Міністерство освіти і науки України
Луцький національний технічний університет

ІНЖЕНЕРІЯ ІНТЕРНЕТУ РЕЧЕЙ

Методичні вказівки до лабораторних занять
для здобувачів першого (бакалаврського) рівня вищої освіти
освітньої програми «Комп'ютерна інженерія»
галузь знань 12 Інформаційні технології
спеціальності 123 Комп’ютерна інженерія
денної та заочної форм навчання

Луцьк 2025

УДК 004.738.5
У І-73

Рекомендовано до видання вченою радою факультету КІТ ЛНТУ,
протокол № _____ від «___ » _____ 20 25 року.

Голова вченої ради факультету КІТ _____ Інна КОНДІУС

Електронна копія друкованого видання передана для внесення в репозитарій ЛНТУ
Директор бібліотеки _____ Наталія ПОЛІЩУК

Розглянуто і схвалено на засіданні кафедри комп'ютерної інженерії та безпеки ЛНТУ, протокол № _____ від « _____ » _____ 20 25 року.

Завідувач кафедри КІБ _____ Тарас ТЕРЛЕЦЬКИЙ

Укладачі: _____ Микола ПОЛІЩУК, кандидат технічних наук, доцент, кафедри комп'ютерної інженерії та безпеки ЛНТУ

Рецензент: _____ Сергій КОСТЮЧКО, кандидат технічних наук, доцент кафедри комп'ютерної інженерії та безпеки ЛНТУ

_____ Анатолій ТКАЧУК, кандидат технічних наук, доцент кафедри електроніки та телекомунікацій

Відповідальний за випуск: _____ Тарас ТЕРЛЕЦЬКИЙ, кандидат технічних наук, доцент кафедри комп'ютерної інженерії та безпеки ЛНТУ

У І-73 Інженерія Інтернету Речей: методичні вказівки до лабораторних занять для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Комп'ютерна інженерія» галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія денної та заочної форм навчання / уклад. М. М. Поліщук : ЛНТУ, 2025. 98 с.

Методичне видання до практичних занять з дисципліни «Інженерії Інтернету Речей»: складене відповідно до діючої програми курсу.

Призначене для здобувачів вищої освіти спеціальності 123 Комп'ютерна інженерія освітньої програми «Комп'ютерна інженерія».

М. М. Поліщук 2025

ЗМІСТ

ВСТУП

Сучасна цифрова епоха визначається стрімким розвитком технологій, серед яких Інтернет речей (Internet of Things, IoT) займає провідне місце. IoT формує нову парадигму взаємодії між фізичним та цифровим світами, забезпечуючи збирання, обробку, передачу та аналіз даних у режимі реального часу. Ці технології знаходять застосування в розумних будинках, промисловості, транспорті, медицині, аграрному секторі, енергетиці тощо.

Метою дисципліни «Інженерія Інтернету речей» є формування у студентів практичних навичок проєктування, реалізації та тестування IoT-рішень, а також розуміння архітектурних принципів, протоколів, засобів зв’язку та безпеки в IoT-системах.

Методичні вказівки до лабораторних робіт містять структурований набір практичних завдань, що охоплюють ключові аспекти IoT-інженерії: підключення сенсорів до мікроконтролерів, передача даних через мережеві протоколи (MQTT, HTTP), робота з хмарними платформами та розробка простих IoT-додатків.

Виконання лабораторного практикуму сприятиме формуванню у студентів необхідних компетентностей у галузі інженерії IoT, що є затребуваними у сучасних індустріях та відповідають потребам ринку праці.

МЕТА ТА ЗАВДАННЯ КУРСУ «ІНТЕРНЕТ РЕЧЕЙ»

Метою викладання дисципліни «Інтернету Речей» призначена для формування у слухачів комплексу професійних знань, вмінь та навичок із впровадження сучасних розумних цифрових технологій Інтернету речей (IoT), організації, проектування та налаштування інтелектуальних комп'ютерних систем і мереж з розумними пристроями (IoT).

Основними завданнями вивчення дисципліни є:

– ознайомлення зі станом проектування та використання технологій проектування систем IoT в Україні та світі;

– здатність проектувати та аналізувати ефективність засобів захисту та управління безпекою в програмно-апаратних рішеннях Інтернету речей;

– уміння створювати і застосовувати інформаційні комп'ютерні системи відповідно до сучасних концепцій інженерії даних і знань;

– здатність мотивувати студентів та рухатися до спільної мети, працюючи в команді.

Найменування та опис компетентностей, формування яких забезпечує вивчення дисципліни «Інженерія Інтернет Речей»:

– загальні компетентності:

ЗК01. Здатність до абстрактного мислення, аналізу і синтезу.

ЗК04. Здатність спілкуватися державною мовою як усно, так і письмово.

ЗК07. Вміння виявляти, ставити та вирішувати проблеми.

– Спеціальні (фахові, предметні) компетентності

СК03. Здатність створювати системне та прикладне програмне забезпечення комп'ютерних систем та мереж.

СК05. Здатність використовувати засоби і системи автоматизації проектування до розроблення компонентів комп'ютерних систем та мереж, Інтернет додатків, кіберфізичних систем тощо.

СК06. Здатність проектувати, впроваджувати та обслуговувати комп'ютерні системи та мережі різного виду та призначення.

СК07. Здатність використовувати та впроваджувати нові технології, включаючи технології розумних, мобільних, зелених і безпечних обчислень, брати участь в модернізації та реконструкції комп’ютерних систем та мереж, різноманітних вбудованих і розподілених додатків, зокрема з метою підвищення їх ефективності.

СК19. Здатність розробляти та впроваджувати як апаратні, так і програмні рішення для комп'ютерних, вбудованих і розподілених систем, включаючи системи Інтернету речей, а також їхні складові компоненти

Програмні результати навчання:

ПРН01. Знати і розуміти наукові положення, що лежать в основі функціонування комп’ютерних засобів, систем та мереж.

ПРН03. Знати новітні технології в галузі комп’ютерної інженерії.

ПРН04. Знати та розуміти вплив технічних рішень в суспільному, економічному, соціальному і екологічному контексті.

ПРН06. Вміти застосовувати знання для ідентифікації, формулювання і розв’язування технічних задач спеціальності, використовуючи методи, що є найбільш придатними для досягнення поставлених цілей.

ПРН07. Вміти розв’язувати задачі аналізу та синтезу засобів, характерних для спеціальності.

ПРН08. Вміти системно мислити та застосовувати творчі здібності до формування нових ідей.

ПРН09. Вміти застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації програмно-технічних засобів комп’ютерних систем та мереж для вирішення технічних задач спеціальності.

ПРН13. Вміти ідентифікувати, класифікувати та описувати роботу комп’ютерних систем та їх компонентів.

ПРН14. Вміти поєднувати теорію і практику, а також приймати рішення та виробляти стратегію діяльності для вирішення завдань спеціальності з урахуванням загальнолюдських цінностей, суспільних, державних та виробничих інтересів.

ПРН22. Вміти створювати та використовувати як апаратне, так і програмне забезпечення для комп'ютерів, вбудованих систем і систем Інтернету речей, включаючи їх складові елементи.

ПРН24. Вміти створювати та використовувати як апаратне, так і програмне забезпечення для комп'ютерів, вбудованих систем і систем Інтернету речей, включаючи їх складові елементи.

ЛАБОРАТОРНА РОБОТА 1
СКЛАДАННЯ КАРТКИ МЕРЕЖІ ІНТЕРНЕТ

Завдання

Частина 1. Перевірка підключення за допомогою команди ping.

Частина 2. Трасування маршруту до віддаленого сервера за допомогою команди Windows tracert.

Частина 3. Трасування маршруту до віддаленого сервера за допомогою програмних та веб-інструментів.

Частина 4. Порівняння результатів команди traceroute**.**

Необхідні ресурси

Один комп'ютер з доступом до Інтернету.

Частина 1. Перевірка підключення за допомогою команди ping

Крок 1. Визначте, чи доступний віддалений сервер.

Для трасування маршруту до віддаленої мережі ПК, що використовується, повинен бути підключений до Інтернету.

1. Спочатку ми скористаємося утилітою ping. p align="justify"> Команда ping служить для перевірки доступності хоста. Пакети даних надсилаються на віддалений хост з вимогою відповіді. Локальний ПК визначає, чи отримано відповідь для кожного пакета, і оцінює, скільки часу зайняло пересилання цих пакетів через мережу. Назва ping надійшла з технології активної гідролокації, де вона позначає підводний звуковий сигнал, який відбивається від дна та інших кораблів.

2. На комп'ютері виконайте пошук «cmd» (рис. 1.1).

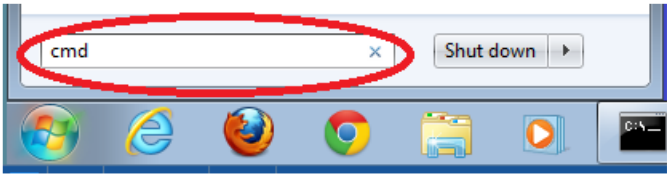


Рисунок 1.1 – Пошук «cmd»

3. Введіть ping Error! Hyperlink reference not valid. у командному рядку (рис. 1.2).

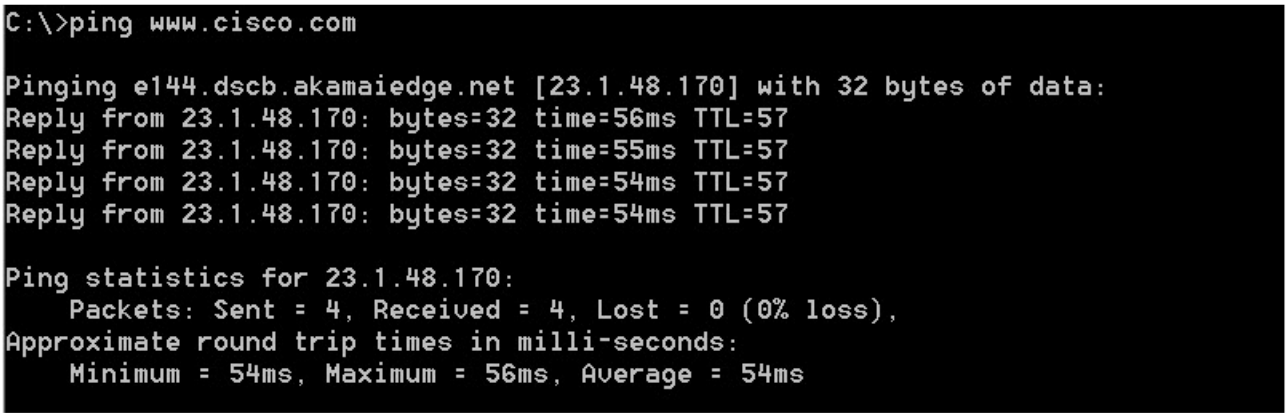


Рисунок 1.2 – Командний рядок

4. У першому рядку отриманих даних відображається повне доменне ім'я (FQDN): e144.dscb.akamaiedge.net. Потім слідує IP-адреса: 23.1.48.170. Веб-вузли компанії Cisco, що містять ту саму інформацію, розміщуються на різних серверах (так званих дзеркалах) по всьому світу. Таким чином, залежно від вашого розташування, FQDN та IP-адреса будуть різними.

5. Візьмемо наведену нижче частину одержаних результатів (рис. 1.3).

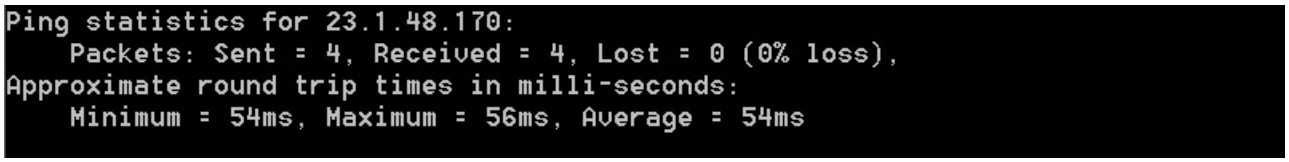


Рисунок 1.3 – Одержані результати

Було надіслано чотири ехо-запити, і на кожен з них було отримано відповідь. Отже, втрата пакетів становила 0%. У середньому для передачі пакетів через мережу потрібно 54 мс (мілісекунди). Мілісекунда – це 1/1000 секунди.

Від втрати пакетів або повільного мережного підключення в першу чергу страждає якість потокового відео та онлайн-ігор. Для того щоб визначити швидкість інтернет-підключення точніше, можна відправити не 4 ехо-запити, передбачені за замовчуванням, а 100. Для цього використовується вказана нижче команда (рис.1.4).

Рисунок 1.4 – Команда «ping»

Вихідні дані будуть виглядати так, як на рисунку 1.5.

```
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 1.5 – Вихідні дані

5. Тепер надішліть ехо-запит на веб-сайти регіонального інтернет-реєстратора (Regional Internet Registry, RIR), розташовані в різних частинах світу.

Африка: C:\> ping www.afrinic.net (рис. 1.6).

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

Pinging www.afrinic.net [196.216.2.136] with 32 bytes of data:
Reply from 196.216.2.136: bytes=32 time=314ms TTL=111
Reply from 196.216.2.136: bytes=32 time=312ms TTL=111
Reply from 196.216.2.136: bytes=32 time=313ms TTL=111
Reply from 196.216.2.136: bytes=32 time=313ms TTL=111

Ping statistics for 196.216.2.136:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 312ms, Maximum = 314ms, Average = 313ms
```

Рисунок 1.6 – Веб-сайти регіонального інтернет-реєстратора для Африки

Австралія: C:\> ping www.apnic.net (рис. 1.7).

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

Pinging www.apnic.net [202.12.29.194] with 32 bytes of data:
Reply from 202.12.29.194: bytes=32 time=286ms TTL=49
Reply from 202.12.29.194: bytes=32 time=287ms TTL=49
Reply from 202.12.29.194: bytes=32 time=286ms TTL=49
Reply from 202.12.29.194: bytes=32 time=286ms TTL=49

Ping statistics for 202.12.29.194:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 286ms, Maximum = 287ms, Average = 286ms
```

Рисунок 1.7 – Веб-сайти регіонального інтернет-реєстратора для Австралії

Європа: C:\> ping www.ripe.net (рис. 1.8).

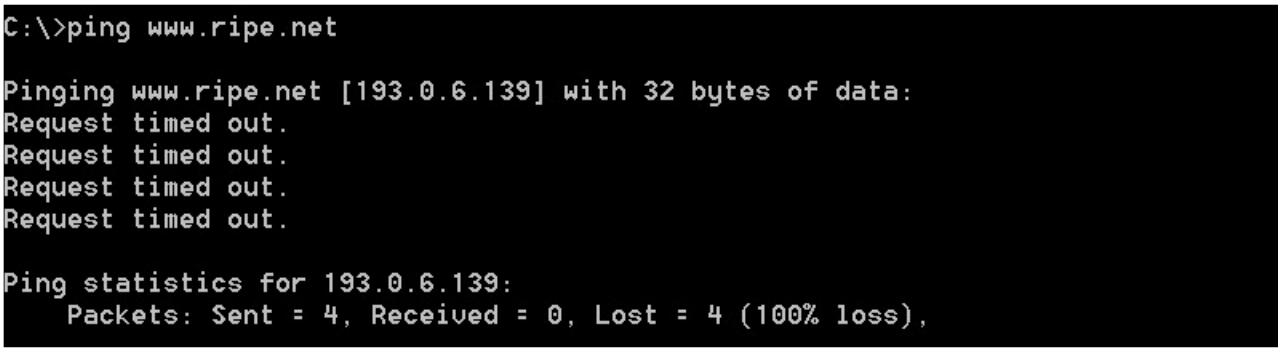


Рисунок 1.8 – Веб-сайти регіонального інтернет-реєстратора для Європи

Південна Америка: C:\> ping www.lacnic.net (рис. 1.9).

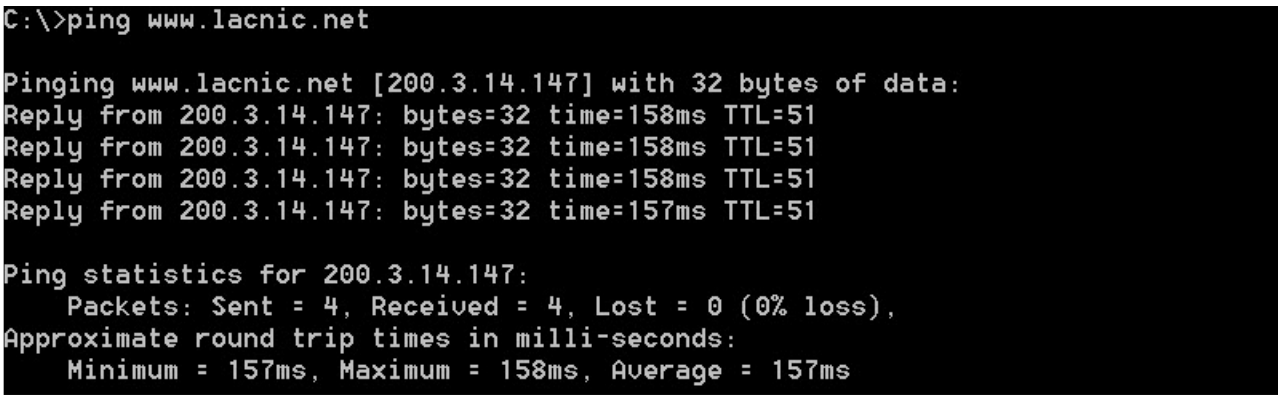


Рисунок 1.9 – Веб-сайти регіонального інтернет-реєстратора для Південної Америки

Питання для самоконтролю:

1. Усі ці команди ping виконуються з комп'ютера, що у США. За який час виконується команда ping (мілісекунди), коли дані передаються в межах одного континенту (Північної Америки), а також коли дані з Північної Америки пересилаються на інші континенти?

2. Що цікавого можна сказати про луна-запити, надіслані на європейський сайт?

Частина 2. Трасування маршруту на віддалений сервер за допомогою команди tracert

Крок 1. Визначте, який маршрут із усього інтернет-трафіку спрямований на віддалений сервер.

Перевіривши доступність сервера за допомогою утиліти ping, варто уважніше

розглянути кожен сегмент мережі, через який проходять дані. Для цього ми скористаємося утилітою tracert.

1. Введіть tracert www.cisco.com у командному рядку (рис. 1.10).

Рисунок 1.10 – Введення tracert www.cisco.com у командному рядку

2. Збережіть результати, отримані після виведення команди tracert, у текстовому файлі, виконавши такі дії:

– Натисніть правою кнопкою миші на рядок заголовка вікна командного рядка та виберіть Правка > Виділити все.

– Ще раз натисніть правою кнопкою миші на рядок заголовка вікна командного рядка та виберіть Правка > Копіювати.

– Знайдіть та відкрийте Блокнот.

– Щоб вставити результат у Блокнот, виберіть меню Правка > Вставити.

– У меню Файл виберіть команду Зберегти як і збережіть файл Блокнота на робочий стіл під ім'ям tracert1.txt.

3. Запустіть утиліту tracert для кожного веб-сайту призначення та збережіть отримані результати у послідовно пронумеровані файли.

C:\> tracert www.afrinic.net

C:\> tracert www.lacnic.net

4. Інтерпретуйте дані, отримані за допомогою утиліти tracert.

Залежно від зони охоплення вашого інтернет-провайдера та розташування вузлів джерела та призначення відстежені маршрути можуть перетинати безліч переходів та мереж. Кожен «перехід» - це один маршрутизатор.

Оскільки комп'ютери спілкуються мовою цифр, а не слів, маршрутизаторам надаються унікальні IP-адреси (числа у форматі x.x.x.x для IPv4). Інструмент tracert показує, яким шляхом проходить пакет даних до кінцевого пункту призначення. Крім того, за допомогою утиліти tracert можна визначити з якою швидкістю проходить трафік через кожен сегмент мережі. Кожному маршрутизатору на шляху проходження даних відправляються три пакети, час відповіді на які вимірюється в мілісекундах. Використовуючи цю інформацію, проаналізуйте результати, отримані за допомогою утиліти tracert під час надсилання пакетів до www.cisco.com. На рисунку 1.11 наведено весь маршрут трасування та деталізовано (рис. 1.12).

```
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 1.11 – Маршрут трасування

Рисунок 1.12 – Деталізований маршрут трасуваня

У наведеному вище прикладі пакети, відправлені утилітою tracert,

пересилаються з ПК джерела на шлюз за промовчанням локального маршрутизатора (перехід 1: 192.168.1.1), а потім на маршрутизатор у точці присутності (POP) до інтернет-провайдера (перехід 2:10).). Кожен провайдер має безліч маршрутизаторів POP. Вони відзначають межі мережі інтернет-провайдера і є точками підключення до Інтернету для клієнтів. Пакети проходять через два переходи в мережі Verizon і потрапляють до маршрутизатора, що належить alter.net. Це може означати, що пакети досягли іншого інтернет-провайдера. Цей момент дуже важливий, оскільки при пересиланні пакетів від одного до іншого провайдеру можливі втрати, а також важливо пам'ятати, що не всі інтернет-провайдери здатні забезпечити однакову швидкість передачі даних.

Існує інтернет-сервіс під назвою whois. Сервіс whois дозволяє з'ясувати, кому належить доменне ім'я. Веб-сервіс whois знаходиться за адресою: http://whois.domaintools.com/. Згідно з інформацією, отриманою за допомогою whois, цей домен також належить компанії Verizon.

```
Registrant:
        Verizon Business Global LLC
        Verizon Business Global LLC
        One Verizon Way
         Basking Ridge NJ 07920
        US
         domainlegalcontact@verizon.com +1.7033513164 Fax: +1.7033513669

    Domain Name: alter.net
```

Отже, інтернет-трафік починається на домашньому ПК та проходить через домашній маршрутизатор (перехід 1). Потім дані надходять до інтернет-провайдера і передаються через його мережу (переходи 2–7), поки не досягнуто віддаленого сервера (перехід 8). Це досить нетиповий приклад, тому що від початку до кінця маршруту задіяно лише один провайдер. Як правило, буває два або кілька Інтернет-провайдерів, як показано в наведених нижче прикладах.

5. Тепер розглянемо приклад із пересиланням інтернет-трафіку через кілька інтернет-провайдерів. Нижче наведено результати команди tracert для www.afrinic.net (рис. 1.3).

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

Tracing route to www.afrinic.net [196.216.2.136]
over a maximum of 30 hops:

  1     1 ms    <1 ms    <1 ms  dslrouter.westell.com [192.168.1.1]
  2    39 ms    38 ms    37 ms  10.18.20.1
  3    40 ms    38 ms    39 ms  G4-0-0-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.197.182]
  4    44 ms    43 ms    43 ms  so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5    43 ms    43 ms    42 ms  0.so-4-0-0.XT2.NYC4.ALTER.NET [152.63.9.249]
  6    43 ms    71 ms    43 ms  0.ae4.BR3.NYC4.ALTER.NET [152.63.16.185]
  7    47 ms    47 ms    47 ms  te-7-3-0.edge2.NewYork2.level3.net [4.68.111.137
]
  8    43 ms    55 ms    43 ms  vlan51.ebr1.NewYork2.Level3.net [4.69.138.222]
  9    52 ms    51 ms    51 ms  ae-3-3.ebr2.Washington1.Level3.net [4.69.132.89]

 10   130 ms   132 ms   132 ms  ae-42-42.ebr2.Paris1.Level3.net [4.69.137.53]
 11   139 ms   145 ms   140 ms  ae-46-46.ebr1.Frankfurt1.Level3.net [4.69.143.13
7]
 12   148 ms   140 ms   152 ms  ae-91-91.csw4.Frankfurt1.Level3.net [4.69.140.14
]
 13   144 ms   144 ms   146 ms  ae-92-92.ebr2.Frankfurt1.Level3.net [4.69.140.29
]
 14   151 ms   150 ms   150 ms  ae-23-23.ebr2.London1.Level3.net [4.69.148.193]

 15   150 ms   150 ms   150 ms  ae-58-223.csw2.London1.Level3.net [4.69.153.138]

 16   156 ms   156 ms   156 ms  ae-227-3603.edge3.London1.Level3.net [4.69.166.1
54]
 17   157 ms   159 ms   160 ms  195.50.124.34
 18   353 ms   340 ms   341 ms  168.209.201.74
 19   333 ms   333 ms   332 ms  csw4-pkl-gi1-1.ip.isnet.net [196.26.0.101]
 20   331 ms   331 ms   331 ms  196.37.155.180
 21   318 ms   316 ms   318 ms  fa1-0-1.ar02.jnb.afrinic.net [196.216.3.132]
 22   332 ms   334 ms   332 ms  196.216.2.136

Trace complete.
```

Рисунок 1.13 – Результати команди tracert для www.afrinic.net

Питання для самоконтролю:

1. Що відбувається на переході 7? Чи належить level3.net тому ж інтернет-провайдеру, що переходи 2-6? Для відповіді на це запитання скористайтесь інструментом whois.
2. Як змінюється час, необхідний для пересилання пакета даних між Вашингтоном та Парижем (перехід 10) порівняно з переходами 1–9?
3. Що відбувається на переході 18? За допомогою whois здійсніть пошук за адресою 168.209.201.74. Хто є власником цієї мережі?

6. Введіть tracert www.lacnic.net. Що відбувається на переході 7?

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

Tracing route to www.lacnic.net [200.3.14.147]
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    38 ms    38 ms    39 ms  G3-0-9-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.196.190]
  4    42 ms    43 ms    42 ms  so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5    82 ms    47 ms    47 ms  0.ae2.BR3.NYC4.ALTER.NET [152.63.16.49]
  6    46 ms    47 ms    56 ms  204.255.168.194
  7   157 ms   158 ms   157 ms  ge-1-1-0.100.gw1.gc.registro.br [159.63.48.38]
  8   156 ms   157 ms   157 ms  xe-5-0-1-0.core1.gc.registro.br [200.160.0.174]

  9   161 ms   161 ms   161 ms  xe-4-0-0-0.core2.nu.registro.br [200.160.0.164]

 10   158 ms   157 ms   157 ms  ae0-0.ar3.nu.registro.br [200.160.0.249]
 11   176 ms   176 ms   170 ms  gw02.lacnic.registro.br [200.160.0.213]
 12   158 ms   158 ms   158 ms  200.3.12.36
 13   157 ms   158 ms   157 ms  200.3.14.147

Trace complete.
```

Частина 3. Прокладіть маршрут до віддаленого сервера за допомогою програмних засобів та інструментів, розміщених в Інтернеті.

Крок 1. Скористайтеся веб-засобом для трасування маршруту.

1. За допомогою http://www.subnetonline.com/pages/network-tools/online-tracepath.php прокладіть маршрут до наступних веб-сайтів:

www.cisco.com
www.afrinic.net
Скопіюйте дані та збережіть їх у файл Блокнота.

```
www.cisco.com:
Вихідні дані запитів TracePath:
1: pera.subnetonline.com (141.138.203.105) 0.157ms pmtu 1500
1: gw-v130.xl-is.net (141.138.203.1) 1.168ms
2: rt-eu01-v2.xl-is.net (79.170.92.19) 0.566ms
3: akamai.telecity4.nl-ix.net (193.239.116.226) 1.196ms

www.afrinic.com:
Вихідні дані запитів TracePath:

1: pera.subnetonline.com (141.138.203.105) 0.175ms pmtu 1500
1: gw-v130.xl-is.net (141.138.203.1) 0.920ms
2: rt-eu01-v2.xl-is.net (79.170.92.19) 0.556ms
3: xl-internetservices.nikhef.openpeering.nl (217.170.0.225) 10.679ms
4: r22.amstnl02.nl.bb.gin.ntt.net (195.69.144.36) asymm 5 4.412ms
5: ae-5.r23.londen03.uk.bb.gin.ntt.net (129.250.5.197) 49.349ms
```

```
6: ae-2.r02.londen03.uk.bb.gin.ntt.net (129.250.5.41) asymm 7 8.842ms
7: dimensiondata-0.r02.londen03.uk.bb.gin.ntt.net (83.231.235.222) 18.080ms
8: 168.209.201.74 (168.209.201.74) 196.375ms
9: csw4-pkl-gi1-1.ip.isnet.net (196.26.0.101) asymm 10 186.855ms
10: 196.37.155.180 (196.37.155.180) 185.661ms
11: fa1-0-1.ar02.jnb.afrinic.net (196.216.3.132) 197.912ms
```

Питання для самоконтролю:

1. Як змінюється трасування маршруту під час переходу на www.cisco.com із командного рядка (див. частина 2), а не через веб-сайт? (Отримані результати можуть змінюватись залежно від географічного місцезнаходження та Інтернет-провайдера.)
2. Порівняйте результати трасування маршруту до Африки з частини 1 із результатами трасування того ж маршруту через веб-інтерфейс. Яку різницю ви помітили?
3. У деяких трасуваннях є скорочення asymm. Чи є ідеї, що воно може означати? У чому його сенс?

Крок 2. Використовуйте VisualRoute Lite Edition.

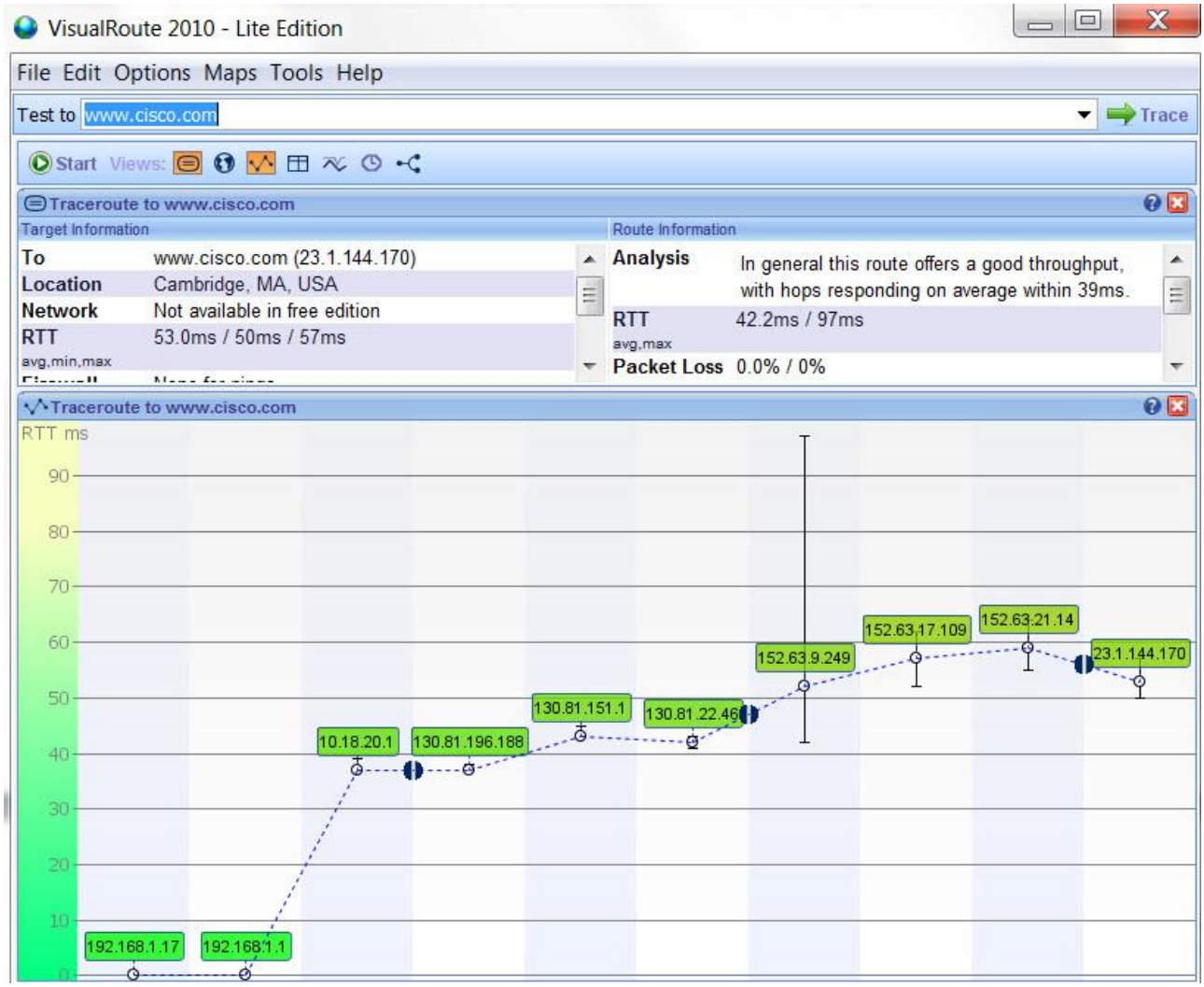
VisualRoute - це пропрієтарна програма, що дозволяє наочно відобразити результати трасування маршруту.

1. Якщо програма VisualRoute Lite Edition на вашому комп'ютері не інстальована, завантажте її за наступним посиланням: http://www.visualroute.com/download.html.

Якщо виникають труднощі при завантаженні або інсталяції VisualRoute, зверніться за допомогою до інструктора. Переконайтеся, що завантажено Lite Edition.

2. За допомогою VisualRoute виконайте трасування маршрутів на адресу www.cisco.com.

3. Збережіть отримані IP-адреси у файлі Блокнота.



Частина 4. Порівняння результатів трасування

Порівняйте результати трасування маршруту до www.cisco.com, отримані у частинах 2 та 3.

Крок 1. Перерахуйте адреси на маршруті www.cisco.com, отримані за допомогою утиліти tracert.

Крок 2. Перерахуйте адреси на маршруті www.cisco.com, отримані за допомогою веб-сервісу subnetonline.com.

Крок 3. Перерахуйте адреси на маршруті до www.cisco.com, отримані за допомогою VisualRoute Lite Edition.

Чи всі інструменти для трасування використовували ті самі маршрути до www.cisco.com? Поясніть відповідь.

Питання для повторення:

Ви скористалися трьома різними засобами для трасування маршруту (утиліта tracert, веб-інтерфейс та програма VisualRoute). Чи можна вважати, що VisualRoute

дозволяє отримати будь-які відомості, які не надаються двома іншими інструментами?

Додаток А

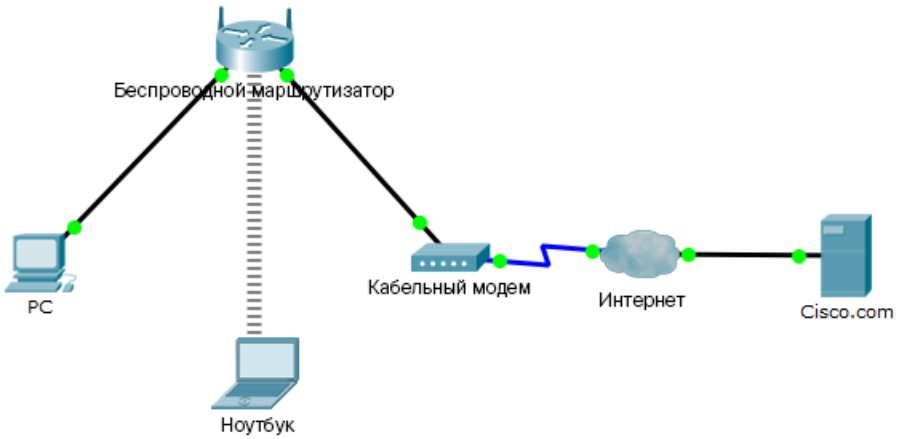
```
C:\> tracert www.cisco.com
Tracing route to e144.dscb.akamaiedge.net [23.1.144.170]
over a maximum of 30 hops:

  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 [130.81.196.190]
  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.
C:\> tracert www.afrinic.net

Tracing route to www.afrinic.net [196.216.2.136]
over a maximum of 30 hops:

  1 1 ms <1 ms <1 ms dslrouter.westell.com [192.168.1.1]
  2 39 ms 38 ms 37 ms 10.18.20.1
  3 40 ms 38 ms 39 ms G4-0-0-2204.ALBYNY-LCR-02.verizon-gni.net [130.81.197.182]
  4 44 ms 43 ms 43 ms so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81.22.46]
  5 43 ms 43 ms 42 ms 0.so-4-0-0.XT2.NYC4.ALTER.NET [152.63.9.249]
  6 43 ms 71 ms 43 ms 0.ae4.BR3.NYC4.ALTER.NET [152.63.16.185]
  7 47 ms 47 ms 47 ms te-7-3-0.edge2.NewYork2.level3.net [4.68.111.137]
  8 43 ms 55 ms 43 ms vlan51.ebr1.NewYork2.Level3.net [4.69.138.222]
  9 52 ms 51 ms 51 ms ae-3-3.ebr2.Washington1.Level3.net [4.69.132.89]
 10 130 ms 132 ms 132 ms ae-42-42.ebr2.Paris1.Level3.net [4.69.137.53]
 11 139 ms 145 ms 140 ms ae-46-46.ebr1.Frankfurt1.Level3.net [4.69.143.137]
 12 148 ms 140 ms 152 ms ae-91-91.csw4.Frankfurt1.Level3.net [4.69.140.14]
 13 144 ms 144 ms 146 ms ae-92-92.ebr2.Frankfurt1.Level3.net [4.69.140.29]
 14 151 ms 150 ms 150 ms ae-23-23.ebr2.London1.Level3.net [4.69.148.193]
 15 150 ms 150 ms 150 ms ae-58-223.csw2.London1.Level3.net [4.69.153.138]
 16 156 ms 156 ms 156 ms ae-227-3603.edge3.London1.Level3.net [4.69.166.154]
 17 157 ms 159 ms 160 ms 195.50.124.34
 18 353 ms 340 ms 341 ms 168.209.201.74
 19 333 ms 333 ms 332 ms csw4-pkl-gi1-1.ip.isnet.net [196.26.0.101]
 20 331 ms 331 ms 331 ms 196.37.155.180
 21 318 ms 316 ms 318 ms fa1-0-1.ar02.jnb.afrinic.net [196.216.3.132]
 22 332 ms 334 ms 332 ms 196.216.2.136

Trace complete.

C:\> tracert www.lacnic.net

Tracing route to lacnic.net [200.3.14.10]
over a maximum of 30 hops:

  1 <1 ms <1 ms <1 ms dslrouter.westell.com [192.168.1.1]
  2 38 ms 37 ms 37 ms 10.18.20.1
  3 37 ms 38 ms 40 ms G3-0-9-2204.ALBYNY-LCR-02.verizon-gni.net [130.81.196.190]
  4 43 ms 42 ms 43 ms so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81.22.46]
  5 46 ms 75 ms 46 ms 0.ae2.BR3.NYC4.ALTER.NET [152.63.16.49]
  6 43 ms 43 ms 43 ms 204.255.168.194
  7 178 ms 182 ms 178 ms ge-1-1-0.100.gw1.gc.registro.br [159.63.48.38]
  8 172 ms 180 ms 182 ms xe-5-0-1-0.core1.gc.registro.br [200.160.0.174]
  9 177 ms 172 ms 181 ms xe-4-0-0-0.core2.nu.registro.br [200.160.0.164]
 10 173 ms 180 ms 176 ms ae0-0.ar3.nu.registro.br [200.160.0.249]
```

```
11 184 ms 183 ms 180 ms gw02.lacnic.registro.br [200.160.0.213]
12 180 ms 179 ms 180 ms 200.3.12.36
13 182 ms 180 ms 180 ms www.lacnic.net [200.3.14.10]
    Trace complete.
```

Лабораторна роботи 2.

Packet Tracer. Створення простої мережі за допомогою Packet Tracer

Топологія



Таблиця адресації

Пристрій	Інтерфейс	IP-адреса	Маска підмережі	Шлюз по замовчуванню
PC	Enternet0	DHCP		192.168.0.1
Безпровідний маршутизатор	LAN	192.168.0.1	255.255.255.0	
	Інтернет	DHCP		
Сервер Cisco.com	Enternet0	208.67.220.220	255.255.255.0	
Ноутбук	Wireless0	DHCP		

Завдання

Частина 1. Створення простої мережі у робочому просторі логічної топології

Частина 2. Налаштування мережевих пристроїв

Частина 3. Перевірка підключення між мережевими пристроями

Частина 4. Збереження файлу та закриття Packet Tracer

Загальні відомості/сценарій

У цій вправі буде з нуля створюватися проста мережа Packet Tracer, яка потім

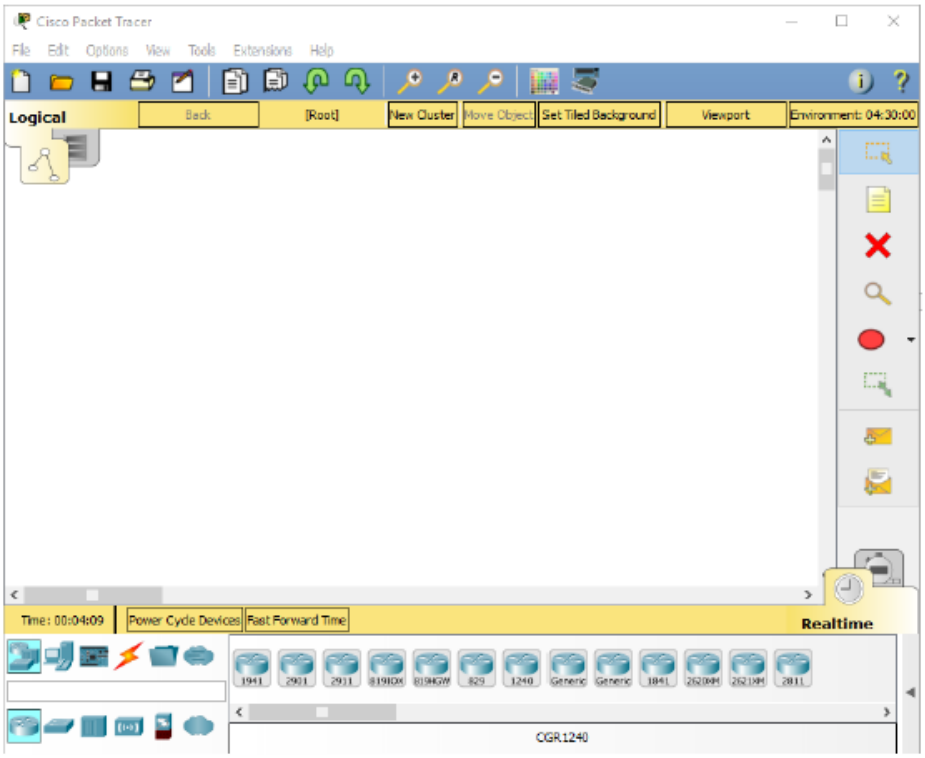
буде збережена у файлі вправи Packet Tracer (з розширенням pkt).

Частина 1: Створення простої мережі у робочому просторі логічної топології

Крок 1: Запуск Packet Tracer

a. Запустіть Packet Tracer на своєму комп'ютері або ноутбуку.

Двічі клацніть піктограму Packet Tracer на робочому столі або перейдіть до каталогу, де знаходиться файл Packet Tracer, що виконується, і запустіть його. Відкриється Packet Tracer з порожнім робочим простором логічної топології за промовчанням, як показано на малюнку.



Крок 2: Побудова топології

a. Додайте до робочого місця мережні пристрої.

За допомогою поля вибору пристрою додайте до робочого простору мережеві пристрої, як показано на діаграмі топології.

Щоб помістити пристрій у робочий простір, спочатку виберіть його тип у полі Device Type Selection (Вибір типу пристрою). Потім виберіть потрібну модель пристрою у полі Device-Specific Selection (Вибір конкретного пристрою). Нарешті, у робочому просторі виберіть місце, в яке слід помістити пристрій. Якщо потрібно скасувати вибір, клацніть піктограму Cancel (Скасувати) для цього пристрою. Також

можна клацнути пристрій та перетягнути його з поля Device-Specific Selection (Вибір конкретного пристрою) у робочий простір.

b. Додайте до робочого місця мережні пристрої.

За допомогою поля вибору пристрою додайте до робочого простору мережеві пристрої, як показано на діаграмі топології.

Щоб помістити пристрій у робочий простір, спочатку виберіть його тип у полі Device Type Selection (Вибір типу пристрою). Потім виберіть потрібну модель пристрою у полі

Device-Specific Selection (Вибір конкретного пристрою). Нарешті, у робочому просторі виберіть місце, в яке слід помістити пристрій. Якщо потрібно скасувати вибір, клацніть піктограму Cancel (Скасувати) для цього пристрою. Також можна клацнути пристрій та перетягнути його з поля Device-Specific Selection (Вибір конкретного пристрою) у робочий простір.

c. Змініть імена мережевих пристроїв.

Щоб змінити відображені імена мережних пристроїв, клацніть піктограму пристрою в логічному робочому просторі Packet Tracer і виберіть вкладку Config (Конфігурація у вікні конфігурації пристрою.) На вкладці Config (Конфігурація) введіть нове ім'я пристрою у полі Display Name (Показати наведене.

d. Додайте фізичні кабельні з'єднання між пристроями у робочому просторі.

За допомогою поля вибору пристрою додайте до робочого простору фізичні кабельні з'єднання, як показано на діаграмі топології.

ПК повинен бути підключений до бездротового маршрутизатора за допомогою прямого мідного кабелю. Виберіть мідний прямий кабель у полі Device-Selection (Вибір пристрою) та підключіть його до інтерфейсу FastEthernet0 на ПК та

інтерфейсу Ethernet 1 на бездротовому маршрутизаторі.

Бездротовий маршрутизатор повинен бути підключений до кабельного модему за допомогою мідного прямого кабелю. Виберіть мідний прямий кабель у полі Device-Selection (Вибір пристрою) та підключіть його до інтернет-інтерфейсу бездротового маршрутизатора та інтерфейсу Port 1 кабельного модему.

Для підключення кабельного модему до хмари Інтернету потрібний коаксіальний кабель.

Виберіть коаксіальний кабель у полі Device-Selection (Вибір пристрою) та підключіть його до інтерфейсу Port 0 кабельного модему та до коаксіального інтерфейсу хмари Інтернету. Для підключення хмари Інтернету до сервера Cisco.com потрібний прямий мідний кабель. Виберіть мідний прямий кабель у полі Device-Selection (Вибір пристрою) та підключіть його до інтерфейсу Ethernet хмари Інтернету та інтерфейсу FastEthernet0 сервера Cisco.com.

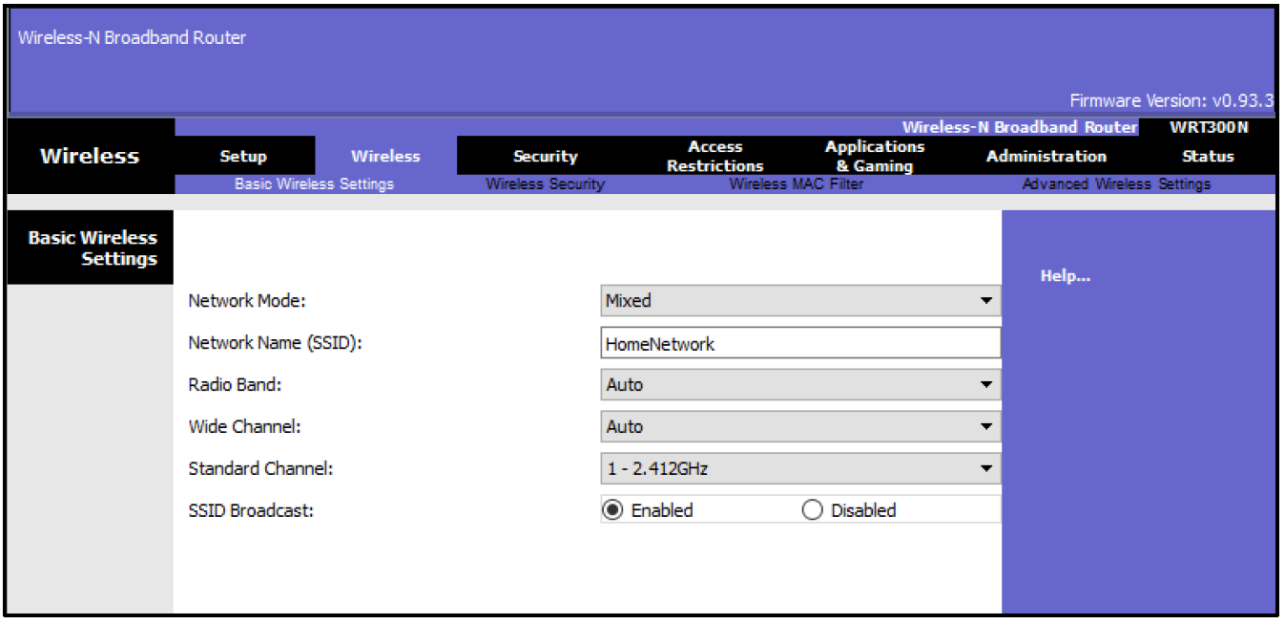
Частина 2: Налаштування мережевих пристроїв

Крок 1: Налаштування бездротового маршрутизатора

а. Створіть бездротову мережу на бездротовому маршрутизаторі.

Клацніть піктограму бездротового маршрутизатора в логічному просторі Packet Tracer, щоб відкрити вікно конфігурації пристрою. У вікні конфігурації бездротового маршрутизатора відкрийте вкладку GUI (Графічний інтерфейс користувача), щоб переглянути параметри конфігурації маршрутизатора.

Потім відкрийте вкладку Wireless (Бездротовий зв'язок) у графічному інтерфейсі користувача, щоб переглянути налаштування бездротового зв'язку. Єдиний параметр, за промовчанням якого потрібно змінити, — Network Name (SSID) (Ім'я мережі). Введіть ім'я "HomeNetwork", як показано на малюнку.

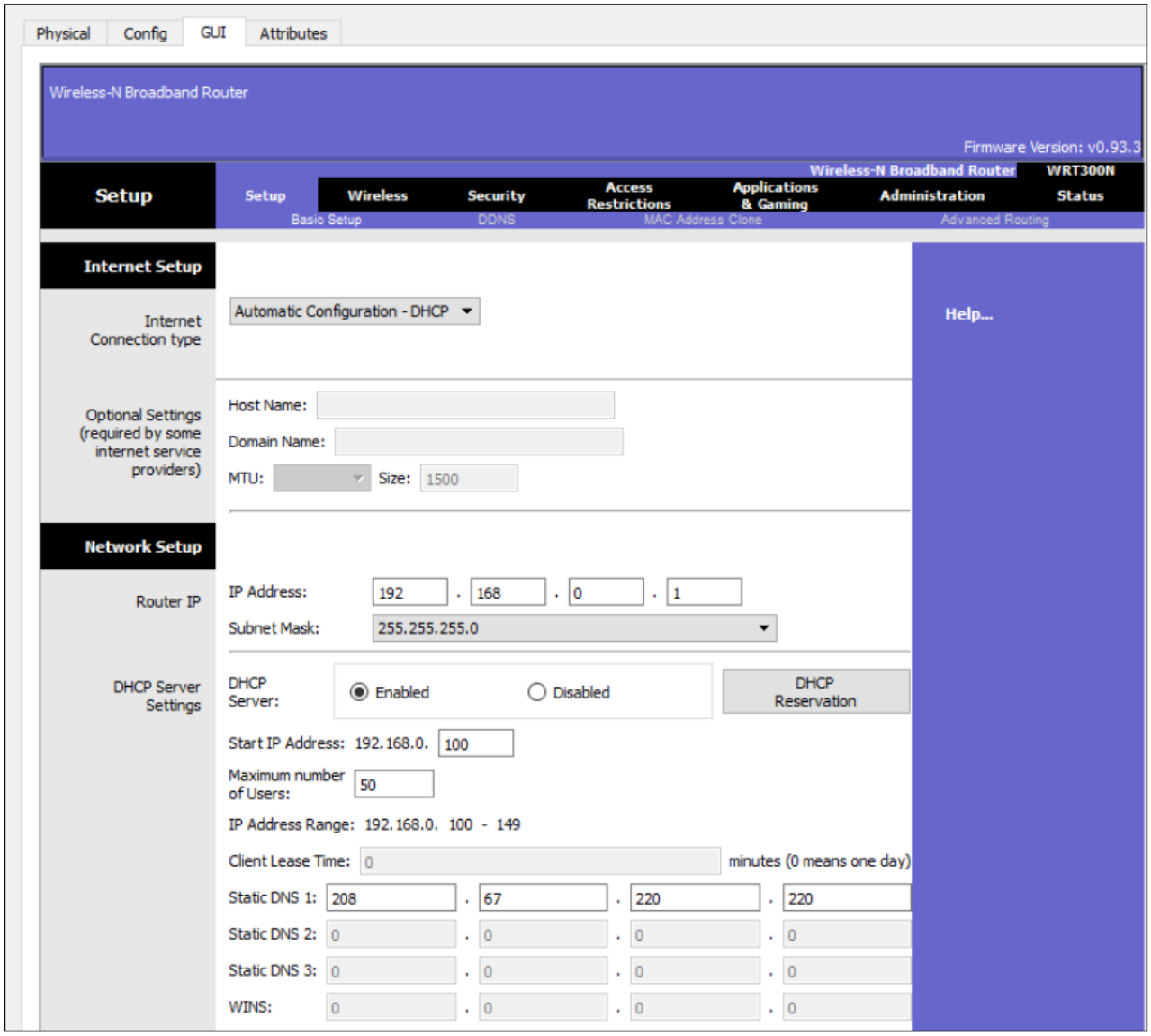


b. Налаштуйте підключення до Інтернету на бездротовому маршрутизаторі.

Перейдіть на вкладку Setup (Налаштування) у графічному інтерфейсі бездротового маршруту.

У налаштуваннях сервера DHCP переконайтеся, що кнопка Enabled (Включено) вибрана, після чого задайте статичну IP-адресу сервера DNS 208.67.220.220, як показано на малюнку.

c. Перейдіть на вкладку Save Settings (Зберегти налаштування).



Крок 2: Налаштування ноутбука

а. На комп'ютері налаштуйте доступ до бездротової мережі.

Клацніть піктограму ноутбука в логічному робочому просторі Packet Tracer та у вікні конфігурації ноутбука виберіть вкладку Physical (Фізичні налаштування).

На вкладці Physical (Фізичні налаштування) необхідно видалити модуль підключення мідного проводу Ethernet та замінити його модулем бездротового зв'язку Wireless WPC300N.

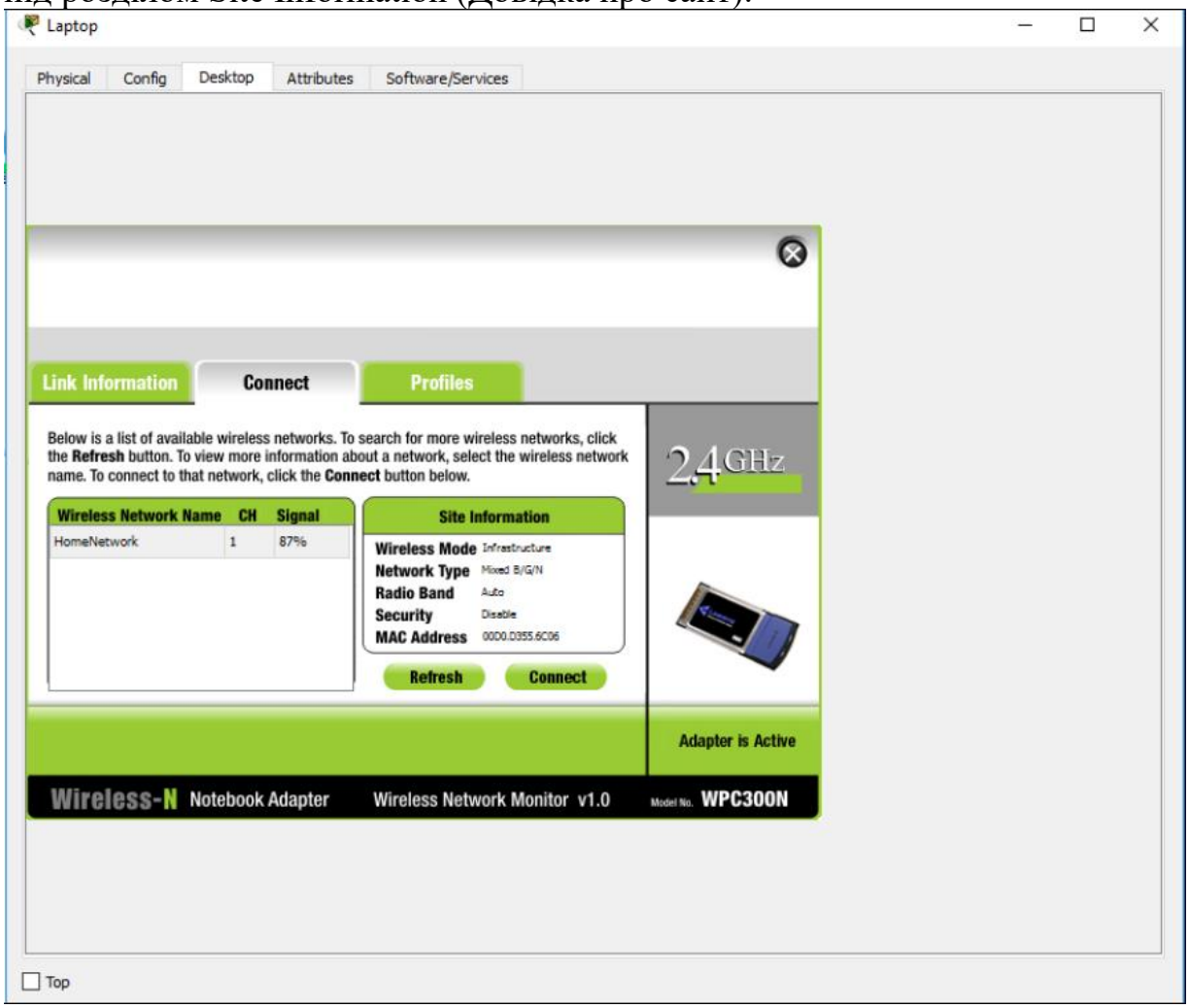
Для цього спочатку вимкніть ноутбук, натиснувши кнопку живлення на його боці. Потім видаліть раніше встановлений модуль підключення Ethernet, перетягнувши модуль збоку ноутбука на панель MODULES (Модулі) у лівій частині вікна Laptop (Ноутбук). Потім встановіть модуль Wireless WPC300N, перетягнувши його з панелі MODULES (Модулі) у порожній порт для модуля на боці ноутбука. Знову увімкніть ноутбук, натиснувши кнопку живлення на ньому.

Наступне завдання після встановлення модуля бездротового зв'язку — підключення ноутбука до бездротової мережі. У верхній частині вікна конфігурації ноутбука відкрийте вкладку Desktop (Робочий стіл) і виберіть піктограму PC Wireless (Бездротова мережа).

Коли відкриються налаштування адаптера ноутбука Wireless-N, перейдіть на вкладку Connect (Підключити). У списку бездротових мереж має бути бездротова

мережа "HomeNetwork", як показано на малюнку.

Виберіть мережу та відкрийте вкладку Connect (Підключити), яка знаходиться під розділом Site Information (Довідка про сайт).

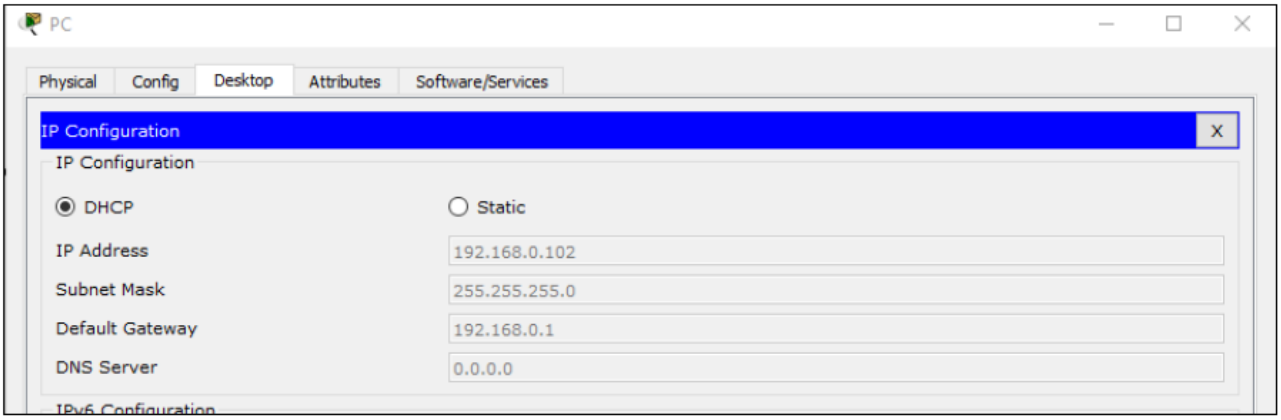


Крок 3: Налаштування ПК

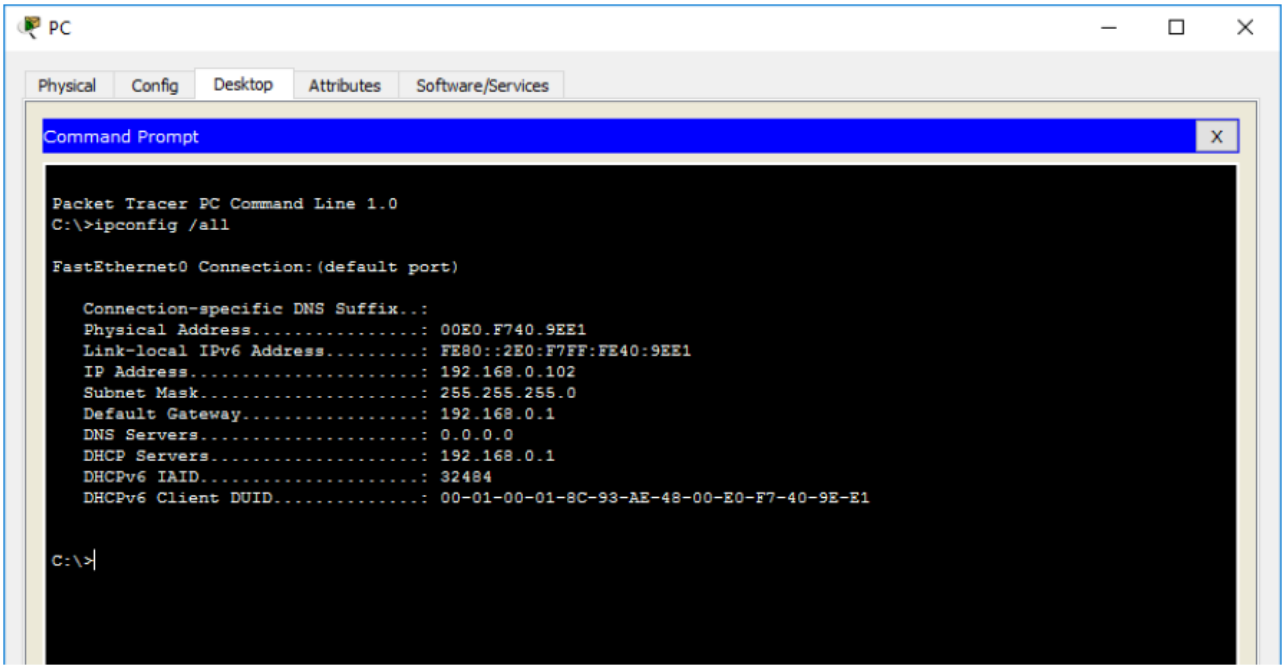
а. Налаштуйте підключення до дротової мережі на комп'ютері.

Натисніть піктограму ПК у логічному робочому просторі Packet Tracer та виберіть вкладку Desktop (Робочий стіл), а потім натисніть піктограму IP Configuration (Налаштування IP-адреси).

У вікні IP Configuration (Налаштування IP-адреси) встановіть перемикач DCHP у положення, показане на малюнку, щоб цей ПК використовував DCHP для отримання IPv4 адреси від бездротового маршрутизатора. Закрийте вікно IP Configuration (Налаштування IP-адреси).



Натисніть кнопку Command Prompt (Командний рядок). Переконайтеся, що ПК отримав адресу IPv4, виконавши командний рядок команду ipconfig /all, як показано на малюнку. ПК повинен отримати IPv4 адресу з діапазону 192.168.0.x.



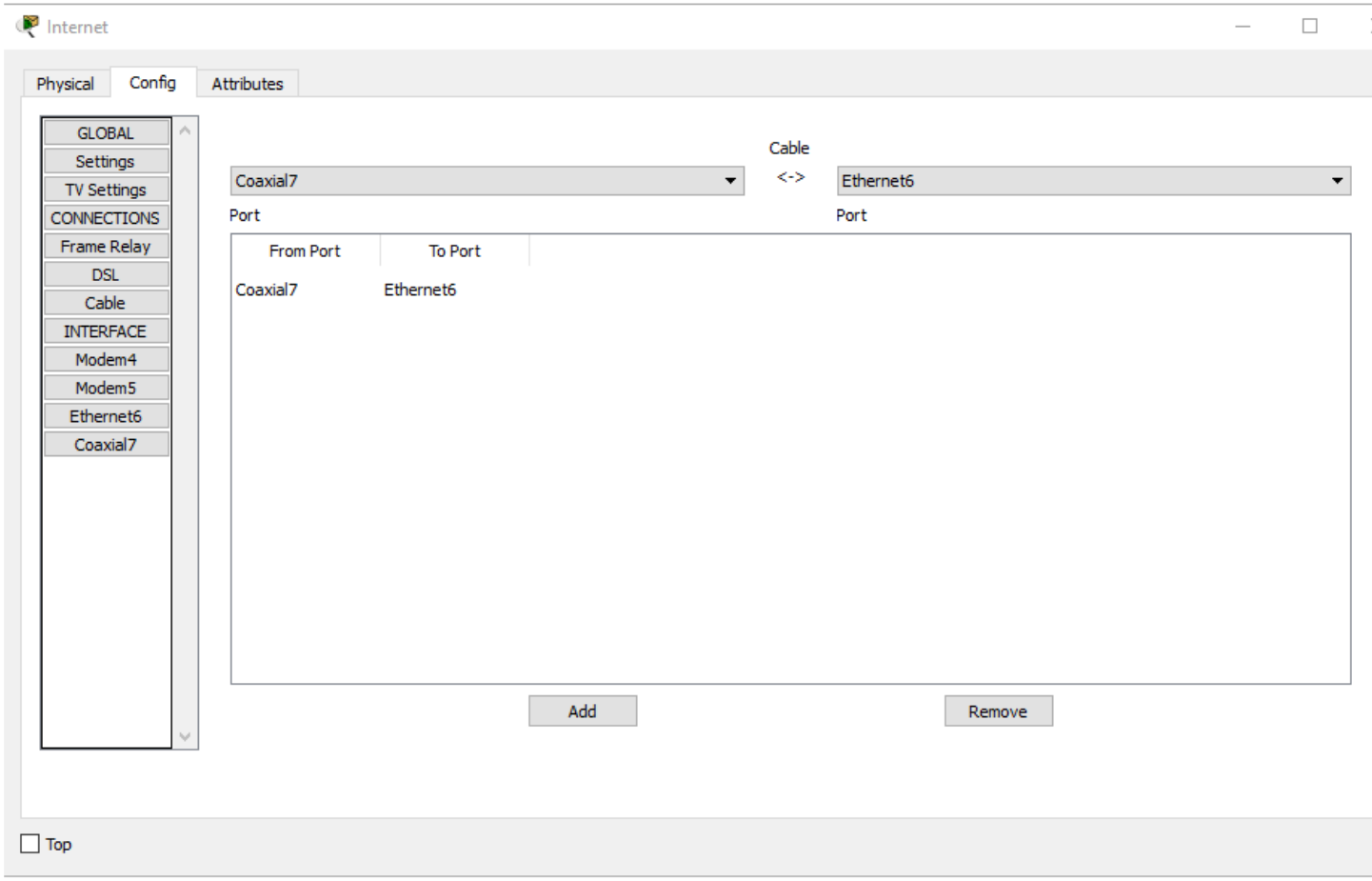
Крок 4: Налаштування хмари Інтернету

a. У разі потреби встановіть мережеві модулі.

Клацніть піктограму хмари Інтернету в логічному робочому просторі Packet Tracer та виберіть вкладку Physical (Фізичні налаштування). Для хмарного пристрою потрібні два модулі, якщо вони ще не встановлені. Модуль PT-CLOUD-NM-1CX потрібен для підключення служби кабельного модему, а модуль PT-CLOUD-NM-1CFE – для підключення мідного кабелю Ethernet. Якщо ці модулі відсутні, відключіть фізичні хмарні пристрої, натиснувши кнопку живлення, і перетягніть обидва модулі в порожні порти для модулів пристрою. Після цього знову увімкніть живлення.

b. Визначте вихідний та вхідний порти.

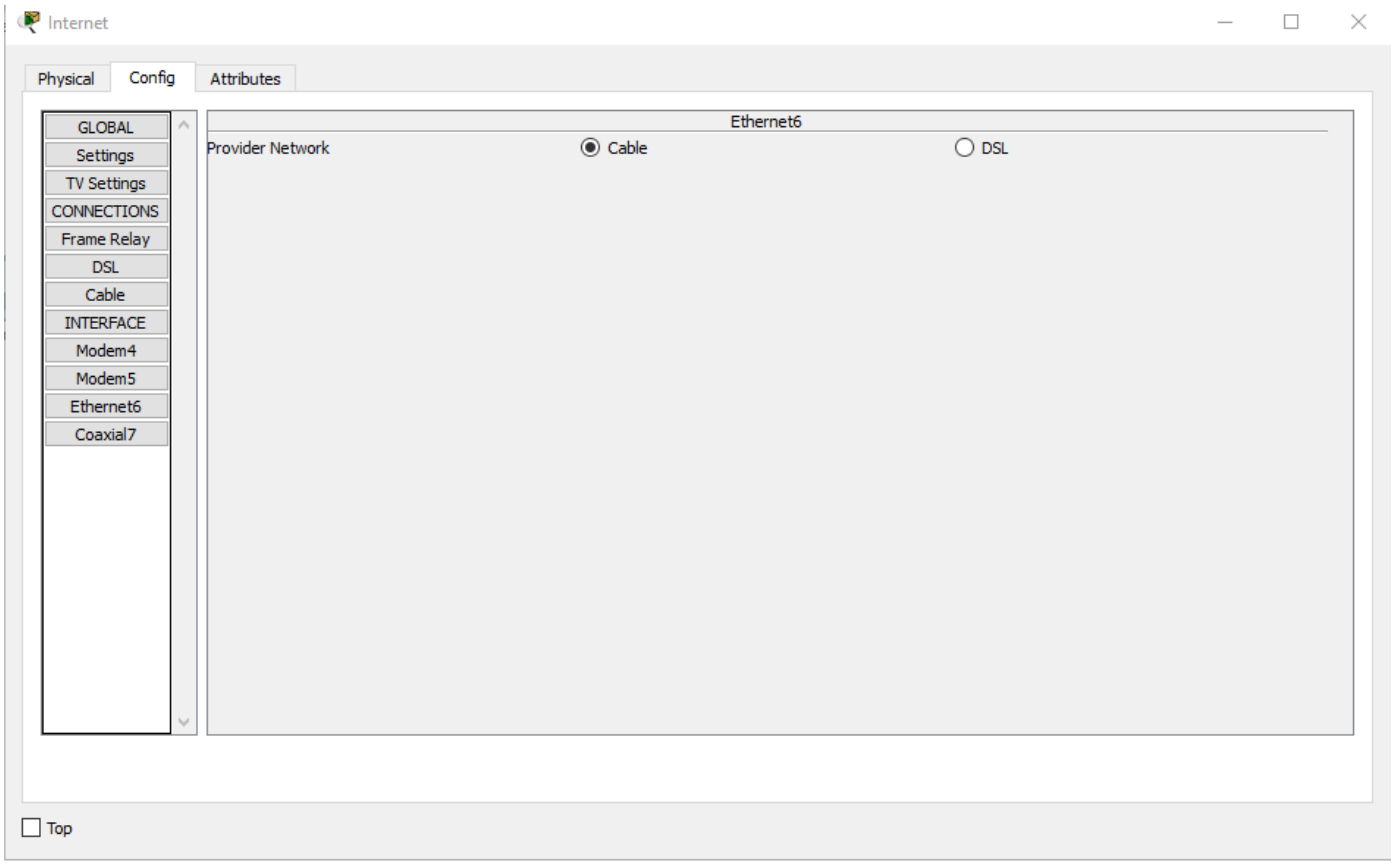
Перейдіть на вкладку Config (Конфігурація) у вікні Cloud device (Хмарний пристрій). У лівій області виберіть Cable (Кабель) у розділі CONNECTIONS (Підключення). У першому списку, що розкривається, виберіть Coaxial (Коаксіальний), а в другому — Ethernet. Потім натисніть кнопку Add (Додати), щоб додати їх як вихідний та вхідний порти, як показано на малюнку.



c. Визначення типу провайдера

Перейдіть на вкладку Config (Конфігурація), виберіть Ethernet у розділі INTERFACE (Інтерфейс) у лівій панелі. У вікні конфігурації Ethernet виберіть Cable (Кабель) у полі

Provider Network (Мережа провайдера), як показано на малюнку.



Крок 5. Налаштування сервера Cisco.com

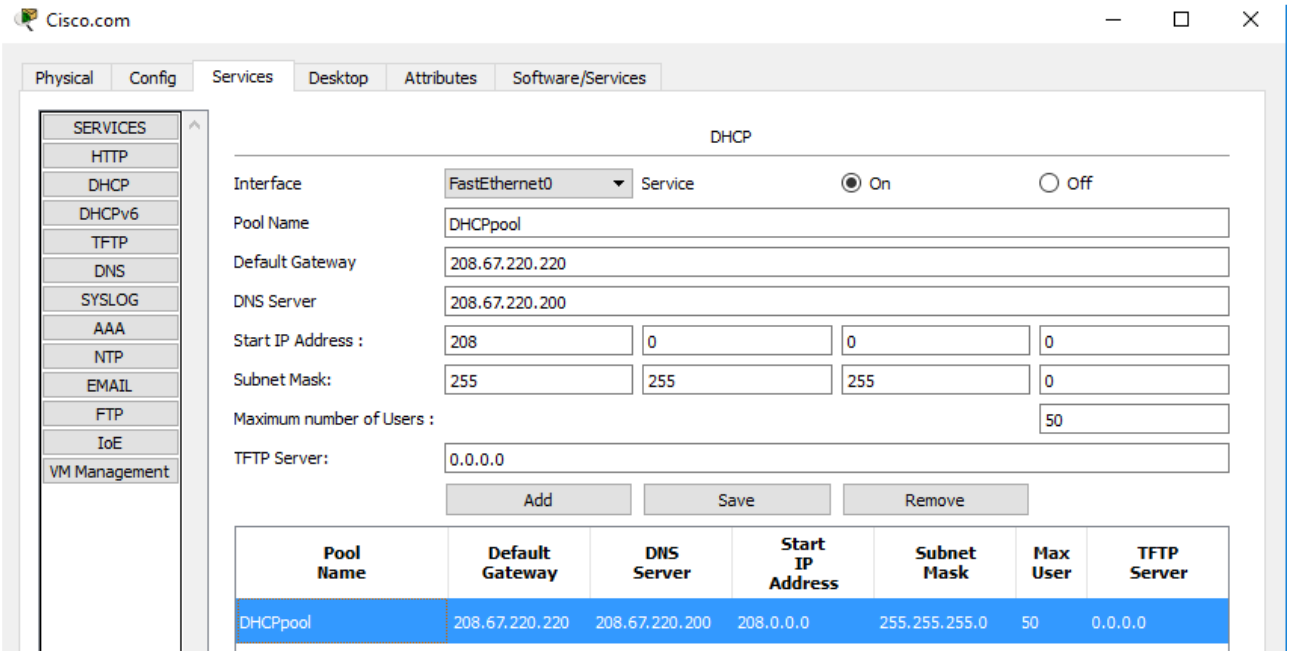
a. Налаштуйте сервер Cisco.com як сервер DHCP.

Клацніть піктограму сервера Cisco.com у робочому просторі Packet Tracer та виберіть вкладку Services (Служби). Виберіть DHCP у списку SERVICES (Служби) на панелі ліворуч.

У вікні конфігурації DHCP настройте наступні параметри DHCP, як показано на малюнку.

• Натисніть On (Увімк.), щоб увімкнути DCHP.
• Pool name (Ім'я пулу): DHCPpool
• Default Gateway (Шлюз за замовчуванням): 208.67.220.220
• DNS Server (DNS-сервер): 208.67.220.220
• Starting IP Address (Початкова IP-адреса): 208.67.220.1
• Subnet Mask (Маска підмережі): 255.255.255.0
• Maximum number of Users (Максимальна кількість користувачів): 50

Натисніть Add (Додати), щоб додати пул.



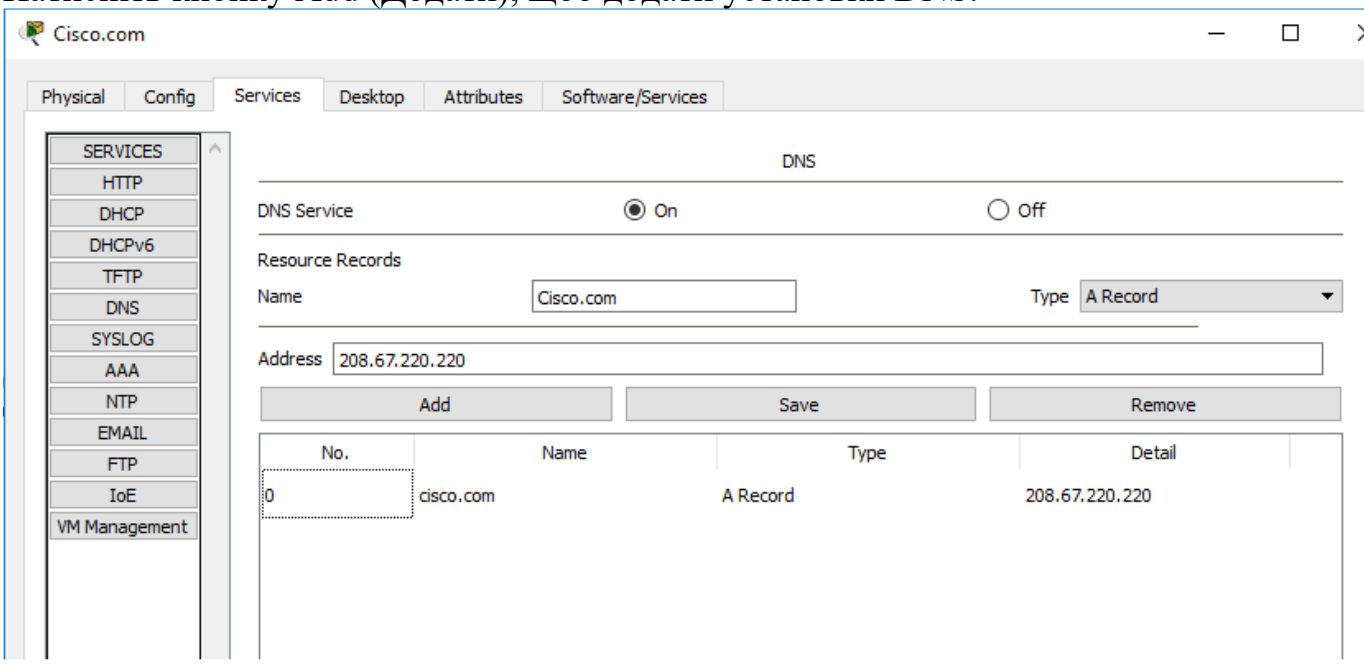
b. Налаштуйте сервер Cisco.com як сервер DNS, який надаватиме ім'я домену для вирішення адрес IPv4.

Перейдіть на вкладку Services (Служби) та виберіть DNS у списку SERVICES (Служби) на панелі ліворуч.

Налаштуйте службу DNS, вказавши такі параметри, як показано на малюнку.

- Натисніть On (Увімк.), щоб увімкнути DNS.
- Name (Ім'я): Cisco.com
- Type (Тип): A Record
- Address (Адреса): 208.67.220.220

Натисніть кнопку Add (Додати), щоб додати установки DNS.



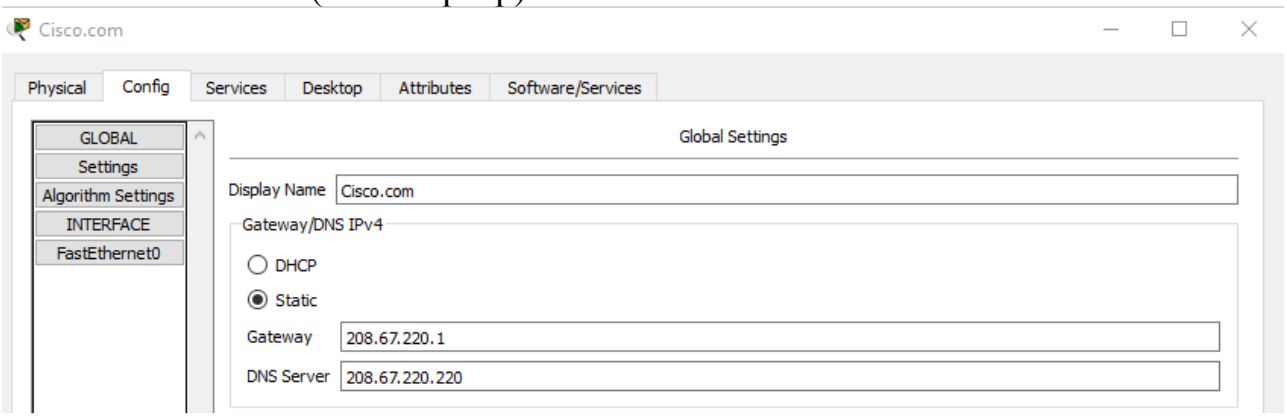
c. Вкажіть глобальні налаштування сервера Ci sco.com.

Виберіть вкладку Config.

Натисніть Settings (Параметри) на панелі ліворуч.

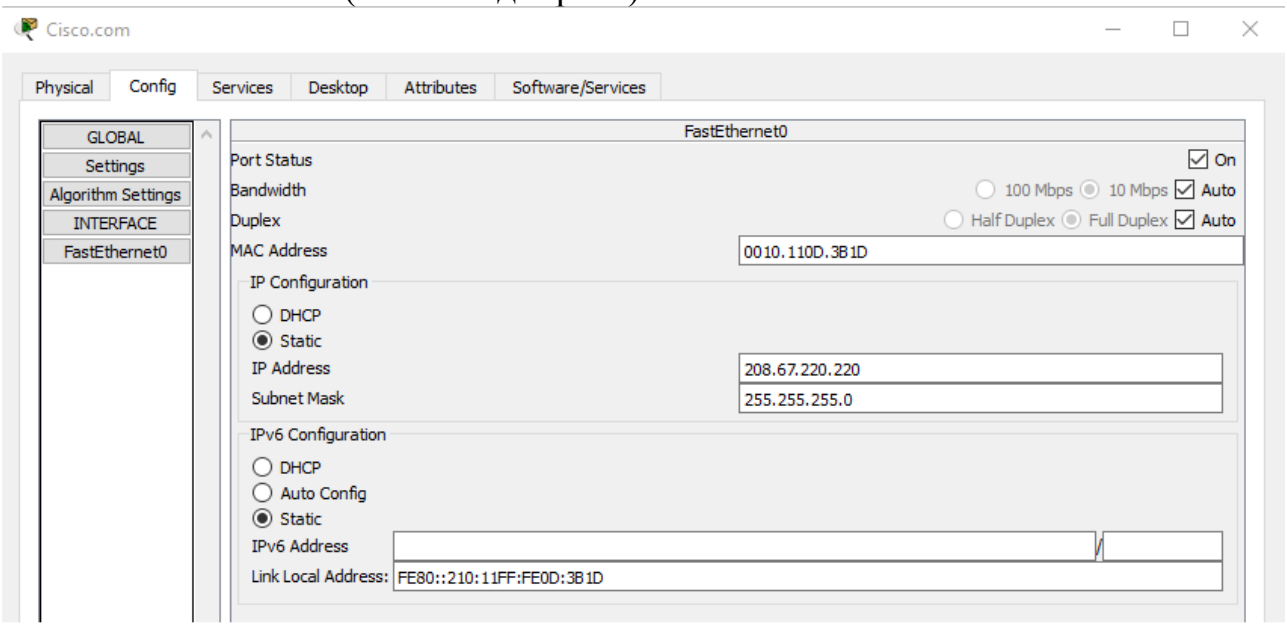
Вкажіть глобальні налаштування сервера таким чином.

• Виберіть Static.
• Gateway (Шлюз): 208.67.220.1
• DNS Server (DNS-сервер): 208.67.220.220



d. Встановіть інтерфейс FastEthernet0 сервера Cisco.com.
Натисніть FastEthernet на лівій панелі вкладки Config (Конфігурація).
Налаштуйте параметри FastEthernet інтерфейсу наступним чином.

• Виберіть Static (Статичний) у розділі IP Configuration (Налаштування IP адреси).
• IP Address (IP-адреса): 208.67.220.220
• Subnet Mask (Маска підмережі): 255.255.255.0



Частина 3: Перевірка підключення

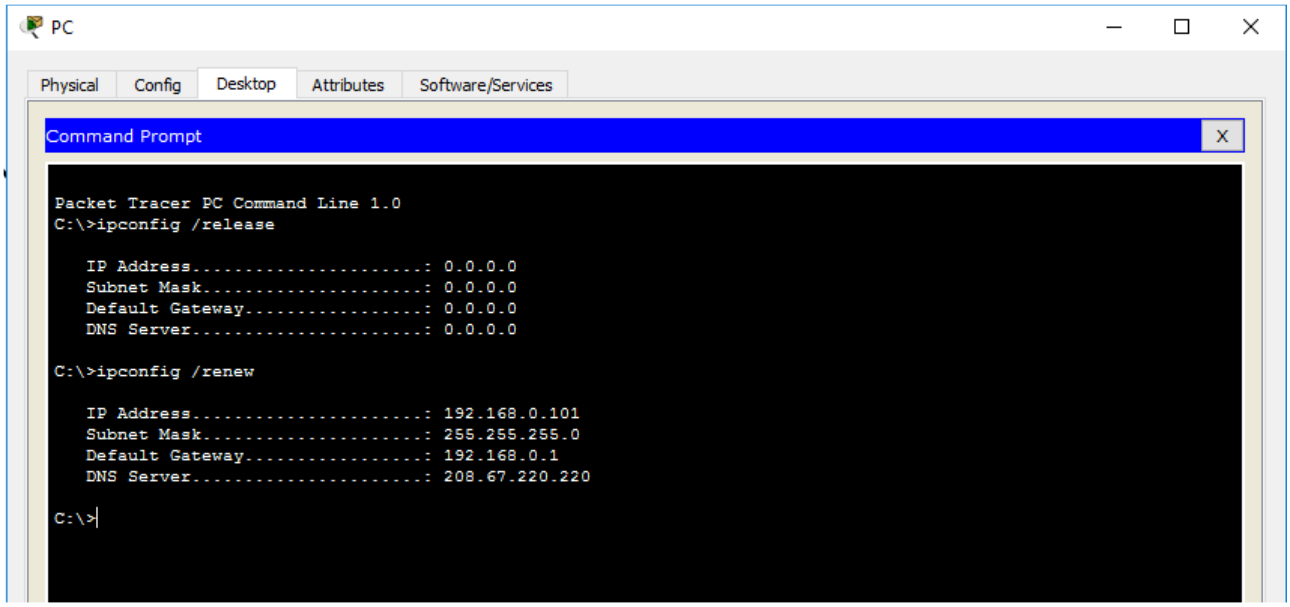
Крок 1: Оновлення параметрів IPv4 на ПК

а) Переконайтеся, що ПК отримує конфігураційні дані IPv4 від DHCP.

Натисніть PC (ПК) у логічному робочому просторі Packet Tracer та виберіть вкладку Desktop (Робочий стіл) у вікні конфігурації ПК.

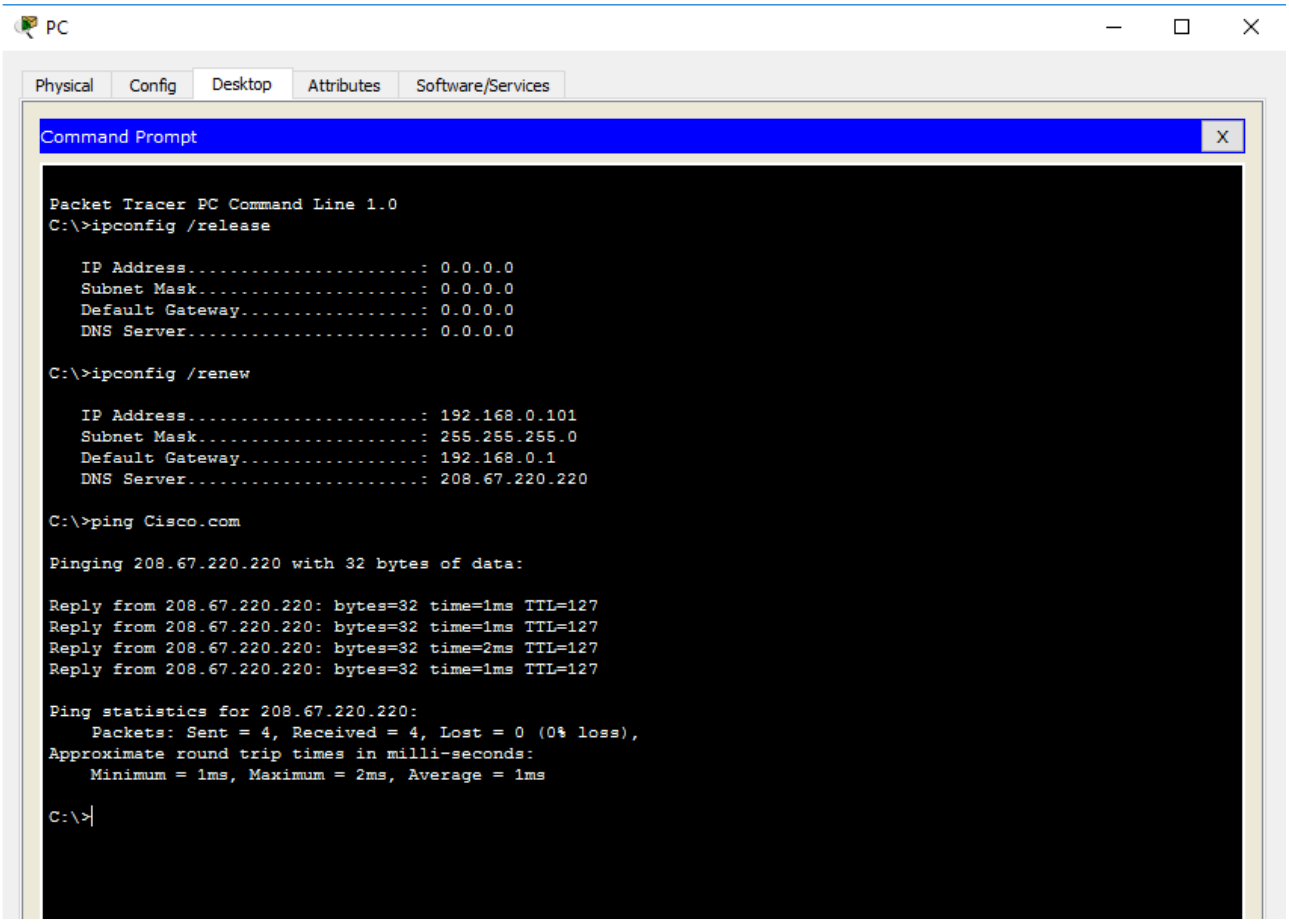
Натисніть кнопку Command Prompt (Командний рядок).

У командному рядку оновіть параметри IP-адреси, виконавши команди ipconfig /release та ipconfig /renew. У вихідних даних має бути зазначено, що ПК має IP-адресу з діапазону 192.168.0.x, маску підмережі, шлюз за замовчуванням та адресу DNS-сервера, як показано на малюнку.



b) Перевірте підключення до сервера Cisco.com із ПК.

У командному рядку виконайте ping Cisco.com. На отримання відповіді від команди ping може піти кілька секунд. Має бути отримано чотири відповіді, як показано малюнку.

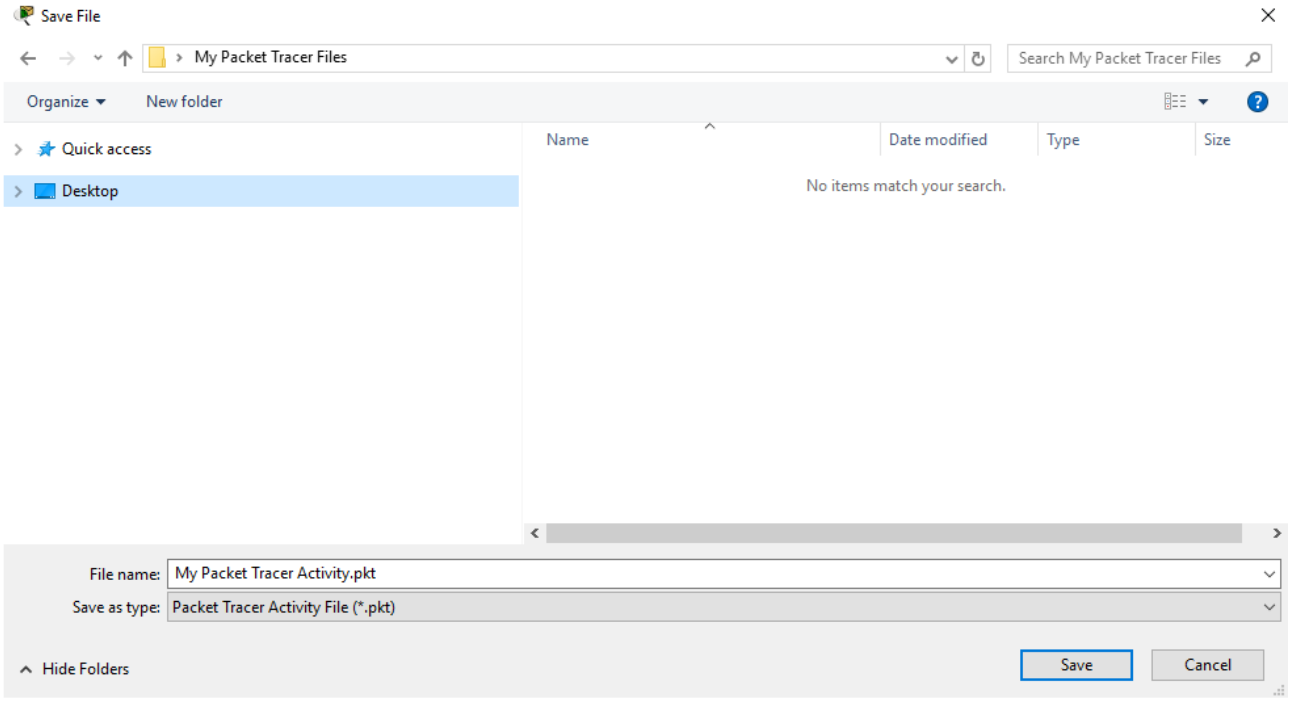


Частина 4: Збереження файлу та закриття Packet Tracer

Крок 1: Збереження файлу у форматі вправи Packet Tracer (*.pkt)

Щоб зберегти створену мережу, клацніть File (Файл) у меню Packet Tracer, а потім виберіть у розкривному меню пункт Save As… (Зберегти як). У вікні Save File (Зберегти файл) виберіть каталог для збереження файлу, а потім введіть файл у

відповідне ім'я. За замовчуванням у полі Save as type (Тип файлу, що зберігається) вибрано Packet Tracer Activity File (*.pkt). (Файл вправи Packet Tracer, *. pkt). Щоб зберегти файл, натисніть Save (Зберегти).



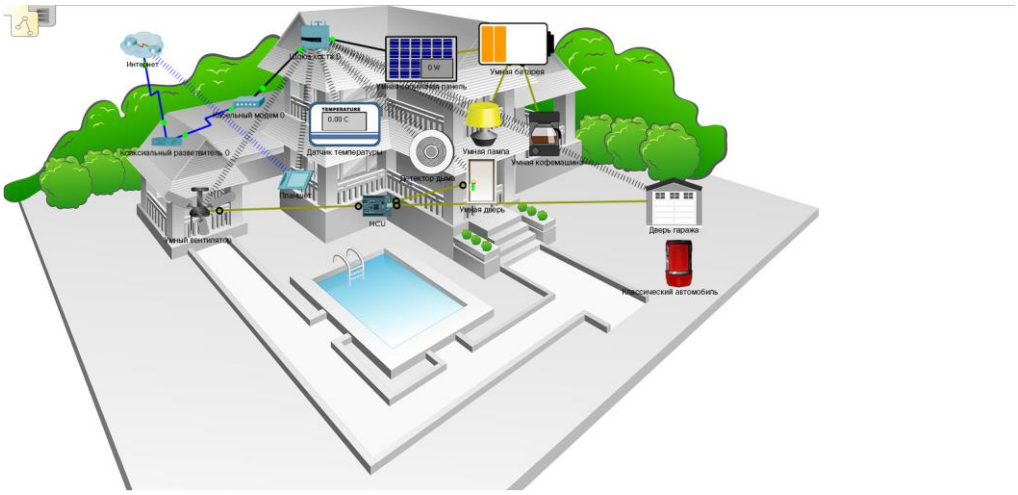
Крок 2: Закриття Packet Tracer

Щоб закрити Packet Tracer, натисніть кнопку X у верхньому правому куті вікна Packet Tracer або виберіть пункт Exit (Вихід) у меню File (Файл).

Лабораторна робота 3

Додавання пристроїв IoT до розумного будинку

Мережа розумного будинку



Завдання

Частина 1. Вивчення існуючої мережі розумного будинку

Частина 2. Додавання дротових пристроїв IoT до мережі розумного будинку

Частина 3. Додавання бездротових пристроїв IoT до мережі розумного будинку

Загальні відомості/сценарій

У цій вправі відкривається файл Packet Tracer із вже налаштованою домашньою мережею, вивчаються підключені до мережі пристрої, а потім додаються додаткові дротові та бездротові пристрої IoT.

Частина 1: Вивчення існуючої мережі розумного будинку

Крок 1: Відкриття файлу Smart_Home_Network.pkt

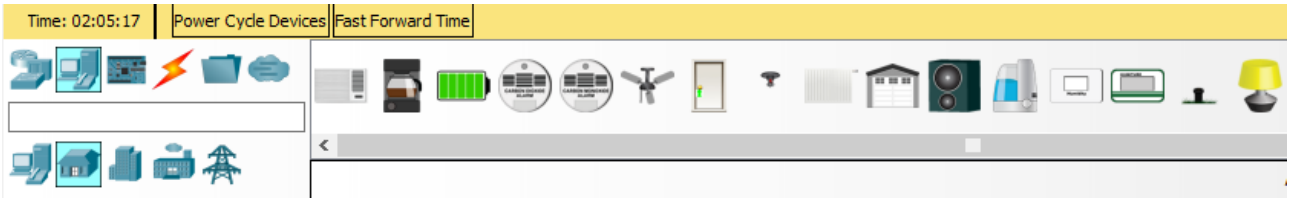
a. Відкрийте файл Smart_Home_Network.pkt.

b. Збережіть файл на комп'ютері.

Крок 2: Вивчення мережі розумного будинку

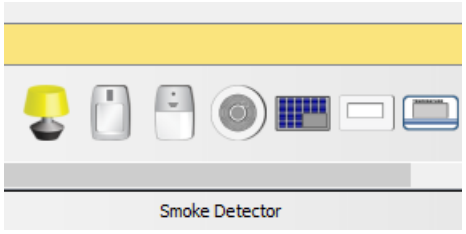
a. Досліджуйте кінцеві пристрої IoT.

У нижньому лівому куті вікна Packet Tracer клацніть піктограму [End Devices] (Кінці пристрої) у верхньому рядку, а потім клацніть піктограму [Home] (Будинок) у нижньому будівництві поля Device-Type Selection (Вибір типу пристрою).

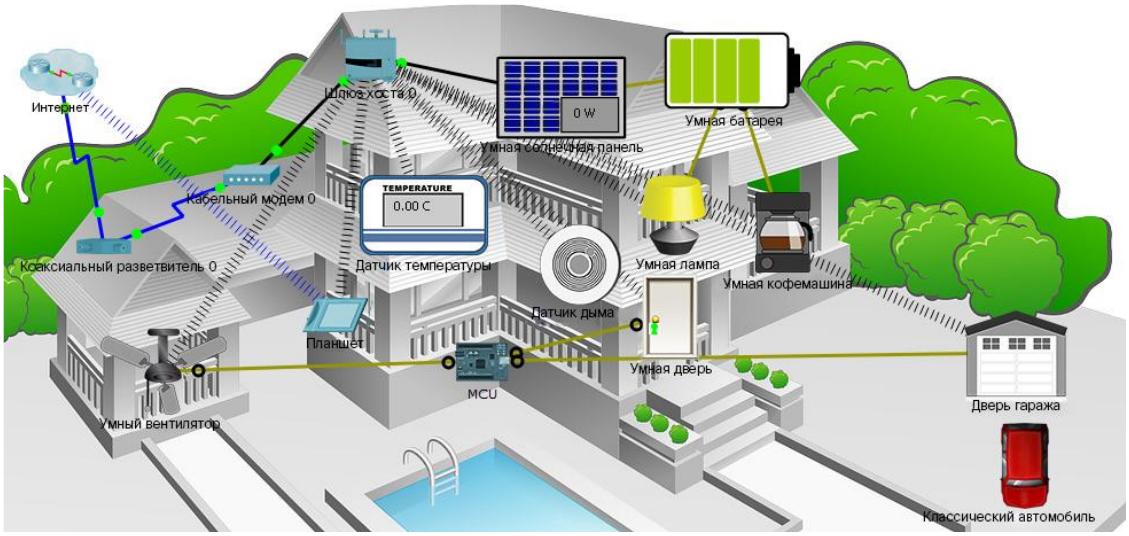


У нижній частині вікна Packet Tracer у полі Device-Specific Selection (Вибір конкретного пристрої) відображається безліч доступних пристроїв IoT для розумного будинку.

Наведіть вказівник миші на кожен пристрій і зверніть увагу, що при цьому в нижній частини поля Device-Specific Selection (Вибір конкретного пристрою) відображається описово Ім'я цього пристрою. Детально розгляньте пристрій кожного типу.



b. Вивчіть мережу розумного будинку.



У логічному робочому просторі знаходиться заздалегідь створена мережа розумного будинку, яка складається з безлічі дротових та бездротових пристроїв IoT, а також пристроїв мережної інфраструктури.

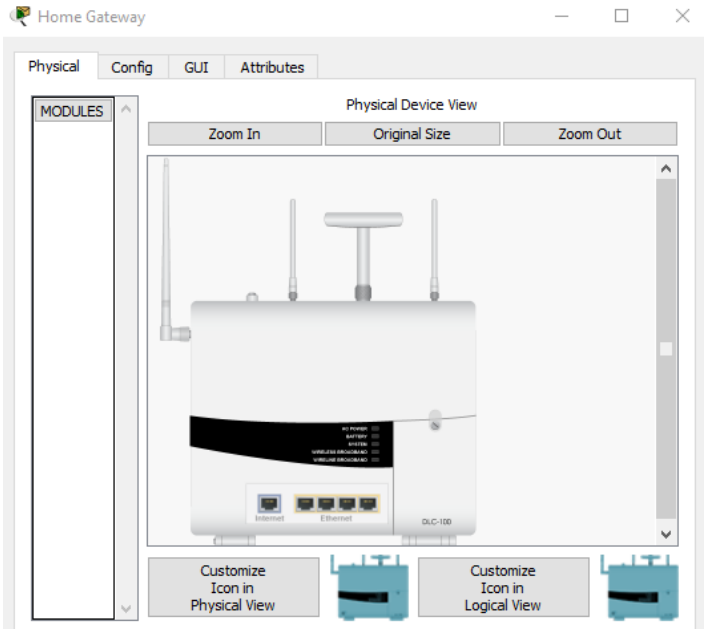
При наведенні курсору на пристрій, наприклад, на розумний вентилятор, відкривається інформаційне вікно з базовою мережевою інформацією про цей пристрій.

Щоб увімкнути або активувати пристрій, просто натисніть клавішу Alt і утримуйте її. натиснутою, клацніть пристрій лівою кнопкою миші. Зробіть це з кожним розумним пристроєм, щоб спостерігати, що з ними відбувається.

У мережі розумного будинку також є пристрої мережної інфраструктури, наприклад, домашній шлюз.

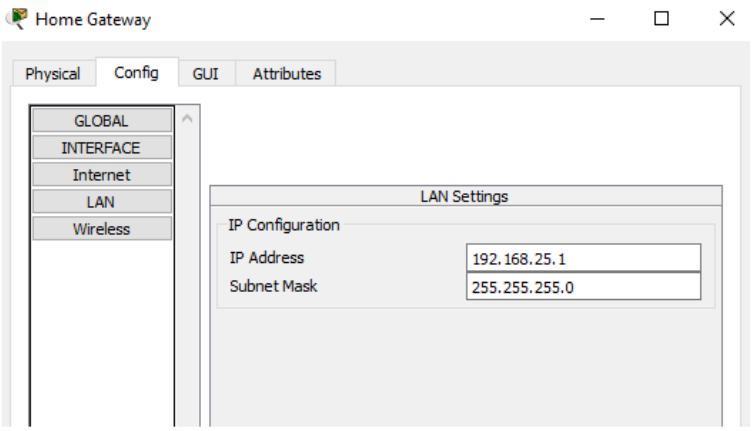
Натисніть піктограму **Home Gateway** (Домашній шлюз), щоб відкрити вікно Home Gateway (Домашній шлюз)

Виберіть вкладку Physical (Фізичні налаштування) за замовчуванням. На ній показано зображення домашнього шлюзу.



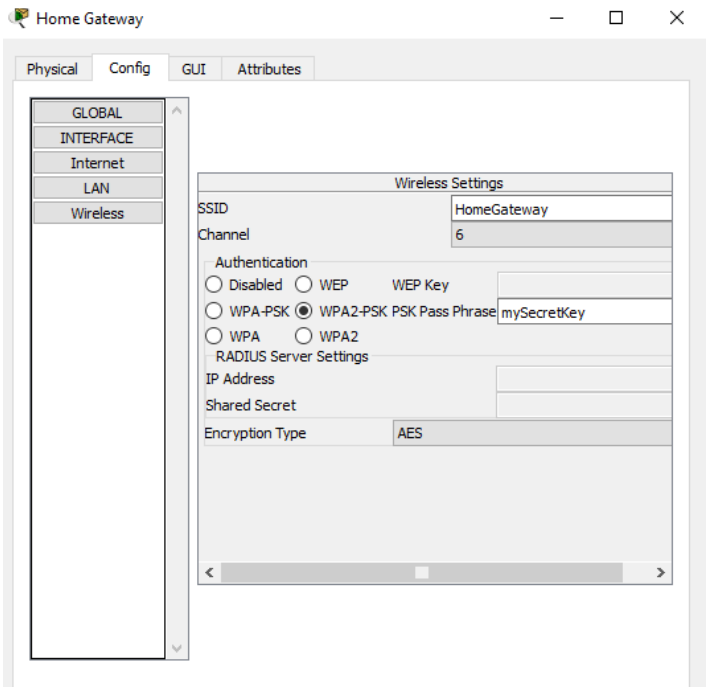
Тепер перейдіть на вкладку Config (Конфігурація), а потім у лівій панелі клацніть LAN (Локальна мережа), щоб переглянути установки локальної мережі домашнього шлюзу.

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



Натисніть Wireless (Бездротовий зв'язок) у лівій панелі, щоб переглянути настройки бездротового зв'язку домашнього шлюзу.

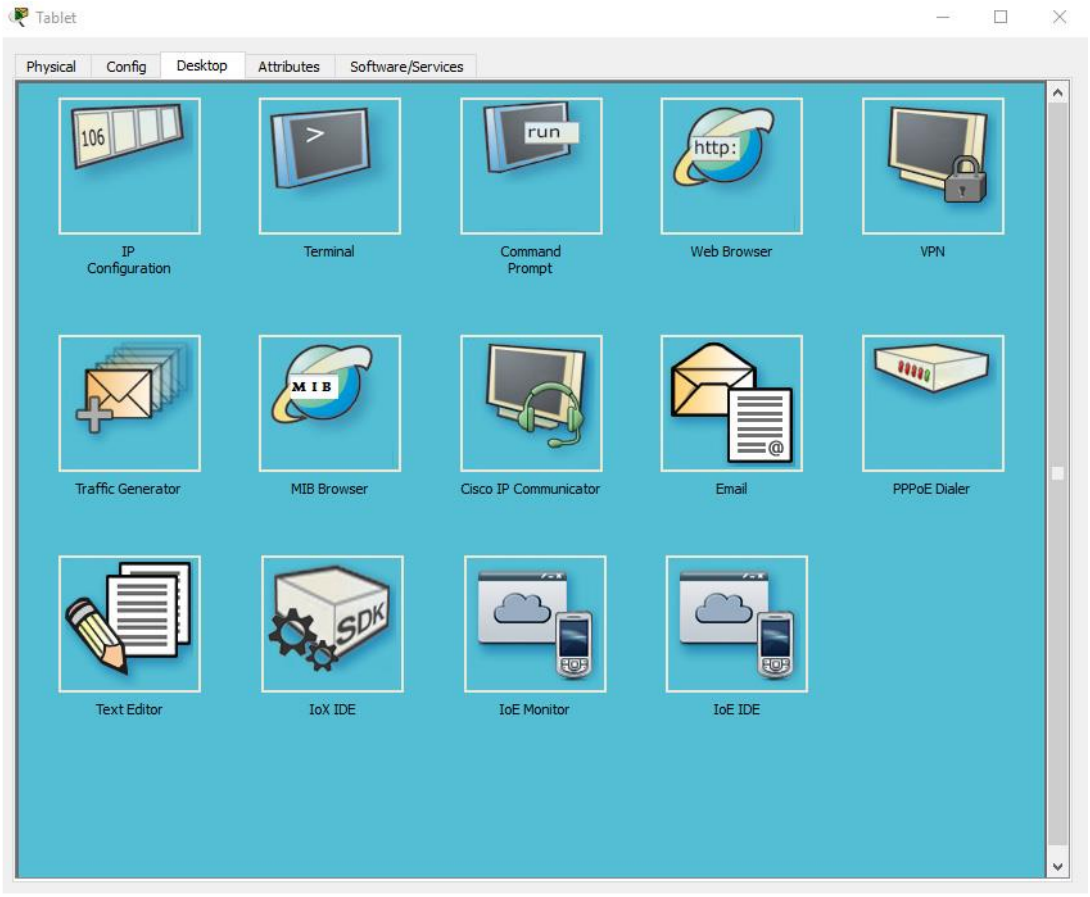
Запишіть ідентифікатор SSID домашньої мережі _____та кодову фразу WPA2-PSK_____ для використання у майбутньому.



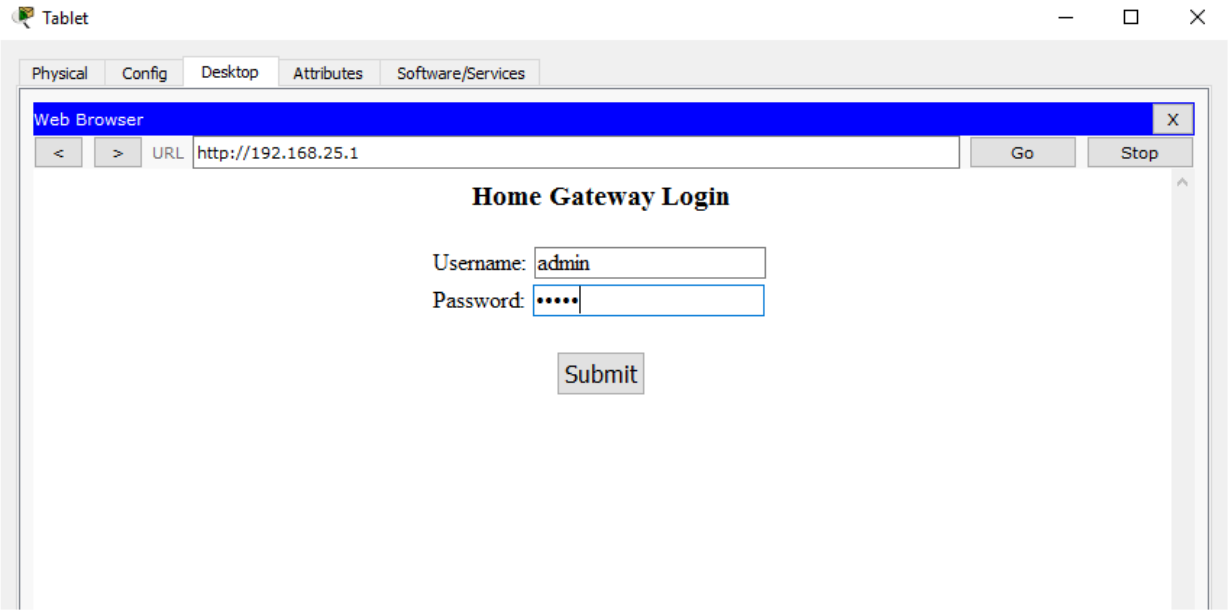
Закрийте вікно Home Gateway (Домашній шлюз).

Потім клацніть піктограму Tablet (Планшет), щоб відкрити вікно Tablet (Планшет).

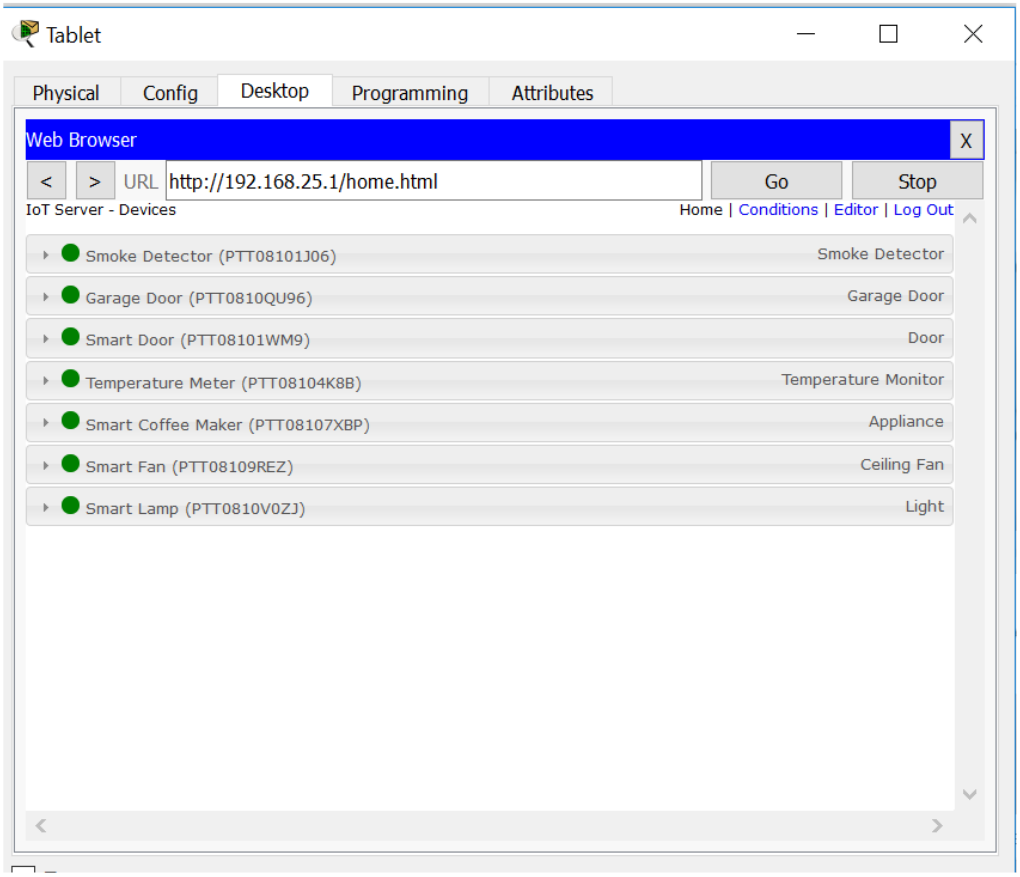
У вікні Tablet (Планшет) виберіть вкладку Desktop (Робочий стіл) та клацніть піктограму Web Browser (Веб-браузер).



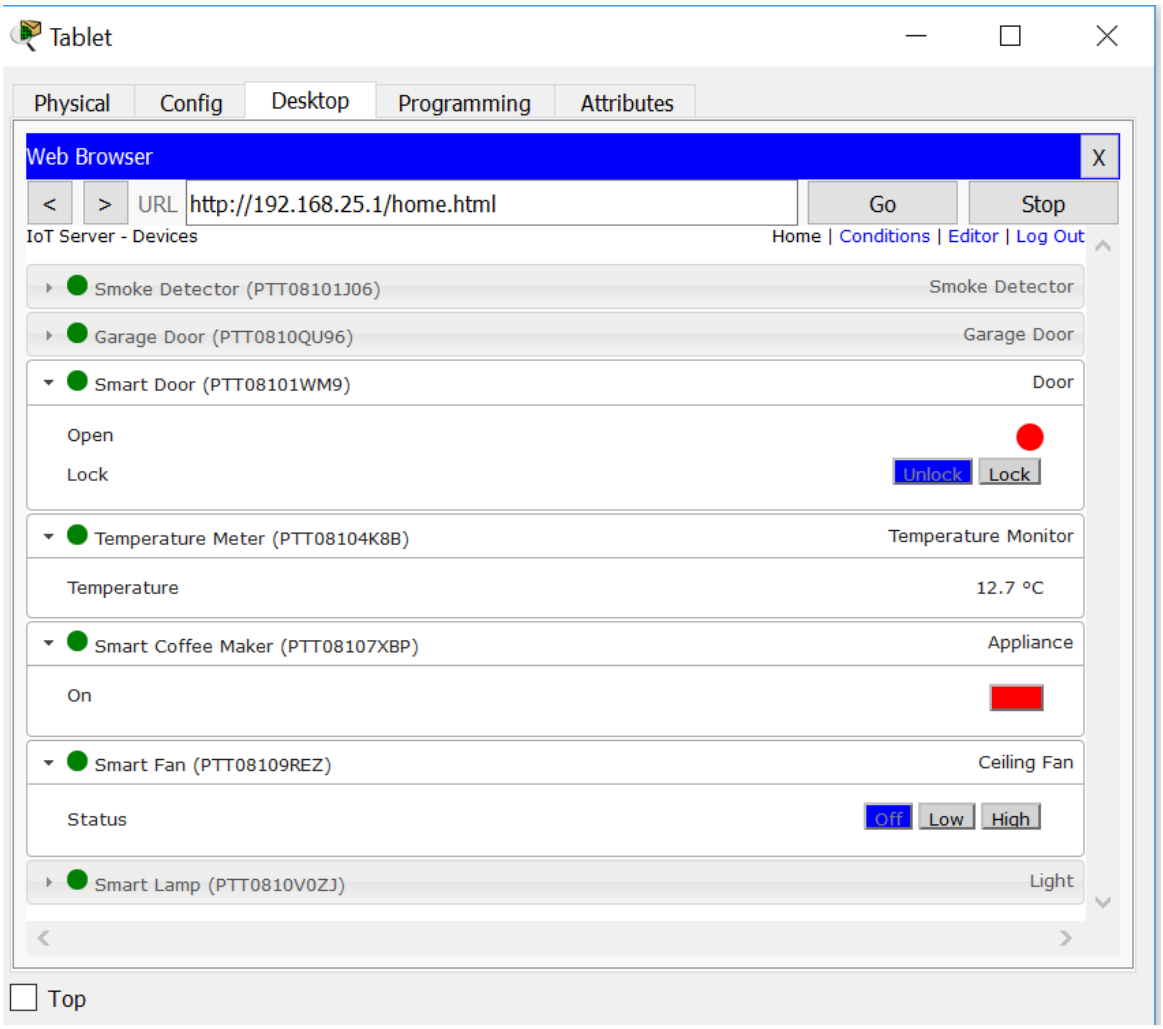
У вікні Web Browser (Веб-браузер) введіть IP-адресу домашнього шлюзу в полі URL-адреси. 192.168.25.1 та натисніть Go (Перейти). На екрані Home Gateway Login (Вхід до домашнього шлюзу) введіть admin як ім'я користувача та пароль, після чого натисніть кнопку Submit (Відправити).



Після підключення до веб-інтерфейсу домашнього шлюзу відкриється список усіх підключених пристроїв IoT.



Якщо клацнути пристрій у списку, на екрані з'явиться його статус та налаштування.



Закрийте вікно Tablet (Планшет).

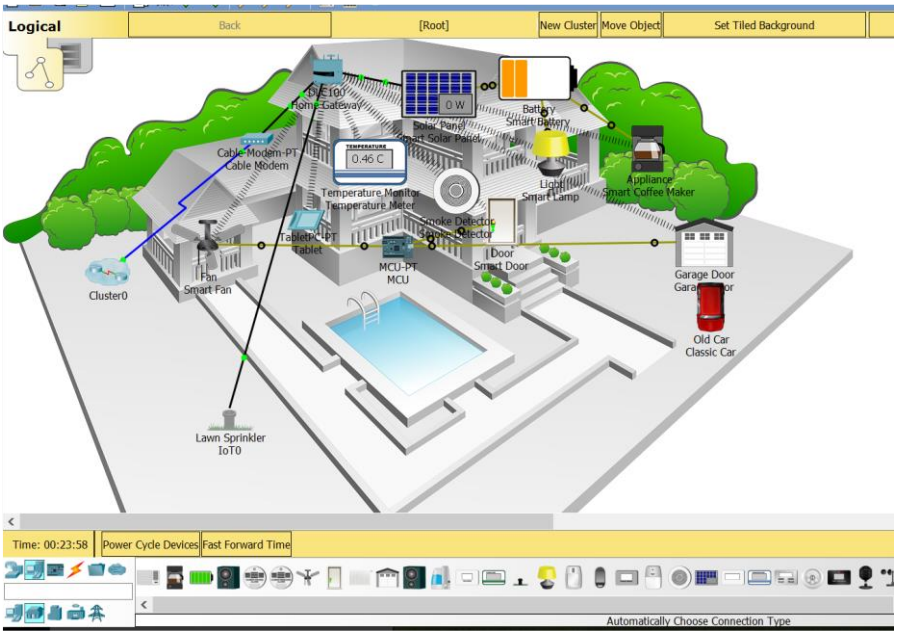
Частина 2: Додавання дротових пристроїв IoT до мережі розумного будинку

Крок 1: Підключення пристрою до мережі

a. У полі Device-Specific Selection (Вибір конкретного пристрою) клацніть піктограму Lawn Sprinkler (Установка для поливу), після чого клацніть там робочого простору, де необхідно розмістити Lawn Sprinkler (установку поливу).

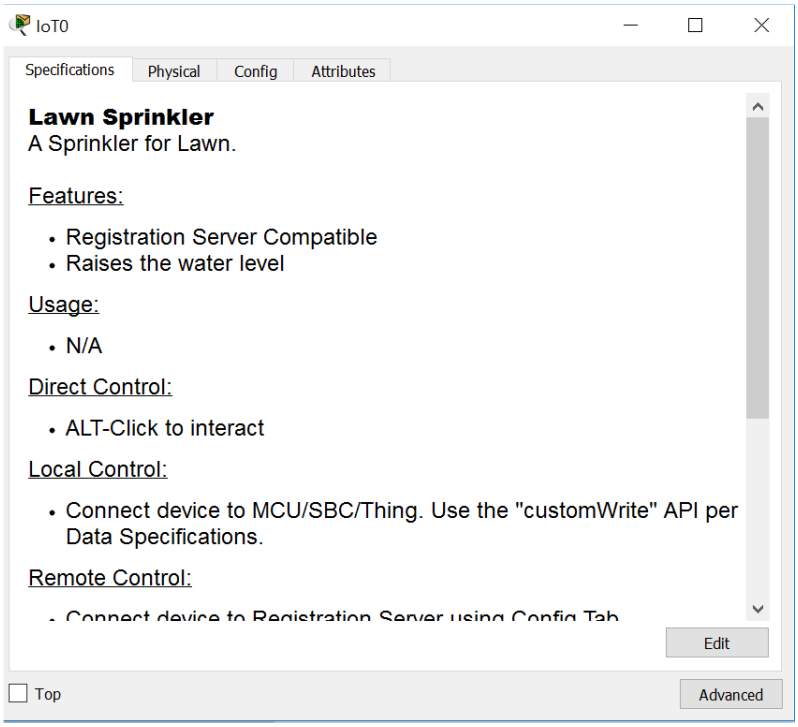
b. Підключіть до домашнього шлюзу систему пожежогасіння.

У полі Device-Type Selection (Вибір типу пристрою) клацніть піктограму [Connections] (Підключення) (вона виглядає як блискавка). Клацніть піктограму типу роз'єму Copper Straight Through (Мідний прямий) у полі Device-Specific Selection (Вибір конкретного пристрою). Далі клацніть піктограму Sprinkler (Розбризкувач) та підключіть один кінець кабелю до інтерфейсу FastEthernet0 розбризкувача. Тепер натисніть піктограму Home Gateway (Домашній шлюз) та підключіть інший кінець кабелю до вільного інтерфейсу Ethernet.



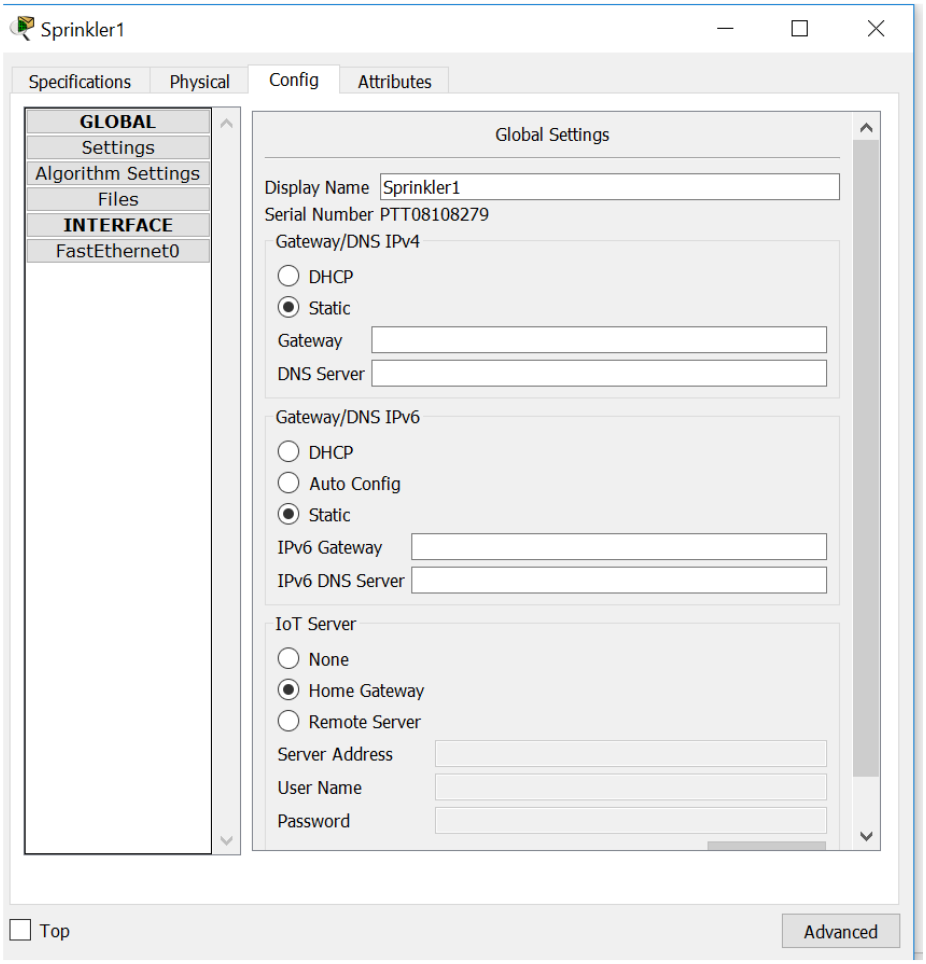
Крок 2. Налаштування підключення розбризкувача до мережі

a. Клацніть піктограму Lawn Sprinkler (Установка для поливу) у робочому просторі, щоб відкрити вікно пристрою. Зверніть увагу, що зараз установка для поливу має Універсальне ім'я IoT0. Вікно пристрою відкривається на вкладці Specification (Додаткові характеристики), де наведено інформація про пристрій, яку можна змінити.

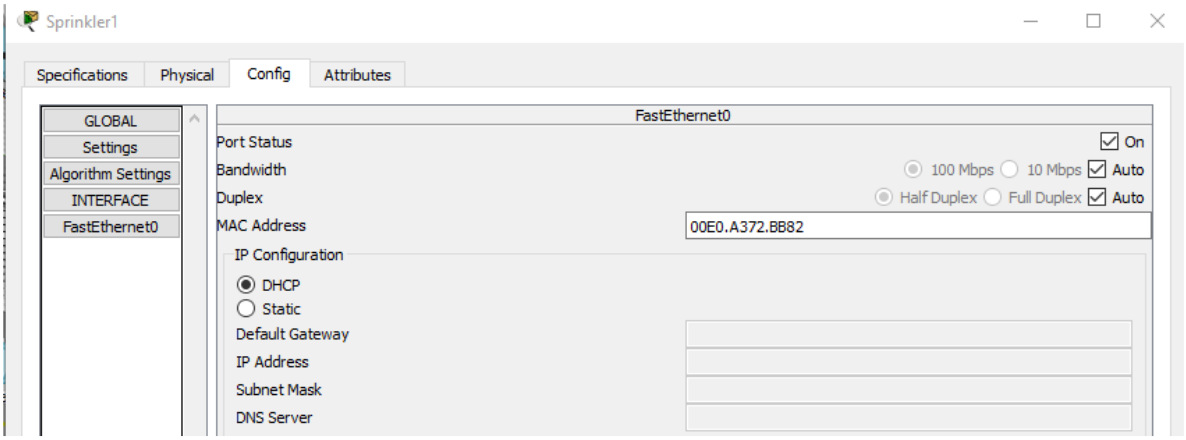


b. Відкрийте вкладку Config (Конфігурація), щоб змінити установки конфігурації пристрою. На вкладці Config (Конфігурація) у розділі Settings (Параметри) внесіть такі зміни.

– У полі Displa y Name (Ім'я, що відображається) введіть Sprinkler1 (зверніть увагу, що ім'я вікна зміниться на Sprinkler1).
– Встановіть Home Gateway (Домашній шлюз) як сервер IoT.



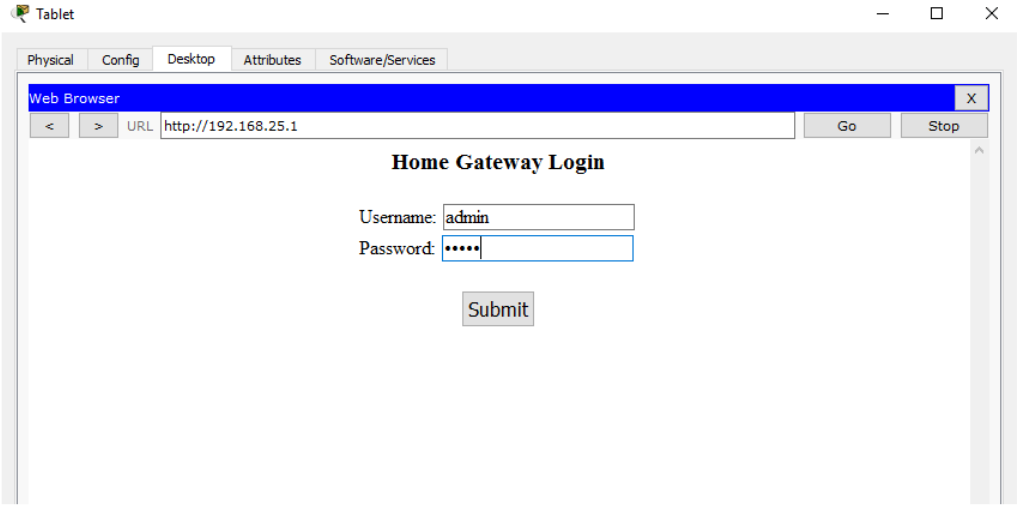
Клацніть FastEthernet0 та змініть значення параметра IP Configuration (Конфігурація IP) на DHCP.



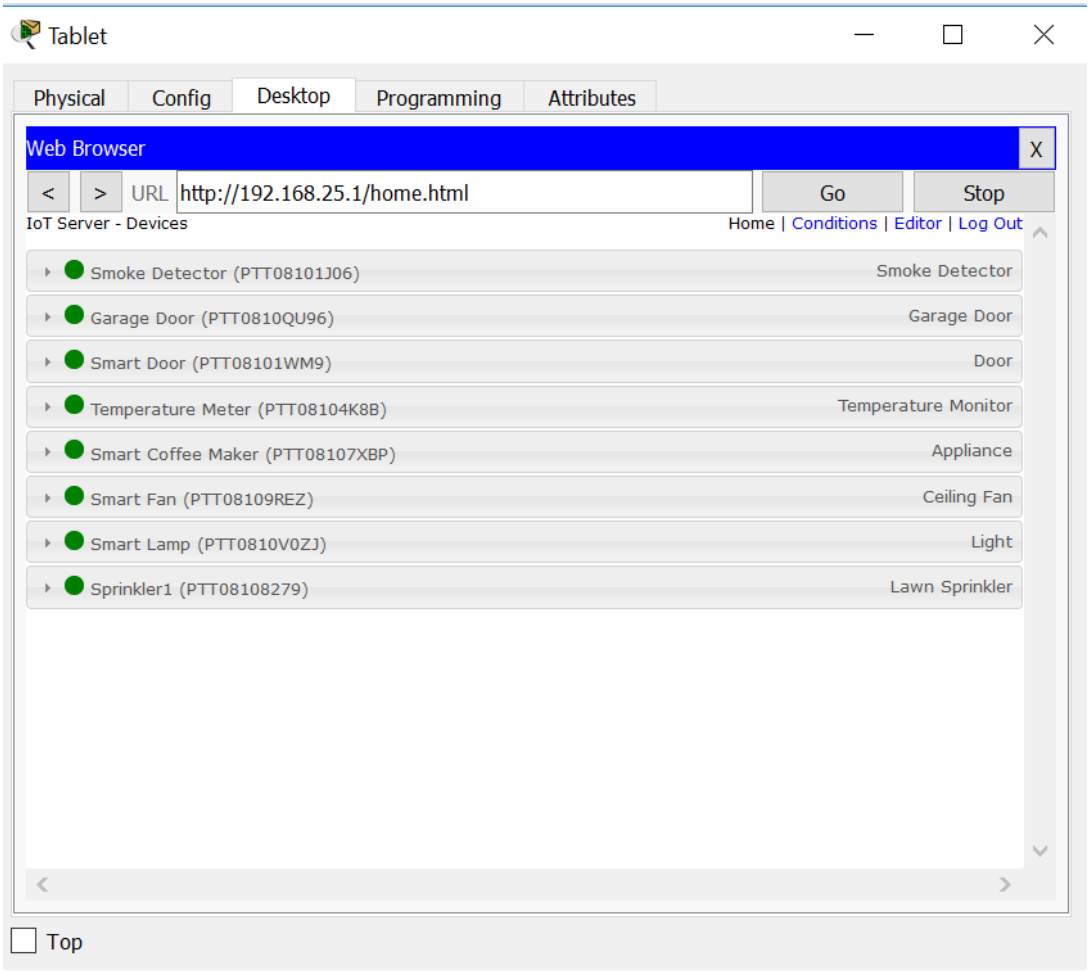
Закрийте вікно Sprinkler1.

с. Переконайтеся, що розбризкувач є у мережі.

Увійдіть до Home Gateway (Домашній шлюз) з вікна Tablet (Планшет).



Пристрій Sprinkler 1 має бути вказаний у списку IoT Server - Devices (Сервер IoT - пристрої).



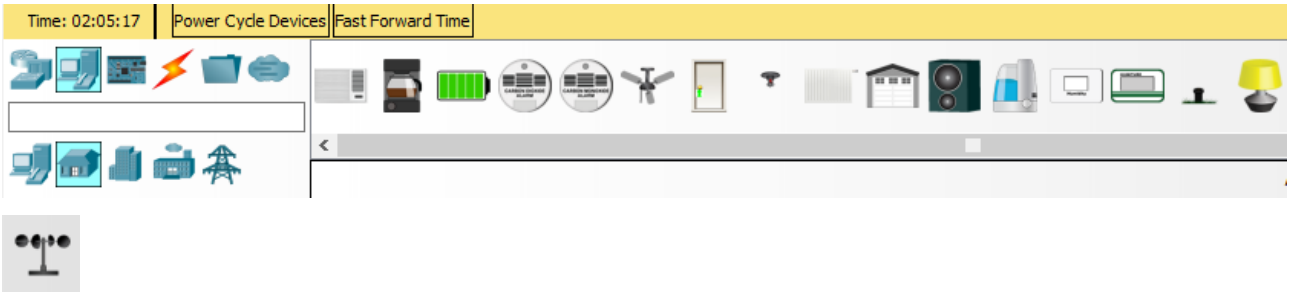
Закрийте вікно Tablet (Планшет).

Крок 3: Експерименти з додаванням до мережі розумного будинку пристроїв IoT інших типів. Додавання бездротових пристроїв IoT до мережі розумного будинку

Крок 4: Додавання бездротового пристрою до мережі

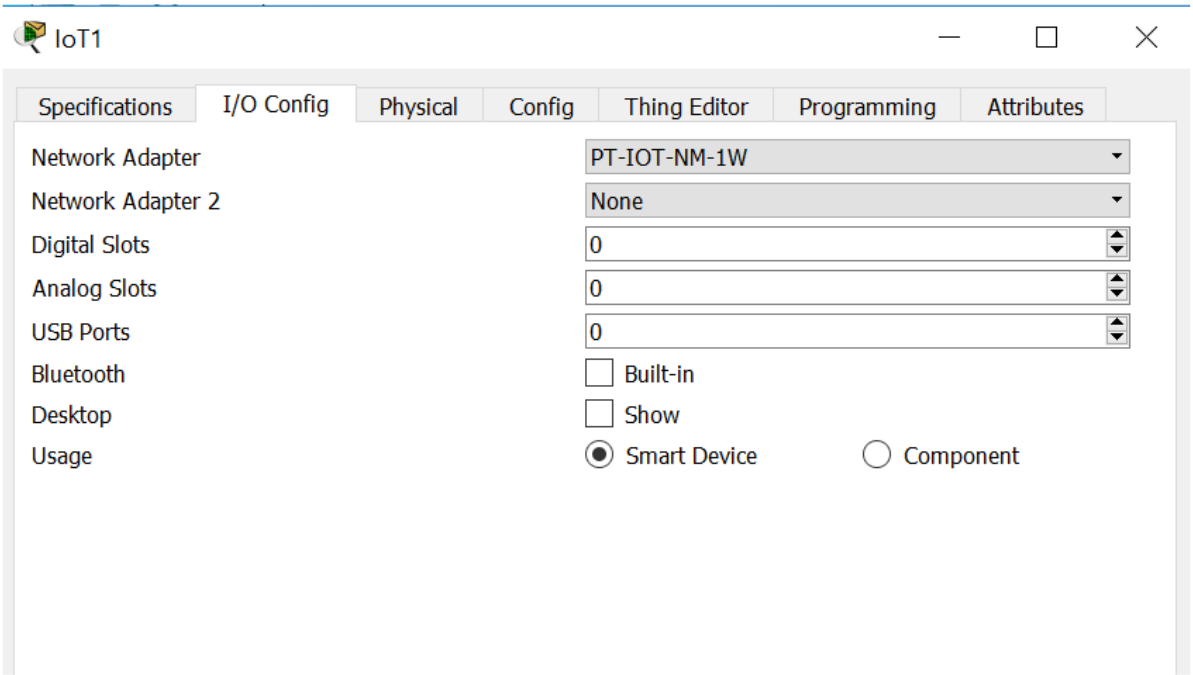
a. У полі Device-Specific Selection (Вибір конкретного пристрою) клацніть піктограму Wind Detector (Датчик вітру), а потім клацніть там робочого простору, де потрібно розмістити цей датчик вітру.

Вибір конкретного пристрою



b. Додайте бездротовий модуль до датчика вітру.

Клацніть піктограму Wind Detector (Датчик вітру) у робочому просторі, щоб відкрити вікно пристрої IoT. У нижньому правому куті вікна пристрою IoT натисніть кнопку Advanced (Додатково). Зверніть увагу, що у верхній частині вікна з'являються додаткові вкладки. Перейдіть на вкладку I/O Config (Налаштування вводу-виводу).

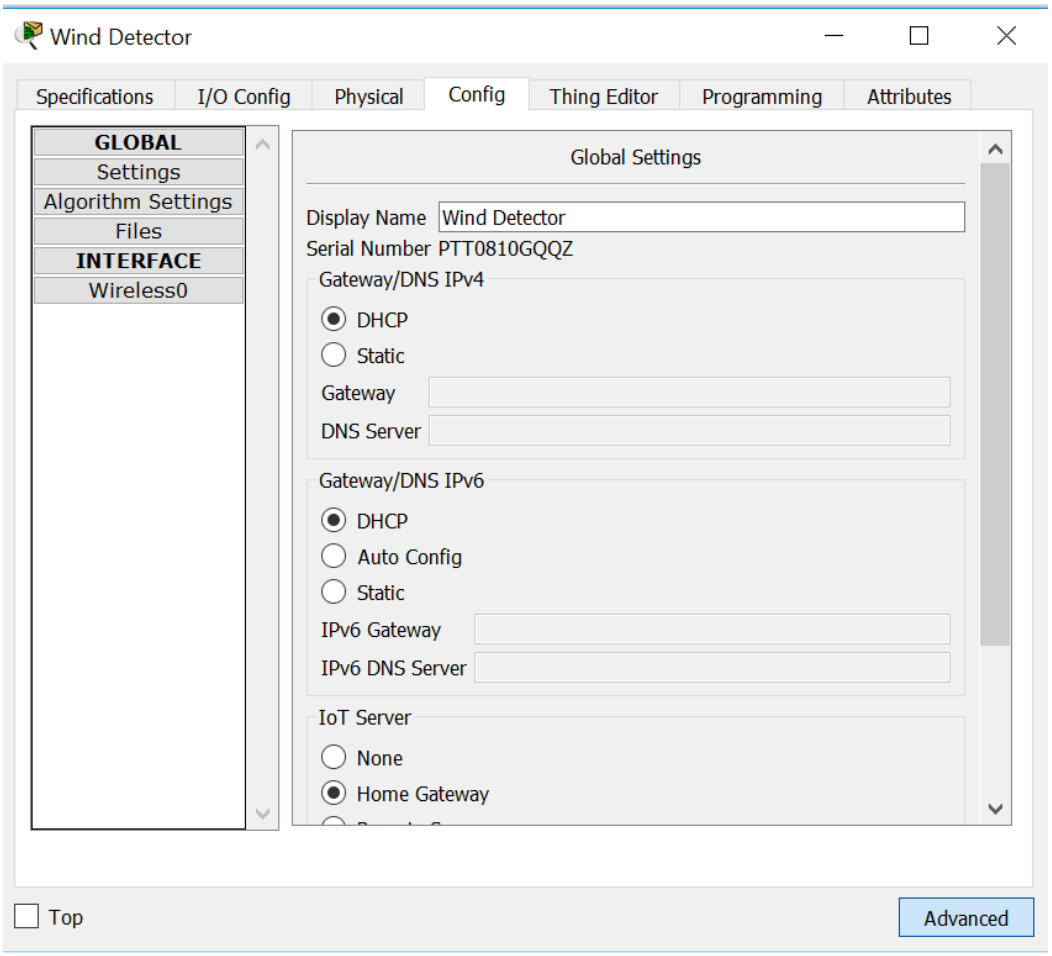


У списку Network Adapter (Мережний адаптер) виберіть PT-IOT-NM-1W (це бездротовий адаптер).

c. Налаштуйте на датчику вітру підключення до бездротової мережі.

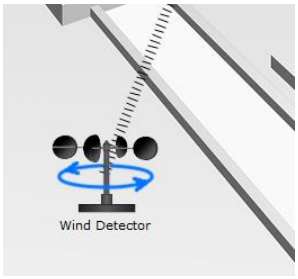
Клацніть вкладку Config (Налаштування).

У полі Display Name (Ім'я, що відображається) введіть Wind_Detector і змініть значення поля IoT Server (сервер IoT) на Home Gateway (Домашній шлюз).



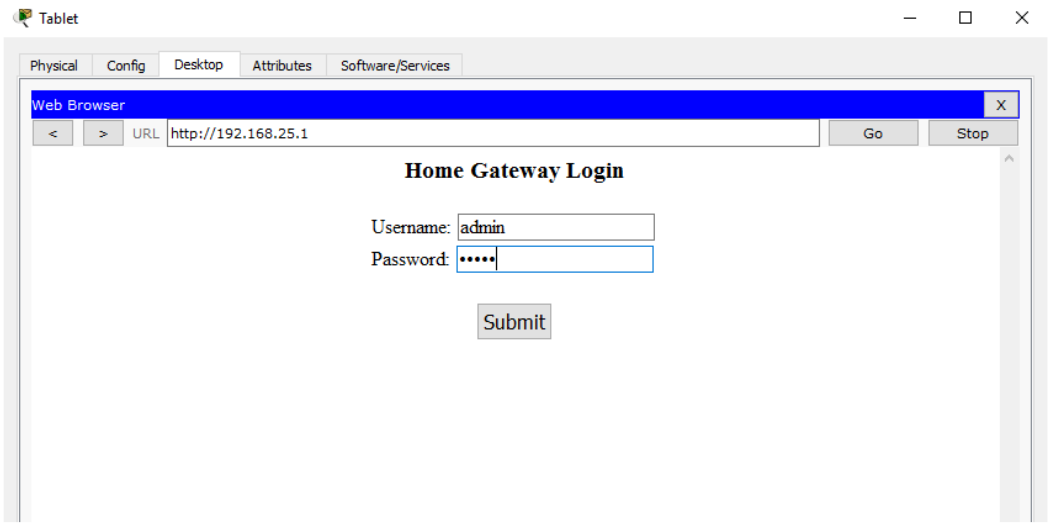
Потім клацніть Wireless0 у лівій панелі. Змініть тип аутентифікації на WPA2-PSK та в полі PSK Pass Phrase (кодова фраза PSK) введіть mySecretKey. Саме ці налаштування бездротовий зв'язок, задані на домашньому шлюзі, були записані під час виконання частини 1.

Потрібно встановити бездротове підключення між датчиком вітру та домашнім шлюзом.

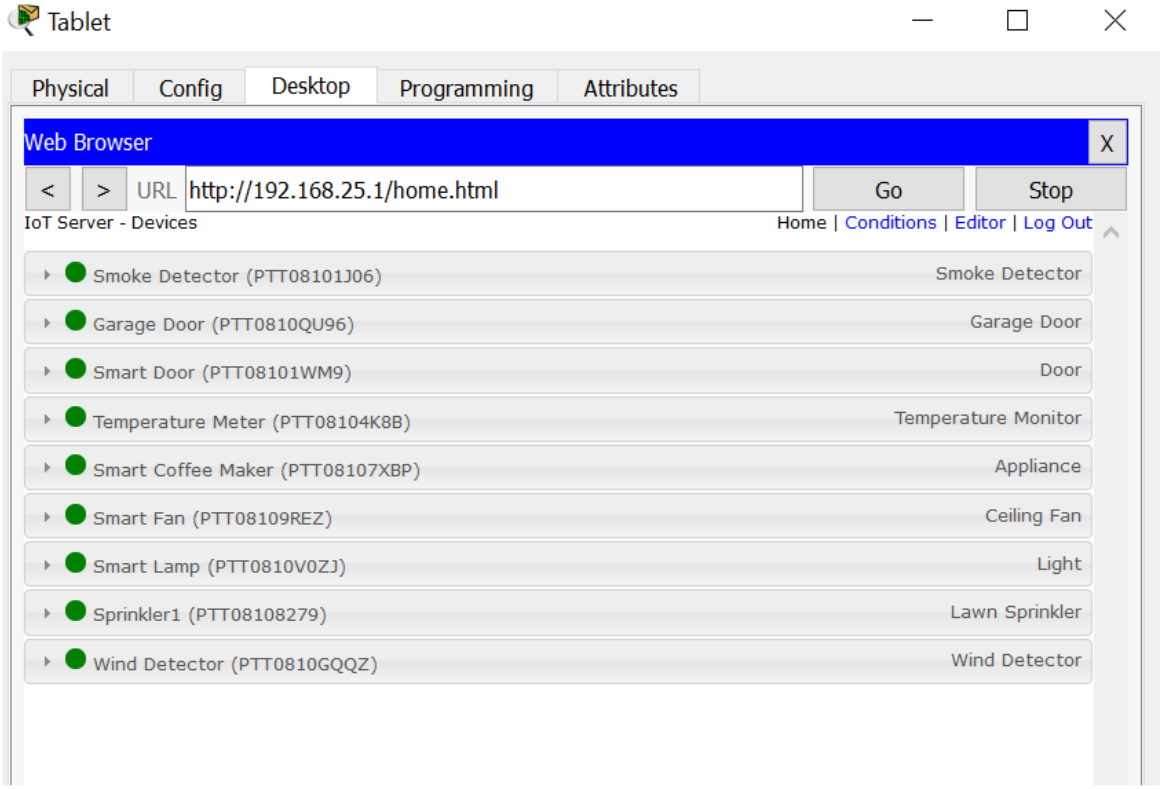


d. Перевірте, чи датчик вітру з'явився в мережі.

Увійдіть до Home Gateway (Домашній шлюз) з вікна Tablet (Планшет).



Тепер пристрій Wind Detector (Датчик вітру) має з'явитися у списку "IoT Server – Devices (Сервер IoT – пристрої).



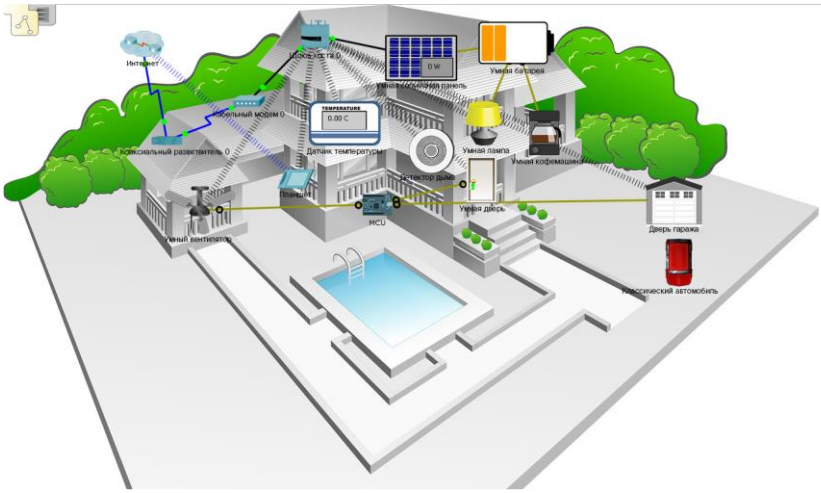
Закрийте вікно Tablet (Планшет).

Крок 5: Експерименти з додаванням до бездротової мережі розумного будинку пристроїв IoT інших типів__

Лабораторна робота 3

Додавання пристроїв IoT до розумного будинку

Мережа розумного будинку



Завдання

Частина 1. Вивчення існуючої мережі розумного будинку

Частина 2. Додавання дротових пристроїв IoT до мережі розумного будинку

Частина 3. Додавання бездротових пристроїв IoT до мережі розумного будинку

Загальні відомості/сценарій

У цій вправі відкривається файл Packet Tracer із вже налаштованою домашньою мережею, вивчаються підключені до мережі пристрої, а потім додаються додаткові дротові та бездротові пристрої IoT.

Частина 1: Вивчення існуючої мережі розумного будинку

Крок 1: Відкриття файлу Smart_Home_Network.pkt

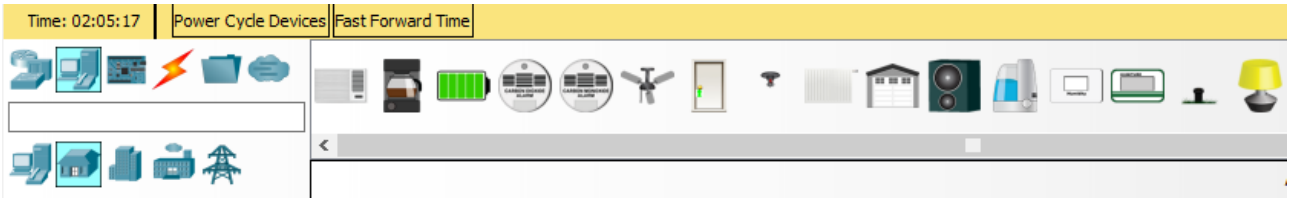
a. Відкрийте файл Smart_Home_Network.pkt.

b. Збережіть файл на комп'ютері.

Крок 2: Вивчення мережі розумного будинку

a. Досліджуйте кінцеві пристрої IoT.

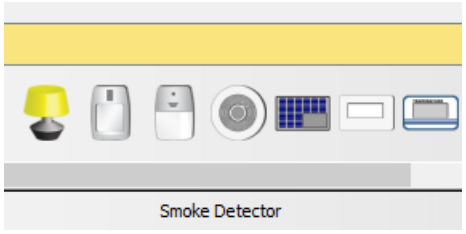
У нижньому лівому куті вікна Packet Tracer клацніть піктограму [End Devices] (Кінці пристрої) у верхньому рядку, а потім клацніть піктограму [Home] (Будинок) у нижньому будівництві поля Device-Type Selection (Вибір типу пристрою).



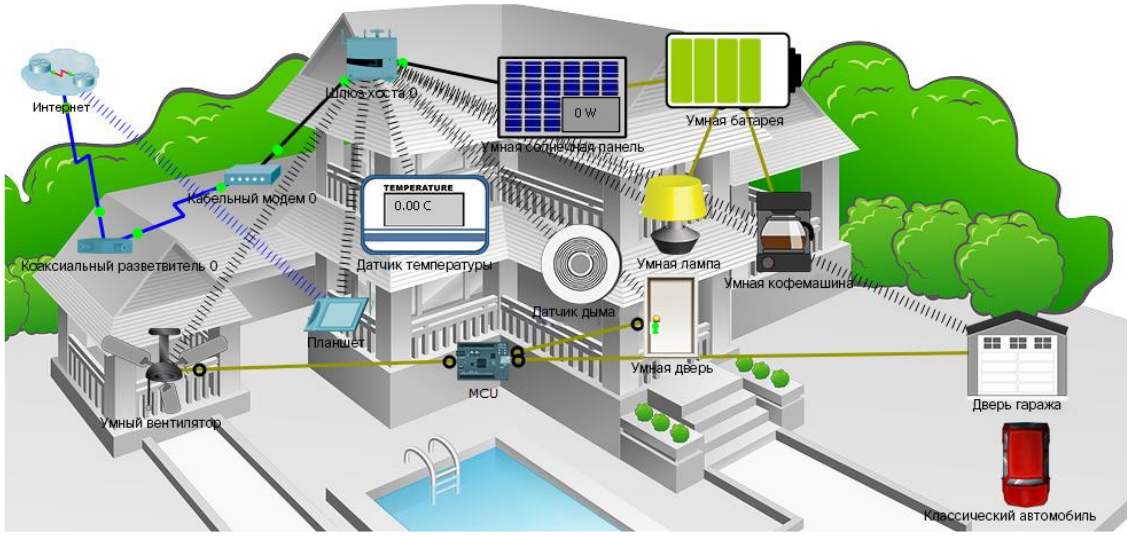
У нижній частині вікна Packet Tracer у полі Device-Specific Selection (Вибір конкретного

пристрої) відображається безліч доступних пристроїв IoT для розумного будинку.

Наведіть вказівник миші на кожен пристрій і зверніть увагу, що при цьому в нижній частини поля Device-Specific Selection (Вибір конкретного пристрою) відображається описово Ім'я цього пристрою. Детально розгляньте пристрій кожного типу.



b. Вивчіть мережу розумного будинку.



У логічному робочому просторі знаходиться заздалегідь створена мережа розумного будинку, яка складається з безлічі дротових та бездротових пристроїв IoT, а також пристроїв мережної інфраструктури.

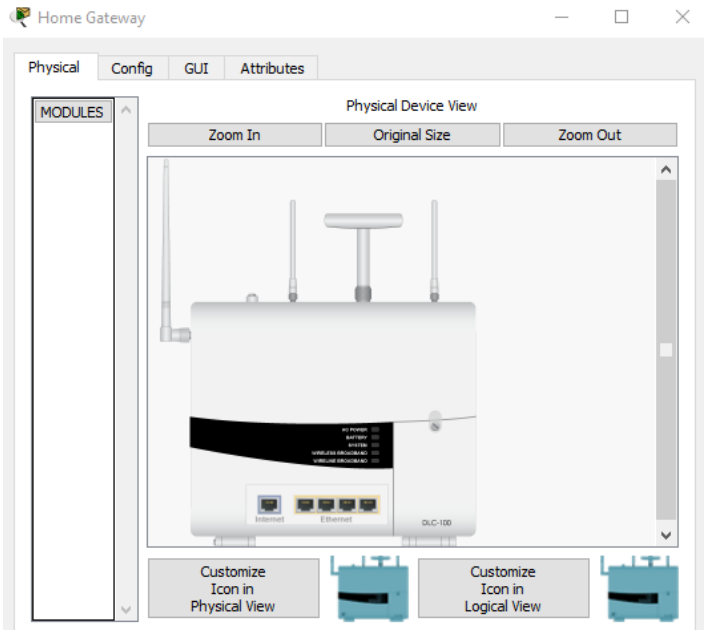
При наведенні курсору на пристрій, наприклад, на розумний вентилятор, відкривається інформаційне вікно з базовою мережевою інформацією про цей пристрій.

Щоб увімкнути або активувати пристрій, просто натисніть клавішу Alt і утримуйте її. натиснутою, клацніть пристрій лівою кнопкою миші. Зробіть це з кожним розумним пристроєм, щоб спостерігати, що з ними відбувається.

У мережі розумного будинку також є пристрої мережної інфраструктури, наприклад, домашній шлюз.

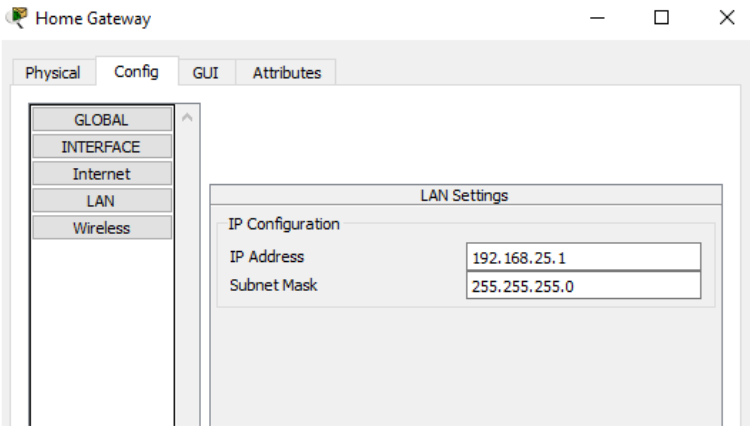
Натисніть піктограму **Home Gateway** (Домашній шлюз), щоб відкрити вікно Home Gateway (Домашній шлюз)

Виберіть вкладку Physical (Фізичні налаштування) за замовчуванням. На ній показано зображення домашнього шлюзу.



Тепер перейдіть на вкладку Config (Конфігурація), а потім у лівій панелі клацніть LAN (Локальна мережа), щоб переглянути установки локальної мережі домашнього шлюзу.

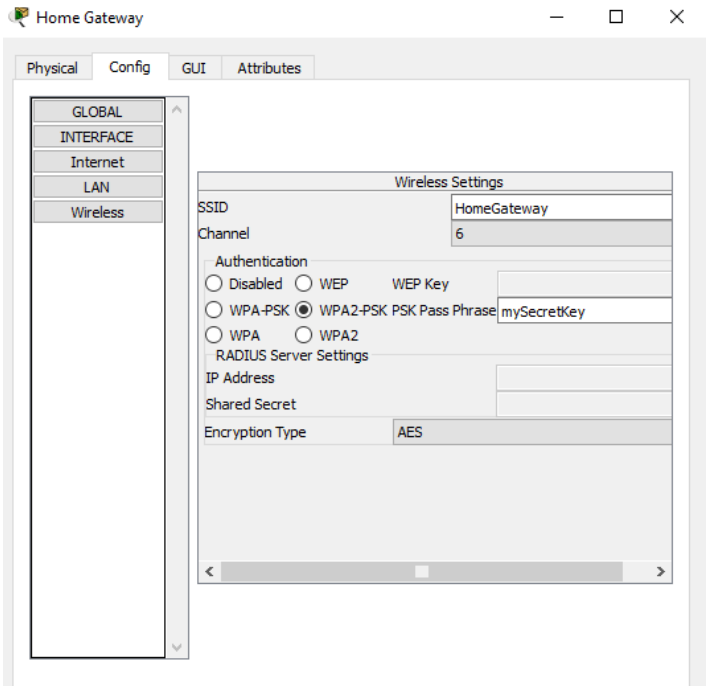
Запишіть IP-адресу домашньої мережі для використання в майбутньому. _____



Натисніть Wireless (Бездротовий зв'язок) у лівій панелі, щоб переглянути настройки бездротового зв'язку домашнього шлюзу.

Запишіть ідентифікатор SSID домашньої мережі _____та кодову фразу WPA2-

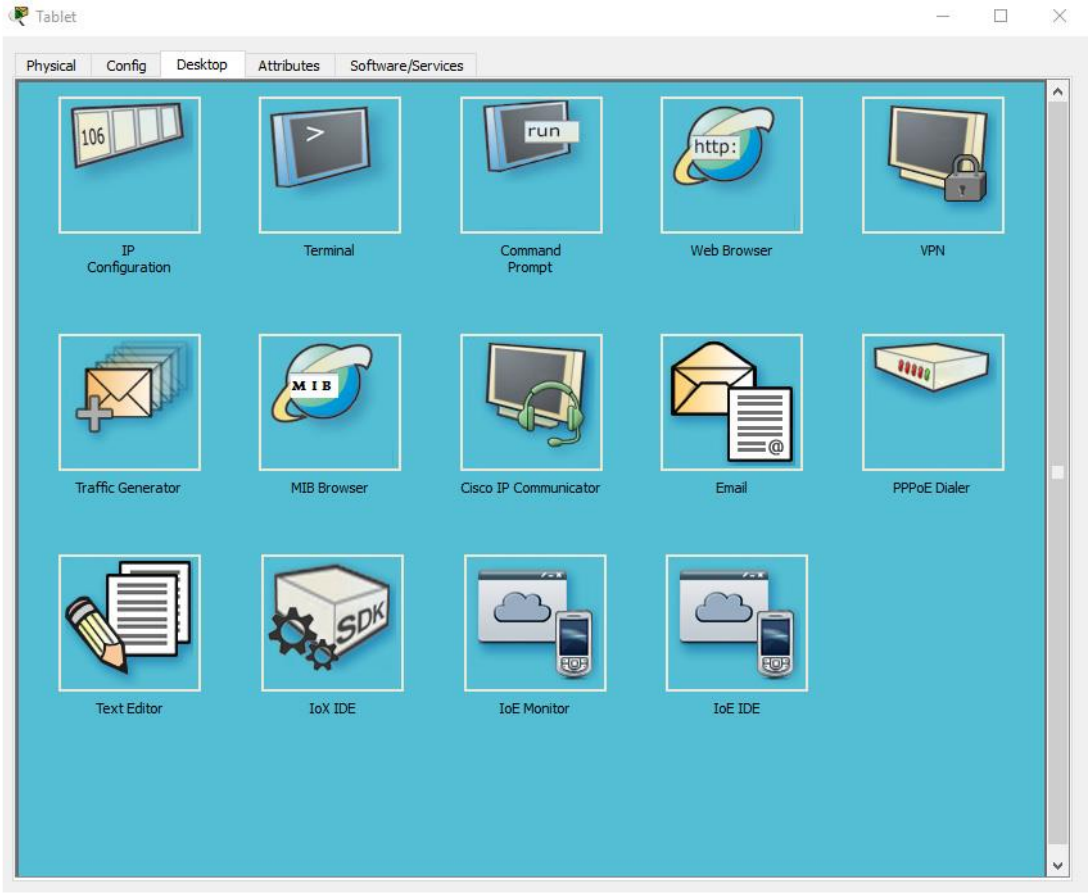
PSK_____ для використання у майбутньому.



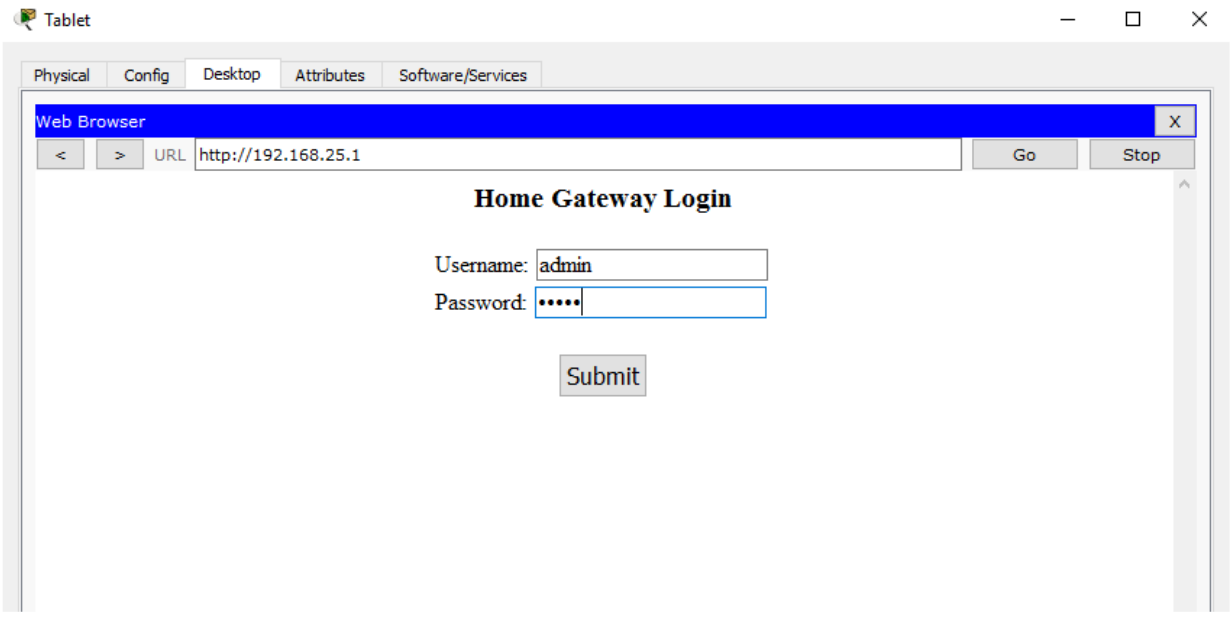
Закрийте вікно Home Gateway (Домашній шлюз).

Потім клацніть піктограму Tablet (Планшет), щоб відкрити вікно Tablet (Планшет).

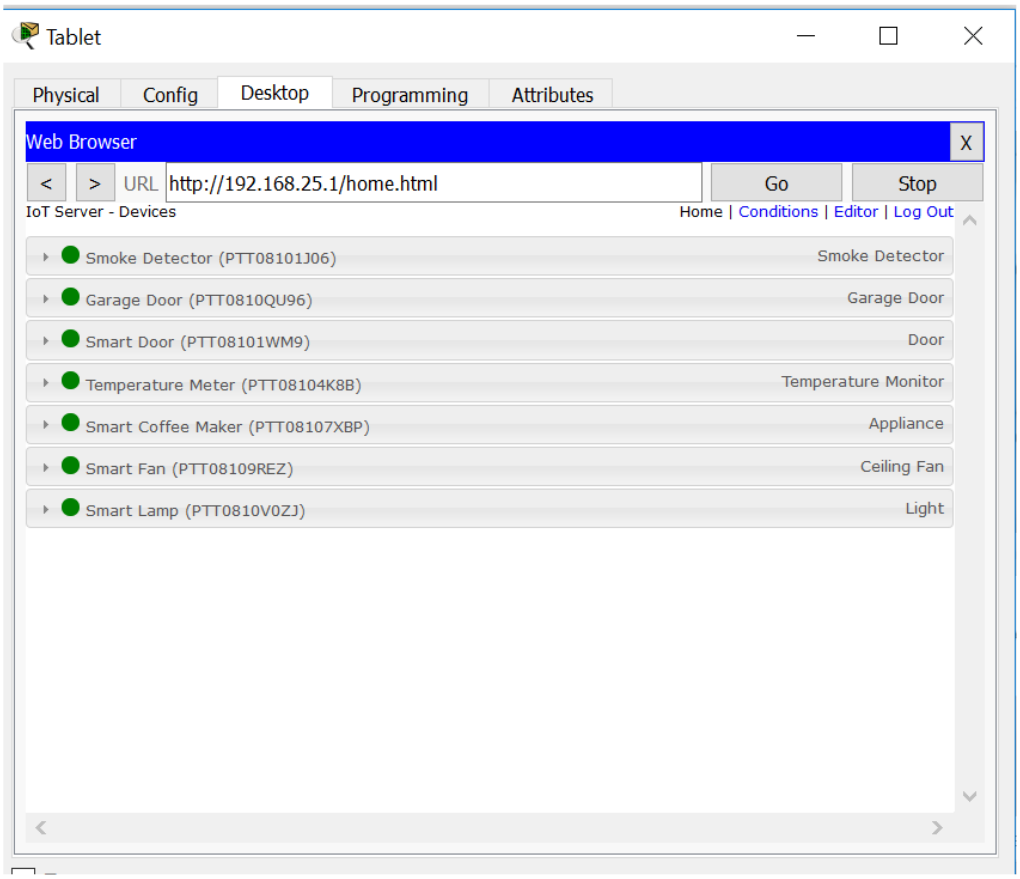
У вікні Tablet (Планшет) виберіть вкладку Desktop (Робочий стіл) та клацніть піктограму Web Browser (Веб-браузер).



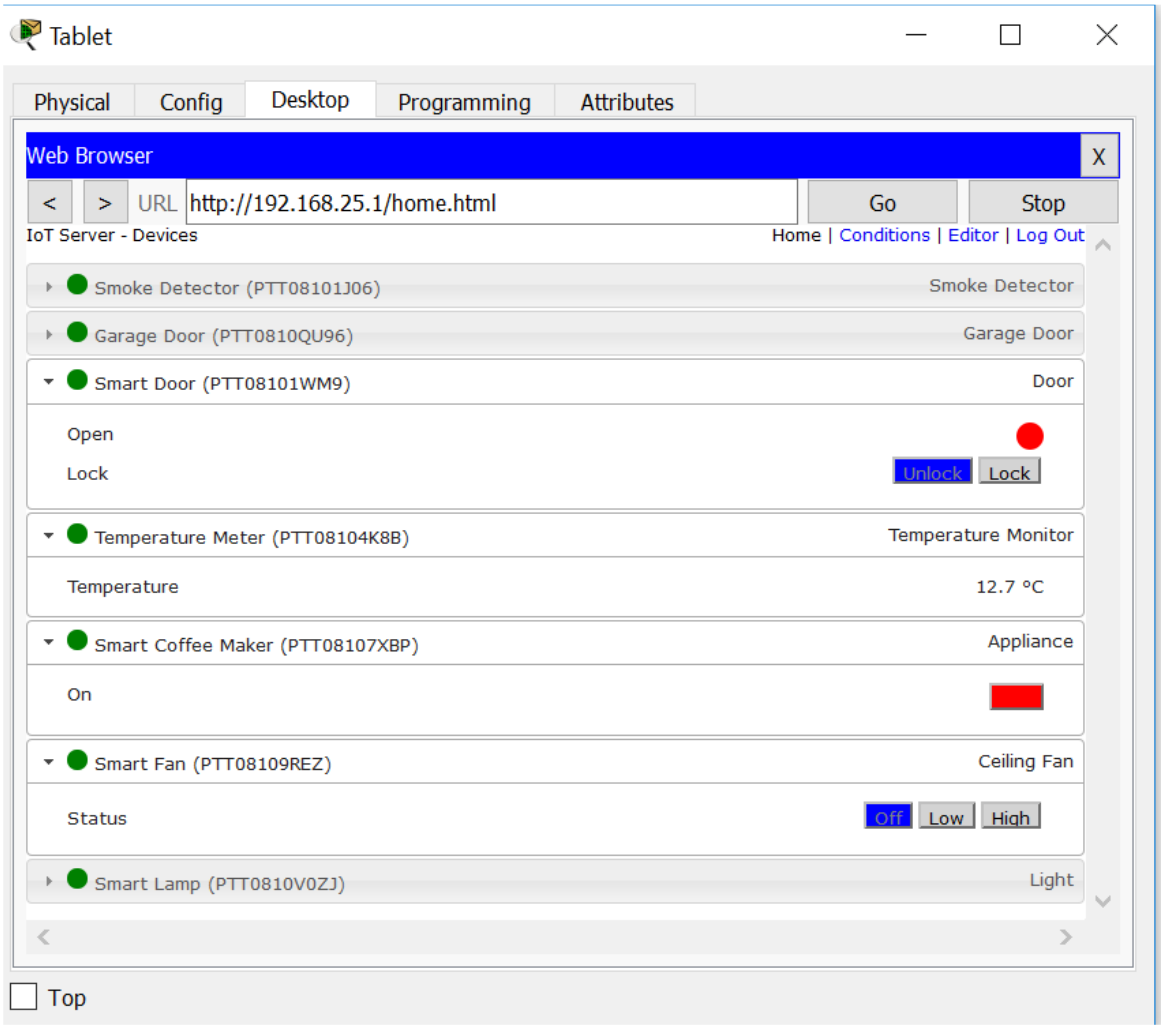
У вікні Web Browser (Веб-браузер) введіть IP-адресу домашнього шлюзу в полі URL-адреси. 192.168.25.1 та натисніть Go (Перейти). На екрані Home Gateway Login (Вхід до домашнього шлюзу) введіть admin як ім'я користувача та пароль, після чого натисніть кнопку Submit (Відправити).



Після підключення до веб-інтерфейсу домашнього шлюзу відкриється список усіх підключених пристроїв IoT.



Якщо клацнути пристрій у списку, на екрані з'явиться його статус та налаштування.



Закрийте вікно Tablet (Планшет).

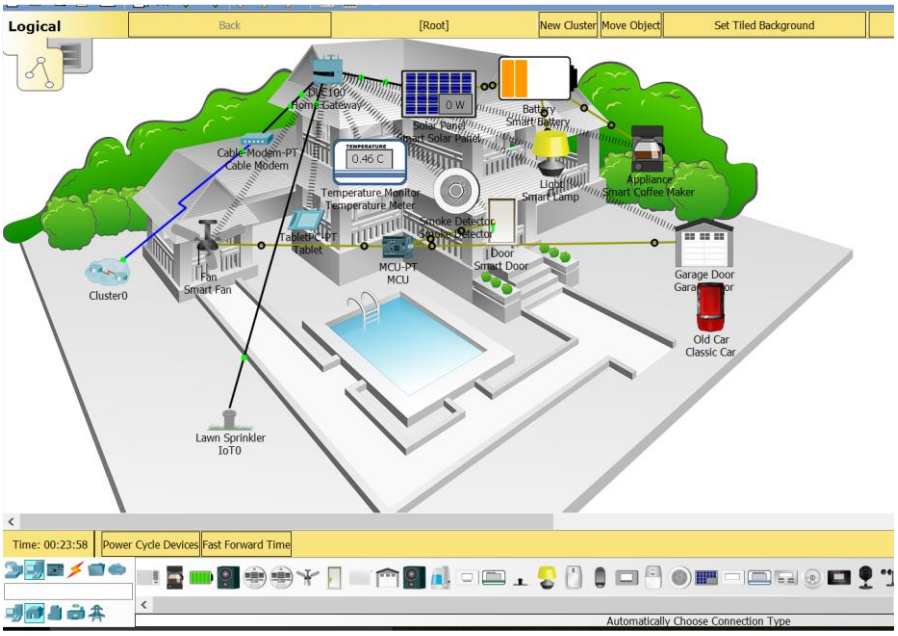
Частина 2: Додавання дротових пристроїв IoT до мережі розумного будинку

Крок 1: Підключення пристрою до мережі

a. У полі Device-Specific Selection (Вибір конкретного пристрою) клацніть піктограму Lawn Sprinkler (Установка для поливу), після чого клацніть там робочого простору, де необхідно розмістити Lawn Sprinkler (установку поливу).

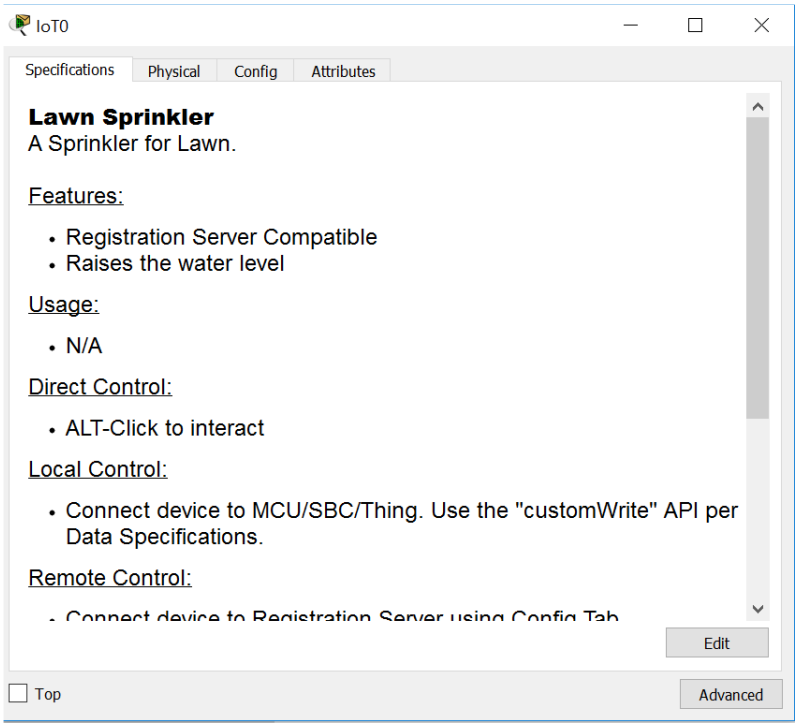
b. Підключіть до домашнього шлюзу систему пожежогасіння.

У полі Device-Type Selection (Вибір типу пристрою) клацніть піктограму [Connections] (Підключення) (вона виглядає як блискавка). Клацніть піктограму типу роз'єму Copper Straight Through (Мідний прямий) у полі Device-Specific Selection (Вибір конкретного пристрою). Далі клацніть піктограму Sprinkler (Розбризкувач) та підключіть один кінець кабелю до інтерфейсу FastEthernet0 розбризкувача. Тепер натисніть піктограму Home Gateway (Домашній шлюз) та підключіть інший кінець кабелю до вільного інтерфейсу Ethernet.



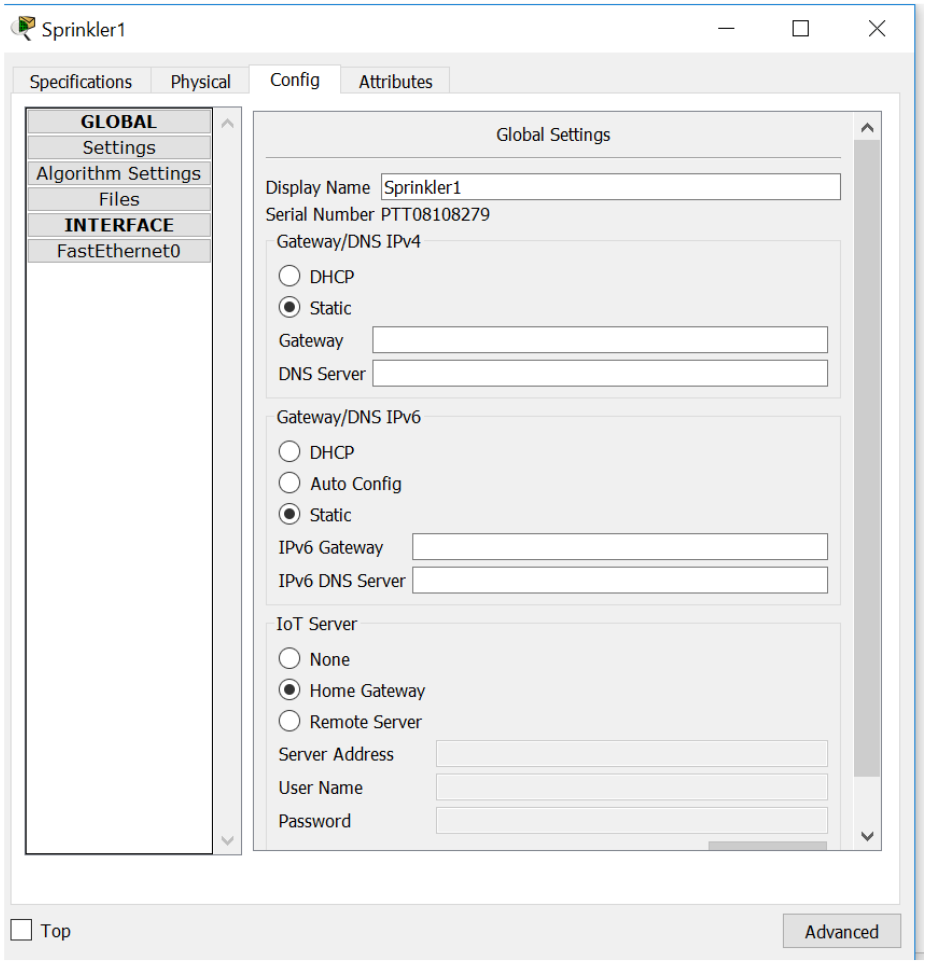
Крок 2. Налаштування підключення розбризкувача до мережі

a. Клацніть піктограму Lawn Sprinkler (Установка для поливу) у робочому просторі, щоб відкрити вікно пристрою. Зверніть увагу, що зараз установка для поливу має Універсальне ім'я IoT0. Вікно пристрою відкривається на вкладці Specification (Додаткові характеристики), де наведено інформація про пристрій, яку можна змінити.

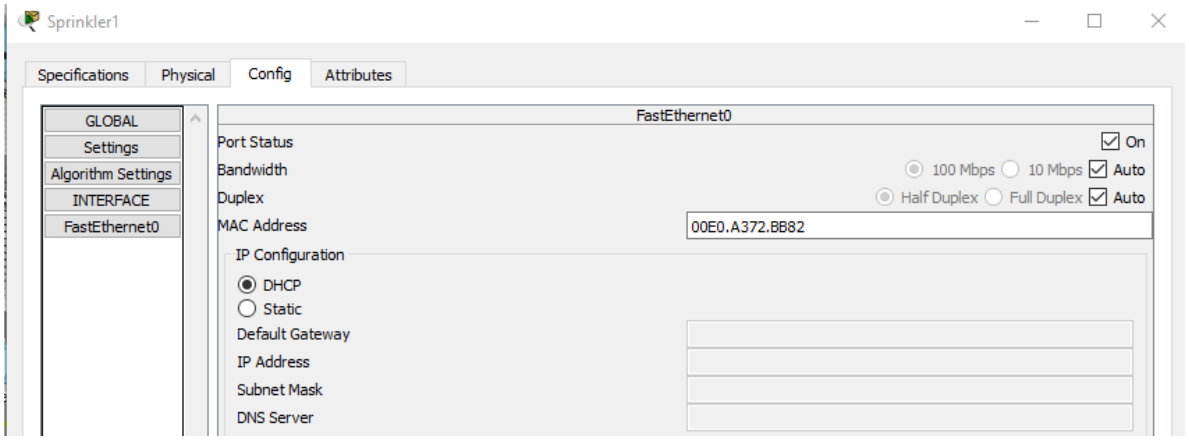


b. Відкрийте вкладку Config (Конфігурація), щоб змінити установки конфігурації пристрою. На вкладці Config (Конфігурація) у розділі Settings (Параметри) внесіть такі зміни.

– У полі Displa y Name (Ім'я, що відображається) введіть Sprinkler1 (зверніть увагу, що ім'я вікна зміниться на Sprinkler1).
– Встановіть Home Gateway (Домашній шлюз) як сервер IoT.



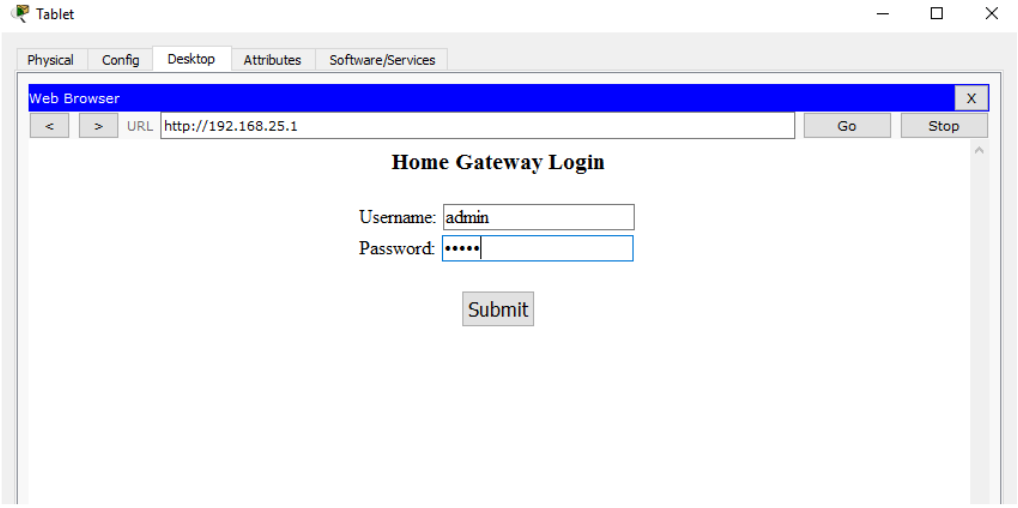
Клацніть FastEthernet0 та змініть значення параметра IP Configuration (Конфігурація IP) на DHCP.



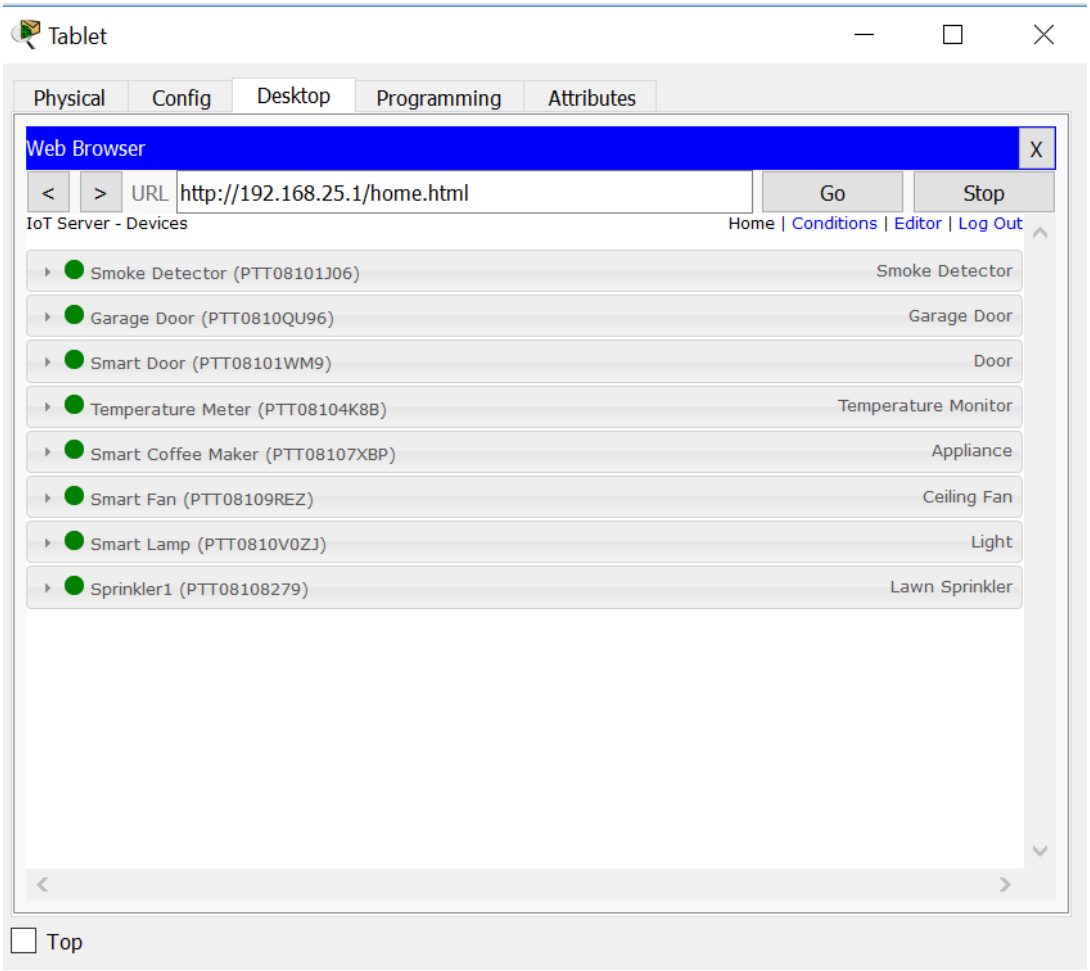
Закрийте вікно Sprinkler1.

с. Переконайтеся, що розбризкувач є у мережі.

Увійдіть до Home Gateway (Домашній шлюз) з вікна Tablet (Планшет).



Пристрій Sprinkler 1 має бути вказаний у списку IoT Server - Devices (Сервер IoT - пристрої).



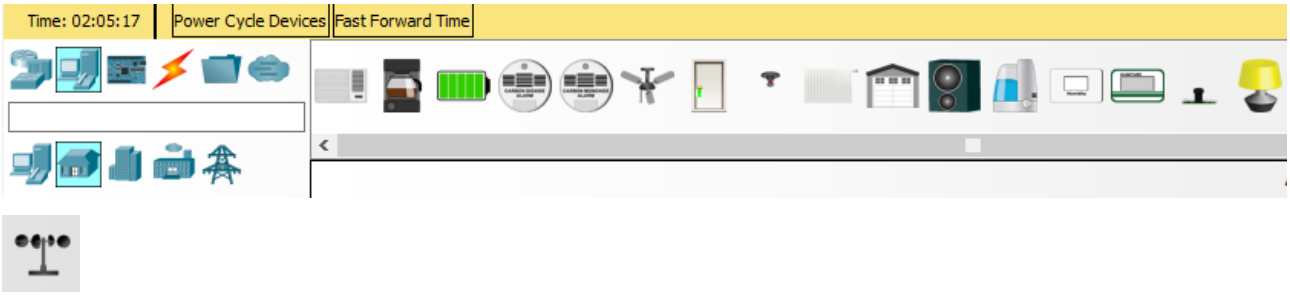
Закрийте вікно Tablet (Планшет).

Крок 3: Експерименти з додаванням до мережі розумного будинку пристроїв IoT інших типів. Додавання бездротових пристроїв IoT до мережі розумного будинку

Крок 4: Додавання бездротового пристрою до мережі

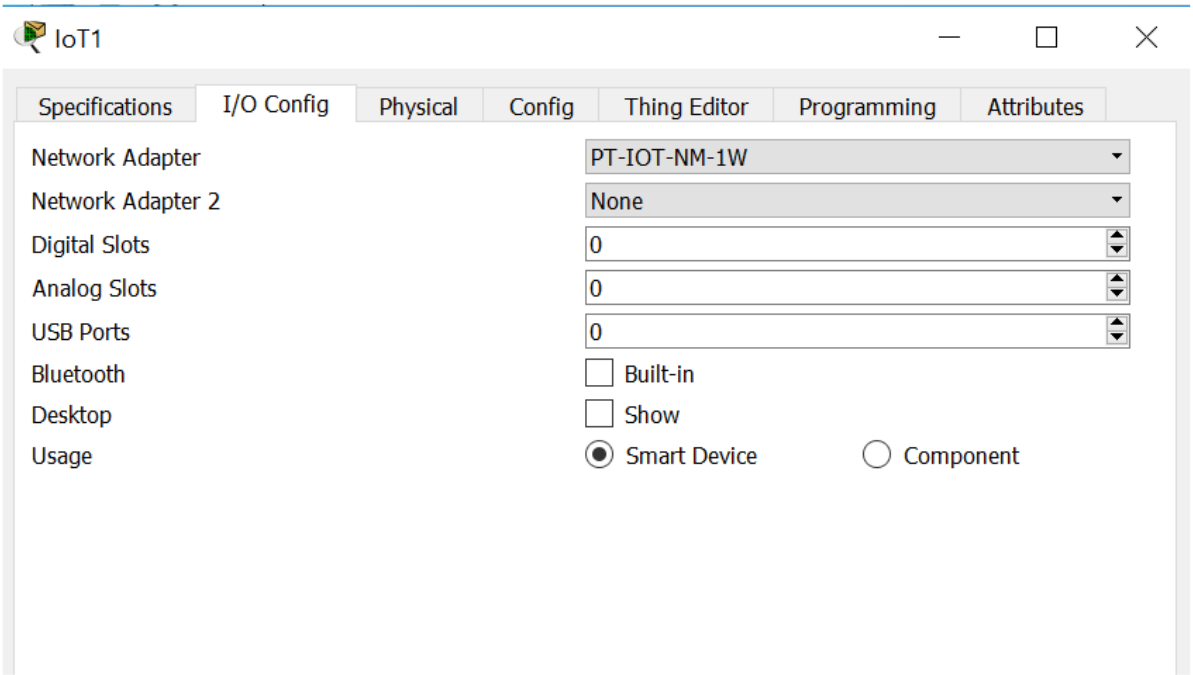
a. У полі Device-Specific Selection (Вибір конкретного пристрою) клацніть піктограму Wind Detector (Датчик вітру), а потім клацніть там робочого простору, де потрібно розмістити цей датчик вітру.

Вибір конкретного пристрою



b. Додайте бездротовий модуль до датчика вітру.

Клацніть піктограму Wind Detector (Датчик вітру) у робочому просторі, щоб відкрити вікно пристрої IoT. У нижньому правому куті вікна пристрою IoT натисніть кнопку Advanced (Додатково). Зверніть увагу, що у верхній частині вікна з'являються додаткові вкладки. Перейдіть на вкладку I/O Config (Налаштування вводу-виводу).

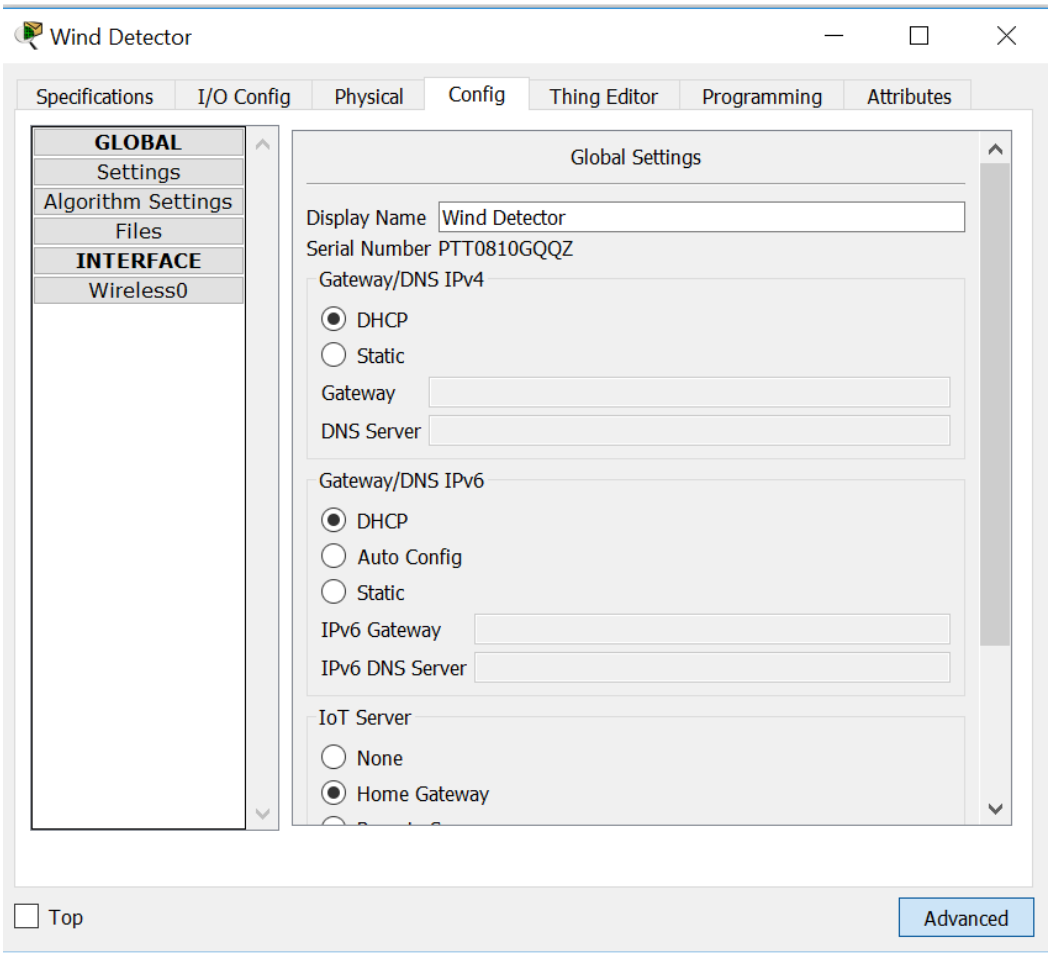


У списку Network Adapter (Мережний адаптер) виберіть PT-IOT-NM-1W (це бездротовий адаптер).

c. Налаштуйте на датчику вітру підключення до бездротової мережі.

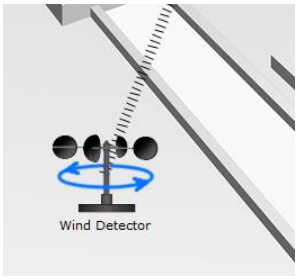
Клацніть вкладку Config (Налаштування).

У полі Display Name (Ім'я, що відображається) введіть Wind_Detector і змініть значення поля IoT Server (сервер IoT) на Home Gateway (Домашній шлюз).



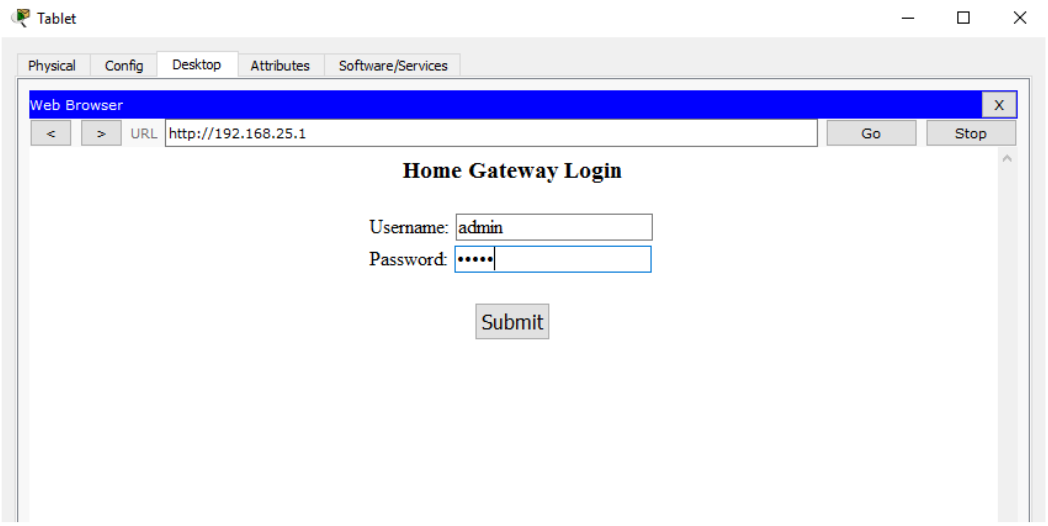
Потім клацніть Wireless0 у лівій панелі. Змініть тип аутентифікації на WPA2-PSK та в полі PSK Pass Phrase (кодова фраза PSK) введіть mySecretKey. Саме ці налаштування бездротовий зв'язок, задані на домашньому шлюзі, були записані під час виконання частини 1.

Потрібно встановити бездротове підключення між датчиком вітру та домашнім шлюзом.

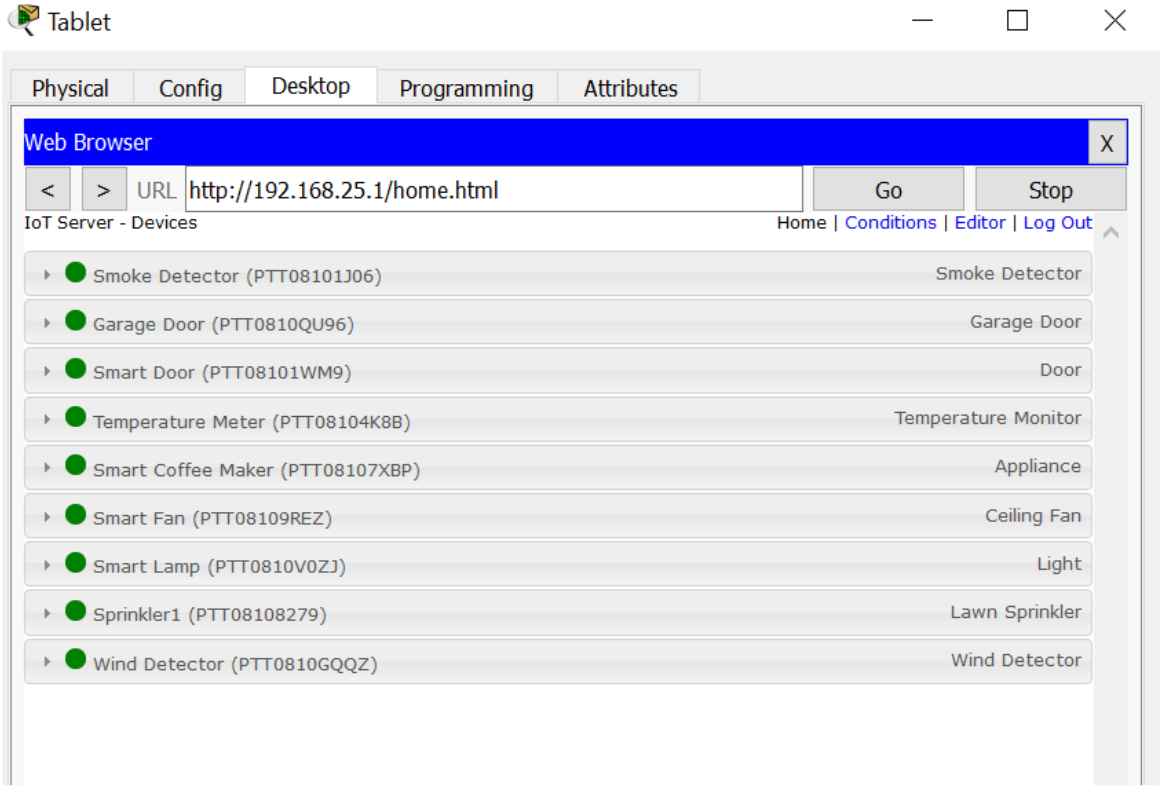


d. Перевірте, чи датчик вітру з'явився в мережі.

Увійдіть до Home Gateway (Домашній шлюз) з вікна Tablet (Планшет).



Тепер пристрій Wind Detector (Датчик вітру) має з'явитися у списку "IoT Server – Devices (Сервер IoT – пристрої).



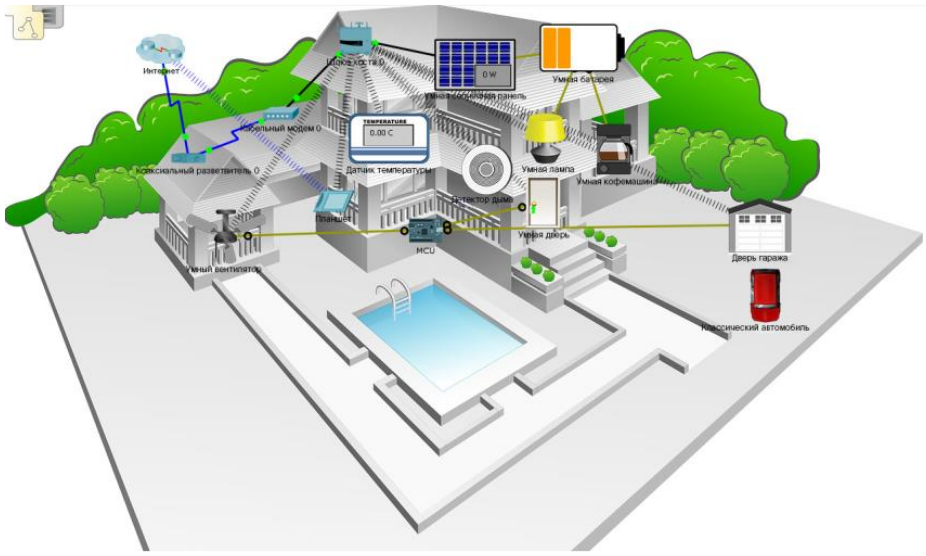
Закрийте вікно Tablet (Планшет).

Крок 5: Експерименти з додаванням до бездротової мережі розумного будинку пристроїв IoT інших типів__

Лабораторна робота 4

Packet Tracer. Підключення пристроїв IoT та моніторинг їх роботи

Мережа розумного будинку



Завдання

Частина 1. Додавання до мережі домашнього шлюзу

Частина 2. Підключення пристроїв IoT до бездротової мережі

Частина 3. Додавання до мережі кінцевого пристрою користувача

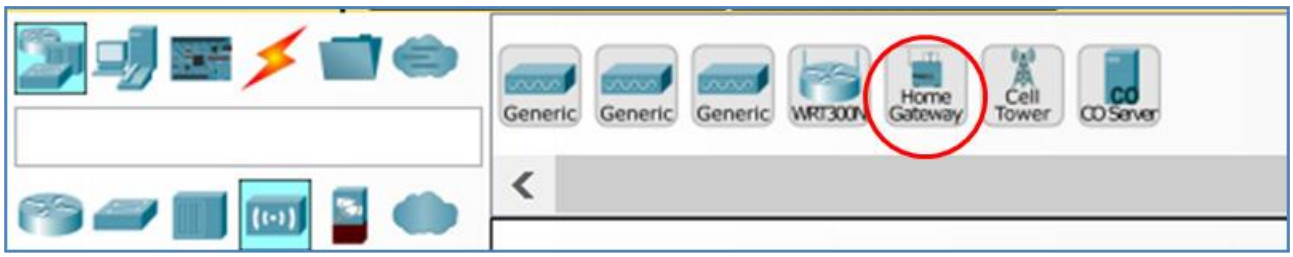
Загальні відомості/сценарій

У цій вправі в існуючу домашню мережу буде додано домашній шлюз і кілька пристроїв IoT, а потім моніторинг роботи цих пристроїв через домашній шлюз.

Частина 1: Підключення домашнього шлюзу до мережі

Крок 1. Додавання домашнього шлюзу

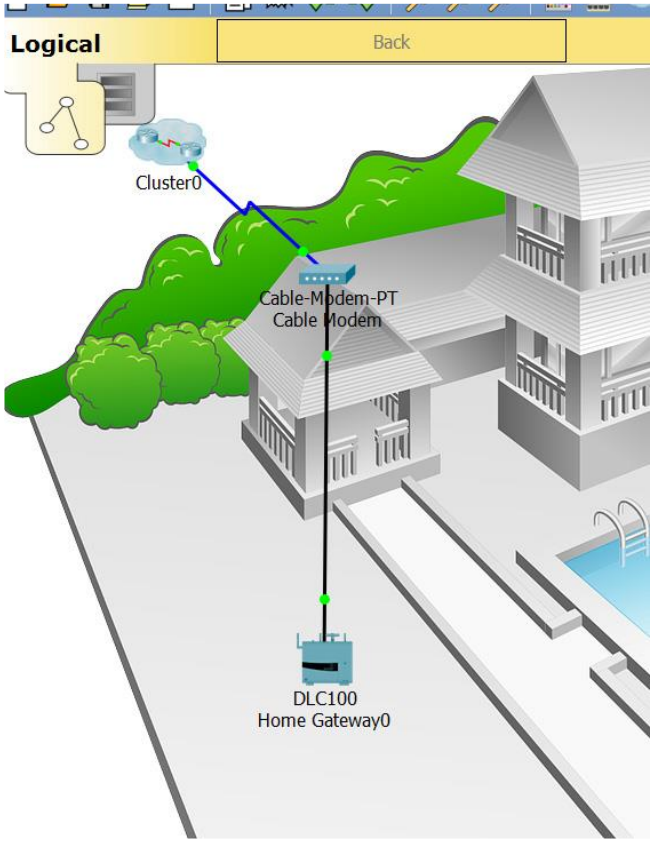
a. Виберіть Home Gateway (Домашній шлюз). Клацніть піктограму Wireless Devices (Бездротові пристрої) у полі Device-Type Selection (Вибір типу пристрою). Натисніть піктограму Home Gateway (Домашній шлюз), а потім натисніть логічний робочий простір, щоб додати його пристрій.



b. Підключіть домашній шлюз до кабельного модему.

Клацніть піктограму з'єднувача Copper Straight-Through (Медний прямий) у полі Device-Type Selection (Вибір типу пристрою), а потім натисніть домашній шлюз, щоб підключити один кінець кабелю. Далі клацніть Cable Modem (Кабельний модем), щоб підключити інший кінець кабелю до порту Internet (Інтернет).

Через кілька секунд на обох кінцях кабелю повинні загорітися зелені індикатори, вказуючи на те, що підключення встановлено.



Частина 2: Підключення IoT до бездротової мережі

Крок 1: Вибір бездротових пристроїв

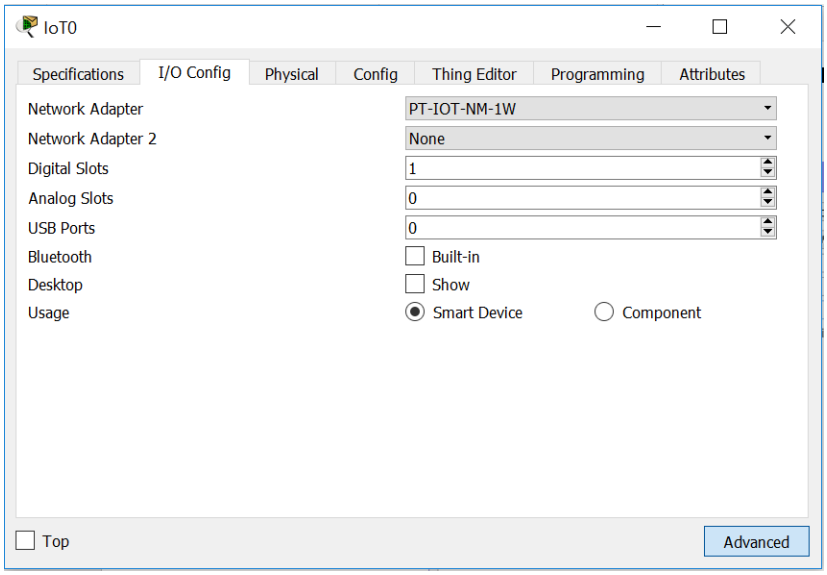
a. Клацніть піктограму Home Devices (Домашні пристрої) у полі Device-Type Selection (Вибір типу пристрою) та додайте в робочий простір Fan (Вентилятор), Door (Двері) та Lamp (Лампа).

Крок 2: Додавання пристроїв у домашню бездротову мережу

a. Додайте бездротовий адаптер до Fan (Вентилятор).

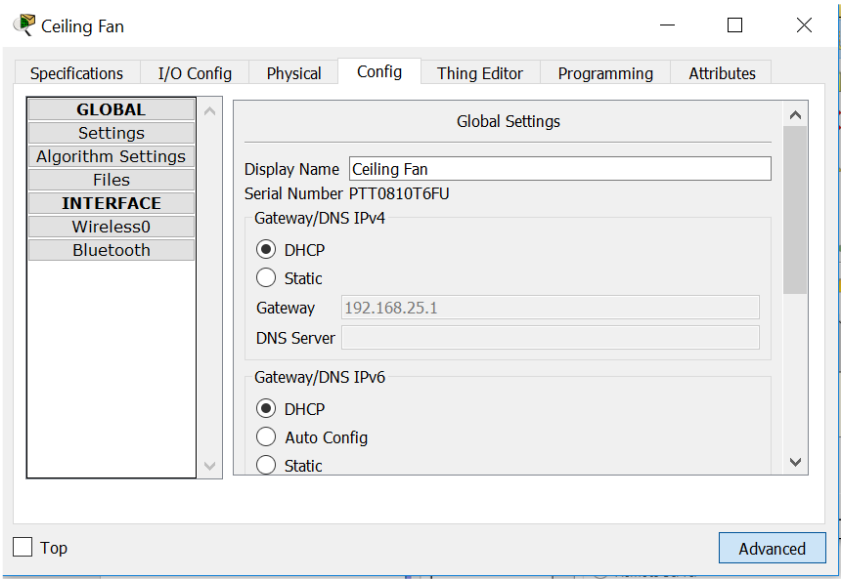
Клацніть піктограму Fan (Вентилятор) у робочому просторі, щоб відкрити вкладку Config (Конфігурація), а потім натисніть кнопку Advanced (Додатково) у нижньому правому куті вікна. Зауважте, що вкладки у верхній частині вікна конфігурації змінилися. З'явилися додаткові вкладки.

Перейдіть на вкладку I/O Config (Налаштування вводу-виводу) і в полі Network Adapter (Мережний адаптер) змініть тип на бездротовий адаптер PT-IOT-NM-1W.



b. Змініть ім'я пристрою Fan (Вентилятор). Клацніть вкладку Config (Налаштування). Введіть у полі Display Name (Відображуване ім'я).

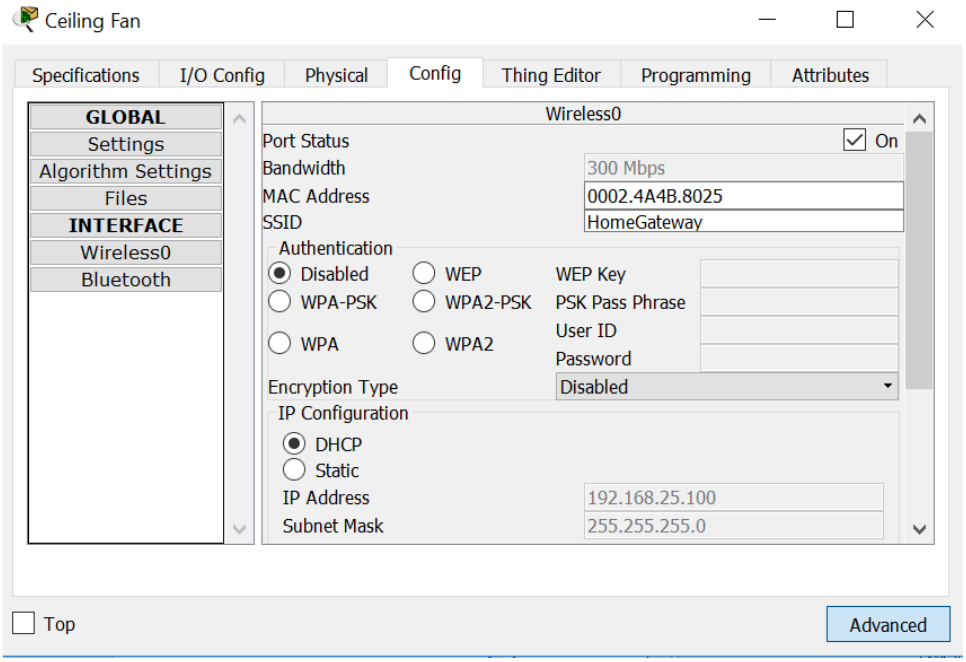
Ceiling Fan (Стельовий вентилятор).



c. Переконайтеся, що пристрій Fan (Вентилятор) підключено до бездротової мережі.

Перейдіть на вкладку Config (Конфігурація), клацніть інтерфейс Wireless0 у лівій панелі.

У параметрах конфігурації мережа HomeGateway повинна бути у списку, наведеному в полі SSID. Переконайтеся, що в параметрах IP Configuration (Конфігурація IP) встановлено прапорець DHCP, вказано IP-адресу 192.168.25.100 та стандартний шлюз 192.168.25.1. Це означає, що вентилятор підключений до мережі та отримує конфігураційні дані IP-адреси від домашнього шлюзу.



Закрийте вікно налаштування стельового вентилятора.

d. Підключіть пристрої Door (Двері) та Lamp (Лампа) до бездротової мережі, виконавши ті ж самі кроки, що й для вентилятора.

Частина 3: Додавання до мережі бездротового планшета

Крок 1: Додавання бездротового планшета до робочого простору

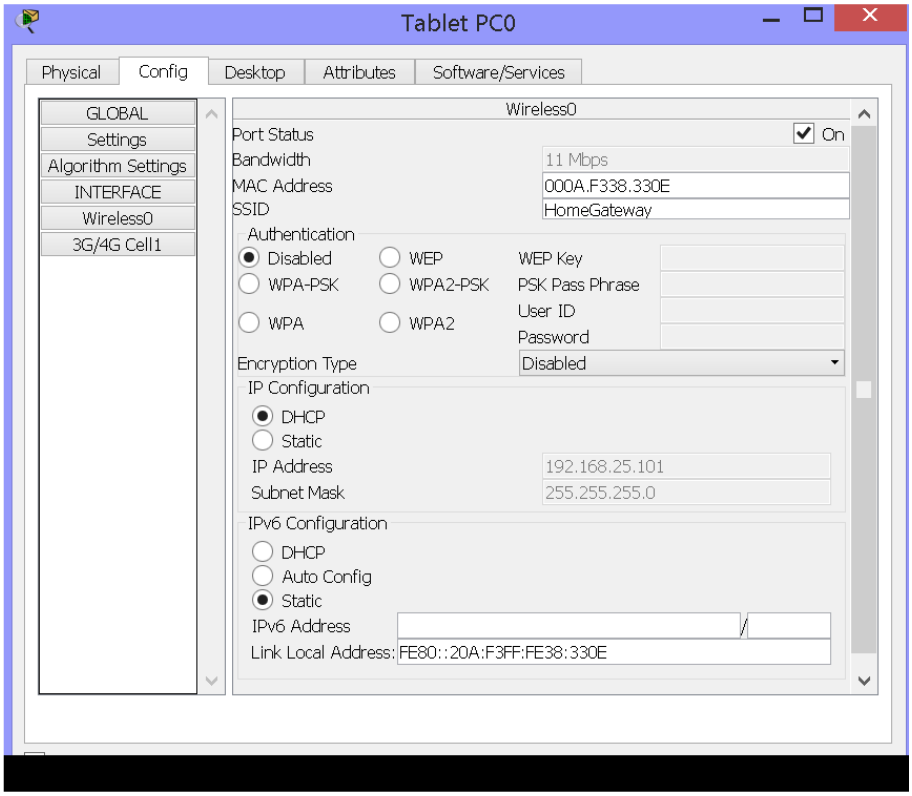
a. Клацніть піктограму End Devices (Кінцеві пристрої) у полі Device-Type Selection (Вибір типу пристрою) та додайте до робочого простору Wireless Tablet (Бездротовий планшет).

Крок 2: Підключення бездротового планшета до мережі HomeGateway

a. Змініть установки мережі бездротового планшета.

Натисніть піктограму Tablet (Планшет), щоб відкрити вікно налаштування планшета.

Перейдіть на вкладку Config (Конфігурація) та клацніть інтерфейс Wireless0. У полі SSID змініть значення Default (За замовчуванням) на HomeGateway. Після зміни ідентифікатора SSID мережі планшет повинен протягом декількох секунд отримати IP-адресу DHCP.

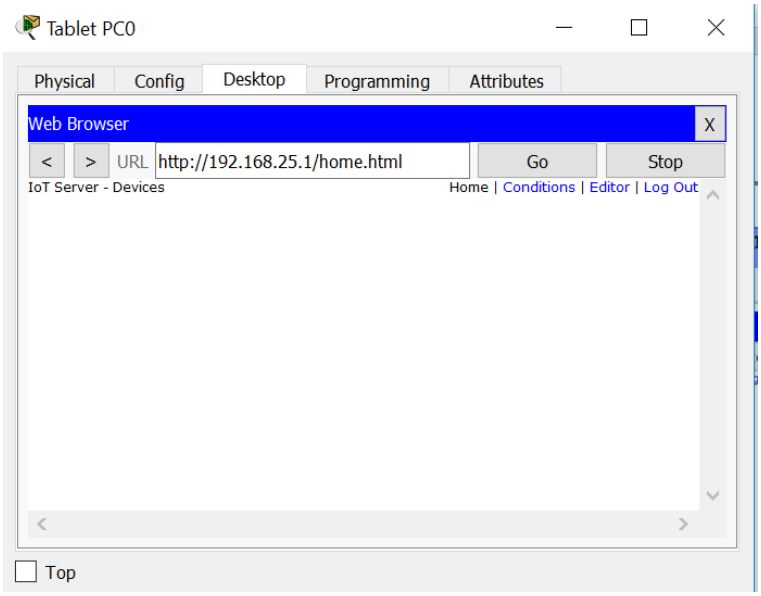


b. Зайдіть на сервер IoT домашнього шлюзу з планшета.

Перейдіть на вкладку Desktop (Робочий стіл) і клацніть піктограму Web Browser (Веб-браузер), щоб відкрити браузер. Введіть 192.168.25.1 (адреса домашнього шлюзу) у полі URL і натисніть Go (Перейти).

На сторінці Home Gateway Login (Вхід до домашнього шлюзу) введіть admin як ім'я користувача та admin як пароль і натисніть Submit (Надіслати), щоб підключитися до сервера домашнього шлюзу.

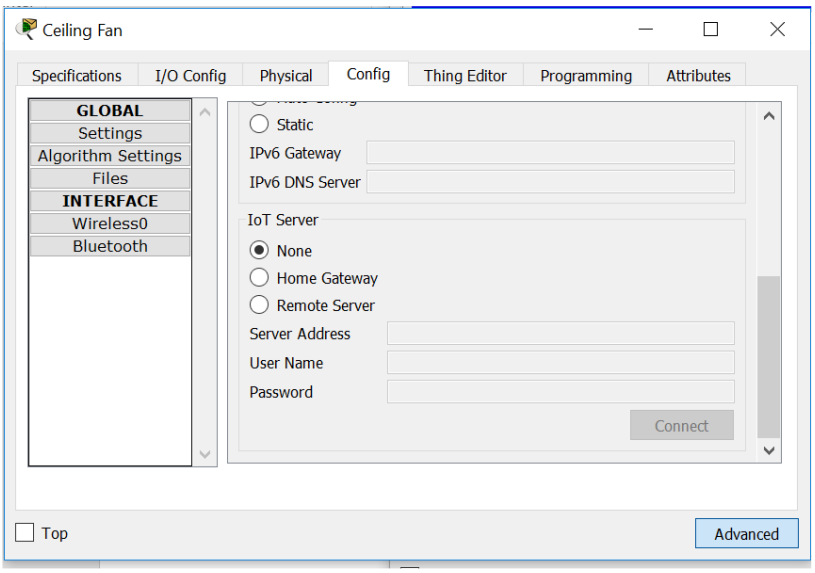
Зверніть увагу, що у списку IoT Server - Devices (Сервер IoT - пристрої) домашнього шлюзу немає пристроїв.



Закрийте вікно Tablet (Планшет).

Крок 3: Налаштування реєстрації пристроїв IoT на сервері домашнього шлюзу

a. Зареєструйте стельовий вентилятор на сервері домашнього шлюзу. Клацніть піктограму Fan (Вентилятор) у робочому просторі, відкрийте вкладку Config (Конфігурація) та виберіть Settings (Параметри) у лівій панелі. У списку параметрів IoT Server (Сервер IoT) натисніть кнопку Home Gateway (Домашній шлюз).



Закрийте вікно Ceiling Fan (Стельовий вентилятор).

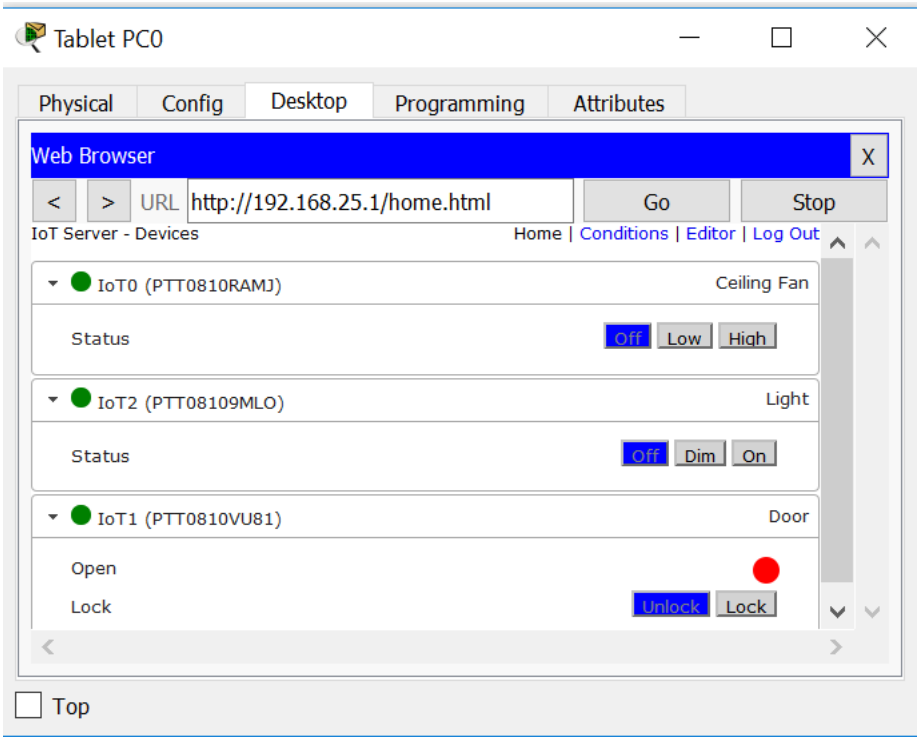
Повторіть кроки з розділу 3a для реєстрації домашнього шлюзу пристроїв

Door (Двері) та Lamp (Лампа).

b. Перевірте, чи пристрої зареєстровані на сервері домашнього шлюзу.

Клацніть піктограму Tablet (Планшет) у робочому просторі та відкрийте веб-браузер. Підключіться до домашнього шлюзу, ввівши 192.168.25.1 у поле URL-адреси та натиснувши Go (Перейти). Введіть admin як ім'я користувача та пароль і натисніть кнопку Submit (Відправити).

Через кілька секунд усі три пристрої повинні з'явитися в списку IoT Server - Devices (Сервер IoT - пристрої) домашнього шлюзу.



Закрийте вікно Tablet (Планшет).

Лабораторна робота 5
Створення блок-схеми процесу

Завдання

Частина 1. Розпізнавання символів, що використовуються в блок-схемі, та опис логічного процесу для вирішення проблеми

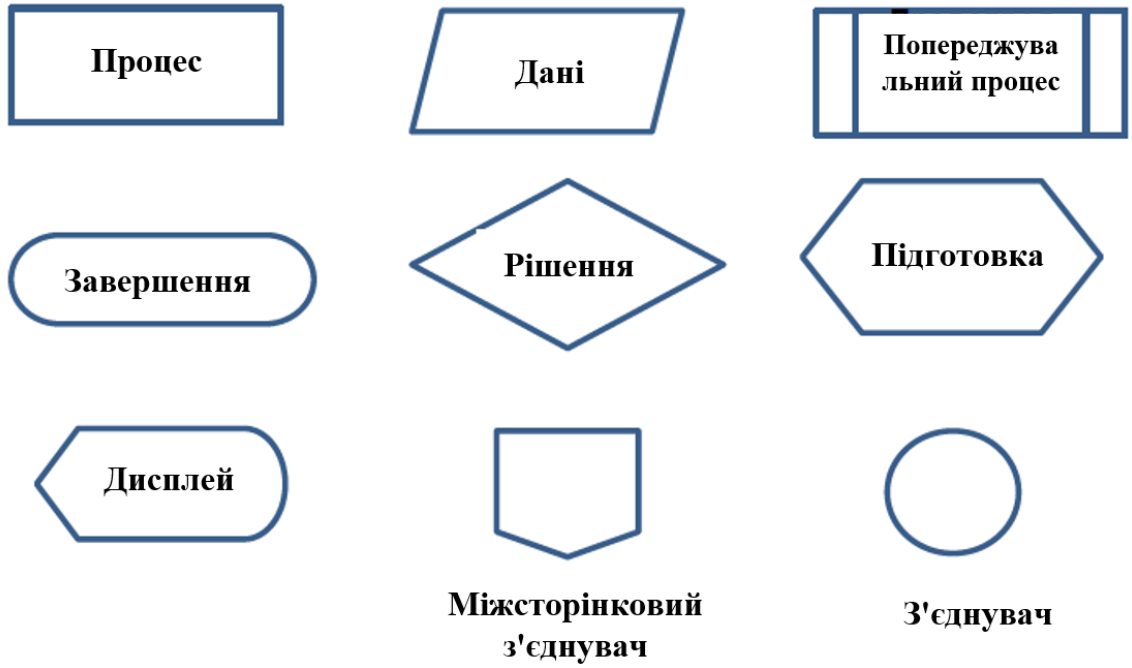
Частина 2. Малювання блок-схеми, що ілюструє процес вирішення проблеми

Загальні відомості

Блок-схеми - це діаграми, що використовуються для представлення процесів

або робочих процесів. За допомогою різноманітних фігур, квадратів та сполучних стрілок блок-схема представляє процес вирішення конкретної проблеми. Як правило, блок-схеми використовуються для представлення програм, алгоритмів та будь-яких упорядкованих процесів у різних галузях. Зазвичай блок-схеми створюються перед початком процесу або написанням програми, щоб перевірити логіку робочого процесу та виявити можливі проблеми, перш ніж рішення буде розроблено та впроваджено.

Блок-схеми можна малювати вручну або створювати за допомогою різних програмних пакетів, включаючи продукти Microsoft Office, LibreOffice, GoogleDocs та різноманітні веб-програми, такі як https://www.draw.io/.



Деякі з найпоширеніших символів блок-схем, що використовуються в програмуванні, показані на схемі разом із призначенням. Лінії зі стрілками вказують напрямок ходу процесу вирішення проблеми.

Сценарій

Необхідно розробити послідовний процес для пошуку зумовленого числа. Розроблений процес представляється як блок-схеми. За допомогою блок-схеми можна перевірити логіку процесу розв'язання задачі.

Необхідні ресурси

- Цю лабораторну роботу можна виконувати на папері олівцем або на ПК з доступом до Інтернету (або з такими офісними програмами, як Microsoft Office, LibreOffice та GoogleDocs).

Частина 1. Перерахування логічних кроків, необхідні вирішення завдання

Завдання полягає у розробці процесу пошуку зумовленого числа. Процес можна

запрограмувати як просту комп'ютерну гру. Гравцеві пропонується замислити число між 0 і 128. Програма використовуватиме метод поділу навпіл для пошуку цього числа.

Крок 1. Перерахування кроків, необхідних для вирішення задачі

a. Попросити гравця замислити ціле число від 0 до 128.

b. Задати **a** як нижню межу, **b** як верхню межу і t як час обчислення.

c. Визначити початкові значення **a** = 0, **b** = 128, **t** = 0.

d. Обчислити середнє значення між a та b. Поставити його як M.

e. Задати t = t +1.

f. Запитати гравця, чи не є **M** задуманим числом.

Якщо так, вивести "Ви задумали число M, і воно вгадане за **t** спроб". Завершити процес.

Else

If t = 6

Якщо так, вивести "На жаль, не вдалося вгадати за 6 спроб". Завершити процес.

Else

Запитати гравця, чи більше M шуканого числа.

Якщо так, то задати a = M, перейти на крок d.

Else

Задати b = M, перейти крок d.

Запитання:

Чи може цей процес визначити число, якщо гравець задумав 0 чи 128? Поясніть свою відповідь.

_____

_____

Якщо визначити 0 або 128 неможливо, що необхідно зробити, щоб виправити це?

_____

_____

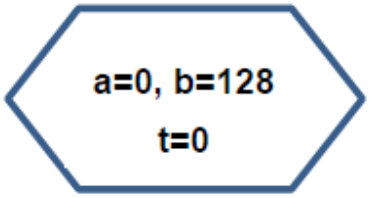
Частина 2. Малювання блок-схеми

Крок 1. Використовуйте відповідні символи блок-схеми для кожної функції.

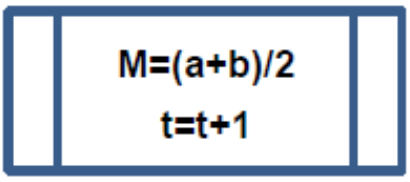
Оскільки список кроків процесу вже визначено, можна уявити кожен крок із допомогою символу блок-схеми.

a. Використовуйте овал як символ початку процесу та символ дисплея для позначення питань. З'єднайте їх за допомогою ліній в такий спосіб.

b. Використовуйте символ підготовки для призначення вихідних параметрів:

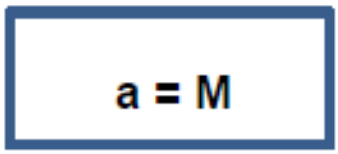


c. Використовуйте символ визначеного процесу для позначення функції або програми:



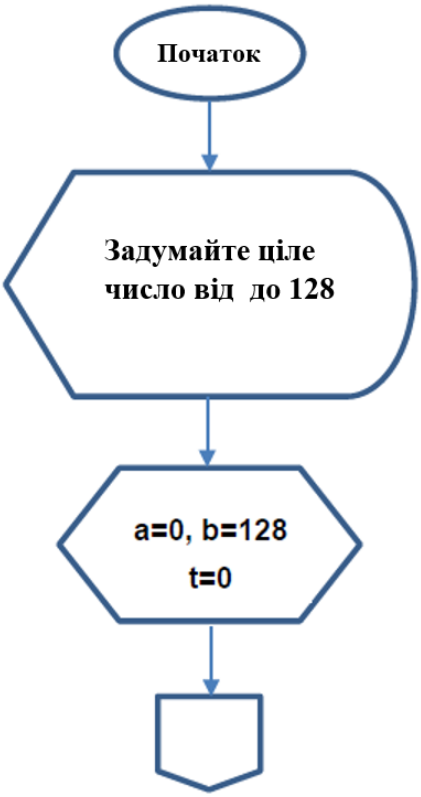
d. Використовуйте символ рішення, щоб перевірити умови:

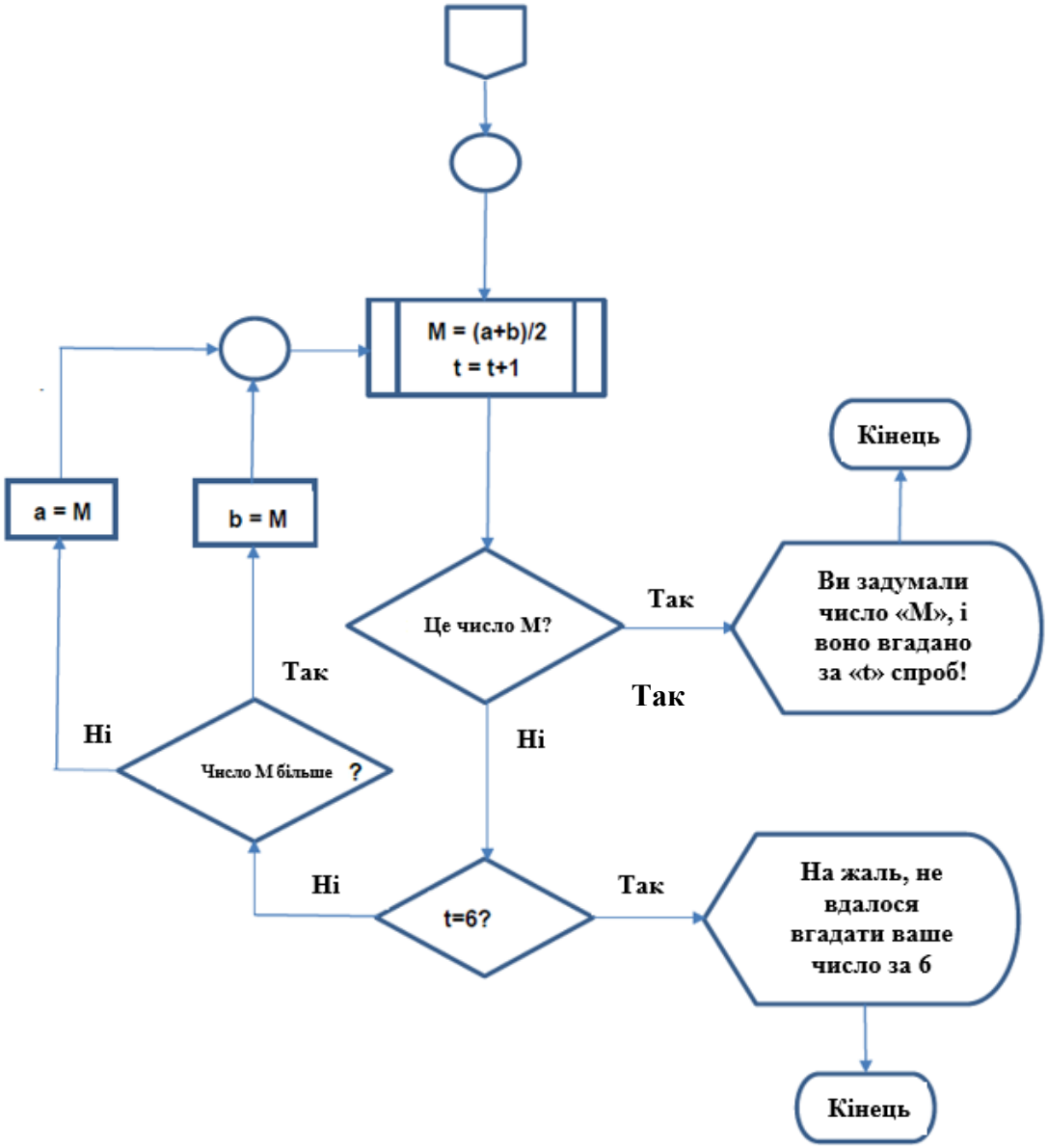
е. Використовуйте символ процесу для позначення операції:



Крок 2. Намалюйте повну блок-схему.

Тепер за допомогою цих символів можна намалювати повну блок-схему. Для продовження блок-схеми на наступній сторінці використовуйте символи міжсторінкового з'єднувача та з'єднувача.





Питання для повторення

У чому сенс перевірки умови **t** = 6?

_____

_____

Куди потрібно помістити перевірку, чи задумано число 0 чи 128?

_____

_____

Лабораторна робота 6.
Вивчення великого набору даних

Загальні відомості/сценарій

Перш ніж дані перетворяться на значну інформацію, їх необхідно обробити.

Необхідні ресурси

ПК з доступом до Інтернету.

Крок 1. Знайдіть велику безкоштовну базу даних із можливістю пошуку.

a. Натисніть тут для доступу до бази статистичного управління Міністерства сільського господарства США

b. Виберіть: Quick Stats (Searchable Database) (Коротка статистика (База даних із можливістю) пошуку))

Зверніть увагу на стан у верхньому правому кутку. Скільки записів на даний момент
міститься у цій базі даних?

_____
_____

Крок 2. Виберіть категорії.

a) З категорій виберіть:

Program: Census (Програма: Census)
Sector: Animals & Products (Сектор: тварини та продукти)
Group: Poultry (Група: птах)
Commodity: Ducks (Товар: качки)
Category: Inventory (Категорія: товари в наявності)
Data Item: Ducks – Inventory (Елемент даних: качки – товари в наявності)
Geographic Level: State (Географічний рівень: штат)
State: Alaska (Штат: Аляска)

Далі виберіть: Get Data (Отримати дані)

*Яка була кількість качок на Алясці у 2012 р.?*_____

Натисніть кнопку Back (Назад) та змініть штат на Гаваї. Переконайтеся, що рік, як і раніше, 2012 року.

Якою була кількість качок у штаті Гаваї у 2012 р.?

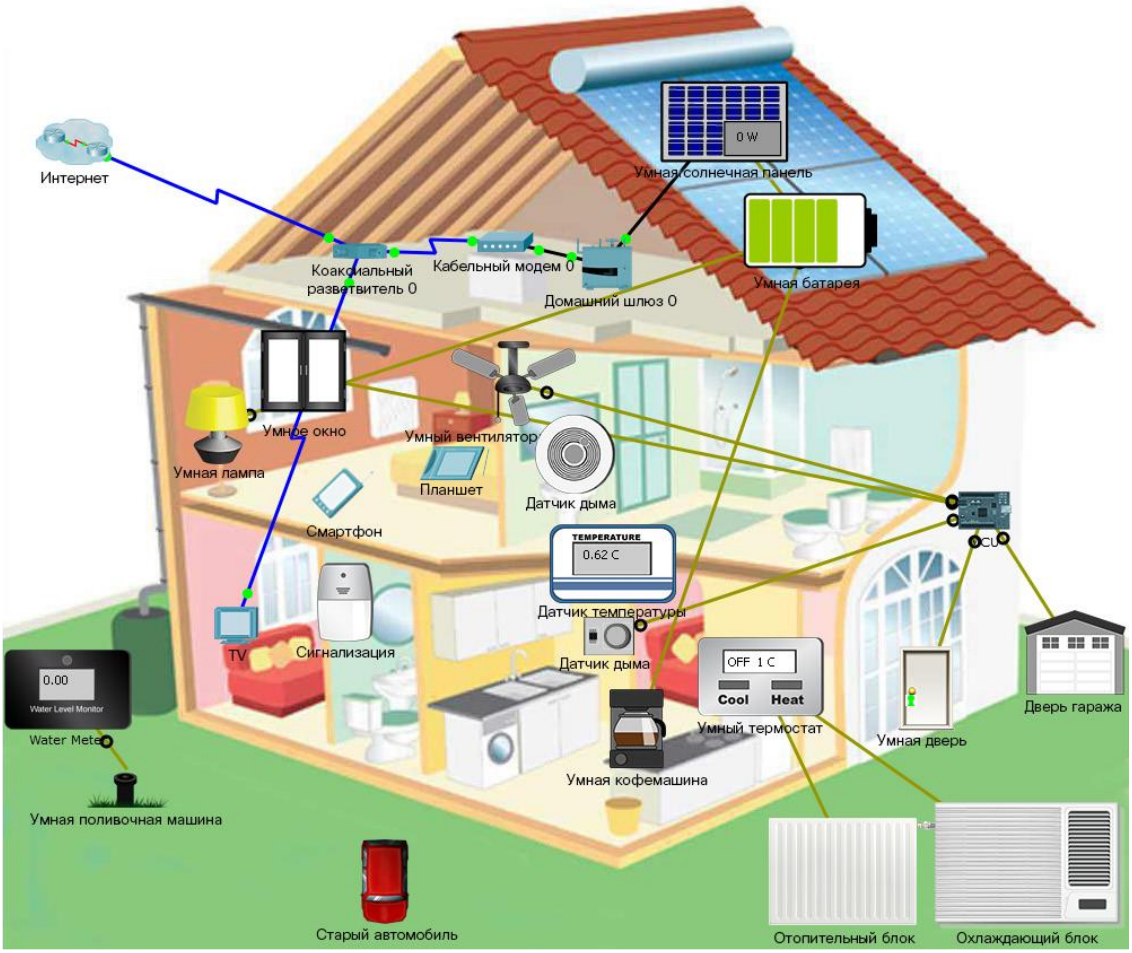
_____

b) Як може використовувати цю базу даних компанія, якій потрібні качки?_____

_____
_

Лабораторна робота 7.
Packet Tracer. Вивчення розумного будинку

Топологія



Мета:

- Вивчення розумного будинку
- Аналіз використання туманних обчислень у розумному будинку

Загальні відомості/сценарій

У цій вправі ви вивчите приклад розумного будинку. Залежно від застосування деякі дані найкраще обробляються близько до джерела. У прикладі розумного будинку використовуються переваги туманних обчислень для моніторингу та реагування на рівні задимленості, виявлені
в будинку.

Частина 1: Вивчення розумного будинку

Крок 1: Опис пристроїв, що утворюють розумний будинок

Зазвичай інтернет-провайдери доставляють дані та відео по одному коаксіальному кабелю. Починаючи з горища, застосовується розгалужувач коаксіального кабелю для розділення сигналів відео та даних.

a. У показаній топології з коаксіального розгалужувача виходять два коаксіальні кабелі. До яких пристроям підключається коаксіальний кабель?____

b. Кабельний модем – це інтерфейс між мережею інтернет-провайдера та

домашньою мережею. До яких пристроїв підключено кабельний модем?_____

Домашній шлюз служить концентратором та маршрутизатором для всіх внутрішніх домашніх пристроїв. Він також надає веб-інтерфейс, який дозволяє користувачам контролювати різні пристрої розумного будинку та керувати ними. Зверніть увагу, що домашні пристрої можна підключати до домашнього шлюзу як бездротовим, так і дротовим способом.

Примітка. У Packet Tracer для представлення бездротових підключень використовуються пунктирні лінії, але за наявності занадто великої кількості пристроїв важко читати схему. Щоб увімкнути цю функцію, перейдіть до розділу Options (Параметри) > Preferences (Параметри) > вкладка Hide (Приховати) та зніміть прапорець Hide Wireless/Cellular Connection (Приховати) бездротове або стільникове підключення).

c. Список всіх домашніх пристроїв, підключених до домашнього шлюзу

_____

Крок 2: Взаємодія з розумним будинком

Пристрої в розумному будинку можна керувати та контролювати їх віддалено з будь-якого комп'ютера в будинку. Всі інтелектуальні пристрої підключаються до домашнього шлюзу, на якому розміщено веб-інтерфейс, тому для взаємодії з інтелектуальними пристроями можна використовувати планшети, смартфони, ноутбуки та настільні комп'ютери.

a. Натисніть на планшет, що лежить на ліжку в спальні господаря.

b. Виберіть «Робочий стіл» > «Веб-браузер».

c. Введіть в адресному рядку 192.168.25.1. Це IP-адреса домашнього шлюзу.

d. Використовуючи admin/admin як ім'я користувача та пароль, виконайте вхід на домашній шлюз.

e. Яку інформацію відображено?_____

f. Розумні двері в даний час розблоковані (на що вказує зелене світло на дверній ручці), але її можна віддалено замкнути. Натисніть на розумні двері в браузері.

g. Натисніть Lock (Зачинити), щоб замкнути двері.

h. Двері були замкнені? Звідки це ви знаєте?_____

i. Натисніть Unlock (Відчинити), щоб відчинити двері.

j. Клацніть датчик диму в браузері. Які показання рівня диму, надані датчиком?_____

k. Чи можна керувати датчиком диму?_____

Інтелектуальними пристроями можна керувати безпосередньо, що відповідає фізичному взаємодії.

l. Утримуючи клавішу ALT, натисніть на розумну кавоварку, щоб увімкнути або вимкнути її.

Частина 2: Туманні обчислення в розумному домі

MCU, що додається до розумного будинку, використовується для відстеження показань рівня диму від датчика та визначення необхідності увімкнення вентиляції будинку. Якщо рівні чадного газу піднімуться вище 10,3 одиниць, MCU відповідно до програми автоматично відкриє вікно, вхідні двері, ворота гаража та запустить вентилятор на високій швидкості. Дана дія скасовується (закриття дверей, воріт і вікон та зупинка вентилятора), тільки коли рівні чадного газу опускаються нижче 1 одиниці.

Крок 1: Запуск класичного автомобіля

Власник містить у гаражі класичний автомобіль, який час від часу необхідно запускати. Класичний автомобіль виділяє чадний газ, що піднімає його рівень у будівлі.

a. Натисніть на планшет, що лежить на ліжку в спальні господаря.

b. Виберіть «Робочий стіл» > «Веб-браузер».

c. Введіть в адресному рядку 192.168.25.1. Це IP-адреса домашнього шлюзу.

d. Використовуючи admin/admin як ім'я користувача та пароль, виконайте вхід на домашній шлюз.

e. Натисніть датчик диму. Залишіть це вікно відкритим, щоб можна було відстежувати рівні диму.

f. Запустіть двигун автом рясні: утримуючи натиснутою клавішу Alt, клацніть класичний автомобіль.

Що відбувається з повітрям усередині будинку, коли автомобіль працює у гаражі?_____

Що відбувається з повітрям усередині будинку після того, як MCU відкриває вікно та двері та запускає вентилятор?_____

MCU закриває двері та вікно і зупиняє вентилятор?_____

g. Продовжуючи відстежувати рівні, зупиніть двигун класичного автомобіля: утримуючи натиснутою клавішу Alt, клацніть класичний автомобіль.

Як змінюється якість повітря всередині будинку після зупинки двигуна?

_____

Що відбувається з дверима, вікном та вентилятором?

_____

Частина 3: Запитання для повторення

Цей приклад показує, що вибір між хмарною та туманною обробкою залежить від застосування.

У прикладі з розумною домівкою туманні обчислення були оптимальним варіантом. У цьому прикладі розумного будинку дані, що видаються датчиком диму, обробляються та використовуються для прийняття рішень щодо якості повітря у

будинку. У цьому сценарії не було необхідності надсилати дані датчика в хмару для обробки. Обробка в хмарі може збільшити час відгуку, потенційно наражаючи на небезпеку життя людей. Інша можлива проблема відноситься до інтернет-каналу: у разі розриву з'єднання з Інтернетом відбудеться збій усієї системи, знову наражаючи на небезпеку життя людей.

Лабораторна робота8.

Вивчення мереж, що керуються на основі намірів (IBN)

Завдання

Частина 1. Ознайомлення з веб-сайтом керованої на основі намірів мережі Cisco (IBN)

Частина 2. Введення в мережі, керовані на основі намірів, на прикладі Cisco DevNet

Частина 3. Вивчення запитів від спільноти IBN та подання власних запитів

Загальні відомості/сценарій

Сьогодні все з'єднане через мережу. Що, якщо мережа зможе постійно пристосовуватися, захищатися та розсилати повідомлення на основі намірів, висловлених власником компанії? Керована на основі намірів мережа на базі відкритої платформи може сприймати бізнес-наміри та узгоджувати з ними комплексну мережу, усуваючи розрив між вимогами бізнесу та функціональністю мережі.

Необхідні ресурси

● Комп'ютер з доступом до Інтернету

Частина 1. Ознайомлення з веб-сайтом керованої на основі намірів мережі Cisco (IBN)

У першій частині лабораторної роботи ви ознайомитеся з оглядом та кількома прикладами використання мереж на основі намірів Cisco. Знайомлячись із цим сайтом та переглядаючи вбудовані відео, ви дізнаєтесь, як наміри людини перетворюються на реалізацію машинних політик. Перейдіть за посиланням нижче, щоб отримати доступ до веб-сайту рішення Cisco IBN. https://www.cisco.com/c/en/us/solutions/Intent-Based-networking.html#~stickynav=6

Крок 1. Ознайомтеся з наведеним вище веб-сайтом Cisco Solutions і дайте відповідь на наступні запитання.

Що таке керована на основі намірів мережа (IBN)?

_____

Вкажіть хоча б дві причини на користь використання керованої на основі намірів мережі.

_____

Частина 2. Введення в мережі, керовані на основі намірів, на прикладі Cisco DevNet

У частині 2 будуть представлені мережі, керовані з урахуванням намірів, з прикладу Cisco DevNet. З цього блогу ви дізнаєтеся про програмовані мережі та про те, як мережі на основі намірів можна інтегрувати за допомогою коду. Натисніть наведене нижче посилання, щоб отримати доступ до блога Cisco.

https://blogs.cisco.com/enterprise/building-Intent-Based-network-with-

devnet?ccid=cc000006&dtid=esoxsp000263&oid=psten009481

Крок 1. Ознайомтеся з блогом за наведеним вище посиланням та дайте відповідь на наступні запитання.

Який перший крок для початку роботи та практичного програмування?

_____

Що станеться при використанні IBN, якщо власник бізнесу вкаже той чи інший намір для мережі?

_____

Частина 3. Вивчення запитів від спільноти IBN та подання власних запитів

У третій частині ви розглянете запити коду IBN від інших учасників спільноти та поділіться із спільнотою своєю ідеєю бізнес-наміру. Розробники у спільноті допоможуть перетворити вашу ідею на код. Перейдіть за посиланням нижче, щоб отримати доступ до спільноти Cisco DevNet, присвяченої мережам на основі намірів, і виконати вхід за допомогою облікового запису Netacad.com:

https://developer.cisco.com/codeintent/

Крок 1. Ознайомтеся з деякими намірами, розробленими спільнотою.

а. Ознайомившись із деякими намірами, створеними учасниками спільноти, виберіть два наміри, що вас цікавлять, і вкажіть їх нижче.

1._____

2._____

Крок 2. Створення власного наміру

а. Створіть свій власний намір на веб-сайті Cisco DevNet та опублікуйте його нижче.

Назва:_____

Подробиці події:_____

Питання для повторення

1. Чи можете ви запропонувати інші приклади використання керованих на основі намірів мереж (IBN), крім виявлених на трьох веб-сайтах?

_____

2. Які навички програмування, на вашу думку, будуть потрібні для розгортання мереж на основі намірів?_____

Лабораторна робота 9.
«Відбиток» людини в Інтернеті

Мета цієї лабораторної роботи - знайомство зі "зняттям відбитків пальців" людини під час використання Інтернету. Завдання — представити різні методи ефективного отримання якомога повнішої інформації за допомогою лише веб-браузера та різних сайтів.

Частина 1. Отримання максимальної інформації про себе за допомогою Internet Edge, Google Chrome та Firefox за допомогою пошукової системи Google.

Частина 2. Використання різних веб-сайтів для поповнення інформації, зібраної за допомогою пошукової системи Google.

Частина 3. Порівняння та зіставлення інформації, зібраної за допомогою пошукової системи Google та інших вказаних сайтів.

Частина 4. Створення власного «інтернет-відбитка» з використанням усіх зібраних відомостей та оцінка інформації, яку слід робити загальнодоступною.

Загальні відомості/сценарій

Щоразу, коли людина переглядає сайти Інтернету, різні відвідувані ним сайти збирають відомості, наприклад, про біографію, політичні уподобання, національність, уподобання тощо. Коли ви відвідуєте сайти, в комп'ютер записуються невеликі файли cookie, що стосуються веб-браузера сайтів. Файли cookie містять невеликі фрагменти даних, що відповідають особливостям браузера та відвідуваних сайтів. Сайти соціальних мереж збирають великий обсяг особистих даних, перш ніж дозволити вам доступ. Вся ця особиста інформація може бути вилучена будь-яким охочим. Таким чином, при відвідуванні Інтернету ви залишаєте яскравий слід файлів cookie, який дозволяє скласти детальне уявлення про вас кожному, хто візьметься шукати в Інтернеті інформацію про вас.

Примітка. Переконайтеся, що на комп'ютері працює операційна система Windows 8 або 10 і доступ до останньої версії Microsoft Edge та Google Chrome або Mozilla Firefox. ПК повинен мати доступ до Інтернету.

Примітка. Перед початком роботи переконайтеся, що на комп'ютері вимкнено підвищений рівень безпеки Windows. Якщо ви не впевнені, зверніться до інструктора.

Необхідні ресурси

● Один ПК (Windows 8 або 10 з доступом до Інтернету)

Примітка. На ПК повинні бути попередньо встановлені останні версії Microsoft Edge, Google Chrome і Mozilla Firefox

Підвищена безпека Інтернету має бути вимкнена на відповідних ПК.

1. Збір інформації про себе за допомогою Mozilla Firefox

a. Відкрийте Mozilla Firefox та перейдіть на сайт https://google.com.

b. При введенні в поле пошуку введіть у лапки ім'я та прізвище людини, яку ви шукаєте (наприклад, "John Smith"). У цій лабораторній роботі людина, про яку проводиться збір даних, — ви самі.

c. Ви можете ввести інші доречні слова, наприклад, професію, роботодавця, розташування або навіть псевдонім, яким, можливо, користувалися.

d. Якщо людина, яку ви шукаєте, швидше за все, є на конкретному веб-сайті (наприклад, школи), виконайте пошук тільки на цьому сайті за допомогою оператора site:URL (наприклад, site:centennialcollege.com "John Smith").

e. Ви можете також шукати людей по обличчю за допомогою служби Google Images, щоб швидко отримати візуальну інформацію. Це особливо корисно у випадку людей з поширеними іменами або щоб визначити стать на ім'я, про яке ви ніколи раніше не чули. Виконайте пошук на всіх сайтах соціальних мереж, які пов'язані з вашим запитом.

f. Задокументуйте всю інформацію, зібрану під час цього пошуку._____
_____

Крок 2. Використання служби PIPL

a. За допомогою служби Free People Search Online виконайте пошук додаткових відомостей у міжнародному масштабі, які могли бути втрачені пошуковою системою Google. Перейдіть на сайт pipl.com та здійсніть пошук.

b. Задокументуйте всі відомості, зібрані під час цього пошуку_____
_____

Крок 3. Використання Zabbasearch

a. Zabbasearch – це комплексна система для пошуку людей. http://www.zabasearch.com/. Перейдіть на сайт, введіть параметри пошуку та запустіть пошук. Задокументуйте всі відомості, зібрані під час пошуку. Зверніть увагу, що цей сайт орієнтований на США._____
_____

Крок 4. Використання People Search Global

a. People Search Global – ще один сайт для простого пошуку людей у міжнародному масштабі. Перейдіть на сайт http://people-search-global.com/, введіть параметри пошуку та запустіть пошук. Задокументуйте всі відомості, зібрані під час цього пошуку.

Крок 5. Використання PeekYou

a. PeekYou - сайт пошуку з величезним охопленням людей, який намагається зібрати всі зв'язки, що є у людини, в соціальних мережах в одному місці. Перейдіть на сайт https://www.peekyou.com/ та запустіть пошук, ввівши відповідні параметри. Зверніть увагу, що цей сайт орієнтований на США.

b. Задокументуйте всі відомості, зібрані під час цього пошуку_____

_____

Питання для повторення

1. Порівняйте та зіставте всі зібрані дані в документованих таблицях. Який пошук приніс найбільшу інформацію?_____

_____

2. Які сайти соціальних мереж, учасником яких ви є, були відкриті під час пошуку?_____

_____

3. Озираючись назад, які дані ви не хотіли б показувати в загальному доступі і чому? _____

Лабораторна робота 9.
«Відбиток» людини в Інтернеті

Мета цієї лабораторної роботи - знайомство зі "зняттям відбитків пальців" людини під час використання Інтернету. Завдання — представити різні методи ефективного отримання якомога повнішої інформації за допомогою лише веб-браузера та різних сайтів.

Частина 1. Отримання максимальної інформації про себе за допомогою Internet Edge, Google Chrome та Firefox за допомогою пошукової системи Google.

Частина 2. Використання різних веб-сайтів для поповнення інформації, зібраної за допомогою пошукової системи Google.

Частина 3. Порівняння та зіставлення інформації, зібраної за допомогою пошукової системи Google та інших вказаних сайтів.

Частина 4. Створення власного «інтернет-відбитка» з використанням усіх зібраних відомостей та оцінка інформації, яку слід робити загальнодоступною.

Загальні відомості/сценарій

Щоразу, коли людина переглядає сайти Інтернету, різні відвідувані ним сайти збирають відомості, наприклад, про біографію, політичні уподобання, національність, уподобання тощо. Коли ви відвідуєте сайти, в комп'ютер записуються невеликі файли cookie, що стосуються веб-браузера сайтів. Файли cookie містять невеликі фрагменти даних, що відповідають особливостям браузера та відвідуваних сайтів. Сайти соціальних мереж збирають великий обсяг особистих даних, перш ніж дозволити вам доступ. Вся ця особиста інформація може бути вилучена будь-яким охочим. Таким чином, при відвідуванні Інтернету ви залишаєте яскравий слід файлів cookie, який дозволяє скласти детальне уявлення про вас кожному, хто візьметься шукати в Інтернеті інформацію про вас.

Примітка. Переконайтеся, що на комп'ютері працює операційна система Windows 8 або 10 і доступ до останньої версії Microsoft Edge та Google Chrome або Mozilla Firefox. ПК повинен мати доступ до Інтернету.

Примітка. Перед початком роботи переконайтеся, що на комп'ютері вимкнено підвищений рівень безпеки Windows. Якщо ви не впевнені, зверніться до інструктора.

Необхідні ресурси

● Один ПК (Windows 8 або 10 з доступом до Інтернету)

Примітка. На ПК повинні бути попередньо встановлені останні версії Microsoft Edge, Google Chrome і Mozilla Firefox

Підвищена безпека Інтернету має бути вимкнена на відповідних ПК.

1. Збір інформації про себе за допомогою Mozilla Firefox

a. Відкрийте Mozilla Firefox та перейдіть на сайт https://google.com.

b. При введенні в поле пошуку введіть у лапки ім'я та прізвище людини, яку ви шукаєте (наприклад, "John Smith"). У цій лабораторній роботі людина, про яку проводиться збір даних, — ви самі.

c. Ви можете ввести інші доречні слова, наприклад, професію, роботодавця, розташування або навіть псевдонім, яким, можливо, користувалися.

d. Якщо людина, яку ви шукаєте, швидше за все, є на конкретному веб-сайті (наприклад, школи), виконайте пошук тільки на цьому сайті за допомогою оператора site:URL (наприклад, site:centennialcollege.com "John Smith").

e. Ви можете також шукати людей по обличчю за допомогою служби Google Images, щоб швидко отримати візуальну інформацію. Це особливо корисно у випадку людей з поширеними іменами або щоб визначити стать на ім'я, про яке ви ніколи раніше не чули. Виконайте пошук на всіх сайтах соціальних мереж, які пов'язані з вашим запитом.

f. Задокументуйте всю інформацію, зібрану під час цього пошуку._____
_____

Крок 2. Використання служби PIPL

a. За допомогою служби Free People Search Online виконайте пошук додаткових відомостей у міжнародному масштабі, які могли бути втрачені пошуковою системою Google. Перейдіть на сайт pipl.com та здійсніть пошук.

b. Задокументуйте всі відомості, зібрані під час цього пошуку_____
_____

Крок 3. Використання Zabbasearch

a. Zabbasearch – це комплексна система для пошуку людей. http://www.zabasearch.com/. Перейдіть на сайт, введіть параметри пошуку та запустіть пошук. Задокументуйте всі відомості, зібрані під час пошуку. Зверніть увагу, що цей сайт орієнтований на США._____
_____

Крок 4. Використання People Search Global

a. People Search Global – ще один сайт для простого пошуку людей у міжнародному масштабі. Перейдіть на сайт http://people-search-global.com/, введіть параметри пошуку та запустіть пошук. Задокументуйте всі відомості, зібрані під час цього пошуку.

Крок 5. Використання PeekYou

a. PeekYou - сайт пошуку з величезним охопленням людей, який намагається зібрати всі зв'язки, що є у людини, в соціальних мережах в одному місці. Перейдіть на сайт https://www.peekyou.com/ та запустіть пошук, ввівши відповідні параметри. Зверніть увагу, що цей сайт орієнтований на США.

b. Задокументуйте всі відомості, зібрані під час цього пошуку_____

_____

Питання для повторення

1. Порівняйте та зіставте всі зібрані дані в документованих таблицях. Який пошук приніс найбільшу інформацію?_____

_____

2. Які сайти соціальних мереж, учасником яких ви є, були відкриті під час пошуку?_____

_____

3. Озираючись назад, які дані ви не хотіли б показувати в загальному доступі і чому? _____

Лабораторна робота 10.
Налаштування безпеки бездротової мережі. Packet Tracer.

Завдання

Створити домашню мережу із захищеним бездротовим маршрутизатором

Вступ

У цій вправі вам слід виконати наступні установки бездротового маршрутизатора.

- Змініть стандартний пароль.
- Змініть SSID за замовчуванням та забороніть широкомовне розсилання
- Використовуйте WPA2 Personal як метод безпеки.
- Застосовуйте фільтрацію MAC-адрес для підвищення інформаційної безпеки.
- Вимкніть віддалене керування.

Крок 1: Завантаження pkt-файлу

a. Завантажте файл 5.1.2.6 Packet Tracer. Налаштування безпеки бездротової мережі. pkt.

b. Натисніть кнопку живлення на ноутбуку Laptop1, щоб вимкнути його.

c. Щоб видалити порт Ethernet, перетягніть його до списку Modules (Модулі).

d. Перетягніть модуль WPC300N у порожній слот на Laptop1 і натисніть кнопку живлення, щоб увімкнути Laptop1.

Крок 2: Змініть стандартний пароль.

a. Натисніть на бездротовий маршрутизатор і виберіть GUI (Графічний інтерфейс користувача) для налаштування.

b. Натисніть Administration > Management (Адміністрування > Керування)

c. Змініть пароль маршрутизатора на надійніший. Змініть пароль на aC0mpAny3.

Зверніть увагу, що новий пароль складається з 8 символів у верхньому та нижньому регістрі, а деякі голосні замінені цифрами. Виберіть Save Settings (Зберегти установки) у нижній частині екрану.

Крок 3: Змініть стандартне ім'я SSID і вимкніть функцію широкомовного розсилання.

a. Натисніть Wireless (Бездротові мережі) та змініть ім'я SSID на aCompany.

b. Виберіть SSID Broadcast (Широкомовне розсилання SSID) та натисніть кнопку Disabled (Вимкнено). Натисніть кнопку Save Settings (Зберегти параметри) у нижній частині екрана.

Перевірте топологію. Чи втратив Laptop0 зв'язок із бездротовим маршрутизатором? Якщо так, то чому?_____

Крок 4: Налаштуйте режим бездротового маршрутизатора безпеки WPA2.

a. Перейдіть на вкладку GUI (Графічний інтерфейс користувача) бездротового маршрутизатор. Натисніть Wireless > Wireless Security (Бездротова мережа > Безпека бездротової мережі). Змініть режим безпеки на WPA2 Personal. В даний час AES вважається найнадійнішим протоколом шифрування. Залишіть цей метод захисту.

b. Введіть aCompWiFi як парольну фразу. Прокрутіть сторінку вниз до кінця та натисніть кнопку Save Settings (Зберегти установки).

Крок 5: Налаштування Laptop0 як бездротовий клієнт

a. Налаштуйте Laptop0 для підключення до бездротової мережі за допомогою

параметрів інформаційної безпеки на бездротовому маршрутизаторі

1) Виберіть Laptop0 > Desktop > PC Wireless (Laptop0 > Робочий стіл > Бездротова мережа).

2) Виберіть Profiles > New (Профілі > Створити) та введіть будь-яке ім'я для профілю.

3) Виберіть Advanced Setup (Розширені налаштування) у нижньому правому куті.

4) Виберіть Wireless Network Name (Ім'я бездротової мережі) та введіть нове ім'я SSID: aCompany.

5) Прийміть параметри мережі за замовчуванням, натиснувши кнопку Далі.

6) Змініть значення у списку Security (Безпека) на WPA2-Personal та натисніть кнопку Далі.

7) Введіть PSK-ключ aCompWiFi і натисніть кнопку Далі.

8) Збережіть профіль.

9) Виберіть Connect to Network (Підключитися до мережі).

10) Якщо ноутбук не вдасться підключити, поверніться до профілю та внесіть зміни. Перевірте правильність введення імені SSID та PSK-ключа.

b. Закрийте вікно PC Wireless (Бездротова мережа) та клацніть командний рядок.

c. Введіть ipconfig /all та запишіть IP- та MAC-адреси.

Крок 6: Налаштування підтримки фільтрації MAC-адрес для WRS1

a. Перейдіть на сторінку конфігурації бездротового маршрутизатора.

b. Перейдіть до Wireless > Wireless MAC Filter (Бездротова мережа > Бездротовий фільтр) MAC-адрес).

c. Виберіть Enabled (Увімк.) та Permit PCs listed below to access wireless network (Дозволити) наведених нижче комп'ютерів доступ до бездротової мережі).

d. Введіть MAC-адресу для Laptop0 у полі MAC 01:. Зверніть увагу, що MAC-адреса повинна бути у форматі XX:XX:XX:XX:XX:XX.

e. Перейдіть до кінця вниз і натисніть кнопку Save Settings (Зберегти параметри).

f. Підключіть Laptop0 до WRS1 ще раз.

Крок 7: Перевірка фільтрації MAC-адрес у мережі WRS1

a. Додайте до топології інший ноутбук.

b. Натисніть кнопку живлення на новому ноутбуку, щоб вимкнути його, та замініть плату Ethernet на бездротову плату.

c. Налаштуйте новий ноутбук за допомогою параметрів інформаційної безпеки, необхідні для підключення до бездротового маршрутизатора.

Чому не вдається зв'язатися з точкою доступу?_____

Крок 8: Вимкніть дистанційне керування на бездротовому маршрутизаторі.

a. Перевірте стан віддаленого керування на бездротовому маршрутизаторі.

Виберіть Administration > Remote Access (Адміністрування > Віддалений доступ). Якщо він вимкнено, увімкніть його.

b. Виберіть Hacker PC (ПК хакера), а потім виберіть Desktop > Web Browser (Робочий стіл > Веб) - браузер). Введіть адресу 192.31.7.100 та натисніть Go

(Перейти). Вам буде запропоновано ввести ідентифікатор користувача та пароль. Введіть правильні дані, і вам буде дозволено доступ до графічного інтерфейсу користувача бездротового маршрутизатора. Вийдіть з робочого столу.

c. Перейдіть на сторінку конфігурації бездротового маршрутизатора.

d. Поверніться до розділу Administration > Management (Адміністрування > Керування) та прокрутіть вниз до пункту Remote Management. Виберіть Disabled (Вимкнено) та натисніть кнопку Save Settings (Зберегти параметри) у нижній частині екрана.

e. Поверніться до Hacker PC (ПК хакера) та виберіть Desktop > Web Browser (Робочий стіл > Веб-браузер). Введіть адресу 192.31.7.100. Тепер має бути неможливо підключитись через веб-браузер.

Лабораторна робота 11.
Виявлення своєї власної ризикованої поведінки у мережі

Завдання

Вивчити дії в Інтернеті, які можуть поставити під загрозу вашу безпеку та конфіденційність.

Загальні відомості/сценарій

Інтернет може бути ворожим середовищем, і необхідно зберігати пильність, щоб дані не виявилися скомпрометовані. Хакери винахідливі і намагаються обдурити користувачів за допомогою численних хитрощів. Ця лабораторна робота допомагає визначити ризиковану поведінку в мережі та містить поради, як підвищити свою безпеку в Інтернеті.

Частина 1. Вивчення умов політики надання послуг

Чесно дайте відповідь на наведені нижче питання і зверніть увагу на кількість балів, які дає кожна відповідь. Додайте всі бали до загального результату та перейдіть до частини 2 для аналізу поведінки в мережі.

a. Якими відомостями ви ділитеся із сайтами соціальних мереж? _____

1) Будь-якими; я використовую соціальні мережі, щоб підтримувати зв'язок із друзями та членами сім'ї. (3 бали)

2) Я шукаю та читаю новини та статті. (2 бали)

3) по-різному; я відбираю інформацію, якою поділяюся, і людей, з якими поділяюся. (1 бал)

4) Ніякими; я не використовую соціальних мереж. (0 бали)

b. Під час створення нового облікового запису на веб-службі ви робите наступне. _____

1) Повторно використовуєте пароль, який використовується в інших службах, який легко запам'ятати. (3 бали)

2) Створіть якнайпростіший пароль, щоб запам'ятати його. (3 бали)

3) Створюєте дуже складний пароль та зберігаєте його у службі диспетчера паролів. (1 бал)

4) Створюєте новий пароль, схожий, але відмінний від пароля, який використовується в іншій службі. (1 бал)

5) Створюєте абсолютно новий надійний пароль. (0 бали)

c. Якщо ви отримали електронний лист із посиланнями на інші сайти, ви робите таке. ____

1) Не відкривайте посилання, оскільки ви ніколи не слідуєте за посиланнями, отриманими електронною поштою. (0 бали)

2) Відкриваєте посилання, оскільки електронний лист уже перевірено на сервері електронної пошти. (3 бали)

3) Відкриваєте всі посилання, якщо електронний лист надійшов від користувача, якого ви знаєте. (2 бали)

4) Наведіть вказівник миші на посилання, щоб перевірити URL-адресу призначення, перш ніж відкрити її. (1 бал)

d. Під час відвідування веб-сайту відкрилося спливаюче вікно. У ньому стверджується, що комп'ютер знаходиться під загрозою і слід завантажити та встановити програму діагностики з метою безпеки. _____

1) Ви натискаєте, завантажуєте та встановлюєте цю програму для захисту комп'ютера. (3 бали)

2) Ви уважно вивчаєте спливаючі вікна і наводите вказівник миші на посилання, щоб перевірити її достовірність. (3 бали)

3) Пропускаєте повідомлення, акуратно уникаєте натискання на нього або завантаження програми та закриваєте веб-сайт. (0 бали)

e. Коли потрібно виконати вхід на веб-сайт фінансової установи, щоб зробити будь-які дії, ви робите таке. _____

1) Негайно вводьте облікові дані. (3 бали)

2) Перевіряєте URL-адресу, щоб переконатися, що це саме та установа, яка вам потрібна, перш ніж ввести будь-яку інформацію. (0 бали)

3) Не використовуєте інтернет-сайти банків та інші фінансові послуги в Інтернеті. (0 бали)

f. Ви прочитали про програму та вирішили її випробувати. Ви знайшли в Інтернеті пробну версію на невідомому сайті, а потім робите таке. _____

1) Негайно завантажуєте та встановлюєте програму. (3 бали)

2) Шукайте додаткові відомості про творця програми, перш ніж завантажити її. (1 бал)

3) Не завантажуєте та не встановлюєте програму. (0 бали)

g. Дорогою на роботу ви знаходите USB-накопичувач. Ваші дії є наступними. _____

1) Підніміть його та вставте у свій комп'ютер, щоб переглянути вміст. (3 бали)

2) Підніміть його та вставте у свій комп'ютер, щоб повністю стерти весь вміст перед подальшим використанням накопичувача. (3 бали)

3) Підніміть його та вставте у свій комп'ютер, щоб перевірити за допомогою антивірусної програми, перш ніж використовувати для зберігання власних файлів. (3 бали)

4) Не піднімете. (0 бали)

h. Вам необхідно підключитися до Інтернету, і ви виявляєте відкриту точку доступу Wi-Fi. Ви: _____

1) Підключаєтеся до неї та виходьте в Інтернет. (3 бали)

2) Не підключаєтеся та чекаєте, доки не встановіть довірене з'єднання. (0 бали)

3) Підключаєтеся та встановлюєте VPN-з'єднання з довіреним сервером перед відправкою будь-яких відомостей. (0 бали)

Частина 2. Аналіз поведінки у мережі

Чим більший результат, тим менш безпечна ваша поведінка в мережі. Ціль полягає в тому, щоб досягти повної безпеки, звертаючи увагу на всі взаємодії в Інтернеті. Це дуже важливо, оскільки достатньо однієї помилки, щоб наразити на небезпеку комп'ютер і дані.

Додати бали з частини 1. Запишіть свій результат. _____

0: рівень вашої безпеки в Інтернеті дуже високий.

0–3: ви певною мірою знаходитесь в безпеці в Інтернеті, але вам все ж таки слід змінити поведінку, щоб бути у повній безпеці.

3–17: Ваша поведінка в Інтернеті є небезпечною, і існує високий ризик компрометації даних.

18 або більше: ви наражаєтеся на дуже велику небезпеку в Інтернеті, і ваші дані рано чи пізно будуть скомпрометовані.

Нижче наведено деякі важливі поради щодо безпеки в мережі.

a. Чим більше ви ділитеся інформацією у соціальних мережах, тим більше хакер може дізнатися про вас. За допомогою додаткових знань хакер зможе точніше націлити свою атаку. Наприклад, оголосивши, що були на автоперегонах, ви дозволите хакеру скласти шкідливий електронний лист нібито від компанії, що розповсюджує квитки на перегони. Оскільки ви щойно були на перегонах, такий лист не викличе підозри.

b. Повторно використовувати паролі – погана звичка. Якщо ви повторно використовуєте пароль у службі, контрольованій зловмисником, він зможе скористатися цим паролем для входу від вашої особи до інших служб.

c. Адреси електронної пошти легко підробити так, щоб вони виглядали вірогідно. Підроблені листи електронної пошти часто містять посилання на шкідливі сайти або програми. Візьміть за правило не відкривати вбудовані посилання, отримані електронною поштою

d. Не встановлюйте жодних програм, які ви не запитували, особливо якщо вони розповсюджуються з веб-сторінок. Дуже малоймовірно, що веб-сторінка містить законне оновлення програмного забезпечення. Рекомендується закрити браузер і використовувати інструменти операційної системи для перевірки наявності оновлень.

e. Шкідливі веб-сторінки легко зробити схожими на веб-сайт банку або фінансової установи. Перш ніж відкривати посилання або надавати будь-яку інформацію, перевірте URL-адресу, щоб переконатися, що перед вами правильна веб-сторінка.

f. Дозволяючи запуск програми на комп'ютері, ви надаєте широкі права. Добре подумайте, перш ніж дозволити запуск програми. Вивчіть усі дані та переконайтеся, що компанія або співробітник, який надає програму, є серйозним і законним автором. Крім того, намагайтеся завантажувати програми лише з офіційного веб-сайту компанії або приватної особи.

g. USB-диски та флеш-карти пам'яті містять мікроконтролер для взаємодії з комп'ютерами. Такий контролер можна заразити і змусити його встановити на комп'ютері шкідливе програмне забезпечення. Оскільки зловмисне програмне забезпечення розміщується в контролері USB, а не в області даних, жодне стирання або антивірусне сканування не виявить його.

h. Хакери часто розгортають підроблені точки доступу Wi-Fi, щоб залучити користувачів. Хакер отримує доступ до всієї інформації, що передається через скомпрометовану точку доступу, тому користувачі, підключені до неї, наражаються на великий ризик. Ніколи не використовуйте невідомі точки доступу Wi-Fi без шифрування трафіку через VPN. Якщо використовується невідома мережа (дротова

або бездротова), ніколи не надавайте конфіденційні дані, такі як номери кредитних карток.

Питання для повторення

Після аналізу своєї поведінки в мережі, які зміни ви зробите, щоб захистити себе в Інтернеті? _____

Лабораторна робота 12.
Можливості навчання та кар’єри в галузі Інтернету речей

Завдання

Мета – вивчення вакансій і можливостей навчання в світі Інтернету речей, що постійно розвивається.

Частина 1. Визначення трьох вакансій, пов'язаних із Інтернетом речей.

Частина 2. Вивчення доступних вакансій та визначення необхідних навичок.

Частина 3. Визначення доступних можливостей для навчання, що дозволяють отримати ці навички.

Частина 4. Обмін цією інформацією з однокурсниками для колективного складання списку вакансій та можливостей навчання у сфері Інтернету речей у своєму регіоні.

Загальні відомості/сценарій

Інтернет речей зростає експонентно. Регулярно з'являються нові технології та програми, і в результаті з'являється безліч нових вакансій, кожна з відповідним набором необхідних навичок. Важливо знати про навички, необхідні на цьому ринку праці, щоб отримати переваги від безлічі можливостей навчання, доступних на сьогоднішній день.

Необхідні ресурси

ПК з доступом до Інтернету та сучасним веб-браузером.

Частина 1. Використовуйте веб-браузер для пошуку вакансій у сфері Інтернету доступних речей.

a. Відкрийте веб-браузер і перейдіть на сайт https://google.com site.

b. Введіть пошуковий запит "types of jobs with learning opportunities in the internet of things" (типи вакансій із можливостями навчання у сфері Інтернету речей).

c. Можна включити інші відповідні слова, наприклад "lifelong learning" (навчання протягом усього життя) або навіть назву посади, на якій ви вже зацікавлені.

d. Визначте та задокументуйте три визначення робочих позицій, у яких ви зацікавлені._____
_____

Частина 2. Визначте набір навичок, необхідних кожної з цих позицій.

a. За допомогою пошукової системи Google досліджуйте посади, які визначили предметом своїх інтересів. Виконайте пошук наборів навичок, необхідних цих посад. Зверніть особливу увагу на навички, які необхідні для кількох позицій._____
_____

Частина 3. Вивчення можливостей навчання.

a. За допомогою пошукової системи Google та інших доступних ресурсів вивчіть можливості навчання, доступні на цих посадах. Задокументуйте всі відомості, отримані у цьому дослідженні._____
_____

Частина 4. Формування бази даних з вакансій та можливостей навчання, пов'язаних з Інтернетом речей.

а. Спільно з однокурсниками складіть перелік доступних вакансій, пов'язаних з Інтернетом речей, необхідних наборів навичок та можливостей навчання. Спробуйте визначити тенденції та скласти особистий план навчання на основі цієї інформації._____
_____

Питання для повторення

Чи спостерігаються якісь тенденції на ринку праці Інтернету речей?

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Поліщук М.М. Інтернет Речей. Конспект лекцій для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Кібербезпека» галузь знань 12 Інформаційні технології спеціальності 125 Кібербезпека денної та заочної форм навчання. Луцьк: ЛНТУ, 2021. 108 с.

2. Технології інтернету речей. Навчальний посібник для студ. спеціальності 126 «Інформаційні системи та технології», спеціалізація «Інформаційне забезпечення робототехнічних систем» / Б. Ю. Жураковський, І.О. Зенів. Київ: КПІ ім. Ігоря Сікорського, 2021. – 271 с. URL: https://ela.kpi.ua/bitstream/123456789/42078/1/Zhurakovskyi_B_Zeniv_Tehnologii_internet_rechey.pdf (Дата звернення: 16.04.2025).

3. Internet of Things (IoT). (2023). (n.p.): SK Research Group of Companies. 4. Сторчак К.П., Тушич А.М., Срібна І.М., Яковенко Н.Д., Кравець Д.В. Технології Інтернет речей. Навч. посібник підготовлено для студентів вищих навчальних закладів – Київ: ДУТ, 2021. – 68 с.

4. Cisco. Networking Academy URL: https://www.netacad.com/ (дата звернення: 28.03.2025).

5. Поліщук, М., Семенюк, О., Поліщук, Л., & Ломакін, М. (2023). Можливості авторизації та захисту даних користувача під час розробки хмарних веб-додатків для IoT. *// Науковий журнал «Комп'ютерно-інтегровані технології: освіта, наука, виробництво».* (52), 94-103. URL: https://doi.org/10.36910/6775-2524-0560-2023-52-12.

6. Tkachuk A., Polishchuk M., Polishchuk L., Kostiuchko S., Hryniuk S., & Konkevych, L. (2025). Investigation of DC-AC converter with microcontroller control of inverter frequency. *Informatyka, Automatyka, Pomiary W Gospodarce I Ochronie Środowiska*, *15*(1), 55-61. URL: https://doi.org/10.35784/iapgos.6984.

7. Douglass Robert et al. IoT for Defense and National Security. Robert Douglass, Keith Gremban, Ananthram Swami, Stephan Gerali. Wiley-IEEE Press, 2023. 516 p. ISBN: 978-1119892144.

8. Al-Turjman F., Yadav S.P., Kumar M., Yadav V., Stephan T. (Eds.) Transforming Management with AI, Big-Data, and IoT. Springer, 2022. 315 p. ISBN 13 9783030867485.

9. Dow Colin. Mastering IoT: Build modern IoT solutions that secure and monitor your IoT infrastructure. Packt Publishing, 2019. 782 p.

10. Heins Kersten. NB-IoT Use Cases and Devices: Design Guide. Springer, 2022. 265 p. ISBN 978-3-030-84973-3.

11. Lele Chitra. Internet of Things (IoT) A Quick Start Guide: A to Z of IoT Essentials. BPB Publications, 2022. 227 p.

У І-73 Інженерія Інтернету Речей: методичні вказівки до лабораторних занять для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Комп'ютерна інженерія» галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія денної та заочної форм навчання / уклад. М. М. Поліщук : ЛНТУ, 2025. 96 с.

Комп'ютерний набір: М. М. Поліщук

Редактор: М. М. Поліщук

Підп. до друку «___» _____ 2025р.
Формат 60х84/16. Папір офс. Гарнітура Таймс.
Ум. друк. арк. ____. Тираж 10 прим. Зам. ____

Відділ іміджу та промоції
Луцького національного технічного університету
43018, м. Луцьк, вул. Львівська, 75
Друк – ВІП ЛНТУ