2023

IoT Network Project

SMART OFFICE IMPLEMENTATION

MOSTAFA ADEL ALI HASSAN

Faculty of Engineering, Helwan University

Supervised by: Dr Ahmed Badawy

Table of Contents

List of Figures

1. Preface

The advent of the Internet of Things (IoT) has ushered in an era of unprecedented connectivity and intelligence, transforming the way we interact with the world around us. This document serves as a comprehensive review, offering an insightful exploration into the multifaceted realm of IoT. From its fundamental concepts to the intricacies of communication protocols, performance evaluation across diverse topologies, and the critical considerations of energy consumption, this review strives to provide a nuanced understanding of the evolving landscape of IoT.

As we navigate the intricate web of interconnected devices, the need for a thorough examination of IoT becomes increasingly evident. The integration of physical objects into the digital fabric of our lives brings forth not only tremendous opportunities but also formidable challenges. From the architecture of IoT networks to the intricacies of protocols that facilitate seamless communication, each facet requires meticulous scrutiny.

The journey through these pages delves into the essence of IoT, unraveling its significance in various domains such as healthcare, smart cities, and industrial automation. Special attention is given to the pivotal role played by communication protocols, with an in-depth focus on MQTT and HTTPS, illuminating their features, use cases, and impact on the IoT ecosystem.

Moreover, we explore the performance of IoT networks under different topologies and scales, recognizing the importance of adaptability and resilience in the face of a dynamically changing landscape. Energy consumption and optimization in IoT networks emerge as critical considerations, underscoring the need for sustainable practices and innovative solutions to mitigate the environmental impact and enhance the longevity of IoT devices.

This document is not only a testament to the current state of IoT but also a roadmap for the future. It is a collaborative effort to understand, analyze, and anticipate the challenges and opportunities that lie ahead. As technology continues to evolve, so too will the landscape of IoT, and with it, the potential to create a smarter, more connected world.

In the spirit of continuous exploration and advancement, this review invites readers to embark on a journey through the intricacies of IoT, encouraging a deeper comprehension of its nuances and fostering a dialogue that will shape the future of interconnected systems.

2. A Comprehensive Review of Internet of Things (IoT)

2.1 Abstract

The Internet of Things (IoT) has emerged as a transformative paradigm, connecting physical devices, and enabling seamless communication and data exchange. This review paper provides an in-depth exploration of IoT, covering its definition, significance, and key protocols. Special emphasis is placed on widely adopted communication protocols such as MQTT and HTTPS, shedding light on their features, use cases, and implications for IoT ecosystems.

2.2 Introduction

The 21st century has witnessed an unprecedented growth in connectivity and data-driven technologies. Among these, the Internet of Things (IoT) stands out as a revolutionary concept, representing the interconnection of everyday objects to the internet, facilitating intelligent communication and data exchange. This paper aims to delve into the fundamental aspects of IoT, unraveling its implications, challenges, and the role of essential communication protocols.

2.3 Internet of Things (IoT)

IoT refers to the network of interconnected devices, embedded with sensors, actuators, and software, enabling them to collect and exchange data. The essence of IoT lies in its ability to create a smart, responsive environment by connecting physical objects to the digital realm. The applications of IoT are diverse, ranging from smart homes and cities to industrial automation and healthcare.

2.4 Importance of IoT

The importance of IoT is underscored by its transformative impact on various industries. In healthcare, IoT devices monitor patient vitals in real-time, enhancing remote patient care. In smart cities, IoT contributes to efficient energy management and urban planning. The industrial sector benefits from IoT by optimizing processes and predictive maintenance. Overall, IoT fosters innovation, efficiency, and improved decision-making across domains.

2.5 Communication Protocols in IoT

Efficient communication is the cornerstone of a functional IoT ecosystem. Several protocols facilitate the seamless exchange of data between IoT devices and the cloud. Two prominent protocols are MQTT (Message Queuing Telemetry Transport) and HTTPS (Hypertext Transfer Protocol Secure).

- **MQTT:**

MQTT is a lightweight and open-source messaging protocol designed for constrained devices and low-bandwidth, high-latency, or unreliable networks. It operates on a publish/subscribe model, allowing devices to communicate asynchronously. MQTT's minimal overhead and support for Quality of Service (QoS) levels make it ideal for IoT applications, particularly those requiring real-time responsiveness.

- **HTTPS:**

HTTPS, an extension of HTTP with added security features, ensures encrypted communication between devices and servers. While HTTPS is widely used in web applications, its relevance in IoT lies in securing data transmission, safeguarding sensitive information from unauthorized access. This protocol is crucial for IoT applications that prioritize data integrity and confidentiality.

In our smart office implementation, we'll be utilizing the HTTPS protocol.

2.6 Other Noteworthy Protocols

Apart from MQTT and HTTPS, other protocols play vital roles in shaping the IoT landscape. CoAP (Constrained Application Protocol) is tailored for resource-constrained devices, providing a lightweight alternative for communication. AMQP (Advanced Message Queuing Protocol) and CoAP complement MQTT in scenarios demanding diverse communication patterns.

2.7 Challenges and Future Perspectives

Despite the remarkable progress, IoT faces challenges such as security vulnerabilities, interoperability issues, and privacy concerns. Future research should focus on addressing these challenges and exploring emerging technologies like 5G and edge computing to enhance IoT capabilities. Standardization efforts and collaborative initiatives will be pivotal in ensuring a cohesive and secure IoT ecosystem.

2.8 Performance Evaluation of IoT Networks

The performance of IoT networks is a crucial aspect that directly impacts the efficiency and reliability of data exchange. Evaluating the performance across different topologies and scales is essential for optimizing IoT deployments. Several factors such as latency, throughput, and scalability need to be considered.

- **Topology Considerations:**

IoT networks can exhibit diverse topologies, including star, mesh, and hybrid configurations. Each topology has its strengths and weaknesses, influencing factors like data transmission efficiency and network resilience. Evaluating the performance of IoT networks under different topologies helps in tailoring solutions to specific use cases. For instance, a mesh topology might be preferred for its resilience in large-scale deployments, while a star topology could be more suitable for simpler setups.

- **Scale Challenges:**

As IoT networks scale, challenges related to data management, device connectivity, and network congestion become more pronounced. Performance evaluation at various scales helps identify bottlenecks and scalability limitations. It enables the development of robust solutions capable of handling large numbers of devices and sustaining efficient communication.

2.9 Energy Consumption and Optimization in IoT Networks

Energy efficiency is a critical concern in IoT networks, particularly for battery-powered devices that may be deployed in remote or inaccessible locations. Optimizing energy consumption is essential to prolong device lifespan, reduce maintenance costs, and minimize the environmental impact.

- **Power-aware Protocols:**

IoT communication protocols play a significant role in energy optimization. Protocols that minimize the duration and frequency of device wakeups contribute to lower energy consumption. Additionally, adaptive communication strategies, such as adjusting transmission power based on proximity, help strike a balance between connectivity and energy efficiency.

- **Edge Computing and Fog Computing:**

Distributing computational tasks to edge devices or fog nodes closer to the data source can significantly reduce energy consumption. By processing data locally, IoT devices can transmit only relevant information to the cloud, minimizing the need for extensive communication and reducing power requirements.

- **Energy Harvesting:**

Exploring renewable energy sources, such as solar or kinetic energy, for powering IoT devices offers a sustainable approach. Energy harvesting technologies can be integrated into IoT nodes to supplement or replace traditional battery power, ensuring continuous operation in resource-constrained environments.

2.10 Future Directions and Recommendations

In the realm of IoT, continuous research and innovation are paramount. Future directions should focus on developing adaptive algorithms and protocols that dynamically adjust to the changing network conditions, optimizing both performance and energy consumption. Collaborative efforts between academia and industry are essential to address the evolving challenges and pave the way for a sustainable and efficient IoT ecosystem. As IoT networks continue to evolve, the integration of performance evaluation and energy optimization strategies will be pivotal in shaping the future of interconnected systems.

2.11 Conclusion

In conclusion, IoT is a transformative force with far-reaching implications for diverse sectors. The selection of communication protocols is a critical aspect of IoT design, with MQTT and HTTPS standing out as key players. As IoT continues to evolve, addressing challenges and embracing emerging technologies will be essential for realizing its full potential in creating a connected and intelligent world.

3. Experiment Goal

3.1 Introduction

In the pursuit of creating an efficient and secure smart office environment, we'll attempt to leverage our expertise in IoT and networking to simulate a robust network infrastructure using Cisco Packet Tracer. This simulation encapsulates four main rooms – the *Admin office*, *Office 1*, *Office 2*, and *Office 3* – each with its distinct subnet, fostering an isolated network for enhanced security and management.

3.2 Network Architecture

The network architecture is structured with attention to subnetting, using the IP address range **192.168.1.0/26** with two subnet bits. The *Admin office*, *Office 1*, *Office 2*, and *Office 3* are allocated distinct subnets, namely **192.168.1.0/26**, **192.168.1.64/26**, **192.168.1.128/26**, and **192.168.1.192/26**, respectively. These subnets are interconnected to a router through dedicated switches, ensuring efficient communication within each office.

The IT room, housing critical infrastructure components, is connected to a separate interface on the router. This room features a *PC* and a *server*, with the network IP assigned as **1.1.1.0/29**. The segregation of the IT room enhances network security and management.

3.3 Device Interaction and Security Measures

A key aspect of the simulation is the incorporation of IoT devices in each main room. These devices interact seamlessly based on predefined scenarios, contributing to an intelligent and responsive office environment. All communications between devices and the server are established through the secure **HTTPS** protocol.

To ensure data integrity and privacy, each main room is assigned unique usernames and passwords, facilitating access control. Moreover, strict security measures have been implemented to restrict packet flow between different offices. This deliberate isolation empowers users to exclusively control their respective room's devices, mitigating any unauthorized access or interference.

3.4 Future Discussions

In subsequent sections of this document, we will delve into specific scenarios illustrating the dynamic interactions among IoT devices within each office. From lighting control to environmental monitoring, the simulation showcases the practical application of IoT in optimizing office functionalities.

Additionally, we will explore the server-client architecture, emphasizing the significance of HTTPS protocol in securing data transmissions. The distinct usernames and passwords allocated to each room will be detailed, outlining the robust access control mechanisms implemented to fortify the smart office network.

In conclusion, this simulation stands as a testament to the integration of cutting-edge technologies in designing a smart office network that prioritizes efficiency, security, and user control. The subsequent sections will unravel the intricacies of the implemented scenarios, shedding light on the transformative potential of IoT in shaping the future of office environments.

4. Simulation

4.1 Design

- **Whole Topology:**

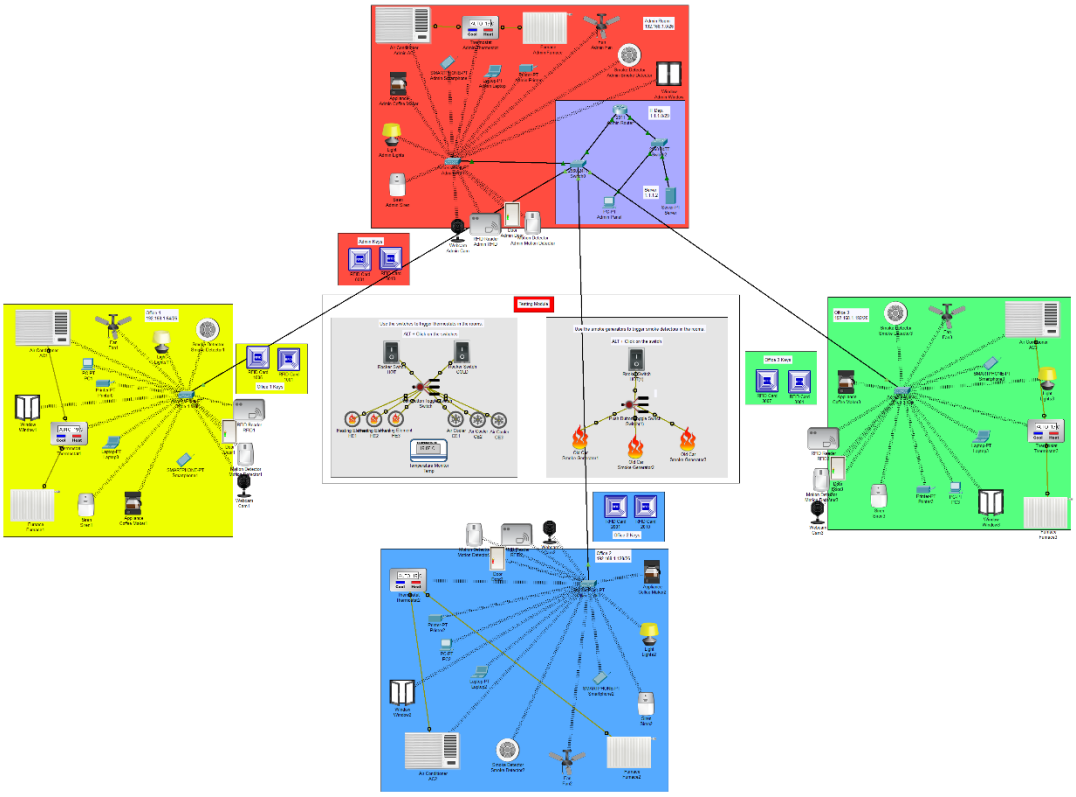


Figure 1 Whole Topology

- **Admin Office:**

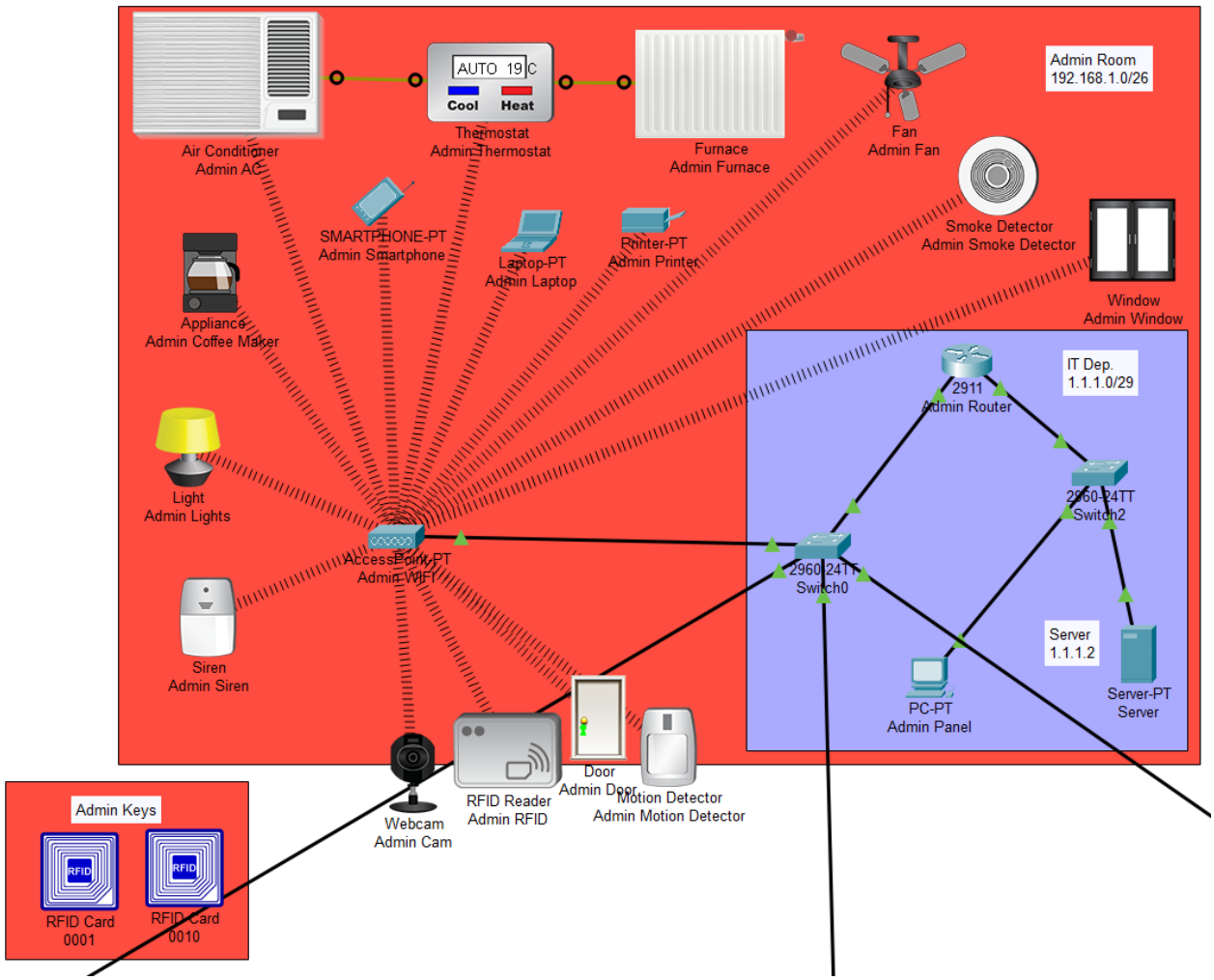


Figure 2 Admin Office

- **Office 1:**

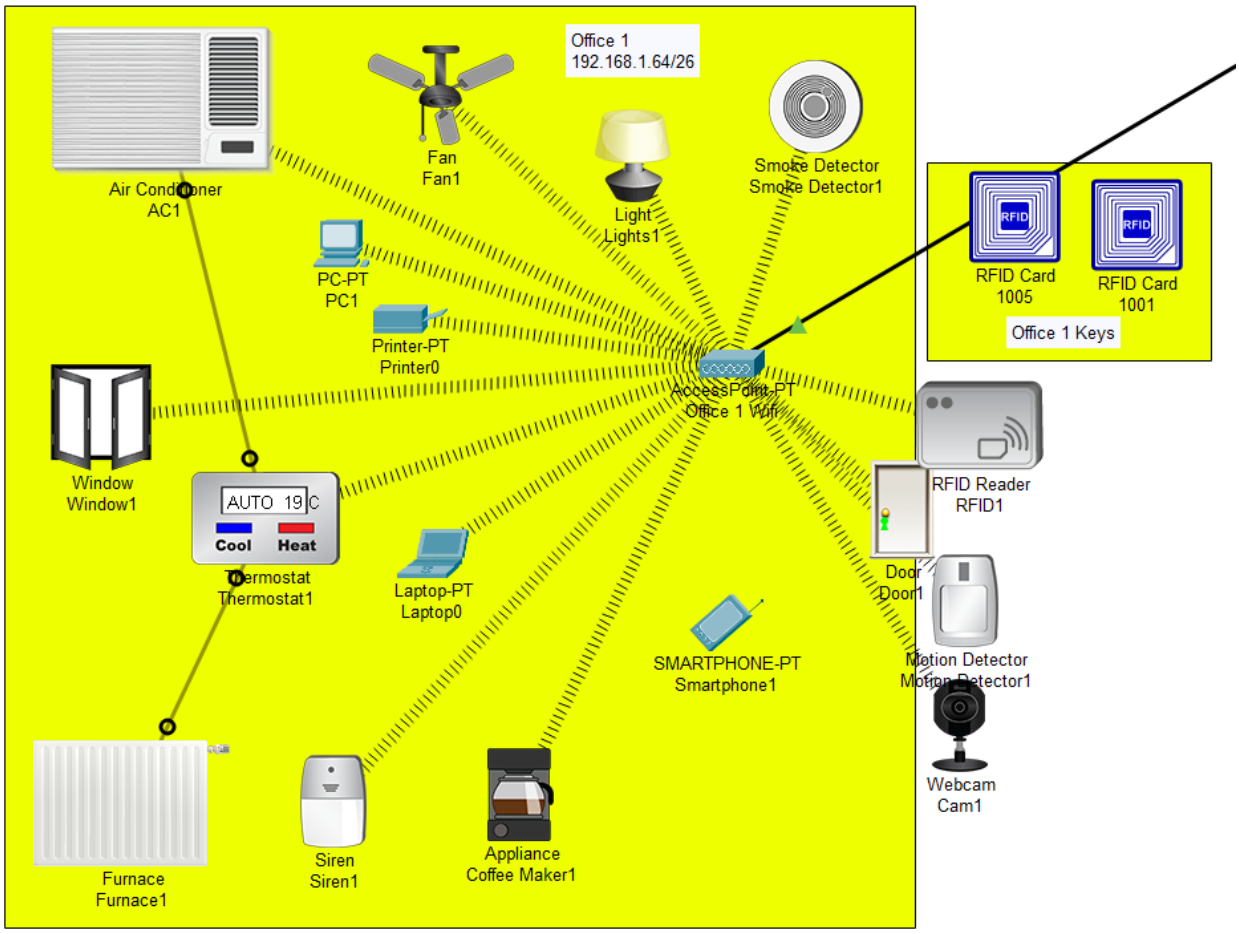


Figure 3 Office 1

- **Office 2:**

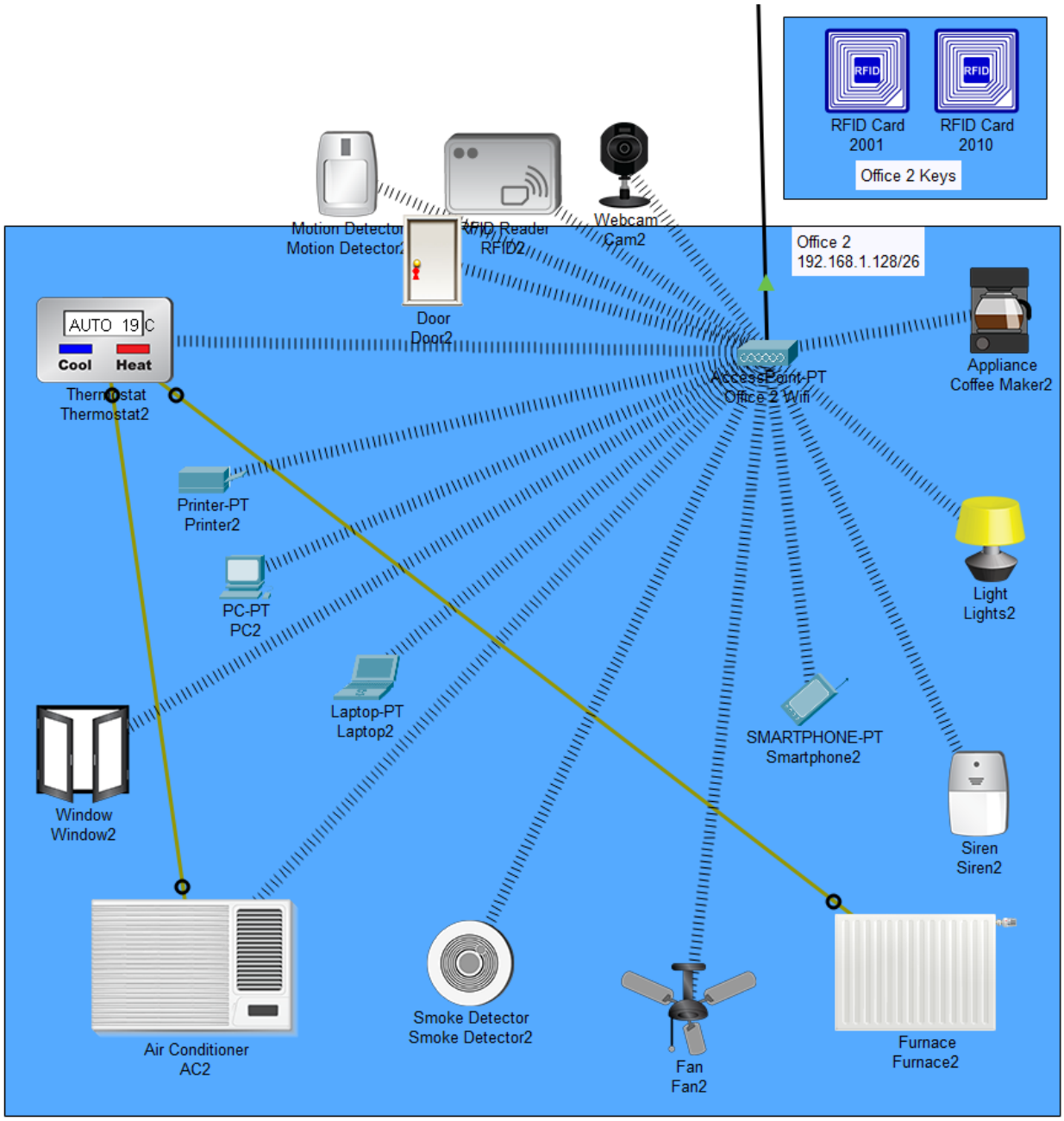


Figure 4 Office 2

- **Office 3:**

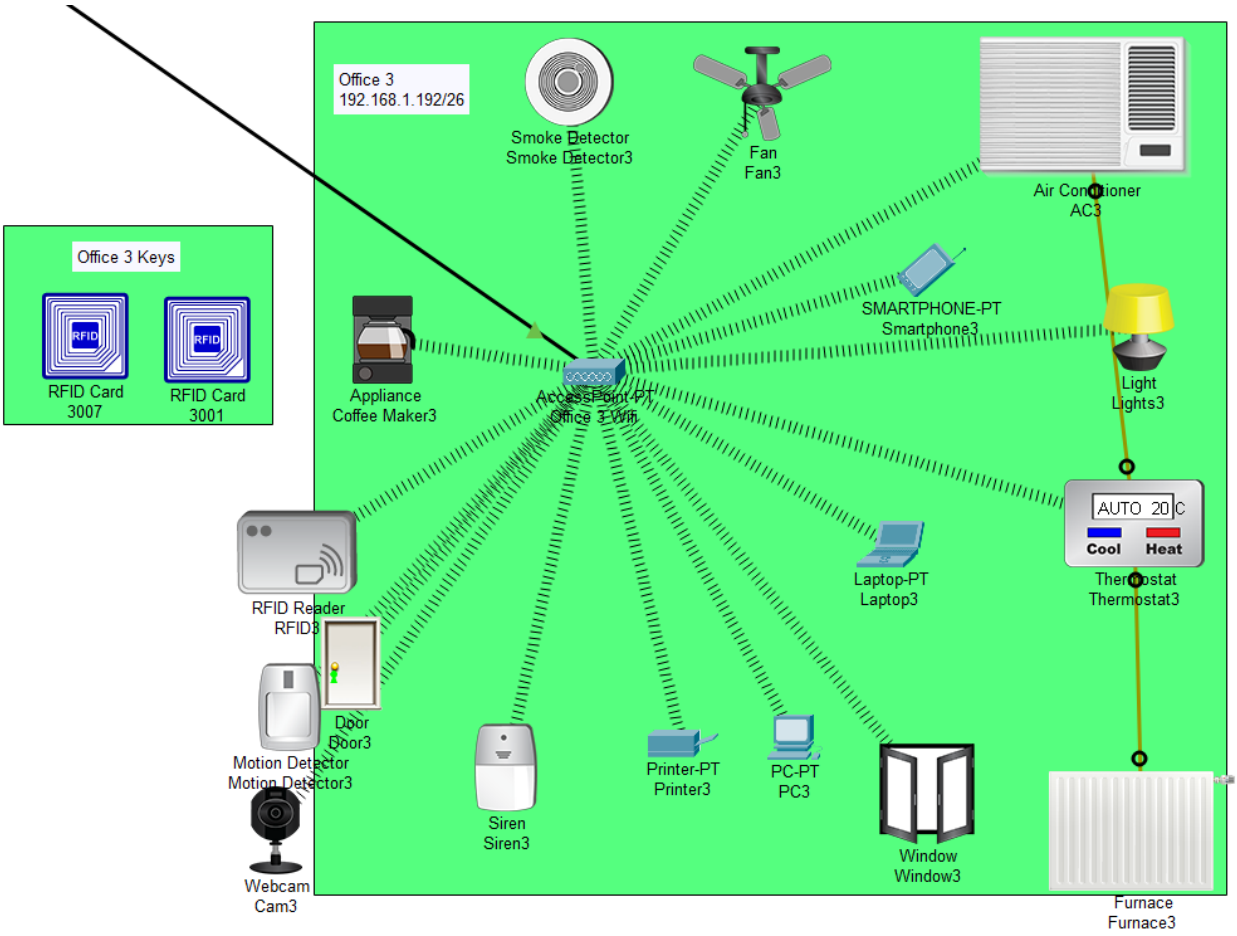


Figure 5 Office 3

- **Testing Module:**

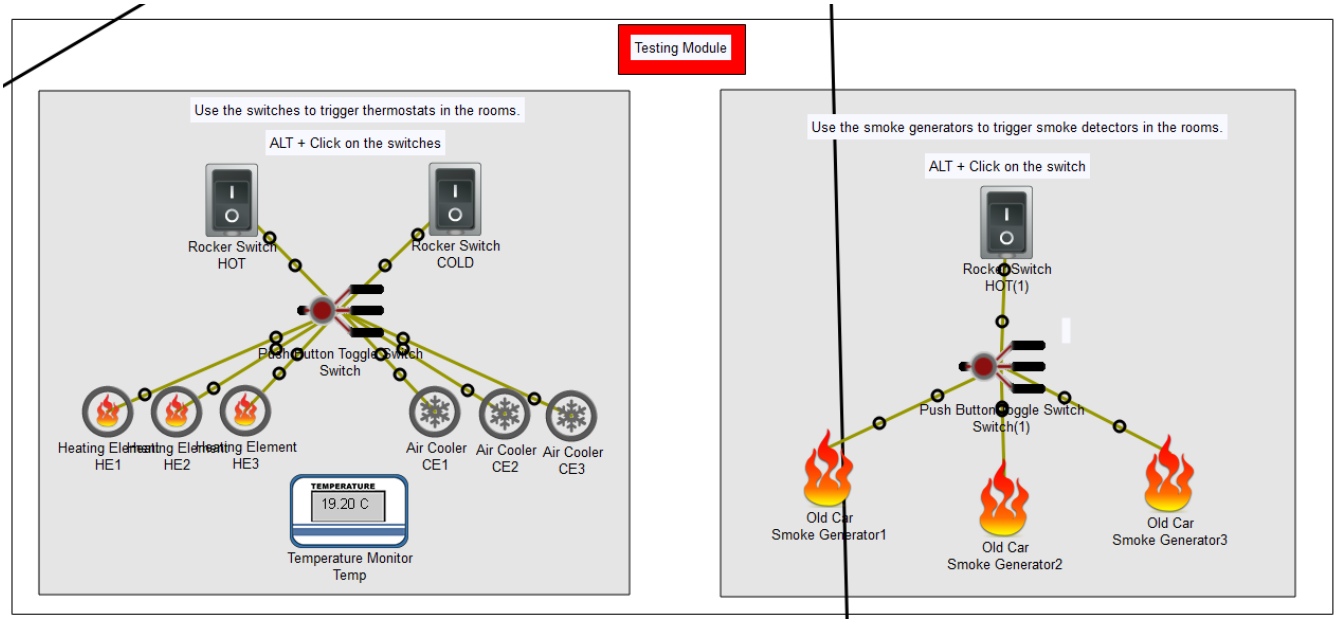


Figure 6 Testing Module

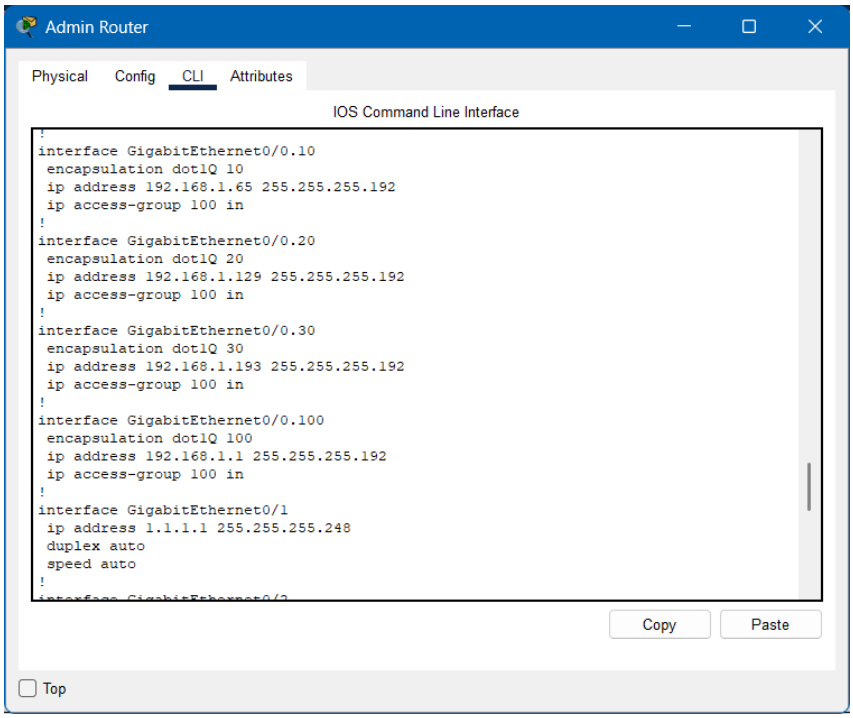
4.2 Configuration

1. Router Configuration:

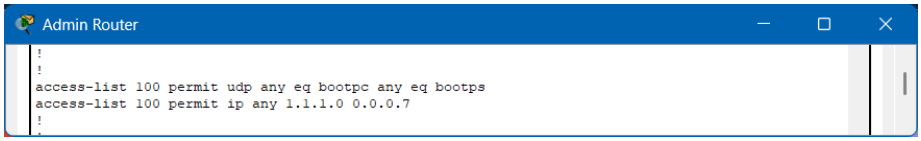
- **Interfaces**

Each office is assigned a sub interface **Gig0/0.x** for its **VLAN** with **192.168.1.0/26**.

The IT room is interfaced on **Gig0/1** with **1.1.1.0/29**.

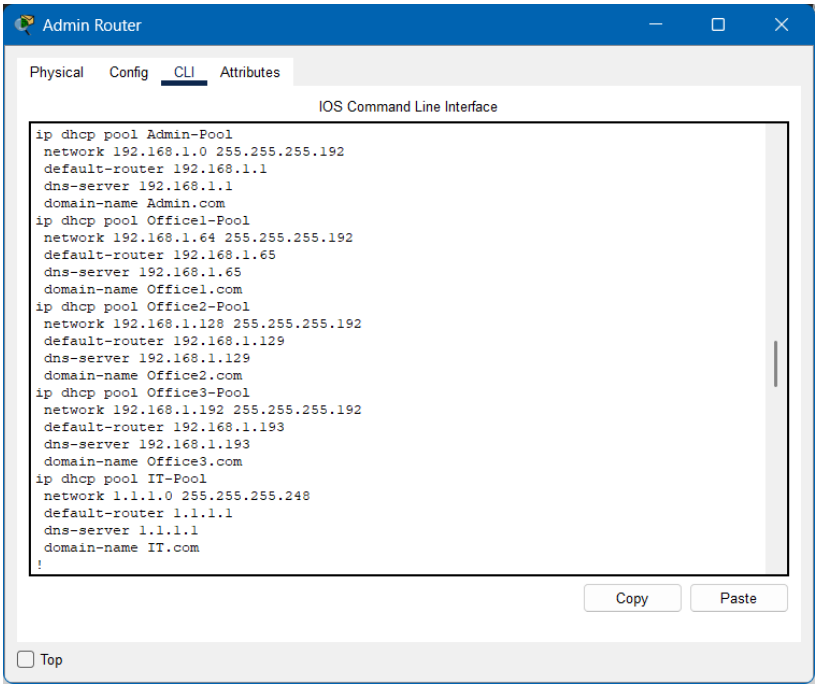


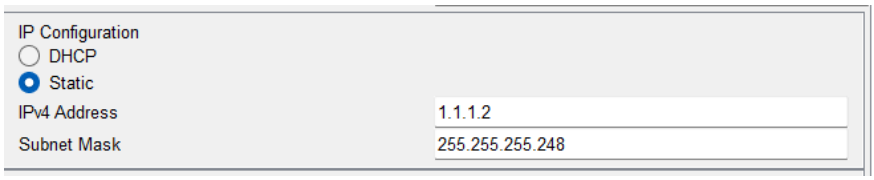
All office sub-interfaces are assigned an extended **Access Control List (ACL)** to limit their access outside of their own network to only the server's network so no user can control another office's devices.



- **DHCP**

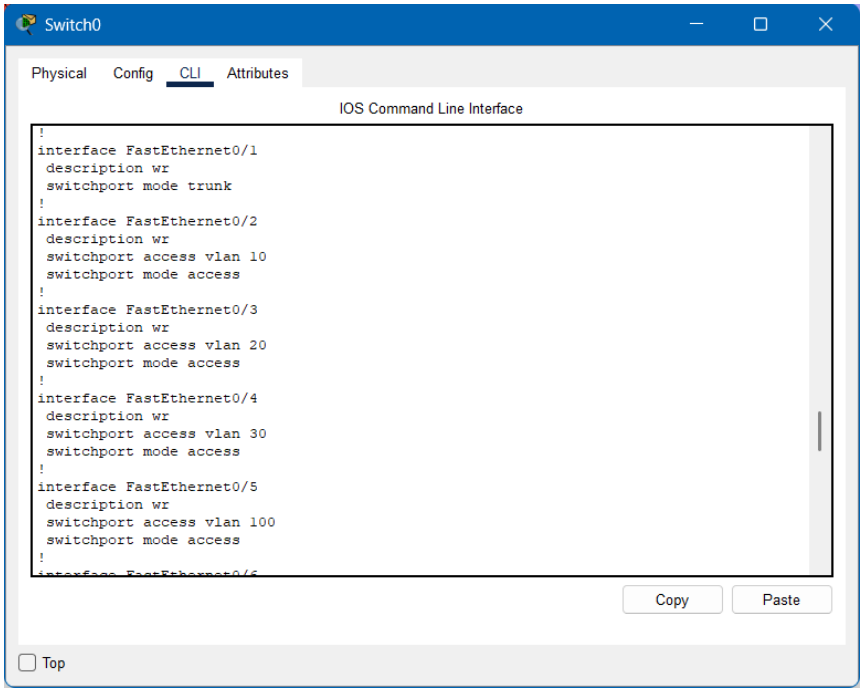
All rooms are assigned their own **DHCP pool** for *dynamic* Ip addressing.
The server is the only host assigned a *static* Ip address of **1.1.1.2**.





2. Switch Configuration:

The switch connecting the offices with the router has its **Fa0/1** port mode set to *trunk* and connected to the router, while its **Fa0/2-5** assigned the appropriate **VLANs**.

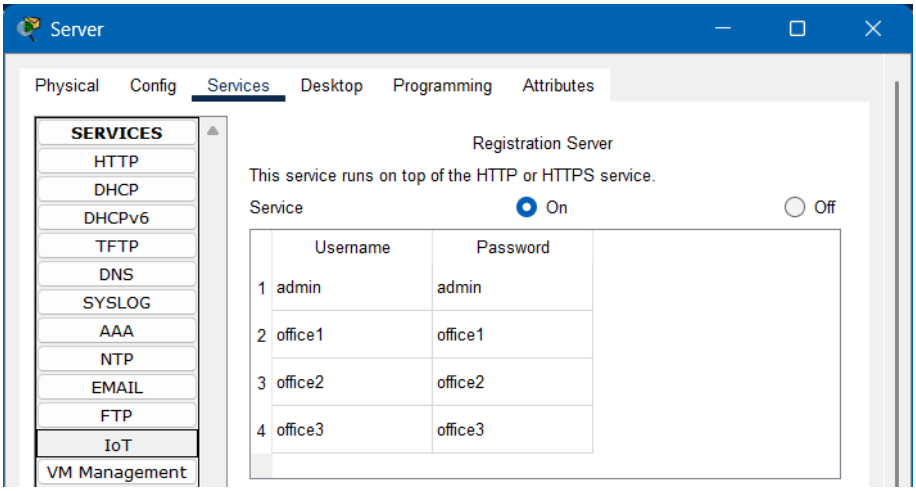


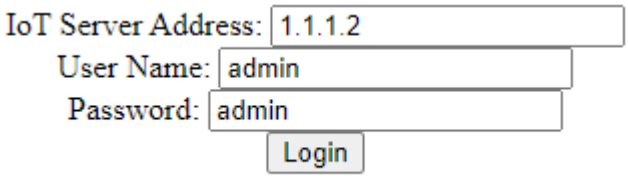
4.3 Server

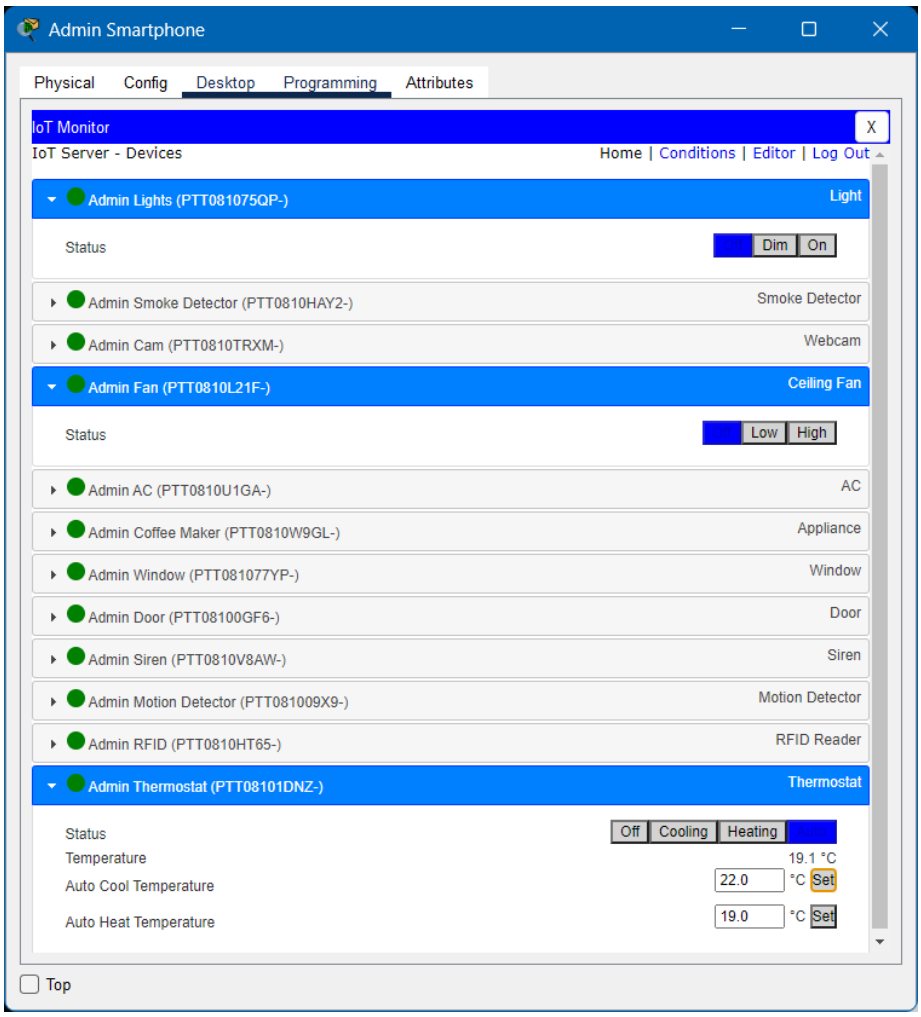
All devices will communicate with the server through **HTTPS** protocol.

Each room has its own **username** and **password**.

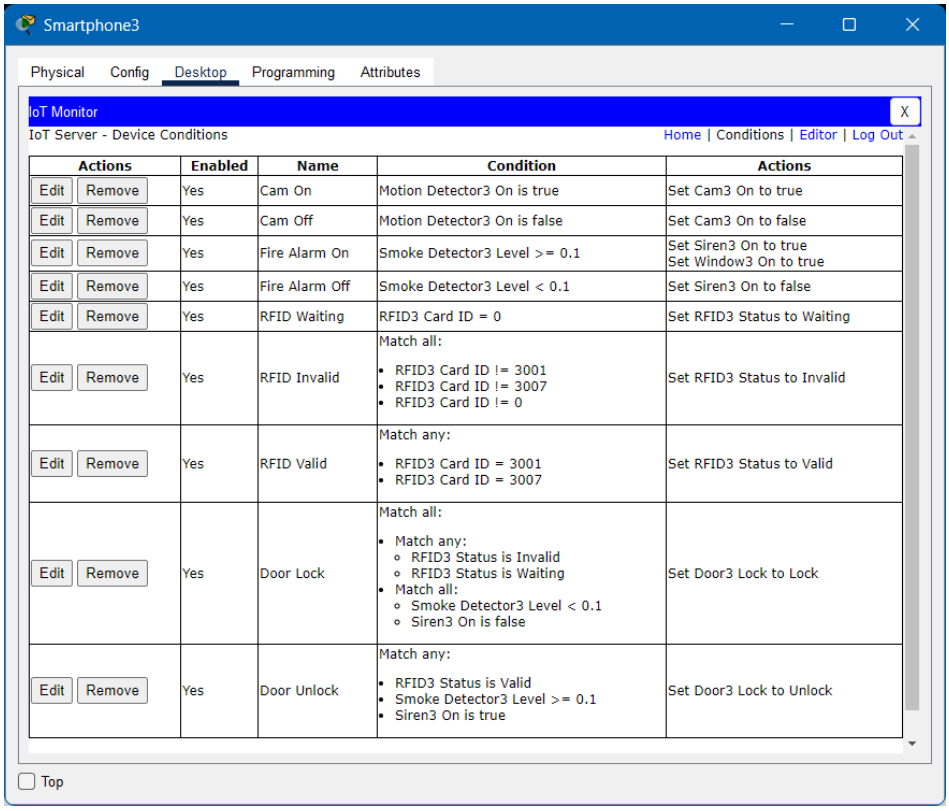
A device such as a smartphone or a laptop can control the office by typing the server's Ip address **(1.1.1.2)** in the *web browser*, or by using the *IoT Monitor app.*






Admin Smartphone
Physical
Config
Desktop
Programming
Attributes
IoT Monitor
X
IoT Server - Devices
Home | Conditions | Editor | Log Out
Admin Lights (PTT081075QP-)
Light
Status
Off
Dim
On
Admin Smoke Detector (PTT0810HAY2-)
Smoke Detector
Admin Cam (PTT0810TRXM-)
Webcam
Admin Fan (PTT0810L21F-)
Ceiling Fan
Status
Off
Low
High
Admin AC (PTT0810U1GA-)
AC
Admin Coffee Maker (PTT0810W9GL-)
Appliance
Admin Window (PTT081077YP-)
Window
Admin Door (PTT08100GF6-)
Door
Admin Siren (PTT0810V8AW-)
Siren
Admin Motion Detector (PTT081009X9-)
Motion Detector
Admin RFID (PTT0810HT65-)
RFID Reader
Admin Thermostat (PTT08101DNZ-)
Thermostat
Status
Off
Cooling
Heating
Auto
Temperature
19.1 °C
Auto Cool Temperature
22.0
°C
Set
Auto Heat Temperature
19.0
°C
Set
Top

4.4 Conditions



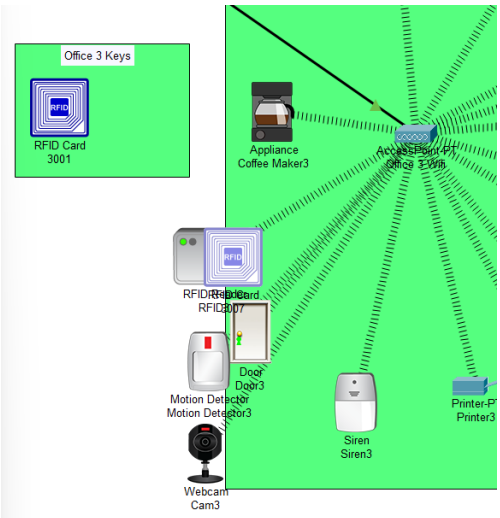
Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	Cam On	Motion Detector3 On is true	Set Cam3 On to true
Edit Remove	Yes	Cam Off	Motion Detector3 On is false	Set Cam3 On to false
Edit Remove	Yes	Fire Alarm On	Smoke Detector3 Level >= 0.1	Set Siren3 On to true Set Window3 On to true
Edit Remove	Yes	Fire Alarm Off	Smoke Detector3 Level < 0.1	Set Siren3 On to false
Edit Remove	Yes	RFID Waiting	RFID3 Card ID = 0	Set RFID3 Status to Waiting
Edit Remove	Yes	RFID Invalid	Match all: • RFID3 Card ID != 3001 • RFID3 Card ID != 3007 • RFID3 Card ID != 0	Set RFID3 Status to Invalid
Edit Remove	Yes	RFID Valid	Match any: • RFID3 Card ID = 3001 • RFID3 Card ID = 3007	Set RFID3 Status to Valid

Edit Remove	Yes	Door Lock	Match all:
			• Match any:
			  ◦ RFID3 Status is Invalid
			  ◦ RFID3 Status is Waiting
			• Match all:
			  ◦ Smoke Detector3 Level < 0.1
			  ◦ Siren3 On is false
				Set Door3 Lock to Lock

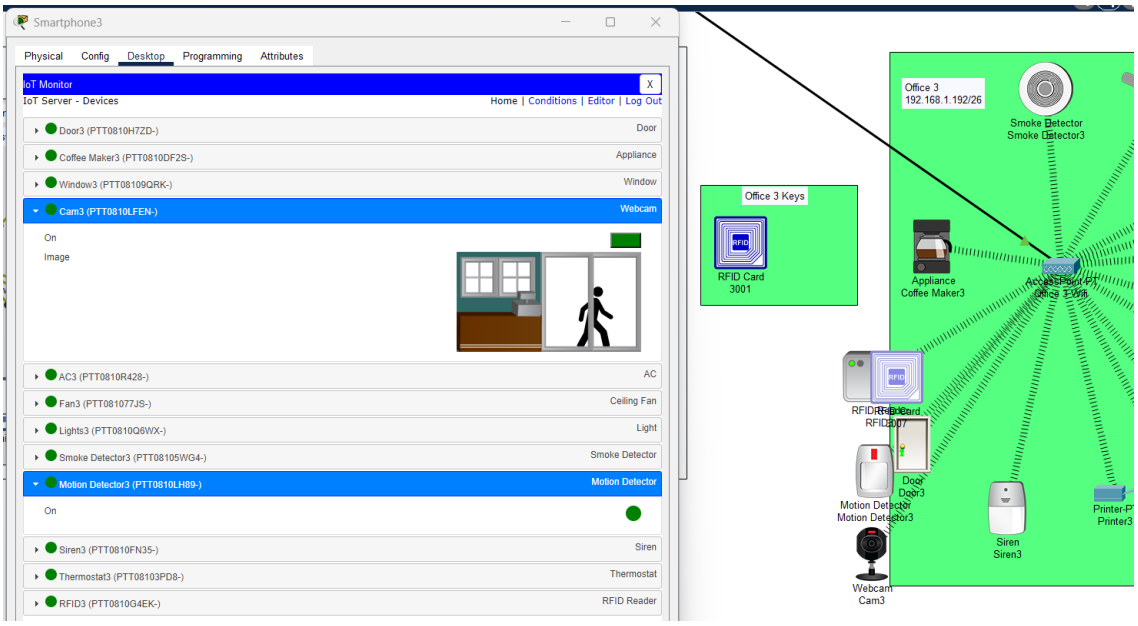
Edit Remove	Yes	Door Unlock	Match any: • RFID3 Status is Valid • Smoke Detector3 Level >= 0.1 • Siren3 On is true	Set Door3 Lock to Unlock

Automation is the essence of IoT. Using a multitude of conditions, we can simulate various scenarios including but not limited to:

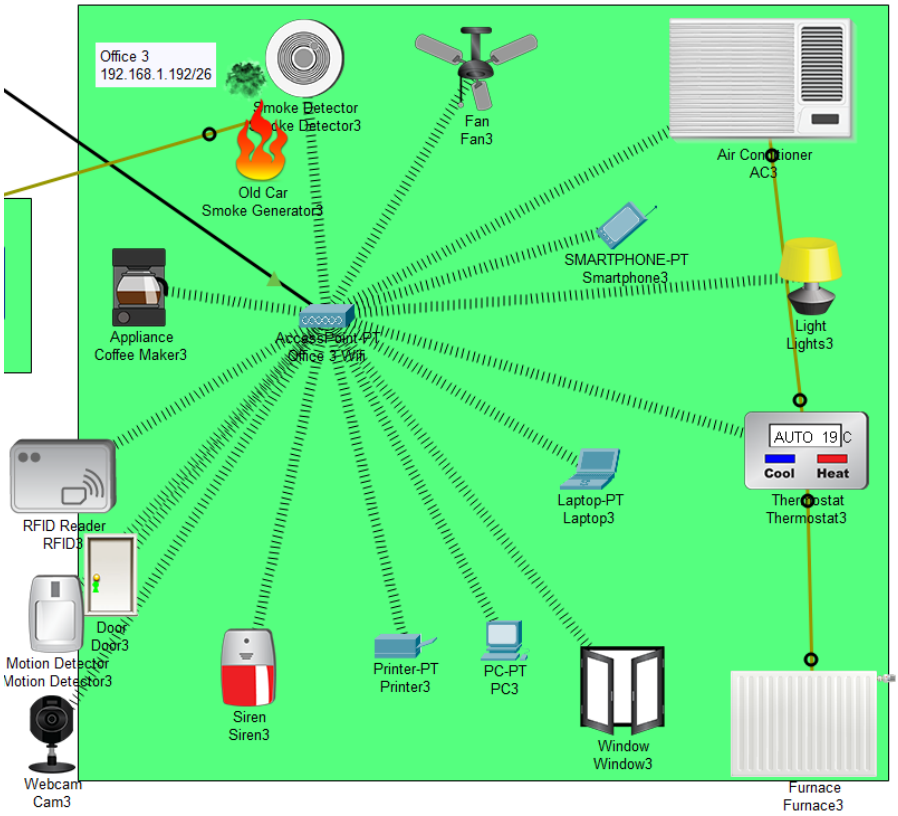
- *RFID readers* are used to allow access only to certain *RFID cards*. Upon validating a card, the office's *door* will automatically open. Each office is assigned its own set of cards, any other card will be rejected.



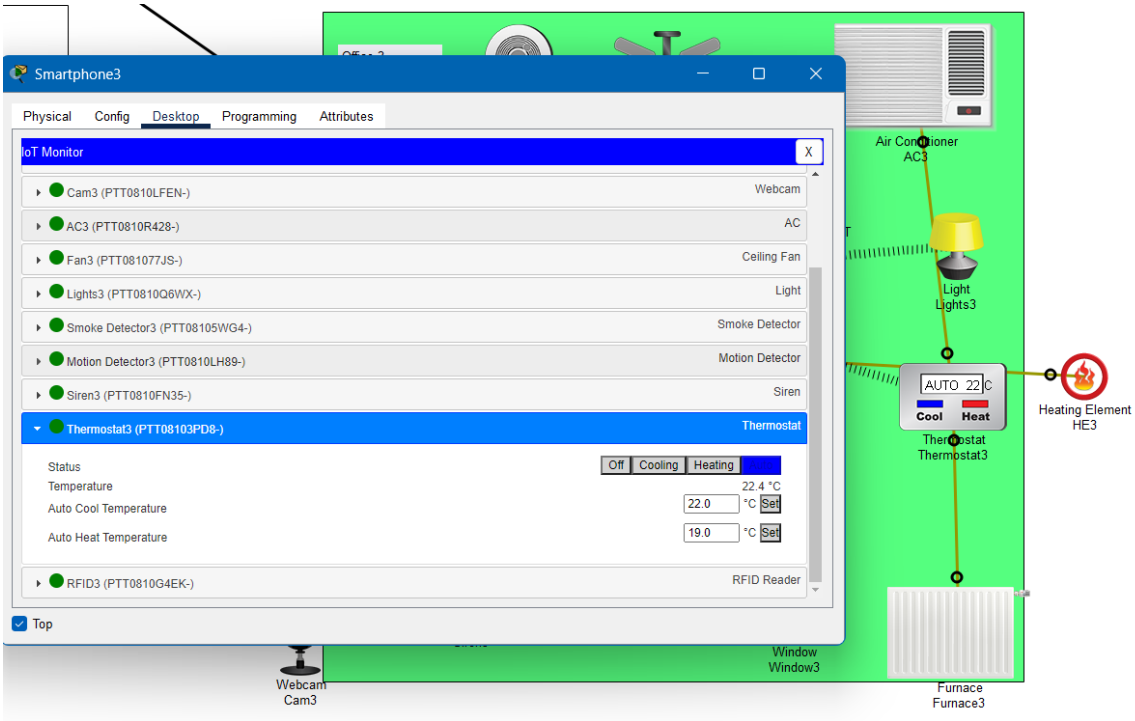
- When a user attempts to scan a card, the *motion detector* senses them, and the *camera* will turn *on* to record a live feed of the scanner.



- In case of a fire or smoke situation triggered by the *smoke detector*, all *siren* alarms will ring, the *windows* will be *opened*, and all *doors* will be *unlocked* for emergency evacuation.

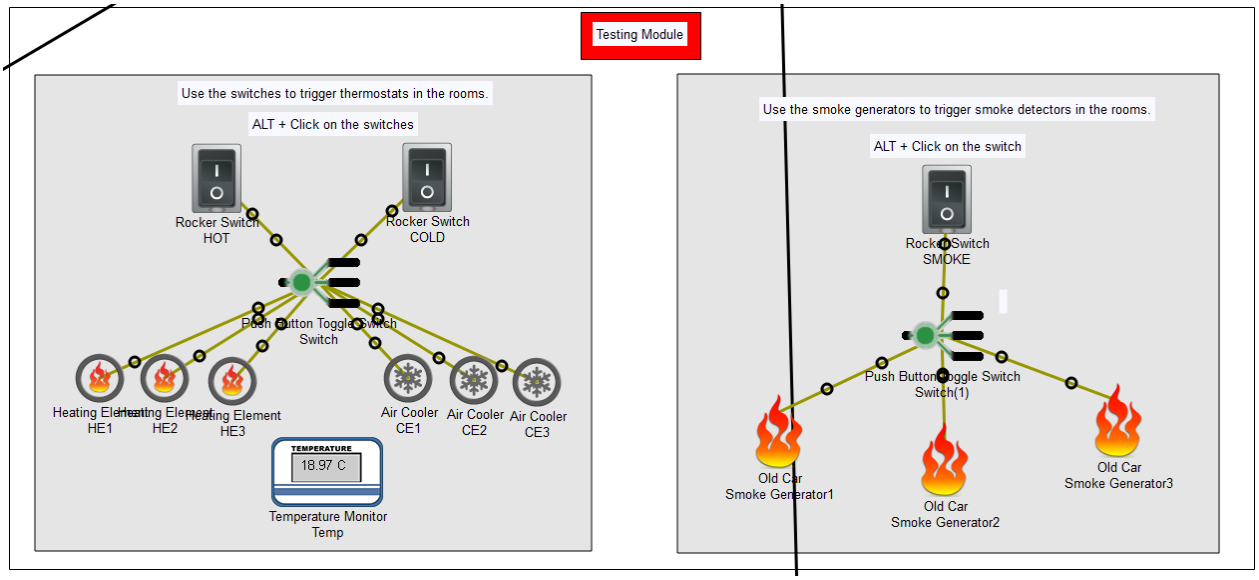


- A *thermostat* is used to control the temperature of the office. The user can set the device to *auto* and set the maximum and minimum temperatures, or the user can set the device manually on either *cooling mode* or *warming mode*.

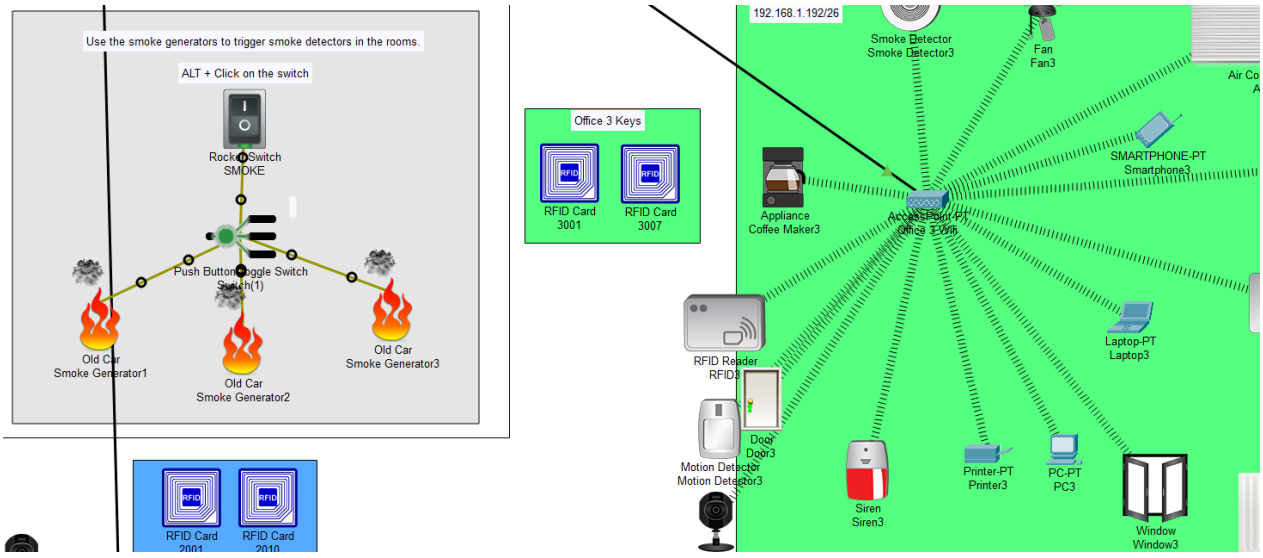


4.5 Testing Module

The user can test environmental scenarios using the test module. If the user wishes to test the thermostat, simply click the *HOT* or *COLD* switch to change the temperature. Likewise, if the user wishes to test a fire or smoke situation, flip the *SMOKE* switch to generate smoke and observe as the intended condition folds.



Ex: Fire scenario:



5. Conclusion

In conclusion, the Cisco Packet Tracer simulation presented a smart office network that harmoniously integrates the Internet of Things (IoT) and networking principles. The allocation of subnet ranges to each office space, coupled with rigorous security measures, signifies a commitment to operational integrity and a controlled network environment.

The strategic use of IoT devices within each office highlights the practical applications of interconnected technologies and the potential for optimizing various facets of office functionalities. From security scenarios to environmental monitoring, the simulation portrays the versatility and adaptability of IoT in enhancing the overall workplace experience.

The emphasis on secure communication through the HTTPS protocol, coupled with individualized usernames and passwords for each room, reinforces the commitment to data integrity and access control. The deliberate isolation of network segments ensures that users have exclusive control over their room's devices, reducing the risks of unauthorized access and preserving the privacy of sensitive information.

As we conclude this exploration, it is evident that the use of IoT and networking technologies together has far-reaching implications for the evolution of smart office environments. The simulation serves as a testament to the transformative potential of these technologies, offering a glimpse into the future of interconnected systems that prioritize efficiency, security, and user empowerment.

In the ever-evolving landscape of technology, this simulation stands as a steppingstone towards creating intelligent, adaptive, and secure office spaces. The scenarios implemented in the simulation provide a foundation for further research and development, encouraging a continued exploration of innovative solutions that cater to the evolving needs of the modern workplace.

In the journey towards a smarter, more connected world, the intersection of IoT and networking principles displayed in this simulation illuminates the path forward. The smart office network designed here serves as an exemplar, inviting further discourse and exploration into the boundless possibilities of technology in shaping the workplaces of tomorrow.

Thus the goal of our experiment has been attained.