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 кібербезпеки
(повне найменування кафедри)

КВАЛІФІКАЦІЙНА РОБОТА ЗА СТУПЕНЕМ ВИЩОЇ ОСВІТИ «БАКАЛАВР»

КОМП'ЮТЕРНА МЕРЕЖА КОМУНАЛЬНОГО НЕКОМЕРЦІЙНОГО ПІДПРИЄМСТВА «ОСТРОЖЕЦЬКА РАЙОННА ЛІКАРНЯ»

COMPUTER NETWORK OF COMMUNAL NON-PROFIT ENTERPRISE «OSTROZHETSK DISTRICT HOSPITAL

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

освітня програма Комп'ютерна інженерія
(назва освітньої програми)

Виконав: здобувач вищої освіти
групи КІс-21
Мосійчук Андрій Сергійович

(підпис)

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

(підпис)

Кваліфікаційну роботу
допущено до захисту
« 11 » червня 2024 р.
Гарант освітньої програми:
к.т.н., доцент
Лавренчук Світлана Василівна

(підпис)

Луцьк – 2024 року

ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

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

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ проф. Н.Чернящук
« 10 » 01 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ВИЩОЇ ОСВІТИ

Мосійчуку Андрію Сергійовичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи *Комп'ютерна мережа комунального некомерційного підприємства «Острожецька районна лікарня»*

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

затверджені наказом закладу вищої освіти від «30» грудня 2023 року № 459/01-02
2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 11.06.2024р.

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 та різні інтернет-ресурси технічного спрямування*

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити):
Вступ
Аналіз завдання
Техніко-економічне обгрунтування
Обладнання та налаштування
Висновки

5. Перелік графічного (ілюстративного) матеріалу:

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис	
		завдання видав	завдання прийняв
Аналіз завдання	*Багнюк Н.В., доцент*		
Техніко-економічне обгрунтування	*Багнюк Н.В., доцент*		
Обладнання та налаштування	*Багнюк Н.В., доцент*		
Нормоконтроль	*Багнюк Н.В., доцент*		
Гарант ОП	*Лавренчук С.В., доцент*		
Показник запозичень тексту	***___%***		
Академічна доброчесність	*Міскевич О.І.,асистент*		

7. Дата видачі завдання 10.01.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	*Розділ 1. Аналіз завдання*	до 15.02.2024 р.	Виконано
2.	*Розділ 2. Техніко-економічне обгрунтування*	до 15.03.2024 р.	Виконано
3.	*Розділ 3. Обладнання та налаштування*	до 04.05.2024 р.	Виконано
4.	*Висновки та пропозиції*	до 07.05.2025 р.	Виконано
5.	*Формування списку використаних джерел*	до 10.05.2024 р.	Виконано
6.	*Формування додатків*	до 15.05.2024 р.	Виконано
7.	*Оформлення ілюстративного матеріалу*	до 20.05.2024 р.	Виконано
8.	*Нормоконтроль*	до 01.06.2024 р.	Виконано
9.	*Інструментальна перевірка на академічний плагіат*	до 04.06.2024 р	Виконано
10.	*Представлення кваліфікаційної роботи бакалавра до захисту*	до 11.06.2024 р.	Виконано

Здобувач вищої освіти _____ Мосійчук А.С.
(підпис) (прізвище, ініціали)

Керівник кваліфікаційної роботи _____ Багнюк Н.В.
(підпис) (прізвище, ініціали)

АНОТАЦІЯ

Мосійчук А.С. Комп’ютерна мережа КНП «Острожецька районна лікарня»

Кваліфікаційна робота бакалавра ОП «Комп’ютерна інженерія» спеціальності 123 Комп’ютерна інженерія. Луцький національний технічний університет. Луцьк, 2024. 64 с.

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

Перший розділ присвячений аналізу проектування комп’ютерної мережі.

Другий розділ розкриває техніко-економічне обґрунтування фізичної топології комп’ютерної мережі.

Третій розділ технічного проекту містить шість підрозділів: вибір активного мережевого обладнання; розрахунок логічної адресації; комутація; маршрутизація; організація доступу до інтернет.

Ключові слова: комп’ютерна мережа, з’єднання, комутатор, налаштування, маршрутизація, інтернет, зв’язок.

ANNOTATION

Mosiychuk A.S. «Computer Network of KNP «Ostrohets Regional Hospital» Bachelor's Qualification Work of the Educational Program «Computer Engineering» in the Specialty 123 Computer Engineering.

Lutsk National Technical University. Lutsk, 2024. 64 pages. The qualification work consists of an introduction, three chapters, conclusions, a list of references, and appendices.

The first chapter is dedicated to the analysis of computer network design.

The second chapter elaborates on the technical and economic justification of the physical topology of the computer network.

The third chapter of the technical project contains six subsections: selection of active network equipment; logical addressing calculation; switching; routing; and organization of internet access.

Keywords: computer network, connection, switch, configuration, routing, internet, communication.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ВТМВ – вторинний телекомунікаційний вузол.

ПТМВ – центральний (первинний) телекомунікаційний вузол.

ПК – персональний комп’ютер.

ВСТУП

В сучасному світі комп’ютерні мережі стали невід’ємною частиною будь-якої організації, забезпечуючи ефективну комунікацію та обмін інформацією між різними підрозділами. Це особливо актуально для медичних закладів, де своєчасний доступ до інформації може врятувати життя пацієнтів та підвищити якість медичних послуг.

Ця кваліфікаційна робота присвячена розробці комп’ютерної мережі для КНП «Острожецька лікарня». Метою роботи є створення надійної та безпечної мережевої інфраструктури, яка задовольняє потреби лікарні в оперативному обміні даними, зберіганні та обробці медичної інформації.

Розробка комп’ютерної мережі для КНП «Острожецька лікарня» включає такі завдання:

– аналіз існуючих систем і потреб лікарні та проектування мережевої архітектури;

– вибір обладнання та програмного забезпечення;

– впровадження і тестування мережі, забезпечення її захисту та надійності.

Особливу увагу приділено питанням безпеки даних, адже медична інформація є надзвичайно чутливою і потребує високого рівня захисту від несанкціонованого доступу та втрат. Важливо також забезпечити високу пропускну здатність і стабільність мережі, щоб забезпечити безперебійний доступ до інформації для медичного персоналу.

У роботі використано сучасні методи і технології проектування та впровадження комп’ютерних мереж з урахуванням специфіки медичного закладу та вимог до захисту медичних даних.

Таким чином, результатом цієї кваліфікаційної роботи є детально розроблений проєкт комп’ютерної мережі для КНП «Острожецька лікарня», який

готовий до впровадження і забезпечить всі необхідні умови для ефективної роботи медичного закладу.

РОЗДІЛ 1
АНАЛІЗ ЗАВДАННЯ

1.1 Характеристика об’єкта проектування

Завдання кваліфікаційної роботи – проектування комп’ютерної мережі для КНП «Острожецька районна лікарня». Забезпечити необхідні служби, організувати вихід в мережу Інтернет.

КНП «Острожецька районна лікарня», для якого розробляється комп’ютерна мережа, складається з 4 корпусів. Корпуси містять кабінети, палати, лабораторії та адміністративні кабінети. У першому корпусі знаходить головний (первинний) телекомунікаційний вузол (ПТМВ), наступні корпуси оснащені вторинним телекомунікаційним вузлом (ВТМВ). Площі кабінетів, їх номери та кількість мережевих розеток під RG-45 описані у таблицях 1.1–1.4 відповідно.

Таблиця 1.1 – Перелік кабінетів, корпус 1

Номер кабінету	Назва кабінету	Площа кабінету, м²	Кількість інформ. розеток, R (R=S/6)
1	Адміністративне приміщення	8	3
2	Приймальне відділення	22	8
3	Приміщення виписки	8	3
7	ПТВМ	10	–
9	Кабінет хірурга	24	4
10	Зав. відділення	24	4
14	Лабораторія	16	3
20	Кабінет рентгену	20	6
32	Черговий	6	2
33	Кабінет окуліста	20	8

Таблиця 1.2 – Перелік кабінетів, корпус 2

Номер кабінету	Назва кабінету	Площа кабінету, м²	Кількість інформ. розеток, R (R=S/6)
2	Кабінет сімейного лікаря	25	16
6	Кабінет кардіолога	24	3
9	Архів	10	3
10	ВТВМ2	10	–
12	Стерилізаційний кабінет	10	2
14	Кабінет лора	24	6
17	Кабінет стоматолога	16	4
20	Кабінет терапевта	20	6
28	Черговий	7	2

Таблиця 1.3 – Перелік кабінетів, корпус 3

Номер кабінету	Назва кабінету	Площа кабінету, м²	Кількість інформ. розеток, R (R=S/6)
5	Приймальне відділення	22	8
6	Приміщення виписки	8	3
7	ВТВМ3	10	–
9	Кабінет головного лікаря	24	4
14	Лабораторія	16	3

Таблиця 1.4 – Перелік кабінетів, корпус 4

Номер кабінету	Назва кабінету	Площа кабінету, м²	Кількість інформ. розеток, R (R=S/6)
2	Лабораторія	20	6
3	Кабінет зуботехніка	20	3
7	ВТВМ4	10	–

1.2 Аналіз вимог до комп’ютерної мережі

Відповідно до вимог ДСТУ та обґрунтувань, включених у технічне завдання кваліфікаційної роботи, комп’ютерна мережа для КНП «Острожецька районна лікарня» має відповідати таким критеріям:

– забезпечити можливість підключення стаціонарних комп’ютерів до локальної мережі лікарні у кабінетах, лабораторіях та інших службових приміщеннях. Також необхідно організувати наявність розеток для підключення до мережі у відповідних приміщеннях;

– забезпечити зв’язок між вузлами всередині мережі. Встановити процеси комутації, а також маршрутизації на активних пристроях обчислювальної мережі;

– використати комутатори третього рівня моделі OSI як активні мережеві пристрої для забезпечення взаємодії між корпусами та налагодження маршрутизації;

– використати апаратний брандмауер для забезпечення з’єднання з провайдерами телекомунікаційних послуг;

– організувати списки контролю доступу для різних функціональних відділень на брандмауері та інших пристроях, у випадку потреби;

– організувати централізовану серверну зону з двома типами доступу: обмеженим та загальним. Дозволити доступ до серверів з обмеженим доступом лише з локальної мережі лікарні.

Для серверів з загальним доступом налаштувати статичну трансляцію мережевих адрес, щоб забезпечити доступ до них з Інтернету;

– фізична структура мережі будується відповідно до стандартів IEEE 802.3z для формування вертикальної кабельної системи за допомогою оптично-волоконного кабелю;

– для забезпечення надійності комп’ютерної мережі потрібно передбачити необхідне резервування. Допускається періодичне оновлення інформації у разі вичерпання пам’яті.

Зовнішні лінії зв’язку мають забезпечувати:

– дотримання стандартів інтерфейсів та протоколів, зокрема IEEE 802.3z;

– забезпечення масштабованості пропускної здатності каналів зв’язку з можливістю налаштування швидкості передачі даних на рівні Nx1 та Nx10 Мбіт/с;

– гарантування виконання угоди щодо рівня обслуговування (SLA).

Комп’ютерна мережа має бути готова до розширення без внесення змін у наявні підсистеми. Це досягається шляхом забезпечення:

– наявності 30% вільного простору в телекомунікаційній шафі для розміщення нового обладнання.

– наповнення кабельних трас на 60%, щоб забезпечити місце для додаткових кабелів.

1.3 Опис інформаційних ресурсів та служб

У рамках кваліфікаційної роботи завданням є організації я служб, які забезпечують загальний, а також обмежений доступ. Сервіси загального доступу включають в себе DNS і HTTP.

DNS (Domain Name System) – це система, яка переводить прості для сприйняття доменні імена, такі як google.com, в унікальні числові IP-адреси, що призначені кожному пристрою в Інтернеті. Це спрощує доступ до веб-сайтів, а також інших ресурсів в Інтернеті для користувачів, оскільки вони не мають запам’ятовувати довгі рядки чисел. Крім того, DNS полегшує комунікацію між пристроями в Інтернеті, дозволяючи їм знаходити один одного за допомогою

доменних імен, замість виключного використання IP-адрес. Загалом, DNS відіграє важливу роль у налаштуванні доступу до Інтернету та робить його більш доступним та зручним для всіх користувачів [1].

Процес роботи протоколу DNS включає такі етапи:

1. Розпізнавання запиту: коли користувач вводить доменне ім’я в браузері, браузер відправляє запит до локального DNS-сервера. Якщо DNS-сервер має в кеші IP-адресу для цього доменного імені, він повертає її. Інакше, він переходить до наступного етапу.

2. Запит до ієрархії DNS-серверів: якщо локальний DNS-сервер не має в кеші необхідної інформації, він відправляє запит до іншого DNS-сервера. Якщо інший DNS-сервер має необхідну інформацію, він повертає її. Якщо ні, він переходить до наступного етапу.

3. Запит до кореневого DNS-сервера: якщо ні один з DNS-серверів не має необхідної інформації, запит відправляється до кореневого DNS-сервера, який містить інформацію про всі доменні зони в Інтернеті.

4. Пошук IP-адреси: коли запит до кореневого DNS-сервера прибуває, він відповідає з інформацією про DNS-сервери верхнього рівня. DNS-сервер, що отримав запит, звертається до одного з цих DNS-серверів, щоб дізнатися, на якому DNS-сервері зберігається інформація про запитуваний домен. Потім він повертає відповідь запитуючому пристрою.

Протокол передачі гіпертексту, або HTTP, є основним протоколом для передачі даних між веб-серверами та веб-клієнтами.

Коли користувач вставляє адресу веб-сайту у свій браузер, браузер надсилає HTTP-запит на веб-сервер. Цей запит містить інформацію про те, які файли або ресурси потрібно отримати, такі як файли HTML чи фотографії. Потім веб-сервер відповідає на цей запит, надсилаючи запрошені матеріали назад через HTTP. У цьому процесі браузер користувача виступає як клієнт, що надсилає

запити, а веб-сервер виконує роль сервера, який відповідає на ці запити, надаючи вміст.

Запит відправляється від клієнта до сервера за допомогою механізму запит-відповідь HTTP. Після цього сервер відповідає кодом статусу, що вказує, чи був запит успішним, і якщо так, то браузер клієнта відтворює отриманий вміст.

В цілому, HTTP є важливою складовою Всесвітньої павутини, що забезпечує користувачам зручний доступ до веб-вмісту та взаємодію з ним.

Основний порядок дій за протоколом HTTP виглядає наступним чином:

1. Встановлення з’єднання: клієнт відкриває з’єднання з сервером, надсилаючи запит з методом «CONNECT». Якщо сервер приймає з’єднання, він відповідає кодом «200 OK», і з’єднання встановлюється.

2. Відправлення запиту: клієнт надсилає запит на сервер з методом, шляхом та версією HTTP. Запит може містити також додаткові параметри, такі як заголовки та дані запиту.

3. Обробка запиту сервером: сервер обробляє отриманий запит і відправляє відповідь клієнту з кодом статусу, який вказує на результат обробки. Коди статусу включають, наприклад, «200 OK» (успішний запит) чи «404 Not Found» (помилка – ресурс не знайдено).

4. Отримання відповіді: клієнт отримує відповідь від сервера, яка містить код статусу, заголовки та дані відповіді. Залежно від коду статусу, клієнт обробляє відповідь і виконує відповідні дії.

5. Закриття з’єднання: після повного оброблення запиту і відповіді з’єднання між клієнтом і сервером закривається.

Цей процес може повторюватися для кожного запиту. Серед служб обмеженого доступу є DHCP і SYSLOG.

DHCP (Dynamic Host Configuration Protocol) – це мережевий протокол, що автоматизує процес призначення IP-адрес пристроям у мережі [2].

Головна перевага DHCP полягає у спрощенні адміністрування мережі, оскільки він усуває потребу для адміністраторів вручну призначати IP-адреси кожному пристрою. DHCP можна налаштувати на автоматичне призначення IP-адрес, масок підмережі, а також шлюзів за замовчуванням пристроям у мережі. Це дозволяє ефективніше використовувати ресурси та зменшує адміністративні витрати.

Поміж інших переваг, які пропонує DHCP, варто відзначити наступне:

– Зменшення простою мережі: DHCP може бути налаштований для автоматичного оновлення оренди IP-адрес для пристроїв у мережі. Це гарантує постійну наявність дійсних IP-адрес, зменшуючи ризик простою мережі через конфлікти або закінчення терміну оренди.

– Централізоване керування: DHCP-сервери можуть бути керовані централізовано, що дозволяє ефективніше управляти призначенням IP-адрес у всій мережі.

– Масштабованість: DHCP розроблено для використання у великих мережах, що робить його ідеальним рішенням для організацій, які мають управляти великою кількістю пристроїв.

– Безпека: DHCP може бути налаштований для забезпечення безпечного призначення IP-адрес, що допомагає запобігти несанкціонованому доступу до мережі.

У різних операційних системах, мережевих пристроях та програмах реєстрація подій виконується за допомогою стандартного протоколу, відомого як Syslog. Цей протокол збирає системні журнали, а також повідомлення з різних джерел і зберігає їх в одному місці для зручного моніторингу, аналізу та виправлення несправностей.

Формат повідомлень журналу та механізм їх передачі через мережеві пристрої визначаються протоколом syslog. Це дає змогу системним адміністраторам відстежувати мережеві події й проблеми і вирішувати їх.

Шляхом перегляду, фільтрування, а також сортування журналів можна виявити можливі проблеми та підвищити ефективність системи. Засоби, серйозного рівню, мітки часу та самі повідомлення є стандартними складовими частинами системного журналу. Ці елементи допомагають визначити джерело повідомлення наприклад, мережевий пристрій або програму та вказують на його серйозність. Кожне повідомлення є фактичним записом у журналі, а мітка часу вказує на дату й час створення цього повідомлення.

Існують як комерційні, так і відкриті системні сервери, які можуть приймати, а також зберігати повідомлення системного журналу. Ці сервери надають можливості централізованого керування журналами й можуть бути налаштовані для надсилання сповіщень у випадку певних подій. Загалом, за допомогою протоколу syslog системні адміністратори можуть в реальному часі відслідковувати та вирішувати мережеві події та збої [3].

Процес роботи syslog складається з таких кроків:

1. Збір повідомлень: системні події, що відбуваються на комп’ютері, фіксуються в журналах, які можуть містити повідомлення про роботу програм, інформацію про помилки та інше.

2. Передача повідомлень: журнали обробляються спеціальною програмою (syslogd), яка відправляє їх на віддалені сервери для аналізу, а також збереження.

3. Обробка повідомлень: на сервері syslog отримані повідомлення класифікуються за типом та пріоритетом, що вказується у заголовку повідомлення.

4. Збереження повідомлень: оброблені повідомлення зберігаються у вигляді журналу або бази даних, де їх можна використовувати для відслідковування проблем, а також відновлення роботи системи.

5. Аналіз і моніторинг: на основі зібраних даних створюються звіти про стан системи, що допомагає зрозуміти, як вона функціонує, виявити можливі

проблеми та прийняти необхідні заходи для їх вирішення. Загалом, syslog дозволяє віддалено контролювати та аналізувати роботу системи, що сприяє забезпеченню її стабільності та неперервності роботи.

РОЗДІЛ 2
ТЕХНІКО-ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ

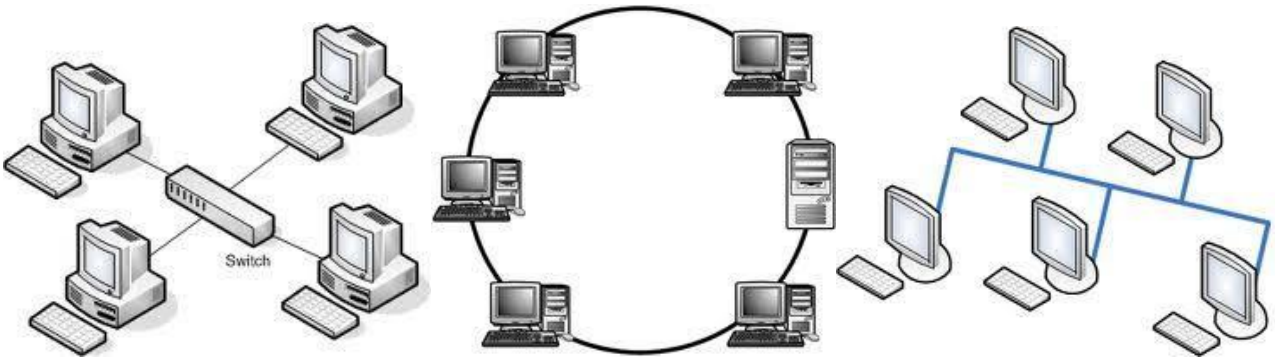
2.1 Обґрунтування фізичної топології комп'ютерної мережі

Структура мережі визначає, як комп'ютери, кабелі, а також інші складові розташовані фізично, що має значний вплив на надійність та ефективність мережі. Вона передбачає використання певного типу кабелю, методику прокладання кабелю та способи взаємодії комп'ютерів. У світі існують три основних типи таких структур: шинна, кільцева та зіркова.

У топології зірка (рис. 2.1, а), центральний вузол з'єднаний з усіма робочими станціями, що забезпечує високу пропускну здатність та ефективність мережі. Однак центральний вузол є найбільш вразливою точкою з погляду надійності мережі: у разі його відмови весь мережевий обмін припиняється. Побудова зіркової топології вважається досить простою, але вона потребує значних витрат на розкладання кабелю, особливо якщо центральний вузол розташований не в центрі географічної області мережі [4].

Кільцева топологія (рис. 2.1, б) передбачає, що кожен вузол мережі має з'єднання тільки з двома іншими вузлами. Кожна робоча станція зв'язана зі станцією посередині та передає інформацію далі вздовж кільця до отримувача. Чим більше станцій у мережі, тим триваліше відбувається передача даних. Географічне розташування вузлів, а також їх віддаленість один від одного можуть вимагати значних витрат на прокладання кабелю, а відмова хоча б однієї станції може призвести до неефективності всієї мережі [5].

У шинній топології (рис. 2.1, в) всі пристрої з'єднані з однією спільною лінією для комунікації. Будь-який пристрій може спілкуватися з будь-яким іншим пристроєм, що також підключений до цієї лінії. Основною перевагою цієї топології є простота розширення мережі, але недоліком є складність централізованого управління [6].



а б в

Рисунок 2.1. – Топології мереж «зірка» (а), «кільце» (б) і шинна (в) [5]

Для створення даної мережі була вибрана розширена зіркова топологія, в якій кожен вузол, який виходить з центрального, є центром нової зірки. Ця топологія є найбільш оптимальною та поширеною для розбудови корпоративних мереж (рис. 2.2).

Рисунок 2.2 – Топологія мережі розширена зірка [4]

2.2 Укрупнений розрахунок варіантів технічних засобів телекомунікацій

Для побудови мережі необхідне відповідне апаратне забезпечення, яке відповідає вимогам, встановленим у завданні. До нього входять такі телекомунікаційні пристрої:

- Firewall;
- комутатор 3 рівня;
- комутатори 2 рівня моделі OSI;
- безпровідна точка доступу.

Устаткування повинно демонструвати надійність та забезпечувати високу якість роботи. Для порівняння було обрано пристрої двох світових лідерів у виробництві телекомунікаційного обладнання – Cisco та D-Link [7].

Для порівняння можна вибрати такі міжмережеві екрани (таблиця 2.1):

- D-Link DFL-860E;
- CISCO ASA 5510.

Таблиця 2.1 – Порівняльна характеристика міжмережевих екранів

Пристрій	D-Link DFL-860E	CISCO ASA 5510
Інтерфейси	2 x 10/100/1000Base-TX WAN 1 x 10/100/1000Base-TX DMZ 8 x 10/100/1000Base-TX LAN 2 x USB 1 x Console RJ-45	2 x USB 4 x 10/100Base-TX 1 x Console RJ-45 1 x AUX

Продовження таблиці 2.1

Пристрій	D-Link DFL-860E	CISCO ASA 5510
Пропускна здатність	200 Мбіт/с VPN: 60 Мбіт/с	300 Мбіт/с VPN: 170 Мбіт / с
Функції	PPPoE, NAT, PAT, OSPF, (ALG), Zone-Defense	NAT, PAT, OSPF, PIM, IPv6, QoS, Risk Rating, Meta Event Generato, IPSec VPN: 250, SSL VPN: 2
VLAN/VPN	+/+	+/+
Відмовостійкість	Резервування каналу WAN	Резервування каналу WAN
Виявлення вторгнень	Автоматичне оновлення шаблонів Захист від атак DoS, DDoS	Система запобігання вторгнення (IPS). Захист від атак «переповнення буферу».

Розглянувши особливості обраних пристроїв, було вирішено використовувати пристрій CISCO ASA 5510 (рис. 2.3) як міжмережевий екран для мережі.

Рисунок 2.3 – Міжмережевий екран Cisco ASA 5510 [8]

Для порівняння бездротового обладнання були обрані наступні дві

бездротові точки доступу: D-Link DAP-2610 і Cisco C9115AXI-H. Їх характеристики наведено в таблиці 2.2.

Таблиця 2.2 – Порівняльна характеристика комутаторів

Характеристика	Cisco C9115AXI-H	D-Link DAP-2610
Швидкість передачі даних	5,2 Гбіт/сек	1,75 Гбіт/сек
Стандарти Wi-Fi	802.11a/b/g/n/ac/ax	802.11a/b/g/n/ac
Кількість антен	4 внутрішніх	4 зовнішніх
Кількість портів Ethernet	2 (10/100/1000 Мбіт/сек)	1 (10/100/1000 Мбіт/сек)
Кількість одночасних підключень	До 200	До 64
Функції безпеки	WPA3, 802.1X, ACL, MAC-адреса, гостьовий доступ, VPN-прохід, радіус-автентифікація	WPA/WPA2, 802.1X, ACL, гостьовий доступ
Управління	Локальне та хмарне управління, контролери Cisco DNA Center і WLC	Локальне управління, без підтримки хмарних технологій

Після аналізу технічних характеристик бездротових точок доступу для забезпечення бездротового доступу до Інтернету, було вирішено обрати Cisco C9115AXI-H (рис. 2.4).

У таблиці 2.3 подано порівняльний аналіз технічних характеристик комутаторів, що підтримують функції на рівні 3 моделі OSI: Cisco Catalyst 2960-X-24 та D-Link DGS-1210-28.

Рисунок 2.4 – Точка доступу Cisco C9115AXI-H [9]

Таблиця 2.3 – Порівняльна характеристика комутаторів 3 рівня

Характеристика	Cisco WS-C2960X-24PS-L	D-Link DGS-1210-28
Кількість портів	24	24
Швидкість передачі даних	10/100/1000 Мбіт/с	10/100/1000 Мбіт/с
Швидкість передачі даних між комутаторами	10 Гбіт/с	4 Гбіт/с
Підтримка стандартів безпеки	802.1X, ACL, DHCP Snooping, IP Source Guard, Private VLAN Edge, Port Security, etc.	802.1X, ACL, D-Link Safeguard Engine, IP-MAC-Port Binding, etc.
Можливість розширення мережі	Да, підтримка стекування (до 8 комутаторів)	Да, підтримка стекування (до 6 комутаторів)
Характеристика	Cisco WS-C2960X-24PS-L	D-Link DGS-1210-28

Продовження таблиці 2.3

Характеристика	Cisco WS-C2960X-24PS-L	D-Link DGS-1210-28
Підтримка VLAN	Да, до 4096 VLAN	Да, до 4K VLAN
Підтримка протоколів маршрутизації	OSPF, EIGRP, BGP, PIM, RIP	OSPF, RIP, VRRP
Управління	CLI, SNMP, RMON, Cisco Prime Infrastructure	Web-інтерфейс, CLI, SNMP, RMON, D-Link Network Assistant

Ці два комутатори подібні у багатьох аспектах, однак Cisco Catalyst WS-C2960X-24PS-L (рис. 2.5) має більше можливостей для розширення мережі та підтримки стандартів безпеки, таких як Private VLAN Edge та IP Source Guard. Саме тому він був обраний для використання як основний комутатор в корпусах (ПТМВ, ВТМВ2-4).

Рисунок 2.5 – Комутатор 3 рівня Cisco Catalyst 2960-X-24 [10]

Таблиця 2.4 містить порівняльний аналіз технічних характеристик комутаторів NETGEAR GS324TP і Cisco Catalyst WS-C2960-24LT-L, які можуть бути використані як некеровані комутатори (на рівні 2).

Таблиця 2.4 – Порівняльна характеристика комутаторів 2 рівня.

Характеристика	Cisco Catalyst WS-C2960	D-Link DGS-1024D
Кількість портів	24	24
Швидкість передачі даних	10/100 Mbps, 1000 Mbps	10/100/1000 Mbps
Керування мережею	Керований	Не керований
Мережеві протоколи	TCP/IP	TCP/IP, IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3x
Таблиця адресів MAC	8K записів	8K записів
Широкомовність і керування потоками	Підтримується	Не підтримується
VLAN	Підтримується	Не підтримується
Типи кабелів	Ethernet/Fast/Gigabit Ethernet (10/100/1000Base-T)	Ethernet/Fast/Gigabit Ethernet (10/100/1000Base-T)
Буферна пам’ять	64 МБ	5.5 МБ
Розміри	44.5 x 27.9 x 4.5 см	28 x 18 x 4.4 см

Вивчивши технічні характеристики обраних комутаторів, було прийнято рішення зупинитися на Cisco Catalyst WS-C2960-24LT-L (рис. 2.6), оскільки його параметри найкраще відповідають вимогам проектованої мережі.

Рисунок 2.6 – Комутатор Cisco Catalyst WS-C2960-24LT-L [11]

2.3 Структура комп’ютерної мережі

Структура комп’ютерної мережі є ключовим елементом для забезпечення її ефективної, надійної та безпечної роботи. Організована та чітка мережа дозволяє з високою якістю здійснювати проектування, впровадження та обслуговування. Недосконала структура може призвести до проблем, таких як вузькі місця, перевантаження, вразливості та труднощі з діагностикою та вирішенням несправностей. Навпаки, ретельно спланована мережа сприяє оптимізації продуктивності, зменшенню часу простою та підвищенню безпеки. Вона також допомагає ефективно використовувати ресурси та маршрутизувати трафік. Отже, структурована комп’ютерна мережа забезпечує високий рівень ефективності, надійності та безпеки в управлінні та плануванні [12].

Основними логічними частинами проектованої мережі є:

- мережа для вузлів 1 корпусу;
- мережа для вузлів 2 корпусу;
- мережа для вузлів 3 корпусу;
- мережа для вузлів 4 корпусу;
- мережа для серверів обмеженого доступу;
- мережа для серверів загально доступу.

Ці компоненти локальної мережі повинні мати доступ до Інтернету, який буде захищений міжмережевим екраном для забезпечення безпеки мережі.

РОЗДІЛ 3
ОБЛАДНЕННЯ ТА НАЛАШТУВАННЯ

3.1 Вибір активного мережевого обладнання

Вибір належного активного мережевого обладнання є ключовим для забезпечення ефективної та безпечної роботи комп'ютерної мережі. Недостатньо потужне або несумісне обладнання може викликати перебої у роботі мережі, повільну передачу даних та потенційну втрату важливої інформації. Окрім цього, застаріле обладнання може стати легкою ціллю для нових загроз та атак, що ставить під загрозу безпеку мережі та всієї організації [13].

Відповідно до вимог комп'ютерної мережі, ДСТУ та фізичної топології, для забезпечення ефективного функціонування обчислювальної мережі необхідно правильно вибрати мережеве обладнання для корпусів.

Перелік активного мережевого обладнання корпусу 1 представлено в таблиці 3.1.

Таблиця 3.1 – Перелік активного мережевого обладнання, корпус 1

Номер кабінету	Назва кабінету	Кількість інформ. розеток, RJ45	Мережеве обладнання, модель
1	Адміністративне приміщення	3	Cisco WS-C2960-24LT-L
2	Приймальне відділення	8	Cisco WS-C2960-24LT-L
3	Приміщення виписки	3	Cisco WS-C2960-24LT-L
7	ПТВМ	–	Cisco ASA 5510
			Cisco WS-C2960X-24PS-L
9	Кабінет хірурга	4	Cisco WS-C2960-24LT-L
10	Зав. відділення	4	Cisco WS-C2960-24LT-L
14	Лабораторія	3	Cisco WS-C2960-24LT-L
20	Кабінет рентгену	6	Cisco WS-C2960-24LT-L
32	Черговий	2	Cisco WS-C2960-24LT-L

Перелік активного мережевого обладнання корпусу 2 представлено в таблиці 3.2.

Таблиця 3.2 – Перелік активного мережевого обладнання, корпус 2

Номер кабінету	Назва кабінету	Кількість інформ. розеток, RJ45	Мережеве обладнання, модель
2	Кабінет сімейного лікаря	16	Cisco WS-C2960-24LT-L
6	Кабінет кардіолога	3	Cisco WS-C2960-24LT-L
9	Архів	3	Cisco WS-C2960-24LT-L
10	ВТВМ2	–	Cisco WS-C2960X-24PS-L
12	Стерилізаційний кабінет	2	Cisco WS-C2960-24LT-L
14	Кабінет лора	6	Cisco WS-C2960-24LT-L
17	Кабінет стоматолога	5	Cisco WS-C2960-24LT-L
20	Кабінет Терапевта	6	Cisco WS-C2960-24LT-L
	Зона Wi-Fi	1	Cisco C9115AXI-H

Перелік активного мережевого обладнання корпусу 3 представлено в таблиці 3.3.

Таблиця 3.3 – Перелік активного мережевого обладнання, корпус 3

Номер кабінету	Назва кабінету	Кількість інформ. розеток, RJ45	Мережеве обладнання, модель
5	Приймальне відділення	8	Cisco WS-C2960-24LT-L
6	Приміщення виписки	3	Cisco WS-C2960-24LT-L
7	ВТВМ3	–	Cisco Catalyst 2960-X-24
9	Кабінет головного лікаря	4	Cisco WS-C2960-24LT-L
14	Лабораторія	3	Cisco WS-C2960-24LT-L

Перелік активного мережевого обладнання корпусу 4 представлено в таблиці 3.4.

Таблиця 3.4 – Перелік активного мережевого обладнання, корпус 4

Номер кабінету	Назва кабінету	Кількість інформ. розеток, RJ45	Мережеве обладнання, модель
2	Лабораторія	6	Cisco WS-C2960-24LT-L
3	Кабінет зуботехніка	3	Cisco WS-C2960-24LT-L
7	ВТВМ4	–	Cisco WS-C2960X-24PS-L

Загальна кількість мережевого обладнання для закладу:

- 1 міжмережевий екран Cisco ASA 5510;
- 1 точка безпроводового доступу Cisco C9115AXI-H;
- 4 комутатори Cisco Catalyst 2960-X-24;
- 22 комутатори Cisco Catalyst WS-C2960-24LT-L.

3.2 Розрахунок логічної адресації

Під час розрахунків логічної адресації було проведено сегментування мережі з адресою 10.13.0.0/16 на функціональні блоки підмереж для корпусів, а також для серверів обмеженого та загального доступу (додаток Б).

Під час сегментування мережі кожен структурний підрозділ бібліотеки отримав власну підмережу. Крім того, були створені окремі підмережі для з’єднання комутаторів, серверів та міжмережевого екрану. Кожна підмережа була призначена для окремого VLAN, що покращує управління трафіком, підвищує безпеку та дозволяє об’єднувати віддалені хости.

У таблиці 3.5 наведено розрахунок маски для сегменту мережі корпусу 1 [14].

Таблиця 3.5 – Маска IP мережевих сегментів, корпус 1

№ каб.	Назва кабінету	К–сть інформ. розеток, R	К–сть IP адрес вузлів, H2 (H2=R+0,5R+1)	Кількість бітів–вузла, h		IP маска мережевого сегменту (/n=32–h)
				H2≤2h–2	h	
1	Адміністративне приміщення	3	5,5	5,5≤30	5	/27
2	Приймальне відділення	8	13	13≤30	5	/27
3	Приміщення виписки	3	5,5	5,5≤30	5	/27
9	Кабінет хірурга	4	7	7≤30	5	/27
10	Зав. відділення	4	7	7≤30	5	/27
14	Лабораторія	3	5,5	5,5≤30	5	/27
20	Кабінет рентгену	6	10	10≤30	5	/27
32	Черговий	2	4	4≤30	5	/27
33	Кабінет окуліста	8	13	13≤30	5	/27

У таблиці 3.6 наведено розрахунок маски для сегменту мережі корпусу 2 [14].

Таблиця 3.6 – Маска IP мережевих сегментів, корпус 2

№ каб.	Назва кабінету	К–сть інформ. розеток, R	К–сть IP адрес вузлів, H2 (H2=R+0,5R+1)	Кількість бітів–вузла, h		IP маска мережевого сегменту (/n=32–h)
				H2≤2h–2	h	
2	Кабінет сімейного лікаря	16	25	25≤30	5	/27
6	Кабінет кардіолога	3	5,5	5,5≤30	5	/27
9	Архів	3	5,5	5,5≤30	5	/27
12	Стерилізаційний кабінет	2	4	4≤30	5	/27

Продовження таблиці 3.6

№ каб.	Назва кабінету	К–сть інформ. розеток, R	К–сть IP адрес вузлів, H2 (H2=R+0,5R+1)	Кількість бітів–вузла, h		IP маска мережевого сегменту (/n=32–h)
				H2≤2h–2	h	
14	Кабінет лора	6	10	10≤30	5	/27
17	Кабінет стоматолога	4	7	7≤30	5	/27
20	Кабінет терапевта	6	10	10≤30	5	/27
28	Черговий	2	4	4≤30	5	/27

У таблиці 3.7 наведено розрахунок маски для сегменту мережі корпусу 3 [14].

Таблиця 3.7 – Маска IP мережевих сегментів, корпус 3

№ каб.	Назва кабінету	К–сть інформ. розеток, R	К–сть IP адрес вузлів, H2 (H2=R+0,5R+1)	Кількість бітів–вузла, h		IP маска мережевого сегменту (/n=32–h)
				H2≤2h–2	h	
5	Приймальне відділення	8	13	13≤30	5	/27
6	Приміщення виписки	3	5,5	5,5≤30	5	/27
9	Кабінет головного лікаря	4	7	7≤30	5	/27
14	Лабораторія	3	5,5	5,5≤30	5	/27

У таблицях 3.8 наведено розрахунок маски для сегменту мережі корпусу 4 [14].

Таблиця 3.8 – Маска IP мережевих сегментів, корпус 4

№ каб.	Назва кабінету	К–сть інформ. розеток, R	К–сть IP адрес вузлів, H2 (H2=R+0,5R+1)	Кількість бітів–вузла, h		IP маска мережевого сегменту (/n=32–h)
				H2≤2h–2	h	
2	Лабораторія	6	10	10≤30	5	/27
3	Кабінет зуботехніка	3	5,5	5,5≤30	5	/27

У таблиці 3.9 наведено розрахунок маски для сегменту мережі корпусу 1 [14].

Таблиця 3.9 – Сегментація загальної мережі 10.13.0.0/16 по масці /20

Номер підмережі	IP–адреса підмережі, /20	IP–адреса підмережі, /24	Призначення підмережі	Кількість підмереж
0	10.13.0.0		Зарезервована	
1	10.13.16.0		Проводові сегменти, корпус 1	8
		10.13.16.0	0а підмережа (зарезервовано)	
		10.13.17.0	1а підмережа (сегментовано по масках IP для корпусу 1)	1
2	10.13.32.0		Проводні сегменти, корпус 2	7
		10.13.32.0	0а підмережа(зарезервовано)	
		10.13.33.0	1а підмережа (сегментовано помасках IP для корпусу 2)	
3	10.13.48.0		Проводові сегменти, корпус 3	4
		10.13.48.0	0а підмережа (зарезервована)	–
		10.13.49.0	1а підмережа (сегментовано по масках IP для корпусу 3)	

Продовження таблиці 3.9

Номер підмережі	IP–адреса підмережі, /20	IP–адреса підмережі, /24	Призначення підмережі	Кількість підмереж
4	10.13.64.0		Проводові сегменти, корпус 4	2
		10.13.64.0	0а підмережа, (зарезервована)	–
		10.13.65.0	1а підмережа (сегментовано помасках IP для корпусу 4)	
5	10.13.80.0			
6	10.13.96.0			
7	10.13.112.00			
8	10.13.128.0			
9	10.13.144.0			
10	10.13.160.0			
11	10.13.176.0			
12	10.13.192.0		Сегменти безпроводового доступу	1
		10.13.192.0	0а підмережа (зарезервована)	–
		10.13.193.0	1а підмережа, використано для «Зона WiFi»	
13	10.13.208.0		Сегменти серверів обмеженого доступу	1
		10.13.208.0	0а підмережа, (зарезервована)	–
		10.13.209.0	1а підмережа, (сегментовано по /28)	
14	10.13.224.0		Сегменти з’єднання мережевих пристроїв (технологічні підмережі)	7
		10.13.224.0	0а підмережа (зарезервована)	–
		10.13.225.0	1а підмережа, (сегментовано по /29)	
15	10.13.240.0		Зарезервована	

3.3 Комутація

3.3.1 Налаштування комутаторів

Комутація в мережі – це процес передачі даних або сигналів між пристроями, який може включати маршрутизацію та управління потоками даних для забезпечення ефективної передачі. Існують різні види комутації, такі як кількісна комутація, пакетна комутація та комутація каналів. У пакетній комутації дані передаються у вигляді пакетів, які можуть слідувати різними шляхами в мережі, тоді як комутація каналів передбачає встановлення постійного з'єднання між пристроями для передачі даних [15].

Кожен тип комутації має свої переваги та недоліки, і вибір залежить від потреб мережі та виду передачі даних.

Нижче наведено набір команд та для базових налаштувань комутаторів ПТМВ і ВТМВ (рис. 3.1-3.2).

```
надання імені пристрою:
enable                      // вхід у привілейований режим
configure terminal          // вхід у конфігураційний термінал
hostname NAME               // встановлення імені вузла комутатора

встановлення пароля доступу до привілейованого режиму:
enable secret ***           // *** - пароль зразу шифрується
enable password ***         // *** - пароль не шифрується

встановлення пароля на лінію консолі:
line console 0
password ***                // *** - пароль
login                       // запитувати пароль при вході у консоль

встановлення пароля на лінію vty для telnet:
line vty 0 15               // створення 16 користувацьких telnet сесій
password ****               // *** - пароль
login                       // запитувати пароль при вході у консоль

описи інтерфейсів:
interface fastEthernet 0/1 // вибір інтерфейсу
interface range fastEthernet 0/1-5 // вибір діапазону інтерфейсів
switchport mode access      // переключення порту у режим access
switchport mode trunk       // переключення порту у режим trunk
switchport access vlan 1    // підключення до vlan 1
no shutdown                 // відсутність відключення
```

Рисунок 3.1 – Набір команд для базових налаштувань комутаторів

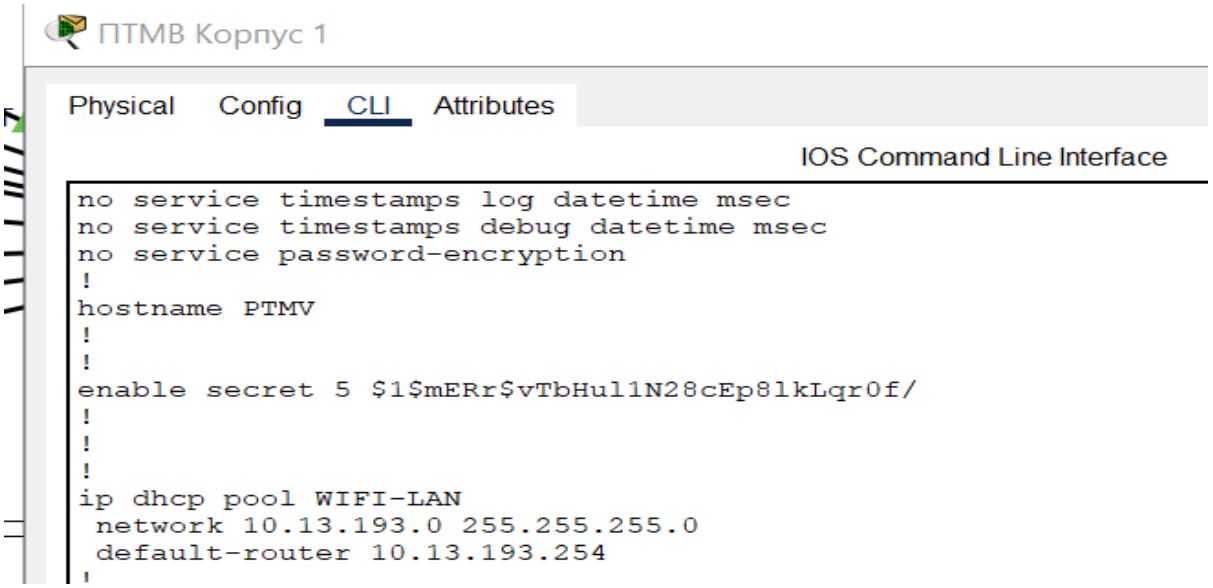


Рисунок 3.2 – Налаштування паролю та DHCP pool

Таким чином можна налаштовувати як комутатори так і маршрутизатори Cisco.

Використання VLAN дозволяє групувати пристрої віртуально, щоб ефективно організувати мережу. Це сприяє зниженню рівня загального трафіку та точному керуванню ним. Також VLAN полегшує реалізацію різних рівнів безпеки та обмежує доступ до ресурсів тільки авторизованим користувачам. Крім того, вона дозволяє налаштовувати швидкість передачі даних для різних користувацьких груп, що сприяє максимальній продуктивності мережі [16].

За допомогою наступних команд налаштовується VLAN на обладнані CISCO (рис. 3.3).

```
vlan 101                    // створення vlan 101 (101 - це ідентифікатор)
name NashVlan               // задається ім'я
ip address 10.13.18.1 255.255.255.248 // присвоєння IP для VLAN
exit                        // вихід з поточних налаштувань

interface GigabitEthernet 0/1 // вибір інтерфейсу або діапазону
switchport mode access/trunk  // переведення порту у режим access/trunk
switchport access vlan 101    // підключення до vlan 101
no shutdown                   // увімкнення порта
exit                          // вихід з поточних налаштувань
```

Рисунок 3.3 – Команди налаштування VLAN на обладнані CISCO

Схема розподілу VLAN мережі лікарні розписана у таблиці 3.10.

Таблиця 3.10 – Схема розподілу VLAN

Діапазон VLAN	Призначення VLAN
101 – 199	Проводові користувацькі сегменти, корпус 1
201 – 299	Проводові користувацькі сегменти, корпус 2
301 – 399	Проводові користувацькі сегменти, корпус 3
401 – 499	Проводові користувацькі сегменти, корпус 4
701	Сегмент безпроводового доступу
702	Сегмент серверві загального доступу
703	Сегмент серверів обмеженого доступу
704 –709	Сегменти з'єднань мережевих пристроїв

Налаштовані VLAN в сегменті мережі корпусу 1 (ПТМВ) зображено на рисунку 3.4.

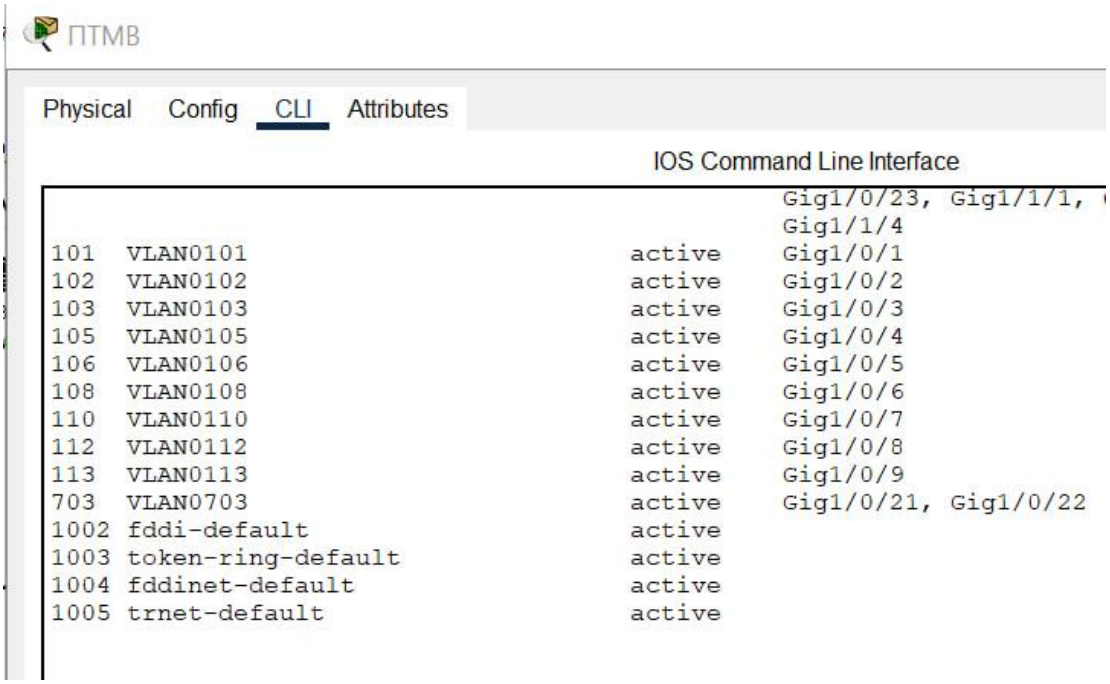


Рисунок 3.4 – Налаштовані VLAN на обладнані CISCO ПТМВ

Налаштовані VLAN в сегменті мережі корпусу 2 (ВТМВ2) зображено на рисунку 3.5.

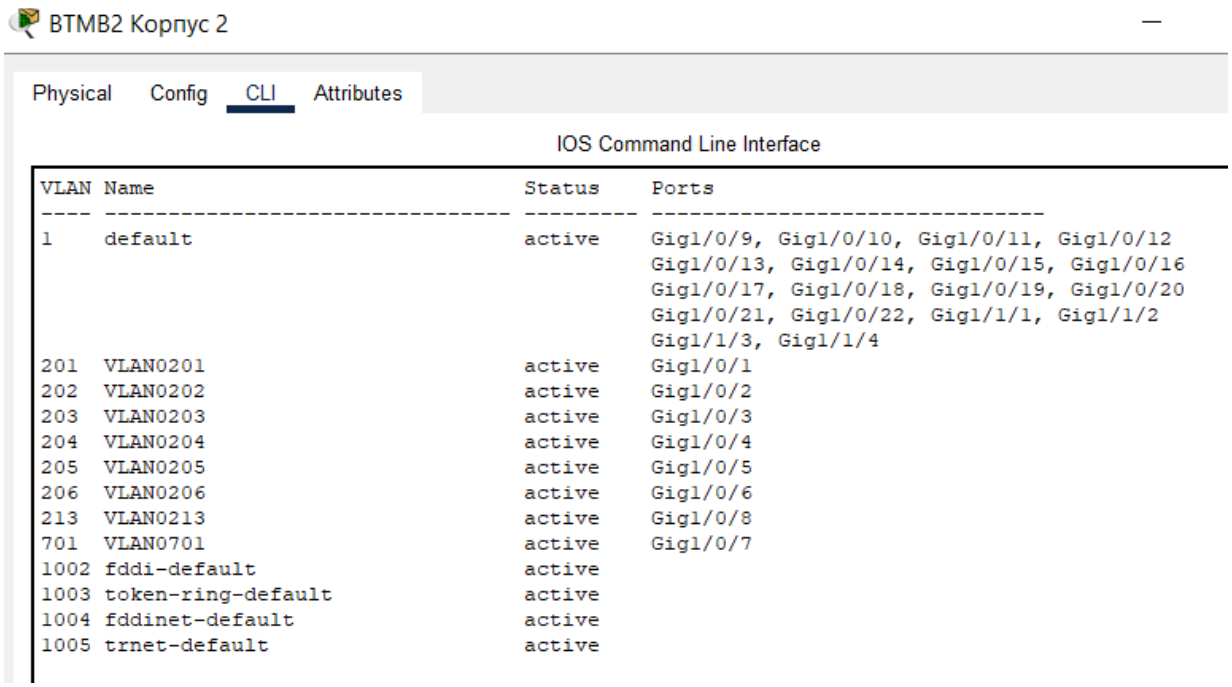


Рисунок 3.5 –Налаштовані VLAN на обладнані CISCO BTMB2

Налаштовані VLAN в сегменті мережі корпусу 3 (BTMB3) зображено на рисунку 3.6.

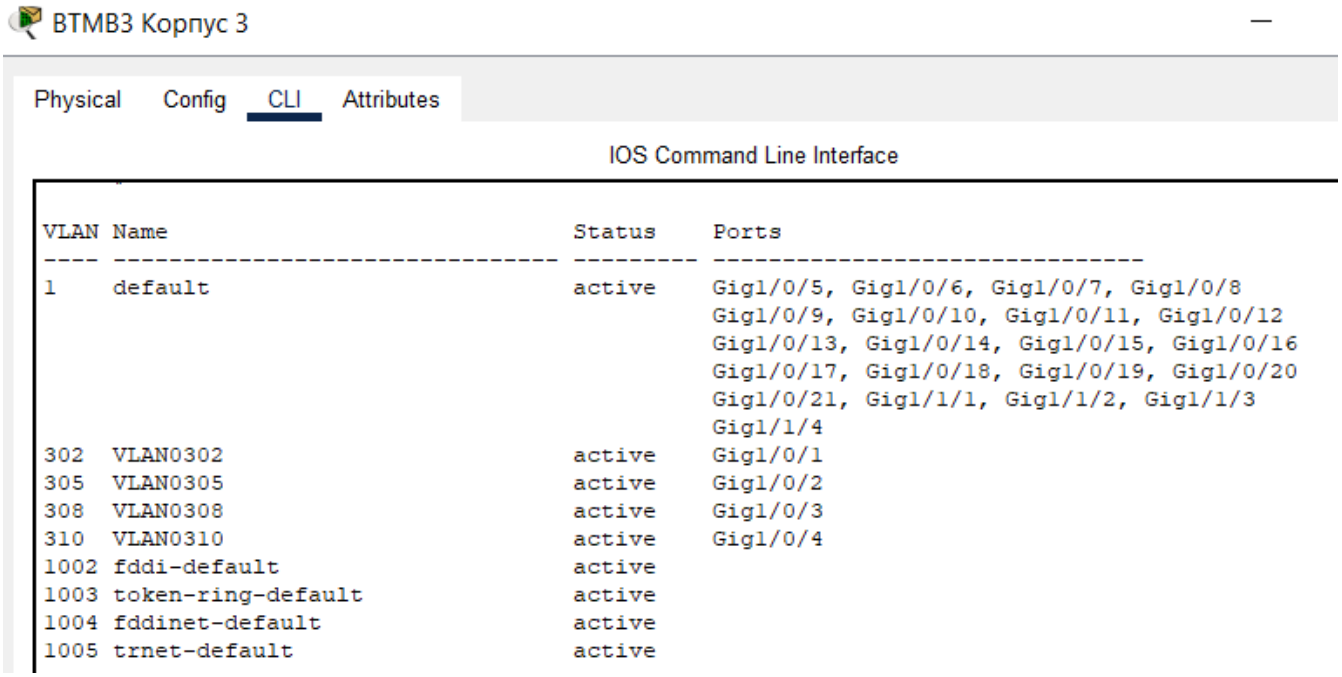


Рисунок 3.6 –Налаштовані VLAN на обладнані CISCO BTMB3

Налаштовані VLAN в сегменті мережі корпусу 4 (ВТМВ4) зображено на рисунку 3.7.

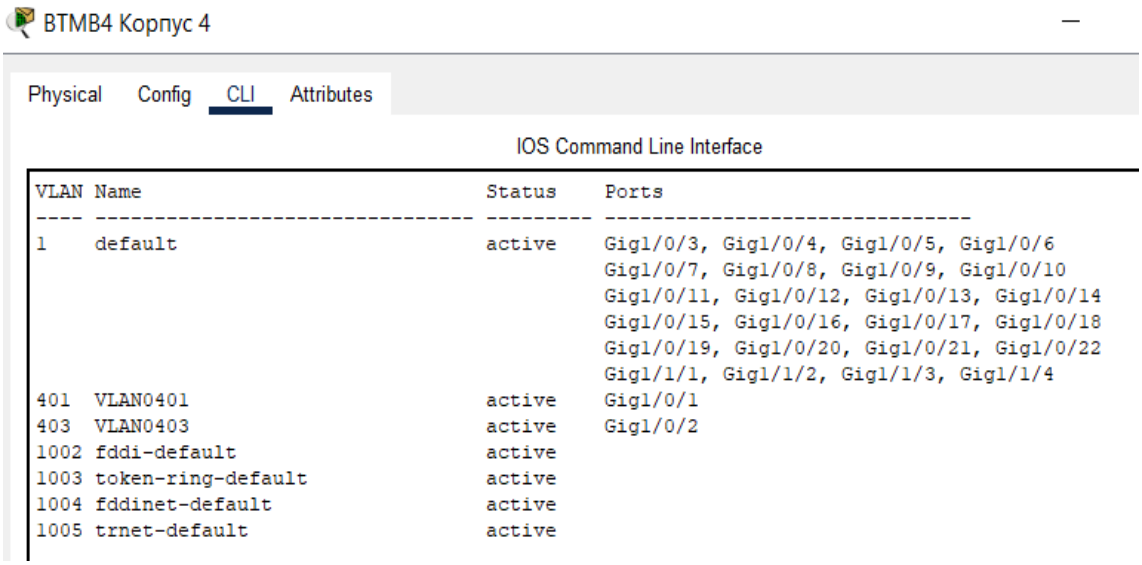


Рисунок 3.7 –Налаштовані VLAN на обладнані CISCO ВТМВ4

3.3.2 Налаштування протоколу резервування з’єднань

Для забезпечення стійкості мережі використовуються додаткові з’єднання, які автоматично активуються при відмові основних. Це гарантує безперервну роботу мережі та постачання високоякісних послуг користувачам. Компанія Cisco пропонує різноманітні методи резервування з’єднань, такі як протоколи Virtual Router Redundancy Protocol (VRRP) та Hot Standby Router Protocol (HSRP).

Для ефективної організації мережі з багатьма зв’язками використовується протокол Spanning Tree Protocol (STP). Цей протокол автоматично блокує зайві зв’язки та створює деревоподібну топологію мережі з багатьма зв’язками. Це запобігає виникненню циклів пакетів та забезпечує повну зв’язність портів, що забезпечує надійну передачу даних без помилок та перерв у роботі мережі [17].

Основні команди для налаштування протоколу Spanning Tree Protocol (STP) накомутаторах Cisco: (рис. 3.8):

```
Ввімкнути STP вибравши режим (PVST, Rapid PVST, MST):
SW1(config)# spanning-tree mode <mode>

Налаштувати пріоритет моста:
SW1(config)# spanning-tree vlan <vlan_id> priority <priority>

Встановити коефіцієнт перезавантаження:
SW1(config)# spanning-tree vlan <vlan_id> hello-time <seconds>

Встановити час відновлення порта:
SW1(config)# spanning-tree vlan <vlan_id> max-age <seconds>

Встановити час блокування порта:
SW1(config)# spanning-tree vlan <vlan_id> forward-time <seconds>

Налаштувати резервні з'єднання:
SW1(config)# interface <interface_id>
SW1(config-if)# spanning-tree guard root

Встановити тип порта (access або trunk):
SW1(config)# interface <interface_id>
SW1(config-if)# spanning-tree portfast <enable/disable>
SW1(config-if)# spanning-tree portfast trunk <enable/disable>

Перевірити стан STP на комутаторі:
SW1# show spanning-tree
```

Рисунок 3.8 – Основні команди для налаштування протоколу (STP).

3.4 Організація безпроводового доступу

Бездротовий зв’язок дозволяє лікарям та іншим службам отримувати доступ до Інтернету без обмежень на кількість одночасних підключень, що сприяє можливості більшої кількості користувачів працювати з різних пристроїв у одному місці. Крім того, це сприяє ефективнішому використанню ресурсів мережі та забезпечує більш гнучке та швидке підключення до мережі для користувачів.

Для надання безпровідного доступу в корпусі 2 використовується обладнання Cisco C9115AXI-H.

Більшість сучасних точок доступу налаштовуються за допомогою графічного інтерфейсу (веб-сторінки або програми).

Однак нижче подано загальні кроки та команди налаштування, які можуть застосовуватися до більшості точок доступу від Cisco (рис. 3.9-3.10):

```
config t
hostname [ім'я точки доступу]

встановіть пароль доступу до налаштувань:
enable secret [пароль доступу]

налаштуйте ip-адресу, маску підмережі та шлюз за замовчуванням:
interface vlan1
ip address [ip-адреса] [маска підмережі]
exit
ip default-gateway [шлюз за замовчуванням]

введіть ім'я безпровідної мережі (ssid):
dot11 ssid [ім'я мережі]

встановіть стандарт безпровідної технології:
dot11 radio [a | b | g | n]

налаштуйте канал роботи:
interface dot11radio0
channel [номер каналу]

встановіть тип автентифікації:
dot11 authentication open

налаштуйте алгоритм шифрування та ключ доступу:
encryption vlan [wep | wpa | wpa2]
wpa-psk ascii [ключ доступу]
```

Рисунок 3.9 – Загальні кроки та команди налаштування, які можуть застосовуватися до більшості точок доступу від Cisco

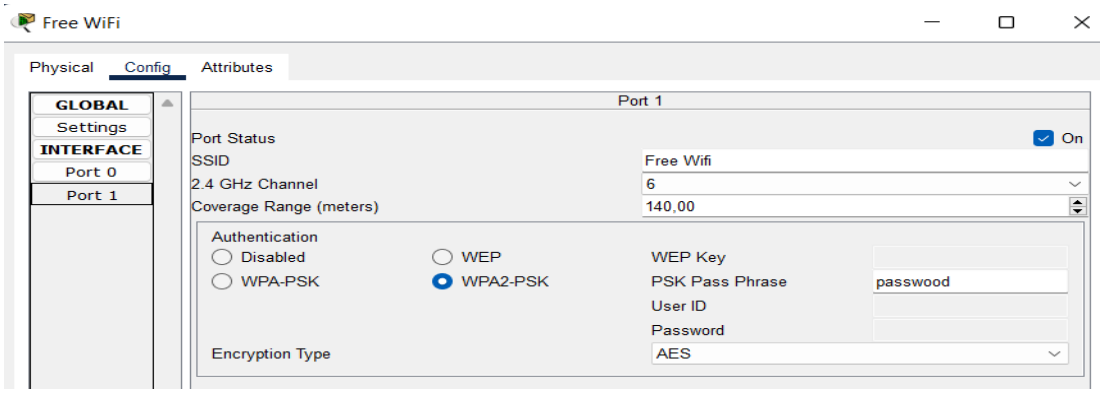


Рисунок 3.10 – Сконфігурована точка доступу Cisco

3.5 Налаштування міжмережевої взаємодії

Для забезпечення зв’язку між різними мережами застосовуються маршрутизатори, які дозволяють передавати дані між різними підмережами.

Для кожної підмережі потрібно налаштувати віртуальний інтерфейс на маршрутизаторі, призначити йому унікальну IP-адресу та встановити адресу відповідного віртуального інтерфейсу як шлюз за замовчуванням [18].

Маршрутизатори зберігають дані про стан мережі та маршрути до різних підмереж, що сприяє ефективній передачі даних від одного пристрою до іншого у мережі.

Крім того, маршрутизація дозволяє розбити великі мережі на менші сегменти, спрощуючи керування мережевим трафіком та зменшуючи його обсяг. Також вона дозволяє створювати різні маршрути для різних типів даних, наприклад, для голосового трафіку та даних, що сприяє підвищенню ефективності мережі та забезпечує якість обслуговування користувачів.

Для налаштування опису фізичного та віртуального інтерфейсів та їх IP-адресів використовуються наступні команди на маршрутизаторах Cisco (рис. 3.11):

```
interface fastEthernet 0/1              // вибір інтерфейсу
interface range fastEthernet 0/1-5      // вибір діапазону інтерфейсів
switchport mode access/trunk            // переключення порту в режим access/trunk
ip address 192.168.1.1 255.255.255.0    // призначення IP для порту
switchport access vlan 2                // підключення до VLAN 2
no shutdown                             // відсутність відключення
```

Рисунок 3.11 – Опис фізичного та віртуального інтерфейсів та їх IP-адресів кроки та команди налаштування

3.5.1 Динамічна маршрутизація

Для ефективної передачі даних у великих мережах використовується протокол динамічної маршрутизації EIGRP (Enhanced Interior Gateway Routing

Protocol). EIGRP автоматично відновлює маршрути в разі виникнення збоїв у мережі та відновлює нормальну роботу мережі. Для цього він використовує механізми, такі як DUAL (Diffusing Update Algorithm) та технологію мультикастингу для передачі інформації про стан мережі між маршрутизаторами. Кожен маршрутизатор у мережі зберігає інформацію про стан мережі та обмінюється нею з сусідніми маршрутизаторами, що дозволяє визначати оптимальний шлях для передачі даних між пристроями мережі [19]. Налаштування протоколу динамічної маршрутизації EIGRP для area 100 можна виконати на маршрутизаторі Cisco за допомогою таких команд: (рис. 3.12):

```
активація EIGRP та налаштування номера автономної системи:
(config)# router eigrp 100
додавання мережевих адрес до EIGRP:
(config-router)# network <IP адреса мережі> <маска мережі>
налаштування максимальної пропускної здатності на інтерфейсах:
(config-router)# interface <номер інтерфейсу>
(config-if)# bandwidth <максимальна пропускна здатність в Кбіт/с>
налаштування метрик маршрутизації:
(config-router)# metric weights <K1> <K2> <K3> <K4> <K5>
встановлення таймерів для протоколу EIGRP:
(config-router)# timers basic <hello час> <hold час>
налаштування дозволу передачі EIGRP пакетів через інтерфейси:
(config-router)# passive-interface <номер інтерфейсу>
налаштування розміру буфера кешу маршрутизації:
(config-router)# maximum-paths <кількість маршрутів>
```

Рисунок 3.12 – Налаштування протоколу динамічної маршрутизації EIGRP для area 100

Після цих налаштувань в мережі буде виконуватися динамічна маршрутизація, що зробить між мережеву маршрутизацію доступною автоматично прокладаючи маршрути. Сконфігурована таблиця марштутизації (рис. 3.13–3.14).

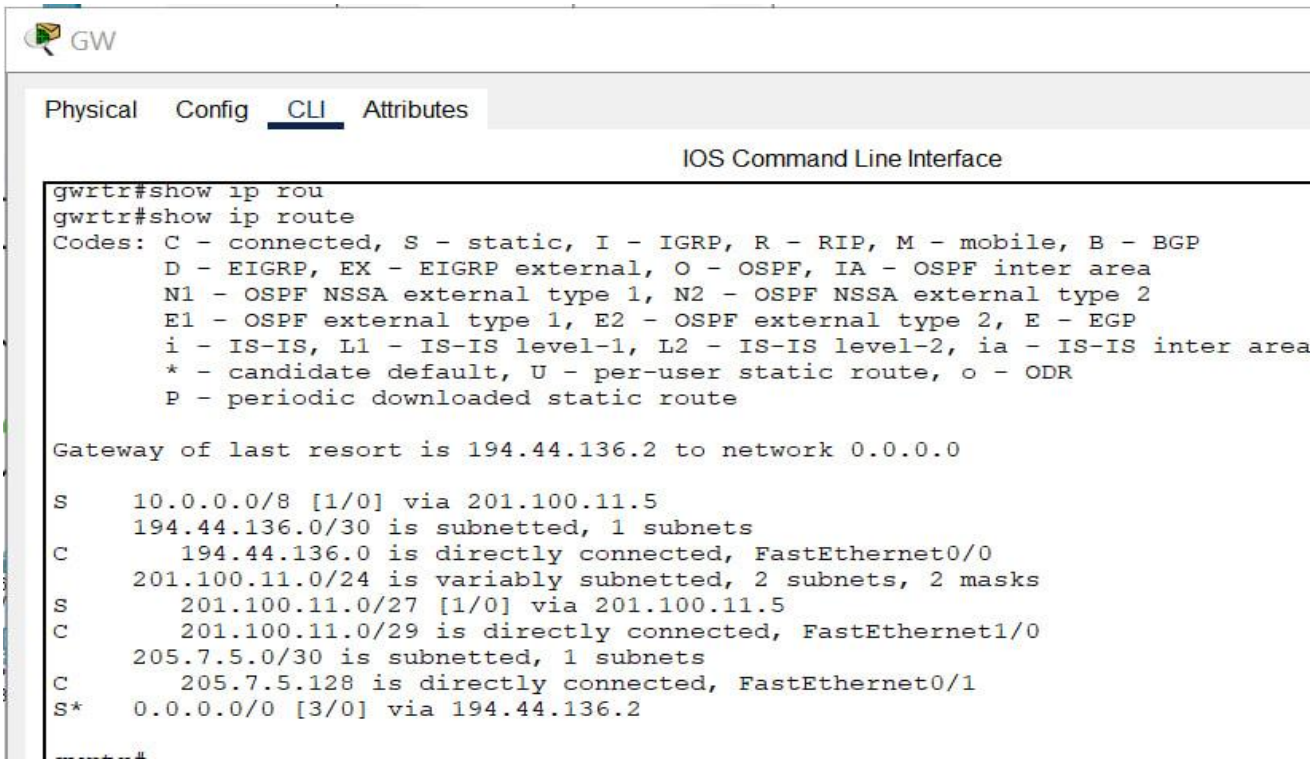


Рисунок 3.13 – Таблиця марштрутизації на маршрутизаторі провайдера

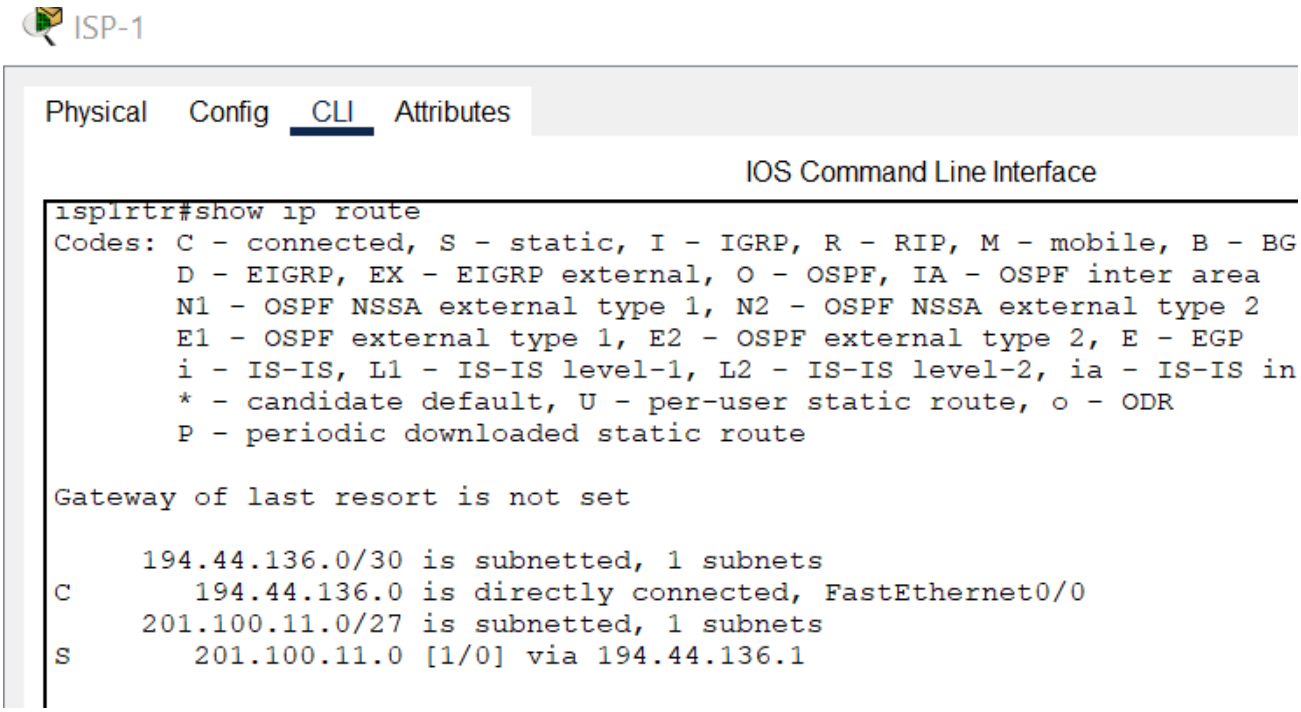


Рисунок 3.14 – Таблиця марштрутизації на маршрутизаторі провайдера

Сконфігурована таблиця марштутизації (рис. 3.15).

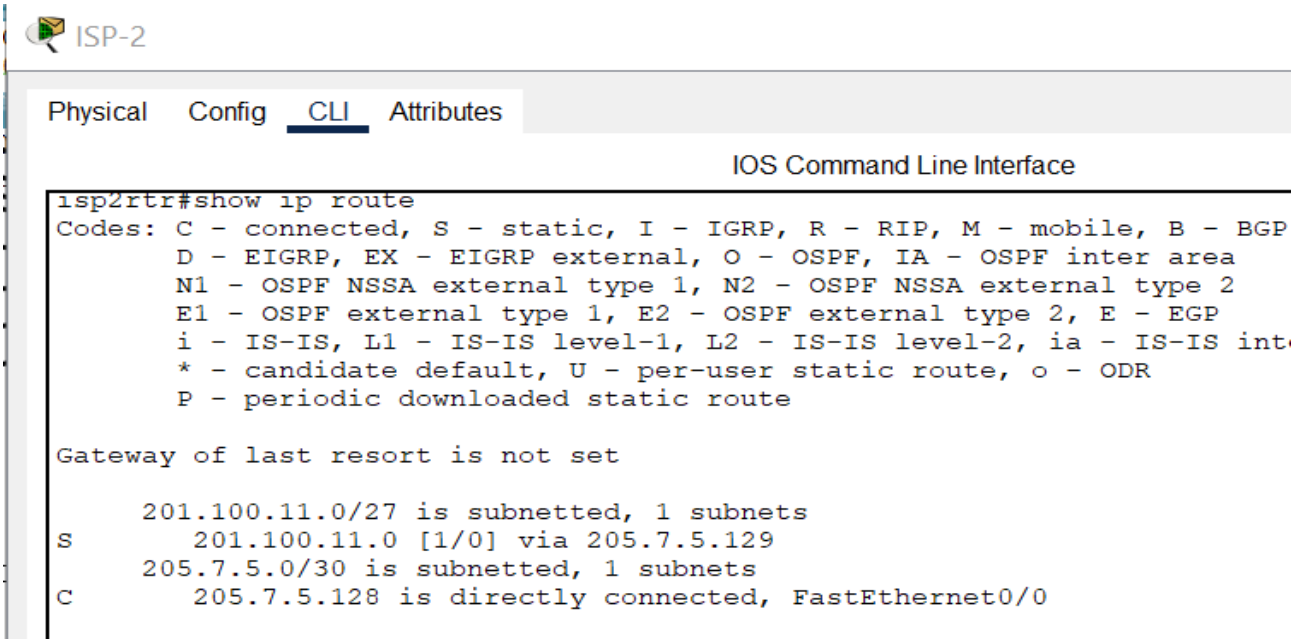


Рисунок 3.15 – Таблиця марштрутизації на маршрутизаторі провайдера

3.6 Організація доступу до Інтернет

Згідно технічного завдання, швидкість основного каналу доступу до мережі Інтернет має бути не більше 50 Мбіт/с, а резервного – до 20 Мбіт/с. Для забезпечення безпеки мережі використовується файрвол CISCO ASA 5510, який відповідає за фільтрацію мережевого трафіку, блокування доступу до потенційно шкідливих веб-сайтів та інших загроз, відслідковування мережевої активності та збереження журналів подій для подальшого аналізу та моніторингу мережі. Крім того, він забезпечує захист від атак на рівні мережевого протоколу, таких як атаки на ARP та ICMP, з метою запобігання шкідливим атакам як з Інтернету, так і зсередини мережі [20].

Для налаштування міжмережевого екрана використовують наступні команди (рис. 3.16).

```
налаштування статичного маршруту за замовчуванням:
ip route 0.0.0.0 0.0.0.0 <IP-адреса-шлюзу>
організація переключення на альтернативний маршрут:
ip route <мережа> <маска> <IP-адрес-шлюзу-першого-маршруту> <метрика> track <номер-монітора>
ip route <мережа> <маска> <IP-адрес-шлюзу-другого-маршруту> <метрика> 254 track <номер-монітора>
налаштування мережевої трансляції адрес NAT:
interface <інтерфейс-зовнішньої-мережі>
ip nat outside  // налаштування зовнішнього адресу
interface <інтерфейс-внутрішньої-мережі>
ip nat inside  // налаштування внутрішнього адресу
ip nat inside source list <номер-ACL> interface <інтерфейс-зовнішньої-мережі> overload
```

Рисунок 3.16 – Налаштування міжмережевого екрана

Сконфігуровані інтерфейси на міжмережевому екрані (рис. 3.17 – 3.18).

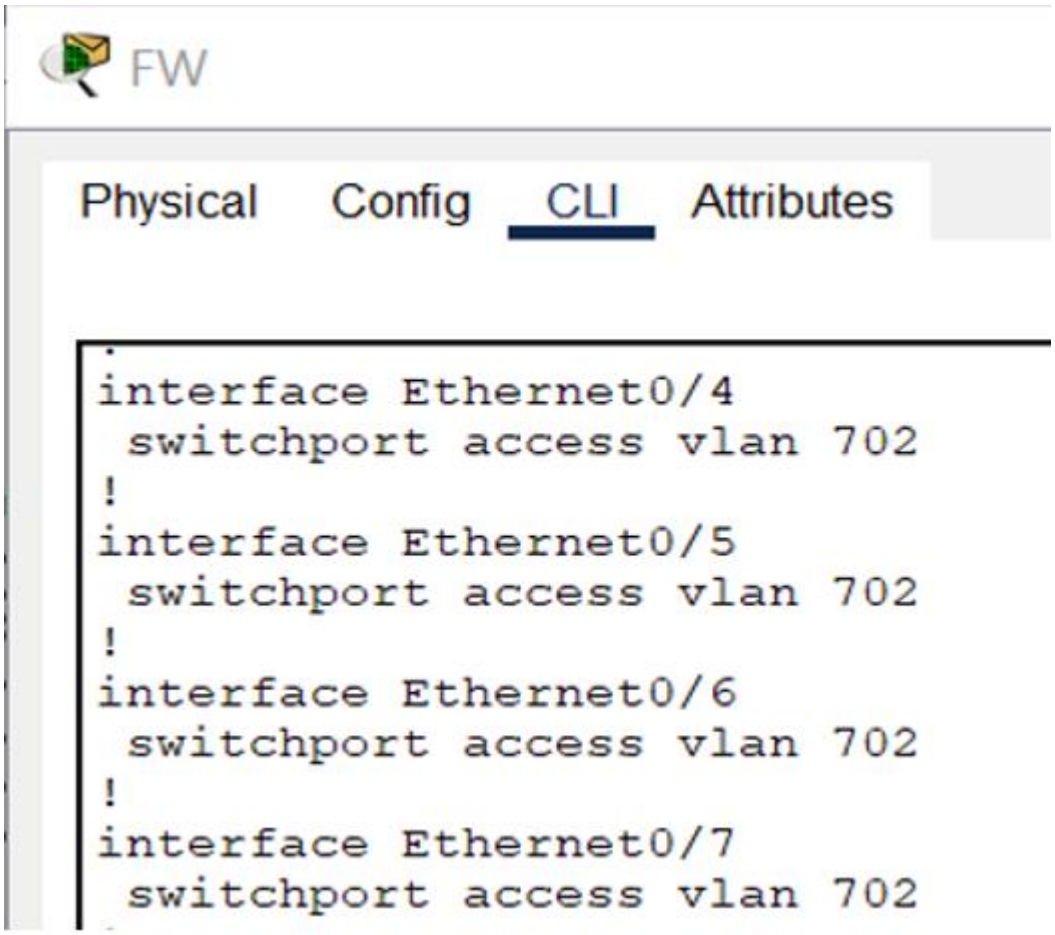


Рисунок 3.17 – Сконфігуровані інтерфейси

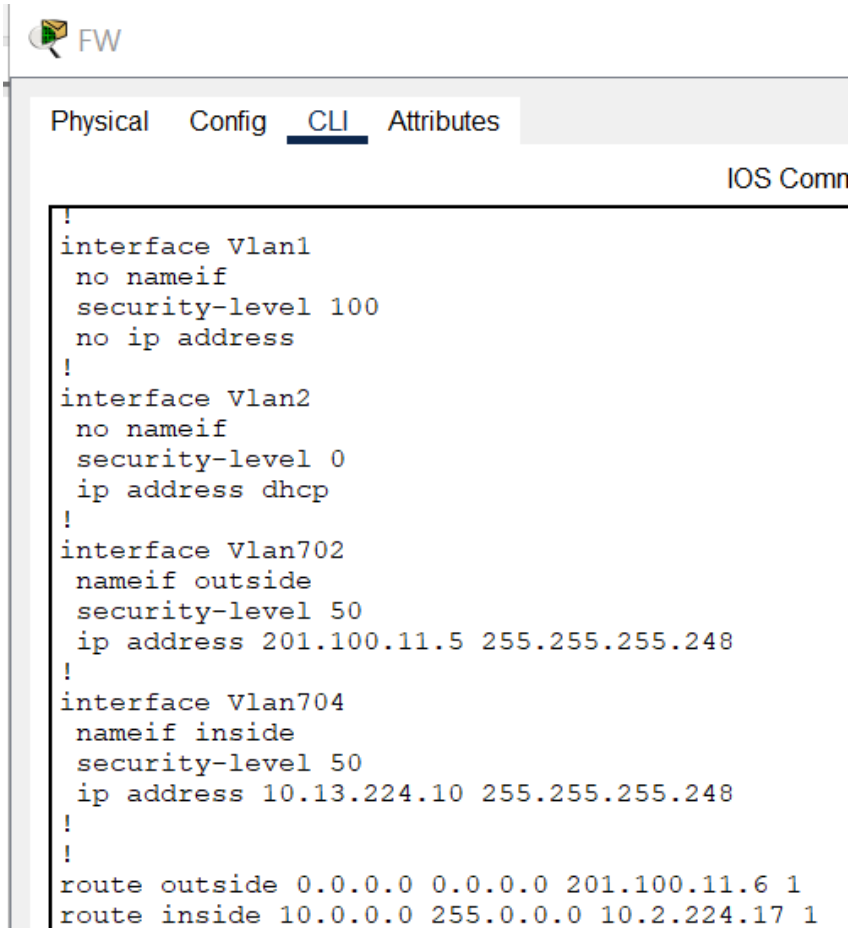


Рисунок 3.18 – Сконфігуровані інтерфейси

Сконфігуроване DHCP на міжмережевому екрані Cisco (рис. 3.19)

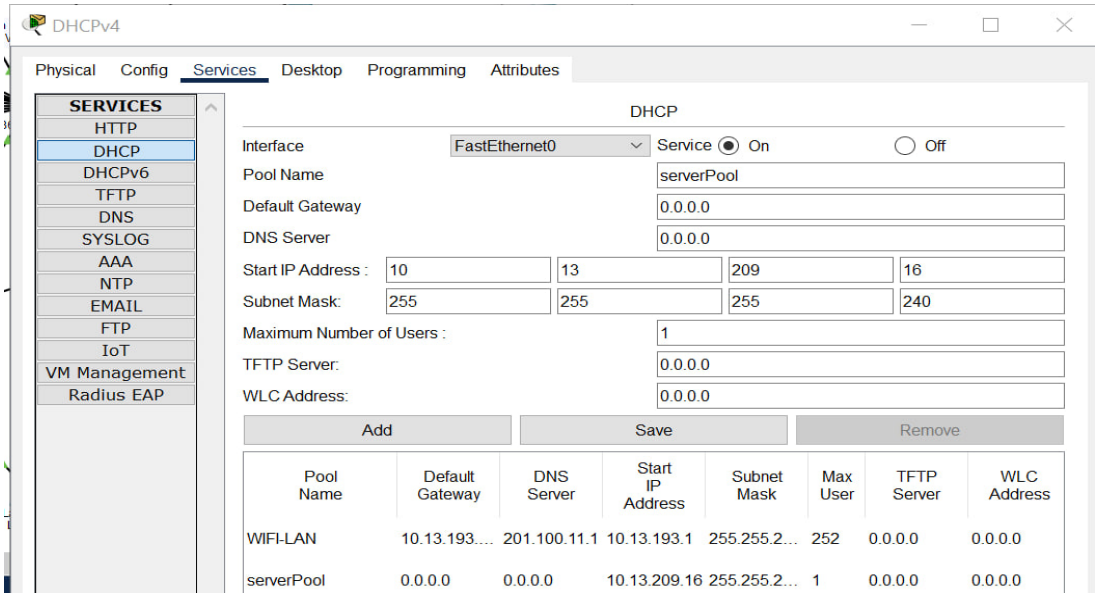


Рисунок 3.19 – Сконфігуроване DHCP

Макет готової мережі розробленої в середовищі Cisco Packet Tracer (рис. 3.20).

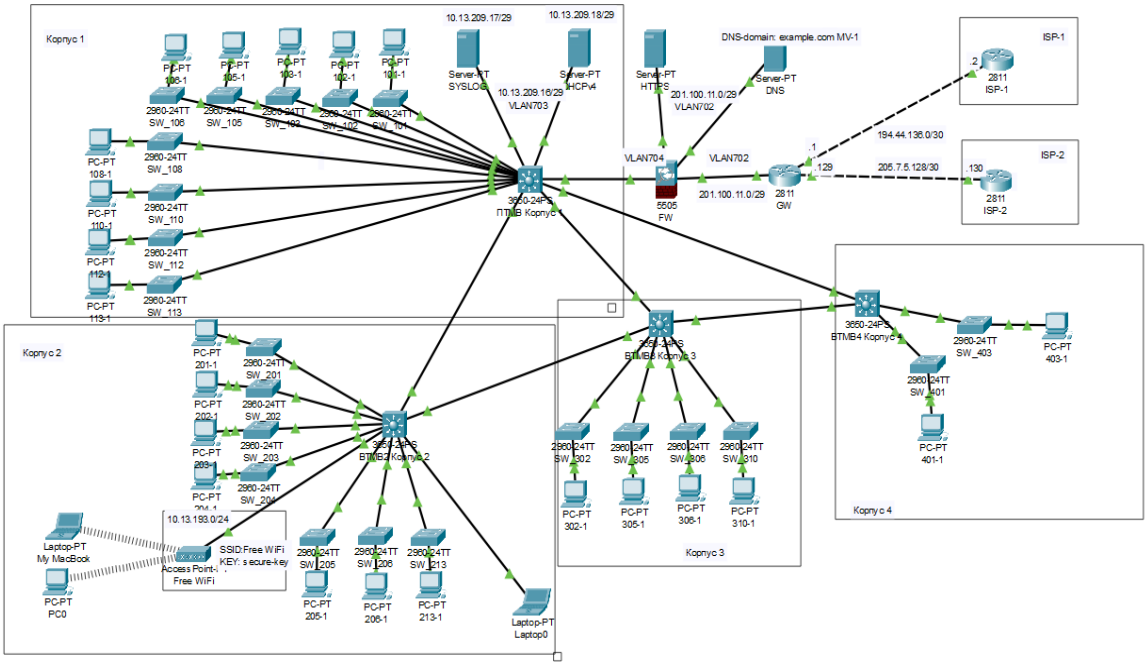


Рисунок 3.20 – Готовий макет мережі

ВИСНОВКИ

У процесі виконання кваліфікаційної роботи здійснено детальний аналіз існуючих потреб та можливостей КНП «Острожецька лікарня» щодо впровадження сучасної комп'ютерної мережі. Розробка мережевої інфраструктури медичного закладу включала декілька ключових етапів, які дозволили забезпечити комплексне рішення, відповідне вимогам і стандартам медичної галузі.

По-перше, проведено аналіз вимог лікарні до мережевої інфраструктури, що включало вивчення поточних процесів обміну інформацією, вимог до пропускної здатності мережі та особливостей медичного обладнання, яке має бути інтегровано в мережу. Це дозволило створити оптимальну архітектуру мережі, яка враховує всі аспекти функціонування закладу.

По-друге, здійснено вибір сучасного мережевого обладнання та програмного забезпечення, яке забезпечує надійність, безпеку та масштабованість мережі. Зокрема для функціонування мережі було обрано таке мережеве обладнання: комутатори 2 рівня моделі OSI Cisco Catalyst WS-C2960; комутатори 3 рівня моделі OSI Cisco WS-C2960X-24PS-L; міжмережевий екран – CISCO ASA 5510; точка доступу – Cisco C9115AXI-H. Маршрутизатори та комутатори налаштовані з використанням програмного забезпечення Cisco IOS. Впроваджені рішення дозволили забезпечити високий рівень захисту медичних даних, що є критично важливим для медичних закладів.

По-третє, розроблено проєкт мережі КНП «Острожецька лікарня», створено документування мережі, яке описує всі аспекти проєкту (від топології мережі до налаштування безпеки та процедур резервного копіювання даних). Це дозволить у майбутньому легко підтримувати та розширювати мережу при зміні потреб закладу.

Результати роботи підтверджують, що розроблена комп’ютерна мережа для КНП «Острожецька лікарня» забезпечує високу ефективність обміну інформацією між підрозділами, підвищує якість надання медичних послуг та відповідає всім вимогам до безпеки та надійності медичних даних.

Впровадження розробленого проєкту дозволить значно підвищити продуктивність роботи медичного персоналу, забезпечити швидкий та надійний доступ до необхідної інформації, що, в свою чергу, сприятиме покращенню якості обслуговування пацієнтів. Розроблена мережа стане міцною основою для подальшого розвитку інформаційних технологій у лікарні, сприяючи її модернізації та відповідності сучасним стандартам медичної допомоги.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. «Network Security Essentials: Applications and Standards» by William Stallings URL: https://www.pearson.com/store/p/network–security–essentials–applications-and–standards/P100000562468 (дата звернення: 04.02.2024).

2. «Computer Networking: A Top–Down Approach» by James Kurose and Keith Ross URL: https://www.pearson.com/store/p/computer–networking–a–top–down–approach/P100000460030 (дата звернення: 01.02.2024).

3. «Nmap Network Scanning: The Official Nmap Project Guide» by Gordon Lyon URL: https://nmap.org/book/ (дата звернення: 04.02.2024).

4. Топологія мережі зірка URL: https://vseosvita.ua/lesson/vydy-topolohii-341873.html (дата звернення: 01.03.2024).

5. Топологія мережі кільце URL: https://studfile.net/preview/5263810/page:3/ (дата звернення: 02.05.2024).

6. Топологія мережі шинна URL: https://kovelpost.com/blogs/214 (дата звернення: 03.04.2024).

7. Обладнання Cisco URL: https://www.cisco.com (дата звернення: 05.04.2024).

8. Мережеве обладнання URL: https://st.in.ua/product/cisco-firewall-and-vpn-appliance-cisco-asa5510/ (дата звернення: 07.04.2024).

9. Точка доступу URL: https://www.router-switch.com/c9115axi-h.html (дата звернення: 09.05.2024).

10. Мережеве обладнання URL: https://servak.com.ua/kommutator/svitch-cisco-catalyst-ws-c2960x-24ts-l-24-port.html(дата звернення: 11.05.2024).

11. Cisco Networking Academy Ukraine» URL: https://www.netacad.com/ (дата звернення: 12.05.2024).

12. «Extreme Networks: Networking the Future» URL: https://www.extremenetworks.com (дата звернення: 13.05.2024).

13. Juniper Networks – Network Solutions and Services URL: https://www.juniper.net (дата звернення: 15.05.2024).

14. «Computer Networking: Principles, Protocols and Practice» by Olivier Bonaventure URL: https://www.computer–networking.info/ (дата звернення: 16.05.2024).

15. «Network Routing: Algorithms, Protocols, and Architectures» by Deep Medhi and Karthik Ramasamy URL: https://www.elsevier.com/books/network–routing/medhi/978–0–12–088588–6 (дата звернення: 17.05.2024).

16. «Palo Alto Networks: Cybersecurity Solutions» URL: https://www.paloaltonetworks.com (дата звернення: 18.05.2024).

17. «Arista Networks: Cloud Networking Solutions» URL: https://www.arista.com (дата звернення: 19.05.2024).

18. Міжмережава взаємодія URL: https://uk.wikipedia.org/wiki/TCP/IP (дата звернення: 26.05.2024).

19. Динамічна марштрутизація URL: https://uk.wikipedia.org/wiki/DSR (дата звернення: 2.06.2024).

20. Таблиця для перетворення адрес URL: https://uk.wikipedia.org/wiki/ARP (дата звернення: 3.06.2024).

ДОДАТКИ

Додаток А

Лістинг конфігураційних файлів

Комутатор ПТМВ:

```
version 16.3.2
no service timestamps log datetime msec
no service timestamps debug datetime
msecno service password-encryption
!
hostname PTMV
!
enable secret 5
$1$mERr$vTbHul1N28cEp8lkLqr0f/
!
ip dhcp pool WIFI-LAN
network 10.13.193.0 255.255.255.0
default-router 10.13.193.254
!
ip routing
!
ip ssh version 1
ip ssh authentication-retries 2ip ssh time-
out 15
no ip domain-lookup
ip domain-name example.com
!
spanning-tree mode pvst
!
interface GigabitEthernet1/0/1switchport
 access vlan 101 switchport mode access
 switchport nonegotiate
 interface GigabitEthernet1/0/2switchport
 access vlan 102 switchport mode access
 switchport nonegotiate
 !
interface GigabitEthernet1/0/3switchport
 access vlan 103 switchport mode access
 switchport nonegotiate
 !
interface GigabitEthernet1/0/4switchport
 access vlan 105 switchport mode access
 switchport nonegotiate
 !
interface GigabitEthernet1/0/5switchport
 access vlan 106 switchport mode access
 switchport nonegotiate
 !
interface GigabitEthernet1/0/6switchport
 access vlan 108 switchport mode access
 switchport nonegotiate
interface GigabitEthernet1/0/22switchport
 access vlan 703 switchport mode access
 switchport nonegotiate
 !
 interface GigabitEthernet1/0/23
 !
interface GigabitEthernet1/0/24no switchport
 ip address 10.13.225.9 255.255.255.248
 duplex autospeed auto

 interface GigabitEthernet1/1/1
 !
 interface GigabitEthernet1/1/2
 !
 interface GigabitEthernet1/1/3
 !
 interface GigabitEthernet1/1/4
 !
interface Vlan1no ip address shutdown
 !
 interface Vlan101
 ip address 10.13.16.30 255.255.255.224
 !
 interface Vlan102
 ip address 10.13.16.62 255.255.255.224
 !
 interface Vlan103
 ip address 10.13.16.94 255.255.255.224
 !
 interface Vlan105
 ip address 10.13.16.126 255.255.255.224
 !
 interface Vlan106
 ip address 10.13.16.158 255.255.255.224
 !
 interface Vlan108
 ip address 10.13.16.190 255.255.255.224
 !
 interface Vlan110
 ip address 10.13.16.222 255.255.255.224
 !
 interface Vlan112
 ip address 10.13.16.254 255.255.255.224
 !
 interface Vlan113
 ip address 10.13.17.30 255.255.255.224
```

```
!
interface GigabitEthernet1/0/7switchport
 access vlan 110 switchport mode access
 switchport nonegotiate
!
interface GigabitEthernet1/0/8switchport
 access vlan 112 switchport mode access
 switchport nonegotiate
!
interface GigabitEthernet1/0/9switchport
 access vlan 113 switchport mode access
 switchport nonegotiate
interface GigabitEthernet1/0/18no
 switchport
 ip address 10.13.225.17 255.255.255.248
 duplex autospeed auto
!
interface GigabitEthernet1/0/19no
 switchport
 ip address 10.13.225.25 255.255.255.248
 duplex autospeed auto
!
interface GigabitEthernet1/0/20no
 switchport
 ip address 10.13.225.33 255.255.255.248
 duplex autospeed auto
!
interface GigabitEthernet1/0/21switchport
 access vlan 703 switchport mode access
 switchport nonegotiate
!
!
interface Vlan701
ip address 10.13.193.254 255.255.255.0
!
interface Vlan703
ip address 10.13.209.30 255.255.255.240
!
interface Vlan704no ip address
!
router eigrp 100
network 10.0.0.0
network 201.100.11.0no auto-summary
!
ip classless
!
ip flow-export version 9
!
banner login "Boss is here!"
banner motd "This is a secure system.
Authorized Access Only!"
!
line con 0
password 7 082048430017login
!
line aux 0
!
line vty 0 4
exec-timeout 3 0
password 7 082048430017logging
synchronous
login local transport input ssh
!
end
```

Комутатор BTMB2:

```
!
version 16.3.2
no service timestamps log datetime msec no
service timestamps debug datetime msecno
service password-encryption
!
hostname VTMV2
!
enable secret 5
$1$mERr$vTbHul1N28cEp8lkLqr0f/
!
ip dhcp pool WIFI-LAN
network 10.13.193.0 255.255.255.0
default-router 10.13.193.254
interface GigabitEthernet1/0/24no switchport
 ip address 10.13.225.18 255.255.255.248
 duplex autospeed auto
 !
 !
interface Vlan1no ip address shutdown
 !
 interface Vlan201
 ip address 10.13.32.30 255.255.255.224
 !
 interface Vlan202
 ip address 10.13.32.62 255.255.255.224
 !
 interface Vlan203
 ip address 10.13.32.94 255.255.255.224
```

```
!
ip routing
!
ip ssh version 1
ip ssh authentication-retries 2ip ssh time-out
15
no ip domain-lookup
ip domain-name example.com
!
spanning-tree mode pvst
interface GigabitEthernet1/0/1
switchport access vlan 201switchport mode
access switchport nonegotiate
!
interface GigabitEthernet1/0/2switchport
access vlan 202 switchport mode access
switchport nonegotiate
!
interface GigabitEthernet1/0/3switchport
access vlan 203 switchport mode access
switchport nonegotiate
!
interface GigabitEthernet1/0/4switchport
access vlan 204 switchport mode access
switchport nonegotiate
!
interface GigabitEthernet1/0/5switchport
access vlan 205 switchport mode access
switchport nonegotiate
!
interface GigabitEthernet1/0/6switchport
access vlan 206 switchport mode access
switchport nonegotiate
!
interface GigabitEthernet1/0/7switchport
access vlan 701 switchport mode access
switchport nonegotiate
!
interface GigabitEthernet1/0/8switchport
access vlan 213 switchport mode access
switchport nonegotiate
!
interface GigabitEthernet1/0/23no switchport
ip address 10.13.225.41 255.255.255.248
duplex autospeed auto
!
!
interface Vlan204
ip address 10.13.32.126 255.255.255.224
!
interface Vlan205
ip address 10.13.32.158 255.255.255.224
!
interface Vlan206
ip address 10.13.32.190 255.255.255.224
!
interface Vlan213
ip address 10.13.32.222 255.255.255.224
!
interface Vlan701
ip address 10.13.193.254 255.255.255.0
!
router eigrp 100
network 10.0.0.0
network 201.100.11.0no auto-summary
!
ip classless
!
ip flow-export version 9
!
banner login "Boss is here!"
banner motd "This is a secure system.
Authorized Access Only!"
!
line con 0
password 7 082048430017login
!
line aux 0
!
line vty 0 4
exec-timeout 3 0
password 7 082048430017logging
synchronous
login local transport input ssh
!
end
```

Комутатор BTMB3:

```
version 16.3.2
no service timestamps log datetime msec no
service timestamps debug datetime msecno
interface GigabitEthernet1/0/23no switchport
ip address 10.13.225.49 255.255.255.248
duplex autospeed auto
```

```
service password-encryption
!
hostname VTMV3
!
enable secret 5
$1$mERr$vTbHul1N28cEp8lkLqr0f/
!
ip routing
!
ip ssh version 1
ip ssh authentication-retries 2ip ssh time-out
15
no ip domain-lookup
ip domain-name example.com
!
spanning-tree mode pvst
!
interface GigabitEthernet1/0/1switchport
access vlan 302 switchport mode access
switchport nonegotiate
!
interface GigabitEthernet1/0/2switchport
access vlan 305 switchport mode access
switchport nonegotiate
!
interface GigabitEthernet1/0/3switchport
access vlan 308 switchport mode access
switchport nonegotiate
!
interface GigabitEthernet1/0/4switchport
access vlan 310 switchport mode access
switchport nonegotiate
no switchport
ip address 10.13.225.42 255.255.255.248
duplex autospeed auto
!
interface GigabitEthernet1/0/23no switchport
ip address 10.13.225.49 255.255.255.248
duplex autospeed auto
!
!
interface GigabitEthernet1/0/24no switchport
ip address 10.13.225.26 255.255.255.248
duplex autospeed auto
!
interface Vlan1no ip address shutdown
!
interface Vlan302
ip address 10.13.48.30 255.255.255.224
!
interface Vlan305
ip address 10.13.48.62 255.255.255.224
!
interface Vlan308
ip address 10.13.48.94 255.255.255.224
!
interface Vlan310
ip address 10.13.48.126 255.255.255.224
!
router eigrp 100
network 10.0.0.0
network 201.100.11.0no auto-summary
!
ip classless
!
ip flow-export version 9
!
!
!
banner login "Boss is here!"
banner motd "This is a secure system.
Authorized Access Only!"
!
line con 0
password 7 082048430017login
!
line aux 0
!
line vty 0 4
exec-timeout 3 0
password 7 082048430017logging
synchronous
login local transport input ssh
!
end
```

Комутатор BTMB4:

```
version 16.3.2
no service timestamps log datetime msec no
service timestamps debug datetime msecno service
password-encryption
!
hostname VTMV4
enable secret 5
$1$mERr$vTbHul1N28cEp8lkLqr0f/
!
ip routing
!
ip ssh version 1
ip ssh authentication-retries 2ip ssh time-out 15
no ip domain-lookup
ip domain-name example.com
!
spanning-tree mode pvst
!
interface GigabitEthernet1/0/1switchport access
vlan 401 switchport mode access switchport
nonegotiate
!
interface GigabitEthernet1/0/2switchport access
vlan 403 switchport mode access switchport
nonegotiate
!
no switchport
ip address 10.13.225.50 255.255.255.248
duplex autospeed auto
!
interface GigabitEthernet1/0/24no switchport
ip address 10.13.225.34 255.255.255.248
duplex autospeed auto
interface Vlan1no ip address shutdown
!
interface Vlan401
ip address 10.13.64.30 255.255.255.224
!
interface Vlan403
ip address 10.13.64.62 255.255.255.224
!
router eigrp 100
network 10.0.0.0
network 201.100.11.0no auto-summary
!
ip classless
!
ip flow-export version 9
!
banner login "Boss is here!"
banner motd "This is a secure system. Authorized
Access Only!"
!
line con 0
password 7 082048430017login
!
line aux 0
!
line vty 0 4
exec-timeout 3 0
password 7 082048430017logging synchronous
login local transport input ssh
!
end
```

1

Додаток Б

Схема IP-адресації

Загальна IP адреса мережі: 10.13.0.0/16.

Таблиця Б.1 – Схема IP-адресації корпусів і мережевих сегментів спеціального застосування

Назва мережевого сегменту	IP-адреса мережі	Маска IP-адреси мережі	Призначення
IP-адреса мережі - корпус 1	10.13.16.0	255.255.240.0	Сумаризована IP-адреса
IP-адреса мережі - корпус 2	10.13.32.0	255.255.240.0	Сумаризована IP-адреса
IP-адреса мережі - корпус 3	10.13.48.0	255.255.240.0	Сумаризована IP-адреса
IP-адреса мережі - корпус 4	10.13.64.0	255.255.240.0	Сумаризована IP-адреса
IP-адреса мережі - безпроводового доступу	10.13.192.0	255.255.240.0	Сумаризована IP-адреса
IP-адреса мережі - сервери загального доступу	201.100.11.0	255.255.255.224	IP-адреси видані Інтернет сервіс провайдером, сумаризовані
IP-адреса мережі - сервери обмеженого доступу	10.13.208.0	255.255.240.0	Сумаризована IP-адреса
IP-адреса мережі - з’єднання мережевих пристроїв (технологічні підмережі)	10.13.224.0	255.255.240.0	Сумаризована IP-адреса

Таблиця Б.2 – Схема IP-адресації мережевих сегментів корпусу 1

Номер каб.	Назва кабінету	IP-адреса мережі/Маска IP-адреси	Діапазон IP-адрес вузлів		IP-адреса шлюз за зам-ям	Приналежність до VLAN	
			Перша IP-адреса	Остання IP-адреса		Номер VLAN	Назва VLAN
1	Адміністративне приміщення	10.13.16.0/27	10.13.16.1	10.13.16.29	10.13.16.30	101	Kab-101
2	Приймальне відділення	10.13.16.32/27	10.13.16.33	10.13.16.61	10.13.16.62	102	Kab-102
3	Приміщення виписки	10.13.16.64/27	10.13.16.65	10.13.16.93	10.13.16.94	103	Kab-103
9	Кабінет хірурга	10.13.16.96/27	10.13.16.97	10.13.16.125	10.13.16.126	105	Kab-105
10	Зав. відділення	10.13.16.128/27	10.13.16.129	10.13.16.157	10.13.16.158	106	Kab-106
14	Лабораторія	10.13.16.160/27	10.13.16.161	10.13.16.189	10.13.16.190	108	Kab-108
20	Кабінет рентгену	10.13.16.192/27	10.13.16.193	10.13.16.221	10.13.16.222	110	Kab-110
32	Черговий	10.13.16.224/27	10.13.16.225	10.13.16.253	10.13.16.254	112	Kab-112
33	Кабінет окуліста	10.13.17.0/27	10.13.17.1	10.13.17.29	10.13.17.30	113	Kab-113

Таблиця Б.3 – Схема IP-адресації мережевих сегментів корпусу 2

Номер каб.	Назва кабінету	IP-адреса мережі/Маска IP-адреси	Діапазон IP-адрес вузлів		IP-адреса шлюз за зам-ям	Приналежність до VLAN	
			Перша IP-адреса	Остання IP-адреса		Номер VLAN	Назва VLAN
2	Кабінет сімейного лікарня	10.13.32.0/27	10.13.32.1	10.13.32.29	10.13.32.30	201	Kab-201
6	Кабінет Кардіолога	10.13.32.32/27	10.13.32.33	10.13.32.61	10.13.32.62	202	Kab-202
9	Архів	10.13.32.64/27	10.13.32.65	10.13.32.93	10.13.32.94	203	Kab-203
12	Стерилізаційний кабінет	10.13.32.96/27	10.13.32.97	10.13.32.125	10.13.32.126	204	Kab-204
14	Кабінет лора	10.13.32.128/27	10.13.32.129	10.13.32.157	10.13.32.158	205	Kab-205
17	Кабінет стоматолога	10.13.32.160/27	10.13.32.161	10.13.32.189	10.13.32.190	206	Kab-206
20	Кабінет терапевта	10.13.32.192/27	10.13.32.193	10.13.32.221	10.13.32.222	213	Kab-213

Таблиця Б.4 – Схема IP-адресації мережевих сегментів корпусу 3

Номер каб.	Назва кабінету	IP-адреса мережі/Маска IP-адреси	Діапазон IP-адрес вузлів		IP-адреса шлюз за зам-ям	Приналежність до VLAN	
			Перша IP-адреса	Остання IP-адреса		Номер VLAN	Назва VLAN
5	Приймальне відділення	10.13.48.0/27	10.13.48.1	10.13.48.29	10.13.48.30	302	Kab-302
6	Приміщення Виписки	10.13.48.32/27	10.13.48.33	10.13.48.61	10.13.48.62	305	Kab-305
9	Кабіненет головного лікаря	10.13.48.64/27	10.13.48.65	10.13.48.93	10.13.48.94	308	Kab-308
14	Лабораторія	10.13.48.96/27	10.13.48.97	10.13.48.125	10.13.48.126	310	Kab-310

Таблиця Б.5 – Схема IP-адресації мережевих сегментів корпусу 4

Номер каб.	Назва кабінету	IP-адреса мережі/Маска IP-адреси	Діапазон IP-адрес вузлів		IP-адреса шлюз за зам-ям	Приналежність до VLAN	
			Перша IP-адреса	Остання IP-адреса		Номер VLAN	Назва VLAN
2	Лабораторія	10.13.64.0/27	10.13.64.1	10.13.64.29	10.13.64.30	401	Kab-401
3	Кабінет зуботехніка	10.13.64.32/27	10.13.64.33	10.13.64.61	10.13.64.62	403	Kab-403

Таблиця Б.6 – Схема IP-адресації мережі безпроводового доступу

Назва мережевого сегменту	Номер каб. підключення Access Point	IP-адреса мережі/Маска	Діапазон IP-адрес вузлів		IP-адерса Access Point	IP-адреса шлюз за зам-ям	Приналежність до VLAN	
			Перша IP-адреса	Остання IP-адреса			Номер VLAN	Назва VLAN
Free WiFi	201-215	10.13.193.0/24	10.13.193.1	10.13.193.252	10.13.193.253	10.13.193.254	701	WiFiV

Таблиця Б.7 – Схема IP-адресації мережевих сегментів серверів

Назва сервера	IP-адреса мережі/Маска IP-адреси	IP-адреса сервера	IP-адреса шлюз за зам-ям	Приналежність до VLAN	
				Номер VLAN	Назва VLAN
Сервери загального доступу					
DNS-SRV-PUB	201.100.11.0/29	201.100.11.1	201.100.11.6	702	SRV-PUB
HTTP-SRV-PUB		201.100.11.2			
Сервери обмеженого доступу					
DHCP-SRV	10.13.209.16/28	10.13.209.17	10.13.209.30	703	SRV-PRV
SYSLOG-SRV		10.13.209.18			

Таблиця Б.8 – Схема IP-адресації з’єднань мережевих пристроїв (технологічні підмережі)

Назва мережевого сегменту (А – В)	IP-адреса мережі/Маска IP-адреси	IP-адреси інтерфейсів мережевих пристроїв		Тип і номер інтерфейсу	
		Підключення А	Підключення В	Підключення А	Підключення В
gw-isp1	194.44.136.0/30	194.44.136.1	194.44.136.2	FE 0/1	FE 0/0
gw-isp2	205.7.5.128/30	205.7.5.129	205.7.5.130	FE 0/2	FE 0/0
fw-gw	201.100.11.0/29	201.100.11.5	201.100.11.6	Vlan702 (FE 0/1)	Vlan702 (FE1/3)
ПТМВ-fw	10.13.225.8/29	10.13.225.9	10.13.225.10	Vlan704 (Gi 0/24)	Vlan704 (FE 0/0)
ПТМВ-ВТМВ2	10.13.225.16/29	10.13.225.17	10.13.225.18	Vlan705 (Gi 0/18)	Vlan705 (Gi 0/24)
ПТМВ-ВТМВ3	10.13.225.24/29	10.13.225.25	10.13.225.26	Vlan706 (Gi 0/19)	Vlan706 (Gi 0/24)
ПТМВ-ВТМВ4	10.13.225.32/29	10.13.225.33	10.13.225.34	Vlan707 (Gi 0/20)	Vlan707 (Gi 0/24)
ВТМВ2-ВТМВ3	10.13.225.40/29	10.13.225.41	10.13.225.42	Vlan708 (Gi 0/23)	Vlan708 (Gi 0/22)
ВТМВ3-ВТМВ4	10.13.225.48/29	10.13.225.49	10.13.225.50	Vlan709 (Gi 0/23)	Vlan709 (Gi 0/23)