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

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

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента Соколовського Дмитра Олександровича
(ПІБ)
академічної групи 123-19-1
(шифр)
спеціальності 123 Комп'ютерна інженерія
(офіційна назва)
на тему "Комп'ютерна система стоматологічної клініки "Amel Dental Clinic" з реалізацією побудови та налаштування корпоративної мережі та підсистеми IoT безпеки"
(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	доц. Бешта Д.О.			
розділів:				
розробка апаратної частини	доц. Бешта Д.О.			
розробка корпоративної мережі	ас. Панферова Я.В.			

Рецензент				

Нормоконтролер	проф. Цвіркун Л.І.			

Дніпро
2023

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

"___" _____ 2023 року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавр

студента Соколовського Д.О. **академічної групи** 123-19-1
(прізвище та ініціали) (шифр)
спеціальності 123 «Комп'ютерна інженерія»
за освітньо-професійною програмою 123 «Комп'ютерна інженерія»
(офіційна назва)
на тему "Комп'ютерна система стоматологічної клініки "Amel Dental Clinic" з реалізацією побудови та налаштування корпоративної мережі та підсистеми IoT безпеки"

затверджену наказом ректора НТУ «Дніпровська політехніка» від 16.05.2023 № 350-с

Розділ	Зміст	Термін виконання
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел конкретизується предмет та мету роботи та виконується постановка завдання	10.05.2022
Розробка апаратної частини	На основі аналізу підприємства формулюються технічні вимоги до комп'ютерної системи та розробляється апаратна частина системи	17.05.2022
Розробка корпоративної мережі	Виконується розрахунок налаштувань корпоративної мережі та перевірка роботи системи, розробляються методи та налаштування обладнання для захисту інформації в системі	24.05.2022
Розробка компонента системи	Виконується детальна розробка компонента системи	31.05.2022

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

Дата видачі 10.02.2023

Дата подання до екзаменаційної комісії 08.06.2023

Прийнято до виконання _____ Соколовський Д.О

РЕФЕРАТ

Пояснювальна записка: 80с., 51рис., 11табл., 2дод., 8джерел.

КОМП’ЮТЕРНА СИСТЕМА, ІНТЕРНЕТ РЕЧЕЙ, СТОМАТОЛОГІЧНА КЛІНІКА, МАРШРУТИЗАТОР, КОМУТАТОР, CISCO, CISCO PACKET TRACER, NAT, VPN, DHCP, VLAN.

Об’єкт розробки – комп’ютерна система стоматологічної клініки “Amel Dental Clinic” з реалізацією побудови та налаштування корпоративної мережі та підсистеми IoT безпеки.

Мета роботи − створення комп’ютерної системи для стоматологічної клініки “Amel Dental Clinic”.

Була розроблена комп'ютерна мережа, яка може гнучко змінювати свій зовнішній вигляд і набір функцій шляхом перепрограмування, та орієнтована на застосування в стоматологічній клініці “Amel Dental Clinic”.

Система дозволяє здійснювати як технічну, так і програмну модернізацію системи. Клініка складається з 12 відділів: IT-відділ, бухгалтерія, відділ кадрів, відділ маркетингу, пародонтологічне, терапевтичне, ортопедичне, ортодонтичне, хірургічне, анестезіологічне, дитячого відділення та відділення загальної терапії.

Розроблена комп’ютерна мережа виконана відповідно до завдання на кваліфікаційну роботу бакалавра.

Розроблена схема мережі виконана та перевірена за допомогою програми Cisco Packet Tracer.

Результати перевірки у вигляді таблиць, графіків описані і наводяться у пояснювальній записці або додатках.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ПК – Персональний комп’ютер.

КС – Комп’ютерна Система.

СКМ – Структурована кабельна мережа.

КТЗ – Комплекс технічних засобів.

DHCP – (Dynamic Host Configuration Protocol) мережевий протокол, який використовується для автоматичного призначення IP-адреси хостам.

VLAN – (Virtual Local Area Network) технологія, яка дозволяє розділити одну фізичну локальну мережу на кілька логічних мереж.

NAT – (Network Address Translation) технологія, яка використовується для перетворення мережевих адрес між двома різними мережами.

VPN – (Virtual Private Network) технологія, яка використовується для створення захищеного з'єднання між двома або більше пристроями через незахищену мережу.

IoT – (Internet of Things) технологія, яка використовується для підключення пристроїв до Інтернету і дозволяє їм комунікувати та обмінюватися даними між собою.

ВСТУП

Розвиток інформаційних технологій суттєво вплинув на комунікацію людей. Одним з найважливіших аспектів цього розвитку є комп'ютерні мережі, які забезпечують зв'язок та обмін інформацією між різними пристроями.

Комп'ютерна мережа – це сукупність поєднаних між собою пристроїв, які можуть взаємодіяти один з одним. Вона забезпечує можливість спільного використання інформації, програм або послуг, а також спрощує процес комунікації між користувачами.

Комп'ютерна мережа може бути локальною, яка охоплює невелику територію, наприклад будинок чи офіс, або глобальною, яка охоплює велику територію, наприклад міста чи країни.

В комп'ютерній мережі кожен пристрій називається вузлом, які можуть бути поєднані між собою за допомогою кабелів, наприклад Ethernet, або за допомогою бездротового зв'язку, наприклад Wi-Fi.

Для передачі даних використовуються набори правил, які називаються протоколами. Вони гарантують правильну та безпечну передачу даних між вузлами мережі.

Комп'ютерні мережі мають дуже багато застосувань, від спільного використання файлів до доступу до Інтернету. Вони використовуються в офісах, навчальних закладах, громадських місцях та в домашніх умовах.

Адже без комп'ютерних мереж складно уявити сучасний світ, тому ця робота є актуальною в контексті розвитку інформаційних технологій та зростаючої необхідності в ефективному обміні інформації та спільному використанні ресурсів.

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

1.1 Стисла характеристика галузі та умов застосування комп’ютерної системи, що проектується

Медична галузь відноситься до сектора, який охоплює різноманітні підприємства, організації, фахівців з області охорони здоров’я, медичні препарати та технології. Ця галузь є дуже важливою для життєдіяльності людини, адже вона грає вирішальну роль в профілактиці та лікуванні захворювань.

Медична галузь складається з декількох ключових компонентів, а саме:

1. Постачальників медичних послуг. Це лікарні або клініки, які надають медичні послуги.
2. Фармацевтична промисловість. Цей компонент включає в себе розробку та виробництво медикаментів, чим займаються фармацевтичні компанії або біотехнологічні фірми.
3. Медичне обладнання. Це розробка медичних інструментів, приладів та пристроїв.
4. Медичні дослідження. Цей компонент включає в себе наукові дослідження та клінічні випробування, чим займаються дослідницькі організації та приватні компанії.
5. Регуляторні органи. Уряд та регуляторні органи створюють правила та принципи, які забезпечують етичність та безпеку медичних продуктів та послуг

Медична галузь постійно розвивається не в останню чергу завдяки комп’ютерним технологіям, які значно покращують умови праці для лікарів, догляд за пацієнтами, діагностику та лікування захворювань, комунікацію між медичними структурами, персоналом, лікарями та пацієнтами. Серед основних застосувань комп’ютерних технологій можна відокремити телемедицину, систему підтримки прийняття рішень, медичну візуалізацію, систему електронних медичних записів.

1.2 Характеристика і структура стоматологічної клініки «Amel Dental Clinic»

Об’єкт впровадження – стоматологічна клініка «Amel Dental Clinic».

Стоматологічна клініка «Amel Dental Clinic» заснована в 2017 році. Основна сфера діяльності клініки – це надання послуг з лікування, профілактики та догляду за зубами, яснами та сусідніми тканинами. Пацієнтам доступне лікування карієсу, кореневих каналів, ясен, видалення, імплантація та протезування зубів, встановлення коронок та брекетів. Також клініка надає послуги із загальної терапії. [1]

Клініка має чотири самостійних підрозділи:

1. Amel Dental – стоматологія класу люкс.
2. Amel Kids – центр дитячої стоматології.
3. Amel Smart – центр естетичної стоматології та здоров'я.
4. Amel Perio - пародонтологічний центр.

Це перша та єдина стоматологічна клініка України, яка отримала міжнародну акредитацію The Global Clinic Rating (GCR) та увійшла до ТОП-200 медичних центрів світу. [1]

Стоматологічна клініка «Amel Dental Clinic» має функціональну організаційну структуру. [1]

Особливість цього типу управління полягає в тому, що для виконання певних задач створюються спеціальні функціональні підрозділи. Керівники функціональних підрозділів є відповідальними за роботу підрозділу. [2]

В клініці є різні функціональні підрозділи, такі як ІТ-відділ, бухгалтерія, відділ кадрів та відділ маркетингу, які в цілому складають адміністративний відділ. Медичний відділ складається з відділень різних сфер медичної допомоги, а саме: пародонтологічного, терапевтичного, ортопедичного, ортодонтичного, хірургічного, анестезіологічного, дитячого відділення та відділення загальної терапії.

Медичний директор є відповідальним за роботи клініки в цілому, тоді як адміністративний відділ керує адміністративними функціями. Завдяки такій структурі клініці легко координувати адміністративними та медичними операціями.

Бухгалтерія займається виплатою заробітних плат працівникам клініки, контролем оплат послуг пацієнтами та формуванням звітів в податкову.

ІТ-відділ займається впровадженням комп'ютерних систем та їх наглядом. Кожен працівник має можливість звернутися до ІТ-фахівця в разі виникнення проблем з обладнанням або програмним забезпеченням.

Відділ кадрів займається пошуком та прийомом на роботу необхідних для лікарні спеціалістів. Кожен кандидат проходить співбесіду з керівником відділення та медичним директором.

Відділ маркетингу займається просуванням клініки та залученням нових клієнтів.

Інші вісім відділень займаються обстеженням та лікуванням пацієнтів в своїх сферах.

Організаційну структуру клініки «Amel Dental Clinic» наведено на рисунку 1.1

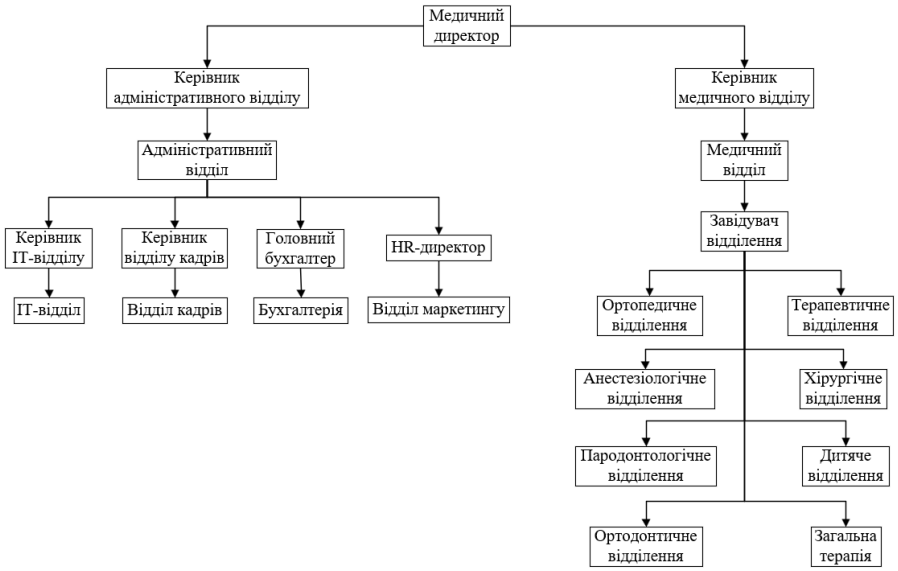

Рисунок 1.1 – Схема організаційної структури стоматологічної клініки «Amel Dental Clinic»

1.3 Стислі відомості про топологічне розміщення структурних підрозділів стоматологічної клініки «Amel Dental Clinic» та технології збору та передачі інформації

Топографічне розміщення структурних підрозділів стоматологічної клініки «Amel Dental Clinic» складається з двох будівель, у яких надаються однакові послуги. [1]

Перша локація приміщень клініки знаходиться за адресою 49000, Україна, Дніпропетровська область, м. Дніпро, бул. Катеринославський 2, ТДК "Босфор". Там клініка орендує другий та п’ятий поверх (рис. 1.2 А). [1]

Друга локація приміщень клініки знаходиться за адресою 49000, Україна, Дніпропетровська область, м. Дніпро, бул. Слави 2Б. Там клініка має власну будівлю, яка складається з двох поверхів (рис. 1.2 Б). [1]

Відстань між будівлями складає 5300 м по прямій.

Топографічна схема розміщення структурних підрозділів клініки показана на рис. 1.2

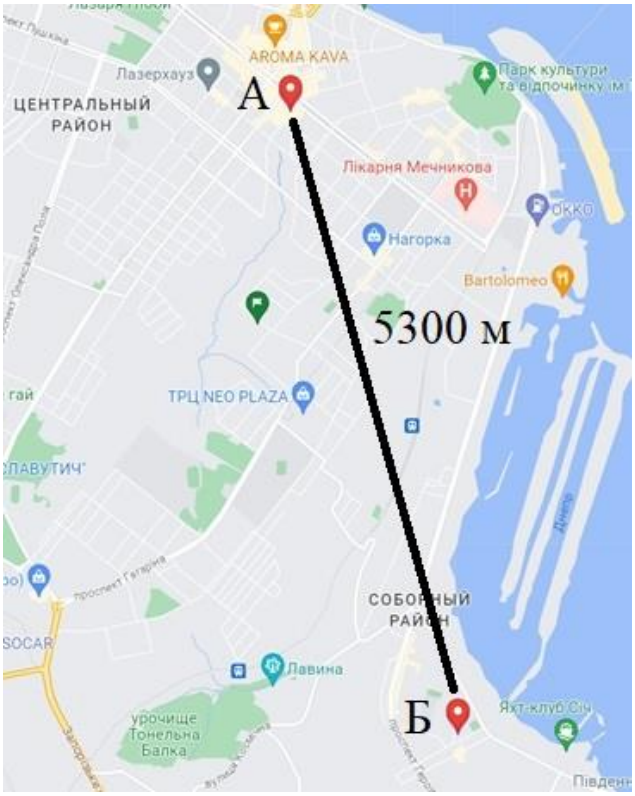

Рисунок 1.2 – Топографічна схема розміщення структурних підрозділів стоматологічної клініки «Amel Dental Clinic»

Розглянемо структурну схему розміщення підрозділів на другому поверсі локації А стоматологічної клініки «Amel Dental Clinic», в якій знаходяться ІТ-відділ (I), відділ кадрів (II), бухгалтерія (III), відділ маркетингу (IV), ортопедичне (V) та анестезіологічного відділення (VI) (рис. 1.3).

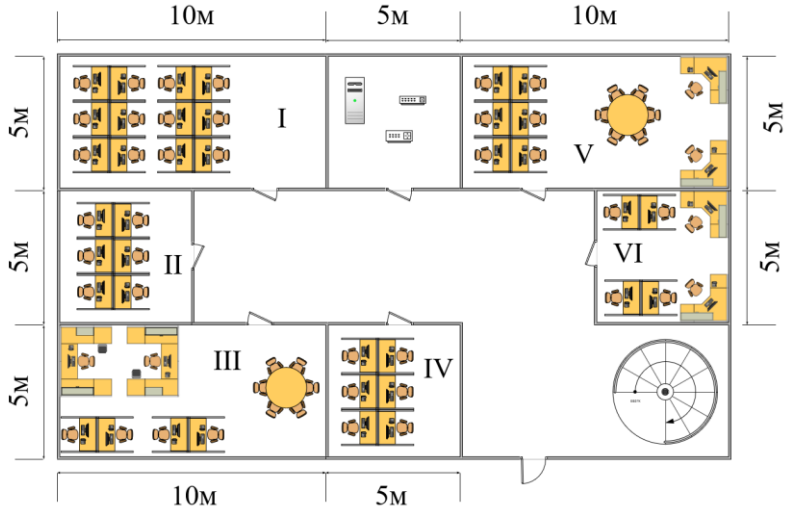

Рисунок 1.3 – Структурна схема розміщення підрозділів на другому поверсі локації А стоматологічної клініки «Amel Dental Clinic»

Також розглянемо структурну схему розміщення підрозділів на першому поверсі локації Б, в якій знаходяться пародонтологічне (I), ортодонтичне (II), терапевтичне (III), хірургічне (IV), дитяче відділення (V) та відділення загальної терапії (VI) (рис. 1.4).

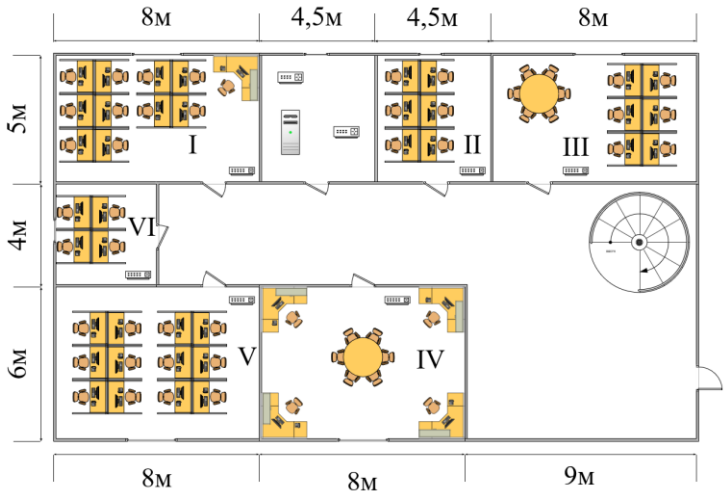

Рисунок 1.4 – Структурна схема розміщення підрозділів на першому поверсі локації Б стоматологічної клініки «Amel Dental Clinic»

1.4 Принципи та технічні способи інформаційного забезпечення об’єкта впровадження

В сфері медицини існує багато принципів, технічних способів та методів інформаційного забезпечення, які постійно розвиваються. Деякі з них наведені нижче:

1. Медичне обладнання. Це комп’ютеризовані системи, такі як МРТ, УЗД, які допомагають при обстеженні пацієнта для виявлення захворювань.
2. Системи підтримки прийняття рішень. Це системи, які допомагають лікарям приймати рішення на основі великого обсягу інформації.
3. Розпізнавання голосу та мови. Ці системи дозволяють пацієнтам та лікарям взаємодіяти з комп’ютерами за допомогою голосових команд.
4. Системи віртуальної реальності. За допомогою цих систем студенти можуть практикуватися на віртуальних пацієнтах, а лікарі можуть підвищувати кваліфікацію та проводити експерименти без ризику для реальних пацієнтів.
5. Системи моніторингу здоров’я. Це різноманітні системи, такі як датчики пульсу, кров’яного тиску, рівню кисню в крові, температури тіла, які допомагають слідкувати за станом пацієнта.
6. Телемедицина. Ця система дозволяє дистанційно проводити консультації та обстеження пацієнтів, що є особливо корисним для пацієнтів з невеликих міст або селищ.
7. Електронні медичні записи. Ці системи дозволяють лікарям та різним медичним закладам швидко обмінюватись інформацією.
8. Системи управління лікарнями. Ці системи дозволяють виставляти рахунки, управляти запасами ліків та обладнання, робити та редагувати записи пацієнтів.
9. Безпечне зберігання та резервне копіювання даних. За допомогою хмарних сервісів та локальних серверів дані про пацієнтів завжди є доступними. На випадок збою в режимі реального часу проводиться резервне копіювання інформації.

10. Мережева інфраструктура. За допомогою добре та безпечно розробленої мережевої інфраструктури буде забезпечуватись ефективна та безпечна робота клініки.

1.5 Аналітичний огляд існуючих способів обробки та передачі інформації, принципів побудови об’єкта впровадження, відомих рішень у галузі

Для клініки потрібно мати багато різних способів обробки та передачі інформації, адже медичним закладам постійно потрібно забезпечувати комунікацію між підрозділами, між персоналом в середині однієї лікарні та між клінікою і пацієнтом. За можливістю, способи передачі інформації повинні бути максимально захищені від третіх осіб. Для досягнення цієї мети будемо використовувати наступні методи:

1. Електронна пошта. Це один з найпоширеніших методів передачі інформації. Можна використовувати шифрування транспортного рівня TLS, що дозволяє зберігати конфіденційність даних при транспорті через Інтернет.

2. Месенджери. Можна використовувати Telegram, Viber або WhatsApp. Всі ці месенджери мають різні технології та методи, спрямовані на забезпечення конфіденційності інформації.

3. Відеозв’язок. Можна використовувати Skype або Zoom для запровадження телемедицини.

4. Гаряча лінія. За допомогою телефонії пацієнтам можуть надавати попередню консультацію та планувати прийоми.

5. Портали для пацієнтів. За допомогою онлайн-платформ пацієнти можуть мати доступ до своїх медичних записів, отримувати результати аналізів, записуватися на прийоми.

1.6 Завдання і мета роботи

Метою кваліфікаційної роботи є розробка комп'ютерної системи стоматологічної клініки "Amel Dental Clinic" з реалізацією побудови та налаштування корпоративної мережі та підсистеми IoT безпеки.

Для вирішення поставленої мети в роботі слід виконати наступні завдання:

- виконати аналіз об'єкта;
- сформулювати технічні вимоги для розробки КС;
- обгрунтувати вибір мережевої архітектури для майбутньої комп'ютерної мережі підприємства;
- розробити специфікацію апаратних засобів та СКМ;
- провести аналіз мережевого трафіку;
- розробити модель комп'ютерної мережі та виконати конфігурування мережевого обладнання ;
- реалізувати IoT-системи безпеки;
- провести тестування мережі в цілому та кожного компонента мережі окремо;

Результуюча мережа має бути масштабованою, надійною, безпечною та швидкою.

1.7 Визначення можливих напрямків рішення поставлених завдань

Для вирішення поставлених завдань щодо розробки комп'ютерної системи стоматологічної клініки "Amel Dental Clinic" з реалізацією побудови та налаштування корпоративної мережі та підсистеми IoT безпеки можуть бути використані наступні рішення:

1. Обрання мережевої архітектури для майбутньої комп'ютерної мережі.

Для комп'ютерної мережі клініки буде вибрано розподілену архітектуру з гібридним підходом. В розподіленій архітектурі передбачається розподіл мережевих ресурсів між взаємопов'язаними вузлами. Мережа також має ознаки

централізованої архітектури, де сервери надають послуги та ресурси клієнтським пристроям.

2. Обрання кабельної системи корпоративної мережі.

Для забезпечення зв’язку між будівлями потрібно обрати оптоволоконний кабель, адже він дозволяє передавати дані на великі відстані із високою швидкістю. Також в нього висока стійкість до електромагнітних перешкод. Для внутрішньої мережі в кожній будівлі буде використовуватися вита пара, яка є стандартом для Ethernet-мереж і забезпечує достатню швидкість передачі даних та надійність. Також буде задіяна технологія Wi-Fi для підключення пристроїв Інтернету речей.

3. Проведення аналізу мережевого трафіку.

Потрібно встановити мережеві монітори, такі як мережеві аналізатори, які можуть моніторити трафік в мережі. Також можна використовувати спеціальні програми, такі як Wireshark, для розшифрування та аналізу трафіку. У разі виявлення збоїв або перевантаження мережі потрібно ідентифікувати причини проблем та розробляти стратегію їх вирішення.

4. Обрання способу управління мережею.

В клініці буде задіяно локальне управління мережею. IT-персонал буде завжди знаходитись безпосередньо в клініці та відповідати за налаштування, моніторинг та вирішення проблем в мережі.

5. Створення фізичної та логічної топології комп’ютерної мережі.

В мережі буде існувати п’ять окремих підмереж, одна з яких буде віддаленою. Буде використовуватися протокол динамічної маршрутизації OSPF та впроваджено VPN для віддаленого підключення.

6. Виконання конфігурування мережевого обладнання комп’ютерної мережі.

В мережі будуть встановлені мережеві пристрої, такі як маршрутизатори та комутатори. Маршрутизатори будуть мати захист у вигляді захисту доступу, використання паролів, шифрування за допомогою SSH для безпечного віддаленого

доступу. Комутатори будуть мати захист доступу та технологію розділення фізичної мережі на віртуальні VLAN.

7. Реалізація IoT-системи безпеки.

Потрібно встановити різноманітні датчики та IoT-пристрої, а потім розробити сценарії дій в залежності від показників датчиків та впровадити IoT-систему до вже побудованої мережі.

8. Проведення тестування мережі в цілому та кожного компонента мережі окремо.

Потрібно провести тестування функціональності, пропускної здатності, навантаження та безпеки мережі.

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ КЛІНІКИ

2.1 Технічні вимоги до комп'ютерної Системи стоматологічної клініки

2.1.1 Вимоги до Системи в цілому

2.1.1.1 Вимоги до структури і функціонуванню Системи

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

Комп'ютерна Система стоматологічної клініки (далі Система) поділяється на локальні мережі (далі Підсистеми) згідно до загальної архітектури, як наведено у додатку А:

1. LAN_1 для хірургічного, дитячого відділення та відділення загальної терапії.
2. LAN_2 для пародонтологічного, ортодонтичного та терапевтичного відділення.
3. LAN_3 для віддаленої мережі.
4. LAN_4 для ортопедичного та анестезіологічного відділення.
5. LAN_5 для IT-відділу, відділу кадрів, бухгалтерії та відділу маркетингу.

Мережа була поділена на п'ять локальних мереж через велику кількість переваг, а саме:

1. Зручність управління. Мережевим адміністраторам набагато простіше керувати мережею, адже можна робити зміни або діагностику локально, не втручаючись у мережу в цілому.
2. Покращена безпека. Локальні мережі дозволяють більш точно налаштовувати правила безпеки. Наприклад, реалізація брендмауерів або VPN є набагато простішою в локальній мережі.

3. Покращена продуктивність. Швидкість передачі даних в локальній мережі буде набагато швидшою, адже пакетам не потрібно проходити через всю мережу.

4. Масштабованість. Поділяючи мережу на локальні мережі набагато легшим стає додавання інших пристроїв за необхідністю.

Локальна мережа LAN_1 повинна забезпечити комунікацію 58 вузлів.

Локальна мережа LAN_2 повинна забезпечити комунікацію 93 вузлів.

Локальна мережа LAN_3, що є віддаленою, повинна забезпечити комунікацію 80 вузлів.

Локальна мережа LAN_4 має забезпечувати 9 вузлів. До неї входять два сервери: HTTP для надання веб-сторінок та DNS для перекладу доменних імен в IP-адреси.

Локальна мережа LAN_5 має забезпечувати 91 вузол. В цій мережі існує сервер TFTP для передачі файлів.

Загалом Підсистема головного офісу налічує 251 вузол, а віддалена мережа 80 вузлів.

Також існує Підсистема Інтернету речей в основній та віддаленій мережах, яка складається з різноманітних датчиків, таких як датчики диму, вологості, руху, температури. зчитувач ID-карток та пристроїв, таких як сирена, зволожувач повітря, веб-камера, кондиціонер, батарея, двері.

2.1.1.1.2 Вимоги до способів і засобів зв'язку для інформаційного обміну між компонентами Системи

В LAN_1 повинна використовуватися технологія EtherChannel, що дозволяє об’єднати декілька фізичних з’єднань між комутаторами в одне логічне. Це дозволяє підвищити пропускну здатність та надійність мережі.

В LAN_5 повинна використовуватися технологія логічного розділення фізичної мережі на окремі віртуальні мережі VLAN.

Віддалена мережа LAN_3 повинна взаємодіяти з основною за допомогою технології VPN, яка робить підключення безпечним.

В мережі повинен використовується протокол динамічної маршрутизації OSPF для виявлення та прокладання маршрутів між різними підмережами.

Мережа повинна бути підключена до Інтернету через постачальника послуг (провайдера) за допомогою технології NAT.

Для внутрішньої мережі основної мережі та віддаленої повинна бути використана вита пара, а для об’єднання мереж – оптичне волокно.

Підсистема Інтернету речей з’єднується між собою за допомогою технології Wi-Fi.

2.1.1.1.3 Вимоги до характеристик взаємозв'язків створюваної Системи із суміжними системами, вимоги до її сумісності, у тому числі вказівки про способи обміну інформацією

Обмін інформацією відбувається за допомогою пересилання документів різних поширених в галузі медицини форматів, таких як DICOM, HL7, CDA, PDF та XML.

2.1.1.1.4 Вимоги до режимів функціонування Системи

Вимоги до режимів роботи функціонування Системи є наступними:

1. Стандартний режим. Система повинна забезпечувати функціонування клініки в години її роботи.

2. Екстрений режим. Цей режим активується у випадку надходження великої кількості пацієнтів або масштабних лихах. В такому режимі Система повинна бути готова до ефективного відгуку, забезпечуючи невідкладну медичну допомогу.

3. Резервний режим. Вся Система повинна працювати навіть в разі відсутності електропостачання.

4. Нічний режим. У нічний час Система повинна знаходитись у зменшеному режимі активності, під час якого деякі функції можуть бути обмеженими або автоматизованими.

5. Режим обслуговування. Цей режим передбачає ремонт, профілактику або налаштування компонентів Системи, під час чого відбувається обмеження функціональності Системи.

6. Режим аварійного відновлення. Цей режим передбачає відновлення роботи Системи в разі її збою або катастрофічної події.

2.1.1.1.5 Вимоги до діагностування Системи

Діагностування Системи повинно проводится не рідше, ніж один раз на пів року відповідальними фахівцями ІТ-відділу. У разі непердбачуваних збоїв аналіз та ремонтні роботи проводяться поза графіком.

Діагностування Системи повинно включати в себе наступні пункти:

1. Перевірка підключень та з’єднань. Потрібно перевірити фізичні підключення кожного пристрою в мережі та виявити можливі проблеми в кабельній Системі

2. Перевірка IP-адресації та мережевих налаштувань. Потрібно перевірити правильність присвоювання IP-адрес мережевим пристроям, комп’ютерам та перевірити налаштування мережевих протоколів.

3. Тестування пропускної здатності. Потрібно виміряти швидкість передачі даних в різних підмережах для виявлення можливих перенавантажень.

4. Виявлення проблем з безпекою. Потрібно перевірити наявність антивірусного програмного забезпечення та увімкнення брендмауерів на кожному комп’ютері.

5. Перевірка мережевих служб. Потрібно перевірити доступність веб-серверів, можливість обміну даними та віддалений доступ.

2.1.1.1.6 Перспективи розвитку Системи

Перспективи розвитку Системи можуть бути наступними:

1. Використання штучного інтелекту. За допомогою впровадження штучного інтелекту в клініці може покращитись діагностування та лікування пацієнтів, а також обслуговування комп'ютерної Системи може стати набаго простішим.

2. Система безпеки. Забезпечення безпеки стає все більш важливим, тому в подальшому планується використовувати новіші методи шифрування, авторизації та аутентифікації.

3. Інтеграція з переносними пристроями. За допомогою отримання даних з пристроїв пацієнтів у реальному часі може суттєво покращитись діагностування захворювань на ранніх стадіях. Завдяки цьому телемедицина вийде на інший рівень.

4. Додавання розумних пристроїв. Можна додати датчики забруднення повітря або протікання води.

5. Масштабування. В майбутньому можливе розширення лікарні.

6. Постійне вдосконалення. Співробітники ІТ-відділу повинні постійно слідкувати за новітніми тенденціями в розвитку комп'ютерних технологій та намагатися впроваджувати найкращі практики швидше за конкурентів.

2.1.1.2 Вимоги до показників призначення

Вимоги до показників призначення включають в себе такі аспекти:

1. Зв'язок. Система повинна забезпечувати зв'язок між персоналом клініки за допомогою миттєвих повідомлень, електронної пошти, відеоконференцій.

2. Обмін даними та доступ. Система повинна надавати лікарям можливість доступу до медичних даних пацієнтів. Це стосується аналізів, медичних зображень, записів пацієнтів.

3. Централізоване зберігання даних. Система повинна дозволяти централізовано зберігати дані на серверах, а також мати можливість відновлення даних за допомогою резервного збереження даних в хмарі.

4. Безпека. Система повинна захищати дані від несанкціонованого доступу та вірусів за допомогою впровадження різних механізмів безпеки.

5. Інтернет. Система повинна надавати можливість доступу до мережі Інтернет.

6. Віддалене підключення. Система повинна надавати можливість віддаленого підключення за допомогою VPN.

2.1.1.3 Вимоги до експлуатації

2.1.1.3.1 Умови і регламент (режим) експлуатації, що повинні забезпечувати використання технічних засобів (ТЗ) Системи з заданими технічними показниками

Система повинна забезпечувати свою працездатність при впливі наступних кліматичних факторів:

- температура навколишнього повітря: від 10°C до 45°C;
- вологість повітря: від 40% до 80% при температурі +10°C;
- атмосферний тиск від 84 кПа до 107 кПа.

При експлуатації потрібно дотримуватись усіх вимог, які зазначені виробником в документації до обладнання.

2.1.1.3.2 Вимоги до параметрів мереж енергопостачання

Вимоги до параметрів живлення включають в себе такі аспекти:

1. Напруга та частота. Напруга в мережі повинна бути 220 В (згідно ДСТУ «ГОСТ 21128» про номінальну напругу допустиме відхилення дорівнює ± 5% від номінальної напруги) з частотою 50 Гц ± 0,2 Гц (ДСТУ «ГОСТ 13109-97»).

2. Надійність. Мережа енергопостачання повинна бути надійною, щоб уникнути перебоїв в роботі Системи.

3. Резервне живлення. Вся Система повинна працювати навіть у випадку відсутності електропостачання за допомогою переходу на живлення від генератора. Генератор повинен бути як в основній, так і у віддаленій мережі. Перехід на резервне живлення повинен відбуватися автоматично.

4. Стабілізація напруги. Живлення повинно бути стабілізовано, щоб запобігти пошкодженню мережевого та медичного обладнання.

5. Заземлення. Всі електричні системи, такі як розетки, мережеве та медичне обладнання, комутаційні шафи повинні бути заземлені для захисту від електричних перешкод.

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

Персонал, що обслуговує Систему повинен мати освіту в області інформаційних технологій, бажано за спеціальністю “Комп’ютерна інженерія”.

Персонал повинен мати знання з протоколів, архітектури мережі, налаштування різних елементів Системи.

ІТ-відділ клініки складається з восьми осіб, що є достатнім для своєчасного обслуговування Системи. В будь-який час роботи клініки фахівці ІТ-відділу повинні бути присутніми для того, щоб клініка не понесла фінансових втрат. Саме для цього створено графік роботи ІТ-відділу – з 9:00 до 18:00 з понеділка по п’ятницю для чотирьох працівників, а з 9:00 до 18:00 з суботи по середу для інших чотирьох працівників відділу. Таким чином завжди хоча б чотири спеціаліста знаходяться на робочому місці.

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

Запасні прилади повинні складатися як мінімум з двох маршрутизаторів, двох комутаторів, одного серверу, одного IoT-шлюзу та п’ятьох ПК. Крім

обладнання, також потрібно мати не менше 30 метрів кабелю витої пари UTP та конекторів RJ-45 у кількості не менше 20.

Запасні прилади повинні знаходитись приміщенні, доступ до якого мають тільки відповідальні фахівці IT-відділу. В приміщенні повинен бути контроль температури, яка повинна бути на рівні 18-24 °C, та вологості, яка повинна бути на рівні 40%-60%.

2.1.1.3.5 Вимоги до регламенту обслуговування

Вимоги до регламенту обслуговування в залежності від виду обслуговування Системи:

1. Планове технічне обслуговування. Це включає в себе регулярні перевірки та профілактичні роботи. У процесі проведення технічного обслуговування повинен проводитися зовнішній і внутрішній огляд технічних засобів, перевірка контактних з'єднань, перевірка налаштування елементів і тестування їх взаємодії. Планове технічне обслуговування повинно проводитись не менше ніж раз на пів року.
2. Ремонт. Це включає в себе ремонт несправних компонентів, що може бути запланованим або невідкладним в залежності від характеру несправності.
3. Оновлення. Це включає в себе оновлення компонентів на більш сучасні, що відбувається в залежності від необхідності оновлення апаратного забезпечення та фінансування.
4. Моніторинг. Це включає в себе постійний нагляд за роботою Системи.

2.1.1.4 Вимоги до патентної чистоти

Обладнання та програмне забезпечення, яке використовується в комп’ютерній Системі, не повинно порушувати патентну чистоту. Для цього потрібно використовувати ліцензійне програмне забезпечення, проводити ретельні дослідження компонентів Системи для виявлення можливих патентів, звертатися за юридичною консультацією, вести документацію проектування компонентів

Системи, щоб в разі виникнення претензій від виробників мати доказову базу щодо патентної чистоти.

2.1.1.5 Додаткові вимоги

2.1.1.5.1 Вимоги до активного обладнання

Вимоги до активного обладнання включають в себе такі аспекти:

1. Надійність. Активне обладнання повинно бути якісним, забезпечувати стабільну роботу та відповідати стандартам якості.
2. Сумісність. Активне обладнання повинно бути сумісним з іншими пристроями в комп'ютерній Системі.
3. Пропускна здатність. Активне обладнання повинно мати достатню пропускну здатність на рівні 1Гбіт/с задля швидкої роботи комп'ютерної Системи без перевантажень.
4. Безпека. Активне обладнання повинно базуватись на платформі Cisco IOS, яка має широкий набір мехінізмів безпеки, таких як шифрування, віртуальні приватні мережі VPN, фаєрвол, контроль доступу та інше.
5. Кількість портів та їх запас. Активне обладнання повинно мати достатню кількість портів для забезпечення потреб мережі та мати вільні порти на випадок розширення мережі.
6. Встановлення. Активне обладнання повинно бути встановлено в спеціальному технічному приміщенні, яке в свою чергу повинно знаходитись на оптимальній відстані від інших вузлів мережі, щоб мінімізувати довжину кабелів. Технічне приміщення повинно знаходитись в безпечному місці та мати двері з доступом по карткам-ключам, які надаються тільки відповідальним фахівцям.

2.1.1.5.2 Вимоги до кабель-каналів, інформаційним та електричним розеткам

У приміщеннях з високою вологістю вимоги до електричних розеток повинні бути наступними:

1. Вологостійкість. Електричні розетки повинні мати достатній рівень захисту від води на рівні IP44.

2. Матеріали. Потрібно використовувати стійкі до вологи та корозії матеріали, такі як ударостійкий пластик.

3. Живлення та заземлення. Електричні розетки повинні мати заземлення, що мінімізує ризик ураження електричним струмом, а також мати захист від перенапруги.

4. Перевірка та технічне обслуговування. Розетки повинні перевірятися мінімум один раз на пів року та у випадку несправностей бути негайно відремонтовані або замінені.

5. Відповідність нормам. Електричні розетки повинні відповідати нормам, які в казані в технічних документах, таких як: ДБН В.2.5-28-2006 "Електроустановки з низьковольтними електричними мережами" – встановлює вимоги до проектування, будівництва та експлуатації електричних мереж, включаючи електричні розетки, ДБН В.2.5-67:2012 "Електричне освітлення" – містить вимоги до електричного освітлення, включаючи розетки для підключення освітлювального обладнання, ДБН В.2.5-32-2013 "Електропостачання споруд" – визначає вимоги до електропостачання будівель і споруд, включаючи розетки для підключення електричних приладів.

Кабель-канали інформаційної кабельної системи повинні відповідати наступним вимогам:

1. Захист. Кабель-канали повинні мати захист від фізичних пошкоджень.

2. Доступність. Кабель-канали повинні бути легко доступними до розміщення та обслуговування.

3. Пожежна безпека. Кабель-канали повинні відповідати нормам пожежної безпеки, будучи виконаними з вогнестійких матеріалів.

2.1.1.5.3 Вимоги до комунікаційного обладнання і його розташування

Вимоги до комунікаційного обладнання включають в себе такі аспекти:

1. Розташування. Комунікаційне обладнання повинно знаходитись в спеціальній комутаційній шафі, яка захищена від вологості , пилу та інших зовнішніх впливів. Шафа повинна знаходитись в технічному приміщенні.

2. Тип шаф. Комутаційні шафи повинні мати достатню ємність для розміщення обладнання, бути стійкими до вібрацій та мати можливість легкого доступу для обслуговування.

3. Тип підводу кабельних трас. Кабельні траси повинні бути правильно спроектовані, забезпечувати належну організацію, відповідати стандартам, бути захищеними від зовнішніх впливів. Також кабельні шляхи повинні бути захищеними від силових кабелів для запобігання перешкодам.

4. Розміщення обладнання усередині шафи. Обладнання повинно бути надійно закріплено та логічно розташовано для легкої ідентифікації. Також повинен бути достатній простір між пристроями для належної вентиляції та легкого доступу.

5. Заземлення. Корпус комутаційної шафи повинен бути заземлений для забезпечення електричної безпеки.

6. Навколишнє середовище. Комунікаційне обладнання повинно знаходитись в середовищі з температурою 18-24 °C, адже висока температура може призвести до перегріву, а низька може спричинити утворення конденсату. Вологість повинна бути на рівні від 40% до 60%. Для забезпечення такого постійного рівня температури та вологості в технічному приміщенні, де повинно знаходитись комунікаційне обладнання, має бути вентиляція, кондиціонер, зволожувачі або осушувачі повітря.

2.1.1.5.4 Вимоги до однорідності

До основних вимог однорідності відносяться:

1. Типи кабелів. Потрібно використовувати єдиний тип кабелю в усій мережі. Для витої пари потрібно використовувати кабель категорії 6A, а для оптоволоконного кабелю – OS1.

2. З’єднувачі. Потрібно використовувати конектори типу RJ-45 для підключення Ethernet.

3. Магістральна інфраструктура. В Системі повинно використовуватися мережеве обладнання Cisco.

4. Протоколи. Потрібно використовувати стандартні протоколи, такі як TCP/IP, Ethernet, Wi-Fi.

2.1.1.5.5 Вимоги до резервування

Серед вимог до резервування можна виділити наступне:

1. Зовнішнє сховище. Резервне копіювання потрібно робити на віддалені місця зберігання, що захищає дані в разі фізичного пошкодження будівлі лікарні внаслідок стихійних лих або крадіжки. Зберігання поза межами об’кту повинно бути впроваджено за допомогою хмарних сервісів.

2. Апаратне резервування. Потрібно забезпечити резервування даних на фізичних пристроях, таких як сервер.

2.1.1.5.6 Вимоги безпеки та захисту інформації від несанкціонованого доступу

Вимоги з безпеки та захисту інформації від несанкціонованого доступу мають вирішальне значення для забезпечення цілісності та конфіденційності даних, тому нижче наведено основні з них:

1. Аутентифікація та авторизація. Повинні бути встановлені механізми аутентифікації, такі як паролі, біометричні дані, цифрові електроні підписи. Кожен

співробітник повинен мати доступ лише до обмеженої інформації в залежності від його відповідальності, що є механізмом авторизації.

2. Фізична безпека. Всі кімнати повинні бути зачиненими на ключ в неробочий час та у випадку, коли персонал залишив робоче місце, а приміщення з мережевим обладнанням повинно зачинятися за допомогою картки-ключа. Повинен бути введений облік взяття та здачі ключа. Також обов'язковим є наявність відеоспостереження. Важливі документи повинні знаходитись в сейфах.

3. Навчання персоналу. Задля збереження цілісності та конфіденційності інформації персонал повинен раз на пів року проходити тест з інформаційної безпеки. Також потрібно раз на три місяці змінювати пароль для входу в Систему. Для цього, в програмному забезпеченні має бути реалізовано нагадування про необхідність змінення паролю.

4. Безпечне віддалене підключення. За допомогою VPN будь-який працівник зможе підключитися до внутрішніх ресурсів клініки з будь-якого комп'ютера з Інтернет-доступом в разі неможливості бути присутнім на робочому місці, адже ця технологія забезпечує конфіденційність даних під час їх передачі через незахищені мережі, такі як Інтернет. Також потрібно використовувати протокол SSH для безпечного віддаленого доступу та керування мережевими пристроями.

5. Захист від шкідливого програмного забезпечення. На кожному комп'ютері повинен бути встановлений антивірус та включений брендамауер для запобігання вірусам.

6. Шифрування. Потрібно використовувати алгоритми шифрування даних, такі як AES або RSA, для того, щоб навіть в разі перехоплення інформації зловмисниками, її було неможливо прочитати.

2.1.2 Вимоги до задач (налаштувань), які виконує КС

Під час розробки адресації підмереж потрібно враховувати наступні вимоги:

- корпоративна мережа повинна складатися з 5 підмереж LAN1-LAN5;

- кількість вузлів в кожній підмережі повинно дорівнювати 58, 93, 80, 9 та 91 відповідно;
- блок адрес для виділення підмереж повинен бути 10.23.60.0/22;
- для каналів між маршрутизаторами повинен застосовуватися блок адрес 10.1.12.0/24;
- середня інтенсивність вихідного трафіку в найбільшій мережі повинна дорівнювати μ =145 кадрів/с;
- середня довжина вихідного повідомлення в найбільшій мережі повинна дорівнювати 650 байт;
- затримка передачі пакету в найбільшій мережі повинна бути ≤6 мс.

Під час розробки адресації пристроїв потрібно враховувати наступні вимоги:

- перші можливі для використання IP-адреси повинні бути призначені інтерфейсам і підінтерфейсам маршрутизаторів у LAN;
- другі з можливих IP-адрес повинні бути призначені комутаторам у LAN;
- серверам повинні бути призначені IP-адреса за правилом: IP-адрес дорівнює першому можливому адресу у мережі+9+12. [3]

Для виконання базового налаштування конфігурації пристроїв необхідно враховувати наступні вимоги:

- потрібно назначити назви пристроям за наступним правилом: Прізвище студента_тип пристрою_номер пристрою;
- на всіх пристроях повинен бути назначений пароль cisco до консолі і vty;
- на всіх пристроях повинен бути назначений пароль class до привілейованого режиму;
- усі паролі, що зберігаються у відкритому вигляді, потрібно зашифрувати;
- потрібно розробити банер MOTD;
- потрібно назначити на усіх лініях vty використання протоколу ssh;

- потрібно призначити ім’я користувача та пароль на всіх пристроях за правилом: група_прізвище з паролем admincisco;
- в якості імені домена потрібно використати ім'я пристрою. Для шифрування даних потрібно створювати ключ RSA завдовжки 1024 біт;
- на DCE-інтерфейсах маршрутизаторів потрібно призначити встановлення значення тактової частоти – 128000;
- потрібно налаштувати аудит і відправку повідомлень про початок і завершення процесу exec, з використанням локальної бази;
- з метою збільшення пропускної здатності і надійності каналів в мережі LAN_1 на комутаторах потрібно виконати об'єднання фізичних ліній. [3]

На маршрутизаторах повинен використовватися протокол динамічної маршрутизації OSPF, що підтримує множинні шляхи, має малий час збіжності і реагування та створює мінімальний службовий трафік. Під час налаштування маршрутизаторів потрібно враховувати наступні вимоги:

- потрібно оголосити безпосередньо підключені мережі і відключити поширення оновлень маршрутизації на інтерфейси в локальні мережі;
- для VLAN мереж потрібно налаштувати сумарний маршрут і оголосити його іншим маршрутизаторам;
- адже в мережі використовується OSPF, то потрібно змінити еталонну пропускну спроможність для обчислення вартості за умовчанням для дозволу інтерфейсів Gigabit на значення = 1000;
- потрібно задати пропускну спроможність на serial-інтерфейсах = 128 Кб/с, вартість метрики = 7500;
- потрібно налаштувати маршрут за умовчанням на маршрутизаторі з прямим підключенням до інтернет-провайдера (ISP) і розповсюдити його через оновлення маршрутизації;
- потрібно налаштувати на цьому маршруті ручне підсумовування. [3]

Під час налаштування всіх маршрутизаторів на підтримку служби AAA необхідно враховувати наступні вимоги:

- для перевірки підключень до VTY ліній на маршрутизаторі потрібно використовувати локальну базу даних користувачів;
- для доступу до консолі потрібно використовувати аутентифікацію на основі протоколу RADIUS і якщо немає − локальну базу даних;
- RADIUS-сервер потрібно налаштувати наступним чином: ключове слово – radius123; в якості облікового запису користувачів потрібно використовувати ім’я пристрою з паролем admin123. [3]

При налаштуванні роботи Інтернет в Системі необхідно враховувати наступні вимоги:

- потрібно встановити одного провайдера послуг доступу до Інтернет (ISP);
- Для виходу робочих станцій в Інтернет необхідно настроїти пограничний маршрутизатор з динамічним NAT за такими даними: ім’я пула: Internet, пул адресів: 209.165.200.5 по 209.165.200.30, номер списку доступу 12;
- потрібно налаштувати сервер HTTP, щоб на вузлах при вводі в рядку браузера http://123.dnipro.ua (http://209.165.200.4) відкривався веб-сайт з відомостями про тему та завдання на кваліфікаційну роботу студента;
- потрібно налаштувати віртуальну приватну мережу site-to-site VPN з використанням IPsec для трафіку, що проходить між «Підмережою підрозділу підприємства» та віддаленою мережею організації через Internet. [3]

Під час налаштування мереж VLAN і маршрутизації між ними потрібно враховувати наступні вимоги:

- в LAN_5 потрібно створити мережі VLAN з номерами 22, 32, 42, 99 та 100 і присвоїти кожній з них відповідне ім'я IT_Department, Accounting_and_Marketing, Human_Resources_Department, Management та Native;
- потрібно налаштувати транкові порти і порти доступу, а також вимкнути усі невикористовувані фізичні порти комутаторів;
- потрібно налаштувати SVI-інтерфейси на комутаторах, призначивши IPv4-адреси з мережі Management VLAN;

- потрібно налаштувати маршрутизацію між мережами VLAN. [3]

При налаштуванні адресації ПК в мережах VLAN необхідно враховувати наступні вимоги:

- потрібно налаштувати маршрутизатор, що здійснює маршрутизацію між VLAN, в якості сервера DHCP для мереж VLAN;
- потрібно створити пули DHCP під назвою pollvlan№, де № − номер VLAN;
- потрібно виключити з пулу перші 10 адрес і для кожного пулу вказати адресу DNS-сервера і шлюз за замовчуванням. [3]

На портах комутаторів, підключених до серверів, потрібно налаштувати функцію безпеки портів, враховуючи наступні вимоги:

- тільки двом унікальним пристроям повинен бути дозволений доступ до порту;
- MAC-адрес пристрою повинен розпізнаватися динамічно і додаватися в поточну конфігурацію;
- під час порушенні системи безпеки повинно з’являтися повідомлення, а порт повинен залишатися включеним. [3]

2.1.3 Вимоги до видів забезпечення КС

2.1.3.1 Вимоги до математичного забезпечення

Вимоги не передбачаються.

2.1.3.2 Вимоги до інформаційного забезпечення

Вимоги до інформаційного забезпечення лікарні повинні бути наступними:

1. Конфіденційність. Система інформаційного забезпечення повинна мати надійні методи захисту даних.
2. Масштабованість. Система повинна мати можливість розширення в разі збільшення лікарні.

3. Доступність. Система повинна працювати безперебійно 24/7, щоб персонал завжди мав доступ до даних пацієнта.

4. Резервне копіювання. Система повинна завжди мати резервне копіювання інформації в разі виходу з ладу сервера.

5. Аналітика даних і звітність. Система повинна мати аналітику даних і можливості звітності, щоб надавати інформацію та підтримувати процеси прийняття рішень.

2.1.3.3 Вимоги до лінгвістичного забезпечення

Основна мова взаємодії користувача з технічним забезпеченням повинна бути українською, але також має бути можливість переключитися на англійську мову.

Сайт клініки повинен бути виконаний українською мовою, а також мати можливість перемикання на англомовну версію.

2.1.3.4 Вимоги до технічного забезпечення

Для ефективної роботи кожне робоче місце повинно бути оснащене комп’ютером з такою конфігурацією:

- процесор з мінімум чотирма ядрами з тактовою частотою не нижче 2 Ггц;
- об’єм опертивної пам’яті не нижче 8 Гб;
- дискретний відеоадаптер;
- об’єм пам’яті не менше 256 Гб;
- операційна система Windows 10 або Windows 11.

Сервер повинен відповідати вимогам:

- процесор не нижче 1,5 Ггц;
- об’єм опертивної пам’яті не нижче 8 Гб.

Комутатор повинен відповідати вимогам:

- 24 порти FastEthernet та порт GigabitEthernet;

- підтримка Etherchannel, VLAN.

Маршрутизатор повинен відповідати вимогам:

- мінімум 2 порти GigabitEthernet, 4 EHWIC слоти;
- підтримка DHCP, NAT, VPN та AAA моделі.

Шлюз IoT повинен відповідати вимогам:

- підтримка Wi-Fi;
- підтримка дистанційного управління.

2.1.3.5 Вимоги до організаційного забезпечення

Працівники IT-відділу повинні мати доступ до технічного приміщення за допомогою картки-ключа.

2.1.3.6 Вимоги до методичного забезпечення

Повинна бути надана структурна схема комплексу технічних засобів, топологічна схема корпоративної мережі, таблиця адресації пристроїв, таблиця специфікації обладнання, таблиця специфікації структурованої кабельної мережі, схема розміщення кабельних мереж.

2.2 Розробка апаратної частини комп'ютерної Системи

2.2.1 Розробка структурної схеми комплексу технічних засобів

Між маршрутизаторами використовуються кабелі Serial DTE або крос-кабелі. Маршрутизатори та комутатори поєднуються між собою за допомогою прямого кабеля, так само як і комп'ютери до комутаторів. Для з'єднання комутаторів використовується крос-кабель.

На основі загальної архітектури клініки (додаток А), кількості підмереж (див.п.2.1.2), кількості вузлів в підмережах (див.п.2.1.2), а також враховуючи вимогу виходу Системи до Інтернету (див.п.2.1.2) та номери VLAN (див.п.2.1.2), була розроблена структурна схема комплексу технічних засобів комп'ютерної Системи клініки, яка показана на рис. 2.2.

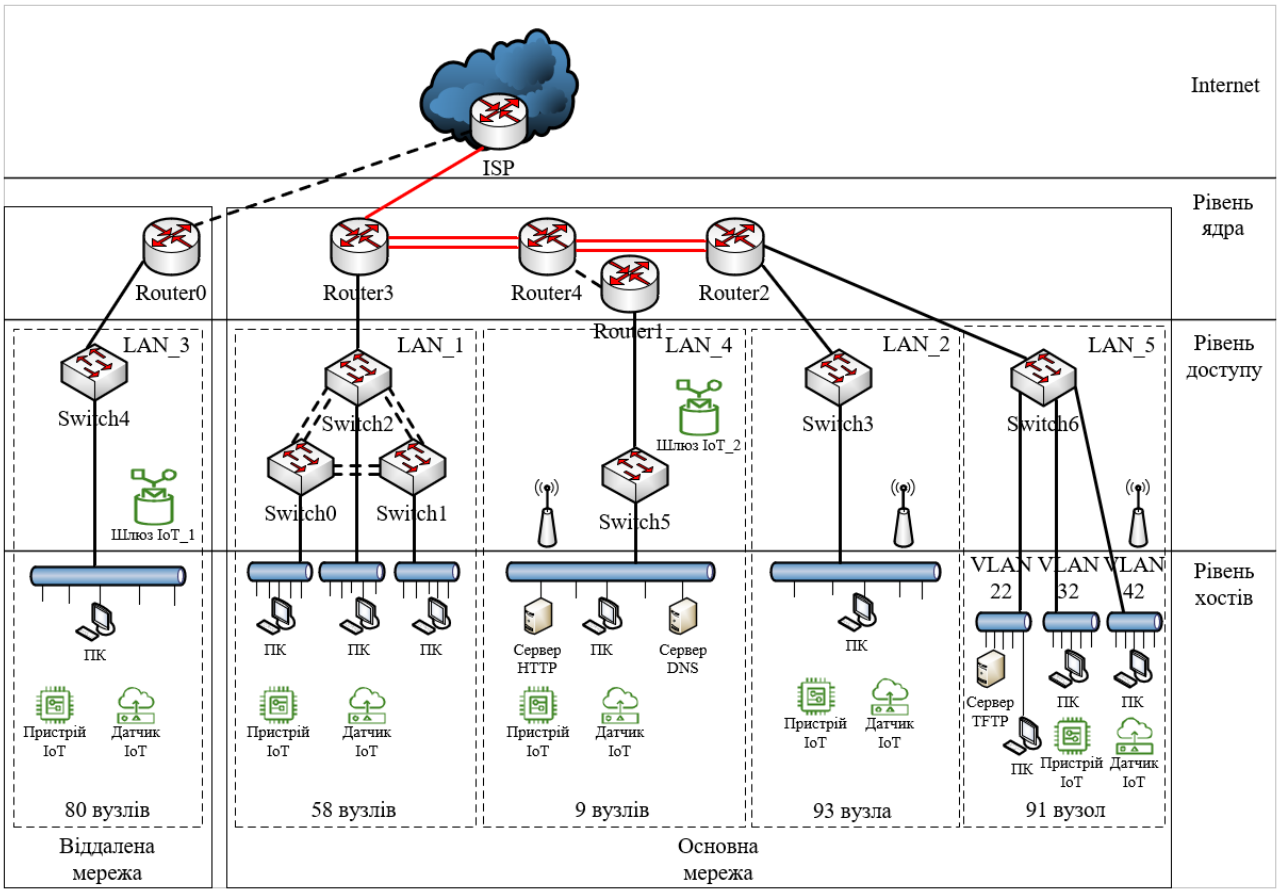

Рисунок 2.2 – Структурна схема комплексу технічних засобів комп’ютерної системи стоматологічної клініки «Amel Dental Clinic»

2.2.2 Розробка специфікації апаратних засобів комп’ютерної Системи

Специфікація обладнання для комп’ютерної Системи наведена в таблиці 2.1.

Таблиця 2.1 – Специфікація обладнання

Позиція	Найменування і технічна характеристика	Тип, марка, позначення документа, опитувального листа	Одиниці виміру	Кількість	Примітки
1	**2**	**3**	**4**	**5**	**6**
1.	Маршрутизатор серії Cisco 2901: 2 onboard GE, 4 EHWIC slots, 2 DSP slots, 1 ISM slot, 256MB CF default, 512MB DRAM default, IP Base	Cisco 2901/K9	од.	6	За структурною схемою КТЗ: Router 0-4 Детальні характеристики: https://stack-systems.com.ua/marshrutizator-cisco-2901-k9
2.	Комутатор серії 2960: 24 10/100 + 2 1000BT LAN Base Image	WS-C2960-24TT-L	од.	18	За структурною схемою КТЗ: Switch 0-6 Детальні характеристики: https://stack-systems.com.ua/kommutator-cisco-ws-c2960-24tt-l
3.	Шлюз IoT: Wi-Fi, Z-Wave, Zigbee Управління SmartThings, Сумісність з Amazon Alexa та Google Assistant, голосове управління	Aeotec Smart Home Hub GP-AEOHUBV3EU	од.	2	За структурною схемою КТЗ: Шлюз IoT_1-2 Детальні характеристики: https://homehub.com.ua/centrali-signalizaciy/aeotec-smart-home-hub-gp-aeohubv3eu.html

Продовження таблиці 2.1

4.	Сервер: 2 шт x Intel Xeon E5-2650L v2 (1.70-2.10 GHz), 8 GB DDR3, 2x порта 1 Gb Ethernet, Cisco Integrated Management Controller (CIMC)	Cisco UCS C220 M3 LFF	од.	3	За структурною схемою КТЗ: Сервер HTTP, DNS, TFTP Детальні характеристики: http://surl.li/hnuad
5.	Комп’ютер: AMD Ryzen 5 5600G (3.9 — 4.4 ГГц), 16 ГБ DDR4, 480 ГБ SSD, AMD Radeon Vega 7, Windows 11 Pro	ARTLINE Business B38v08Win	од.	331	За структурною схемою КТЗ: ПК Детальні характеристики: https://comfy.ua/ua/nettop-artline-business-b38-b38v08win.html

Усе мережеве обладнання підібрано фірми Cisco, тому проблем з сумісністю компонентів Системи бути не повинно.

Розглянемо вибір СКМ на прикладі LAN_3 стоматологічної клініки «Amel Dental Clinic». Для цього проектуємо схему поверху та розміщення кабелів, як показано на рис. 2.3.

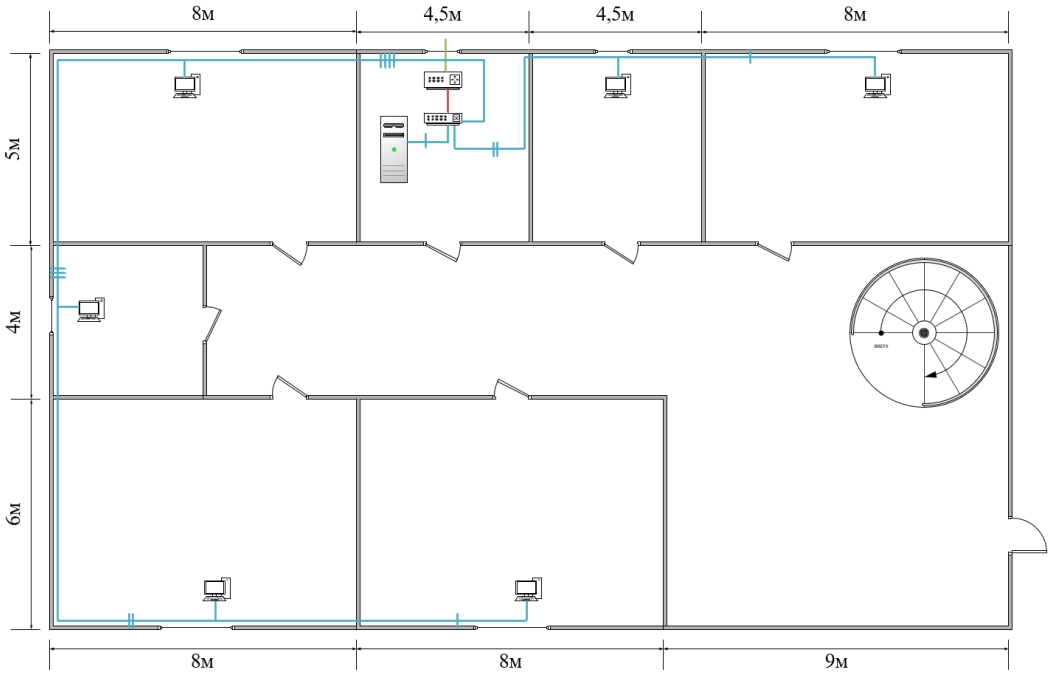

Рисунок 2.3 – Схема розміщення кабельних мереж першого поверху локації Б стоматологічної клініки «Amel Dental Clinic»

Специфікація структурованої кабельної мережі наведена в таблиці 2.2.

Таблиця 2.2 – Специфікація структурованої кабельної мережі

Позиція	Найменування і технічна характеристика	Тип, марка, позначення документа, опитувального листа	Одиниці виміру	Кількість	Примітки
1	**2**	**3**	**4**	**5**	**6**
1.	Кабельний канал 40×25 мм	«ЭЛЕКОР»	м.	65	За проектом для LAN_3 для крученої пари
2.	Розетка комп’ютерна RJ-45 UTP подвійна	Schneider Electric Asfora	од.	40	За проектом для LAN_3
3.	Lan кабель UTP КПВ-ВП cat.5E 4x2x0,51	Одескабель	м.	80	За проектом для LAN_3
4.	Розетка із заземленням подвійна	Videx Binera	од.	42	За проектом для LAN_3

Продовження таблиці 2.2

5.	Кабель живлення ПВС 3*1	Одескабель	м.	80	За проектом для LAN_3
6.	Кабельний канал 40×25 мм	«ЭЛЕКОР»	м.	65	За проектом для LAN_3 для кабелю живлення
7.	Комутаційна коробка	«IEK»	од.	1	За проектом для LAN_3

2.2.3 Розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі підприємства

Пропускна здатність лінії вихідного каналу дорівнює 1000Мбіт/с.

Швидкість надходження пакетів повинна бути менше, ніж швидкість відправлення для того, щоб не перевантажувати канал.

Середня інтенсивність трафіку μ=145 кадрів/с (див.п.2.1.2), а середня довжина повідомлення складає 650 байт.

Припустимо, що всі користувачі одночасно використовують послуги. Розрахуємо пропускну здатність LAN_2, яка складається з 93 вузлів. Пропускна здатність мережі на рівні доступу буде дорівнювати:

$$P_{р.р} = \mu * L_{пов} * N * 8 = 145 * 650 * 93 * 8 = 70{,}122 \text{ Мбіт/с}, \quad (2.1)$$

де N – кількість вузлів в мережі

$L_{пов}$ – середня довжина повідомлення

Отримані результати не перевищують заданих параметрів мережі по вихідному каналу, тому перевантажень не буде.

Комутатор рівня доступу передає трафік до маршрутизатора через вихідний порт зі швидкістю передачі даних 1000Мбіт/с.

Загальне навантаження на комутатор не повинно перевищувати:

$$\mu_{вих} = 1000\,000\,000/(650*8) = 192308 \text{ пакетів/с} \quad (2.2)$$

Оскільки кожне джерело в середньому виробляє в середньому 145 пакетів/с, то кількість приєднань, якими обмежен комутатор рівня доступу, складає максимум:

$$N = \mu_{вих}/\mu = 192308/145 = 1326 \text{ джерел} \quad (2.3)$$

Це задовольняє найбільшу мережу з 93 ПК.

Кожен з 93 ПК посилає потік заявок з інтенсивністю 145 кадрів/с. Інтенсивність вихідного трафіку:

$$\lambda=N*\mu=93*145=13\ 485 \text{ пакетів/с} \quad (2.4)$$

Коефіцієнт затримки:

$$\rho=\lambda/\mu_{вих}=13\ 485/192308=0,07 \quad (2.5)$$

Коефіцієнт зайнятості комутатора рівня доступу:

$$\rho=\rho/(1-\rho)=0,07/0,93=0,075 \quad (2.6)$$

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

$$T=1/(\mu_{вих}-\lambda)=1/(192308-13\ 485)=5,59 \text{ мкс} \quad (2.7)$$

Середня довжина черги:

$$L_{чер}= \rho^2/(1-\rho)=0,07^2/0,93=0,005 \quad (2.8)$$

Середній час перебування пакета у черзі:

$$T_{оч}= L_{чер}/ \lambda=0,005/13\ 485=0,37 \text{ мкс} \quad (2.9)$$

Це значення менше 6 мс, що задовольняє вимогам (див.п.2.1.2)

3 ПРОЕКТУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА РОЗРАХУНОК ЇЇ НАЛАШТУВАНЬ

3.1 Розрахунок адресації комп'ютерної мережі

Розділення мережі на підмережі є процесом поділу IP-адресного простору мережі на менші окремі підмережі. В таблиці 3.1 наведено блок адрес мережі та кількість вузлів в кожній підмережі.

Таблиця 3.1 – Блок адрес мережі та кількість вузлів в кожній підмережі

№	Блок адрес	LAN1	LAN2	LAN3	LAN4	LAN5
12	10.23.60.0/22	58	93	80	9	91

Тобто, необхідно створити 5 підмереж для 331 користувачів.

Розділення мережі на підмережі відбувається за допомогою методу VLSM (маскування підмережі змінної довжини). За допомогою цього методу можна розділити мережу на кілька підмереж із різною довжиною маски підмережі. Головною перевагою цього методу є ефективне використання простору IP-адрес. В залежності від розміру підмережі можна виділяти менші або більші блоки IP-адрес, що значно впливає на ефективність розподілу ресурсів та збереження IP-адрес. Це покращує масштабованість мережі та її управління.

Для розділення мережі 10.23.60.0/22 на п'ять підмереж, спочатку потрібно визначити маску для кожної підмережі.

Адже в роботі буде використовуватись протокол IPv4, то мережу можна розділити на підмережу, яка складається з 1 (маска /32), 2 (маска /31), 4 (маска /30), 8 (маска /29), 16 (маска /28), 32 (маска /27), 64 (маска /26), 128 (маска /25) або 256 (маска /24) адрес, що відповідає двійкам в ступені від 0 до 8. Потрібно враховувати, що 2 адреси, а саме адресу мережі та широкомовну адресу, в підмережі не можна буде використовувати. Також потрібно враховувати кількість комутаторів в підмережах, яким потрібно буде призначено адресу SVI-інтерфейсу.

Враховуючи те, що мережа повинна бути масштабованою, для підмережі LAN1 з 58 вузлами, візьмемо 128 (маска /25) адрес. Для підмереж LAN2 та LAN3 з

93 та 80 вузлами відповідно, візьмемо теж по 128 (маска /25) адрес. Для мережі LAN4 з 9 вузлами візьмемо 32 (маска /27) адреси. Для мережі LAN5 візьмемо 256 (маска /24) адрес, враховуючи наявність віртуальних локальних мереж VLAN.

Для виділення підмережі переведемо адресу мережі в двійковий вид і відокремимо частину, в яку входить вже вибрана маска.

Вибираємо блок в 256 адрес. 256 = 2^8, тому відрізуємо сім біт справа.

10.23.00111100.|00000000

Заповнюємо частину справа одиницями і отримуємо кінець діапазону IP-адрес.

10.23.00111100.|11111111

Отримуємо підмережу 10.23.60.0/24 з діапазоном IP-адрес 10.23.60.1 - 10.23.60.254. Широкомовна адреса – 10.23.60.255.

Збільшуємо останню адресу отриманої мережі на одиницю і виділяємо блок в 128 адрес, відрізавши справа 7 бітів, адже 128 = 2^7:

10.23.00111101.0|0000000

10.23.00111101.0|1111111

Отримуємо підмережу 10.23.61.0/25 з діапазоном IP-адрес 10.23.61.1 - 10.23.61.126. Широкомовна адреса – 10.23.61.127.

Збільшуємо останню адресу отриманої мережі на одиницю і виділяємо блок в 128 адрес:

10.23.00111101.1|0000000

10.23.00111101.1|1111111

Отримуємо підмережу 10.23.61.128/25 з діапазоном IP-адрес 10.23.61.129 - 10.23.61.254. Широкомовна адреса – 10.23.61.255.

Збільшуємо останню адресу отриманої мережі на одиницю і виділяємо блок в 128 адрес:

10.23.00111110.0|0000000

10.23.00111110.0|1111111

Отримуємо підмережу 10.23.62.0/25 з діапазоном IP-адрес 10.23.62.1 - 10.23.62.126. Широкомовна адреса – 10.23.62.127.

Збільшуємо останню адресу отриманої мережі на одиницю і виділяємо блок в 32 адрес, відрізавши справа 5 біти, адже 32 = 2^5:

10.23.00111110.100|00000

10.23.00111110.100|11111

Отримуємо підмережу 10.23.62.128/27 з діапазоном IP-адрес 10.23.62.129 - 10.23.62.158. Широкомовна адреса – 10.23.62.159.

Схема адресації мережі наведена в таблиці 3.2

Таблиця 3.2 – Схема адресації мережі

Назва мережі	Кількість вузлів	Номер мережі	Маска мережі	Початкове значення діапазону можливих адрес вузлів у підмережі	Кінцеве значення діапазону можливих адрес вузлів у підмережі
LAN1	58	10.23.61.0	/25	10.23.61.1	10.23.61.126
LAN2	93	10.23.61.128	/25	10.23.61.129	10.23.61.254
LAN3	80	10.23.62.0	/25	10.23.62.1	10.23.62.126
LAN4	9	10.23.62.128	/27	10.23.62.129	10.23.62.158
LAN5	91	10.23.60.0	/24	10.23.60.1	10.23.60.254

Для каналів між маршрутизаторами буде застосовуватися блок адрес 10.1.12.0/24. Так само за допомогою методу VLSM розділимо мережу на п’ять підмереж з двома вузлами в кожній. В таблиці 3.3 представлено схему адресації каналів між маршрутизаторами.

Таблиця 3.3 – Схема адресації каналів між маршрутизаторами

Назва мережі	Кількість вузлів	Номер мережі	Маска мережі	Початкове значення діапазону можливих адрес вузлів у підмережі	Кінцеве значення діапазону можливих адрес вузлів у підмережі
WAN1	2	10.1.12.0	/30	10.1.12.1	10.0.12.2
WAN2	2	10.1.12.4	/30	10.1.12.5	10.0.12.6

Продовження таблиці 3.3

WAN3	2	10.1.12.8	/30	10.1.12.9	10.0.12.10
WAN4	2	10.1.12.12	/30	10.1.12.13	10.0.12.14
WAN5	2	10.1.12.16	/30	10.1.12.17	10.0.12.18

3.2 Розрахунок адресації пристроїв

У таблиці 3.4 наведена адресація всіх маршрутизаторів мережі.

Таблиця 3.4 – Схема адресації пристроїв

Пристрій	Інтерфейс	IP-адреса	Маска
Sokolovskyi_Router_0	Gig0/0	10.23.62.1	255.255.255.128
	Gig0/1	64.100.13.1	255.255.255.252
Sokolovskyi_Router_1	Gig0/0	10.1.12.17	255.255.255.252
	Gig0/1	10.23.62.129	255.255.255.224
Sokolovskyi_Router_2	Se0/0/0	10.1.12.2	255.255.255.252
	Se0/0/1	10.1.12.6	255.255.255.252
	G0/1	10.23.61.129	255.255.255.128
	Gig0/0.22	10.23.60.65	255.255.255.192
	Gig0/0.32	10.23.60.129	255.255.255.192
	Gig0/0.42	10.23.60.1	255.255.255.192
	Gig0/0.99	10.23.60.193	255.255.255.240
Sokolovskyi_Router_3	Gig0/0	10.23.61.1	255.255.255.128
	Se0/1/0	209.165.202.1	255.255.255.252
	Se0/0/0	10.1.12.9	255.255.255.252
	Se0/0/1	10.1.12.13	255.255.255.252
Sokolovskyi_Router_4	Se0/1/0	10.1.12.10	255.255.255.252
	Se0/1/1	10.1.12.14	255.255.255.252
	Se0/0/0	10.1.12.1	255.255.255.252
	Se0/0/1	10.1.12.5	255.255.255.252
	Gig0/0	10.1.12.18	255.255.255.252
Sokolovskyi_Router_ISP	Gig0/0	64.100.13.2	255.255.255.252
	Gig0/1	209.165.201.1	255.255.255.240
	Se0/0/0	209.165.202.2	255.255.255.252

Адреси SVI-інтерфейсів комутаторів наведені у таблиці 3.5.

Таблиця 3.5 – IP-адреси комутаторів в підмережах відділів

Підмережа	Пристрій	IP-адреса SVI інтерфейсу	Маска підмережі	Адреса шлюзу
LAN1	Sokolovskyi_Switch_0	10.23.61.2	255.255.255.128	10.23.61.1
	Sokolovskyi_Switch_1	10.23.61.3		
	Sokolovskyi_Switch_2	10.23.61.4		
LAN2	Sokolovskyi_Switch_3	10.23.61.130	255.255.255.128	10.23.61.129
	Sokolovskyi_Switch_4	10.23.61.131		
	Sokolovskyi_Switch_5	10.23.61.132		
	Sokolovskyi_Switch_6	10.23.61.133		
	Sokolovskyi_Switch_7	10.23.61.134		
LAN3	Sokolovskyi_Switch_8	10.23.62.2	255.255.255.128	10.23.62.1
	Sokolovskyi_Switch_9	10.23.62.3		
	Sokolovskyi_Switch_10	10.23.62.4		
	Sokolovskyi_Switch_11	10.23.62.5		
LAN4	Sokolovskyi_Switch_12	10.23.62.130	255.255.255.224	10.23.62.129
LAN5	Sokolovskyi_Switch_13	10.23.60.194	255.255.255.240	10.23.60.193
	Sokolovskyi_Switch_14	10.23.60.195		
	Sokolovskyi_Switch_15	10.23.60.196		
	Sokolovskyi_Switch_16	10.23.60.197		
	Sokolovskyi_Switch_17	10.23.60.198		

3.3 Розробка топологічної схеми корпоративної мережі

На рисунку 3.1 зображена топологічна схема корпоративної мережі. Топологічна схема складається з основної та віддаленої мережі, а також мережі провайдера. Мережа з’єднана між собою за допомогою кабелів SerialEthernet та GigabitEthernet.

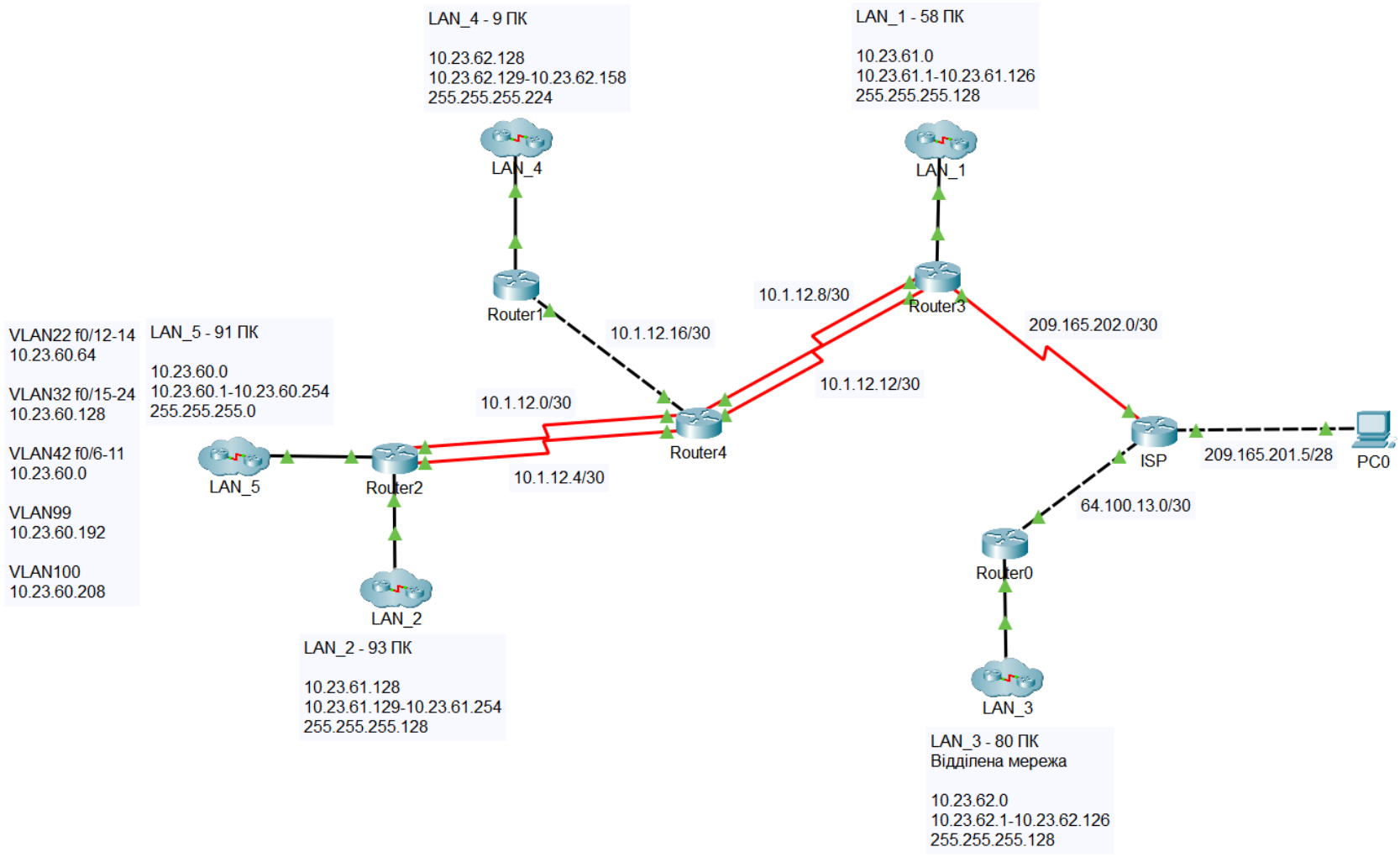

Рисунок 3.1 – Топологічна схема корпоративної мережі стоматологічної клініки «Amel Dental Clinic

3.4 Налаштування та перевірка роботи комп’ютерної Системи

3.4.1 Базове налаштування конфігурації пристроїв

Базове налаштування конфігурації пристроїв на прикладі Sokolovskyi_Router_4:

hostname Sokolovskyi_Router_4 // призначення назви пристрою

line console 0 // вхід в конфігураційний режим лінії консолі

password cisco // призначення паролю до консолі

login // вимикання анонімного доступу

line vty 0 15 // вхід в конфігураційний режим лінії VTY

password cisco // призначення паролю до лінії VTY

login // вимикання анонімного доступу

enable secret class // встановлення зашифрованого паролю для привілейного режиму

service password-encryption // шифрування паролів

banner motd #Sokolovskyi_Router_4# // налаштування банера MOTD

line vty 0 15 // вхід в конфігураційний режим лінії VTY

transport input ssh // назначення використання протоколу SSH

login local // налаштування локальної аутентифікації

username 123191_Sokolovskyi password admincisco // призначення імені користувача та паролю

ip domain-name Sokolovskyi_Router_4 // налаштування імені домена

crypto key generate rsa // створення ключа шфируваня

1024 // вибір довжини ключа шифрування

int se0/0/0 // вибір DCE-інтерефейсу

clock rate 128000 // встановлення значення тактової частоти

int se0/0/1

clock rate 128000

В LAN_1 використовується технологія Etherchannel, яка дозволяє об’днати декілька фізичних інтерфейсів мережевого пристрою в один логічний канал. Це дозволяє збільшити пропускну здатність та підвищити надійність каналів в мережі.

Налаштування Etherchannel на прикладі комутатора Sokolovskyi_Switch_1:

interface range fa0/1-2 // вибір інтерфейсів

channel-group 1 mode active // налаштування режиму портової групи

interface port-channel 1 // вибір інтерфейсу портової групи

switchport mode trunk // налаштування портової групи в режим транку

switchport trunk allowed vlan all // встановлення всіх VLAN як дозволених для проходженя даних через транковий порт

interface range fa0/3-4

channel-group 2 mode active

interface port-channel 2

switchport mode trunk

switchport trunk allowed vlan all

3.4.2 Налаштування маршрутизаторів корпоративної мережі

Для призначення адрес комп’ютерам в мережі буде використовуватись DHCP – мережевий протокол, який дозволяє автоматично призначати IP-адреси вузлам в підмережах. Це спрощує адміністрування мережі та налаштування пристроїв.

Налаштування DHCP на прикладі маршрутизатора Sokolovskyi_Router_1:

ip dhcp excluded-address 10.23.62.129 10.23.62.131 // виключення вказаних адрес з dhcp пулів

ip dhcp excluded-address 10.23.62.150

ip dhcp excluded-address 10.23.62.151

ip dhcp pool LAN-4 // створення та вказання адреси dhcp пулу

network 10.23.62.128 255.255.255.224 // вказання IP-адреси мережі

default-router 10.23.62.129 // вказання IP-адреси шлюзу

dns-server 10.23.62.151 // вказання IP-адреси dns сервера

Для того, щоб користувача різних підмереж могли взаємодіяти один з одним потрібно налаштувати маршрутизацію між мережами.

Існує два підходи до налаштування маршрутів в мережах: статична та динамічна. У випадку статичної маршрутизації маршрути вказуються вручну. При впровадженні динамічної маршрутизації маршрути оновлюються автоматично, що забезпечує більш гнучкий та автоматичний підхід до налаштування мережі.

В роботі буде використовуватись протокол динамічної маршрутизації OSPF, один з найпопулярніших протоколів в сучасних мережах. Він використовує алгоритм SPF, який вміє знаходити найкоротші маршрути, що робить мережу більш швидкою. Також серед переваг OSPF можна відмітити велику масштабованість, безпеку, підтримку VLSM та сумісність з обладнанням різних виробників.

Налаштування протоколу OSPF на прикладі маршрутизатора Sokolovskyi_Router_4:

router ospf 1 // увімкнення протоколу

network 10.1.12.0 0.0.0.3 area 0 // анонсування всіх необхідних для маршрутизації мереж

network 10.1.12.4 0.0.0.3 area 0

network 10.1.12.8 0.0.0.3 area 0

network 10.1.12.12 0.0.0.3 area 0

network 10.1.12.16 0.0.0.3 area 0

network 10.1.12.18 0.0.0.3 area 0

passive-interface default // відключення поширення оновлень за замовчуванням на всіх портах

no passive-interface Serial0/0/0 // увімкнення поширення оновлень на портах, через які будуть передаватись дані щодо підключених мереж

no passive-interface Serial0/0/1

no passive-interface Serial0/1/0

no passive-interface Serial0/1/1

no passive-interface GigabitEthernet0/0

На граничному маршрутизаторі Sokolovskyi_Router_3 налаштовуємо маршрут за замовчуванням до маршрутизатора ISP (інтернет-провайдер) і виконуємо його розповсюдження:

ip route 0.0.0.0 0.0.0.0 209.165.202.2 // налаштовуємо маршрут за замовчуванням

router ospf 1 // увімкнення протоколу

redistribute static subnets // увімкнення розповсюдження статичних маршрутів через протокол OSPF

Додаємо статичний маршрут до мережі провайдера ISP:

ip route 209.165.201.0 255.255.255.240 209.165.202.2

Налаштовуємо пропускну спроможність, тактову частоту на Serial-інтерфейсах та змінюємо еталонну пропускну спроможність для обчислення вартості за умовчанням для дозволу інтерфейсів Gigabit на значення 1000 на прикладі Sokolovskyi_Router_4:

int se0/0/0 // вибір інтерфейсу

bandwidth 128 // налаштування пропускної спроможності на рівні 128 Кб/с

delay 7500 // налаштування метрики

router ospf 1 // увімкнення протоколу

auto-cost reference-bandwidth 1000 // змінення еталонної пропускної спроможності для обчислення вартості за замовчуванням для дозволу інтерфейсів Gigabit

int se0/0/1

bandwidth 128

delay 7500

router ospf 1

auto-cost reference-bandwidth 1000

int se0/1/0

bandwidth 128

delay 7500

router ospf 1

auto-cost reference-bandwidth 1000

int se0/1/1

bandwidth 128

delay 7500

router ospf 1

auto-cost reference-bandwidth 1000

int GigabitEthernet0/0

router ospf 1

auto-cost reference-bandwidth 1000

3.4.3 Налаштування роботи Інтернет

Для того, щоб Система мала доступ до мережі Інтернет потрібно налаштувати NAT – технологію перетворення однієї або кількох внутрішніх IP-адрес на одну або кілька публічних IP-адрес і навпаки, а також перетворення номерів портів.

Пул адрес NAT: 209.165.202.5 – 209.165.202.30.

Переглянемо налаштування NAT на прикладі прикордонного маршрутизатора Sokolovskyi_Router_3:

ip access-list extended NAT12 // створення списку NAT12

deny ip 10.23.61.0 0.0.0.127 10.23.62.0 0.0.0.127 // заборона находження пакетів з віддаленої мережі до основної мережі

deny ip 10.23.62.128 0.0.0.31 10.23.62.0 0.0.0.127

deny ip 10.23.60.0 0.0.0.255 10.23.62.0 0.0.0.127

deny ip 10.23.61.128 0.0.0.127 10.23.62.0 0.0.0.127

deny ip 10.1.12.0 0.0.0.255 10.23.62.0 0.0.0.127

permit ip 10.23.61.0 0.0.0.127 any // дозвіл на надходження будь-яких пакетів з основної мережі

permit ip 10.23.62.128 0.0.0.31 any

permit ip 10.23.60.0 0.0.0.255 any

permit ip 10.23.61.128 0.0.0.127 any

permit ip 10.1.12.0 0.0.0.255 any

ip nat pool Internet 209.165.200.5 209.165.200.30 netmask 255.255.255.224 // створення пулу адрес

ip nat inside source list NAT12 pool Internet // прив'язка списку NAT16 до пулу Internet

ip nat inside source static 10.23.62.150 209.165.200.4 // призначення HTTP серверу IP-адреси NAT

ip nat inside source static 10.23.62.151 209.165.200.3 // призначення DNS серверу IP-адреси NAT

interface Serial0/0/0 // вибір інтерфейсу

ip nat inside // вказання інтерфейсу як внутрішнього

interface Serial0/0/1

ip nat inside

interface GigabitEthernet0/0

ip nat inside

interface Serial0/1/0

ip nat outside // вказання інтерфейсу як зовнішнього [4]

3.5 Захист інформації в комп'ютерній Системі

3.5.1 Налаштування маршрутизаторів на підтримку служби AAA

AAA – це модель, яка використовується для керування доступом та контролем мережевих ресурсів. AAA забезпечує авторизацію доступу та ідентифікацію користувачів.

Одним з компонентів AAA є RADIUS-сервер, який надає централізовану аутентифікацію та авторизацію користувачів, які намагаються отримати доступ до мережевих ресурсів через комутатори або маршрутизатори.

Налаштовуємо всі маршрутизаторів на підтримку служби AAA на прикладі Sokolovskyi_Router_1:

aaa new-model // увімкнення служби AAA

radius-server host 10.23.61.150 auth-port 1645 key radius123 // вказання IP-адреси RADIUS-серверу, порту підключення та ключа аутентифікації

aaa authentication login console group radius local // налаштування аутентифікації для консольного доступу до мережевого пристрою з використанням RADIUS-сервера

line console 0 // вхід в режим конфігурації лінії консолі

login authentication console // встановлення методу аутентифікації для доступу до консольного порту

aaa authentication login default local // створення локальної бази даних користувачів

username Sokolovskyi_Router_1 password admin123 // налаштування логіну та паролю у локальній базі

line vty 0 15 // вхід в режим конфігурації ліній віртуального терміналу

login authentication default // встановлення за замовчуванням методу аутентифікації для доступу через VTY-порти

3.5.2 Налаштування мереж VLAN, безпеки комутаторів та адресації ПК в мережах VLAN

Технологія VLAN використовується для того, щоб розділити одну фізичну мережу на декілька віртуальних підмереж. Використання VLAN дозволяє зменшити фізичне розташування пристроїв та кабелів, підвищити рівень безпеки та забезпечити кращий контроль трафіку.

Підмережа LAN_3 була розділена на три підмережі VLAN. Номери та назви VLAN мереж представлені в таблиці 3.6

Таблиця 3.6 – Мережі VLAN

Номер VLAN	Ім’я VLAN	Примітка
VLAN1	Default	Не використовується
VLAN42	Human_Resources_Department	Відділ кадрів
VLAN22	IT_Department	IT-відділ
VLAN32	Accounting_and_Marketing	Відділ маркетингу та бухгалтерія
VLAN99	Management	Для управління пристроями
VLAN100	Native	Власна

Таблиця схеми адресації підмереж VLAN представлена в таблиці 3.7.

Таблиця 3.7 – Схема адресації мереж VLAN

Назва	Розмір	Адреса	Маска	Діапазон адрес	Широкомовна адреса
VLAN42	62	10.23.60.0	255.255.255.192	10.23.60.1 - 10.23.60.62	10.23.60.63
VLAN22	62	10.23.60.64	255.255.255.192	10.23.60.65 - 10.23.60.126	10.23.60.127
VLAN32	62	10.23.60.128	255.255.255.192	10.23.60.129 - 10.23.60.190	10.23.60.191
VLAN99	14	10.23.60.192	255.255.255.240	10.23.60.193 - 10.23.60.206	10.23.60.207
VLAN100	14	10.23.60.208	255.255.255.240	10.23.60.209 - 10.23.60.222	10.23.60.223

Таблиця розподілу портів для окремих мереж VLAN представлена в таблиці 3.8.

Таблиця 3.8 – Розподіл портів для окремих мереж VLAN

Назва	VLAN	Розподіл портів
Human_Resources_Department	42	F0/6-11
IT_Department	22	F0/12-14
Accounting_and_Marketing	32	F0/15-24

Таблиця адресації пристроїв в LAN_5 представлена в таблиці 3.9.

Таблиця 3.9 – Адресація пристроїв в LAN_3

Пристрій	Інтерфейс	Адреса	Маска	Шлюз	VLAN
Switch13	SVI	10.23.60.194	255.255.255.240	10.23.60.193	99
Switch14	SVI	10.23.60.195	255.255.255.240	10.23.60.193	99
Switch15	SVI	10.23.60.196	255.255.255.240	10.23.60.193	99
Switch16	SVI	10.23.60.197	255.255.255.240	10.23.60.193	99
Switch17	SVI	10.23.60.198	255.255.255.240	10.23.60.193	99
Router0	G0/0.42	10.23.60.1	255.255.255.192	-	22
	G0/0.22	10.23.60.65	255.255.255.192	-	32
	G0/0.32	10.23.60.129	255.255.255.192	-	42
	G0/0.99	10.23.60.193	255.255.255.240	-	99

Налаштування VLAN на прикладі комутатора Sokolovskyi_Switch_13:

int range fa0/6-11 // вибір портів

switchport mode access // налаштування портів

switchport access vlan 42 // присвоювання портам влану

int range fa0/12-14

switchport mode access

switchport access vlan 22

int range fa0/15-24

switchport mode access

switchport access vlan 32

int range fa0/1-5

switchport mode trunk // налаштування портів в режим транку

switchport trunk native vlan 100 // налаштування власної мережі на транковому порті

switchport trunk allowed vlan 42,22,32,99-100 //налаштування списку дозволених VLAN на транковому порті

vlan 22 // вибір VLAN

name IT_Department // призначення назви вибраному VLAN

vlan 42

name Human_Resources_Department

vlan 32

name Accounting_and_Marketing

vlan 99

name Management

vlan 100

name Native [5]

Налаштування портів на комутаторах, привласнивши їм адреси з мережі Management VLAN, на прикладі комутатора Sokolovskyi_Switch_13:

int vlan 99 // вибір VLAN

ip address 10.23.60.194 255.255.255.240 // призначення IP-адреси

ip default-gateway 10.23.60.193 // вказання IP-адреси шлюзу за замовчуванням [5]

Налаштовуємо підінтерфейси на маршрутизаторі Sokolovskyi_Router2, що будуть виступати в ролі шлюзу для вказаних VLAN:

int g0/0.42 // вибір підінтерфейсу

encapsulation dot1Q 42 // встановлення мітки для вибраного порту

ip address 10.23.60.1 255.255.255.192 // вказання IP-адреси підінтерфейсу

int g0/0.22

encapsulation dot1Q 22

ip address 10.23.60.65 255.255.255.192

int g0/0.32

encapsulation dot1Q 32

ip address 10.23.60.129 255.255.255.192

int g0/0.99

encapsulation dot1Q 99

ip address 10.23.60.193 255.255.255.240 [5]

Для автоматичного призначення IP-адрес вузлам в різних VLAN буде використовуватись протокол DHCP. Налаштування DHCP на маршрутизаторі Sokolovskyi_Router_2, який буде виступати в ролі DHCP-сервера:

ip dhcp excluded-address 10.23.60.1 10.23.60.10 // виключення вказаних адрес з dhcp пулів

ip dhcp excluded-address 10.23.60.65 10.23.60.74

ip dhcp excluded-address 10.23.60.129 10.23.60.138

ip dhcp excluded-address 10.23.60.86

ip dhcp pool LAN5-VLAN42 // створення та вказання адреси dhcp пулу

network 10.23.60.0 255.255.255.192 // вказання IP-адреси мережі

default-router 10.23.60.1 // вказання IP-адреси шлюзу

dns-server 10.23.62.151 // вказання IP-адреси dns сервера

ip dhcp pool LAN5-VLAN22

network 10.23.60.64 255.255.255.192

default-router 10.23.60.65

dns-server 10.23.62.151

ip dhcp pool LAN5-VLAN32

network 10.23.60.128 255.255.255.192

default-router 10.23.60.129

dns-server 10.23.62.151 [5]

На порті комутатора Sokolovskyi_Switch_15, підключеного до сервера TFTP, налаштовуємо функцію безпеки:

int f0/14 // вибір необхідного порту

switchport mode access // налаштування режиму порту

switchport port-security // увімкнення захисту порту

switchport port-security maximum 2 // налаштування кількості унікальних пристроїв, яким дозволений доступ

switchport port-security mac-address sticky // налаштування автоматичного розпізнавання MAC-адресу та додавання його в поточну конфігурації

switchport port-security violation restrict // налаштування дії комутатора на випадок порушення безпеки

3.5.3 Налаштування віртуальної приватної мережі VPN

VPN – це технологія, яка використовується для забезпечення безпечного з’єднання в незахищених мережах, таких як Інтернет. В нашому випадку VPN буде використовуватись для підключення з віддаленої мережі до основної.

Налаштування VPN розглянемо на прикладі Sokolovskyi_Router_0:

license boot module c2900 technology-package securityk9 // активація модуля securityk9

ip access-list extended VPN12 // створення ACL-списку VPN12, щоб визначити трафік з основної мережі до віддаленої

permit ip 10.23.62.0 0.0.0.127 10.23.61.0 0.0.0.127 // надання доступу на проходження пакетів з основної на віддалену мережу

permit ip 10.23.62.0 0.0.0.127 10.23.62.128 0.0.0.31

permit ip 10.23.62.0 0.0.0.127 10.23.60.0 0.0.0.255

permit ip 10.23.62.0 0.0.0.127 10.23.61.128 0.0.0.127

permit ip 10.23.62.0 0.0.0.127 10.1.12.0 0.0.0.255 [6]

crypto isakmp policy 10 // створення криптографічної політики

encr 3des // вибір алгоритму шифрування

hash md5 // вибір алгоритму створення геш-суми

authentication pre-share // вибір методу аутентифікації пірів

group 2

crypto isakmp key cisco address 209.165.202.1 // створення ключа для взаємодії з обраним партнером

crypto ipsec transform-set TS esp-3des esp-md5-hmac // створення набору перетворень

crypto map MAP 10 ipsec-isakmp // створення криптографічного зіставлення

set peer 209.165.202.1 // створення піра

set transform-set TS // вибір набору перетворень

match address VPN12 // прив’язка до списку VPN12

int GigabitEthernet0/1 // вибір інтерфейсу

crypto map MAP // прив’язка криптографічного зіставлення MAP до вихідного інтерфейсу [7]

3.6 Перевірка комп’ютерної Системи підприємства

Перевіряємо базове налаштування пристроїв на прикладі маршрутизатора Sokolovskyi_Router_1. За допомогою команди do show running-config перевіряємо назву пристрою (рис. 3.2), призначення паролю до консолі (рис. 3.3) паролю до ліній vty та використання на них протоколу ssh (рис. 3.4), паролю до привілейованого режиму (рис. 3.5), банеру MOTD (рис. 3.6), імені та паролю користувача (рис. 3.7), імені домену (рис. 3.8).

```
!
hostname Sokolovskyi_Router_1
!
```

Рисунок 3.2 – Назва пристрою

```
!
line con 0
 password 7 0822455D0A16
 login authentication console
!
```

Рисунок 3.3 – Пароль до консолі

```
!
line vty 0 4
 password 7 0822455D0A16
 login authentication default
 transport input ssh
line vty 5 15
 password 7 0822455D0A16
 login authentication default
 transport input ssh
!
```

Рисунок 3.4 – Пароль до ліній vty та використання на них протоколу ssh

```
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
```

Рисунок 3.5 – Пароль до привілейованого режиму

```
!
banner motd ^CSokolovskyi_Router_1^C
!
```

Рисунок 3.6 – Банер MOTD

```
username Sokolovskyi_Router_1 password 7 082048430017544541
```

Рисунок 3.7 – Ім’я користувача та пароль

```
!
ip domain-name Sokolovskyi_Router_1
!
```

Рисунок 3.8 – Ім’я домена

Як бачимо, усі паролі зашифровані.

Перевіряємо тактову частоту на DCE-інтерфейсах маршрутизаторів (рис. 3.9) на прикладі маршрутизатора Sokolovskyi_Router_4 за допомогою команди do show controllers, попередньо зайшовши на необхідний інтерфейс за допомогою команди int serial0/0/0.

```
Sokolovskyi_Router_4(config-if)#do show controllers
Serial0/0/0
Interface Serial0/0/0
Hardware is PowerQUICC MPC860
DCE V.35, clock rate 128000
```

Рисунок 3.9 – Тактова частота на DCE-інтерфейсах маршрутизаторів

Перевіряємо технологію EtherChannel в LAN_1 на прикладі комутатора Sokolovskyi_Switch_0 (рис. 3.10).

```
Sokolovskyi_Switch_0(config)#do show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


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

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

1      Po1(SU)           LACP   Fa0/1(P) Fa0/2(P)
3      Po3(SU)           LACP   Fa0/3(P) Fa0/4(P)
```

Рисунок 3.10 – Технологія EtherChannel

Перевіряємо налаштування маршрутизаторів на прикладі маршрутизатора Sokolovskyi_Router_1. За допомогою команди do show ip protocols перевіряємо налаштування протоколу ospf та вказані маршрути (рис. 3.11).

```
Sokolovskyi_Router_4(config)#do show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 10.1.12.18
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.1.12.0 0.0.0.3 area 0
    10.1.12.4 0.0.0.3 area 0
    10.1.12.8 0.0.0.3 area 0
    10.1.12.12 0.0.0.3 area 0
    10.1.12.16 0.0.0.3 area 0
  Passive Interface(s):
    Vlan1
    GigabitEthernet0/1
    GigabitEthernet0/2
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.1.12.18           110      00:28:03
    10.23.61.129         110      00:28:43
    10.23.62.129         110      00:28:08
    209.165.202.1        110      00:28:41
  Distance: (default is 110)
```

Рисунок 3.11 – Налаштований OSPF

Як бачимо з рис. 3.12, зв’язок між різними підмережами на прикладі підмереж LAN_4 та LAN_2 є успішним.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Failed	PC12	PC4	ICMP		0.000	N	0	(edit)	
	Successful	PC12	PC4	ICMP		0.000	N	1	(edit)	

Рисунок 3.12 – Зв’язок між LAN_4 та LAN_2

Перевіряємо назначену пропускну спроможність на serial-інтерфейсах на прикладі маршрутизатора Sokolovskyi_Router_4 за допомогою команди do show interfaces serial0/0/0 (рис. 3.13).

```
Sokolovskyi_Router_4(config)#do show interfaces serial0/0/0
Serial0/0/0 is up, line protocol is up (connected)
  Hardware is HD64570
  Internet address is 10.1.12.1/30
  MTU 1500 bytes, BW 128 Kbit, DLY 75000 usec,
```

Рисунок 3.13 – Пропускна спроможність на serial-інтерфейсі

За допомогою команди show ip route static перевіряємо налаштування маршруту за замовчуванням на маршрутизаторі Sokolovskyi_Router_3 з прямим підключенням до інтернет-провайдера (рис. 3.14).

```
Sokolovskyi_Router_3(config)#do show ip route static
      209.165.201.0/28 is subnetted, 1 subnets
S        209.165.201.0 [1/0] via 209.165.202.2
S*    0.0.0.0/0 [1/0] via 209.165.202.2
```

Рисунок 3.14 – Налаштований маршрут за замовчуванням на маршрутизаторі Sokolovskyi_Router_3

Перевіряємо налаштування всіх маршрутизаторів на підтримку служби AAA на прикладі Sokolovskyi_Router_1. Як бачимо, при вході система запитує логін та пароль (рис. 3.15).

```
User Access Verification

Username: 123191_Sokolovskyi
Password:
Sokolovskyi_Router_1>en
Password:
Sokolovskyi_Router_1#conf t
Enter configuration commands, one p
Sokolovskyi_Router_1(config)#
```

Рисунок 3.15 – Налаштований маршрутизатор на підтримку служби AAA

Налаштування RADIUS-сервера показано на рис. 3.16.

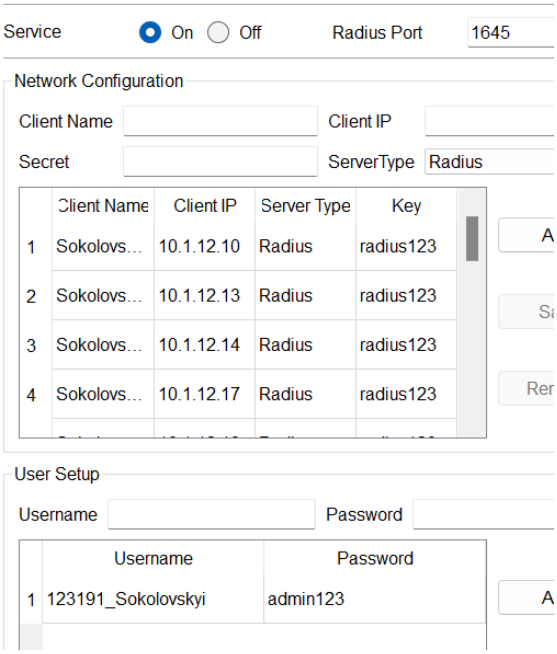

Рисунок 3.16 – Налаштування RADIUS-сервера

Налаштування DHCP перевіряємо на прикладі комп'ютера PC12, який знаходиться в LAN_4 (рис. 3.17).

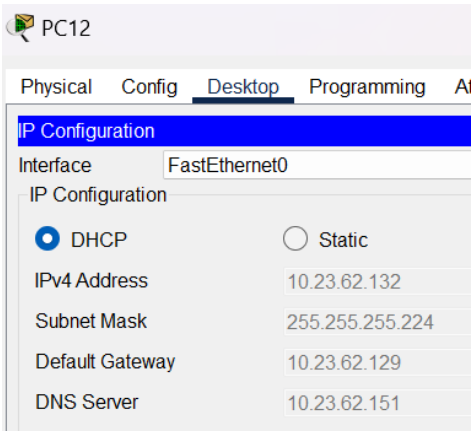

Рисунок 3.17 – IP-адреса PC12

Перевіряємо призначені статичні IP-адреси серверам DNS (рис. 3.18), HTTP (рис. 3.19) та TFTP (рис. 3.20).

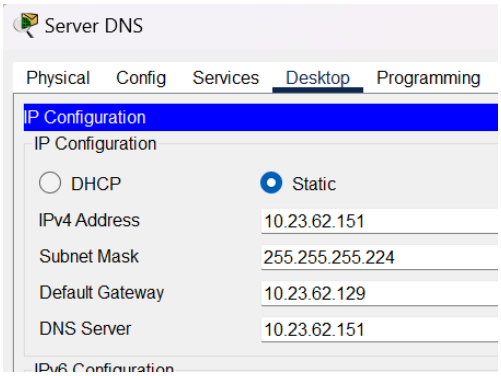

Рисунок 3.18 – IP-адреса DNS-сервера

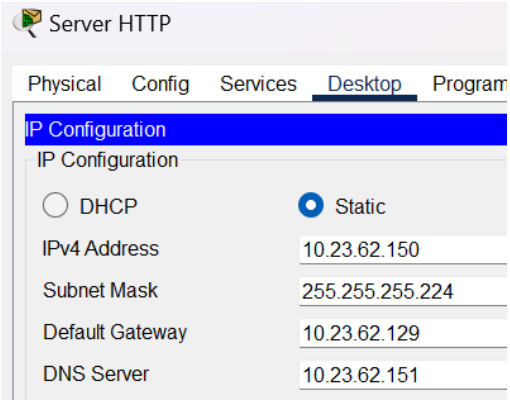

Рисунок 3.19 – IP-адреса HTTP-сервера

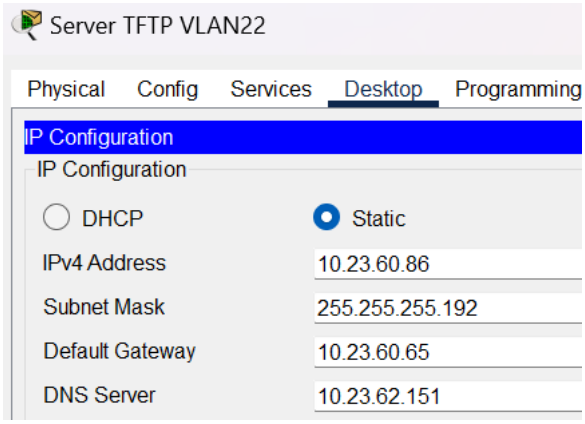

Рисунок 3.20 – IP-адреса TFTP-сервера

Перевіряємо призначені IP-адреси маршрутизаторам на прикладі маршрутизатора Sokolovskyi_Router_1 за допомогою команди do show ip interface brief (рис. 3.21).

```
Sokolovskyi_Router_1(config)#do show ip interface brief
Interface              IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0     10.1.12.17      YES manual up
up
GigabitEthernet0/1     10.23.62.129    YES manual up
up
GigabitEthernet0/2     unassigned      YES unset
administratively down down
Vlan1                  unassigned      YES unset
administratively down down
```

Рисунок 3.21 – IP-адреси маршрутизатора

Перевіряємо призначення IP-адреси SVI-інтерфейсам комутаторів на прикладі комутатора Sokolovskyi_Switch_3 за допомогою команди do show int vlan1 (рис. 3.22).

```
Sokolovskyi_Switch_3(config)#do show int vlan1
Vlan1 is up, line protocol is up
  Hardware is CPU Interface, address is 0001.c75e.4c93 (bia
0001.c75e.4c93)
  Internet address is 10.23.61.130/25
```

Рисунок 3.22 – IP-адреса комутатора

Перевіряємо налаштування безпеки порту комутатора Sokolovskyi_Switch_15, підключеного до TFTP-сервера, за допомогою команди do show port-security (рис. 3.23).

```
Sokolovskyi_Switch_15(config)#do show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation
Security Action
                (Count)       (Count)         (Count)
---------------------------------------------------------
-------
       Fa0/14         2           1                 0
Restrict
---------------------------------------------------------
---------
```

Рисунок 3.23 – Налаштована безпека порту комутатора, підключеного до TFTP-сервера

Перевіряємо призначені імена різним VLAN та порти, які належать кожному VLAN, на прикладі комутатора Sokolovskyi_Switch_16, за допомогою команди do show vlan (рис. 3.24).

```
Sokolovskyi_Switch_16(config)#do show vlan

VLAN Name                              Status    Ports
---- --------------------------------- ---------
--------------------------------
1    default                           active    Fa0/2, Fa0/3,
Fa0/4, Fa0/5
                                                 Gig0/1,
Gig0/2
22   IT_department                     active    Fa0/12,
Fa0/13, Fa0/14
32   Accounting_and_Marketing          active    Fa0/15,
Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19,
Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23,
Fa0/24
42   Human_Resources_Department        active    Fa0/6, Fa0/7,
Fa0/8, Fa0/9
                                                 Fa0/10,
Fa0/11
99   Management                        active
100  Native                            active
```

Рисунок 3.24 – Імена та порти VLAN

Перевіряємо транкові порти (рис. 3.25).

```
Sokolovskyi_Switch_16(config)#do show interfaces trunk
Port        Mode         Encapsulation  Status        Native
vlan
Fa0/1       on           802.1q         trunking      100

Port        Vlans allowed on trunk
Fa0/1       22,32,42,99-100

Port        Vlans allowed and active in management domain
Fa0/1       22,32,42,99,100

Port        Vlans in spanning tree forwarding state and not
pruned
Fa0/1       22,32,42,99,100
```

Рисунок 3.25 – Транкові порти

Перевіряємо налаштування DHCP для VLAN на прикладі PC22, який знаходиться в VLAN42 (рис. 3.26).

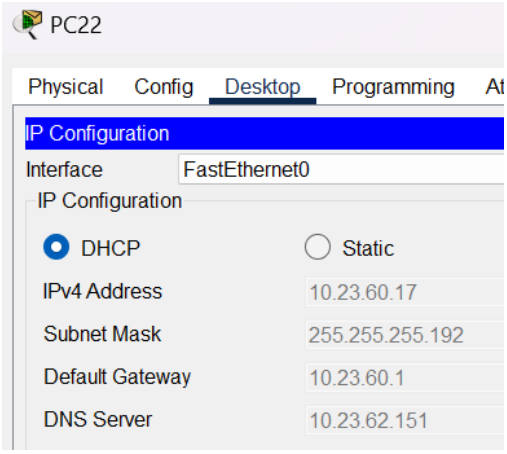

Рисунок 3.26 – IP-адреса PC22

Як бачимо з рис. 3.27, зв'язок між PC22(3) та PC22(5), які знаходять в VLAN42 та VLAN22 відповідно, є успішним.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Failed	PC22(3)	PC22(5)	ICMP		0.000	N	0	(edit)	
	Successful	PC22(3)	PC22(5)	ICMP		0.000	N	1	(edit)	

Рисунок 3.27 – Зв'язок між VLAN42 та VLAN22

Перевіряємо роботу NAT на маршрутизаторі Sokolovskyi_Router_3 за допомогою команди do show ip nat translations, застосувавши її після відправки пакету від ПК в LAN_1 до віддаленого ПК (рис. 3.28).

```
Sokolovskyi_Router_3(config)#do sh ip nat tran
Pro  Inside global     Inside local       Outside local
Outside global
icmp 209.165.200.5:1   10.23.61.59:1      209.165.201.5:1
209.165.201.5:1
icmp 209.165.200.5:2   10.23.61.59:2      209.165.201.5:2
209.165.201.5:2
---  209.165.200.3     10.23.62.151       ---
---
---  209.165.200.4     10.23.62.150       ---
---
```

Рисунок 3.28 – Робота NAT

Перевіряємо роботу VPN на маршрутизаторі Sokolovskyi_Router_0 за допомогою команди do show crypto ipsec sa, застосувавши її після відправки пакету від ПК в віддаленій LAN_3 до ПК в LAN_1 основної мережі (рис. 3.29).

```
Sokolovskyi_Router_0#sh crypto ipsec sa

interface: GigabitEthernet0/1
    Crypto map tag: MAP, local addr 64.100.13.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port):
(10.23.62.0/255.255.255.128/0/0)
   remote  ident (addr/mask/prot/port):
(10.23.61.0/255.255.255.128/0/0)
   current_peer 209.165.202.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 1, #pkts encrypt: 1, #pkts digest: 0
   #pkts decaps: 2, #pkts decrypt: 2, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 1, #recv errors 0

     local crypto endpt.: 64.100.13.1, remote crypto endpt.:
209.165.202.1
     path mtu 1500, ip mtu 1500, ip mtu idb
GigabitEthernet0/1
     current outbound spi: 0xACA05EB8(2896191160)
```

Рисунок 3.29 – Робота VPN

Перевіряємо відкриття веб-сайту з відомостями про тему та завдання на кваліфікаційну роботу студента на прикладі PC0 (рис. 3.30).

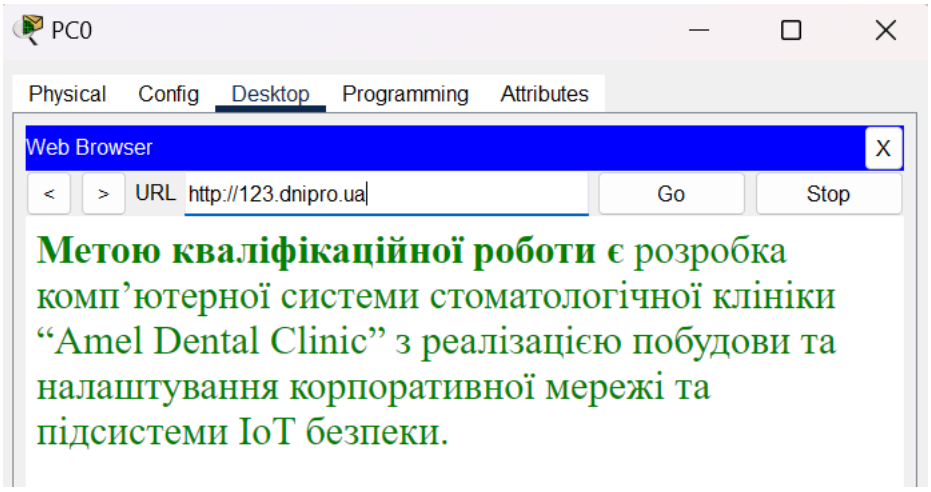

Рисунок 3.30 – Відкритий веб-сайт з відомостями про тему та завдання на кваліфікаційну роботу студента

4 РОЗРОБКА КОМПОНЕНТА СИСТЕМИ

4.1 Інженерне рішення по розробці компонента Системи

Інтернет речей – це мережа фізичних пристроїв, які мають підключення до Інтернету та можуть взаємодіяти один з один. Зазвичай система Інтернету речей складається з датчиків, які постійно відстежують показники зовнішнього середовища, та пристроїв, які вмикаються або вимикаються в залежності від показників датчиків та умов, заданих користувачем. Завдяки цьому можна автоматизувати різні процеси, такі як увімкнення або вимикання освітлення, регулювання температури, вологості та багато іншого. [8]

Система Інтернету речей складається з датчиків вогню, руху та зчитувача ID-картки. Серед пристроїв в системі існує сирена, веб-камера та двері.

Зв’язок між пристроями організований за допомогою шлюзу для розумного будинку HomeGateway, на якому прописані умови спрацювання пристроїв в залежності від показників датчиків, такі як:

1. При фіксуванні вогню, вмикається сирена.
2. При фіксації руху, вмикається веб-камера.
3. При вдалому зчитуванні ID-картки, відчиняються двері.

З’єднання пристроїв та датчиків зі шлюзом HomeGateway відбувається за допомогою технології Wi-Fi, яка базується на стандарті IEEE 802.11. Для управління IoT-пристроями використовується смартфон, підключений до шлюзу.

Система Інтернету речей впроваджена в основній та віддаленій мережі.

В основній мережі впроваджено 4 датчики вогню для кожної підмережі та 1 датчик для технічного приміщення. Датчики вогню, руху, зчитувач ID-картки та пристрої, такі як веб-камера та двері впроваджено тільки для технічного приміщення. Сирена використовується одна для основної мережі. Також додано шлюз та смартфон.

У віддаленій мережі впроваджено датчик вогню та сирена, а також додано шлюз та смартфон.

4.2 Налаштування обладнання та сервісів системи IoT

Для створення IoT-системи безпеки клініки спочатку встановлюємо IoT-пристрої, датчики, смартфон та під’єднуємо все до HomeGateway.

На HomeGateway основної мережі налаштовуємо бездтротову точку доступу з SSID Sokolovskyi з паролем 123191_Sokolovskyi протоколу безпеки WPA2-PSK, який використовує метод шифрування AES. На HomeGateway_1 віддаленої мережі налаштовуємо бездтротову точку доступу з SSID Sokolovskyi2 та паролем 123191_Sokolovskyi2.

На кожному IoT-пристрої налаштовуємо підключення до Home Gateway, ввівши SSID та пароль. В якості IoT-сервера вибираємо Home Gateway.

Топологічна схема корпоративної мережі клініки з розміщенням IoT-пристроїв показана на рис. 4

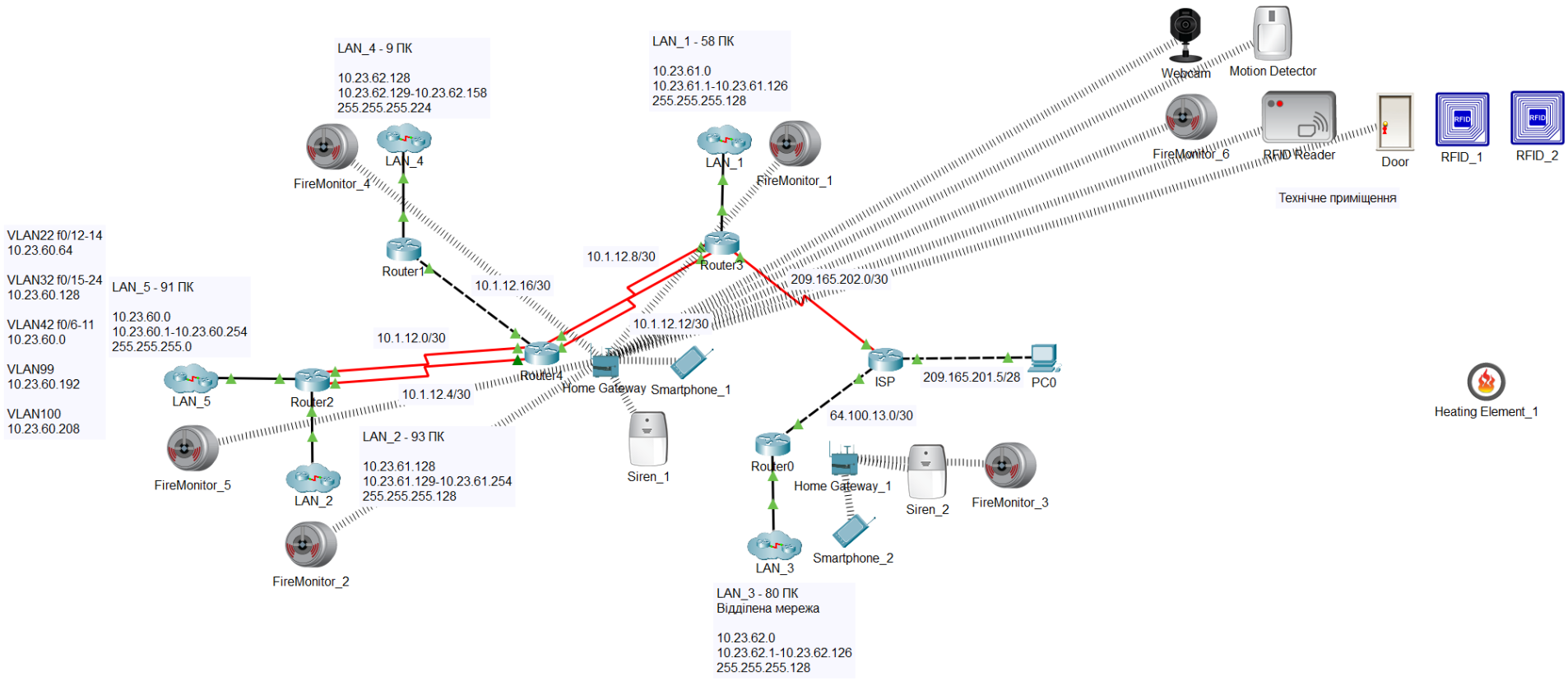

Рисунок 4.1 – Топологічна схема корпоративної мережі стоматологічної клініки «Amel Dental Clinic» з розміщенням IoT-пристроїв

Для налаштування умов роботи IoT-системи в смартфоні відкриваємо IoT Monitor, вводимо адресу шлюзу та логін з паролем. Після цього відкривається сторінка з усіма підключеними IoT-пристроями, яка показана на рис. 4.2.

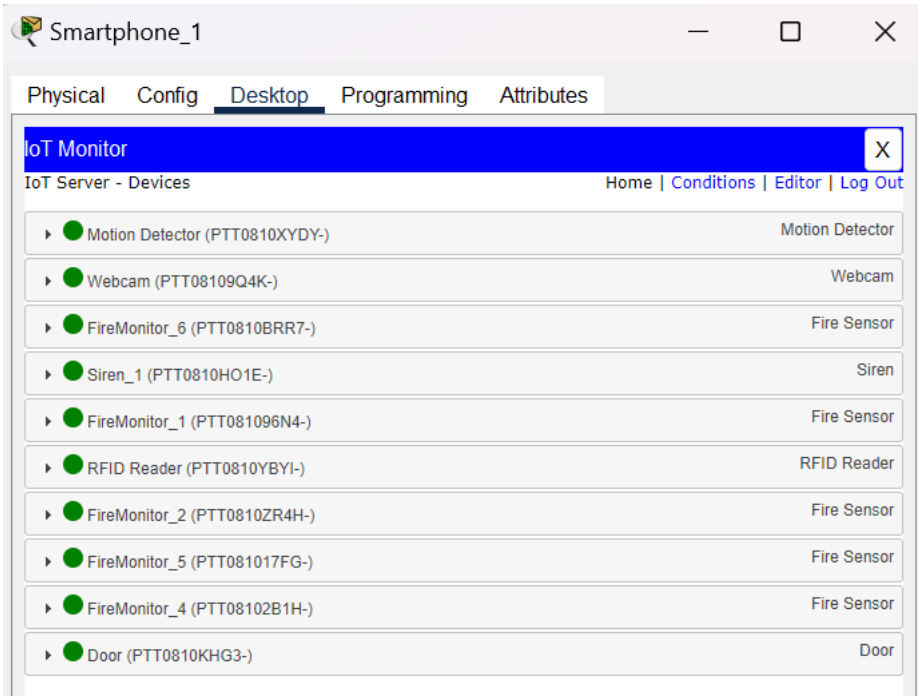

Рисунок 4.2 – Під’єднані IoT-пристрої основної мережі

Заходимо на вкладку «Conditions» та натискаємо «Add» для додавання умов спрацювання пристроїв.

Для спрацювання сирени потрібна умова фіксації вогню відповідним датчиком. Цей сценарій показано на рис. 4.3.

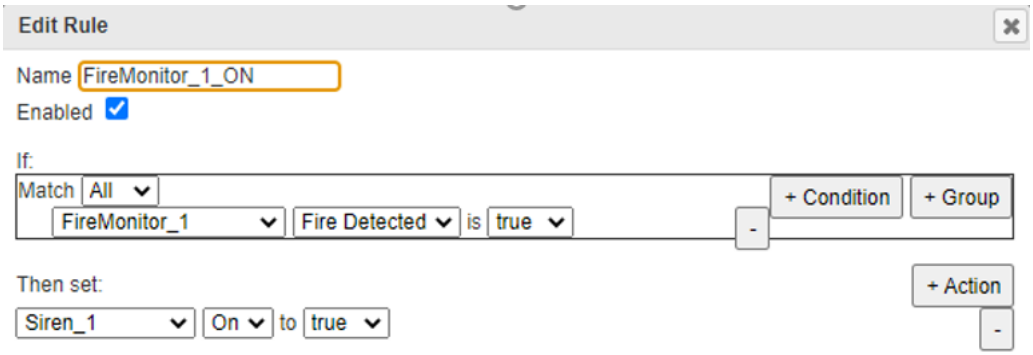

Рисунок 4.3 – Сценарій спрацювання сирени

Також додаємо сценарій для того випадку, коли датчик не фіксує вогонь, який показано на рис. 4.4.

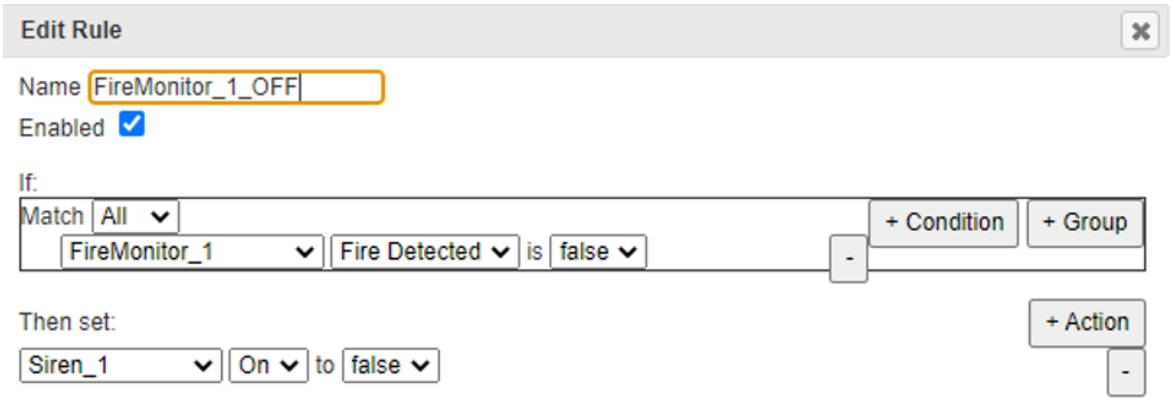

Рисунок 4.4 – Сценарій не спрацювання сирени

Такі ж самі дії виконуємо і для віддаленої мережі.

Для того, щоб працювала веб-камера повинна бути виконана умова спрацювання датчику руху. Цей сценарій показано на рис. 4.5.

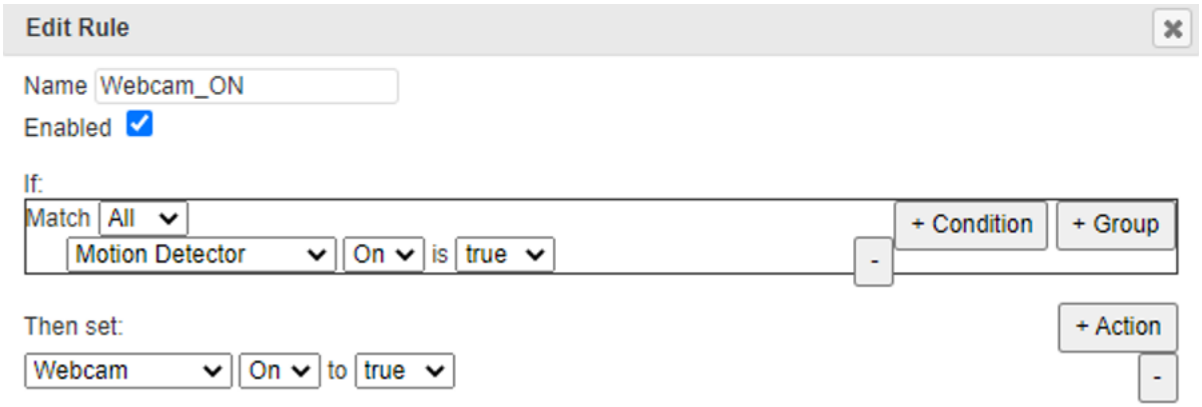

Рисунок 4.5 – Сценарій спрацювання веб-камери

Якщо рух не зафіксовано відповідним датчиком, то веб-камера не працює. Цей сценарій показано на рис. 4.6.

Рисунок 4.6 – Сценарій не спрацювання веб-камери

Для того, щоб зчитувач ID-картки підтвердив правильність картки, її ID повинен бути 1001. В іншому випадку зчитувач не підтверджує правильність картки. Сценарії для цього показано на рис.4.7 та 4.8 відповідно.

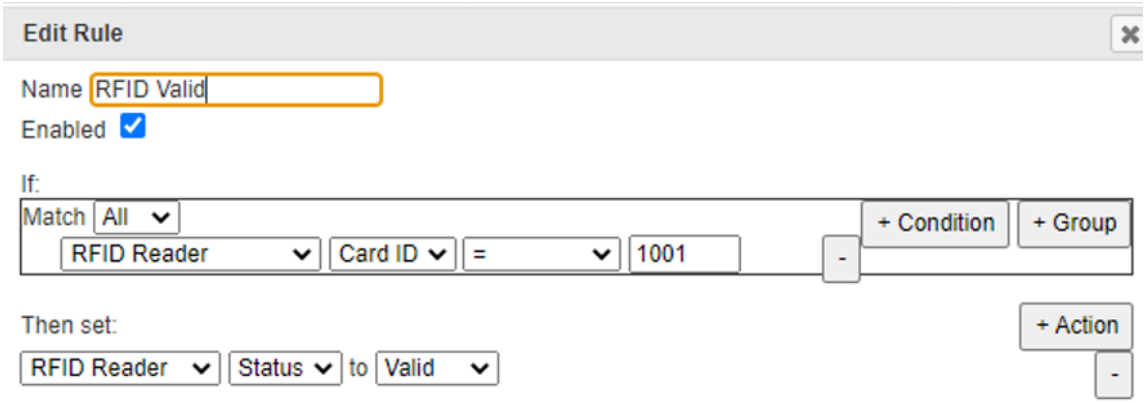

Рисунок 4.7 – Сценарій підтвердження картки

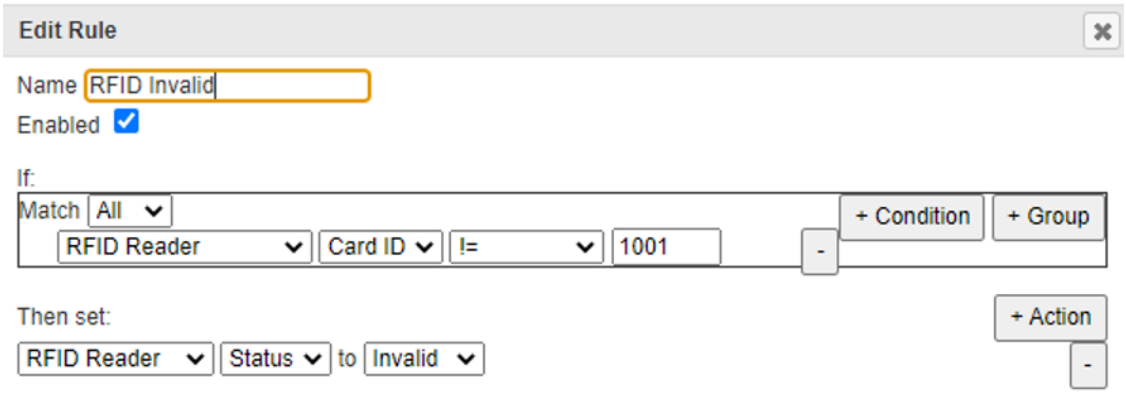

Рисунок 4.8 – Сценарій не підтвердження картки

Якщо зчитувач ID-картки підтвердив правильність картки, двері відчиняються. В іншому випадку двері залишаються зачиненими. Сценарії для цього показано на рис.4.9 та 4.10 відповідно.

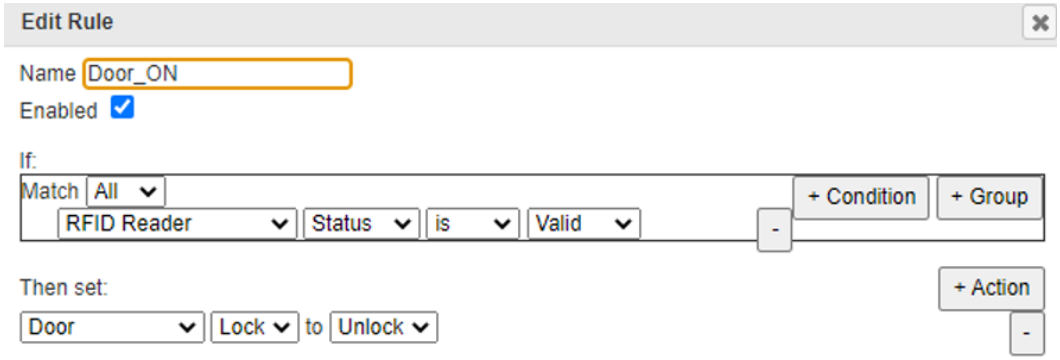

Рисунок 4.9 – Сценарій відкриття двері

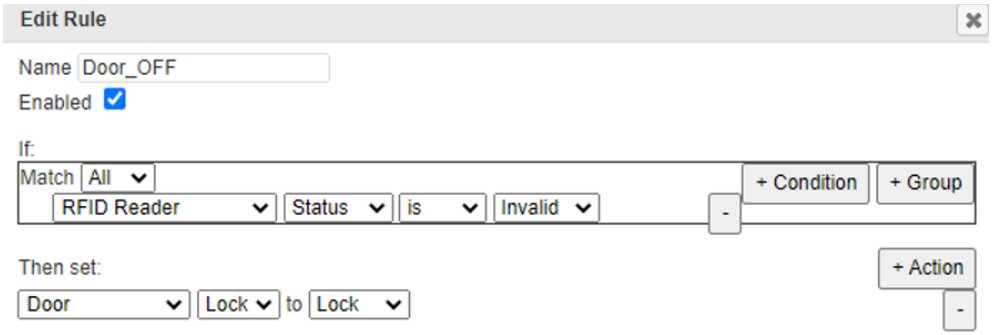

Рисунок 4.10 – Сценарій зачиненої двері

4.3 Перевірка роботи компонента Системи

Для перевірки працездатності зчитувача ID-картки було додано картки з ID 1001 та 1002 для спрацювання та не спрацювання зчитувача відповідно.

Також було додано нагріваючий елемент, на якому прописали скрипт мовою програмування Javascript для імітації вогню. Завдяки цьому можна перевіряти спрацювання сирени.

Для написання скрипту заходимо до налаштувань нагріваючого елементу, натискаємо «Advanced», а потім «Programming». Створюємо новий проект з ім’ям Fire, натиснувши «New». Пишемо скрипт та натискаємо Run. Скрипт мовою Javascript:

```
function setup (){
setDeviceProperty(getName(), 'IR', 900);
}
```

Перевіряємо роботу сирени, перемістивши вогонь близько до датчику вогню (рис. 4.11).

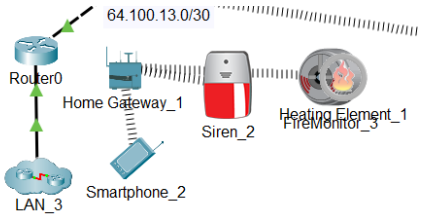

Рисунок 4.11 – Робота сирени

Перевіряємо роботу зчитувача ID-картки та двері, піднісши картку з ID 1001 (рис. 4.12) та 1002 (рис. 4.13).

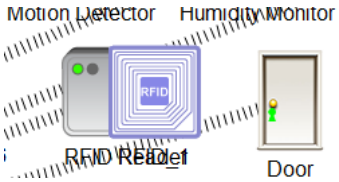

Рисунок 4.12 – Двері відчинені

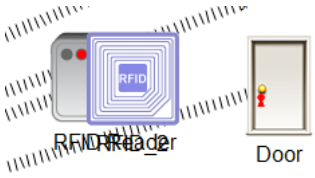

Рисунок 4.13 – Двері зачинені

Перевіряємо роботу веб-камери при фіксуванні руху (рис. 4.14)

Рисунок 4.14 – Веб-камера працює

ВИСНОВКИ

В даній кваліфікаційній роботі була розроблена та налаштована корпоративна мережа стоматологічної клініки “Amel Dental Clinic”. Також було реалізовано компонент Системи у вигляді IoT-системи безпеки.

Був проведений ретельний огляд об’єкту та прописано вимоги до комп’ютерної Системи. Згідно цих вимог було підібрано необхідно обладнання та побудовано комп’ютерну мережу у середовищі Cisco Packet Tracer.

Згідно завдання була розрахована адресація підмереж та було призначено IP-адресу кожному пристрою. Були налаштовані різні технології, такі як EtherChannel для об’єднання фізичних портів в один логічний задля більшої надійності та пропускної здатності мережі, DHCP для автоматичного призначення IP-адреси пристроям, VLAN для розділення мережі на віртуальні підмережі, NAT для можливості виходу в Інтернет, VPN для безпечного віддаленого підключення, AAA для авторизації доступу. Для проходження трафіку між різними підмережами було налаштовано протокол динамічної маршрутизації OSPF. Також було виконано базову конфігурацію всіх пристроїв та налаштовано функції безпеку порту комутатора, підключеного до сервера TFTP. Крім сервера TFTP, було налаштовано сервер HTTP та DNS, завдяки чому кожен користувач може заходити на веб-сайт з відомостями про тему та завдання на кваліфікаційну роботу студента як за IP-адресою, так і за доменним ім’ям.

Після створення основної мережі, було розроблено та налаштовано компонент Системи у вигляді системи безпеки клініки, створеної за допомогою технології Інтернету речей.

В кінці роботи було проведено тестування окремих компонентів Системи та роботи Системи в цілому.

Кваліфікаційна робота виконана в повній відповідності до теми і поставлених завдань. Оформлення роботи відповідає всім нормативним вимогам та рекомендаціям, встановленим методичним керівництвом.

ПЕРЕЛІК ПОСИЛАНЬ

1. Сайт стоматологічної клініки “Amel Dental Clinic” – Education [Електронний ресурс] – Режим доступу до ресурсу: https://ameldental.com/uk/ (дата звернення 15.05.2023р.)

2. Структура управління організацією. Лекція з навчальної дисципліни «Менеджмент організацій» Для студентів спеціальності 073 «Менеджмент» / Павленчик А. О. – Львівський державний університет фізичної культури імені Івана Боберського, 2020. – 16 с

3. Методичні рекомендації до виконання кваліфікаційної роботи бакалавра студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп’ютерна інженерія / Л.І. Цвіркун, С.М. Ткаченко, Я.В. Панферова, Д.О. Бешта, Л.В. Бешта. – Д.: НТУ «ДП», 2022. – 62 с.

4. Налаштування NAT – Education [Електронний ресурс] – Режим доступу до ресурсу: http://surl.li/hsyzr (дата звернення 20.05.2023р.)

5. Налаштування VLAN – Education [Електронний ресурс] – Режим доступу до ресурсу: http://surl.li/hrjwk (дата звернення 23.05.2023р.)

6. ACL списки – Education [Електронний ресурс] – Режим доступу до ресурсу: http://surl.li/hszbq (дата звернення 26.05.2023р.)

7. Налаштування VPN – Education [Електронний ресурс] – Режим доступу до ресурсу: http://surl.li/hrjwr (дата звернення 26.05.2023р.)

8. Інтернет речей – Education [Електронний ресурс] – Режим доступу до ресурсу: http://surl.li/dcsqu (дата звернення 31.05.2023р.)

Додаток А

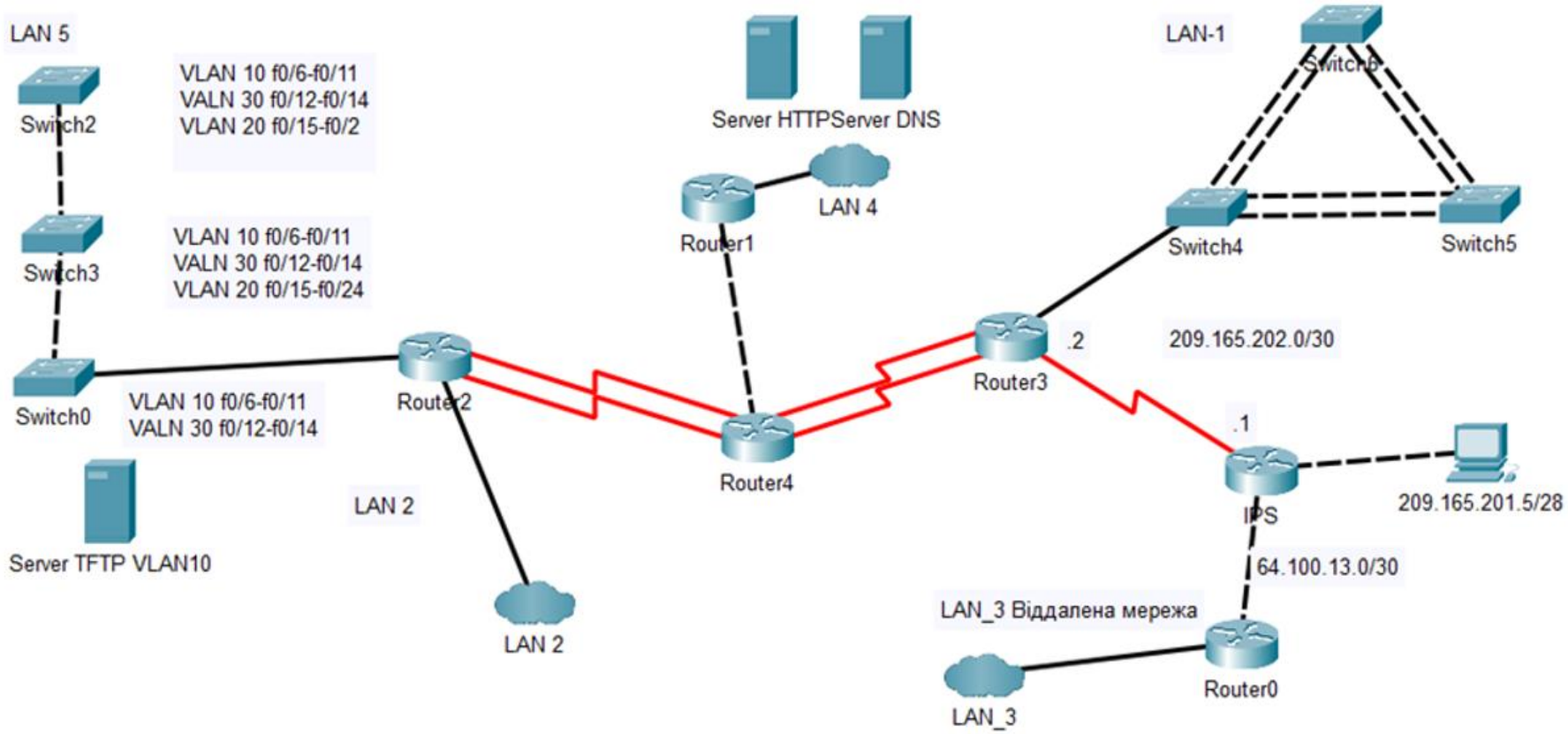

Рисунок ДА.1 – Загальна архітектура мережі клініки

Додаток Б

Текст програми налаштування комп’ютерної мережі клініки

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

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Текст програми

804.02070743.23012-01 12 01

Листів 21

2023

АНОТАЦІЯ

Дана програма містить в собі команди для налаштування маршрутизаторів та комутаторів корпоративної мережі.

Команди призначені для налаштування IP-адрес, базового налаштування пристроїв, налаштування DHCP, NAT, VPN, AAA, OSPF, VLAN, статичних маршрутів, EtherChannel та безпеки портів.

ЗМІСТ

1. Sokolovskyi_Router_0

```
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
// Шифрування паролів
service password-encryption
!
// Ім’я пристрою
hostname Sokolovskyi_Router_0
!
// Пароль до привілейованого режиму
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
// Налаштування DHCP
ip dhcp excluded-address 10.23.62.1 10.23.62.6
!
ip dhcp pool LAN-3
network 10.23.62.0 255.255.255.128
default-router 10.23.62.1
dns-server 209.165.200.3
!
// Налаштування AAA
aaa new-model
!
aaa authentication login console group radius local
aaa authentication login default local
!
ip cef
no ipv6 cef
!
// Ім’я користувача та пароль
username 123191_Sokolovskyi password 7 082048430017061E010803
username Sokolovskyi_Router_0 password 7 082048430017544541
!
// Налаштування VPN
license udi pid CISCO2911/K9 sn FTX1524WW2V-
license boot module c2900 technology-package securityk9
!
crypto isakmp policy 10
encr 3des
hash md5
authentication pre-share
group 2
```

```
!
crypto isakmp key cisco address 209.165.202.1
!
crypto ipsec transform-set TS esp-3des esp-md5-hmac
!
crypto map MAP 10 ipsec-isakmp
set peer 209.165.202.1
set transform-set TS
match address VPN12
!
// Доменне ім’я
ip domain-name Sokolovskyi_Router_0
!
spanning-tree mode pvst
!
// Налаштування інтерфейсів
interface GigabitEthernet0/0
ip address 10.23.62.1 255.255.255.128
ip nat inside
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 64.100.13.1 255.255.255.252
ip nat outside
duplex auto
speed auto
crypto map MAP
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Vlan1
no ip address
shutdown
!
// Налаштування статичних маршрутів
ip nat pool Internet 209.165.205.5 209.165.205.30 netmask 255.255.255.224
ip nat inside source list NAT12 pool Internet
ip classless
```

```
ip route 0.0.0.0 0.0.0.0 64.100.13.2
ip route 209.165.201.0 255.255.255.240 64.100.13.2
ip route 64.100.13.0 255.255.255.252 GigabitEthernet0/1
!
ip flow-export version 9
!
// Налаштування ACL списку для VPN
ip access-list extended VPN12
permit ip 10.23.62.0 0.0.0.127 10.23.61.0 0.0.0.127
permit ip 10.23.62.0 0.0.0.127 10.23.62.128 0.0.0.31
permit ip 10.23.62.0 0.0.0.127 10.23.60.0 0.0.0.255
permit ip 10.23.62.0 0.0.0.127 10.23.61.128 0.0.0.127
permit ip 10.23.62.0 0.0.0.127 10.1.12.0 0.0.0.255
// Налаштування ACL списку для NAT
ip access-list extended NAT12
deny ip 10.23.62.0 0.0.0.127 10.23.61.0 0.0.0.127
deny ip 10.23.62.0 0.0.0.127 10.23.62.128 0.0.0.31
deny ip 10.23.62.0 0.0.0.127 10.23.60.0 0.0.0.255
deny ip 10.23.62.0 0.0.0.127 10.23.61.128 0.0.0.127
deny ip 10.23.62.0 0.0.0.127 10.1.12.0 0.0.0.255
permit ip 10.23.62.0 0.0.0.127 any
!
no cdp run
!
// Банер MOTD
banner motd ^CSokolovskyi_Router_0^C
!
// Адреса та порт RADIUS-сервера
radius server 10.23.62.151
address ipv4 10.23.62.151 auth-port 1645
key radius123
!
// Пароль до лінії консолі
line con 0
password 7 0822455D0A16
login authentication console
!
line aux 0
!
// Пароль до ліній vty та використання ssh
line vty 0 4
password 7 0822455D0A16
login authentication default
```

```
transport input ssh
line vty 5 15
password 7 0822455D0A16
login authentication default
transport input ssh
!
end
```

2. Sokolovskyi_Router_2

```
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
// Шифрування паролів
service password-encryption
!
// Ім’я пристрою
hostname Sokolovskyi_Router_2
!
// Пароль до привілейованого режиму
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
// Налаштування DHCP
ip dhcp excluded-address 10.23.61.129 10.23.61.135
ip dhcp excluded-address 10.23.60.1 10.23.60.10
ip dhcp excluded-address 10.23.60.65 10.23.60.74
ip dhcp excluded-address 10.23.60.129 10.23.60.138
ip dhcp excluded-address 10.23.60.86
!
ip dhcp pool LAN-2
network 10.23.61.128 255.255.255.128
default-router 10.23.61.129
dns-server 10.23.62.151
ip dhcp pool LAN5-VLAN42
network 10.23.60.0 255.255.255.192
default-router 10.23.60.1
dns-server 10.23.62.151
ip dhcp pool LAN5-VLAN22
network 10.23.60.64 255.255.255.192
default-router 10.23.60.65
dns-server 10.23.62.151
ip dhcp pool LAN5-VLAN32
network 10.23.60.128 255.255.255.192
default-router 10.23.60.129
```

```
dns-server 10.23.62.151
!
// Налаштування AAA
aaa new-model
!
aaa authentication login console group radius local
aaa authentication login default local
!
no ip cef
no ipv6 cef
!
// Ім’я користувача та пароль
username 123191_Sokolovskyi password 7 082048430017061E010803
username Sokolovskyi_Router_2 password 7 082048430017544541
!
license udi pid CISCO2911/K9 sn FTX15249UGZ-
!
// Доменне ім’я
ip domain-name Sokolovskyi_Router_2
!
spanning-tree mode pvst
!
// Налаштування інтерфейсів
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
!
interface GigabitEthernet0/0.22
encapsulation dot1Q 22
ip address 10.23.60.65 255.255.255.192
!
interface GigabitEthernet0/0.32
encapsulation dot1Q 32
ip address 10.23.60.129 255.255.255.192
!
interface GigabitEthernet0/0.42
encapsulation dot1Q 42
ip address 10.23.60.1 255.255.255.192
!
interface GigabitEthernet0/0.99
encapsulation dot1Q 99
ip address 10.23.60.193 255.255.255.240
```

```
!
interface GigabitEthernet0/1
ip address 10.23.61.129 255.255.255.128
duplex auto
speed auto
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/0/0
bandwidth 128
ip address 10.1.12.2 255.255.255.252
delay 7500
!
interface Serial0/0/1
bandwidth 128
ip address 10.1.12.6 255.255.255.252
delay 7500
!
interface Vlan1
no ip address
shutdown
!
// Налаштування OSPF
router ospf 1
log-adjacency-changes
passive-interface default
no passive-interface Serial0/0/0
no passive-interface Serial0/0/1
auto-cost reference-bandwidth 1000
network 10.23.61.128 0.0.0.127 area 0
network 10.1.12.0 0.0.0.3 area 0
network 10.1.12.4 0.0.0.3 area 0
network 10.23.60.0 0.0.0.255 area 0
!
ip classless
!
ip flow-export version 9
!
no cdp run
```

```
!
// Банер MOTD
banner motd ^CSokolovskyi_Router_2^C
!
// Адреса та порт RADIUS-сервера
radius server 10.23.62.151
address ipv4 10.23.62.151 auth-port 1645
key radius123
!
// Пароль до лінії консолі
line con 0
password 7 0822455D0A16
login authentication console
!
line aux 0
!
// Пароль до ліній vty та використання ssh
line vty 0 4
password 7 0822455D0A16
login authentication default
transport input ssh
line vty 5 15
password 7 0822455D0A16
login authentication default
transport input ssh
!
end
```

3. Sokolovskyi_Router_3

```
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
// Шифрування паролів
service password-encryption
!
// Ім’я пристрою
hostname Sokolovskyi_Router_3
!
// Пароль до привілейованого режиму
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
// Налаштування DHCP
ip dhcp excluded-address 10.23.61.1 10.23.61.5
```

```
!
ip dhcp pool LAN-1
network 10.23.61.0 255.255.255.128
default-router 10.23.61.1
dns-server 10.23.62.151
!
// Налаштування AAA
aaa new-model
!
aaa authentication login console group radius local
aaa authentication login default local
!
no ip cef
no ipv6 cef
!
// Ім’я користувача та пароль
username 123191_Sokolovskyi password 7 082048430017061E010803
username Sokolovskyi_Router_3 password 7 082048430017544541
!
// Налаштування VPN
license udi pid CISCO2911/K9 sn FTX152493C3-
license boot module c2900 technology-package securityk9
!
crypto isakmp policy 10
encr 3des
hash md5
authentication pre-share
group 2
!
crypto isakmp key cisco address 64.100.13.1
!
crypto ipsec transform-set TS esp-3des esp-md5-hmac
!
crypto map MAP 10 ipsec-isakmp
set peer 64.100.13.1
set transform-set TS
match address VPN12
!
// Доменне ім’я
ip domain-name Sokolovskyi_Router_3
!
spanning-tree mode pvst
!
```

```
// Налаштування інтерфейсів
interface GigabitEthernet0/0
ip address 10.23.61.1 255.255.255.128
ip nat inside
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/0/0
bandwidth 128
ip address 10.1.12.9 255.255.255.252
delay 7500
ip nat inside
clock rate 128000
!
interface Serial0/0/1
bandwidth 128
ip address 10.1.12.13 255.255.255.252
delay 7500
ip nat inside
clock rate 128000
!
interface Serial0/1/0
bandwidth 128
ip address 209.165.202.1 255.255.255.252
delay 7500
ip nat outside
crypto map MAP
!
interface Serial0/1/1
no ip address
clock rate 2000000
```

```
shutdown
!
interface Vlan1
no ip address
shutdown
!
// Налаштування OSPF
router ospf 1
log-adjacency-changes
redistribute static subnets
passive-interface default
no passive-interface Serial0/0/0
no passive-interface Serial0/0/1
auto-cost reference-bandwidth 1000
network 10.1.12.8 0.0.0.3 area 0
network 10.1.12.12 0.0.0.3 area 0
network 10.23.12.12 0.0.0.3 area 0
network 10.23.61.0 0.0.0.127 area 0
default-information originate
!
// Налаштування статичних маршрутів
ip nat pool Internet 209.165.200.5 209.165.200.30 netmask 255.255.255.224
ip nat inside source list NAT12 pool Internet
ip nat inside source static 10.23.62.150 209.165.200.4
ip nat inside source static 10.23.62.151 209.165.200.3
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.202.2
ip route 209.165.201.0 255.255.255.240 209.165.202.2
ip route 209.165.202.0 255.255.255.252 Serial0/1/0
!
ip flow-export version 9
!
// Налаштування ACL списку для VPN
ip access-list extended VPN12
permit ip 10.23.61.0 0.0.0.127 10.23.62.0 0.0.0.127
permit ip 10.23.62.128 0.0.0.31 10.23.62.0 0.0.0.127
permit ip 10.23.60.0 0.0.0.255 10.23.62.0 0.0.0.127
permit ip 10.23.61.128 0.0.0.127 10.23.62.0 0.0.0.127
permit ip 10.1.12.0 0.0.0.255 10.23.62.0 0.0.0.127
// Налаштування ACL списку для NAT
ip access-list extended NAT12
deny ip 10.23.61.0 0.0.0.127 10.23.62.0 0.0.0.127
deny ip 10.23.62.128 0.0.0.31 10.23.62.0 0.0.0.127
```

```
deny ip 10.23.60.0 0.0.0.255 10.23.62.0 0.0.0.127
deny ip 10.23.61.128 0.0.0.127 10.23.62.0 0.0.0.127
deny ip 10.1.12.0 0.0.0.255 10.23.62.0 0.0.0.127
permit ip 10.23.61.0 0.0.0.127 any
permit ip 10.23.62.128 0.0.0.31 any
permit ip 10.23.60.0 0.0.0.255 any
permit ip 10.23.61.128 0.0.0.127 any
permit ip 10.1.12.0 0.0.0.255 any
!
no cdp run
!
// Банер MOTD
banner motd ^CSokolovskyi_Router_3^C
!
// Адреса та порт RADIUS-сервера
radius server 10.23.62.151
address ipv4 10.23.62.151 auth-port 1645
key radius123
!
// Пароль до лінії консолі
line con 0
password 7 0822455D0A16
login authentication console
!
line aux 0
!
// Пароль до ліній vty та використання ssh
line vty 0 4
password 7 0822455D0A16
login authentication default
transport input ssh
line vty 5 15
password 7 0822455D0A16
login authentication default
transport input ssh
!
end
```

4. Sokolovskyi_Switch_0

```
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
// Шифрування паролів
```

```
service password-encryption
!
// Ім’я пристрою
hostname Sokolovskyi_Switch_0
!
// Пароль до привілейованого режиму
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
// Доменне ім’я
ip domain-name Sokolovskyi_Switch_0
!
// Ім’я користувача та пароль
username 123191_Sokolovskyi privilege 1 password 7
082048430017061E010803
!
spanning-tree mode pvst
spanning-tree extend system-id
!
// Налаштування EtherChannel на інтерфейсах
interface Port-channel1
switchport mode trunk
!
interface Port-channel3
switchport mode trunk
!
interface FastEthernet0/1
switchport mode trunk
channel-group 1 mode active
!
interface FastEthernet0/2
switchport mode trunk
channel-group 1 mode active
!
interface FastEthernet0/3
switchport mode trunk
channel-group 3 mode active
!
interface FastEthernet0/4
switchport mode trunk
channel-group 3 mode active
!
// Налаштування інших інтерфейсів
interface FastEthernet0/5
```

```
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
// Адреса SVI-інтерфейса
```

```
!
interface Vlan1
ip address 10.23.61.2 255.255.255.128
!
// Банер MOTD
banner motd ^CSokolovskyi_Switch_0^C
!
// Пароль до лінії консолі
line con 0
password 7 0822455D0A16
login
!
// Пароль до ліній vty та використання ssh
line vty 0 4
password 7 0822455D0A16
login local
transport input ssh
line vty 5 15
password 7 0822455D0A16
login local
transport input ssh
!
end
```

5. Sokolovskyi_Switch_15

```
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
// Шифрування паролів
service password-encryption
!
// Ім’я пристрою
hostname Sokolovskyi_Switch_15
!
// Пароль до привілейованого режиму
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
// Доменне ім’я
ip domain-name Sokolovskyi_Switch_15
!
// Ім’я користувача та пароль
username 123191_Sokolovskyi privilege 1 password 7
082048430017061E010803
```

```
!
spanning-tree mode pvst
spanning-tree extend system-id
!
// Налаштування інтерфейсів vlan
interface FastEthernet0/1
switchport trunk native vlan 100
switchport trunk allowed vlan 22,32,42,99-100
switchport mode trunk
!
interface FastEthernet0/2
switchport trunk native vlan 100
switchport trunk allowed vlan 22,32,42,99-100
switchport mode trunk
!
interface FastEthernet0/3
switchport trunk native vlan 100
switchport trunk allowed vlan 22,32,42,99-100
switchport mode trunk
!
interface FastEthernet0/4
switchport trunk native vlan 100
switchport trunk allowed vlan 22,32,42,99-100
switchport mode trunk
!
interface FastEthernet0/5
switchport trunk native vlan 100
switchport trunk allowed vlan 22,32,42,99-100
switchport mode trunk
!
interface FastEthernet0/6
switchport access vlan 42
switchport mode access
!
interface FastEthernet0/7
switchport access vlan 42
switchport mode access
!
interface FastEthernet0/8
switchport access vlan 42
switchport mode access
!
interface FastEthernet0/9
```

```
switchport access vlan 42
switchport mode access
!
interface FastEthernet0/10
switchport access vlan 42
switchport mode access
!
interface FastEthernet0/11
switchport access vlan 42
switchport mode access
!
interface FastEthernet0/12
switchport access vlan 22
switchport mode access
!
interface FastEthernet0/13
switchport access vlan 22
switchport mode access
!
// Налаштування інтерфейсу vlan з безпекою
interface FastEthernet0/14
switchport access vlan 22
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
switchport port-security mac-address sticky 0005.5E6A.AC01
!
// Налаштування інтерфейсів vlan
interface FastEthernet0/15
switchport access vlan 32
switchport mode access
!
interface FastEthernet0/16
switchport access vlan 32
switchport mode access
!
interface FastEthernet0/17
switchport access vlan 32
switchport mode access
!
interface FastEthernet0/18
```

```
switchport access vlan 32
switchport mode access
!
interface FastEthernet0/19
switchport access vlan 32
switchport mode access
!
interface FastEthernet0/20
switchport access vlan 32
switchport mode access
!
interface FastEthernet0/21
switchport access vlan 32
switchport mode access
!
interface FastEthernet0/22
switchport access vlan 32
switchport mode access
!
interface FastEthernet0/23
switchport access vlan 32
switchport mode access
!
interface FastEthernet0/24
switchport access vlan 32
switchport mode access
!
interface GigabitEthernet0/1
switchport trunk native vlan 100
switchport trunk allowed vlan 22,32,42,99-100
switchport mode trunk
!
// Налаштування інших інтерфейсів
interface GigabitEthernet0/2
!
// Адреса SVI-інтерфейса
interface Vlan1
no ip address
shutdown
!
// Налаштування vlan99
interface Vlan99
ip address 10.23.60.196 255.255.255.240
```

```
!
ip default-gateway 10.23.60.193
!
// Банер MOTD
banner motd ^CSokolovskyi_Switch_15^C
!
// Пароль до лінії консолі
line con 0
password 7 0822455D0A16
login
!
// Пароль до ліній vty та використання ssh
line vty 0 4
password 7 0822455D0A16
login local
transport input ssh
line vty 5 15
password 7 0822455D0A16
login local
transport input ssh
!
end
```