

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Сумський державний університет
Факультет електроніки та інформаційних технологій
Кафедра електроніки, загальної та прикладної фізики

«До захисту допущено»

Завідувачка кафедри

_____ Лариса ОДНОДВОРЕЦЬ

_____ 2024 р.

КВАЛІФІКАЦІЙНА РОБОТА
на здобуття освітнього ступеня «магістр»

за спеціальністю 171 «Електроніка» освітньо-наукової програми «Електронні інформаційні системи»

на тему: Електронні властивості цифрової розумної мережі на базі Cisco Systems

Здобувача групи ЕП.м-21н Павленка Андрія Анатолійовича

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

_____ Андрій ПАВЛЕНКО

Керівник, ст. викладач кафедри ЕЗПФ,
канд. фіз.-мат. наук

_____ Олександр ПИЛИПЕНКО

Суми – 2024

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
Факультет електроніки та інформаційних технологій
Кафедра електроніки, загальної та прикладної фізики
Спеціальність 171 «Електроніка», освітньо-наукова програма
«Електронні інформаційні системи»

ЗАТВЕРДЖУЮ

Зав. кафедри ЕЗПФ

Л.В.Одноворець

«01» травня 2024 року

**ІНДИВІДУАЛЬНЕ ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ МАГІСТРА**

Павленка Андрія Анатолійовича

1. Тема роботи: **«ЕЛЕКТРОННІ ВЛАСТИВОСТІ ЦИФРОВОЇ РОЗУМНОЇ МЕРЕЖІ НА БАЗІ CISCO SYSTEMS»**

затверджена наказом СумДУ від «16» квітня 2024 р., № 0394-VI

2. Термін здачі здобувачем закінченої роботи: 16 травня 2024 року

3. Вихідні дані до роботи (актуальність, мета): Розробка інтелектуальної мережі для офісного середовища, використовуючи технології та обладнання від Cisco Systems. Актуальність теми розробки розумної мережі для офісного середовища полягає в тому, що сучасні офіси потребують більш ефективних, безпечних і гнучких рішень для підтримки своєї діяльності. З розвитком технологій, зростає кількість пристроїв, які підключаються до мережі, що створює додаткові виклики для їх інтеграції.

4. Зміст текстової частини роботи (перелік питань, які необхідно розробити):

1. Аналіз проблеми предметної області, постановка й формування завдань дослідження.

2. Огляд технологій, що використовуються розробки розумних мереж.

3. Розробка інтелектуальної електронної мережі для офісного середовища.

4. Аналіз отриманих результатів.

5. Перелік графічного матеріалу для презентації:

Слайд №1-2. Актуальність і мета роботи.

Слайд №3-4. Маршрутизація даних.

Слайд №5-6. Електронні пристрої та сенсори, що забезпечують «розумні» функції.

Слайд №7-14. Цифрова модель розумної мережі для офісного середовища.

Слайд №15. Висновки.

Слайд №16. Подяка.

6. Дата видачі індивідуального завдання: 01.05.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ пор.	Назва етапів виконання кваліфікаційної роботи	Термін виконання етапів роботи	Примітка про стан виконання роботи
1	Аналіз літературних даних	до 04.05.2024 р.	<i>вик.</i>
2	Проведення експерименту, моделювання, розрахунків, обробка результатів	до 14.05.2023 р.	<i>вик.</i>
3	Оформлення тексту кваліфікаційної роботи	до 16.05.2023 р.	<i>вик.</i>
4	Попередній захист роботи	17.05.2024 р., онлайн	<i>вик.</i>
5	Захист кваліфікаційної роботи	21.05.2024 р., 11- 40 онлайн	

Здобувач вищої освіти

Павленко А.А.

Керівник

Пилипенко О.В.

АНОТАЦІЯ

Кваліфікаційна робота викладена на 42 сторінках, зокрема, містить 35 рисунків, 1 додатку, список використаних джерел складається з 15 найменувань.

Актуальність теми розробки розумної мережі для офісного середовища полягає в тому, що сучасні офіси потребують більш ефективних, безпечних і гнучких рішень для підтримки своєї діяльності. З розвитком технологій, зростає кількість пристроїв, які підключаються до мережі, що створює додаткові виклики для їх інтеграції. Розумні мережі, які використовують передові технології та обладнання, такі як рішення від Cisco Systems, дозволяють створити інфраструктуру, яка автоматично адаптується до потреб користувачів і ситуацій. Це включає автоматизацію рутинних завдань, оптимізацію використання ресурсів і забезпечення високого рівня комфорту. Крім того, розумні мережі можуть легко масштабуватися, що дозволяє офісам рости і змінюватися без значних перебудов інфраструктури.

Мета кваліфікаційної роботи магістра полягає в розробці інтелектуальної мережі для офісного середовища, використовуючи технології та обладнання від Cisco Systems.

Під час виконання роботи використовували метод розробки цифрової моделі розумної мережі в програмному середовищі Cisco Packet Tracer.

У результаті проведених наукових досліджень була розроблена модель інтелектуальної мережі для офісного середовища, використовуючи технології та обладнання від Cisco Systems. Ця робота сприяла поглибленню знань у галузі розробки мережевої архітектури, зокрема, щодо застосування сучасних технологій для створення розумних мереж.

Отримані результати можна використати для вдосконалення мережевих рішень та підвищення ефективності роботи офісних середовищ.

Ключові слова: Інтернет речей, маршрутизація даних, розумна мережа, автоматизація, Cisco Packet Tracer, Cisco Systems.

ЗМІСТ

	С.
ВСТУП	6
РОЗДІЛ 1 ІНФОРМАЦІЙНО-АНАЛІТИЧНИЙ ОГЛЯД ПРЕДМЕТНОЇ ОБЛАСТІ	7
1.1. Маршрутизація даних та керування мережевим трафіком	7
1.2. Технології та архітектура побудови інтелектуальних мереж для офісного середовища.....	11
1.3. Застосування розумних мереж у різних сферах життєдіяльності.....	14
РОЗДІЛ 2 ПОСТАНОВКА ЗАВДАННЯ ТА ВИБІР МЕТОДІВ РІШЕННЯ	16
2.1. Розробка інтелектуальної мережі	16
2.2. Програмне забезпечення для моделювання розумної мережі	17
РОЗДІЛ 3 МОДЕЛЮВАННЯ РОЗУМНОЇ МЕРЕЖІ ДЛЯ ОФІСНОГО СЕРЕДОВИЩА	19
3.1. Конфігурація компонентів.....	19
3.2. Взаємодія компонентів розумної мережі	27
ВИСНОВКИ	37
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	38
ДОДАТКИ	40

ВСТУП

В умовах стрімкого технологічного прогресу сучасні мережі виявляють себе не лише як засіб обміну даними між комп'ютерами, але й як універсальне середовище для інтеграції різноманітних електронних інформаційних систем та пристроїв.

Останні декілька десятиліть характеризуються стрімким розвитком електронних технологій, що спричинило появу нових типів інтелектуальних пристроїв. Актуальним стає питання ефективної інтеграції таких пристроїв в єдину інформаційну мережу з метою забезпечення безперервного та безпечного обміну даними між ними.

Зростаюча потреба в інтеграції таких пристроїв з мережами зв'язку спонукає розробників до пошуку ефективних рішень для забезпечення безперервного обміну даними. Застосування технологій та протоколів глобальної мережі інтернет стає невід'ємною частиною цього процесу, дозволяючи створити єдине інформаційне середовище для взаємодії між пристроями.

Сучасні інтернет-технології, зокрема, забезпечують можливість інтеграції інтелектуальних пристроїв у мережу завдяки дотриманню концептуальної моделі систем зв'язку OSI. Це дозволяє створювати масштабовані та гнучкі мережеві рішення, здатні підтримувати високий рівень інтеграції інтелектуальних пристроїв.

Серед провідних розробників мережевих технологій і пристроїв виділяється Cisco Systems, яка відзначається своїми передовими розробками та інноваціями у цій сфері. У даній науковій роботі буде розглянуто процес розробки інтелектуальної мережі для офісного середовища з використанням технологій та обладнання від Cisco Systems, з метою дослідження їх потенціалу та можливостей для покращення ефективності та функціональності офісних процесів.

РОЗДІЛ 1 ІНФОРМАЦІЙНО-АНАЛІТИЧНИЙ ОГЛЯД ПРЕДМЕТНОЇ ОБЛАСТІ

1.1. Маршрутизація даних та керування мережевим трафіком

Маршрутизація даних в мережі зазвичай включає досить складну сукупність алгоритмів, які працюють незалежно, але підтримують один одного шляхом обміну інформацією. Складність алгоритмів маршрутизації обумовлена низкою причин. По-перше, маршрутизація вимагає координації між усіма вузлами підмережі, а не лише парою модулів, як, наприклад, у протоколах транспортного рівня моделі OSI. По-друге, система маршрутизації повинна справлятися зі збоями каналів і вузлів, що вимагає перенаправлення трафіку та оновлення баз даних, які підтримує система. По-третє, щоб досягти високої продуктивності, алгоритму маршрутизації може знадобитися змінити свої маршрути, коли деякі області в мережі стають перевантаженими.

Основні функції, які виконує алгоритм маршрутизації — це вибір маршрутів для різних пар «відправник-призначення» та доставка повідомлень до правильного пункту призначення після вибору маршрутів. Функція вибору маршрутів є концептуально простою і полягає у використанні різноманітних протоколів маршрутизації і структур даних, відомих як таблиці маршрутизації.

Є два основних параметри продуктивності, на які суттєво впливає алгоритм маршрутизації: пропускна здатність і середня затримка пакетів. Маршрутизація взаємодіє з керуванням потоком у визначенні цих показників продуктивності за допомогою механізму зворотного зв'язку, показаного на рисунку 1.1. Коли навантаження трафіку, яке пропонують зовнішні сайти для підмережі, є відносно низьким, він буде повністю прийнятий у мережу. Коли запропонований трафік надмірний, частина буде відхилена алгоритмом керування потоком.

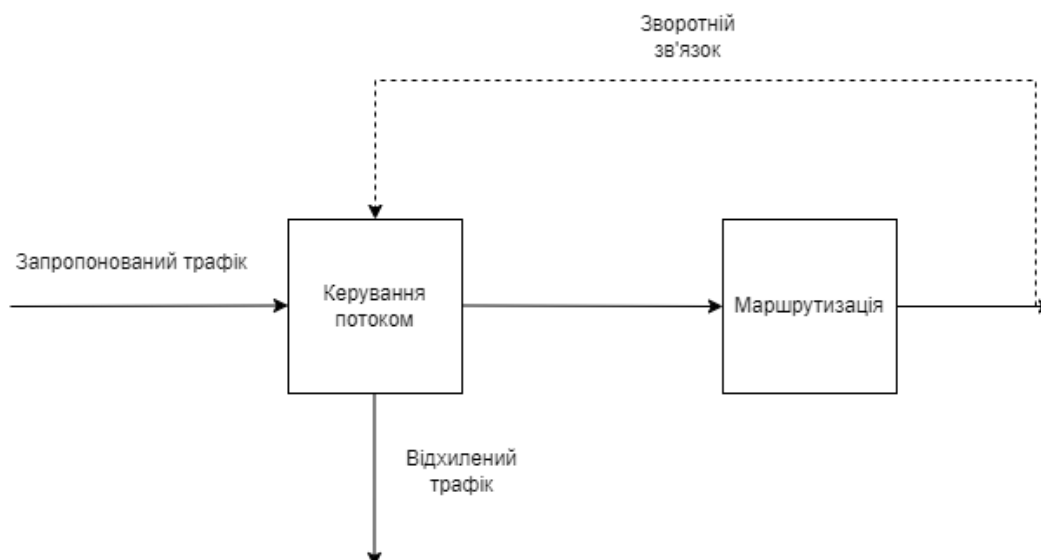


Рисунок 1.1 – Взаємодія керування маршрутизацією та потоком [1]

Трафік, який приймається в мережу, матиме середню затримку на пакет, яка залежить від маршрутів, вибраних алгоритмом маршрутизації. Однак на пропускну здатність значно впливає саме алгоритм маршрутизації, оскільки типові схеми керування потоком працюють на основі досягнення балансу між пропускну здатністю та затримкою, тобто вони починають відхиляти трафік, коли затримка починає ставати надмірною. Таким чином алгоритм маршрутизації має забезпечувати низьку затримку, а алгоритм керування потоком відповідає за пропускну здатність.

Маршрутизатори та багаторівневі комутатори зв'язують підмережі разом і використовують IP-адреси для визначення місць призначення пакетів даних отриманих від хостів, які знаходяться в безпосередньо під'єднаних мережах, і від імені хостів, які можуть бути розташовані на відстані багатьох маршрутизаторів або переходів [1].

Маршрутизатори додають IP-маршрути до своїх таблиць маршрутизації за допомогою трьох методів: безпосередньо підключених маршрутів, статичних маршрутів і маршрутів, отриманих за допомогою протоколів динамічної маршрутизації. Таблиця маршрутизації зберігає інформацію лише про наступний крок на шляху пакету даних до призначення або наступний маршрутизатор на шляху до місця призначення.

Протоколи маршрутизації виконують такі загальні функції [2]:

1. Отримують інформацію про IP-підмережі від сусідніх маршрутизаторів.
2. Передають інформацію про маршрути до IP-підмереж сусіднім маршрутизаторам.
3. Якщо існує більше ніж один можливий маршрут для досягнення однієї підмережі, обирають найкращий маршрут на основі метрик.
4. Якщо топологія мережі змінюється, наприклад через збій зв'язку, протоколи маршрутизації реагують на зміни, повідомляючи, що деякі маршрути вийшли з ладу і необхідно вибрати новий маршрут.

Протоколи маршрутизації поділяються на протоколи зовнішньої маршрутизації і внутрішньої маршрутизації [3]. Протоколи зовнішньої маршрутизації використовуються для маршрутизації між автономними системами, наприклад маршрутизація, що відбувається в межах глобальної мережі інтернет. Прикладами таких протоколів є Border Gateway Protocol (BGP) і на даний час застарілий Exterior Gateway Protocol (EGP).

Протоколи внутрішньої маршрутизації призначені для використання в межах автономної системи. Їх можна класифікувати на основі методу, яким вони визначають найкращий маршрут для передачі даних: протоколи векторної дистанції та протоколи стану зв'язку. Ці два типи відрізняються в основному метрикою, яка використовується керування маршрутизацією пакетів даних.

Протоколи векторної дистанції використовують дуже просту метрику під назвою кількість переходів. Кількість переходів описує кількість маршрутизаторів між джерелом і пунктом призначення, які використовують цей маршрутизатор. На рисунку 1.2 якби маршрутизатор Router0 отримав пакет від PC0, призначений для PC2, він мав би доступні два маршрути: через Router1 або Router2. Маршрут через Router1 мав би складатися з двох переходів, а маршрут через Router2 мав би бути одним переходом. У випадку використання протоколу векторної дистанції, було б обрано маршрут через Router2.

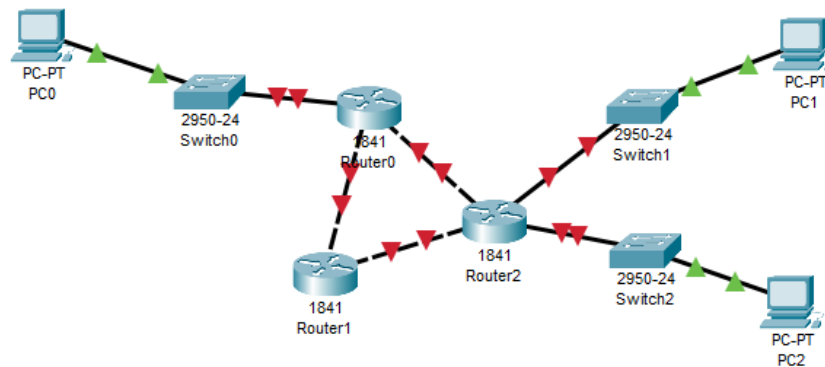


Рисунок 1.2 – Вибір маршруту протоколом векторної дистанції [3]

Прикладами протоколів векторної дистанції є RIP (Routing Information Protocol), IGRP (Interior Gateway Routing Protocol), EIGRP (Enhanced Interior Gateway Routing Protocol).

Протоколи стану зв'язку використовують комбінацію факторів під час визначення найкращого маршруту. Вони звичайно враховують кількість переходів, але вони також враховують пропускну здатність залучених маршрутів і затримку, про яку повідомляє трафік який був надісланий у певному напрямку. Потім ця інформація обробляється алгоритмом, який генерує числове значення для використання як показник стану зв'язку та для побудови повної карти мережі. На основі цієї карти кожен маршрутизатор самостійно визначає найкращі маршрути за допомогою алгоритму Дейкстри. Такими протоколами є OSPF (Open Shortest Path First) та IS-IS (Intermediate System to Intermediate System).

Застосування пристроїв і систем керування мережевим трафіком є необхідним для забезпечення стабільності, безпеки та ефективності електронних інформаційних систем. Одними з ключових елементів мережевої інфраструктури, що відповідають за ці задачі, є маршрутизатори, комутатори, міжмереві екрани, проксі-сервери та мережеві контролери. Ці пристрої разом формують основу для керування потоками даних у мережах різних масштабів та конфігурацій.

1.2. Технології та архітектура побудови інтелектуальних мереж для офісного середовища

Інтелектуальна мережа для офісного середовища являє собою програмно-апаратний комплекс для автоматичного керування системами та пристроями, який дозволяє об'єднати всю інженерну складову підприємства в єдину систему управління. Основна мета інтелектуальних технологій – збирати дані з навколишнього середовища та допомагати користувачам у повсякденній діяльності. Застосування інтелектуальних технологій у виробництві розглядається з точки зору автоматизації робочих процесів та переваг, які це може принести завдяки зниженню операційних витрат, людських помилок, що, як наслідок, підвищує продуктивність [4].

Концепція, яка охоплює підключення електронних пристроїв до мережі з метою збору та обміну даними називається інтернет речей. Інтернет речей (ІоТ) — це взаємозв'язок обчислювальних пристроїв і фізичних об'єктів з унікальними ідентифікаторами, датчиками та можливістю обробки та обміну даними. Вважається, що це одна з найбільш новаторських технологічних розробок останнього часу [5].

Сучасні технології ІоТ надають можливість обмінюватися інформацією в різних обсягах і на різних відстанях: від кількох метрів до десятків кілометрів. Оскільки потреба в передачі інформації різного обсягу та параметрів якості обслуговування зростає, потреба в поєднанні цих технологій для задоволення потреб користувачів у розробці розумних інфраструктур стає актуальною. Архітектура технології ІоТ для розробки розумних інфраструктур зображена на рисунку 1.3.

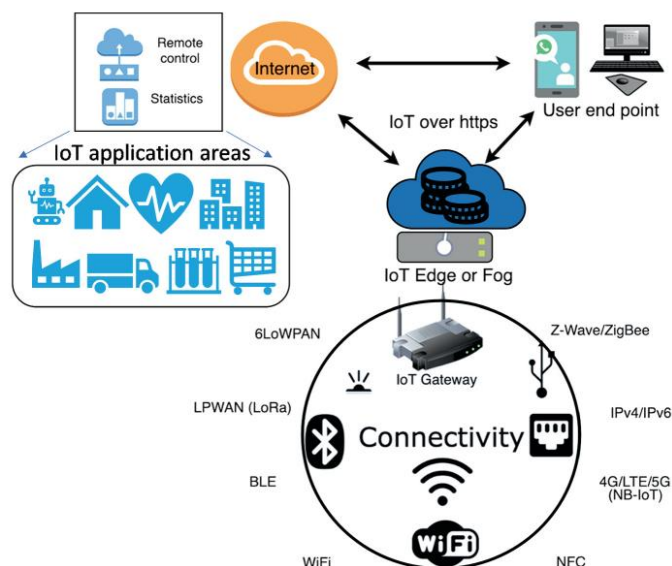


Рисунок 1.3 – Архітектура технологій IoT для розробки інфраструктури розумної мережі. Адаптовано з праці [6]

На ранніх етапах дослідження розумних мереж та IoT була розроблена найбільш фундаментальна архітектура в цій галузі. Вона містить три рівні: прикладний, мережевий рівень та рівень сприйняття [7], як показано на рисунку 1.4. Рівень сприйняття складається з фізичних компонентів, які мають датчики для спостереження та збору інформації про навколишнє середовище. Мережевий рівень відповідає за керування з'єднаннями зі службами, мережевим обладнанням та іншими електронними об'єктами. Крім того, мережевий рівень використовуються для розповсюдження та аналізу даних датчиків. Прикладний рівень відповідає за надання користувачу інтерфейсу для керування мережею.

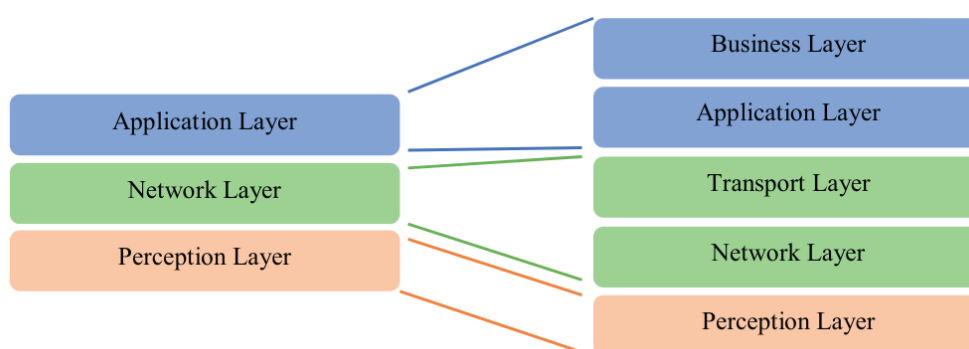


Рисунок 1.4 – Тривірнева та п'ятирівнева архітектури типових систем IoT. Адаптовано з праці [8]

Рівні сприйняття, обробки, транспортний рівень, бізнес рівень та прикладний складають п'ятирівневу архітектуру [9]. Транспортний рівень використовує мережі для передачі інформації з рівня сприйняття на рівень обробки і назад. Рівень проміжного програмного забезпечення, також відомий як рівень обробки, збирає, аналізує та оцінює великі обсяги даних транспортного рівня. Він має можливість наглядати та пропонувати різноманітні зручності для різних рівнів. Бізнес-рівень відповідає за всю інфраструктуру IoT, яка включає програми, сервіси, бізнес-моделі та захист конфіденційності. Більш конкретно, рівні цієї архітектури включають рівень фізичного сприйняття, протоколу та мережі, транспортний, прикладний, а також хмарні сервіси та рівні служб даних.

IoT підтримується різними динамічними технологіями, адаптованими до конкретних застосувань (рисунок 1.5). Ці технології відіграють вирішальну роль у створенні ландшафту додатків розумних мереж у різних галузях.

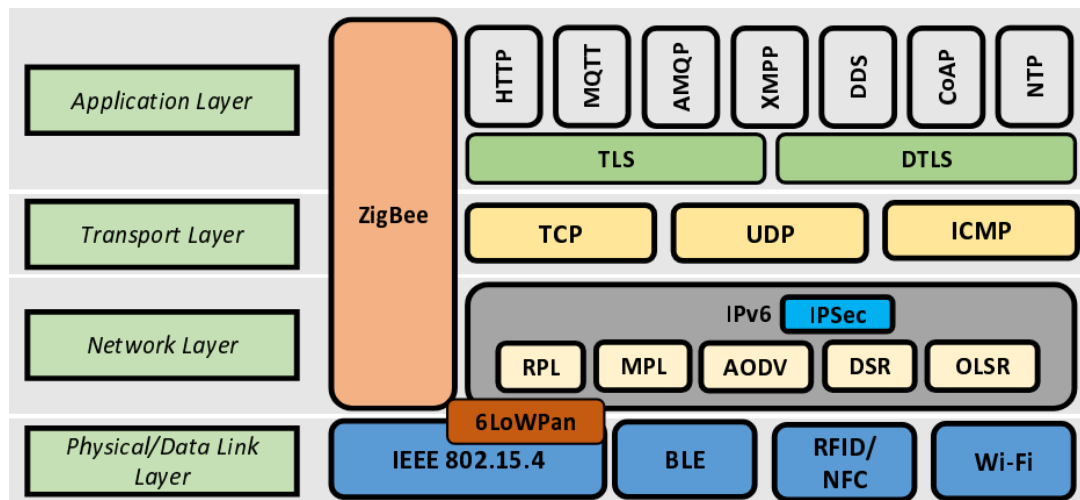


Рисунок 1.5 – Стек технологій розумної мережі. Адаптовано з праці [10]

Ці технології призначені для задоволення конкретних потреб і обмежень розгортання розумних мереж IoT, таких як робота з низьким енергоспоживанням, ефективність використання ресурсів і сумісність.

1.3. Застосування розумних мереж у різних сферах життєдіяльності

Розумні мережі та інтернет речей мають велику кількість можливих застосувань. Промислові мережі розвиваються завдяки впровадженню розумних пристроїв і сенсорів та збору величезних обсягів корисних даних, які можна використовувати для керування різними бізнес-операціями. Мережі IoT можуть бути налаштовані майже для будь-якої галузі, включаючи лікарні, системи керування, розумні пристрої, транспортні засоби та розумні переносні пристрої.

Забезпечуючи моніторинг, контроль і оптимізацію розподілу енергії в реальному часі, інтеграція IoT в електромережі трансформує звичайну електричну інфраструктуру на інтелектуальні адаптивні системи, які можуть задовольнити мінливі потреби сучасного суспільства, одночасно підвищуючи стійкість і надійність. Інтелектуальні лічильники з підтримкою IoT збирають детальну інформацію про перебої в електропостачанні, рівні напруги та тенденції споживання енергії. Комунальні підприємства можуть використовувати ці дані для зниження споживацьких витрат на електроенергію шляхом впровадження програм реагування на попит, ефективного розподілу ресурсів і пом'якшення пікового навантаження [11].

Технології розумних мереж дозволяють впроваджувати інтелектуальні мобільні рішення, які покращують стійкість, безпеку та ефективність транспорту. Обмін інформацією в режимі реального часу між транспортними засобами та компонентами інфраструктури стає можливим через зв'язок між транспортними засобами (V2V – Vehicle to vehicle) і транспортним засобом та інфраструктурою (V2I – Vehicle to infrastructure), що сприяє проактивному управлінню дорожнім рухом, уникненню зіткнень і оптимізації маршрутів [12].

Доступний широкий спектр рішень для застосування розумних мереж у сфері громадської безпеки для покращення боротьби зі стихійними лихами, запобігання злочинам і реагування на надзвичайні ситуації. Моніторинг громадських місць, важливої інфраструктури та регіонів високого ризику в

режимі реального часу стає можливим завдяки інтелектуальним системам відеоспостереження, оснащеним датчиками IoT і відеоаналітикою [13].

Розумні мережі та технології IoT змінили повсякденне життя, дозволивши будувати розумні будинки, які забезпечують більший комфорт, зручність та енергоефективність. Екосистеми розумного дому з підтримкою інтернету речей можуть навчатися та адаптуватися до вподобань і поведінки мешканців з часом, що призводить до більш персоналізованого досвіду та кращої енергоефективності [14]. Розумні будинки, які використовують технологію IoT, забезпечують підвищену зручність, безпеку та енергоефективність, одночасно підвищуючи загальну якість життя.

Загалом, за останні роки IoT досяг значного прогресу, повністю змінивши способи, якими ми взаємодіємо з технологіями. Завдяки зростанню кількості розумних пристроїв інтернет речей поширився в багатьох галузях, від медицини до виробництва, транспорту та розумних будинків. Останні досягнення в мережевих технологіях, таких як 5G і периферійні обчислення, дали можливість аналізувати дані в реальному часі на самій периферії мережі. Крім того, системи інтернету речей тепер можуть отримувати корисну інформацію з величезних обсягів даних завдяки впровадженню штучного інтелекту та машинного навчання.

РОЗДІЛ 2

ПОСТАНОВКА ЗАВДАННЯ ТА ВИБІР МЕТОДІВ РІШЕННЯ

2.1. Розробка інтелектуальної мережі

Завдання роботи полягає в розробці інтелектуальної мережі для офісного середовища, використовуючи технології та обладнання від Cisco Systems. Мережа включає в себе розумні пристрої та сенсори інтернету речей для забезпечення розумних функцій. Метою проекту є створення мережі, яка буде забезпечувати високу продуктивність, безпеку та ефективне управління ресурсами офісного середовища.

Розроблена мережа повинна задовольняти такі основні вимоги:

- Мережа повинна забезпечувати високу швидкодію та надійність з'єднання для всіх пристроїв, що підключені до неї;
- Система повинна бути легко масштабована, щоб враховувати зростаючі потреби користувачів;
- Мережа повинна бути сумісна з різноманітними пристроями та сенсорами інтернету речей, що використовуються в офісному середовищі для автоматизації процесів та підвищення ефективності;
- Забезпечення стабільності роботи мережі з мінімальними перервами у доступності;
- Мережа повинна бути інтегрована з існуючими системами керування офісом та інфраструктурою.

Для реалізації поставленої задачі потрібно провести аналіз області дослідження, визначити актуальні потреби користувачів, обрати програмне забезпечення для проектування мережі, розробити проект архітектури мережі з використанням обладнання Cisco, виконати налаштування компонентів та провести тестування.

Очікуваним результатом проекту є створення інтелектуальної мережі, що забезпечує високу продуктивність, безпеку та ефективне управління ресурсами офісного середовища з використанням технологій та обладнання Cisco Systems,

зокрема сучасних рішень для IoT, що дозволить оптимізувати витрати та покращити загальну ефективність робочого процесу.

2.2. Програмне забезпечення для моделювання розумної мережі

У даній роботі моделювання мережі буде виконуватись в програмному середовищі Cisco Packet Tracer. Cisco Packet Tracer — це програмний інструмент для візуального моделювання мереж, розроблений компанією Cisco Systems, який дозволяє користувачам створювати мережеві топології та імітувати сучасні мережі. Програмне забезпечення дозволяє користувачам імітувати конфігурацію маршрутизаторів і комутаторів Cisco за допомогою інтерфейсу командного рядка. Packet Tracer дозволяє будувати мережеві топології, імітує поведінку мережі, маршрутизаторів та комутаторів, а також пристрої та сенсори IoT які забезпечують розумні функції мережі.

У контексті моделювання мереж програмне середовище Cisco Packet Tracer пропонує кілька ключових переваг і застосувань [15]:

- **Покращення практичних знань:** Cisco Packet Tracer забезпечує динамічне та інтерактивне середовище, де користувач може експериментувати з різними мережевими концепціями та протоколами. Він усуває розрив між теорією та практикою, дозволяючи користувачам налаштовувати та виправляти мережеві сценарії у безпечному віртуальному середовищі.
- **Інновації та креативність:** користувачі можуть використовувати Cisco Packet Tracer для розробки та реалізації інноваційних проєктів. Це заохочує творчі здібності та навички вирішення проблем, оскільки вони застосовують принципи мереж у реальних сценаріях.
- **Розуміння мережевих протоколів:** Cisco Packet Tracer дозволяє користувачам спостерігати за мережевими протоколами в дії. Він надає платформу для проєктування, налаштування та аналізу мереж, допомагаючи користувачам зрозуміти практичне застосування цих протоколів.

- Економічність: доступ до фізичних мережевих пристроїв може бути обмежений через вартість і технічні обмеження. Cisco Packet Tracer усуває ці бар'єри, пропонуючи віртуальне середовище, де користувачі можуть отримати доступ і експериментувати з віртуальними мережевими пристроями в будь-який час, без ризику пошкодження фізичного обладнання.
- Візуалізація та моделювання: програмне забезпечення дозволяє користувачам візуалізувати рух пакетів даних у мережі в режимі реального часу. Цей візуальний зворотний зв'язок допомагає зрозуміти складні мережеві концепції та протоколи.

Cisco Packet Tracer має вбудовану бібліотеку розумних пристроїв та сенсорів які можуть збирати та обмінюватися даними в мережі. Вона містить датчики, виконавчі механізми та різноманітні гаджети, які забезпечують автоматизацію та дистанційне керування ресурсами:

Cisco Packet Tracer надає користувачам мережеве лабораторне середовище для виконання операцій або програм Cisco без використання фізичних пристроїв. Інструмент пропонує широкий набір віртуального апаратного забезпечення, що дозволяє користувачам налаштовувати від базової до дуже складної конфігурації мережі, саме тому ця робота була сфокусована на моделюванні розумної мережі в даному програмному середовищі.

РОЗДІЛ 3

МОДЕЛЮВАННЯ РОЗУМНОЇ МЕРЕЖІ ДЛЯ ОФІСНОГО СЕРЕДОВИЩА

3.1. Конфігурація компонентів

Щоб реалізувати розумну мережу, яку можна автоматично та віддалено контролювати з будь-якого пристрою підключеного до мережі 3G/4G, мережа була логічно розділена на чотири зони: офісне середовище, хмара інтернет-провайдера, мережа сервісного обладнання і мережа провайдера 3G/4G. Рисунок 3.1 демонструє топологію змодельованої мережі.

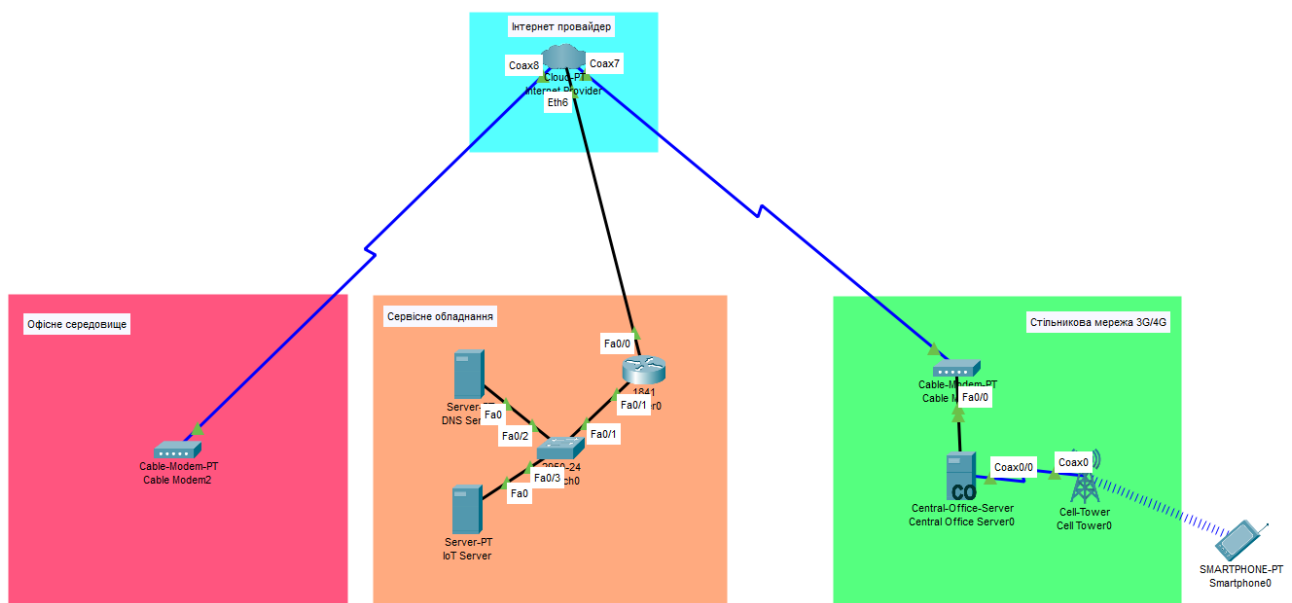


Рисунок 3.1 – Топологія мережі

Щоб забезпечити доступ до Інтернету для всіх компонентів, необхідна віртуальна система, яка працює в якості інтернет провайдера шляхом передачі сигналів від порту Coax7 до порту Ethernet6 і від порту Coax8 до порту Ethernet6, як показано на рисунку 3.2.

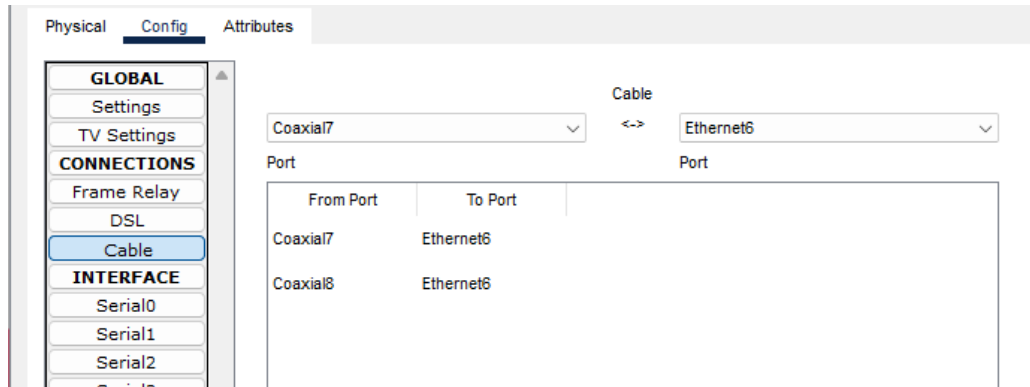


Рисунок 3.2 – Конфігурація хмари інтернет провайдера

Як сервісне обладнання використовуємо маршрутизатор Router0, що з'єднує локальну мережу сервісного обладнання, підключену до його інтерфейсу Fa0/1, з іншими локальними мережами через WAN, підключену до інтерфейсу Fa0/0.

Адреса інтерфейсу Fa0/0 має бути встановлена як маршрутизатор за замовчуванням для сервера DHCP, щоб надавати адреси з мережі 10.0.0.0/8 з DNS сервером 192.168.1.2. Для цього на маршрутизаторі Router0 було налаштовано DHCP сервер.

Щоб транслювати IP-адресу сервера IoT 192.168.1.3 в домен smartoffice.com на сервері потрібно увімкнути службу DNS і додати доменне ім'я та IP-адресу, як показано на рисунку 3.3.

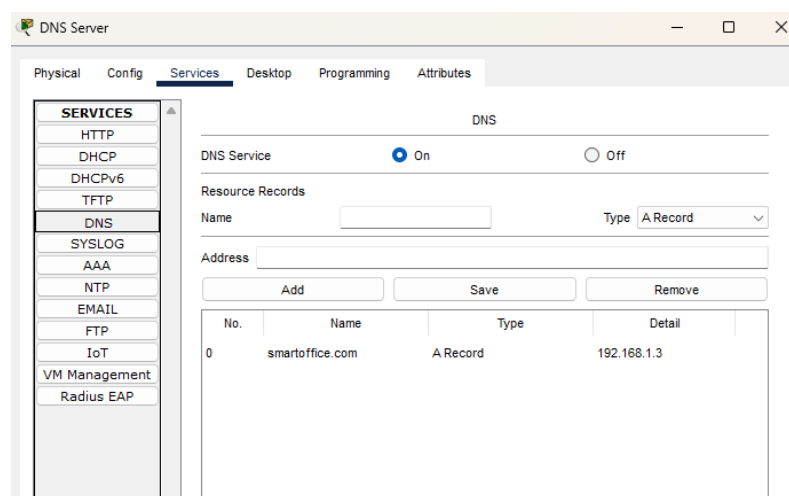


Рисунок 3.3 – Конфігурація DNS серверу

Щоб налаштувати IoT сервер, послугу IoT потрібно ввімкнути на вкладці Services. Потім необхідно створити обліковий запис на сервері, запустивши веб-браузер із робочого столу самого сервера та ввести в адресну стрічку адресу сервера IoT 192.168.1.3 або ім'я домену smartoffice.com (малюнок 3.6). Оскільки у нас ще немає облікового запису, нам потрібно натиснути «Sign up now».

Було зареєстровано аккаунт з ім'ям користувача «admin» і паролем «admin».

В результаті, так як IoT сервер підключений до мережі, ми можемо отримати доступ до панелі керування відкривши веб-браузер на будь-якому пристрої підключеному до мережі і ввівши в адресний рядок адресу сервера «smartoffice.com».

Використання стільникової мережі 3G/4G було реалізовано з використанням серверу центрального офісу стільникової мережі 3G/4G, що має два інтерфейси: магістральний для підключення провайдера до глобальної мережі та коаксіальний інтерфейс для підключення сервера до вишки стільникового зв'язку.

Магістральний інтерфейс підключений до інтернет-провайдера. Отже, він отримає динамічну адресу, коли ми ввімкнемо протокол DHCP.

Сервер центрального офісу стільникової мережі також працює як сервер DHCP для всіх пристроїв, підключених до стільникової мережі.

Підключення до стільникової мережі зі смартфона можна здійснити ввівши назву провайдера 3G/4G «SMARTNET», телефон буде підключено до вежі. Таким чином, сервер призначить для смартфона адресу з мережі 172.16.1.0/24, як показано на рисунку 3.4 нижче.

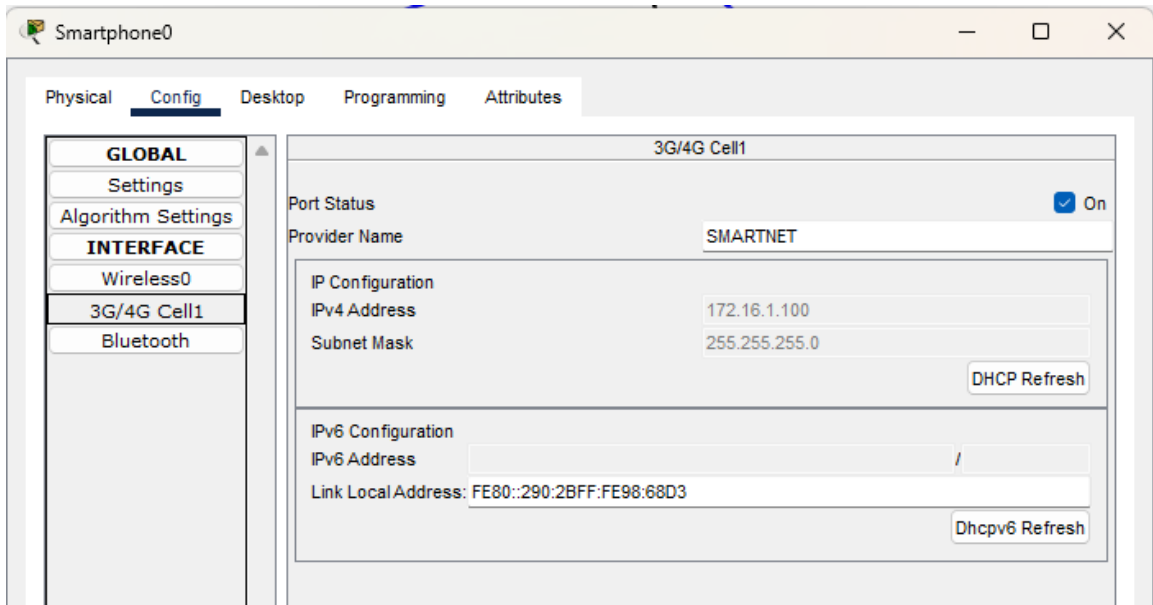


Рисунок 3.4 – Налаштування підключення смартфона до мережі 3G/4G

Виконуючи описані кроки, смартфон буде підключено до інтернету та матиме доступ до сервера IoT.

3.1.5. Налаштування шлюзу та комп'ютера для керування ресурсами мережі

Шлюз «HomeGateway» (рисунок 3.5) має три інтерфейси: Інтернет, локальна мережа та бездротовий інтерфейс.

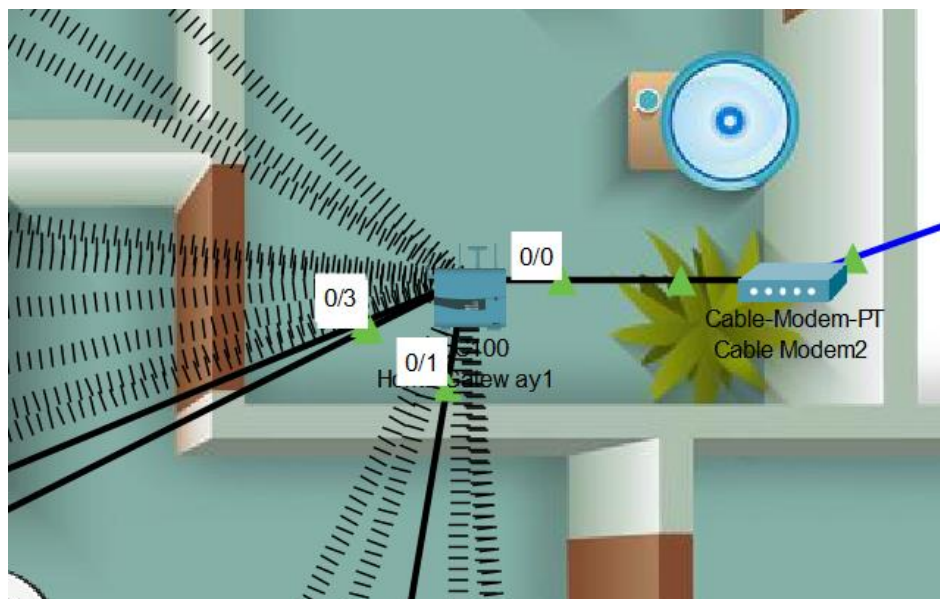


Рисунок 3.5 – Шлюз HomeGateway

Інтернет інтерфейс підключає офіс до Інтернету через модем, оскільки цей інтерфейс підключений до інтернет-провайдера. Після того, як ми виберемо DHCP на вкладці «Internet», інтерфейс отримає динамічну IP-адресу з пулу «RouterPool», шлюз за замовчуванням — 10.0.0.1, а сервер DNS — 192.168.1.2, як показано на рисунку 3.6.

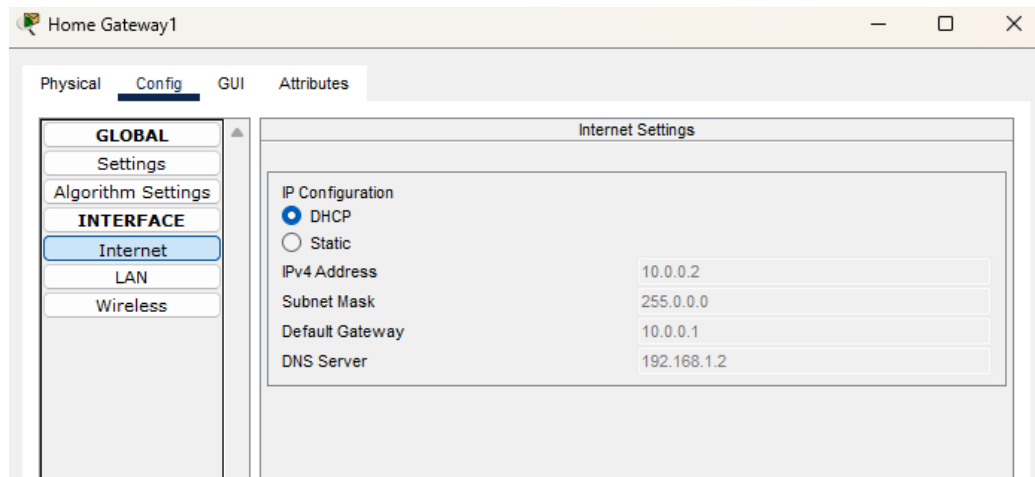


Рисунок 3.6 – Інтернет інтерфейс шлюзу HomeGateway

На вкладці конфігурації бездротового інтерфейсу, показаній на рисунку 3.7, можна встановити особистий SSID і пароль. SSID домашнього шлюзу встановлено на «HomeGateway» і пароль «smartoffice». Алгоритм авторизації WPA2-PSK. Він використовуватиметься для всіх пристроїв які підключаються до шлюзу по WiFi.

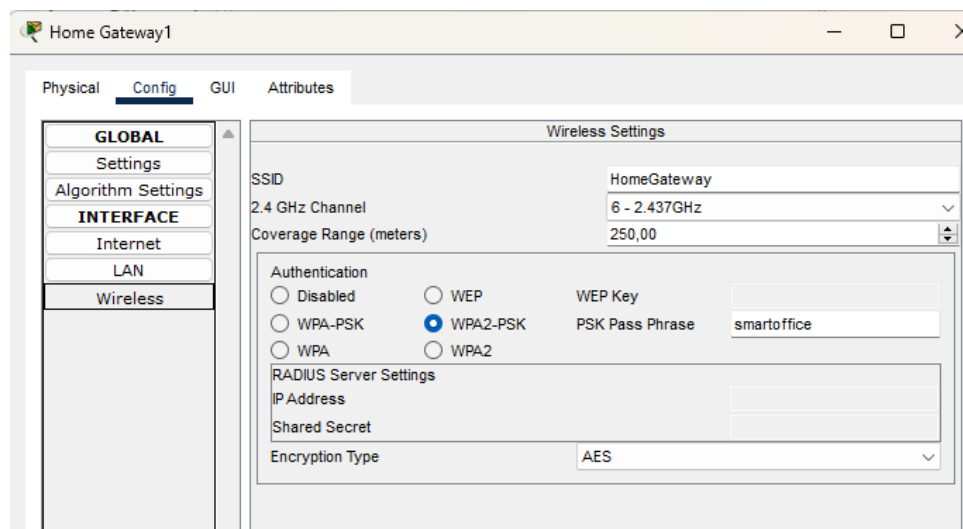


Рисунок 3.7 – Бездротовий інтерфейс шлюзу HomeGateway

Для керування ресурсами мережі в межах офісного середовища, до шлюзу HomeGateway було підключено ноутбук. Після введення «HomeGateway» у полі SSID, вибору алгоритму авторизації WPA2-PSK та введення паролю «smartoffice» на вкладці конфігурації бездротового інтерфейсу ноутбук фізично підключається до шлюзу. Якщо ми виберемо DHCP шлюз надасть ноутбуку динамічну адресу.

Підключення розумних пристроїв та сенсорів. Після введення «HomeGateway» у полі SSID інтерфейсу wireless0, вибору алгоритму авторизації та введення паролю на вкладці «Config» пристрій підключається до шлюзу, як показано на рисунку 3.8. Раніше було зазначено, що шлюз «HomeGateway» працює як сервер DHCP, таким чином, будь-який пристрій повинен мати динамічну IP-адресу.

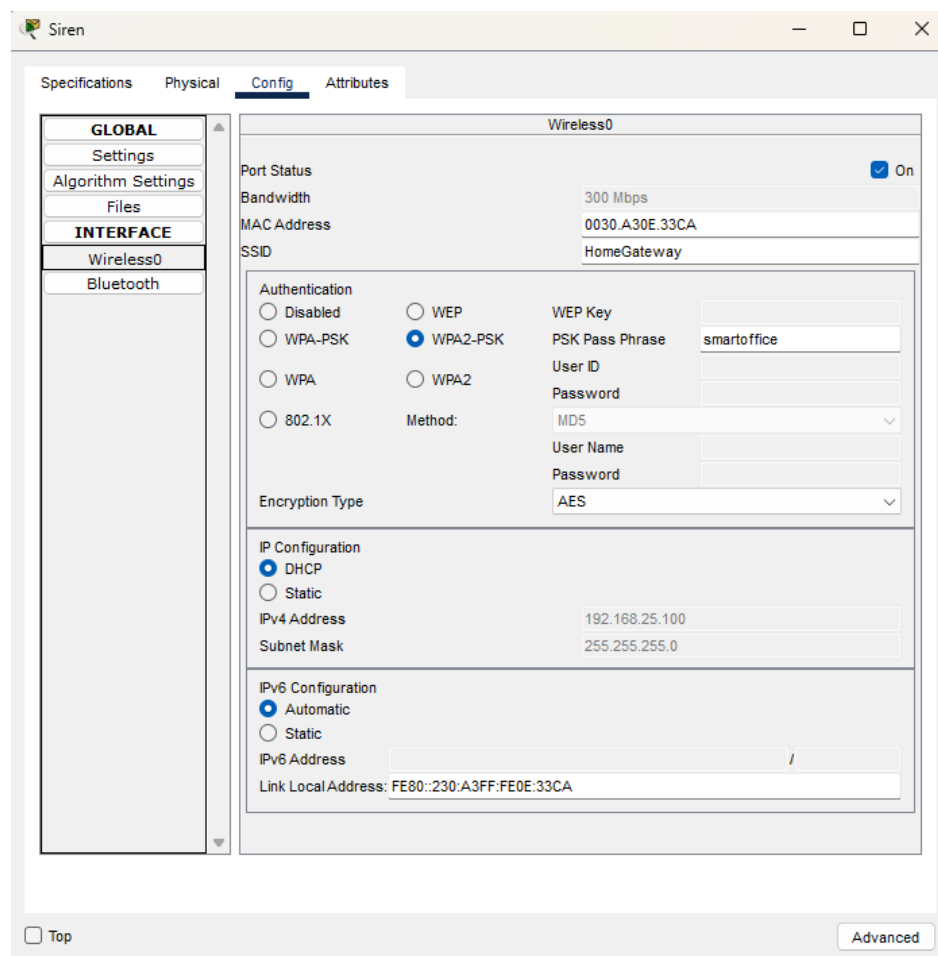


Рисунок 3.8 – Підключення пристрою до шлюзу «HomeGateway»

Пристрої автоматично отримують адреси шлюзу за умовчанням і DNS-сервера, як показано на рисунку 3.9.

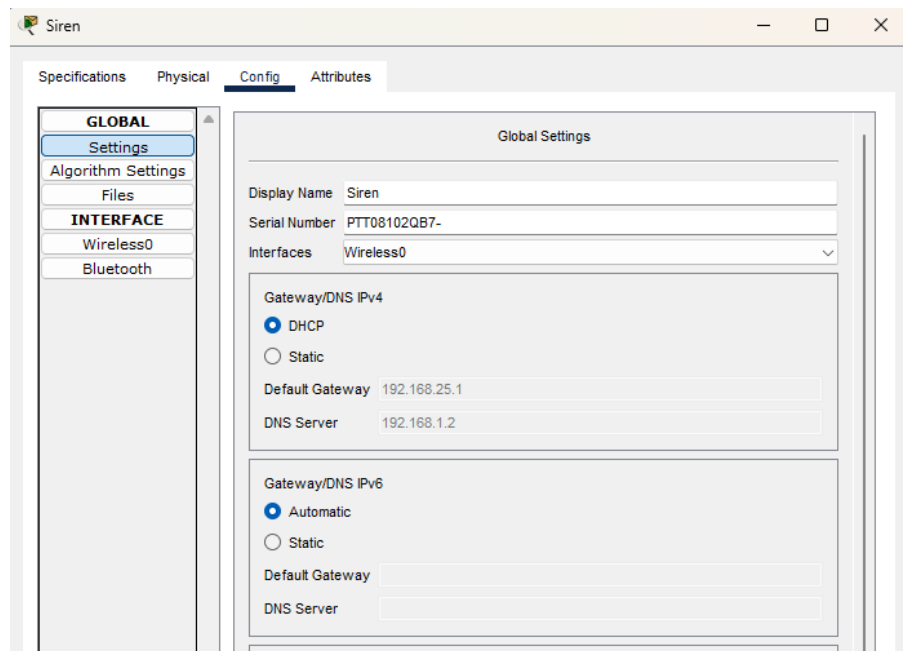


Рисунок 3.9 – Шлюз за замовчуванням та адреса DNS сервера

Сервер IoT повинен знати всі пристрої IoT, які встановлені в офісному середовищі. Імена пристроїв IoT за замовчуванням — «IoT» плюс число, тож потрібно зробити чіткі назви для пристроїв, щоб уникнути помилок.

Щоб зареєструвати пристрій на IoT сервері, потрібні адреса сервера, ім'я користувача та пароль облікового запису. Усі пристрої мають використовувати однакові облікові дані для Інтернету речей, ті самі облікові дані також були використані для проходження автентифікації під час підключення через браузер до сервера IoT.

На вкладці конфігурації пристрою в полі сервер IoT треба обрати «Remote Server» (рисунок 3.10); потім ввести необхідну інформацію та натиснути «підключити».

IoT Server

None
 Home Gateway
 Remote Server

Server Address:

User Name:

Password:

Рисунок 3.10 – Реєстрація пристрою на сервері IoT

Якщо користувач використовує браузер ноутбука для доступу до IoT-сервера, після підключення користувача до «smartoffice.com» через браузер або «IoT Monitor» на вкладці «Desktop» він може візуалізувати статус IoT-пристроїв, зареєстрованих на IoT-сервері. На рисунку 3.11 показано інтерфейс керування пристроями зареєстрованими на сервері IoT.

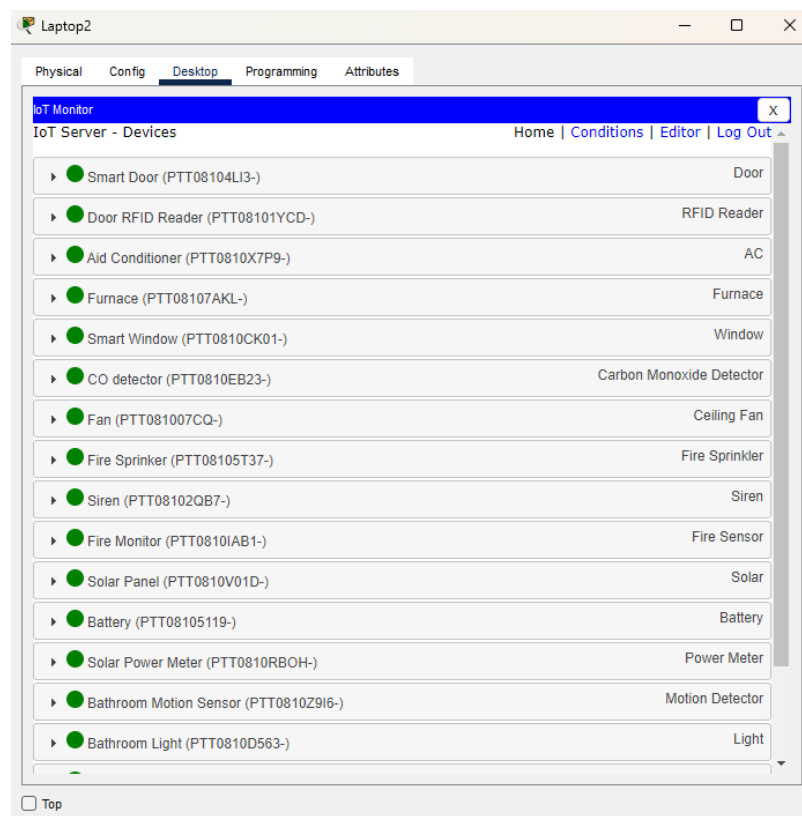


Рисунок 3.11 – Статус пристроїв зареєстрованих на сервері IoT

Цей веб-інтерфейс дозволяє користувачу контролювати пристрої що зареєстровані на сервері IoT і бачити деякі пристрої, які надають корисну інформацію. З цієї вкладки також користувач може взаємодіяти з пристроями.

3.2. Взаємодія компонентів розумної мережі

Система охорони для вхідних дверей (рис. 3.12) складається зі зчитувача RFID міток, розумного дверного замка, сенсору руху та камери відеоспостереження.

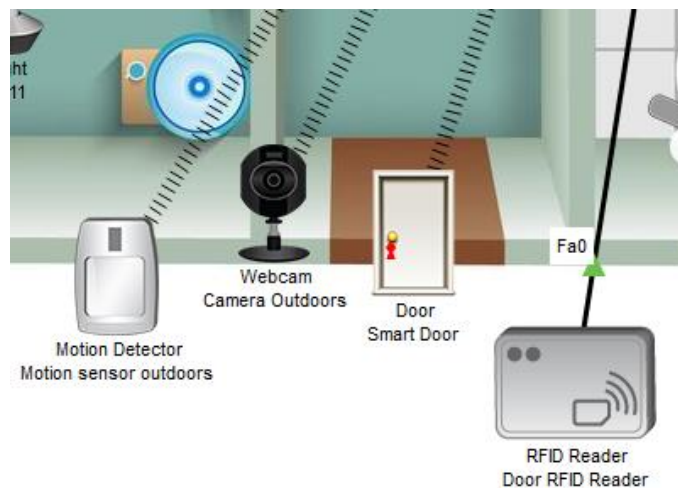


Рисунок 3.12 – Компоненти системи охорони вхідних дверей

Щоб керувати безпекою вхідних дверей за допомогою RFID, нам потрібно встановити деякі умови на сервері IoT. Таким чином, використовуються дві RFID мітки: одна має авторизований ідентифікатор 2001, а друга має неавторизований ідентифікатор 3001. Зчитувач RFID налаштований таким чином, що мітки з ідентифікатором в діапазоні від 2000 до 3000 є авторизованими (рис. 3.13).

Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	RFID valid	Door RFID Reader Card ID is between 2000 and 3000	Set Door RFID Reader Status to Valid
Edit Remove	Yes	RFID door unlock	Door RFID Reader Status is Valid	Set Smart Door Lock to Unlock
Edit Remove	Yes	RFID door lock	Match any: • Door RFID Reader Status is Invalid • Door RFID Reader Status is Waiting	Set Smart Door Lock to Lock
Edit Remove	Yes	RFID invalid	Match any: • Door RFID Reader Card ID < 2000 • Door RFID Reader Card ID > 3000	Set Door RFID Reader Status to Invalid

Рисунок 3.13 – Конфігурація алгоритму роботи RFID зчитувача

Алгоритм системи можна описати за допомогою наступних кроків:

- Зчитувач RFID працює, якщо картка знаходиться досить близько до нього.
- Якщо авторизовану ідентифікаційну картку буде зчитано, пристрій надішле «дійсний» сигнал на сервер; інакше він надішле сигнал «недійсний».
- Якщо жодна картка не знаходиться поблизу зчитувача RFID, пристрій продовжує надсилати сигнал «очікування».
- Якщо сервер отримує «дійсний» сигнал, він відкриває дверний замок (рис. 3.14). В іншому випадку замок залишається зачиненим (рис. 3.14).

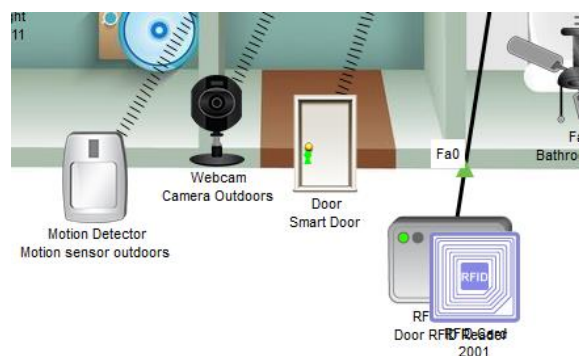


Рисунок 3.14 – Зчитувач RFID отримав дійсну мітку з ідентифікатором 2001. Замок відкритий про що свідчить зелений індикатор

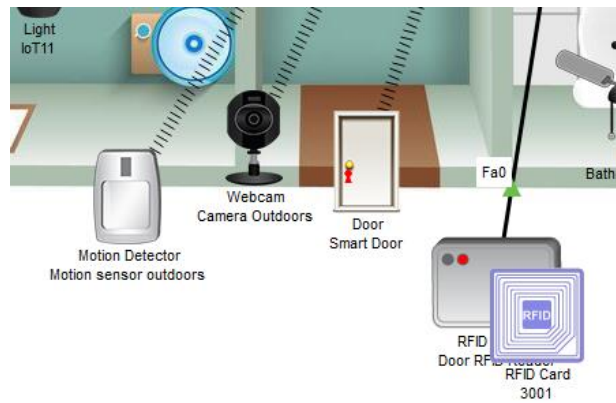


Рисунок 3.15 – Зчитувач RFID отримав недійсну мітку з ідентифікатором 3001. Замок зачинений про що свідчить червоний індикатор

Система відеонагляду складається з сенсору руху та камери відеоспостереження. Камера активується і починає запис за умов коли сенсор бачить рух (рис. 3.16).

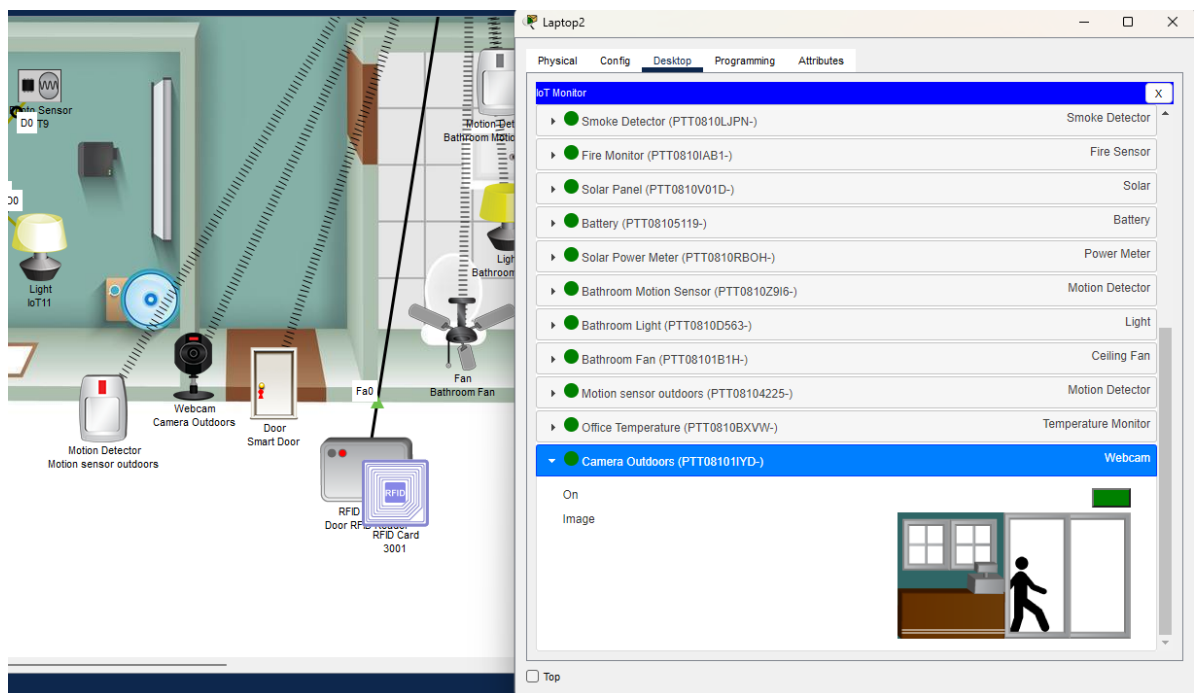


Рисунок. 3.16 – Камера відеоспостереження активується сенсором руху. За активністю системи відеоспостереження можна спостерігати з веб-інтерфейсу керування мережею

Система керування кліматом складається з термостату, кондиціонера, обігрівача та додаткового сенсору температури зареєстрованих на сервері IoT для віддаленого керування (рис. 3.17).

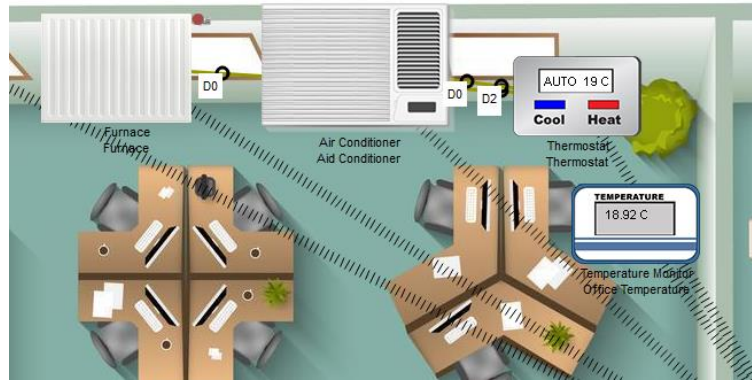


Рисунок 3.17 – Компоненти системи керування кліматом

Кондиціонер та обігрівач керуються термостатом автономно. Система може працювати в ручному режимі обігріву або кондиціонування або в режимі підтримки заданого діапазону температури. Керувати параметрами системи можна безпосередньо за допомогою термостату або віддалено за допомогою веб-інтерфейсу (рис. 3.18).

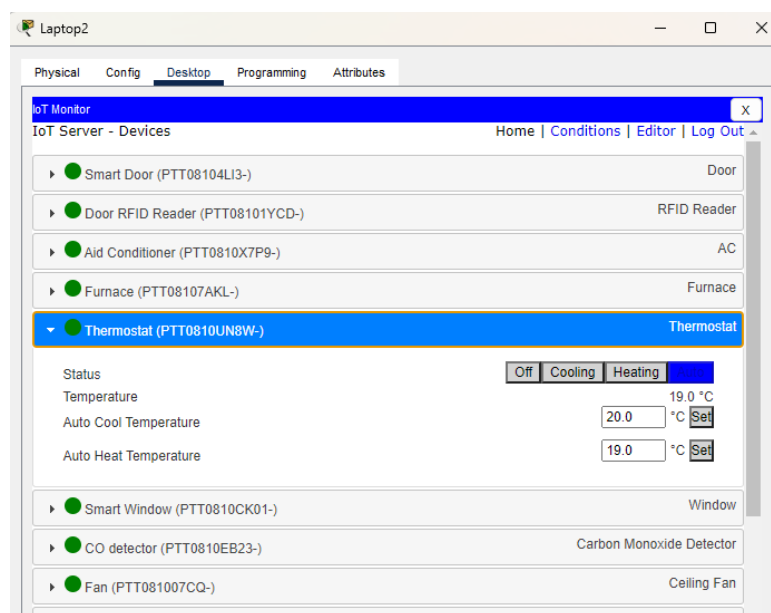


Рисунок 3.18 – Налаштування параметрів системи керування кліматом

Система моніторингу якості повітря складається з сенсора вмісту оксидів вуглецю, розумного вікна та вентиляції.

При досягненні в повітрі рівня оксидів вуглецю в межах 20-25% відчиняється розумне вікно і вмикається вентиляція на низьку швидкість. При рівні вище 25% вікно залишається відчиненим а вентиляція перемикається на високу швидкість роботи (рисунок 3.20).

Edit Remove	Yes	CO between 20 and 25	CO detector Level is between 20 and 25	Set Smart Window On to true Set Fan Status to Low
Edit Remove	Yes	CO more than 25	Match any: <ul style="list-style-type: none"> CO detector Level > 25 CO detector Alarm is true 	Set Fan Status to High Set Smart Window On to true
Edit Remove	Yes	CO normal	CO detector Level < 5	Set Smart Window On to false Set Fan Status to Off
Edit				Set Fire Sprinkler Status to

Рисунок 3.20 Конфігурація алгоритму роботи системи моніторингу якості повітря.

Для тестування роботи системи в параметрах віртуального середовища було налаштовано підйом рівня оксидів вуглецю в повітрі до 40% (рисунок 3.21).

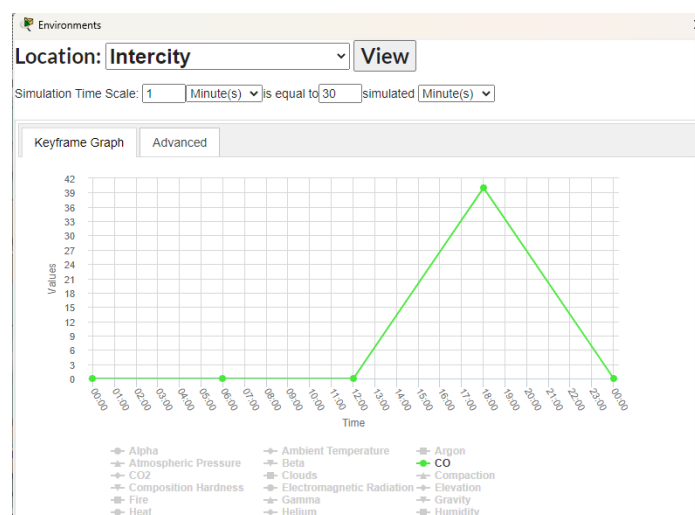


Рисунок 3.21 – Конфігурація рівня оксидів вуглецю у віртуальному середовищі

При досягненні підвищеного рівня оксидів вуглецю, можемо спостерігати як система автоматично відчинила вікно та ввімкнула вентиляцію (рисунок 3.22). Про досягнення підвищеного рівня вуглецю сигналізує червоний індикатор на сенсорі вмісту оксидів вуглецю.

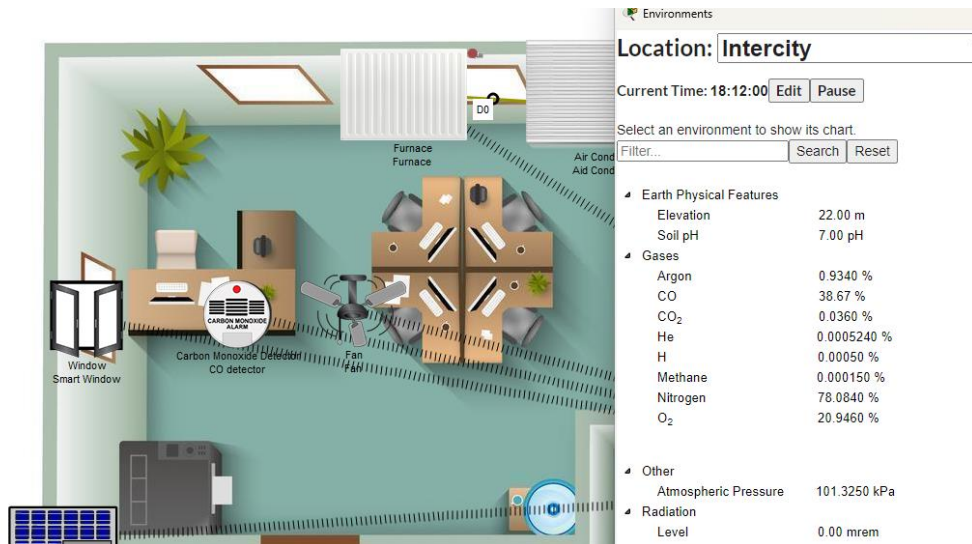


Рисунок 3.22 – Робота системи моніторингу якості повітря

Система пожежної безпеки складається з сенсора диму, сенсора вогню, форсунки для гасіння пожежі та сигналізації.

При досягненні рівня задимлення вище 40%, автоматично вмикається сигналізація (рисунок 3.23).



Рисунок 3.23 Робота системи сигналізації при задимленні

При виявленні вогню активується пожежна сигналізація та форсунка пожежогасіння (рисунок 3.24). Конфігурація роботи системи пожежної безпеки зображена на рисунку 3.25.

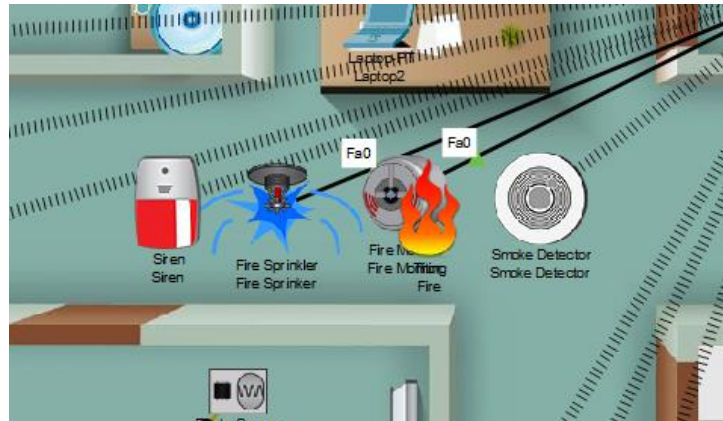


Рисунок 3.24 – Робота пожежної сигналізації

<input type="button" value="Edit"/> <input type="button" value="Remove"/>	Yes	Fire detected	Fire Monitor Fire Detected is true	Set Fire Sprinkler Status to true Set Siren On to true
<input type="button" value="Edit"/> <input type="button" value="Remove"/>	Yes	Smoke detected	Smoke Detector Alarm is true	Set Siren On to true

Рисунок 3.25 – Конфігурація системи пожежної безпеки

Система автоматичного керування вентиляцією та освітленням складається з сенсору руху, розумної лампи та вентиляції. При виявленні руху, сервер автоматично активує вентиляцію та освітлення. Конфігурація системи зображена на рисунку 3.26.

<input type="button" value="Edit"/> <input type="button" value="Remove"/>	Yes	Bathroom Motion	Bathroom Motion Sensor On is true	Set Bathroom Light Status to On Set Bathroom Fan Status to Low
<input type="button" value="Edit"/> <input type="button" value="Remove"/>	Yes	Bathroom no motion	Bathroom Motion Sensor On is false	Set Bathroom Light Status to Off Set Bathroom Fan Status to Off

Рисунок 3.26 – Конфігурація системи автоматичного освітлення та вентиляції для ванної кімнати

Для тестування роботи системи потрібно задіяти сенсор руху. При виявленні руху автоматично вмикається лампа та вентиляція відповідно до налаштувань алгоритму (рис. 3.27). Окремо була змодельована система автоматичного освітлення на основі показників фотосенсору та мікроконтролера (рис. 3.28). До компонентів системи входить сенсор освітлення, мікроконтролер та лампа.

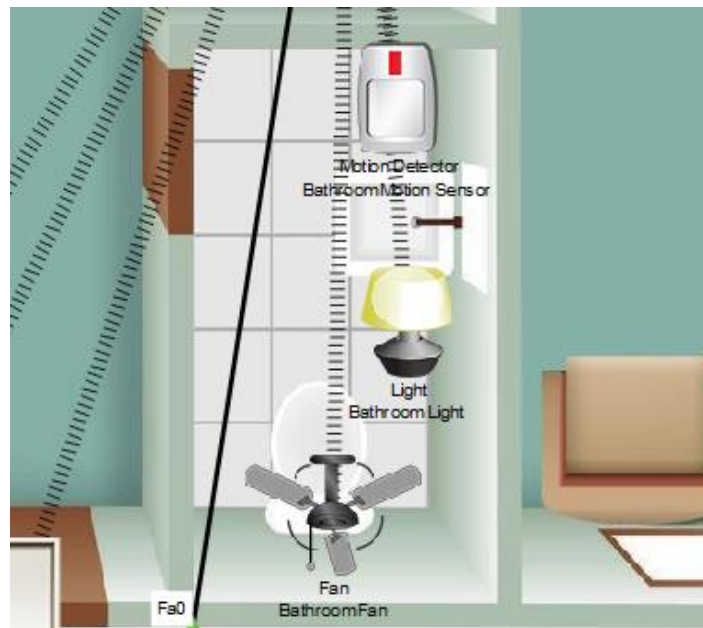


Рисунок 3.27 – Робота системи автоматичного освітлення та вентиляції

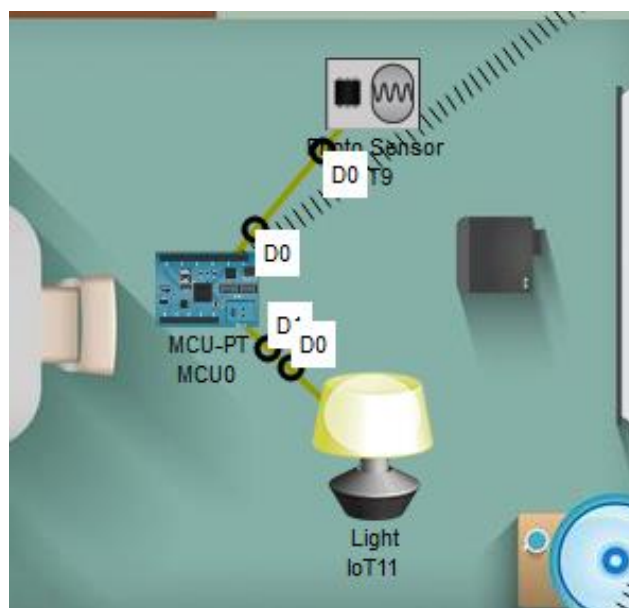


Рисунок 3.28 – Система автоматичного освітлення на основі фотосенсору та мікроконтролера

Мікроконтроллер зчитує показники з фотосенсору і коли рівень освітлення падає нижче порогового значення дає команду на включення освітлення. Також було запрограмовано API для віддаленого керування системою з сервера IoT.

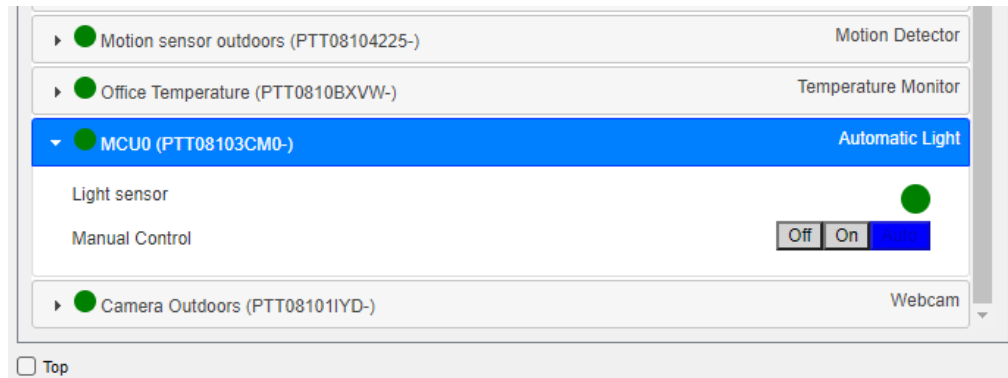


Рисунок 3.29 – Інтерфейс віддаленого керування системою

Показник «Light Sensor» відображає статус фотосенсора. Зелений індикатор означає що світло буде активовано в автоматичному режимі. «Manual Control» дозволяє в ручному режимі ввімкнути чи вимкнути світло або ввімкнути автоматичний режим.

Код програми мікроконтролера прикріплений у додатку 1.

До складу системи автономного електроживлення входить сонячна панель, лічильник потужності, батарея та світлодіод у якості моделі споживача електроенергії (рисунок 3.30).

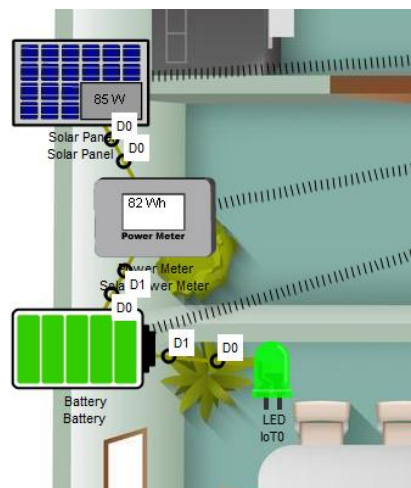


Рисунок 3.30 – Компоненти системи автономного електроживлення

Сонячна панель заряджає батарею при значенні змінної середовища «Sunlight» більше 0%.

При наявності достатнього рівня заряду активуються споживачі електроенергії, які підключені до батареї. Оскільки компоненти системи підключені до центрального IoT сервера, є можливість віддалено моніторити стан системи через веб-інтерфейс (рисунок 3.31).



▶ ● Smoke Detector (PTT0810LJPN-)	Smoke Detector
▶ ● Fire Monitor (PTT0810IAB1-)	Fire Sensor
▼ ● Solar Panel (PTT0810V01D-)	Solar
Status	126 Wh
▼ ● Battery (PTT08105119-)	Battery
Available power	99.33 %
▼ ● Solar Power Meter (PTT0810RBOH-)	Power Meter
Status	118.123 Watts
▶ ● Bathroom Motion Sensor (PTT0810Z9I6-)	Motion Detector
▶ ● Bathroom Light (PTT0810D563-)	Light

Рисунок 3.31 – Відображення параметрів системи у веб-інтерфейсі IoT сервера

ВИСНОВКИ

У ході виконання кваліфікаційної роботи магістра було виконано аналіз проблематики розробки інтелектуальної електронної системи для офісного середовища, використовуючи технології та обладнання від Cisco. Проведено огляд обладнання та технологій які використовуються для розробки розумних мереж, методів маршрутизації даних та керування мережевим трафіком.

У результаті виконання роботи була розроблена модель інтелектуальної розумної мережі для офісного середовища, використовуючи технології та обладнання від Cisco Systems. Реалізація розумної мережі була здійснена шляхом логічного поділу на чотири зони: офісне середовище, хмару інтернет-провайдера, мережу сервісного обладнання та мережу провайдера 3G/4G. Значна увага була приділена розробці автоматизованих електронних систем, а саме: охорони, пожежної безпеки, керування кліматичною установкою та якістю повітря для офісного середовищ. Система якості повітря була побудована на принципі контролю та утримання рівня оксидів вуглецю в повітрі нижче ніж 20-25%. Система пожежної безпеки була налаштована на спрацювання при рівні задимлення вище 40%, або спрацювання датчика полум'я.

Робота сприяла поглибленню знань у галузі розробки мережевої архітектури, зокрема, щодо застосування сучасних технологій для створення розумних мереж. Отримані результати можуть бути використані для вдосконалення мережевих рішень та підвищення ефективності роботи офісних приміщень, що підкреслює актуальність виконаної роботи. Розроблена цифрова модель може бути адаптована та впроваджена у реальне офісне середовище, враховуючи можливості існуючого обладнання, програмного забезпечення та індивідуальних потреб користувачів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Коробейнікова Т.І., Загарченко С.М. Комп'ютерні мережі. Навчальний посібник, Львів, Львівська політехніка, 2022. – с. 228.
2. Odom W. Cisco CCNA Routing and Switching: Official Cert Guide Library. Cisco Press, 2017. с. 172.
3. Types of Routing Protocols. Cisco Networking Academy's Introduction to Routing Dynamically | Cisco Press [Електронний ресурс] – Режим доступу
<https://www.ciscopress.com/articles/article.asp?p=2180210&seqNum=7>
4. Smart manufacturing: Past research, present findings, and future directions / H. S. Kang et al. *International Journal of Precision Engineering and Manufacturing-Green Technology*. 2016. Vol. 3, no. 1. с. 111–128.
5. Nord J. H., Koohang A., Paliszkievicz J. The Internet of Things: Review and theoretical framework. *Expert Systems with Applications*. 2019. Vol. 133. с. 97–108.
6. Technologies and Solutions for Smart Home and Smart Office / A. Luntovskyy et al. *Studies in Systems, Decision and Control*. Cham, 2023. с. 190–191.
7. A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis / H. Mrabet et al. *Sensors*. 2020. Vol. 20, no. 13. с. 3625.
8. Ag-IoT for crop and environment monitoring: Past, present, and future / N. Chamara et al. *Agricultural Systems*. 2022. Vol. 203. с. 103497.
9. Zhu J. Y., Tang B., Li V. O. K. A five-layer architecture for big data processing and analytics. *International Journal of Big Data Intelligence*. 2019. Vol. 6, no. 1. с. 39.
10. Rullo A., Bertino E., Sacca D. PAST: Protocol-Adaptable Security Tool for Heterogeneous IoT Ecosystems. *2018 IEEE Conference on Dependable and Secure Computing (DSC)*, Kaohsiung, Taiwan, 2018 p. – с.2.

11. Smart Grid Technologies: Communication Technologies and Standards / V. C. Gungor et al. *IEEE Transactions on Industrial Informatics*. 2011. Vol. 7, no. 4. c. 529–539.
12. Parallel Transportation Systems: Toward IoT-Enabled Smart Urban Traffic Control and Management / F. Zhu et al. *IEEE Transactions on Intelligent Transportation Systems*. 2020. Vol. 21, no. 10. c. 4063–4071.
13. Future IoT-enabled threats and vulnerabilities: State of the art, challenges, and future prospects / A. Srivastava et al. *International Journal of Communication Systems*. 2020. Vol. 33, no. 12. c. e4443.
14. Building the Internet of Things with bluetooth smart / S. Raza et al. *Ad Hoc Networks*. 2017. Vol. 57. c. 19–31.
15. Allison J. Simulation-Based Learning via Cisco Packet Tracer to Enhance the Teaching of Computer Networks. *ITiCSE 2022: Innovation and Technology in Computer Science Education*, Dublin Ireland. New York, NY, USA, 2022. c. 68–74.

ДОДАТКИ

Додаток 1.

```

var MANUAL_CONTROL = 2;

function setup() {
  pinMode(1, OUTPUT);
  pinMode(0, INPUT);
  IoEClient.setup({
    type: "Automatic Light",
    states: [{
      name: "Light sensor",
      type: "bool",
    }, {
      name: "Manual Control",
      type: "options",
      options: {
        0: "Off",
        1: "On",
        2: "Auto",
      },
      controllable: true
    }
  ]
});
  IoEClient.onStateSet = function(stateName, value) {
    if (stateName == "Manual Control") {
      MANUAL_CONTROL = Number(value);
    }
  };
}

function loop() {
  var light = digitalRead(0);
  var sensorResultOutput = 0;
  if (light == HIGH) {
    IoEClient.reportStates([false, MANUAL_CONTROL]);
  }
}

```



```
        sensorResultOutput = 0;
    } else {
        IoEClient.reportStates([true, MANUAL_CONTROL]);
        sensorResultOutput = 2;
    }

    if (MANUAL_CONTROL == 2) {
        customWrite(1, sensorResultOutput);
    } else if (MANUAL_CONTROL == 1) {
        customWrite(1, 2);
    } else {
        customWrite(1, 0);
    }
    delay(1000);
}
```