Projet Smart Home IoT

Conception d'un Système Domotique Intelligent Basé sur l'IoT

Surveillance, Sécurité Incendie et Contrôle à Distance

Année : 2025

Table des matières

Chapitre 1

Introduction Générale

L'Internet des Objets (IoT) s'impose aujourd'hui comme une révolution technologique majeure, transformant notre façon d'interagir avec notre environnement quotidien. En connectant des objets physiques à Internet, l'IoT permet de collecter, analyser et échanger des données en temps réel, ouvrant ainsi la voie à des systèmes intelligents capables de réagir de manière autonome aux événements de leur environnement.

Dans le contexte résidentiel, cette transformation se traduit par l'émergence des Smart Homes, ou maisons intelligentes, qui intègrent des dispositifs connectés pour améliorer significativement le confort, la sécurité et l'efficacité énergétique des habitations. Face aux risques domestiques tels que les incendies, les intrusions et la surconsommation énergétique, les systèmes domotiques intelligents offrent des solutions innovantes de détection et de réponse automatisée.

Dans ce projet, nous avons conçu et implémenté un système Smart Home complet, basé sur une architecture IoT robuste et sécurisée. Le système repose sur des objets IoT interconnectés capables de détecter des événements critiques et de déclencher automatiquement des actions correctives tout en notifiant l'utilisateur via un smartphone.

Notre solution intègre trois scénarios complémentaires répondant à des besoins essentiels :

- Un **système de sécurité incendie** capable de détecter la présence de fumée et de déclencher automatiquement une sirène d'alarme, un système d'extinction (sprinkler) et l'envoi de notifications en temps réel
- Un **système de surveillance d'accès** utilisant la détection de mouvement pour activer intelligemment l'éclairage et une webcam, permettant un contrôle à distance de l'accès via une porte intelligente
- Un **système de régulation thermique** optimisant la consommation énergétique en adaptant automatiquement le fonctionnement du climatiseur et de la fenêtre selon la présence détectée et les besoins climatiques

L'architecture réseau développée constitue le socle technique de notre système, intégrant une connectivité sans fil sécurisée (Wi-Fi), le protocole HTTP pour les échanges de

données, et un serveur IoT centralisé assurant la coordination de tous les équipements. Cette infrastructure garantit une communication fiable entre les capteurs, les actionneurs et l'interface utilisateur, tout en permettant un accès distant sécurisé.

Ce rapport présente l'ensemble de notre démarche, depuis la modélisation UML du système jusqu'à l'implémentation et la validation des différents scénarios. Le chapitre 2 expose la conception fonctionnelle à travers les diagrammes de cas d'utilisation et de séquence. Le chapitre 3 détaille l'infrastructure réseau et la configuration de tous les équipements. Le chapitre 4 décrit les trois scénarios IoT implémentés avec leurs logiques de fonctionnement respectives. Enfin, le chapitre 5 conclut ce travail et ouvre des perspectives d'évolution prometteuses.

Chapitre 2

Conception et Modélisation du Système IoT

Ce chapitre présente la modélisation fonctionnelle du système à travers les diagrammes UML.

2.1 Diagramme de Cas d'Utilisation

Le diagramme de cas d'utilisation permet de visualiser les fonctionnalités globales du système Smart Home.

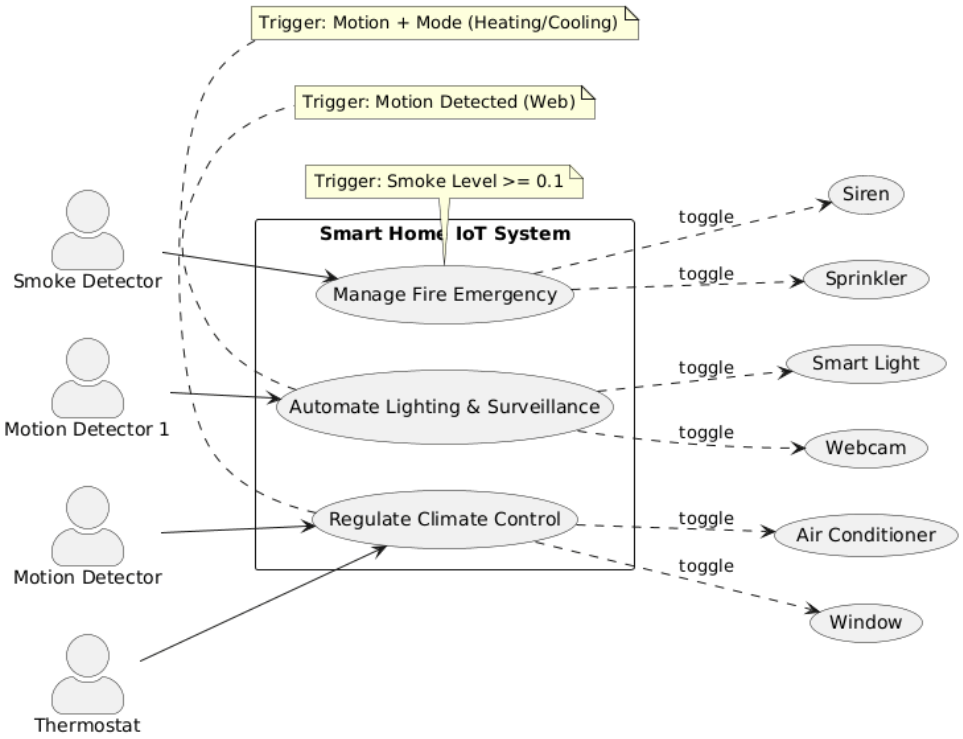

FIGURE 2.1 – Diagramme de cas d'utilisation des trois scénarios IoT.

— **Manage Fire Safety :** Déclenché par le *Smoke Detector* pour activer l'alerte et l'extinction.
— **Automate Surveillance :** Géré par le *Motion Detector 1* pour piloter l'éclairage et la webcam.
— **Regulate Climate :** Ce cas d'utilisation nécessite à la fois la détection d'une présence et un état spécifique du thermostat pour piloter l'Air conditioner et la fenêtre.

2.2 Diagramme de Séquence

2.2.1 Scénario 1

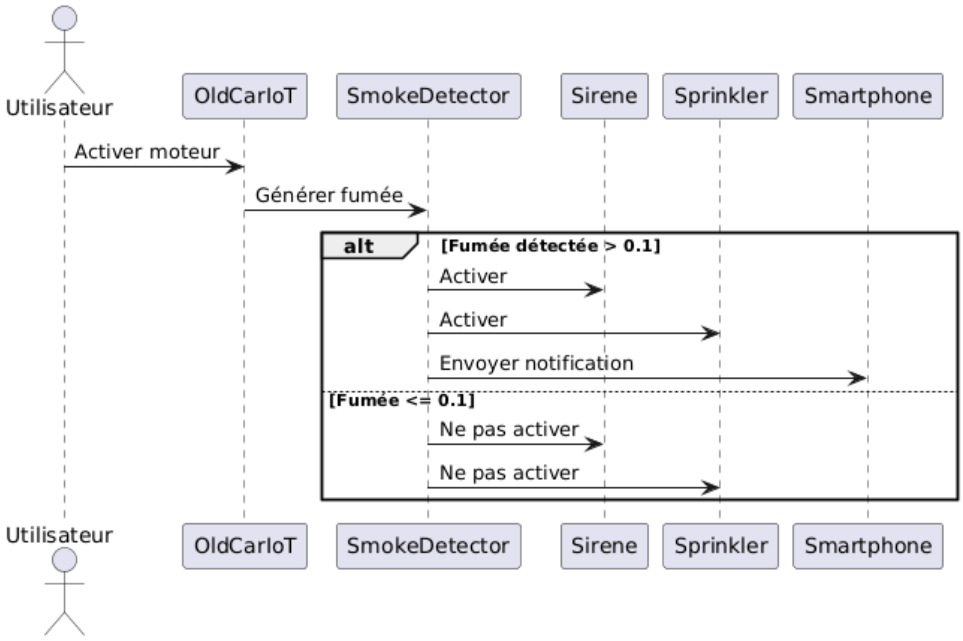

FIGURE 2.2 – Diagramme de séquence pour le scénario 1

2.2.2 Scénario 2

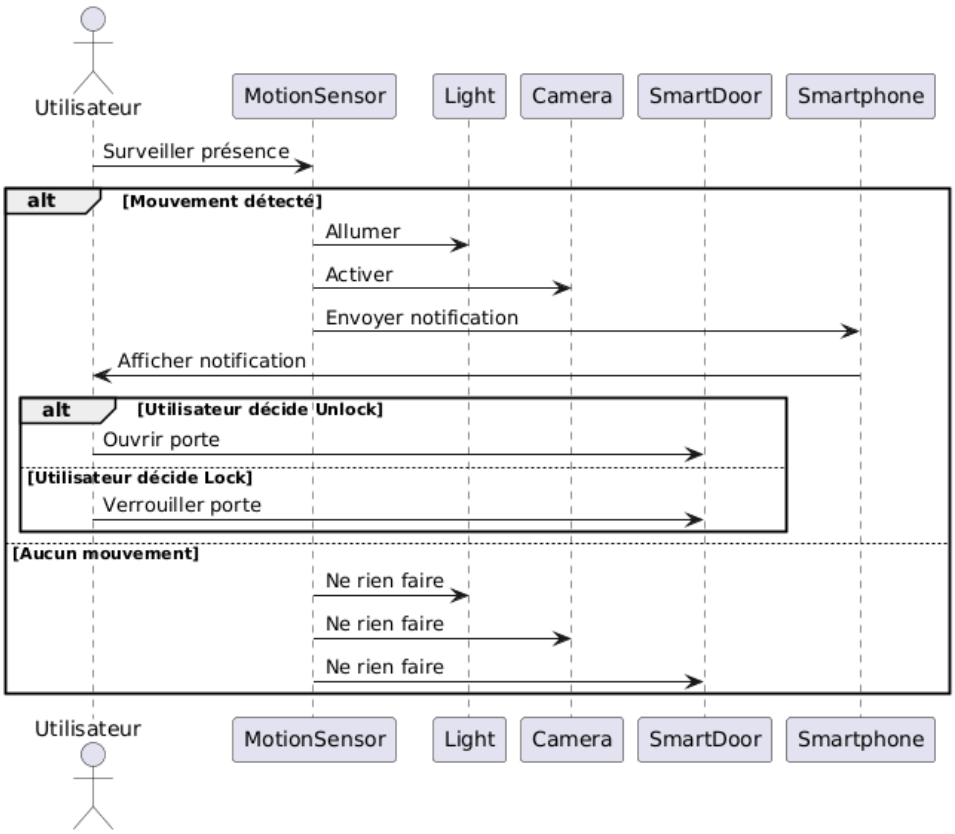

FIGURE 2.3 – Diagramme de séquence pour le scénario 2

2.2.3 Scénario 3

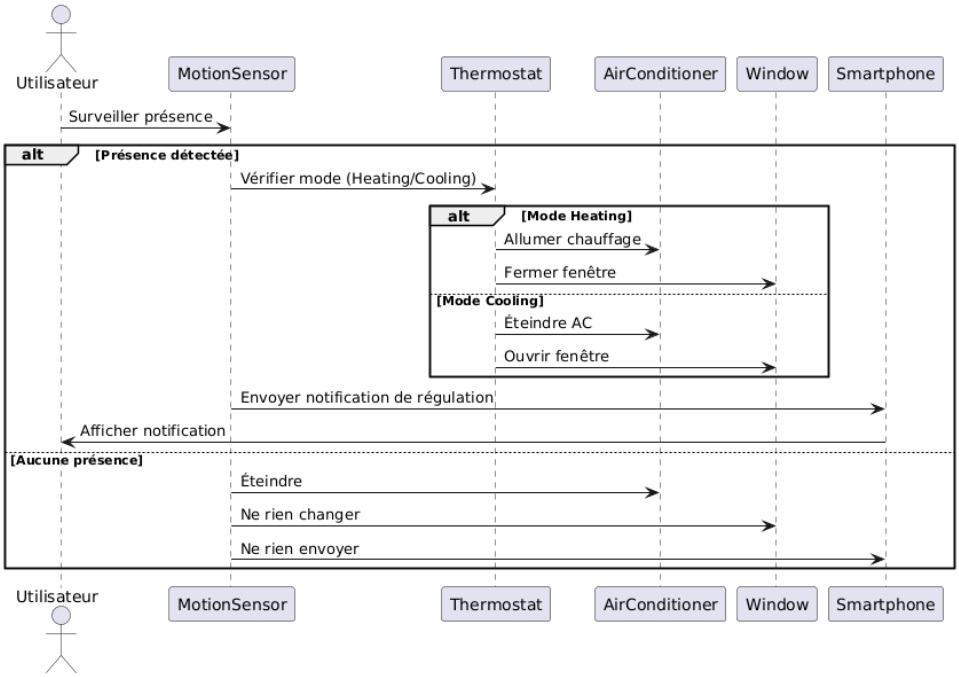

FIGURE 2.4 – Diagramme de séquence pour le scénario 3

Chapitre 3

Infrastructure Réseau et Base HTTP du Projet IoT

Ce chapitre décrit l'ensemble des configurations réseau mises en place afin de constituer l'infrastructure de base du projet Smart Home IoT. Cette architecture est indispensable pour assurer la connectivité des objets IoT, la communication avec le serveur IoT ainsi que l'accès distant via HTTP depuis un smartphone ou un ordinateur.

Sans cette infrastructure réseau, les scénarios intelligents du Smart Home (détection de fumée, activation de la sirène, déclenchement du sprinkler et notification utilisateur) ne pourraient pas fonctionner de manière fiable.

3.1 Vue Globale de l'Architecture Réseau

L'architecture réseau du projet repose sur une organisation hiérarchique reliant les objets IoT au réseau Internet via plusieurs équipements intermédiaires.

Les objets IoT sont connectés sans fil au **Home Gateway**, qui joue le rôle de point d'accès Wi-Fi et de routeur domestique. Le Home Gateway est ensuite relié au routeur du fournisseur d'accès Internet (ISP), permettant l'accès au réseau WAN / Internet et aux serveurs distants.

Cette architecture assure :

— Une connectivité continue des objets IoT

— Une communication avec le serveur IoT (IoE-Server)

— Un accès distant depuis un smartphone ou un ordinateur via HTTP

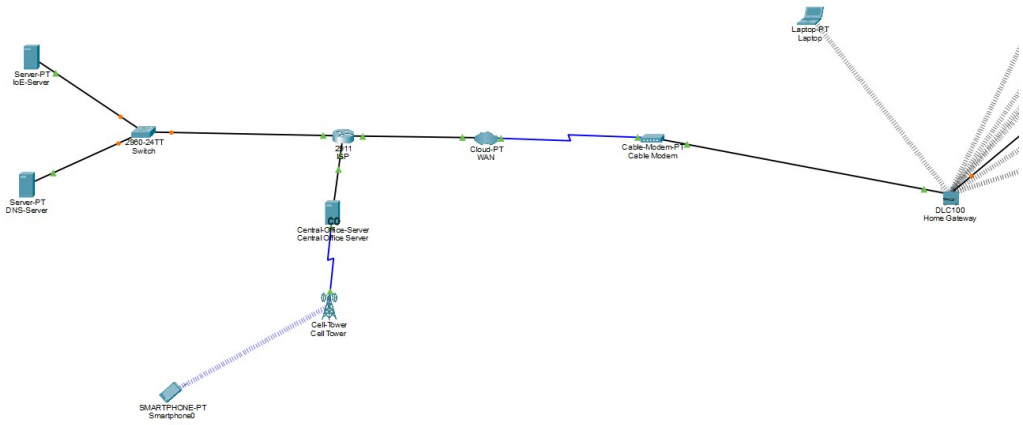

FIGURE 3.1 – Vue globale de l'architecture réseau du Smart Home IoT

3.2 Configuration des Appareils IoT

Les appareils IoT (IoT0, IoT1 et IoT2) constituent les éléments finaux du système Smart Home. Ils doivent être correctement équipés et configurés afin de pouvoir se connecter au réseau sans fil domestique et communiquer avec le serveur IoT.

3.2.1 Ajout des Modules Réseau

Avant toute configuration logique, les objets IoT doivent être équipés de modules réseau adaptés. Les modules sans fil permettent aux objets de se connecter au réseau Wi-Fi du Home Gateway.

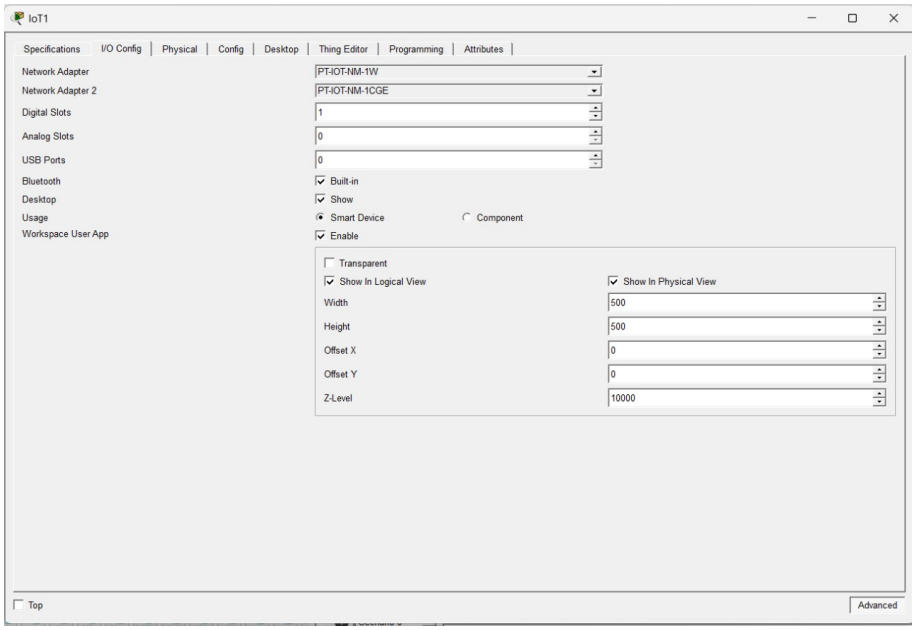

FIGURE 3.2 – Installation du module réseau sans fil sur l'objet IoT1

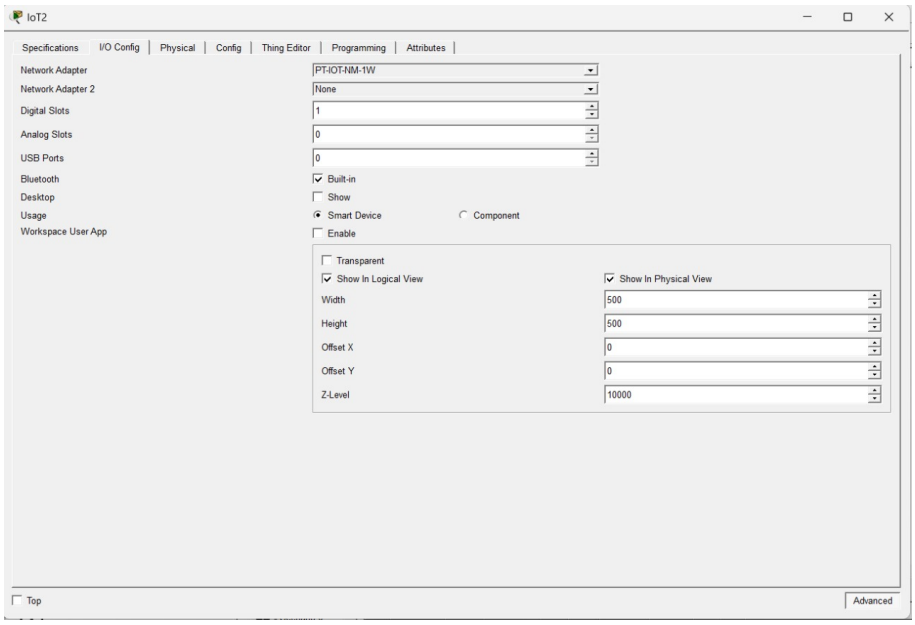

FIGURE 3.3 – Installation du module réseau sans fil sur l'objet IoT2

Remarque : L'appareil IoT1 utilise le module **PT-IOT-NM-1CGE**, qui offre à la fois une connectivité Ethernet et une connectivité Wi-Fi, tandis que IoT0 et IoT2 utilisent uniquement le module sans fil PT-IOT-NM-1W.

3.2.2 Configuration de l'Interface Sans Fil

Une fois les modules installés, l'interface sans fil (**Wireless0**) de chaque objet IoT est configurée afin de se connecter au réseau domestique sécurisé.

Les paramètres communs sont :

— SSID : **SMARTIOT**

— Authentification : WPA2-PSK

— Clé de sécurité (Pass Phrase) : 1234qwer

— Type de chiffrement : AES

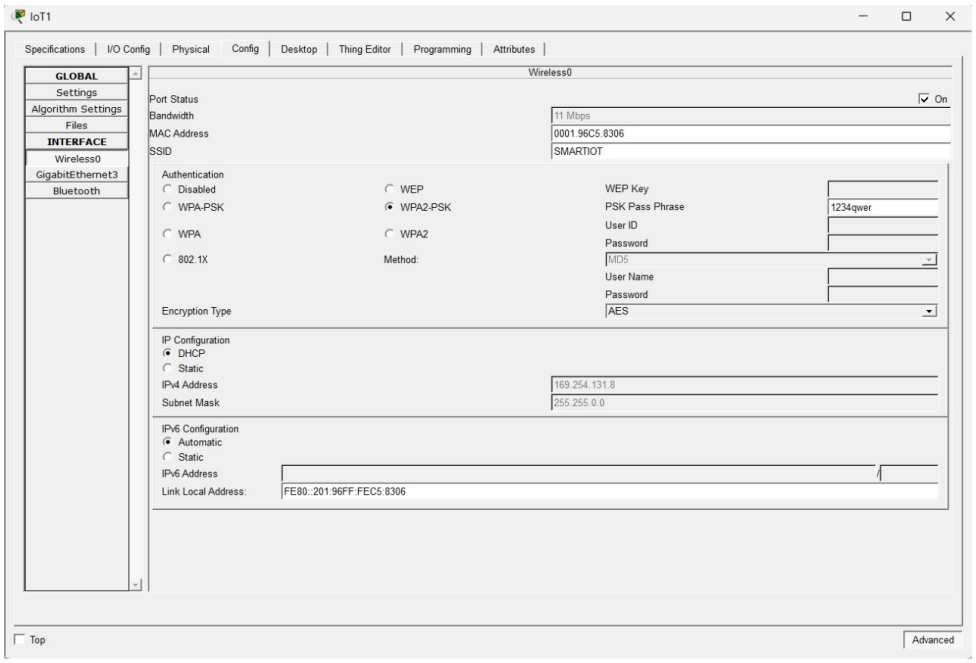

FIGURE 3.4 – Configuration Wi-Fi de l'interface Wireless0

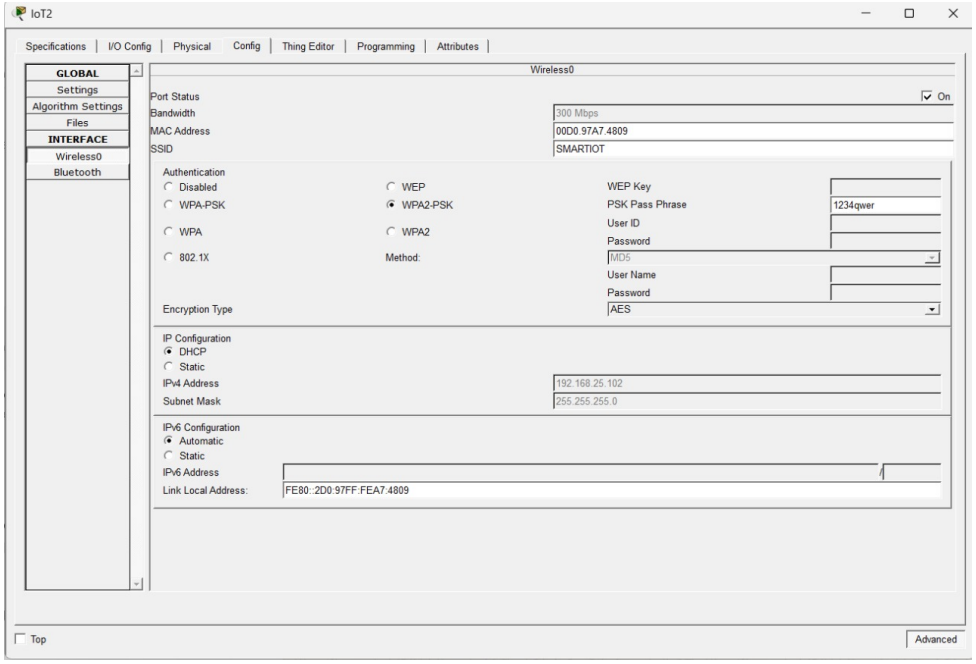

FIGURE 3.5 – Connexion réussie des objets IoT au réseau SMARTIOT

3.2.3 Configuration des Adresses IP

Les objets IoT sont configurés avec des adresses IP statiques afin d'assurer une communication fiable avec le serveur IoT et les autres équipements du réseau.

— IoT1 : 169.254.131.8 / 255.255.0.0 (adresse APIPA utilisée lors des tests initiaux)

— IoT2 : 192.168.25.102 / 255.255.255.0

— IoT0 : 192.168.25.104 / 255.255.255.0

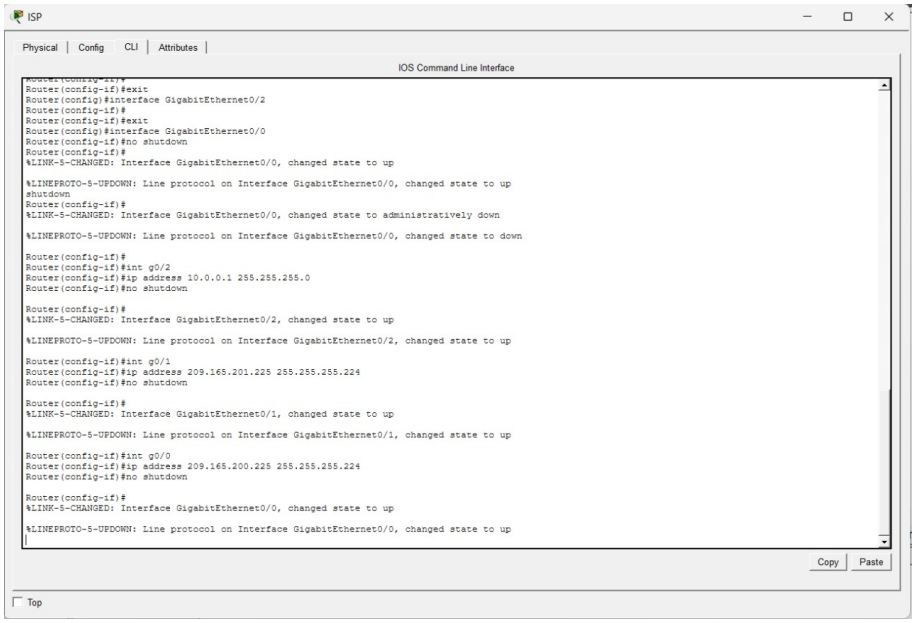

FIGURE 3.6 – Configuration IP statique des objets IoT

3.3 Configuration du Home Gateway

Le Home Gateway constitue le cœur du réseau domestique. Il agit comme point d'accès sans fil pour les objets IoT, routeur local et passerelle vers Internet.

3.3.1 Configuration de l'Interface Sans Fil

Les paramètres Wi-Fi du Home Gateway sont configurés de manière cohérente avec ceux des objets IoT.

— SSID : SMARTIOT
— Canal : 6 (2.437 GHz)
— Portée : 250 mètres
— Sécurité : WPA2-PSK (AES)

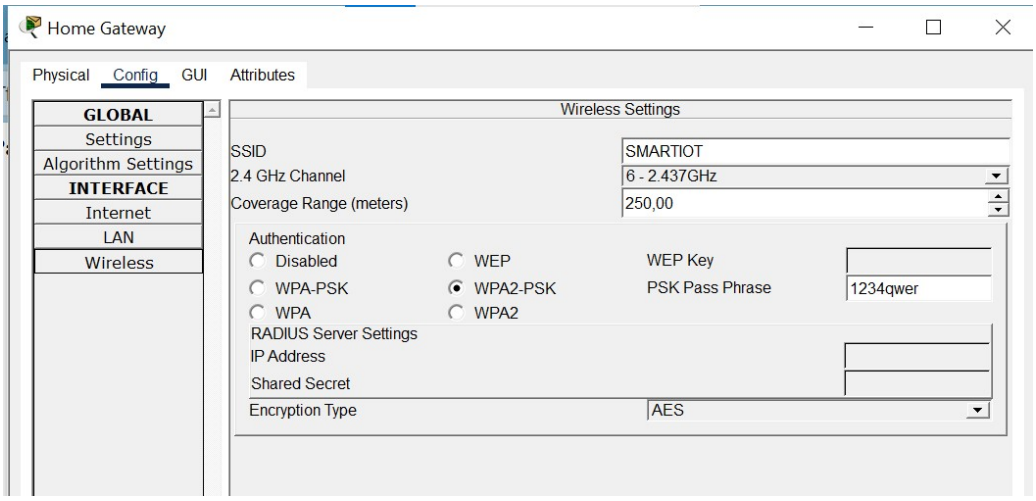

FIGURE 3.7 – Configuration sans fil du Home Gateway

3.4 Poste Client : Laptop et Validation de la Connectivité

Le laptop intégré au réseau Smart Home IoT joue un rôle essentiel en tant qu'interface de supervision et de contrôle des objets IoT. Grâce à une interface web dédiée, il permet à l'utilisateur de consulter en temps réel l'état des équipements (sirène, porte, fenêtre, webcam) et de piloter certains dispositifs via le protocole HTTP.

Afin de simplifier l'accès aux services IoT, un serveur DNS local a été configuré. Ce serveur permet la résolution des noms de domaine internes, notamment le domaine `www.iot.org`, qui est associé à l'adresse IP du serveur IoT (10.0.0.253). Cette résolution facilite la communication entre les objets et le serveur tout en rendant le réseau plus intuitif pour l'utilisateur.

Pour s'assurer de la bonne configuration et du bon fonctionnement du réseau, des tests de connectivité ont été réalisés depuis le laptop. Ces tests, basés sur des commandes ping, ont permis de vérifier que le laptop peut atteindre l'adresse IP du serveur DNS (10.0.0.254), ainsi que le serveur IoT via son nom de domaine. Ces validations confirment l'intégrité et la cohérence de la connectivité réseau locale, garantissant ainsi une communication fiable avant la mise en place des accès WAN via le routeur ISP.

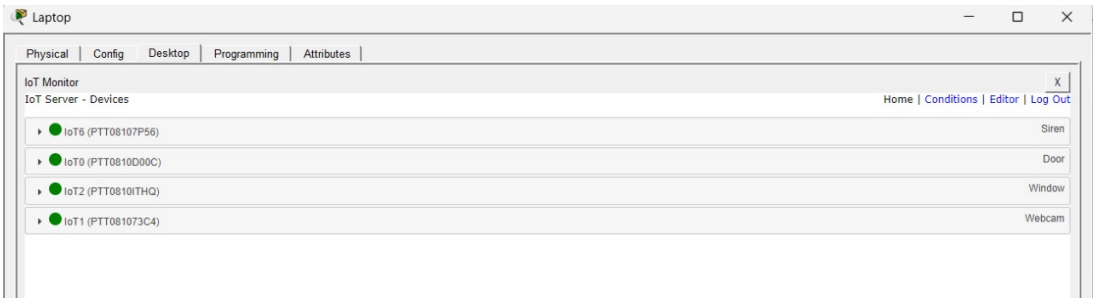

FIGURE 3.8 – Interface de supervision des objets IoT sur le laptop
Affiche l'état des objets IoT (sirène, porte, fenêtre, webcam).

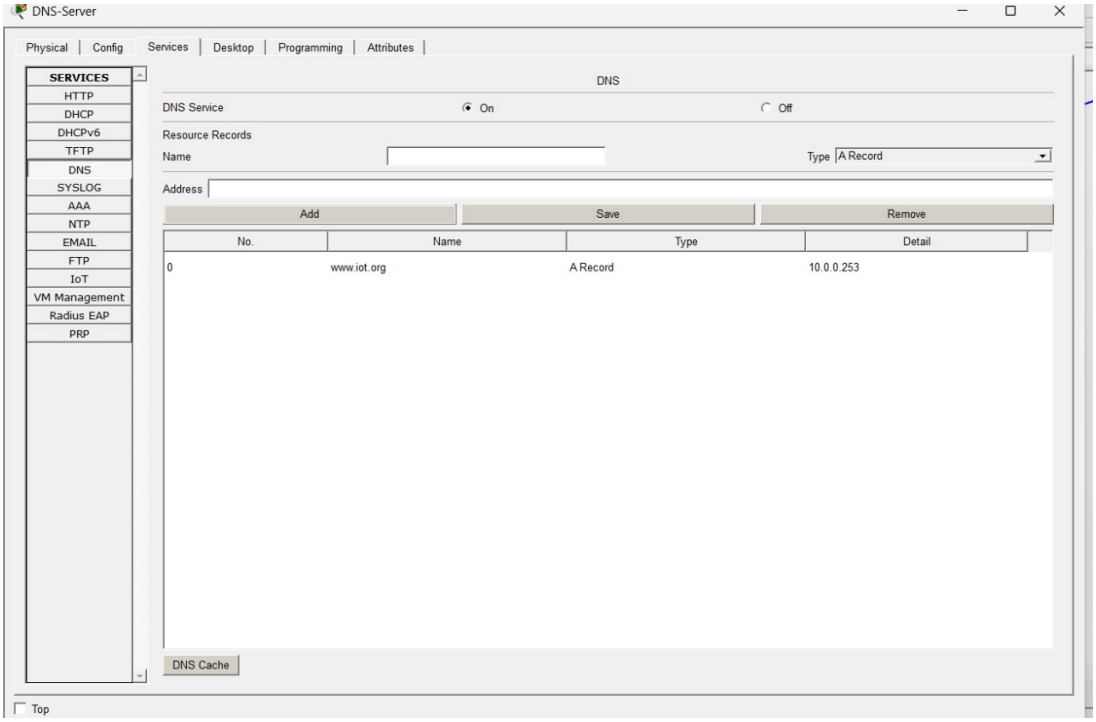

FIGURE 3.9 – Configuration du serveur DNS avec l'enregistrement pour `www.iot.org`
Permet la résolution du nom de domaine vers l'adresse IP 10.0.0.253.

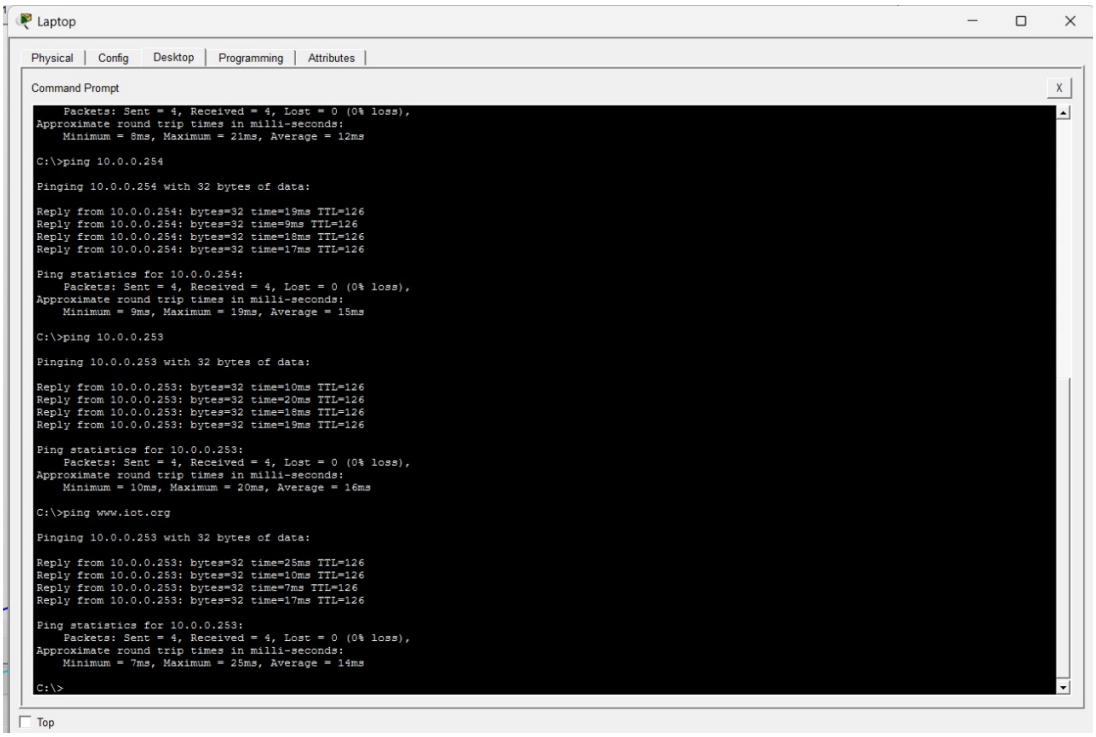

FIGURE 3.10 – Test ping depuis le laptop
Validation de la connectivité IP vers le serveur DNS (10.0.0.254), le serveur IoT (10.0.0.253) et résolution du nom `www.iot.org`.

3.5 Configuration du Routeur ISP

Le routeur ISP assure la connexion du réseau domestique au réseau WAN / Internet. Il fournit également les services DHCP nécessaires aux réseaux externes.

3.5.1 Configuration des Interfaces Réseau

Les interfaces du routeur ISP sont configurées via la ligne de commande (CLI).

— GigabitEthernet0/2 : 10.0.0.1 / 255.255.255.0
— GigabitEthernet0/1 : 209.165.201.225 / 255.255.255.224
— GigabitEthernet0/0 : 209.165.200.225 / 255.255.255.224

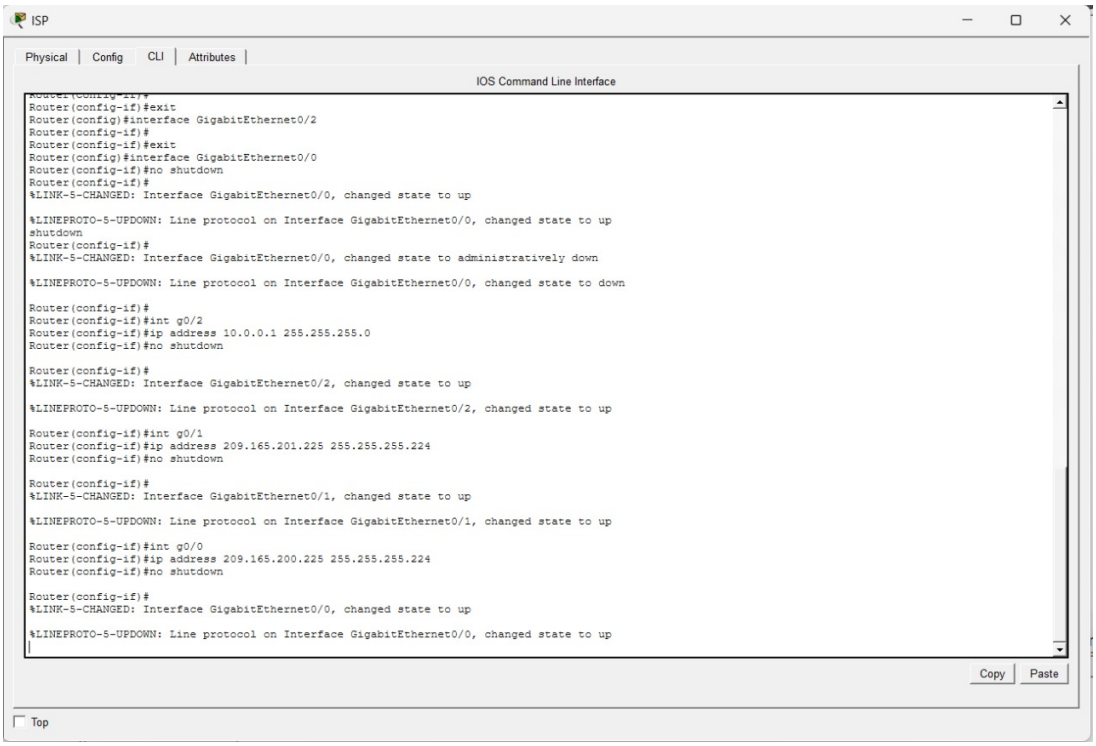

FIGURE 3.11 – Configuration des interfaces du routeur ISP

3.5.2 Configuration des Services DHCP

Le routeur ISP fournit des services DHCP afin d'assurer une configuration automatique des équipements connectés aux réseaux WAN et CELL.

Pool DHCP WAN

- Réseau : 209.165.200.224 / 255.255.255.224
- Passerelle : 209.165.200.225
- DNS : 10.0.0.254

Pool DHCP CELL

- Réseau : 209.165.201.224 / 255.255.255.224
- Passerelle : 209.165.201.225
- DNS : 10.0.0.254

```
Router(config-if)#exit
Router(config)#ip dhcp excluded-address 209.165.201.225 209.156.201.229
Router(config)#
Router(config)#ip dhcp excluded-address 209.165.201.225 209.165.201.229
Router(config)#ip dhcp pool CELL
Router(dhcp-config)#network 209.165.201.224 255.255.255.224
Router(dhcp-config)#default-router 209.165.201.225
Router(dhcp-config)#dns-server 10.0.0.254
Router(dhcp-config)#
```

FIGURE 3.12 – Configuration du pool DHCP CELL

```
Router>
Router>enable
Router#config term
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip dhcp excluded-address 209.165.200.225 209.165.200.229
Router(config)#ip dhcp pool WAN
Router(dhcp-config)#network 209.165.200.224 255.255.255.224
Router(dhcp-config)#default-router 209.165.200.225
Router(dhcp-config)#dns-server 10.0.0.254
Router(dhcp-config)#
```

FIGURE 3.13 – Configuration du pool DHCP WAN

3.6 Support du Protocole HTTP et Accès Smartphone

L'ensemble de cette infrastructure réseau constitue la base nécessaire au fonctionnement du Smart Home IoT et au support du protocole HTTP.

Grâce à HTTP, le système permet :

— La communication entre les objets IoT et le serveur IoT (IoE-Server)

— L'envoi et la réception des données des capteurs et actionneurs

— L'accès distant depuis un smartphone ou un ordinateur

— La réception de notifications en temps réel

— Le contrôle manuel des équipements du Smart Home

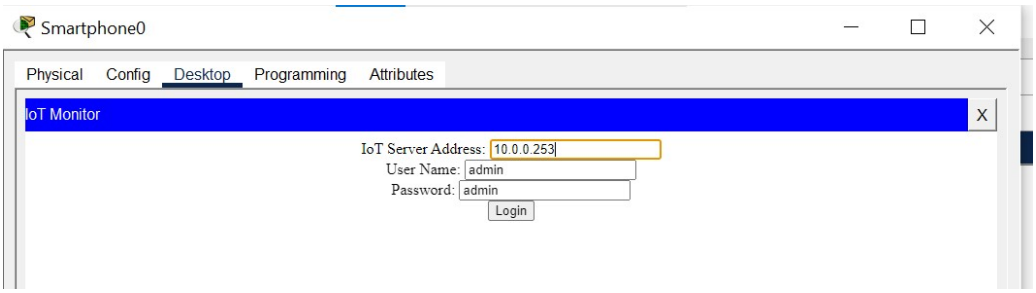

FIGURE 3.14 – Accès HTTP au serveur IoT depuis un navigateur web

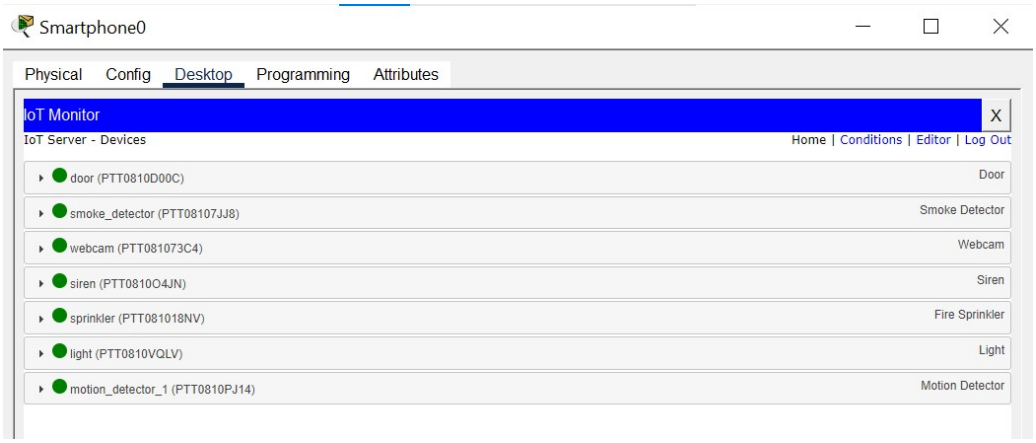

FIGURE 3.15 – Intégration des objets IoT connectés au serveur central

Chapitre 4

Présentation du Smart Home et des Scénarios IoT

4.1 Composants du Smart Home

Le système Smart Home est composé des éléments suivants :

— Détecteur de fumée (Smoke Detector)
— Sirène d'alarme
— Système d'arrosage automatique (Sprinkler)
— Smartphone (interface utilisateur)
— Serveur IoT (IoE-Server)

4.2 Scénario 1 : Système de Sécurité Incendie

4.2.1 Connexion des équipements IoT

Connexion du détecteur de fumée

Le détecteur de fumée est connecté au *Home Gateway* via une connexion sans fil. Le SSID et le mot de passe configurés sur la passerelle ont été utilisés afin d'assurer une communication correcte avec le serveur IoT.

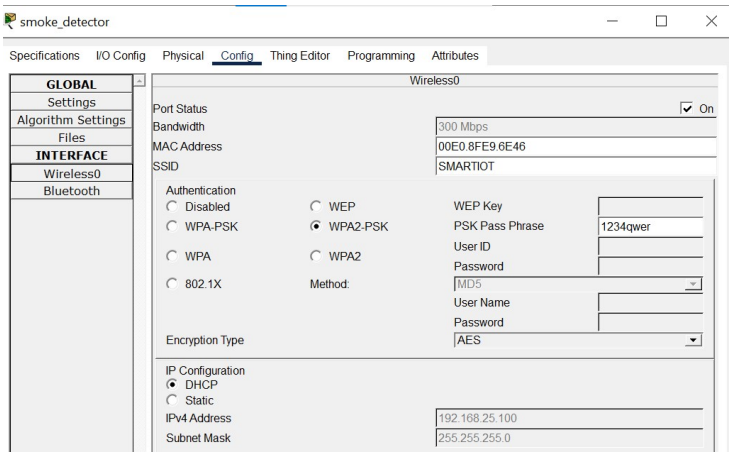

FIGURE 4.1 – Connexion du détecteur de fumée au Home Gateway

Connexion de l'Old Car IoT

L'équipement *Old Car IoT* est intégré au réseau IoT afin de simuler une situation réelle d'incendie. Lorsque le moteur de la voiture est activé, celle-ci génère de la fumée, permettant ainsi de tester le comportement du détecteur de fumée.

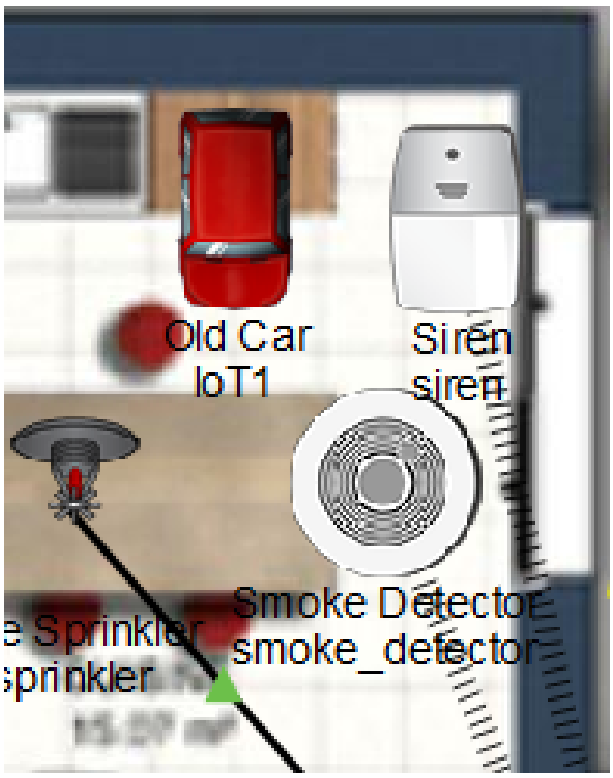

FIGURE 4.2 – Simulation de fumée à l'aide de l'Old Car IoT

Connexion de la sirène

La sirène est reliée au *Home Gateway* par une connexion IoT sans fil. Cette connexion permet son activation automatique en cas de détection de fumée.

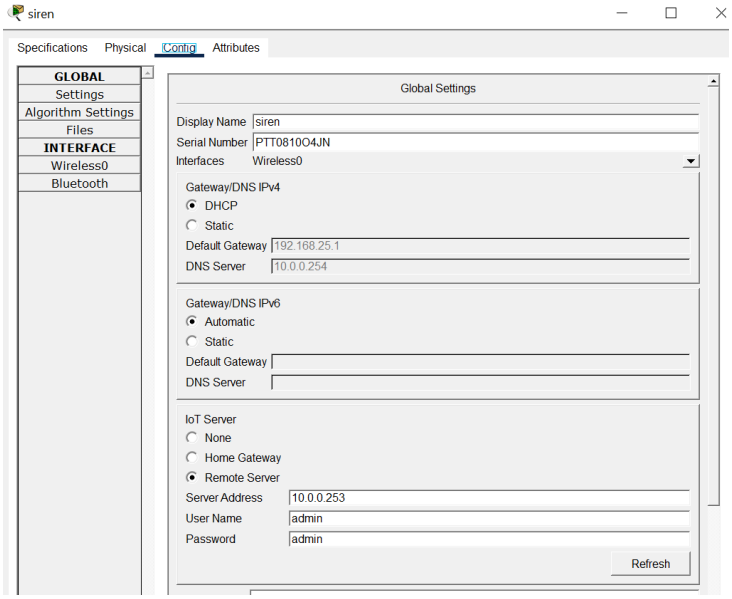

FIGURE 4.3 – Connexion de la sirène au Home Gateway

Connexion du système de sprinkler

Le système de sprinkler est connecté au *Home Gateway* via le réseau IoT. Il permet d'intervenir automatiquement pour limiter la propagation du feu.

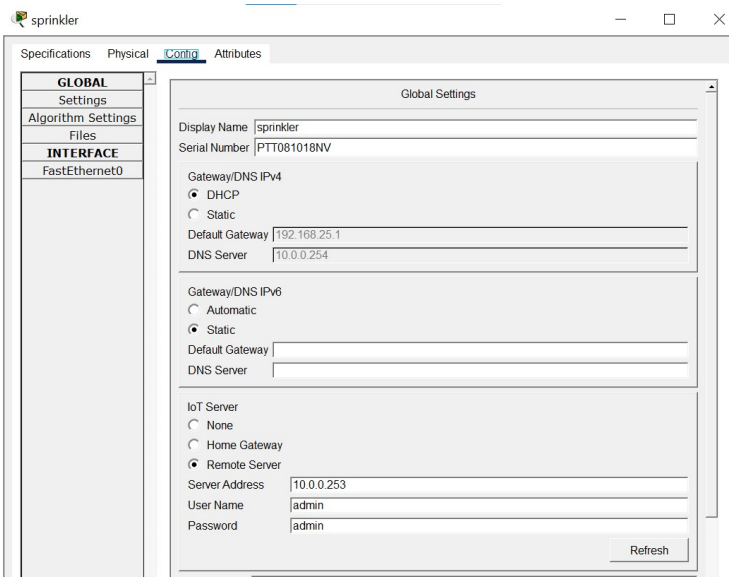

FIGURE 4.4 – Connexion du système de sprinkler au Home Gateway

Connexion du smartphone utilisateur

Le smartphone de l'utilisateur est configuré avec l'application *IoT Monitor*. Il est relié au serveur IoT afin de recevoir des alertes en temps réel lors d'une détection de fumée.

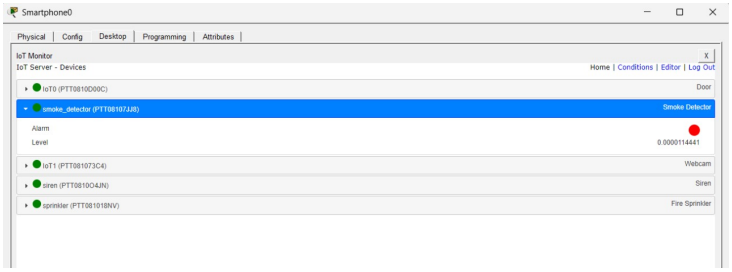

FIGURE 4.5 – Réception d'une notification d'alerte incendie sur le smartphone

4.2.2 Supervision et logique de fonctionnement

Le système de sécurité incendie est supervisé à l'aide de l'application *IoT Monitor* installée sur le smartphone de l'utilisateur. Cette application permet de surveiller l'état des capteurs et de définir les règles de fonctionnement du scénario.

Condition : détection de fumée (ON)

Lorsque l'*Old Car IoT* est activée, elle génère de la fumée. Le détecteur de fumée passe alors à l'état *ON*, ce qui déclenche automatiquement les actions suivantes :

— activation de la sirène,
— déclenchement du système de sprinkler,
— envoi d'une notification d'alerte sur le smartphone de l'utilisateur.

Condition : absence de fumée (OFF)

Lorsque l'*Old Car IoT* est désactivée et qu'aucune fumée n'est détectée, le détecteur de fumée reste à l'état *OFF*. Dans ce cas :

— la sirène reste désactivée,
— le système de sprinkler ne se déclenche pas,
— aucune notification n'est envoyée à l'utilisateur.

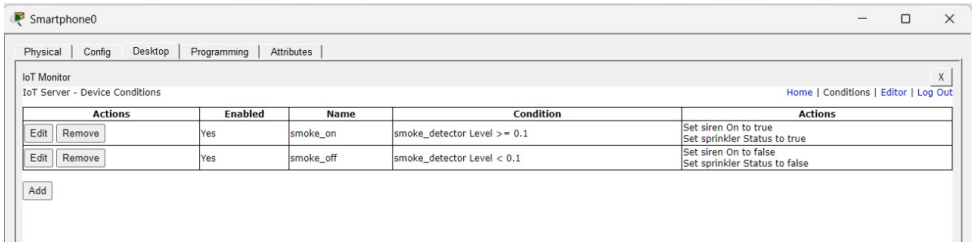

FIGURE 4.6 – Supervision du système incendie : conditions de fonctionnement avec et sans détection de fumée

Scénario de sécurité incendie en état actif

La figure ci-dessous illustre le fonctionnement global du scénario lorsque la fumée est détectée par le capteur.

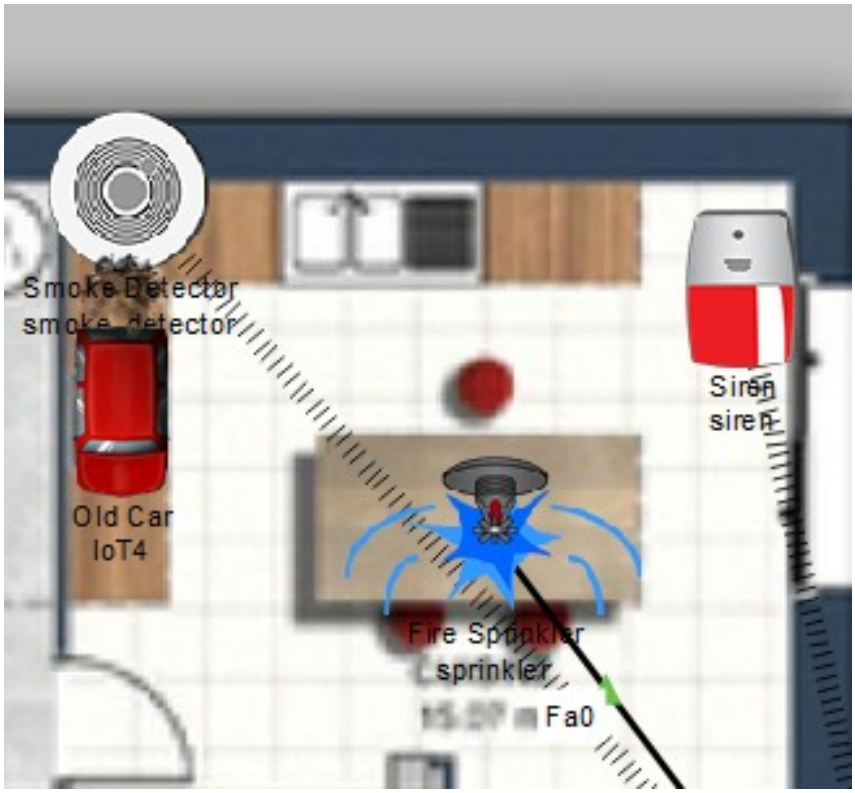

FIGURE 4.7 – Scénario de sécurité incendie en état actif

4.3 Scenario 2 : Smart Door Security System

4.3.1 Connexion des équipements IoT

Connexion du capteur de mouvement

Le capteur de mouvement est connecté au *Home Gateway* via le réseau sans fil. Le SSID et le mot de passe définis sur la passerelle ont été configurés afin d'assurer la connexion.

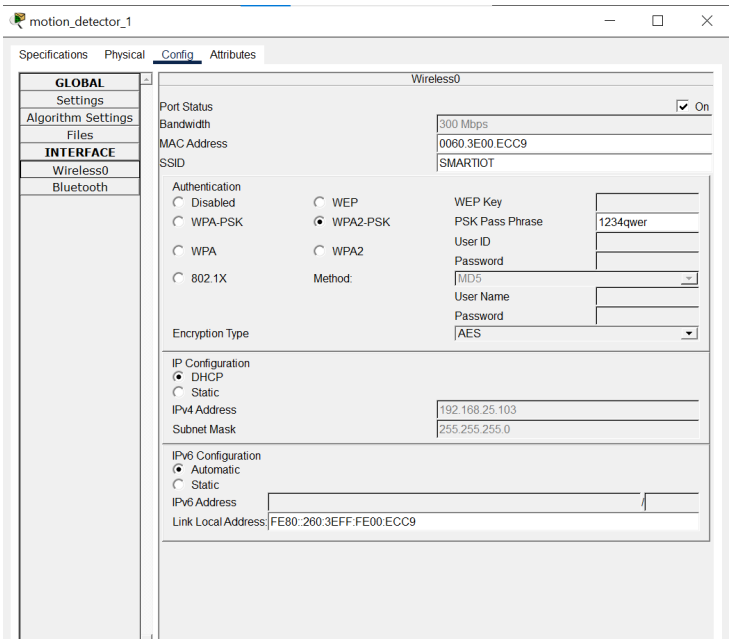

FIGURE 4.8 – Connexion du capteur de mouvement au Home Gateway

Connexion de la webcam

La webcam est reliée au *Home Gateway* en utilisant une connexion Wi-Fi sécurisée. Elle utilise le même SSID et mot de passe configurés sur la passerelle.

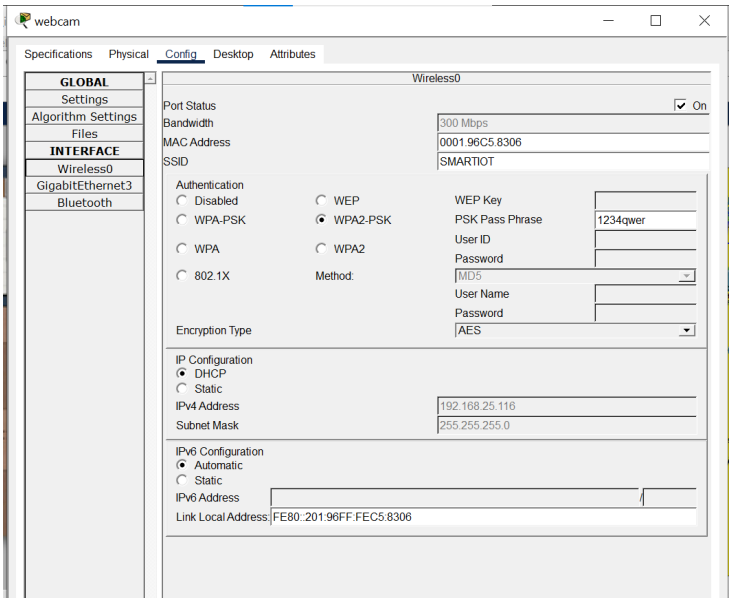

FIGURE 4.9 – Connexion de la webcam au Home Gateway

Connexion de la lumière intelligente

La lumière intelligente est connectée sans fil au *Home Gateway*. Cette connexion permet son activation automatique selon l'état du capteur de mouvement.

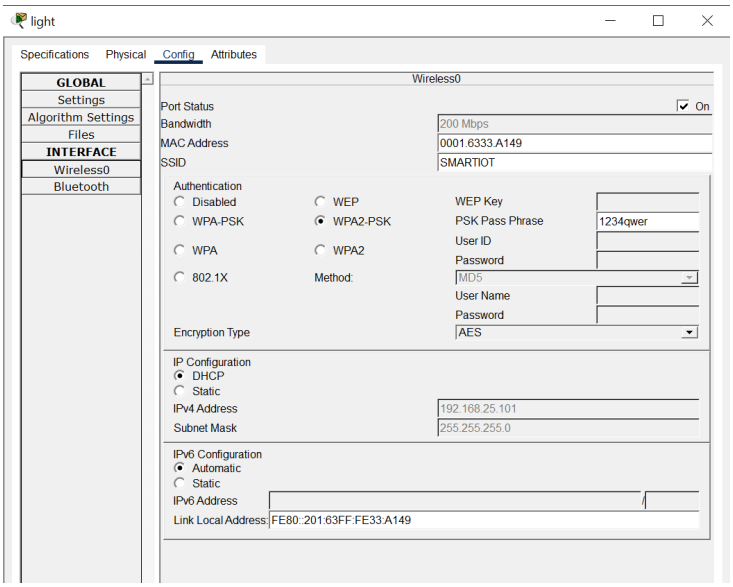

FIGURE 4.10 – Connexion de la lumière intelligente au Home Gateway

Connexion de la porte intelligente

La porte intelligente est configurée pour communiquer avec le *Home Gateway* via le réseau Wi-Fi. Cette connexion permet au responsable de la maison de contrôler l'accès à distance.

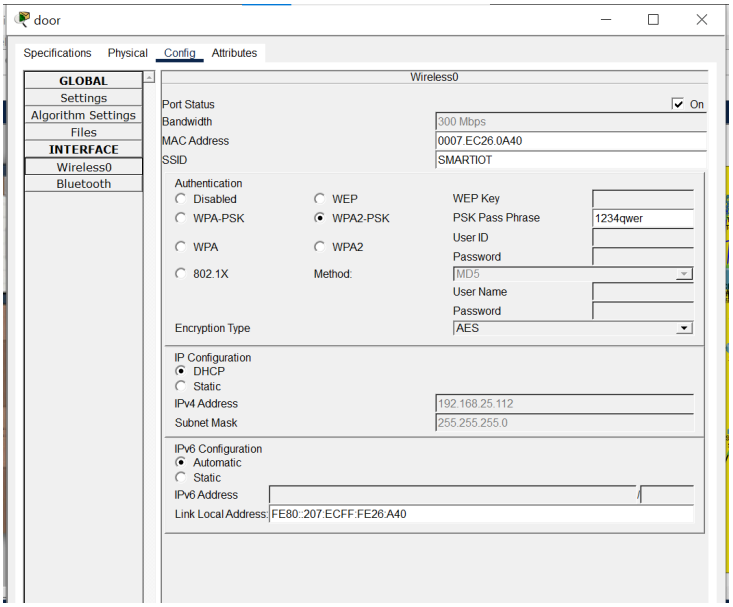

FIGURE 4.11 – Connexion de la porte intelligente au Home Gateway

4.3.2 Supervision et logique de fonctionnement

Le système est contrôlé à partir de l'application *IoT Monitor* installée sur un smartphone, configuré avec l'adresse IP `10.0.0.253`. Cette interface permet de surveiller les équipements et de définir les règles de fonctionnement du scénario.

Condition : détection de mouvement (ON)

Lorsque le capteur de mouvement est activé, la lumière et la webcam s'allument automatiquement. Le responsable de la maison peut alors visualiser la personne via la webcam et décider d'ouvrir la porte à distance.

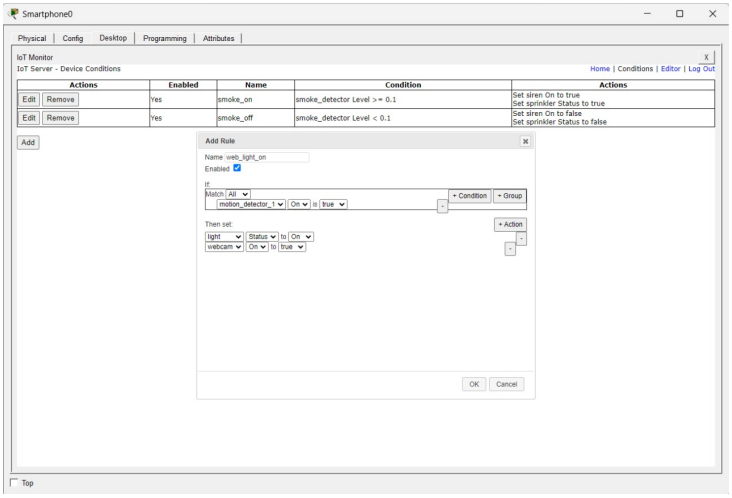

FIGURE 4.12 – Condition de fonctionnement lorsque le capteur de mouvement est activé

Condition : absence de mouvement (OFF)

Lorsque le capteur de mouvement est désactivé, la lumière et la webcam sont automatiquement arrêtées. Aucune action d'accès à la porte n'est alors autorisée.

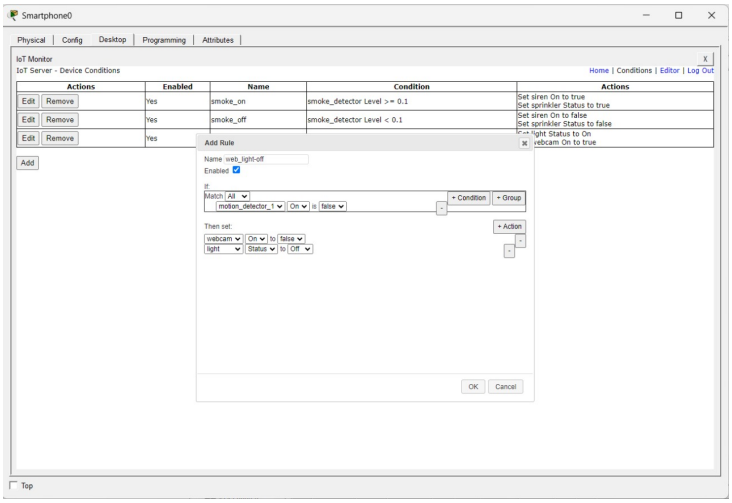

FIGURE 4.13 – Condition de fonctionnement lorsque le capteur de mouvement est désactivé

Scénario de sécurité en état actif

La figure ci-dessous illustre le fonctionnement global du scénario lorsque le capteur de mouvement détecte une présence.

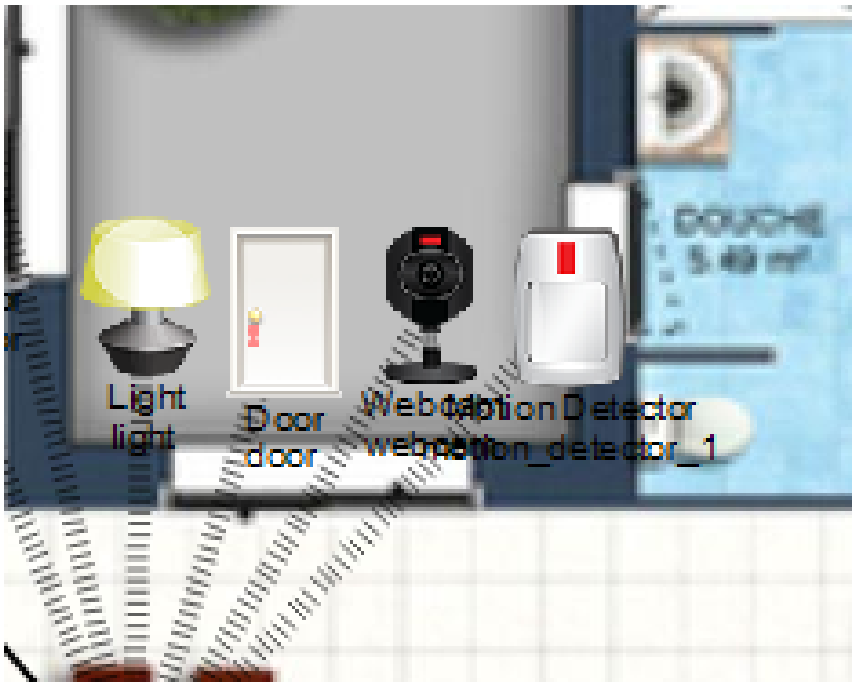

FIGURE 4.14 – Scénario de sécurité lorsque le capteur de mouvement est activé

Contrôle de la porte via smartphone

Le responsable de la maison peut contrôler la porte intelligente à distance à partir de l'application *IoT Monitor* sur son smartphone. Il peut cliquer sur *Lock* ou *Unlock* afin d'autoriser ou de refuser l'accès.

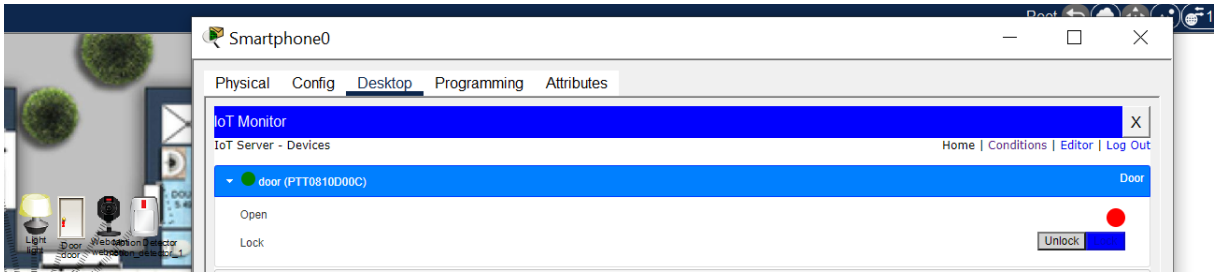

FIGURE 4.15 – Contrôle de la porte intelligente via smartphone (Lock / Unlock)

Lorsque le responsable sélectionne l'option *Unlock*, la porte s'ouvre automatiquement.

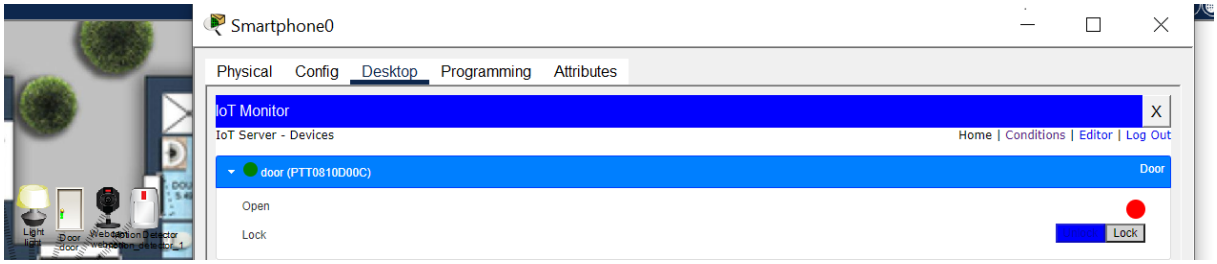

FIGURE 4.16 – Porte intelligente ouverte après autorisation du responsable

4.4 Scenario 3 : Smart Thermal Control System

Ce scénario décrit l'implémentation d'un système de régulation thermique automatisé. L'objectif est de coordonner l'action du climatiseur et de la fenêtre en fonction de la détection de mouvement et du mode du thermostat pour optimiser la consommation énergétique.

4.4.1 Topologie et Disposition Physique

La disposition des équipements dans la pièce permet une interaction directe entre les capteurs et les actionneurs via le réseau sans fil.

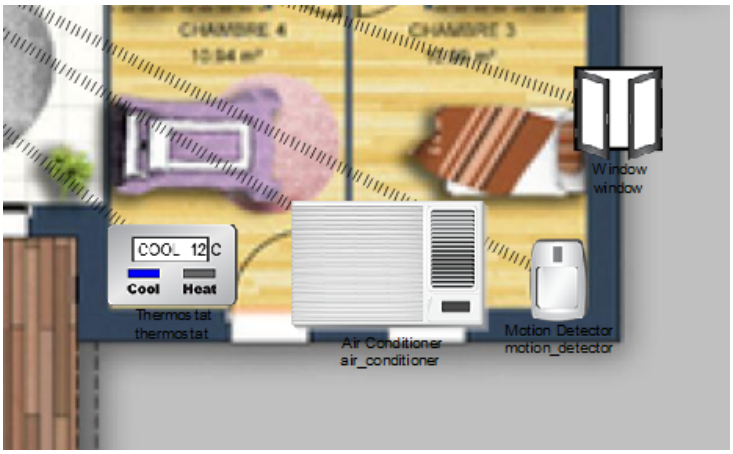

FIGURE 4.17 – Topologie logique et emplacement des périphériques IoT.

4.4.2 Configuration Réseau et Connectivité Sans-fil

Tous les dispositifs utilisent une interface sans fil (*Wireless0*) pour se connecter au SSID **SMARTIOT** avec une sécurité **WPA2-PSK**. Les adresses IP sont attribuées dynamiquement par **DHCP**.

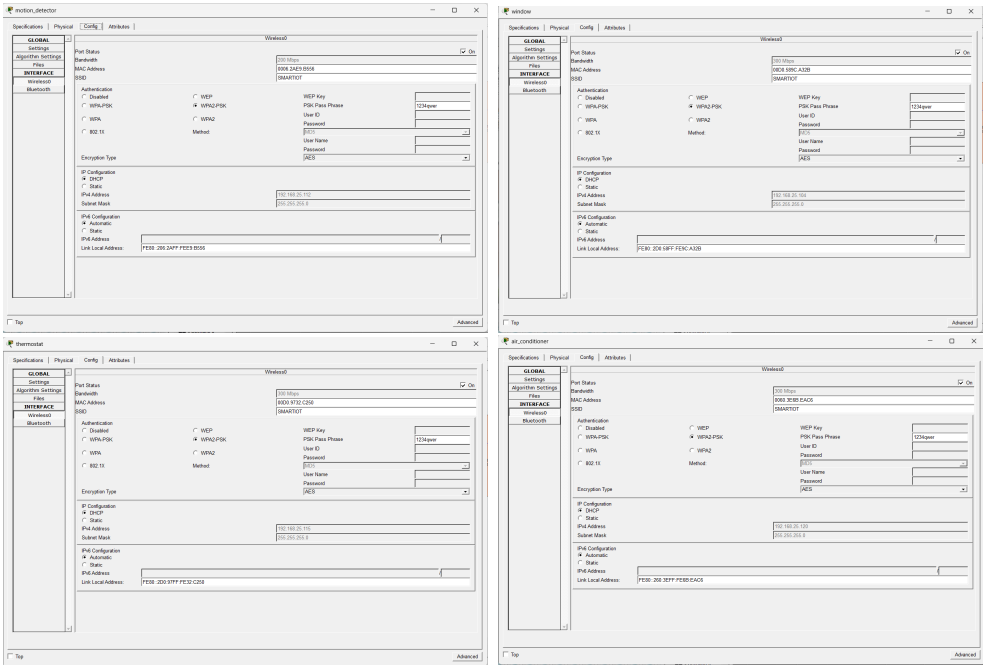

FIGURE 4.18 – Configuration Réseau et Connectivité Sans-fil pour chaque dispositif.

4.4.3 Configuration du Serveur IoT

Pour centraliser la gestion, chaque appareil est configuré pour communiquer avec un **Remote Server** situé à l'adresse `10.0.0.253`.

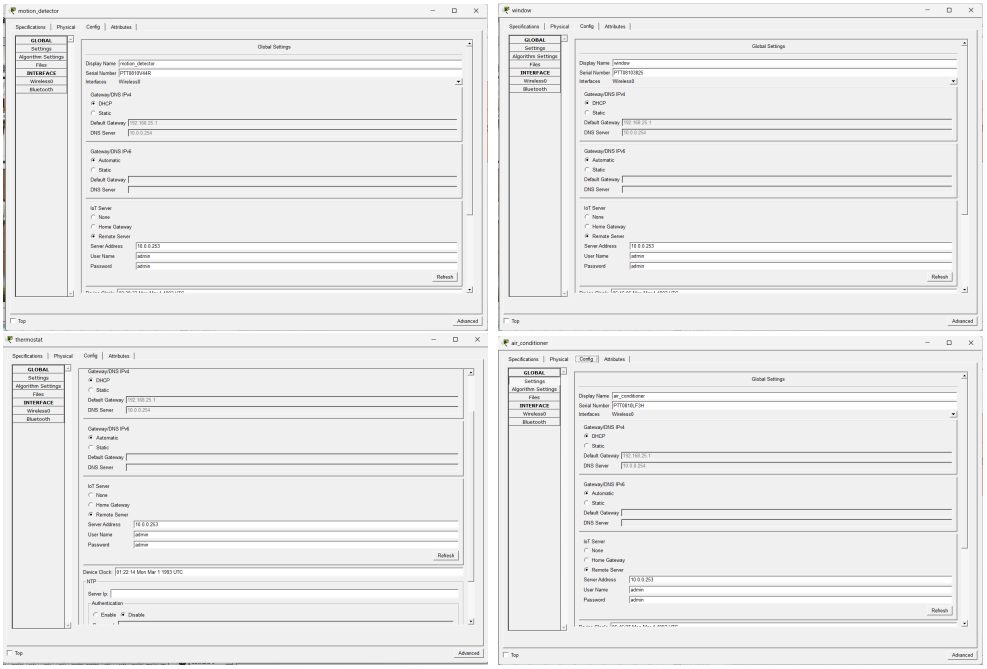

FIGURE 4.19 – Configuration des services IoT (Remote Server) pour chaque dispositif.

4.4.4 Logique d'Automatisation (IoT Monitor)

Le contrôle du système repose sur deux règles principales. La logique utilise l'opérateur **Match All**, signifiant que toutes les conditions doivent être vraies simultanément pour déclencher l'action.

L'aperçu global montre les conditions `temp_heating` et `temp_cooling` actives dans le moniteur.

Edit Remove	Yes	temp_heating	Match all: • thermostat Status is Heating • motion_detector On is true	Set air_conditioner On to true Set window On to false
Edit Remove	Yes	temp_cooling	Match all: • thermostat Status is Cooling • motion_detector On is true	Set air_conditioner On to false Set window On to true

FIGURE 4.20 – Vue d'ensemble des conditions programmées sur le serveur pour scénario 3.

Détails des Conditions

1. **Mode Chauffage (temp_heating) :** Si le thermostat est en mode *Heating* et qu'une présence est détectée, le climatiseur s'allume et la fenêtre se ferme pour isoler la pièce.
2. **Mode Refroidissement (temp_cooling) :** Si le thermostat est en mode *Cooling* et qu'une présence est détectée, le système privilégie la ventilation naturelle en ouvrant la fenêtre et en éteignant le climatiseur.

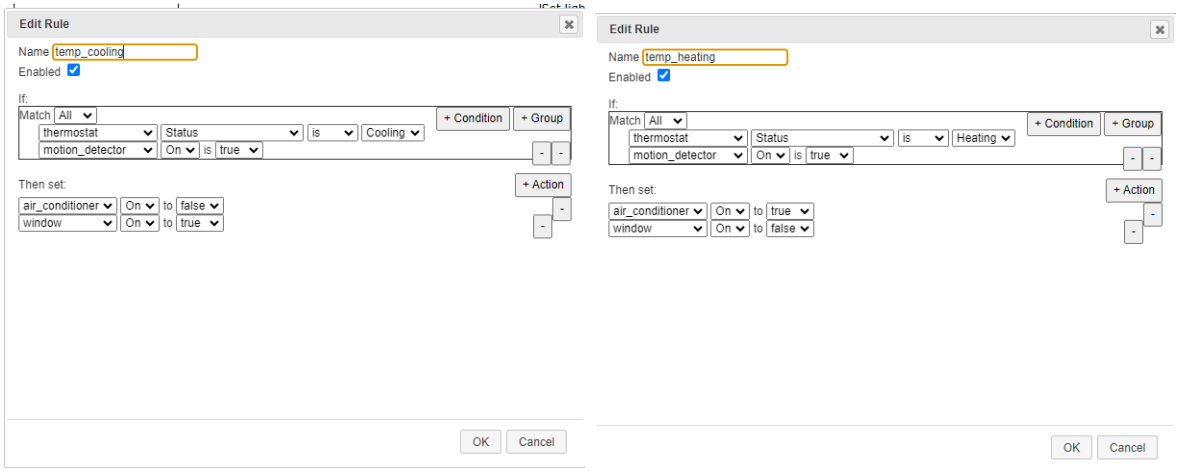

FIGURE 4.21 – Détails des règles logiques pour le chauffage (gauche) et le refroidissement (droite).

Interface de Supervision (IoT Monitor)

Enfin, l'interface principale du moniteur IoT permet de visualiser en temps réel l'état de tous les objets connectés au serveur. La figure ci-dessous montre un exemple où le

thermostat est réglé sur le mode "Cooling" et les différents périphériques affichent leur statut actuel (Marche/Arrêt).

FIGURE 4.22 – Tableau de bord de supervision montrant l'état temps réel des dispositifs.

Chapitre 5

Conclusion et Perspectives

Ce projet a permis de concevoir et d'implémenter avec succès un système Smart Home IoT complet et fonctionnel. À travers la mise en place d'une architecture réseau robuste et la configuration des différents équipements, nous avons développé une infrastructure solide capable de supporter des scénarios intelligents d'automatisation et de sécurité.

Les trois scénarios implémentés démontrent l'efficacité du système : le système de sécurité incendie assure une protection automatisée avec détection de fumée et déclenchement des mesures d'extinction, le système de surveillance d'accès combine détection de mouvement et contrôle à distance, et le système de régulation thermique optimise la consommation énergétique selon les conditions d'occupation.

L'infrastructure réseau déployée, basée sur le protocole HTTP et une connectivité Wi-Fi sécurisée, garantit une communication fiable entre tous les composants. L'intégration d'un serveur IoT centralisé facilite la gestion et le contrôle de l'ensemble des équipements via une interface accessible depuis un smartphone.

Plusieurs perspectives d'évolution se dessinent pour enrichir ce système :

- Ajout d'une caméra IP pour améliorer les capacités de surveillance
- Intégration de l'intelligence artificielle pour adapter le comportement du système aux habitudes des occupants
- Support de standards IoT universels (MQTT, Matter) pour une meilleure interopérabilité
- Déploiement sur une infrastructure réelle avec prise en compte des contraintes physiques

En conclusion, ce projet démontre le potentiel des technologies IoT pour créer des solutions domotiques intelligentes et efficaces. L'architecture réseau constitue une base solide et évolutive, permettant l'ajout progressif de nouveaux scénarios selon les besoins. Les résultats obtenus confirment que l'IoT apporte une réelle valeur ajoutée en termes de sécurité, de confort et d'efficacité énergétique dans l'habitat moderne.