІКТОРОВА
(підпис) (прізвище, ініціали)

Керівник кваліфікаційної роботи _____ Наталія БАГНЮК
(підпис) (прізвище, ініціали)

АНОТАЦІЯ

Вікторова Я. А. Комп’ютерна мережа медичного закладу. Рукопис.

Кваліфікаційна робота бакалавра ОП «Комп’ютерна інженерія» спеціальності 123 Комп’ютерна інженерія. Луцький національний технічний університет. Луцьк, 2026.

Кваліфікаційна робота складається з вступу, трьох розділів, висновків, списку використаних джерел, додатків.

Перший розділ присвячено аналізу завдання, де охарактеризовано об’єкт проєктування, визначено основні вимоги до комп’ютерної мережі медичного закладу та описано інформаційні ресурси й служби.

У другому розділі здійснено техніко-економічне обґрунтування проєкту: обґрунтовано вибір фізичної топології, проведено порівняльний аналіз варіантів обладнання різних виробників та розроблено логічну структуру мережі.

Третій розділ присвячено практичній реалізації мережі та охоплює вибір активного мережевого обладнання, розрахунок логічної адресації з використанням VLSM, налаштування комутації (VLAN, trunk, STP), організацію безпроводового доступу, налаштування міжмережевої взаємодії з використанням Inter-VLAN routing, HSRP та ACL, а також конфігурування захищеного доступу до мережі Інтернет через NAT на Cisco ASA 5505.

Ключові слова: медичний заклад, VLAN, Inter-VLAN routing, HSRP, мережева безпека, ACL, NAT, Cisco Packet Tracer, Wi-Fi.

ANNOTATION

Viktorova Ya. Computer Network of a Medical Institution. Manuscript.

Qualifying work of a bachelor of EP «Computer Engineering» specialty 123 Computer Engineering. Lutsk National Technical University. Lutsk, 2026.

Qualification work consists of an introduction, three sections, conclusions, a list of references, and appendices.

The first section is devoted to the analysis of the task, where the design object is characterized, the main requirements for the computer network of the medical institution are determined, and the information resources and services are described.

The second section presents the technical and economic justification of the project: the choice of physical topology is substantiated, a comparative analysis of equipment options from different manufacturers is carried out, and the logical structure of the network is developed.

The third section is devoted to the practical implementation of the network and covers the selection of active network equipment, the calculation of logical addressing using VLSM, switching configuration (VLAN, trunk, STP), wireless access organization, inter-network interaction configuration using Inter-VLAN routing, HSRP and ACL, as well as the configuration of secure Internet access through NAT on Cisco ASA 5505.

Keywords: medical institution, VLAN, Inter-VLAN routing, HSRP, network security, ACL, NAT, Cisco Packet Tracer, Wi-Fi.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ 7
ВСТУП 8
РОЗДІЛ 1 АНАЛІЗ ВИМОГ ТА ІНФРАСТРУКТУРИ КОМП'ЮТЕРНОЇ МЕРЕЖІ МЕДИЧНОГО ЗАКЛАДУ 10
1.1 Характеристика об'єкта проєктування 10
1.2 Аналіз вимог до комп'ютерної мережі 19
1.3 Опис інформаційних ресурсів та служб 21
РОЗДІЛ 2 ТЕХНІКО-ЕКОНОМІЧНЕ ОБҐРУНТУВАННЯ ТА ВИБІР ЗАСОБІВ ПОБУДОВИ МЕРЕЖІ 25
2.1 Обґрунтування фізичної топології комп'ютерної мережі 25
2.2 Укрупнений розрахунок варіантів технічних засобів телекомунікацій 29
2.3 Структура комп'ютерної мережі 37
РОЗДІЛ 3 ПРОЄКТУВАННЯ, РОЗГОРТАННЯ ТА ТЕСТУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ 40
3.1 Вибір активного мережевого обладнання 40
3.2 Розрахунок логічної адреси 45
3.3 Комутація 49
3.4 Організація безпроводового доступу 55
3.5 Налаштування міжмережевої взаємодії 57
3.6 Організація доступу до Інтернету 60
3.7 Перевірка працездатності мережі 62
ВИСНОВКИ 69
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ 71

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ПК – персональний комп’ютер.

DTP (Dynamic Trunking Protocol) – динамічний протокол компанії Cisco для узгодження режиму роботи магістрального каналу.

ACL (Access Control List) – список контролю доступу.

OSI (Open Systems Interconnection) – базова еталонна модель взаємодії відкритих систем.

HSRP (Hot Standby Router Protocol) – протокол резервування шлюзу за замовчуванням з можливістю гарячої заміни.

STP (Spanning Tree Protocol) – протокол захисту від петель у мережах другого рівня).

Rapid PVST+ (Rapid Per-VLAN Spanning Tree Plus) – покращення протоколу STP, яке забезпечує швидку збіжність для кожної віртуальної мережі окремо.

VLAN (Virtual Local Area Network) – віртуальна локальна мережа.

SVI (Switched Virtual Interface) – логічний інтерфейс рівня 3, пов’язаний з конкретною VLAN.

VLSM (Variable Length Subnet Mask) – маска підмережі змінної довжини.

ВСТУП

Актуальність теми. Сучасний світ диктує власні правила та вимагає використання цифрових технологій у найрізноманітніших сферах. Значний вплив на роботу будь-якої компанії чинить цифровізація всіх її процесів, а медична галузь не є винятком. Оскільки перехід від паперового документообігу до медичної електронної системи, впровадження інформаційних систем, баз зберігання даних тощо потребують швидкого, надійного та високозахищеного каналу зв’язку, доцільно створити комп’ютерну мережу медичного закладу.

Цифровізація медичного закладу значно підвищує ефективність роботи установи, дозволяє швидко зберігати, обробляти та передавати дані, а також зменшує кількість помилок в документації. Зважаючи на те, що медичний заклад зобов’язаний зберігати конфіденційні дані пацієнтів, згідно з Законом України «Про захист персональних даних», необхідно забезпечити конфіденційність, цілісність та доступність інформації. Також значну увагу слід приділити безперервній роботі мережі, оскільки це критична умова для функціонування відділень (особливо операційних блоків) – навіть короткочасний збій може становити загрозу не лише здоров’ю пацієнтів, але й їхньому життю.

Оскільки існує критична потреба в комп’ютерній мережі для функціонування медичного закладу, а також вимога держави щодо забезпечення електронного обігу медичних даних, розробка комп’ютерної мережі для медичного закладу є актуальною.

Метою роботи є проєктування та розгортання сучасної комп’ютерної мережі для медичного закладу із врахуванням вимог до безпеки, продуктивності, надійності та масштабованості.

Об’єкт дослідження – комп’ютерна мережа медичного закладу.

Предмет дослідження – технології та методи проєктування, моделювання та конфігурування комп’ютерної мережі медичного закладу на базі обладнання Cisco.

Завдання, які необхідно виконати:

– описати об’єкт проєктування та проаналізувати функціональні й технічні вимоги до комп’ютерної мережі;

– підібрати оптимальну топологію мережі;

– розробити план VLAN-сегментування та IP-адресації з використанням технології VLSM (масок підмереж змінної довжини);

– здійснити обґрунтований вибір активного мережевого обладнання;

– провести повне налаштування та розгортання мережі;

– здійснити комплексну перевірку працездатності мережі медичного закладу на відповідність технічним вимогам та вимогам безпеки.

Практична цінність роботи полягає в тому, що розроблена мережа охоплює всі основні сучасні технології та методи побудови мережевої інфраструктури, а отже може бути використана як основа для проєктування реальної мережі медичного закладу подібного масштабу. Спроєктована модель забезпечує високий рівень відмовостійкості, ефективну сегментацію трафіку, базовий рівень безпеки, а також можливість подальшого масштабування без суттєвих перебудов та значних фінансових вкладень.

РОЗДІЛ 1
АНАЛІЗ ВИМОГ ТА ІНФРАСТРУКТУРИ КОМП'ЮТЕРНОЇ МЕРЕЖІ МЕДИЧНОГО ЗАКЛАДУ

1.1 Характеристика об'єкта проєктування

У даній кваліфікаційній роботі об'єктом проєктування виступає сучасний багаторівневий медичний центр, який розташований в межах чотирьох поверхів офісної будівлі. Дана структура є типовою для великих закладів. Оскільки кожен поверх має свій напрям, то потреби у трафіку та кількості пристроїв можуть певною мірою відрізнятись, однак вимоги до безпеки для всієї мережі однаково високі. Мережа медичного центру розміщена у межах лікувального закладу, що займає чотири поверхи. Далі детальніше розглянуто структуру та функції кожного поверху:

– перший поверх (розміщено приймальне та діагностичне відділення. Функція поверху: робота з пацієнтами, реєстрація та первинна діагностика/обстеження);

– другий поверх (розміщено амбулаторне відділення та палати. Функція поверху: лікування та спостереження за пацієнтами);

– третій поверх (розміщено операційних блок та відділ інтенсивної терапії. Функція поверху: критичні медичні процеси);

– четвертий поверх (розміщено адміністративний відділ лікарні та IT-інфраструктуру. Функція поверху: управління, документообіг, серверна інфраструктура).

Для розуміння того, де потрібно розміщувати мережеве обладнання і для яких потреб, – спроєктовано план кожного поверху медичного центру. На рисунках 1.1-1.2 представлено план першого поверху, який демонструє назву кабінетів, розташування приміщень та потребу кожного приміщення в устаткуванні.

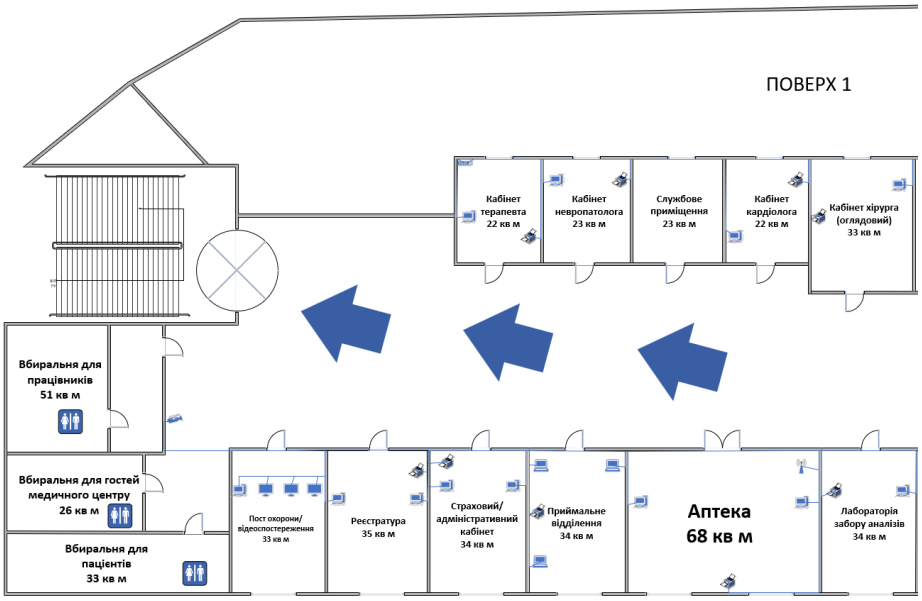

Рисунок 1.1 – Фрагмент лівої частини плану першого поверху медичного центру

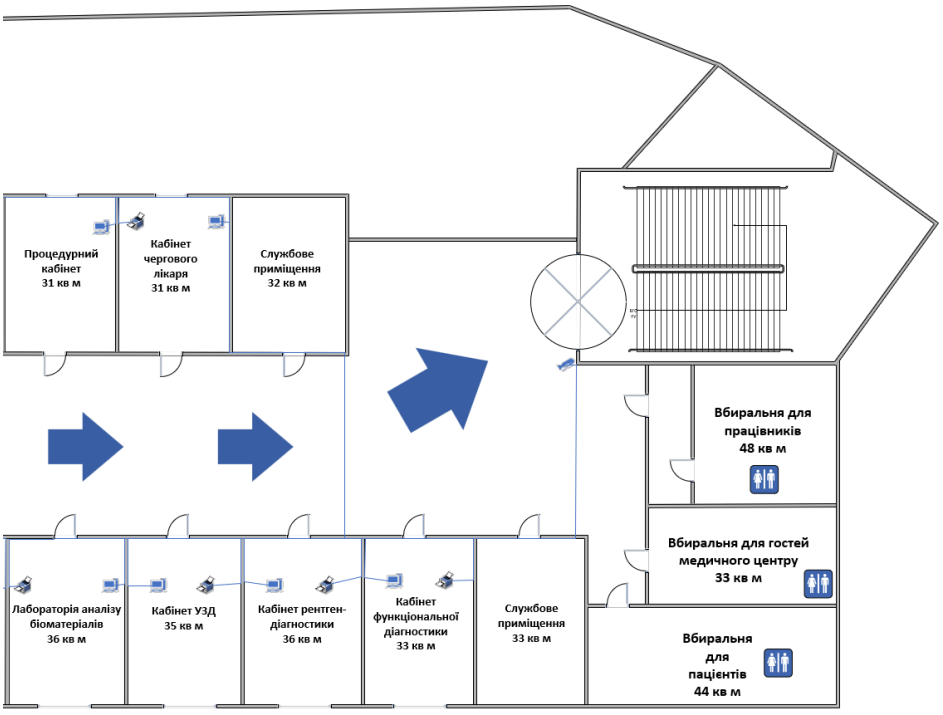

Рисунок 1.2 – Фрагмент правої частини плану першого поверху медичного центру

Оскільки на кожному поверсі є значна кількість приміщень (кабінети, палати, технічні кімнати, лабораторії, зали), в таблицях 1.1-1.2 наведено назву кожного приміщення по поверхах, а також їх площа та потреба в мережевих розетках RG-45.

Таблиця 1.1 – Перелік приміщень, їх площа та кількість мережевих розеток (поверх 1)

Номер кабінету	Найменування	Площа приміщення, м2	Кількість мережевих розеток
1	Пост охорони/відеоспостереження	33	3
2	Реєстратура	35	3
3	Страховий/адміністративний кабінет	34	3
4	Приймальне відділення	34	4
5	Аптека	68	4
6	Лабораторія збору аналізів	34	2
7	Лабораторія аналізу біоматеріалів	36	2
8	Кабінет УЗД	35	3
9	Кабінет рентген-діагностики	36	2
10	Кабінет функціональної діагностики	33	3
11	Службове приміщення	33	-
12	Кабінет терапевта	22	2
13	Кабінет невропатолога	23	2
14	Службове приміщення	23	-
15	Кабінет кардіолога	22	2
16	Кабінет хірурга (оглядовий)	33	3
17	Процедурний кабінет	31	1
18	Кабінет чергового лікаря	31	3
19	Службове приміщення	32	-

Таблиця 1.2 – Перелік приміщень, їх площа та кількість мережевих розеток (поверх 2)

Номер кабінету	Найменування	Площа приміщення, м2	Кількість мережевих розеток
1	Службове приміщення	33	-
2	Службове приміщення	35	-
3	Кімната відпочинку персоналу	34	4
4	Санітарна кімната персоналу	34	4
5	Пост медсестер	68	4
6	Перев’язочна	34	2
7	Маніпуляційна	36	2
8-9	Палати пацієнтів №4-5	35, 36	2
10	Службове приміщення	33	-
11	Службове приміщення	33	-
12	Службове приміщення	22	-
13	Кімната зберігання медикаментів	23	3
14	Кабінет завідувача відділенням	23	3
15	Кабінет лікуючого лікаря	22	3
16	Ординаторська	33	3
17-19	Палати пацієнтів	31, 31, 32	3

Рисунок 1.3 ілюструє планування другого поверху медичного закладу. На даному поверсі розміщено амбулаторне відділення та палати пацієнтів. Центральне місце займає пост медсестер площею 68 кв. м, який є основним координаційним вузлом поверху. Також на поверсі розташовано перев’язочну, маніпуляційну, ординаторську, санітарну кімнату персоналу та кімнату відпочинку персоналу. Палатний фонд поверху складається з п’яти палат для пацієнтів. Окрім цього, поверх містить низку службових приміщень та вбиральні для пацієнтів, персоналу та гостей медичного закладу. Наявність значної кількості приміщень різного функціонального призначення зумовлює необхідність організації надійного мережевого покриття на цьому поверсі.

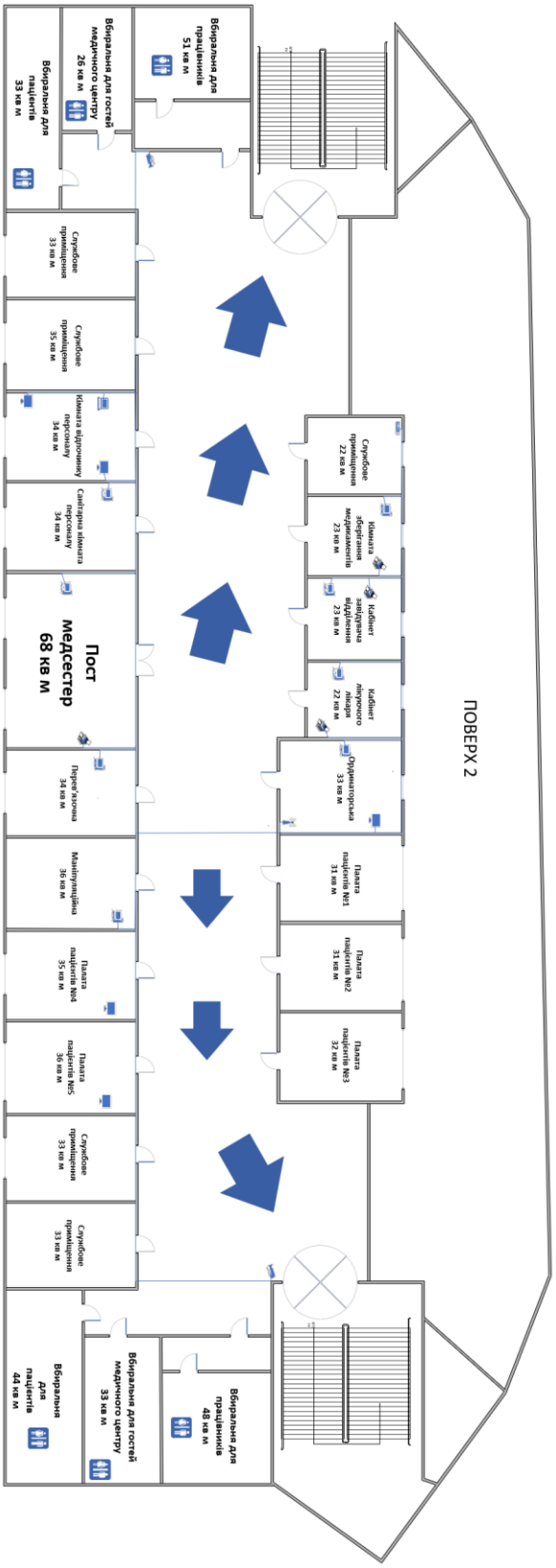

Рисунок 1.3 – План 2-го поверху медичного центру

В таблицях 1.3-1.4 представлено відомості про приміщення третього та четвертого поверхів медичного закладу.

Таблиця 1.3 – Перелік приміщень, їх площа та кількість мережевих розеток (поверх 3)

Номер кабінету	Найменування	Площа приміщення, м2	Кількість мережевих розеток
1	Службове приміщення	33	-
2	Стерилізаційна	35	2
3	Пост анестезіологів	34	2
4	Передопераційна	34	3
5	Операційно №1	68	4
6	Операційно №2	70	4
7	Реанімація	35	2
8	Післяопераційна палата	36	2
9	Службове приміщення	33	-
10	Службове приміщення	33	-
11	Кабінет зберігання обладнання	22	3
12	Технічне приміщення	23	-
13	Кімната чергування лікарів	23	3
14	Службове приміщення	22	-
15	Кімната медичного персоналу	33	5
16-18	Службові приміщення	31, 31, 32	-

Таблиця 1.4 – Перелік приміщень, їх площа та кількість мережевих розеток (поверх 4)

Номер кабінету	Найменування	Площа приміщення, м2	Кількість мережевих розеток
1	Службове приміщення	33	-
2	Навчальний клас	70	4
5	Конференц зал	140	5
6	Службове приміщення	36	-
7	Відділ кадрів	35	3
8	Юридичний відділ	36	3
9	Планово-економічний відділ	33	3
10	Службове приміщення	33	-

Продовження таблиці 1.4

Номер кабінету	Найменування	Площа приміщення, м2	Кількість мережевих розеток
11	Серверна	22	5
12	Архів	23	3
13	Бухгалтерія	23	3
14	Кабінет заступника головного лікаря	22	3
15	Кабінет головного лікаря	33	3
16	Офіс директора	31	3
17	Службове приміщення	31	-
18	Службове приміщення	32	-

Рисунок 1.4 відображає планування третього поверху медичного закладу із зазначенням назв кабінетів, розташування приміщень та їх потреби в мережевому обладнанні. На третьому поверсі розміщено операційний блок та відділення інтенсивної терапії, які є критично важливими для функціонування медичного закладу. Центральне місце поверху займають дві операційні площею 68 та 70 кв. м відповідно, які потребують безперебійного мережевого з’єднання. Також на поверсі розташовано стерилізаційну, пост анестезіологів, передопераційну, реанімацію та післяопераційну палату. Окрім цього, поверх містить кімнату медичного персоналу, кімнату чергування лікарів, кабінет зберігання обладнання та низку службових приміщень. Наявність критичних медичних підрозділів на цьому поверсі зумовлює підвищені вимоги до надійності та безперебійності роботи мережевої інфраструктури. Саме тому мережеве обладнання третього поверху виділено в окремий сегмент з обмеженим доступом та посиленими правилами безпеки. Будь-який збій мережі на цьому поверсі може мати критичні наслідки, тому під час проєктування особливу увагу приділено резервуванню каналів зв’язку та відмовостійкості мережевих з’єднань.

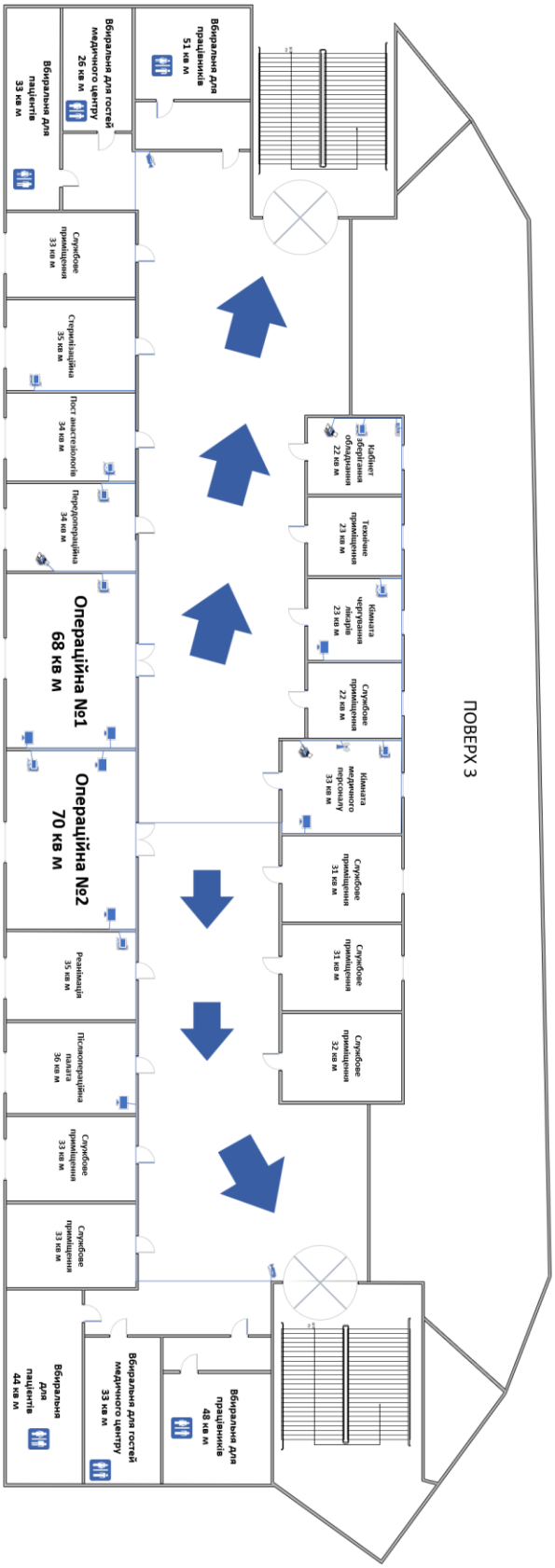

Рисунок 1.4 – План 3-го поверху медичного центру

На рисунку 1.5 зображено план четвертого поверху медичного закладу.

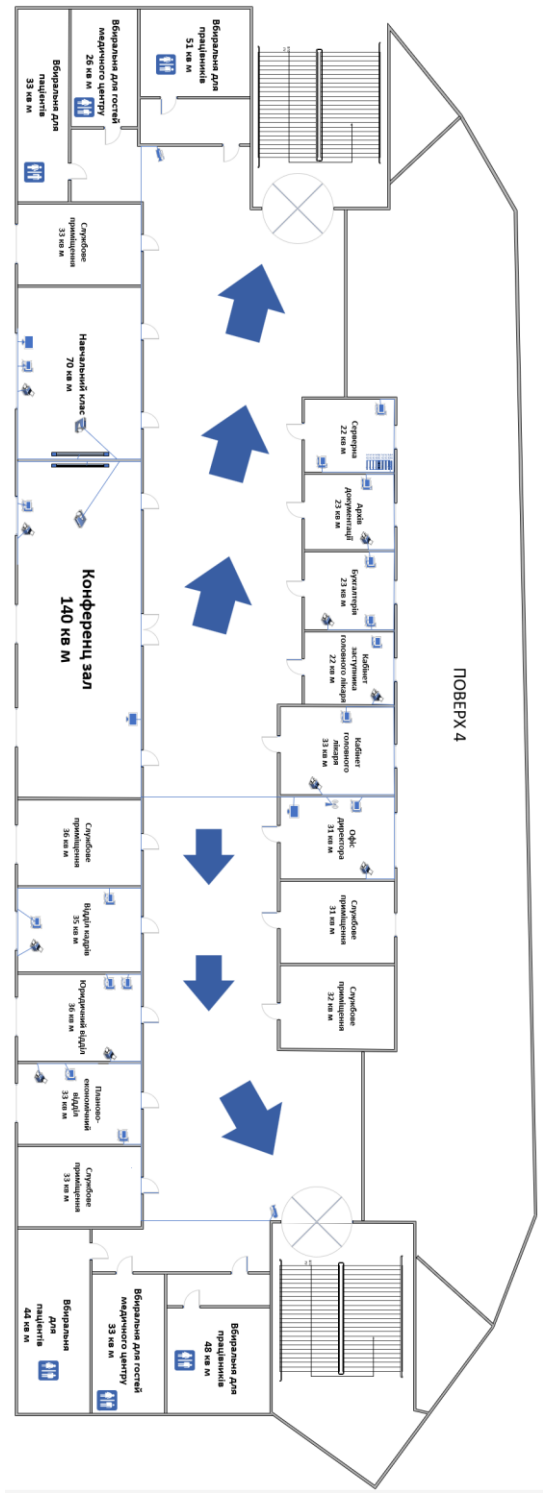

Рисунок 1.5 – План 4-го поверху медичного центр

1.2 Аналіз вимог до комп'ютерної мережі

Аналіз вимог до комп'ютерної мережі установи – це один з ключових етапів, бо саме на ньому визначать вимоги до проєктування сучасної мережі: технічні, функціональні та ті, які впливають на продуктивність та безпеку усієї інфраструктури. Оскільки мережу медичного центру можна віднести до критичної інфраструктури, то всі вимоги будуть проаналізовані відповідно до умов критичності специфіки роботи у медичному середовищі. Отже, до проєктованої мережі поставлені наступні вимоги:

– сегментація трафіку (це одна з найважливіших та найпотрібніших вимог, оскільки мережа медичного центру складається з чотирьох поверхів, які мають різне функціональне призначення. На першому поверсі домінуватиме трафік приймального та діагностичного відділення, на другому – трафік медичного персоналу та палатного відділення, на третьому поверсі повинна бути забезпечена критична робота сегменту мережі операційних та реанімації, а на четвертому – трафік адміністрації центру та робота серверної. Сегментація трафіку забезпечена за допомогою технології VLAN. Дана сегментація дозволить збільшити продуктивність (трафік різних підрозділів не перебуватиме в одному broadcast-домені) та забезпечити мінімізацію ризиків несанкціонованого доступу. Також завдяки використання сегментації трафіку можна спростити застосування політик безпеки);

– контроль доступу (ще одна не менш важлива вимога для проєктування безпечної мережі медичного центру. Оскільки в медичному центрі значна кількість людей: від медперсоналу до відвідувачів пацієнтів установи, то логічним є той факт, що не всі користувачі мають бути забезпечені однаковим доступ до ресурсів мережі. Наприклад, пацієнти, відвідувачі, гості медичного закладу, а також медперсонал повинен мати безпровідну мережу, з якої потрібно забезпечити доступ тільки до Інтернет мережі, але водночас заборонити доступ до будь-яких ресурсів

внутрішньої мережі центру, окрім сайту установи. Також потрібно забезпечити ізоляцію системи відеоспостереження від усіх користувачів, однак дозволити цьому сегменту здійснювати запис відеоматеріалів на файловий сервер. Не менш важливим є забезпечення обмеженого доступу до сегменту мережі операційних та реанімації. Отже, контроль доступу між VLAN-сегментами повинен забезпечуватиметься за допомогою розширених ACL – списків контролю доступу);

– надійність мережі (третя важлива вимога для проєктування сучасної та надійної мережі медичного центру. Оскільки мережа повинна працювати цілодобово, то потрібно забезпечити швидке перемикання лінків в мережі при відмові основного каналу зв'язку за допомогою протоколу Rapid Per-VLAN Spanning Tree. Також для виключення атак типу VLAN hopping – потрібно вимикати на портах комутаторів Dynamic Trunking Protocol (для портів доступу обов'язково, а для магістральних – як рекомендація для стабільності мережі). Для забезпечення запобігання створення петель (як випадкових, так і у зловмисницьких цілях) – на портах доступу вмикати PortFast і BPDU). Щоб забезпечити максимальну відмовостійкість мережі – потрібно використати другий (резервний) core-комутатор, який працювати поруч з основним в режимі HSRP (об'єднання двох комутаторів ядра у віртуальний шлюз));

– масштабованість (як і будь-яке підприємство та установа – медичний центр розвивається, а отже потрібно забезпечити можливість для будь-якого виду масштабування. Одним з напрямів розвитку може бути встановлення IoT-пристроїв для моніторингу критичних показників тяжких пацієнтів. Також з часом з'явиться потреба в додаткових робочих місцях та необхідність у розширенні палатного фонду. Для забезпечення виконання цих вимог потрібно використати комутатори для access-рівня з 48 портами, також виконати розподіл адрес у сегментах мережі за допомогою технології VLSM (змінних масок). Використання даної технології дозволить забезпечити достатній резерв адрес для майбутнього розширення та надасть зможу масштабувати мережу без потреби у глобальній перебудові наявної);

– доступ до мережі Інтернет (п’ята важлива вимога при проєктування будь-якої сучасної мережі. Медичний центр повинен мати не просто вихід у мережу Інтернет, а саме: безпечний вихід. Для забезпечення виконання такої вимоги потрібно здійснити організований доступ до глобальної мережі через фаєрвол Cisco ASA 5505, за допомогою якого налаштовані рівні довіри та дозволити доступ тільки для потрібного трафіку ззовні. Також завдяки використанню фаєрвола потрібно організувати доступ до Інтернету для всієї локальної мережі через одну адресу з використанням технології трансляції адрес PAT);

– розгортання безпровідних мереж (оскільки медичному персоналу, пацієнтам та відвідувачам потрібен доступ до мережі Інтернет з власних пристроїв, то є вимога для створення захищеної безпровідної мережі. Мережу винесено в окремий сегмент (VLAN) та організовано спільний доступ для всіх категорій користувачів. Однак, вона повинна мати обмеження: доступ тільки до мережі Інтернет та вебсайту медичного центру. Є потреба у розгортанні точок безпроводового доступу Wi-Fi на кожному поверсі, а для мінімізації кабельної структури – живлення потрібно забезпечити від комутаторів рівня доступу).

Отже, проаналізувавши наведені вимоги слід зазначити, що виконання поставлених вимог дозволить забезпечити не тільки технічно-правильну роботу мережі, але також дозволить відповідати всім сучасним стандартам безпеки та ефективності.

1.3 Опис інформаційних ресурсів та служб

Інформаційні ресурси та служби – це основа будь-якої сучасної мережі, а для медичного центру – це як зберігання даних, так і обмін ними в режимі реального часу. Оскільки медичний центр є багаторівневим та складається з великої кількості підрозділів, то його медичні служби мають бути не тільки доступними, але також захищеними та інтегрованими в єдину систему. Для запобігання витоку

персональних даних та будь-яких затримок в мережі – всі служби будуть розміщені в окремому сегменті мережі (VLAN 70) та матимуть власні політики доступу. Існують базові інфраструктурні служби, без яких неможлива робота будь-якої мережі. Якщо йде мова про мережу сучасного медичного центру, то до таких служб належать DHCP, DNS та FTP.

DHCP-сервіс (Dynamic Host Configuration Protocol) – служба, яка забезпечує автоматичне призначення мережевих даних (IP-адреси, маски та шлюзу) усім кінцевим пристроям в мережі (винятком слугуватимуть пристрої, яким потрібні постійні IP-адреси). Оскільки у медичному центрі є значна кількість пристроїв, а їх кількість може легко досягати 150 одиниць (це як ПК, IP-камери, так і безпровідні пристрої, які підключені до точок доступу Wi-Fi), то ручне налаштування кожного пристрою є незручним та неприйнятним. Даний DHCP-сервер розміщений у сегменті VLAN 70 та йому призначена власна статична адреса. Для всіх інших підмереж також використовуватиме автоматичне призначення адрес за допомогою даного сервера. Зважаючи на те, що кожна підмережа містить певний резерв адрес, то додавання обладнання та масштабування відділів пройде з максимальною простотою та легкістю. Достатньо підключити пристрій у порт комутатора, який належить до потрібної VLAN та натиснути одержати автоматичні мережеві налаштування. Після цього новий ПК готовий до роботи [1].

DNS-сервіс (Domain Name System) – це служба, яка відповідає за перетворення імен ресурсів, які зрозумілі для користувачів, на IP-адреси. У існуючій мережі медичного центру даний сервіс повинен забезпечити розпізнання імен медичної інформаційної системи (HIS/EMR), а також FTP-серверу тощо. Даний підхід є надзвичайно затребуваним, оскільки медичний персонал не повинен запам’ятовувати IP-адреси. Коли дехто з медичного персоналу вводитиме ім’я домену, наприклад, google.com, щоб потрапити в мережу Інтернет, то виконуватиметься ряд кроків [2]:

– браузер перевіряє файл hosts.txt на пристрої, з якого набрано google.com. За

умови, що там відсутня IP-адреса, – браузер звертається до локального DNS-сервера (у моєму випадку DNS-сервера медичного центру). IP-адреса цього DNS-сервера автоматично знаходиться в мережевих налаштуваннях кожного пристрою, яку вони отримали від DNS-сервісу;

– локальний DNS може не знати IP-адресу особисто, тому він також може обмінюється інформаційними даними з іншими DNS-серверами: поки браузер чекає на відповідь – локальний DNS виконує власне звернення до ключових серверів у світі (кореневих DNS-серверів). У власному зверненні локальний DNS-сервер просить IP-адресу для google.com. Коренений DNS-сервер також не знає адреси google.com, однак він знає IP-адреси серверів DNS, які відповідають за зони, що знаходяться в зоні .com;

– після того як локальний DNS-сервер отримає IP-адресу одного з DNS-серверів (який відповідає за зону .com), то він їм задає таке ж питання, яке задавав попереднім. Оскільки даний DNS-сервер теж не знаєш IP-адреси даного пошукового вебсайту google.com, але знає IP-адреси DNS-серверів, що використовує google.com, і надає їх [3];

– далі локальний DNS-сервер звертається до однієї з IP-адрес нового DNS-сервера, а він уже знає потрібну IP-адресу та відправляє її;

– локальний DNS-сервер у свою чергу відправляє дану IP браузеру;

– браузер, який отримав IP-адресу вебсайту google.com, уже звертається до нього з прохання відправити сайт.

Файловий сервер (FTP) – це служба, яка виконує роль сховища як документів установи, так і архівів, бекапів чи записів з камер спостережень [4]. Розгорнутий централізований файловий сервер використовуватиметься як адміністративними працівниками, так і медичним персоналом. Також на даному FTP розгорнута централізована система резервного копіювання даних. Дана система повинна автоматично створювати копії баз даних медичної інформаційної системи (HIS/EMR, на базі вебсерверу) та інших критичних даних медичного центру.

Резервне копіювання налаштоване за деяким графіком: щоденне мінімально потрібне та щотижневе повне.

Найважливішим та ключовим ресурсом медичної мережі центру становитиме медична інформаційна система (HIS/EMR). Вона працюватиме на базі вебсерверу (HTTPS) та надаватиме можливість медичному персоналу вести медичні картки, призначати обстеження, виписувати рецепти, а також вести обмін даними між відділами, лабораторіями та аптекою. Доступ до цієї системи можна отримати з веббраузера, ввівши medcenter в пошуковий рядок. Увійти на вебсайт зможуть всі користувачі медцентру: як пацієнти, так і медичний персонал. Однак для отримання функцій медичного персоналу – потрібно ввійти у власний обліковий запис. Пацієнти ж у свою чергу зможуть переглядати розроблене для них лікування (при власній авторизації) та замовляти додаткові послуги, які пропонує медичний центр. Інформаційна медична система мусить бути високодоступною, тому вона розмішена на серверах медичного центру, містить регулярне резервне копіювання та забезпечена резервним живленням. Оскільки медична інформаційна система знаходиться на сервері 2 та у VLAN 70, що у серверному приміщенні, то для захисту даних будуть застосовані жорсткі ACL: пацієнти матимуть доступ лише до сайту вебсистеми, тоді як доступ до інших ресурсів для них повністю обмежений (окрім мережі Інтернет).

Також у комп’ютерній мережі медичного центру розгорнена система відеоспостереження (CCTV). Вона складається з робочих станцій охорони та IP-камер. Запис з даних камер будуть зберігатись на файловому сервері медичного центру. Оскільки камери записують інформацію, яка не призначена для будь-кого, то даний ресурс повністю ізольований у власному сегменті (VLAN 80). Однак для зберігання записів з IP-камер йому наданий доступ лише до FTP-серверу.

РОЗДІЛ 2
ТЕХНІКО-ЕКОНОМІЧНЕ ОБҐРУНТУВАННЯ ТА ВИБІР ЗАСОБІВ ПОБУДОВИ МЕРЕЖІ

2.1 Обґрунтування фізичної топології комп’ютерної мережі

Вибір фізичної топології будь-якої комп’ютерної мережі є не тільки важливим, але й потрібним етапом, тому що топологія має значний вплив, як на надійність мережі, так і на масштабованість, продуктивність та зручність в майбутньому обслуговуванні. Мережа медичного центру належить до критичної інфраструктури, тому допущення помилок під час вибору фізичної топології є недопустимим, оскільки це може привести до втрати даних, зниження рівня безпеки, а також тривалого простою мережі при будь-яких збоях. Отже, для проєктування комп’ютерної мережі медичного центру проведено порівняльний аналіз ключових типів фізичних топологій. Даний аналіз проведено з урахуванням специфіки медичного центру, а саме: значної щільності пристроїв на кожному поверсі, забезпечення максимальної доступності в роботі медичної інформаційної системи тощо.

Існує декілька варіантів топологій, а кожна із них має як свої переваги, так і недоліки. Надалі всі вони будуть оцінені за критеріями масштабованості, надійності, вартості та простоти в обслуговуванні, а також швидкості відновлення після збоїв. Отже, будуть розглянуті наступні фізичні топології: зірка (повна), розширена зірка (часткова), топологія кільце, шина, сітка (mesh), а також ієрархічна (трирівнева). На рисунку 2.1 представлено схематичний вигляд кожної топології [4, 5].

Топологія повної зірки – це така топологія мережі, в якій кожен пристрій має власне підключення до центрального комутатора (або хабу). Хоча дана топологія забезпечує максимальну продуктивність та простоту, однак вона не підходить до

мережі медичного центру, оскільки на її побудову витрачена значна кількість кабельної структури, яка не забезпечить наявність резервного зв’язку.

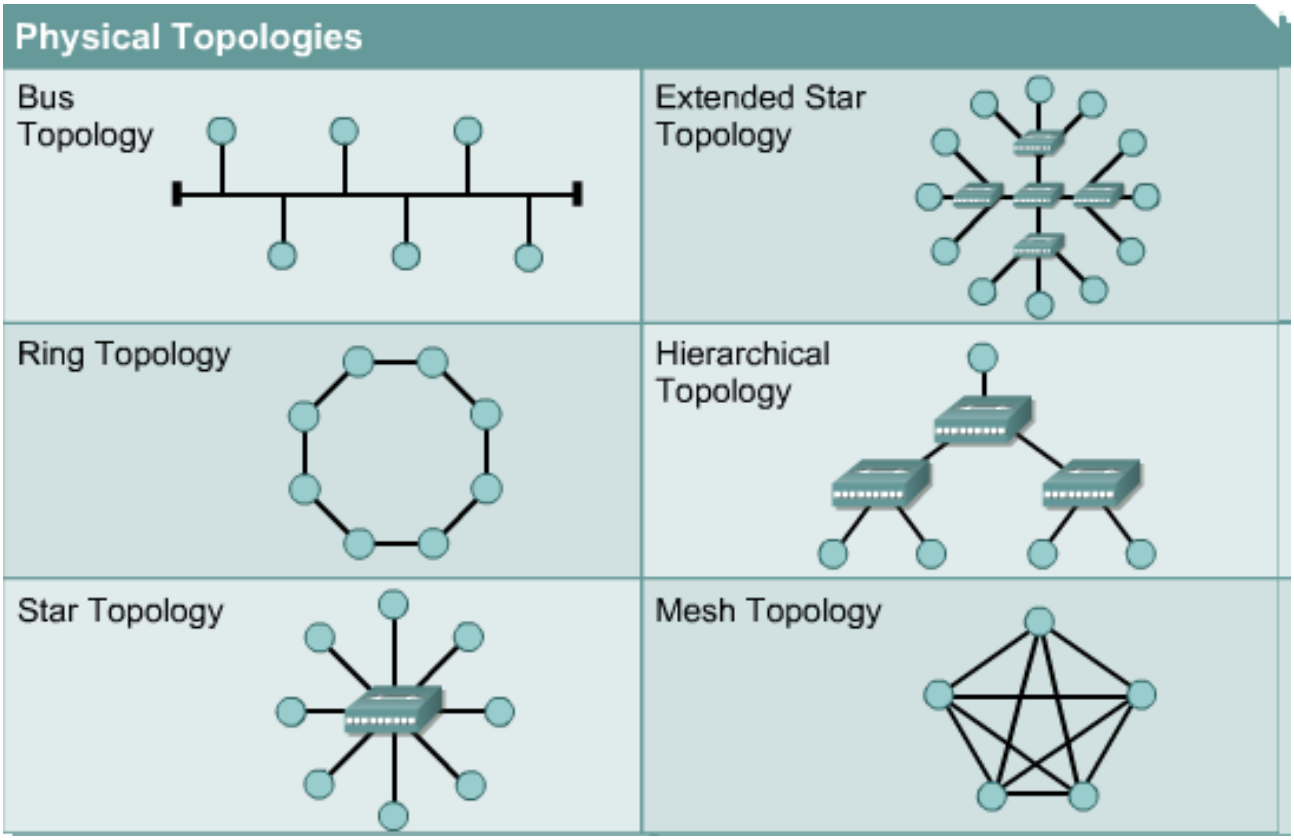

Рисунок 2.1 – Класичні варіанти фізичних топологій мереж [5]

Топологія кільце – належить до топології, яка забезпечує як хорошу відмовостійкість, так і ускладнене управління мережею. Також у даній мережі повільно проводиться відновлення під час різного роду збоїв та неполадок.

Топологія шина є застарілою на сьогоднішній час. Дана топологія уже не відповідає ніяким сучасним вимогам, оскільки вона характеризується низькою відмовостійкістю, а також присутністю проблем з колізіями.

Топологія типу сітка – це топологія, яка забезпечує максимальний рівень надійності, однак вона є дороговартісною. Також використання цієї топології в мережі медичного центру є складним.

Отже, найбільш практичною та доцільною для використання у сучасних кампусних та корпоративних мережах, до яких також відносять і медичні мережі, є топологія ієрархічної розширеної зірки. Під час використання даної топології мережу ділять на наступні рівні [6]:

– Core Layer (рівень ядра. У даній комп'ютерній мережі медичного центру на цьому рівні працюватимуть два високопродуктивні multilayer-комутатори. Вони повинні забезпечити централізоване керування усім трафіком, який протікає мережею, за допомогою технологій: Inter-VLAN routing, HSRP та ACL);

– Access Layer (рівень доступу. На цьому рівні працюватимуть чотири комутатори у кількості один на поверх, які забезпечуватимуть підключення до кінцевих користувачів: бездротові точки доступу, ПК, принтери, IP-камери тощо).

Для забезпечення максимальної швидкодії та ефективності медичної мережі між рівнем доступу та ядра будуть організовані з'єднання за допомогою trunk-лінків Gigabit Ethernet. Комутатори рівня ядра будуть розміщенні у серверній шафи, яка знаходитиметься на четвертому поверсі приміщення серверної. Таке розміщення дозволяє спростити обслуговування мережі сервісного центру, а також мінімізувати довжину кабельної структури мережі.

Вибір фізичної топології на користь ієрархічної розширеної зірки містить наступні ключові переваги:

– забезпечує високу надійність та відмовостійкість мережі (оскільки в мережі використано два core-комутатори, які працюватимуть у режимі HSRP, то даний підхід дозволить забезпечити швидке автоматичне перемикання шлюзів у разі виходу основного. Також використана технологія Rapid PVST+, яка гарантуватиме швидке відновлення зв'язку при відмові будь-якого з'єднання);

– забезпечує відмінну масштабованість (даний підхід до проєктування комп'ютерної мережі медичного центру дозволить додавати нові пристрої без перебудови існуючої мережі. Навіть під час масштабування медичного центру до п'яти поверхів достатньо просто підключити новий комутатор рівня доступу до

комутаторів рівня ядра та провести мінімальні доналаштування);

– централізоване керування (оскільки всі основні налаштування проводяться на комутаторах рівня ядра, то це значно спрощує адміністрування мережі ІТ-спеціалістами);

– оптимальне використання коштів (завдяки правильному розподілу кабінетів по поверхах та вірно підібраній фізичній топології можна використовувати по одному 48-ми портовому комутатору рівня доступу на кожен поверх. Даний підхід значно економить бюджет при побудові мережі, оскільки зменшує потребу в кількості активних пристроїв, а також дозволяє залишити резерв портів для масштабування).

Якщо брати у порівняння ієрархічну розширену зірку з іншими топологіями, то розширена зірка на відміну від топології кільце не має ніяких проблем із затримками проходження трафіку, а також має кращі швидкості при відновленні (перебудові мережі). А якщо брати у порівняння розширену зірку та топологію типу сітка, то перша набагато дешевша не тільки в реалізації, а також і в обслуговуванні.

Отже, у рамках даної кваліфікаційної роботи фізична топологія мережі реалізована наступним чином: у серверній розміщено два комутатори рівня ядра (перший основний, а другий резервний), які з’єднані між собою для надійності. На кожному поверсі розміщено по одному комутатору рівня доступу, які мають по два trunk-лінки. Перший проведено до основного комутатора рівня ядра, а інший – до резервного. Такий підхід дозволить забезпечити максимальну надійність та відмовостійкість. Для проведення усіх кабельних з’єднань використовуватиметься вита пара категорії 6А, яка забезпечить не тільки високу швидкість до 10 Гбіт/с, а також гарантуватиме PoE+ для живлення як бездротових точок доступу Wi-Fi, так і IP-камер.

2.2 Укрупнений розрахунок варіантів технічних засобів телекомунікацій

Комп’ютерна мережа медичного центру складатиметься із великої кількість підрозділів, а отже вони будуть винесені у власні підмережі (VLAN). Під час проєктування мережі потрібно передбачити взаємодію (Inter-VLAN routing) між сегментами (підмережами), тому для виконання такого роду зв’язку потрібен пристрій 3-го рівня OSI: L3-комутатор чи маршрутизатор. З цього випливає, що існує два підходи для міжмережевої взаємодії: Router-on-a-Stick (маршрутизатор, який має один фізичний інтерфейс та підінтерфейси) та Layer 3 Switch (комутатор з використанням SVI (Switched Virtual Interfaces)) [7].

Перший підхід (Router-on-a-Stick) є простішим під час реалізації, але для проєктування комп’ютерної мережі медичного центру він не підходить через суттєвий недолік. Оскільки під час проєктування мережі Router-on-a-Stick вся маршрутизація реалізується тільки завдяки одному фізичному інтерфейсу, то при значному обсягу мережевих даних – дане місце стає проблемним: виникає значна затримка та проблеми продуктивності. Також при відмові такого маршрутизатора вся мережа розпадається та втрачає зв’язок.

Другий підхід (Layer 3 Switch) здатен забезпечити значну продуктивність, оскільки кожен віртуальних інтерфейс (SVI) маршрутизується безпосередньо на комутаторі. Це найсучасніших та найшвидший підхід, який забезпечує максимальну продуктивність, бо трафік не покидає комутатор під час маршрутизації. Оскільки у процесі проєктування комп’ютерної мережі медичного центру передбачено використання резервного L3 Core Switch, то даний підхід є пріоритетний – при виході з ладу основного – другий (резервний) комутатор зразу перейме його функції.

Для виконання всіх поставлених вимог для мережі медично центру потрібне відповідне апаратне устаткування. Згідно завдання, до мережі входитимуть наступні критичні пристрої:

– міжмережевий екран (Firewall);

– два комутатори 3 рівня (Core Layer);

– чотири комутатори 2 рівня (Access Layer);

– чотири бездротові точки доступу (WiFi);

– вісім IP-камер.

Обране мережеве устаткування повинно підтримувати всі затребувані функціональні потреб, безпекові функції, також технологію PoE. Отже, для виконання порівняльного аналізу обрано обладнання світового мережевого лідера Cisco та значно дешевшого виробника обладнання MikroTik.

Обрано наступні фаєрволи для порівняння (табл. 2.1):

– Cisco ASA 5505;

– MikroTik RB4011iGS+ (містить функції міжмережевого екрану).

Таблиця 2.1 – Порівняльна характеристика міжмережевих екранів [8, 9]

Пристрій	Cisco ASA 5505	MikroTik RB4011iGS+
Тип	Міжмережевий екран	Маршрутизатор (з функцією Firewall)
Процесор, ОЗП, Flash	AMD Geode LX, 500 МГц, 256 MB, 128 МБ	AL21400 1,4 ГГц 4 ядра, 1 GB, 512 MB
Інтерфейси	6 x 100Base-TX - RJ-45 2 x 100Base-TX (PoE) - RJ-45 3 x USB 2.0 - Type A 1 x management - RJ-45	10 x 10/100/1000 Ethernet, 1 x SFP+ 1 x Serial port RJ45
Особливості	Firewall throughput: 150 Mbps VPN throughput: 100 Mbps	Підтримка PoE, Підтримка VPN, Підтримка L2TP, DHCP, NAT
NAT / PAT	Апаратний	Програмний
Розміри	20 x 17,4 x 4,4 см	22,8 x 12 x 3 мм
Вага	1,8 кг	0,85 кг

Проаналізувавши таблицю 2.1 можна зробити висновок, що Cisco ASA 5505 (рис. 2.2) хоч і поступається швидкістю сучасному MikroTik RB4011iGS+, однак він

повноцінний міжмережевий екран і справлятиметься з цією функцією краще. Медичний центр хоч і має потребу в мережі Інтернет, однак більшість його трафіку «ходитиме» у внутрішніх частині мережі, тому швидкість 150 мбіт/с є достатньою для зовнішнього виходу у глобальну мережу.

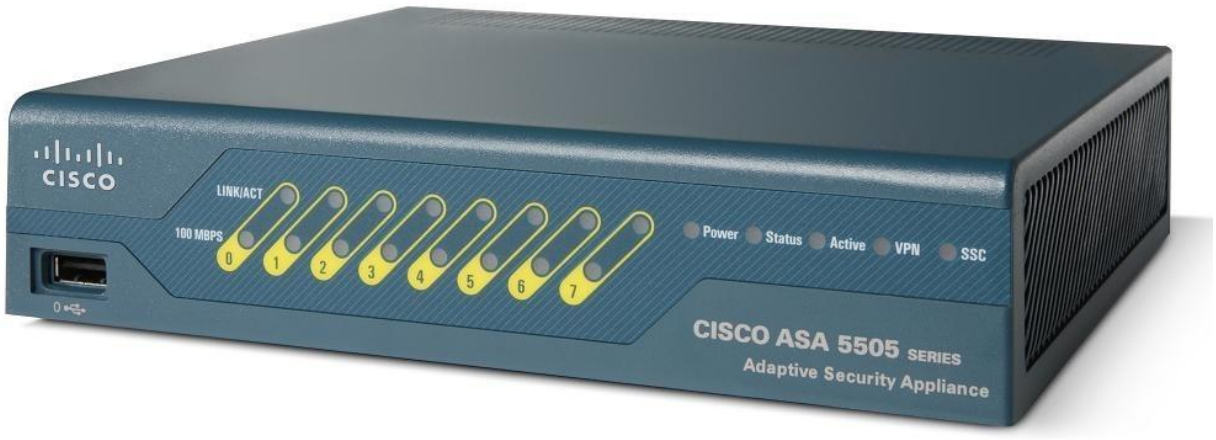

Рисунок 2.2 – Міжмережевий екран Cisco ASA 5505 [8]

Для порівняльного аналізу комутаторів рівня ядра обрано Cisco Catalyst WS-C3650-24PD-S та MikroTik CCR2004-16G-2S+. Детальні характеристики даних комутаторів наведено в таблиці 2.2.

Таблиця 2.2 – Порівняльна характеристика комутаторів рівня ядра [10, 11]

Пристрій	Cisco Catalyst WS-C3650-24PD-S	MikroTik CCR2004-16G-2S+
Тип	Multilayer L3 Switch	Маршрутизатор з L3 функціями
ОЗП, Flash	4 ГБ, 2 ГБ	4 ГБ, 128 МБ
Підтримка HSRP/VRRP	Повна (HSRP v2)	VRRP (обмежена)

Продовження таблиці 2.2

Пристрій	Cisco Catalyst WS-C3650-24PD-S	MikroTik CCR2004-16G-2S+
ACL на апаратному рівні	Так	Ні
Інтерфейси	24 x Ethernet 10/100/1000 PoE+ 2 x 10G Uplink SFP+ і 2 x 1G Uplink SFP або 4 x 1G Uplink SFP 1 x USB 1 x консольний порт RJ-45	16 x 1 Гбіт/с Ethernet 2 x SFP+ порт (підтримуються SFP модулі 1.25G і 10G) 1 × повнорозмірний USB 3.0 для підключення 3G/4G модему або зовнішнього накопичувача 1 x serial console port RJ45
Особливості	підтримка PoE протоколи маршрутизації PIM-SM; PIM-DM; IS-IS; RIP; OSPF; BGP; PIM; EIGRP розмір таблиці MAC адрес 32000	відсутність підтримки PoE протоколи маршрутизації PIM-SM; PIM-DM; IS-IS; RIP; OSPF; BGP; PIM розмір таблиці MAC-адрес 16000
Розміри	4,4 x 44,5 x 44,8 см	44,3 x 21 x 4,4 см
Вага	7,26 кг	2,52 кг

Проаналізувавши таблицю 2.2 можна зробити висновок, що Cisco Catalyst WS-C3650-24PD-S (рис. 2.3) краще підійде у якості ядра мережі, оскільки він дозволить забезпечити маршрутизацію між VLAN з мінімальною затримкою, а також має апаратну обробку ACL.

Рисунок 2.3 – Комутатор 3 рівня Cisco Catalyst WS-C3650-24PD-S

Для порівняльного аналізу комутаторів рівня доступу обрано Cisco Catalyst 2960X-48FPS-L та MikroTik CRS354-48P-4S+2Q+RM. Детальні характеристики даних комутаторів наведено в таблиці 2.3.

Таблиця 2.3 – Порівняльна характеристика комутаторів рівня доступу [12, 13]

Пристрій	Cisco Catalyst 2960X-48FPS-L	MikroTik CRS354-48P-4S+2Q +RM
Тип	Ethernet Switch	Ethernet Switch
ОЗП, Flash	512 МБ, 128 МБ	64 МБ, 16 МБ
Керування мережею	Керований	Керований
Підтримка Rapid PVST+	Rapid PVST+	Обмежена
Максимальна кількість активних VLAN	1023	До 4096
Таблиця MAC-адрес	4096	32000
Інтерфейси	4 8x 10/100/1000 Gigabit Ethernet 4 x 1 Gb SFP	48 x 10/100/1000 Mbit/s Ethernet with Auto-MDI/X 1 x 10/100 Mbit/s Ethernet with Auto-MDI/X for management 4 x 10G SFP+ port (підтримуються модулі 1,25G SFP і 10G SFP+) 2 x 40G SFP+ port, 1 x serial port RJ45
Особливості	SSH, SSL, SCP; RADIUS, TACACS+; SNMPv3; 802.1X (Accounting, MAB, Voice/Guest/Dynamic VLAN); BPDU/Root guard; Port security; Private VLAN edge; Storm control; Block unknown unicast/multicast; IGMP snooping/filter	SSH, SSL, SCP; RADIUS, TACACS+; SNMPv3; 802.1X (Accounting, Dynamic VLAN, MAB); BPDU/Root guard; Loop protect; Port security; Bridge Horizon (Private VLAN); Storm control; Block unknown unicast/multicast; IGMP snooping/filter; HW Offloaded L3 (OSPF, BGP); Dual Boot (RouterOS/SwOS); PoE-out monitoring
Розміри	4,5 x 27,9 x 44,5 см	44,3 x 38,2 x 4,4 см

Продовження таблиці 2.3

Пристрій	Cisco Catalyst 2960X-48FPS-L	MikroTik CRS354-48P-4S+2Q +RM
Вага	4,2 кг	6,45 кг

Проаналізувавши табл. 2.3 можна зробити висновок, що Cisco Catalyst 2960X-48FPS-L (рис. 2.4) краще підійде у якості комутатора рівня доступу, оскільки він має розвинену систему безпеки, а також краще себе демонструє в умовах сумісності.

Рисунок 2.4 – Комутатор 2 рівня Cisco Catalyst 2960X-48FPS-L

Для порівняльного аналізу бездротових точок доступу WiFi обрано Cisco AIR-AP1852I-E-K9 та MikroTik cAP ax. Детальні характеристики даних точок доступу наведено в таблиці 2.4.

Таблиця 2.4 – Порівняльна характеристика бездротових точок доступу WiFi [14, 15]

Пристрій	Cisco AIR-AP1852I-E-K9	MikroTik cAP ax
Тип	Точка доступу	Точка доступу
Покоління	Wi-Fi 5	Wi-Fi 6
Діапазон частот	2,4/5 ГГц	2,4/5 ГГц
Тип антен	Вбудовані	Вбудовані

Продовження таблиці 2.4

Пристрій	Cisco AIR-AP1852I-E-K9	MikroTik cAP ax
К-сть антен	4	4
Потужність передатчика	23 дБм	24 дБм
Порти	3xRJ-45, USB	2x 1000 Мбіт/с RJ-45
Напруга живлення	44-57 В	18-57 В (DC jack), 18-57 В (PoE-In)
Розміри	21 x 21 x 5 см	22,8 x 4,4 см
Вага	1,41 кг	1,2 кг

Проаналізувавши таблицю 2.4 можна зробити висновок, що Cisco AIR-AP1852I-E-K9 (рис. 2.5) краще підійде у якості бездротових точок доступу WiFi, оскільки дана модель має кращу систему керування та повну інтеграцію з enterprise-інфраструктурою Cisco. Також ці точки доступу WiFi краще зарекомендували себе в умовах великої щільності користувачів, що якраз характерно для медичного центру.

Рисунок 2.5 – Бездротова точка доступу WiFi Cisco AIR-AP1852I-E-K9

Для порівняльного аналізу IP-камер обрано Cisco Meraki MV72-HW та Hikvision DS-2CD2143G0-I (оскільки MikroTik не виробляє готові IP-камери). Детальні характеристики даних IP-камер наведено в таблиці 2.5.

Таблиця 2.5 – Порівняльна характеристика IP-камер [16, 17]

Пристрій	Cisco Meraki MV72-HW	Hikvision DS-2CD2143G0-I
Тип	Вулична, внутрішня	Вулична, внутрішня
Тип оптичного сенсора	CMOS - 1/3" - 4 MP	1/3 Progressive Scan CMOS
Максимальне розширення	1920 x 1080	2560x1440
Оптичний зум	3x	-
Фокусна відстань	3-9 mm	6 mm
Технології з’єднання	Wired, wireless	Wired
Діапазон частот	2,4/5 ГГц	-
Відеокомпресія	H.264	H.264, H.264+, H.265+, MJPEG, H.265
Регулювання по осях	нахил: 65°, обертання: +/- 90°, панорамування: 354 °	поворот: 0° - 355°, нахил: 0° - 75°, обертання: 0° -355°
Дальність підсвітки	30 м	30 м
Мережеві інтерфейси	Ethernet 10Base-T/100Base-TX/1000Base-T	1 RJ45 10M/100M Ethernet
Живлення	PoE	DC 12 В± 25%, PoE (802,3af)
Розміри	16,5 x 10,3 см	11,1 x 8,24 см
Вага	1,247 кг	0,61 кг

Проаналізувавши таблицю 2.5 можна зробити висновок, що Cisco Meraki MV72-HW (рис. 2.6) краще підійде у якості IP-камери, оскільки вона повністю інтегрується в єдину мережеву інфраструктуру та відповідає найвищому рівню кібербезпеки. Також як і все обладнання Cisco – Meraki MV72-HW характеризується високою стабільністю роботи та надає можливості централізованого хмарного керування через Meraki Dashboard.

Рисунок 2.6 – IP-камера Cisco Meraki MV72-HW

2.3 Структура комп’ютерної мережі

Розробка логічної структури комп’ютерної мережі медичного центру є надзвичайно важливою у ході проєктування. Саме на цьому етапі визначають права доступу між різними функціональними підрозділами, які існують в рамках медичної установи. Також правильно організована структура дозволяє уникнути перевантаження та спрощує як обслуговування, так і діагностику мережі.

Логічна структура мережі побудована на базі технології VLAN. Кожен поверх медичної установи містить найрізноманітніші за своїм функціональним призначення приміщення, що у свою чергу потребувало б значною кількості підмережі (VLAN). Оскільки більшість приміщень тісно пов’язані з іншими, тобто виконують подібні завдання та мають обмінюватись спільними даними, то прийнято рішення здійснити їх групування. Отже, після групування сформовано 11 підмереж, які згодом будуть призначити у наступні VLAN:

– VLAN10 (Reception/Administration, входить приймальне відділення, реєстратура, страховий/адміністративний кабінет, аптека);

– VLAN 20 (Diagnostics, входять лабораторії забору аналізів, кабінети УЗД, рентген-діагностики, функціональної діагностики);

– VLAN 30 (Patient rooms, входять палати, а також інші безпровідні користувачі);

– VLAN 40 (Medical staff, входять кабінети лікарів/лікуючих лікарів, процедурний кабінет, пост медсестер, ординаторська, перев'язочна, маніпуляційна та кімнати відпочинку медперсоналу);

– VLAN 45 (Medical storage, входить тільки приміщення для зберігання медикаментів);

– VLAN 50 (Surgery & ICU, входять як операційні, так і до-, післяопераційні палати, реанімація та пост анестезіологів);

– VLAN 55 (Medical equipment, входить стерилізаційна, кабінет зберігання обладнання та технічні приміщення);

– VLAN 60 (Administration, входить офіс директора центру, кабінет головного лікаря, кабінет заступника головного лікаря, бухгалтерія, відділ кадрів (HR), юридичний, планово-економічний відділи та архів);

– VLAN 65 (Training/Conference, входить конференц-зал та навчальний клас);

– VLAN 70 (IT Servers, входить серверна та IT-відділ);

– VLAN 70 (Security/CCTV, входить пост охорони, а також всі камери відеоспостереження).

Для забезпечення максимального захисту та надійності роботи комп'ютерної мережі медичного центру проведено диференціація доступу до інформаційних ресурсів. Доступ організовано наступним чином:

– сегмент VLAN 50 (операційна, реанімація та дотичні приміщення) матиме повноцінний доступ тільки до інформаційної системи медичного центру (HIS/EMR)

та VLAN 70, а також зв’язок з підмережею медичного персоналу VLAN 40;

– сегмент VLAN 30 (вся бездротова мережа медичного центру, до якого зможу підключатись як працівники, так і пацієнти) матиме повноцінний доступ тільки до мережі Інтернет, а також ресурсів вебсайту медичної інформаційної системи. Доступ до всіх інших підмереж та ресурсів закритий;

– сегмент VLAN 80 (CCTV) матиме повноцінний доступ тільки ресурсу Server 2, оскільки там знаходиться FTP-сервер, на якому зберігатимуть записи з камер відеоспостереження.

РОЗДІЛ 3
ПРОЄКТУВАННЯ, РОЗГОРТАННЯ ТА ТЕСТУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ

3.1 Вибір активного мережевого обладнання

Не менш важливим етапом проєктування мережі медичного центру виступає вибір обладнання. Даний етап певною мірою є критичним, оскільки саме від характеристик обладнання, що використовується при розгортанні мережі, залежить швидкість передачі даних, надійність та безперервність роботи інформаційних систем, а також захист від зловнимисницького впливу.

Отже, розгортання комп'ютерної мережі медичного центру проводиться із використанням обладнання корпорації Cisco, яке широко зарекомендувало себе у світі як високопродуктивне та безпечне. За допомогою таблиці 3.1 наведено детальний перелік обраного устаткування.

Таблиця 3.1 – Перелік обраного устаткування

№	Назва пристрою	Модель	Роль у мережі	Кі-сть портів	Розташування
1	Core Switch 1 (основний)	WS-C3650-24PD-S	Виступає ядром мережі, Inter-VLAN routing (SVI), HSRP Active	24	4 поверх (серверна)
2	Core Switch 2 (Резервний)	WS-C3650-24PD-S	Виступає ядром мережі, Inter-VLAN routing (SVI), HSRP Standby	24	4 поверх (серверна)
3	Access Switch 1	2960X-48FPS-L	Рівень доступу	48	1 поверх
4	Access Switch 2	2960X-48FPS-L	Рівень доступу	48	2 поверх
5	Access Switch 3	2960X-48FPS-L	Рівень доступу	48	3 поверх
6	Access Switch 4	2960X-48FPS-L	Рівень доступу	48	4 поверх

Продовження таблиці 3.1

№	Назва пристрою	Модель	Роль у мережі	Кі-сть портів	Розташування
7	Firewall	Cisco ASA 5505 (ASA5505-BUN-K9)	Дозволяє безпечний вихід в Інтернет (NAT/PAT)	8	4 поверх (серверна)
8	Маршрутизатор	Cisco 2911 ISR (CISCO2911/K9	Пристрій, який під’єднано до мережі провайдера	8	4 поверх (серверна)
9	Точки доступу	Cisco AIR-AP1852I-E-K9	Wi-Fi для персоналу та гостей	4	1-4 поверх

Також слід навести перелік кабінетів та присвоєне йому мережеве обладнання. Даний поділ продемонстровано за поверхами (табл. 3.2-3.3).

Таблиця 3.2 – Перелік активного мережевого обладнання (поверх 1)

Номер кабінету	Найменування	Кількість мережевих розеток	Тип та модель мережевого обладнання
1	Пост охорони/відеоспостереження	3	Access Switch 1, 2960X-48FPS-L; Точка доступу 1, Cisco AIR-AP1852I-E-K9
2	Реєстратура	3	
3	Страховий/адміністративний кабінет	3	
4	Приймальне відділення	4	
5	Аптека	4	
6	Лабораторія збору аналізів	2	
7	Лабораторія аналізу біоматеріалів	2	
8	Кабінет УЗД	3	
9	Кабінет рентген-діагностики	2	
10	Кабінет функціональної діагностики	3	
11	Службове приміщення	-	-

Продовження таблиці 3.2

Номер кабінету	Найменування	Кількість мережевих розеток	Тип та модель мережевого обладнання
12	Кабінет терапевта	2	Access Switch 1, 2960X-48FPS-L
13	Кабінет невропатолога	2	
14	Службове приміщення	-	-
15	Кабінет кардіолога	2	Access Switch 1, 2960X-48FPS-L
16	Кабінет хірурга (оглядовий)	3	
17	Процедурний кабінет	1	
18	Кабінет чергового лікаря	3	
19	Службове приміщення	-	-

Таблиця 3.3 – Перелік активного мережевого обладнання (поверх 2)

Номер кабінету	Найменування	Кількість мережевих розеток	Тип та модель мережевого обладнання
1	Службове приміщення	-	-
2	Службове приміщення	-	-
3	Кімната відпочинку персоналу	4	Access Switch 2, 2960X-48FPS-L
4	Санітарна кімната персоналу	4	
5	Пост медсестер	4	
6	Перев’язочна	2	
7	Маніпуляційна	2	
8-9	Палата пацієнтів	1	Точка доступу 2, Cisco AIR-AP1852I-E-K9
10	Службове приміщення	-	-
11	Службове приміщення	-	-
12	Службове приміщення	-	-
13	Кімната зберігання медикаментів	3	Access Switch 2, 2960X-48FPS-L
14	Кабінет завідувача відділенням	3	
15	Кабінет лікуючого лікаря	3	
16	Ординаторська	3	
17-19	Палати пацієнтів	1	Точка доступу, Cisco AIR-AP1852I-E-K9

Перелік кабінетів та відповідного мережевого обладнання наведено в таблицях 3.4-3.5 у розрізі поверхів.

Таблиця 3.4 – Перелік активного мережевого обладнання (поверх 3)

Номер кабінету	Найменування	Кількість мережевих розеток	Тип та модель мережевого обладнання
1	Службове приміщення	-	-
2	Стерилізаційна	2	Access Switch 3, 2960X-48FPS-L
3	Пост анестезіологів	2	
4	Передопераційна	3	
5	Операційно №1	4	
6	Операційно №2	4	
7	Реанімація	2	
8	Післяопераційна палата	2	
9	Службове приміщення	-	-
10	Службове приміщення	-	-
11	Кабінет зберігання обладнання	3	
12	Технічне приміщення	-	-
13	Кімната чергування лікарів	3	Точка доступу 3, Cisco AIR-AP1852I-E-K9
14	Кімната медичного персоналу	5	
15	Службове приміщення	-	-
16	Службове приміщення	-	-
17	Службове приміщення	-	-

Таблиця 3.5 – Перелік активного мережевого обладнання (поверх 4)

Номер кабінету	Найменування	Кількість мережевих розеток	Тип та модель мережевого обладнання
1	Службове приміщення	-	-
2	Навчальний клас	4	Access Switch 4, 2960X-48FPS-L
5	Конференц зал	5	
6	Службове приміщення	-	-
7	Відділ кадрів	3	Access Switch 4, 2960X-48FPS-L
8	Юридичний відділ	3	
9	Планово-економічний відділ	3	
10	Службове приміщення	-	-

Продовження таблиці 3.5

Номер кабінету	Найменування	Кількість мережевих розеток	Тип та модель мережевого обладнання
11	Серверна	5	Firewall, Cisco ASA 5505 (ASA5505-BUN-K9); Точка доступу 4, Cisco AIR-AP1852I-E-K9, Core Switch 1 (основний) WS-C3650-24PD-S, Core Switch 2 (резервний)WS-C3650-24PD-S
12	Архів	3	Access Switch 4, 2960X-48FPS-L
13	Бухгалтерія	3	
14	Кабінет заступника головного лікаря	3	
15	Кабінет головного лікаря	3	
16	Офіс директора	3	
17	Службове приміщення	-	-
19	Службове приміщення	-	-

З таблиць 3.2-3.5 можна побачити, що на кожному поверсі передбачено по одному 48-портовому комутаторі. Це пояснюється великою кількістю користувачів на поверхах 1-4. Комутатори з кількістю 48 портів зможуть забезпечити як теперішні потреби у портах, так і майбутнє масштабування (додавання в деяких кабінетах додаткового мережевого обладнання). Використання 24-портових комутаторів в якості комутаторів доступу вимагало б встановлення двох пристроїв на один поверх, а це у свою чергу збільшувало б кількість точок відмов, а також підвищувало витрати на обслуговування. Комутатор 3 рівня WS-C3650-24PD-S виступатиме ядром мережеві медичного центру, таких комутаторів два (основний та резервний). Вони знаходитимуться у серверній кімнаті. Також у серверній встановлено фаєрвол Cisco ASA 5505 (ASA5505-BUN-K9), який дозволить здійснювати безпечний вихід в мережу Інтернет як працівникам лікарні, так і

пацієнтам/гостям (відвідувачам). Окрім того, будуть розмішені точки доступу Cisco AIR-AP1852I-E-K9 в кількості одна на поверх.

3.2 Розрахунок логічної адреси

Виконання розрахунку (поділу) логічної адреси – це один з ключових аспектів в побудові сучасної, надійної, безпечної та масштабованої мережі. Логічна адресації дозволяє визначити структуру підмереж та виконати розподіл адрес між підмережами (VLAN). IP-планування надзвичайно важливе, особливо у медичних мережах, оскільки воно забезпечує:

– швидку діагностику та усунення неполадок в мережі;

– мінімізацію широкомовного трафіку у великих VLAN;

– дозволяє виконувати масштабування мережі без глобальної переадресації;

– забезпечує ефективну робочу списків контролю доступу (ACL).

Застосування фіксованих масок (наприклад, маска /24 для всіх підмереж)) призводить до марнування адрес, тому використано VLSM – технологію масок змінної довжини. VLSM забезпечить створення гнучких підмереж різного розміру під різні потреби.

Згідно логічної структури комп’ютерної мережі, яка наведена у підрозділі 2.3, кабінети поверхів груповано за призначенням та об’єднано в 11 підмереж, а кожна підмережа призначена у власну (окрему) VLAN. За допомогою таблиці А.1 представлено розрахунок масок для сегментів мережі медичного центру у додатку А.

Комутатор 3 рівня WS-C3650-24PD-S виступатиме ядром мережеві медичного центру, таких комутаторів два (основний та резервний). Вони знаходитимуться у серверній кімнаті.

Медичному центру надано мережу 192.168.0.0/16. Згідно вибраних масок (табл. 3.6) мережу поділено на 11 підмереж. За допомогою таблиці 3.6 представлено поділ мережі, який включає IP-мережу, кількість адрес в мережі, а також адреси, які придатні для адресації [18].

Таблиця 3.6 – Розрахунок мережі 192.168.0.0/16

Підмережа	VLAN 40	VLAN 60	VLAN 10	VLAN 20	VLAN 50	VLAN 65
IP-мережа, маска	192.168.0.0/26	192.168.0.64/26	192.168.0.128/27	192.168.0.160/27	192.168.0.192/27	192.168.0.224/27
Кількість IP адрес в IP-мережі	64	64	32	32	32	32
Адреси, які придатні для адресації	.1-.62	.65-.126	.129-.158	.161-.190	.193-.222	.225-.254
Підмережа	VLAN 30	VLAN 55	VLAN 70	VLAN 80	VLAN 45	
IP-мережа, маска	192.168.1.0/28	192.168.1.16/28	192.168.1.32/28	192.168.1.48/28	192.168.1.64/29	
Кількість IP адрес в IP-мережі	16	16	16	16	8	
Адреси, які придатні для адресації	.1-.14	.17-.30	.33-.46	.49-.62	.65-.70	

Варто зауважити, що для з’єднання ядра мережі з фаєрволом використовується технічна підмережа 192.168.2.0/28, яка є ізольованою від інших

сегментів мережі та призначена виключно для забезпечення зв’язку між цими пристроями. Для з’єднання фаєрволу з маршрутизатором провайдера використовується локальна провайдерська мережа 10.10.2.0/30, яка містить лише дві адреси для вузлів, що є достатнім для організації точки з’єднання між двома пристроями. Схему розподілу адрес ключового обладнання наведено в таблиці 3.7.

Таблиця 3.7 – Схема розподілу адрес ключового обладнання

Номер підмережі/пристрій	Інтерфейс/Мережний адаптер/Шлюз/vlan	Адреса підмережі/інтерфейсу	Маска підмережі	Префікс
Підмережа 1 (VLAN 40)	40	192.168.0.0	255.255.255.192	/26
Підмережа 2 (VLAN 60)	60	192.168.0.64	255.255.255.192	/27
Підмережа 3 (VLAN 10)	10	192.168.0.128	255.255.255.224	/27
Підмережа 4 (VLAN 20)	20	192.168.0.160	255.255.255.224	/27
Підмережа 5 (VLAN 50)	50	192.168.0.192	255.255.255.224	/27
Підмережа 6 (VLAN 65)	65	192.168.0.224	255.255.255.224	/27
Підмережа 7 (VLAN 30)	30	192.168.1.0	255.255.255.240	/28
Підмережа 8 (VLAN 55)	55	192.168.1.16	255.255.255.240	/28
Підмережа 9 (VLAN 70)	70	192.168.1.32	255.255.255.240	/28
Підмережа 10 (VLAN 80)	80	192.168.1.48	255.255.255.240	/28
Підмережа 11 (VLAN 45)	45	192.168.1.64	255.255.255.248	/29
Підмережа 12 (технічна VLAN 3)	3	192.168.2.0	255.255.255.240	/28
Підмережа 13 (провайдерська)	13	10.10.2.0	255.255.255.252	/30

Продовження таблиці 3.7

Номер підмережі/пристрій	Інтерфейс/Мережний адаптер/Шлюз	Адреса підмережі/інтерфейсу	Маска підмережі	Префікс
Фаєрвол ASA0	Інтерфейс Gig0/7	10.10.2.2	255.255.255.240	/28
	Інтерфейс Gig0/0	VLAN 3 (192.168.2.1)	255.255.255.240	/28
	Інтерфейс Gig0/1		255.255.255.240	/28
Комутатор Core_SW1 (основний)	Інтерфейс Gig1/0/24 (VLAN 3)	192.168.2.2	255.255.255.240	/28
	Інтерфейс Gig1/0/1-4	VLAN 10-80		
	VLAN 10	192.168.0.30	255.255.255.224	/27
	VLAN 20	192.168.0.160	255.255.255.224	/27
	VLAN 30	192.168.1.2	255.255.255.240	/28
	VLAN 40	192.168.0.2	255.255.255.192	/26
	VLAN 45	192.168.1.66	255.255.255.248	/29
	VLAN 50	192.168.0.194	255.255.255.224	/27
	VLAN 55	192.168.1.18	255.255.255.240	/28
	VLAN 60	192.168.0.66	255.255.255.192	/27
	VLAN 65	192.168.0.226	255.255.255.224	/27
	VLAN 70	192.168.1.34	255.255.255.240	/28
	VLAN 80	192.168.1.50	255.255.255.240	/28
	VLAN 3	192.168.2.2	255.255.255.240	/28
Комутатор Core_SW2 (резервний)	Інтерфейс Gig1/0/1-4	VLAN 10-80		
	VLAN 10	192.168.0.31	255.255.255.224	/27
	VLAN 20	192.168.0.161	255.255.255.224	/27
	VLAN 30	192.168.1.3	255.255.255.240	/28
	VLAN 40	192.168.0.3	255.255.255.192	/26
	VLAN 45	192.168.1.67	255.255.255.248	/29
	VLAN 50	192.168.0.195	255.255.255.224	/27
	VLAN 55	192.168.1.19	255.255.255.240	/28
	VLAN 60	192.168.0.67	255.255.255.192	/27
	VLAN 65	192.168.0.227	255.255.255.224	/27
	VLAN 70	192.168.1.35	255.255.255.240	/28
	VLAN 80	192.168.1.51	255.255.255.240	/28
	VLAN 3	192.168.2.3	255.255.255.240	/28

Продовження таблиці 3.7

Номер підмережі/пристрій	Інтерфейс/Мережний адаптер/Шлюз/vlan	Адреса підмережі/інтерфейсу	Маска підмережі	Префікс
Сервери: Server 1 – DHCP Server 2 - HTTPS/DNS	Мережний адаптер	192.168.1.45 - 192.168.1.46	255.255.255.240	/28
	Шлюз за замовчуванням	192.168.1.33	255.255.255.240	/28
IP-камери	Мережний адаптер	192.168.1.55 - 192.168.1.62	255.255.255.240	/28
	Шлюз за замовчуванням	192.168.1.48	255.255.255.240	/28
ПК VLAN 10-80	Мережний адаптер	DHCP		
	Шлюз за замовчуванням			
Принтери	Мережний адаптер	DHCP		
	Шлюз за замовчуванням			

3.3 Комутація

Комутація належить до одного з основних рівнів функціонування будь-яких комп’ютерних мереж і відповідає за передачу даних на рівнів 2 моделі OSI. Завдяки комутації існує доставка кадрів між пристроями в фізичній сегментованій мережі. Комутація виконує такі кричні функції:

– запобігає петлям в топології;

– дозволяє ізолювати структурні підрозділи за допомогою сегментації трафіку на VLAN (віртуальні локальні мережі);

– виключає непотрібний трафік з портів, що у свою чергу підвищує ефективність роботи мережі;

– забезпечує швидке відновлення мережі.

Сучасні комутатори аналізуються MAC-адреси в таблиці комутації, і коли пристрій надсилає кадр, то комутатор виконує такі функції: перевіряє MAC-адресу призначення. У випадку її присутності в таблиці – пересилає отриманий кадр тільки на необхідний порт, якщо адреса відсутня – комутатор виконує надсилання кадру на всі порти (звісно, окрім того, з якого прийшов кадр). Далі комутатор вивчає MAC-адресу джерела, а вже після цього – оновлює свою таблицю комутації.

Такий підхід покращує передачу даних, оскільки значно зменшує непотрібний трафік (на відміну від концентраторів). Однак присутній один недолік – broadcast-домени у великих мережах стають досить великі, що у свою чергу впливає на продуктивність мережі. Для вирішення цього недоліку використовують віртуальні локальні мережі.

Мережа медичного центру складається з великої кількості віртуальних мереж. Ці мережі (VLAN’и) потрібно створити на всіх комутатора core та access, слідкуючи, щоб всюди були однакові імена. Як видно з рисунку 3.1, для кожної віртуальної мережі задається унікальний ідентифікатор та відповідна назва, що дозволяє чітко ідентифікувати належність трафіку до конкретного підрозділу медичного закладу. Правильне іменування VLAN спрощує подальше адміністрування та діагностику мережі.

Для забезпечення передавання трафіку між різними VLAN на комутаторах використовуються trunk-порти. Вони дають змогу передавати через один фізичний канал дані одразу декількох віртуальних мереж завдяки використанню стандарту IEEE 802.1Q, який додає до кадру спеціальну мітку з ідентифікатором VLAN. Такий підхід значно спрощує побудову масштабованої мережевої інфраструктури, оскільки дозволяє уникнути необхідності використання окремого фізичного з’єднання для кожної VLAN. Trunk-з’єднання зазвичай застосовуються між core та access-комутаторами, забезпечуючи коректну маршрутизацію й розподіл трафіку між різними сегментами мережі медичного центру. Крім цього, правильне налаштування trunk-портів є важливим елементом мережевої безпеки та стабільної

роботи всієї інфраструктури, оскільки помилки в конфігурації можуть призвести до витоку трафіку між VLAN, появи широкомовних штормів або несанкціонованого доступу до мережевих ресурсів.

```
L3-SW1-Primary>en
L3-SW1-Primary#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
L3-SW1-Primary(config)#vlan 10
L3-SW1-Primary(config-vlan)# name Reception-Administration
L3-SW1-Primary(config-vlan)#vlan 20
L3-SW1-Primary(config-vlan)# name Diagnostics
L3-SW1-Primary(config-vlan)#vlan 30
L3-SW1-Primary(config-vlan)# name Patient-Rooms-Internet-Only
L3-SW1-Primary(config-vlan)#vlan 40
L3-SW1-Primary(config-vlan)# name Medical-Staff
L3-SW1-Primary(config-vlan)#vlan 45
L3-SW1-Primary(config-vlan)# name Medical-Storage
L3-SW1-Primary(config-vlan)#vlan 50
L3-SW1-Primary(config-vlan)# name Surgery-ICU
L3-SW1-Primary(config-vlan)#vlan 55
L3-SW1-Primary(config-vlan)# name Medical-Equipment
L3-SW1-Primary(config-vlan)#vlan 60
L3-SW1-Primary(config-vlan)# name Administration
L3-SW1-Primary(config-vlan)#vlan 65
L3-SW1-Primary(config-vlan)# name Training-Conference
L3-SW1-Primary(config-vlan)#vlan 70
L3-SW1-Primary(config-vlan)# name IT-Servers
L3-SW1-Primary(config-vlan)#vlan 80
L3-SW1-Primary(config-vlan)# name Security-CCTV
L3-SW1-Primary(config-vlan)#vlan 999
L3-SW1-Primary(config-vlan)# name Transit-Firewall
L3-SW1-Primary(config-vlan)#exit
```

Рисунок 3.1 – Конфігурування VLAN на комутаторах core та access рівнів

Для того, щоб VLAN’и могли проходити між різними комутаторами – застосовують trunk-порти. Такі порти дозволяють надсилати IEEE 802.1Q кадри з інформацією про VLAN. Наведено основні вимоги для правильного налаштування trunk-конфігурацій:

– повинен бути вимкненим Dynamic Trunking Protocol (DTP – протокол, який дозволяє автоматично узгоджувати режим роботи портів між комутаторами. Рекомендується його не використовувати, оскільки через нього зловмисники можуть отримати доступ до VLAN);

– потрібно явно вказувати VLAN, які дозволено;

– слід змінити native VLAN на невикористовуваний, для запобігання атакам.

Фрагмент конфігурації транк-портів, які йдуть від core до access комутаторів представлено на рисунку 3.2 [19].

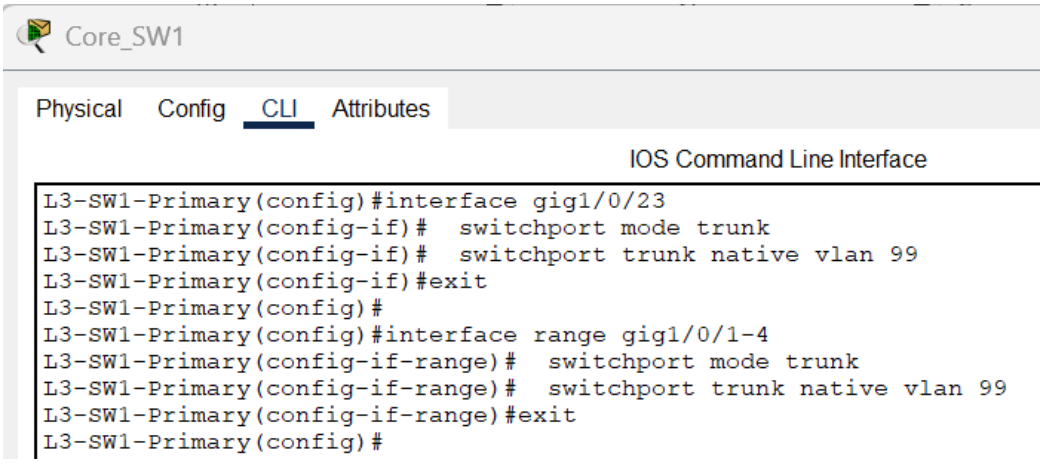

Рисунок 3.2 – Конфігурування транк-портів на комутаторах core та access рівнів

З рисунку 3.2 видно, що на транк-портах явно вказано перелік дозволених VLAN, а протокол DTP вимкнено вручну. Також визначено native VLAN, відмінний від стандартного значення, що унеможливлює проведення атак типу VLAN hopping. Такий підхід до налаштування транк-з'єднань є обов'язковим для мереж із підвищеними вимогами до безпеки, до яких відноситься мережа медичного закладу.

За допомогою рисунку 3.3 продемонстровано налаштування конфігурації на access-комутаторах, які підключені до кінцевих пристроїв. Для таких портів використовується режим доступу (access) [19]. Наведена конфігурація свідчить про те, що кожному порту доступу призначено конкретну VLAN відповідно до функціонального призначення підключеного пристрою. Увімкнення функцій PortFast та BPDU Guard на портах доступу дозволяє пришвидшити підключення кінцевих пристроїв та одночасно захистити мережу від випадкового або зловмисного створення петель у топології.

```
ACCESS-1F>en
ACCESS-1F#conf t
Enter configuration commands, one per line.  End with
ACCESS-1F(config)#interface range fa0/1 - 6
ACCESS-1F(config-if-range)# switchport mode access
ACCESS-1F(config-if-range)# switchport access vlan 10
ACCESS-1F(config-if-range)#exit
ACCESS-1F(config)#
ACCESS-1F(config)#interface range fa0/7 - 13
ACCESS-1F(config-if-range)# switchport mode access
ACCESS-1F(config-if-range)# switchport access vlan 20
ACCESS-1F(config-if-range)#exit
ACCESS-1F(config)#
ACCESS-1F(config)#interface range fa0/14 - 21
ACCESS-1F(config-if-range)# switchport mode access
ACCESS-1F(config-if-range)# switchport access vlan 40
ACCESS-1F(config-if-range)#exit
ACCESS-1F(config)#
ACCESS-1F(config)#interface range fa0/14 - 21
ACCESS-1F(config-if-range)# switchport mode access
ACCESS-1F(config-if-range)# switchport access vlan 40
ACCESS-1F(config-if-range)#exit
ACCESS-1F(config)#
ACCESS-1F(config)#interface range fa0/22 - 23
ACCESS-1F(config-if-range)# switchport mode access
ACCESS-1F(config-if-range)# switchport access vlan 80
ACCESS-1F(config-if-range)#exit
ACCESS-1F(config)#
ACCESS-1F(config)#interface fa0/24
ACCESS-1F(config-if)# switchport mode access
ACCESS-1F(config-if)# switchport access vlan 30
ACCESS-1F(config-if)#exit
ACCESS-1F(config)#
```

Рисунок 3.3 – Конфігурування access-портів на комутаторі рівня доступу SW1

Оскільки спроєктована мережа медичного центру матиме резервні канали зв’язку, то потрібно подбати, щоб не утворились петлі. Для вирішення цієї проблеми використовують протокол Spanning Tree (STP). У самій мережі використано Rapid Per-VLAN Spanning Tree+ (скорочено Rapid PVST+). Цей протокол – модифікація STP. А до переваг Rapid PVST+ відносять:

– значно швидша збіжність (кілька секунд проти 30-50 в STP);

– відмова в певному VLAN ніяким чином не впливає на інші;

– можна точно призначити root bridge на рівні ядра.

Для переведення протоколу STP в режим Rapid PVST+ на кожному комутаторі слід ввести команду spanning-tree mode rapid-pvst (рис. 3.4).

```
L3-SW1-Primary(config)#spanning-tree mode rapid-pvst
```

Рисунок 3.4 – Переведення протоколу STP в режим Rapid PVST+ на комутаторі Core_SW1

У протоколі STP головним стає той комутатор, який має найменший пріоритет. Інколи пріоритет потрібно виставляти в ручному режимі, оскільки мережа сама обирає Root Bridge на основі найменшої MAC-адреси. У деякий випадках кореневим комутатором може стати не той, який потрібно, а це несе значний вплив на роботу мережі: від затримки роботи мережі (трафік почне ходити хаотичними шляхами) до перевантаження каналів. Отже, для того, щоб мережа чітко мала кореневий комутатор, який потрібно, на основному ядрі мережі Core_SW1 потрібно прописати spanning-tree vlan 1,3,10,20,30,40,50,60,70,80 priority 0 (рис. 3.5), а на резервному Core_SW2 – spanning-tree vlan 1,10,20,30,40,50,60,70,80 priority 8192 (рис. 3.6).

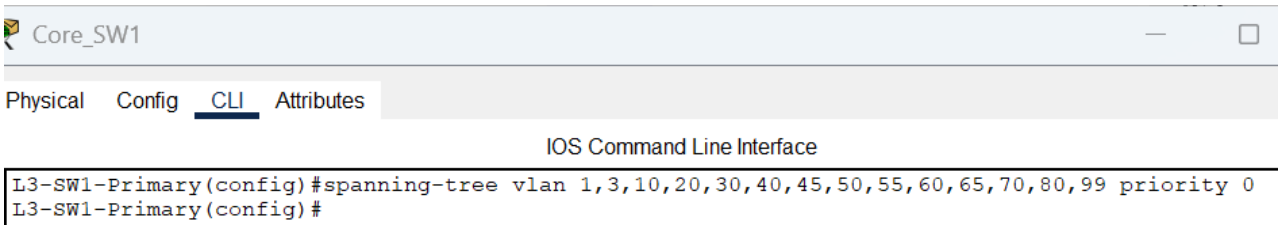

Рисунок 3.5 – Задання основного комутатора Core_SW1 кореневим

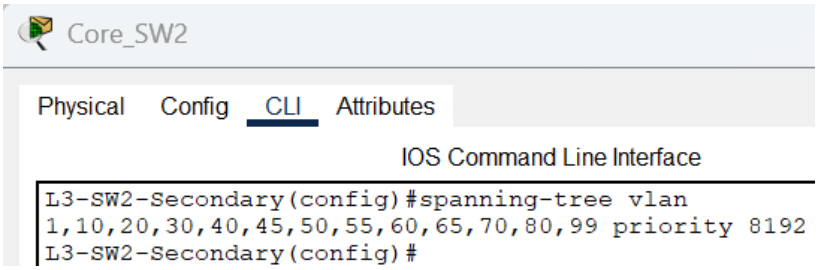

Рисунок 3.6 – Задання пріоритету для резервного комутатора Core_SW2

3.4 Організація безпроводового доступу

Точка доступу Wi-Fi є важливим та невід'ємним елементом побудови сучасної мережевої інфраструктури. У комп'ютерній мережі медичного закладу передбачено чотири точки доступу – по одній на кожному поверсі, що забезпечує рівномірне покриття безпроводовим сигналом усієї будівлі.

Спроєктована безпроводова мережа розміщена у власній підмережі (VLAN 30) та є спільною для всіх категорій користувачів: пацієнтів, відвідувачів та працівників медичного закладу. Винесення безпроводової мережі в окремий сегмент є обґрунтованим рішенням з точки зору безпеки, оскільки дозволяє чітко розмежувати трафік між внутрішньою інфраструктурою закладу та загальнодоступною мережею.

Особливість цієї мережі полягає в тому, що доступ до ресурсів внутрішньої мережі медичного закладу для користувачів VLAN 30 повністю заблоковано засобами ACL, однак надано вільний вихід у глобальну мережу Інтернет та доступ до вебсайту медичного закладу. Така організація доступу є обґрунтованим рішенням, оскільки дозволяє розмежувати трафік зовнішніх користувачів та внутрішньої інфраструктури закладу, не обмежуючи при цьому базові потреби у доступі до мережі Інтернет. Завдяки цьому пацієнти та відвідувачі можуть залишатись на інформаційному зв'язку під час перебування в закладі, а працівники – отримувати доступ до особистих кабінетів на вебсайті медичного закладу з власних мобільних пристроїв. Це значно підвищує зручність користування

мережею для всіх категорій користувачів без шкоди для безпеки внутрішньої інфраструктури.

Для реалізації безпроводової мережі обрано точки доступу Cisco AIR-AP1852I-E-K9, які добре зарекомендували себе в умовах великої щільності користувачів та забезпечують стабільне покриття сигналом у межах одного поверху. Кожна точка доступу розміщена в оптимальному місці поверху з урахуванням планування приміщень, що дозволяє забезпечити рівномірне покриття безпроводовим сигналом усіх кабінетів та коридорів. Живлення точок доступу здійснюється через технологію PoE від комутаторів рівня доступу, що дозволяє уникнути прокладання додаткових електричних кабелів та спрощує монтаж обладнання.

З метою забезпечення захисту безпроводової мережі на кожній точці доступу налаштовано шифрування WPA2-PSK, яке є сучасним стандартом захисту безпроводових мереж та забезпечує надійне шифрування переданих даних. Пароль доступу змінюється щотижня відповідно до встановленої політики безпеки медичного закладу, що мінімізує ризик несанкціонованого підключення до мережі. Додатково, завдяки виділенню безпроводової мережі в окремий сегмент VLAN 30, навіть у разі компрометації пароля доступу зловмисник не отримає доступу до внутрішніх ресурсів мережі медичного закладу. На рисунку 3.7 представлено базові налаштування однієї з точок безпроводової мережі [19].

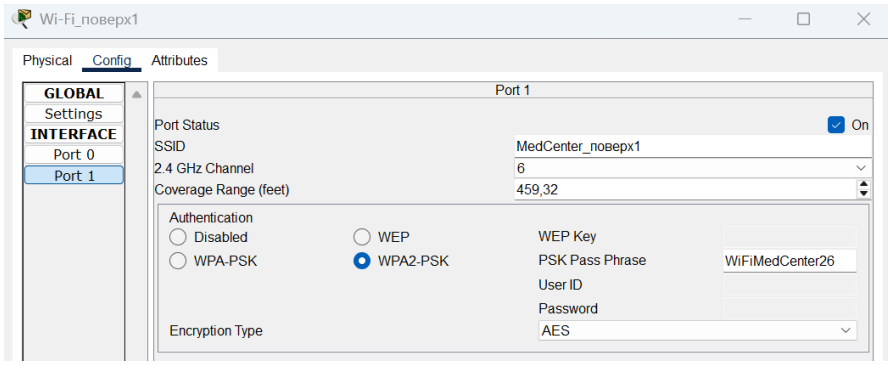

Рисунок 3.7 – Задання SSID, типу шифрування та паролю для точки доступу

3.5 Налаштування міжмережевої взаємодії

У спроєктованій мережі медичного центру міжмережева взаємодія відбувається на рівні ядра за рахунок інтерфейсів SVI (Switched Virtual Interface), що налаштовані на комутаторах 3-го рівня Core_SW1 (основний) та Core_SW2 (резервний). Дані комутатори забезпечують Inter-VLAN routing, а маршрутизація здійснюється командою ip routing. Також в мережі налаштована відмовостійкість, яка забезпечується за рахунок роботи протоколу HSRP (Hot Standby Router Protocol). Для роботи цього протоколу на кожному SVI створюється адреса, яка є шлюзом для клієнтів за замовчуванням. На основному Core_SW1 комутаторі встановлюється пріоритет 110 (в статусі Active), а для резервного 90 (перебування в режимі Standby). При відмові основного комутатора рівня ядра здійснюється перемикання на резервний. На рисунку 3.8 представлено фрагмент налаштувань HSRP на основному комутаторі Core_SW1 для VLAN 10, а на рисунку 3.9 – фрагмент на резервному комутаторі Core_SW2 для VLAN 10 [20].

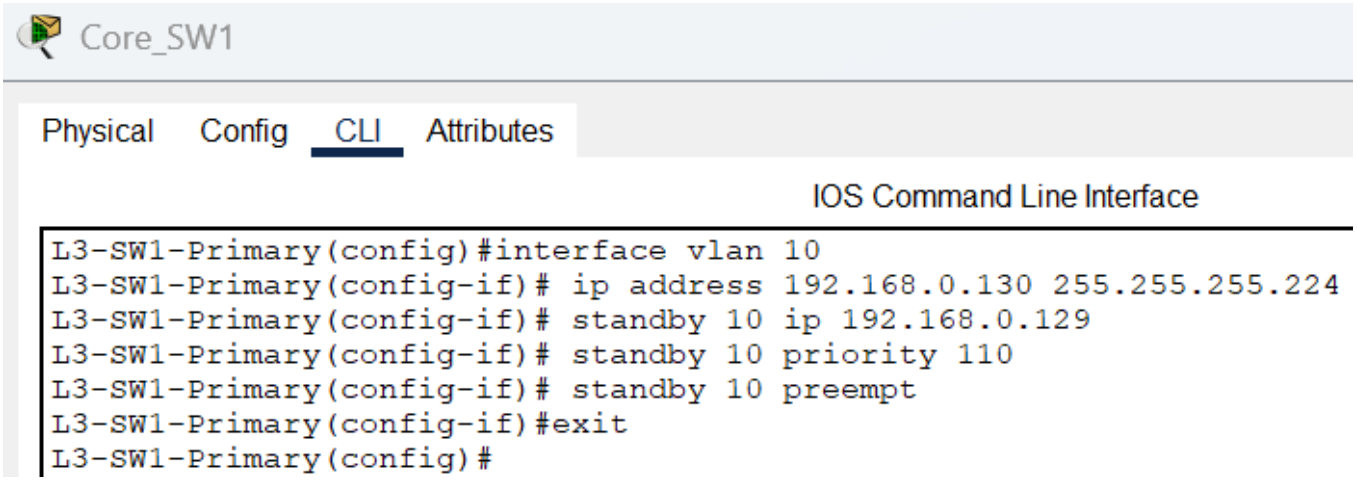

Рисунок 3.8 – Фрагмент конфігурації HSRP на основному комутаторі Core_SW1 для VLAN 10

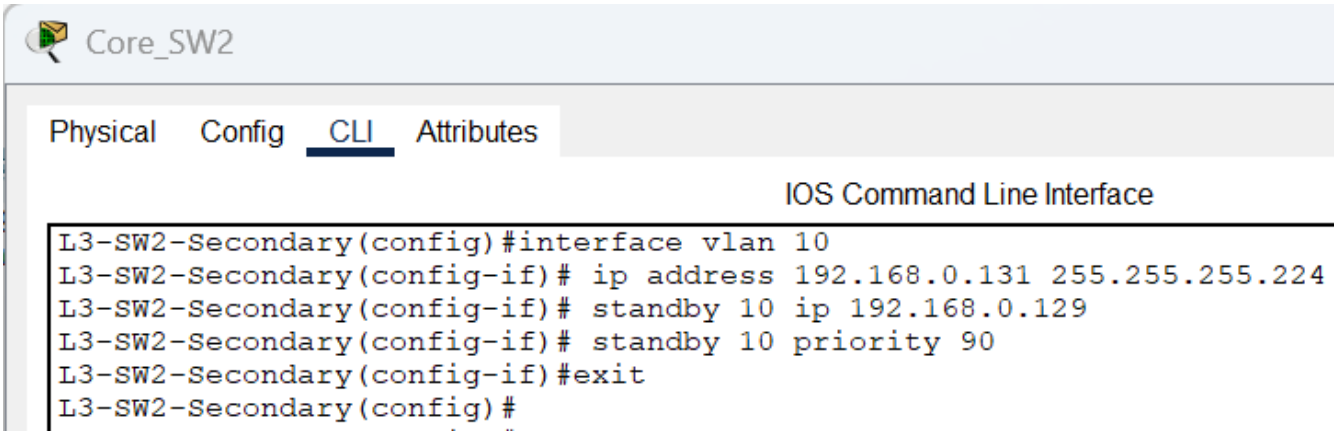

Рисунок 3.9 – Фрагмент конфігурації HSRP на резервному комутаторі Core_SW2 для VLAN 10

Оскільки на комутаторах присутня маршрутизація між всіма віртуальними мережами, то після створення SVI та налаштування протоколу HSRP, реалізовано політику безпеки за допомогою extended ACL (розширених списків контролю доступу). Щоб фільтрувати трафік до того, як його маршрутизовано, ACL слід застосовувати за вхідним напрямком на інтерфейсах VLAN.

Отже, для обмеження доступу з VLAN 80 до всі мереж, окрім сервера 192.168.1.46, прописано наступний список доступу (рис. 3.10) [21]:

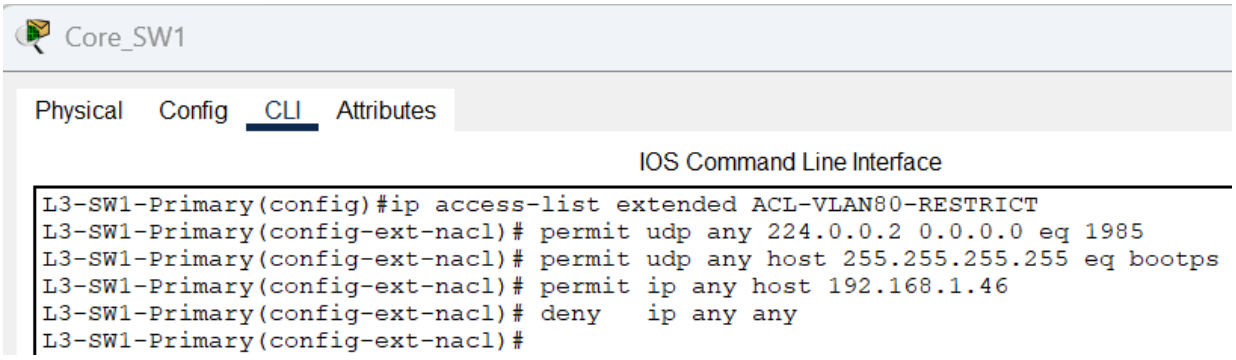

Рисунок 3.10 – Extended ACL для VLAN 80

Щоб дозволити доступ з VLAN 50 до VLAN 40 та VLAN 70 (серверної) прописано наступний список доступу (рис. 3.11) [21]:

Рисунок 3.11 – Extended ACL для VLAN 50

Щоб дозволити доступ з VLAN 30 тільки до мережі Інтернет та сервера 192.168.1.46, що у VLAN 70 (серверної), – прописано наступний список доступу (рис. 3.12) [21]:

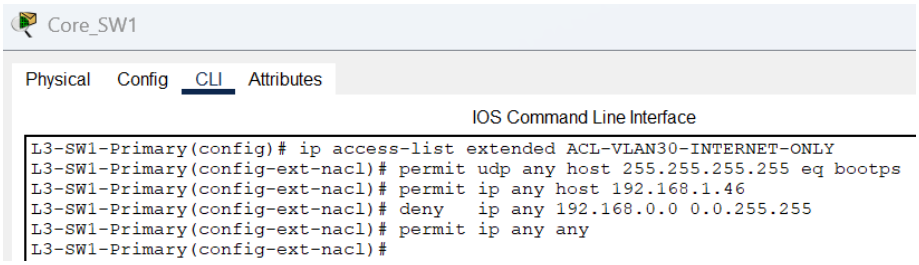

Рисунок 3.12 – Extended ACL для VLAN 30

Рисунок 3.13 демонструє застосування списків на інтерфейсах.

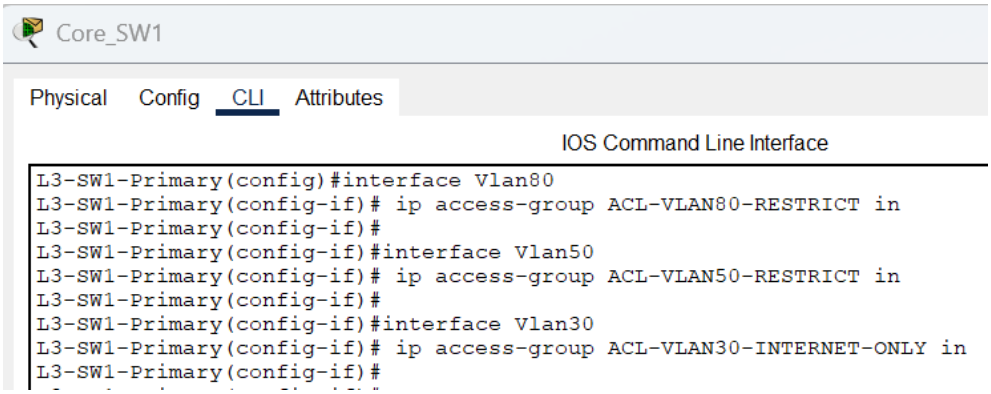

Рисунок 3.13 – Застосування розширених ACL для інтерфейсів VLAN 30, 50 та 80

3.6 Організація доступу до Інтернету

Для забезпечення доступу до глобальної мережі Інтернет в комп'ютерній мережі медичного центру використовують фаєврол Cisco ASA 5505. У даній мережі він виконує функції NAT/PAT, а також базового захисту. Фаєрвол підключається за допомогою внутрішнього (inside) порту до ядра мережі через VLAN 3 та зовнішнього (outside) порту до Інтернет-провайдера через VLAN 2. Для внутрішнього та зовнішнього інтерфейсів встановлюються рівні безпеки відповідно 100 та 0. Внутрішні адреси мережі медичного центру (192.168.0.0/16) транслюються за допомогою NAT overload. Це дозволяє медичному центру використовувати єдину публічну адресу для виходу в мережу Інтернет усієї внутрішньої мережі. На рис. 3.14 представлено фрагмент налаштування NAT на ASA [22].

```
object network LAN
 subnet 192.0.0.0 255.0.0.0
 nat (inside,outside) dynamic interface
```

Рисунок 3.14 – Створення об'єкту та задання динамічної трансляції для роботи NAT

Також на комутаторі рівня ядра Core SW1 потрібно налаштувати статичний маршрут за замовчування, який вказуватиме на внутрішню IP-адресу фаєвролу ASA (рис. 3.15), а на самому фаєрволі – додати маршрут за замовчуванням до провайдера (рис. 3.16).

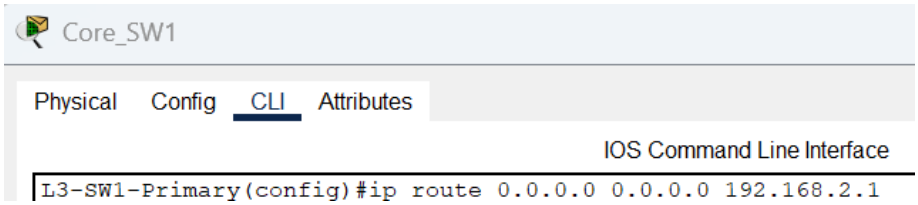

Рисунок 3.15 – Налаштування статичного маршруту за замовчування на комутаторі 3 рівня Core SW1

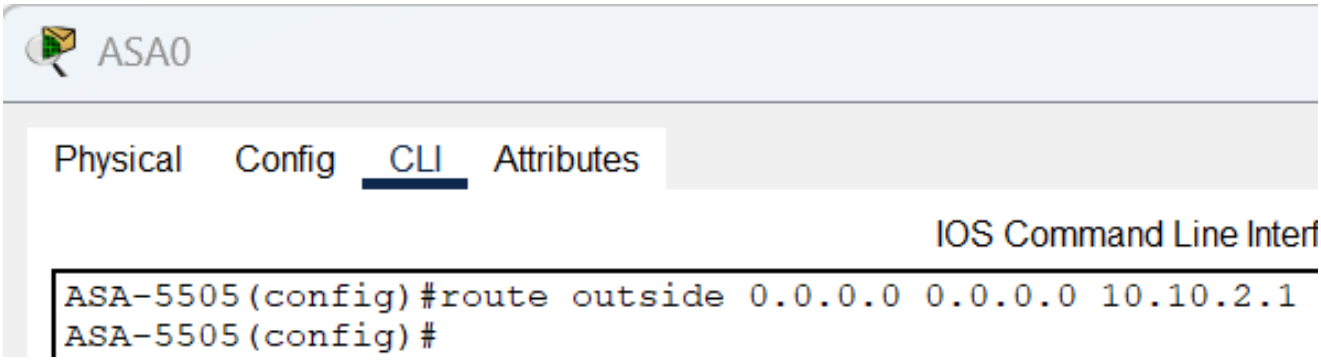

Рисунок 3.16 – Налаштування статичного маршруту за замовчування на фаєрволі

За допомогою наступного налаштування (рис. 3.17) на Cisco ASA 5505 встановлюється базова інспекція трафіку для таких протоколів як ICMP та HTTP. Дане налаштування забезпечує відповіді на вихідні запити, які надходитимуть зсередини мережі. Також додатково прописано ACL, який явно дозволяє вхідні ICMP echo-reply та unreachable-повідомлення.

```
!
access-list OUTSIDE_IN extended permit icmp any any echo-reply
access-list OUTSIDE_IN extended permit icmp any any unreachable
!
!
access-group OUTSIDE_IN in interface outside
!
!
class-map inspection_default
 match default-inspection-traffic
!
policy-map global_policy
 class inspection_default
  inspect http
  inspect icmp
!
service-policy global_policy global
```

Рисунок 3.17 – Конфігурація політики безпеки та інспекції на Cisco ASA 5505

3.7 Перевірка працездатності мережі

Оскільки на Сервері 1 будо піднято DHCP-сервіс для кожної підмережі (рис. 3.18), то слід перевірити його роботу. Як результат (рис. 3.19) – ПК успішно отримують мережеві налаштування для своїх карт.

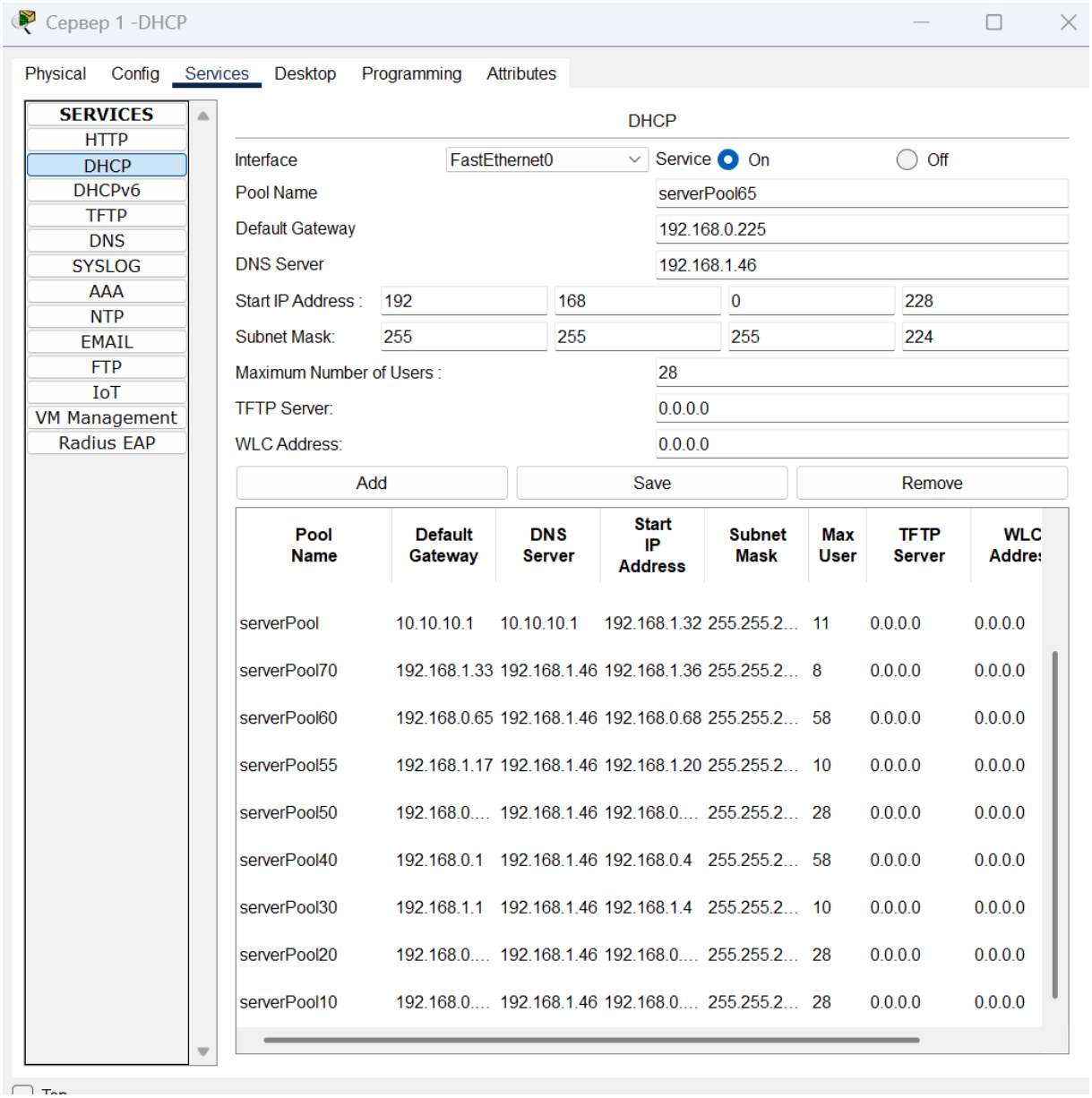

Рисунок 3.18 – Конфігурація DHCP-пулів на Сервер 1

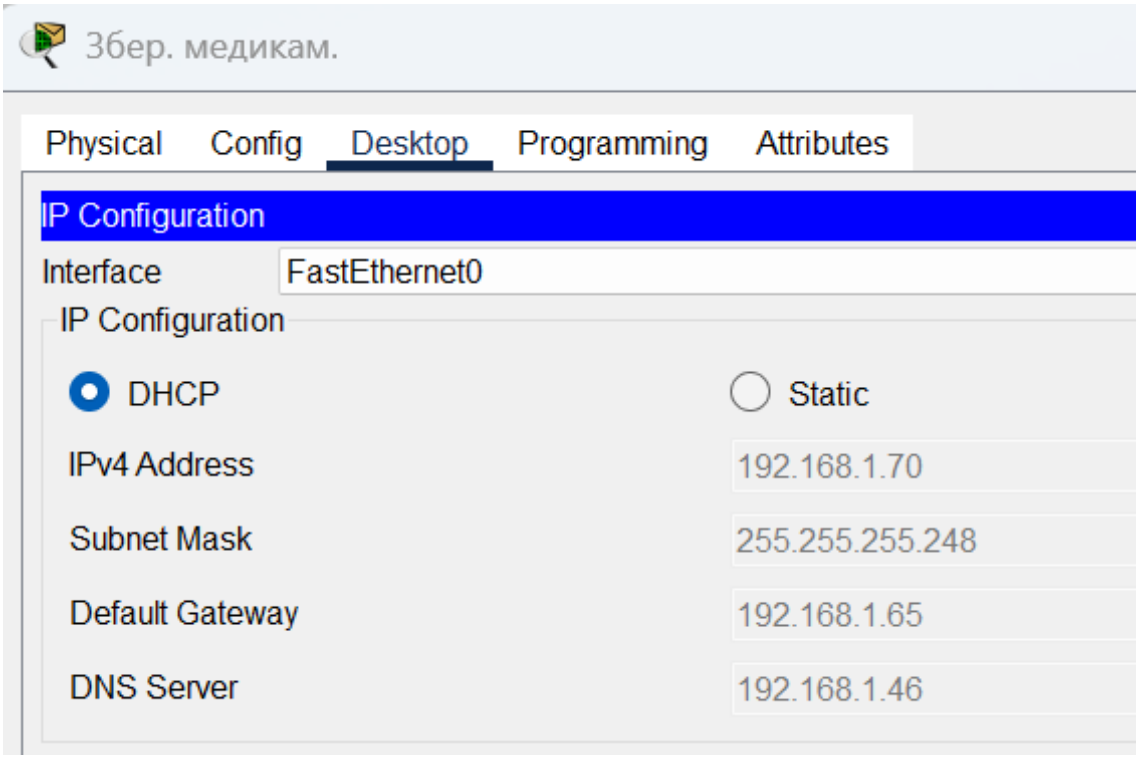

Рисунок 3.19 – Перевірка працездатності DHCP-сервісу

На ПК з будь-якої VLAN, (наприклад, 10) протестовано доступ до мережі Інтернет (рис. 3.20) та вебсайту компанії (рис. 3.21), який розміщений на сервері 2.

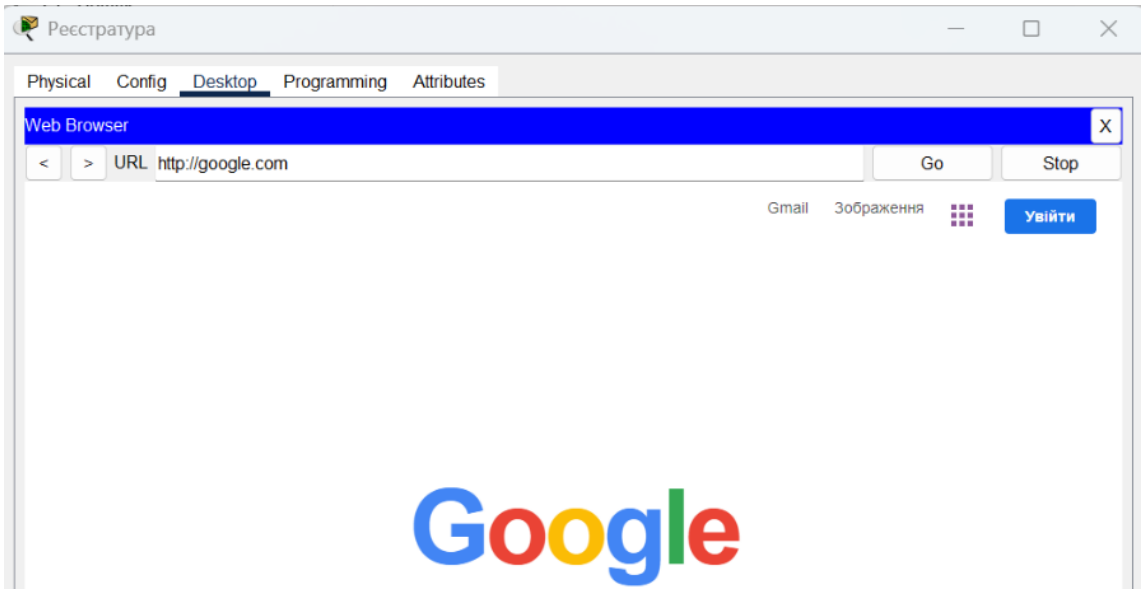

Рисунок 3.20 – Доступ до мережі Інтернет присутній

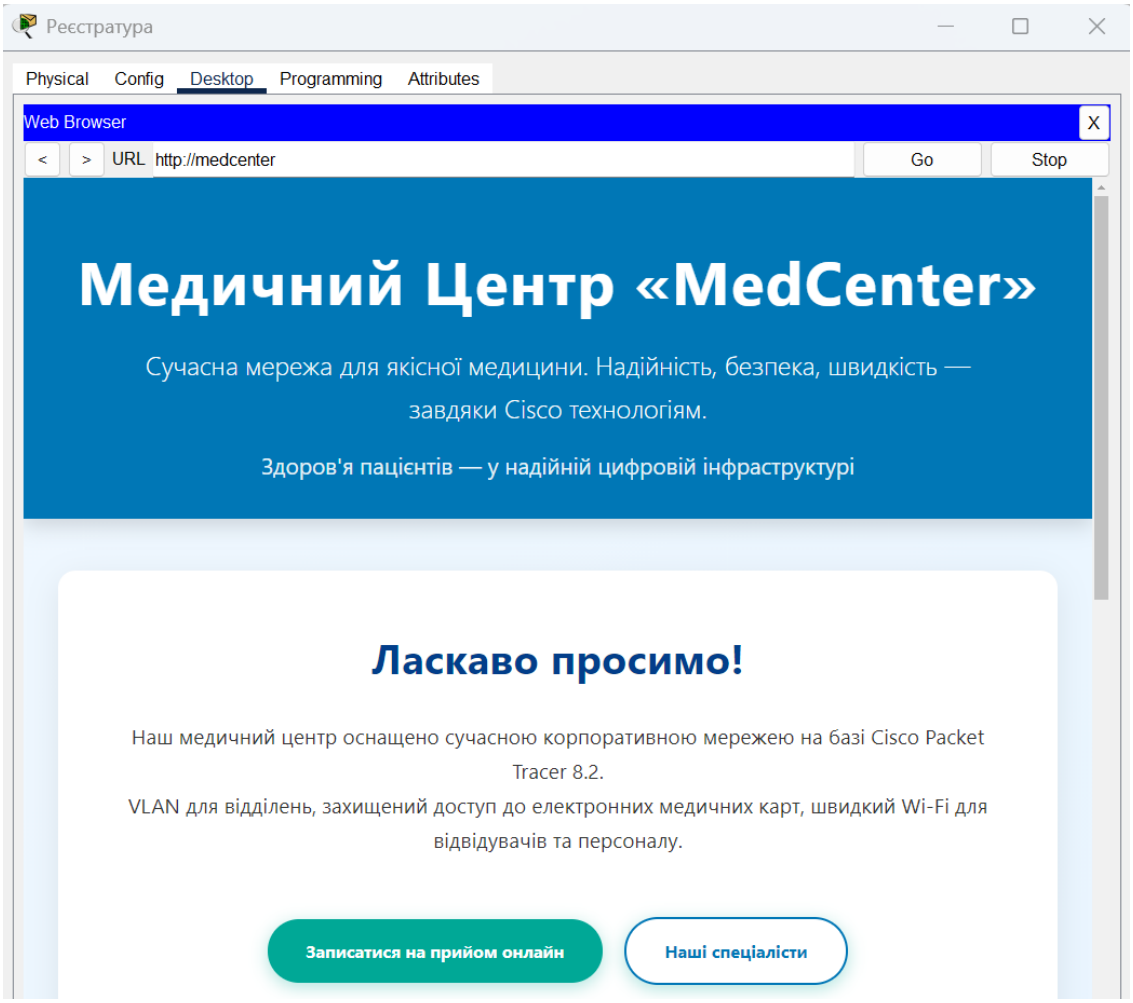

Рисунок 3.21 – Вебсайт медичного центру успішно функціонує

Для перевірки коректності роботи списків контролю доступу з робочої станції поста охорони (VLAN 80) виконано спробу отримати доступ до мережі Інтернет, сервера 1 та сервера 2, на якому розміщено FTP-сервер. Перевірка проводилась шляхом надсилання ICMP-запитів (команда ping) до відповідних адресатів з метою підтвердження або спростування наявності з’єднання. Як результат перевірки (рис. 3.22) встановлено, що робоча станція поста охорони не має доступу до мережі Інтернет та до підмережі серверної кімнати, що повністю відповідає налаштованим правилам ACL. Водночас доступ до сервера 2, на якому розміщено FTP-сервер для зберігання записів з камер відеоспостереження, єнаявним, що також підтверджує коректність налаштованих дозвільних правил для цього сегмента мережі [23].

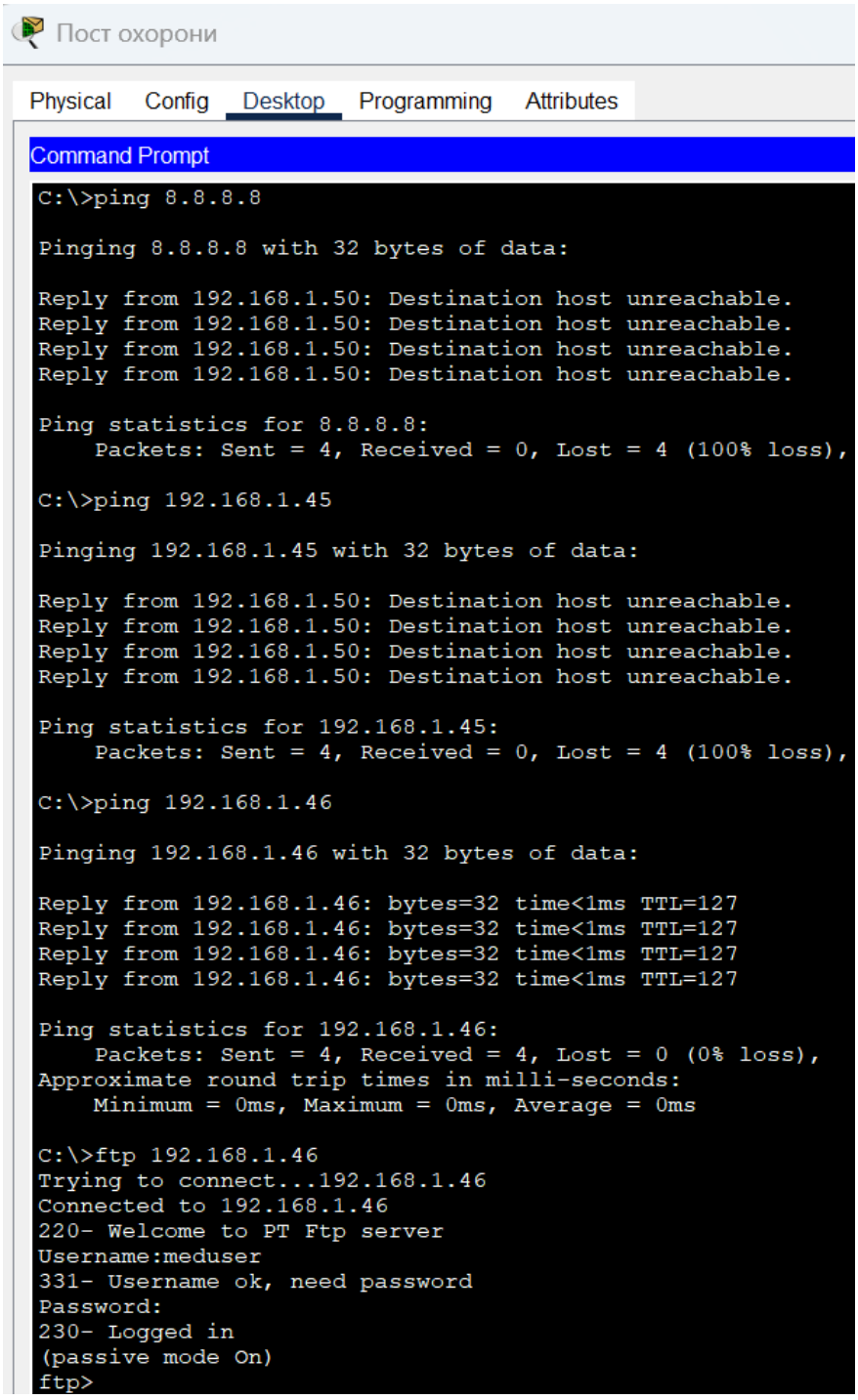

Рисунок 3.22 – Успішне функціонування ACL для VLAN 80

Також перевірено роботу списку доступу для VLAN 30. Як результат (рис. 3.23) – безпровідні клієнти мають доступ до Інтернету та до вебсайту медцентру, але не отримають доступ до інших ресурсів. Отже, даний список доступу для VLAN 30 працює добре.

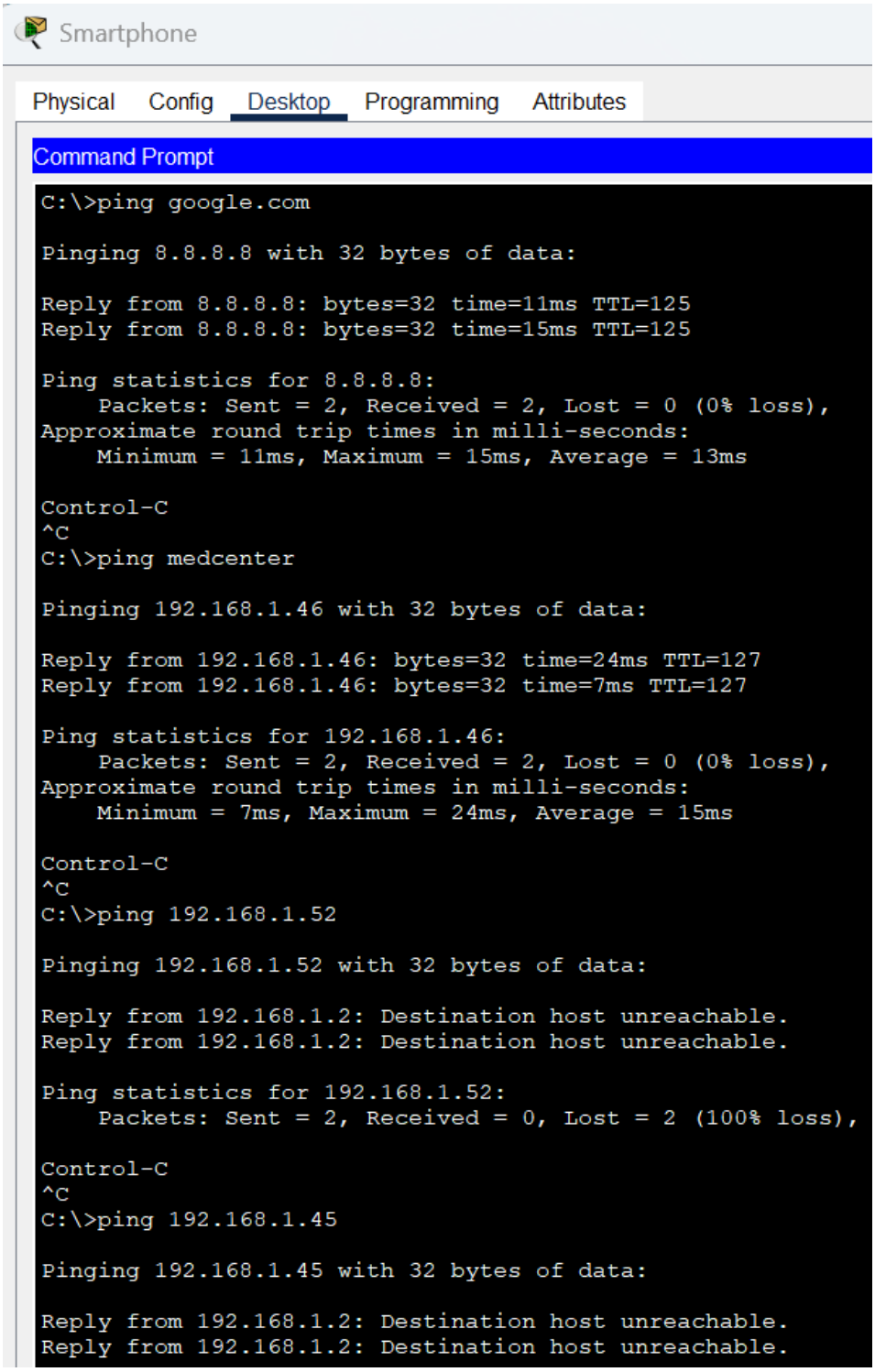

Рисунок 3.23 – Успішне функціонування ACL для VLAN 30

Для перевірки безпечного виходу в мережу Інтернет (NAT/PAT) – з ПК Реєстратура до Server Internet надіслано ping-запит. Як результат – технологія NAT/PAT дозволила приховати IP-адресу ПК Реєстратура. На виході з фаєрволу

ASA 5505 у пакеті IP Header Src. IP: 192.168.0.137 змінилась на зовнішню IP-адресу фаєрволу – 10.10.2.2 (рис. 3.24). Даний підхід забезпечив вихід в мережу Інтернет всього медичного центру лише за допомогою однієї зовнішньої адреси, а також дозволив приховати внутрішню мережу (її будову, конкретні адреси) від зловмисників [23].

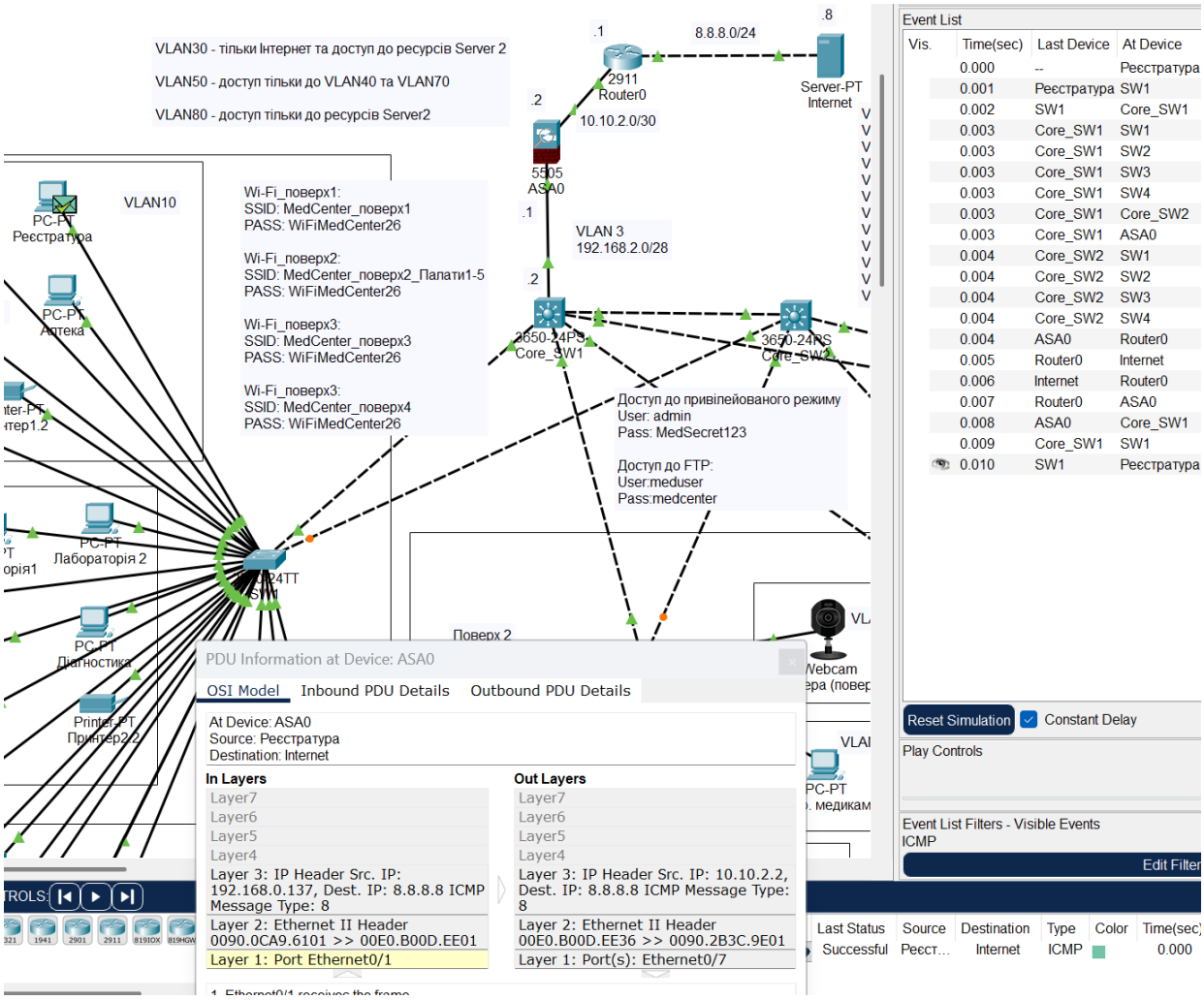

Рисунок 3.24 – Успішне функціонування технології NAT/PAT при доступі в мережу Інтернет

У підсумку представлено макет готової мережі для медичного центру, яка розроблена в середовищі проєктування Cisco Packet Tracer (рис. 3.25).

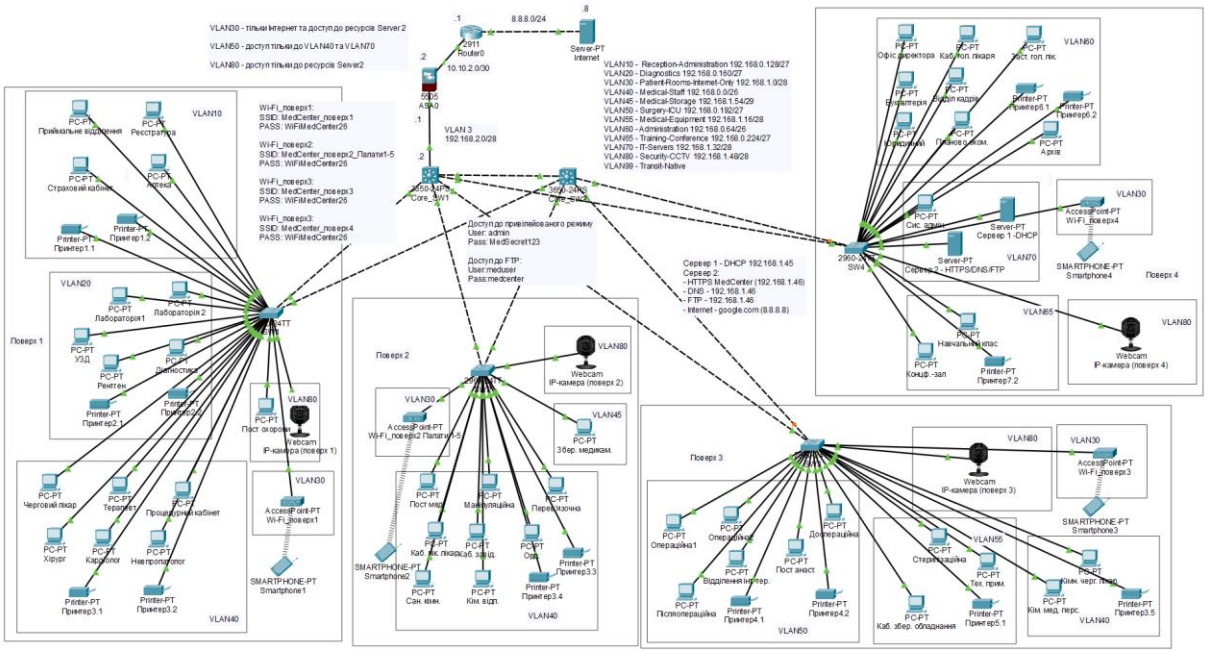

Рисунок 3.25 – Вигляд макету спроєктованої мережі для медичного центру

ВИСНОВКИ

У ході виконання кваліфікаційної роботи спроєктовано сучасну мережу медичного центру. Основна мета роботи – створення надійної, безпечної та високопродуктивної комп'ютерної мережі медичного закладу, яка відповідає усім стандартам та поставленим вимогам.

В кваліфікаційній роботі здійснено детальний аналіз медичного центру, розглянуто структуру та функції кожного поверху, а також завдяки спроєктованому плану – визначено функціональні потреби та сформовано основні технічні вимоги до мережі. Зазначено, що потрібно чітко сегментувати трафік (VLAN), забезпечити контроль доступу (ACL), надійність мережі (HSRP), масштабованість та безпечний вихід у глобальну мережу Інтернет (NAT/PAT).

В роботі обґрунтовано вибір фізичної топології мережі, в ході якого обрано ієрархічну розширену зірку, та здійснено підбір обладнання на користь провідного лідера Cisco. Обрано мережевий екран Cisco ASA 5505, два комутатори 3 рівня Cisco Catalyst WS-C3650-24PD-S, чотири комутатори 2 рівня Cisco Catalyst 2960X-48FPS-L, чотири бездротові точки доступу WiFi Cisco AIR-AP1852I-E-K9 та вісім IP-камер Cisco Meraki MV72-HW.

При проєктуванні мережі зроблено поділ мережі 192.168.0.0/16 на дванадцять підмереж (включаючи одну технічну) з використанням технології VLSM. Кожну підмережу призначено власній VLAN, налаштовано комутатори для кінцевих пристроїв, створено trunk-порти для магістральної передачі трафіку, забезпечено роботу Inter-VLAN routing з протоколом HSRP, налаштовано розширені списки контролю доступу (ACL), сконфігуровано сервери, а також налаштовано NAT overload на фаєрволі ASA 5505 для безпечного виходу в Інтернет. Заключним етапом стало проведення комплексного тестування працездатності та безпеки мережі, яке підтвердило, що забезпечено виконання усіх поставлених вимог та функціональних потреб.

Оскільки розроблена модель комп’ютерної мережі відповідає всім сучасним стандартам, то її можна рекомендувати як технічну основу для впровадження в закладах медичних центрів аналогічних масштабів. Також завдяки правильному підходу до процесу проєктування, розроблена мережа має значні перспективи для подальшого розвитку, а саме: можна впровадити єдину централізовану систему моніторингу та керування, можна організувати додаткові DMZ-зони, забезпечити підключення до резервного Інтернет-провайдера, здійснити додатковий поділ WiFi для гостьової мережі, а також провести інтеграцію мережі з системами IoT для моніторингу показників пацієнтів у реальному часі.

Отже, мета, яка була поставлена для виконання в цій кваліфікаційній роботі, досягнута в повному обсязі. Спроєктоване рішення є сучасним, надійним, ефективним та повністю готовим до використання.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Що таке DHCP? Простий посібник із розуміння призначення IP-адрес. Fiberroad Technology. URL: https://fiberroad.com/uk/resources/glossary/what-is-dhcp/ (дата звернення: 12.02.2026).

2. DNS – що це і як працює? Для новачків простими словами | Блог HOSTiQ.ua. Блог хостера HOSTiQ.ua. URL: https://hostiq.ua/blog/ukr/how-does-dns-work/?gad_source=1&gad_campaignid=23093471662&gbraid=0AAAAAC7A2B_Bb1V_HDLa4AgbxCkGSKrxR&gclid=CjwKCAjw8arQBhB9EiwAfIKdQvub8Uvz7RXrbayiG6t9oAU7IbDNbcNHxvKNmYbgy3xUvzTfG0o53RoCofUQAvD_BwE (дата звернення: 12.02.2026).

3. FTP: що це таке і як працює | HOSTiQ Wiki. HOSTiQ Wiki. URL: https://hostiq.ua/wiki/ukr/ftp/ (дата звернення: 13.02.2026).

4. IT Essentials. Захищена сторінка. URL: https://surl.li/xaapuz (date of access: 18.02.2026).

5. Мережні топології. StudFiles. URL: https://surl.li/ikfwcc (дата звернення: 19.02.2026).

6. Будуємо доступ: топології та обладнання - Компанія "Бізнес-Технології Онлайн". Компанія "Бізнес-Технології Онлайн". URL: https://cbto.com.ua/budujemo-dostup-topolohiji-ta-obladnannya.html (дата звернення: 20.02.2026).

7. What Is Inter-VLAN Routing?. JumpCloud. URL: https://jumpcloud.com/it-index/what-is-inter-vlan-routing (date of access: 27.02.2026).

8. Міжмережевий екран Cisco ASA 5505 (PoE) - опис, характеристики, ціна. Маршрутизатор Cisco від serversell.com.ua. Serversell - Интернет магазин серверного оборудования. URL: https://serversell.com.ua/merezheve-obladnannja/marshrutizator/mizhmerezhevij-ekran-cisco-asa-5505 (дата звернення: 01.03.2026).

9. MikroTik. MikroTik · Routers and Wireless. URL: https://mikrotik.com/ (date of access: 09.03.2026).

10. Cisco Catalyst 3650 Series Switches Data Sheet. Cisco. URL: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3650-series-switches/data_sheet-c78-729449.html (date of access: 16.03.2026).

11. ТехноТрейд. Інтернет-магазин Wi-Fi обладнання ТехноТрейд. Мережеве Wi-Fi обладнання для інтернета. Інтернет-магазин по продажу обладнання для локальної мережі. Купити WiFi обладнання для бездротової мережі. URL: https://www.technotrade.com.ua/Products/MikroTik_CCR2004-16G-2Splus.php (дата звернення: 21.03.2026).

12. Комутатор cisco catalyst ws-c2960x-48fps-l - купити недорого, Prom.ua: ціни, акції і відгуки | Україна, Київ. Prom.ua. URL: https://prom.ua/ua/Kommutator-cisco-catalyst-ws-c2960x-48fps-l.html (дата звернення: 25.03.2026).

13. Комутатори на HOTLINE - купити комутатори 8 порти | вигідні ціни в Києві, Харкові, Дніпрі, Одесі. Hotline.ua. URL: https://surl.lt/cyacgl (дата звернення: 27.03.2026).

14. Точка доступу Cisco AIR-AP1852I-E-K9. Cisco.com.ua. URL: https://xn--h1aemkx.com.ua/tochka-dostupa-cisco-air-1852i-air-ap1852i-e-k9 (дата звернення: 28.03.2026).

15. cAP ax | MikroTik. MikroTik · Routers and Wireless. URL: https://mikrotik.com/product/cap_ax (date of access: 01.04.2026).

16. MV72 Series Datasheet. Cisco Meraki. URL: https://meraki.cisco.com/product-collateral/mv72-datasheet/?file. (date of access: 05.04.2026).

17. Придбати HikVision DS-2CD2143G0-I у Києві. Найкраща ціна по Україні. Огляд, характеристики. Network Tools. URL: https://ntools.com.ua/uk/hikvision-ds-2cd2143g0-i-ip-kamera (дата звернення: 08.04.2026).

18. GeeksforGeeks. Introduction of Variable Length Subnet Mask (VLSM) - GeeksforGeeks. GeeksforGeeks. URL: https://www.geeksforgeeks.org/computer-networks/introduction-of-variable-length-subnet-mask-vlsm/ (date of access: 13.04.2026).

19. VLAN Configuration on Cisco Packet Tracer - 2026 Updated. IPCisco. URL: https://ipcisco.com/lesson/cisco-packet-tracer-vlan-configuration-example-ccna/. (date of access: 19.04.2026).

20. Packet Tracer 8.2 - HSRP Configuration - Packet Tracer Network. Packet Tracer Network. URL: https://www.packettracernetwork.com/tutorials/hsrp-configuration-new.html (date of access: 26.04.2026).

21. 3 Steps of Cisco Extended ACL Configuration with Packet Tracer ⋆ IPCisco. IPCisco. URL: https://ipcisco.com/lesson/extended-access-list-configuration-with-packet-tracer-2/ (date of access: 01.05.2026).

22. Cisco & Cisco Router, Network Switch. Configuring NAT on Cisco ASA - Cisco & Cisco Network Hardware News and Technology. Cisco & Cisco Network Hardware News and Technology. URL: https://ciscorouterswitch.over-blog.com/article-configuring-nat-on-cisco-asa-117127180.html (date of access: 12.05.2026).

23. ITExamAnswers. 5.4.6 Packet Tracer - Use Diagnostic Commands Answers. ITExamAnswers.net. URL: https://itexamanswers.net/5-4-6-packet-tracer-use-diagnostic-commands-answers.html (date of access: 18.05.2026).