**Лабораторна робота №2**

**Моделювання IoT мережі розумного будинку засобами програми Cisco Packet Tracer**

Зміст

[Мета і завдання 1](#_Toc54820462)

[Література 5](#_Toc54820463)

[Додаток А 6](#_Toc54820464)

[А.1 Теоретичні відомості 6](#_Toc54820465)

[А.2 Дослідження компонентів «Розумного будинку» 8](#_Toc54820466)

[**Дослідження центрального шлюзу IoT** 8](#_Toc54820467)

[**Дослідження кінцевих пристроїв IoT** 11](#_Toc54820468)

[А.3 Побудова власної мережі 12](#_Toc54820469)

[**Налаштування** **центрального шлюзу IoT** 12](#_Toc54820470)

[**Комплектація хмарного комутаційного пристрою** 14](#_Toc54820471)

[**Підключення пристроїв** 15](#_Toc54820472)

[**Налаштування хмарного комутаційного пристрою** 15](#_Toc54820473)

[**Налаштування сервера** 17](#_Toc54820474)

[**Перевірка мережевих налаштувань** 20](#_Toc54820475)

[А.4 Додавання провідних пристроїв в інтелектуальну домашню мережу з використанням технології Ethernet 21](#_Toc54820476)

[**Приєднання газонного розпилювача до домашнього шлюзу** 21](#_Toc54820477)

[**Налаштування розпилювача для мережевого підключення** 22](#_Toc54820478)

[**Перевірка налаштування розпилювача** 24](#_Toc54820479)

[А.5 Додавання бездротових пристроїв в домашню мережу з використанням технології WiFi 26](#_Toc54820480)

[Додаток Б Варіанти завдань 33](#_Toc54820481)

# Мета і завдання

**Метою лабораторної роботи** є ознайомлення з архітектурою IoT системи на прикладі мережі «Розумного будинку» і придбання початкових навичок налаштування компонентів такої мережі.

Програма моделювання Cisco Packet Tracer призначена для проектування різних видів мереж, в тому числі IoT. «Розумний будинок» – єдина система управління в квартирі, офісі або будинку, що включає в себе датчики, керуючі елементи і виконавчі пристрої.

**Рекомендації**

Перед виконанням лабораторної роботи слід:

1. Повторити теоретичний матеріал, пригадати виконання і подивитись «Додатки» **до лабораторних робіт №3 і №3-а за 4-й курс з дисципліни «Комп’ютерні мережі»**.
2. Прочитати розділи 2 і 9 з конспекту лекцій даного курсу а також прочитати про загальну архітектуру ІоТ з файлу «Інтернет речей». Познайомитись з теоретичними відомостями (Додаток А.1).
3. **Виконувати роботу буде простіше**, якщо спочатку прочитати певний пункт завдання, а потім дивитись його виконання в Додатку А.2–А.5.

**Завдання**

1. Дослідження існуючої інтелектуальної домашньої мережі і кінцевих IoT пристроїв в ній (файл із заготівлею додається).

1.1. Ознайомитись з налаштування мережевих інтерфейсів головного шлюзу LAN, wireless та Internet, записавши:

- IP-адресу і маску домашньої мережі;

- IP-адресу LAN інтерфейсу головного шлюзу;

- для wireless інтерфейсу: SSID точки доступу, режим безпеки і пароль, номер радіочастотного каналу.

- для Internet інтерфейсу: IP-адресу і маску інтерфейсу, IP-адресу DNS серверу і шлюзу за замовчанням, які він отримує від хмарного сервера;

1.2. Ознайомитись з налаштування хмарного сервера. Для цього потрібно клацнути на піктограмі хмари, натисніть на сервер, виберіть Config і записати:

- IP-адреси для інтерфейсу, підключеного до нашої мережі (IP-адресу і маску інтерфейсу, IP-адресу DNS серверу і шлюзу за замовчанням);

- налаштування DHCP сервісу для зовнішнього інтерфейсу домашнього шлюзу. Для цього потрібно вибрати вкладку Services, в ній зліва – DHCP і записати: IP-адресу і маску мережі, початкову адресу пулу динамічних IP-адрес, максимальну кількість вузлів, що можуть отримати динамічні налаштування стеку TCP/IP, IP-адресу DNS серверу і шлюзу за замовчанням. Закрити вікно сервера. Щоб повернутись до основного робочого поля потрібно натиснути Back на верхньому меню головного вікна програми Packet Tracer.

1.3. Ознайомитись з налаштування мережевих інтерфейсів IoT пристроїв, записавши: IP-адресу і маску інтерфейсу, IP-адресу DNS серверу і шлюзу за замовчанням (планшет, двері в будинок та гараж), які вони отримують від DHCP сервісу головного шлюзу.

2. Побудувати власну мережу з ІоТ пристроями, яка має мати вигляд, як на рис.1. **Варіанти обираються за списком групи (денної/заочної)** в Додатку Б.

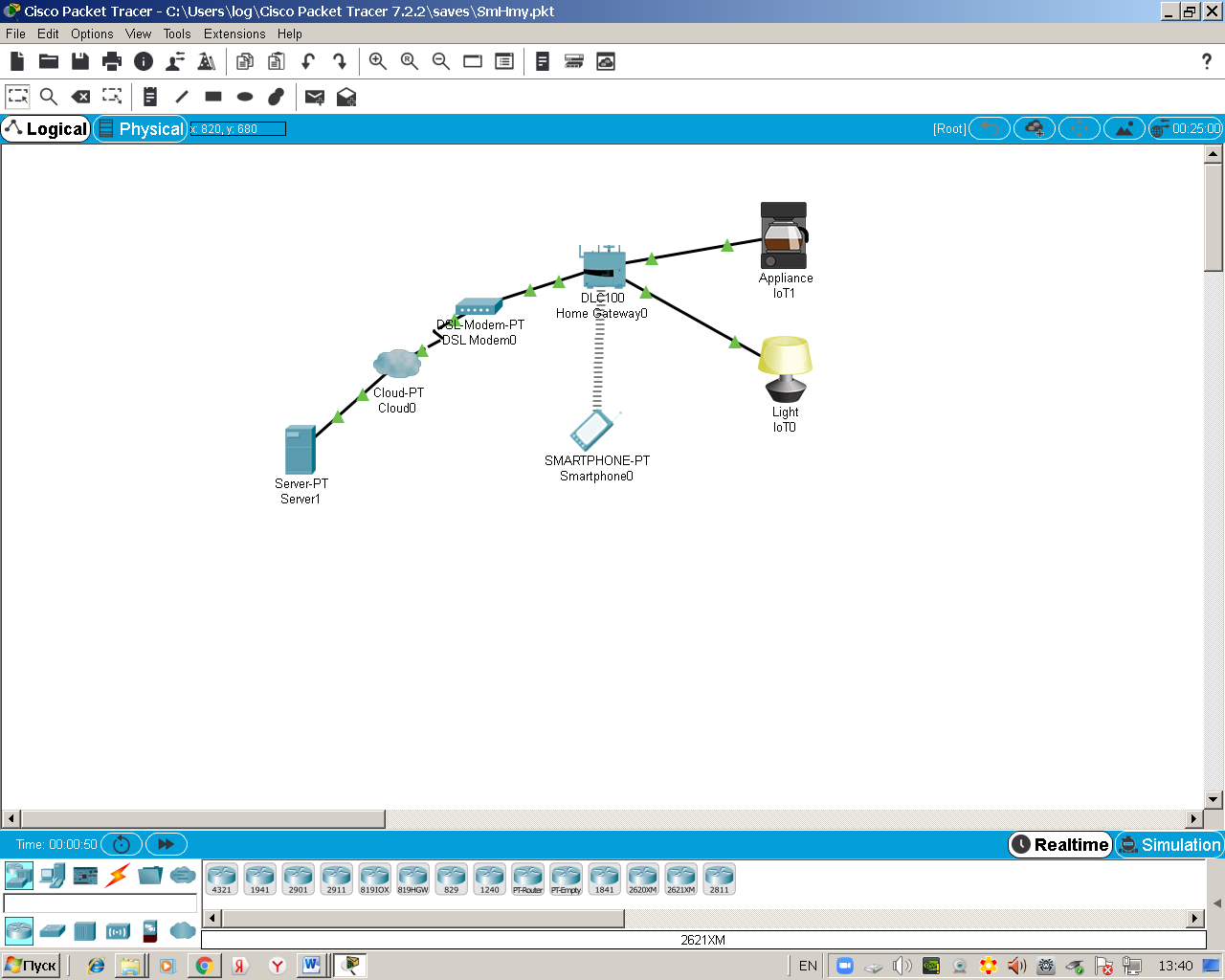


Рис. 1. Приклад мережі ІоТ пристроїв

2.1. В кінці імен кінцевих пристроїв додайте через пробіл 3 літери свого прізвища.

Сервер належить до мережі провайдера. Шлюз підключений до сервера в режимі віддаленого доступу з використанням технології DSL або CaTV (за варіантом). Абстрактно будь-яка мережа доступу, технологія останньої милі чи інша провайдерська мережа в програмі Packet Tracer зображується у вигляді Інтернет-хмари, а інше залежить від налаштувань комутаційного обладнання. Інтерфейси DTE-DCE для шлюзу і сервера – технологія Ethernet/FastEthernet.

Для побудови мережі потрібно спочатку створити і налаштувати локальну мережу, а потім – глобальну.

|  |  |  |  |
| --- | --- | --- | --- |
| Мережа/Пристрій | Технології/Інтерфейси | ІР-адреси | Маска |
| Домашня мережа | Ethernet i WiFi | З простору приватних адрес класу С, в 3-му байті – № варанту | 255.255.255.0 |
| Шлюз | Internet | DHCP |  |
| Локальна мережа | Статично |  |
| Пристрої локальної мережі | Ethernet, WiFi і аналогові (в деяких варіантах) | DHCP |  |
| Мережа провайдера | Fast Ethernet, технологія доступу DSL або CaTV | З простору публічних адрес класу С, в 2-му байті – № варанту | 255.255.255.0 |
| Сервер |  | Статично |  |

Будувати локальну WiFi мережу потрібно в такому порядку:

- додати і налаштувати шлюз;

- додати і налаштувати пристрій управління ІоТ сервером (планшет, смартфон або ноутбук).

Будувати глобальну мережу потрібно в такому порядку:

- вибрати DCE пристрій відповідно до типу технології віддаленого доступу (за варіантом);

- підключити DCE – модем до шлюзу;

- додати мережу доступу (хмару) і сервер;

- підключити сервер і модем до хмари;

- налаштувати передачу даних через хмарний комутаційний пристрій, який відіграє роль DCE з боку сервера;

- налаштувати хмарний сервер як DHCP – сервер для зовнішнього інтерфейсу шлюзу, як DNS – сервер для локальної мережі ІоТ, та як ІоТ сервер (якщо вказано за варіантом в Додатоку Б).

- перевірити правильність налаштувань за допомогою пристрою реєстрації.

- тепер як варіант потрібно налаштувати параметри стеку TCP/IP для Інтернет інтерфейсу шлюзу статично. Що можна змінити (чи не задавати) порівняно з налаштуваннями через DHCP без впливу на перевірку правильності налаштувань в даній топології?

3. Додавання провідних і бездротових IoT пристроїв за варіантом в інтелектуальну домашню мережу.

Додайте 1 пристрій бездротовим з’єднанням і 1 пристрій – провідним з’єднанням з переліку програми. В кінці імені пристрою додайте через пробіл 3 літери свого прізвища.

4. Узгодьте роботу ІоТ пристроїв за умовами варіанту.

**Звіт**

Привести відповідні скриншоти і виписані дані по пунктах завдання.

**Контрольні запитання**

1. Розуміти значення полів таблиці маршрутизації. Що таке Gateway та Interface? Які значення вини повинні мати для конкретних пристроїв в даній топології?
2. Які IP- адреси потрібно налаштувати на кінцевій РС, щоб забезпечити передавання даних по доменних іменах і IP- адресах?
3. Як налаштувати бездротовий WiFi інтерфейс?
4. Яке призначення і основні функції протоколів DHCP, DNS, NAT?
5. Яку загальну архітектуру має мережа Інтернет?
6. Що таке режим віддаленого доступу, і чи використовується він у даній топології?
7. Що таке DTE, DCE, інтерфейси DTE-DCE? Привести приклади з даної топології.
8. Що таке технологія останньої милі і мережа доступу? Що з цього є у даній топології.
9. Яка загальна архітектура ІоТ системи?
10. Які функції виконує ІоТ шлюз і інші компоненти ІоТ системи?
11. Яку архітектуру мають туманні, хмарні і крайові обчислення? Що з цього є в даній топології, а чого немає?
12. Скільки портів і які протоколи транспортного рівня використовують у своїй роботі ці протоколи?
13. Вміти пояснити всі пункти роботи.

# Література

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. — СПб.: Питер, 2010. — 944 c.
2. Компьютерные сети. Сертификация Networks+ .Учебный курс/Пер. с англ.-М.: Издательско-торговый дом «Русская редакция». 2002.-703с.
3. Робота в пакеті Cisco Packet Tracer: <https://www.intuit.ru/studies/courses/3549/791/info>
4. Посібник з роботи у CISCO\_PACKET\_TRACER\_6 <https://cloudofscience.ru/sites/default/files/files/2016_Kulakov_V.G.,_Leohin_YU.L._Modelirovanie_kompyuternyh_setej_v_simmulyatore_CISCO_PACKET_TRACER_6.pdf>
5. Форум – запитання з використання CISCO\_PACKET\_TRACER <http://www.cyberforum.ru/cisco/thread968802.html>

# Додаток А

# А.1 Теоретичні відомості

IoT система розумного будинку складається з типових елементів: мережі датчиків, граничного шлюзу (Home Gateway), який з одного боку підтримує технології периферійної мережі, а з іншого – технологію глобальної мережі, за допомогою якої шлюз підключено до хмарного серверу. В даному прикладі кінцеві пристрої об’єднані стандартними технологіями локальних мереж (Ethernet і WiFi) та підтримують стек TCP/IP як і мережа Інтернет. Домашній IoT шлюз виконує функції бездротової точки доступу для пристроїв з WiFi інтерфейсами, IPv4 маршрутизатора для провідних і бездротових пристроїв, DHCP серверу для всіх пристроїв локальної мережі, NAT - для зовнішньої мережі, а також IoT серверу для пристроїв IoT (в частині варіантів). Сервер в даному прикладі знаходиться в мережі локального провайдера, і шлюз підключається до нього в режимі віддаленого доступу, а не через мережу Інтернет.

**Бездротова точка доступу** використовує унікальне мережеве ім'я для ідентифікації мережі - ідентифікатор обслуговування мережі - SSID, а також працює в певному частотному каналі. При установці адаптера Wi-Fi потрібно вказати SSID точки доступу. При підключенні до існуючої бездротової мережі, необхідно вказати ім'я цієї мережі. Ім'я може мати довжину до 32 символів і містити букви і цифри.

Трафік між точкою доступу і кінцевими пристроями шифрується. На сьогоднішній день існує три типи шифрування Wi-Fi підключень: WPA. WPA2. WEP.

WEP (Wired Equivalent Privacy) - алгоритм для забезпечення безпеки мереж Wi-Fi. WPA (Wi-Fi Protected Access) - являє собою технологію захисту бездротової Wi-Fi мережі. Плюсами WPA є посилена безпека даних і посилений контроль доступу до бездротових мереж, а також - сумісність між безліччю бездротових пристроїв як на апаратному рівні, так і на програмному. WPA2 - вдосконалений варіант WPA, зокрема в ньому реалізовано понад стійке шифрування AES.

Типи шифрування мережі WPA і WPA2 вимагають від абонентів введення унікального пароля – ключа шифрування. Після перевірки введеного ключа всі дані, які передаються між учасниками мережі, шифруються. Протокол WPA2 у зв'язці з алгоритмом AES надає більш високий ступінь захисту. При наявності можливості слід вибирати саме їх.

Також для WPA і WPA2 визначений спрощений режим Pre-Shared Key (WPA-PSK і WPA2-PSK). Режим дозволяє використовувати один пароль, який зберігається безпосередньо на маршрутизаторі. Тобто всі користувачі заходять з одним паролем, і немає необхідності супроводжувати базу користувачів. Це доцільно і достатньо безпечно в умовах домашньої мережі.

**DHCP сервер** - дозволяє організовувати пули мережевих налаштувань для автоматичної конфігурації мережевих інтерфейсів. Dynamic Host Configuration Protocol забезпечує автоматичний розподіл IP-адрес між комп'ютерами-клієнтами в мережі і налаштування на них інших параметрів стека TCP/IP (IP-адреси DNS-сервера і наступного маршрутизатора - шлюзу).

Інтерфейс точки доступу/роутера з боку локальної мережі автоматично отримує першу IP адресу з адресного простору мережі за замовчуванням на постійній основі, а всі пристрої отримають наступні динамічні адреси.

Адреси за замовчуванням можна змінити на потрібні. На рис.А.1 у якості прикладу показано налаштування DHCP сервісу на комп’ютері-сервері. У мережі 192.168.39.0/24 задано адресний простір для 40 інтерфейсів пристроїв з динамічним призначенням адрес, починаючи з адреси 192.168.39.16 (стартова+1). Адреси 192.168.39.1 - 192.168.39.15 резервуються для призначення статично. Всі пристрої будуть використовувати DNS сервер з адресою 192.168.39.2 та шлюз за замовченням (Default Gateway) з адресою 192.168.39.254. Ці статичні адреси були раніше призначені при безпосередньому налаштуванні DNS серверу та інтерфейсу маршрутизатора, до якого вузли будуть звертатися при необхідності передачі даних за межі мережі 192.168.39.0/24.

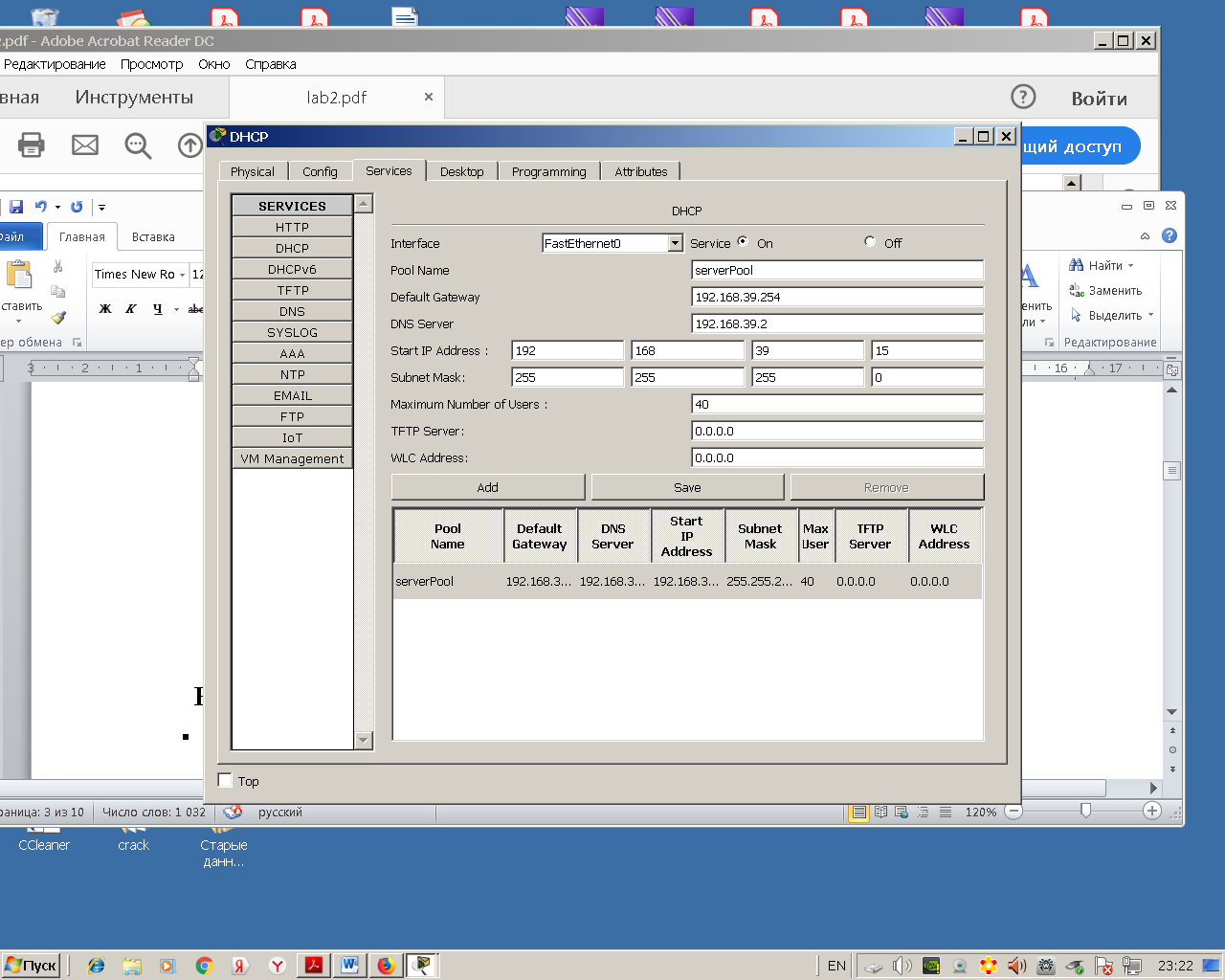


Рис.А.1. Приклад налаштування DHCP сервера

**NAT (Network Address Translation** - перетворення мережних адрес) - це механізм в мережах TCP / IP, що дозволяє перетворювати (підміняти) IP-адреси транзитних пакетів.

Перетворення адреси методом NAT може проводитися маршрутизатором, сервером доступу, фаєрволом. Найбільш популярним є NAPT – форма NAT, при якій кілька незареєстрованих IP- адрес внутрішньої мережі відображаються в єдину зареєстровану зовнішній IP- адресу. Додатково проводиться заміна номерів портів в заголовках протоколів TCP і UDP. При проходженні пакета в одну сторону проводиться заміна адреси і порту джерела (source), а у пакеті відповіді – зворотна заміна адреси і порту призначення (destination).

При пересиланні пакета від локального комп'ютера в Інтернет маршрутизатор транслює (підміняє) в заголовку пакета IP-адресу відправника на свою зовнішню IP-адресу, а номер порту джерела замінює на деякий унікальний. Відповідність «локальна IP-адреса + номер порту відправника – унікальний номер порту відправника» роутер зберігає у себе в тимчасовій таблиці. Коли на маршрутизатор з Інтернет приходять пакети відповідей, адресовані різним локальним комп'ютерам, маршрутизатор по таблиці знову робить заміну в заголовках IP- пакетів. Тепер маршрутизатор змінює адресу і порт одержувача, та відправляє пакети в локальну мережу. Через певний час після того, як деякий клієнт і сервер закінчать обмінюватися пакетами, роутер стирає у себе в таблиці відповідний запис за терміном давності.

Використання NAT дозволяє:

- Економити обмежений простір унікальних IP-адрес.

- Приховати від зовнішнього спостерігача структуру внутрішньої IP- мережі, яка ззовні виглядає як єдине IP-підключення.

# А.2 Дослідження компонентів «Розумного будинку»

**Дослідження центрального шлюзу IoT**

Натиснувши піктограму Home Gateway в робочому просторі Packet Tracer Logical, відкриємо вікно його налаштувань.



Рис.А.2. Піктограма ІоТ шлюзу домашньої мережі

Вкладенка Phisical (вибрана за замовчанням) відображує зовнішній вигляд головного шлюзу.

Рис. А.3. Зовнішній вигляд ІоТ шлюзу

Вкладка Config показує мережеві налаштування шлюзу. Натиснувши в лівій панелі Settings, можна переглянути загальні налаштування пристрою. В даному випадку задається тільки його ім’я. В переліку INTERFACE, натиснувши LAN, Wireless або Internet, можна переглянути налаштування мережевих інтерфейсів головного шлюзу. Після перегляду вікно Home Gatewy потрібно закрити.

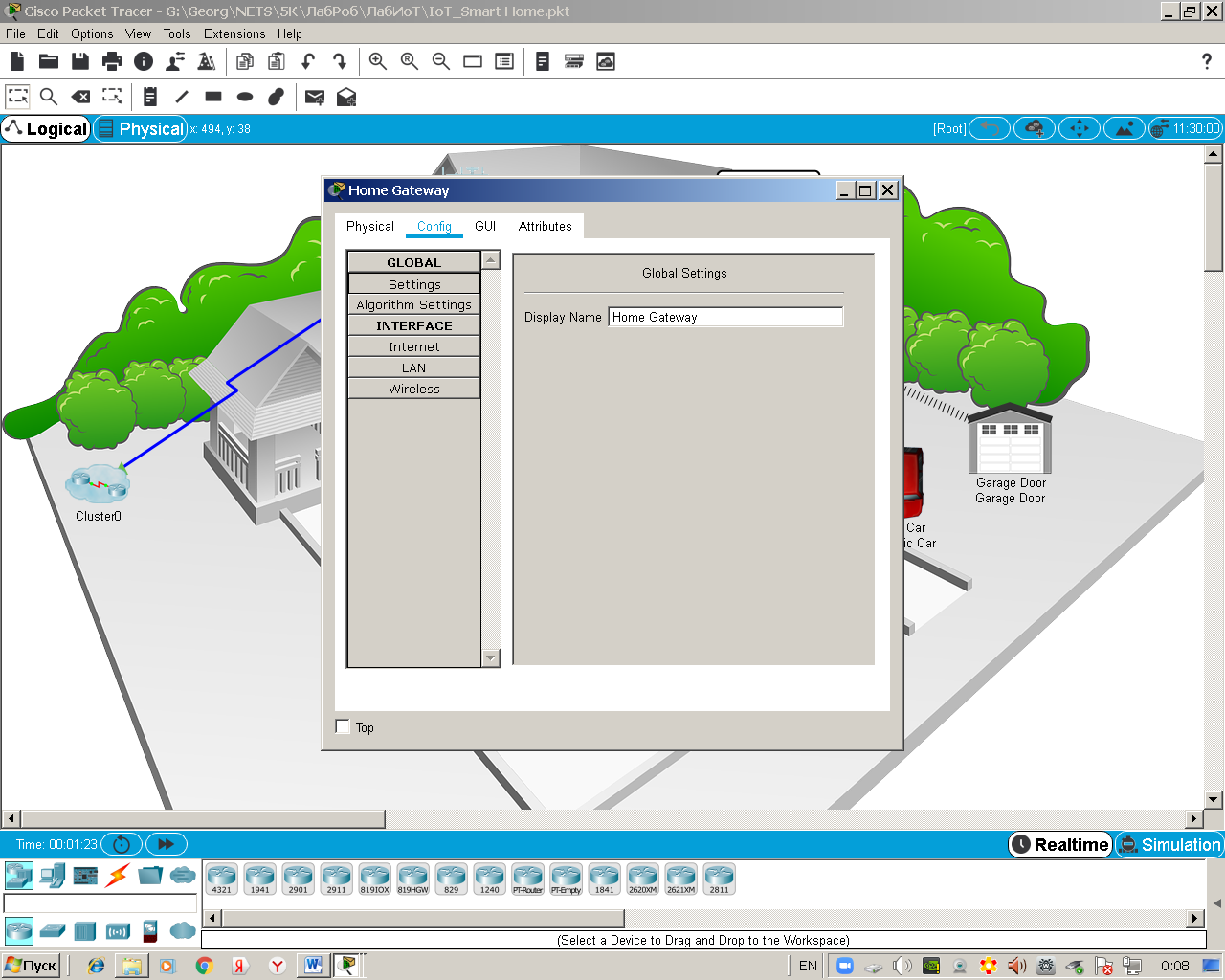


Рис. А.4. Загальні налаштування головного шлюзу

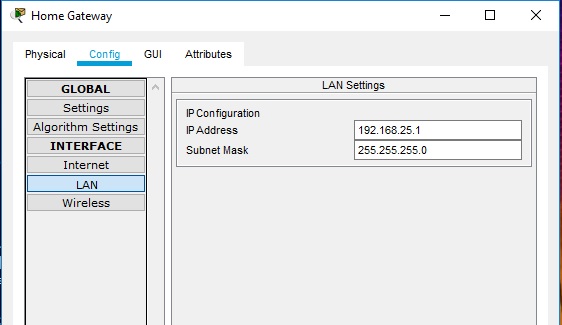


Рис. А.5. Мережеві налаштування ІоТ шлюзу для локальної мережі

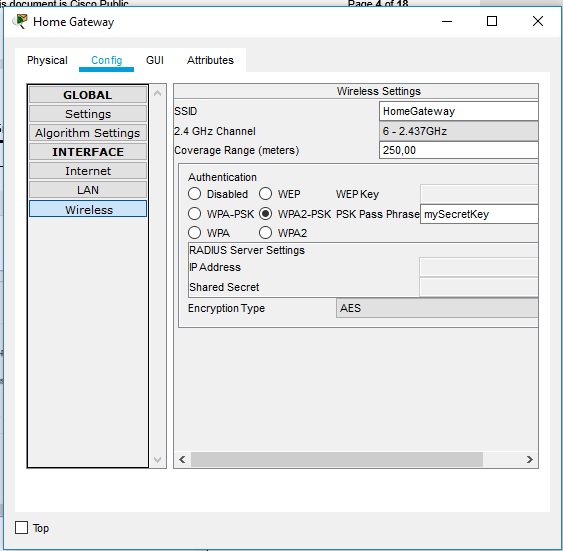


Рис.А.6. Мережеві налаштування ІоТ шлюзу для безпровідного інтерфейсу

Серед кінцевих пристроїв розумного будинку є **планшет,** що використовується у якості **пристрою управління ІоТ сервером**, за допомогою якого можна керувати підключеними ІоТ пристроями і здійснювати моніторинг їхнього стану через Web браузер. Натиснемо піктограму планшету.



Рис.А.7. Піктограма планшету

У вікні планшету виберемо вкладку Descktop (Робочий стіл), а на ньому натискаємо значок Web Browser.

У вікні веб-браузера в полі URL потрібно ввести IP-адресу інтерфейсу Home Gateway в локальній мережі і натиснути Go. На екрані веб-інтерфейсу Home Gateway, що з’явиться, пропонується ввести логін і пароль (за замовчанням і те і друге – слово admin), потім потрібно натиснути Submit (Відправити).

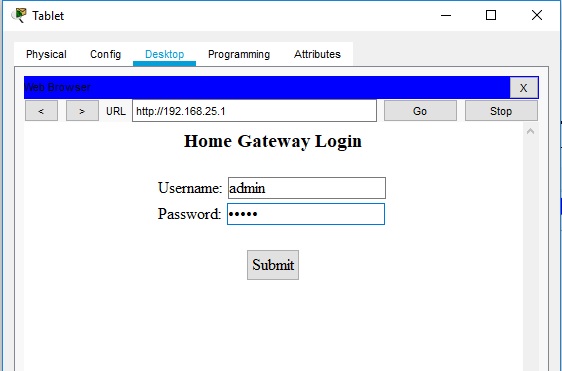


Рис.А.8. Вікно веб інтерфейсу ІоТ шлюзу

Після підключення до веб-інтерфейсу Home Gateway, з'явиться список всіх підключених IoT пристроїв.

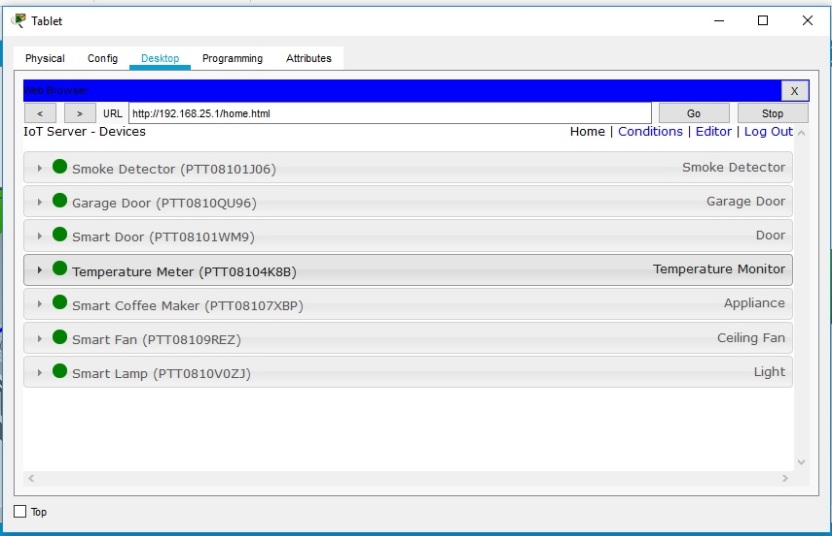


Рис. А.9. Вікно підключених пристроїв ІоТ шлюзу

При натисканні на пристрій в списку можна переглянути статус і налаштування цього пристрою. Вікно планшета можна не закривати, щоб слідкувати за зміною статусу пристроїв і керувати ними.



Рис. А.10. Перегляд статусу пристроїв на ІоТ шлюзі

**Дослідження кінцевих пристроїв IoT**

У нижньому меню програми Cisco Packet Tracer у вкладці End Devise вибираємо Home та інші праворуч від нього, де знаходяться різні елементи Smart IoT для розумного будинку, міста, підприємства.

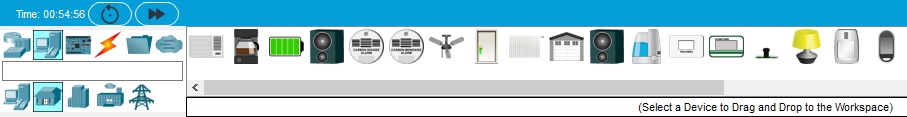


Рис. А.11. Кінцеві пристрої IoT в програмі Cisco Packet Tracer

При клацанні мишкою на піктограмі пристрою в робочій області відкривається вікно основного переліку його властивостей і способи роботи з ним.

При безпосередній активації пристрою, натисканням Alt + лівий клік миші на пристрій в робочій області, можна активувати його (побачити, як пристрій працює – зміну картинки).

При наведенні мишкою на пристрій в робочій області, відкривається вікно його мережевих налаштувань.

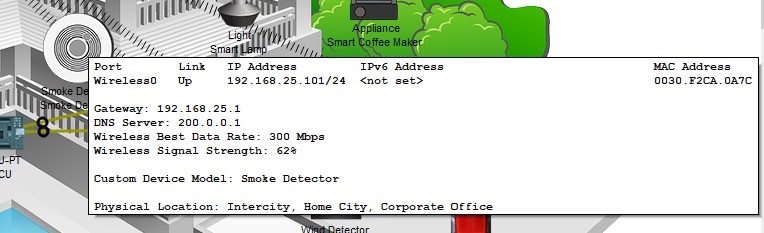
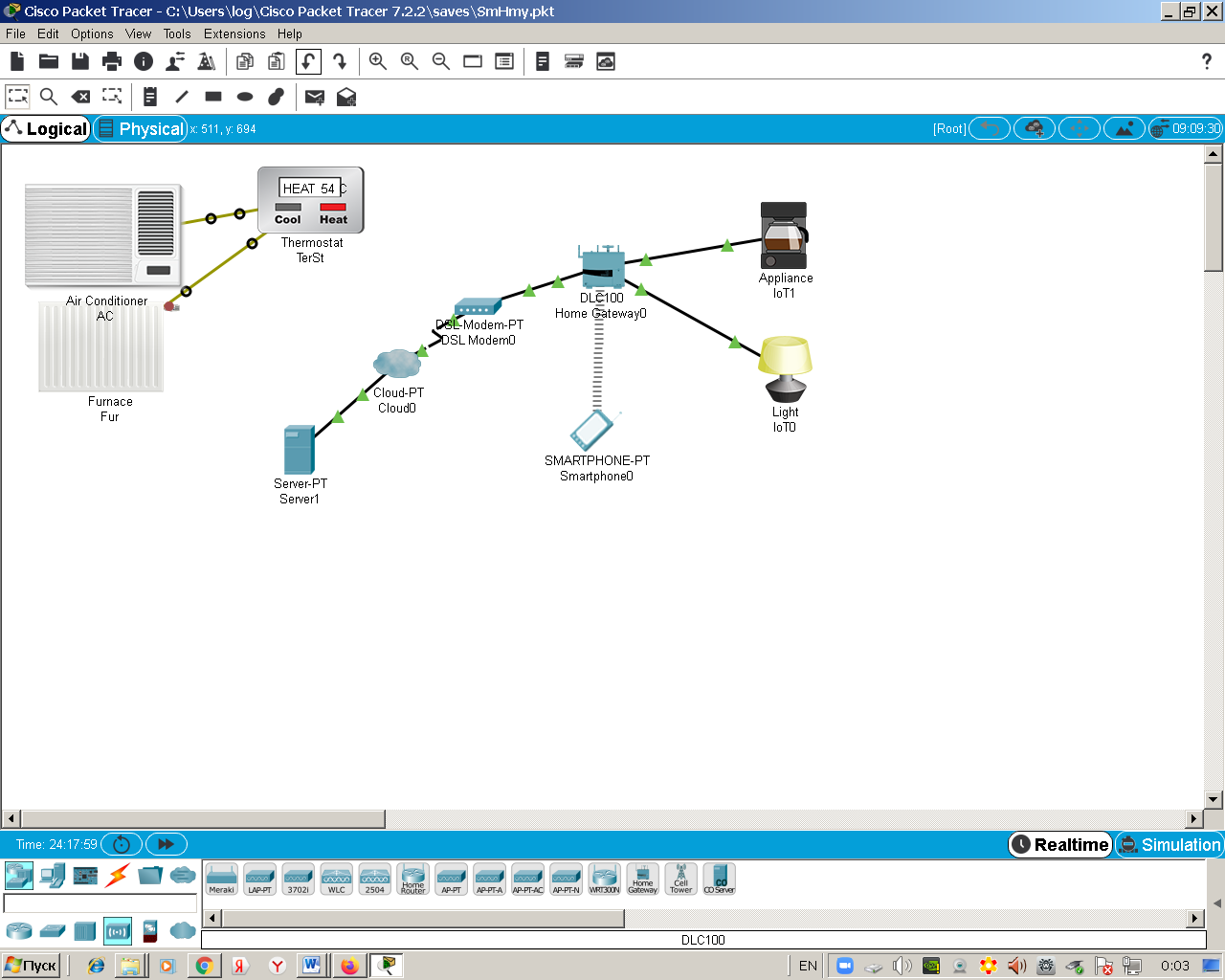


Рис. А.12. Вікно з основною мережевий інформацією про пристрій

# А.3 Побудова власної мережі

**Налаштування** **центрального шлюзу IoT**

Додайте в поле топології шлюз ІоТ, який знаходиться серед Network Devices -> Wireless Devices.



1

2

3

Рис. А.13. Вибір ІоТ шлюзу

Додайте в поле топології пристрій керування ІоТ сервером (планшет, смартфон або ноутбук), який виберіть серед End Devices -> End Devices (зліва від Home).

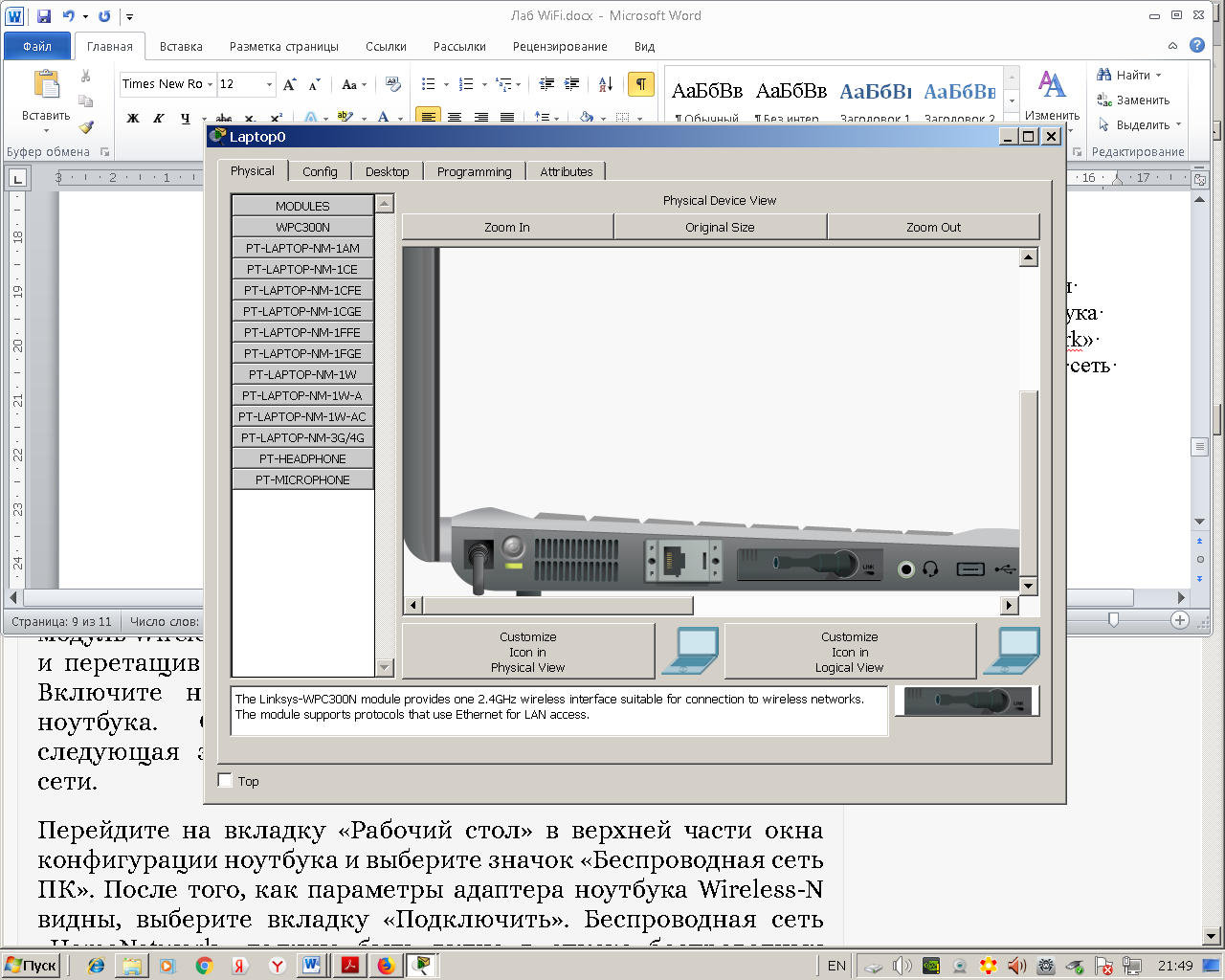
Налаштуйте інтерфейси шлюзу. Інтерфейс Internet – отримує налаштування динамічно від провайдера за DHCP. Для інтерфейсу LAN – задається ІР – адреса і маска в локальній мережі. Оскільки шлюз є складним пристроєм, в Packet Tracer використовується його спрощена модель, в якій всі дротові і безбровий інтерфейс шлюзу отримують одну загальну ІР – адресу і маску. Для інтерфейсу Wireless – налаштуйте WiFi інтерфейс Home Gateway, **змінивши** будь-які параметри за власним вибором порівняно з параграфом А.2.

Налаштуйте безпровідне підключення між Home Gateway і пристроєм керування (якщо використовується ноутбук, то його налаштування описано нижче). Для налаштування підключення до планшету або смартфону потрібно налаштувати його WiFi інтерфейс. В меню Config пристрою керування потрібно встановити IPv4 – конфігурацію на DHCP, щоб він отримав ІР – адресу від шлюзу, в якому за замовчанням налаштовано DHCP– сервер. Далі на лівій панелі потрібно вибрати інтерфейс Wireless0 і змінити ім’я мережі SSID, тип аутентифікації та PSC Pass Phrase на налаштування безпровідної мережі Home Gateway (у прикладі було – Home Gateway, WPA2-PSK та mySecretKey).

Тепер в локальну мережу можна додавати ІоТ пристрої і налаштовувати їх.

**Налаштування** **ноутбука**

Натисніть значок «Ноутбук» на робочому столі топології Packet Tracer, а у вікнах конфігурації ноутбука виберіть вкладку «Фізичні». На цій вкладці вам потрібно буде видалити модуль Ethernet адаптера і замінити його на модуль Wireless WPC300N. Для цього потрібно спочатку вимкнути ноутбук, натиснувши кнопку живлення на бічній панелі ноутбука (зелена лампочка згасне). Для видалення модуля Ethernet потрібно клацнути на модуль на бічній панелі ноутбука і перетягнути його в панель MODULES зліва від вікна ноутбука. Потім клацнути на модуль Wireless WPC300N і перетягнувши його в порожній порт модуля на стороні ноутбука. Після цього потрібно включити ноутбук, знову натиснувши кнопку живлення.



1, 4

3

2

Рис. А.14. Заміна мережевого адаптера в ноутбуці

Тепер необхідно підключити ноутбук до бездротової мережі. Для цього потрібно на вкладці Config вибрати Interface бездротової мережі Wireless0. Після того, як з’являться параметри адаптера ноутбука, необхідно задати ім'я SSID і параметри шифрування аналогічні налаштувань шлюзу, а також включити DHCP в положення ON.

Потім, якщо на зображенні топології мережі не з'явиться лінія бездротового зв'язку, потрібно зайти у Desktop на вкладку командного рядка і ***оновити настройки стека TCP/IP*** ноутбука через DHCP командою ipconfig.

**Нагадаємо**, що оновлення IP конфігурації вузла необхідно в тому випадку, якщо вузол вже отримував настройки від DHCP сервера, а тепер вони змінилися того, що сервер DHCP був переналаштований.

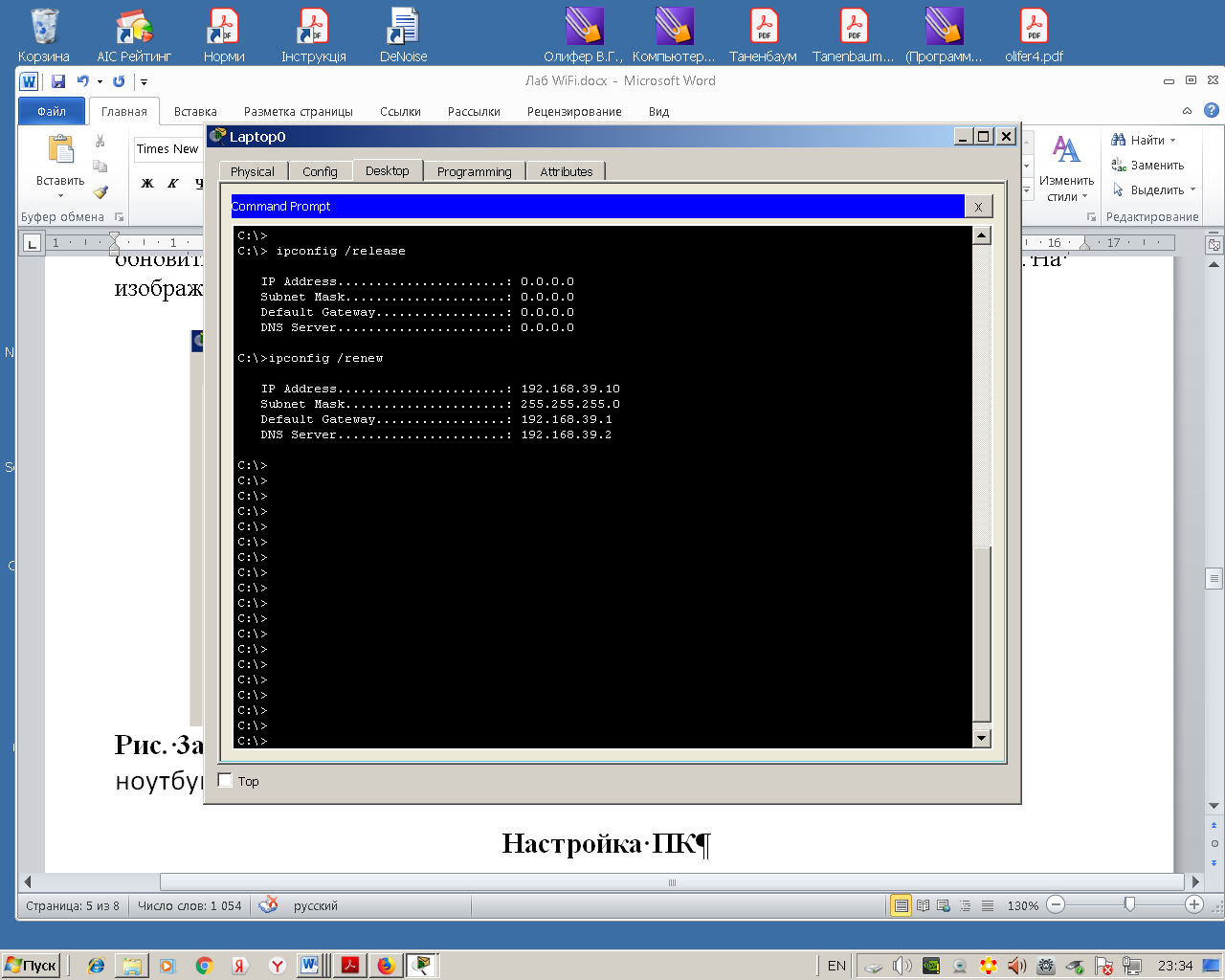


Рис.А.15. Видалення старої конфігурації стека TCP/IP для адаптера пристрою і отримання нової конфігурації від DHCP сервера

**Організація підключення до глобальної мережі**

Підключення до глобальної мережі потрібно проводити у такій послідовності.

1. Додайте до робочої області програми хмарний server-РТ (з End Devices) та мережу доступу Сloud-PT і відповідне DCE – модем (з Network Devices -> WAN emulation).
2. Укомплектуйте хмарний комутаційній пристрій в мережі провайдера (хмара).
3. Підключить шлюз до модему, а модем і сервер до хмари.
4. Налаштуйте комунікацію через хмарний комутаційній пристрій.

**Комплектація хмарного комутаційного пристрою**

У хмарного пристрою повинні бути встановлені необхідні інтерфейсні модулі для підключення сервера і модема. Для перевірки потрібно натиснути значок «Інтернет-хмара» в робочій області програми і перейти на вкладку «Фізичні». Наводячи мишкою на кожний модуль можна прочитати в нижньому вікні його призначення. Якщо необхідні модулі відсутні, потрібно вимкнути комутуючий пристрій, натиснувши на кнопку живлення, і перетягнути кожен модуль на порожній порт на пристрої, а потім знову ввімкніть пристрій (дивись «Налаштування ноутбука»).

Для хмарного пристрою потрібно буде встановити два модулі, якщо вони ще не встановлені: для технології Ethernet та для однієї з глобальних технологій (за варіантом).

Модуль PT-CLOUD-NM-1CFE, який забезпечує один інтерфейс Fast-Ethernet для використання з мідними носіями і пропонує автоматичне визначення 10BaseT/100BaseTX.

Модуль PT-CLOUD-NM-1CX має єдиний коаксіальній роз’їм, який використовується для підключення послуги кабельного модему.

Модуль PT-MODEM-NM-1CE має єдиний порт для підключення технологій на звитій парі з цифровими методами кодування (Ethernet, 6 PRI-з'єднань для сукупності ліній ISDN, або 24 синхронних / асинхронних портів).

**Підключення пристроїв**

В якості інтерфейсу DТE-DCE шлюзу з модемом використаємо технологію Ethernet. Для підключення потрібний мідний прямий кабель (звита пара не перехрещена). Кабель вибирається з меню в нижньому лівому куті вікна програми (значок блискавки, чорна лінія) і прикріпляється до порту 1 модему та WAN інтерфейсу шлюзу (порт Internet).

Для підключення модему до хмари буде потрібний або телефонний або коаксіальний кабель в залежності від технології. Кабель прикріплюється до порту 0 модему і відповідного інтерфейсу хмари (Modem4 – для DSL чи Coaxial – для CaTV).

Сервер підключається до хмари за технологією FastEthernet або Ethernet за допомогою мідного прямого кабелю.

**Налаштування хмарного комутаційного пристрою**

Коли пристрої до портів хмарного комутаційного пристрою підключені, потрібно задати, між якими з портів повинна відбуватися передача даних. В прикладі сервер було підключено до порту FastEthernet8, а кабельний модем – до порту Coaxial7.

Потрібно натиснути на зображення хмари, перейти на вкладку Конфігурація, вибрати натисканням серед INTERFACE на лівій панелі той, до якого було підключено сервер (FastEthernet8 – у прикладі). У вікні, що відкриється, потрібно вибрати технологію доступу шлюзу (Cable – у прикладі).

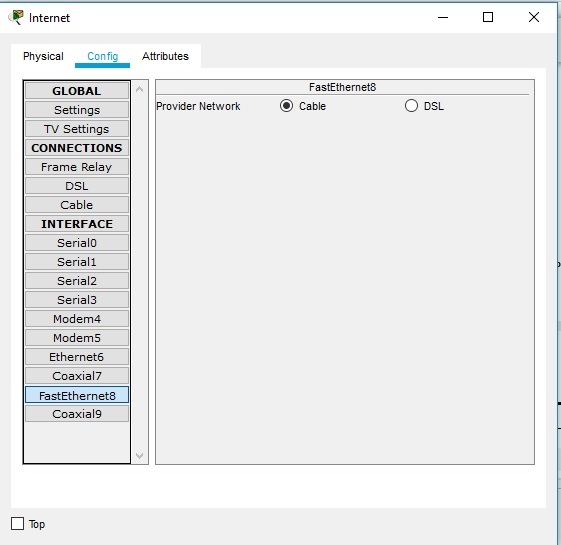


Рис. А.16. Вибір технології доступу до мережі провайдера

Тепер потрібно з переліку «CONNECTIONS» у лівій панелі вибрати натисканням технологію доступу шлюзу (Cable – у прикладі), а потім у вікні, що відкриється, вибрати порти, між якими потрібно встановити обмін даними (у прикладі з першого списку потрібно вибрати порт Coaxial7, а в другому – FastEthernet8). Потім потрібно натиснути кнопку Add, щоб додати цей шлях до таблиці хмарного комутаційного пристрою.

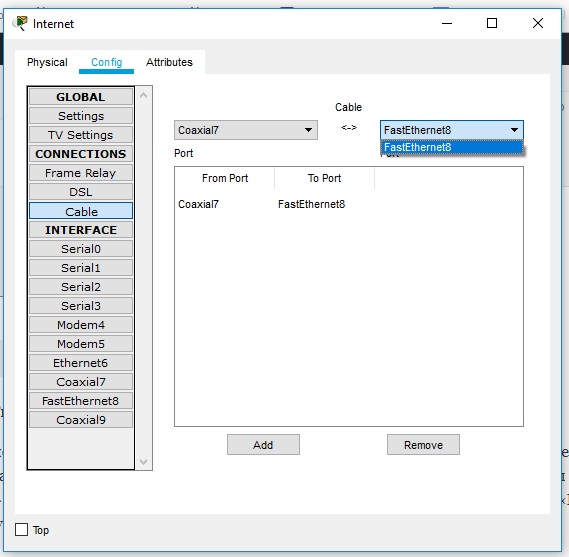


Рис. А.17. Налаштування комутації між потрібними портами

**Налаштування сервера**

У прикладі параметри стеку TCP/IP сервера налаштовуються в провайдерській мережі 208.67.220.0/24. Також на цьому сервері налаштована служба DNS- сервера і DHCP- сервера .

1. Налаштування стеку TCP/IP.

Зайдіть на вкладку Config, натисніть Settings в лівій панелі та налаштуйте загальні параметри сервера наступним чином:

Призначте серверу **ім’я**.com, де ім’я – перші літери свого прізвища (у прикладі це Cisco.com).

Задайте статичні налаштування стеку TCP/IP (загальні).

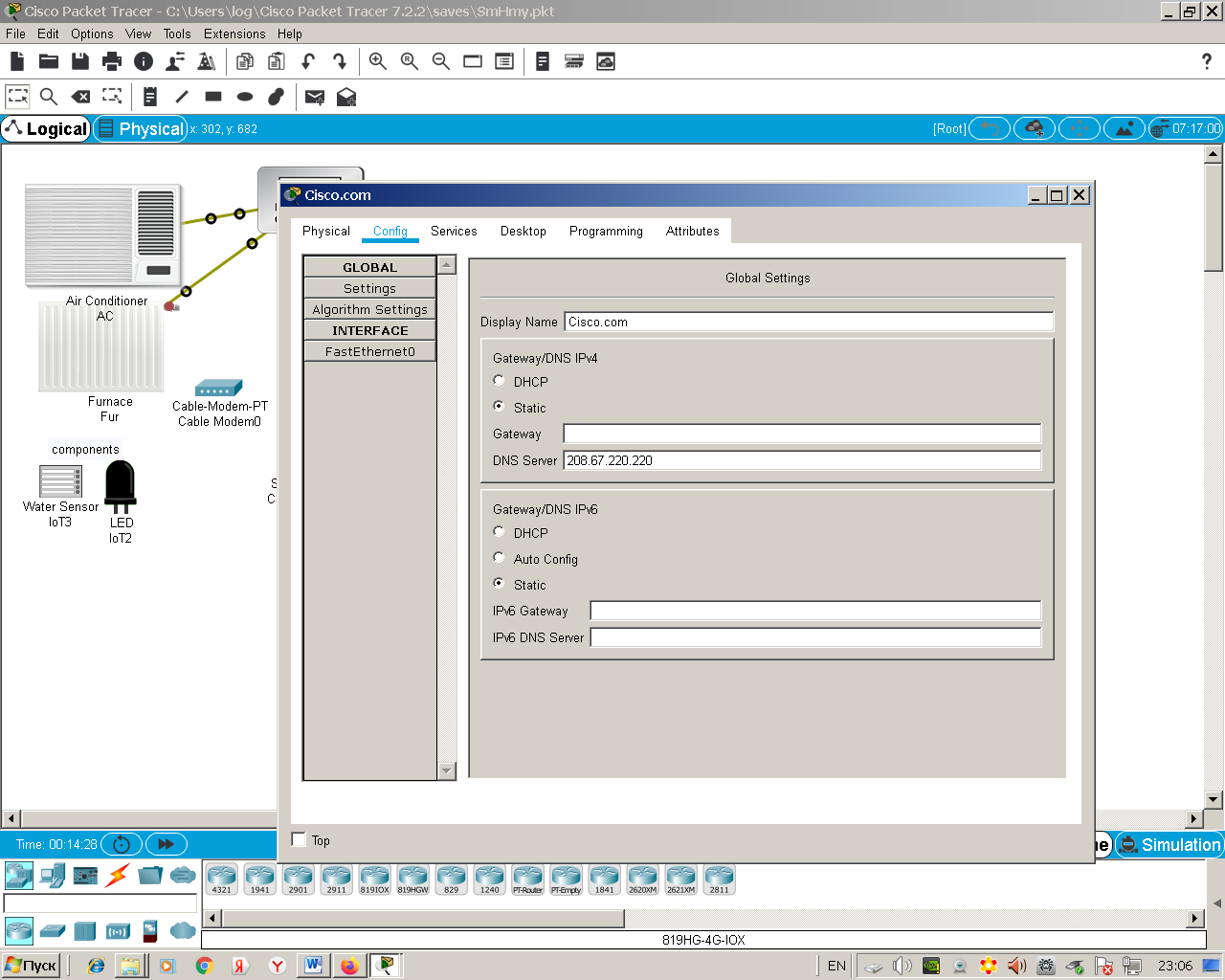


Рис. А.18. Загальні налаштування стеку TCP/IP сервера

Тепер налаштуйте параметри інтерфейсу сервера. Для цього натисніть INTERFACE, потім натисканням виберіть потрібний інтерфейс в лівій панелі (тут він один – FastEthernet0) і призначте статичну ІР- адресу і маску цьому інтерфейсу.



Рис. А.19. Налаштування стеку TCP/IP для інтерфейсу сервера

1. Налаштування хмарного сервера як сервера DHCP

Натисніть значок сервера, виберіть вкладку Servises, а в ній – службу DHCP. У вікні конфігурації DHCP налаштуйте службу для пристроїв провайдерської мережі :

• Натисніть «On», щоб увімкнути службу DCHP.

• Задайте ім'я нового пулу (у прикладі DHCPpool) або відкоригуйте параметри даного пулу.

• Задайте ІР – адреси шлюзу за замовчуванням, DNS-сервера, стартову адресу для інтерфейсів пристроїв мережі (перша адреса буде призначатися як стартова+1), маску мережі і максимальна кількість користувацьких інтерфейсів.

• Натисніть Add, щоб додати пул. При зміні параметрів існуючого пулу натисніть Save.

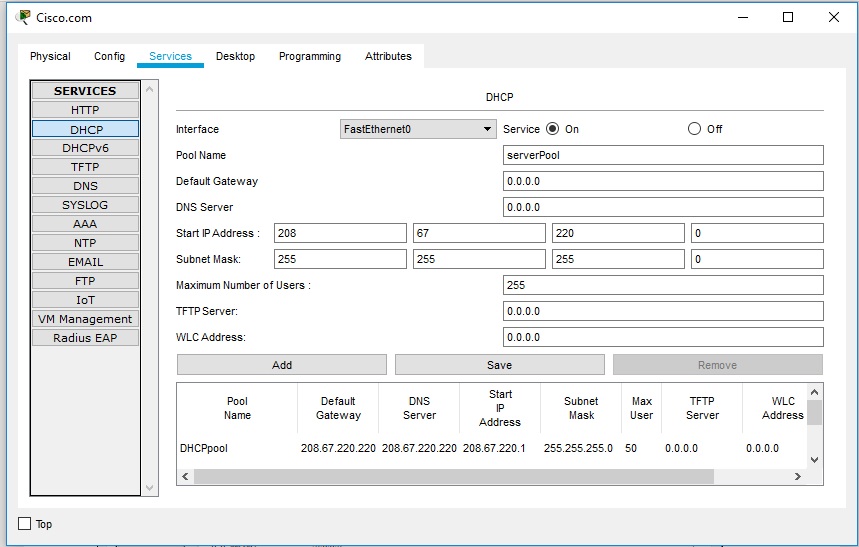


Рис. А.20. Налаштування DHCP сервера. Параметри нового доданого пулу DHCPpool показано в нижньому рядку вікна

1. Налаштування хмарного сервера як DNS-сервера для надання по імені домену адреси IPv4

На вкладці «Servises» виберіть DNS службу з перерахованих на лівій панелі і налаштуйте її. В даному прикладі було додано одну ресурсну запис типу А для сервера Cisco.com, щоб до нього можна було звертатися по доменному імені. Ресурсна запис – одиниця зберігання і передачі інформації в DNS. Існує багато типів ресурсних записів. Запис типу A (address record) пов'язує ім'я хосту з адресою IPv4. Запит A-запису на задане доменне ім'я повертає його IPv4-адресу.

• Натисніть «On», щоб увімкнути службу DNS.

• Налаштуйте службу DNS. Для чого виберіть тип запису –А, задайте ім'я хмарного сервера і його IP-адресу.

• Натисніть «Add, щоб додати запис до налаштувань служби DNS.

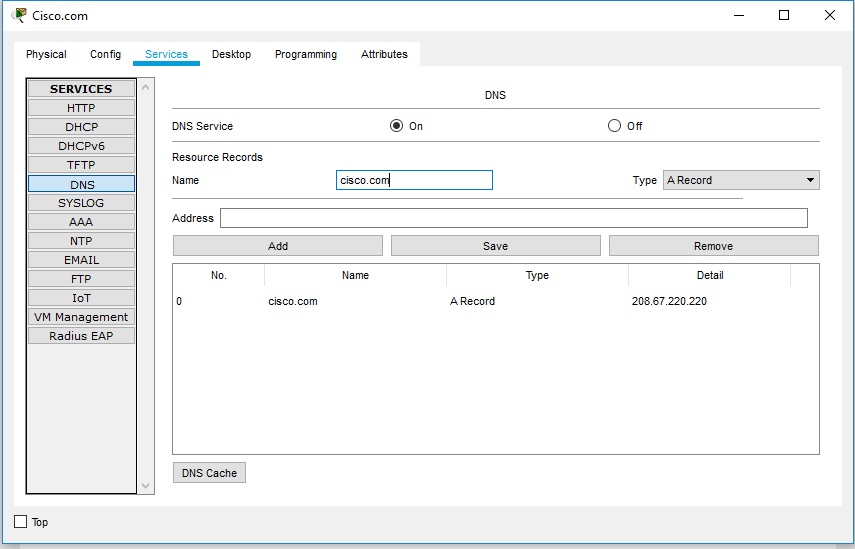


Рис. А.21. Налаштування DNS сервера. Параметри доданого запису показано в нижньому рядку вікна

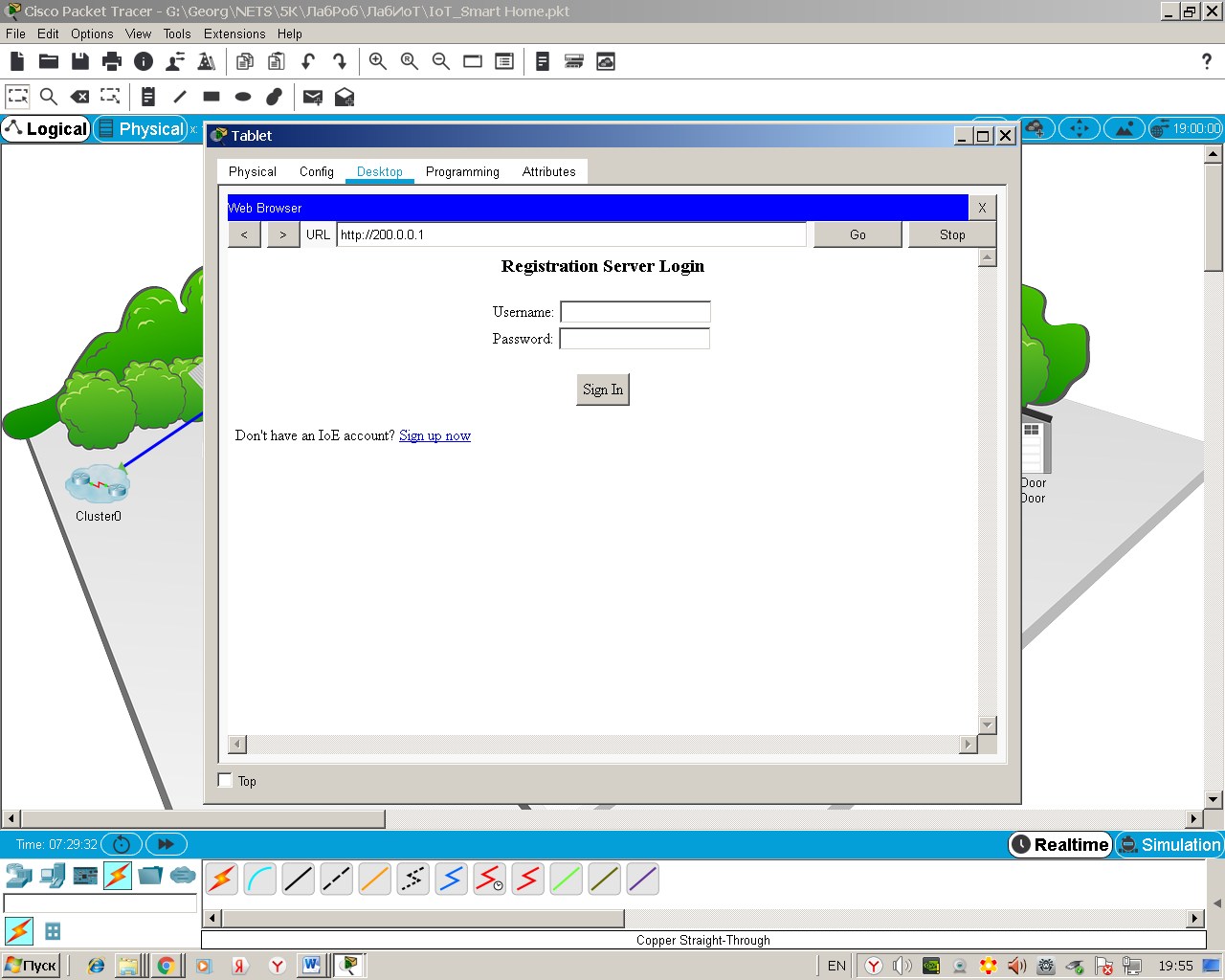
1. Налаштування хмарного сервера як сервера ІоТ

Натисніть значок сервера, виберіть вкладку Servises, а в ній – службу ІоТ. У вікні конфігурації ІоТ:

• Натисніть «On», щоб увімкнути службу.

• Увійдіть з пристрою керування ІоТ сервером (планшет у прикладі) через Web Browser до веб-інтерфейсу віддаленого ІоТ серверу, ввівши його IP адресу. На екрані веб-інтерфейсу, що з’явиться, потрібно зареєструватися. Для цього потрібно натиснути Sing up now (1 на рис. А.20).

• В новому вікні потрібно ввести логін і пароль і натиснути Sing in (2 на рис. А.20).



1

2

Рис.А.22. Вікно веб інтерфейсу ІоТ шлюзу

**Увага!** Для проведення реєстрації потрібно, щоб мережеве з’єднання між пристроєм керування і віддаленим ІоТ сервером було налаштоване правильно. Тому реєстрацію на ІоТ сервері з пристрою керування краще провести після перевірки мережевих налаштувань.

**Перевірка мережевих налаштувань**

1. Переконайтеся, що пристрій управління ІоТ сервером отримує інформацію про конфігурацію IPv4 від DHCP служби шлюзу (дивись оновлення настройки стека TCP/IP ноутбука на рис. А13). Для цього на пристрої управління зайдіть у вкладку Desktop, а в ній виберіть вкладку командного рядка RUN.
2. Перевірте підключення до хмарного сервера з пристрою управління ІоТ сервером. Для цього на пристрої управління зайдіть у вкладку Desktop, а в ній виберіть вкладку командного рядка запустіть команду ping імя сервера (у прикладі ping Cisco.com). Оскільки Packet Tracer імітує передачу даних у глобальній мережі, для повернення відповіді ping може знадобитися кілька секунд.

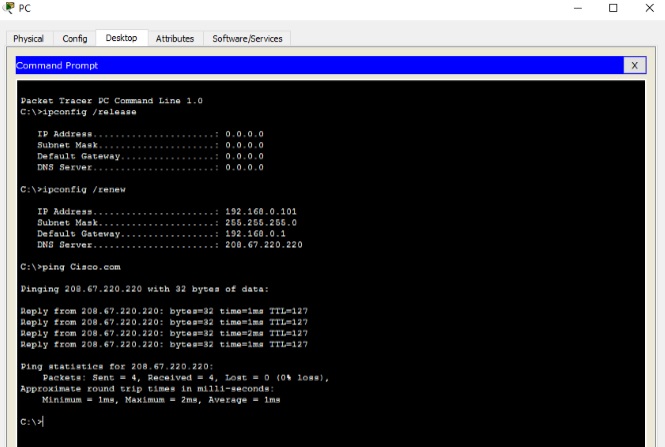


Рис. А.23. Перевірка підключення до хмарного сервера пристрою управління ІоТ сервером в локальній мережі

У разі виникнення проблем, потрібно спочатку перевірити правильність налаштування DNS служби на сервері, командою ping IP- адреса сервера. Якщо команда проходить, значить помилка в налаштуванні DNS служби. Якщо команда не проходить, потрібно шукати помилки в налаштуваннях стеку ТСР/ІР зовнішнього інтерфейсу шлюзу (зверніть увагу на значення IP- адреси Gateway) або провайдерської мережі (хмари і сервера).

Для оновлення настройки стека TCP/IP для зовнішнього інтерфейсу шлюзу, зайдіть на ньому на вкладку Config і виберіть інтерфейс Internet, через пару секунд отримаєте оновлені налаштування.

# А.4 Додавання провідних пристроїв в інтелектуальну домашню мережу з використанням технології Ethernet

ІоТ пристрої і окремі компоненти знаходяться у End Devise і Сomponents. Розглянемо підключення пристроїв на прикладах.

**Приєднання газонного розпилювача до домашнього шлюзу**

1) З поля End Devise ->Home виберемо значок Lawn Sprinkler (Газонний розприскувач), а потім клацнімо в робочій області, де хочемо його розмістити.

2) З цого ж поля виберемо натисканням значок підключення (виглядає як блискавка), потім виберемо мідний прямий кабель (Copper Straight Through). Потім натискаємо піктограму розбризкувача і підключаємо один кінець кабелю до інтерфейсу FastEthernet0 Sprinkler. Клацаємо на значку Home Gateway і підключаємо інший кінець кабелю до одного з його Ethernet інтерфейсів.

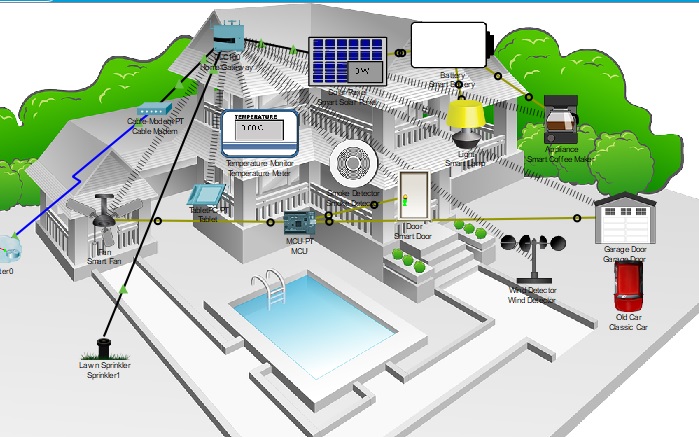


Рис. А.24. Вікно робочої області Cisco Packet Tracer з підключеними IoT пристроями

**Налаштування розпилювача для мережевого підключення**

1. Відкриваємо вікно пристрою натисканням на його піктограмі в робочій області.
2. Вкладка Specification (Специфікація) надає інформацію про пристрій і способи його активації.

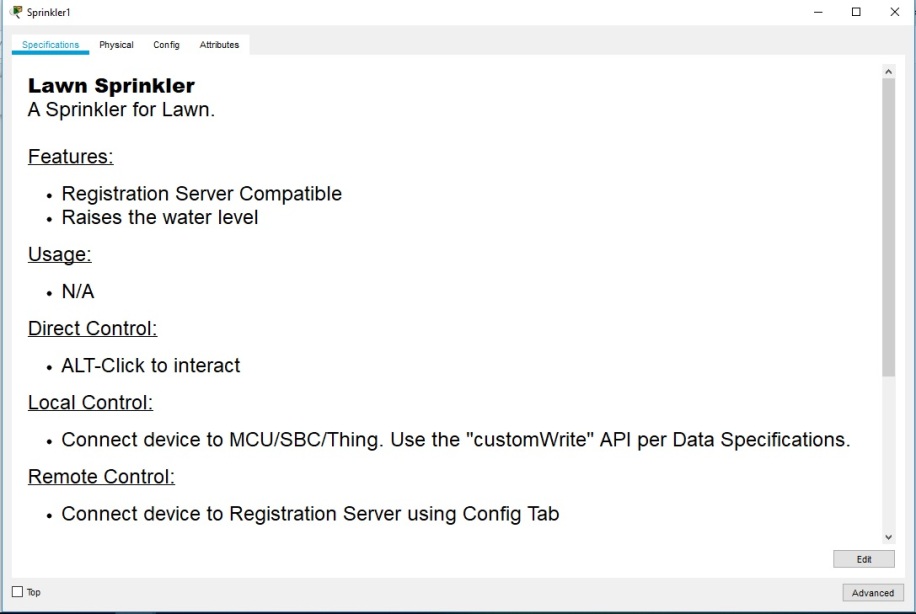


Рис. А.25. Вікно властивостей IoT пристрою

2). Перейдемо на вкладку конфігурації пристрою і проведемо наступні налаштування:

* Надамо ім’я пристрою – Sprinkler\_АВС, де АВС – перші літери свого прізвища.
* Вибираємо зліва інтерфейс FastEthernet0 і встановлюємо IPv4 - конфігурацію на DHCP, щоб пристрій отримував всі необхідні налаштування (власну IP-адресу, адресу DNS серверу і маршрутизатора за замовчанням - Gateway) від DHCP серверу.
* Визначаємо сервер IoT для керування пристроєм: домашній шлюз (А.26) або віддалений сервер (А.27).
* Закриваємо вікно розпилювача.

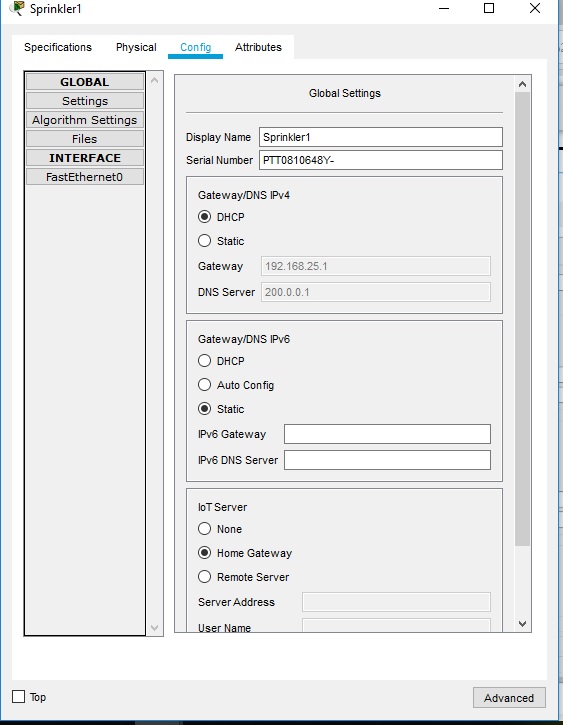


Рис. А.26. Вікно конфігурації інтерфейсів IoT пристрою. ІоТ сервер розташовано на шлюзі локальної мережі.

У випадку віддаленого сервера потрібно ще вказати його IP адресу та логін і пароль, які були задані при реєстрації на сервері. Потім внизу вікна натиснути Connect (і за потреби ще раз refresh).

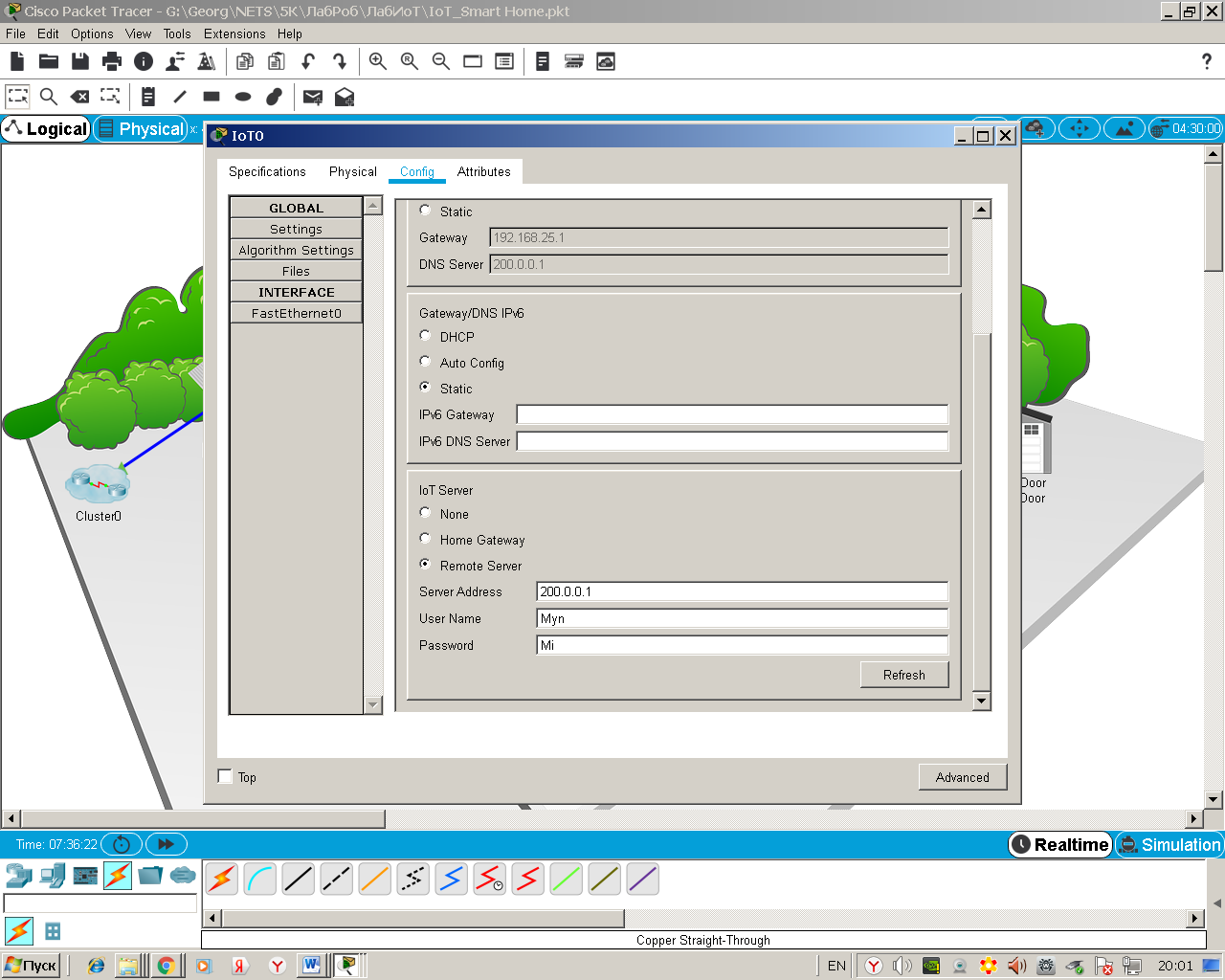


Рис. А.27. Вікно конфігурації інтерфейсів IoT пристрою. ІоТ сервер розташовано на сервері провайдера.

**Перевірка налаштування розпилювача**

1. Увійдемо до ІоТ сервера (Home Gateway або віддалений) з пристрою керування (наприклад, планшету).
2. Впевнимося, що пристрій, наприклад, на ім’я Sprinkler1, знаходиться у мережі. Його ім’я має з’явитися у списку IoT Server – Devices.

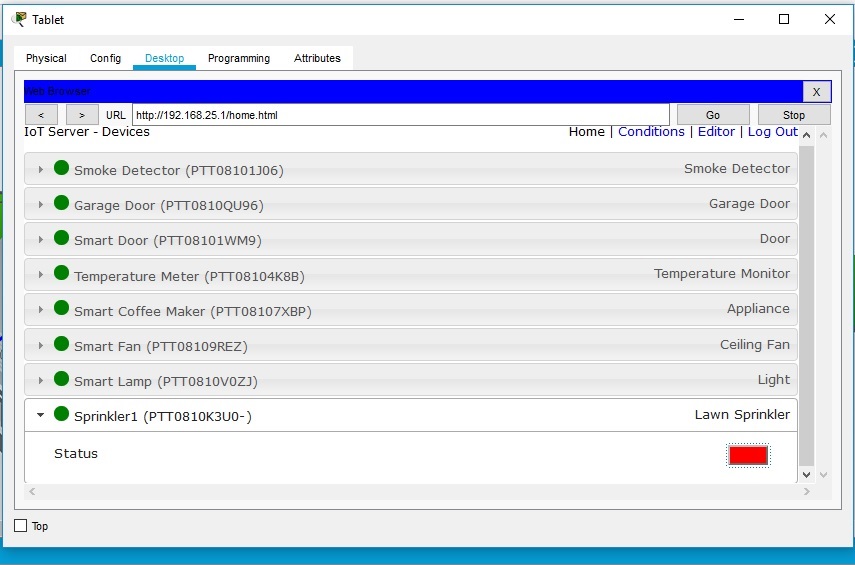


Рис. А.28. Перегляд статусу пристроїв на ІоТ шлюзі

1. Змінюємо статус розпилювача на увімкнено, натискаючи на червону кнопку, яка повинна стати зеленою.



Зображення розпилювача на робочому полі повинно змінитися.



Рис. А.29. Вигляд ввімкнутого розбризкувача

1. Вимикаємо пристрій і закриваємо його вікно.

# А.5 Додавання бездротових пристроїв в домашню мережу з використанням технології WiFi

1) З поля End Devise ->Home виберемо пристрій Wind Detector (детектор вітру) і розташовуємо його в робочій області.



Рис. А.30. Піктограма детектору вітру

2). Додати бездротовий модуль в пристрій.

Натиснувши на значок Wind Detector в робочій області відкриємо вікно налаштувань пристрою IoT. У правому нижньому кутку вікна пристрою IoT натискаємо кнопку «Додатково» і переходимо на вкладку IO Config (конфігурація введення-виведення).

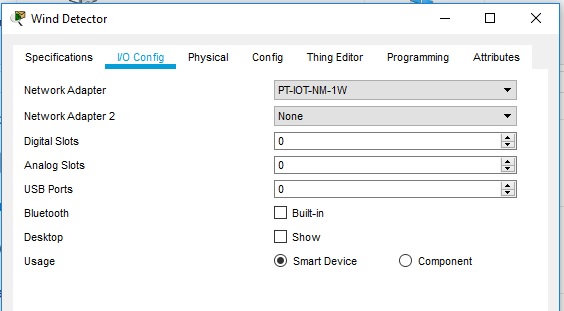


Рис. А.31. Заміна мережевого адаптера на ІоТ пристрої

Змінюємо Network Adapter на бездротовий Wi-FI, вибравши у випадаючому меню адаптер PT-IOT-NM-1W.

3) Налаштування бездротового з’єднання детектор вітру.

* перейдемо на вкладку Config. Аналогічно налаштуванню провідного з’єднання надамо ім’я пристрою – Wind\_Detector\_АВС, встановлюємо сервер IoT для пристрою на Home Gateway, а IPv4 - конфігурацію на DHCP.
* - на лівій панелі виберемо інтерфейс Wireless0 і змінимо тип аутентифікації та PSC Pass Phrase на налаштування бездротової мережі Home Gateway (у прикладі, WPA2-PSK та mySecretKey).

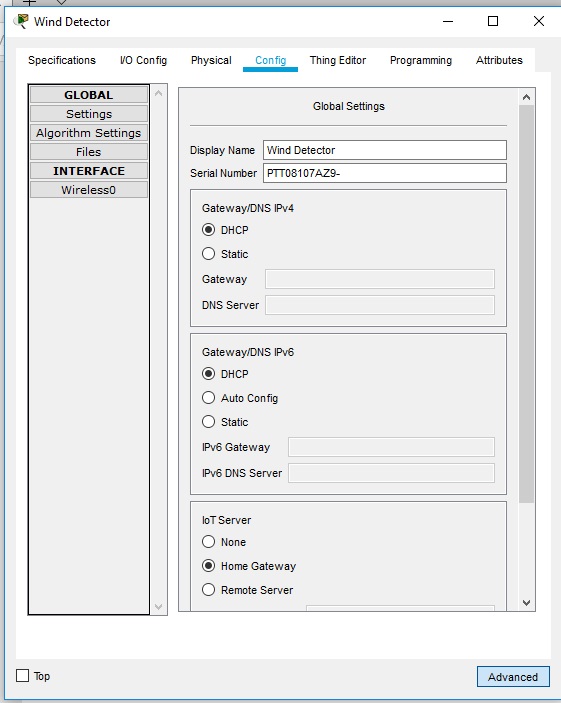


Рис. А.32. Вікно конфігурації інтерфейсів IoT пристрою

* між детектором вітру і домашнім шлюзом повинно бути встановлено бездротове з'єднання. Закриваємо вікно.

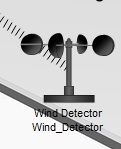


Рис.А.33. Зображення наявності бездротового з'єднання між детектором вітру і домашнім шлюзом.

**Перевірка налаштування детектору вітру**

1. Увійдемо в Home Gateway з планшету.
2. Впевнимося, що пристрій Wind Detector знаходиться у мережі. Його ім’я має з’явитися у списку IoT Server — Devices.

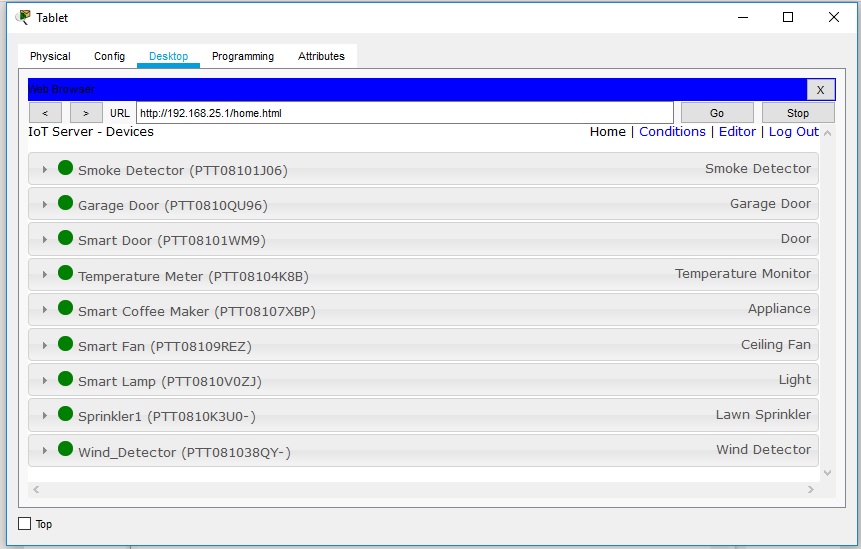


Рис. А.34. Вікно статусу пристроїв на ІоТ шлюзі

1. Закриваємо вікно пристрою.

**Узгодження роботи пристроїв**

Узгодження роботи 2-х пристроїв можна розглянути на прикладі датчика руху і веб-камери. Додамо до розумного будинку датчик руху та web-камеру і зробимо так, щоб веб-камера включалася при спрацьовуванні датчика руху і вимикалася, коли рух припинявся.

1. Розмістимо датчик руху на території розумного дому, а web-камеру напроти нього.
2. Підключаємо два нових пристрої Motion\_Detector і webcam до Home Gateway через WI-FI аналогічно іншим бездротовим пристроям.
3. Тепер необхідно створити правила включення і виключення для веб-камери. Взагалі, правил може бути багато, як і пристроїв, які вони зв’язують. Для цього зайдемо на головний шлюз через web-браузер і виберемо вкладку Conditions, а в ній створимо два правила на вмикання та на вимикання. Перше правило Pr1: **If** Motion\_Detector on **is** true **Then set** webcam on **is** true та друге правило Pr1.1: **If** Motion\_Detector on **is** false **Then set** webcam on **is** false

Щоб це зробити, треба натиснути Add;

На вкладці, що відкриється, потрібно

* ввести ім’я правила;
* з меню **if** вибрати по черзі:назву пристрою, праворуч – on, праворуч - true/false;
* натиснути OK.

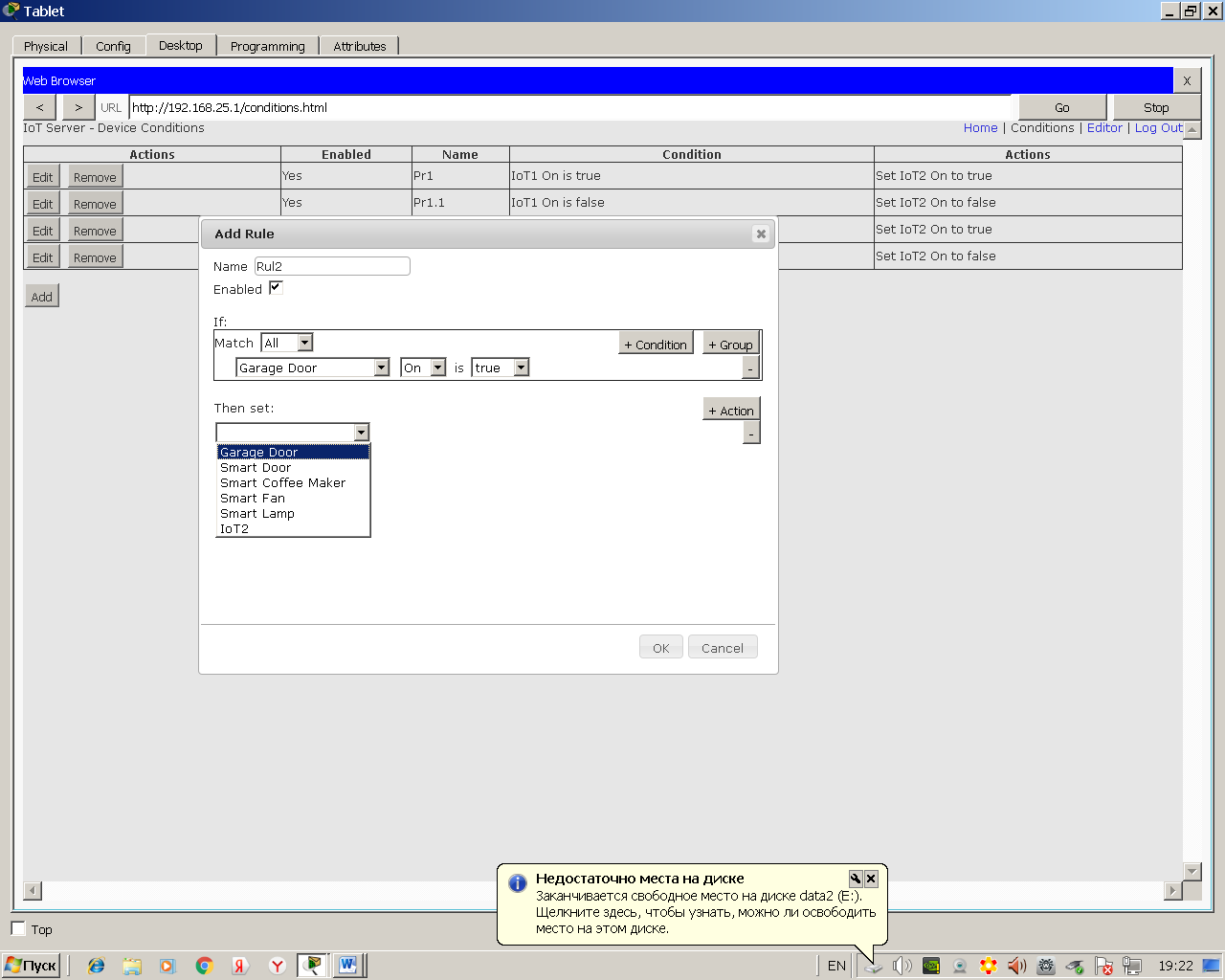


Рис. А.35. Додавання правил в логіку роботи пристроїв

1. Перевіримо тепер як спрацьовує веб-камера при фіксуванні руху. Для цього заходимо через планшет на домашній шлюз, розгортаємо статус Motion\_Detector та webcam, встановлюємо Motion\_Detector у статус ON і слідкуємо за статусом webcam. Аналогічно, можна відкрити двері безпосередньо (Alt + лівий клік миші) і також спостерігати за статусом webcam.

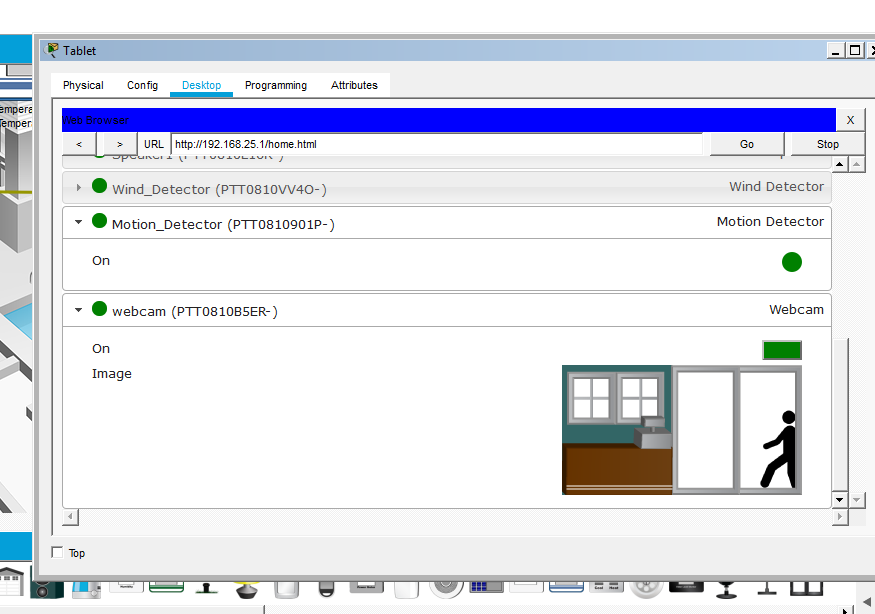
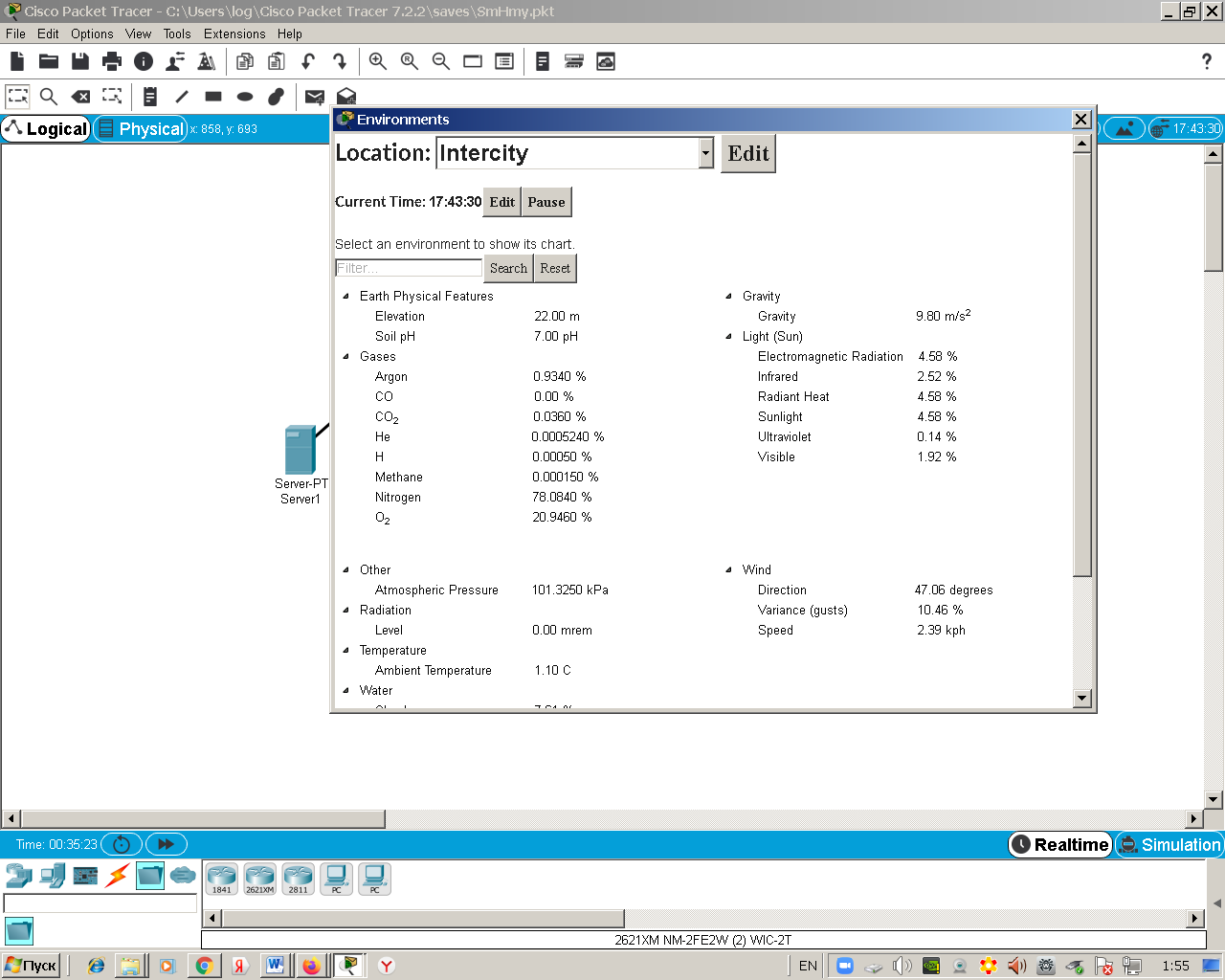


Рис. А.36. Включення веб-камери при спрацьовуванні датчика руху.

***Особливості налаштування деяких пристроїв***

1. Деякі пристрої включаються і виключаються залежно від параметрів навколишнього середовища. **Налаштування температури навколишнього середовища**.

На верхній панелі головного вікна вибрати крайню справа кнопку Environment (1). У вікні, що відкрилося, натиснуть кнопки меню в послідовності, показаній на рис. А.30. Наприклад, натискання (3) дозволить побачити зміну температури під час моделювання, а натискання Edit (2), відкриває графік зміни температури середовища протягом доби для редагування.



1

2

4

3

Рис. А.37. Вікно налаштувань навколишнього середовища

У вікні, що відкрилося, можна редагувати швидкість моделювання. Наприклад, за 1секунда моделювання – 30 хвилин змодельованого часу.

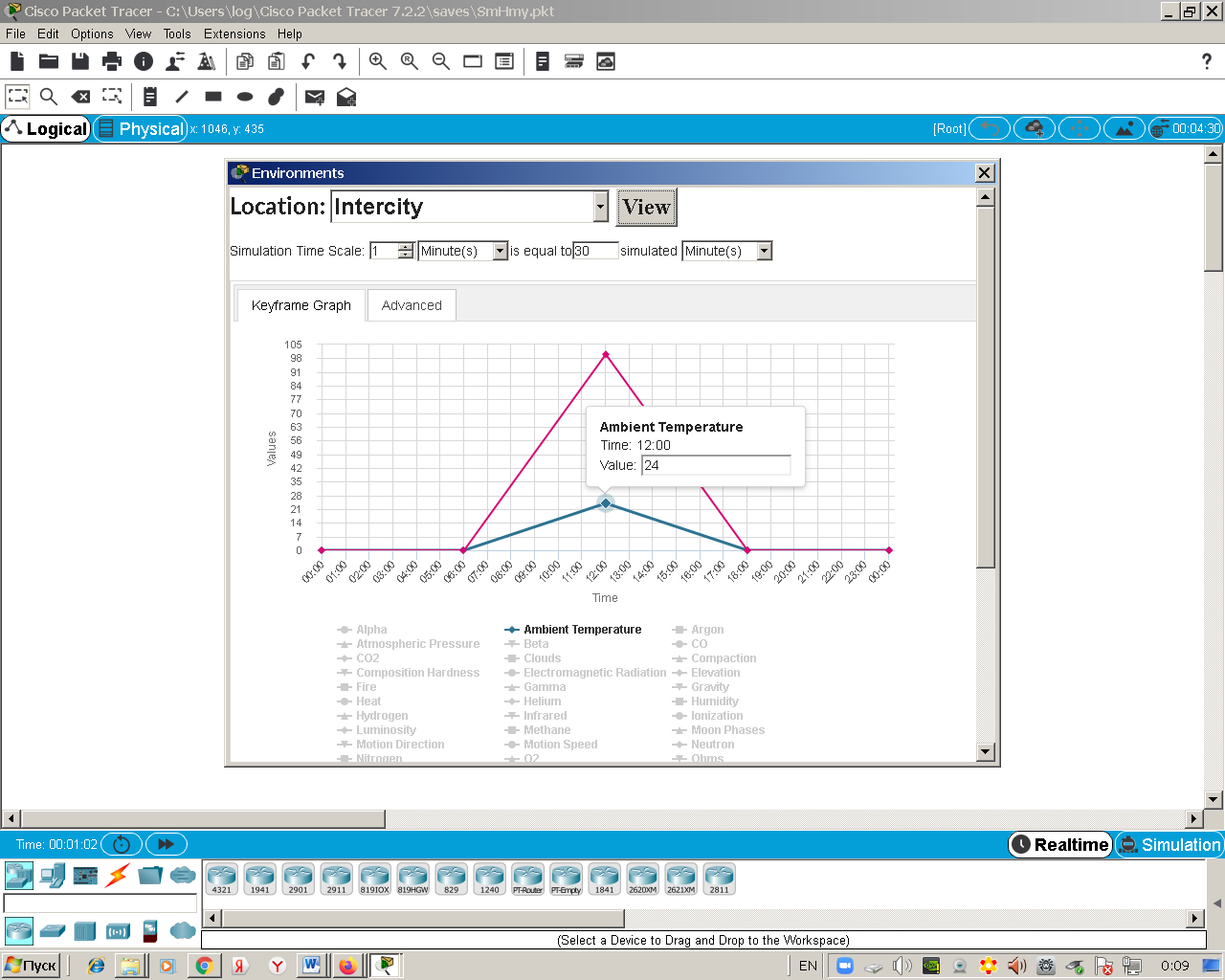


Рис.А.38.Графік зміни добової температури за замовчанням

Переміщуючи курсором миші точки синього графіку *по сітці вгору*, вирівнюємо температуру відповідно до типової літньої. Наприклад, як на наступному рисунку. Повертаємось в режим спостереження, натискаючи View (2), закриваємо вікно. Далі, можемо спостерігати за графіком зміни температури і освітлення, або закриваємо вікно Environment і спостерігаємо за роботою ІоТ пристрою, який реагує на зміну параметрів навколішнього середовища.

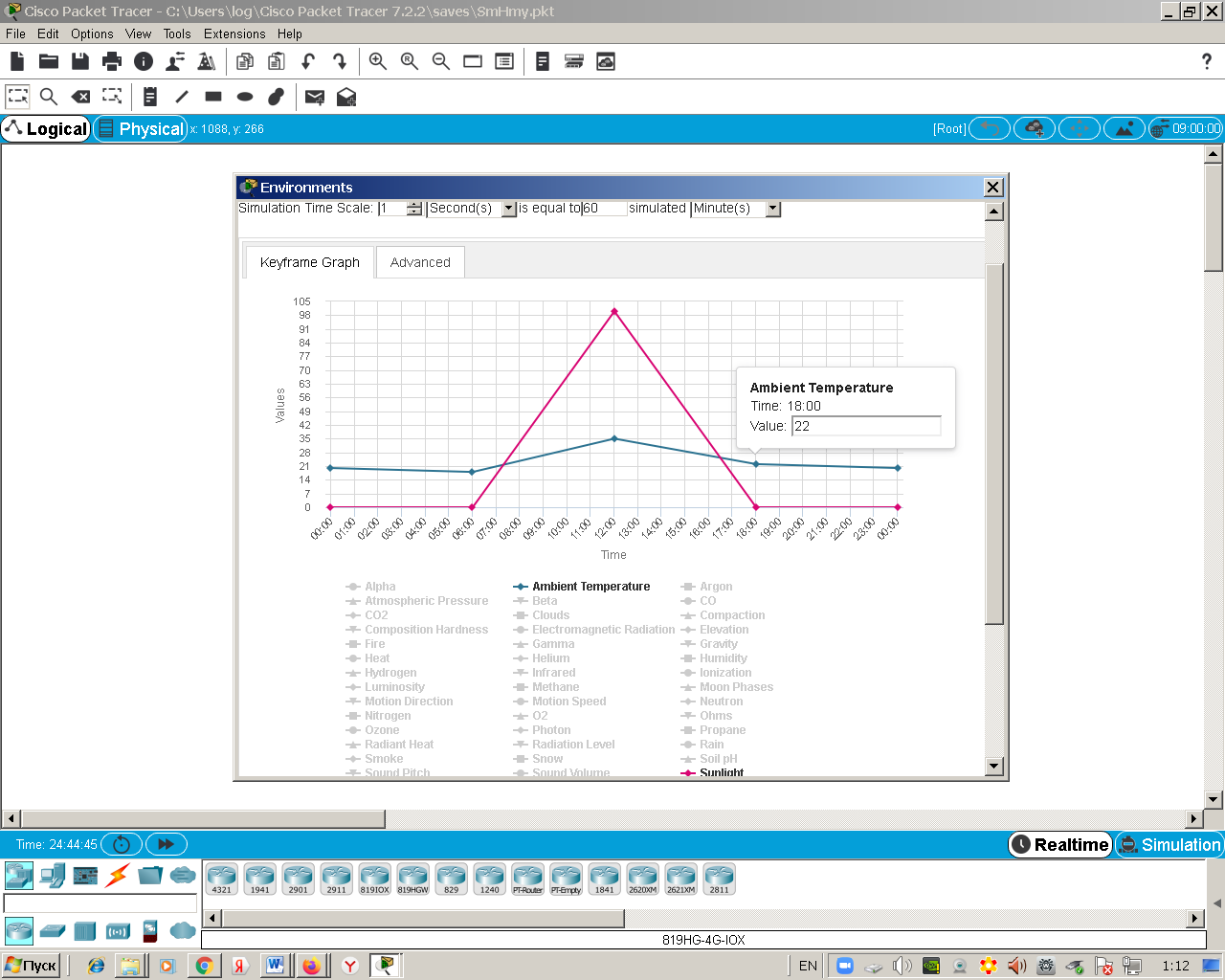


Рис.А.39. Редагування графіка зміни добової температури середовища

На рисунку червоним показано графік зростання і зменшення сонячного світла протягом доби. Найбільша його частина припадає на дванадцяту годину дня. Наприклад, для забезпечення безперебійного живлення «розумного будинку» використано ***сонячну панель та акумулятор***. Для цього пристрої з’єднані між собою спеціальним кабелем IoT (аналоговий сигнал) і кожен з них підключено окремо до шлюзу. Швидкість заряду акумулятора можна спостерігати на табло сонячної панелі.

***Термостат*** – датчик температури у приміщенні підключено до шлюзу. Налаштований на автоматичний режим, він намагатиметься встановити значення 20°C (за замовчанням). Вмикає охолодження, якщо температура перевищить 20°С, або нагрівання, коли температура опуститься нижче 19°С. Це робиться шляхом надсилання сигналу через D1 і D2. D1 використовується для нагрівання, а D2 – для охолодження. Потрібно підключити обігрівач (піч) до D1, а АС (кондиціонер) до D2 через аналоговий інтерфейс (кабель ІоТ). На печі та АС при вмиканні буде червона крапка. Змінити стандартні значення Auto Cool та Auto Hea можна через веб – інтерфейс з пристрою керування (відкрити пристрій, поставити нові значення, натиснути Set). Термостат можна також переключати в рижим нагрівання або охолодження. Режими можна змінювати з пульта або Alt +ліва кнопка миші.

*Примітка.* Вибираючи значення налаштування слід пам’ятати, що всі пристрої нагрівання та охолодження інерційні, а на температуру в приміщенні також впливає температура навколишнього середовища в даний час доби.

1. Для слідкування **за** роботою ***датчиків газу і диму*** з головного шлюзу тримайте його вікно відкритим поруч з головним робочим полем, в якому безпосередньо вмикайте і вимикайте (Alt+лівий клік миші) старий автомобіль, який знаходиться у промислових пристроях. Наприклад, коли детектор виявив рівень газу вище заданого, він може активувати інший пристрій. Для спрацьовування датчика диму до нього можна підводити вогонь.

Для перевірки руху детектора його активують переміщенням миші з натисканням клавіші Alt на клавіатурі, коли курсор рухається до детектора, детектор включається. Вимикається автоматично через 5 секунд.

# Додаток Б Варіанти завдань

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | № варіанту | ІоТ пристрої і сценарій узгодження їх роботи | Додатково | Тип глобальної мережі |
|  |  | **ДЕННА** |  |  |
| Вовк Ірина Сергіївна |  | Монітор температури, обігрівач. Коли температура нижче заданого рівня, вмикається обігрівач, інакше – вимикається. | Пристрій управління ІоТ сервером – планшет/ смартфон  ІоТ сервер -локальний | CaTV |
| Грищенко Олена Юріївна |  | Монітор температури, кондиціонер. Коли температура вище заданого рівня, вмикається кондиціонер, інакше – вимикається. | Пристрій управління ІоТ сервером – планшет/ смартфон  ІоТ сервер -локальний | CaTV |
| Скріпченко Максим Олександрович |  | Термостат + піч. При температурі, нижче заданої, піч вмикається, інакше - вимикається. | Аналогове з’єднання між собою  ІоТ сервер -локальний | DSL |
| Заговора Денис Сергійович |  | Детектор вітру, двері гаража. Коли датчик спрацьовує і двері відкриті, закрити двері. | Пристрій управління ІоТ сервером – ноутбук  ІоТ сервер -віддалений | DSL |
| Загородній Дмитро Олександрович |  | Газонний розприскувач, детектор вітру. Коли піднімається вітер (детектор включається), розприскувач виключити, інакше включається. | Пристрій управління ІоТ сервером – планшет/ смартфон  ІоТ сервер -віддалений | CaTV |
| Задорожний Артем Сергійович |  | Детектор руху, замок дверей будинку. При виявленні датчиком руху двері автоматично запираються на замок. Виключаються пристрої з реєстратора. | Пристрій управління ІоТ сервером – ноутбук  ІоТ сервер -локальний | DSL |
| Зарічний Ярослав Сергійович |  | Монітор температури, газонний розприскувач. Задати допустимий рівень температури, вище якого розприскувач вмикається, а нижче – вимикається. | Пристрій управління ІоТ сервером – планшет/ смартфон  ІоТ сервер -локальний | CaTV |
| Кандель Кирило Володимирович |  | Замок на дверях будинку, вентилятор. При розблокуванні дверей, вентилятор автоматично вмикається. При блокуванні дверей, вентилятор автоматично вимикається. | Пристрій управління ІоТ сервером – ноутбук  ІоТ сервер -віддалений | CaTV |
| Кузнєцов Олексій Андрійович |  | Двері гаража, web-камера. При відкриванні дверей включається web-камера. Коли двері зачинені – камера вимикається. | Пристрій управління ІоТ сервером – планшет/ смартфон  ІоТ сервер -віддалений | CaTV |
| Кулик Вячеслав Олександрович |  | Замок на дверях будинку, кавоварка, лампа. При відкриванні замка дверей будинку автоматично включається кавоварка і лампа. | Пристрій управління ІоТ сервером – планшет/ смартфон  ІоТ сервер -локальний | DSL |
| Луценко Іван Андрійович |  | Датчик вітру, вікно. Коли датчик спрацьовує і вікно відкрите, закрити вікно. | Пристрій управління ІоТ сервером – планшет/ смартфон  ІоТ сервер -віддалений | DSL |
| Макаров Ігнат Вячеславович |  | Монітор вологи (в промислових пристроях), зволожувач повітря. Задати допустимий діапазон температури для вмикання та вимикання, якщо рівень вологи виходить за межі заданого діапазону. | Пристрій управління ІоТ сервером – планшет/ смартфон  ІоТ сервер -віддалений | CaTV |
| Медвідь Владислав Андрійович |  | Двері гаража, лампа. При відкритті дверей гаража автоматично включати світло, при закриванні – світло вимикається. | Пристрій управління ІоТ сервером – ноутбук  ІоТ сервер -локальний | DSL |
| Мельник Олексій Русланович |  | Вікно будинку, web-камера. При відкриванні вікна включається web-камера. Коли вікно зачиняється – камера вимикається. | Пристрій управління ІоТ сервером – ноутбук  ІоТ сервер -віддалений | CaTV |
| Михайловин Роман Геннадійович |  | Датчик діоксиду вуглецю, вентилятор, вікно будинку. У випадку досягнення рівня діоксиду вуглецю вище попередньо встановленої межі, включається вентилятор і відкривається вікно. | Пристрій управління ІоТ сервером – ноутбук  ІоТ сервер -локальний | DSL |
| Молчанова Варвара Сергіївна |  | Монітор температури, газонний розприскувач. Задати 2 допустимих рівня температури, вище і нижче яких розприскувач вимикається (жарко і холодно), а між ними – вмикається. | Пристрій управління ІоТ сервером – планшет/ смартфон  ІоТ сервер -віддалений | CaTV |
| Музика Олександр Андрійович |  | Детектор чадного газу, двері гаража. Коли, детектор чадного газу виявить рівень вище 0.2, двері гаража автоматично піднімаються. | Пристрій управління ІоТ сервером – ноутбук  ІоТ сервер -віддалений | DSL |
| Охота Денис Леонідович |  | Монітор рівня води, водостік, газонний розприскувач. Коли рівень води перевищую межу (наприклад, 5см), автоматично вмикати стік, інакше стік вимикається. | Пристрій управління ІоТ сервером – ноутбук  ІоТ сервер -локальний | DSL |
| Самвелян Артур Рафаельович |  | Детектор руху, вікно будинку. При виявленні датчиком руху вікно автоматично закривається. Виключаються пристрої з реєстратора. | Пристрій управління ІоТ сервером – ноутбук  ІоТ сервер -віддалений | DSL |
| Скорик Дарія Юріївна |  | Вікно будинку, сирена. При відкриванні дверей спрацьовує сирена. Виключаються пристрої з реєстратора. | Пристрій управління ІоТ сервером – планшет/ смартфон  ІоТ сервер -локальний | DSL |
| Степанюк Владислав Сергійович |  | Детектор диму, вікно, двері будинку. Коли, детектор диму виявить рівень вище припустимого, вікно і двері автоматично відкриваються. | Пристрій управління ІоТ сервером – ноутбук  ІоТ сервер -віддалений | CaTV |
| Стефура Олег Ярославович |  | Монітор вологи (в промислових пристроях), газонний розприскувач. Задати допустимий діапазон температури для вмикання та вимикання, якщо рівень вологи виходить за межі заданого діапазону. | Пристрій управління ІоТ сервером – планшет/ смартфон  ІоТ сервер -локальний | CaTV |
| Тараненко Андрій Володимирович |  | Детектор диму, сирена. Коли, детектор диму виявить рівень вище припустимого, спрацьовує сирена. | Пристрій управління ІоТ сервером – ноутбук  ІоТ сервер -локальний | DSL |
| Фуголь Максим Дмитрович |  | Датчик діоксиду вуглецю, вентилятор, двері гаража. У випадку досягнення рівня діоксиду вуглецю вище попередньо встановленої межі, включити вентилятор і відкриваються двері гаража. | Пристрій управління ІоТ сервером – планшет/ смартфон  ІоТ сервер -віддалений | DSL |