

ОСНОВИ ІНТЕРНЕТУ РЕЧЕЙ ТА АНАЛІТИКА ВЕЛИКИХ ДАНИХ

ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ

Навчально-науковий інститут цивільного захисту

Кафедра управління інформаційною безпекою



НАВЧАЛЬНИЙ ПОСІБНИК

(лабораторний практикум)
з дисципліни «Основи інтернету речей та аналітика великих даних»
для студентів
денної та заочної форм навчання
галузі знань F «Інформаційні технології»
спеціальності F5 «Кібербезпека та захист інформації»

Львів
ЛДУ БЖД
2026

Навчальний посібник (лабораторний практикум) з дисципліни «Основи інтернету речей та аналітика великих даних» для студентів інституту цивільного захисту галузі знань F «Інформаційні технології» спеціальності F5 «Кібербезпека та захист інформації». Уклад.: Пановик У.П. Ткачук Р.Л., Полотай О.І., Маслова Н.О. Львів: ЛДУ БЖД, 2026. 147 с.

Затверджено на засіданні кафедри управління інформаційною безпекою ЛДУ БЖД. Протокол № 5 від 03 грудня 2025р.

Рекомендовано навчально-методичною комісією інституту цивільного захисту (протокол № 12/2025 від 16.12.2025)

Навчальний посібник (лабораторний практикум)
з дисципліни «Основи інтернету речей та аналітика великих даних»
для студентів інституту цивільного захисту
спеціальності F5 «Кібербезпека та захист інформації»

Укладачі: Уляна Петрівна Пановик, к.т.н., доцент
Ростислав Львович Ткачук, д.т.н, професор
Орест Іванович Полотай, к.т.н., доцент
Наталія Олександрівна Маслова, к.т.н., доцент

Літературний редактор: Галина Марянівна ПАДИК

Посібник призначений для опанування практичних навичок, необхідних майбутнім фахівцям для вивчення дисципліни «Основи інтернету речей та аналітика великих даних». Обсяг та перелік тем повністю підпорядковані навчальній програмі дисципліни, змістовні модулі якої визначені в освітньо-професійній програмі спеціальності. Навчальний посібник призначений для студентів спеціальності F5 «Кібербезпека та захист інформації» всіх форм навчання.

ЗМІСТ

ВВЕДЕННЯ В CISCO PACKET TRACER 6
ЛАБОРАТОРНА РОБОТА № 1. ВВЕДЕННЯ ДО IOT 20
ЛАБОРАТОРНА РОБОТА № 2. СТВОРЕННЯ ПРОСТОЇ МЕРЕЖІ ЗА ДОПОМОГОЮ PACKET TRACER 46
ЛАБОРАТОРНА РОБОТА № 3. ПІДКЛЮЧЕННЯ ПРИСТРОЇВ IOT ДО РОЗУМНОГО БУДИНКУ 59
ЛАБОРАТОРНА РОБОТА № 4. ПІДКЛЮЧЕННЯ ТА МОНІТОРИНГ ПРИСТРОЇВ IOT 70
ЛАБОРАТОРНА РОБОТА № 5. ПОБУДОВА МОДЕЛІ РОЗУМНОЇ КІМНАТИ ЗА ДОПОМОГОЮ CISCO PACKET TRACER 77
ЛАБОРАТОРНА РОБОТА № 6. ПІДКЛЮЧЕННЯ ПРИСТРОЇВ IOT ДО СЕРВЕРА В CISCO PACKET TRACER 88
ЛАБОРАТОРНА РОБОТА № 7. ВИКОРИСТАННЯ FOG COMPUTING У РОЗУМНОМУ ДОМІ 108
ЛАБОРАТОРНА РОБОТА № 8. ПІДКЛЮЧЕННЯ ТА ВІЗУАЛЬНЕ ПРОГРАМУВАННЯ МІКРОКОНТРОЛЕРА IOT 120
ЛАБОРАТОРНА РОБОТА № 9. НАЛАШТУВАННЯ ДОМАШНЬОЇ МЕРЕЖІ З ВІДДАЛЕНИМ ДОСТУПОМ ДО ПРИСТРОЇВ IOT 132
ЛАБОРАТОРНА РОБОТА № 10. НАЛАШТУВАННЯ БЕЗПЕКИ БЕЗДРОТОВОГО ЗВ'ЯЗКУ 142
ЛАБОРАТОРНА РОБОТА № 11. ЗАХИСТ ХМАРНИХ СЛУЖБ В IOT 151
ЛАБОРАТОРНА РОБОТА № 12. ДОСЛІДЖЕННЯ SMART CITY ТА SMART GRID 161
ЛАБОРАТОРНА РОБОТА № 13. НАЛАШТУВАННЯ ВІРТУАЛЬНОГО СЕРВЕРНОГО СЕРЕДОВИЩА 173

ВСТУП

Користувачі інтернету використовують хмарні технології, навіть не підозрюючи про це. Ви дивитеся онлайн-відео, вебінари, граєте в онлайн-ігри, завантажуєте музику через YouTube, переглядаєте пошту на Gmail або заходите на Facebook – усе це хмарні технології. Ми використовуємо все більш потужні й ресурсомісткі програми, які потребують для своєї роботи набагато потужніших засобів. Ми змушені оперувати дедалі більшими обсягами даних і ці дані потрібно десь зберігати. Чи не найвдалішим рішенням цієї проблеми є використання хмарних технологій.

Хмарні технології – це модель організації доступу користувачів через інтернет до деякого загального фонду обчислювальних ресурсів. Самі ресурси можуть бути різними – віддалені сервіси, пристрої зберігання даних, сервери, програмне забезпечення тощо. У сучасних центрах обробки даних зосереджені колосальні обчислювальні потужності і величезні обсяги дискового простору. Сучасне програмне забезпечення і канали зв’язку дають змогу серверам, розташованим на різних континентах, працювати як єдине ціле. Потрібно лише створити зручну систему доступу, і тоді весь масив цієї могутності можна надавати тим, хто його потребує. Засоби віртуалізації дають нагоду розділяти обчислювальні потужності на осібних споживачів у будь-яких пропорціях.

Використання хмарних технологій набуває дедалі більшої популярності й в Україні, а особливо в галузі Інтернету речей (IoT). Сфера IoT – один із головних світових трендів. Старі-добрі пристрої стають частиною інтернет – мережі і виконують нові функції. IoT являє собою величезну базу даних, у якій, інтелектуальні пристрої обмінюються інформацією за допомогою датчиків, електроніки, системної мережі й апаратного забезпечення.

Хмарні обчислення, а також IoT працюють над підвищенням ефективності повсякденних завдань, й обидві мають взаємодоповнюючі відносини. З одного боку, IoT генерує багато даних, а з іншого – хмарні обчислення прокладають шлях для цих даних. Хмарні обчислення забезпечують кращу спільну роботу для розробників пристроїв IoT. Завдяки тому, що розробники можуть зберігати й отримувати доступ до даних віддалено, хмара дозволяє розробникам без затримок реалізовувати проекти. Крім того, зберігаючи дані в хмарі, компанії IoT можуть одержувати доступ до величезної кількості великих даних. Отже, у

спробі встановити відносини між IoT і хмарою, варто набути теоретичних знань та практичних вмінь у сфері проектування, впровадження, безпечної експлуатації та супроводження інтелектуальних систем.

Дисципліна «Основи інтернету речей та аналітика великих даних» призначена для вивчення теоретичних і практичних основ організації комп'ютерних мереж, програмування пристроїв Інтернету речей та аналізу даних мережі Інтернет. Мета дисципліни – формування теоретичних і практичних знань щодо технологій хмарних обчислень та їх безпечної інтеграції в інформаційні системи; ознайомлення з поняттями, моделями та архітектурами хмарних сервісів, методами забезпечення конфіденційності, цілісності та доступності даних у хмарному середовищі; опанування інструментів дослідження, аудиту, проектування й захисту IoT-інфраструктури, що забезпечить розуміння принципів кіберзахисту, безпечної взаємодії пристроїв і сервісів, а також протидії кіберзагрозам у хмарних та IoT-екосистемах.

Метою лабораторного практикуму є ознайомлення студентів з особливостями розроблення програмного забезпечення для роботи в мережі пристроїв Інтернету речей за допомогою середовища моделювання Cisco Packet Tracer; ознайомлення з методами захисту хмарних сервісів Інтернету речей та методами аналізу даних мережі Інтернет.

Методичні вказівки включають низку частково взаємопов'язаних лабораторних робіт, під час виконання яких студенти мають можливість отримати досвід роботи із середовищем Cisco Packet Tracer.

Перед виконанням лабораторної роботи студенти мають:

- ознайомитися з методичними вказівками;
- повторити лекційний матеріал, пов'язаний із лабораторною роботою.

Виконавши ці завдання, студент має продемонструвати викладачеві роботу на комп'ютері, оформити звіт за результатами даної лабораторної роботи, захистити його та здати викладачеві.

У лабораторному практикумі використано матеріали мережевої академії Cisco Networking Academy з електронного курсу Cisco:

- Introduction to the Internet of Things (IoT) – Введення до IoT»;
- IoT Fundamentals: Connecting Things – Основи IoT: Підключення речей.

ВВЕДЕННЯ В CISCO PACKET TRACER

Cisco Packet Tracer (CPT) – інноваційний інструмент моделювання та візуалізації мережі. Це безкоштовне програмне забезпечення допомагає практикувати в налаштуваннях мережі та набути навики усунення несправностей. Packet Tracer доступний, як для робочих середовищ Linux, так і для Windows.

Packet Tracer є важливим інструментом навчання, який використовується в багатьох програмах Cisco Networking Academy. Packet Tracer має такі особливості:

- моделювання логічної топології: робочий простір для того, щоб створити мережі будь-якого розміру;
- моделювання в режимі реального часу;
- режим симуляції;
- моделювання фізичної топології: взаємодія з фізичними пристроями, використовуючи такі поняття як місто, будинок тощо;
- GUI, необхідний для якісного розуміння організації мережі, принципів роботи пристроїв;
- багатомовна підтримка: можливість перекладу даного програмного продукту практично на будь-яку мову;
- зображення мережевого устаткування зі здатністю додавати або видаляти різні компоненти;
- наявність Activity Wizard дає можливість створювати шаблони мереж і використовувати їх надалі.

За допомогою даного програмного продукту можна будувати та конфігурувати мережі і проводити в них пошук несправностей. Даний симулятор дає змогу проектувати свої власні мережі, створюючи і відправляючи різноманітні пакети даних, зберігати й коментувати свою роботу.

Після того, як мережа спроектована, можна приступати до конфігурування обраних пристроїв за допомогою термінального доступу або командного рядка. Для побудови моделі мережі Packet Tracer дозволяє моделювати основні типи

мережевого обладнання: комп'ютерів, серверів, Ethernet комутаторів, маршрутизаторів тощо. За допомогою «перетаскування» активних елементів мережі з панелі компонентів мережі на робоче поле та з'єднання їх кабелями та каналами зв'язку можуть бути утворені найрізноманітніші конфігурації мереж.

Щоб отримати та встановити програму Cisco Packet Tracer, виконайте такі прості кроки:

1. Увійдіть до своєї мережі Cisco Networking Academy: https://www.netacad.com/courses/packet-tracer.
2. Виберіть Getting Started with Cisco Packet Tracer.
3. Виберіть Get Started та завантажте Packet Tracer.
4. Виберіть версію Packet Tracer, яка вам потрібна.
5. Збережіть файл на своєму комп'ютері.
6. Запустіть програму встановлення Packet Tracer.
7. Після встановлення закрийте та перезапустіть веббраузер.
8. Запустіть пакет Cisco Packet Tracer, вибравши відповідний значок.
9. Коли з'явиться запит, використовуйте дані входу до Netacad для автентифікації.

З процесом завантаження та встановлення Packet Tracer можна ознайомитись із відео «How to Download Cisco Packet Tracer» за посиланням: https://www.youtube.com/watch?v=vARil54x41g&ab_channel=IgoroTechOfficial

Після запуску програми Packet Tracer відкривається головне вікно програми (рис. 1). Основне вікно програми містить 6 основних меню, 4 з яких використовуються найбільш часто.

Програма Cisco Packet Tracer має підтримку Internet of Things (Інтернет речей). Інтернет речей – це концепція мережі, яка складається з пристроїв, які здійснюють обмін даними між фізичним світом і комп'ютерними системами, за допомогою використання стандартних протоколів зв'язку. На додаток до класичних мережевих пристроїв, таких як маршрутизатори та комутатори, Packet

Tracer Network Component Box містить широкий спектр інтелектуальних речей та компонентів:

- ***Розумні речі*** – це фізичні об’єкти, які можуть підключатися до сервера реєстрації або домашнього шлюзу через мережевий інтерфейс. Вони поділяються на 5 підкатегорій: End Devices, Home, Smart City, Industrial і Power Grid.

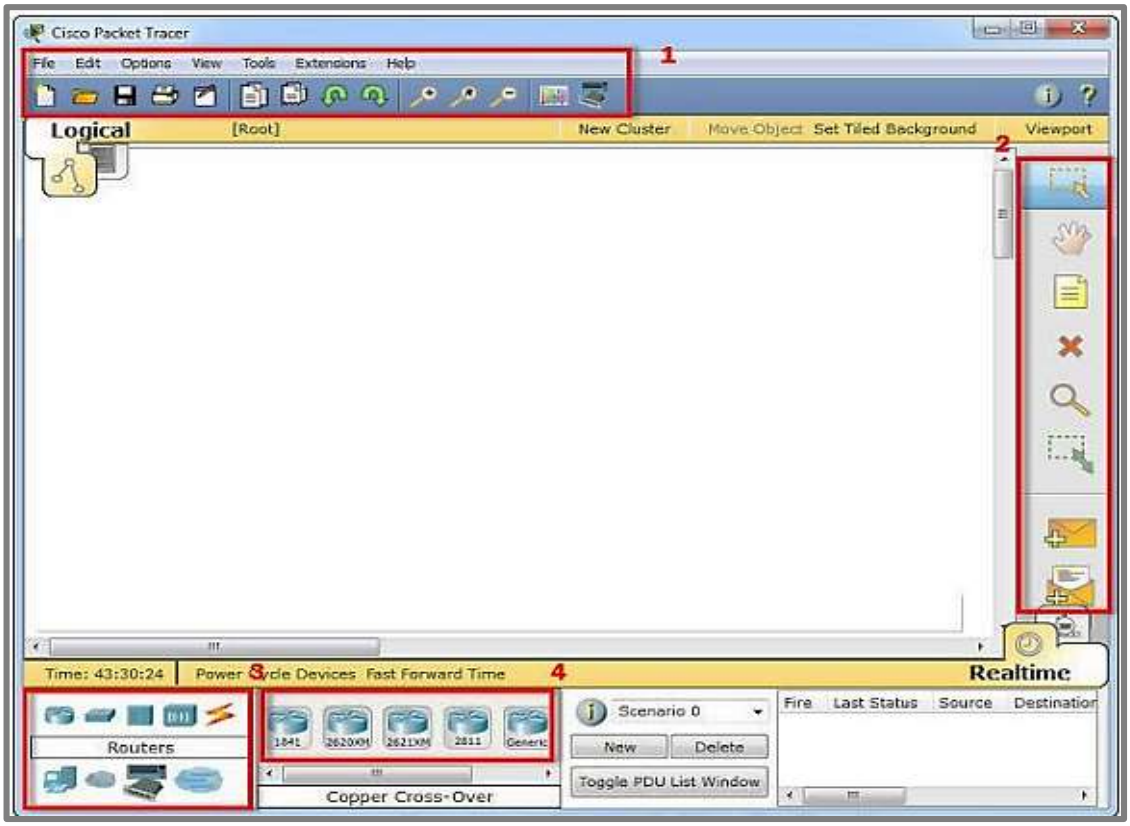


Рисунок 1 – Інтерфейс програми Cisco Packet Tracer: 1– панель інструментів; 2 – графічне меню; 3 – панель обладнання; 4 – панель пристроїв

- ***Компоненти*** – це фізичні об’єкти, які підключаються до мікроконтролера (MCU-PT) або односторонніх комп’ютерів (SBC-PT). Вони, як правило, не мають мережевого інтерфейсу й покладаються на MCU-PT або SBC-PT для доступу до мережі. Це прості пристрої, які спілкуються лише через аналогові або цифрові слоти.

Packet Tracer проводить управління динамічним середовищем (температура, газ, тиск, світло тощо), щоб зробити симуляцію пристроїв IoT

більш реалістичними. Багато пристроїв чи речей впливають або реагують на довкілля в Packet Tracer: пожежний розприскувач підвищить рівень води та вологість у контейнері, стара машина збільшить рівень газів та температуру навколишнього середовища при включенні, детектор диму може бути використаний для запуску сигналу, коли дим у довкіллі збільшується до певної відмітки. Отже, розглянемо, які можливості надає нам Cisco Packet Tracer.

Унизу, під робочою областю, розташована панель елементів (рис. 2). Дана панель містить у своїй лівій частині типи (класи) пристроїв, а в правій частині – їх найменування (моделі). У разі наведенні курсору на пристрій, у прямокутнику, що знаходиться по центру між ними, буде відображатися його тип.

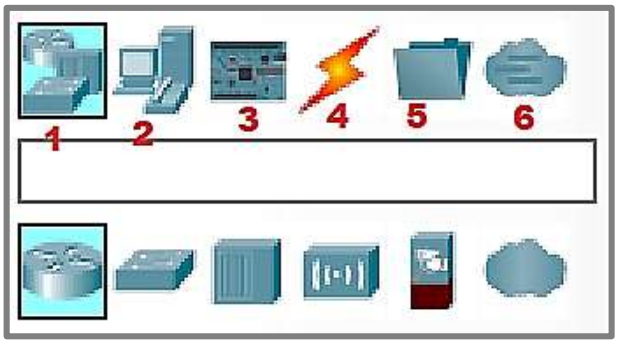


Рисунок 2 – Панель елементів: 1 – мережеві пристрої; 2 – кінцеві пристрої; 3 – компоненти; 4 – з'єднання; 5 – різне; 6 – з'єднання мультикористувача

Елементи Internet of Things розташовуються переважно у вкладці 2. Проте є один елемент із вкладки 1. Цей елемент називається домашнім шлюзом (рис. 3).



Рисунок 3 – Вкладка мережевих пристроїв (підгрупа бездротових пристроїв)

На вкладці кінцевих пристроїв є декілька категорій:

1. ***кінцеві пристрої*** (End Devices), такі як ПК, смартфон, телефон, сервер, телевізор тощо (рис. 4).



Рисунок 4 – Вкладка кінцевих пристроїв (жовтим маркером виділенні елементи, що використовуються в Internet of Things)

2. ***дім*** (Home), який містить такі елементи (рис. 5), які детально описані в таблиці 1:

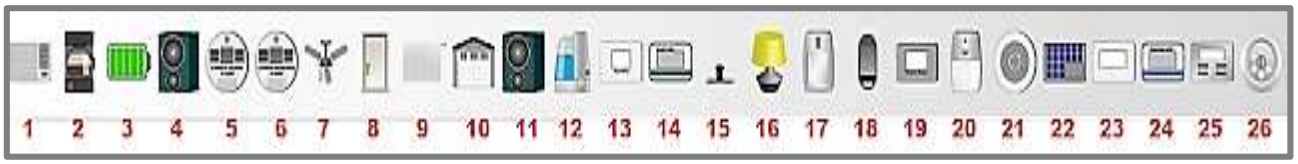


Рисунок 5 – Компоненти вкладки «Дім»

3. ***розумне місто*** (Smart City), яке містить (рис. 6):

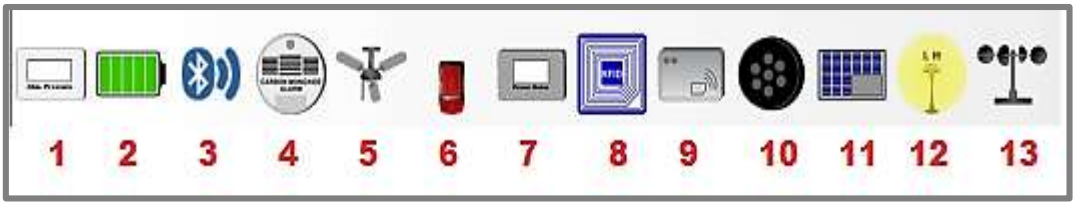


Рисунок 6 – Компоненти вкладки «Розумне місто»: 1 – контролер атмосферного тиску; 2 – батарея (акумулятор); 3 – передавач Bluetooth -маяків; 4 – детектор карбон моноксиду; 5 – розумний вентилятор на стелі; 6 – стара машина; 7 – вимірювач напруги; 8 – картка радіочастотної ідентифікації; 9 – зчитувач карток радіоактивної ідентифікації; 10 – розумна LED лампа; 11 – сонячна панель; 12 – розумний вуличний ліхтар; 13 – детектор вітру

3. ***індустріальне*** (Industrial), яке містить елементи, що зображені на рис. 7:



Рисунок 7 – Компоненти вкладки «Індустріальне»

4. ***енергосистема*** (Power Grid), яка містить (рис. 8):

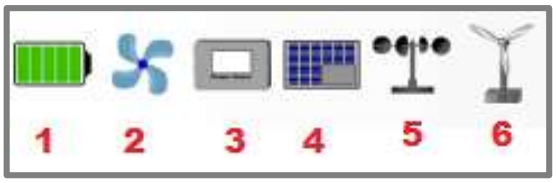
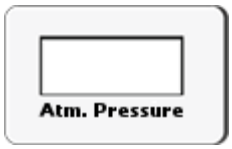


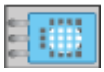
Рисунок 8 – Компоненти вкладки «Енергосистема»

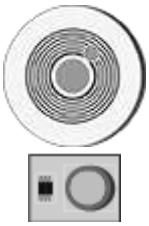
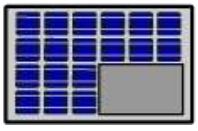
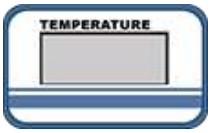
У наведеній нижче таблиці перелічено всі речі, доступні в Packet Tracer, та їх поведінка щодо імітованого середовища:

Таблиця 1

Розумні речі, доступні в Packet Tracer

Розумні речі	***Позначення***	***Опис***
ATM Pressure Sensor		Виявляє атмосферний тиск і відображає його. Діапазон детектування за замовчуванням становить від 0 до 110 кПа.
Carbon Dioxide Detector		Виявляє діоксид вуглецю.
Carbon Monoxide Detector		Визначає монооксид вуглецю.
Door		Впливає на аргон, монооксид вуглецю, двоокис вуглецю, водень, гелій, метан, азот, O_2, озон, пропан та дим. Коли двері відкриються, ці гази зменшуються до максимум 2%. Коли двері відкриті, швидкість переносу для вологості та температури збільшується на 25%. Швидкість перенесення для газів збільшується на 100%.
Fan		Впливає на швидкість вітру, вологість та температуру довкілля. За низької швидкості встановлено значення швидкості вітру 0,4 км/год. Швидкість охолодження температури довкілля встановлюється до -1^0C/год. Швидкість зменшення вологості становить 1% за годину. На високошвидкісній установці швидкість вітру встановлюється до 0,8 км/год.

Розумні речі	***Позначення***	***Опис***
Fire Sprinkler, Ceiling Sprinkler		Впливає на рівень води в 0,1 см/сек. Впливає на вологість у розмірі 5% на годину.
Garage Door		Впливає на всі параметри, що й Door. Коли двері відкриються, загальні зміни цих газів зменшяться до максимум 4%. Коли двері відкриті, швидкість передачі для вологості та температури збільшується на 50%. Швидкість перенесення для газів збільшується на 100%.
Home Speaker, Speaker		Впливає на гучність звуку при 65 дБ. Впливає на шум звуку при 20 CPS до 60 CPS. Вплив на білий шум при 20%.
Humidifier		Впливає на вологість у розмірі 1% на годину.
Humidity Sensor		Визначає вологість.
Humiture Monitor, Humiture Sensor		Визначає температуру навколишнього середовища та вологість; виводить значення як суму температури навколишнього середовища та вологості, розділеній на 2.
Lawn Sprinkler, Floor Sprinkler		Впливає на рівень води в 0,1 см/сек. Впливає на вологість у розмірі 5% на годину.
LED		Впливає на Visible Light з максимальним виходом 1%.
Light		Впливає на Visible Light з максимальним виходом 20%.
Old Car		Впливає на монооксид вуглецю в розмірі 1% на год. Впливає на діоксид вуглецю в розмірі 2% на год. Впливає на дим зі ставкою 3% на год. Впливає на температуру навколишнього середовища зі швидкістю 1% на годину.

Розумні речі	***Позначення***	***Опис***
Photo Sensor		Виявляє видиме світло.
Piezo Speaker		Впливає на гучність звуку на 10 дБ. Впливає на Sound Pitch 20 CPS.
RGB LED		Впливає на Visible Light з максимальним виходом 2%.
Smart LED, Dimmable LED		Впливає на Visible Light з максимальним виходом 3%.
Smoke Detector, Smoke Sensor		Виявляє дим.
Solar Panel		Виявляє сонячне світло для генерування електроенергії.
Temperature Monitor		Визначає температуру навколишнього середовища.
Temperature Sensor		Визначає температуру навколишнього середовища.
Water Level Monitor, Water Detector		Визначає рівень води.
Wind Sensor		Визначає швидкість вітру.
Wind Turbine		Визначає швидкість вітру для генерації електроенергії.

Розумні речі	*Позначення*	*Опис*
Window		Впливає на всі параметри, що й Door. Коли вікно відкривається, ці гази зменшуються до максимум 1% у загальній зміні. Коли вікно відкрите, швидкість переносу для вологості та температури збільшується на 20%. Швидкість перенесення для газів збільшується на 100%.
Drain Actuator		Впливає на рівень води зі швидкістю 0,5 см/с.
Sound Frequency Detector		Виявляє Sound Pitch і відображає його.
Furnace, Heating Element		Впливає на вологість при швидкості -2% на годину. Впливає на температуру довкілля зі швидкістю 10°C на годину.
AC, Air Cooler		Впливає на вологість при швидкості -2% на годину. Впливає на температуру довкілля зі швидкістю -10°C на годину.

Також ще використовуються елементи з третьої вкладки «Компоненти» (рис. 9). Усі компоненти можна програмувати відповідно до поставленого завдання або для досягнення бажаного результату. Ці компоненти можна застосовувати в проектах проектування розумних будинків, автоматизованих приміщень, розумних міст та інших проектів. Головною перевагою розумних речей є самостійне прийняття рішень та віддалене керування.

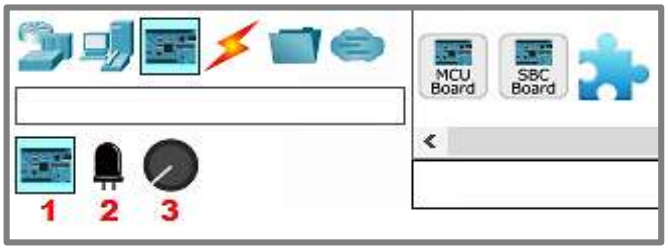


Рисунок 9 – Вкладка «Компоненти»

Перша категорія – це плати: мікроконтролери (MCU-PT), одноплатні комп'ютери (SBC-PT) та спеціальні розумні пристрої Thing, які використовуються для створення автономних фізичних об'єктів, таких як кавоварки або димові сигнали За допомогою цих плат (мікроконтролери та однопроцесорні плати) ми можемо програмувати речі (одну або декілька речей одночасно) та додавати їм новий функціонал. За допомогою елементу «пристрій» ми маємо можливість створити свою розумну річ, надати їй бажані стани, запрограмувати відповідним чином, обрати зображення для нашого пристрою, написати специфікацію пристрою, задати відповідні слоти та мережеві адаптери.

Друга категорія – це виконавчі механізми, приводи (рис. 10). Ці компоненти маніпулюють навколишнім середовищем, або областю навколо себе. Категорія містить:

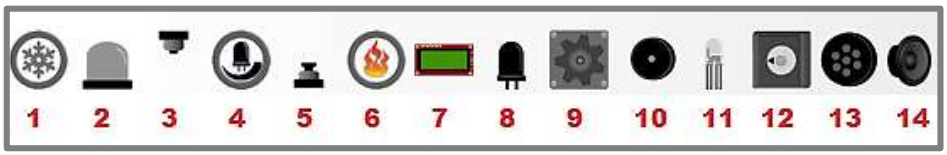


Рисунок 10 – Виконавчі механізми: 1 – охолоджувач повітря; 2 – лампа тривоги; 3 – розбризкувач на стелі; 4 – затемнена лампа; 5 – розбризкувач на підлозі; 6 – нагрівальний елемент; 7 – LCD; 8 – LED; 9 – мотор; 10 – п'єзодинамік; 11 – кольорова LED; 12 – серводвигун; 13 – розумна LED; 14 – динамік

Третя категорія – сенсори, датчики (рис. 11). Ці компоненти функціонують від довкілля (фотодетектори, датчик температури), зони навколо них (RFID, датчик металу) або взаємодії (потенціометр, кнопка):

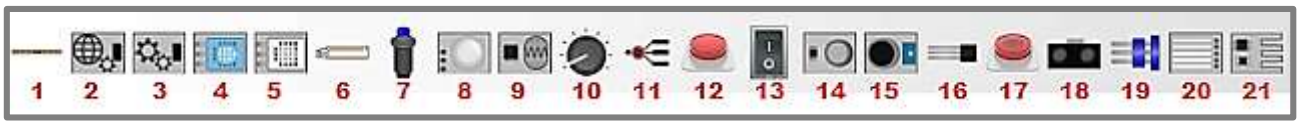


Рисунок 11 – Сенсори: 1 – сенсор гнучкості; 2 – сенсор довкілля; 3 – сенсор, який можна створити і запрограмувати; 4 – сенсори вологи; 5 – сенсор дискомфорту (вологість+температура); 6 – мембранний потенціометр; 7 – сенсор металу; 8 – сенсор руху; 9 – фото (світловий) сенсор; 10 – потенціометр; 11 – кнопка перемикання; 12 – кнопка з одноразовим натиском; 13 – вмикач; 14 – сенсор диму; 15 – сенсор звуку; 16 – сенсор температури; 17 – кнопка з постійним натиском; 18 – лазерний сенсор руху; 19 – детектор води; 20 – сенсор води; 21 – сенсор вітру

З’єднання вузлів мережі в єдину топологію здійснюється за допомогою ліній зв’язку. Водночас кожен тип кабелю може бути з’єднаний лише з визначеними типами інтерфейсів пристроїв (рис. 12).



Рисунок 12 – Типи ліній зв’язку

Автоматичний тип (Automatically Choose Connection Type) – при даному типі з’єднання Packet Tracer автоматично обирає найкращі типи з’єднання для обраних пристроїв.

Консоль (Console) – консольне з’єднання. Консольне з’єднання може бути виконано між ПК і маршрутизаторами чи комутаторами.

Мідний прямий (Cooper Straight-Throught) – з’єднання мідним кабелем типу вита пара, обидва кінці кабелю обтиснуті в однаковій розкладці.

Мідний перехресний (Cooper Cross-Over) – з’єднання мідним кабелем типу вита пара, кінці кабелю обтиснуті перехресно.

Оптика (Fiber) – з’єднання за допомогою оптичного кабелю, необхідне для з’єднання пристроїв, що мають оптичні інтерфейси.

Телефонний кабель (Phone) – кабель для підключення телефонних апаратів. З’єднання через телефонну лінію може бути здійснене між пристроями, що мають модемні порти.

Коаксіальний кабель (Coaxial) – використовується для з’єднання між кабельним модемом і хмарою.

Серійний DCE і серійний DTE (Serial DCE / DTE) – з’єднання через послідовні порти для зв’язку Інтернет. Для настройки таких з’єднань необхідно

встановити синхронізацію на стороні DCE-пристрою. Сторону DCE можна визначити за маленькою іконкою "годинника" поряд із портом.

У програмі можливе фізичне представлення обладнання у вигляді його фізичної конфігурації (рис. 13).



Рисунок 13 – Фізична конфігурація ПК

Для зміни комплектації обладнання необхідно відключити його живлення, клацнувши мишкою на кнопку живлення і перетягнути мишкою потрібний модуль до вільного слоту, а потім включити живлення. Решта модулів додаються до пристроїв аналогічно.

Пристрої IoT можуть безпосередньо реєструватися на домашньому шлюзі або на серверному пристрої, налаштованому службою IoT.

Домашній шлюз забезпечує чотири Ethernet-порти, а також точку бездротового доступу, налаштовану за допомогою SSID «Home Gateway» На рисунку 14 показано чотири IoT, а домашній шлюз підключений до Інтернету через його Ethernet порт WAN Інтернет.

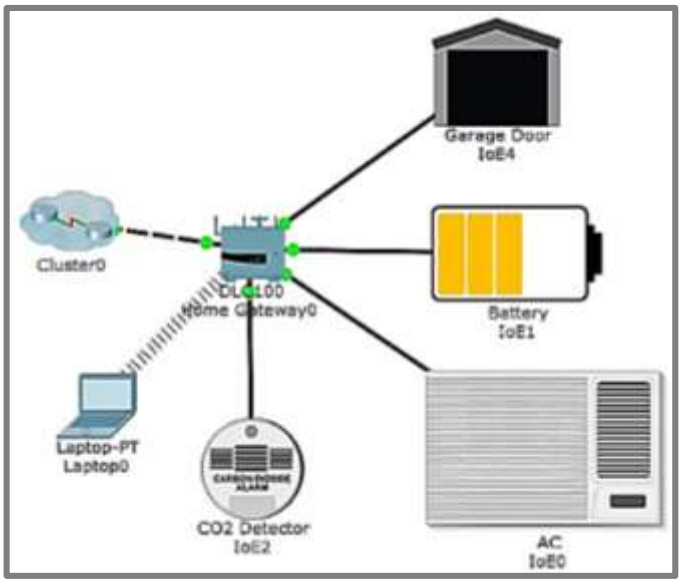


Рисунок 14 – Розумні речі, що приєднані до домашнього шлюзу

IoT можна дистанційно керувати за допомогою вебінтерфейсу, який розміщений у домашньому шлюзі (рис. 15). IP-адреса внутрішньої локальної мережі (LAN) – *192.168.25.1*, але до неї також можна отримати доступ через IP-адресу, на яку звертається Інтернет. Логін домашнього шлюзу (веб): *admin*; пароль головного шлюзу: *admin.*

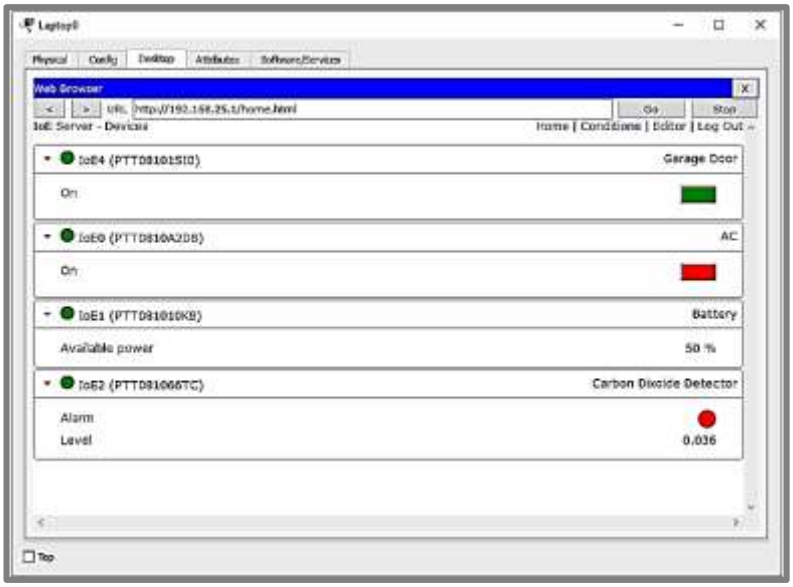


Рисунок 15 – Статус чотирьох IoT, підключених до шлюзу

Оскільки компоненти IoT не мають інтерфейсу Ethernet, то вони не можуть бути безпосередньо підключені до домашнього шлюзу. Ці менші датчики або

виконавчі елементи підключаються до мікроконтролерів MCU-PT (рис. 16). MCU-PT підключається до шлюзу, який бачить лише плату мікроконтролера, а не компоненти IoT. Домашній шлюз покладається на API-інтерфейс дистанційного керування, запрограмований на MCU-PT, щоб отримати статус датчика. Реальний світ MCU – це, наприклад, дошки Arduino, такі як Arduino Yun Shield.

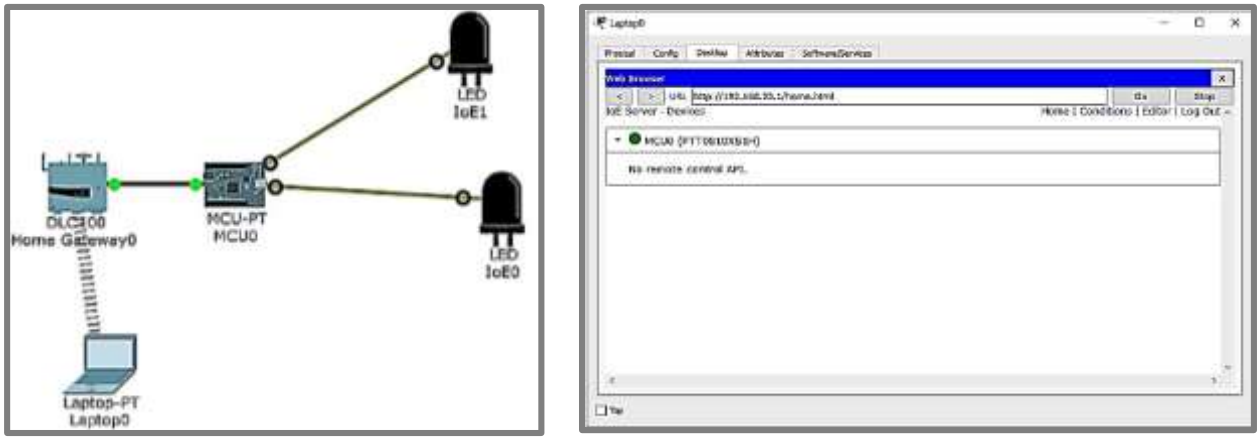


Рисунок 16 – Підключення компонентів IoT до мікроконтролерів

Редактор програмування IoT включений у вебінтерфейс Home Gateway. Це дає можливість програмування Javascript або Python мікроконтролера MCU-PT (рис. 17). Код програмується через вебінтерфейс, а потім публікується на плату MCU.

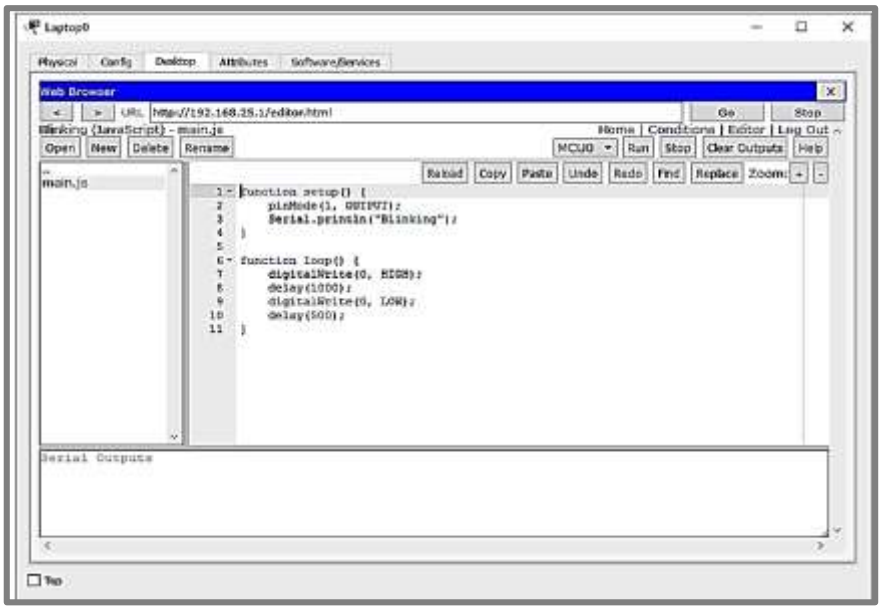


Рисунок 17 – Приклад коду, що призводить до того, що світлодіодний порт підключений до цифрового порту

ЛАБОРАТОРНА РОБОТА № 1
ВВЕДЕННЯ ДО ІОТ

Мета роботи: Ознайомитись із програмою Cisco Packet Tracer для моделювання комп'ютерних мереж. Набути практичні навички з базового налаштування мережних пристроїв для підключення пристроїв Інтернету речей.

ЧАСТИНА 1
ЕВОЛЮЦІЯ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

ТЕОРЕТИЧНІ ВІДОМОСТІ

У нашому світі на сьогодні є більше розумних пристроїв, ніж є людей. Зростає кількість людей, що підключені до Інтернету 24 години на добу. Зростаюча кількість людей підключає (використовує) три, чотири або більше розумних пристроїв. Вони можуть включати в себе смартфони, засоби моніторингу фізичних вправ та здоров'я, електронних книг і планшетів.

Як можна підключити стільки пристроїв? Еволюція цифрової трансформації, сучасні цифрові мережі роблять усе це можливим. Світ швидко покривається мережами, які дають змогу цифровим пристроям взаємоз'єднуватися та передавати дані. Завдяки мережам можливе підключення всіх мобільних пристроїв, електронних датчиків, електронних вимірювальних приладів, медичних приладів та датчиків. Вони відслідковують, обмінюються, оцінюють та, у деяких випадках, автоматично коригують дані, які збираються та передаються. Поняття «Інтернет речей» є комплексним та має кілька рівнів: кінцеві пристрої (датчики, виконавчі пристрої), транспортний рівень (телекомунікаційне середовище, що включає дротові та бездротові мережі) та рівень роботи з даними (збір, зберігання та обробку).

Оскільки суспільство охоплює ці цифрові пристрої, цифрові мережі продовжують зростати у всьому світі, і економічні вигоди від оцифровування надалі зростають, ми спостерігаємо цифрові перетворення.

Цифрова трансформація – це застосування цифрових технологій, щоб забезпечити етап для інновацій бізнесу та промисловості. Ця цифрова інновація зараз застосовується до всіх аспектів людського суспільства.

ЗАВДАННЯ ДО ЧАСТИНИ 1

1 • *Дослідження – як ви підключені?*

Завдання: Опитайте 3–4 особи: родину, колег і друзів. Визначте, скільки годин вони «підключені» через будь-який пристрій упродовж дня.

Важливо розуміти, що більшість людей, які народилися у 2000-х роках, виросли переважно в цифровому світі. Комп'ютери, Інтернет, мобільні телефони, текстові повідомлення, соціальні мережі – все це друга натура для членів цієї групи. Це опитування допоможе вам визначити, скільки часу насправді ви проводите на зв'язку. Це допоможе нам побачити вплив цього покоління на бізнес та економіку.

Вказівки до виконання завдання:

1. Створіть електронну таблицю, схожу на наведену нижче. За потреби додайте додаткові рядки для отримання додаткової інформації.

	A	B	C	D	E	F
1	How Many Hours are You Connected during the Day?					
2						
3	Person 1	Age	Gender	Device	Task	Time in hours
4		43	M	Smartphone	Facebook	4
5					Talking	2
6					Texting	10
7					Twitter	3
8				Fitbit	Tracking exercise	14
9				Tablet	On-line banking	0.5
10						
11					Total	33.5
12	Person 2	Age	Gender	Device	Task	Time
13						
14						
15						
16						
17	Person 3	Age	Gender	Device	Task	Time
18						
19						

2. Узагальніть висновки та дайте відповіді на такі запитання:

- Яку середню кількість часу проводили «на зв'язку» всі ваші респонденти?
- Скільки людей було підключено до кількох пристроїв одночасно?
- Чи впливав вік на кількість «зв'язаного» часу упродовж дня? Якщо так, то в чому, на вашу думку, причина?
- Чи вплинула стать на кількість «зв'язаного» часу упродовж дня? Якщо так, то в чому, на вашу думку, причина?

Цифрова технологія дала можливість бізнесу інноваційно використовувати свій підхід до взаємодії із суспільством. Люди всіх поколінь більш комфортно використовують цифрові технології та використовують розумні пристрої для своїх переваг упродовж своїх напружених днів.

Багато компаній зараз надають частину або всі свої послуги в режимі онлайн. З вашого комфортного будинку, автомобіля, тренажерного залу або офісу ви можете купувати бакалійну продукцію в режимі онлайн, замовляти страви з ресторану, щоб доставили її до ваших дверей, забронювати поїздки онлайн, замовляти одяг, кемпінг, таксі, залишатися на зв'язку з друзями.

Датчики скрізь створюють величезну кількість даних. Розумні будинки можуть бути обладнані датчиками руху, датчиками води, датчиками світла, датчиками дверних дзвінків та датчиками температури. Можуть бути датчики у світлофорах, транспортних вантажівках, гаражах паркування, камерах безпеки, поїздах і літаках. Усі ці датчики та вимірювальні прилади збирають та передають свої дані. Дані можуть бути збережені та проаналізовані пізніше, або їх можна негайно проаналізувати, щоб вони використовувалися для модифікації комп'ютерів, мобільних пристроїв або будь-яких процесів.

2 • Як використовуються збережені та аналізовані дані?

Передумова:

Підприємства: визначають моделі покупки, прогнозують нові тенденції та спрощують виробництво.

Установи: здійснюють моніторинг довкілля, прогнозують демографічні тенденції, прогнозують рівень злочинності та планують соціальні послуги.

Міста: контролюють дорожній рух, контролюють паркування, контролюють поводження з відходами.

Вказівки до виконання завдання: Дайте відповіді на питання:

Запитання	***Варіанти відповідей***
1. Проаналізовані дані датчиків приносять користь бізнесу, а не установам	1. Правда
	2. Неправда
2. Датчики склали дані про кількість велосипедів, проданих у місті. Як місто може використовувати цю інформацію?	1. Для визначення впливу викидів автомобілів на навколишнє середовище.
	2. Для оцінювання рівня фізичного догляду мешканців певної території.
	3. Щоб визначити кількість велосипедних доріг, які будуть створені в місті.
	4. Для визначення інвентарних вимог у спортивних магазинах

3 • Чи можуть розумні пристрої думати?

Передумова:

1. Усі цифрові пристрої працюють на основі комп'ютерних програм та наданих даних. Штучний інтелект означає, що ці пристрої здатні самостійно думати. Якщо вони належним чином запрограмовані, інтелектуальні пристрої можуть оцінювати надані їм дані та змінювати процеси або параметри «на

льоту». Якщо їм надаються достатні дані, вони можуть «вчитися» та змінювати свій власний код на основі нових параметрів.

2. Розумні міста, такі як Барселона, Іспанія, використовують датчики для управління багатьма їхніми системами інфраструктури, такими як транспортний потік, парковка, водокористування та гідроенергія.

Приклад 1: Датчики ваги на стоянках дають змогу водіям швидко дізнатись, де є доступне місце для паркування. Це зменшує час їзди та час простою для водія і знижує викиди вуглекислого газу для довкілля.

Приклад 2: Датчики на світлофорах можуть виявити затори в дорозі. Ці дані надсилаються до комп'ютерної системи, яка збирає дані та приймає рішення. Нові рішення надсилаються на пристрої, які змінюють час червоного та зеленого світла, щоб сприяти потоку трафіку.

3. Уявіть собі рефрижератор, що перевозить заморожені товари, який оснащений глобальним датчиком позиціонування. Коли вантажівка заїжджає у велике місто, датчик визначає, де трапилась аварія, що спричиняє великі затори. Датчик надсилає дані до комп'ютерної системи, яка збирає дані та приймає рішення. Потім система попереджає водія про нові умови, щоб аварію можна було оминути. Ця автоматична взаємодія зберігає час драйвера і швидше доставляє транспортований продукт на ринок, який усе ще заморожений.

4. Самохідні автомобілі революціонують на транспорті. Автомобілі обладнані багатьма датчиками ультразвуку, камерами, точністю GPS та комп'ютерами. Комбінація бортового обладнання дає змогу комп'ютерам ідентифікувати інші автомобілі, смуги, пішоходи та перешкоди. Ця інформація дозволяє автомобілю залишатися на своїй смузі, зупинятися, коли це потрібно, і переплітати навколо перешкод.

Шлях до повної автономії з використанням цієї технології складний. Там були багато високих профілів аварій і деякі серйозні аварії, пов'язані із самохідними машинами. Деякі держави в США вже затвердили обмежене

використання самохідних автомобілів, але дослідники вважають, що за кілька років ця технологія стане основною.

5. Корпоративні офіси можуть займати тисячі співробітників. Зберігання довкілля, таких як освітлення, тепло, вологість у будівлі в межах прийнятних параметрів, допомагає працівникам бути щасливими і, отже, більш продуктивними.

Вказівки до виконання завдання:

Вставте запропоновані слова в потрібні поля : ***проаналізовано; онлайн; цифрова трансформація; розумні пристрої; датчик; безпілотні автомобілі; запрограмований?***

_____ це пристрій, який виявляє чи вимірює подію.

Багато людей вважають за краще купувати послуги та продукти _____.

Штучний інтелект сприяє створенню _____.

_____ це застосування цифрових технологій, що стимулює інновації бізнесу.

Для того, щоби бути корисним підприємствам та урядам, дані мусять бути створені _____.

Якщо _____ це правильно, розумні пристрої можуть навчатися та модифікувати свій власний код на основі нових параметрів.

У світі сьогодні більше _____ ніж людей.

ЧАСТИНА 2
РОЗГОРТАННЯ ТА ПІДКЛЮЧЕННЯ ПРИСТРОЇВ

Програма Packet Tracer імітує мережі та мережевий трафік, а також моделює фізичні аспекти цих мереж. Це передбачає фактичне знаходження та розгортання фізичних пристроїв, налаштовування цих пристроїв та їх підключення. Після фізичного розгортання та підключення проходить час для конфігурації інтерфейсів, які використовуються для підключення пристроїв.

Пошук пристрою для розгортання вимагає перегляду в області вибору типу пристрою. Блок вибору типу пристрою працює з поняттям категорій і підкатегорій.

ЗАВДАННЯ ДО ЧАСТИНИ 2

4 • *Packet Tracer – Розгортання та підключення мережевих пристроїв*

Передумова:

У цьому завданні ви знайдете, розгорнете та з’єднаєте кілька типів мережевих пристроїв.

Вказівки до виконання завдання:

1. Відкрийте файл ***Packet Tracer - Deploying and Cabling Devices.pkt.***

Перед вами з’явиться екран, як показано на рис. 1.1. Якщо файл не відкривається, переконайтеся, що ви правильно встановили прикладну програму Packet Tracer.

2. Дізнайтеся, як розгортати пристрої та підключати їх кабелем у Packet Tracer.

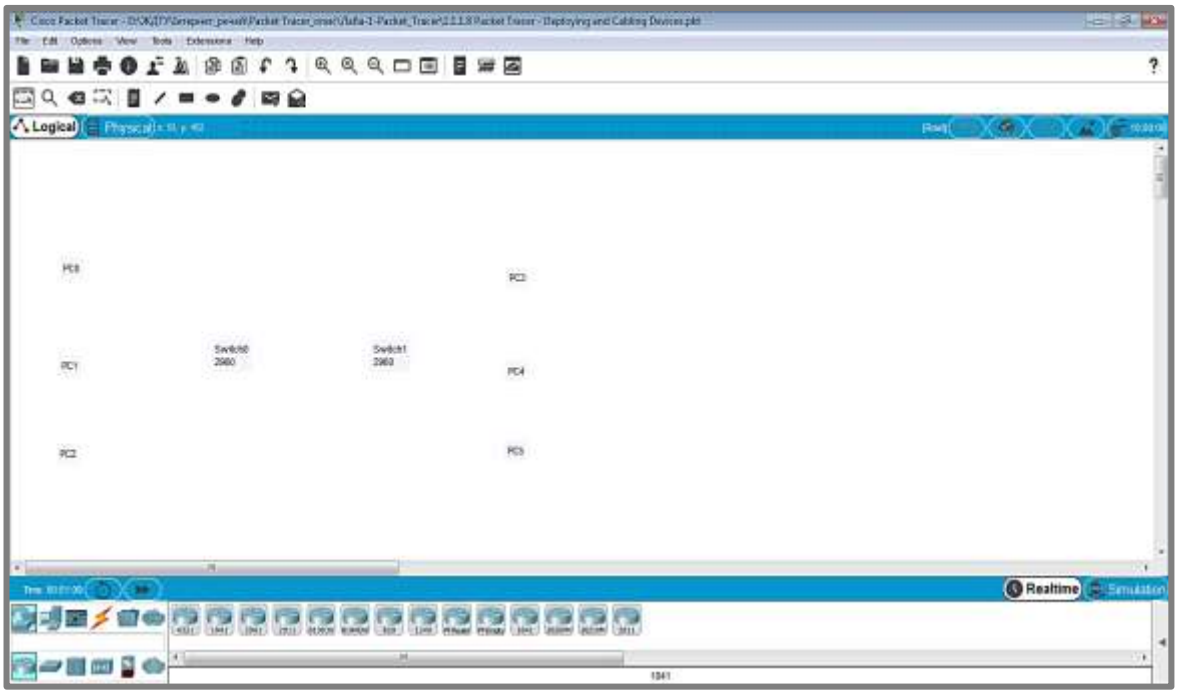


Рисунок 1.1 – Вікно програми Packet Tracer

2.1. Попрактикуйтеся у використанні поля вибору типу пристрою

Верхній ряд піктограм (рис. 1.2) представляє категорії пристроїв, а нижній – підкатегорії. Повільно наведіть курсор на верхній ряд піктограм і подивіться на поле *Label* (*Мітка*) між рядками, з'являться назви категорій. Тепер наведіть курсор на піктограми нижнього ряду, і ви побачите їхні назви.

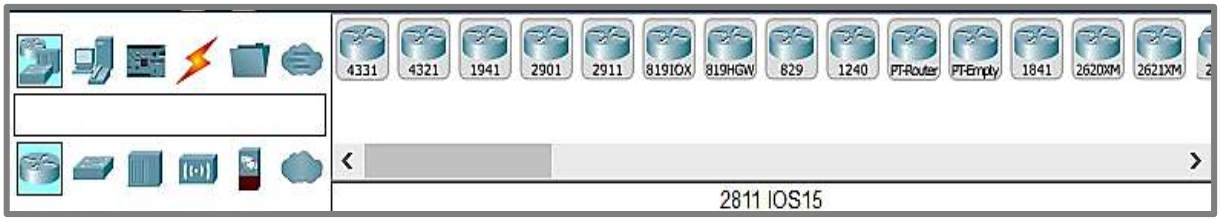


Рисунок 1.2 – Панель пристроїв

У цій роботі ми розгорнемо комутатори та ПК. Наведіть вказівник на піктограми нижнього ряду, доки не побачите одну з позначкою ***Switches*** (Перемикачі). Клацніть цю піктограму, і ви побачите зміни пристроїв у вікні вибору для певного пристрою.

Тепер він показує перемикачі, доступні в Packet Tracer. Розгорніть два комутатори – ***Switches 2960*** над мітками ***Switch0 і Switch1*** у робочій області.

Тепер клацніть категорію ***End Device*** (Кінцевий пристрій) у вікні вибору типу пристрою та розгорніть шість ***PC***. Якщо ви не впевнені, який пристрій є PC, просто наведіть на пристрій у вікні вибору для певного пристрою та подивіться на область напису під пристроями, там має бути написано PC-PT. Тепер ваша робоча область має виглядати як на рис. 1.3.



Рисунок 1.3 – Вибір пристроїв

2.2. Підключення ПК до комутаторів

Клацніть на категорію, яка виглядає як блискавка, з написом ***Connections.*** У вікні ***Device-Specific Box Selection*** з'явиться серія типів кабелю, виберіть тип ***Copper Straight-Through*** (Мідний прямий кабель). Тепер наведіть курсор на центр ***PC0*** і натисніть на нього. Ви побачите спливаюче меню з типами кабельного підключення. Наведіть курсор на пункт ***FastEthernet0*** і клацніть його. Тепер з'явиться провід, прив'язаний до ПК. Наведіть курсор на ***Switch0*** і натисніть на нього. З'явиться ще одне спливаюче меню з набагато більшим набором пунктів вибору, наведіть курсор на пункт ***FastEthernet0/1*** й натисніть його. Кабель буде під'єднано, і з'являться два блимаючих індикатори з'єднання: один зелений і один жовтий. Через деякий час жовтий індикатор стане зеленим із причин, які ви зрозумієте, коли дізнаєтесь про роботу в мережі. Підключіть усі шість ПК до комутаторів (або щоразу вибирайте кабель, або використовуйте клавішу ***Ctrl***). Набір з'єднань, які необхідно виконати наведений на рисунку 1.3.

```
PC1 FastEthernet0 до Switch0 FastEthernet0/2
PC2 FastEthernet0 до Switch0 FastEthernet0/3
PC3 FastEthernet0 до Switch1 FastEthernet0/1
PC4 FastEthernet0 до Switch1 FastEthernet0/2
PC5 FastEthernet0 до Switch1 FastEthernet0/3
```

Рисунок 1.3 – Набір зєднань

2.3. З'єднання двох комутаторів

Тепер нам потрібен інший тип кабелю. Виберіть ***Copper Cross-Over cable*** (Мідний перехресний кабель). Клацніть на ньому, а потім наведіть на ***Switch0*** і натисніть на нього. У спливаючому меню виберіть інтерфейс ***Gigabit0/1*** у нижній частині списку. Потім наведіть курсор і клацніть ***Switch1*** і виберіть той самий інтерфейс із цього списку. З'явиться кабель, й обидва індикатори зв'язку горітимуть жовтим, але приблизно через хвилину вони стануть зеленими. Завершена дія має виглядати так, як на рис. 1.4.

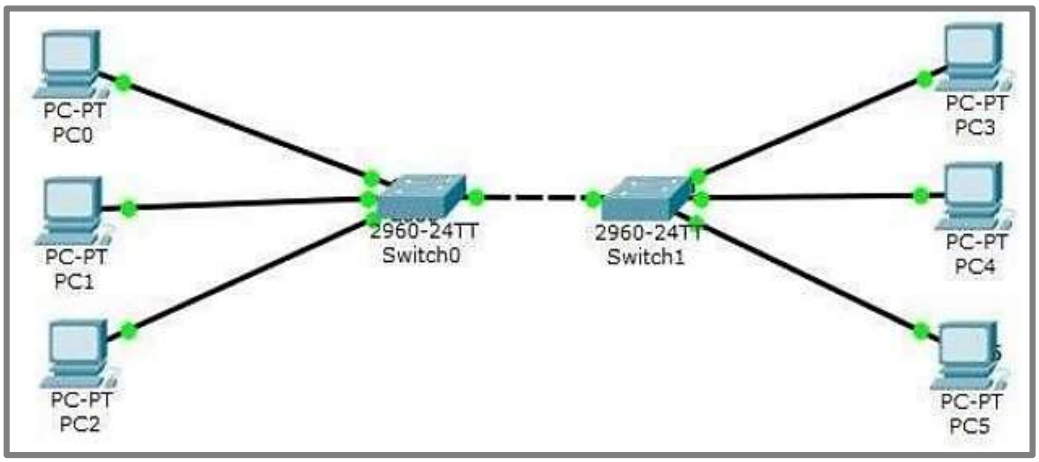


Рисунок 1.4 – З'єднання пристроїв

Якщо ваша робоча область виглядає як наведене вище, збережіть файл і вийдіть з Packet Tracer. Якщо це не так, ви можете повторити ці дії знову, щоби попрактикуватися.

ЧАСТИНА 3
ВСЕ ПОВ'ЯЗАНО ЧЕРЕЗ МЕРЕЖІ

3.1. Мережа – це основа

Тридцять мільярдів речей дають трильйони гігабайт даних. Як вони можуть спільно працювати над покращенням процесу прийняття рішень та вдосконалення нашого життя та нашого бізнесу? Включення цих з'єднань – це мережі, які ми використовуємо щодня. Ці мережі є основою для Інтернету та оцифрованого світу.

Методи, які ми використовуємо для спілкування, продовжують розвиватися. У той час, як ми колись були обмежені кабелями й розетками, прориви в бездротовій і цифровій технології значно розширили доступність наших комунікацій.

Мережі становлять основу оцифрованого світу. Мережі доступні у всіх розмірах. Вони можуть варіюватися від простих мереж, що складаються з двох комп'ютерів, до мереж, що з'єднують мільйони пристроїв.

Прості мережі в будинках дають змогу підключитися до Інтернету. Вони також дозволяють розподіляти ресурси, такі як принтери, документи, зображення та музику, між декількома локальними комп'ютерами.

У бізнесі та великих організаціях мережі можуть надавати продукти та послуги клієнтам через їх підключення до Інтернету. Мережі також можна використовувати в ще більш широкому масштабі, щоб забезпечити консолідацію, зберігання та доступ до інформації на мережевих серверах. Мережі дають можливість використовувати електронні листи, обмін миттєвими повідомленнями та співробітництво між співробітниками. Крім того, мережа забезпечує підключення до нових місць, що дає машинам більшу цінність у промислових умовах.

Інтернет є найбільшою мережею існування та ефективно забезпечує «електронну шкіру», яка оточує планету. Справді, термін «Інтернет» означає «мережа мереж». Інтернет – це буквально сукупність взаємопов'язаних

приватних та громадських мереж. Компанії, невеликі офісні мережі та домашні мережі підключаються до Інтернету.

3.2. Типи мереж

Сучасні мережі можуть бути трохи заплутаними. Є багато типів, які характеризуються географічним розміром, кількістю пристроїв або мереж, з якими вони підключаються, а також тим, чи підтримують вони мобільні пристрої чи ні. Мережі також можуть характеризуватися своєю функцією та призначенням.

Персональна мережа – Personal Area Network (PAN)

Персональні мережі є невеликими мережами, де підключені бездротові пристрої перебувають в межах особистої доступності (рис. 1.5). Прикладом PAN є підключення вашого смартфона до вашої машини через Bluetooth.

Локальна мережа – Local Area Network (LAN)

Локальні мережі, як правило, є мережами в невеликій або локальній географічній зоні, наприклад, вдома, малих підприємствах або відділеннях у великій корпорації (рис. 1.6). Локальні мережі можуть з'єднувати два або більше пристроїв, включно з комп'ютерами, принтерами та бездротовими пристроями. LAN забезпечують доступ до великих широкосмугових мереж (WAN) та Інтернету.



Рисунок 1.5 – Приклад використання PAN

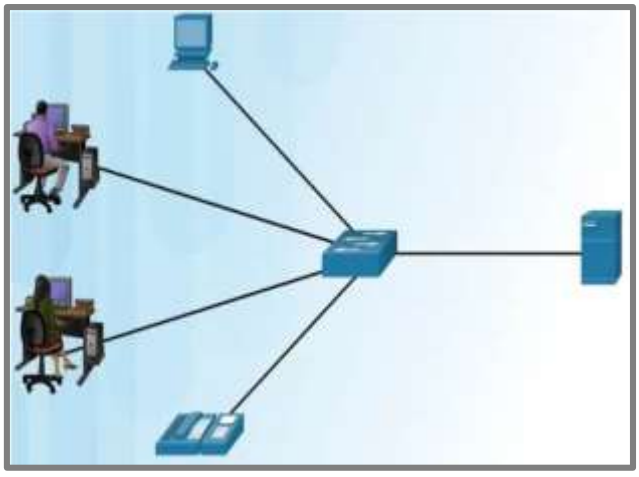


Рисунок 1.6 – Приклад використання LAN

Широкосмугові мережі – Wide Area Networks (WANs, WAN)

Термін WAN зазвичай належить до набору мереж локальної мережі, що забезпечує зв'язок між мережами та Інтернетом для підприємств та урядів (рис. 1.7).

Інтернет – Internet

Інтернет – це багатошарова глобальна мережева система, яка об'єднує сотні мільйонів комп'ютерів. Інтернет не належить жодній особі чи організації. Ця велика система складається з декількох локальних та глобальних мереж, що обслуговують приватні, державні, бізнесові, академічні та державні цілі (рис. 1.8). Це дає змогу обмінюватися даними понад ста Інтернет-сторінками по всьому світу. Це робить Інтернет величезним носієм різних інформаційних ресурсів та послуг. Деякі з них включають текстові та мультимедійні дані, електронну пошту, онлайн-чат, передачу файлів, обмін файлами, електронну комерцію та онлайн-ігри.

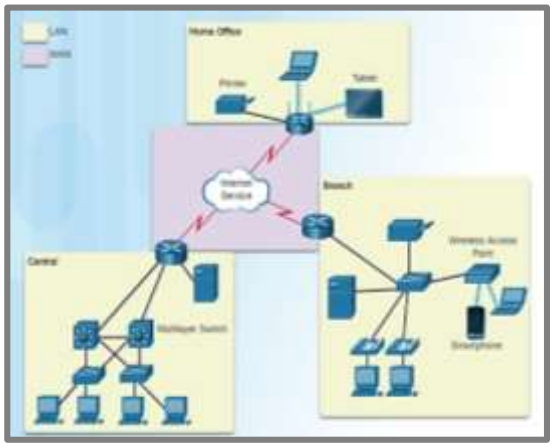


Рисунок 1.7 – Топологія мережі WAN

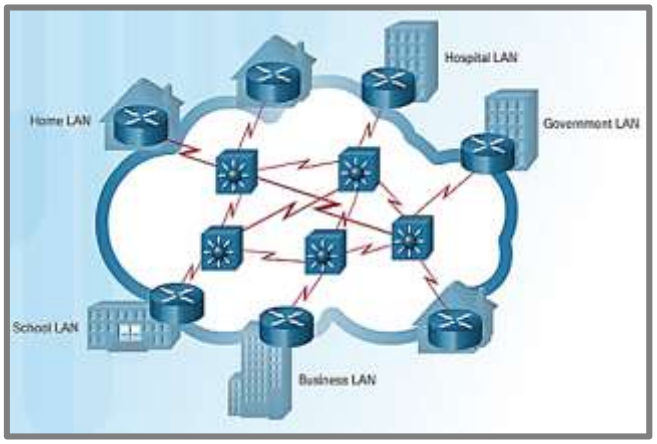


Рисунок 1.8 – Глобальна мережева система Інтернет

Бездротові мережі – Wireless Networks

Бездротові мережі – це ті комп'ютерні мережі, які використовують електромагнітні хвилі замість проводів для передачі сигналів у різні частини мережі. Бездротові мережі можуть бути описані як PAN, LAN або WAN, залежно від їх масштабу.

Оскільки перегляд Інтернету вважається звичайною щоденною активністю, то сьогодні бездротові точки доступу стають загальним місцем в інфраструктурі зв'язку. Публічні місця, пов'язані з Інтернетом, включають бібліотеки, аеропорти, кафе, готелі та спеціалізовані інтернет-кафе. Завдяки технології Wi-Fi, тепер кожна людина може отримати доступ до Інтернету за допомогою ноутбука, планшета або смартфона. На рис. 1.9 показані різні категорії доступних бездротових мереж.

Wireless Networks

Type	Range	Standards
Personal area network (PAN)	Within reach of a person	Bluetooth, ZigBee, NFC
Local area network (LAN)	Within a building or campus	IEEE 802.11 (WiFi)
Metropolitan area network (MAN)	Within a city	IEEE 802.15 (WiMAX)
Wide area network (WAN)	Worldwide	Cellular (UMTS, LTE, etc.)

Рисунок 1.9 – Категорії доступних бездротових мереж

Хмара – Cloud

Термін «хмара» використовується багатьма різними способами. Хмара – не стільки тип мережі, скільки колекція центрів обробки даних або групи підключених серверів, які використовуються для зберігання та аналізу даних, забезпечення доступу до онлайнових програм і надання послуг резервного копіювання для особистого та корпоративного використання (рис. 1.10). Обласні сервіси надаються різними організаціями.

Край – Edge

Край означає фізичний «край» корпоративної мережі.

Туманне обчислення – Fog Computing

Зі зростанням кількості датчиків, які використовуються в Інтернеті речей, часто потрібно зберігати датчики даних надійно і ближче до того, де дані можуть бути проаналізовані. Далі аналізовані дані можуть бути використані швидко й ефективно для оновлення або зміни процесів в організації. На рис. 1.11 показано

приклад розумного міста та обробки даних датчиків. Туман знаходиться на краю ділової або корпоративної мережі. Сервери та комп'ютерні програми дають можливість попередньо обробляти дані для негайного використання. Потім попередньо оброблені дані можна надсилати в хмару для більш глибоких обчислень.

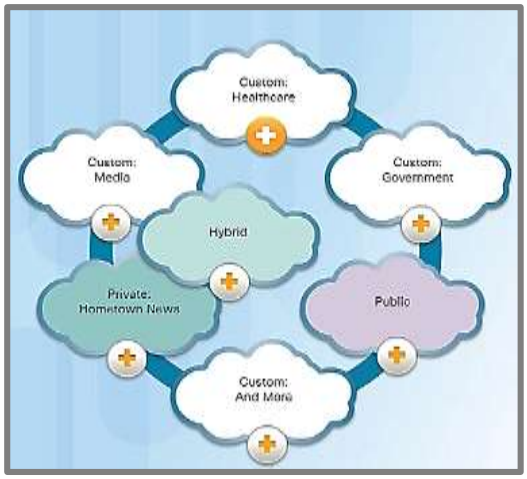


Рисунок 1.10 – Хмарні обчислення

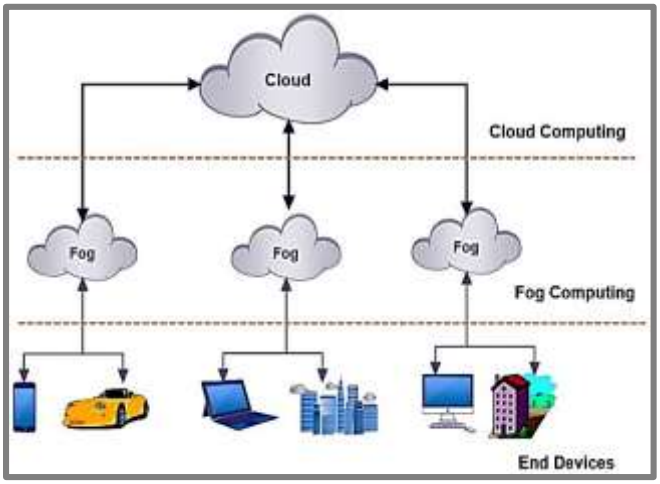


Рисунок 1.11 – Туманні обчислення та Інтернет речей

ЗАВДАННЯ ДО ЧАСТИНИ 3

5 • *Дослідження мережі*

Вказівки до виконання завдання: Дайте відповіді на питання:

Запитання	***Варіанти відповідей***
1. Який тип обчислень дає змогу попередньо обробляти локальні дані на краю мережі?	1. Wireless
	2. Fog
	3. Sensor
	4. Cloud
2. Яке скорочення типу мережі, що дає можливість персональному монітору фітнесу підключатися до смартфону?	1. Internet
	2. LAN
	3. WAN
	4. PAN
	1. Internet

3. Що описується мережею мереж і є найбільшою мережею у світі?	2. Cloud 3. LAN 4. PAN
4. Яка технологія дає можливість бездротовим пристроям підключатися до інших пристроїв на відстані однієї руки?	1. Wi-Fi 2. Cellular 3. Fog Computing 4. Bluetooth
5. Які мережі використовують електромагнітні хвилі замість проводів?	1. Cloud 2. Wireless 3. Internet 4. Ethernet
6. Яка назва набору серверів та центрів обробки даних в Інтернеті, які використовуються для зберігання та доступу до даних у будь-якому місці, у будь-який час та на будь-якому пристрої?	(*запропонувати відповідь*)
7. Що означає акронім для мережі малого бізнесу, який може з'єднати 3 комп'ютери та 4 бездротових пристрої?	(*запропонувати відповідь*)

ЧАСТИНА 4
КАРТОГРАФУВАННЯ МЕРЕЖІ

Сьогодні до інтернету підключено безліч найнесподіваніших, на перший погляд, пристроїв – від нешкідливих вебкамер і телевізорів до систем управління світлофорами й електростанцій. Водночас безпека таких підключень залишає бажати кращого, і здебільшого неживі відвідувачі мережі практично беззахисні перед хакерами й нездатні витримати навіть найпримітивнішу кібератаку.

Картографування мережі – це процес створення мережевих карт для візуалізації мережевих пристроїв, віртуальних доменів, мобільних елементів та взаємозалежностей пристроїв, що допомагає в моніторингу мережі та усуненні несправностей. Картографування мережі – основне завдання, яке потрібно виконати під час моніторингу та управління мережею.

ЗАВДАННЯ ДО ЧАСТИНИ 4

6 • *Картографування мережі Інтернет*

Передумова:

Програмне забезпечення для відстеження маршруту використовується для переліку мереж, якими мають пройти дані від вихідного кінцевого пристрою користувача до віддаленої мережі призначення.

Цей мережевий інструмент зазвичай виконується в командному рядку як:

```
tracert <назва мережі призначення або адреса кінцевого пристрою>
```

(системи Microsoft Windows)

або

```
traceroute <назва мережі призначення або адреса кінцевого пристрою>
```

(Unix та подібні системи)

Утиліти відстеження маршруту дають можливість користувачеві визначати шлях або маршрути, а також затримку в IP-мережі. Є кілька інструментів для виконання цієї функції.

Інструмент ***traceroute*** (або ***tracert***) часто використовується для усунення несправностей мережі. Відображаючи список пройдених маршрутизаторів, він дає змогу користувачеві визначити шлях, яким він дістався до певного пункту призначення в мережі або між мережами. Кожен маршрутизатор представляє точку, де одна мережа з'єднується з іншою мережею і через яку пересилається пакет даних. Кількість маршрутизаторів відома як кількість «стрибків», за якими дані пройшли від джерела до місця призначення.

Відображений список може допомогти виявити проблеми з потоком даних під час спроби отримати доступ до служби, наприклад, вебсайту. Це, також, може бути корисним під час виконання таких завдань, як завантаження даних. Якщо є кілька вебсайтів (дзеркал), доступних для одного файлу даних, можна відстежити кожне дзеркало, щоб отримати гарне уявлення про те, яке дзеркало буде найшвидшим для використання.

Два маршрути трасування між одним і тим же джерелом і місцем призначення, проведені через деякий час окремо, можуть дати різні результати. Це пов'язано із «з'єднаною» природою взаємопов'язаних мереж, які складають Інтернет, і здатністю Інтернет-протоколу вибирати різні шляхи для надсилання пакетів.

Інструменти відстеження маршрутів на основі командного рядка зазвичай вбудовані в операційну систему кінцевого пристрою. Інші інструменти, такі як VisualRoute™, є запатентованими програмами, які надають додаткову інформацію. VisualRoute використовує доступну онлайн-інформацію для графічного відображення маршруту.

Вказівки до виконання завдання:

1. Перевірка підключення до мережі за допомогою Ping

Необхідно визначити, чи доступний віддалений сервер. Щоби простежити маршрут до віддаленої мережі, використовуваний комп'ютер має мати робоче з'єднання з Інтернетом.

1.1. *Перший інструмент, який ми будемо використовувати, це* ***ping***.

Ping – це інструмент, який використовується для перевірки доступності хоста. Пакети інформації надсилаються на віддалений хост з інструкціями щодо відповіді. Ваш локальний ПК вимірює, чи отримано відповідь на кожен пакет, і скільки часу потрібно, щоб ці пакети перетнули мережу. Назва ping походить від технології активного гідролокатора, у якій звуковий імпульс надсилається під водою, щоб відбити рельєф або інші кораблі.

1.2. *На комп'ютері знайдіть «**cmd**» (рис. 1.10).*

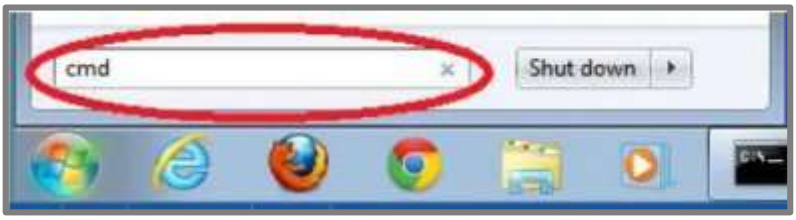


Рисунок 1.10 – Хмарні обчислення

1.3. *У командному рядку введіть **ping www.cisco.com** рис. 1.10).*

```
C:\>ping www.cisco.com

Pinging e144.dscb.akamaiedge.net [23.1.48.170] with 32 bytes of data:
Reply from 23.1.48.170: bytes=32 time=56ms TTL=57
Reply from 23.1.48.170: bytes=32 time=55ms TTL=57
Reply from 23.1.48.170: bytes=32 time=54ms TTL=57
Reply from 23.1.48.170: bytes=32 time=54ms TTL=57

Ping statistics for 23.1.48.170:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 54ms, Maximum = 56ms, Average = 54ms
```

Рисунок 1.10 – Хмарні обчислення

Перший вихідний рядок відображає повне доменне ім'я (FQDN) – *e144.dscb.akamaiedge.net*. Далі йде IP-адреса *23.1.48.170*. Cisco розміщує той самий вебвміст на різних серверах у всьому світу (відомих як дзеркала). Отже, залежно від того, де ви перебуваєте, FQDN та IP-адреса відрізнятимуться.

Із цієї частини виведення (рис. 1.10):

```
Ping statistics for 23.1.48.170:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 54ms, Maximum = 56ms, Average = 54ms
```

Рисунок 1.10 – Хмарні обчислення

було надіслано чотири запити ping, і на кожен запит отримано відповідь. Оскільки на кожен ping відповідали, було 0% втрат пакетів. У середньому потрібно було 54 мс (54 мілісекунди), щоби пакети перетнули мережу.

Потокове відео та онлайн-ігри – це дві програми, які страждають у разі втрати пакетів або повільного з'єднання з мережею. Точніше визначити швидкість з'єднання з Інтернетом можна, надіславши 100 ping замість 4 за замовчуванням. Ось як це зробити (рис. 1.10):

```
C:\>ping -n 100 www.cisco.com
```

Рисунок 1.10 – Хмарні обчислення

Й ось як виглядає результат (рис. 1.10):

```
Ping statistics for 23.45.0.170:
    Packets: Sent = 100, Received = 100, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 46ms, Maximum = 53ms, Average = 49ms
```

Рисунок 1.10 – Хмарні обчислення

1.4. *Тепер пінгуйте вебсайти регіонального Інтернет-реєстру (RIR), які розташовані в різних частинах світу:*

Для Африки:

```
C:\> ping www.afrinic.net
```

Для Австралії:

```
C:\> ping www.apnic.net
```

Для Європи:

```
C:\> ping www.ripe.net
```

Для Південної Америки:

```
C:\> ping www.lacnic.net
```

Усі ці запити ping були запущені з комп'ютера, розташованого в Україні.

Що відбувається із середнім часом ping у мілісекундах, коли дані переміщуються в межах одного континенту (Європа), в порівнянні з даними з Європи, які переміщуються на різні континенти?

Відповідь:_____

Що Ви можете сказати про ping, які були відправлені на вебсайт Південної Америки?

Відповідь:_____

2. Трасування маршруту до віддаленого сервера за допомогою Tracert

Необхідно визначити, який маршрут Інтернет-трафіка йде до віддаленого сервера. Тепер, коли базову доступність перевірено за допомогою інструмента ping, корисно уважніше розглянути кожен сегмент мережі, який перетинається. Для цього буде використано інструмент ***tracert.***

2.1. *У командному рядку введіть tracert www.cisco.com (рис. 1.10)*

```
C:\>tracert www.cisco.com

Tracing route to e144.dscb.akamaiedge.net [23.1.144.170]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  dslrouter.westell.com [192.168.1.1]
  2    38 ms    38 ms    37 ms  10.18.20.1
  3    37 ms    37 ms    37 ms  G3-0-9-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.196.190]
  4    43 ms    43 ms    42 ms  so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5    43 ms    43 ms    65 ms  0.so-4-0-2.XT2.NYC4.ALTER.NET [152.63.1.57]
  6    45 ms    45 ms    45 ms  0.so-3-2-0.XL4.EWR6.ALTER.NET [152.63.17.109]
  7    46 ms    48 ms    46 ms  TenGigE0-5-0-0.GW8.EWR6.ALTER.NET [152.63.21.14]

  8    45 ms    45 ms    45 ms  a23-1-144-170.deploy.akamaitechnologies.com [23.
1.144.170]

Trace complete.
```

Рисунок 1.10 – Хмарні обчислення

2.2. *Збережіть результат* ***tracert*** *у текстовому файлі таким чином:*

1. Клацніть правою кнопкою миші рядок заголовка вікна командного рядка та виберіть ***Edit / Select All*** (Правка / Вибрати все).
2. Знову клацніть правою кнопкою миші рядок заголовка вікна командного рядка та виберіть ***Edit / Copy*** (Правка / Копіювати).
3. Знайдіть і відкрийте ***Блокнот***.
4. Щоб вставити результат у блокнот, виберіть ***Edit / Paste*** (Правка / Вставити).
5. Виберіть ***File / Save As*** (Файл / Зберегти як) і збережіть файл «Блокнот» як ***tracert1.txt***.

2.3. *Інтерпретація результату* ***tracert.***

Маршрути, що відстежуються, можуть проходити через багато стрибків і кілька різних Інтернет-провайдерів (ISP), залежно від розміру вашого Інтернет-провайдера та розташування хостів джерела та призначення. Кожен «стрибок» представляє маршрутизатор.

Оскільки комп’ютери говорять цифрами, а не словами, маршрутизатори унікально ідентифікуються за допомогою IP-адрес (числа у форматі xxxx для адрес IPv4). Інструмент tracert показує, який шлях через мережу проходить пакет інформації, щоб досягти кінцевого пункту призначення. Інструмент tracert також дає вам уявлення про швидкість трафіка в кожному сегменті мережі. На кожен маршрутизатор на шляху надсилається три пакети, а час повернення вимірюється в мілісекундах. Покажемо розбивку (рис. 1.10):

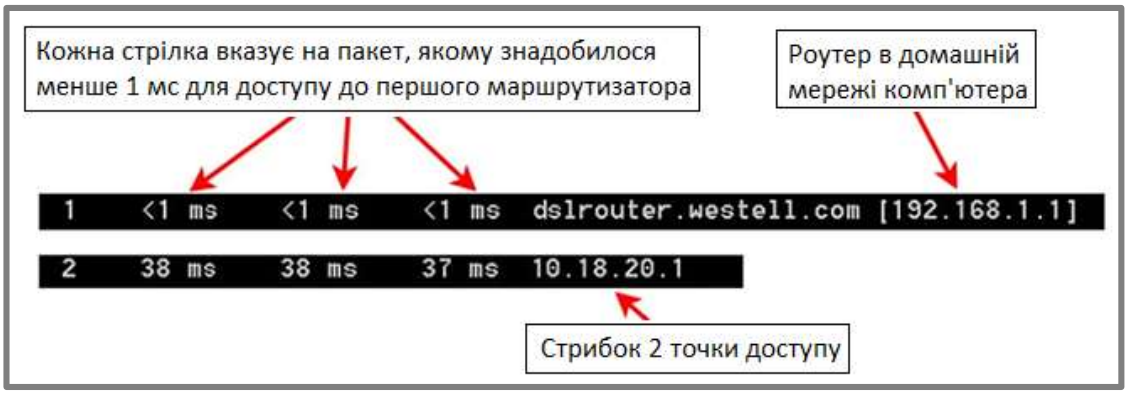


Рисунок 1.10 – Хмарні обчислення

У наведеному вище прикладі вихідних даних пакети tracert переміщуються від вихідного ПК до шлюзу за замовчуванням локального маршрутизатора (стрибок 1: 192.168.1.1) до маршрутизатора точки присутності ISP (POP) (стрибок 2: 10.18.20.1). Кожен Інтернет-провайдер (ISP) має численні маршрутизатори POP. Ці POP-маршрутизатори знаходяться на межі мережі провайдера і є засобом, за допомогою якого клієнти підключаються до Інтернету. Пакети подорожують у мережі Verizon упродовж двох стрибків, а потім переходять на маршрутизатор, який належить alter.net. Це може означати, що пакети потрапили до іншого провайдера. Це важливо, оскільки іноді відбувається втрата пакетів під час переходу між провайдерами Інтернет-послуг, або іноді один провайдер працює повільніше, ніж інший.

Є Інтернет-інструмент, відомий як ***Whois***. Інструмент Whois дає можливість нам визначити, хто є власником доменного імені. Вебінструмент Whois можна знайти за адресою: http://whois.domaintools.com/.

Згідно з вебінструментом Whois, цей домен також належить Verizon (рис. 1.10).



Whois Record for Alter.net

— Domain Profile

Registrant Org	Verizon Business Global LLC
Registrant Country	us
Registrar	MarkMonitor, Inc. MarkMonitor Inc. IANA ID: 292 URL: http://www.markmonitor.com Whois Server: whois.markmonitor.com abusecomplaints@markmonitor.com (p) 12086851750
Registrar Status	clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited
Dates	11,858 days old Created on 1990-07-26 Expires on 2023-07-25 Updated on 2022-06-23
Name Servers	AUTH00.NS.UU.NET (has 24,587 domains) AUTH200.NS.UU.NET (has 24,587 domains) AUTH210.NS.UU.NET (has 24,587 domains) AUTH60.NS.UU.NET (has 24,587 domains)

Рисунок 1.10 – Хмарні обчислення

Отже, Інтернет-трафік починається на домашньому комп'ютері та проходить через домашній маршрутизатор (стрибок 1). Потім він підключається до провайдера та подорожує через його мережу (стрибки 2–7), поки не досягне віддаленого сервера (стрибок 8). Це відносно незвичайний приклад, коли від початку до кінця бере участь лише один провайдер. Як правило, залучено два або більше провайдерів, як показано в наведених нижче прикладах.

2.4. *Розглянути Інтернет-трафік, що перетинає кілька провайдерів.*

Запустіть ***tracert*** для кожного цільового вебсайту та збережіть вихідні дані у файлах із послідовною нумерацією:

```
C:\> tracert www.afrinic.net
```

```
C:\> tracert www.lacnic.net
```

Що відбувається на 7-му етапі? Чи змінюються на стрибках провайдери? Щоб відповісти на це запитання, скористайтеся інструментом Whois. Кому належать ці мережі?

Відповідь:_____

Що відбувається на стрибках із часом, який потрібен пакету для подорожі? Порівняйте декілька стрибків.

Відповідь:_____

3. Трасування маршруту до віддаленого сервера за допомогою вебінтерфейсу та програмного забезпечення

Використовуйте вебінструмент traceroute: http://www.subnetonline.com/pages/network-tools/online-tracepath.php, щоби простежити маршрут до таких вебсайтів:

- www.cisco.com
- www.afrinic.net

Захопіть і збережіть результат у Блокноті.

Чим відрізняється traceroute під час переходу на www.cisco.com із командного рядка (див. п. 2), а не з онлайн-сайту? (Ваші результати можуть відрізнятися залежно від вашого географічного розташування та того, який провайдер надає вам підключення.)

Відповідь:_____

Порівняйте tracert із п. 2, який надсилає в Африку, з tracert, який надходить до Африки через вебінтерфейс. Яку різницю ви помічаєте?

Відповідь:_____



ВИМОГИ ДО ОФОРМЛЕННЯ ЗВІТУ

1. *Сформуйте файл для звіту. Звіт про виконання роботи має включати:*

- Титульний аркуш, вказуючи номер і назву роботи, прізвище і групу студента.

- Покроковий опис основних етапів виконання роботи. Отримані результати підтверджуються скріншотами екрану.
- Відповіді на поставлені запитання до кожного завдання.
- Висновки щодо проведеної роботи.

2. *За завданнями 4 створений файл із назвою LR-1_XXXXX.pkt, де XXXXX – позначення прізвища студента.*



КОНТРОЛЬНІ ЗАПИТАННЯ

1. Який тип мережі використовується для з’єднання компанії, розташованої в одному районі міста, з іншим місцем у далекому місті?
2. Що складається з мільйонів розумних пристроїв і датчиків, підключених до Інтернету?
3. Яка найбільша мережа з існуючих?
4. Що таке хмарні обчислення?
5. Який інструмент дає змогу користувачеві імітувати реальні мережі?
6. Що дає можливість цифровим пристроям з’єднуватися та передавати дані?
7. Для чого використовують утиліти відстеження маршруту?
8. Яка команда використовується для перевірки підключення до мережі та надання відповіді на кожен пакет, отриманий віддаленим хостом?
9. Які є методи трасування маршруту?

ЛАБОРАТОРНА РОБОТА № 2
СТВОРЕННЯ ПРОСТОЇ МЕРЕЖІ ЗА ДОПОМОГОЮ PACKET TRACER

Мета роботи: створення простої мережі логічної топології в робочому просторі Packet Tracer та налаштування мережевих пристроїв із подальшою перевіркою з'єднання.

ЗАВДАННЯ ДО ВИКОНАННЯ РОБОТИ

1. Створення простої мережі в робочому просторі логічної топології

1.1. *Запустіть Packet Tracer на ПК. Packet Tracer має відкритися з порожньою робочою областю логічної топології за умовчанням.*

1.2. *Використовуючи поле вибору пристрою, додайте мережеві пристрої до робочого простору, як показано на схемі топології (рис. 2.1).*

Щоб розмістити пристрій у робочому просторі, спочатку виберіть тип пристрою з ***Device-Type Selection***. Потім натисніть потрібну модель пристрою у вікні вибору. Нарешті, клацніть місце в робочій області, щоб розмістити свій пристрій у цьому місці. Якщо ви хочете скасувати свій вибір, клацніть значок ***Cancel*** (Скасувати) для цього пристрою. Крім того, ви можете натиснути та просто перетягнути пристрій із вікна вибору для певного пристрою в робочу область. Для ***Wireless Router*** (бездротового маршрутизатора) виберіть пристрій ***WRT300N***.

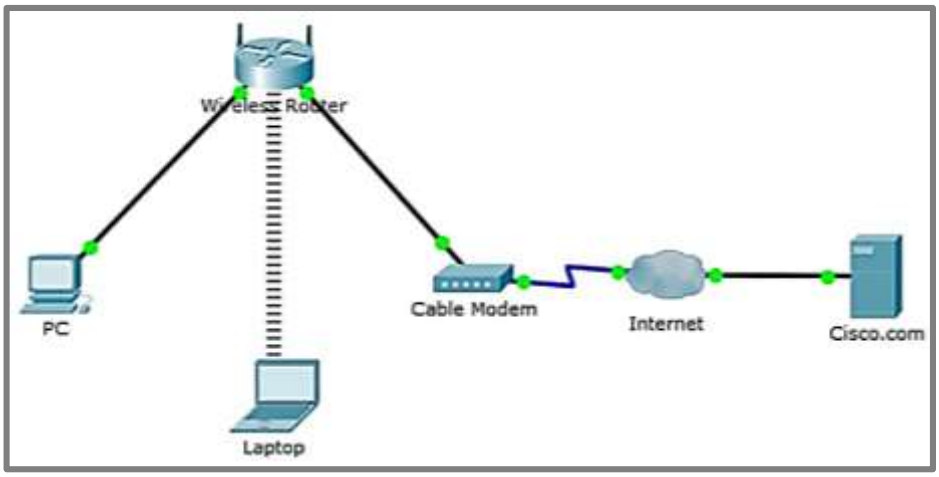


Рисунок 2.1 – Топологія мережі

1.3. *Змініть відображувані назви нових пристроїв.*

Щоб змінити відображувані назви мережевих пристроїв, натисніть піктограму пристрою в логічній робочій області Packet Tracer, а потім клацніть вкладку ***Config*** (Конфігурація) у вікні конфігурації пристрою. На вкладці ***Config*** введіть нове ім’я пристрою в поле ***Display Name***, як показано на рис. 2.2.



Рисунок 2.2 – Зміна назви пристрою

1.4. *Додайте фізичні кабелі між пристроями в робочій області.*

Використовуючи поле вибору пристрою, додайте фізичні кабелі між пристроями в робочій області, як показано на схемі топології (рис. 2.1).

Для підключення ***Wireless Router*** (Бездротового маршрутизатора) до PC знадобиться ***Copper straight-through cable*** (Мідний прямий кабель). Виберіть мідний прямий кабель у полі ***Device-Type Selection*** та під’єднайте його до порту

FastEthernet0 інтерфейсу PC та інтерфейсу ***Ethernet 1*** бездротового маршрутизатора Wireless Router.

Для підключення бездротового маршрутизатора до кабельного модему ***Cable Modem*** потрібен ***Copper straight-through cable*** (Мідний прямий кабель). Виберіть мідний прямий кабель у вікні вибору пристрою та під'єднайте його до ***Internet*** інтерфейсу бездротового маршрутизатора та ***Port 1*** інтерфейсу кабельного модему.

Для підключення до Інтернет-хмари кабельному модему знадобиться ***Coaxial cable*** (Коаксіальний кабель). Виберіть коаксіальний кабель у полі ***Device-Type Selection*** та підключіть його до інтерфейсу ***Port 0*** кабельного модему та ***Coaxial*** інтерфейсу Інтернет-хмари.

Для підключення до сервера Cisco.com хмарі Internet знадобиться мідний прямий кабель. Виберіть мідний прямий кабель у полі ***Device-Type Selection*** та підключіть його до інтерфейсу ***Ethernet*** Інтернет-хмари та інтерфейсу ***FastEthernet0*** сервера Cisco.com.

2. Налаштування мережевих пристроїв

2.1. Налаштуйте бездротовий маршрутизатор.

Необхідно створити бездротову мережу на бездротовому маршрутизаторі. Натисніть піктограму ***Wireless Router*** в логічній робочій області Packet Tracer, щоб відкрити вікно конфігурації пристрою.

У вікні конфігурації бездротового маршрутизатора натисніть вкладку ***GUI***, щоби переглянути параметри конфігурації бездротового маршрутизатора.

Далі клацніть вкладку ***Wireless*** (Бездротовий зв'язок) у графічному інтерфейсі користувача, щоби переглянути параметри бездротового зв'язку. Єдине налаштування, яке потрібно змінити в порівнянні зі значеннями за замовчуванням, це ім'я мережі ***Network Name (SSID)***. Тут введіть назву ***HomeNetwork*** (Домашня мережа), як показано на рис. 2.3.

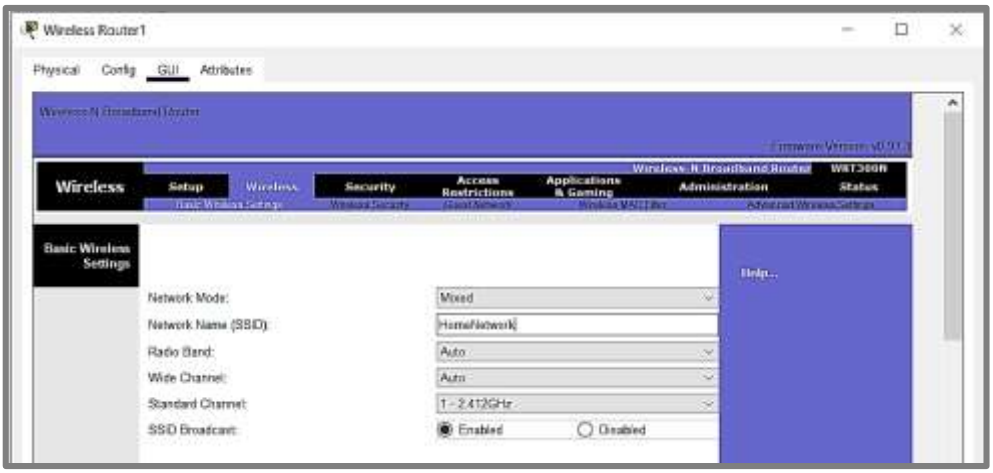


Рисунок 2.3 – Налаштування мережі для Wireless Router

2.2. *Налаштуйте підключення до Інтернету на бездротовому маршрутизаторі.*

Натисніть вкладку ***Setup*** (Налаштування) у графічному інтерфейсі ***GUI*** бездротового маршрутизатора. У налаштуваннях сервера ***DHCP Server*** переконайтеся, що вибрано кнопку ***Enabled*** (Увімкнено), і налаштуйте статичну IP-адресу DNS-сервера ***Static DNS*** як ***208.67.220.220***, що показано на рис. 2.4. Клацніть вкладку ***Save Settings*** (Зберегти налаштування).

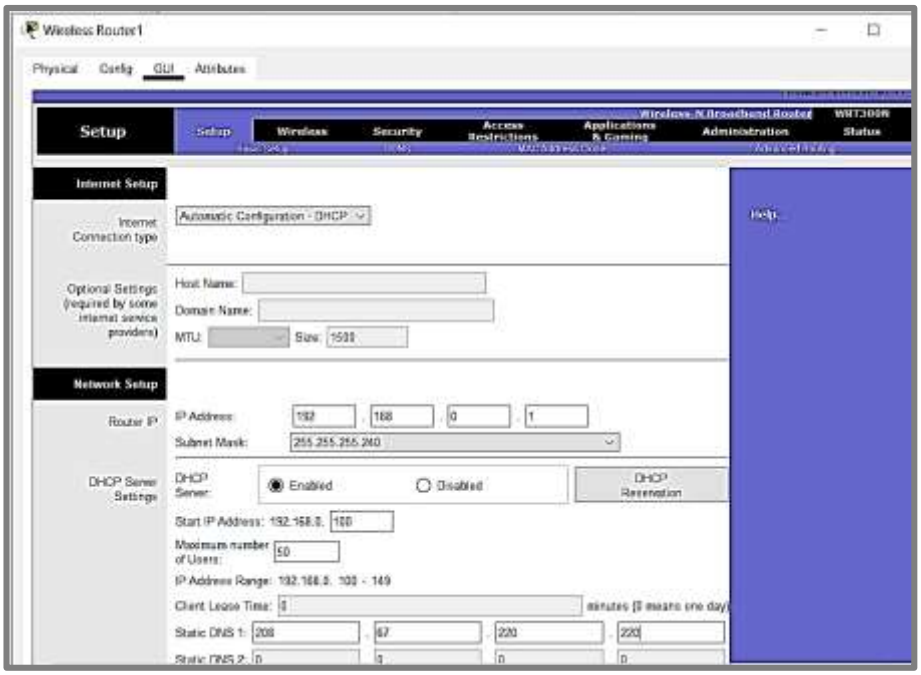


Рисунок 2.4 – Налаштування Static DNS

2.3. *Налаштуйте ноутбук для доступу до бездротової мережі.*

Клацніть піктограму ноутбука ***Laptop*** в логічній робочій області Packet Tracer і у вікні конфігурації ноутбука виберіть вкладку ***Physical*** (Фізичні). На вкладці ***Physical*** вам потрібно буде видалити мідний модуль ***Ethernet*** і замінити його модулем ***Wireless WPC300N***.

Для цього спочатку вимкніть ноутбук, натиснувши кнопку живлення збоку ноутбука. Потім видаліть наразі встановлений мідний модуль ***Ethernet***, клацнувши модуль збоку ноутбука та перетягнувши його на панель ***MODULES*** ліворуч від вікна ноутбука. Потім інсталюйте модуль ***Wireless WPC300N***, натиснувши його на панелі ***MODULES*** та перетягнувши до порожнього порту модуля збоку ноутбука. Увімкніть ноутбук, знову натиснувши кнопку живлення ноутбука.

Після встановлення бездротового модуля наступне завдання – підключити ноутбук до бездротової мережі. Натисніть вкладку ***Desktop*** (Робочий стіл) у верхній частині вікна конфігурації ноутбука та виберіть піктограму ***PC Wireless*** (Бездротовий зв'язок ПК). Коли параметри Wireless-N Notebook Adapter стануть видимими, виберіть вкладку ***Connect***. Бездротова мережа ***HomeNetwork*** має бути видимою в списку бездротових мереж, як показано на рис. 2.5.

Виберіть мережу та клацніть вкладку ***Connect*** (Підключити), що розташована під інформацією про сайт ***Site Information***.



Рисунок 2.5 – Налаштування Laptop для доступу до Wireless

2.4. *Налаштуйте ПК для дротової мережі.*

Клацніть піктограму ***PC*** у логічній робочій області Packet Tracer і виберіть вкладку ***Desktop***, а потім піктограму ***IP Configuration***.

У вікні IP Configuration виберіть перемикач ***DHCP***, як показано на рис.2.6, щоби ПК використовував DHCP для отримання адреси IPv4 від бездротового маршрутизатора. Закрийте вікно ***IP Configuration***.

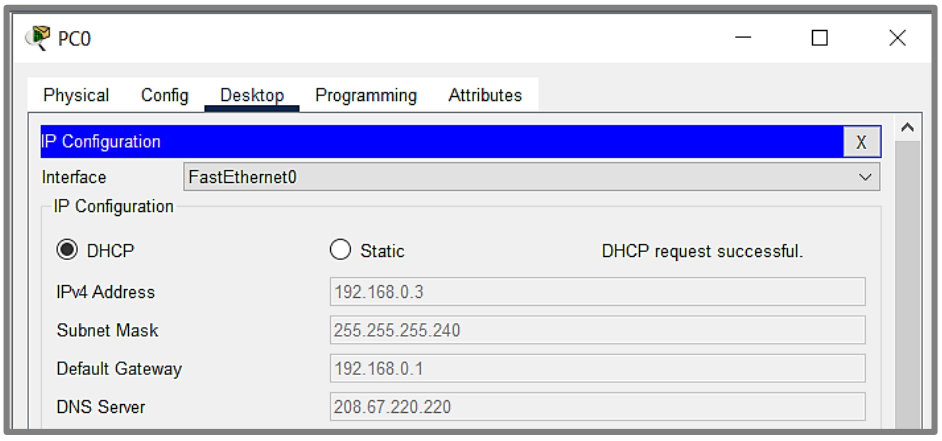


Рисунок 2.6 – Вибір перемикача DHCP

Клацніть піктограму командного рядка ***Command Prompt***. Переконайтеся, що ПК одержав адресу IPv4, виконавши команду ***ipconfig /all*** із команди, як показано на рис. 2.7. ПК має дістати адресу IPv4 у діапазоні 192.168.0.x.

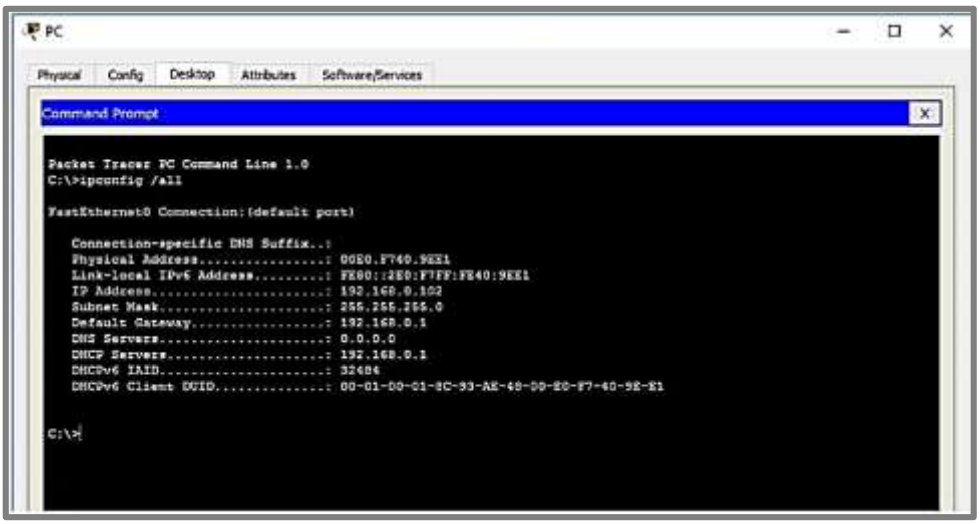


Рисунок 2.7 – Отримання адреси IPv4 за допомогою командного рядка

2.5. *Налаштуйте Інтернет-хмару, за необхідності встановіть мережеві модулі.*

Клацніть піктограму Інтернет-хмари в логічній робочій області Packet Tracer, а потім клацніть вкладку ***Physical***. Для хмарного пристрою знадобляться два модулі, якщо вони ще не встановлені. ***PT-CLOUD-NM-1CX*** призначений для підключення служби кабельного модему та ***PT-CLOUD-NM-1CFE*** – для підключення мідного кабелю Ethernet. Якщо ці модулі відсутні, вимкніть живлення фізичних хмарних пристроїв, натиснувши кнопку живлення, перетягніть кожен модуль у порожній порт модуля на пристрої, а потім знову ввімкніть пристрій.

Визначте тип провайдера. Перебуваючи на вкладці ***Config***, клацніть ***Ethernet*** у розділі ***INTERFACE*** на лівій панелі. У вікні конфігурації ***Ethernet*** виберіть ***Cable***, як мережу провайдера, що показано на рис. 2.8.

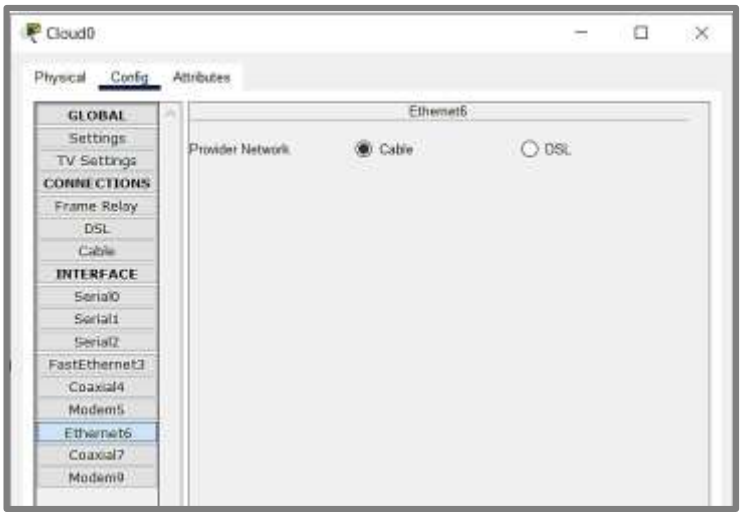


Рисунок 2.8 – Вибір Cable

Визначте порти From і To. Натисніть вкладку ***Config*** у вікні Хмарного пристрою. На лівій панелі клацніть ***Cable*** у розділі ***CONNECTIONS***. У першому спадаючому списку виберіть ***Coaxial***, а в другому – ***Ethernet***, а потім натисніть кнопку ***Add*** (Додати), щоб додати їх як ***From Port*** та ***To Port***, як показано на рис. 2.9.

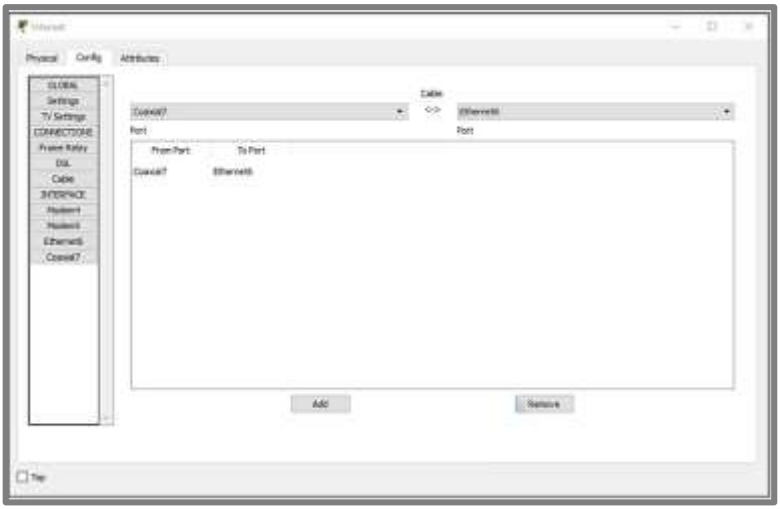


Рисунок 2.9 – Визначення портів From і To

2.6. Налаштуйте сервер Cisco.com, як сервер DHCP.

Натисніть піктограму сервера Cisco.com у логічній робочій області Packet Tracer і виберіть вкладку ***Services*** (Служби). Виберіть ***DHCP*** зі списку ***SERVICES*** на лівій панелі.

1) У вікні конфігурації DHCP налаштуйте DHCP, як показано на рис. 2.10, з такими параметрами.

- Натисніть ***On***, щоб увімкнути службу DCHP.
- Назва пулу: ***DHCPpool.***
- Default Gateway: ***208.67.220.220.***
- DNS Server: ***208.67.220.220.***
- Starting IP Address: ***208.67.220.1.***
- Subnet Mask ***255.255.255.0.***
- Maximum number of Users: ***50.***

Натисніть ***Add***, щоб додати пул.

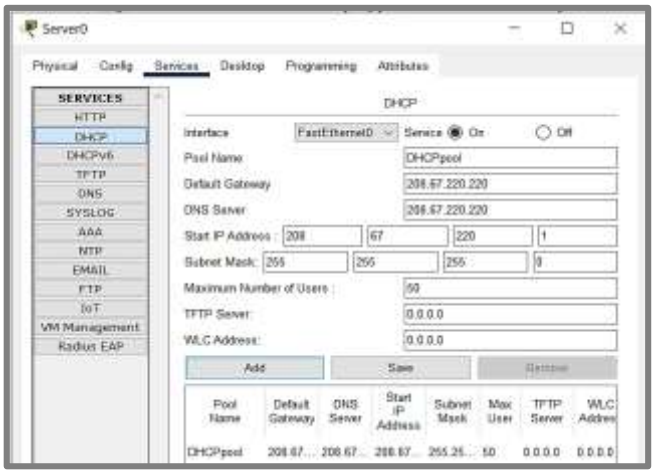


Рисунок 2.10 – Налаштування DHCP

2) Налаштуйте сервер Cisco.com як DNS-сервер, щоб забезпечити роздільну здатність доменного імені до адреси IPv4.

Перебуваючи на вкладці ***Services***, виберіть ***DNS*** із ***SERVICES***, перелічених на лівій панелі. Налаштуйте службу DNS за допомогою наведених нижче параметрів, як показано на рис. 2.11.

- Натисніть ***On***, щоб увімкнути службу ***DNS.***
- Name: ***Cisco.com.***
- Type: ***A Record.***
- Address: ***208.67.220.220.***

Натисніть ***Add***, щоб додати налаштування служби DNS.

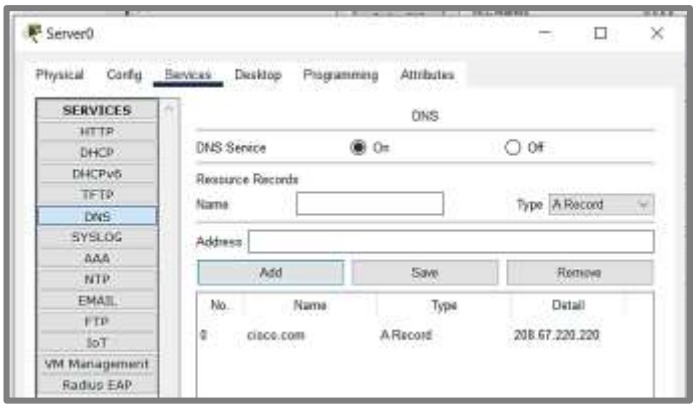


Рисунок 2.11 – Налаштування служби DNS

3) Налаштуйте глобальні параметри сервера Cisco.com.

Виберіть вкладку ***Config.*** Натисніть ***Settings*** на лівій панелі. Налаштуйте глобальні параметри сервера таким чином (рис. 2.12):

- Виберіть ***Static.***
- Gateway: ***208.67.220.1.***
- DNS Server: ***208.67.220.220.***

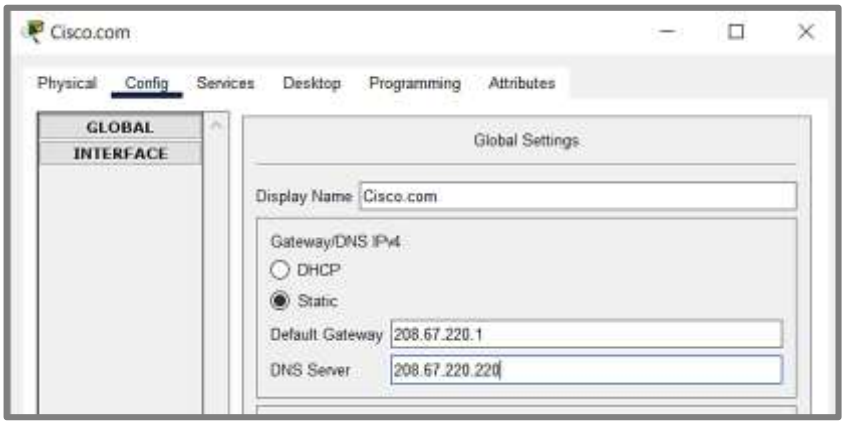


Рисунок 2.12 – Налаштування глобальних параметрів сервера Cisco.com

4) Налаштуйте параметри інтерфейсу FastEthernet0 сервера Cisco.com.

Клацніть ***FastEthernet*** на лівій панелі вкладки ***Config.*** Налаштуйте параметри інтерфейсу FastEthernet сервера таким чином (рис. 2.13):

- Виберіть ***Static*** у розділі ***IP Configuration***.

- IP Address: ***208.67.220.220.***
- Subnet Mask: ***255.255.255.0.***

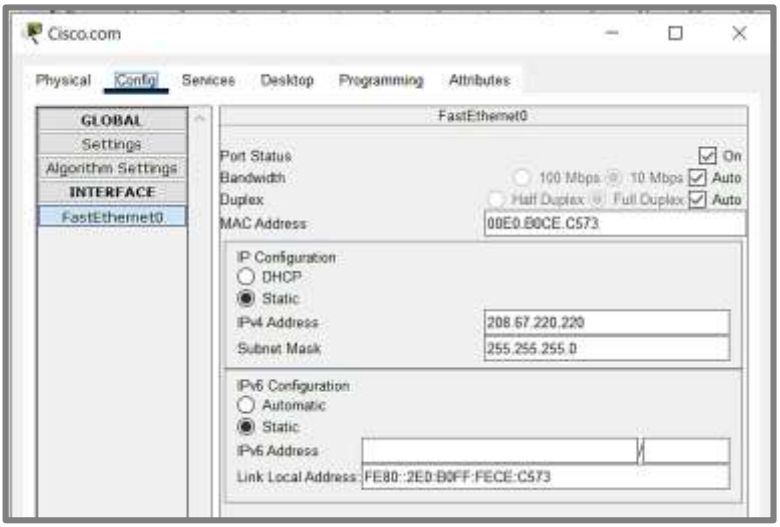


Рисунок 2.13 – Налаштування параметрів інтерфейсу FastEthernet

3. Перевірка з'єднання між мережевими пристроями

3.1. *Оновіть налаштування IPv4 на ПК. Переконайтеся, що ПК одержує конфігураційну інформацію IPv4 від DHCP.*

Натисніть ***PC*** у логічній робочій області Packet Tracer, а потім виберіть вкладку ***Desktop*** у вікні конфігурації ***PC***. Клацніть піктограму командного рядка ***Command Prompt.*** У командному рядку оновіть параметри IP, виконавши команди ***ipconfig /release***, а потім ***ipconfig /renew***. Вихідні дані мають показати, що ПК має IP-адресу в діапазоні 192.168.0.x, маску підмережі, шлюз за замовчуванням і адресу DNS-сервера, як показано на рис. 2.14.

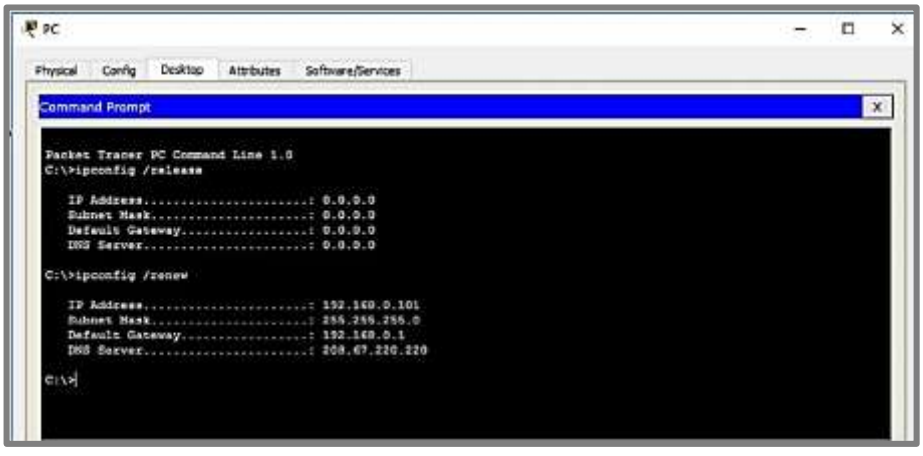


Рисунок 2.14 – Оновлення параметрів IP у командному рядку

3.2. *Перевірте підключення до сервера Cisco.com з ПК.*

З командного рядка ***Command Prompt*** виконайте команду ***ping Cisco.com***. Для повернення ping може знадобитися кілька секунд. Має бути отримано чотири відповіді, як показано на рис. 2.15.

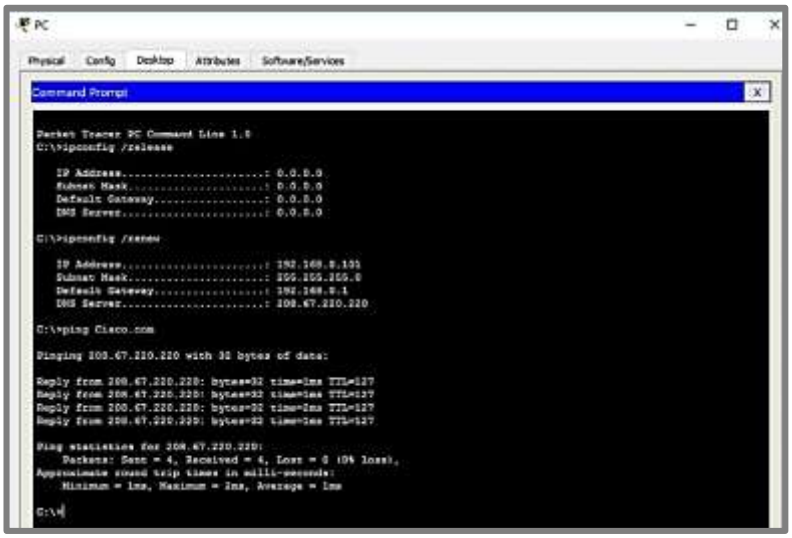


Рисунок 2.15 – Результат пінгування

4. ***Збережіть файл, як файл Packet Tracer (*.pkt).***

ВИМОГИ ДО ОФОРМЛЕННЯ ЗВІТУ

1. Сформуйте файл для звіту. Звіт про виконання роботи має включати:

- Титульний аркуш, вказуючи номер і назву роботи, прізвище і групу студента.
- Покроковий опис основних етапів виконання роботи. Отримані результати підтверджуються скріншотами екрану.
- Висновки щодо проведеної роботи.

2. Створений файл із назвою LR-2_XXXXX.pkt, де XXXXX – позначення прізвища студента.



КОНТРОЛЬНІ ЗАПИТАННЯ

1. Яке призначення програми Cisco Packet Tracer?
2. Які мережеві симулятори ви знаєте?
3. Які типи мережевих з’єднань в Packet Tracer ви знаєте?
4. Яке призначення утиліти ip config?
5. Яке призначення утиліти ping?
6. Який слід використовувати кабель при підключенні двох ПК між собою?
7. На якому рівні моделі OSI працює комутатор?
8. Перерахуйте всі можливі режими роботи програми Cisco Paket Tracer?
9. Навіщо призначений протокол DHCP?
10. Вкажіть особливості протоколу DHCP.
11. Що таке DHCP пул?
12. Які параметри вказуються при налаштуванні протоколу DHCP?

ЛАБОРАТОРНА РОБОТА № 3
ПІДКЛЮЧЕННЯ ПРИСТРОЇВ ІОТ ДО РОЗУМНОГО БУДИНКУ

Мета роботи: дослідження пристроїв, які присутні в мережі та додавання IoT компонентів, які можна під'єднати через кабель та бездротову мережу за використання файлу Packet Tracer зі створеною домашньою мережею.

ВКАЗІВКИ ДО ВИКОНАННЯ РОБОТИ

1. Дослідження наявної мережі Smart Home

1.1. Відкрийте файл **Packet Tracer - Adding IoT Devices to a Smart Home.pkt** та збережіть файл на комп'ютері.

1.2. Дослідіть мережу розумного дому

1) Дослідіть кінцеві пристрої IoT. У нижньому лівому куті вікна Packet Tracer знайдіть і клацніть піктограму **End Devices** у верхньому рядку та піктограму **Home** у нижньому рядку поля **Device-Type Selection** (рис. 3.1).

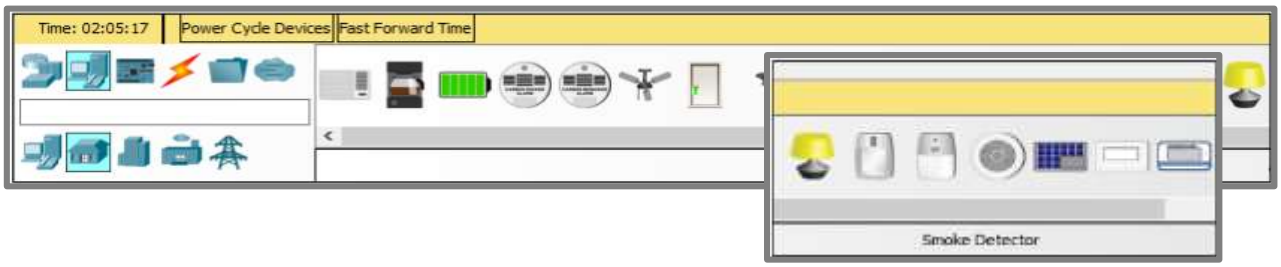


Рисунок 3.1 – Компоненти вкладки Home

У нижній частині вікна Packet Tracer у полі **Device-Specific Selection** відображається багато різних доступних пристроїв Smart Home IoT.

Наведіть вказівник миші на кожен пристрій і зверніть увагу, що описове ім'я пристрою відображається внизу вікна **Device-Specific Selection**. Зверніть увагу на кожен тип пристрою.

2) Дослідіть мережу Smart Home.

Логічне робоче середовище – це попередньо побудована розумна домашня мережа, яка складається з багатьох дротових і бездротових пристроїв Інтернету речей, а також пристроїв мережевої інфраструктури (рис. 3.2). Коли ви накладаєте курсор на пристрій, наприклад, **Smart Fan**, відкривається інформаційне вікно, що містить основну мережеву інформацію про цей пристрій.

Щоб увімкнути або активувати пристрій, просто утримуйте клавішу **Alt** на клавіатурі, а потім клацніть пристрій лівою кнопкою миші. Спробуйте це на кожному з розумних пристроїв, щоби поспостерігати, що вони роблять.

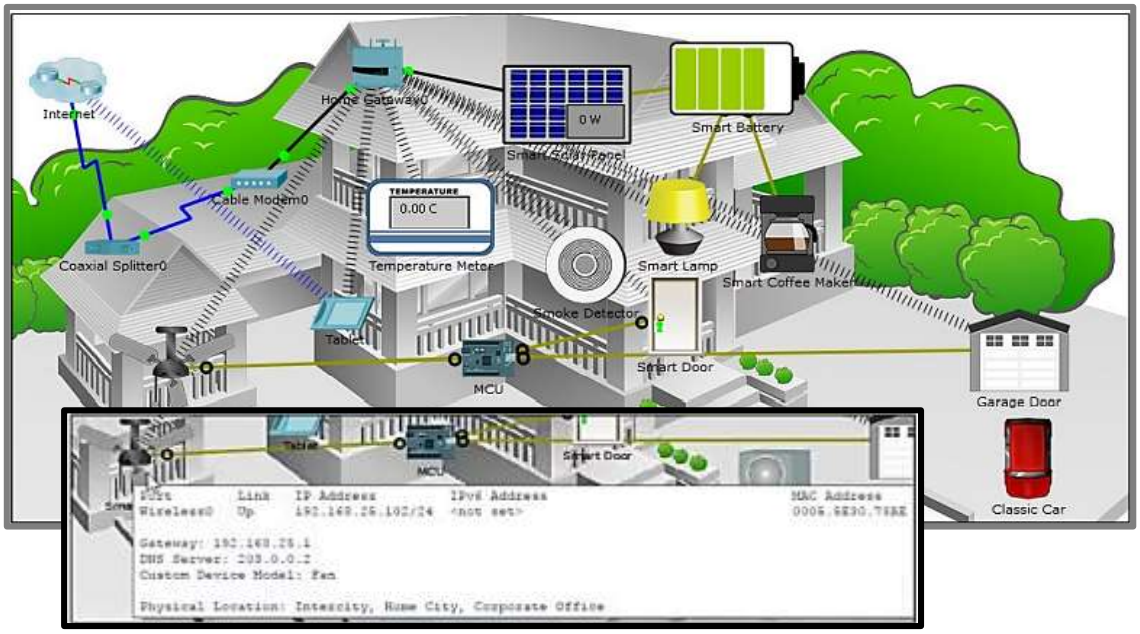


Рисунок 3.2 – Мережа Smart Home

Розумна домашня мережа також складається з інфраструктурних пристроїв, таких як домашній шлюз **Home Gateway** (рис. 3.3). Натисніть піктограму **Home Gateway**, щоб відкрити вікно Home Gateway.

Вкладку **Physical** вибрано за замовчуванням і відображає зображення домашнього шлюзу.

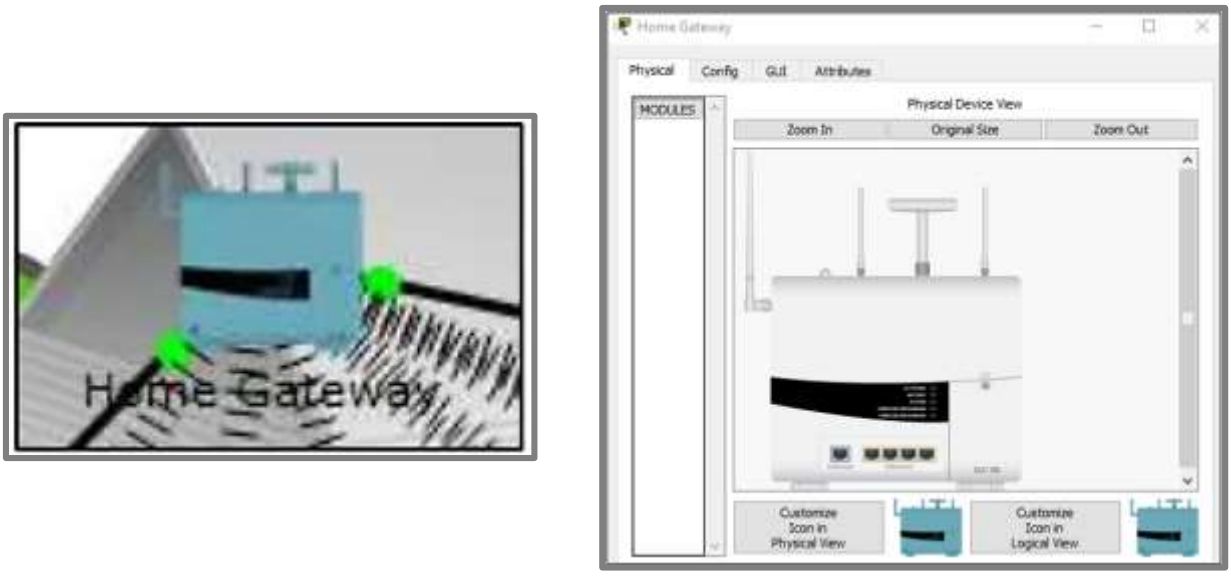


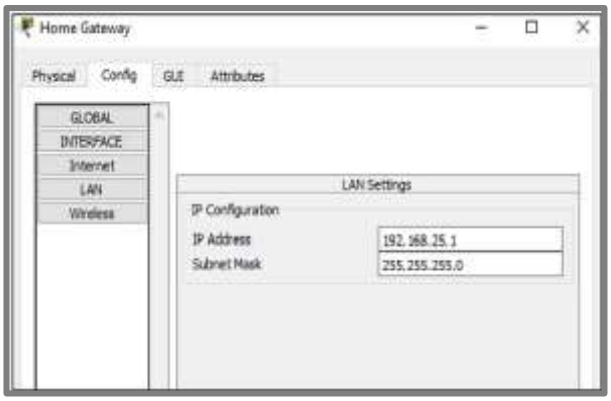
Рисунок 3.3 – Домашній шлюз Home Gateway

Далі клацніть вкладку **Config**, а потім на лівій панелі клацніть **LAN**, щоби переглянути параметри LAN домашнього шлюзу Home Gateway (рис. 3.4).

✓ ***Запишіть IP-адресу домашньої мережі для використання в майбутньому:*** _____.

Клацніть **Wireless** на лівій панелі, щоби переглянути параметри бездротового зв'язку домашнього шлюзу Home Gateway (рис. 3.5).

✓ ***Запишіть SSID домашньої мережі*** _____ ***і парольну фразу WPA2-PSK*** _____ ***для використання в майбутньому.***



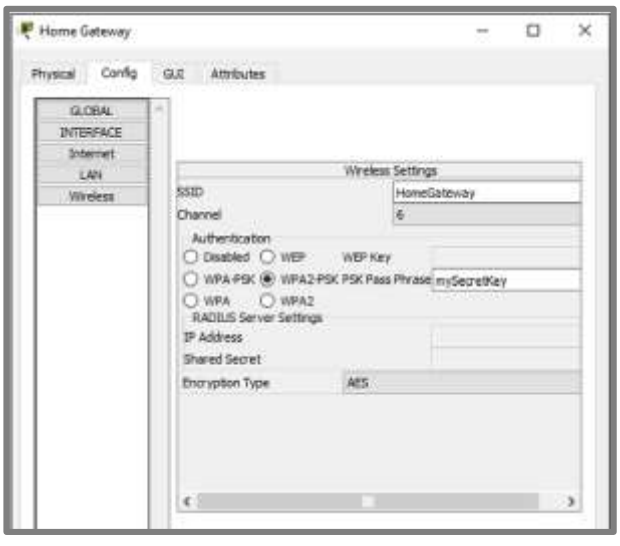


Рисунок 3.4 – Параметри LAN домашнього шлюзу Home Gateway

Рисунок 3.5 – Параметри Wireless домашнього шлюзу Home Gateway

Закрийте вікно Home Gateway.

Далі натисніть піктограму планшетного пристрою **Tablet**, щоб відкрити вікно планшета (рис. 3.6). У вікні **Tablet** виберіть вкладку **Desktop**, а потім клацніть піктограму **Web Browser**.

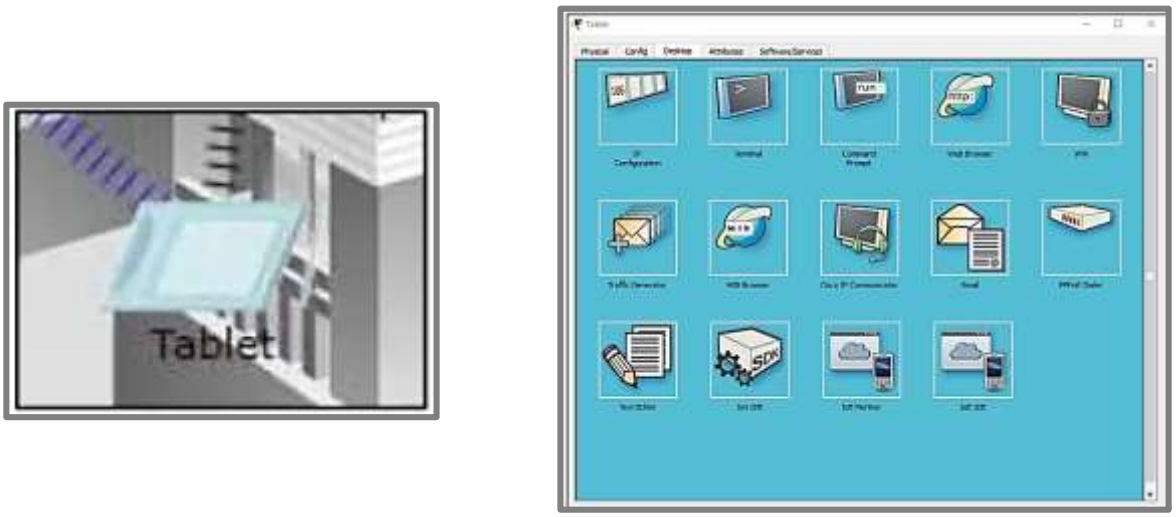


Рисунок 3.6 – Планшетний пристрій Tablet

У вікні **Web Browser** введіть IP-адресу домашнього шлюзу Home Gateway **192.168.25.1** у полі URL-адреси (рис. 3.7) та натисніть **Go (**Перейти**)**. На екрані входу в домашній шлюз введіть **admin** як ім’я користувача, так і пароль і натисніть **Submit** (Надіслати).



Рисунок 3.7 – Екран входу в домашній шлюз Home Gateway

Примітка: *якщо ви не можете ввійти в Home Gateway за допомогою «веббраузера», ви можете використовувати* **IoT Monitor** *для входу (рис. 3.8).*

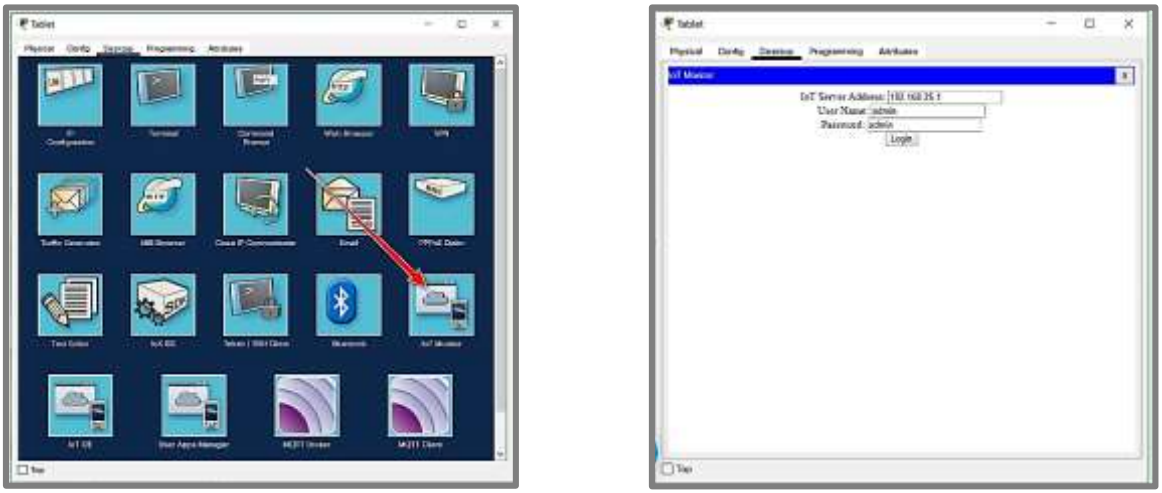


Рисунок 3.8 – Вхід в Home Gateway через IoT Monitor

Після підключення до вебінтерфейсу Home Gateway з'являється список усіх підключених пристроїв IoT. Коли ви натискаєте на пристрій у списку, відображається стан і налаштування цього пристрою (рис. 3.9).

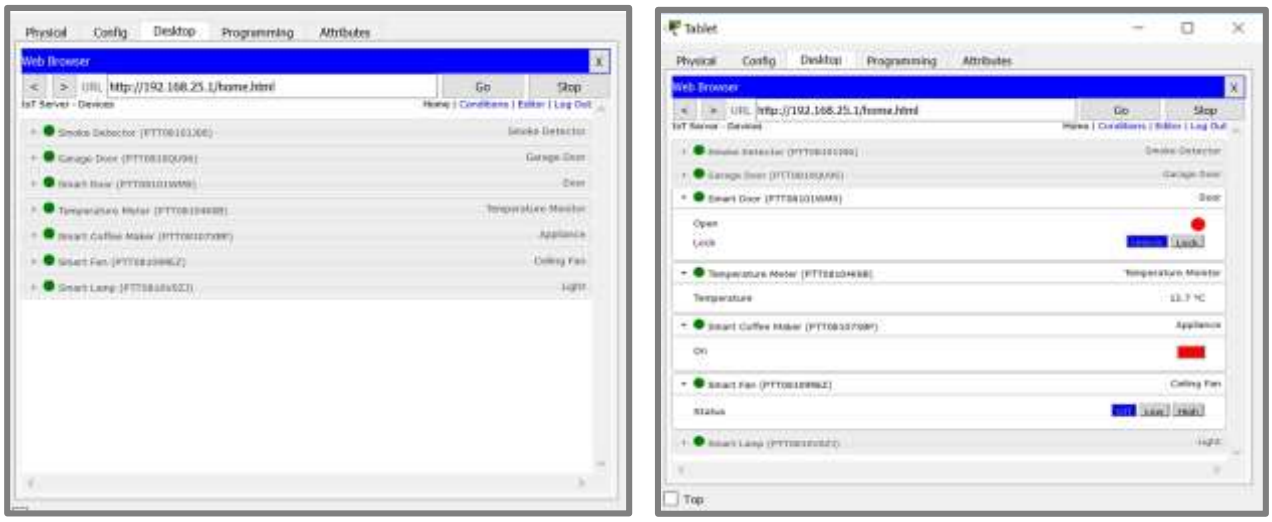


Рисунок 3.9 – Відображення всіх підключених пристроїв IoT

Закрийте вікно планшета Tablet.

2. Додавання Wired IoT Devices (дротових пристроїв IoT) до Smart Home Network (мережі розумного дому)

2.1. Підключіть пристрій до мережі

1) У вікні **Device-Specific Selection** клацніть піктограму **Lawn Sprinkler** (газонний розбризкувач), а потім клацніть у робочій області, де ви хочете розмістити **Lawn Sprinkler**.
2) Підключіть **Lawn Sprinkler** до домашнього шлюзу Home Gateway. У вікні **Device-Type Selection** натисніть піктограму **Connections** (це виглядає як блискавка) та клацніть піктограму типу **Copper Straight Through**. Потім клацніть піктограму **Sprinkler** і підключіть один кінець кабелю до інтерфейсу **FastEthernet0** розбризкувача. Потім натисніть піктограму Home Gateway і підключіть інший кінець кабелю до доступного інтерфейсу **Ethernet** (рис. 3.10).

Примітка: *якщо ви не знайшли інтерфейс* **FastEthernet0** *на Lawn Sprinkler, натисніть* **Advanced**, *перейдіть на вкладку* **I/O Config**, *виберіть* **PT-IOT-NM-1CFE** *у полі* **Network Adapter**.

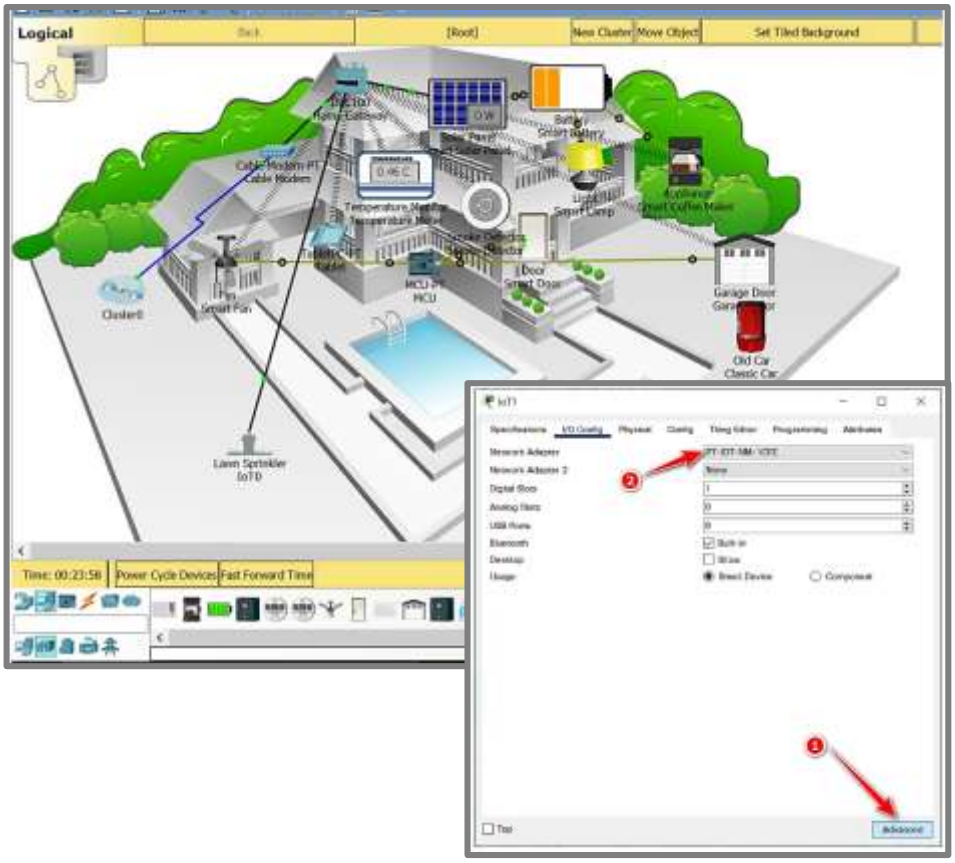


Рисунок 3.10 – Відображення всіх підключених пристроїв IoT

2.2. Налаштування Sprinkler для підключення до мережі

1) Щоб відкрити вікно пристрою, клацніть піктограму пристрою **Lawn Sprinkler** в робочій області. Зауважте, що наразі назва Lawn Sprinkler є загальною назвою IoT0.

У вікні пристрою відкриється вкладка **Specification (**Специфікація**)**, яка містить інформацію про пристрій, яку можна редагувати (рис. 3.11).

2) Натисніть вкладку **Config**, щоб змінити параметри конфігурації пристрою (рис. 3.11). На вкладці **Config** внесіть такі зміни в **Settings:**

- Встановіть **Display Name** на Sprinkler1 (зверніть увагу, що назва вікна зміниться на Sprinkler1);
- Встановіть сервер IoT на **Home Gateway.**

Натисніть **FastEthernet0** і змініть **IP Configuration** на **DHCP** (рис. 3.11). Закрийте вікно **Sprinkler1**.

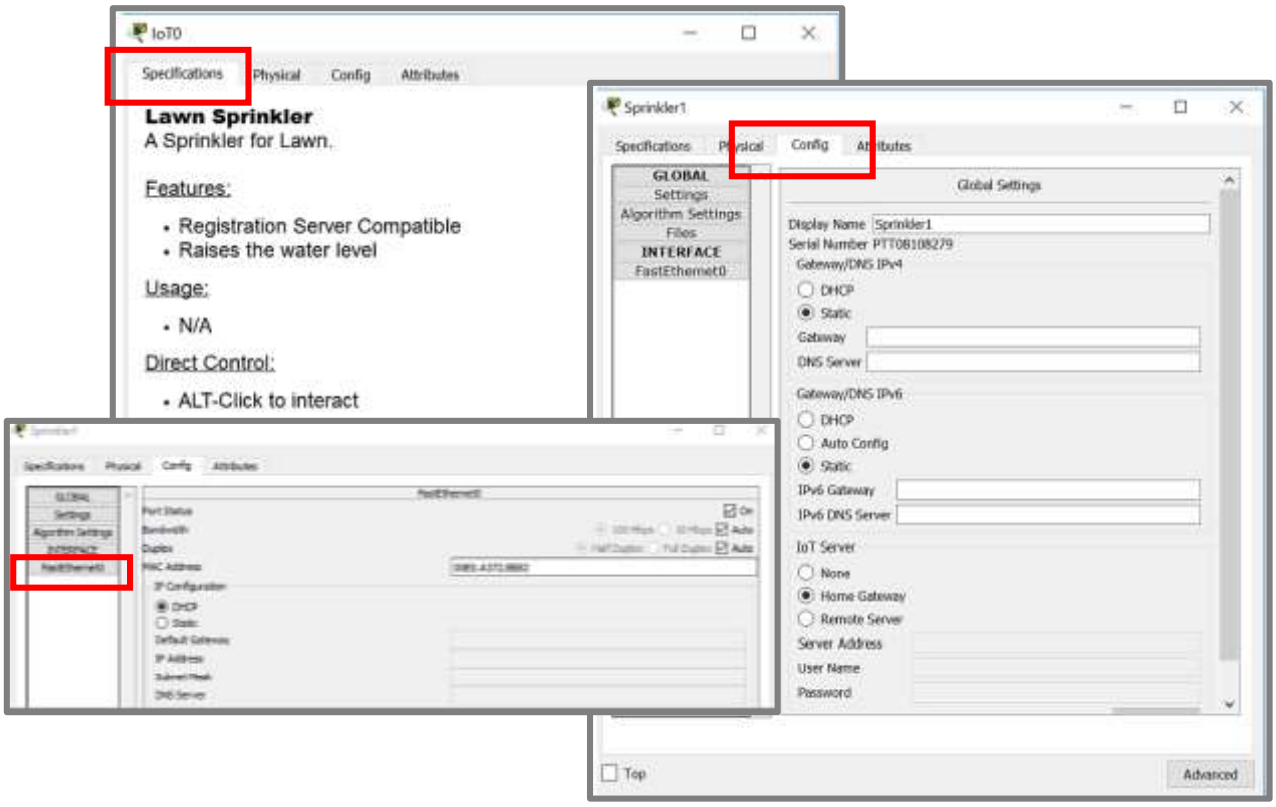


Рисунок 3.11 – Налаштування Sprinkler для підключення до мережі

3) Переконайтеся, що **Sprinkler** підключений до мережі. Увійдіть у **Home Gateway** із планшета **Tablet**. Тепер пристрій **Sprinkler1** має з'явитися в списку IoT Server – Devices (рис. 3.12). Закрийте вікно планшета.

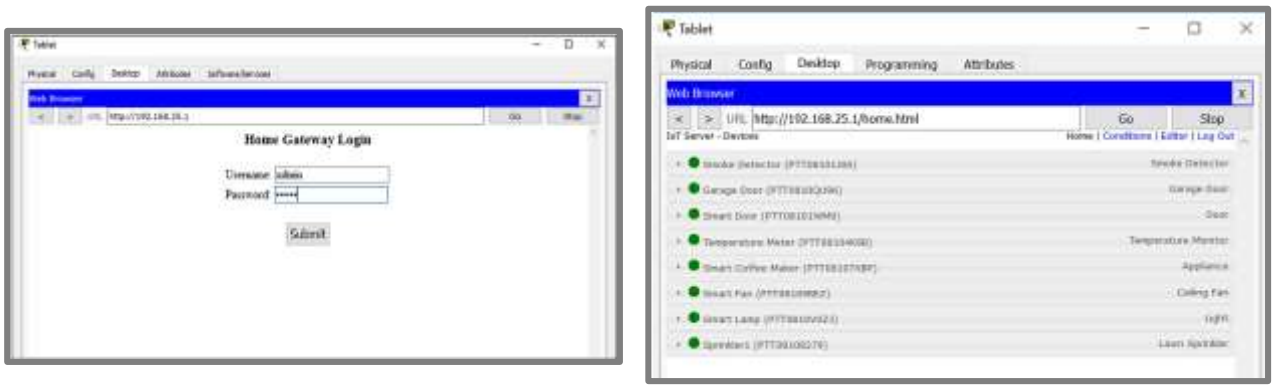


Рисунок 3.12 – Підключення Sprinkler до мережі

2.3. Додавання інших типів пристроїв IoT до розумної домашньої мережі.

✓ **Додайте 2–3 дротові пристрої IoT до мережі розумного дому.**

3. Додавання Wireless IoT Devices (бездротових пристроїв IoT) до Smart Home Network.

3.1. Додайте бездротовий пристрій до мережі

1) У вікні **Device-Specific Selection** натисніть піктограму **Wind Detector** (Детектор вітру), а потім клацніть у робочій області, де ви бажаєте розташувати **Wind Detector** (рис. 3.13).
2) Додайте бездротовий модуль до детектора вітру. Натисніть піктограму **Wind Detector** у робочій області, щоб відкрити вікно пристрою IoT. У нижньому правому куті вікна пристрою IoT натисніть кнопку **Advanced** (Додатково). Зверніть увагу, що у верхній частині вікна стало видно більше вкладок. Натисніть вкладку **I/O Config**. Змініть у спадаючому списку мережевого адаптера **Network Adapter** на **PT-IOT-NM-1W**, який є бездротовим адаптером (рис. 3.13).

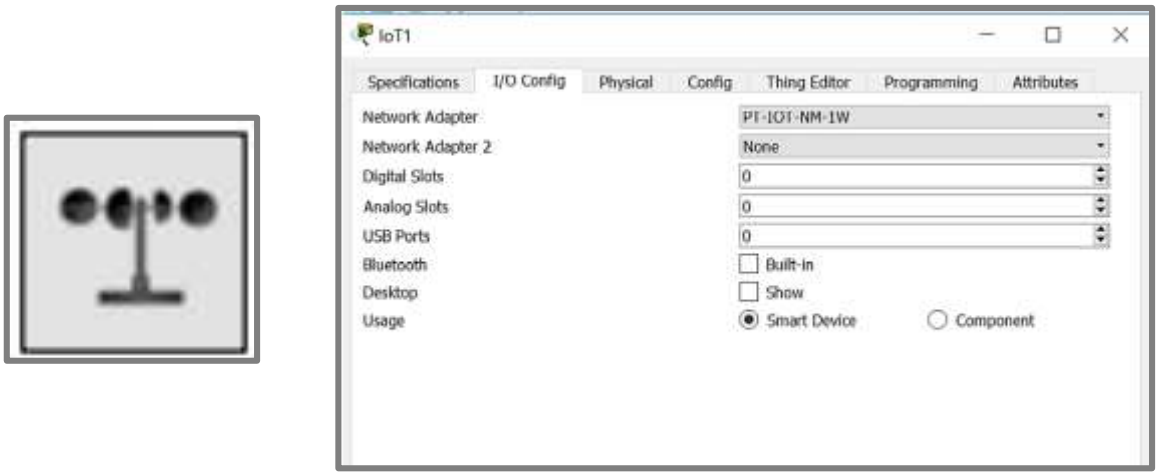


Рисунок 3.13 – Бездротовий пристрій – Wind Detector

3) Налаштуйте **Wind Detector** для бездротової мережі. Перейдіть на вкладку **Config**. Змініть **Display Name** на **Wind_Detector** і змініть **IoT Server** на **Home Gateway**.

Потім натисніть **Wireless0** на лівій панелі. Змініть тип автентифікації на **WPA2-PSK** і в полі **PSK Pass Phrase** введіть **mySecretKey**. Це налаштування бездротового зв'язку з домашнього шлюзу, які ви записали в пункті 1. Між детектором вітру та домашнім шлюзом має бути встановлено бездротове з'єднання (рис. 3.14).

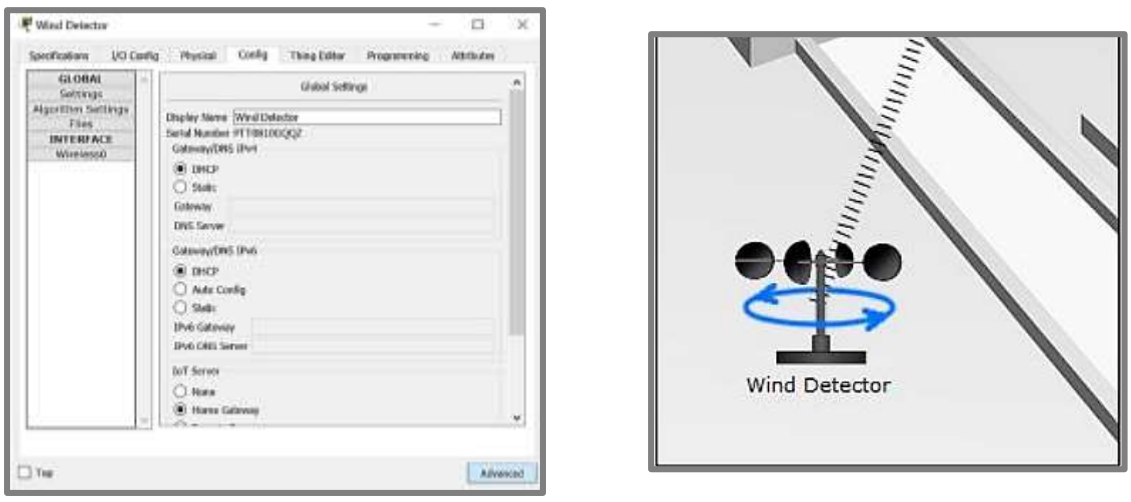


Рисунок 3.14 – Налаштуйте Wind Detector для бездротової мережі

4) Переконайтеся, що детектор вітру підключено до мережі. Увійдіть у **Home Gateway** із **Tablet**. Тепер пристрій Wind Detector має з'явитися в списку IoT Server – Devices. Закрийте вікно планшета (рис. 3.15).

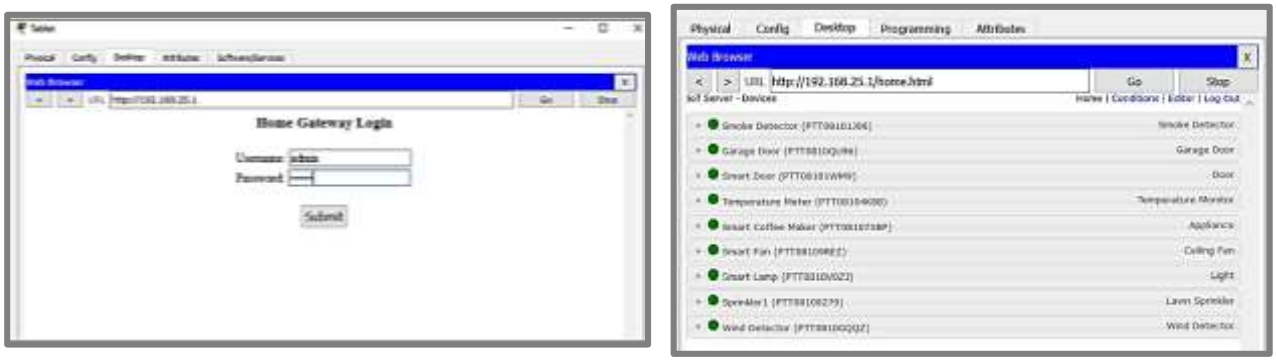


Рисунок 3.15 – Підключення Wind Detector до бездротової мережі

3.2. Додавання інших типів пристроїв IoT до бездротової мережі.

✓ **Додайте інші 2–3 типи пристроїв IoT до бездротової мережі розумного дому.**

ВИМОГИ ДО ОФОРМЛЕННЯ ЗВІТУ

1. Сформуйте файл для звіту. Звіт про виконання роботи має включати:

- Титульний аркуш, вказуючи номер і назву роботи, прізвище і групу студента.
- Покроковий опис основних етапів виконання роботи. Отримані результати підтверджуються скріншотами екрана.
- Висновки щодо проведеної роботи.

2. Створений файл із назвою LR-3_XXXXX.pkt, де XXXXX – позначення прізвища студента. У файлі мають бути збережені налаштування вибраних дротових/бездротових пристроїв IoT, що підключені до мережі розумного будинку.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Що таке датчик?
2. Яка вимога до пристрою, щоб його називали смарт-пристроєм?
3. Які технології використовуються для обміну інформацією між пристроями?
4. Що використовується для унікальної ідентифікації пристроїв, підключених до Інтернету?
5. Яку інформацію передає SSID, налаштований на пристрої IoT?
6. Що потрібно в розумному будинку для підключення датчиків і розумних пристроїв до мережі?
7. Які команди використовуються для налаштування протоколу DHCP на роутері?
8. Яка команда використовується для виключення IP-адреси з DHCP пулу?
9. У якому типі сценарію шлюз IoT не потрібен для перетворення трафіка на Wi-Fi або дротовий Ethernet?

ЛАБОРАТОРНА РОБОТА № 4
ПІДКЛЮЧЕННЯ ТА МОНІТОРИНГ ПРИСТРОЇВ ІОТ

Мета роботи: підключення домашнього шлюзу Home Gateway і додавання кінцевих пристроїв користувача до наявної домашньої мережі; проведення вистежування цих пристроїв через домашній шлюз.

ВКАЗІВКИ ДО ВИКОНАННЯ РОБОТИ

1. Підключення домашнього шлюзу Home Gateway до мережі

1) Відкрийте файл **Connect and Monitor IoT Devices.pkt** та збережіть файл на комп'ютері. Виберіть пристрій домашнього шлюзу Home Gateway. Натисніть значок **Wireless Devices** (Бездротові пристрої) у полі **Device-Type Selection**. Натисніть піктограму пристрою **Home Gateway** (рис. 4.1), а потім клацніть у логічній робочій області, щоб додати пристрій.
2) Підключіть домашній шлюз до кабельного модему Cable Modem. Клацніть піктограму **Copper Straight-Through** у вікні Device-Type Selection (рис. 4.1), а потім клацніть **Home Gateway**, щоб додати один кінець кабелю до шлюзу. Потім клацніть піктограму **Cable Modem**, щоби під'єднати інший кінець кабелю до порту **Internet**.

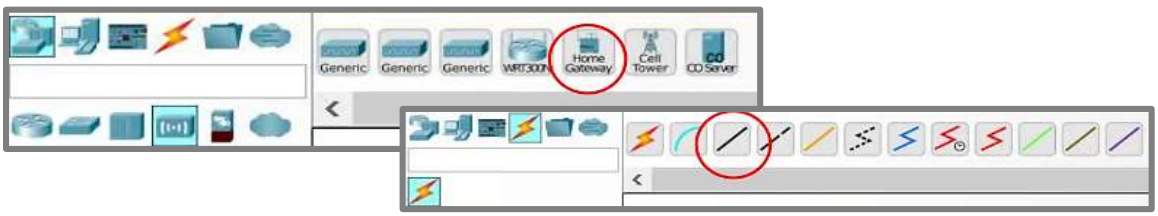


Рисунок 4.1 – Вибір Home Gateway та кабелю Copper Straight-Through

Через кілька секунд на обох кінцях кабелю мають засвітитися зелені індикатори, що вказує на підключення (рис. 4.2).

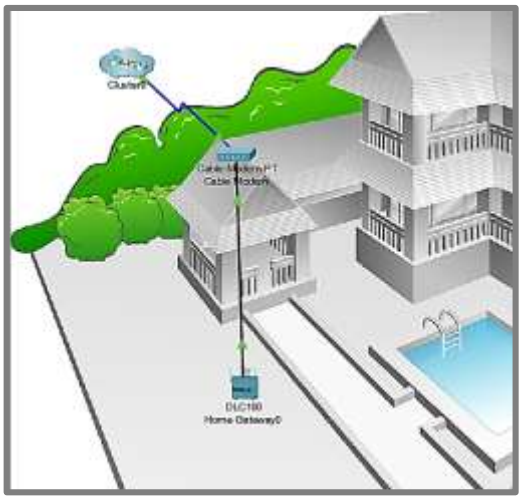


Рисунок 4.2 – Підключення Home Gateway

2. Підключення пристроїв IoT до бездротової мережі

2.1. Виберіть бездротові пристрої. Клацніть піктограму **Home Devices** в полі **Device-Type Selection** та додайте в робочу область **Fan (**вентилятор**)**, **Door (**двері**)** та **Lamp** (лампа), як на рис. 4.3.



Рисунок 4.3 – Вибір пристроїв мережі

2.2. Додайте пристрої до домашньої бездротової мережі

1) Додайте бездротовий адаптер до пристрою **Fan**. Натисніть значок **Fan** у робочій області, щоб відкрити вкладку **Config,** а потім натисніть кнопку **Advanced** (Додатково) у нижньому правому куті вікна. Зверніть увагу, що вкладки у верхній частині вікна конфігурації змінюються. Тепер вкладок більше. Натисніть вкладку **I/O Config** і змініть тип **Network Adapter** на бездротовий адаптер **PT-IOT-NM-1W** (рис. 4.4).
2) Змініть відображуване ім’я пристрою **Fan**. Перейдіть на вкладку **Config.** У полі **Display Name** введіть **Ceiling Fan** (рис. 4.4).

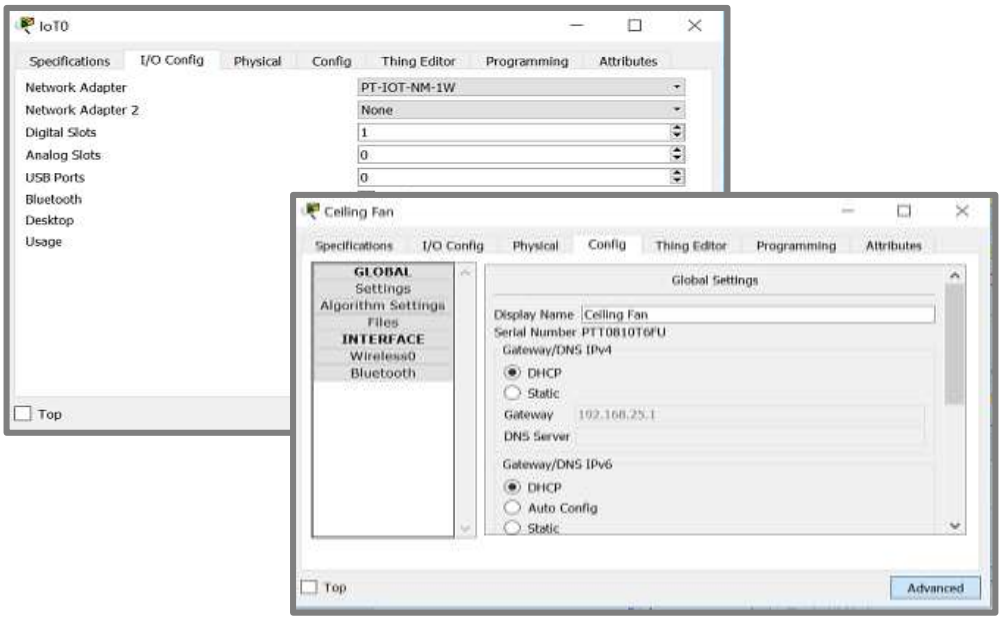


Рисунок 4.4 – Налаштування Ceiling Fan

3) Переконайтеся, що **Fan** підключено до бездротової мережі. Перебуваючи на вкладці **Config**, натисніть інтерфейс **Wireless0** на лівій панелі. У налаштуваннях конфігурації мережа **HomeGateway** має бути вказана в полі **SSID**. Переконайтеся, що в налаштуваннях **IP Configuration** вибрано **DHCP**, **IP address** – **192.168.25.100**, а шлюз за замовчуванням – **192.168.25.1** (рис. 4.5). Це означає, що вентилятор підключено до мережі та одержує інформацію про конфігурацію IP від домашнього шлюзу. Закрийте вікно налаштування вентилятора.

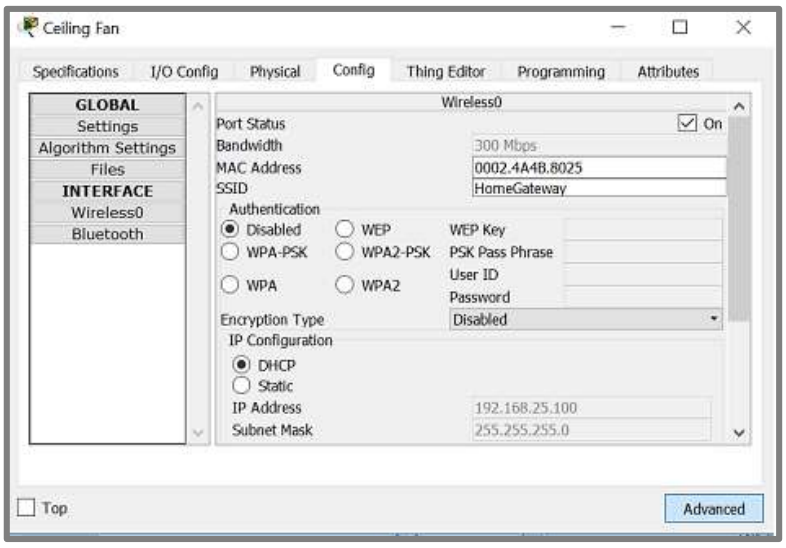


Рисунок 4.5 – Підключення вентилятора до мережі

4) Підключіть **Door** та **Lamp** до бездротової мережі, дотримуючись тих самих кроків, що і для вентилятора.

3. Додавання кінцевих пристроїв користувача до мережі

3.1. Додайте бездротовий планшет до робочого простору. Клацніть піктограму **End Devices** у вікні **Device-Type Selection** та додайте **Wireless Tablet** (рис. 4.6) до робочої області.

3.2. Підключіть бездротовий планшет до мережі HomeGateway

1) Змініть параметри бездротової мережі планшета. Натисніть піктограму **Tablet,** щоб відкрити вікно конфігурації планшета. Перейдіть на вкладку **Config**, а потім виберіть інтерфейс **Wireless0**. Змініть **SSID** з **Default** на **HomeGateway** (рис. 4.6). Після зміни SSID мережі Tablet має дістати IP-адресу через DHCP упродовж кількох секунд.

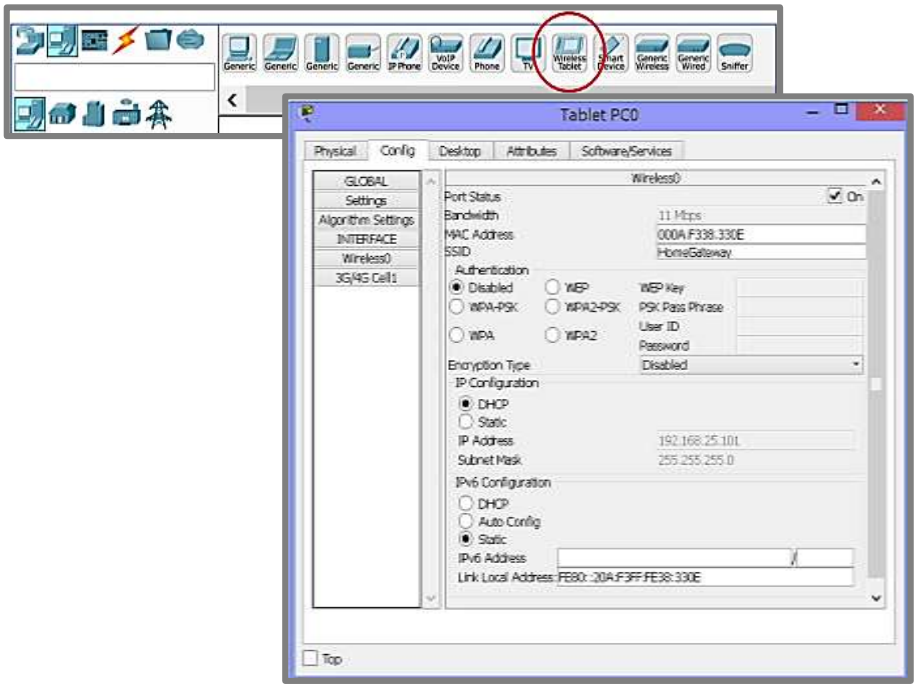


Рисунок 4.6 – Планшет Wireless Tablet та зміни його параметрів

2) Одержіть доступ до домашнього шлюзу IoT-сервера з планшета. Клацніть вкладку **Desktop**, а потім піктограму **Web Browser**, щоб відкрити веббраузер. Введіть 192.168.25.1 (адреса домашнього шлюзу) у полі URL-адреси та

натисніть **Go**. На сторінці входу в **Home Gateway** введіть **admin** як ім'я користувача та **admin** як пароль і натисніть кнопку **Submit**, щоби підключитися до сервера. Зауважте, що в списку пристроїв Home Gateway IoT Server – Devices немає пристроїв (рис. 4.7). Закрийте вікно планшета.

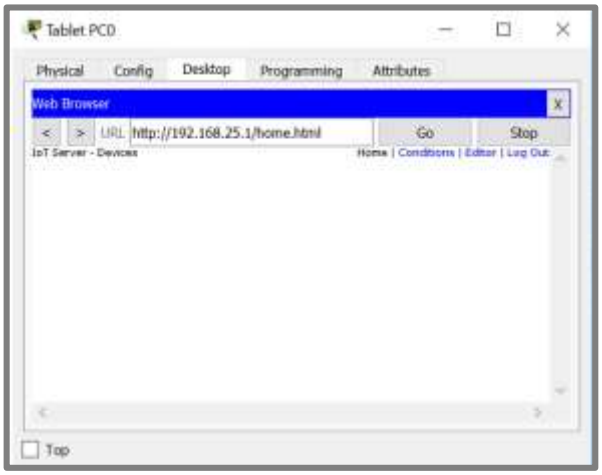


Рисунок 4.7 – Доступ до домашнього шлюзу IoT-сервера з планшета

3.3. Налаштуйте пристрої IoT для реєстрації на сервері Home Gateway:

1) Зареєструйте Ceiling Fan на сервері домашнього шлюзу. Клацніть піктограму **Fan** у робочій області, виберіть вкладку **Config**, а потім клацніть **Settings** на лівій панелі (рис. 4.8). У списку параметрів **IoT Server** натисніть кнопку **Home Gateway**. Закрийте вікно **Ceiling Fan**. Повторіть кроки цього пункта, щоб зареєструвати пристрої **Door** і **Lamp** на домашньому шлюзі.

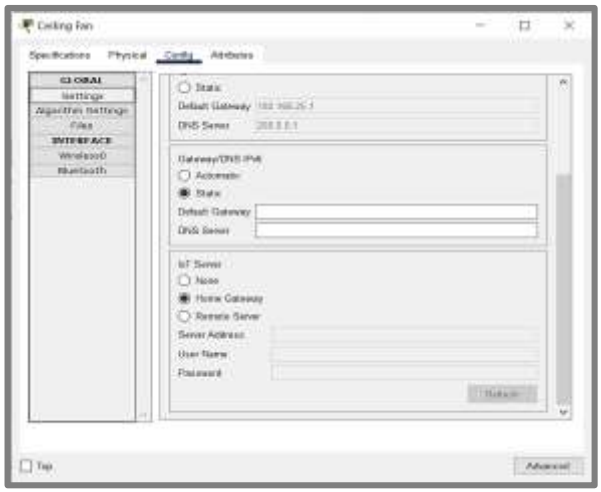


Рисунок 4.8 – Реєстрація Ceiling Fan на сервері домашнього шлюзу

2) Переконайтеся, що пристрої зареєстровані на сервері Home Gateway. Клацніть піктограму **Tablet** в робочій області та відкрийте **Web Browser**. Підключіться до Home Gateway, ввівши **192.168.25.1** у полі URL-адреси та клацнувши **Go**. Введіть **admin** як ім'я користувача та пароль і натисніть **Submit**. Через кілька секунд усі три пристрої мають бути вказані в списку пристроїв Home Gateway **IoT Server – Devices** (рис. 4.9). Закрийте вікно **Tablet**.

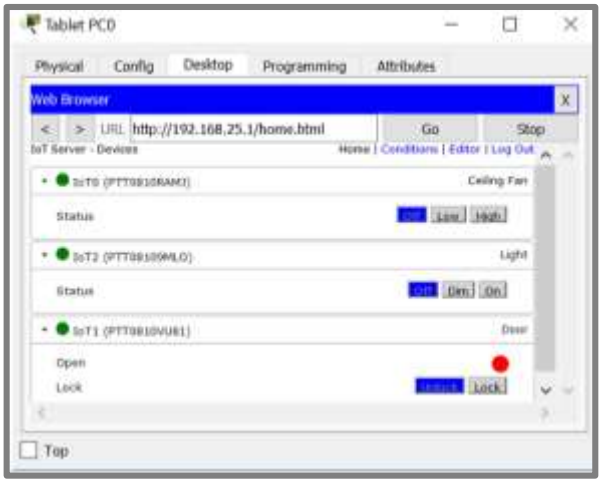


Рисунок 4.9 – Підключення пристроїв до мережі

ВИМОГИ ДО ОФОРМЛЕННЯ ЗВІТУ

1. Сформуйте файл для звіту. Звіт про виконання роботи має включати:

- Титульний аркуш, вказуючи номер і назву роботи, прізвище і групу студента.
- Покроковий опис основних етапів виконання роботи. Отримані результати підтверджуються скріншотами екрану.
- Висновки щодо проведеної роботи.

2. Створений файл із назвою LR-4_XXXXX.pkt, де XXXXX – позначення прізвища студента.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Пояснити термін та концепцію IoT. Навести приклади.

2. Які можливості середовища Cisco Packet Tracer для створення та налаштування IoT рішень ви знаєте?
3. Як працює Wi-Fi?
4. Що таке SSID?
5. Що таке DHCP?
6. Які дві вимоги є для підключення інтелектуального пристрою до домашньої бездротової мережі?
7. Який пристрій надає послуги автоматичного виявлення для інтелектуальних пристроїв, підключених до мережі?
8. Які дві найпоширеніші бездротові технології використовуються в системах домашньої автоматизації та домашньої безпеки?

ЛАБОРАТОРНА РОБОТА № 5
ПОБУДОВА МОДЕЛІ РОЗУМНОЇ КІМНАТИ ЗА ДОПОМОГОЮ CISCO PACKET TRACER



Мета роботи: проведення моделювання «розумної кімнати», яка включає такі елементи як: домашній шлюз (Home Gateway); вентилятор; вікно; моделювання режимів регулювання температури у IoT кімнаті та рівня газів у гаражному приміщені. За результатами навчання необхідно провести розроблення технічних рішень житлової IoT кімнати з описом логіки з'єднання пристроїв та правил управління пристроями.



1. Моделювання мережі житлової IoT кімнати

1.1. Відкрийте в **Network devices** підрозділ **Wireless devices**, знайдіть у ньому домашній шлюз **Home Gateway** та перетягніть його на робоче поле.

1.2. У розділі **End devices** виберіть підрозділ **Home,** оберіть елемент **Fan** та перетягніть його на робоче поле (рис. 5.1). Натисніть на значок **Fan**. У вікні властивостей на вкладці **Config** змініть ім'я пристрою на **Ceiling Fan** (Вентилятор на стелі), як показано на рис. 5.1.

1.3. У правому куті підрозділу **Home** оберіть елемент **Window** (**Вікно**) та перетягніть його на робоче поле. Аналогічно до попереднього елемента змініть назву на **Window** (рис. 5.1).

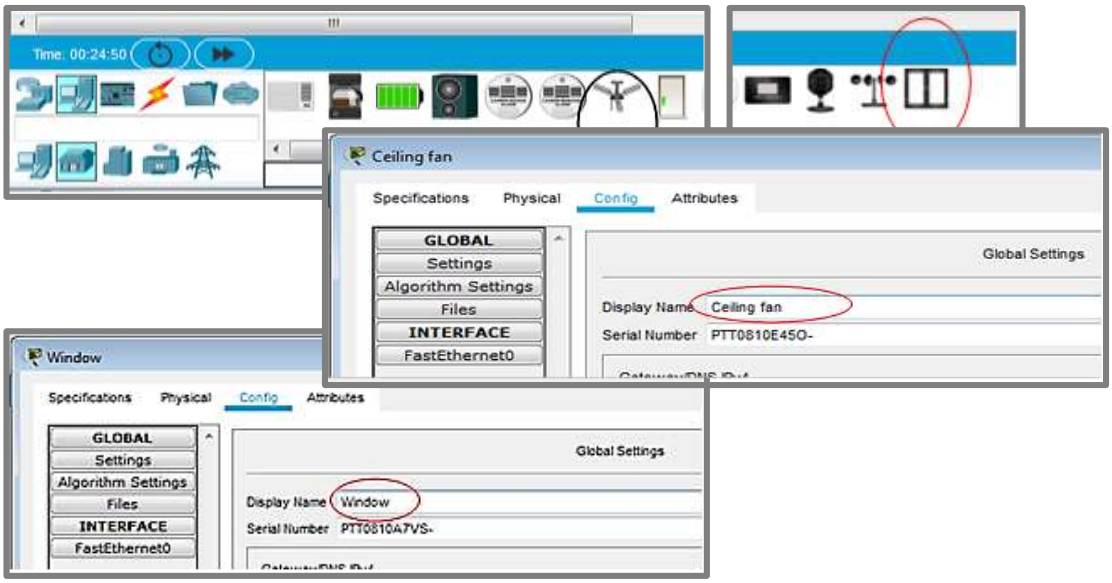


Рисунок 5.1 – IoT пристрій Ceiling Fan та Window

1.4. Обведіть прямокутником елементи кімнати: вентилятор і вікно, почергово виконавши дії 1–3 (рис. 5.2). Підпишіть назву кімнати, виконавши пункт 4 (рис. 5.2).

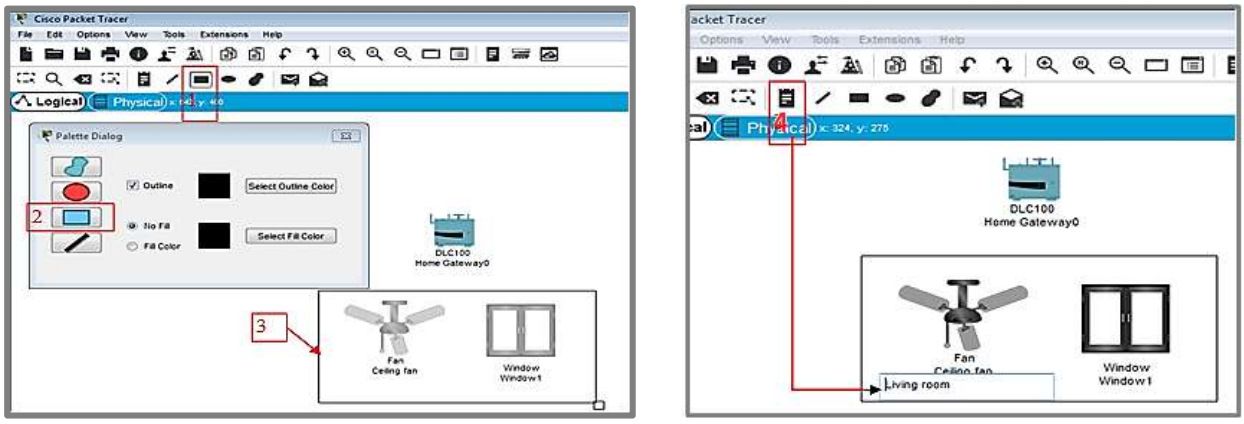


Рисунок 5.2 – Виділення області розумної кімнати

1.5. Для з’єднання елементів із домашнім шлюзом **Home Gateway** необхідно налаштувати бездротову мережу.

Натисніть на елементі **Ceiling Fan**. У відкритому вікні справа внизу натисніть кнопку **Advanced** (Розширено). У вкладці конфігурації входів/виходів **I/O Config** оберіть мережевий адаптер для бездротової мережі, як показано на рис. 5.3. Аналогічні дії виконайте для елемента **Window**.



Рисунок 5.3 – Вибір мережевого адаптера для бездротової мережі

У результаті одержимо підключення, як показано на рис. 5.4.

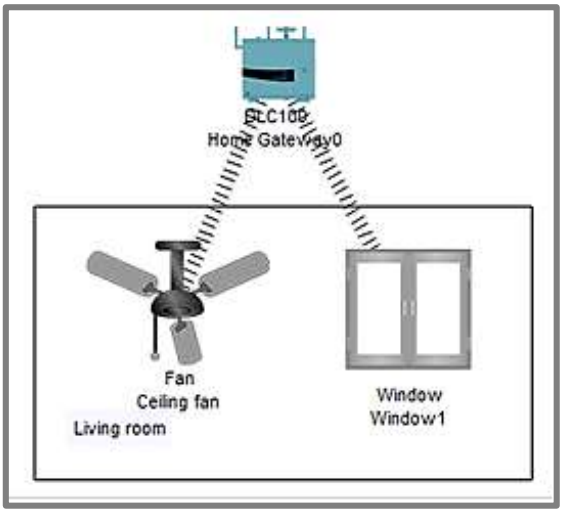


Рисунок 5.4 – Бездротова домашня мережа

1.6. Управління пристроями будемо здійснювати смартфоном **Smartphone**. Перенесемо **Smartphone** на робоче поле, натискаємо на зображенні та налаштовуємо його на підключення до **Home Gateway**, виконуючи дії 1–2–3 (рис.5.5).



Рисунок 5.5 – Налаштування Smartphone

Переходимо у вкладку смартфона **Desktop** та обираємо **IoT Monitor**. Перевіряємо відповідність IP-адрес **IoT Monitor** смартфона та **Home Gateway** (рис. 5.6).

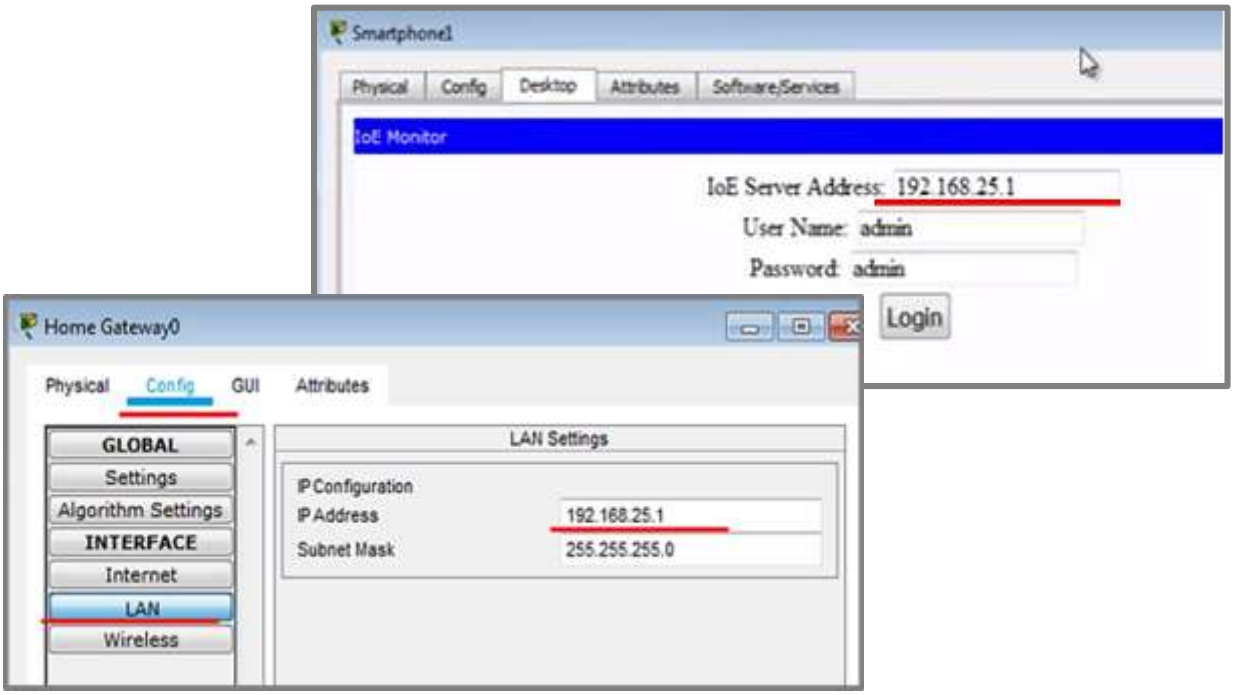


Рисунок 5.6 – Відповідність IP-адрес IoT Monitor смартфона та Home Gateway

1.7. У робочому полі натискаємо на елемент **Ceiling Fan** та у вкладці **Config** прокручуємо до низу та вмикаємо кнопку **Home Gateway** (1–2–3 на рис. 5.7). Аналогічні дії виконуємо і для **Window**.

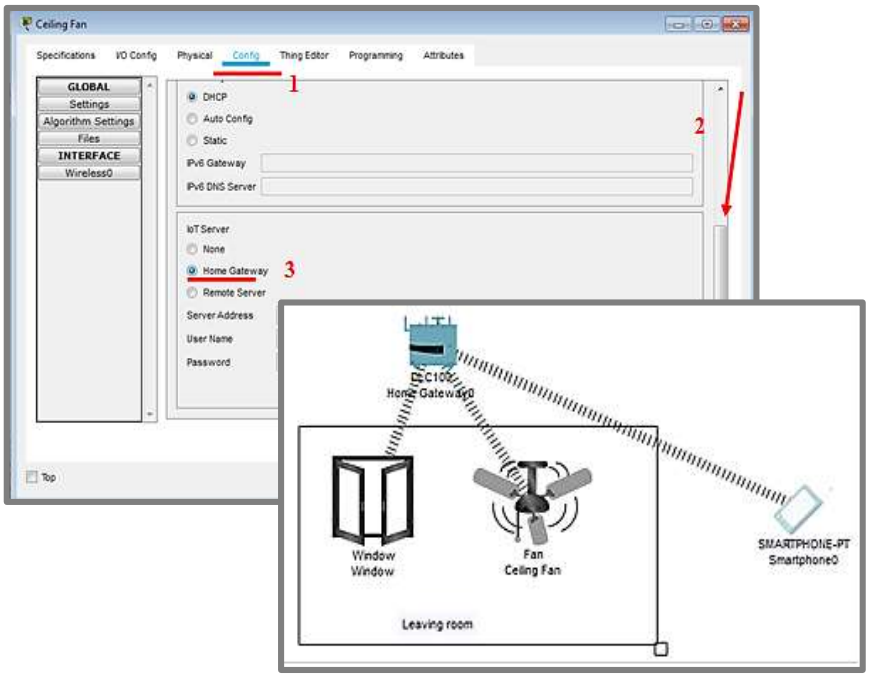


Рисунок 5.7 – Під'єднання Ceiling Fan до мережі Home Gateway

1.8. Повертаємось у **Desktop** смартфона (рис. 5.8) та обираємо **IoT Monitor**. Тепер речами можна управляти через смартфон, натискаючи на їх підключення. Пробуємо змінювати рух вентилятора (1) та відкривати/закривати вікно (2).

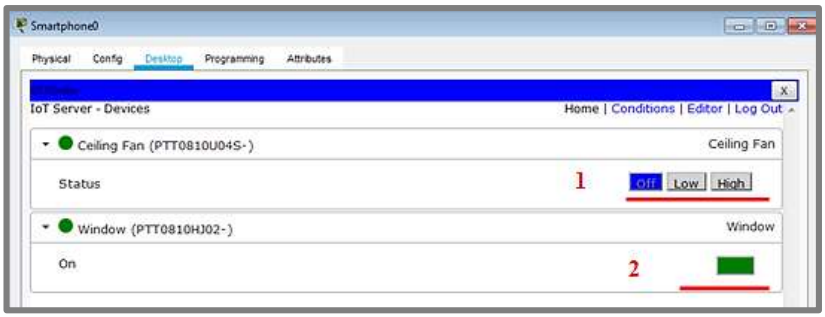


Рисунок 5.8 – Керування пристроями IoT через смартфон

2. Моделювання регулювання температури у IoT кімнаті

2.1. Добавляємо до кімнати термостат **Temperature Monitor** (рис. 5.9). Під'єднаємо його дротовим з'єднанням **Cooper Straight-Throught** (Мідний кабель).

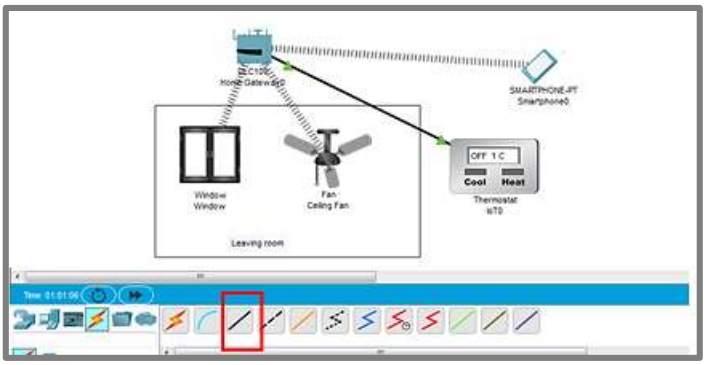


Рисунок 5.9 – Підключення термостата

2.2. Заходимо в смартфон та налаштовуємо його конфігурацію для управління термостатом. Натискаємо **Condition** (рис. 5.10).

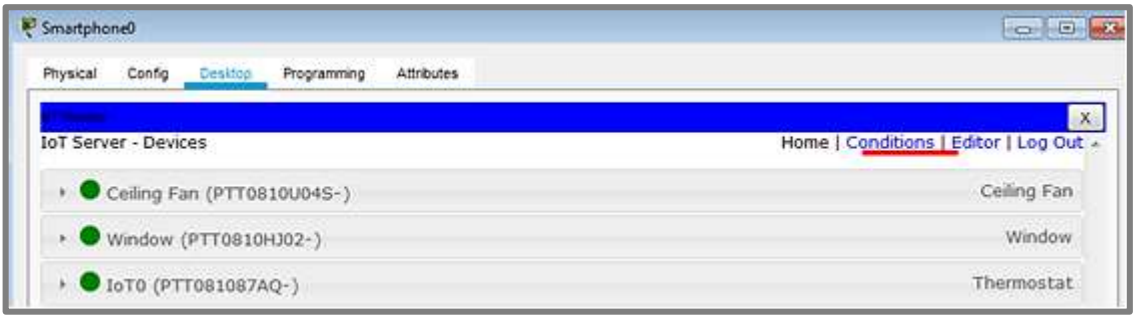


Рисунок 5.10 – Налаштування конфігурації смартфона

Далі заповнюємо поля за порядком (1–10), як на рис. 5.11.

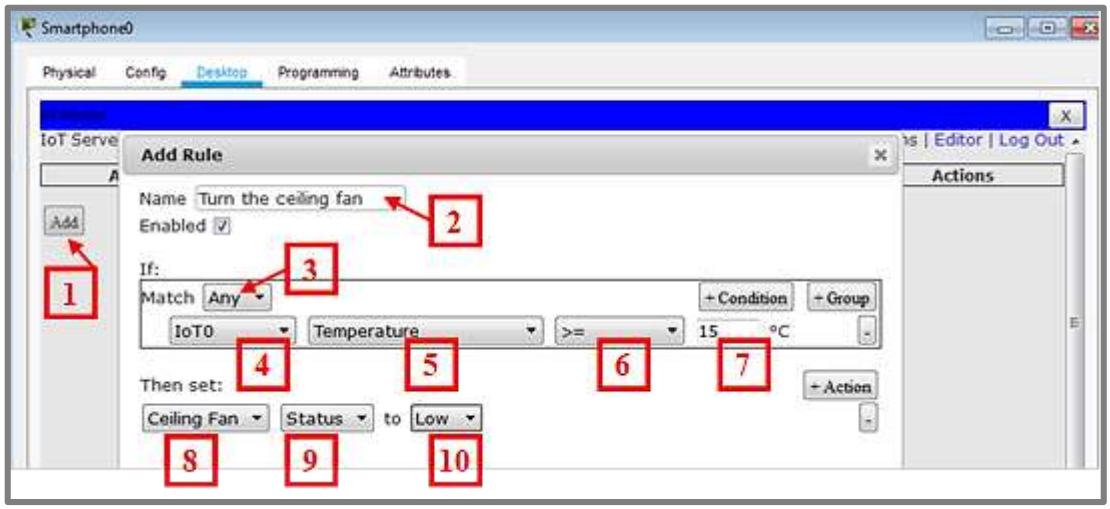


Рисунок 5.11 – Налаштування режиму роботи вентилятора

Далі натискаємо кнопку **Ок** внизу цього вікна. Повторюємо дії для іншого режиму роботи (рис. 5.12).

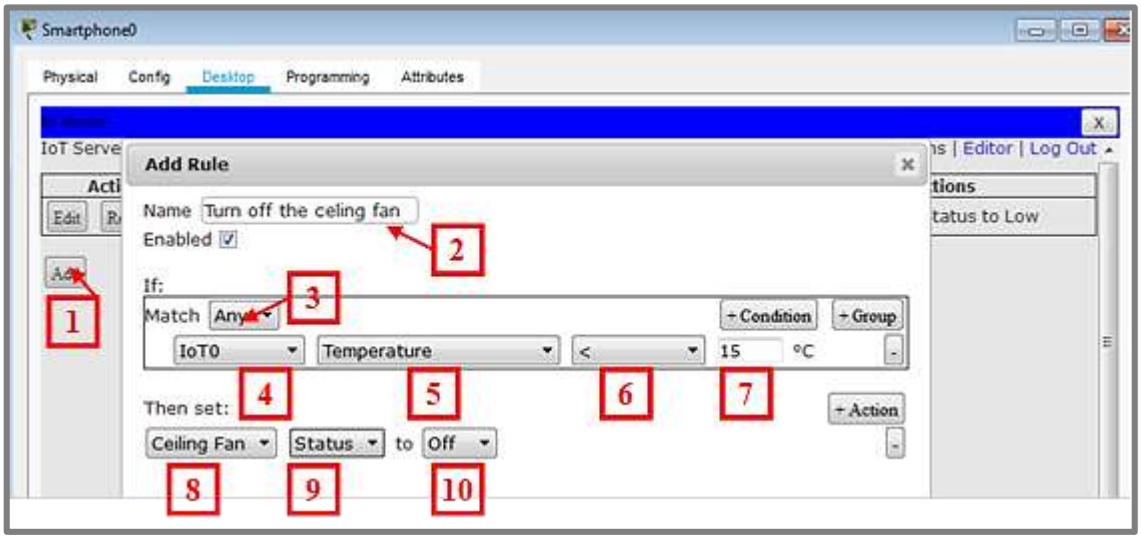


Рисунок 5.12 – Налаштування другого режиму роботи вентилятора

Натискаємо кнопку **Ок** внизу цього вікна та одержимо зображення, як на рис. 5.13. Система має бути керованою, а під час зміни температури вентилятор змінює режими роботи.

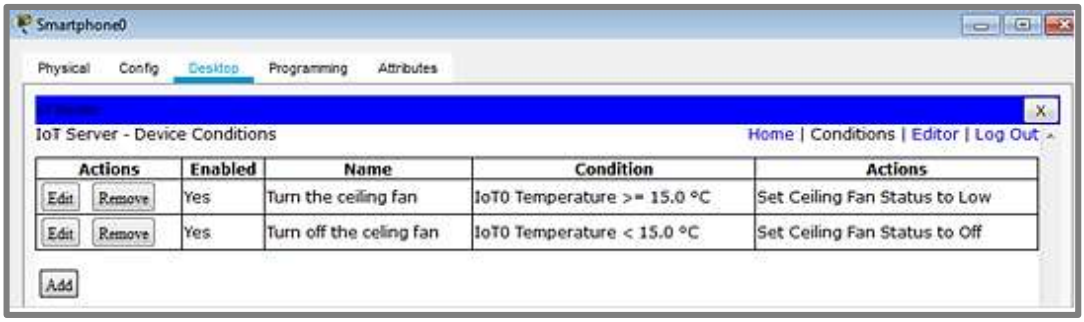


Рисунок 5.13 – Налаштування режиму роботи вентилятора залежно від температури

Опишіть принцип налаштування режимів роботи вентилятора

Відповідь:_____

3. Моделювання мережі IoT гаража

3.1. Встановлюємо та підключаємо IoT пристрій – **Smoky detector** (Детектор диму).

3.2. Встановлюємо та підключаємо IoT пристрій – **Siren** (Сирена).

3.3. Встановлюємо та підключаємо IoT пристрій – **Fire Sprinkler** (Пожежний розпилювач).

3.4. Добавляємо червону машину **Old Car**.

3.5. На смартфоні встановлюємо правило роботи для **Smoky detector**: якщо рівень газів на **Smoky detector** перевищує значення 10, то вмикається аварійна сигналізація **Siren**.

3.6. На смартфоні встановлюємо правило роботи для пожежного розпилювача **Fire Sprinkler**: якщо рівень газів на **Smoky detector** перевищує значення 10,5 то вмикається пожежний розпилювач **Fire Sprinkler**.

3.7. Перевіряємо правильність роботи. Вмикаємо машину декілька разів, щоб рівень газів перевищив норму й перевіряємо чи спрацьовують сирена та пожежний розпилювач.

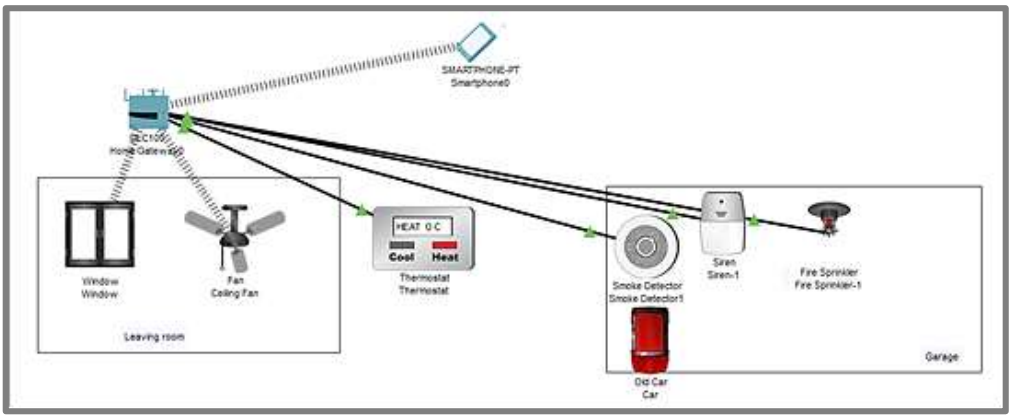


Рисунок 5.14 – Пояснення до пунктів 3.1–3.4

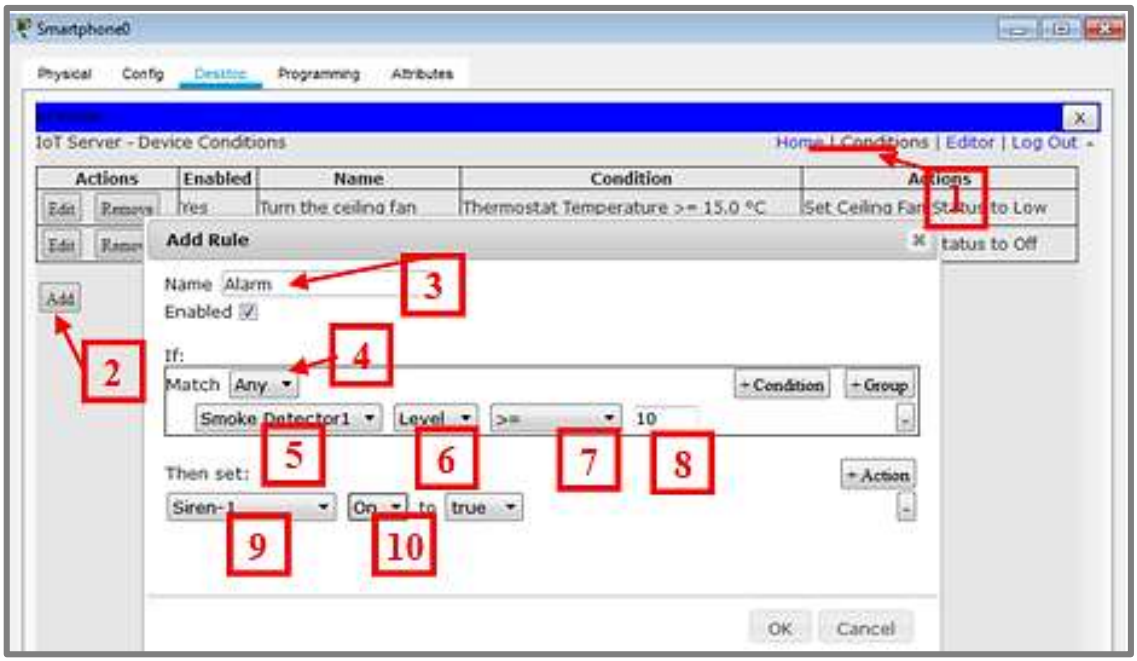


Рисунок 5.15 – Пояснення до пункту 3.5



Рисунок 5.16 – Пояснення до пункту 3.6

4. Розроблення технічних рішень житлової IoT кімнати

4.1. Провести моделювання «розумної кімнати», яка включає такі елементи: **Window** (Вікно), **Thermostat** (Термостат), **Furnace** (Батарея обігріву), **Air Conditioner** (Кондиціонер), **Door** (Двері), як показано на рис. 5.17.

Управління пристроями здійснюйте через **Home Gateway** за допомогою **Smartphone**.

4.2. Опишіть логіку з’єднання пристроїв.

4.3. Опишіть правила управління пристроями.

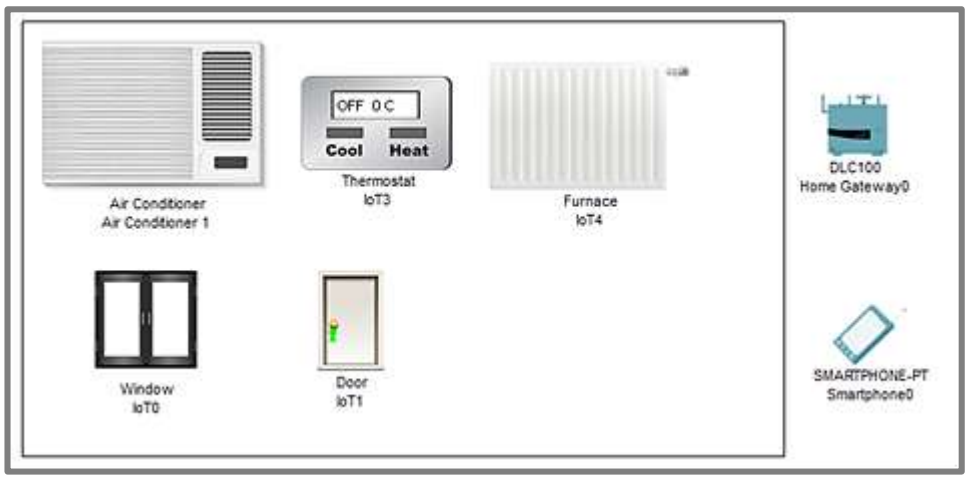


Рисунок 5.17 – IoT пристрої для розумної кімнати

ВИМОГИ ДО ОФОРМЛЕННЯ ЗВІТУ

1. Сформуйте файл для звіту. Звіт про виконання роботи має включати:

- Титульний аркуш, вказуючи номер і назву роботи, прізвище і групу студента.
- Покроковий опис основних етапів виконання роботи. Отримані результати підтверджуються скріншотами екрана.
- Пояснення прийнятих рішень, логіки з'єднання пристроїв та правил керування пристроїв при розробленні власної моделі розумної житлової кімнати.
- Висновки щодо проведеної роботи.

2. За завданнями 1–3: створений файл моделі житлової кімнати й гаража з назвою LR-5-1_XXXXX.pkt, де XXXXX – позначення прізвища студента.

3. За завданням 4: створений файл моделі житлової кімнати з рішенням студента з назвою LR-5-2_XXXXX.pkt, де XXXXX – позначення прізвища студента.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Яке призначення Packet Tracer?
2. Який пристрій у типовому розумному домі забезпечує підключення до мережі для розумних пристроїв IoT?
3. Опишіть налаштування бездротової мережі для пристроїв IoT.
4. Як можна здійснювати управління пристроями IoT?
5. Опишіть процес налаштування конфігурації IoT-пристрою для його управління зі смартофона чи планшета?

ЛАБОРАТОРНА РОБОТА № 6
ПІДКЛЮЧЕННЯ ПРИСТРОЇВ IOT ДО СЕРВЕРА В CISCO PACKET TRACER

Мета роботи: підключення пристроїв IoT до сервера за допомогою swith та домашнього шлюзу (Home Gateway); розроблення IoT проекту з'єднань Інтернет-провайдера, клієнтів для модему та 3G/4G.

ВКАЗІВКИ ДО ВИКОНАННЯ РОБОТИ

1. Підключення пристроїв IoT до сервера за допомогою swith

1.1. Для виконання цього завдання необхідні такі елементи: детектор руху **Motion Detector**, вебкамера **Webcam**, **Server-PT** та **Swith 2960. Server** для реєстрації обирається, як показано на рис. 6.1.



Рисунок 6.1 – Вибір сервера з панелі пристроїв

Виконайте підключення, як показано на рисунку 6.2. Підключення здійснюється за допомогою кабелю **Copper Straight Through.**

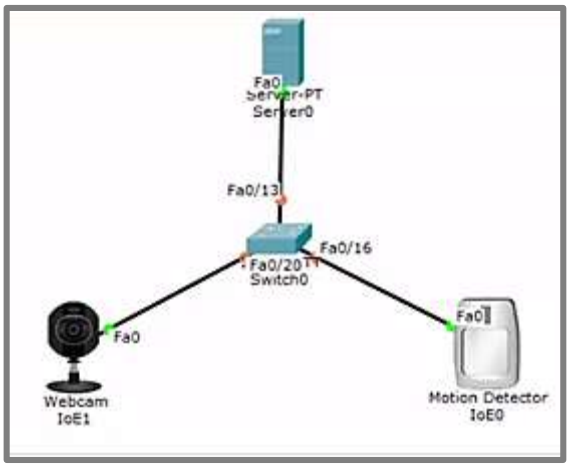


Рисунок 6.2 – Підключення пристроїв

1.2. Присвоєння статичних адрес

Присвойте серверу статичну IP-адресу – **1.1.1.1**. Відповідно присвойте вебкамері IP-адресу – **1.1.1.2** (рис. 6.3.) та змініть її назву на **Webcam-1**; а детектору руху присвойте статичну IP-адресу – **1.1.1.3** та змініть його назву на моніторі – **Motion Detector-1**.

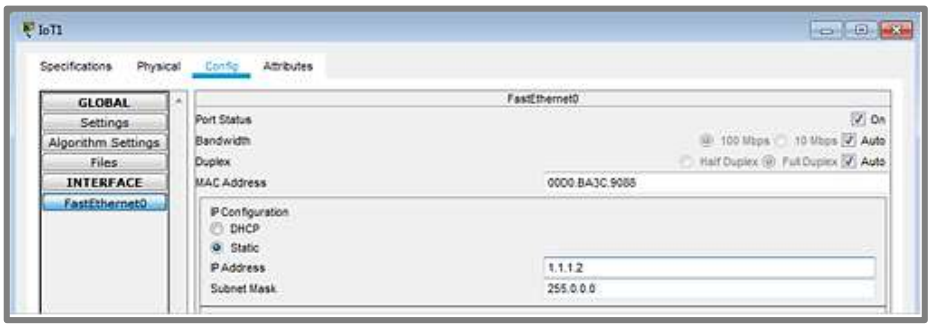
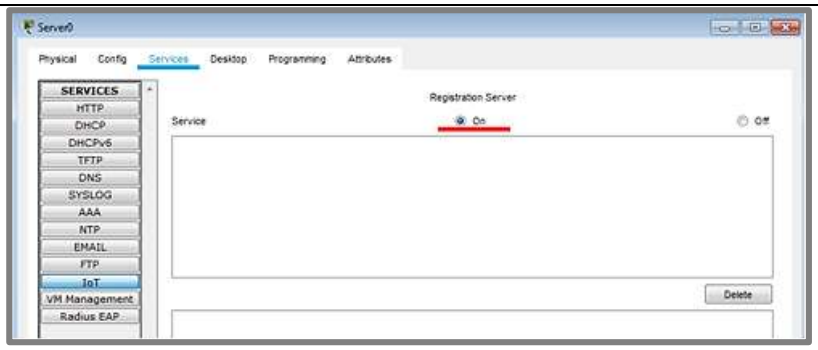
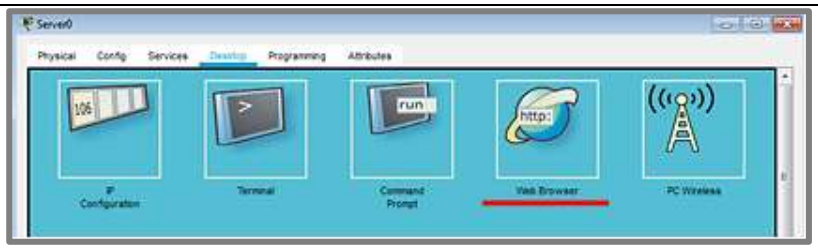


Рисунок 6.3 – Присвоєння статичних IP-адрес

1.3. Налаштуйте сервер на реєстрацію інформації від пристроїв 1–3:

Алгоритм присвоєння серверу статичної IP-адреси

1	Включіть режим реєстрації	
2	Зайдіть у веббраузер сервера	
3	Для першої реєстрації введіть ім’я користувача та пароль	

1.4. Налаштуйте вебкамеру **Webcam** на роботу із сервером (рис. 6.4).



Рисунок 6.4 – Налаштування Webcam на роботу із сервером

1.5. Налаштуйте детектор руху **Motion Detector-1** на роботу із сервером (аналогічно пункту 1.4.).

1.6. Натисніть на іконку **Server** та через **Desktop** / **Web-browser** наберіть адресу, а потім ім'я користувача та пароль сервера. Перевірте підключення пристроїв до сервера (рис. 6.5).

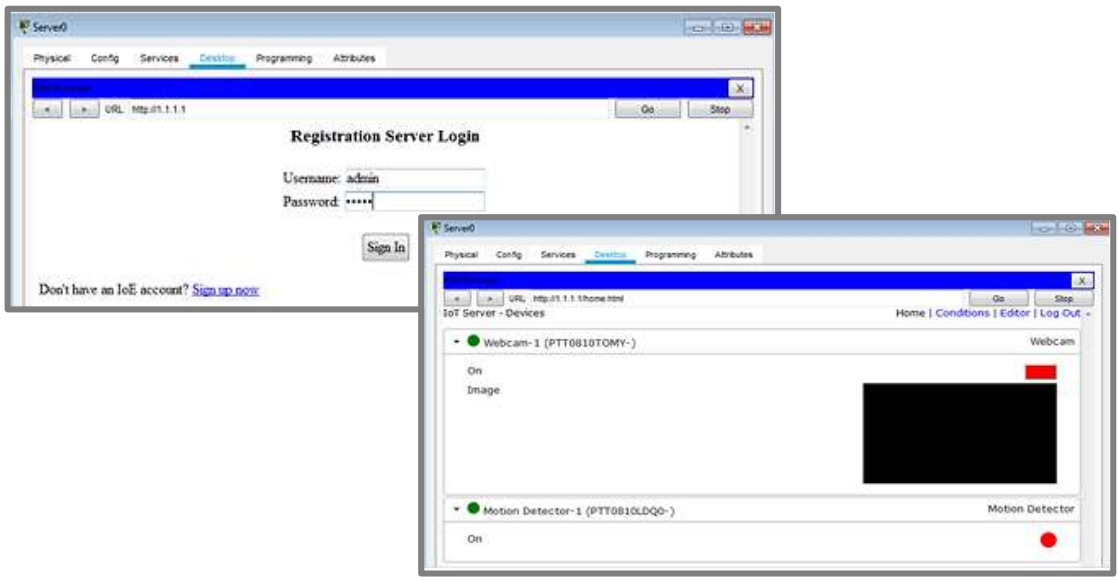


Рисунок 6.5 – Підключення пристроїв до сервера

Не закриваючи вікно сервера, проконтролюйте чи працює детектор. Натисніть і утримуйте **Alt** та проведіть курсором миші перед **Motion Detector** у полі моделювання. Він має спрацьовувати й у моделі й у сервері.

1.7. Встановіть правила роботи пристроїв. У вікні сервера натисніть **Conditions** та введіть правила роботи (рис. 6.6).

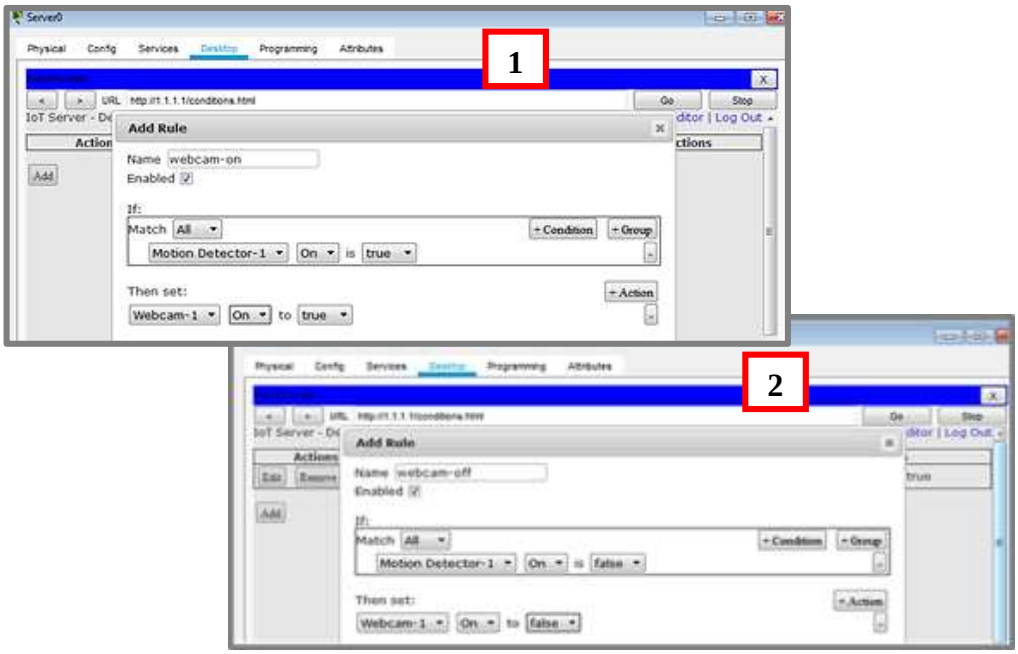


Рисунок 6.6 – Пояснення до пункту 1.7

У результаті одержимо такі режими роботи (рис. 6.7):

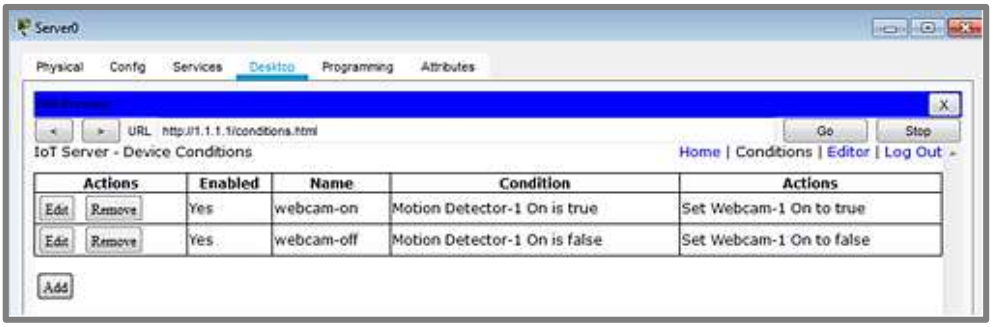


Рисунок 6.7 – Налаштування режимів роботи пристроїв

1.8. Не закриваючи вікно сервера перевірте правильність роботи.

Перейдіть у вкладку **Home**. Розмістіть на екрані монітора модель і налаштування сервера так, щоб їх було видно одночасно. Натисніть і утримуйте **Alt** та проведіть курсором миші перед **Motion Detector** у полі моделювання. Він має спрацьовувати, а **Webcam** має «фіксувати» рух порушника (рис. 6.8).

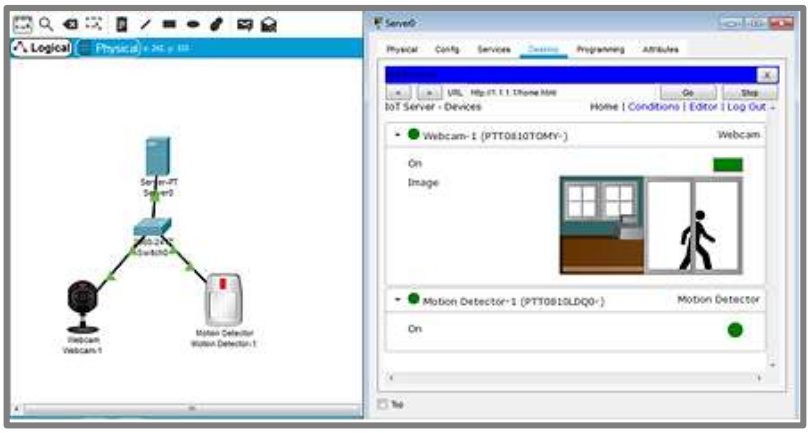


Рисунок 6.8 – Перевірка правильності роботи пристроїв

1.9. Збережіть отриману модель в файл під назвою LR-6-1-XXXXX.pkt.

2. Підключення пристроїв IoT до сервера за допомогою Home Gateway.

Самостійно побудуйте схему з аналогічними правилами, але замініть **Swith** на домашній шлюз **Home Gateway**. Налаштуйте **Webcam** та **Motion Detector** для роботи у бездротовій мережі. Для цього у властивостях входів/виходів оберіть адаптер бездротової мережі (рис. 6.9).

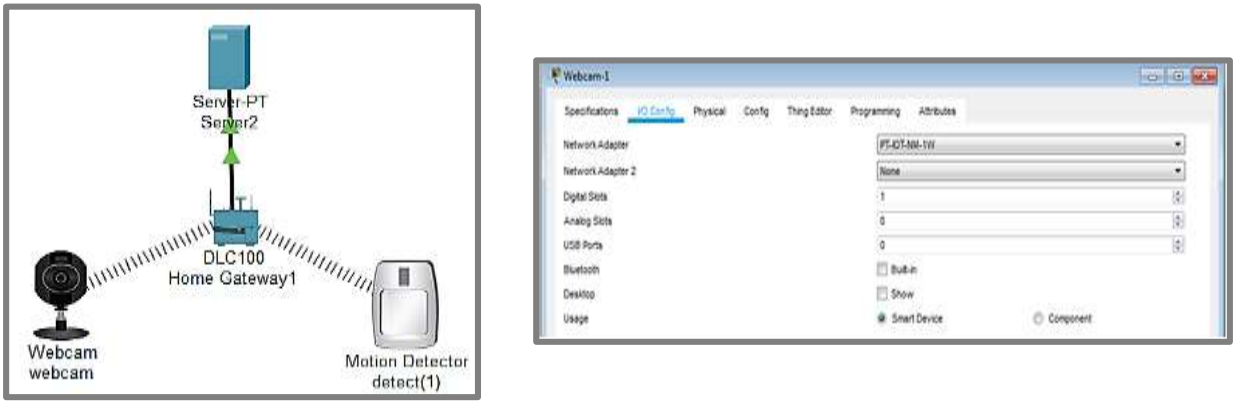


Рисунок 6.9 – Підключення пристроїв до сервера за допомогою Home Gateway

3. Розроблення IoT проекту з'єднань Інтернет-провайдера, клієнтів для модему та 3G/4G

3.1. Знайдіть елементи та розмістіть їх на робочій області програми. Перейменуйте пристрої відповідно до рис. 6.10.

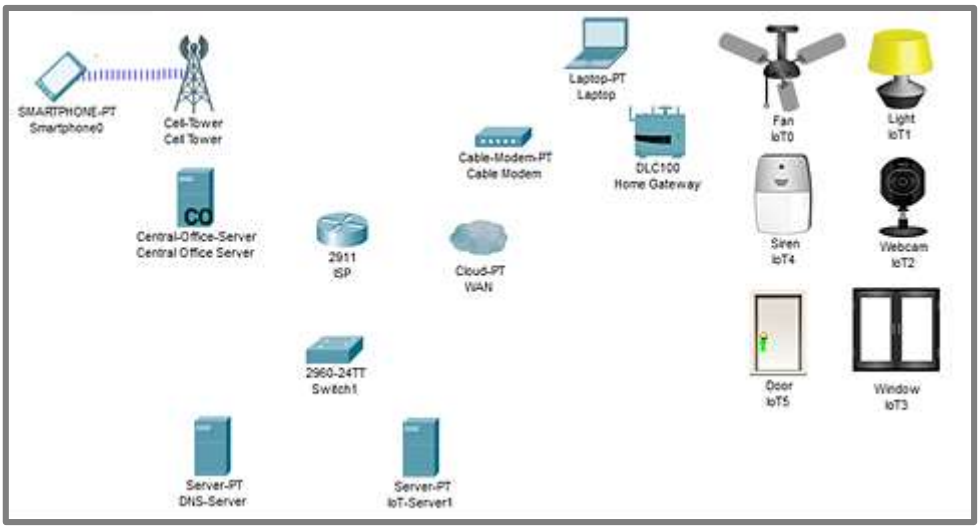


Рисунок 6.10 – Набір пристроїв для мережі

3.2. Підключіть пристрої один до одного, як показано на рис. 6.11. Зверніть увагу на кабелі підключення та оберіть відповідні входи/виходи.

Карта **PT-CLOUD-NM-1AM** має подвійні роз'єми RJ-11, які використовуються для підключення базових телефонних послуг. **WIC-1AM** використовує один порт для підключення до стандартної телефонної лінії, а інший порт може бути підключений до базового аналогового телефона для використання, коли модем перебуває в режимі очікування.

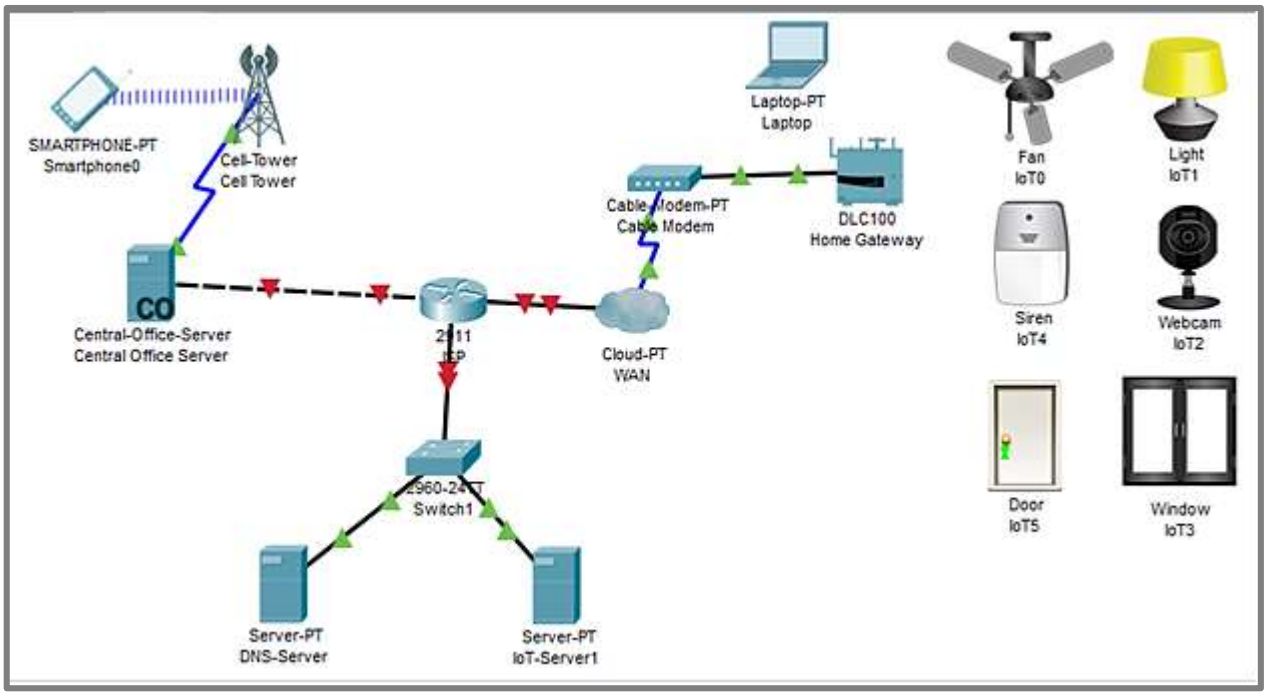


Рисунок 6.11 – Підключення пристроїв

3.3. Налаштуйте **Home Gateway**.

Для бездротової мережі встановіть параметри, як показано на рис. 6.12. Перевірте обов'язково, щоби був підключений **DHCP**.

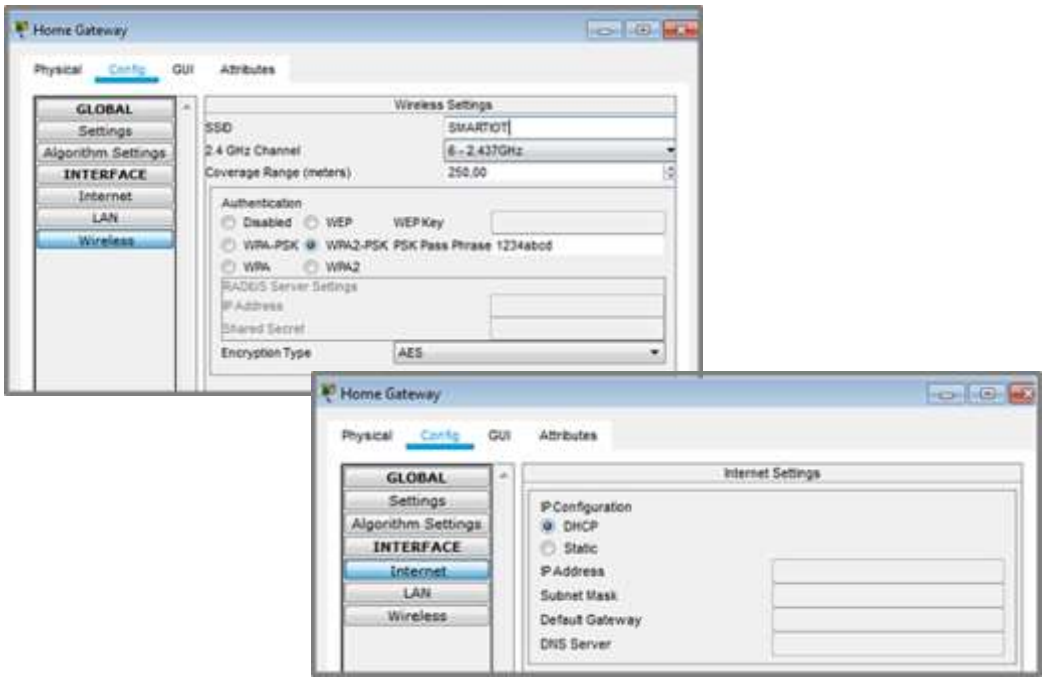


Рисунок 6.12 – Налаштування Home Gateway

3.4. Налаштуйте ноутбук. Вставте в порт ноутбука радіомодем (рис. 6.13). Для цього:

- вимкніть ноутбук (1);
- перетягніть карту (2) на місце (3);
- перетягніть модуль **Linksys-WPC300N** з місця (3) у ноутбук на місце (2);
- ввімкніть ноутбук (1).

Модуль **Linksys-WPC300N** забезпечує один бездротовий інтерфейс на 2,4 ГГц, який придатний для підключення до бездротових мереж. Модуль підтримує протоколи, які використовують Ethernet для доступу до локальної мережі.

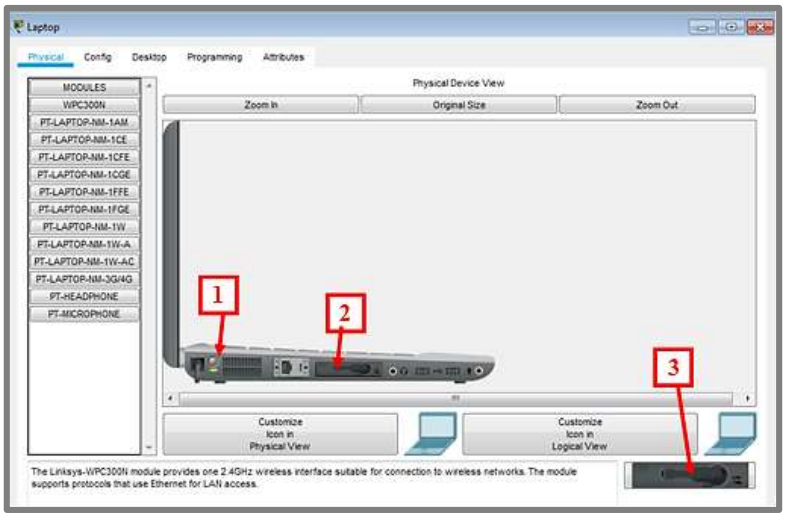


Рисунок 6.13 – Налаштування ноутбука

Зайдіть у бездротове з’єднання (рис. 6.14).



Рисунок 6.14 – Вкладка бездротового з’єднання

У вкладці **Connect** натисніть кнопку **Connect** (рис. 6.15). У новому вікні введіть пароль, як на рис. 6.15.



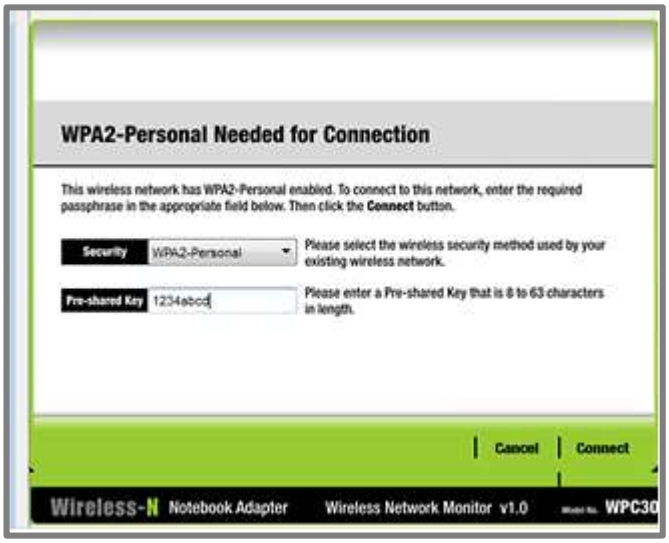


Рисунок 6.15 – Налаштування Laptop для доступу до Wireless

3.5. Налаштуйте **Webcam**. Добавте модуль **PT-IOT-NM-1W** та введіть SSID – **SMARTIOT** і пароль – **1234abcd** (рис. 6.16).

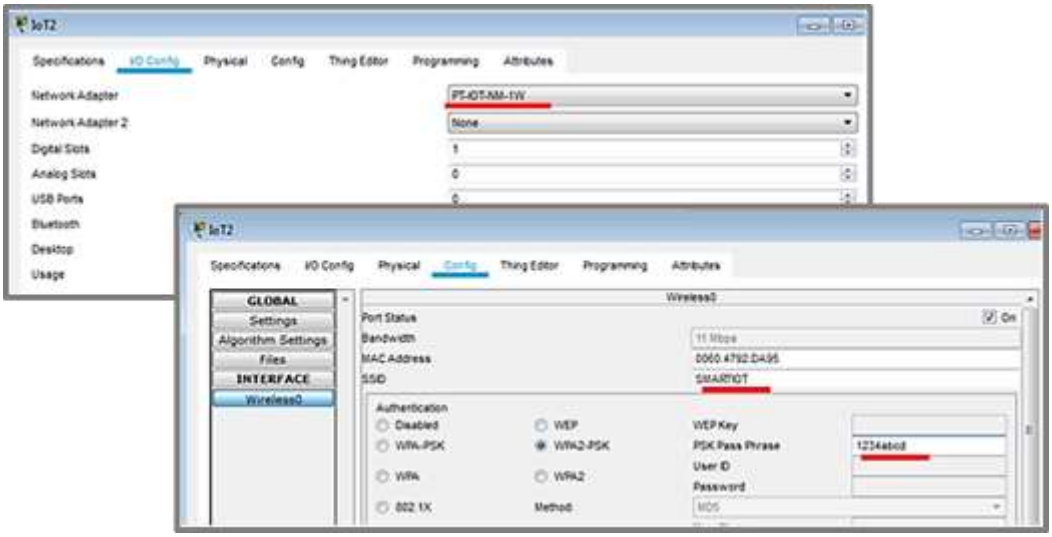


Рисунок 6.16 – Налаштування Webcam

3.6. Аналогічним чином налаштуйте решту IoT пристроїв: сирену **Siren**, вікно **Window**, двері **Door**, вентилятор **Fan** та лампу **Light**. Добавте модуль до пристроїв **PT-IOT-NM-1W** та введіть SSID – **SMARTIOT** і пароль – **1234abcd**. За бажанням можна з'єднати декілька пристроїв кабельним з'єднанням.

3.7. Використовуючи інструменти 1 та 2 виділіть функціональні області та підпишіть їх, як показано на рис. 6.17. Перевірте правильність підключення портів.

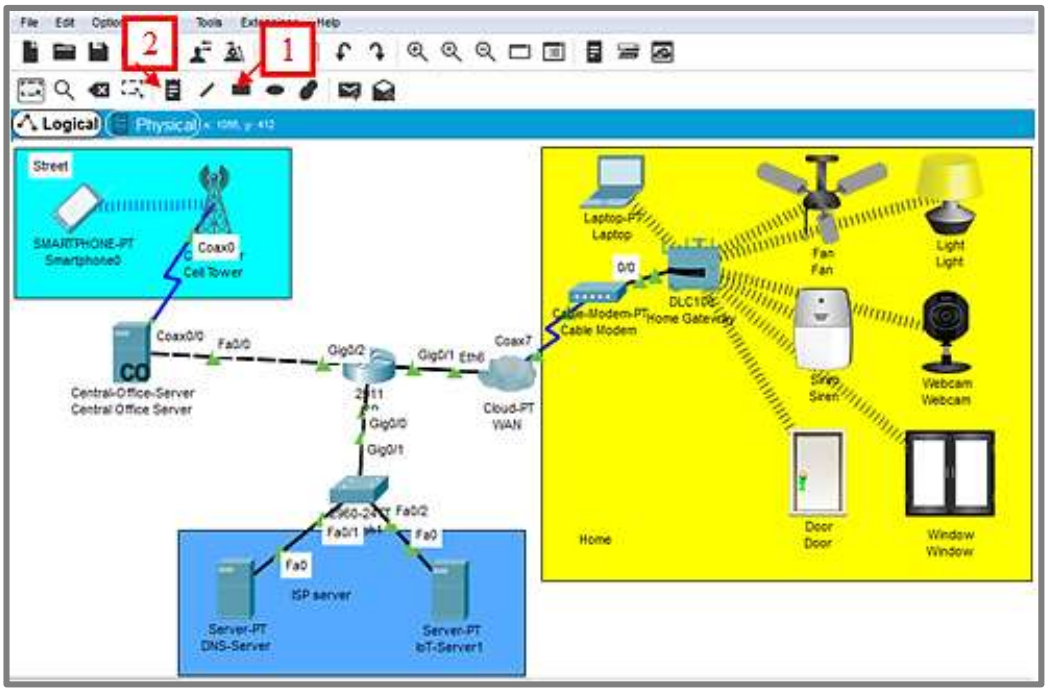


Рисунок 6.17 – Виділення функціональних областей

3.8. Налаштуйте ISP. Для цього з командного рядка введіть управління адресацією так, як показано на рис. 6.18. Після набору кожної команди натискайте **Enter**.

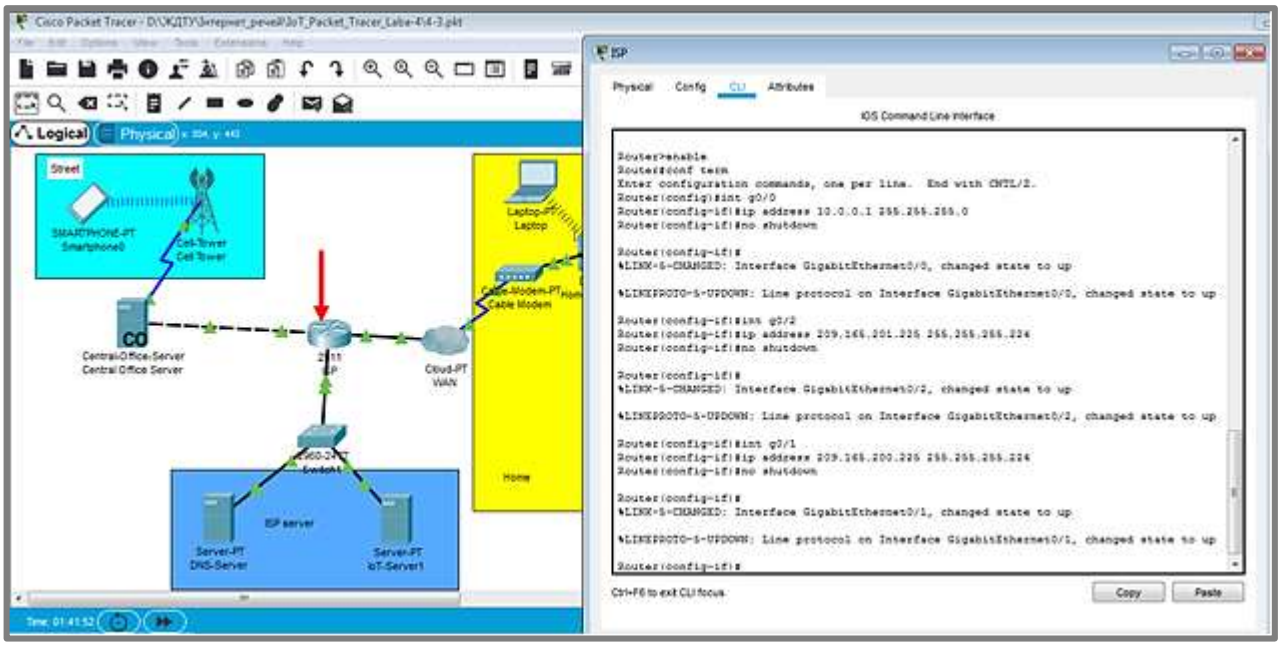


Рисунок 6.18 – Налаштування ISP з командного рядка

3.9. Налаштуйте ISP на роботу з **Cell** через **Central Office Server** (рис. 6.19)

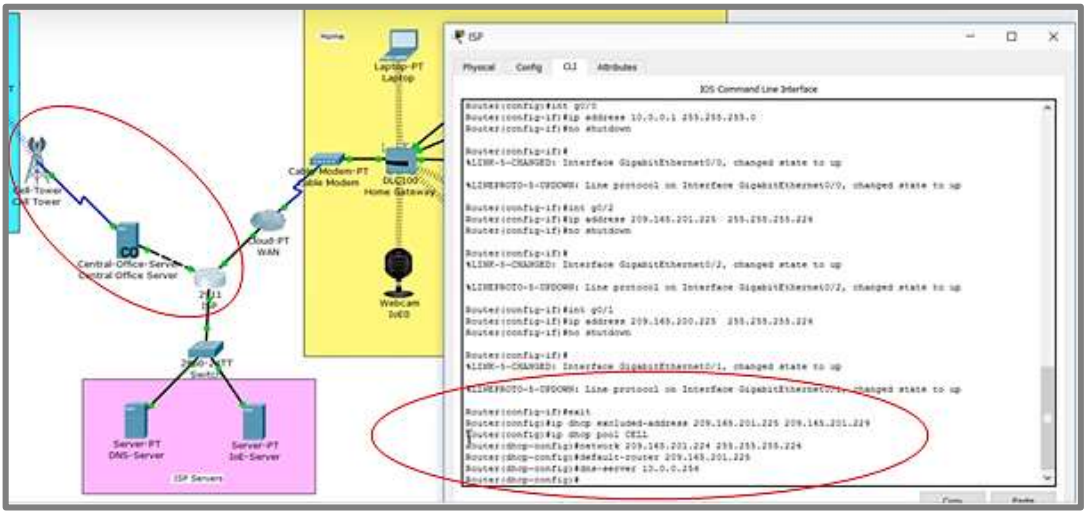


Рисунок 6.19 – Налаштування ISP на роботу з Cell через Central Office Server

3.10. Налаштуйте ISP на роботу з **Home Gateway** через **WAN** (рис. 6.20).

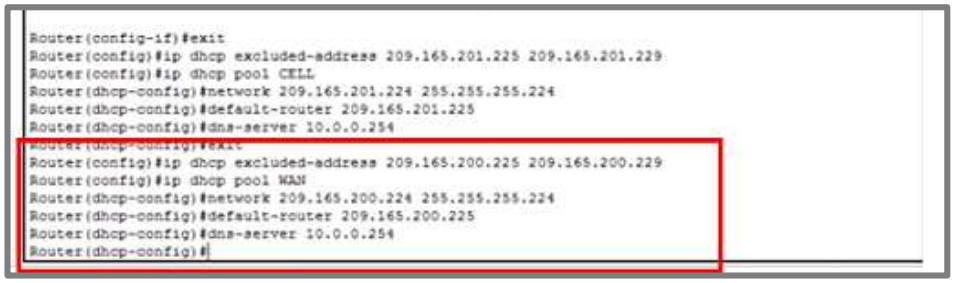


Рисунок 6.20 – Налаштування ISP на роботу з Home Gateway через WAN

Загалом, комбінація групового коду буде мати вигляд

```
Router>enable
Router#config terminal

Router(config-router)#int g0/0
Router(config-if)#ip address 10.0.0.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#int g0/1
Router(config-if)#ip address 209.165.200.225 255.255.255.224
Router(config-if)#no shutdown

Router(config-if)#int g0/2
Router(config-if)#ip address 209.165.201.225 255.255.255.224
Router(config-if)#no shutdown

Router(config-if)#exit
Router(config)#ip dhcp excluded-address 209.165.201.225 209.165.201.229
Router(config)#ip dhcp pool CELL
Router(dhcp-config)#network 209.165.201.224 255.255.255.224
Router(dhcp-config)#default-router 209.165.201.225
Router(dhcp-config)#dns-server 10.0.0.254

Router(config-if)#exit
Router(config)#ip dhcp excluded-address 209.165.200.225 209.165.200.229
Router(config)#ip dhcp pool WAN
Router(dhcp-config)#network 209.165.200.224 255.255.255.224
Router(dhcp-config)#default-router 209.165.200.225
Router(dhcp-config)#dns-server 10.0.0.254
```

У налаштуваннях **WAN** оберіть відповідні **Coaxial** та **Ethernet** (рис. 6.21). У вкладці **Ethernet** оберіть **Cable**.

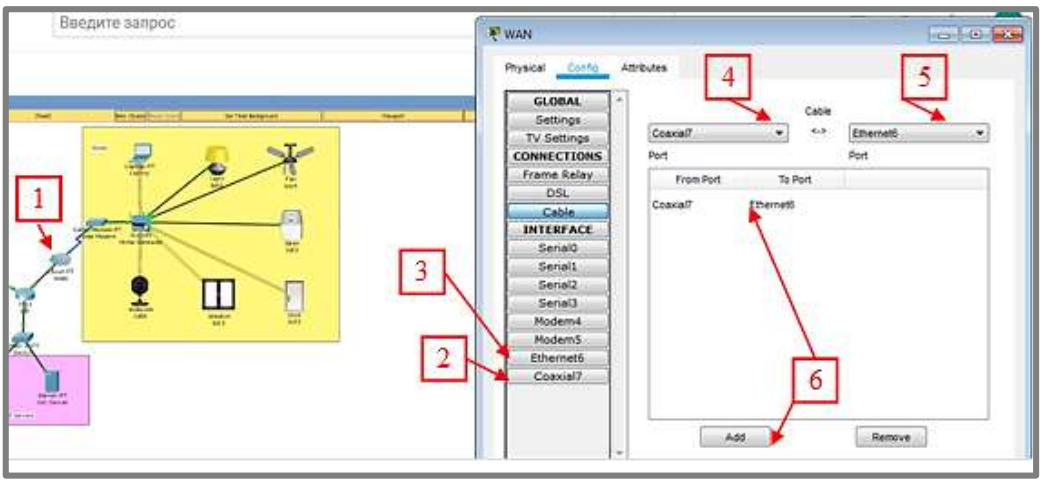


Рисунок 6.21 – Налаштування WAN

Перевіряємо, щоб адреси обновилися в **Home Gateway**. Для цього натискаємо по черзі **DHCP** – **Static** – **DHCP**). Оновлюємо параметри мережі в **Laptop** (рис. 6.22).

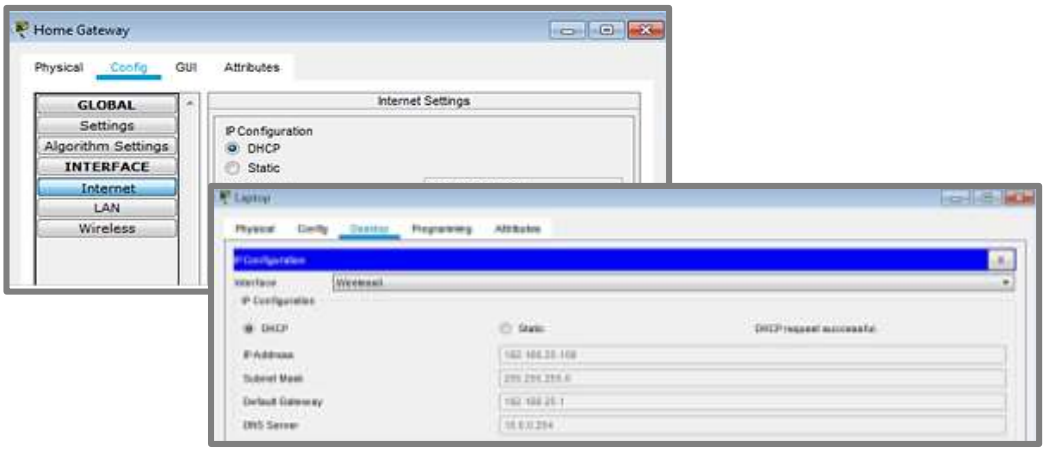


Рисунок 6.22 – Оновлення адрес Home Gateway та Laptop

Оновлюємо параметри мережі у всіх інших IoT пристроях **Home** (рис. 6.23).

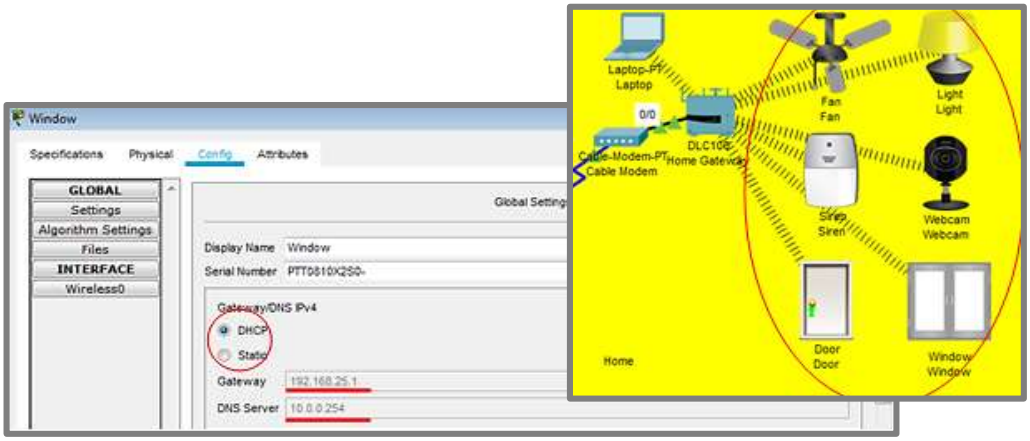


Рисунок 6.23 – Оновлення параметрів мережі у всіх IoT пристроях Home

3.11. Налаштовуємо **DNS-Server**. Заходимо в **Desktop** натискаємо **IP Configuration** та вводимо статичні адреси (рис. 6.24). Переходимо у вкладку **Services** та вмикаємо **DNS-Service**.

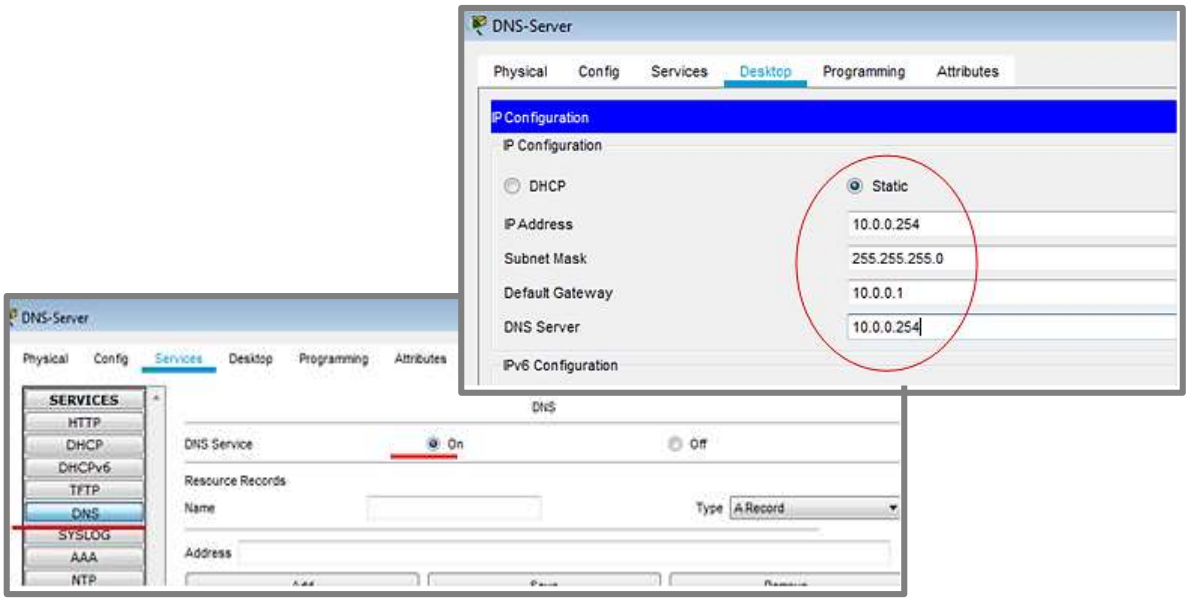


Рисунок 6.24 – Налаштування DNS-Server

3.12. Аналогічно конфігуруємо **IoT-Server** (рис. 6.25). Вмикаємо сервіс IoT.

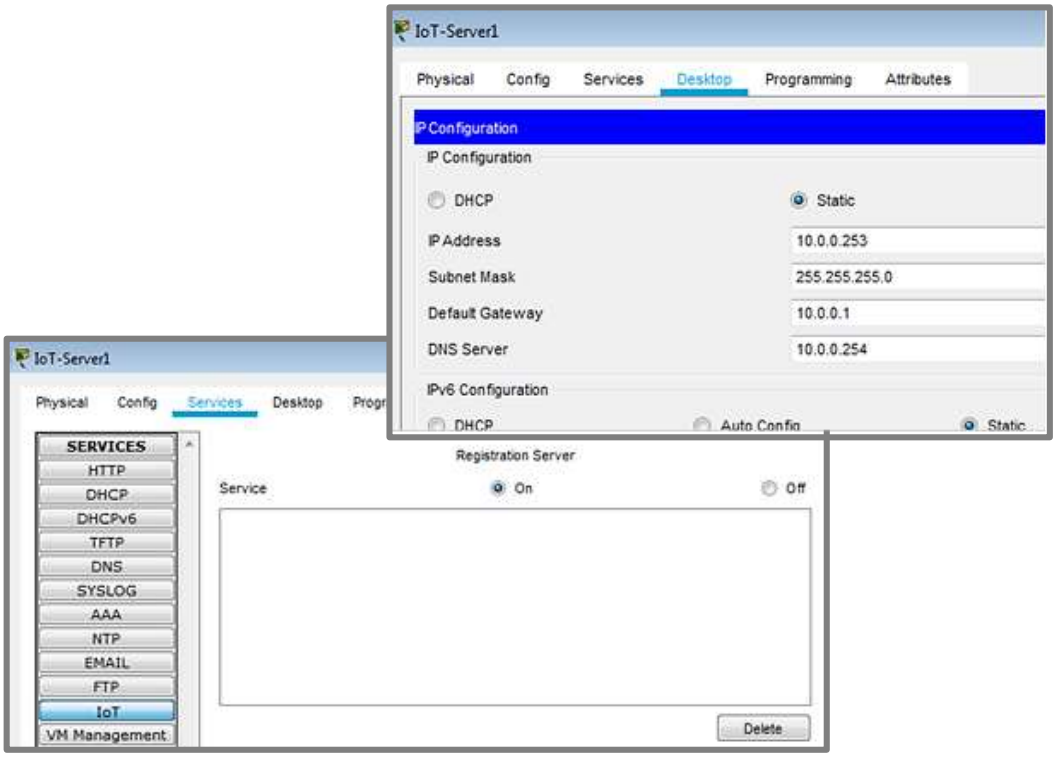


Рисунок 6.25 – Конфігурація IoT-Server

3.13. Асоціюємо IoT-пристрої з IoT-Server. Заходимо в налаштування вебкамери та підключаємо її до IoT-Server (рис. 6.26). Аналогічно підключаємо всі інші IoT-пристрої.

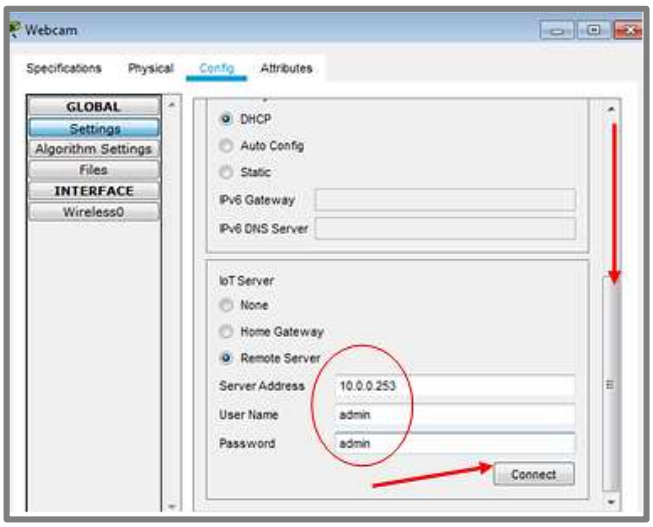
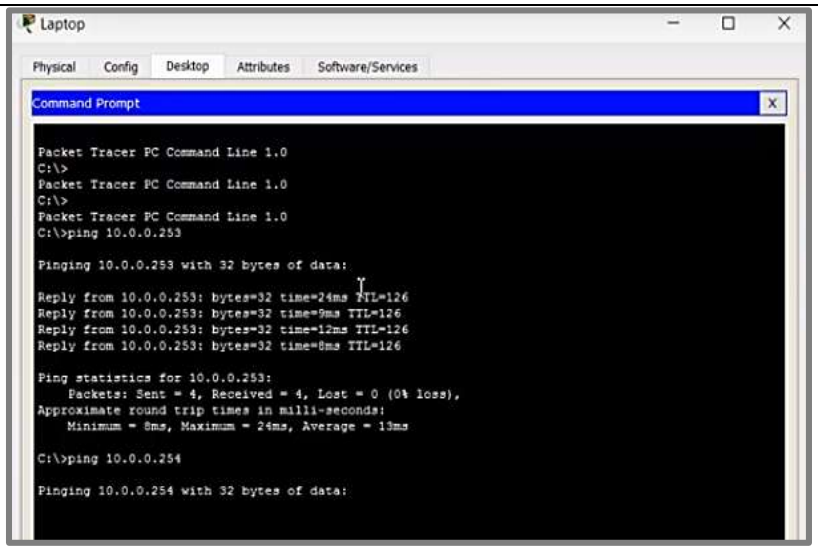
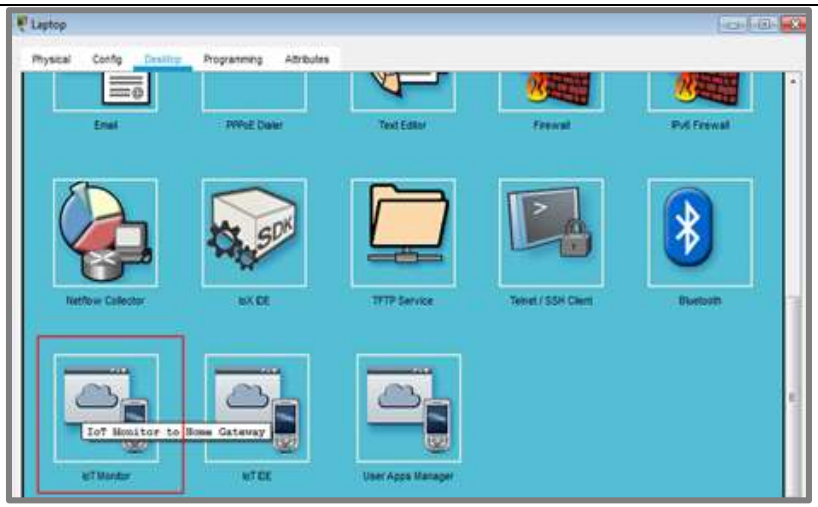
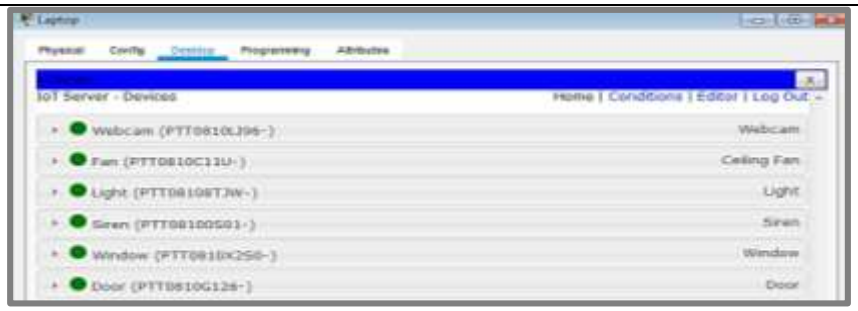


Рисунок 6.26 – Підключення IoT-пристроїв до IoT-Server

3.14. Перевіряємо підключення ноутбука командами **ping** до серверів. Алгоритм дій:

1	Вводимо в командному рядку: **ping 10.0.0.253**	

2	Заходимо в IoT Monitor	
3	Міняємо адресу IoT-Server (**10.0.0.253**) **admin**	
4	Реєструємо новий сервер	
5	Вводимо логін і пароль – **admin**	
6	Відображення IoT-пристроїв в IoT Monitor	

***Примітка**: Якщо IoT-пристрої не відобразяться в IoT Monitor, то необхідно повторити пункт 3.13 та перепідключити їх.*

3.15. Перевіряємо роботу всіх пристроїв із ноутбука.

3.16. Перевіряємо роботу всіх пристроїв зі смартфона.

3.17. Узгоджуємо роботу двох серверів за назвою. Добавляємо ім'я і адресу (рис. 6.27).



Рисунок 6.27 – Узгодження роботи двох серверів

3.18. Перевіряємо доступ із ноутбука (ping www.iot.org або ping www.ioe.org), як на рис. 6.28.

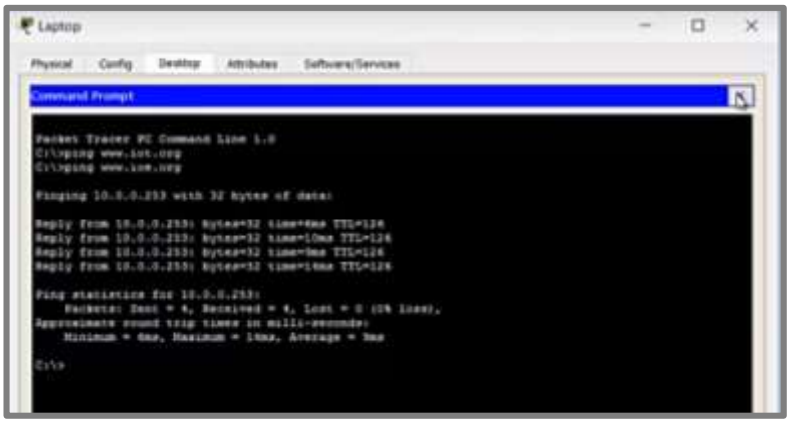


Рисунок 6.28 – Перевірка доступу з ноутбука

Перевіряємо підключення з ноутбука за ім'ям (рис. 6.29).



Рисунок 6.29 – Перевірка підключення з ноутбука

3.19. Перевіряємо доступ зі смартфона аналогічно пункту 3.18.

3.20. Перейменовуємо доступ до **IoT-Server** (рис. 6.30).

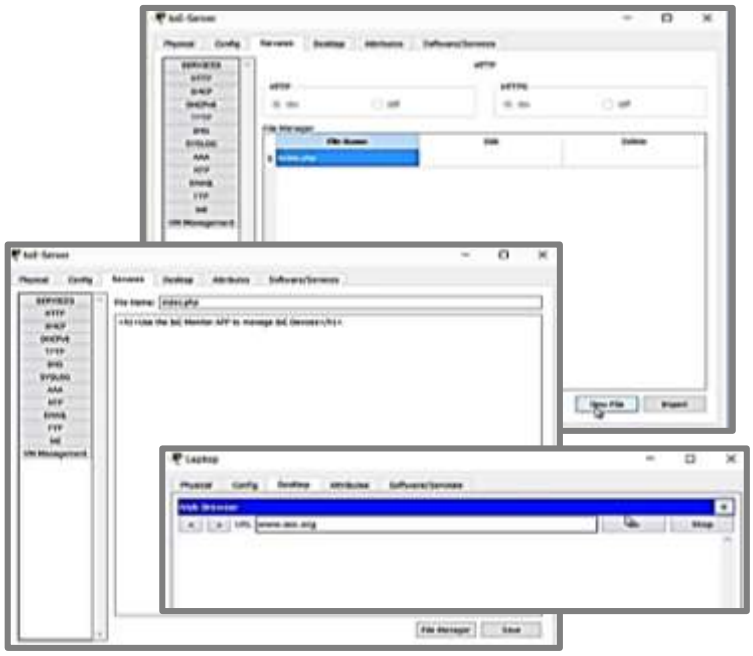


Рисунок 6.30 – Перейменування доступу до IoT-Server

ВИМОГИ ДО ОФОРМЛЕННЯ ЗВІТУ

1. Сформуйте файл для звіту. Звіт про виконання роботи має включати:

- Титульний аркуш, вказуючи номер і назву роботи, прізвище і групу студента.
- Покроковий опис основних етапів виконання роботи. Отримані результати підтверджуються скріншотами екрана.
- Висновки щодо проведеної роботи.

2. За завданнями 1: створений файл моделі з назвою LR-6-1_XXXXX.pkt, де XXXXX – позначення прізвища студента.

3. За завданням 2: створений файл моделі з назвою LR-6-2_XXXXX.pkt, де XXXXX – позначення прізвища студента.

4. За завданням 3: створений файл моделі з назвою LR-6-3_XXXXX.pkt, де XXXXX – позначення прізвища студента



КОНТРОЛЬНІ ЗАПИТАННЯ

1. Що таке DNS-сервер?
2. Для чого використовується DHCP?
3. Які етапи процесу отримання клієнтом IP-адреси із сервера DHCP?
4. Які повідомлення надсилає DHCP для виконання завдань, що не пов’язані з отриманням IP-адреси?
5. Вкажіть переваги застосування протоколу DHCP.
6. Наведіть недоліки застосування протоколу DHCP.
7. Як встановлюється зв’язок між датчиками та виконавчими елементами?
8. Як налаштувати провайдера послуг Інтернету на роботу з Home Gateway та інших пристроїв?
9. Як перевірити підключення пристроїв до сервера?

ЛАБОРАТОРНА РОБОТА № 7
ВИКОРИСТАННЯ FOG COMPUTING У РОЗУМНОМУ ДОМІ

Мета роботи: дослідження розумного будинку й аналіз використання туманних обчислень для моніторингу та керування IoT-пристроями; ознайомлення з мікроконтролером PT-MCU та його аспектом програмування.

ЧАСТИНА 1
ДОСЛІДЖЕННЯ SMART HOME

ВКАЗІВКИ ДО ВИКОНАННЯ РОБОТИ

1. Дослідження розумного будинку.

1.1. Розуміння пристроїв, які входять до складу розумного дому.

Відкрийте файл **Explore the Smart Home.pkt**. Інтернет-провайдери зазвичай передають дані та відео через один коаксіальний кабель. У показаній топології (рис. 7.1) починаючи з горища, для відділення відеосигналу від сигналу даних використовується коаксіальний розгалужувач.

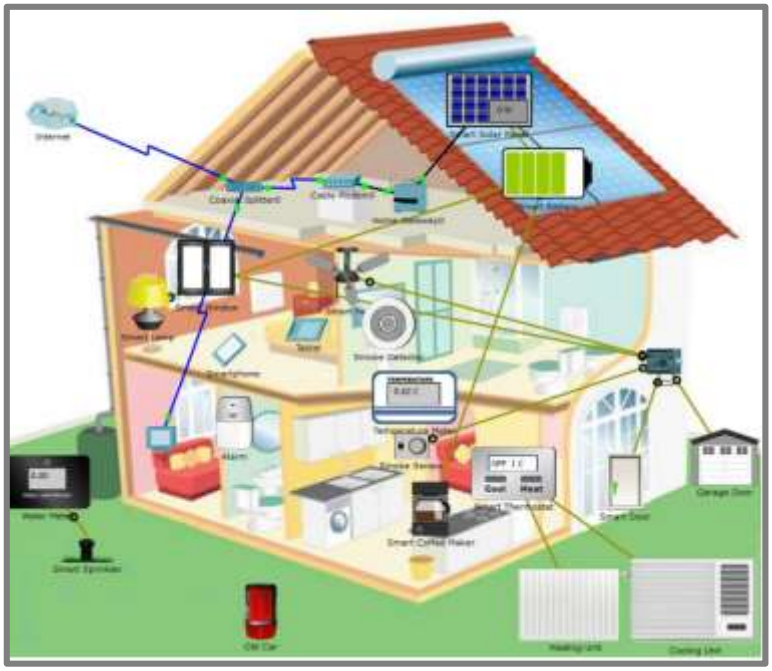


Рисунок 7.1 – Топологія мережі розумного будинку

1) Два коаксіальних кабелі виходять із коаксіального розгалужувача в показаній топології.

❓ До яких пристроїв підключається коаксіальний кабель?

Відповідь:_____

2) Кабельний модем Cable modem є інтерфейсом між мережею провайдера та домашньою мережею.

❓ До яких пристроїв підключається кабельний модем?

Відповідь:_____

Домашній шлюз Home Gateway діє як концентратор і маршрутизатор для всіх внутрішніх домашніх пристроїв. Він також надає вебінтерфейс, який дає змогу користувачам контролювати різноманітні розумні домашні пристрої. Зауважте, що домашні пристрої можуть підключатися до домашнього шлюзу як через бездротові, так і через дротові з'єднання.

Примітка: *Packet Tracer використовує пунктирні промені для представлення бездротових з'єднань, але це може ускладнити читання, якщо присутній занадто багато пристроїв. Щоб увімкнути його, перейдіть до* Options / Preferences / Hide Tab та *зніміть прапорець* **Hide Wireless/Cellular Connection.**

❓ Перелічіть усі домашні пристрої, підключені до Home Gateway

Відповідь:_____

_____

1.2. Взаємодія з розумним будинком

Пристрої в розумному домі можна моніторити та контролювати віддалено через будь-який комп'ютер у домі. Оскільки всі розумні пристрої підключаються

до Home Gateway, який містить вебінтерфейс, планшети, смартфони, ноутбуки або настільні комп'ютери можна використовувати для взаємодії з розумними пристроями.

1) Клацніть планшет **Tablet** (він на ліжку, у головній спальні).
2) Перейдіть до **Desktop** / **Web Browser**.
3) В адресному рядку введіть **192.168.25.1**. Це IP-адреса Home Gateway.
4) Використайте **admin**/**admin** як ім'я користувача та пароль для входу в Home Gateway.

❓ Що відображається?

Відповідь:_____

_____

5) Розумні двері наразі розблоковані (позначається зеленим світлом на дверній ручці), але їх можна заблокувати дистанційно. Натисніть розумні двері в браузері.
6) Натисніть **Lock**, щоб заблокувати двері.

❓ Чи зачинено двері? Звідки ви знаєте?

Відповідь:_____

_____

7) Натисніть **Unlock**, щоб розблокувати двері.

❓ Клацніть детектор диму **SmokeDetector** в браузері. Який рівень диму показує детектор диму?

Відповідь:_____

❓ Чи можна контролювати детектор диму?

Відповідь:_____

Смарт-пристроями також можна керувати безпосередньо, представляючи фізичну взаємодію.

8) Утримуйте клавішу **Alt** і натисніть на розумну кавоварку, щоб увімкнути або вимкнути її.

2. Fog Computing у розумному домі

MCU, який доданий до «розумного дому», використовується для моніторингу рівня диму, який зчитує датчик диму, і вирішує, чи потрібно провітрювати будинок. Якщо рівень чадного газу підвищується понад 10,3 одиниць, MCU запрограмований на автоматичне відкриття вікна, вхідних дверей, дверей гаража та запуск вентилятора на високій швидкості. Ця дія повертається лише тоді (зачинити двері та вікна та зупинити вентилятор), коли рівень чадного газу падає нижче 1 одиниці.

У представленому прикладі власник тримає в гаражі класичний автомобіль, який час від часу потребує обкатки. Класичний автомобіль виробляє чадний газ, який підвищує рівень у приміщеннях.

1) Клацніть планшет (він на ліжку, у головній спальні).
2) Перейдіть до **Desktop / Web Browser.**
3) В адресному рядку введіть **192.168.25.1**. Це IP-адреса Home Gateway.
4) Використайте **admin/admin** як ім’я користувача та пароль для входу в Home Gateway.
5) Натисніть детектор диму; залиште це вікно видимим, щоб ви могли контролювати рівень диму.
6) Запустіть двигун **класичного автомобіля**, утримуючи клавішу **Alt** і натиснувши на класичний автомобіль.

Що відбувається з повітрям у будинку, коли машина працює в гаражі?

Відповідь:_____

Що відбувається з повітрям у будинку після того, як MCU відкриває двері та вікна та запускає вентилятор?

Відповідь:_____

Чи закриває MCU двері та вікна та зупиняє вентилятор?

Відповідь:_____

7) Продовжуючи стежити за рівнями, зупиніть двигун класичного автомобіля, утримуючи клавішу **Alt** і натиснувши на класичний автомобіль.

Що відбувається з якістю повітря в будинку після зупинки двигуна?

Відповідь:_____

Що відбувається з дверима, вікном і вентилятором?

Відповідь:_____

3. Міркування

Цей приклад показує, що рішення між хмарними обчисленнями й туманними залежить від програми. У прикладі розумного будинку найкращим варіантом було туманне обчислення. У прикладі смарт-будинку дані, отримані датчиками диму, оброблялися та використовувалися для прийняття рішень щодо якості повітря в будинку. У цьому сценарії не було необхідності надсилати дані датчиків у хмару для обробки. Хмарні обчислення можуть призвести до уповільнення часу відгуку, що може призвести до небезпеки життя людей. Інша можлива проблема пов'язана з інтернет-посиланням; якщо з'єднання з Інтернетом було втрачено, уся система могла б поставити життя в небезпеку

ЧАСТИНА 2
МІКРОКОНТРОЛЕРИ PT-MCU ТА ЇХ ПРОГРАМУВАННЯ



ТЕОРЕТИЧНІ ВІДОМОСТІ

Блок мікроконтролера (**MCU**) – це невеликий комп'ютер, побудований на системному чіпі **System on a Chip** (SoC). Він містить ядро процесора, пам'ять і програмовані периферійні пристрої вводу/виводу. Мікроконтролери розроблені для вбудованих додатків або додатків, які потребують мало ресурсів комп'ютера. Навпаки, мікропроцесори, що використовуються в персональних комп'ютерах, зазвичай використовуються для підтримки інших програм загального призначення, які потребують більше комп'ютерних ресурсів.

Прикладами програм, які покладаються на мікроконтролери, є системи керування двигуном автомобіля, імплантовані медичні пристрої, пульти дистанційного керування, офісні машини, прилади, електроінструменти, іграшки та інші вбудовані системи. Також поширені мікроконтролери зі змішаними сигналами, які об'єднують аналогові компоненти, необхідні для керування нецифровими електронними системами.

Packet Tracer забезпечує підтримку емулятора MCU. Користувач може запрограмувати PT MCU для виконання завдань, подібних до реальних MCU. Щоб спростити процес, PT MCU можна запрограмувати за допомогою Java і Python.

ЗАВДАННЯ ДО ВИКОНАННЯ РОБОТИ

1. Ознайомлення з мікроконтролером PT-MCU

Відкрийте файл **Packet Tracer - Sensors and the PT Microcontroller.pka**.

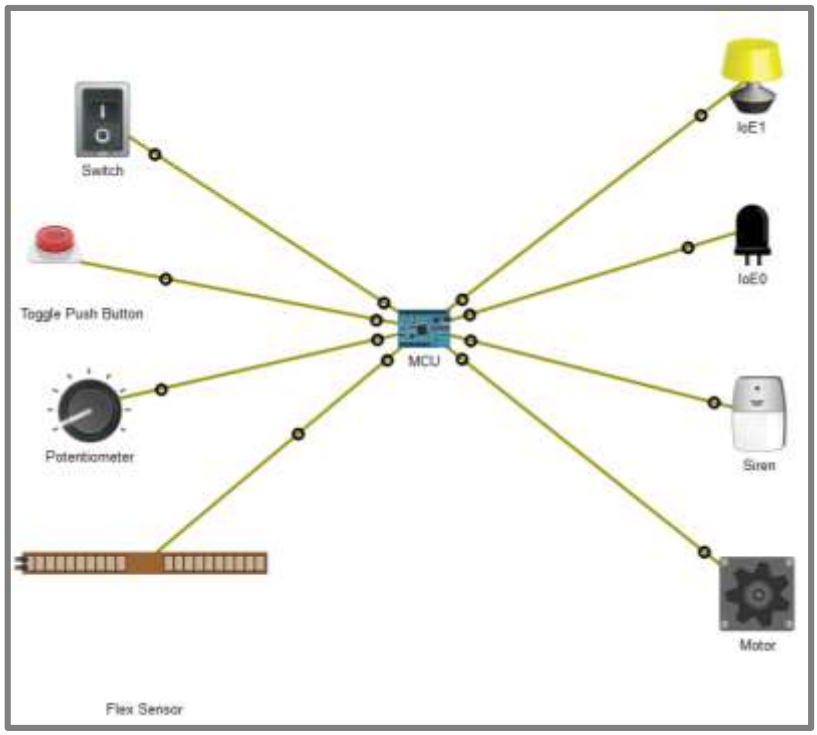


Рисунок 7.2 – Демонстрація підключення мікропроцесора та датчиків

PT MCU – це плата, яка має USB-порт, шість цифрових портів вводу-виводу та чотири аналогових порти вводу-виводу. Цифрові порти введення/виведення на PT MCU даю можливість користувачеві підключати цифрові датчики та виконавчі механізми. Аналогові порти введення/виведення дають змогу користувачеві підключати аналогові датчики та виконавчі механізми. У цій демонстрації є один PT MCU, підключений до чотирьох датчиків і чотирьох приводів. Чотири датчики включають цифровий перемикач **Switch**, цифрову кнопку перемикання **Toggle Push Button**, аналоговий потенціометр **Potentiometer** і аналоговий датчик гнучкості **Flex Sensor**. Чотири приводи включають світло **Light**, світлодіод **LED**, сирену **Siren** та аналоговий двигун **Motor**. PT MCU запрограмовано на Python на безперервне зчитування значень датчика, а потім записування у виконавчі механізми, керуючись умовною логікою. Взаємозв'язок між датчиками та виконавчими механізмами можна підсумувати так:

- Перемикач керує світлом.
- Кнопка керує світлодіодом.

- Потенціометр керує сиреною.
- Датчик гнучкості керує двигуном.

2. Датчики та PT MCU

2.1. Проаналізуйте топологію. **MCU,** розміщеного в центрі. Пристрої введення (датчики та перемикачі) розміщені ліворуч, а пристрої виведення – праворуч.

2.2. Дослідіть **MCU**, датчики, перемикачі та керовані пристрої, щоб відкрити їх вікна конфігурації. Зверніть увагу, що на різних пристроях доступні різні вкладки. У вікні **MCU** вкладка **Programming** містить запущений код Python. Код Python визначає поведінку пристрою.

2.3. Утримуйте клавішу **Alt**, клацаючи на пристрій, щоб взаємодіяти з пристроєм. Можливо, вам також доведеться утримувати **Shift**:

- ✓ **Alt +** натисніть **Switch**, щоб увімкнути/вимкнути світло **Light**.
- ✓ **Alt +** натисніть **Push Button**, щоб увімкнути/вимкнути **світлодіод LED**.
- ✓ **Alt** + натисніть, утримуйте та прокрутіть **Potentiometer**, щоб контролювати гучність сирени **Siren**.
- ✓ **Alt +** натисніть, утримуйте та перетягніть датчик гнучкості **Flex Sensor,** щоб контролювати швидкість двигуна **Motor**.

2.4. Зверніть увагу на те, до яких портів **MCU** підключено датчики, комутатори та пристрої.

3. Програмування MCU

Примітка: *Python, який використовується в PT, є інтерпретатором Python у JavaScript з відкритим кодом, який не оновлюється до Python 3.0. Із цієї причини можуть бути невеликі відмінності в синтаксисі між кодом, який спостерігається в PT, і кодом у пристроях, що використовують Python 3.*

3.1. Відкрийте **MCU**, розташований у центрі топології.

3.2. Виберіть вкладку **Programming** (рис. 7.3), щоб одержати доступ до коду Python, який працює на **MCU**.

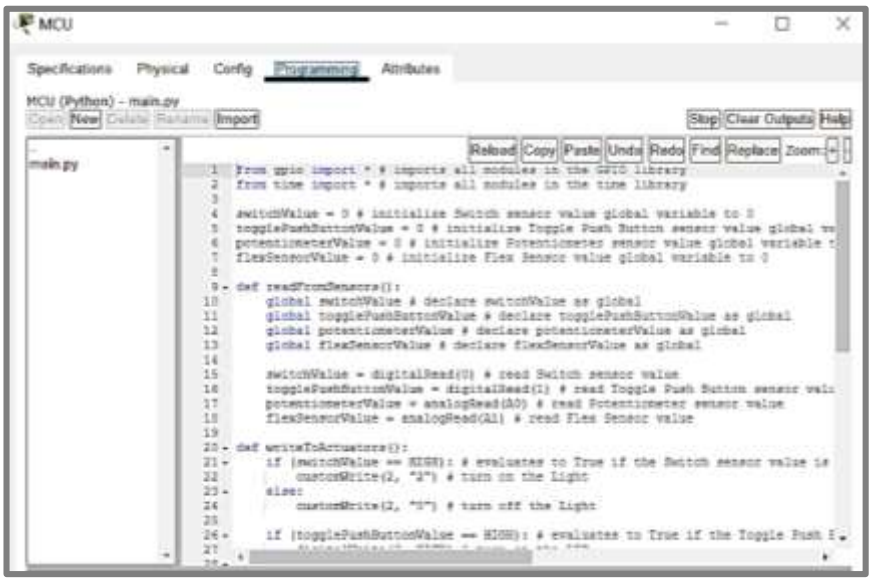


Рисунок 7.3 – Вкладка MCU Programming

3.3. Подивіться на код і спробуйте його зрозуміти. Нижче наведено короткий перелік завдань, які він виконує:

У рядках 1 і 2 усі класи в бібліотеках **time** і **gpio** імпортуються в програму. Це важливо для надання доступу до функцій часу та загального введення/виведення (GPIO).

Потім оголошуються та ініціалізуються чотири глобальні змінні в рядках 4, 5, 6 і 7. Ці змінні будуть використовуватися для зберігання значень датчиків.

Потім створюється функція під назвою **readFromSensors()** (рядки з 9 до 18). Спочатку функція готує змінні датчика (рядки з 10 до 13). Потім функція **readFromSensors()** викликає дві інші функції **digitalRead()** і **analogRead()**, щоб зафіксувати стан датчиків і зберегти його у відповідних змінних (рядки з 15 до 18). Зауважте, що **digitalRead()** і **analogRead()** приймають пін-код як параметр. Підключивши певні датчики до певних контактів, програма може фіксувати певний стан датчика.

Потім у рядках з 20 до 39 створюється інша функція: **writeToActuators()** використовується для зміни стану приводів на основі стану датчиків. У рядках з 21 до 24 програма перевіряє вміст змінної **switchValue**. Оскільки **switchValue**

зберігає стан контакту 0 (див. рядок 15), програма може вирішити, чи варто їй увімкнути світло; якщо значення, що зберігається в **switchValue**, дорівнює HIGH (напруга подана або перемикач увімкнено), то програма вмикає світло, записуючи значення 2 до актуатора 2. І навпаки, якщо **switchValue** дорівнює LOW (немає напруги або перемикач OFF), програма вимикає світло, записуючи 0 на актуатор 2.

Аналогічно рядки з 26 до 39 перевіряють і модифікують інші виконавчі механізми на основі їхніх відповідних контрольних датчиків.

Рядки з 41 до 54 визначають функцію **main()**. Як зазначено в її назві, функція **main()** автоматично виконується, коли MCU вперше ввімкнено. Рядки з 42 до 46 ініціалізують контакти; контакти 0 і 1 налаштовані як ВХІД (лінії 42 і 43), тоді як контакти 2, 3 і 4 встановлені як ВИХІД. Це важливо, оскільки контакти INPUT отримують напругу, тоді як контакти OUTPUT виділяють напругу, що генерується самим мікроконтролером.

Нескінченний цикл **while** створюється в рядках з 48 до 51. Оскільки умова в циклі просто означає **true**, MCU виконуватиме рядки 49, 50 і 51 постійно. Цей нескінченний цикл **while** змушує MCU:

1. Запустити функцію **readFromSensors()** у рядку 49.
2. Запустити функцію **writeToActuators()** у рядку 50.
3. Зачекати 1 секунду в рядку 51 (1000 мс = 1 секунда).
4. Перезапустити цикл із початку, повернувшись до рядка 49 і знову запустити функцію **readFromSensors()**.

Зауважте, що незважаючи на те що нескінченні цикли зазвичай небажані, вони корисні в цій програмі; нескінченний цикл тут гарантує, що **MCU** завжди перевіряє стан датчиків і перемикачів (запускаючи **readFromSensors()** щосекунди) і завжди вживаючи відповідних дій щодо приводів (запускаючи **writeToActuators())** на основі стану датчиків.

3.4. Наразі світлом керує вимикач, а світлодіодом – кнопка. Змініть код, щоби перемикач керував світлодіодом, а кнопка – світлом.

4. Міркування

Впровадження програмованого PT MCU в Packet Tracer дає можливість створити потужне середовище моделювання IoT. Використання Python, як мови програмування, також сприяє створенню надійної платформи.



ВИМОГИ ДО ОФОРМЛЕННЯ ЗВІТУ

1. Сформуйте файл для звіту. Звіт про виконання роботи має включати:

- Титульний аркуш, вказуючи номер і назву роботи, прізвище і групу студента.
- Покроковий опис основних етапів виконання роботи. Отримані результати підтверджуються скріншотами екрана.
- Відповіді на поставлені запитання до кожного завдання.
- Висновки щодо проведеної роботи.

2. За завданнями 3.4 частини 2 представити змінений код управління лампою та світлодіодом.



КОНТРОЛЬНІ ЗАПИТАННЯ

1. Який тип обчислювальної техніки розташований на межі ділової чи корпоративної мережі та дає можливість попередньо обробляти дані з датчиків?
2. Які переваги хмарних обчислень?
3. Яка мета туманного обчислення?
4. Який рівень еталонної моделі IoT перетворює дані в інформацію, придатну для зберігання та обробки вищого рівня?
5. Яке призначення мікроконтролера?
6. Як встановлюється зв’язок між датчиками та виконавчими елементами?

7. Як відбувається програмування MCU?

ЛАБОРАТОРНА РОБОТА № 8
ПІДКЛЮЧЕННЯ ТА ВІЗУАЛЬНЕ ПРОГРАМУВАННЯ МІКРОКОНТРОЛЕРА IOT

Мета роботи: провести симулювання роботи з мікроконтролерними пристроями та навчання з їх програмування.

ВКАЗІВКИ ДО ВИКОНАННЯ РОБОТИ

1. Підключення мікроконтролера IoT.

1.1. Зберіть на робочій області Packet Tracer схему, як показано на рис. 8.1. Мікроконтролер **SBC** знаходиться в групі **Components / Boards / SBC-PT**. Кавоварку **Appliance** та настільну лампу **Light** можна знайти в розділі **End Devices / Home.** За допомогою спеціального кабелю **IoT Custom Cable** підключіть пристрої до відповідних портів плати **SBC-PT** (D0, D1, D2). **IoT Custom Cable** можна знайти в розділі **Connections**. Проведіть правильне під'єднання контактів.



Рисунок 8.1 – Збірка схеми на робочій області Packet Tracer

1.2. Програмування SBC – мікроконтролера

Зайдіть в **SBC0** на вкладку **Programming**. Натисніть на лівій частині панелі **Blink Python**, а потім **New** та введіть назву нового проекту. Оберіть різновид програмування **Empty Visual** (рис. 8.2). Натисніть кнопку **Create**.

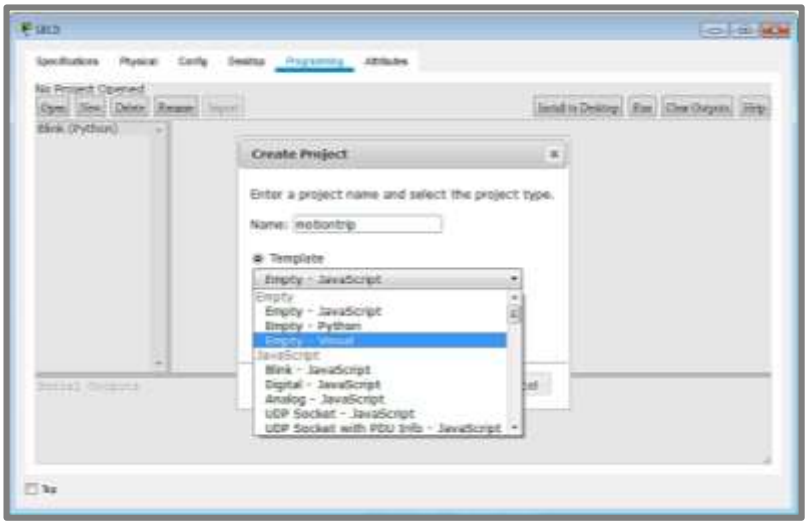


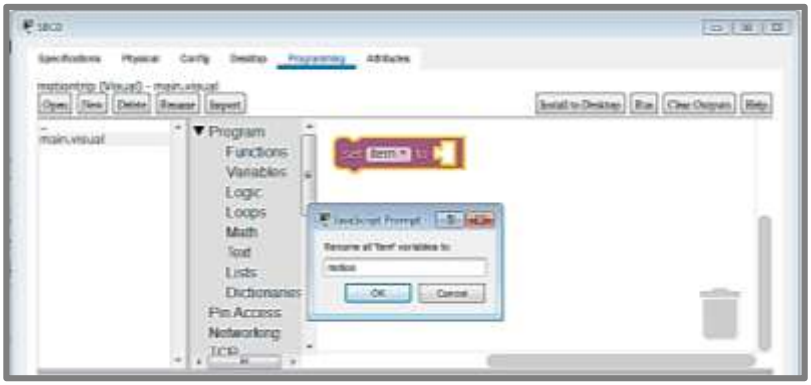
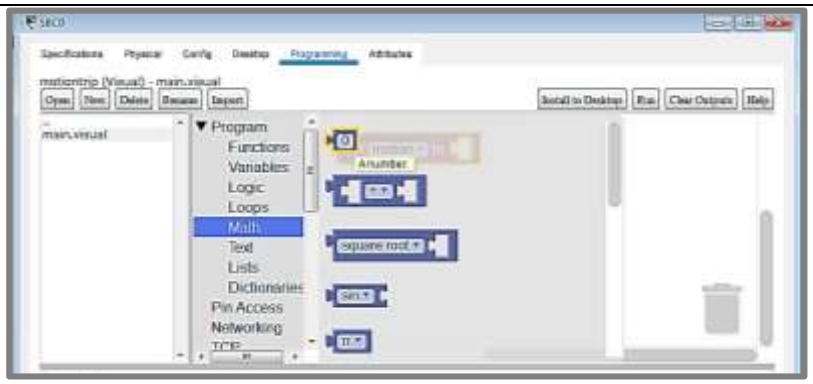
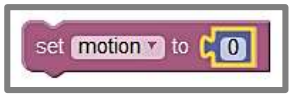
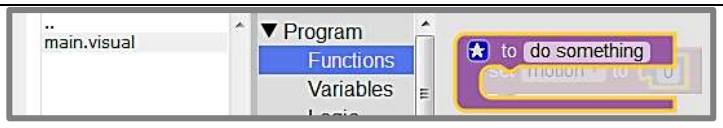
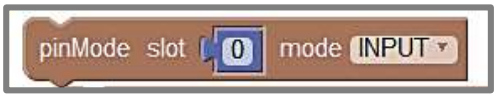
Рисунок 8.2 – Створення проекту

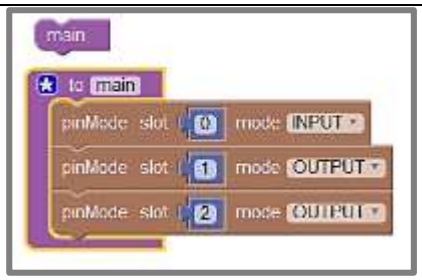
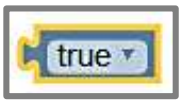
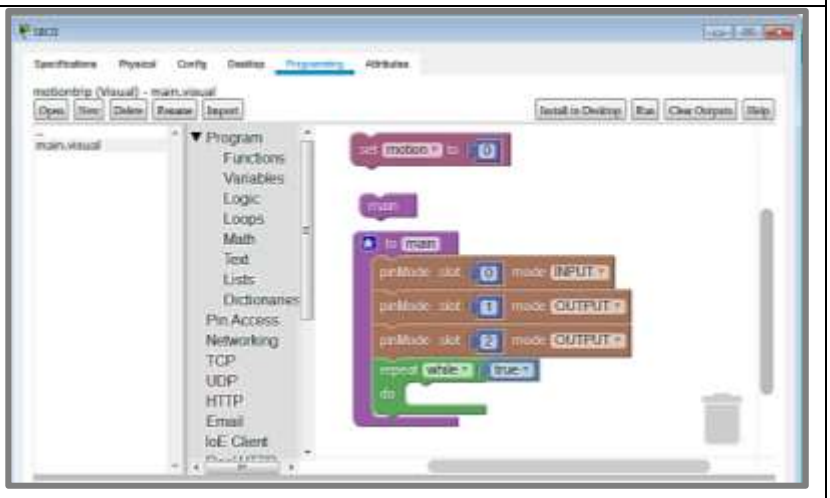
Натисніть 2 рази на **main.visual**, потім на **Program** та ознайомтесь з усіма елементами візуального програмування (рис. 8.3).



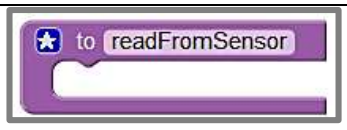
Рисунок 8.3 – Елементи візуального програмування мікроконтролера

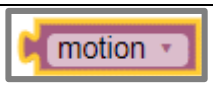
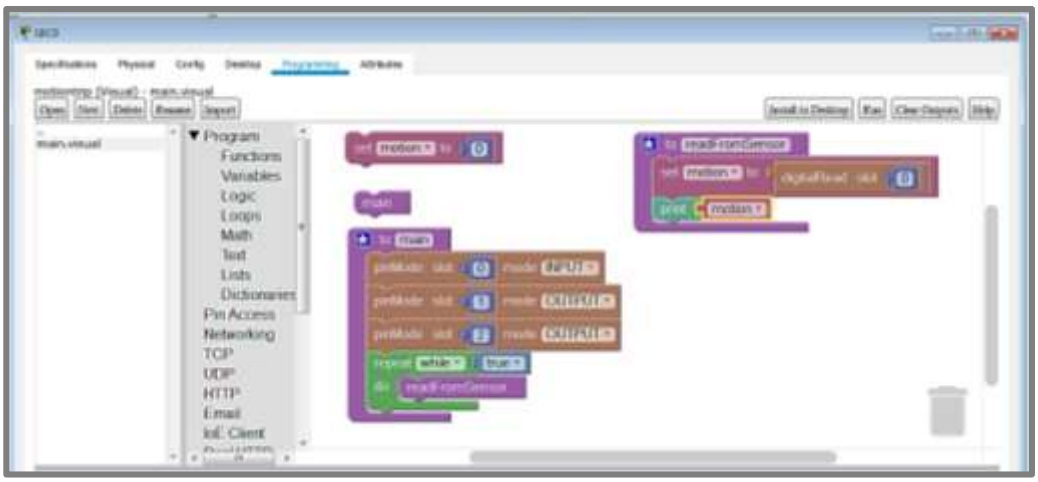
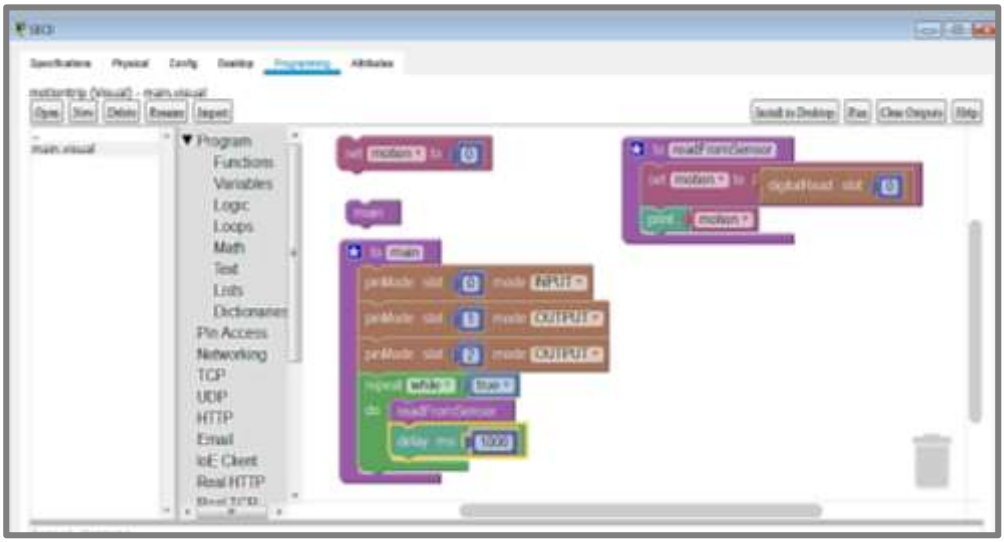
1.3. Проведемо програмування SBC – мікроконтролера за таким алгоритмом:

1	Оберіть **Variables** (Змінні) та за допомогою спадаючого тексту перейменуйте змінну **Rename variables** на **motion**.	
2	Оберіть **Math** та **0** і вставте його в порожню комірку.	
3	Утворюється рядок коду	
4	З **Functions** вибираємо і встановлюємо початок основної функції **Main**	
5	Встановлюємо функцію	
6	Перейменовуємо її на **main**	
	Розподіляємо контакти плати	
7	З **Pin Access** дістаємо функцію **pinMode**. Натискаємо на ній	

	правою кнопкою миші та дублюємо **Duplicate** цей елемент (3 шт)	
8	Міняємо слоти та входи/виходи і вставляємо ці піни в тіло функції	
9	З підрозділу **Loops** вибираємо функцію циклу	
10	З підрозділу **Logic** вибираємо функцію	
11	Збираємо «пазли», як відображено на схемі	

1.4. Формуємо підфункцію для циклу. Для цього:

1	З розділу **Functions** обираємо та перейменовуємо функцію	
2	Із цього ж розділу перетягуємо звертання до неї, яке сформувалося після перейменування:	

3	З розділу **Pin Access** дістаємо функцію	
4	З розділу **Text** дістаємо функцію **print**	
5	З розділу **Variables** функцію **motion**	
6	Формуємо підфункцію, як показано на рисунку 	
7	З розділу **Pin Access** дістаємо функцію затримки	
8	Одержимо таку програму 	

1.5. Розташуйте вікна, як показано на рисунку 8.4.

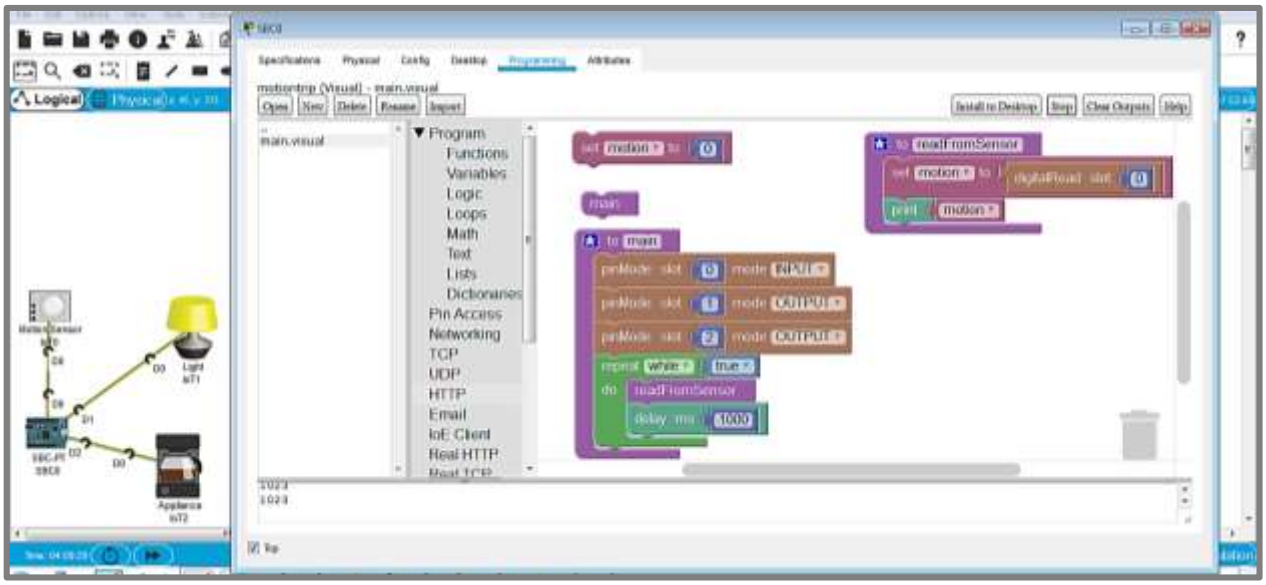
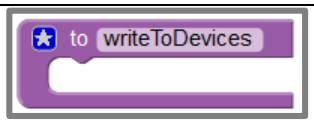


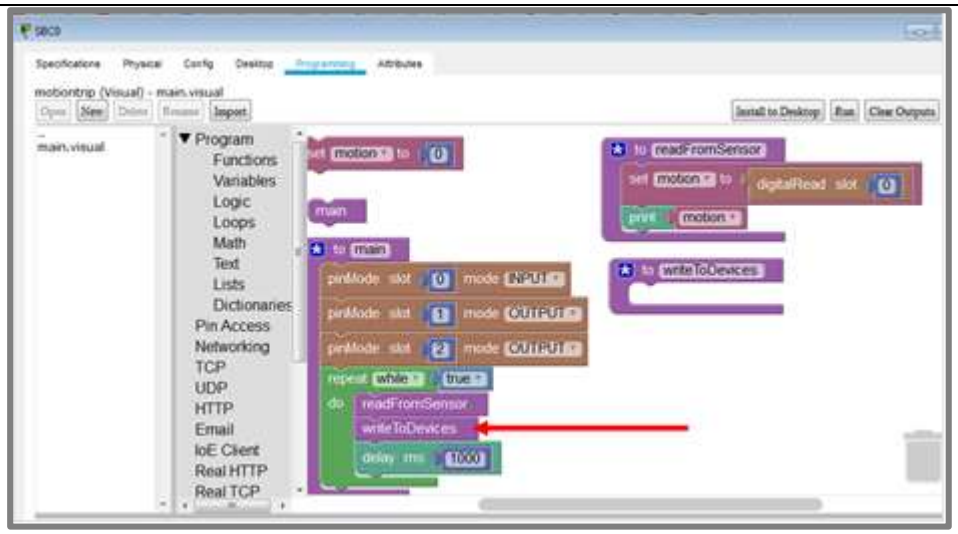
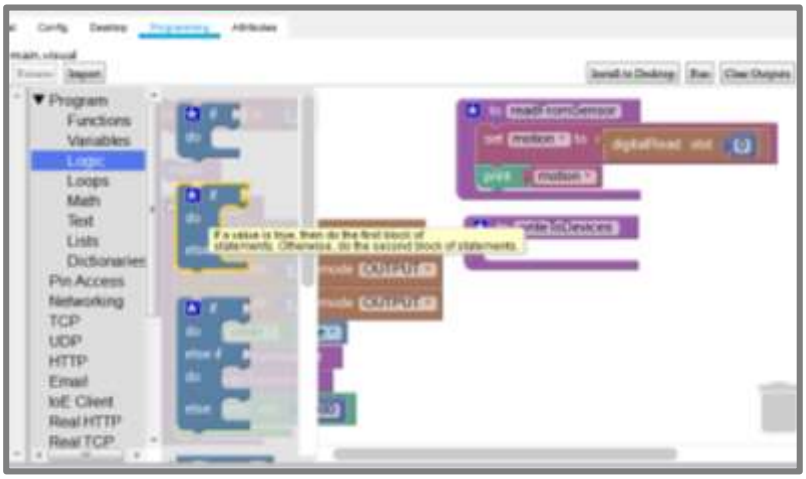
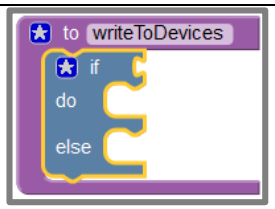
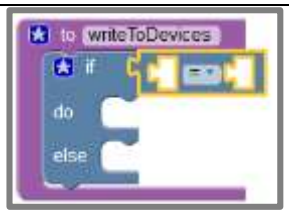
Рисунок 8.4 – Розташування вікон

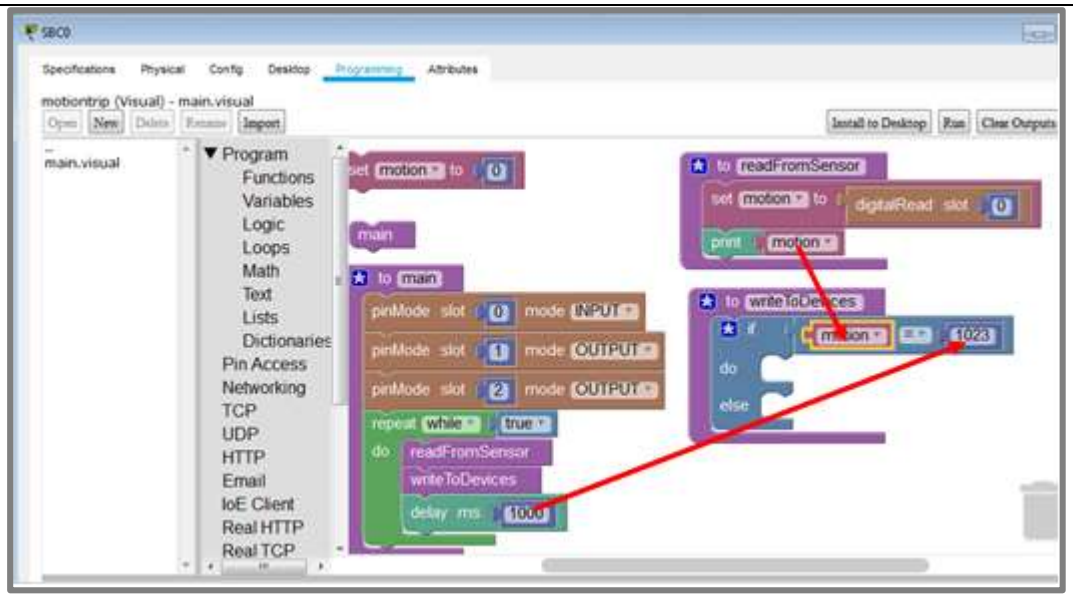
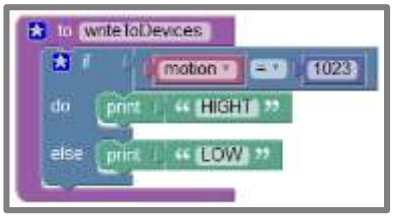
Запускаємо на виконання кнопкою **Run**. У низу вікна буде відображатись **0**, а коли натиснути й утримувати **Alt** та провести мишею біля детектора руху – внизу з’явиться код, що свідчить про роботу датчика.

1.6. Пишемо підпрограму для управління пристроями IoT.

Алгоритм дій:

1	Формуємо функцію (підпрограму) запису	
2	Після того, як її перейменували, в підрозділі **Program/Function** автоматично з’являється функція звернення до підпрограми	
3	Вставляємо її до основної програми	

	
4	Далі необхідно забезпечити виконання умови: коли зчитали сигнал із датчика (**D0**), то – виконати якусь дію (записати активний рівень в **D1** та **D2**). Для цього скористаємось логічною функцією **if-do-else** 
5	Вставляємо її в підпрограму запису 
6	Формуємо логічну умову **if** – для чого з підрозділу **Logic** обираємо функцію умови та вставляємо її в тіло функції  
7	Формуємо правило умови. Дублюємо елементи та вставляємо їх в умову. Міняємо в умові код спрацювання датчика

<table>
<tr><td></td><td colspan="2">
</td></tr>
<tr><td>8</td><td>Вставляємо елементи print та «лапки» з підрозділу Text та пишемо високий HIGHT і низький LOW рівні </td><td></td></tr>
</table>

1.7. Перевіряємо роботу підпрограми. Натискаємо **Run** та перевіряємо роботу детектора, як у попередньому випадку. (утримуючи **Alt** проводити мишею перед датчиком). При виявленні руху передається код 1023 та напис **HIGHT** (рис. 8.5).

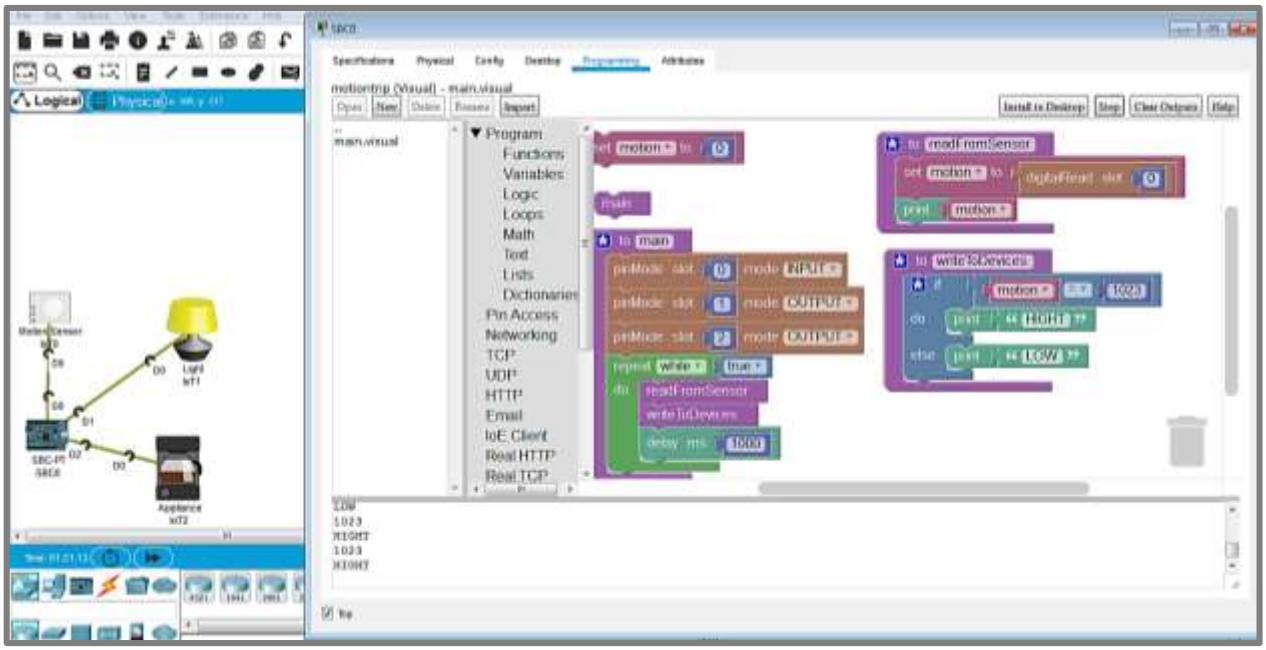
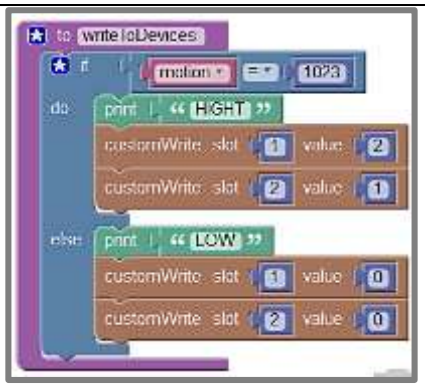


Рисунок 8.5 – Реалізація підпрограми

1.8. Напишемо функцію управління пристроєм:

1	З розділу **Pin Access** обираємо функцію	
2	Формуємо логіку роботи	

Програма готова. Запускаємо її на виконання (рис. 8.6).

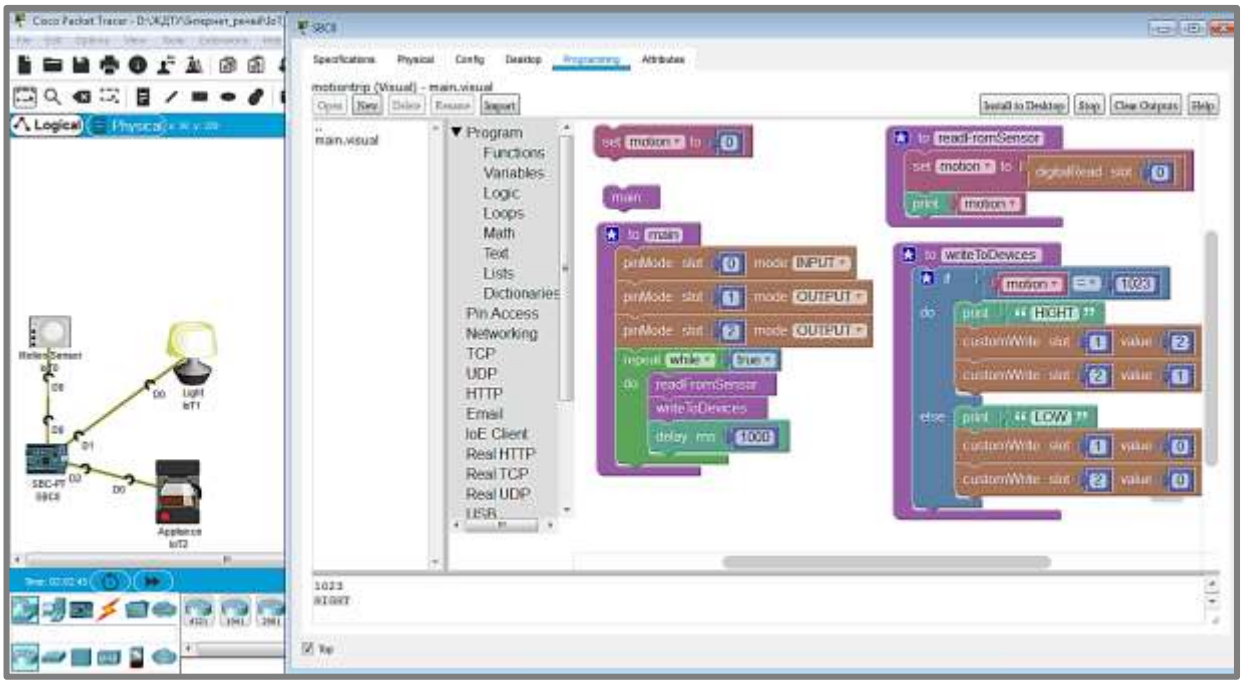


Рисунок 8.6 – Реалізація програми

Тепер під час спрацювання датчика руху вмикається лампа та кавоварка. Вони працюють деякий час (час затримки delay = 1000) та вимикаються і схема знову готова до роботи.

2. Реалізація IoT-проекту з програмуванням

2.1. Перетягніть на робоче поле необхідні елементи згідно з схемою (рис. 8.7). Підключіть всі компоненти через спеціальні кабелі IoT до SBC пристрою.

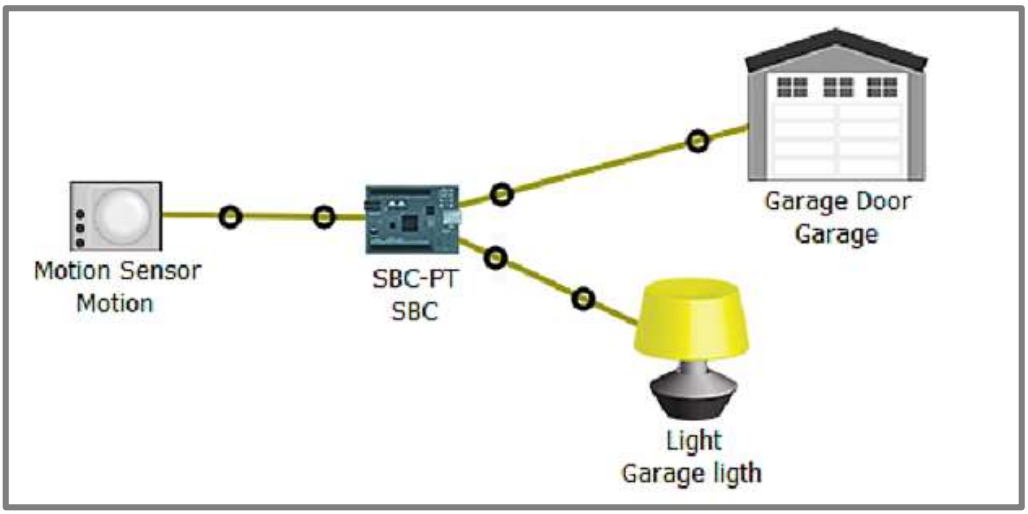


Рисунок 8.7 – Пристрої IoT для реалізації проекту

2.3. Змоделюйте відкриття гаражних дверей разом із включенням світла, коли датчик руху виявляє певний рух. У цьому випадку логіка симуляції не буде реалізована сервером IoT, а індивідуальним програмним забезпеченням, що працює на платі SBC.

Логіка програмного забезпечення дуже проста, сенсор безпосередньо підключений до входу SBC. Коли об'єкт буде виявлено, то датчик подає величину вхідного штифта SBC. Контролер потім порівнює його із заздалегідь встановленим пороговим значенням, і якщо логічна пропозиція є зустрічною, то буде відправлено команду до вихідних штифтів. Команда призводить до відкривання гаражних дверей та ввімкнення світла.

Зображення програми, що працює на SBC, подано на рис. 8.8. Реалізуйте цю програму та перевірте роботу схеми.

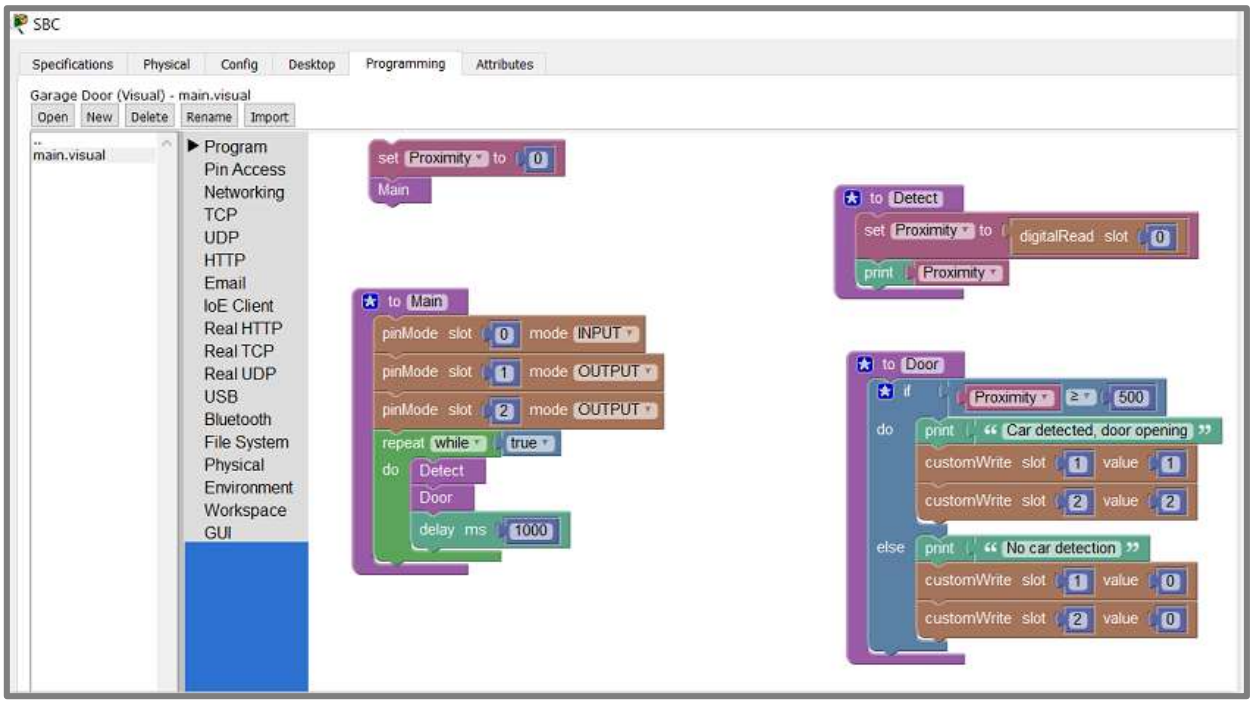


Рисунок 8.8 – Реалізація проекту відкриття гаражних дверей

ВИМОГИ ДО ОФОРМЛЕННЯ ЗВІТУ

1. Сформуйте файл для звіту. Звіт про виконання роботи має включати:

- Титульний аркуш, вказуючи номер і назву роботи, прізвище і групу студента.
- Покроковий опис основних етапів виконання роботи. Отримані результати підтверджуються скріншотами екрана.
- За завданням 2 пояснення прийнятих рішень, логіки з'єднання пристроїв та правил керування пристроїв при розробленні проекту.
- Висновки щодо проведеної роботи.

2. За завданнями 1: створений файл моделі з назвою LR-8-1_XXXXX.pkt, де XXXXX – позначення прізвища студента.

3. За завданням 2: створений файл моделі реалізації проекту з назвою LR-8-2_XXXXX.pkt, де XXXXX – позначення прізвища студента.



КОНТРОЛЬНІ ЗАПИТАННЯ

1. Що використовується для забезпечення доступу датчиків IoT до мережі?
2. Яка технологія використовується як інструмент візуального програмування для створення програми через з'єднання кольорових блоків?
3. Які елементи використовуються для представлення різних програмних структур у Blockly?
4. Як відбувається програмування SBC?
5. Назвіть основні функції мікроконтролера та опишіть процес їх формування.
6. У чому особливість візуального програмування SBC?

ЛАБОРАТОРНА РОБОТА № 9
НАЛАШТУВАННЯ ДОМАШНЬОЇ МЕРЕЖІ З ВІДДАЛЕНИМ ДОСТУПОМ ДО ПРИСТРОЇВ IOT

Мета роботи: виконати з'єднання комп'ютерних та IoT-пристроїв із домашньою мережею, які налаштовані на роботу з перемикачами, підключеними до одноплатного контролера (SBC). Пристрої IoT мають бути підключені до домашнього шлюзу та зареєстровані на реєстраційному сервері www.register.pka.

ВКАЗІВКИ ДО ВИКОНАННЯ РОБОТИ

Після того, як пристрої IoT підключені до домашньої мережі та зареєстровані на реєстраційному сервері, ви зможете керувати пристроями IoT вдома або далеко від дому через сервер реєстрації.

1. Створення домашньої мережі IoT

1.1. Пошук та підключення пристроїв IoT

1) Завантажте файл **Packet Tracer – Install and Configure IoT Devices.pka**. Виберіть та перетягніть на робоче поле відповідні елементи IoT, як показано на рисунку. Поміняйте назви елементів відповідно до рис. 9.1.

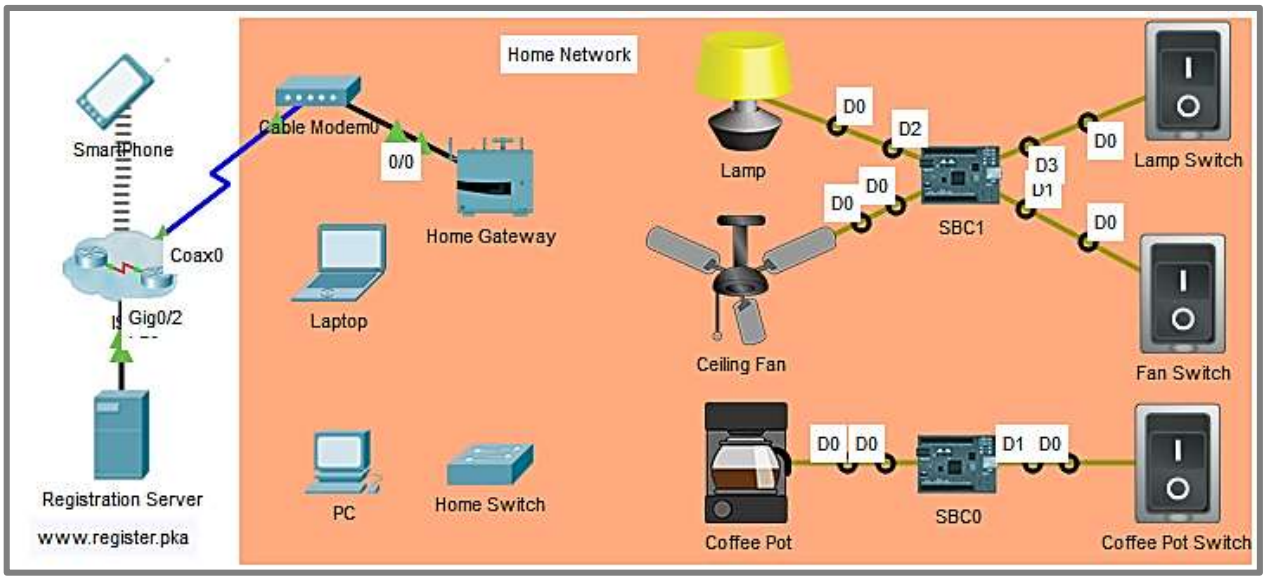


Рисунок 9.1 – Набір елементів IoT для домашньої мережі

2) Підключіть за допомогою **IoT Custom Cable** кавоварку **Coffee Pot** до мікроконтролера **SBC0** та **Coffe Pot Switch**. Дотримуйтесь відповідності контактів (**D0**, **D1**) під час підключення.
3) Підключіть дротами лампу **Lamp** і стельовий вентилятор **Ceiling Fan** та їх вимикачі до мікроконтролера **SBC1**. Дотримуйтесь відповідності контактів під час підключення.

1.2. Створення прямого управління через мікроконтролер для IoT кавоварки:

1) Для більш пізніх версій Packet Tracer мікроконтролери **SBC** автоматично підключаються до бездротової мережі. Для цього завдання ця властивість не потрібна. Тому в разі необхідності вимкніть його бездротову мережу. Для цього натисніть на **SBC**, перейдіть на вкладку **Config** та витріть в **SSID** напис (рис. 9.2).



Рисунок 9.2 – Вимкнення бездротової мережі

2) Визначаємо логіку роботи вмикання кавоварки через вимикач. Логіка роботи: мікроконтролер **SBC0** у циклі має зчитувати інформацію зі свого входу – контакту (**pin D1**), до якого підключений вимикач та, у разі появи сигналу включено, подати сигнал на свій вихід (**pin D0**), який включить кавоварку.
3) Програму пишемо на Python. Для цього створюємо новий проект (рис. 9.3).



Рисунок 9.3 – Створення проекту

Вводимо програму, як на рис. 9.4:



Рисунок 9.4 – Код програми

✓ Необхідно розібратися, що робить кожен рядок програми та вміти відповісти на питання по програмі.

4) Після введення програми запускаємо її на виконання, натиснувши **Run** у правому верхньому кутку. Якщо помилок немає, то внизу вікна буде напис про початок і кінець роботи (рис. 9.5).

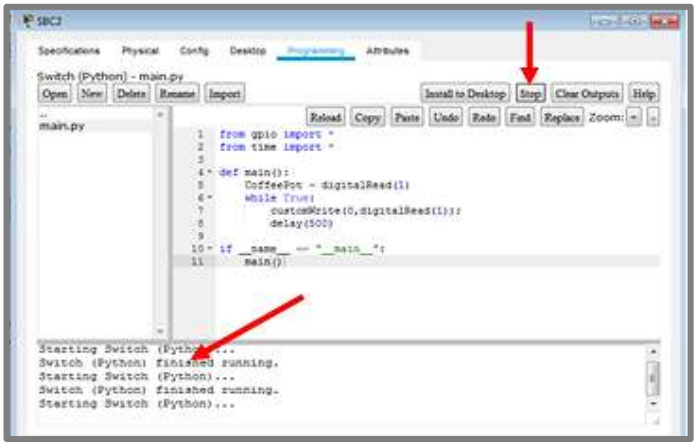


Рисунок 9.5 – Реалізація програми

5) Залишаємо програму на виконанні та перевіряємо її роботу. Для цього, тримаючи **Alt+ліва кнопка «миші»,** проводимо над вимикачем. Він має ввімкнутися сам та ввімкнути кавоварку. Вимикаємо кавоварку аналогічним чином, провівши над вимикачем.

6) Залишивши програму в робочому стані (не натискаємо **Stop**) закриваємо вікно **SBC0**.

1.3. Створення прямого управління через мікроконтролер для IoT вентилятора та лампи. Виконуємо всі дії аналогічно пункту 1.2:

1) Самостійно розпишіть логіку роботи мікроконтролера **SBC1**.

2) Напишіть програму роботи на Python (рис. 9.6).

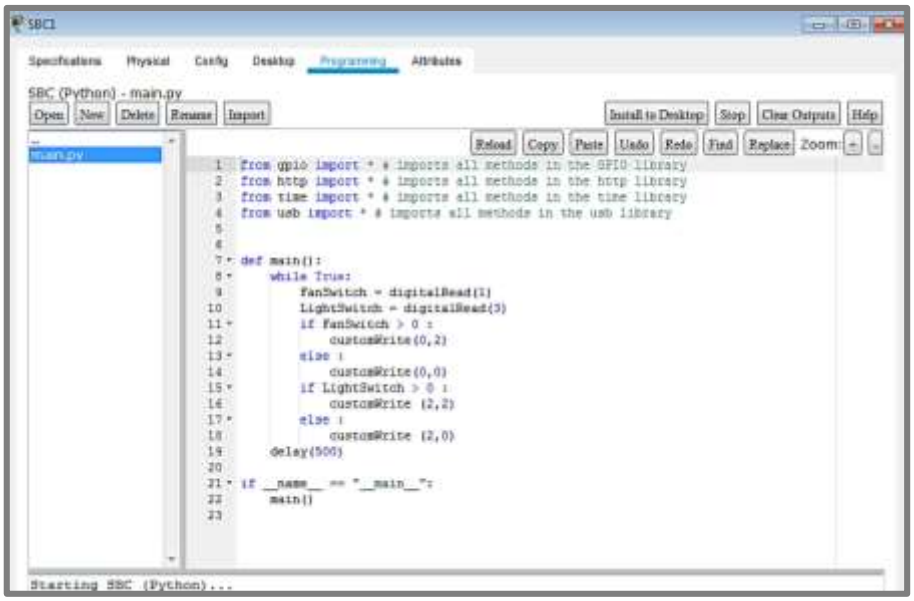


Рисунок 9.6 – Програма управління вентилятора та лампи

3) Перевірте правильність роботи. Необхідно розібратися, що робить кожен рядок програми та вміти відповісти на питання по програмі.
4) Залишивши програму в робочому стані (не натискаємо **Stop**) закриваємо вікно **SBC1**.

2. Налаштування домашньої мережі

2.1. Налаштуйте дротову мережу:

1) Підключіть будь-який доступний порт **FastEthernet** з **Home Switch** на будь-який доступний порт **Ethernet** на **Home Gateway**, використовуючи мідний прямоточний кабель **Copper straight-through cable**.
2) Підключіть порт **FastEthernet0** на ПК до будь-якого доступного порту **FastEthernet** на домашньому комутаторі, використовуючи **Copper straight-through cable**.
3) Натисніть **PC**. Натисніть кнопку **Desktop**. Натисніть **IPConfiguration**. Виберіть **DHCP** для конфігурації IP.

2.2. Налаштування бездротової мережі:

1) Натисніть **Home Gateway**. Перейдіть на вкладку **Config**. На панелі ліворуч натисніть **Internet**.

2) Натисніть кнопку **DHCP** в розділі **Internet Settings**. **Home Gateway** отримає установки від інтернет-провайдера.
3) У розділі **Home Gateway** натисніть **Wireless**.
4) Змінити **SSID** на **MyHomeGateway**. Змініть **Authentication** на **WPA2-PSK**. Введіть як пароль **Phrase PSK** – **CiscoIoT**.
5) Натисніть кнопку **Desktop**. Натисніть **PC Wireless**.
6) Натисніть вкладку **Connect**. Виберіть мережу **MyHomeGateway**. Якщо ім'я бездротової мережі не відображається, натисніть кнопку **Refresh** (Оновити).
7) Натисніть **Connect**. Введіть **CiscoIoT** як попередньо спільний ключ. Натисніть **Connect**.

2.3. Підключіть пристрої IoT до мережі.

IoT пристрої можуть бути підключені за допомогою проводів або бездротовим способом. Кавоварка **Coffee Pot** буде підключено до мережі за допомогою кабелів **Ethernet**. Лампа **Lamp** та вентилятор **Ceiling Fan** для потоку будуть підключені без проводів:

1) Підключіть кавоварку **Coffee Pot** до будь-якого доступного порту **FastEthernet** за допомогою мідного прямоточного кабелю **Copper straight-through cable**.
2) Натисніть **Coffee Pot**. Натисніть **Config**. Натисніть **FastEthernet0**. Виберіть **DHCP** для конфігурації IP.
3) Натисніть лампу **Lamp**. Натисніть **Config**. Натисніть **Wireless0**. Введіть **MyHomeGateway** як SSID. Натисніть **WPA2-PSK**. Введіть **CiscoIoT** як Phrase Pass PSK. Виберіть **DHCP** для конфігурації IP.
4) Повторіть крок «3» для стельового вентилятора **Ceiling Fan**.

3. Взаємодія з пристроями IoT

Пристрої IoT можуть бути налаштовані на керування безпосередньо, за допомогою вимикачів або через вебінтерфейс. Підключимо пристрої IoT до

реєстраційного сервера, щоби була змога керувати пристроями IoT через вебінтерфейс.

3.1. Доступ до пристроїв IoT локально.

Пристроями IoT можна керувати безпосередньо, одночасно натискаючи **Alt** і натискаючи пристрій:

1) Кілька разів натисніть **Alt + Lamp**.

Скільки налаштувань має Лампа, і які налаштування?

Відповідь:_____

2) Натисніть **Alt + Lamp Switch** кілька разів.

Скільки налаштувань має перемикач лампи та які налаштування?

Відповідь:_____

3) Повторіть із вентилятором і кавоваркою та їх перемикачами.

3.2. Налаштування пристроїв IoT для віддаленого доступу:

Щоб керувати пристроями IoT дистанційно через вебінтерфейс, пристрої мають бути зареєстровані на сервері реєстрації.

1) Натисніть лампу **Lamp**. Натисніть **Config**.
2) Під заголовком **IoT Server** натисніть кнопку **Remote Server**. Надайте таку інформацію для підключення до сервера реєстрації.

   Адреса сервера: **www.register.pka**

   Ім’я користувача: **admin**

   Пароль: **admin**
3) Натисніть **Connect** (Підключити), щоби підключитися до сервера.
4) Повторіть кроки «1–3» для стельового вентилятора та кавового горщика.

3.3. Надайте доступ до пристроїв IoT:

1) Натисніть ноутбук **Laptop**. Натисніть вкладку **Desktop**.

2) Натисніть веббраузер **Web Browser**. Введіть **www.register.pka**. Введіть **admin** як ім'я користувача та пароль. Натисніть **Sign In** (Увійти).
3) Клацніть на елементах управління, щоби переглянути стан пристрою та контролери.
4) Увімкніть лампу, натиснувши **Dim**.

❓ Що сталося з лампою в топології?

Відповідь:_____

❓ Що треба натискати, щоб включити із ноутбука кавовий горщик?

Відповідь:_____

4. Віддалений доступ до пристроїв IoT

Ви також можете керувати пристроями, коли ви перебуваєте далеко від дому, звернувшись до сервера реєстрації.

1) Натисніть та розгорніть кластер ISP (рис. 9.7).

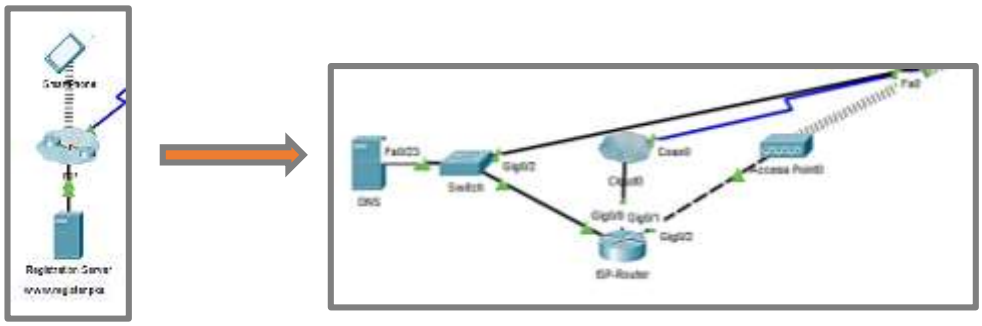


Рисунок 9.7 – Розгортання кластера ISP

2) Ознайомтесь та розберіться з налаштуваннями всіх елементів кластера ISP.
3) Натисніть **SmartPhone**. Налаштуйте його для віддаленого доступу до сервера реєстрації (рис. 9.8).

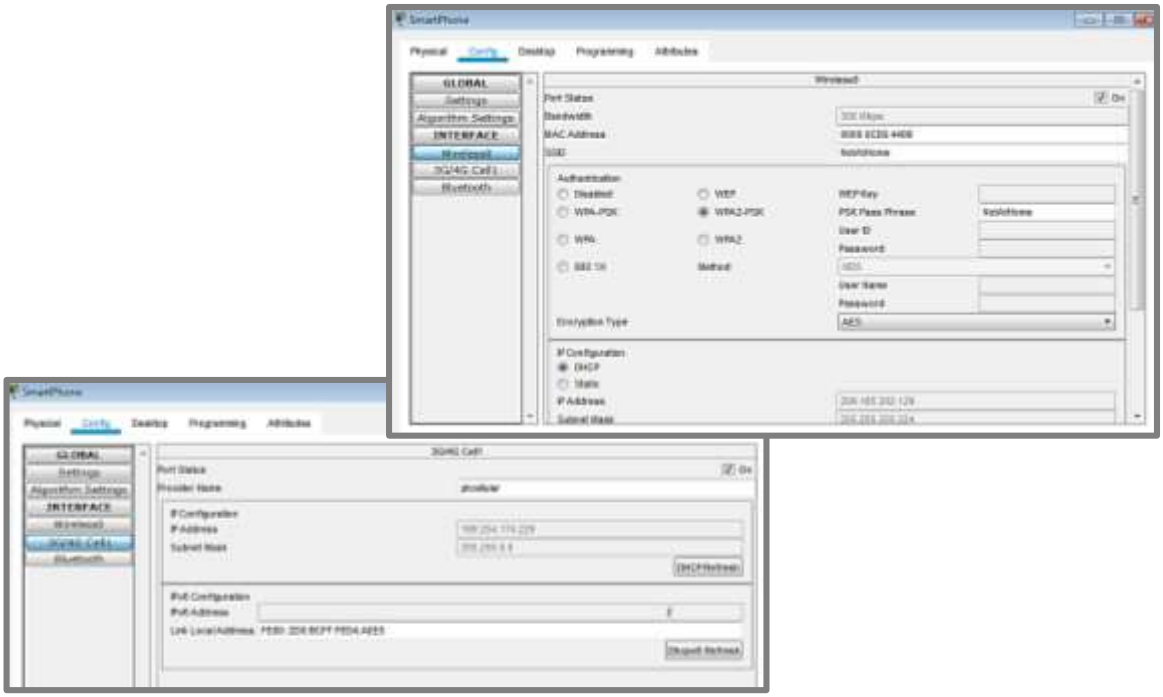


Рисунок 9.8 – Налаштування SmartPhone

4) Натисніть кнопку **Desktop**. Натисніть **Web Browser**. Введіть **www.register.pka**. Введіть **admin** як ім’я користувача та пароль. Натисніть **Sign In**.

5) Перевірте управління пристроями IoT зі смартфона.

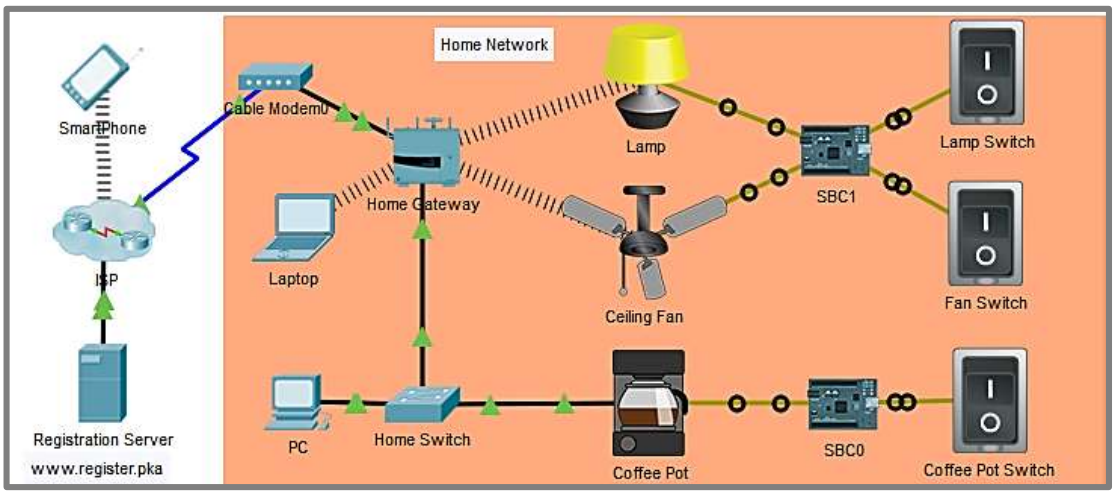


Рисунок 9.9 – Загальний вигляд підключеної мережі



ВИМОГИ ДО ОФОРМЛЕННЯ ЗВІТУ

1. Сформуйте файл для звіту. Звіт про виконання роботи має включати:

- Титульний аркуш, вказуючи номер і назву роботи, прізвище і групу студента.
- Покроковий опис основних етапів виконання роботи. Отримані результати підтверджуються скріншотами екрана.
- Відповіді на поставлені запитання.
- Висновки щодо проведеної роботи.

2. Створений файл моделі з назвою LR-9_XXXXX.pkt, де XXXXX – позначення прізвища студента.



КОНТРОЛЬНІ ЗАПИТАННЯ

1. Чи застосовується протокол DHCP в сучасних комп’ютерних мережах?
2. Що використовується для ідентифікації бездротової мережі?
3. Яка роль маршрутизації в мережах передачі даних?
4. Чому здебільшого пристрої IoT не підключені безпосередньо до точки доступу Wi-Fi або маршрутизатора?
5. Як можна забезпечити пряме управління IoT-пристроїв через мікроконтролер?
6. Якій мові програмування використовуються для написання коду управління?
7. Опишіть ключові моменти програми управління, що написана на Python.

ЛАБОРАТОРНА РОБОТА № 10
НАЛАШТУВАННЯ БЕЗПЕКИ БЕЗДРОТОВОГО ЗВ'ЯЗКУ

Мета роботи: Створити домашню мережу за допомогою безпечного бездротового маршрутизатора, використовуючи зміну пароля, заміну стандартного SSID, захист WPA2 та фільтрацію MAC для підвищення безпеки.

ВКАЗІВКИ ДО ВИКОНАННЯ РОБОТИ

1. Налаштування ноутбука.

1.1. Завантажте файл **Configure Wireless Security.pkt** (рис. 10.1).

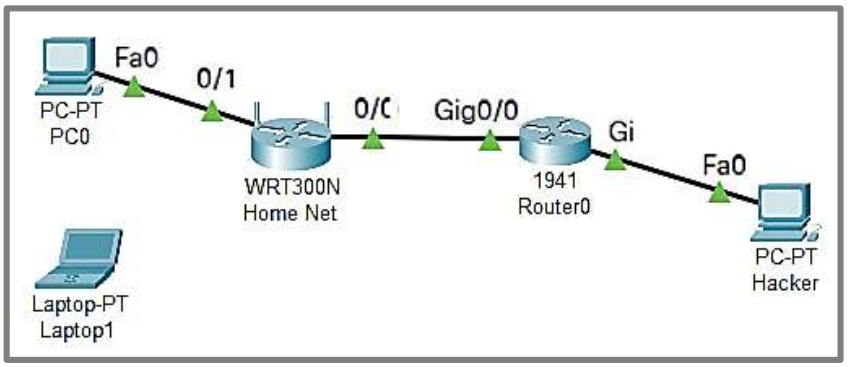


Рисунок 10.1 – Схема мережі

1.2. Натисніть кнопку **Power** на **Laptop1**, щоб вимкнути його.

1.3. Перетягніть порт **Ethernet** до списку **Modules**, щоб видалити його.

1.4. Перетягніть модуль **WPC300N** у порожній слот на **Laptop1** й натисніть кнопку **Power**, щоб завантажити **Laptop1** (рис. 10.2).



Рисунок 10.2 – Налаштування Laptop1

2. Зміна пароля за умовчанням

2.1. Натисніть бездротовий маршрутизатор **Wireless Router** і виберіть **GUI** для налаштування.

2.2. Натисніть **Administration / Management.**

2.3. Змініть пароль маршрутизатора на більш надійний. Змініть пароль на **aC0mpAny3** (рис. 10.3). Зауважте, що новий пароль складається з 8 символів у верхньому та нижньому регістрах, а деякі голосні замінено на цифри. Виберіть **Save Settings** внизу екрана.

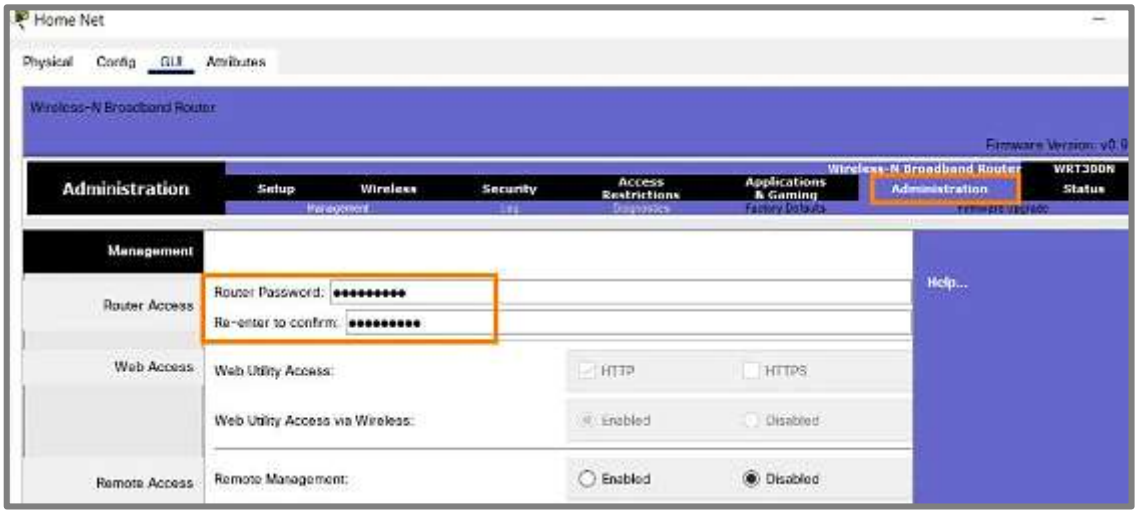


Рисунок 10.3 – Заміна паролю

3. Зміна назви SSID за замовчуванням і вимкнення функції трансляції

3.1. Натисніть **Wireless** і змініть ім'я SSID на **aCompany**.

3.2. Виберіть **SSID Broadcast** і натисніть **Disabled**. Натисніть **Save Settings** внизу цього екрана (рис. 10.4).

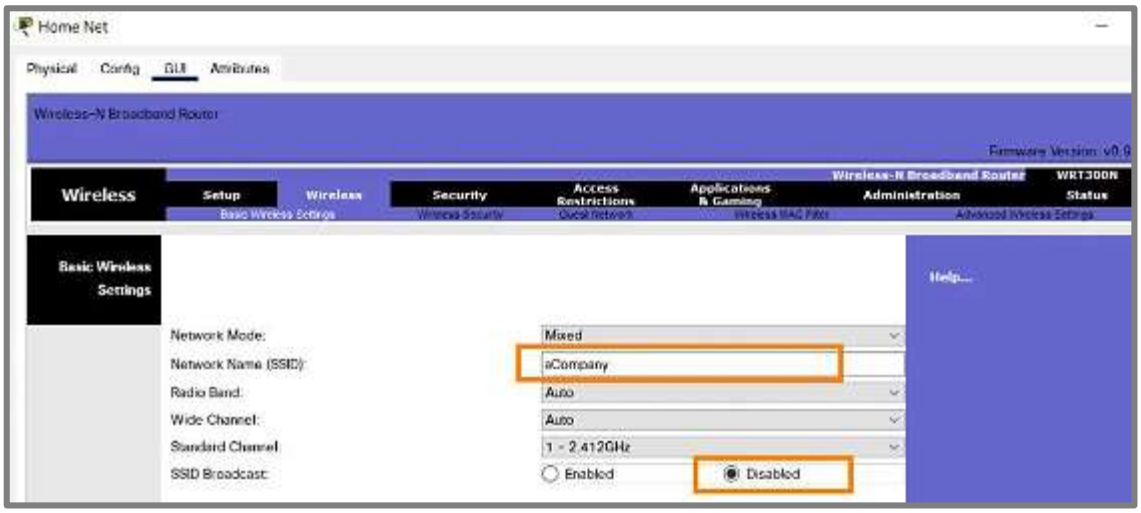


Рисунок 10.4 – Зміна назви SSID за замовчуванням

Перевірте топологію. Laptop0 втратив з'єднання з бездротовим маршрутизатором? Якщо так, то чому?

Відповідь:_____

4. Налаштування захисту WPA2 на бездротовому маршрутизаторі

4.1. Поверніться до вкладки **GUI** бездротового маршрутизатора. Натисніть **Wireless / Wireless Security**. Змініть режим безпеки Security Mode на **WPA2 Personal** (рис. 10.5). **AES** наразі є найнадійнішим доступним протоколом шифрування. Залиште його вибраним.

4.2. Налаштуйте парольну фразу як **CompWiFi** (рис. 10.5). Покрутіть донизу вікна та натисніть **Save Settings**.

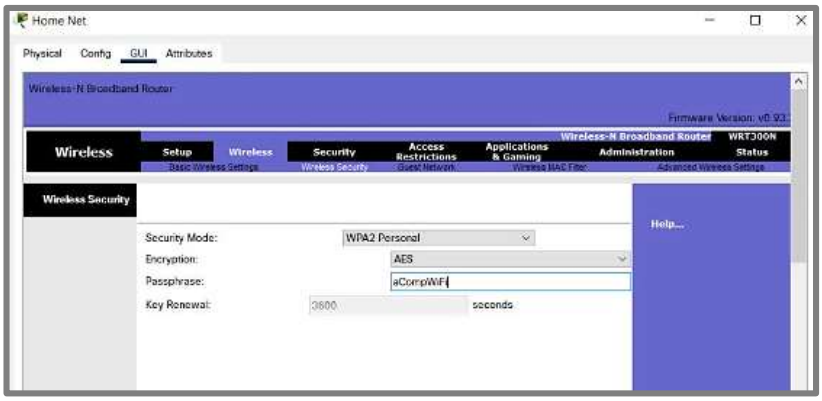


Рисунок 10.5 – Налаштування захисту WPA2

5. Налаштування Laptop0 як бездротовий клієнт

5.1. Налаштуйте **Laptop0** для підключення до бездротової мережі за допомогою параметрів безпеки, налаштованих на бездротовому маршрутизаторі.

1) Виберіть **Laptop0 / Desktop / PC Wireless**.
2) Виберіть **Profiles / New** та додайте будь-яку назву для профілю.
3) Виберіть **Advanced Setup** в нижньому правому куті.
4) Виберіть **Wireless Network Name** та введіть нове ім'я SSID: **aCompany** (рис. 10.6).



Рисунок 10.6 – Введення нового ім'я SSID

5) Прийміть налаштування мережі за замовчуванням, вибравши **Next.**
6) Змініть **Security** за допомогою спадного меню на **WPA2-Personal** і виберіть **Next** (рис. 10.7).



Рисунок 10.7 – Заміна Security

7) Введіть попередній спільний ключ: **aCompWiFi** і виберіть **Next** (рис. 10.8).
8) Збережіть профіль.
9) Виберіть **Connect to Network** (рис. 10.9).



Рисунок 10.8 – Введення спільного ключа



Рисунок 10.9 – З'єднання з бездротовою мережею

10) Якщо ноутбук Laptop не підключається успішно, поверніться до профілю та відредагуйте. Перевірте, як ви ввели ім'я SSID і попередній ключ.

5.2. Закрийте вікно бездротового зв'язку **PC Wireless** і натисніть командний рядок **Command Prompt**.

5.3. Введіть **ipconfig /all** і запишіть IP address та MAC addresses (рис. 10.10).

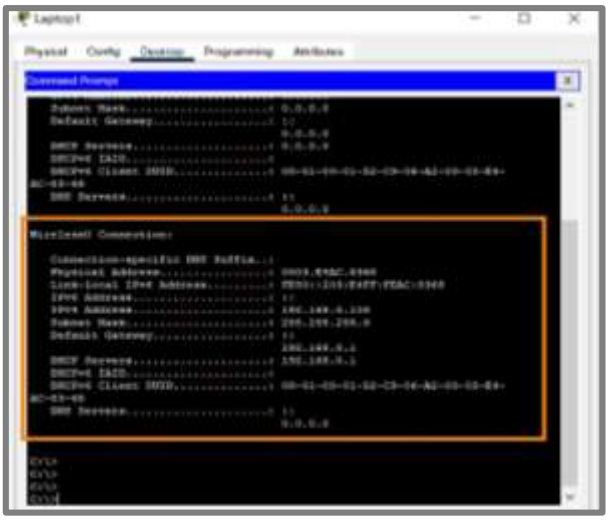


Рисунок 10.10 – Визначення IP address та MAC addresses

6. Налаштування WRS1 для підтримки фільтрації MAC

6.1. Поверніться на сторінку конфігурації бездротового маршрутизатора.

6.2. Перейдіть до **Wireless / Wireless MAC Filter**.

6.3. Виберіть **Enabled** та **Permit PCs listed below to access wireless network**.

6.4. Введіть MAC-адресу **для Laptop0** у полі **MAC 01** (рис. 10.11). Зверніть увагу, що MAC-адреса має бути у форматі **XX:XX:XX:XX:XX:XX.**



Рисунок 10.11 – Введення MAC-адреси

6.5. Покрутіть донизу вікна та натисніть **Save Settings**.

6.6. Повторно підключіть **Laptop0** до мережі **WRS1** .

7. Перевірка фільтрації MAC WRS1.

7.1. Додайте другий ноутбук до топології.

7.2. Натисніть кнопку **power** на новому ноутбуці, щоб вимкнути його та замінити карту **Ethernet** на бездротову.

7.3. Налаштуйте на новому ноутбуку параметри безпеки, необхідні для підключення до бездротового маршрутизатора.

Чому ви не можете зв'язатися з точкою доступу?

Відповідь:_____

8. Вимкнення віддаленого керування на бездротовому маршрутизаторі

8.1. Перевірте поточний статус віддаленого керування на бездротовому маршрутизаторі. Виберіть **Administration / Remote Access**. Якщо він вимкнений, увімкніть його (рис. 10.12).

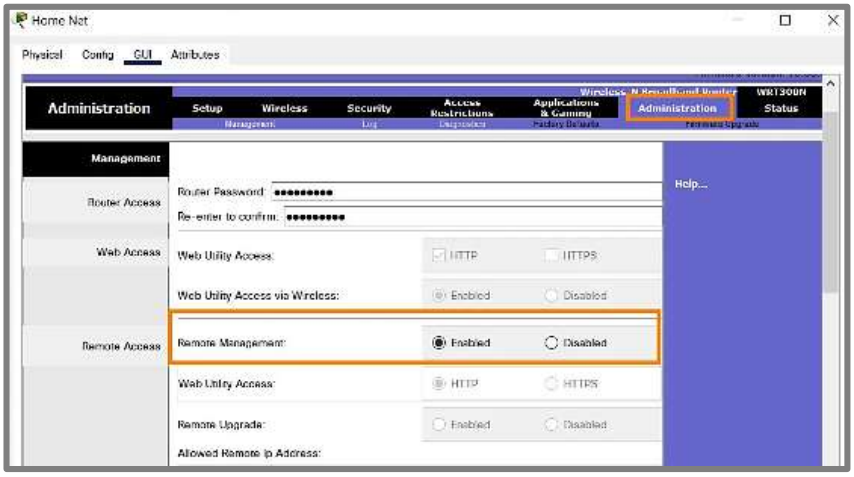


Рисунок 10.12 – Вимкнення віддаленого керування на бездротовому маршрутизаторі

8.2. Виберіть **Hacker PC** та виберіть **Desktop / Web Browser**. Введіть адресу **192.31.7.100** і натисніть **Go**. Ви маєте одержати запит на ідентифікатор користувача та пароль. Введіть дійсну інформацію, і ви зможете дістати доступ до графічного інтерфейсу бездротового маршрутизатора. Вийдіть із робочого столу: username: **admin** | password: **aC0mpAny3**.

8.3. Поверніться на сторінку конфігурації бездротового маршрутизатора.

8.4. Поверніться до **Administration / Management** та покрутіть униз до **Remote Management**. Виберіть **Disabled** та натисніть **Save Settings** внизу екрана.

8.5. Поверніться до **Hacker PC** та виберіть **Desktop / Web Browser**. Введіть адресу **192.31.7.100**. Ви більше не зможете підключитися через веббраузер.



ВИМОГИ ДО ОФОРМЛЕННЯ ЗВІТУ

1. Сформуйте файл для звіту. Звіт про виконання роботи має включати:

- Титульний аркуш, вказуючи номер і назву роботи, прізвище і групу студента.
- Покроковий опис основних етапів виконання роботи. Отримані результати підтверджуються скріншотами екрана.
- Відповіді на поставлені запитання.
- Висновки щодо проведеної роботи.

2. Створений файл із назвою LR-10_XXXXX.pkt, де XXXXX – позначення прізвища студента.



КОНТРОЛЬНІ ЗАПИТАННЯ

1. Яку проблему зберігання даних, пов'язану з великими даними, вирішує надання доступу до даних лише авторизованим користувачам?
2. Назвіть призначення IP-адреси та маски підмережі.
3. Що забезпечує стабільний захист бездротового каналу?
4. Як скинути маршрутизатор Wi-Fi?
5. Що таке найкраща практика безпеки бездротового маршрутизатора, яка обмежує доступ лише до певних внутрішніх хостів?
6. Які рекомендовані кроки для захисту бездротової мережі?
7. Які дії в Інтернеті створюють високий ризик безпеки?
8. Які паролі є найменш безпечними?

9. Які елементи необхідно поєднати під час створення надійного пароля?

ЛАБОРАТОРНА РОБОТА № 11
ЗАХИСТ ХМАРНИХ СЛУЖБ В ІОТ

Мета роботи: Розгортання базових заходів безпеки для систем Інтернету речей із хмарними службами.

ВКАЗІВКИ ДО ВИКОНАННЯ РОБОТИ

Сценарій: ABC Company розробляє системи IoT на своєму головному складі. Мета полягає в тому, щоб розгорнути деякі пристрої фізичної безпеки навколо складу, щоб, коли склад закрито, ці пристрої контролювали двері та вікна. При виявленні зловмисника вмикається світло і вебкамери починають запис.

Безпека є важливим аспектом на додаток до функції систем IoT із хмарними службами. У цій роботі виконується завдання налаштування:

- реєстрація чотирьох IoT-пристроїв на складі компанії ABC: детектор руху, спрямоване світло, вебкамеру та датчик проїзду. Необхідно додати умови на сервері реєстрації, щоби під час активації детектора руху або датчика відключення вмикалися спрямоване світло та вебкамера;
- налаштування складського маршрутизатора у такий спосіб, щоб він потребував надійної автентифікації для консолі та віддаленого доступу;
- налаштування ACL для обмеження мережевого трафіка між сервером реєстрації та складом компанії ABC;
- налаштування вебсервера в мережі постачальника хмарних послуг, щоб забезпечити безпеку передачі даних.

1. Реєстрування пристроїв IoT на сервері реєстрації.

1.2. Відкрийте файл **Packet Tracer - Securing Cloud Services in the IoT.pka.**

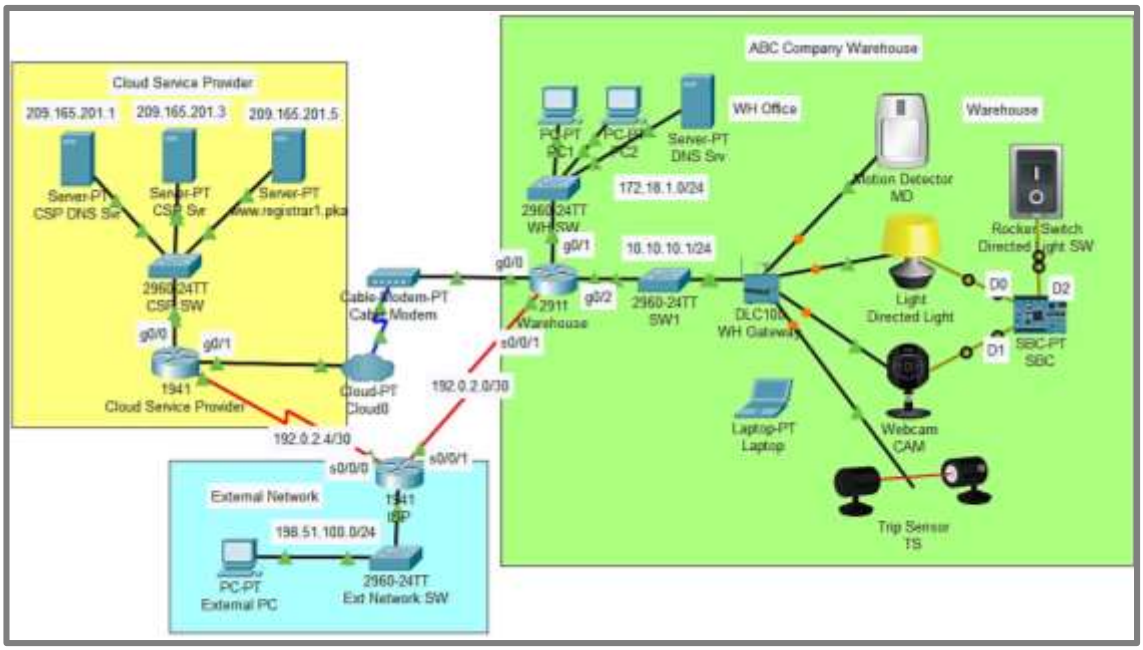


Рисунок 11.1 – Мережа ABC Company

1.2. Додайте користувача на сервер реєстрації **www.registrar1.pka** з надійним паролем:

1) Використовуйте **PC** в офісі **WH office**. На вкладці **Desktop** відкрийте **Web Browser**, введіть **www.registrar1.pka** та виберіть **Go**. Відобразиться вікно входу на сервер реєстрації (рис. 11.2).
2) Клацніть **Sign up now** і створіть власний обліковий запис із надійним паролем (переконайтеся, що пароль має довжину принаймні 8 символів із комбінацією великих символів, символів нижнього регістру та цифр).

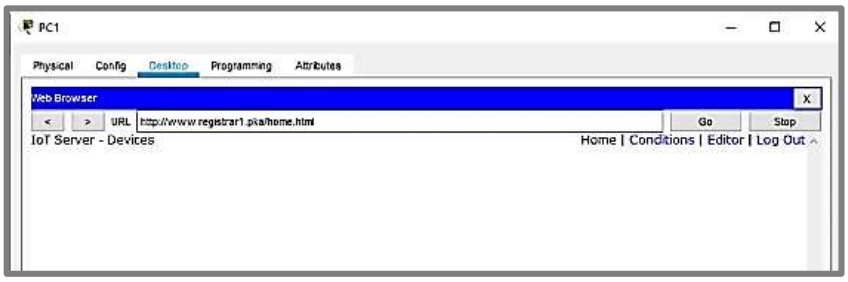


Рисунок 11.2 – Реєстрація на сервері

Яке ваше ім’я користувача та пароль?

Відповідь:_____

1.3. Реєстрація пристроїв IoT на сервері реєстрації:

1) На складі **Warehouse** натисніть **Motion Detector**. На вкладці **Config** виберіть **Remote Server** у розділі IoT Server. Введіть **www.registrar1.pka** як адресу сервера та натисніть **Connect** (рис. 11.3). Введіть ім'я користувача/пароль, які ви щойно створили.

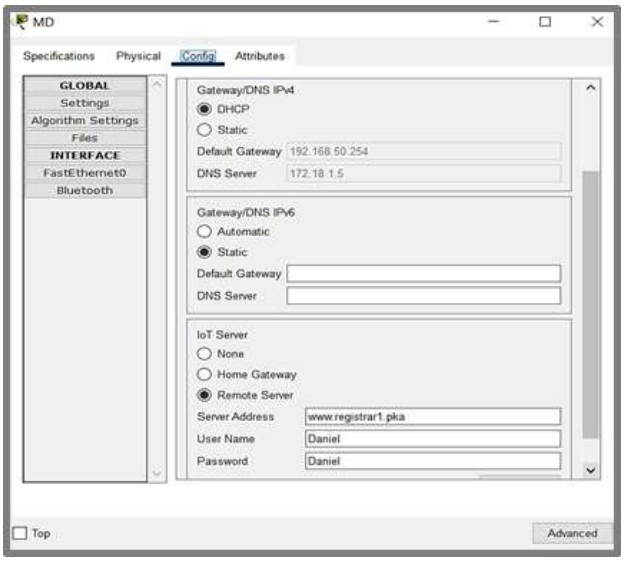


Рисунок 11.3 – Реєстрація Motion Detector на сервері

Чи відображається **Motion Detector** на сервері реєстрації?

Відповідь:_____

2) Аналогічно зареєструйте **Light**, **Webcam** та **Trip Sensor**.

2. Додавання умови на сервері реєстрації

Додайте умови на реєстраційному сервері, щоби під час активації **Motion Detector** або **Trip Sensor** вмикалися спрямоване світло та вебкамера.

2.1. Увійдіть на сервер реєстрації, використовуючи ім'я користувача/пароль, які ви створили.

Скільки ви бачите пристроїв IoT у списку?

Відповідь:_____

2.2. Натисніть **Conditions** та додайте такі три умови:

1) Призначте **LightsOn1**, якщо статус MD під час ввімкнення має вірне значення – **MD On is true**, тоді встановіть для статусу направленого світла ввімкнено, тобто значення On – **Set Directed Light Status to On** та встановіть для статусу камери значення true – **Set CAM On to true**.
2) Позначте **LightsOn2**, якщо статус датчика Trip Sensor у разі ввімкнення має вірне значення – **TS On is true**, тоді встановіть для стану Directed Light значення On – **Set Directed Light Status to On** та встановіть для статусу CAM під час ввімкнення значення true – **Set CAM On to true**.
3) Призначити **LightsOff**, якщо статус MD та TS у разі ввімкненя є помилковим – **MD On is false**; **TS On is false**, тоді встановіть для статусу Directed Light значення Off – **Set Directed Light to Off** та встановіть для статусу CAM On значення false – **Set CAM On to false**.
4) Перевірте умови (рис. 11.4).

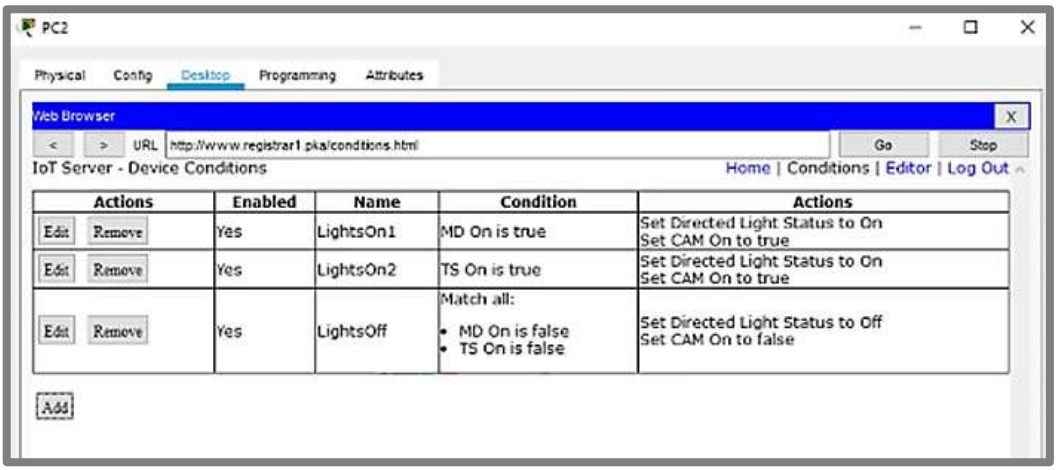


Рисунок 11.4 – Умови на сервері реєстрації

Утримуйте клавішу **Alt** і наведіть курсор на детектор руху. Чи ввімкнено спрямоване світло Directed Light та вебкамеру Webcam?

Відповідь:_____

Відведіть мишку та зачекайте кілька секунд. Чи вимкнено спрямоване світло та вебкамеру?

Відповідь:_____

3. Налаштування надійної автентифікації для мережевих пристроїв

3.1. Налаштуєте надійну автентифікацію для бездротового з'єднання на пристрої шлюзу WH:

1) В області складі клацніть пристрій **WH Gateway**. На вкладці **Config** у параметрі **Wireless** встановіть SSID на **WhGateway1**, встановіть Authentication на **WPA2-PSK** із паролем як **IoTWh001**. Залиште тип шифрування **AES** (рис. 11.5).

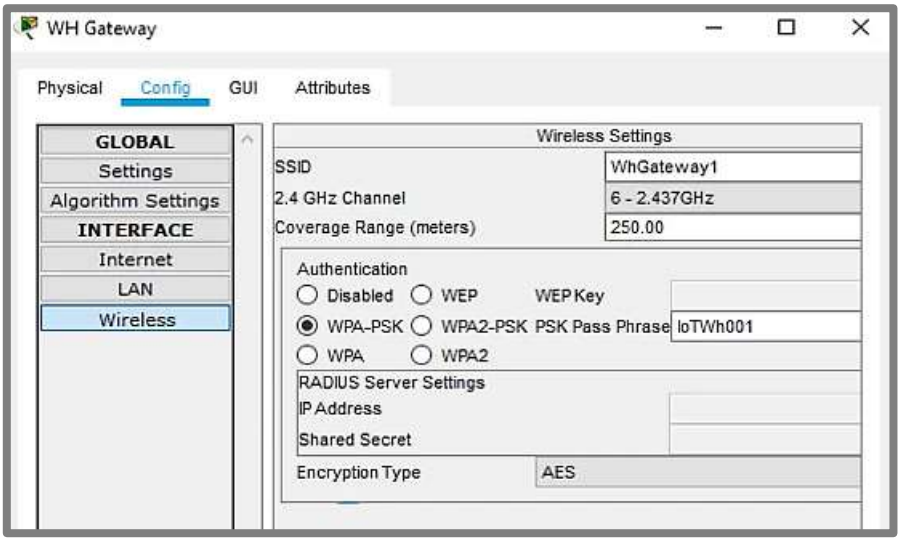


Рисунок 11.5 – Налаштування WH Gateway

2) Натисніть на ноутбук **Laptop**. На вкладці **Config** у параметрі **Wireless0** встановіть SSID на **WhGateway1**, а для автентифікації встановіть **WPA2-PSK** із паролем як **IoTWh001**. Залиште тип шифрування **AES** (рис. 11.6).

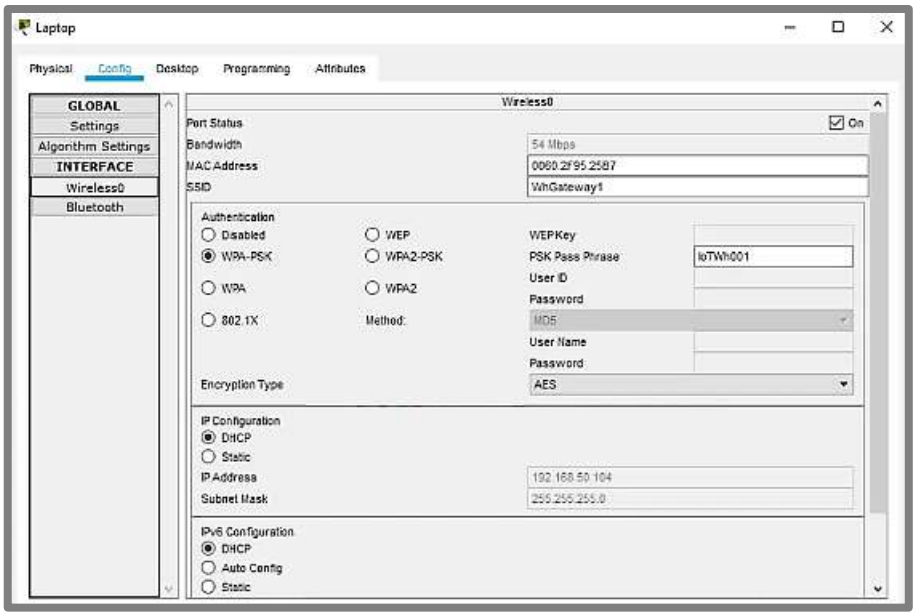


Рисунок 11.6 – Налаштування Laptop

Ноутбук успішно підключається до WH Gateway?

Відповідь:_____

3.2. На маршрутизаторі складу налаштуйте банер для відображення попереджувального повідомлення про незаконний доступ. Хоча банерне повідомлення само собою не є засобом безпеки, воно може діяти як стримуючий засіб для зловмисників. Встановіть зашифрований пароль для входу в режим виконання Exec mode. Налаштуйте локальний обліковий запис користувача для лінії консолі та віддаленого доступу.

1) Натисніть маршрутизатор Warehouse 2911, потім натисніть вкладку **CLI** та введіть ці команди:

```
Warehouse> enable
Warehouse# config terminal
Warehouse(config)# banner login %Login with valid password%
Warehouse(config)# banner motd %Authorized Access Only!
Unauthorized access is ubject to Federal Prosecution.%
Warehouse(config)#
```

2) Встановіть безпечний пароль для режиму Exec:

```
Warehouse(config)# enable secret AbcWh001
```

```
Warehouse(config)# exit
```

3) Встановіть локальне ім’я користувача для доступу до консольної лінії та ліній VTY:

```
Warehouse# configure terminal
Warehouse(config)# username WhAdmin secret AbcLine001
Warehouse(config)# line console 0
Warehouse(config-line)# login local
Warehouse(config-line)# exit
Warehouse(config)# line vty 0 4
Warehouse(config-line)# login local
Warehouse(config-line)# end
Warehouse#
```

4. Налаштування списків доступу для обмеження трафіка між пристроями IoT компанії ABC і мережею постачальника хмарних послуг

4.1. На складському маршрутизаторі налаштуйте та застосуйте список доступу 10, щоб дозволити трафік лише з DNS-сервера та сервера реєстрації входити в мережу складських пристроїв IoT компанії ABC:

```
Warehouse# configure terminal
Warehouse(config)# access-list 10 permit host 172.18.1.5
Warehouse(config)# access-list 10 permit host 209.165.201.5
Warehouse(config)# interface g0/2
Warehouse(config-if)# ip access-group 10 out
Warehouse(config-if)# end
Warehouse#
```

4.2. На маршрутизаторі постачальника хмарних послуг налаштуйте та застосуйте список доступу 110, щоб дозволити доступ до сервера реєстрації трафіку лише з мережі складських пристроїв IoT компанії ABC Company:

```
CSP# configure terminal
CSP(config)# access-list 110 permit ip host 209.165.200.226 host
209.165.201.5
```

```
CSP(config)# access-list 110 deny ip any host 209.165.201.5
CSP(config)# access-list 110 permit ip any any
CSP(config)# interface g0/0
CSP(config-if)# ip access-group 110 out
CSP(config-if)# end
CSP#
```

Чому в ACL 110 IP-адресу інтерфейсу маршрутизатора складу вибрано як джерело в ACL 110?

Відповідь:_____

5. Налаштування захищеного вебзв'язку із вебсервером у мережі постачальника хмарних послуг

Компанія ABC використовує вебсервер постачальника хмарних послуг для частини своєї роботи. Налаштуйте вебсервер у мережі постачальника хмарних послуг для доступу лише через HTTPS:

1) Натисніть **CSP Svr**, а потім клацніть вкладку **Services.**
2) Натисніть **HTTP** на лівій панелі. Переконайтеся, що HTTP вимкнено, а HTTPS увімкнено (рис. 11.7).

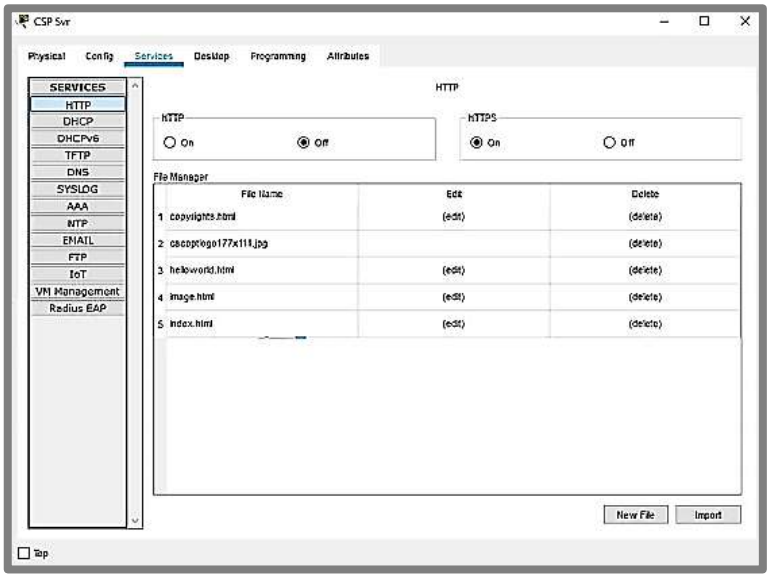


Рисунок 11.7 – Налаштування захищеного вебзв'язку

6. Протестуйте систему.

6.1. З ноутбука в складській мережі зайдіть на сервер реєстрації. Увімкніть детектор руху або датчик відключення та спостерігайте за дією спрямованого світла та вебкамери.

6.2. З PC1 або PC2 відкрийте веббраузер.

Чи може він отримати доступ до сервера реєстрації?

Відповідь:_____

Чи може він отримати доступ до вебсервера 209.165.201.3 через HTTP?

Відповідь:_____

Чи може він отримати доступ до вебсервера 209.165.201.3 через HTTPS?

Відповідь:_____

Які заходи безпеки вживаються?

Відповідь:_____

Які інші заходи безпеки варто враховувати під час розгортання рішень IoT із хмарними обчисленнями?

Відповідь:_____

ВИМОГИ ДО ОФОРМЛЕННЯ ЗВІТУ

1. Сформуйте файл для звіту. Звіт про виконання роботи має включати:

- Титульний аркуш, вказуючи номер і назву роботи, прізвище і групу студента.
- Покроковий опис основних етапів виконання роботи. Отримані результати підтверджуються скріншотами екрану.
- Відповіді на поставлені запитання.
- Висновки щодо проведеної роботи.

2. Створений файл із назвою LR-11_XXXXX.pkt, де XXXXX – позначення прізвища студента.



КОНТРОЛЬНІ ЗАПИТАННЯ

1. Які заходи безпеки IoT рішень ви знаєте?
2. Які заходи безпеки варто враховувати при розгортанні рішень IoT з використанням хмарних обчислень?
3. Як відбувається налаштування надійної аутентифікації на мережевих пристроях?
4. Як відбувається налаштування списків доступу для обмеження трафіка між пристроями IoT компанії та мережею постачальників?
5. Як здійснюється налаштування безпечної вебкомунікації на вебсервері в мережі?
6. Яка найкраща практика безпеки передбачає визначення правил компанії, посадових обов’язків і очікувань?
7. Які правила регулюють обмін даними між мережевими пристроями?
8. Які рекомендовані заходи безпеки варто виконати під час використання готових пристроїв Інтернету речей?

ЛАБОРАТОРНА РОБОТА № 12
ДОСЛІДЖЕННЯ SMART CITY ТА SMART GRID

Мета роботи: Дослідити Smart City та Smart Grid. Проаналізуйте використання хмарних обчислень у розумному місті та розумній електромережі.

ВКАЗІВКИ ДО ВИКОНАННЯ РОБОТИ

ЧАСТИНА 1
ДОСЛІДЖЕННЯ SMART CITY

У цій роботі досліджується приклад розумного міста Smart City. Ідея розумного міста базується на території міста, яке використовує програмне забезпечення для моніторингу та аналізу різноманітних подій і прийняття рішень для покращення життя своїх мешканців.

Розумне місто Smart City в цьому прикладі розбито на кластери. Залежно від програми, деякі дані найкраще обробляти та контролювати з віддаленого місця. Офіси Smart City пропонують можливості, які дають можливість міському адміністратору контролювати різноманітні події в місті.

1. Дослідження Smart City

1.1. Розуміння пристроїв, які складають розумне місто.

Завантажте файл **Packet-Tracer-Explore-the-Smart-City.pka.** Оскільки датчики та пристрої IoT розповсюджені у розумному місті, перед тим, як вони зможуть обмінюватися даними, має бути створена належна мережева інфраструктура. Smart City – це міська мережа (MAN), що складається з менших мереж. Ці мережі часто з’єднані за допомогою WAN-зв’язків, які дають змогу спілкуватися на великих географічних відстанях. Хмара провайдера ISP Cloud provides надає доступ по всьому місту різним особам і організаціям.

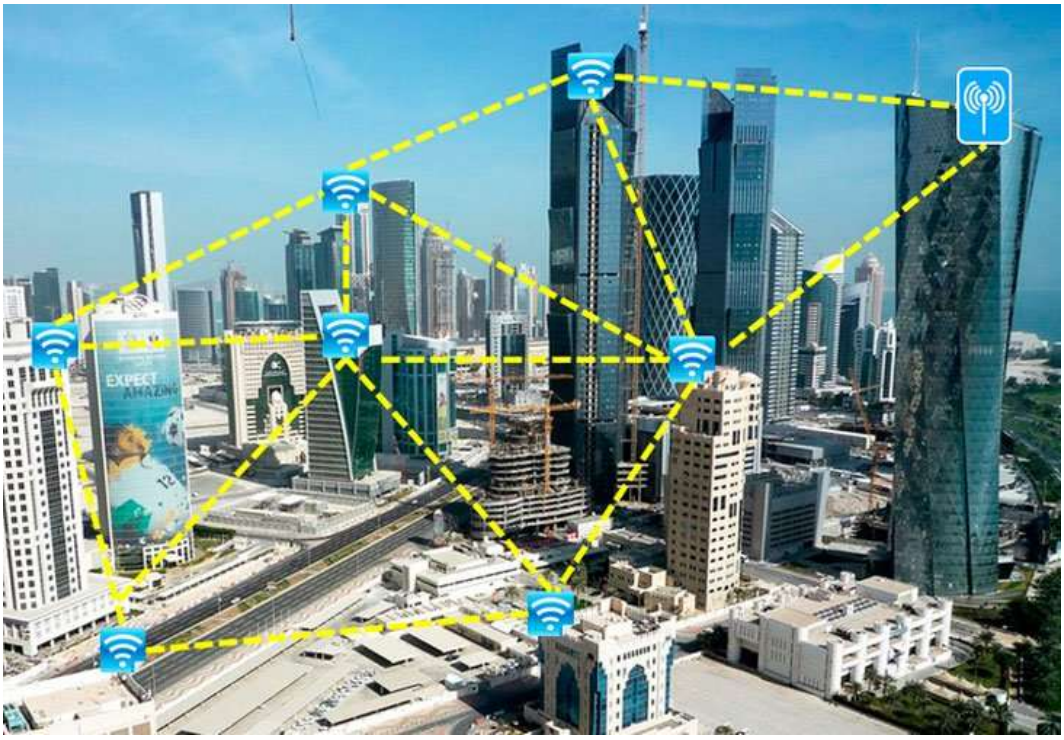


Рисунок 12.1 – Мережа розумного міста

1.2. Натисніть **ISP Cloud** і перегляньте ресурси, які вона пропонує місту.

1.3. Натисніть кнопку **Go Back**.

❓ Які міські мережі підключені за допомогою червоних послідовних кабелів?

Відповідь:_____

Примітка. *Packet Tracer позначає з'єднання між мережевими пристроями, але його можна вимкнути для зручності читання. Щоб вимкнути маркування, перейдіть до* **Options / Preferences / Interface** *та зніміть прапорець* **Always Show Port Labels in Logical Workspace**.

❓ До яких міських мереж підключаються сині коаксіальні кабелі?

Відповідь:_____

❓ Натисніть кластер **City Offices**. Чому з хмари провайдера **ISP Cloud** до нього ведуть два з'єднання?

Відповідь:_____

Натисніть кнопку **Go Back**. Які міські мережі бездротово підключені до **Cell-Tower**?

Відповідь:_____

Які пристрої в **Smart Home** підключені до **Cell-Tower**?

Відповідь:_____

Які пристрої в кластері **Smart Parking** підключені до **Cell-Tower**?

Відповідь:_____

2. Розумне паркування

Розумне місто Smart City складається з ряду систем, представлених у цьому прикладі кластерами. Кластер Smart Parking дає можливість міській владі та громадянам одержати вигоду від впровадження IoT.

2.1. Взаємодія з кластером Smart Parking (персонал міських офісів).

Пристрої в кластері розумного паркування можна відстежувати та керувати дистанційно через будь-який комп'ютер у кластері міських офісів. Оскільки всі розумні пристрої паркувального кластера підключаються до **City IoT Server**, який містить вебінтерфейс, планшети, смартфони, ноутбуки або настільні комп'ютери, то їх можна використовувати для взаємодії з розумними пристроями.

1) Натисніть **City IT Laptop** у кластері **City Offices**.
2) Перейдіть до **Desktop** / **Web Browser**.
3) В адресному рядку URL-адреси введіть **195.0.0.2**. Це IP-адреса **City IoT Server**.
4) Використовуйте **Park** / **Park** як ім'я користувача та пароль для входу на City IoT Server (рис. 12.2).

Примітка. *Можливо, вам знадобиться кілька хвилин, поки всі мережеві пристрої не підключаться до Інтернету речей, а паркомати зможуть підключитися до сервера реєстрації Інтернету речей*.

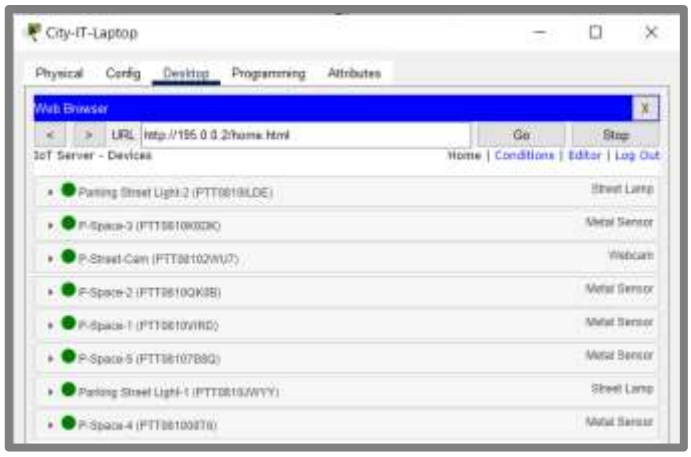


Рисунок 12.2 – Відображення City IoT Server

Що відображається?

Відповідь:_____

5) Паркомати реєструються на сервері та періодично надсилають оновлення статусу. Натисніть лічильник **P-Space-1**, щоб розгорнути його (рис. 12.3).

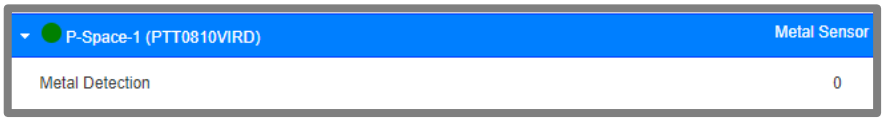


Рисунок 12.3 – Відображення P-Space-1

Яке значення відображається?

Відповідь:_____

6) Не закриваючи вікно **City IT Laptop**, поверніться до кластера розумного паркування, клацніть і перетягніть червоний автомобіль на місце паркування **Parking Spot 1**. Parking Spot 1 – це крайнє ліве місце паркування в кластері.
7) Поверніться до вікна **City IT Laptop** і знайдіть **P-Space-1** (розгорніть його, якщо необхідно), як на рис. 12.4.



Рисунок 12.4 – Відображення P-Space-1 після парковки

Яке значення відображається зараз?

Відповідь:_____

Датчики паркувальних місць – це металеві датчики PT, налаштовані на реакцію на металеві об'єкти (у цьому випадку автомобілі), якщо вони розташовані досить близько.

2.2. Взаємодія з кластером Smart Parking (звичайні громадяни)

Хоча це корисно як інструмент моніторингу для міської адміністрації, звичайні громадяни не мають мати доступу до інтерфейсу на сервері. Для того, щоб громадяни могли контролювати наявність місць для паркування на тій чи іншій вулиці (рис. 12.5), була створена ще одна вебсторінка.

1) Закрийте вікно **City IT Laptop** і поверніться до кластера **Smart Parking.**
2) Натисніть **Smartphone** і відкрийте його веббраузер, перейшовши на вкладку **Desktop Tab / Web Browser**.
3) В адресному рядку введіть **10.10.10.10** – адреса сервера паркування, представленого PT-MCU.

Примітка: *може пройти кілька секунд, перш ніж сторінка завантажиться у веббраузері смартфона*.



Рисунок 12.5 – Відображення Smart Parking на Smartphone

Що ви бачите після завантаження сторінки?

Відповідь:_____

4) Не закриваючи вікна **Smartphone**, перетягніть зелений автомобіль на місце паркування **Parking Spot 5**. **Місце паркування 5** – це крайнє праве місце паркування в кластері **Smart Parking.**
5) Поверніться до вікна смартфона (веббраузер усе ще має відображати сторінку, завантажену із сервера паркування MCU), як на рис. 12.6.



Рисунок 12.6 – Відображення Smart Parking на Smartphone після паркуваннння

Що ви бачите після завантаження сторінки?

Відповідь:_____

Примітка. *Оновлення сторінки може зайняти кілька секунд.*

6) Паркувальні місця не лише звітують на реєстраційний сервер Інтернету речей **IoT Registration Server**, розміщений у кластері **City Offices**, а й на локальний сервер паркування. Це дає можливість громадянам переглядати та дізнаватися про наявність паркувальних місць ще до того, як вони вийдуть на вулицю.
7) Опрацюйте код, на якому працює сервер паркування в MCU.

3. Smart Traffic

Ще одна складова розумного міста – **Smart Traffic**. У цьому прикладі **Smart Traffic** дозволяє транспортним засобам екстреної допомоги, таким як

машини швидкої допомоги або парамедики, зв'язуватися з системою світлофора та запитувати вільний проїзд у разі надзвичайної ситуації. Перейдіть до кластера **Smart Traffic.**

1) У цьому прикладі **Street Light 1** і **Street Light 2** виконують роль світлофора. Швидка медична допомога надає екстрену допомогу. Коли автомобіль парамедиків наближається до світлофора, він стає зеленим. Натисніть і перетягніть вантажівку фельдшера та помістіть її ближче до світлофора праворуч, який зараз горить червоним.

Що відбувається зі світлофором праворуч?

Відповідь:_____

2) Відведіть парамедиків від світлофора праворуч і поставте його ближче до червоної машини.

Що відбувається зі світлофором?

Відповідь:_____

3) Автомобіль парамедиків надсилає повідомлення до MCU, що контролює світлофор, і просить проїзд. MCU визнає парамедиків законним транспортним засобом екстреної допомоги та дозволяє йому проїзд, увімкнувши світло – зелений. MCU також вмикає відповідні індикатори червоними для забезпечення безпечного проходу. Коли автомобіль швидкої допомоги безпечно проїхав, MCU повертає систему до нормального режиму роботи.
4) Проаналізувати код, що працює в MCU для машини швидкої допомоги, перейшовши на вкладку **Programming.**

Примітка. *Можливо, вам знадобиться натиснути кнопку* ***Advanced*** *внизу вікон пристроїв, перш ніж можна буде відобразити вкладку* ***Programming.***

4. Міркування

Коли датчики, програмне забезпечення та сервери взаємопов'язані, можна збирати дані та відстежувати події. Це дає змогу приймати рішення на основі даних, керованих подіями. Ключовий момент цього прикладу – показати, що пов'язані речі можуть контролювати та діяти, якщо вони:

- здатні виконувати програми;
- підключаються до датчиків або виконавчих механізмів;
- підключені до інших пристроїв через мережу.

ЧАСТИНА 2
ДОСЛІДЖЕННЯ SMART GRID

У цій роботі досліджується розумна мережа Smart Grid. Smart Grid відстежує енергію, що надходить із різних джерел, і перемикається на найбільш ефективне доступне джерело живлення. Smart Grid використовує переваги розумного перемикача, щоб вирішити, яке джерело живлення використовувати.

1. Розуміння пристроїв, які складають розумну мережу Smart Grid

1.1. Завантажте файл **Packet-Tracer-Explore-the-Smart-Grid.pka.** Для роботи розумної мережі необхідні різні типи пристроїв. Мережеві пристрої потрібні для забезпечення зв'язку в інтелектуальній мережі Smart Grid. За виробництво енергії відповідають сонячні батареї, вітрові турбіни та вугільна станція. Лічильники та датчики використовуються для збору даних і полегшення моніторингу джерел енергії.

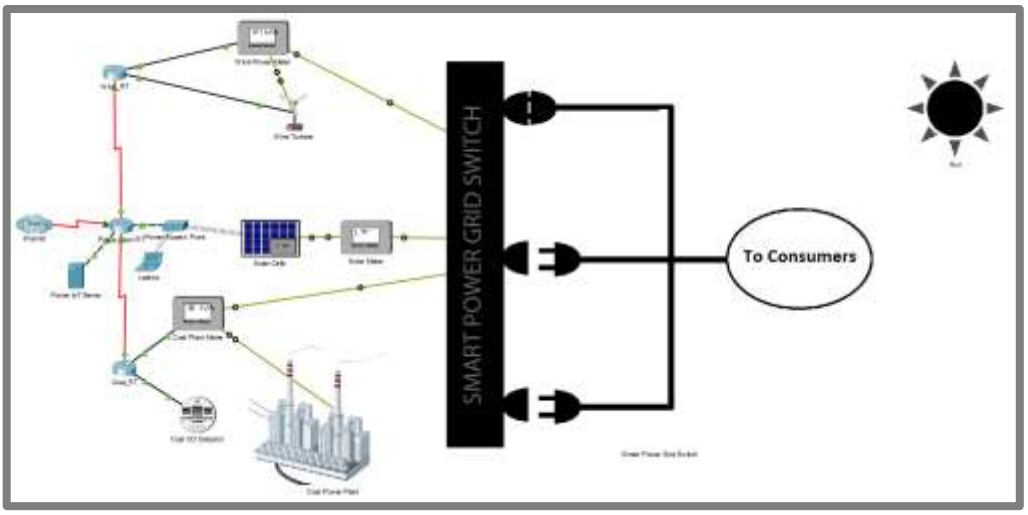


Рисунок 12.7 – Відображення розумної електромережі

1.2. Перегляньте Smart Grid.

Скільки маршрутизаторів ви бачите в розумній мережі? Яке їх позначення?

Відповідь:_____

Яку функцію виконують маршрутизатори?

Відповідь:_____

В Smart Grid використовується бездротова точка доступу. Як вона називається? Яка її функція?

Відповідь:_____

Чи є спосіб визначити, яке джерело живлення активно виробляє енергію?

Відповідь:_____

Який пристрій відповідає за перемикання між різними джерелами живлення?

Відповідь:_____

Як Smart Power Grid Switch визначає, яке джерело живлення використовувати?

Відповідь:_____

Яка IP-адреса сервера Power IoT Server?

Відповідь:_____

1.3. Ноутбук використовується техніками для моніторингу кількості енергії. Використовуйте Web Browser для віддаленого підключення до сервера Power IoT. Вам знадобиться знати ім'я користувача та пароль, щоб увійти на сервер. Ви можете дізнатися ім'я користувача та пароль, перевіривши інші пристрої в Smart Grid.

Яке ім'я користувача та пароль і за допомогою якого пристрою ви їх виявили?

Відповідь:_____

2. Вивчення програми Smart Power Grid Switch

Перемикач **Smart Power Grid Switch** має можливість запуску програм. У цьому прикладі програма була написана на Javascript. Він відстежує рівні потужності від усіх джерел (вітряної електростанції, сонячних батарей і вугільної електростанції) і вирішує, яке джерело є найкращим.

2.1. Натисніть **Smart Power Grid Switch**.

2.2. Перейдіть на вкладку **Programming.** Якщо вкладка **Programming** не відображається, натисніть кнопку **Advanced** внизу вікна, щоб відобразити додаткові вкладки.

2.3. У лівій частині вкладки Programming двічі клацніть **power_switch(Javascript)**, а потім двічі клацніть **main.js.** Програма Javascript, запущена на Smart Power Grid Switch, має з'явитися в правій частині вкладки Programming.

Розташування електромережі дає можливість спостерігати сонячне світло з 6:00 до 18:00. Через близькість до океану вітер зазвичай дме з 3:00 до 22:00. Програма гарантує, що сонячна енергія є найбільш переважним джерелом енергії. Якщо сонячна енергія недоступна (сонячне світло), програма перемикається на вітряну енергію, якщо вона доступна. Якщо вітер не дме, програма повертається до енергетики на основі вугілля.

Який розділ програми чітко визначає це налаштування (сонячна енергія / вітер / вугілля)?

Відповідь:_____

3. Міркування

Ключовим аспектом IoT є інтелект, доданий до речей. Програми дають можливість пристроям бути більш обізнаними та приймати рішення на основі подій тригерів. Для цього доступно багато мов програмування, які можна використовувати.

Перш ніж програми можуть виконуватися речами, має бути встановлена належна апаратна платформа, яка, по суті, перетворює річ на комп'ютер. Зазвичай це робиться через додавання процесора, пам'яті та певної можливості введення-виведення.

Нарешті, новостворена розумна річ повинна мати можливості мережевого зв'язку, щоб стати частиною IoT.

У цьому прикладі інтелектуальної мережі Smart Power Grid Switch одержав можливості обробки для запуску програм Javascript. На основі датчиків і лічильників він міг би знати про своє оточення та діяти відповідно до набору заздалегідь визначених умов. Мережеві пристрої та можливості дозволяють комутатору Smart Power Grid Switch спілкуватися через мережу та приєднуватися до IoT.



ВИМОГИ ДО ОФОРМЛЕННЯ ЗВІТУ

1. Сформуйте файл для звіту. Звіт про виконання роботи має включати:

- Титульний аркуш, вказуючи номер і назву роботи, прізвище і групу студента.
- Покроковий опис основних етапів виконання роботи. Отримані результати підтверджуються скріншотами екрана.
- Відповіді на поставлені запитання в кожній частині завдання.
- Висновки щодо проведеної роботи.



КОНТРОЛЬНІ ЗАПИТАННЯ

1. Що таке Smart City?
2. Які мережі охоплює Smart City?
3. Які кластери можливі для Smart City?
4. Які переваги їх використання?
5. Опишіть роботу одного з відомих вам кластерів розумного міста.
6. Які заходи безпеки рекомендовано вжити під час використання стандартних пристроїв IoT?
7. Що таке Smart Grid?
8. Опишіть принцип роботи Smart Grid?
9. Які переваги використання Smart Grid?

ЛАБОРАТОРНА РОБОТА № 13
НАЛАШТУВАННЯ ВІРТУАЛЬНОГО СЕРВЕРНОГО СЕРЕДОВИЩА



Мета роботи: Встановити віртуальну машину (VM) сервера I2IoT у VirtualBox; здійснити доступ до I2IoT Server VM та ознайомитися з основною навігацією в CentOS 7; набути навичок у базовому програмуванні на Python.



ТЕОРЕТИЧНІ ВІДОМОСТІ

За останні роки обчислювальна потужність і ресурси надзвичайно зросли. Однією з переваг доступу до багатоядерних процесорів і великого обсягу оперативної пам'яті є можливість використовувати програмне забезпечення віртуалізації для спільного використання ресурсів. За допомогою віртуалізації користувач може запускати декілька віртуальних комп'ютерів на одному фізичному комп'ютері, таким чином оптимізуючи використання ресурсів.

Віртуальні комп'ютери, які працюють у фізичному комп'ютері, називаються віртуальними машинами (VM). Віртуальні машини працюють в ізольованому середовищі, і діяльність однієї віртуальної машини ізольована від активності інших віртуальних машин. Стан віртуальної машини можна зберегти та відновити, дозволяючи повернутися до попереднього обчислювального середовища. Віртуальні машини можна легко створювати, копіювати та ділитися ними, що робить їх чудовими інструментами для експериментів і створення прототипів.

Сьогодні організації використовують віртуалізоване середовище для розміщення великої кількості віртуальних машин для задоволення обчислювальних потреб своїх користувачів. На рівні персонального комп'ютера кожен із сучасним комп'ютером і операційною системою також має можливість запускати кілька віртуальних машин із робочого столу.

ВКАЗІВКИ ДО ВИКОНАННЯ РОБОТИ

У роботі використовується сервер I2IoT для вивчення основи програмування комп'ютерних додатків на Python. Сервер I2IoT – це віртуальна машина, розміщена в середовищі віртуалізації. Кілька продуктів забезпечують віртуалізацію на персональному комп'ютері. Для курсу I2IoT використовується безкоштовний продукт Oracle VirtualBox для віртуалізованого середовища. Розглянемо процес завантаження та встановлення VirtualBox.

1. Підготовка комп'ютера до середовища віртуалізації шляхом встановлення VirtualBox

Необхідно завантажити та встановити програмне забезпечення віртуалізації VirtualBox, безкоштовний продукт від Oracle.

1.1. Завантаження VirtualBox.

1) Перевірте оперативну пам'ять комп'ютера. ***Рекомендується встановити 4 ГБ+ оперативної пам'яті.***
2) Відкрийте веббраузер і перейдіть на сайт завантаження VirtualBox: https://www.virtualbox.org/wiki/Downloads
3) Виберіть пакет, який працює з операційною системою вашого комп'ютера, і завантажте пакет (рис. 13.1). Ви можете завантажити пакет розширення, який забезпечує підтримку VirtualBox RDP, шифрування диска, завантаження NVMe і PXE для карт Intel.

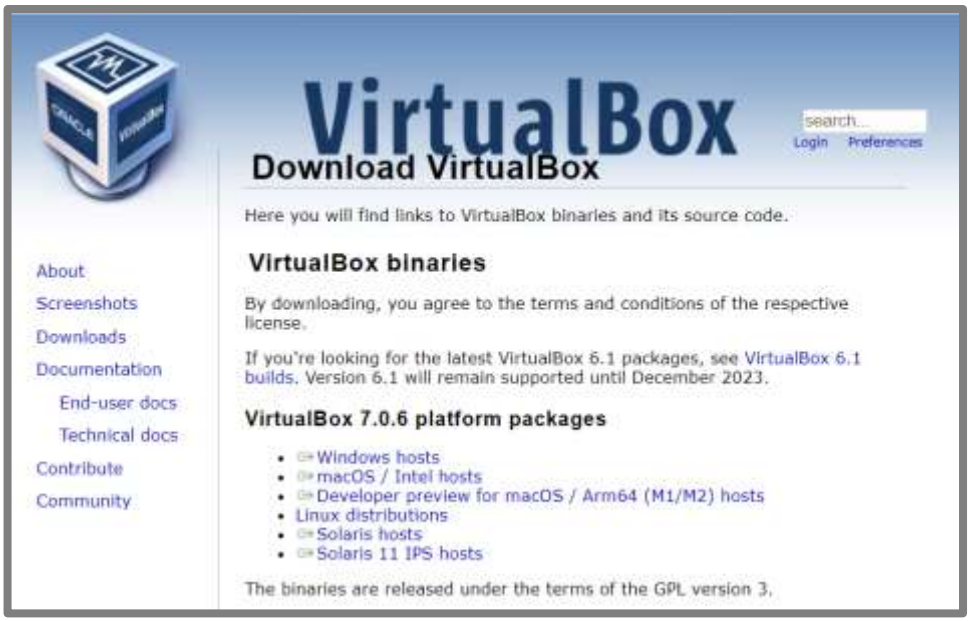


Рисунок 13.1 – Вікно сайту для завантаження VirtualBox

1.2. Встановлення VirtualBox.

1) Використовуйте звичайний метод інсталяції, щоб встановити VirtualBox на свій комп'ютер. Для Windows двічі клацніть завантажений файл exe, щоб інсталювати VirtualBox (рис. 13.2).



Рисунок 13.2 – Вікно завантаження

2) Покроково натисніть **Next** (рис. 13.3).

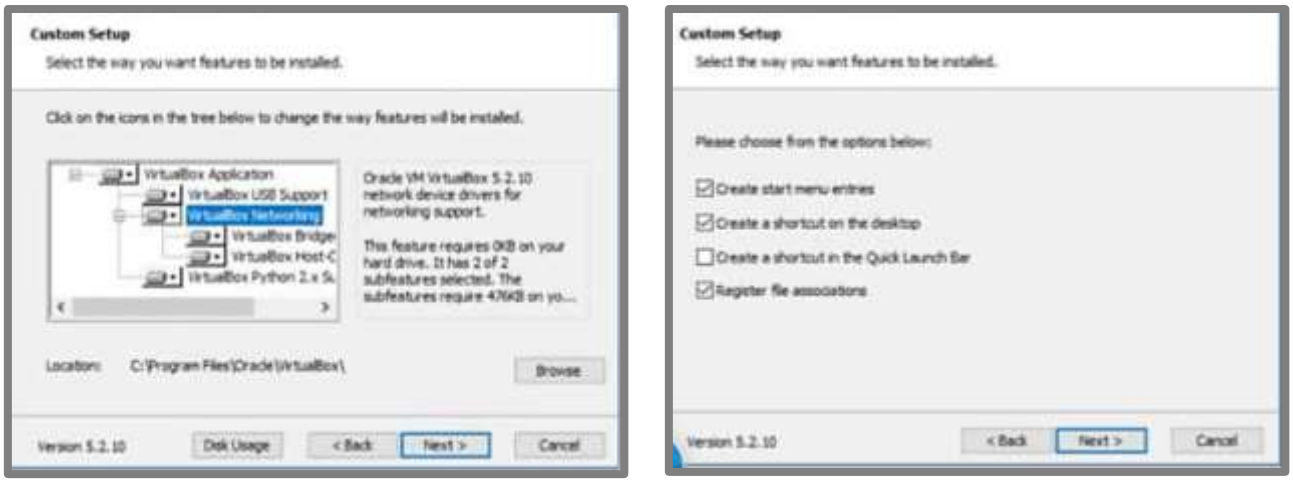


Рисунок 13.3 – Покрокове виконання

3) Натисніть **Yes** та **Install.** Розпочнеться встановлення (рис. 13.4).

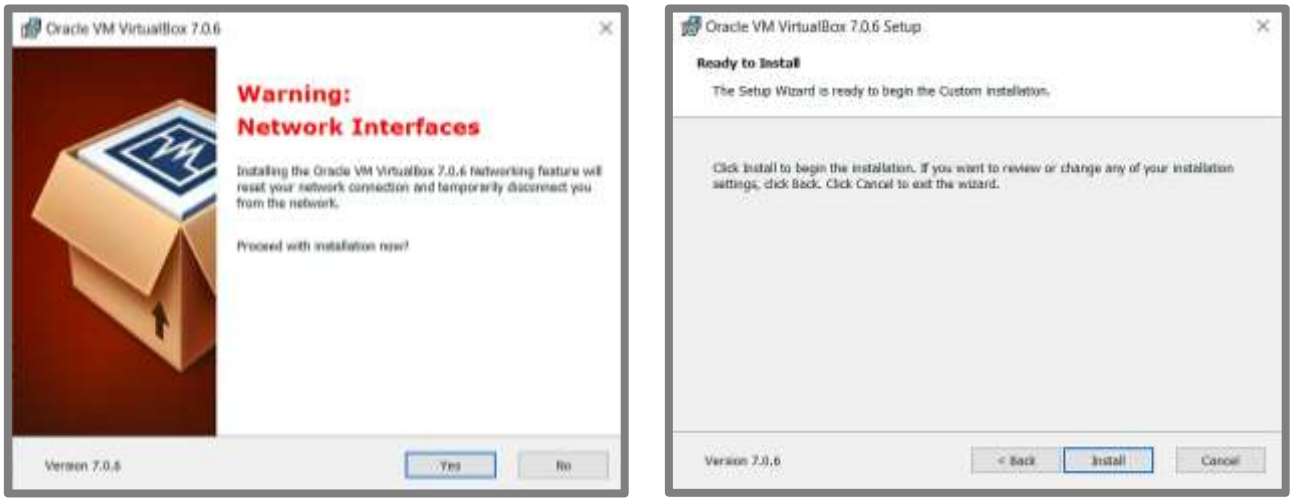


Рисунок 13.4 – Встановлення віртуальної машини

4) Після завершення встановлення натисніть **Finish**, щоби продовжити (рис. 13.5).



Рисунок 13.5 – Завершення завантаження

5) Якщо ви також завантажили пакет розширення, ви можете встановити його, двічі клацнувши пакет розширення. Натисніть **Install.**
6) З'явиться вікно про ліцензію VirtualBox. Прокрутіть униз і натисніть кнопку **I Agree**.

2. Встановлення віртуальної машини (VM) сервера I2IoT у віртуалізоване середовище VirtualBox

2.1. Завантажте пакет віртуальної машини сервера I2IoT.

Сервер I2IoT упаковується та розповсюджується як файл .ova. Файл OVA є відкритим пристроєм віртуалізації, який використовується такими програмами віртуалізації, як VMware Workstation і Oracle VM Virtualbox. Він містить стиснуту версію віртуальної машини, яку можна імпортувати в підтримуване середовище віртуалізації.

1) Відкрийте веббраузер і завантажте файл OVA курсу Virtual Machine, перейшовши за URL-адресою: https://drive.google.com/file/d/1BSlvXkei5TmLxmhB7ggShfACL_I5U_5j/view?usp=sharing
2) Скопіюйте або перемістіть завантажений файл у місце, яке легко запам'ятати, наприклад, C:\I2IoT\VM (рис. 13.6).



Рисунок 13.6 – Розміщення завантаженого файлу

2.2. Імпортуйте віртуальну машину I2IoT у VirtualBox.

1) Двічі клацніть піктограму **I2IoT**-GUI.ova.
2) Позначте опцію **Generate new MAC addresses for all network adapters** (Згенеруйте нові MAC-адреси для всіх мережевих адаптерів) (або **Reinitialize the MAC address of all network cards** і натисніть **Import** (рис. 13.7).

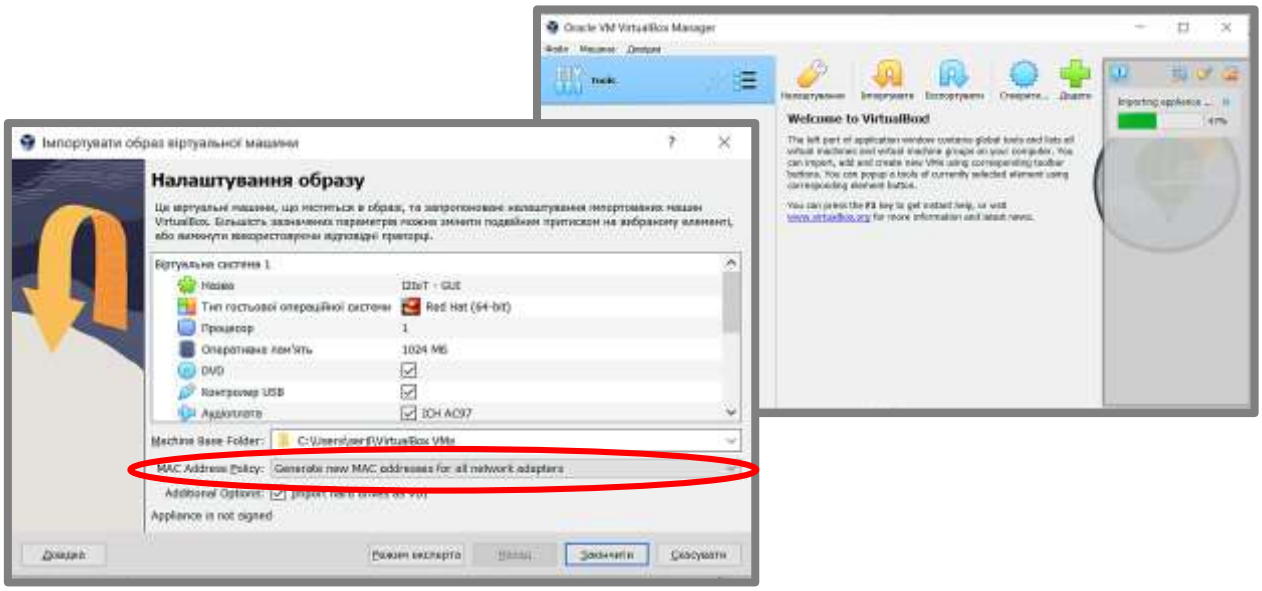


Рисунок 13.7 – Імпортування віртуальної машини I2IoT

3) Після завершення імпорту з’явиться вітальне повідомлення (рис. 13.8). Зверніть увагу, що віртуальна машина I2IoT знаходиться на лівій панелі VirtualBox зі статусом **Powered Off** (Вимкнено).



Рисунок 13.8 – Інсталяція віртуальної машини I2IoT

3. Налаштування віртуальної машини та доступ до I2IoT Server VM за допомогою дійсного облікового запису

3.1. Виконайте початкові налаштування.

1) Виділіть віртуальну машину, клацнувши піктограму віртуальної машини на лівій панелі.

2) Натисніть **Settings** (Налаштування), як на рис. 13.9.

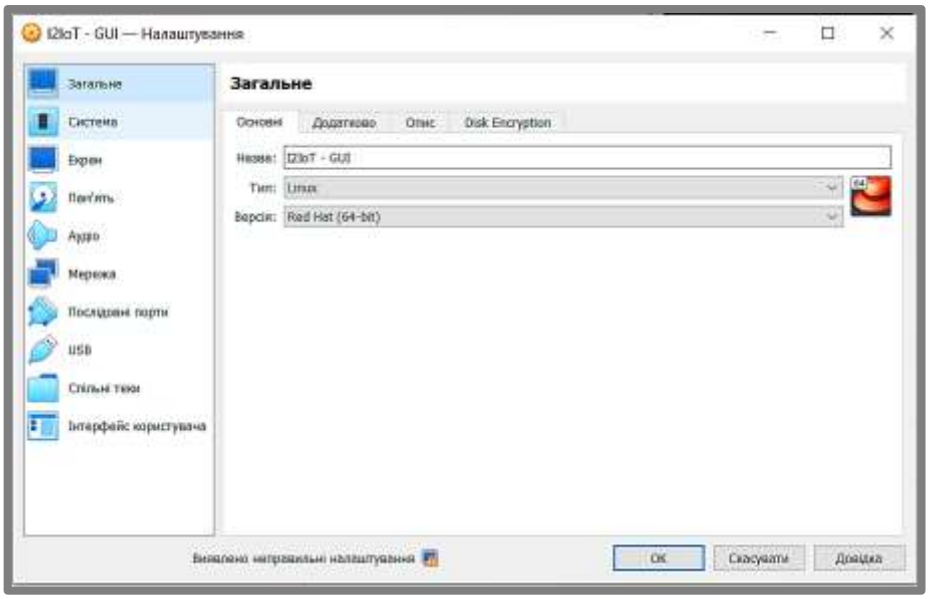


Рисунок 13.9 – Вікно налаштування

3) Клацніть елементи на лівій панелі та ознайомтеся з поточними параметрами віртуальної машини.

4) Клацніть **System**. На вкладці **Motherboard** містяться параметри використання оперативної пам'яті (**Base Memory**) і порядок завантаження **Boot Order**. Ви можете налаштувати розмір оперативної пам'яті RAM (рис. 13.10). Чим більше оперативної пам'яті ви призначаєте віртуальній машині, тим кращу продуктивність (теоретично) можна очікувати від віртуальної машини. Однак, оскільки віртуальна машина споживає фактичну оперативну пам'ять на головному комп'ютері (вашому ПК), відсутність достатньої кількості оперативної пам'яті, доступної для операційної системи головного комп'ютера, вплине на продуктивність віртуальної машини VM.

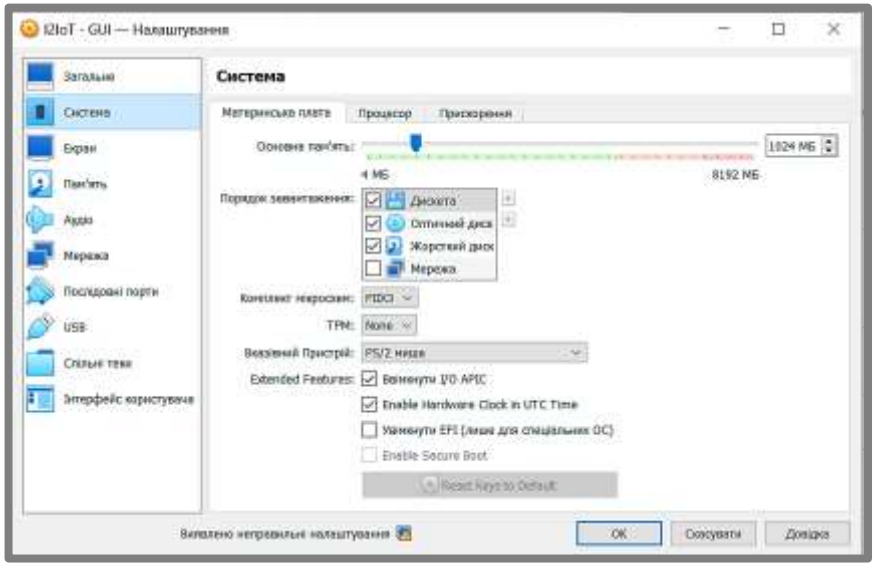


Рисунок 13.10 – Налаштування розміру оперативної пам'яті RAM

5) Натисніть **OK**, щоб закрити налаштування **Settings**.

3.2. Увімкніть віртуальну машину.

1) Натисніть **Start**, щоб увімкнути віртуальну машину VM (рис. 13.11). Якщо машина не запустилася і видала помилку **VT-x is disabled in the BIOS for all CPU modes** (VT-x відключений в BIOS для всіх режимів процесора») потрібно внести зміни в BIOS.

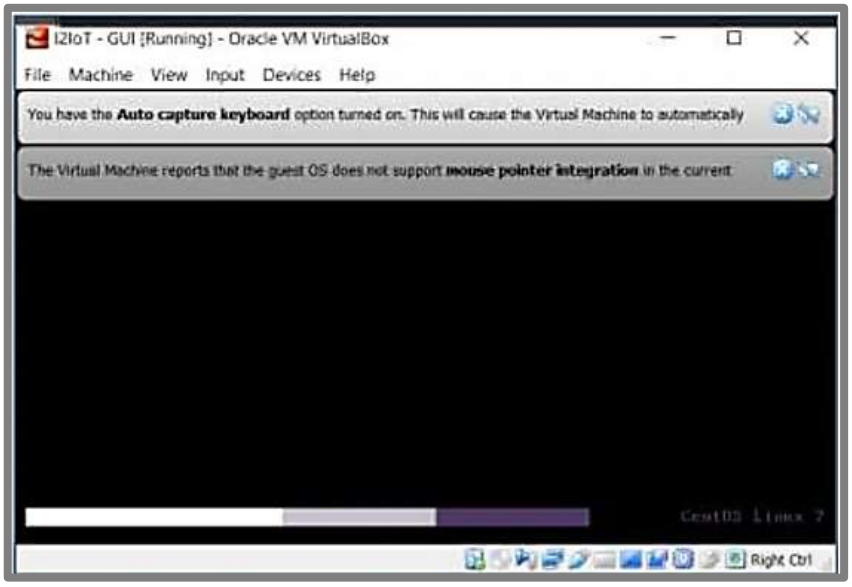


Рисунок 13.11 – Запуск віртуальної машини

2) Після ввімкнення віртуальної машини з'являється вікно входу **Login** (рис. 13.12).

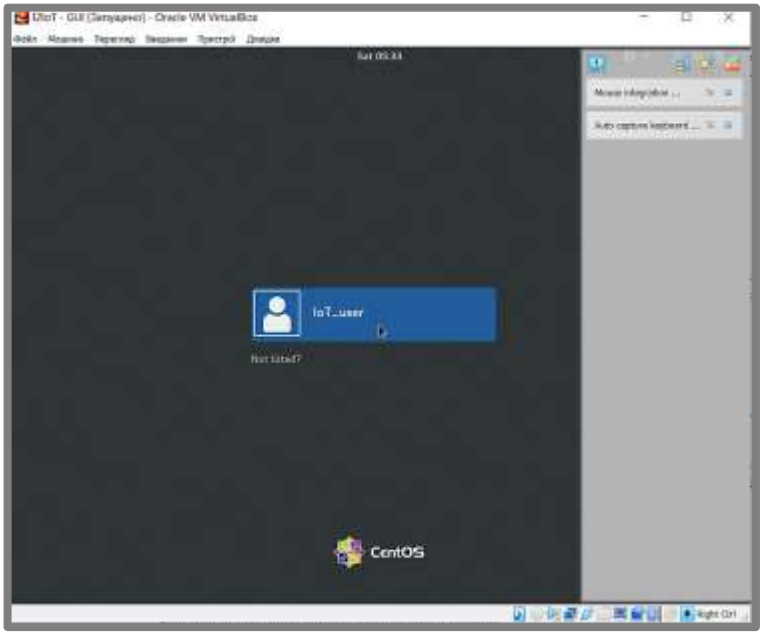


Рисунок 13.12 – Вікно входу

3) Прочитайте два попередження. Ви можете закрити повідомлення, натиснувши піктограму **X**.
4) Натисніть на екран. З'являється повідомлення про роботу мишки (рис. 13.13):

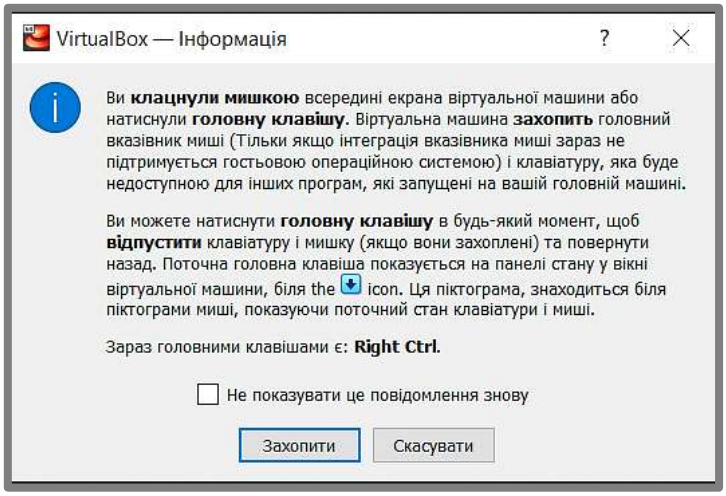


Рисунок 13.13 – Повідомлення про роботу мишки

Щоби продовжити, потрібно натиснути **Capture** (Захопити). Якщо ви більше не бажаєте бачити це повідомлення, ви можете поставити прапорець **Do not show this message again** (Не показувати це повідомлення знову), перш ніж натиснути **Capture.** Згідно з повідомленням, кожного разу, коли ви клацаєте на екрані віртуальної машини, віртуальна машина захоплює вказівник миші, що означає, що рух миші відбувається в межах екрана віртуальної машини. Щоби повернути вказівник миші на головний комп’ютер, ви можете натиснути клавішу **Host**, яка за замовчуванням визначена як **Right Ctrl**.

5) Віртуальна машина ввімкнула функцію заставки (рис. 13.14). Якщо VM не активна упродовж 5 хвилин, вікно буде зайнято таким зображенням.

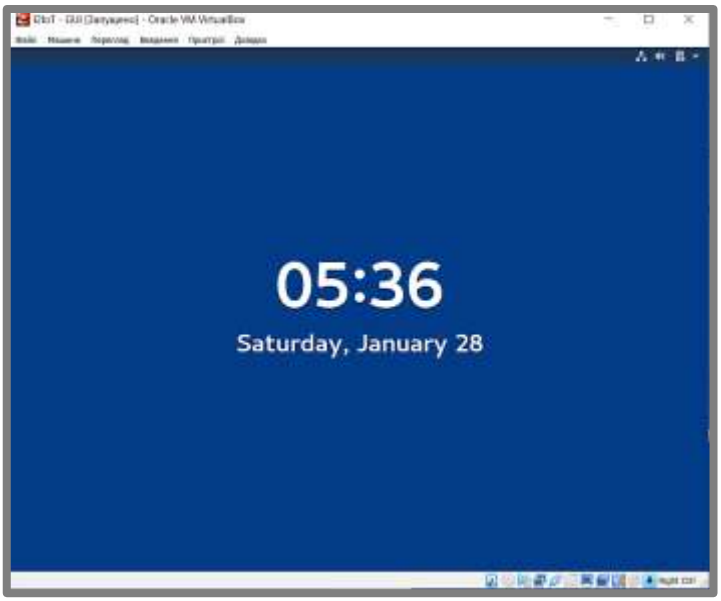


Рисунок 13.14 – Заставка віртуальної машини

6) Щоби потрапити на робочий екран, клацніть у вікні та перемістіть вказівник миші вгору, утримуючи ліву кнопку. Екран входу показано вище під кроком 2.
7) Ім’я користувача за умовчанням – **IoT_user** без пароля. Натисніть синю панель **IoT_user** посередині екрану, щоб увійти у VM (рис. 13.15).

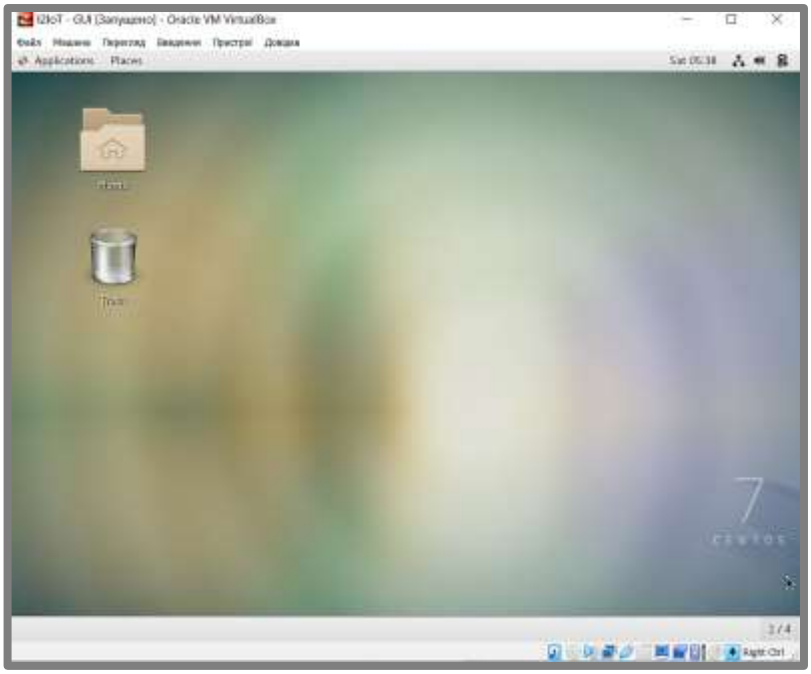


Рисунок 13.15 – Робочий стіл віртуальної машини

8) Як бачите, віртуальна машина працює під керуванням CentOS 7, дистрибутива Linux з відкритим кодом.

4. Основні інструменти навігації в CentOS 7

4.1. Щоби перевірити мережеве підключення, клацніть **Application / Firefox**, потім введіть www.google.com або будь-який вебсайт, який ви виберете. Вебсторінка має відображати (рис. 13.16):

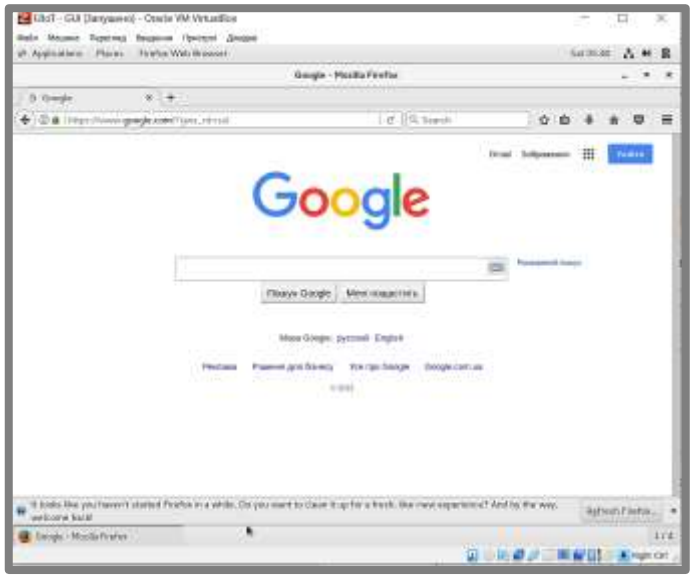


Рисунок 13.16 – Відображення вебсторінки

Якщо вебсайт не вдається підключити, усуньте несправність, переконавшись, що хост-комп'ютер має доступ до того самого вебсайту.

4.2. Щоб одержати доступ до інтерфейсу командного рядка (**CLI**), натисніть **Application / Terminal** (рис. 13.17):

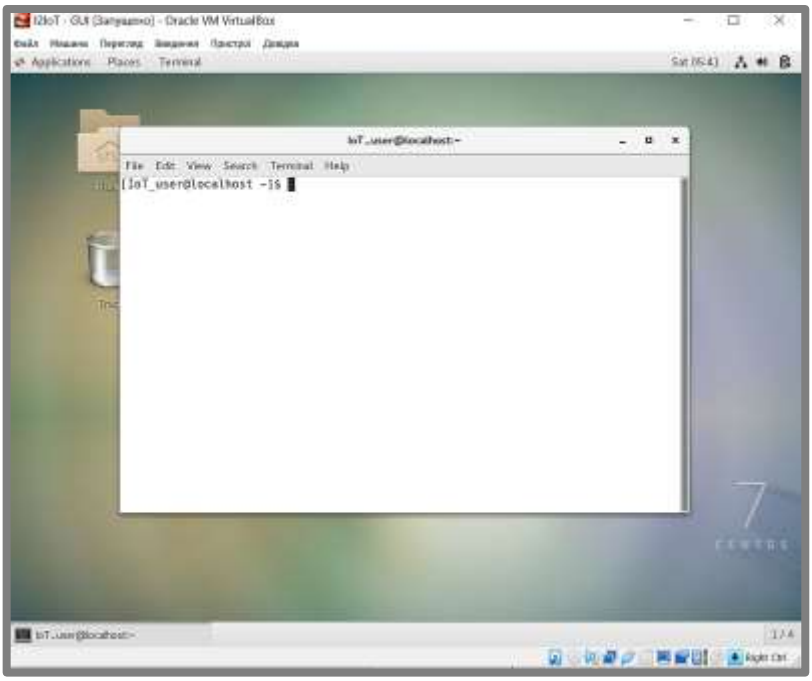
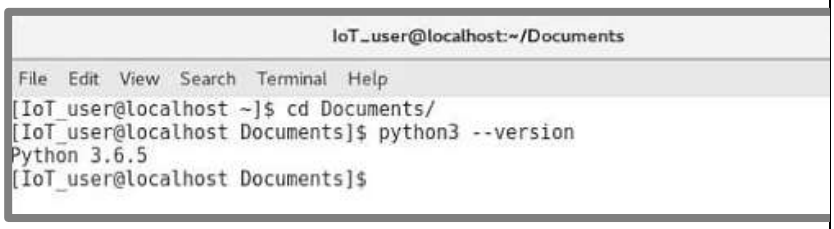


Рисунок 13.17 – Доступ до інтерфейсу командного рядка

Примітка: ви також можете клацнути правою кнопкою миші на робочому столі та вибрати **Open Terminal**.

4.3. Використовуйте команди:

Команду **pwd**, щоб відобразити поточний каталог	IoT_user@localhost:~ File Edit View Search Terminal Help [IoT_user@localhost ~]$ pwd /home/IoT_user [IoT_user@localhost ~]$
Команду **ls** (від List), щоби показати список вмісту в поточному каталозі. Використання команди **ls** із параметром **–l** відобразить детальну інформацію про вміст.	IoT_user@localhost:~ File Edit View Search Terminal Help [IoT_user@localhost ~]$ pwd /home/IoT_user [IoT_user@localhost ~]$ ls Desktop Documents Downloads Music Pictures Public Templates Videos [IoT_user@localhost ~]$ ls -l total 0 drwxr-xr-x. 2 IoT_user IoT_user 6 Apr 16 2018 Desktop drwxr-xr-x. 2 IoT_user IoT_user 6 Apr 16 2018 Documents drwxr-xr-x. 2 IoT_user IoT_user 6 Apr 16 2018 Downloads drwxr-xr-x. 2 IoT_user IoT_user 6 Apr 16 2018 Music drwxr-xr-x. 2 IoT_user IoT_user 6 Apr 16 2018 Pictures drwxr-xr-x. 2 IoT_user IoT_user 6 Apr 16 2018 Public drwxr-xr-x. 2 IoT_user IoT_user 6 Apr 16 2018 Templates drwxr-xr-x. 2 IoT_user IoT_user 6 Apr 16 2018 Videos

Команду **cd Documents**, щоби змінити каталог на /home/IoT_user/Documents. Перевірте за допомогою команди **pwd**.	
Команду **python3 –version**, щоб перевірити версію Python, встановлену на віртуальній машині	

4.6. Щоб вийти з вікна **Terminal**, скористайтеся командою **exit**.

4.7. Щоб вимкнути віртуальну машину, клацніть піктограму батареї у верхньому правому куті (рис.13.18), потім кнопку живлення та виберіть **power off**.

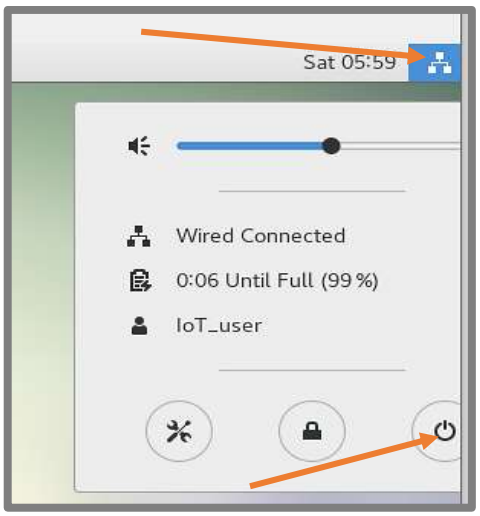


Рисунок 13.18 – Вимкнення віртуальної машини

5. Основи програмування на Python

Python, мова програмування, яка дає можливість створювати простіші оператори. Python дуже простий у використанні, потужний і універсальний. Програма стала мовою вибору для багатьох розробників IoT. Однією з головних причин популярності Python є спільнота розробників. Розробники Python

створили та зробили доступними багато спеціальних модулів, які можна імпортувати в будь-яку програму, щоб негайно надати додаткові функції.

5.1. Програмування Python в інтерактивному інтерпретаторі

Як інтерпретована мова, команди Python можна видавати в інтерактивному інтерпретаторі:

1) Використовуйте команду **python3**, щоб запустити інтерпретатор Python (рис. 13.19).

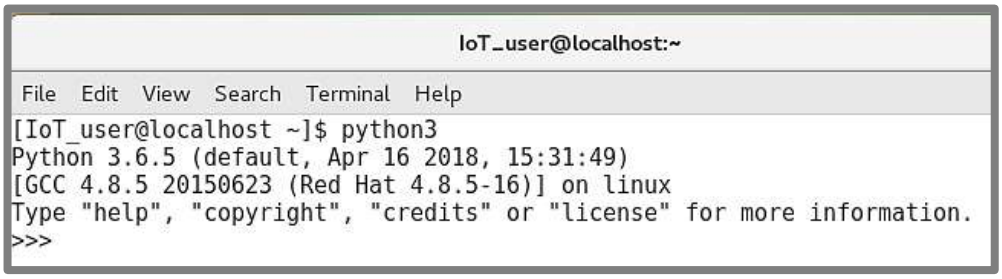


Рис 13.19 – Запуск інтерпретатора Python

2) Виконайте обчислення.

```
>>> 1 + 2
3
>>> 2 * 4
8
>>> 6 / 2
3.0
>>>
```

3) Надрукуйте текстовий рядок.

```
>>> “How are you?”
‘How are you?’
>>>
```

4) Використовуйте команду **type()**, щоб визначити базовий тип даних: int, float, string, Boolean.

```
>>> type(65)
```

```
<class 'int'>
>>> type(45.6)
<class 'float'>
>>> type("Hi!")
<class 'str'>
>>> type(True)
<class 'bool'>
>>> 1<2 True >>> 1<1 False >>> 1==1
True
>>> 1>=1
True
>>>
```

5) Створіть змінну.

```
>>> x=3
>>> x*5
15
>>> "Good!"*x
'Good!Good!Good!'
>>>
```

6) Об'єднайте кілька рядків разом і надрукуйте як один рядок.

```
>>> str1="Cisco"
>>> str2="Networking"
>>> str3="Academy"
>>> space=" "
>>> print(str1+space+str2+space+str3)
Cisco Networking Academy
>>>
```

7) Перетворення типу даних із числового числа на рядок.

```
>>> x=5
>>> str(x)
```

```
>>> '5'
>>> y=4.2
>>> str(y)
>>> y='4.2'
>>>
```

8) Зауважте, що цілі числа не округлюються в більшу сторону під час перетворення із числа з плаваючою точкою. Десяткові значення – ігноруються.

```
>>> int(8.21)
8
>>> int(8.99)
8
>>> int(8.21) + int(8.99)
16
>>>
```

9) Перетворення цілого числа на число з плаваючою точкою.

```
>>> x=5
>>> x
5
>>> float(x)
5.0
>>> type(x)
<class 'int'>
>>> x=float(x)
>>> type(x)
<class 'float'>
>>> x
5.0
>>>
```

10) Отримайте дані користувача.

```
>>> name=input("What is your name? ")
What is your name? John
>>> print("Hi " + name + ", it is nice to meet you!")
Hi John, it is nice to meet you!
>>>
```

11) Використовуйте **quit()**, щоб вийти з інтерактивного інтерпретатора.

5.2. IDLE для Python

IDLE (Integrated Development and Learning Environment) підтримується та включений у пакет Python. Ось кілька ключових функцій IDLE для Python:

- Вікно оболонки Python (interactive interpreter) із розфарбуванням введення, виведення та повідомлень про помилки.
- Багатовіконний текстовий редактор із множинним скасуванням, розфарбуванням Python, розумним відступом, підказками для виклику, автозавершенням та іншими функціями.
- Можливість пошуку в будь-якому вікні, заміни у вікнах редактора та пошуку в кількох файлах (grep).
- Налагоджувач із постійними точками зупинки, кроками та переглядом глобальних і локальних просторів імен.
- Конфігурація, браузери та інші діалогові вікна

1) Щоб запустити IDLE використайте команду **idle3** (рис. 13.20). За замовчуванням він запускається у вікні Python Shell або інтерактивного інтерпретатора.

```
[IoT_user@stueverj-vm2 Documents]$ idle3
```

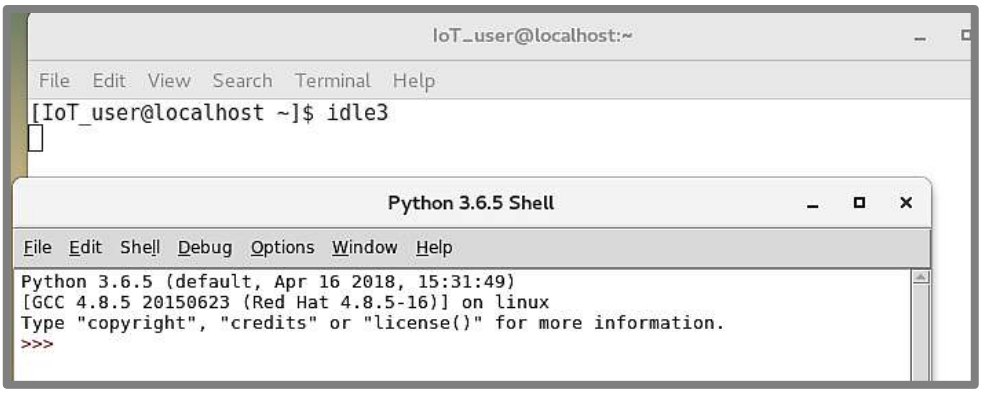


Рисунок 13.20 – Запуск IDLE

2) Натисніть **File / New File**, щоб відкрити новий (без назви) сценарій Python (рис. 13.21).



Рисунок 13.21 – Створення нового сценарію

3) Введіть код у сценарій **print («Hello World!»)**, зверніть увагу, що коди пофарбовані, а відкриваючі та закриваючі дужки збігаються (рис. 13.22).



Рисунок 13.22 – Відображення коду

4) Натисніть **File / Save**, збережіть поточний сценарій як **1.py** у поточному каталозі. Натисніть кнопку **Save** (рис. 13.23).



Рисунок 13.23 – Збереження поточного сценарію

5) Натисніть **Run / Run Module** (або натисніть **F5**). У вікні оболонки буде показано результат (рис. 13.24).

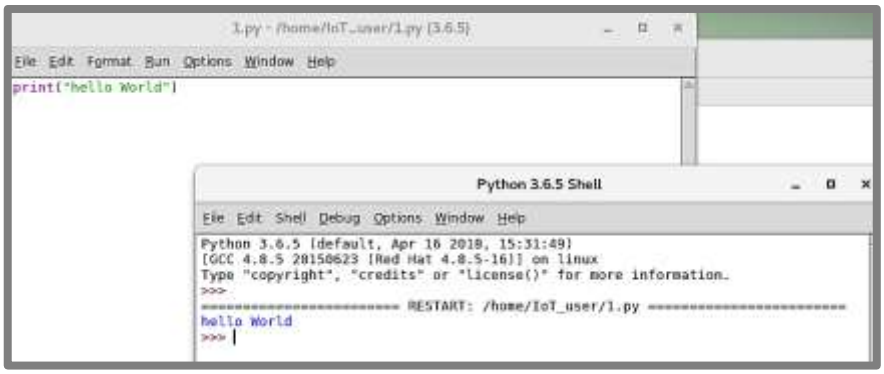


Рисунок 13.24 – Відображення результату написання коду

5.3. Створення простої гри за допомогою Python IDLE

Створіть просту гру за допомогою Python IDLE. Мета гри полягає в тому, щоб знайти число, вибране гравцем, у межах від 0 до 1024 методом ділення навпіл.

1) Запустити IDLE використовуючи команду **idle3**.

```
[ IoT_user@stueverj-vm2 Документи]$ idle3
```

2) Натисніть **File / New File**, щоб відкрити новий (без назви) сценарій Python.
3) Введіть коди в сценарій та зверніть увагу, що коди позначено кольором зі збігом відкритих і закритих дужок (рис.13.25).

```
x=input("Enter an integer between 0 and 1024 --")
```

```
x=int(x)
a=0
b=1024
test=True
if x == 0:
	print("Your number is 0, thank you for playing.")
	test=False
else:
	if x == 1024:
		print("Your number is 1024, thank you for playing.")
		test=False

	while test == True:
		m=int((a+b)/2)
		if m == x:
			print("Your number is ", m,", thank you for
playing")
			break
		else:
			if m < x:
				a = m
			else:
				b=m
```

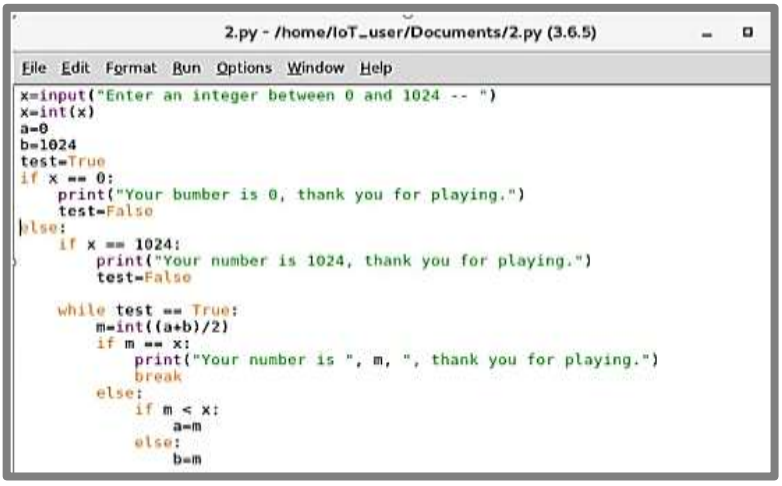


Рисунок 13.25 – Вікно з написаним кодом гри

4) Натисніть **File / Save** та збережіть поточний сценарій як **2.py** у поточному каталозі. Натисніть кнопку **Save**.

5) Натисніть **Run / Run Module** (або натисніть **F5**). У вікні оболонки буде показано результат (рис. 13.26).



Рисунок 13.26 – Вікно з результатами гри

6) Усуньте неполадки, якщо під час оцінювання синтаксису коду виникає помилка.

Як зловити, якщо гравець вводить число за межами діапазону від 0 до 1024?

Відповідь:_____

Як зловити, якщо гравець вводить число з плаваючою комою float?

Відповідь:_____

ВИМОГИ ДО ОФОРМЛЕННЯ ЗВІТУ

1. Сформуйте файл для звіту. Звіт про виконання роботи має включати:

- Титульний аркуш, вказуючи номер і назву роботи, прізвище і групу студента.

- Покроковий опис основних етапів виконання роботи. Отримані результати підтверджуються скріншотами екрана.
- Відповіді на поставлені запитання в завданнях.
- Висновки щодо проведеної роботи.



КОНТРОЛЬНІ ЗАПИТАННЯ

1. Які ви знаєте програми для віртуалізації операційних систем?
2. Охарактеризуйте програмний продукт для віртуалізації операційних систем Oracle VM VirtualBox.
3. Назвіть основні кроки налаштувань для запуску віртуальної операційної системи в програмі Oracle VM VirtualBox.
4. Коротко опишіть основні кроки встановлення віртуальної машини I2IoT у VirtualBox.
5. Які основні характеристики мови програмування Python?
6. Яка функція програмування Python використовується для відображення результату?
7. Який результат очікується, коли функцію (>>>print Cisco 1) введено в програмний інтерпретатор Python?
8. У чому полягає перевага виконуваної програми, закодованої інтерпретованою мовою, над скомпільованою мовою?

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Finardi A. IoT Simulations with Cisco Packet Tracer [online] URL: https://www.theseus.fi/bitstream/handle/10024/150158/Andrea%20Finardi%20%20Master%20of%20Engineering%20%20Information%20technology.pdf
2. Flavio Bonomi, Rodolfo Milito, Jiang Zhu, Sateesh Addepalli. Fog Computing and Its Role in the Internet of Things [online] URL: http://conferences.sigcomm.org/sigcomm/2012/paper/mcc/p13.pdf
3. Introduction to IoT (Cisco Networking Academy) [online] URL: https://www.netacad.com.
4. IoT Fundamentals Big Data & Analytics (Cisco Networking Academy) [online] URL: https://www.netacad.com.
5. Leading the IoT [online] URL: https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf
6. Things and Components available in Packet Tracer 7.2 [online] URL: https://www.packettracernetwork.com/internet-of-things/pt7-iotdevices-configuration.html
7. Top cloud security controls you should be using [online] URL: https://www.csoonline.com/article/3208905/cloud-security/top-cloudsecurity-controls-you-should-be-using.html
8. IoT Fundamentals Connecting Things (Cisco Networking Academy) [online] URL: https://www.netacad.com.
9. Python data analysis library [online] URL: https://pandas.pydata.org
10. Changing the programming paradigm for the embedded in the IoT domain [online] URL: http://ieeexplore.ieee.org/document/7389059/?arnumber=7389059