

IoT-Based Home Automation with Network Segmentation

A M Nakul

Dept. of Electronics and Communication
Amrita Vishwa Vidyapeetham Amritapuri
Kerala, India
amnakul15@gmail.com

Abhijith K

Dept. of Electronics and Communication
Amrita Vishwa Vidyapeetham Amritapuri
Kerala, India
abhijithk6203kvk@gmail.com

Abhinav Nambiar

Dept. of Electronics and Communication
Amrita Vishwa Vidyapeetham Amritapuri
Kerala, India
abhinavnambiar1532@gmail.com

Adith S H

Dept. of Electronics and Communication
Amrita Vishwa Vidyapeetham Amritapuri
Kerala, India
adithshpriv@gmail.com

K V Abhishek

Dept. of Electronics and Communication
Amrita Vishwa Vidyapeetham Amritapuri
Kerala, India
abhishek.kv2004@gmail.com

Abstract—As Internet of Things (IoT) devices have become common in households, vulnerabilities stemming from a lack of segmentation on the home network poses a significant security risk. With IoT devices including smart lights, smart cameras, and smart thermostats among others typically running a flat network architecture, devices are open to Cyberattacks which could easily spread across the entire network. In this project, a secure smart home automation network architecture will be designed and simulated using Cisco Packet Tracer. Using Virtual Local Area Networks (VLANs) and Access Control Lists (ACLs) as a security framework, the proposed home automation network can have three main VLANs; IoT devices, personal user devices, and guest users. Inter-VLAN routing is implemented using a Layer 3 switch or router-on-a-stick, with ACLs enforcing strict communication boundaries. IoT devices are allowed internet access but restricted from communicating with personal or guest networks. Network segmentation through VLANs provides logical segregated networks, added security, and controlled data flow. The project demonstrates the main elements of core networking principles, as well as, a tangible way of securing smart homes.

Index Terms—IoT, Smart Home, Cisco Packet Tracer, Network Segmentation, Automation, Wireless Router, DHCP, Static IP

I. INTRODUCTION

The Internet of Things (IoT) has completely changed how modern homes operate offering convenience, automation, and power efficiency. Smart devices such as voice assistants, air conditioners, lights, thermostats, security cameras, and fire sensors are being used more and more frequently. As more of these devices are connected to a home network, there is a growing need for robust and secure network infrastructure to support their functionality. Even as such systems bring about convenience, integrating many connected devices in a home network poses possible cybersecurity threats.

Hackers might take advantage of loosely configured or compromised devices to access personal data or authority over personal systems. Additionally, if all the devices share the same flat network, it will be easier for the threats to spread across systems.

This project tackles these problems by demonstrating a secure home automation network through Cisco Packet Tracer, focusing on network segmentation and access control. Rather than utilizing sophisticated enterprise methods like VLANs and firewalls, the setup relies on IP-based logical partitioning and Access Control Lists (ACLs) to segment various classes of devices (IoT, personal, guest). There is a central server that is added to mimic web-based registration, management, and automation logic. The aim is to have a functional, secure, and educational representation of a smart home network that incorporates both networking and cybersecurity best practice.

II. OBJECTIVES

- Simulate a homogeneous smart home network via wireless routers and IoT devices.
- Implement IP-based segmentation through DHCP and static IP addressing.
- Develop a centralized server for controlling device automation through web interface.
- Implement automation from sensor input through the use of conditional logic.

III. PROPOSED WORK

This project offers a simulation of an IoT-based network of an intelligent home focusing on security and automation, developed with Cisco Packet Tracer. The primary aim is to design a secure, working home automation system that logically divides devices and prevents unwarranted communication between them. The network is separated into three logical subgroups: IoT devices (smart air conditioners, fire sensors, thermostats), personal devices (PCs, laptops, smartphones), and guest devices. A wireless router is set to enable all devices with WPA2 encryption and DHCP for assigning IP automatically. Critical elements such as the central server are given static IPs to ensure consistent identification. The central server has a web-based interface through which users

can register, observe, and manage smart devices via HTTP services. The network is based on a client-server model where the server is used as the command center for all automation operations. Access Control Lists (ACLs) are used as added protection to limit communication between groups. For instance, guest devices may not be allowed to communicate with IoT or personal devices, and IoT devices are kept off direct access to the internet or personal systems. This segmentation offers an underlying level of network security without needing intricate VLAN setups. Automation capabilities are also built in: devices such as fire and temperature sensors can initiate changes in other devices—like shutting off the AC or opening windows—mimicking real-world smart home actions. The interactive simulation give insights to users about fundamental networking concepts such as IP addressing, routing, ACL setup, DHCP setup, and packet traversal. In general, the project not only demonstrates smart home architecture and how it works but also highlights best practices for security and device management. It is a hands-on and instructive resource to learn about actual networking and automation environments.

IV. IMPLEMENTATION AND RESULTS

A. Network Configuration and Setup

The setup started with the installation of a wireless router that served as the central connection point for all the devices. The router was secured using WPA2 security to provide encrypted wireless communication and given a custom SSID for network identity. The DHCP protocol was also enabled on the router to dynamically allocate IP addresses to end devices. In addition to that, a central server was given a static IP address (10.1.2.2) to ensure consistency in control and communication.

1) *Network Initialization:* The home network is set up by using a wireless router with SSID, WPA2 encryption, and DHCP service. The home router gets a static IP of 10.1.1.2 with gateway 10.1.1.1 and DNS server at 10.1.2.2. The router's internal IP is assigned as 192.168.0.1, issuing dynamic IPs starting from 192.168.0.100.

2) *Server and Core Network:* An IP-enabled IoT server with 10.1.2.2 is linked through a switch and router, symbolizing core infrastructure. The server runs an IoT dashboard available on <http://10.1.2.2/home.html>, permitting monitoring and control of all smart devices.

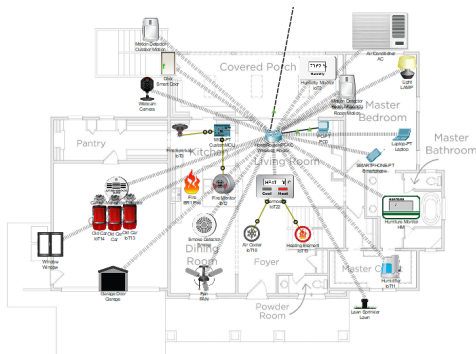


Fig. 1. Smart Home Device Layout in Cisco Packet Tracer

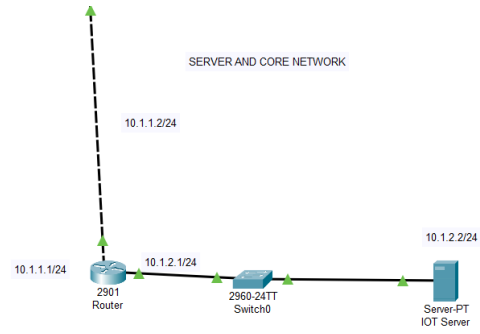


Fig. 2. Server and Core Network in Cisco Packet Tracer

B. Device Integration

Different end devices were integrated into the network, including IoT devices like smart air conditioners, fire detectors, and thermostats, and personal devices (laptops, mobile phones) and guest devices. The devices were connected wirelessly with the router and received their IP addresses through DHCP. Devices were manually registered or automatically discovered by the central server, which was set up with HTTP and IoT services. This server contained a web-based dashboard through which users could engage and manage the devices.

Web Browser	
<	> URL http://10.1.2.2/home.html Go Stop
IoT Server - Devices Home Conditions Editor Log Out	
▶ FAN (PTT0810E0RJ-)	Ceiling Fan
▶ AC (PTT08103610-)	AC
▶ Smart Door (PTT0810A85T-)	Door
▶ HM (PTT08109M9I-)	Humidor Sensor
▶ LAMP (PTT081040A7-)	Light
▶ Garage (PTT081059Q6-)	Garage Door
▶ Window (PTT08102A6W-)	Window
▶ IoT3 (PTT08105G8E-)	Humidity Sensor
▶ CO Detector (PTT081086T0-)	Carbon Monoxide Detector
▶ Lawn (PTT0810YB00-)	Lawn Sprinkler
▶ Outdoor Motion (PTT08103E09-)	Motion Detector
▶ Smoke (PTT0810A90L-)	Smoke Detector
▶ IoT11 (PTT081055J9-)	Humidifier
▶ Room Motion (PTT08102FH5-)	Motion Detector
▶ IoT22 (PTT08103ZME-)	Thermostat
▶ Room Motion(1) (PTT0810Y2V6-)	Motion Detector
▶ Camera (PTT081086B0-)	Webcam

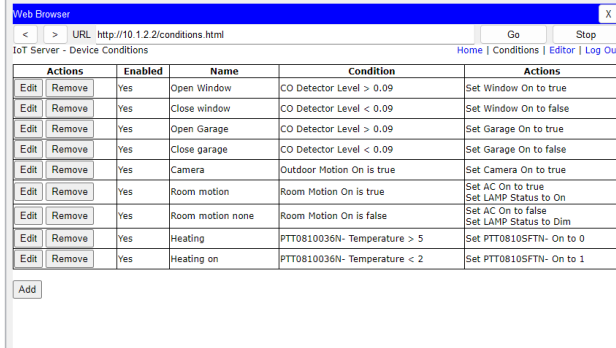
Fig. 3. IoT Web Dashboard for Device Status and Control

C. Logical Segmentation and Access Control

The network architecture had logical segmentation by dividing the devices into three categories: IoT, personal, and guest. Segmentation was done by applying ranges of IP addresses. To limit unauthorized communications between these groups, Access Control Lists (ACLs) were implemented on the router. For instance, guest devices were not allowed access to IoT systems and personal devices, while IoT devices were not allowed access to user systems or the broader internet

D. Automation and Control Testing

The simulation had automation based on sensors. When conditions were initiated in the environment (e.g., a fire sensor detecting smoke or a heat sensor sensing too much heat), corresponding devices such as the smart AC or window systems acted in response. These actions were regulated by using logic setup in the server and could be seen by looking at real-time logs on the server's dashboard. Moreover, the control activities like switching devices on/off or thermostat setting adjustment were conducted from PCs and smartphones using a simulated web browser interface.



Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	Open Window	CO Detector Level > 0.09	Set Window On to true
Edit Remove	Yes	Close window	CO Detector Level < 0.09	Set Window On to false
Edit Remove	Yes	Open Garage	CO Detector Level > 0.09	Set Garage On to true
Edit Remove	Yes	Close garage	CO Detector Level < 0.09	Set Garage On to false
Edit Remove	Yes	Camera	Outdoor Motion On is true	Set Camera On to true
Edit Remove	Yes	Room motion	Room Motion On is true	Set AC On to true
Edit Remove	Yes	Room motion none	Room Motion On is false	Set AC On to false
Edit Remove	Yes	Heating	PTT0810036N- Temperature > 5	Set LAMP Status to Dim
Edit Remove	Yes	Heating on	PTT0810036N- Temperature < 2	Set PTT0810036N- On to 0

Fig. 4. IOT Web Dashboard for Automation and Control

E. Functional Validation and Observations

Connectivity and routing between devices were verified through ping tests and packet tracing. All devices were able to communicate with the server, and ACL policies were confirmed by seeing blocked attempted communication between unauthorized device groups. The DHCP functionality behaved as expected, assigning IPs dynamically without conflict, and static IP configurations provided consistent identification for mission-critical components. In general, the system performed as intended. It effectively showed home automation, safe network partitioning, controlled communication, and device responsiveness, meeting the project goals and reinforcing key computer networking principles.

```
C:\>ping 10.1.2.2

Pinging 10.1.2.2 with 32 bytes of data:

Reply from 10.1.2.2: bytes=32 time<1ms TTL=126
Reply from 10.1.2.2: bytes=32 time<1ms TTL=126
Reply from 10.1.2.2: bytes=32 time<1ms TTL=126
Reply from 10.1.2.2: bytes=32 time<1ms TTL=126

Ping statistics for 10.1.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 2ms

C:\>ping 10.1.2.1

Pinging 10.1.2.1 with 32 bytes of data:

Reply from 10.1.2.1: bytes=32 time<1ms TTL=254
Reply from 10.1.2.1: bytes=32 time<1ms TTL=254
Reply from 10.1.2.1: bytes=32 time<1ms TTL=254
Reply from 10.1.2.1: bytes=32 time<1ms TTL=254

Ping statistics for 10.1.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 6ms, Average = 1ms
```

```
C:\>ping 192.168.0.101

Pinging 192.168.0.101 with 32 bytes of data:

Reply from 192.168.0.101: bytes=32 time=26ms TTL=128
Reply from 192.168.0.101: bytes=32 time=19ms TTL=128
Reply from 192.168.0.101: bytes=32 time=5ms TTL=128
Reply from 192.168.0.101: bytes=32 time=6ms TTL=128

Ping statistics for 192.168.0.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 6ms, Maximum = 26ms, Average = 15ms
```

Fig. 5. Ping testing for verifying connectivity

V. CONCLUSION

This project effectively demonstrates the design and simulation of a safe smart home automation network with Cisco Packet Tracer. Through the use of VLANs and Access Control Lists (ACLs), the network implements logical segregation of devices into IoT, personal, and guest zones, thus securing and facilitating easier management. Implementation of inter-VLAN routing through a Layer 3 switch or router-on-a-stick setup enables the controlled communication between segments, and lateral movement in case a device is compromised becomes less likely. It emphasizes critical networking principles like IP addressing, policy enforcement at the device level, traffic segmentation, and secure automation practices. Internet access is provided to IoT devices while denying them access to more sensitive areas of the network, ensuring confidentiality, integrity, and availability of the system. In summary, this work is a realistic and learning-oriented model for constructing secure, scalable, and effective smart home networks and continues to highlight network-level security in the IoT age.

VI. FUTURE SCOPE

The project can be scaled up by implementing device grouping per IP range to mimic role-based access control for user, guest, and admin levels. Inserting logging or simulated notification systems—such as pop-up notifications during fire or gas leaks—can be added for more effective emergency feedback. More complex automation rules using multiple conditions and time-based triggers can be tested to increase system intelligence. Furthermore, simulating multiple homes connected to a common central server could help analyze data routing and multi-node management. These developments will ensure much greater practicality, accessibility, and robustness of smart home systems.

ACKNOWLEDGMENT

We would like to express their sincere gratitude to Ms. Aswathy K. Nair, Assistant Professor (Sr. Gr.), Department of Electronics and Communication Engineering, School of Engineering, Amritapuri, for her invaluable guidance and support throughout the completion of this project.

REFERENCES

- [1] N. Gwangwava and T. B. Mubvirwi, "Design and Simulation of IoT Systems Using the Cisco Packet Tracer," *Advances in Internet of Things*, vol. 11, no. 2, pp. 1–18, 2021. doi: 10.4236/ait.2021.112005.

- [2] P. R. Bathula, S. Pv, L. L. Anumakonda, M. M. Basha, and P. V. Naishadhkumar, "Home Automation Using Packet Tracer," in *Advances in Communication, Devices and Networking*, 2022, pp. 611–623. [Online]. Available: https://link.springer.com/chapter/10.1007/978-981-19-1360-6_49
- [3] D. C. P. Sinaga, G. J. Tampubolon, and I. Ndruru, "Implementation of a Smart Home Based on Internet of Things Using Cisco Packet Tracer," *Journal of Computer Networks, Architecture and High Performance Computing*, vol. 6, no. 1, pp. 20–29, Jan. 2024. doi: 10.47709/cnahpc.v6i1.3518.
- [4] N. Nanthini, J. Sugee, and A. G. Priya, "Smart Home Security Enhancements with Cisco Packet Tracer," in *Proc. 2024 Int. Conf. on Computing and Data Science (ICCDs)*, IEEE, 2024, doi: 10.1109/IC-CDS2024.65337.
- [5] T. Davis III, M. Wang, T. Zavarella, and M. Zhang, "Analysis and Extension of Home IoT Network Segmentation Architectures," Massachusetts Institute of Technology, Tech. Rep., 2023.
- [6] K. Olson and N. Scaife, "All Your Data Are Available to Us: A Need for Network Segmentation with IoT Devices," University of Colorado - Boulder, 2023.
- [7] Cisco Networking Academy, "Introduction to Packet Tracer," [Online]. Available: <https://www.netacad.com>