Міністерство освіти і науки України

Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра мережевих та інтернет технологій

ЗАТВЕРДЖУЮ
завідувач кафедри
мережевих та інтернет технологій

_____ Ю.В. Кравченко

«_____»_____2022 року

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

галузі знань 17 «Електроніка та телекомунікації»
за спеціальністю 172 «Телекомунікації та радіотехніка»

на тему:

Моделювання системи запобігання проникненню подвійного призначення

Виконав: студент групи МІТ -41

Минюк Павло Сергійович _____
(прізвище ім'я по-батькові) (підпис)

Керівник: доцент кафедри мережевих та інтернет технологій

д.т.н., доцент Дуднік А.С _____
(посада, прізвище ім'я по-батькові) (підпис)

Київ 2022

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра мережевих та інтернет технологій

ЗАТВЕРДЖУЮ
завідувач кафедри
мережевих та інтернет технологій

_____ Ю.В. Кравченко

«_____»_____2022 року

ЗАВДАННЯ
НА ДИПЛОМНУ РОБОТУ

Здобувачу вищої освіти Минюк Павло Сергійович
(прізвище, ім'я, по батькові)

1. Тема роботи: Моделювання системи запобігання проникненню подвійного призначення
затверджена на засіданні кафедри МІТ «___»_____20___р. протокол №____
2. Термін здачі закінченої роботи «30» червня 2022 р.
3. Вихідні дані до проекту (роботи)
Програма моделювання мереж – Cisco Packet Tracer
4. Зміст пояснювальної записки (перелік питань, що їх потрібно розробити, обсяг – 35-43 стор.)
Аналіз систем запобігання проникнення
Аналіз основних технологічних елементів систем запобігання
Побудова моделі та експерименти
5. Перелік графічного матеріалу, слайдів

Дата видачі завдання _____
Керівник роботи д.т.н., доцент кафедри МІТ Дуднік А.С
(підпис) (посада, прізвище, ім'я, по батькові)

Завдання прийняла до виконання Минюк Павло Сергійович

КАЛЕНДАРНИЙ ПЛАН ВИКОНАННЯ РОБОТИ

Номер	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Підготовчий	30.04.22	
2	Розділ 1	05.05.22	
3	Розділ 2	19.05.22	
4	Розділ 3	02.06.22	
5	Доповідь та слайди	16.06.22	
6	Пояснювальна записка	20.06.22	

Здобувач вищої освіти Минюк Павло Сергійович

Керівник Дуднік Андрій Сергійович

РЕФЕРАТ

Дипломна робота темою якої є «Моделювання системи запобігання проникненню подвійного призначення» для здобуття освітньо-кваліфікаційного рівня «Бакалавр» із спеціальності «Мережеві та інтернет технології» написана обсягом 43 сторінки, має 32 ілюстрацій і 16 використаних джерел.

Мета роботи: розроблення системи запобігання проникнення подвійного призначення

Методи дослідження: загалом це методи імітаційного моделювання

Було змодельовано систему запобігання проникненню подвійного призначення. В системі реалізовано різні методи визначення проникнення та проведено тестування їхньої роботоздатності.

Результати даної роботи можуть використовуватися як в цивільної частини населення країни, так і у військової. Для цивільної частини населення дана система може бути використання для будівель, наприклад як захист від проникнення до свого будинку. В свою чергу для військової частини населення дана система може використовуватися для визначення місцезнаходження ворога.

Щодо подальших досліджень, то одним із можливих напрямків може бути продовження роботи з безпровідними сенсорними мережами, а саме додати систему протипожежної безпеки.

Ключові слова: БЕЗПРОВІДНА СЕНСОРНА МЕРЕЖА, ПРОНИКНЕННЯ, ZIGBEE, WI-FI, BLUETOOTH

ABSTRACT

Thesis, which is the topic of "Modeling a dual-purpose intrusion prevention system" for the educational qualification level "Bachelor" in "Network and Internet Technologies" is written in 43 pages, has 32 illustrations and 16 sources used.

Purpose: development of a dual-purpose intrusion prevention system

Research methods: in general, these are simulation methods

A dual-purpose intrusion prevention system was modeled. Various methods of penetration determination have been implemented in the system and their operability has been tested.

The results of this work can be used both in the civilian part of the population and in the military. For the civilian population, this system can be used for buildings, such as protection against intrusion into your home. In turn, for the military part of the population, this system can be used to determine the location of the enemy.

Regarding further research, one of the possible directions may be to continue working with wireless sensor networks, namely to add a fire safety system.

Keywords: WIRELESS SENSOR NETWORK, PENETRATION, ZIGBEE, WI-FI, BLUETOOTH

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

IoT	Internet of Things
MCU	Microcontroller Unit
DHCP	Dynamic Host Configuration Protocol
IP	Internet Protocol
WSN	Wireless Sensor Network
Wi-Fi	Wireless Fidelity
SBC	Session Border Controller
БСМ	Бездротова Сенсорна Мережа
OSI	Open systems interconnection
TCP	Transmission control protocol
UDP	User datagram protocol
ATM	Automated teller machine
LAN	Local area network
xDSL	Digital subscriber line
VPN	Virtual private network
NGN	Next-generation network
SIP	Session initiation protocol

ВСТУП

Актуальність теми. Відчувати себе в безпеці - одна з базових потреб будь-якої людини. Дана система допоможе уникнути проникнення до будівлі, та повідомить про пожежу, тому що має детектор диму, після спрацювання якого ввімкнеться сирена, і надасть інформацію про небезпеку. Система може визначити «непроханого гостя» за гучністю, переміщенням, якщо той в свою чергу потрапить в зону дії системи.

Зараз коли в нашій країні проходять бойові дії, дана система може бути дуже корисною для військових нашої країни. За допомогою цієї системи можна відслідковувати рухи, звуки, дим і визначати місце знаходження ворога, також дивлячись яка частина системи спрацювала, можна більш точно визначити що це, чи певний транспорт, чи просто людина.

Мета і завдання дослідження. Метою даної дипломної роботи є моделювання та розроблення системи запобігання проникненню подвійного призначення.

Щоб досягнути даної мети потрібно було вирішити наведенні нище завдання:

1. Провести аналіз систем запобігання проникнення
2. Визначити датчики та адаптери які будуть використовуватися в даній системі та змоделювати систему
3. Розробити модель системи в Cisco Packet Tracer
4. Протестувати систему на коректну роботу та наявність помилок

Об’єкт дослідження: система запобігання проникнення в бездротових сенсорних мережах

Предмет дослідження: моделювання системи запобігання проникнення в бездротових сенсорних мережах

Методи дослідження: у даній дипломній роботі присутній метод імітаційного моделювання, що є одним із найголовнішим для моделювання системи запобігання проникненню подвійного призначення

1 АНАЛІЗ СИСТЕМ ЗАПОБІГАННЯ ПРОНИКНЕННЯ

1.1 Історія системи запобігання проникнення або охороної системи

Протягом усієї історії свого існування люди шукали способи, які б допомогли їм захистити себе і своє майно. Люди опанували зброю, приручили тварин, люди будували стіни та копали рови. І все ж, злодії, розбійники і загарбники, як і раніше, знаходили способи забиратися в чужі володіння, незважаючи на всі заходи безпеки.

Зрештою люди усвідомили, що клин клином вибивають, і для захисту свого майна почали використовувати інших людей - охоронців.

Першими охоронцями які з'явилися були вартові. Вперше таке поняття як охоронці з'явилося у Стародавньому Римі, у VI столітті. Охоронці, або вартові, мали назву "вігіли" і також ще були пожежниками Риму. Очевидно, судячи з їхніх обов'язків, саме їх можна віднести до перших в історії співробітників служб безпеки.

Незважаючи на те, що вігили служили, перш за все, пожежними, вони також мали обов'язки і поліцейських Риму. До їхніх обов'язків входило затримання злодіїв і грабіжників, також вони були відповідальні за забезпечення громадського порядку в цілому.

Багато років по тому, під час промислової революції, що відбувалася у світі наприкінці 1800-х років, стався «бум» на володіння власністю. В результаті збільшилася кількість людей, яким для захисту життя та цінного майна були потрібні наймані особисті охоронці. Проте, найм охоронців був недешевим задоволенням і, здебільшого, дозволити собі таку розкіш могли лише дуже багаті люди.

Сьогодні у всіх країнах світу охоронці зустрічаються набагато частіше. Безперечно, забезпеченням своєї безпеки стурбовані знаменитості, спортсмени та політики, однак, принаймні, одного охоронця сьогодні також

можна побачити практично у будь-якій великій компанії чи магазині роздрібної торгівлі.

Охоронці - ефективне, але, звичайно, далеко не найпрактичніше рішення для захисту майна, свого здоров'я та здоров'я членів твоєї сім'ї, безсумнівно, домовласникам було потрібне більш доступне рішення щодо забезпечення безпеки.

На щастя, в 1853 винахідник на ім'я Августус Поуп запатентував першу електромагнітну систему сигналізації, проклавши шлях для домашніх систем безпеки, які ми знаємо сьогодні.

В кінці 1990х – на початку 2000х рр. все більшої популярності набували бездротові охороні системи.

На початку 2000х популярності набрав спосіб передачі сигналу від охороної системи через GSM-мережі.

На початку 2010х найбільш передові комплекси отримали можливість інтеграції з хмарними технологіями і віддаленого доступу і керування за допомогою мережі Internet.

1.2 Види систем запобігання проникнення

Налічують багато систем запобігання проникнення. Наприклад:

- Системи охороної сигналізації
- Системи пожежної сигналізації
- Системи відеоспостереження
- Системи захисту периметру
- Системи інформаційної безпеки

Кожна система запобігання проникненню важлива по своєму, але хотілось би відмітити систему інформаційної безпеки, тому що з кожним

днем світ все більше оцифровується, тому безпека в мережі набуває дуже великої популярності, і є дуже корисною для сучасної людини.

1.3 Склад елементів які можуть використовуватися в системах

В системах запобігання проникнення можуть бути присутні ті чи інші елементи, тому нижче наведено список датчиків, адаптерів і т.п., які можуть використовуватись в тих чи інших системах запобігання проникнення:

- Датчики руху, удару, диму і тд.
- Звуковий оповіщувач
- Світловий оповіщувач
- Відеокамера, відеореєстратори
- Керуючий сервер
- Генератори охороного диму
- Виконуючі пристрої
- Різні типи плат для програмування датчиків, сенсорів і тп.

1.4 Класифікація систем запобігання проникнення

Системи запобігання проникненню класифікують на наступні:
за взаємодією із загрозою безпеці та за способом передачі інформації

- **Системи за взаємодією із загрозою безпеці**

Системи за взаємодією із загрозою бувають активні та пасивні.

Активні системи – це системи які призначені для запобігання проникнення в об’єкт що охороняється.

Пасивні системи – це комплекс засобів і дій, спрямованих на залучення уваги власника майна або ж охоронних служб.

Активні сигналізації мають підключенні сирени, проблискові маячки, їх спрацювання може налякати зловмисника і змусити його втікти. Ще одне призначення такої сигналізації – привернути увагу людей, найчастіше сусідів. Якщо будинок знаходиться наприклад в селі і іншого житла поблизу немає або коли сусіди є але вважають за краще не втручатися в чужі проблеми, то доводиться покладатися лише на психологічний фактор злочинця. Гучний звук сирени і яскраві спалахи світла можуть викликати відчутний фізичний, а не тільки психологічний дискомфорт. Але якщо грабіжник виявиться не сором'язливим, з міцними нервами, до того ж з навушниками та окулярами, а на допомогу прийти нікому, сигналізація не виконає свого призначення.

Активні системи використовуються для привернення уваги до будівлі. Наприклад, коли в дім вламується зловмисник, система його помічає і вмикає сирену, проблискові маячки, та все що привертає увагу, та є у системі, і тоді тяжко буде не замітити такий дім, квартиру чи магазин.

Також варто зазначити, що для організації активних систем потрібно керуватися діючим законодавством країни. Тобто, якщо зловмисник отримає шкоду для здоров'я, то піде судовий процес, і це все може призвести до кримінальної відповідальності.

В свою чергу пасивні системи працюють по іншому. Вони реагують на зловмисника зовсім по іншому. Коли злодій проникає до будівлі то не буде чути ніяких сирен, проблискових маячків і тп., проте система відправить тривожне повідомлення зацікавленим особам, які повинні негайно виїхати на об'єкт і/або зателефонувати до поліції. Якщо вчасно прибути до місця призначення то можна затримати злодія на гарячому.

- **Системи за способом передачі інформації**

За способом передачі інформації існують такі системи:

- Дротові

- Аналогові
- Адресні

- Бездротові
  - Без попереднього зв’язку
  - З попереднім зв’язком
- Передача інформації відбувається по GMS – мережі
- Передача інформації відбувається по протоколам Wi-Fi

Дротові – зазвичай, рішення про встановлення даного виду системи приймається на етапі будівництва будинку. Дротові системи вважаються надійнішими, тому що важче порушити їхню роботу. Але їх встановлення вимагає втручання в конструкцію будівлі, тому краще запланувати її на етапі будівництва будинку чи квартири, або зробити це з нагоди поновлення фасаду.

Бездротові охоронні системи не вимагають проведення будівельних робіт, однак, передові рішення хорошої якості такого роду є дорожчими, ніж провідна версія. У такій системі не потрібне дротове підключення. Плюси бездротового підключення:

- Установка сигналізації дуже проста та швидка, що робить її привабливою для вже готових будинків.
- Можливість встановлення таких охоронних систем для приватного будинку своїми руками додатково знижує вартість такого рішення.
- Блок управління пов'язаний з невеликими датчиками руху в приміщеннях і так званими контакторами, розташованими на дверях і вікнах.
- Обслуговування системи просте – для віддаленого керування використовується пульт дистанційного керування, за допомогою якого можна ввімкнути або вимкнути сигналізацію за допомогою індивідуального коду.

- ❖ Розміщення додаткових контролерів у різних місцях будинку полегшує активацію сигналу тривоги у разі потреби.

Зазвичай бездротові системи використовуються, коли немає можливості зробити дротову систему. Також спеціалісти рекомендують комбінувати пасивні системи з активними та бездротові з дротовими.

Передача інформації відбувається по GMS – мережі – використовується як сигнал тривоги який передається на пульт охороної компанії, так і як сигнал який інформує власника об’єкта який охороняється. Також власник може отримувати різну інформації про різні події, такі як: тривога, пожежа, несправність і т.д. у вигляді повідомлення на свій мобільний пристрій. Для цього використовуються GSM-комунікатори.

Передача інформації відбувається по протоколам Wi-Fi – чимось схоже на попередній варіант з передачею інформації по GMS. Доступ користувача здійснюється за допомогою Internet, наприклад: Web сторінка, портал. Але найчастіше це відбувається зо допомогою мобільного додатку (Apple IOS, Android).

2. АНАЛІЗ ОСНОВНИХ ТЕХНОЛОГІЧНИХ ЕЛЕМЕНТІВ СИСТЕМ ЗАПОБІГАННЯ

2.1 Елементи які використовуються в системі

В системі використовуються такі елементи як: мережевий комутатор, детектор диму, сирена, вебкамера, детектор руху, датчик відключення, звуковий сенсор, SBC та MCU контролери. Більше про кожен елемент який наведений вище буде описано в наступних підпунктах.

2.1.1 Мережевий комутатор

Мережевий комутатор (Home Gateway) – це пристрій, призначений для об'єднання двох мереж (передачі між ними трафіку користувача), які мають різні характеристики, використовують різні протоколи або технології. Gateway може працювати на будь-якому із 7 рівнів моделі взаємодії відкритих систем (OSI). Сполучні мережі можуть мати різні швидкості передачі, затримки, процедури безпеки. Крім того можуть використовуватися різні протоколи (TCP та UDP), технології (ATM та Ethernet) і навіть середовища передачі (оптичне волокно). Також знайшли широке застосування повністю бездротові комутатори, які, наприклад, можуть використовувати технологію WiFi на рівні доступу, а для зв'язку із зовнішніми мережами – стільникові системи зв'язку.

Одним із найпоширеніших способів застосування Gateway є забезпечення доступу з локальної мережі (LAN) у зовнішню мережу, наприклад, Інтернет. При цьому в LAN може використовуватися одна технологія, а в зовнішньому з'єднанні інша: Ethernet - xDSL, PDH - Ethernet,

SDH - ATM і т.п. Також комутатор може виконувати завдання брандмауера, бути точкою початку VPN або бути сервером автентифікації.

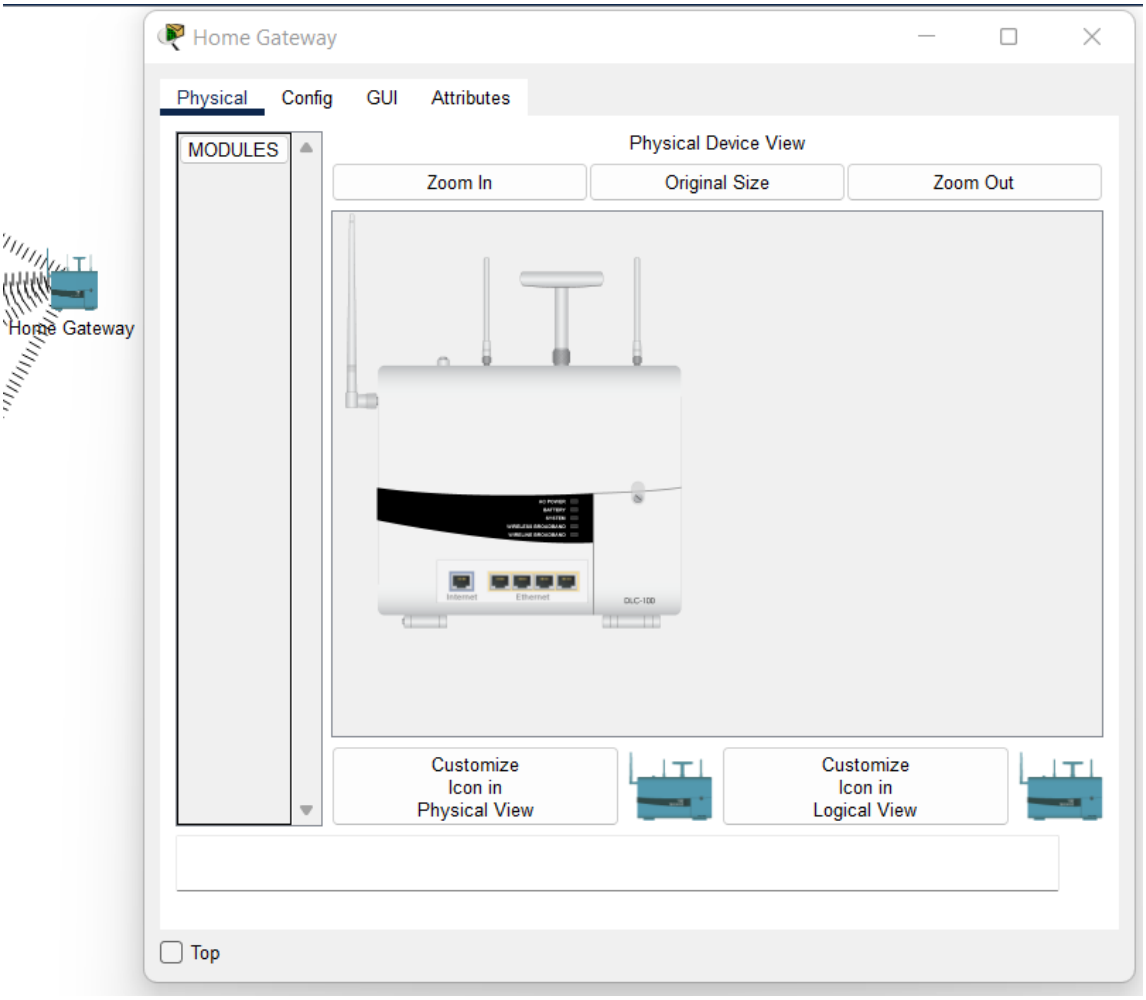

Рисунок 2.1 – Мережевий комутатор в Cisco Packet Tracer

2.1.2 Детектор диму

Датчик диму - пристрій, встановлений на об'єкті, функціонал якого налаштований на виявлення та сповіщення про початок розповсюдження диму, що дозволяє вчасно запобігти спалаху, оскільки пожежа починається з задимлення з поширенням полум'я та підвищенням температур.

При загорянні в приміщенні концентрація диму піднімається вгору, для чого датчик завжди розміщується на стелі і принцип роботи досить простий. Конструктивно складається з корпусу, плати та оптичної системи, до якої

входить світлодіод та фотоелемент. Світлодіод випромінює спрямований в одному положенні в бік від фотоелемента промінь, таким чином у разі появи диму в приміщенні, в корпусі датчика починають відображатися світлові промені в різні боки, при попаданні на фотоелемент він спрацьовує, це контролює електронна схема і передає сигнал каналами зв'язку на централь. На рисунку 2.2 зображено детектор диму

Рисунок 2.2 – детектор диму в Cisco Packet Tracer

2.1.3 Сирена

Принцип роботи пристрою дуже простий, при цьому обладнання добре справляється із захистом майна в період відсутності господарів будинку. Сирена є невід'ємною частиною систем запобігання проникненню, сигналізації, що встановлюється на приватні будинки, квартири, виробничі об'єкти, офіси, автомобілі. Існують різні сирени, що відрізняються за принципом спрацьовування, звуковим сигналом та іншими параметрами. Варто зауважити, що сама сирена не захищає, вона тільки сповіщає про небезпеку в будівлі чи в іншому місці. Сирена зображена на рисунку 2.3

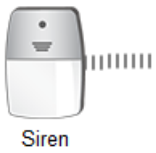

Рисунок 2.3 – сирена в Cisco Packet Tracer

2.1.4 Вебкамера

Об'єктив фокусує зображення на матриці. Матриця перетворює колір на електричний сигнал. Сигнал надходить на процесор для обробки кольоровості, яскравості та іншого. Відеопотік надходить на компресор. Компресор стискає потік – тепер дані готові до передачі до мережі через Ethernet-контролер.

Кожна IP-камера має власну IP-адресу, що передається з підключенням і використовується для синхронізації камери з реєстратором: за допомогою команди або спеціальної програми реєстратор використовує IP-адресу камери і підключається по ньому. Без IP-адреси неможливо налаштувати обладнання на спільну роботу, отримати доступ до IP-камери з мобільного пристрою чи SBC контролера.

Завдяки цифровій начинці функціонал IP-камери прагне незкінечності за рахунок різноманітності програмного забезпечення, а отримати доступ до даних можна з будь-якої віддаленої точки планети, де є інтернет.

Рисунок 2.4 – веб-камера в Cisco Packet Tracer

2.1.5 Детектор руху

Датчики руху призначені для розпізнавання переміщення у заданій області та подальшої передачі даних про зафіксовану подію на виконавчий пристрій. Основною сферою їхньої дії є системи охоронної сигналізації. Де датчики руху здійснюють спостереження за територією, будинками, спорудами, приміщеннями та іншими об'єктами. Крім охоронних систем їх

встановлюють для комутації систем освітлення, виконання контролю доступу до певних приміщень або їх частин.

Всі бездротові датчики руху, залежно від їхнього ступеня захищеності від впливу зовнішніх факторів поділяються на сенсори зовнішньої та внутрішньої установки. Визначальним фактором якої є ступінь пилу-вологозахищеності, що позначається індексом IP і двома цифрами. Відповідно до розділів 5 та 6 ГОСТ 14254-2015 цифрові показники варіюються від 0 до 6 для пилостійкості та від 0 до 9 для вологостійкості. Чим більше значення, тим більше агресивних умовах зможе працювати датчик руху.

Залежно від принципу виявлення предмета, що переміщається, бездротові датчики руху можуть бути пасивними, активними і комбінованими. Пасивні рецептори спрямовані на власні випромінювання людського тіла, їх зіставлення зі станом навколишнього простору. Для активних закономірна власна генерація імпульсів у контрольовану область та подальший вимір цього ж випромінювання у прямому або відбитому спектрі. Комбіновані моделі поєднують принципи і активних та пасивних пристроїв. В Cisco Packet Tracer детектор руху виглядає так, як показано на рисунку 2.5

Рисунок 2.5 – детектор руху в Cisco Packet Tracer

2.1.6 Датчик відключення (інфрачервоний датчик)

Інфрачервоні датчики реагують на переміщення в полі їх огляду об'єктів, що випромінюють тепло, – насамперед людей та тварин. Вони

пасивні, тобто самі нічого не випромінюють, лише фіксують теплове випромінювання. Працюють інфрачервоні датчики в зоні прямої видимості, тобто якщо між об'єктом та датчиком немає перешкод. При цьому вони досить чутливі навіть до незначних змін температури, що дозволяє виконувати точне налаштування.

З іншого боку, ці особливості обмежують сферу застосування інфрачервоних датчиків. Щоб уникнути помилкових спрацьовувань, їх не рекомендується встановлювати в зоні дії джерел тепла: опалювальних приладів, теплових завіс, кондиціонерів, інфрачервоних обігрівачів, у цехах підприємств, поблизу потужних джерел освітлення, наприклад, галогенних ламп та ін. Крім того, чутливість інфрачервоних датчиків залежить від навколишнього середовища, але на вулиці їх точність знижується. Типова сфера їх застосування – житлові будинки, громадські, офісні та підсобні приміщення, теплі склади, фойє, холи, під'їзди, сходові клітки тощо.

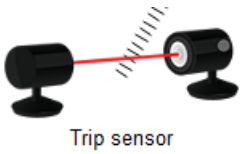

Рисунок 2.6 – Датчик відключення в Cisco Packet Tracer

2.1.7 Звуковий сенсор

Датчик звуку визначається як модуль, який виявляє звукові хвилі за їх інтенсивністю та перетворює їх в електричні сигнали.

Датчик розпізнавання звуку працює так само, як і наші вуха, маючи діафрагму, яка перетворює вібрацію в сигнали. Однак, відрізняється тим, що звуковий датчик складається з вбудованого ємнісного мікрофона, пікового детектора та підсилювача (LM386, LM393 тощо), який дуже чутливий до звуку.

Завдяки цим компонентам датчик може опрацьовувати:

- Звукові хвилі, які поширюються через молекули повітря
- Такі звукові хвилі, які викликають вібрування діафрагми мікрофона, що призводить до зміни ємності
- Зміну ємності яка потім посилюється і оцифровується для обробки інтенсивності звуку

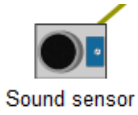

Рисунок 2.7 – звуковий сенсор в Cisco Packet Tracer

2.1.8 SBC

Session Border Controller (SBC) – це обладнання операторського класу, яке широко використовується при побудові мереж NGN. Прикордонний контролер сесій встановлюється на межі мережі оператора і є єдиною точкою входу-виходу в «домашню» мережу, завдяки чому ховається її топологія, підвищується надійність і стійкість до відмови, спрощуються завдання конфігурування та адміністрування. SBC вирішує цілу низку завдань, пов'язаних з доступом і пакетною комутацією, з керуванням викликами, щоб знизити навантаження з елементів усередині домашньої мережі оператора. Особливе значення SBC має у мережах сервіс-провайдерів управління SIP-трафіком. У цьому випадку він здійснює взаємодію різнорідного VoIP-обладнання, підтримку транскодування та реалізацію деяких функцій, які зазвичай не вирішують брандмауери та маршрутизатори.

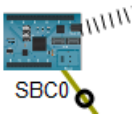

Рисунок 2.8 - SBC в Cisco Packet Tracer

2.1.9 MCU

MCU – Multipoint Control Unit, відповідає за контроль медіа потоків. Підмережа MCU визначає налаштування інтерфейсів MCU для прийому та відправки медіа від/до Оператора, дозволяє обмежувати кількість одночасних аудіо/відеосесій. На наступному рисунку буде зображено MCU controller в Cisco Packet Tracer.

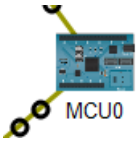

Рисунок 2.9 - MCU в Cisco Packet Tracer

3 ПОБУДОВА МОДЕЛІ ТА ЕКСПЕРИМЕНТИ

3.1 Встановлення детектора диму та сирени використовуючи мережевий комутатор за допомогою безпровідного підключення

В першу чергу відкриємо програму Cisco Packet Tracer та виберемо необхідні елементи: детектор диму, сирену та Home Gateway на панелі Devices. З'єднання відбувається за допомогою бездротового підключення

Рисунок 3.1 – Панель знаків

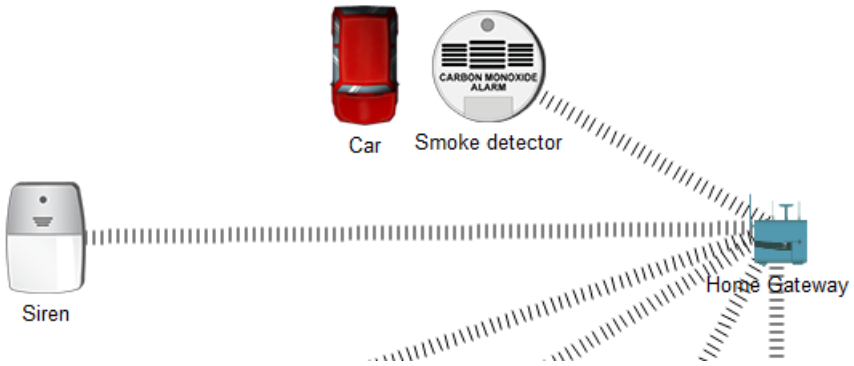

Рисунок 3.2 – Зображення мережі з безпровідним підключенням

На рисунку 3.2 також зображено автомобіль. Він слугує для того, щоб перевіряти систему на працездатність. Тобто коли заводиться автомобіль, він виділяє дим, а детектор диму в свою чергу показує рівень забруднення, і коли рівень забруднення перевищує заданий, то спрацьовує сирена.

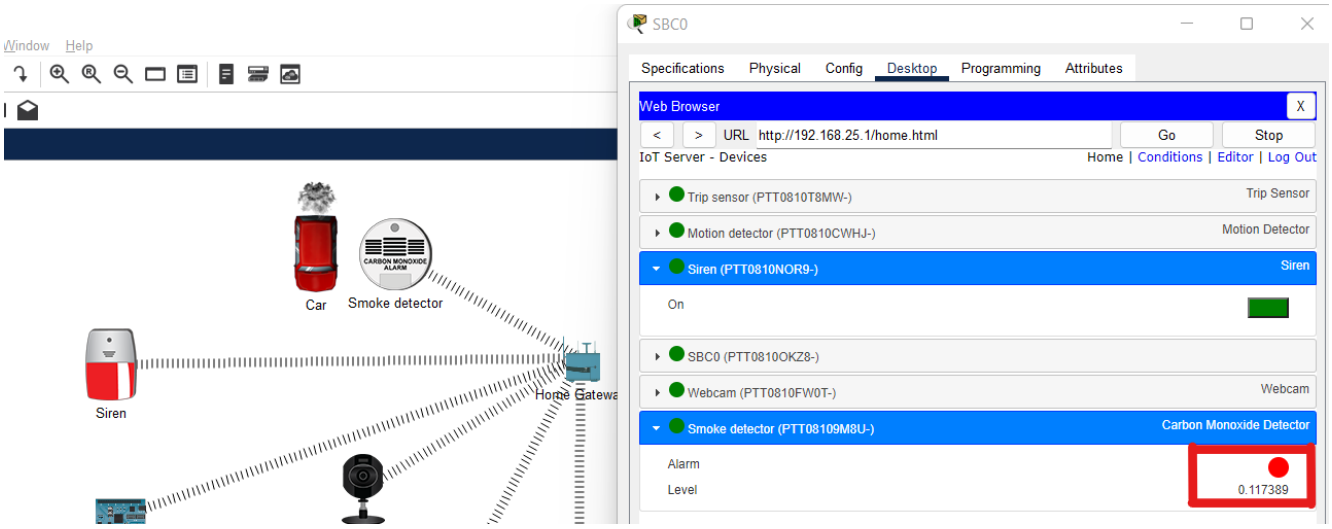

Рисунок 3.3 – Демонстрація роботи детектора диму

Actions		Enabled	Name	Condition	Actions
Edit	Remove	Yes	smoke1	Smoke detector Level >= 0.1	Set Siren On to true
Edit	Remove	Yes	smoke2	Smoke detector Level <= 0.1	Set Siren On to false

Рисунок 3.4 – Правила для детектора диму

3.2 Встановлення датчика відключення та веб-камери використовуючи мережевий комутатор, та під'єднання за допомогою безпровідного підключення

Наступним кроком буде встановлення датчика відключення(інфрачервоний датчик), веб-камери та під'єднання цих елементів до вже існуючого Home Gateway бездротовим з'єднанням

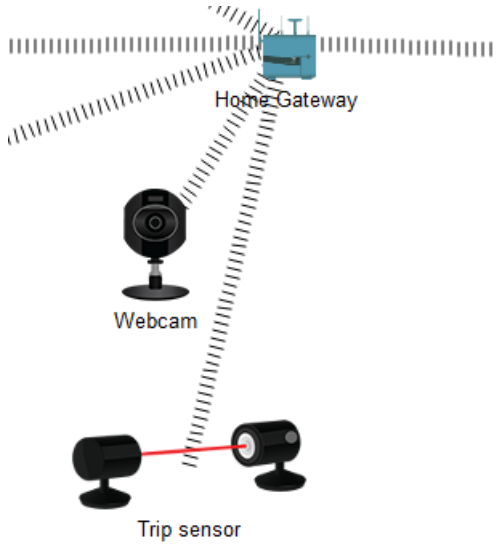

Рисунок 3.5 – Встановленні датчик відключення та веб-камера

Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	trip1	Trip sensor On is true	Set Webcam On to true
Edit Remove	Yes	trip2	Trip sensor On is false	Set Webcam On to false

Рисунок 3.6 – правила для датчика відключення

Даний датчик працює наступним чином, коли людина, транспорт і т.д. перетинають промінь який належить датчику відключення, передається сигнал через мережевий комутатор до веб-камери, і остання в свою чергу вмикається і фіксує того хто перетнув промінь датчика відключення, та передає дані.

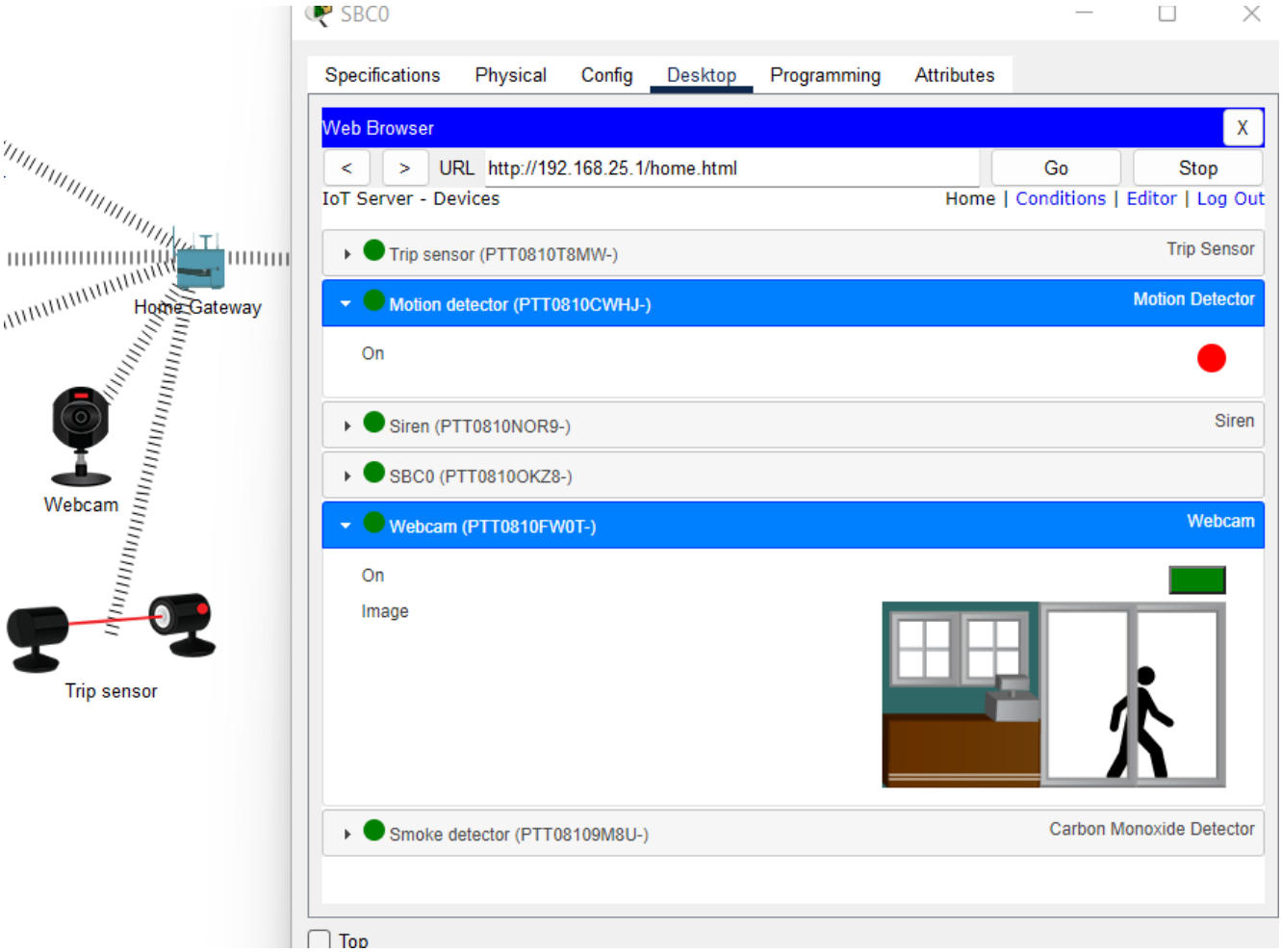

Рисунок 3.7 – Демонстрація роботи датчика відключення

Тобто, коли було проведено курсором миші через промінь датчика, ввімкнулась веб-камера і почала фіксувати порушення.

3.3 Додання детектора рухів до вже існуючої системи та з'єднання його з цією ж системою за допомогою безпровідного підключення

На панелі інструментів обираємо даний детектор і переміщуємо його до робочого середовища

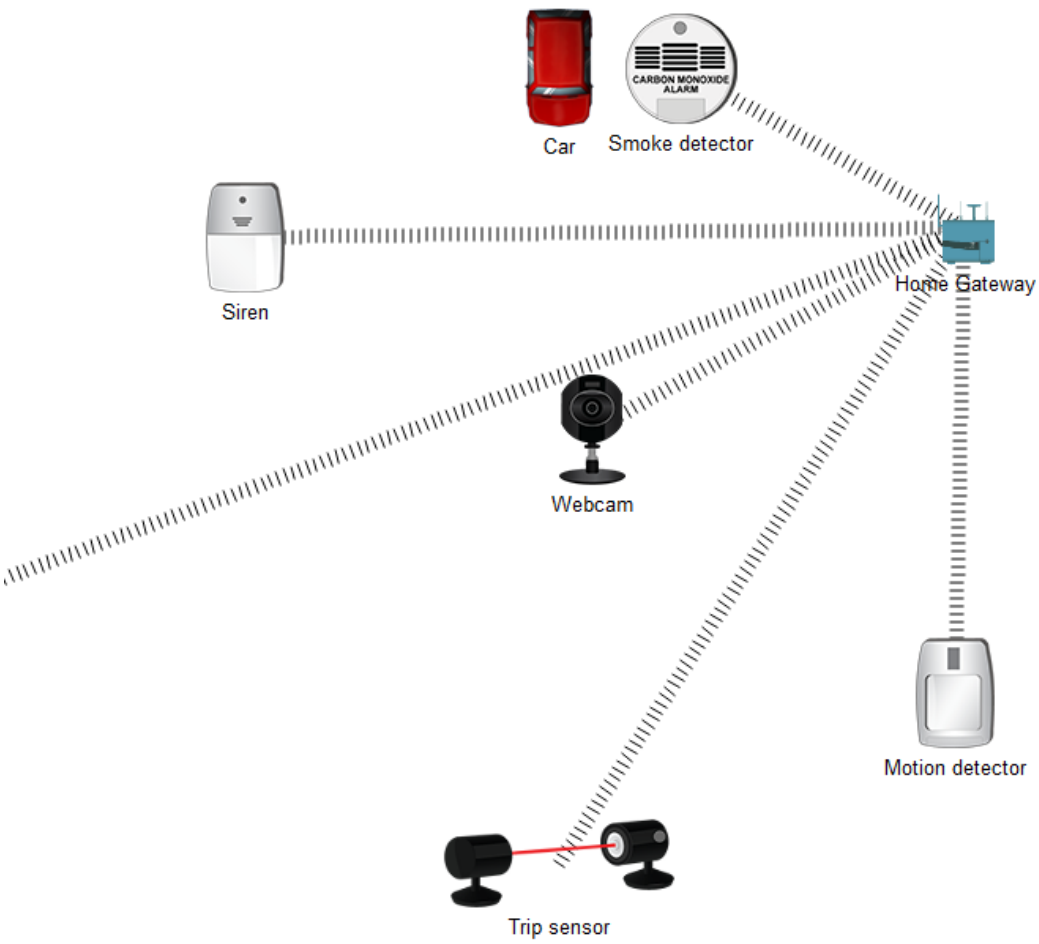

Рисунок 3.8 – вигляд системи з доданим детектором руху

Даний детектор в системі працює наступним чином. При фіксуванні перешкоди детектором, даний елемент вмикає сирену.

Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	motion1	Motion detector On is true	Set Siren On to true
Edit Remove	Yes	motion2	Motion detector On is false	Set Siren On to false

Рисунок 3.9 – правила для роботи детектора руху

На рисунку 3.10 конкретно зображена робота детектора руху

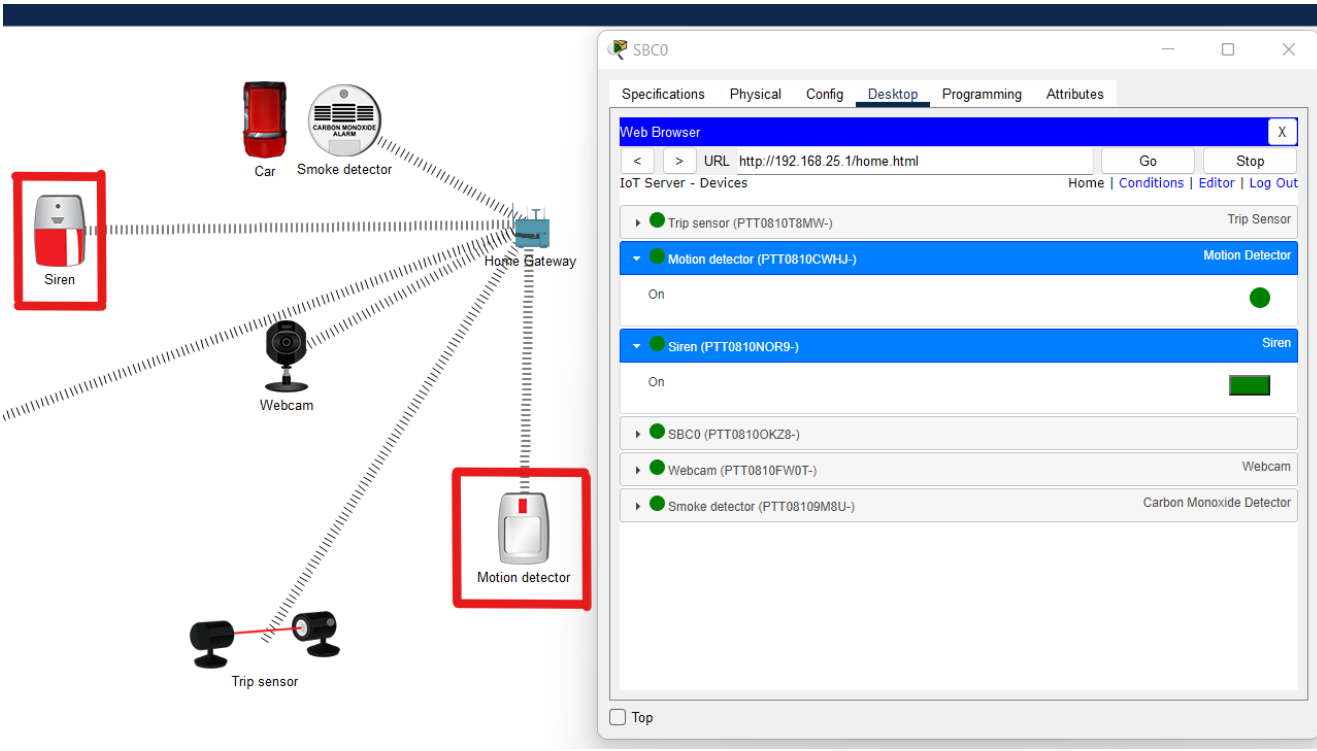

Рисунок 3.10 – демонстрація роботи детектора руху

Отже, при ввімкненому детектору руху який засік перешкоду, спрацьовує сирена.

3.4 Додання звукового сенсору, MCU плати до вже існуючої системи та з'єднання плати використовуючи бездротове з'єднання, а плату з сенсором – за допомогою нестандартного кабелю інтернет речей (IoT custom cable)

На наступному рисунки можна побачити як виглядає система з підключенням звукового сенсору.

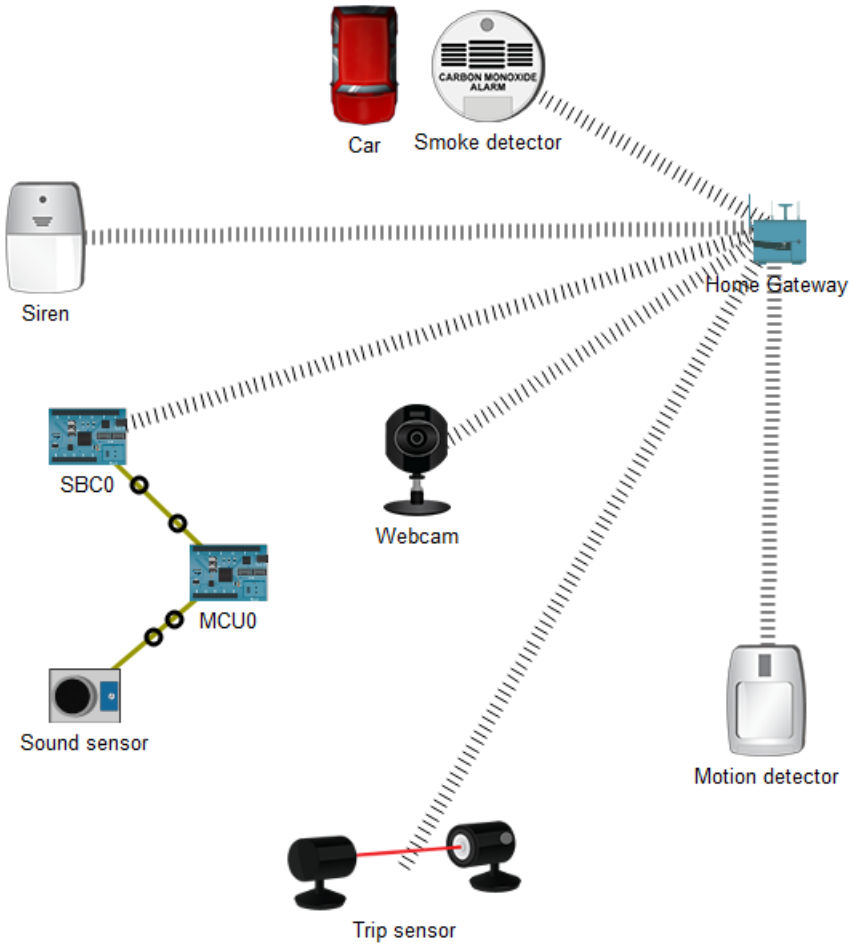

Рисунок 3.11 – вигляд системи після додання звукового сенсору

Для коректної роботи звукового сенсору його потрібно запрограмувати. Код програми для роботи сенсору зображений на рисунку нижче.

Рисунок 3.12 – код програми для роботи звукового сенсора

3.4 SBC контролер, як елемент який керує всім процесом

В попередніх підпунктах даного розділу можна було замітити SBC контролер, про якого не було сказано нічого, хоча це настільки важлива річ в системі, що було вирішено винести його в окремий підпункт.

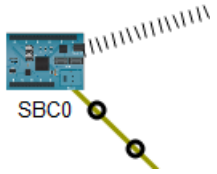

Рисунок 3.13 – вигляд SBC контролера в Cisco Packet Tracer

За допомогою даного контролера можна керувати всією системою. Саме в цьому контролері прописані всі правила для інших датчиків.

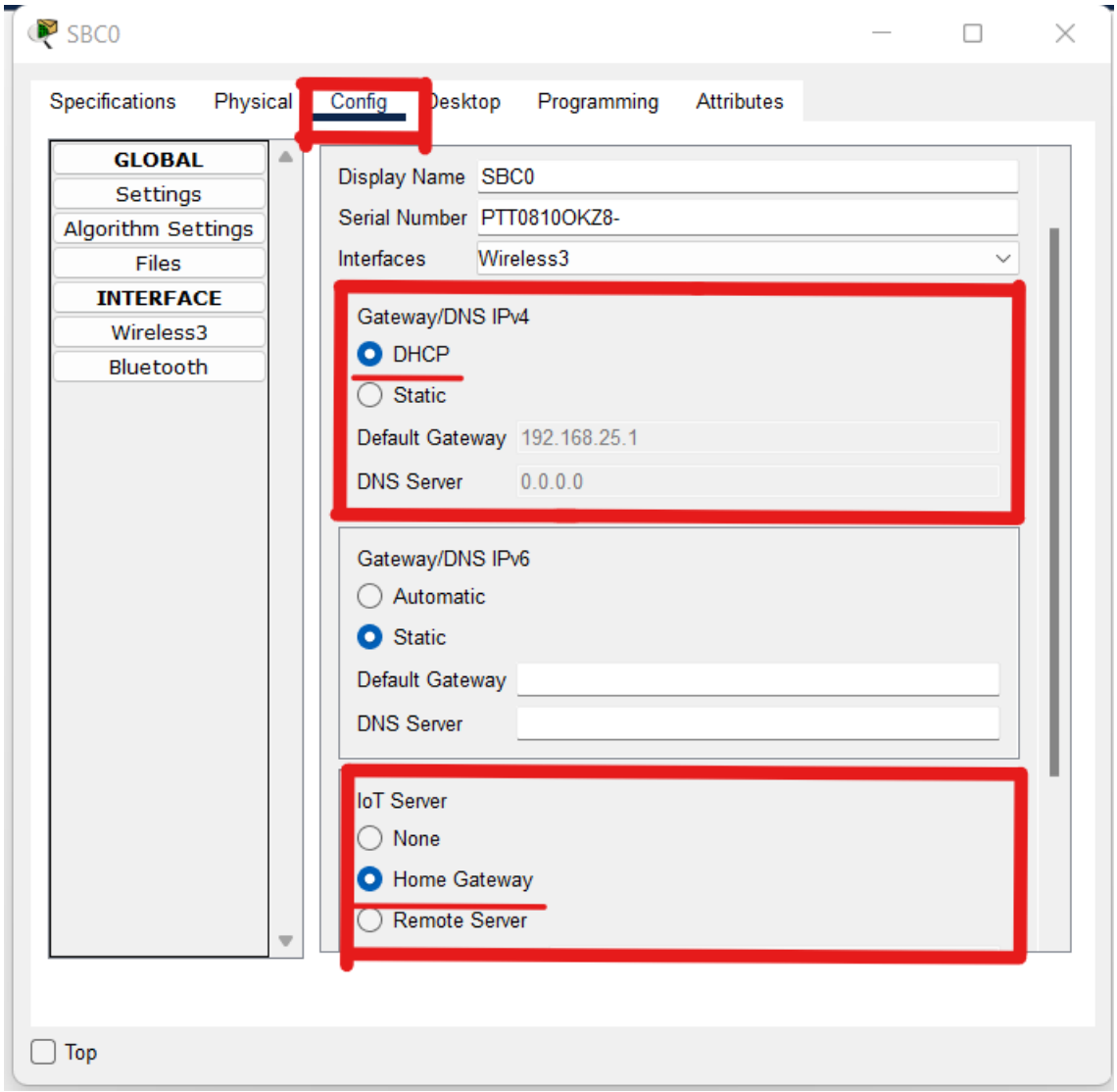

Рисунок 3.14 – налаштування під’єднання SBC контролера до Home Gateway бездротовим з’єднанням

На рисунку 3.14 зображенно налаштування SBC контролера для його бездротового підключення до Home Gateway. Відкриваючи SBC контролер в Cisco Packet Tracer потрібно перейти на вкладку «Config» і обрати в пунктах «Gateway/DNS IPv4» і «IoT Server» «DHCP» та «Home Gateway» відповідно. Всі ці дії зображено на рисунку вище. Тоді зв'явиться бездротове підключення між SBC контролером та Home Gateway.

Щоб перейти на сторінку з якої можна безпосередньо керувати системою потрібно перейти до вкладки «Desktop» та обрати «Web Browser». Детальніше на рисунку 3.15.

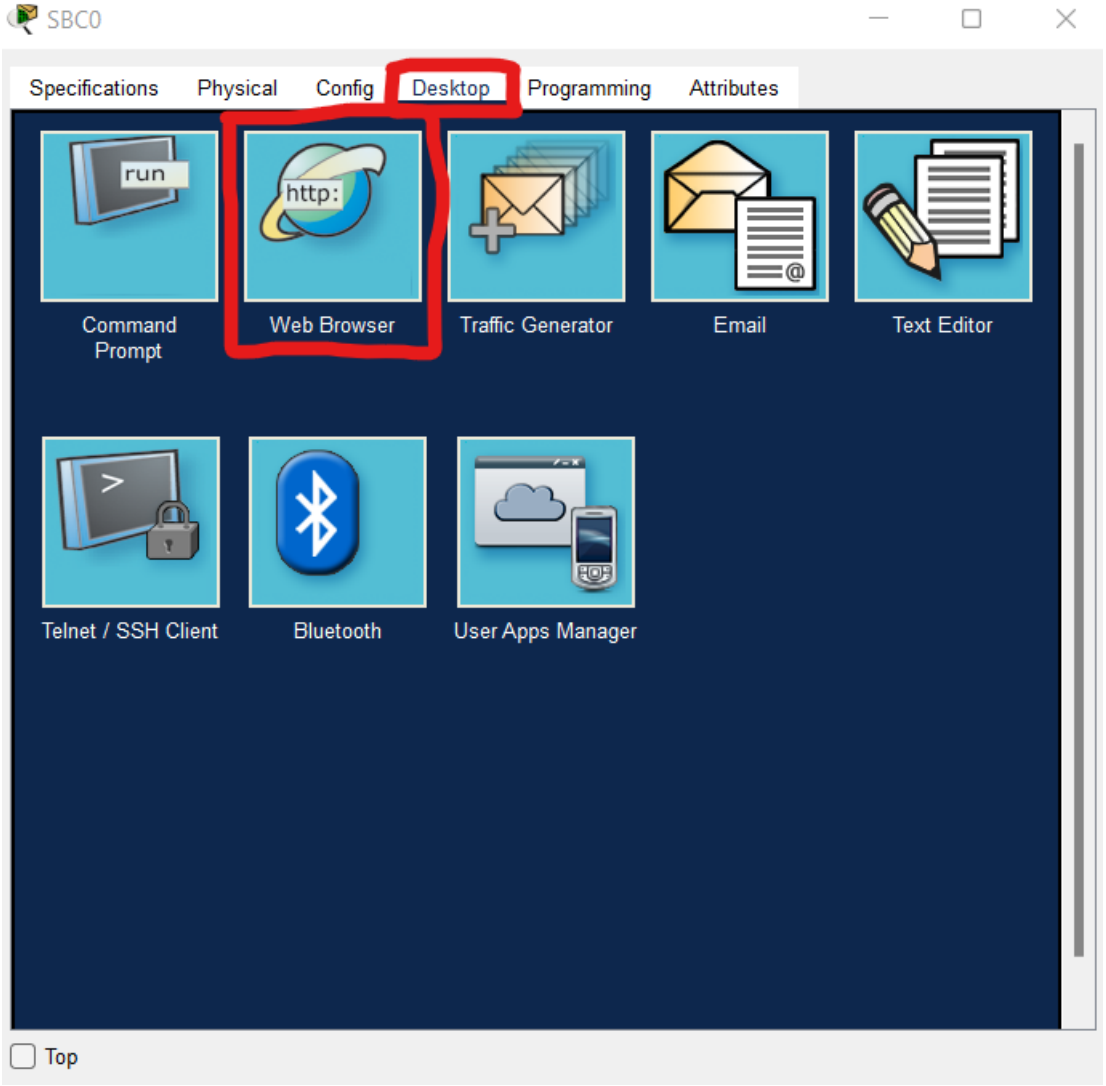

Рисунок 3.15 – перехід до сторінки з якої можна керувати системою

Після цього потрібно ввести адресу сторінки з якої здійснюється керування

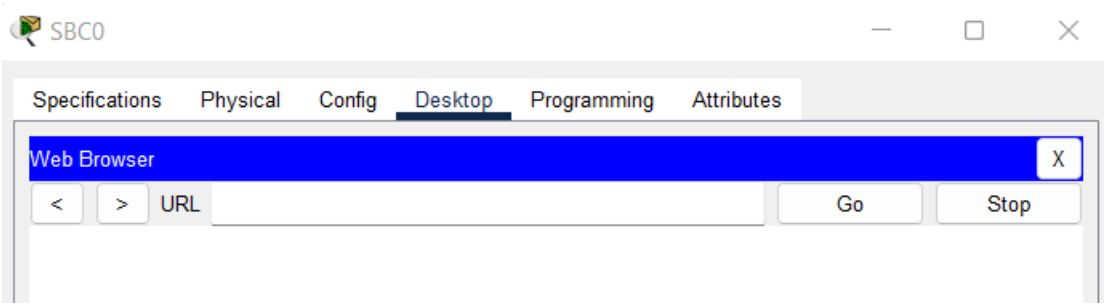

Рисунок 3.16 – поле в яке потрібно ввести адресу сторінки

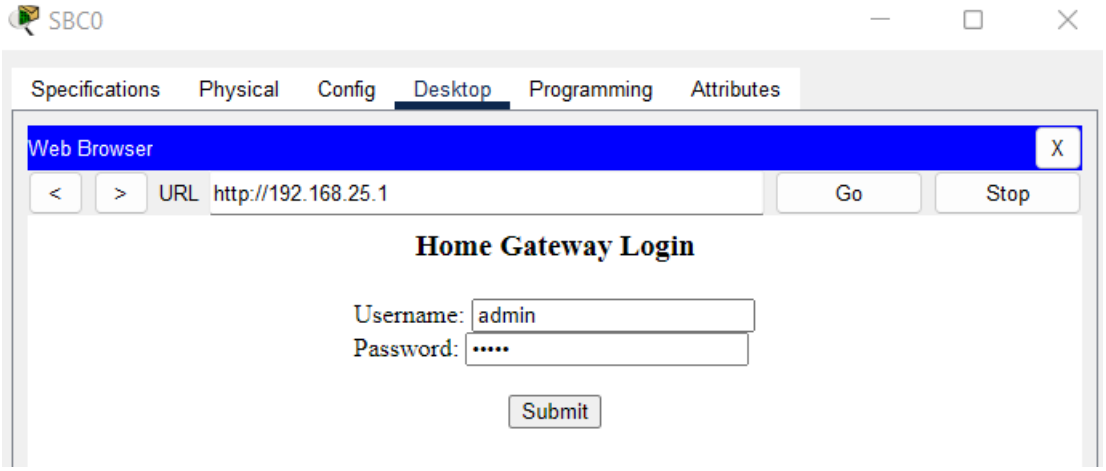

Рисунок 3.17 – введення логіну та паролю для переходу на сторінку

На рисунку 3.17 зображено введення паролю та логіну після переходу по адресі 192.168.25.1. Після авторизації ми отримаємо доступ до керування системою запобігання проникнення.

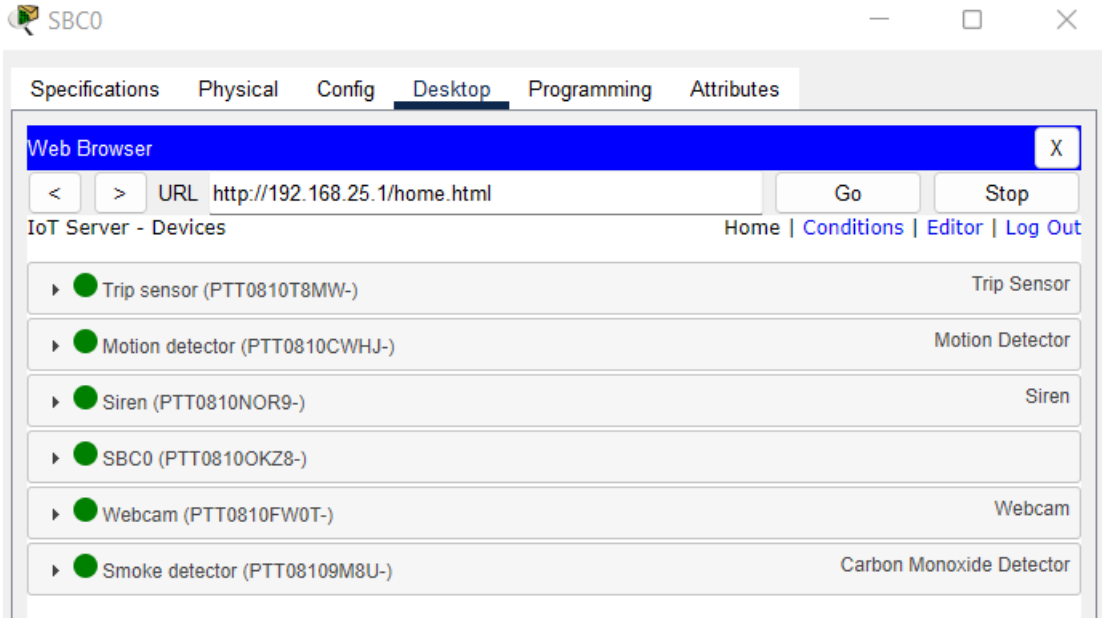

Рисунок 3.18 – головна сторінка управління системою з SBC контролера

У вкладці «Conditions» прописуються правила для роботи датчиків

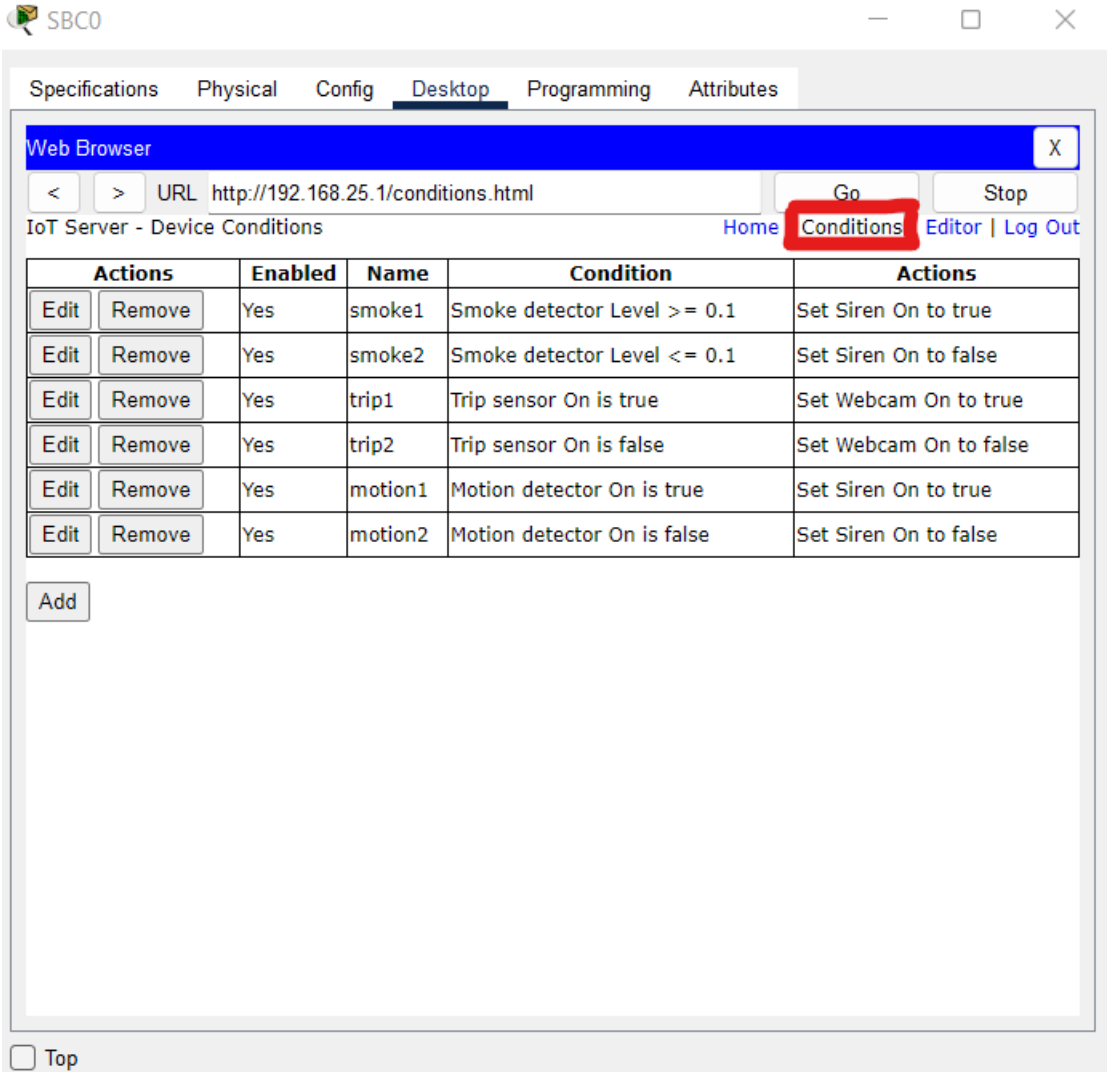

Рисунок 3.19 – всі прописані правила до датчиків для роботи системи

Отже, SBC контроллер є одним із найголовніших елементів системи, тому що завдяки йому здійснюється керування цією системою.

3.6 Для коректної роботи системи перевіримо правильність з’єднання всіх елементів

Для того щоб підключити всі датчики бездротовим з’єднанням потрібно їх налаштувати(всі окрім звукового сенсора, тому що даний сенсор під’єднується фізично). У всіх датчиків підключення схоже, тому буде продемонстровано все на детекторі руху.

Для початку вікдкриємо налаштування датчика, і перейдемо в розширенні налаштування як зображенно на рисунку 3.20

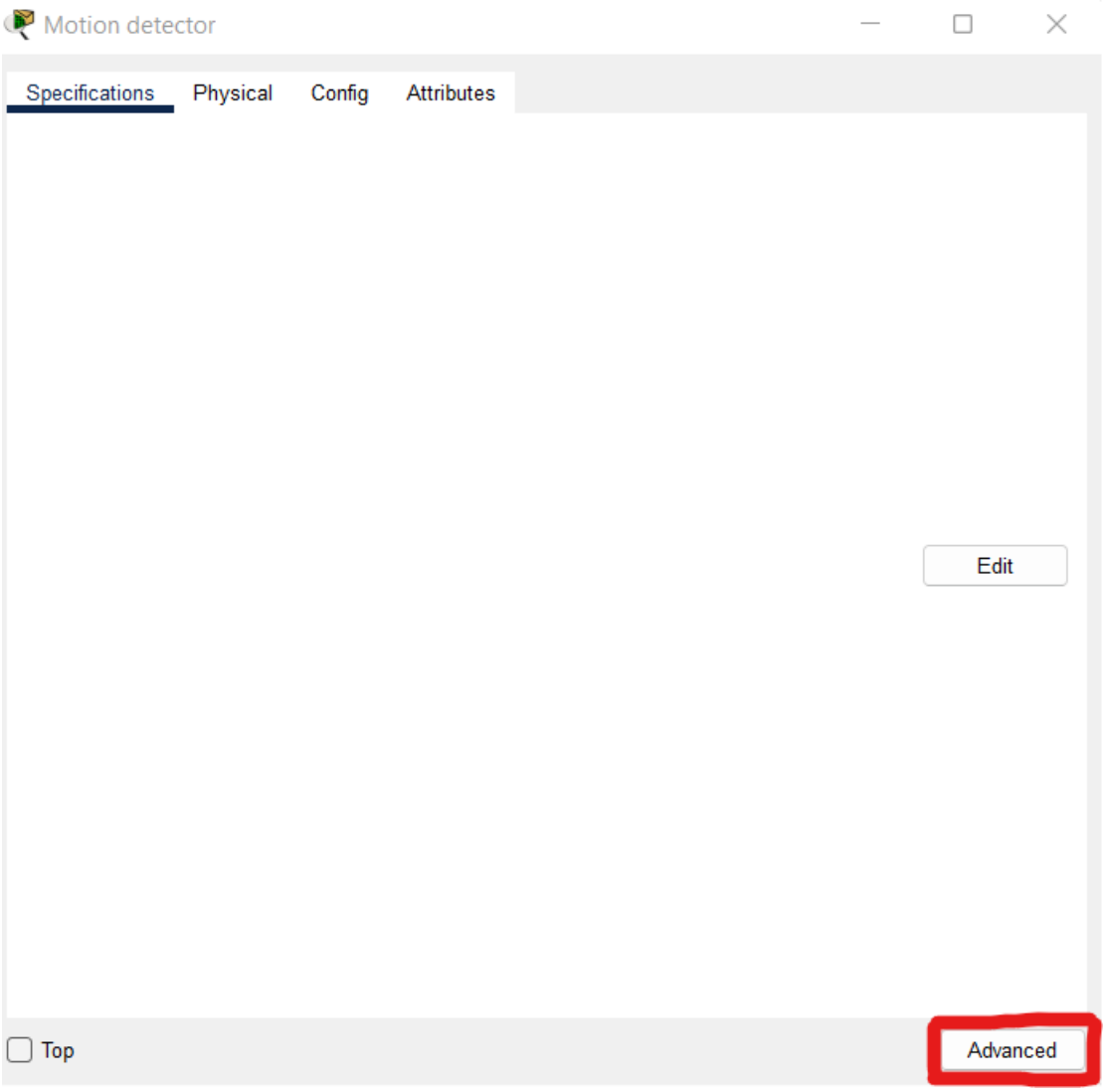

Рисунок 3.20 – відкриття розширених налаштувань

Після ввімкнення розширених налаштувань переходимо до вкладки «I/O Config», де в рядку «Network Adapter» обираємо «PT-IOT-NM-1W». На рисунку нижче буде продемонстровано графічно.

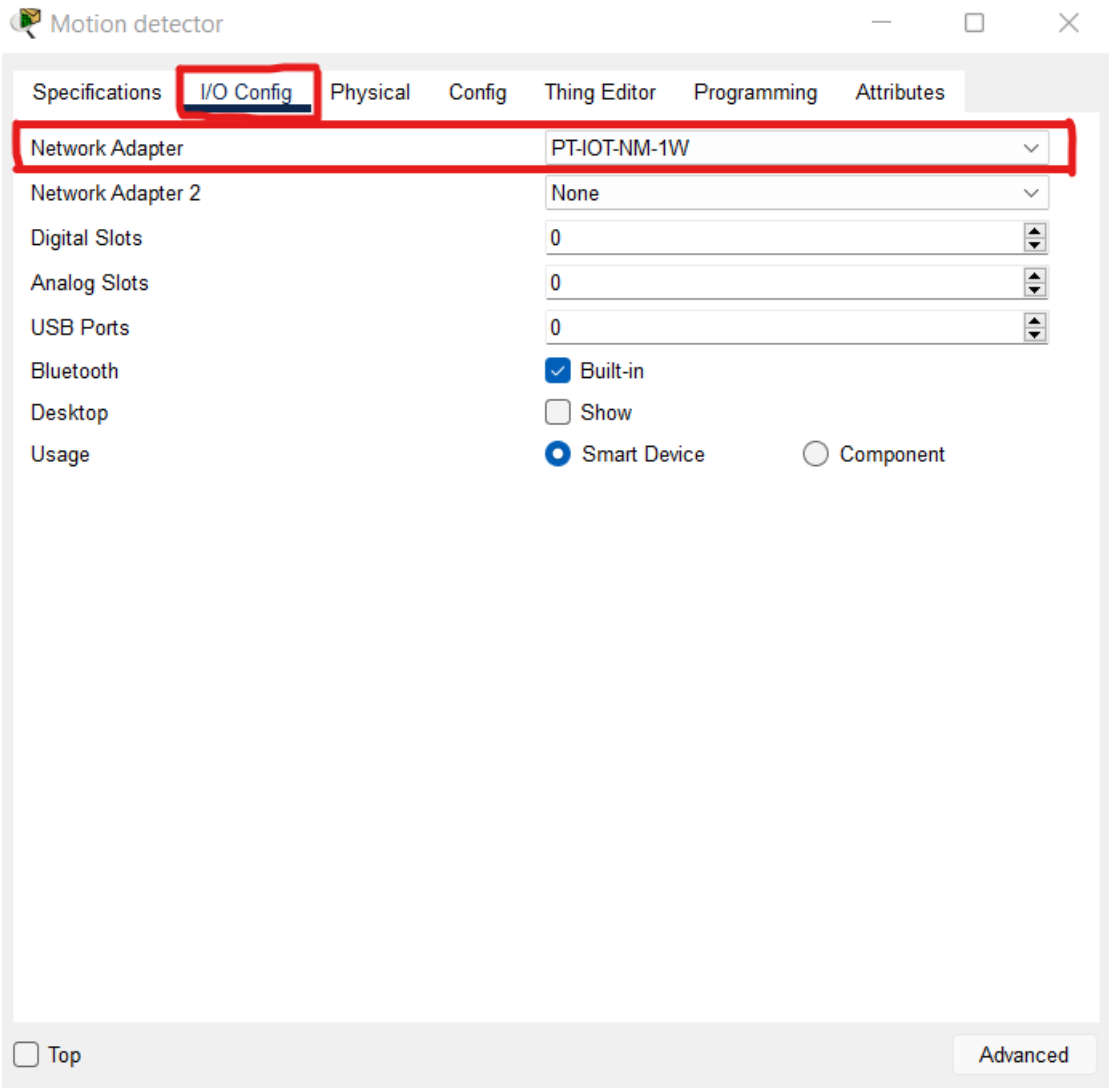

Рисунок 3.21 – Вибір мережевого адаптера для детектора руху

Наступник кроком, переходимо на вкладку «Config» і в налаштуваннях у полі «Gateway/DNS IPv4» обираємо «DHCP», що означає автоматичне налаштування IP адреси, також у полі «IoT Server» обираємо «Home Gateway», що означає підключення до мережевого комутатора. Детальніше зображено на рисунку 3.22

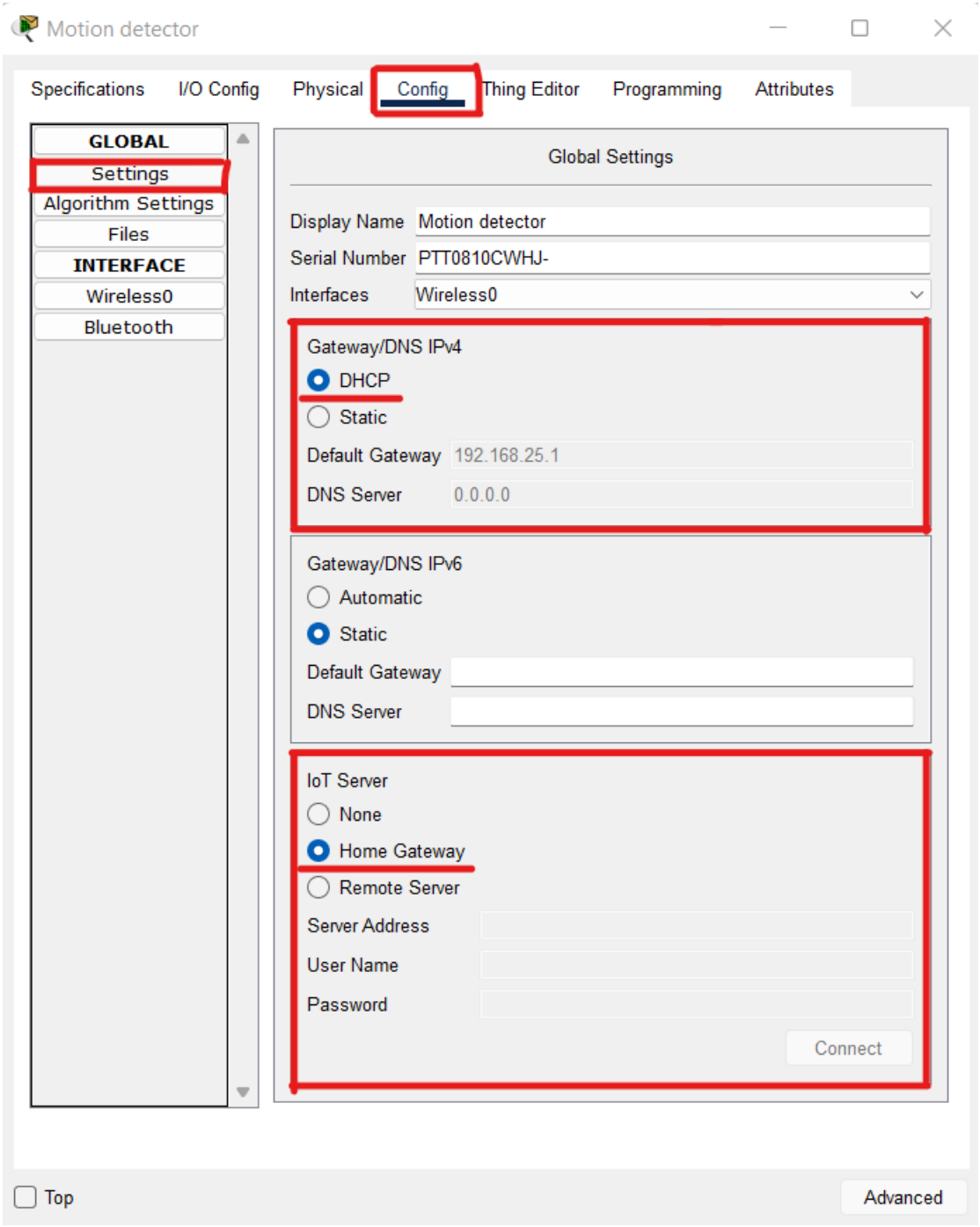

Рисунок 3.22 – Налаштування датчику для відображення даного пристрою на сайті в SBC

На цьому підключення бездротовим з’єднанням виконано. Таким чином підключаємо всі датчики. На рисунку нижче продемонстровано зв’язок між мережевим комутатором та підключеним детектором руху, та всіма іншими елементами системи.

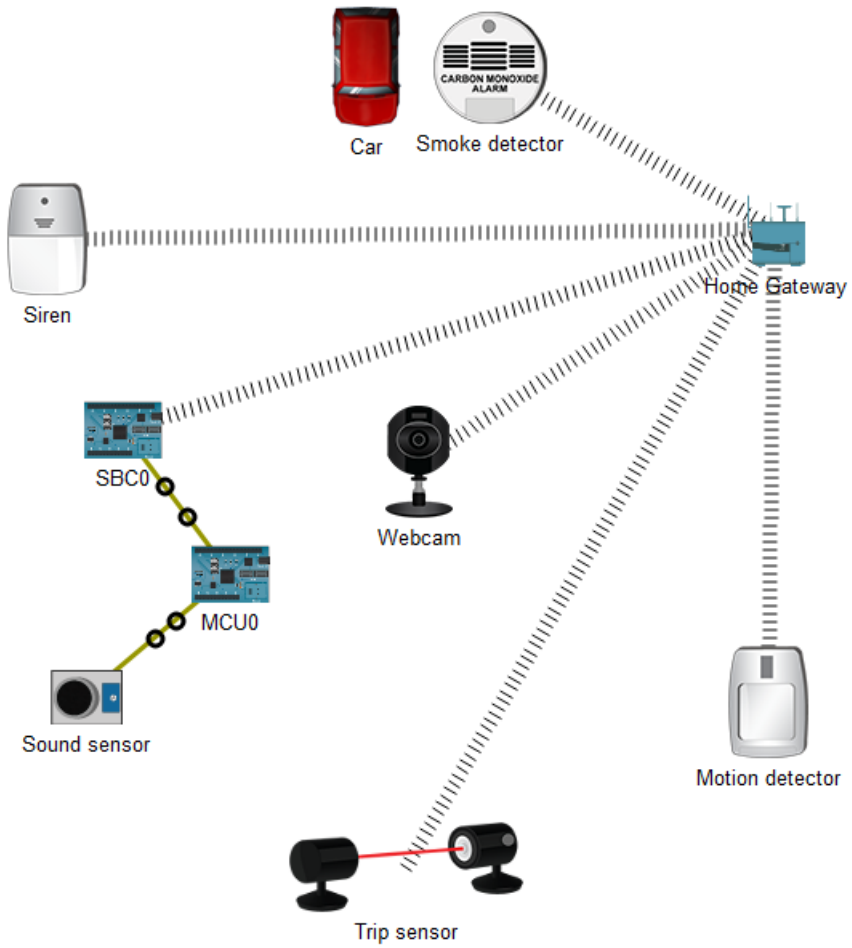

Рисунок 3.23 – Демонстрація всіх бездротових підключень

ВИСНОВКИ

В ході виконання даної дипломної роботи було отримано наступні результати. Проаналізовано різні системи запобігання проникнення, їхній склад датчиків, роботу цих датчиків і використання систем в правильному місці.

Було розглянуто різні види датчиків, їхні характеристики та склад, тобто з чого зроблені датчики. Всі датчики розглядалися із програми Cisco Packet Tracer.

В системі було використано бедротовий зв’язок між датчиками та мережевим комутатором, та фізичний – при підключенні звукового сенсору.

На основі досліджень датчиків, типів їх з’єднань з іншими датчиками та мережевим комутатором, було змодельовано та розроблено систему запобігання проникнення подвійного призначення в програмі Cisco Packet Tracer.

Після побудови системи також було додано правила роботи датчиків, та перевірено їх на працездатність.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Silicon Laboratories, The Evolution of Wireless Sensor Networks, 2013. [Електронний ресурс]. – Режим доступу: https://www.silabs.com/documents/public/white-papers/evolution-of-wireless-sensor-networks.pdf
2. Jiang Q. Routing Protocols for Sensor Networks / Q. Jiang, D. Manivannan // IEEE Consumer Communications and Networking Conference (CCNC'04). - 2004.
3. В.А. Бабошин, Е.А. Бубнова, Р.В. Ковальчук. Особенности использования технологии сенсорных сетей всистеме связи специального назначения. [Електронний ресурс]. – Режим доступу: http://www.npomars.com/db/ru/news/ofic_inf/178-2014-04-07/sec1/3.pdf
4. Dionisis Kandris, Christos Nakas , Dimitrios Vomvas and Grigorios Koulouras, Applications of Wireless Sensor Networks: An Up-to-Date Survey, 25 February 2020, [Електронний ресурс]. – Режим доступу: https://www.mdpi.com/2571-5577/3/1/14
5. Кучерявый, А. Е. Самоорганизующиеся сети / А. Е. Кучерявый, А. В. Прокопьев, Е. А. Кучерявый // Издательство «Любавич». — СПб. — 2011.
6. Сергиевский М. Беспроводные сенсорные сети. Часть 1, 2, 3, 4 // Компьютер Пресс. – 2008. – №№ 4, 8, 11.
7. РУКОВОДСТВО ПО ЭКСПЛУАТАЦИИ «Session Border Controller (SBC)» https://protei.ru/sites/default/files/media/2019-09SBC_Guide_2018.pdf
8. Akyildiz I. F. Wireless sensor networks: A survey. Computer Networks // IEEE Communications Magazine. –2002. – P.250.
9. Альянс ZigBee [Електронний ресур]. – Режим доступу: http://spectron.com.ua/ua/zigbee.html. Безпровідні радіо мережі Zigbee .
10. Панфилов Д. Л. Введение в беспроводную технологию стандарта 802.15.4 // Электронные компоненты. 2004. № 12. – С.73–79.

11. Wireless Sensor Networks: a Survey on the State of the Art and the 802.15.4 and ZigBee Standards / P. Baronti, P. Prashant, V. Chook, S. Chessa / Computer Communication. – 2007. – Volume 30., Issue 7. – P. 1655-1695.
12. ZIGBEE STANDARDS [Електронний ресур]. – Режим доступу: http://www.zigbee.org/Standards/. ZigBee Technical Documents.
13. Еркин. А.Н. Особенности проектирования беспроводных ZigBee - сетей на базе микроконтроллеров фирмы Jennic / А.Н. Еркин. // Беспроводные технологии. Москва. - 2010. - №8. – С. 48-60.
14. Яцків Н.Г. Визначення координат вузлів безпровідних сенсорних мереж / Н.Г. Яцків, В.А Мандзій//Матеріали ІІ Всеукраїнської школи-семінару молодих вчених і студентів «Сучасні комп'ютерні інформаційні технології» ACIT'2012, (4-5 травня 2012 р., м. Тернопіль). – Тернопіль: ТНЕУ, 2012. – С.80
15. Elson J. Time synchronization in wireless sensor networks // Department Computer Sciences, University of California, Ph.D. dissertation, Los Angeles. – 2003.
16. Boukerche A., Nakamura E. Localization systems for wireless sensor networks. IEEE Wireless Communications Special Issue on Wireless Sensor Networks, 2007. – P. 6–12