## Unit title: Internet of Things (SCQF level 7) Unit code: J0HC 34

## Practical Assessment

You have been tasked with setting up a smart home in Packet tracer with the following items outlined in the table below.

You have been provided with a PT template called ***Smart home assessment.pkt*** in which you will configure your smart home devices.

When accessing the registration server IoT service from the Admin PC web browser for the first time, create a new user account by clicking sign up now and the username should be your **surname** with password **surname1234.** This will then be used to login in to manage devices on the registration server and also for adding wireless smart devices. Some IoT devices will require wireless network cards to communicate with the homegateway.

Over and above what has been covered in class, **4.2.3.3 Packet Tracer - Securing Cloud Services in the IoT**, particularly steps 1 and 2 will be most helpful in assisting with this task. You must use *conditions* in the registration server where appropriate to configure sensors / devices. *Using Alt+click will activate actuators.*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Item** | **Placement** | **IP address** | **Registration server?** | **Comments** | **Testing** | **Check off when completed** |
| **Home gateway** | Upper hall | 192.168.25.1 | No | Connected wired to PC and registration server and connecting smart devices wirelessly |  | v |
| **Admin PC** | Bedroom | 192.168.25.100 | No | Wired into LAN interface on Home gateway, and web browser used for accessing IoT Registration server | Use web browser to | v |
| **Registration server** | Bedroom | 192.168.25.10 | No | Wired into LAN interface on Home gateway, and IOT registration service used for managing smart devices | Ensure smart devices can access this server | v |
| **Music player** | Bedroom | Uses layer 2 address | No | Paired directly with Bluetooth Speaker | Successful pairing | v |
| **Bluetooth Speaker** | Lower Hall | Uses layer 2 address | No | Paired directly with music player | Successful pairing | v |
| **Motion detector** | Front door | DHCP from Home Gateway | yes | Connected wirelessly to HomeGateway, registered on IoT registration server, and triggers webcam when activated | Triggers webcam when motion | v |
| **Trip Sensor** | Back door Patio | DHCP from Home Gateway | Yes | Connected wirelessly to HomeGateway, registered on IoT registration server, and triggers Siren when activated | triggers Siren when activated | v |
| **Webcam** | Front door | DHCP from Home Gateway | Yes | Connected wirelessly to HomeGateway, registered on IoT registration server, and triggered by motion detector | Triggered by motion detector | v |
| **Siren** | Back door Patio | DHCP from Home Gateway | Yes | Connected wirelessly to HomeGateway, registered on IoT registration server, and triggered by tripwire | Triggered by tripwire | v |
| **Humidifier** | Basement | DHCP from Home Gateway | Yes | Connected wirelessly to HomeGateway, registered on IoT registration server, and triggered by humidity sensor 70% | Triggered by humidity sensor | v |
| **Humidity Monitor** | Basement | DHCP from Home Gateway | Yes | Connected wirelessly to HomeGateway, registered on IoT registration server, and triggers Dehumidifier when activated | Used to trigger dehumidifier | v |
| **Temp Monitor** | Upper Hall | DHCP from Home Gateway | Yes | Connected wirelessly to HomeGateway, registered on IoT registration server, and triggers Ceiling fan when activated 21.5 degrees | triggers Ceiling fan when activated 21.5 degrees | v |
| **Ceiling Fan** | Upper Hall | DHCP from Home Gateway | Yes | Connected wirelessly to HomeGateway, registered on IoT registration server, and triggered by temp sensor 21.5 degrees | Triggered by temp sensor | v |
| **Old car** | Driveway | DHCP from Home Gateway | Yes | triggers CD alarms when started or activated | Start to produce fumes and trigger carbon monoxide and carbon dioxide alarms | v |
| **Blower** | Lower Hall | DHCP from Home Gateway | Yes | Connected wirelessly to HomeGateway, registered on IoT registration server, and triggered by carbon dioxide alarm | triggered when carbon dioxide alarm reaches 6% . Blower must come on high. | v |
| **Carbon dioxide detector** | Lower Hall | DHCP from Home Gateway | Yes | Connected wirelessly to HomeGateway , registered on IoT registration server, and triggered by old car | triggered by old car fumes and activates blower at 6% | v |

Answer these questions:

1. **Why were these IoT devices chosen (for what purpose) and what type of IoT data will be collected / used?**

- Carbon Dioxide Detector: the purpose of this device is to monitor indoor air quality and make sure proper ventilation. It collects IoT data based on CO2 levels, which may include timestamps and alerts for high concetrations.

- Music Player: this device improves automations and comfrot by allowing you to schedule or trigger music based on specific events. It collects data on playback status, track information and whether a user is present.

- Wbcam: the main purpose of a webcam is for security, surveillance or video communication. It collects data from IoT video streams, image, capture, and meta data related to audio detection.

-Temperature Monitor: this device measures indoor temperature to improve comfrot and energy efficiency and to trigger the HVAC system when necessary. The collected data includes temperature readings in celcius or fahrenheit, timestamps and trends over time.

1. **Are / could there be any security vulnerabilities with the smart home you have configured e.g. IoT devices, network devices / servers, communication / security protocols etc and what could be done to help mitigate these?**

There are potential security vulnerabilities associated with IoT devices. Many of these devices come with default usernames or passwords that are easy to guess. In addition, the firmware may contain unpatched vulnerabilities. Weak network security is another concern, for example poorly configured wifi networks might not use encryption or could be utilising outdated protocols like WEP. If devices do not get regular firmware updates, they can become vulnerable. Poor update practices can allo security problems to continue without being fixed.

1. **Choose one device from the smart home and implement one or more of the mitigation techniques you identified in question 2 above**.

Smart home webcams have some potential risks. These include unauthorised access, hackers watching or recording video, and data being intercepted if videos are sent without encryption. Weak default usernames and passwords, as well as unpatched firmware, create vulnerabilities. To reduce these risks, change the default username and password. Use a unique and complex password that is long complex, such as Moth3rw3ll\_1993. this hel stop unauthorised from logging in with the factory credentials.