Smart Home Network based on Cisco Equipment

Kateryna Kolbasova[1], Bohdan Zhurakovskyi[1], Vadym Poltorak[1], Volodymyr Nakonechnyi[2], and Roman Kyrychok[3]

[1] *National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute,” 37 Peremogy ave., Kyiv, 03056, Ukraine*
[2] *Taras Shevchenko National University of Kyiv, 60 Volodymyrska str., Kyiv, 01601, Ukraine*
[3] *Borys Grinchenko Kyiv University, 18/2 Bulvarno-Kudriavska str., Kyiv, 04053, Ukraine*

Abstract

This paper develops and implements a smart home concept using sensors and actuators that are connected to a gateway via Wi-Fi communication protocol. The 3G/4G client can control the home remotely using an account on the IoT server. The project is simulated using the Cisco Packet Tracer simulation tool. Networking and programming is a powerful foundation for this research as it provides the interface between sensors actuators and devices to be controlled. The proposed system can be applied in many areas, including home security, lighting control, flame detection, intelligent heating, motion sensor, door control, etc., to provide homeowner comfort, safety, energy efficiency (low operating costs), and convenience at any time.

Keywords

Internet of Things, network, smart home, automation, Cisco Packet Tracer, wireless connection.

1. Introduction

A modern “smart house” is an advanced automated living space. By this term, we understand a system that not only reads data from sensors but also transmits them. It is also able to recognize specific situations occurring in the room and react to them. One of the main features of an intelligent building is the unification of separate subsystems into one controlled complex [1].

Mobile or fixed communication technologies are used to control modern intelligent home systems. The control center can be connected to the Internet and cloud service, which are provided by providers of equipment or services for “smart homes.” This simplifies the use of the software and interaction with the Smart Home system. All system parameters are managed using a special application or a web interface, where you can turn on or off the devices and set their settings [2].

The purpose of the study is to design a network for an individual smart residential building using equipment from Cisco Systems.

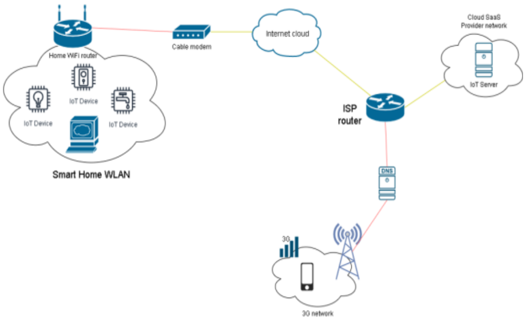


Figure 1: Network topology for the implementation of a “smart house”

2. Statement of Research Problem

2.1. Selection of Network Equipment

In this case, standard equipment (hubs, switches, routers, etc.) is enough to make a physical connection. Interconnection can also

CPITS-2023-II: Cybersecurity Providing in Information and Telecommunication Systems, October 26, 2023, Kyiv, Ukraine
EMAIL: kn.kolbasova152@gmail.com (K. Kolbasova); zhurakovskybiyu@tk.kpi.ua (B. Zhurakovskyi); andr.vadym.2012@gmail.com (V. Poltorak); Nvc2006@i.ua (V. Nakonechnyi); r.kyrychok@kubg.edu.ua (R. Kyrychok)
ORCID: 0009-0007-2261-204X (K. Kolbasova); 0000-0003-3990-5205 (B. Zhurakovskyi); 0000-0001-9231-9411 (V. Poltorak); 0000-0002-0247-5400 (V. Nakonechnyi); 0000-0002-9919-9691 (R. Kyrychok)

apply to remote networks. Then it is necessary to connect these networks using a telephone connection (modem) [3].

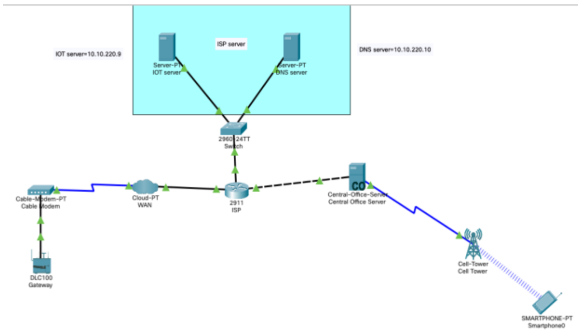


Figure 2: A model of a telecommunications network

2.1.1. Network Router

A router is a network device that connects different computer networks by routing packets from one network to another. The Cisco 2811 was chosen for the model—a 1U router with 2 10/100Mbps ports, 4 HWIC slots, and one slot NM, NME. Typically, this device connects to two or more different networks. When a data packet arrives at a router port, it reads the address information in the packet to determine which port to send the packet to [4].

2.1.2. Network Switch

It is a tool that connects devices on a local network. An Ethernet switch typically operates at the link layer of the OSI model (Layer 2). It controls the flow of data in a network by checking the destination MAC address of an incoming frame and forwarding the frame only to the host for which the message was intended. Each switch has a dynamic table (called a MAC address table) that maps MAC addresses to ports. Using this information, the switch can determine which system is sitting on which port and where to send the received frame [3].

CiscoCatalyst 2960-24TT is used in this work. The switch has 24 Fast Ethernet ports (10/100) and 2 Gigabit Ethernet ports (10/100/1000).

2.1.3. Network Modem

The modem is defined as an abbreviation for modulator-demodulator, a modem is a hardware device that allows a computer to send and receive information over telephone lines or coaxial cables [3].

When sending a signal, the device converts ("modulates") the digital data into an analog signal and transmits it over the phone line. Similarly, when an analog signal is received, the modem converts it back ("demodulates") to a digital signal [5].

A cable modem is a common technology for broadband connection to home networks [6].

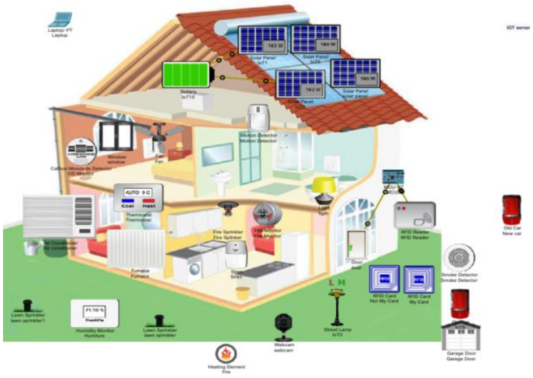


Figure 3: Equipment is necessary for a smart home

2.1.4. Home Gateway

The home gateway is used to assign IP addresses to smart devices and to register smart devices.

This integrated Cisco router features a Dynamic Host Configuration Protocol (DHCP) server [7], Network Address Translation (NAT) and Network Address Port Translation (NAPT), and Stateful Packet Interfacing (SPI) [8]. These features provide a single high-speed public Internet connection and allow users to share files and folders between devices on a home network by connecting multiple wireless devices in an active home to a wireless residential gateway.

Main features:

- Compliant with DOCSIS 3.0, 2.0, 1.1, and 1.0 standards for high performance and reliability.
- Four 10/100/1000BASE-T Ethernet ports for wired connectivity.
- High-performance broadband Internet connection.
- One USB 2.0 Type 2 connection.
- Dual-band 802.11ac simultaneous Wireless Access Point (WAP) with eight Service Set Identifiers (SSIDs), backward compatible with 802.11b/g/n [9].

- Including a push-button switch to activate WPS for a simplified and highly secure wireless network setup.
- Configurations with MoCA 2.0 are available for home networks using existing coaxial cables.

2.1.5. Server

A server is a device or software that receives requests received over the network and provides responses to them. A client is a device that initiates a request and receives a response from the server. In the modern Internet, the term "server" refers to a computer system that processes requests for web pages and sends relevant information to the client [10].

In this project, three servers are needed: the first for DNS, the second for IoT, and the last one for the 3G/4G provider [11].

2.1.6. Cloud

A cloud network or cloud-based network is when some or all of an organization's network resources are hosted in the cloud. This can be a public cloud or a private cloud. This abstract "cloud" of computers provides vast distributed storage and computing power that can be accessed by any Internet-connected device with a web browser [3].

2.1.7. Cellular Tower

A cell tower is a tall tower equipped with electronics along with an antenna that transmits data to cell phones. Cell towers are clustered in geographic locations where population density is high and there is likely to be a large number of cell phone users. This helps avoid saturation of available capacity, which can lead to busy signals and unhappy customers. Cell phones are designed to be aware of the nearest tower. This is displayed to the user in the form of signal strength, which represents the strength of the connection between the user's location and the nearest tower that provides the service.

For this project, the 3G/4G client will be connected to this cell tower; the tower itself will be connected to the Internet through a server.

2.1.8. Access Control System

RFID is an automatic identification technology that uses radio waves to capture data from tags. One of the main advantages of the RFID system is that the tag does not have to be in the line of sight for the reader to read the data stored in it, and several tags can be read simultaneously [12, 13].

2.2. Design Methodology

The network topology used to realize a smart home consists of four parts: a smart home, an Internet cloud, an IoT server, and a 3G network [14–16].

In the first part, we have a home network with various IoT devices connected to a home gateway (a home Wi-Fi router in the topology).

The second part of the network is the Internet Cloud (WAN), which is connected to the home Wi-Fi router via a cable modem to provide Internet connectivity for IoT devices [17].

The third part is about the IoT (Internet of Things) server, which registers all the devices connected to it to provide more IoT features [18].

Then comes the last part of the "3G Network" topology, the smartphone connects to a cell tower to connect to the Internet for remote device access [19].

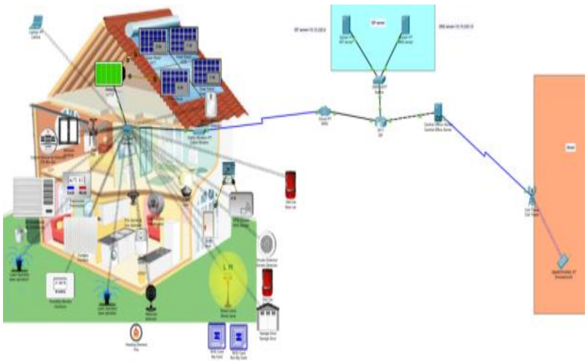


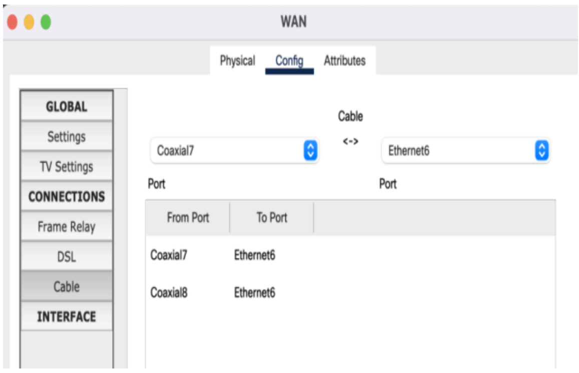
Figure 4: Equipment is necessary for a smart home

2.3. Network Configuration

We need to configure configurations for all devices to ensure proper communication between home devices and servers [20]. And provide the customer with 3G/4G access to the home.

IoT cloud (WAN)

To provide Internet access for all sections, a cloud is required, which performs the functions of cable forwarding, from the Coax8 port to the Ethernet6 port and from the Coax7 port to the Ethernet6 port. (Fig. 5) The WAN is used to transmit data collected by smart devices from the home to the IoT server for storage. Smart devices receive an IP address from a home gateway through the cloud [21].



Coaxial7 <-> Ethernet6

From Port	To Port
Coaxial7	Ethernet6
Coaxial8	Ethernet6

Figure 5: WAN Configuration tab

An Internet Service Provider (ISP) router is used to connect all network interfaces, and a DHCP server is configured on it to dynamically assign an IP address to each connected device, whether it is a "smart" device or not, to simulate a connection to the Internet [22].

ISP router configuration is performed using the Cisco Packet Tracer command-line interface. Configuration consists of assigning a hostname and setting an IP address.

Assigning a hostname and IP address to the ISP router:

```
    Router>
Router>enable
Router#conf terminal
Router(config)#hostname ISP
    ISP(config)#intgigabitEthernet0/2
ISP(config-if)#ip address 10.10.220.1
255.255.255.0 ISP(config-if)#no
shutdown

    ISP(config)#intgigabitEthernet0/0
ISP(config-if)#ip address
209.165.200.225 255.255.255.224
ISP(config-if)#no shutdown
ISP(config)#intgigabitEthernet0/1
ISP(config-if)#ip address
209.165.201.225 255.255.255.224

    ISP(config-if)#no shutdown
```

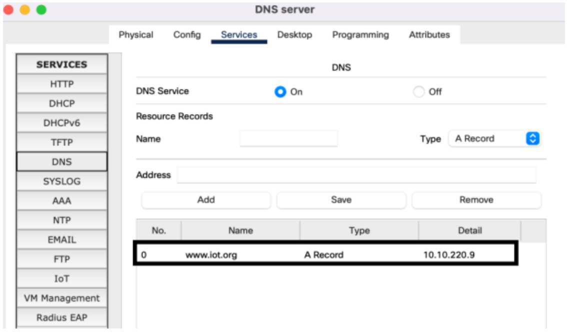
Configuring DHCP Server for Cellular and IOE Device:

```
    ISP(config)#ipdhcp excluded-
address 209.165.201.225
209.165.201.230
SP(config)#ipdhcp pool cell
ISP(dhcp-config)#network
209.165.201.225 255.255.255.224
ISP(dhcp-config)#default-router
209.165.201.225
ISP(dhcp-config)#dns-server
10.10.220.10

    ISP(config)#ipdhcp excluded-
address 209.165.200.225
209.165.200.230
ISP(config)#ipdhcp pool ioe
ISP(dhcp-config)#network
209.165.200.224 255.255.255.224
ISP(dhcp-config)#default-router
209.165.200.225
ISP(dhcp-config)#dns-server
10.10.220.10
```

DNS server

The DNS server is used to allow the user to remotely access the Internet of Things server, not by IP address [23], but by using the domain name of the DNS server, i.e. "iot.org", as shown in Fig. 6. It is important to configure the DNS server with a static IP address as shown in Fig. 7.



DNS Service ● On ○ Off

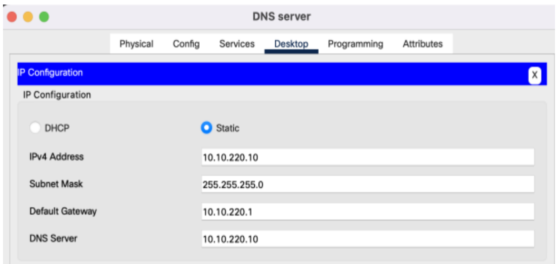
Resource Records

Name: Type: A Record

Address:

No.	Name	Type	Detail
0	www.iot.org	A Record	10.10.220.9

Figure 6: Domain name configuration



IP Configuration

○ DHCP ● Static

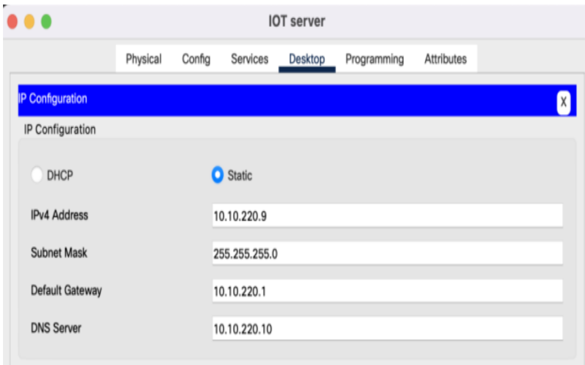
IPv4 Address	10.10.220.10
Subnet Mask	255.255.255.0
Default Gateway	10.10.220.1
DNS Server	10.10.220.10

Figure 7: The IP address for the DNS server

An IoT server is used to remotely connect IoT devices to it to access it through a web interface using a computer or smartphone. In general, all smart objects registered on the IoT server can be remotely controlled through a web interface hosted on the IoT server [24].

The IoT server is configured with a static IP address so that all smart devices can connect to it using the same IP address. Fig. 8 shows the IP address configuration using Static.

Devices can be accessed using a username and password already created on the IoT server, so when registering devices, you must specify the same username and password along with the IP address of the IoT server.



IP Configuration

○ DHCP ● Static

IPv4 Address 10.10.220.9

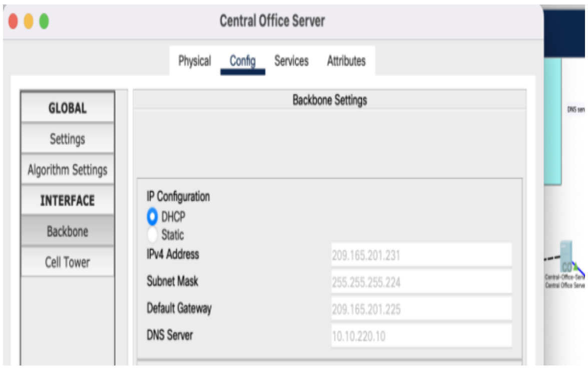
Subnet Mask 255.255.255.0

Default Gateway 10.10.220.1

DNS Server 10.10.220.10

Figure 8: The IP address for the IoT server

The central office server is used to connect the cell tower to the router of the provider and vice versa to transfer information between them. After configuring the DHCP server and DNS server on the ISP router, the central office server automatically receives all IP information from the ISP [25], as shown in Fig. 9.



IP Configuration

● DHCP ○ Static

IPv4 Address 209.165.201.231

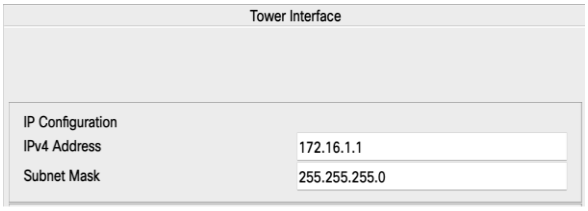
Subnet Mask 255.255.255.224

Default Gateway 209.165.201.225

DNS Server 10.10.220.10

Figure 9: Central Office Server

Cell towers are used to provide cellular coverage for a homeowner to access and control a home appliance remotely.



IP Configuration

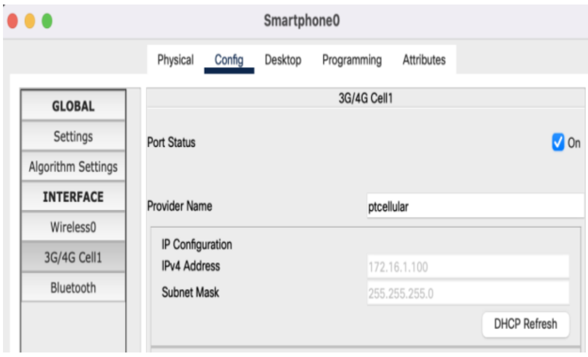
IPv4 Address 172.16.1.1

Subnet Mask 255.255.255.0

Figure 10: Cell tower configuration

A smartphone is used to remotely access the smart object through a web interface using the URL www.iot.org with an Internet connection [26].

To connect the smartphone to the 3G cell tower, let's set the correct APN (access point name) "cell" in the smartphone, as shown in Fig. 11.



Port Status ☑ On

Provider Name ptcellular

IP Configuration

IPv4 Address 172.16.1.100

Subnet Mask 255.255.255.0

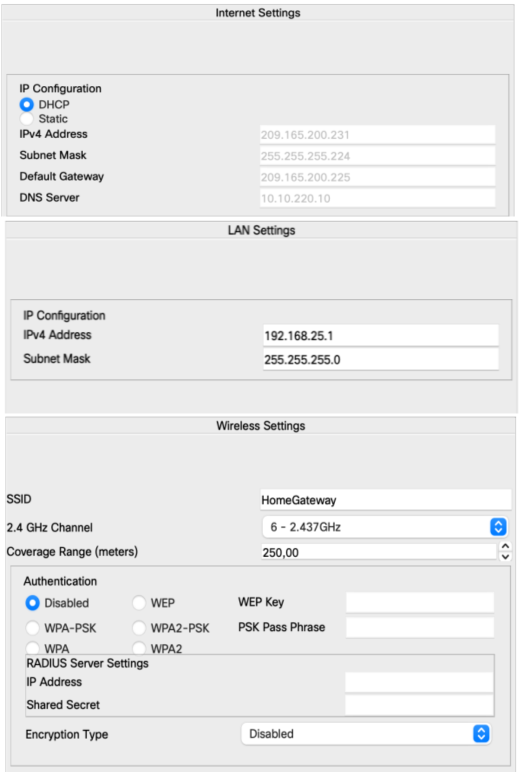
Figure 11: Connecting a smartphone to a cellular tower

The home gateway is used to assign IP addresses to smart devices and to register smart devices. The home gateway automatically obtains an IP address from the ISP router after establishing a connection to the cloud WAN. In addition, all smart objects connected to the home gateway automatically obtain an IP address from the ISP router via the cloud (WAN). A cable modem is used to connect the home gateway to the cloud. Home Gateway provides different programming environments for devices: JavaScript, Python, and Visual Basic.

The home gateway has four Ethernet ports and a wireless access point with the SSID of the home gateway. We can configure WEP/WPA—PSK/WPA2 protocols to authenticate the wireless connection [27].

To connect the devices to the home gateway, you need to select wireless as the devices will be connected using a wireless connection, and then specify the SSID of the home gateway in the devices [28].

The home gateway has three interfaces: the Internet, a local network, and a wireless interface (Fig. 12).



Internet Settings

IP Configuration
● DHCP
○ Static
IPv4 Address: 209.165.200.231
Subnet Mask: 255.255.255.224
Default Gateway: 209.165.200.225
DNS Server: 10.10.220.10

LAN Settings

IP Configuration
IPv4 Address: 192.168.25.1
Subnet Mask: 255.255.255.0

Wireless Settings

SSID: HomeGateway
2.4 GHz Channel: 6 - 2.437GHz
Coverage Range (meters): 250,00

Authentication
● Disabled ○ WEP ○ WPA-PSK ○ WPA2-PSK ○ WPA ○ WPA2
WEP Key:
PSK Pass Phrase:
RADIUS Server Settings
IP Address:
Shared Secret:
Encryption Type: Disabled

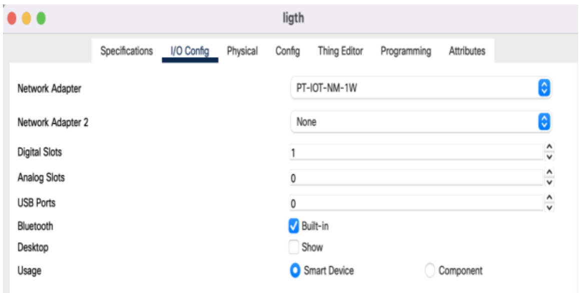
Figure 12: Internet, local network, and wireless interface

2.4. Configuring IoT Devices

Wireless interface

By default, IoT devices in Cisco Packet Tracer have an Ethernet network adapter that needs a cable to connect to the home gateway, so you need to change the network adapter for all devices to allow them to connect via the wireless interface [29]. For this you need:

1. Open the extended list of device tabs (Fig. 13).
2. Go to the “I/O Config” tab.
3. Any device can support two network cards. For the network adapter, select “PT-IOT-NM-1W” [30].

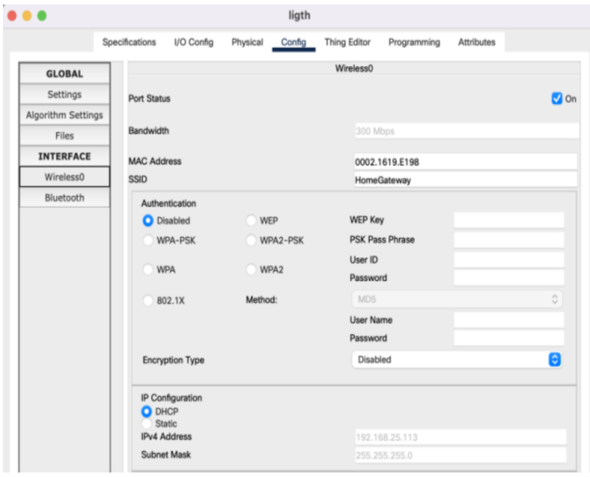


Network Adapter: PT-IOT-NM-1W
Network Adapter 2: None
Digital Slots: 1
Analog Slots: 0
USB Ports: 0
Bluetooth: ☑ Built-in
Desktop: □ Show
Usage: ● Smart Device ○ Component

Figure 13: IoT device I/O Config tab

Connecting devices to the Internet

After entering “HomeGateway” in the SSID field of the Wireless0 interface on the “Config” tab, the interface is connected to the home gateway (Fig. 14). The home gateway acts as a DHCP server; thus, any device must have an IP address in the range “192.168.3.2” to “192.168.3.254” because “192.168.3.1” is the gateway address.



Wireless0

Port Status: ☑ On
Bandwidth: 300 Mbps
MAC Address: 0002.1619.E198
SSID: HomeGateway

Authentication
● Disabled ○ WEP ○ WPA-PSK ○ WPA2-PSK ○ WPA ○ WPA2 ○ 802.1X
WEP Key:
PSK Pass Phrase:
User ID:
Password:
Method: MD5
User Name:
Password:
Encryption Type: Disabled

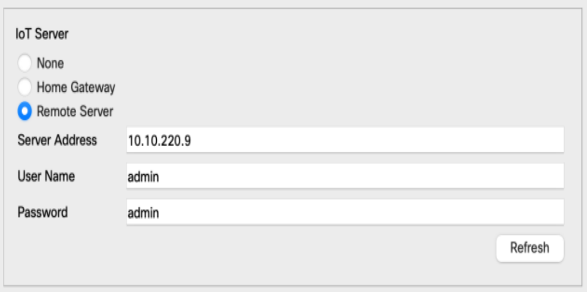
IP Configuration
● DHCP
○ Static
IPv4 Address: 192.168.25.113
Subnet Mask: 255.255.255.0

Figure 14: “Config” tab

Devices will automatically receive default gateway and DNS server addresses. Finally, if any device is connected to the home gateway and receives an IP address, it will be connected to the Internet.

Registration server

To register a device with a server, you need the server address, username, and password. All devices must use the same IoT credentials [31], the same credentials were also used by the homeowner to authenticate when connecting through a browser to the IoT server [32].



IoT Server
○ None
○ Home Gateway
● Remote Server
Server Address: 10.10.220.9
User Name: admin
Password: admin

Figure 15: IoT server field on the Config tab of the device

As mentioned earlier, this home can be controlled in two ways: from a laptop at home for local monitoring or from a 3G/4G smartphone away from home [33].

2.5. Interaction Between Devices

Doors: To control the security and lighting system at the entrance using RFID, some conditions must be set on the IoT *server.*

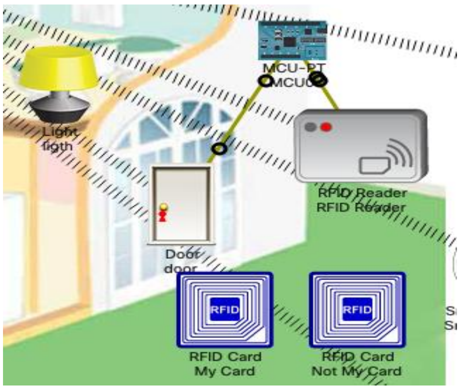


Figure 16: Security system and door lighting

The system works according to the following scenario [34]:

- Card authorization: If ID = 1001 then RFID is available, otherwise not available.
- Door opening: If RFID is available, the door is unlocked and opened, otherwise it is locked.
- Turning on the light: if the door is opened, the light turns on.

Climate control

An air conditioner and a heater are used to maintain a comfortable temperature in the room. The temperature is controlled by the thermostat (Fig. 17).

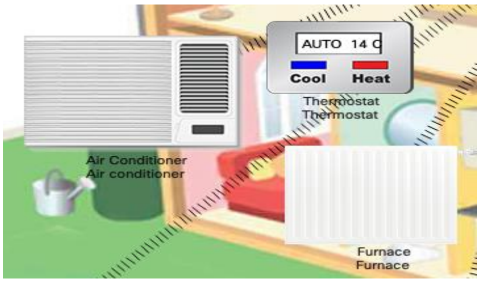


Figure 17: Climate control system

Climate control scenario:

- Cooling: If the thermostat registers a temperature greater than or equal to 23 degrees, the air conditioner is turned on. Otherwise disabled.
- Heating: If the thermostat registers a temperature less than or equal to 10 degrees, the heater is turned on. Otherwise disabled.
- At temperatures between the above, both devices are turned off.

The carbon monoxide control system in the room

CO Alarm is used as an alarm and a sensor at the same time, the alarm will turn on if the carbon monoxide in the room exceeds 20%. The CO alarm in the package tracking system is programmed to activate by default when it detects a carbon monoxide level of 20%. To automate this part, you need to set the following conditions on the IoT server conditions tab:

- The first condition is to open the window and start the fan in the Low state when the CO level is between 20% and 25%.
- When the CO level exceeds 25%, a second condition is set to switch the fan to high and keep the window open.
- The third condition works when the CO level is below 2%; he closes the window and turns off the fan. If these conditions are disabled, the window can be opened manually.

Self-watering in the garden

Sprinklers and a humidity controller are used for the automatic watering system (Fig. 18).

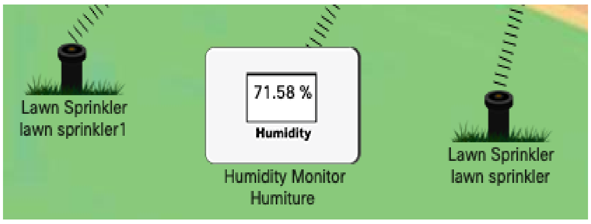


Figure 18: Self-watering in the garden

A lawn sprinkler raises the water level every time it is turned on. The water level monitor receives the water level in the environment and prints it. To automate this part, you should add some conditions on the IoT server:

- The first condition turn off the sprinklers if the level measured by the water level monitor exceeds 55%.
- The second condition turn on the sprinklers if the water level drops less than 30%. Of course, the garden will not be watered all day, for this condition you can turn it off whenever you want. We can do manual watering from the IoT server account.

Fire monitoring of the kitchen

A siren, sprinkler, and fire monitor are used for fire alarm and watering (Fig. 19).

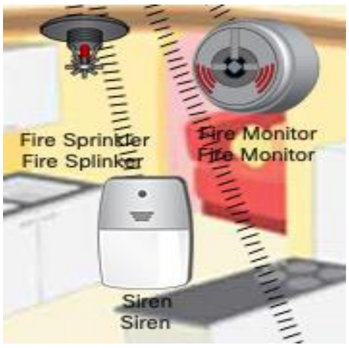


Figure 19: Fire monitoring

The following conditions must be added:

- A condition to activate the sprinkler and siren if the fire alarm detects a fire in the kitchen.
- Condition for stopping the sprinkler and siren if there is no fire in the kitchen.

Monitoring of exhaust gases in the garage

When starting the car in the garage, it is necessary to control the content of exhaust gases. A smoke detector is used for this. (Fig. 20)

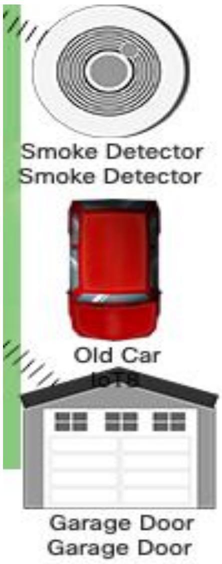
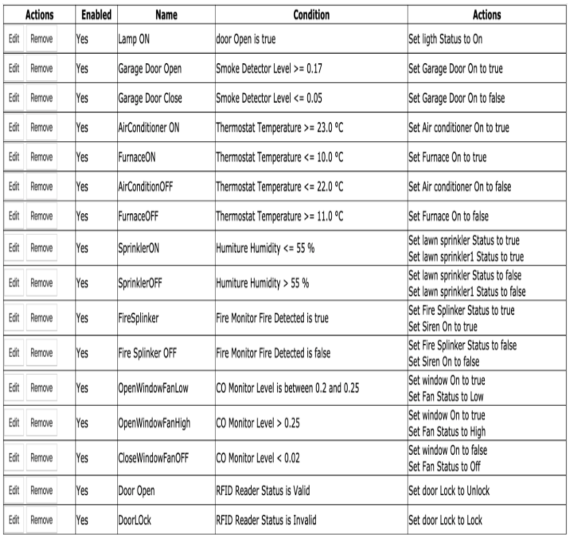


Figure 20: Smoke monitoring in the garage

To automatically open the garage door, you must add the following conditions:

- If the smoke detector detects a smoke level greater than or equal to 0.17, then the gate in the garage opens.
- If the smoke level is less than 0.05, the door is closed.

All scenarios are registered on the IoT server conditions tab (Fig. 21).



Actions		Enabled	Name	Condition	Actions
Edit	Remove	Yes	Lamp ON	door Open is true	Set ligth Status to On
Edit	Remove	Yes	Garage Door Open	Smoke Detector Level >= 0.17	Set Garage Door On to true
Edit	Remove	Yes	Garage Door Close	Smoke Detector Level <= 0.05	Set Garage Door On to false
Edit	Remove	Yes	AirConditioner ON	Thermostat Temperature >= 23.0 °C	Set Air conditioner On to true
Edit	Remove	Yes	FurnaceON	Thermostat Temperature <= 10.0 °C	Set Furnace On to true
Edit	Remove	Yes	AirConditionOFF	Thermostat Temperature <= 22.0 °C	Set Air conditioner On to false
Edit	Remove	Yes	FurnaceOFF	Thermostat Temperature >= 11.0 °C	Set Furnace On to false
Edit	Remove	Yes	SprinklerON	Humiture Humidity <= 55 %	Set lawn sprinkler Status to true Set lawn sprinkler1 Status to true
Edit	Remove	Yes	SprinklerOFF	Humiture Humidity > 55 %	Set lawn sprinkler Status to false Set lawn sprinkler1 Status to false
Edit	Remove	Yes	FireSplinker	Fire Monitor Fire Detected is true	Set Fire Splinker Status to true Set Siren On to true
Edit	Remove	Yes	Fire Splinker OFF	Fire Monitor Fire Detected is false	Set Fire Splinker Status to false Set Siren On to false
Edit	Remove	Yes	OpenWindowFanLow	CO Monitor Level is between 0.2 and 0.25	Set window On to true Set Fan Status to Low
Edit	Remove	Yes	OpenWindowFanHigh	CO Monitor Level > 0.25	Set window On to true Set Fan Status to High
Edit	Remove	Yes	CloseWindowFanOFF	CO Monitor Level < 0.02	Set window On to false Set Fan Status to Off
Edit	Remove	Yes	Door Open	RFID Reader Status is Valid	Set door Lock to Unlock
Edit	Remove	Yes	DoorLOck	RFID Reader Status is Invalid	Set door Lock to Lock

Figure 21: Device interaction scenarios on the IoT server conditions tab

2.6. Environmental Variables

Variables are adjustable parameters to represent real-life conditions, such as the amount of sunlight, temperature, carbon dioxide and monoxide concentrations in the air, water levels, and more. Cisco Packet Tracer has over fifty different variables that can be adjusted accordingly based on a 24-hour time range. Fig. 22 below shows the amount of sunlight and smoke throughout the day.

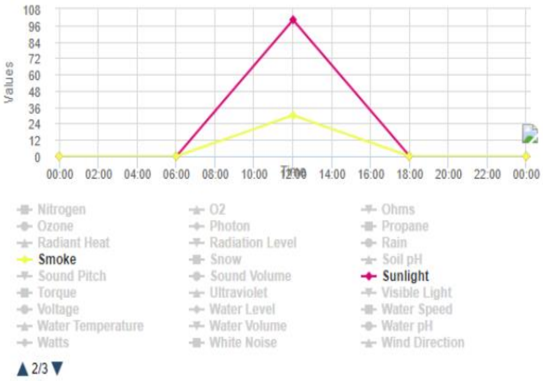


Figure 22: An example of setting an environment variable

Variables are needed to influence sensor behavior in IoT simulations. Variables are detected by the sensor and, as a result, actions are triggered. Regulated variables also helped to quickly test IoT logic settings.

The following variables were used in this simulation:

- Carbon monoxide level to know the CO level in the room so that the windows are opened automatically. For this part, you can also use an old car to generate CO in the environment.

- The ambient temperature level was used during a random time of day to activate the room temperature sensor.
- Water level used by garden water lever monitor to detect excess water level and stop lawn sprinklers.

2.7. IoT Device Automation Testing

Door

For this part, the security of the door is checked using two cards (My Card) and (Not My Card). Three scenarios were created, which are described below:

Scenario 1: An authorized card (My Card) is held close to the RFID reader to check what is happening with the door. In this case, the door is unlocked to allow the person to enter the house, and then the door is closed again. When the door is opened, the light inside turns on. So, the first test is successful.

Scenario 2: In this case, an unauthorized card (by an unknown person) is presented to the RFID reader to check what is happening to the door. The door is still locked. Thus, the second scenario is confirmed.

Scenario 3: In this case, no card is near the RFID reader. The RFID reader is in a “standby” state and the door will not unlock. So, the third door test was successful.

Automatic CO monitoring

There are two ways to control the CO level in the environment: by changing its values in the environment tab, like for sunlight, or by using an old car (if it’s on, the CO level goes up).

Indoor CO monitoring system:

Scenario 1: An old car is inserted and turned on (can be activated by ALT+click); thus increasing the CO level. The IoT server can monitor the CO level. When the CO level is above 20% but below 25%, the window opens and the fan runs at low speed.

Scenario 2: The window and fan are not enough to remove all the CO from the room because the CO level is still rising, so they will stay on until the machine is turned off. If the CO level exceeds 25%, the fan starts to work faster.

Scenario 2: The windows and fan will remain on until the CO level drops below 2%, then the window closes and the fan turns off. So, this test is successfully verified.

Automatic smoke monitoring in the garage

Scenario 1: An old car is inserted and turned on (can be activated by ALT+click); thus increasing the smoke level. When the smoke level exceeds 0.17, the garage door opens.

Scenario 2: The gate will remain open until the machine is turned off and the smoke level drops to 0.05, then the gate closes. So, this test is successfully verified.

Automatic temperature control

It consists of two systems: a room cooling system and a room heating system. Yes, it is necessary to set the appropriate values for the ambient temperature. For the air conditioner, the temperature should be set between 23°C and 30°C.

Whereas for the oven, the temperature should be set in the range from 0°C to 10°C.

Heating system

First, the performance of the heater is tested if the temperature is below 10°C; thus, the time is adjusted around midnight. The temperature monitor is used to display the current temperature.

When the temperature changes over time, we observe the operation of the heater.

- The heater is set to start when the temperature is below 10°C and continues to heat until the temperature reaches 11°C.
- Second, the heater is tested after stopping heating and when the temperature drops below 10°C again, the heater starts heating.

Cooling system

Here, approximately the same test as with the heater is repeated. It’s just that the time the period changes to about noon:

- The air conditioner is set to start when the temperature exceeds 23°C and continue to cool until the temperature drops below 22°C.
- When the air conditioner stops cooling, it starts working again when the temperature exceeds 23°C. The temperature rise test was successful.

Fire control system

Fire is not included in the environment variables. Therefore, objects imitating fire are needed.

This object must have an "IR" property with a value that can be considered a fire. See addition.

We will check the siren and sprinkler in the event of a fire and the opposite case: when a fire is detected in the kitchen, the siren turns on and the sprinkler starts spraying water. Otherwise, the siren and sprinkler are off. So, the fire control system of the kitchen is working.

3. Conclusion

To conduct the study, the necessary devices were selected based on the network topology that was used to implement a smart home. The implementation consists of four parts: a smart home, an Internet cloud, an IoT server, and a 3G network.

The configuration for all devices has been configured. The Cisco Packet Tracer environment helps ensure proper communication between home devices and servers and solves the issue of their interaction.

Based on the simulated scenarios, the automated operation of the devices and their management were configured. Cisco Packet Tracer enables you to modify device functionality by writing your code using JavaScript, Python, and Visual. This allows you to expand the capabilities of device management.

References

[1] B. Zhurakovskyi, et al., Smart House Management System, TCSET 2022: Emerging Networking in the Digital Transformation Age (2023) 268–283. doi:10.1007/978-3-031-24963-1_15.

[2] M. Soliman, et al. Smart Home: Integrating Internet of Things with Web Services and Cloud Computing, IEEE 5th Int. Conf. Cloud Comput. Technol. Sci. (2013). doi:10.1109/CloudCom.2013.155.

[3] Ukrinform, How to Choose the Right Network Equipment (2022). URL: https: //www.ukrinform.ua/rubric-other_news /3395359-ak-pravilno-vibrati-merezne-obladnanna.html

[4] A. Tanenbaum, D. Wetherall. Computer Networks, 5th Edition (2010).

[5] R. Khouchane, S. Rabouhi, Study of the Installation of a Fiber Network Optical.

[6] A. Al-Alawi. Wi-Fi Technology: Future Market Challenges and Opportunities, J. Comput. Sci. 2(1) (2006) 13–18.

[7] M. Yaibuates, R. Chaisricharoen, ICMP based Malicious Attack Identification Method for DHCP, 4th Joint Int. Conf. Info. Commun. Technol. Electron. Electr. Eng. (2014). doi: 10.1109/jictee.2014.6804073.

[8] M. Rouse, Internet of things (IoT), IOT Agenda (2019).

[9] Z. Hu, et al., Development and Operation Analysis of Spectrum Monitoring Subsystem 2.4–2.5 GHz Range, Data-Centric Business and Applications 48 (2020) 675–709. doi: 10.1007/978-3-030-43070-2_29

[10] M. Zennaro, Introduction to the Internet of Things, PhD Telecommunications, The Abdus Salam International Centre for Theoretical Physics Trieste.

[11] A. Elshafee, K. Hamed. 2012 Design and Implementation of a WiFi Based Home Automation System, World Acad. Sci. Eng. Technol. 68 (2012) 2177–2180.

[12] E. Kosmatos, N. Tselikas, A. Boucouvalas Integrating RFIDs and Smart Objects into a Unified Internet of Things Architecture, Adv. Internet Things 1(1) (2011) 5–12. doi: 10.4236/ait.2011.11002.

[13] M. Vladymyrenko, et al., Analysis of Implementation Results of the Distributed Access Control System. in: 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (2019). doi: 10.1109/picst47496.2019.9061376

[14] I. Kuzminykh, et al., Investigation of the IoT Device Lifetime with Secure Data Transmission, Internet of Things, Smart Spaces, and Next Generation Networks and Systems, vol. 11660 (2019) 16–27. doi: 10.1007/978-3-030-30859-9_2

[15] V. Sokolov, et al., Method for Increasing the Various Sources Data Consistency for IoT Sensors, in: IEEE 9th International Conference on Problems of

Infocommunications, Science and Technology (PICST) (2023) 522–526. doi:10.1109/PICST57299.2022.10238518.

[16] Z. Hu, et al., Bandwidth Research of Wireless IoT Switches, in: IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (2020). doi: 10.1109/tcset49122.2020.2354922

[17] A. Rajabzadeh, A. Manashty, Z. Jahromi, A Mobile Application for Smart House Remote Control System, World Acad. Sci. Eng. Technol. 62 (2010) 80–86.

[18] Wonderbit, Internet of Things for Command and Control. URL:https://www.wonderbit.com/en/our-work/ncia-iot-for-c2

[19] Azure, IoT Protocols and Connectivity. URL: https://azure. microsoft.com/en-us/solutions/iot/iot-technology-protocols

[20] M. Moshenchenko, et. al., Optimization Algorithms of Smart City Wireless Sensor Network Control, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3188 (2021) 32–42.

[21] Constrained Application Protocol. URL: https://en.wikipedia.org/wiki/Constrained_Application_Protocol

[22] B. Zhurakovskyi, et al., Calculation of Quality Indicators of the Future Multiservice Network, Future Intent-Based Networking (2022) 197–209. doi: 10.1007/978-3-030-92435-5_11.

[23] S. Obushnyi, et al., Autonomy of Economic Agents in Peer-to-Peer Systems, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3288 (2022) 125–133.

[24] O. Shevchenko, et al., Methods of the Objects Identification and Recognition Research in the Networks with the IoT Concept Support, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 2923 (2021) 277–282.

[25] H.-C. Chao, et al., The Network Topology Based Domain Name Service (1999) 528–533. doi: 10.1109/ICPPW.1999.800111.

[26] B. Zhurakovskyi, et al., Comparative Analysis of Modern Formats of Lossy Audio Compression, International Workshop on Cyber Hygiene, vol. 2654 (2020).

[27] B. Zhurakovskyi, et al., Modifications of the Correlation Method of Face Detection in Biometric Identification Systems, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3288 (2022) 55–63.

[28] MQTT: The Standard for IoT Messaging. URL: https://mqtt.org

[29] Radio-frequency identification. URL: https://en.wikipedia.org/wiki/Radio-frequency_identification

[30] V. Saiko, et al., A Method of Increasing the Reliability of Heterogeneous 5g/Iot Special Communication Networks when Using the Terahertz Wave Range, Information Technology and Implementation, vol. 3384 (2022) 120–131.

[31] B. Zhurakovskyi, et al., Secured Remote Update Protocol in IoT Data Exchange System, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 67–76.

[32] F. Nataliia, et al., Software System for Processing and Visualization of Big Data Arrays, Advances in Computer Science for Engineering and Education (2022). 324–336. doi: 10.1007/978-3-031-04812-8_28.

[33] O. Sihombing, et al., Smart Home Design for Electronic Devices Monitoring Based Wireless Gateway Network Using Cisco Packet Tracer, J. Physics Conf. Series 1007 (2017). doi: 10.1088/1742-6596/1007/1/012021.

[34] A. Mishra, et al., Design and Implementation of Smart Home Network using Cisco Packet Tracer, ITM Web Conf. Int. Conf. Autom. Comput. Commun. 44 (2022) doi: 10.1051/itmconf/20224401008.