SECURE SMART HOME NETWORKING

Helly Patel
Fadi Meleika
Jared Collazo
Jesus Calvo

Table of Contents

Chapter 4: Design

4.1 Entity-Relationship (ER) Diagram

4.2 Class Diagram

4.3 Network Diagram

4.4 3 Alternative Solutions and Comparisons

Chapter 5: Development

5.1 Solution Overview

5.2 Outputs

5.3 User Manual

Chapter 6: Evaluation and Conclusion

6.1 Solution Testing

6.2 Verification

6.3 Validation

6.4 Team Conclusion

Chapter 1: Introduction

1.1 Project Background

The Secure Smart Home Networking project aims to create a secure, efficient, and scalable smart home network. As the number of IoT devices continues to increase and make their way into homes, the project aims to create a robust networking platform that not only accommodates several smart devices but also prioritizes security.With Cisco solutions such as routers, switches, firewalls, SecureX, and AnyConnect VPN, the network is engineered to not just provide performance but protection. Some of its major functions include segmentation (VLANs) within the network, quality-grade encryption (WPA3), settings to the firewalls, and safe remote access through VPN.

1.2 Problem Definition

Modern smart homes are often vulnerable to hacking, phishing, data breaches, and unauthorized access due to poorly managed network configurations. Most home networks lack extra security measures, thus susceptible to intrusion. In addition, potential system downtime due to equipment failure and costly proper hardware are challenges. This project addresses this issue by architecting a safe, segmented network design that ensures data privacy, reliability, and compliance with standards such as GDPR, CCPA, and the NIST Cybersecurity.

1.3 Glossary

Term	Definition
IoT (Internet of Things)	Devices that talk and exchange information over a network without the intervention of humans.
Cisco SecureX	A security that provides centralized management and visibility across a network.
VLAN (Virtual LAN)	A method to segment networks into multiple broadcast domains for security and performance.
WPA3	The new Wi-Fi security protocol with enhanced encryption.
Cisco AnyConnect VPN	A secure mobility solution that enables secure remote access to the network.
Packet Tracer	A Cisco network simulator for designing, setting up, and testing network environments.
Firewall	A security device that monitors and regulates incoming and outgoing network traffic.
Man-in-the-middle Attack (MitM)	An attack where the attacker surreptitiously intercepts communication between two parties.
GDPR/CCPA	Regulations that govern data privacy and security for personal data of individuals.
Network Segmentation	Segmenting a network into smaller networks to enhance performance and security.

1.4 Iteration The project developed under iterative method divided into different phases:

- **Design Phase:** Network written design with Cisco hardware, VLANs, security features, and VPN configuration.
- **Simulation Phase:** Simulated the network environment on Cisco Packet Tracer to test and validate network design functionality.
- **Implementation Phase:** Configured firewalls, access control, WPA3 encryption, and secure remote connection. Installed Wireshark monitoring for network testing.
- **Testing Phase:** Performed security testing using tools like Wireshark to identify vulnerabilities and enhance configurations.
- **Deployment and Monitoring:** Deployed the finished secure smart home network and outlined step-by-step procedures for ongoing monitoring and maintenance.

Each cycle allowed for tuning based on performance, security testing outcomes, and review of compliance standards to ensure the final network was robust and secure.

Chapter 2: Project Management

2.1 Task Analysis

All work was evenly divided among all four of us. Since packet tracer does not support multiple people working on a file at a given time, one person would have the main file and work on it. Then, they would pass the file on to the next group member. While a group member worked on the packet tracer file, the others worked on the documentation required for the project so that there was no time wasted. If team members was stuck on something or having problems group would help out and try to figure out as a group

---

2.2 Roles

Helly Patel (Project manager)

- As a project manager, she managed the structure/organization of the project and team meetings. She attended all project manager meetings and then relayed the information to the rest of the team. Helped with research and was responsible for implementing the layout of the packet tracer file.

Jesus Calvo

- Also helped with research and was responsible for IoT configuration and implementation. After implementation, all IoT was connected to the server to control them from a single device. Also helped with network setup.

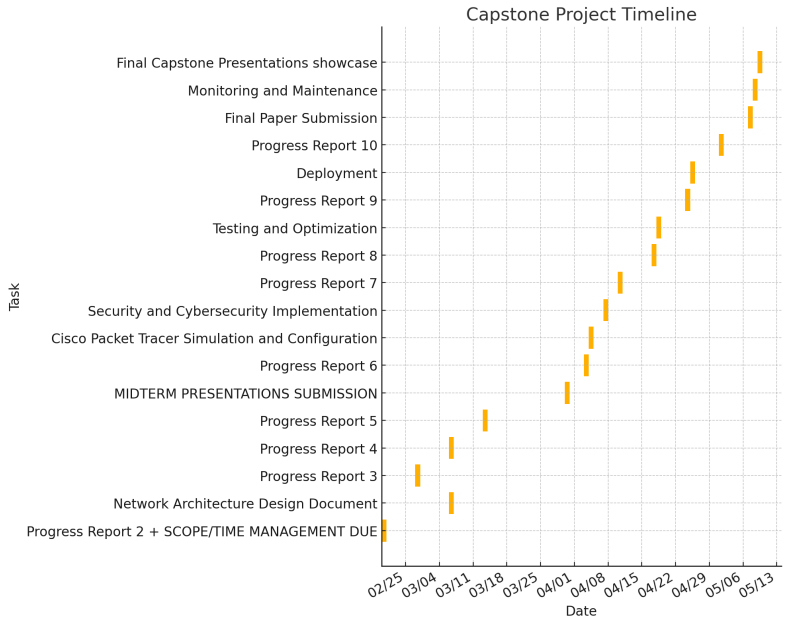
Jared Collazo

- Help with research and was responsible for network configuration and security implementation. Made sure the network was protected from outside attacks and the client could access the IoT devices from anywhere through a clientless VPN.

Fadi Meleika

- Helped with research and was responsible for setting up smart sensors that worked with IoT devices.Also, help others with their responsibility as needed.

2.3 Work Breakdown Structure/ Gantt Chart



All work/tasks were split up evenly among all team members.

2.4 Risk Management

Having risk management is very important for any project. One of the biggest risks that needs to be managed for us is timing. Making sure that everyone is available to meet to work on and discuss the project. Everyone has school,work and personal lives so it is important to communicate in order to schedule meetings. Something else to keep an eye out for is making sure that the product works Properly. These are some ways that we managed these risks. We have a group text chat and a group discord chat. We all put our availability in the group chat for each week and then based on that we would schedule meetings for the week. If anyone had any scheduling issues that would also be communicated through the group chat. We made sure that everything in our packet file was working before we moved on to the next feature/step. We would also help each other out if anyone was having any issues implementing anything.

Chapter 3: Define

3.1 Stakeholders

So, as in any network design and industry project, it is integral to investigate and determine who the stakeholders are, it is essential. Stakeholders are categorized as being the people or groups who have an interest in or are invested in the results or standings of the project. This could be an active involvement or indirect involvement. In the case of the Smart Home Network Security project, there are a few stakeholders. For those that fall under primary stakeholders, you have the network administrators, who are responsible for setting up the configurations, maintaining the network, and securing the network. Network administrators have the chief interest in ensuring the network infrastructure is quality, has the scaling factor, and durable against threats, all whilst being easy to manage.

Another stakeholder is the Smart Home Residents, which are considered the end users who rely on the functionality of the devices that are connected to the internet/network. This reality provides the users with convenience, automation, and security. The home residents are accustomed to having stable, fast, and secure connectivity without the expertise of setting the network up themselves.

The last primary stakeholders are to be the IT instructors and evaluators. Ultimately, these instructors and evaluators are here to validate and observe functionality of the Smart Home Network. They are responsible for checking if the project meets the requirements and

integral aspects of the project. These instructors play an active role in facilitating the arrangement of the teams and are actively invested in the outcome of the project. These instructors are constantly reminding the students of their responsibilities and duties, and are always there to offer moral support, and advice.

We cannot forget about the secondary stakeholders of this project. The secondary stakeholders can involve the visitors or guests. The guests of visitors of the supposed smart home, would temporarily connect to the guest wireless access point and use the home owner's wifi for a time being. They also rely on the durability, robustness, and security of the smart home network, their access would be isolated and limited for security reasons however. We also have vendors or IoT providers, who supply the smart devices and verify their compatibility with the network. Let us not forget about the literal guests and visitors who come to the presentation event. These individuals have the pleasure of interacting with group members and asking questions that relate to the product or project. They rely on the availability of the project at hand.

Lastly we can consider a simulated attacker to be a secondary stakeholder. This is because in a project that involves implementations of cybersecurity measures, simulated attackers represent an abstract stakeholder used for testing. A simulated hacker's involvement helps gauge the sturdiness and safety measures when combating unauthorized access and rogue devices.

3.2 Requirements Gathering

The project originated from gathering detailed technical and functional requirements with a smart home use-case scenario in mind. The requirements for this project were brainstormed based on a top-down approach, considering general goals. General goals like the network being secure and having the ability to segment traffic, and sectioned off to specific network roles.

To go over the functional requirements, we can say we have VLAN segmentation for isolation of different device groups, those groups being Admin, IoT, Guest, and User. Another aspect is our router-on-a-stick, or ROAS for short, meant for inter-VLAN routing with subinterfaces and appropriate IPs. We also have DHCP configuration for each VLAN using pools and exclusion lists. Next, is our port security, or sticky MAC to prevent unauthorized device connections, which is applied directly on the switch interfaces of end devices. We also have DHCP Snooping to detect and prevent rogue DHCP servers. Email Logging & Alerts through syslog configuration. Access Control Lists (ACLs) to restrict traffic between VLANs. Clientless VPN through the ASA Firewall Access Control for remote user authentication and internal resource access. DNS & HTTP Server Hosting on VLAN 20 for internal control panel and access verification. Lastly, we have Remote Logging and NTP Synchronization using the internal server.

To name some Non-Functional Requirements, we can talk about reliability. That goes to say DHCP and DNS services must be consistently available. Next, we have scalability, meaning the design must allow the future addition of VLANs and ACLs without the

inconvenience of tedious reconfiguration. Lastly, users have to be able to access resources seamlessly.

3.3 Project Scope

The project scope defines the boundaries and extent of the smart home security network project. We can say in our scope is the creation of five VLANs (default, Admin, IoT, Guest, Users). The functionality of a DHCP server, capable of dealing appropriate IPs for each VLAN. Implementation of DHCP snooping with proven tests. Configuration of Port Security using sticky MAC addresses with shutdown violation actions. Involvement of ACLs, in this project it was HTTP-only access on VLAN 30 (Guest) and blocking ICMP/ping. Syslog server and NTP server setup with centralized logging from the switch and router. Combination of ASA Firewall with NAT and WebVPN to demonstrate external access that required login credentials. Lastly we had configuration of DNS and HTTP servers internally, with proper resolution of smart home domain names. The factors that was excluded from our scope was actual internet connectivity, not possible in Cisco packet tracer scenarios. Actual physical layer security such as cable locks or wireless signal shielding. Advanced IDS/IPS integration or real-time anomaly detection. Lastly, Load balancing or high availability configurations. The scope prioritizes security, segmentation, and controlled access, highlighting realistic issues where home networks must support multiple device types while maintaining security.

3.4 FDD Requirement Grouping and Case Diagrams

In order to compile and monitor the project's technical objectives, a Functional Decomposition Diagram (FDD) was necessary. FDD is a visual tool that allows organizing features by their function and showing their correlation.

FDD Requirement Groups:

Group	Feature/Component
VLAN makeup	VLANs 10, 20, 30, 40 and port assignments
Routing	router-on-a-stick, inter-VLAN communication
DHCP	DHCP pools, prevented IP specifications, and testing against foreign DHCP leases.
Port Security	Port sticky MACs, violation counters/measures
ACLs	Guest VLAN/Permitted only HTTP access, VLAN 20 restrictions
Logging & Email	Syslogs are sent to the internal server, implementing email alerts between end devices.
Remote Access	ASA NAT, VPN, bookmark access
DNS & HTTP	Name resolution and web access for IoT resources

Use Case Diagram Summary:

1. Smart Home User Connects to IoT
    - Trigger: IoT device starts or reconnects.
    - Action: DHCP lease obtained from router. ACL allows HTTP to server.
    - Expected: Device cannot ping admin network.
2. Guest User Attempts Full Internet Access
    - Trigger: Laptop connects to Guest WAP.
    - Action: ACL restricts access to only HTTP/s, or DNS only.
    - Expected: PC won't be able to ping or access devices in Admin VLAN per restrictions placed.
3. Simulated foreign server plugged into IoT port
    - Trigger: fabricated a fictitious server with DHCP present, connected to an IoT port.
    - Action: DHCP snooping prevents dhcp lease to pc.
    - Expected: Connected client fails to obtain IP.
4. External User Accesses SmartHome Controls
    - Trigger: Outside PC connects to ASA public IP.
    - Action: Must authenticate (test/test) to access bookmark.
    - Expected: Cannot access server directly via IP.

CHAPTER - 4 : DESIGN

4.1 Entity-Relationship (ER) Diagram

The Entity-Relationship (ER) for our project which is Secure Smart Home Networking structure demonstrates the relationships of a lot of stuff between devices, users and monitoring affairs in the network. The objective is to show how the aspects of the smart home collaborate with users and the control system.

Key aspects:

- **User:** It's typically the owner or a person that has the authority of the smart home structure.
- **Device:** In our topology any thing that is an IoT unit can be characterized as a device. This could be the door lock, motion sensor, sirens, lights and many more.
- **Room:** Can be a group of devices at location for example: Livingroom, Kitchen,Garage.
- **Event:** Classifies as an activity or condition, for example motion detector or device trigger.

Relationships:

- A User is authorized to have control over the devices.
- A Device can establish many Events.
- A Device is in one Room, but a room can have a collective amount of devices.

4.2 Class Diagram

In our smart home network, the class diagram forms the framework of how devices, automated processes and users engage. It shows how every part of the system works and what info it has. Below are the main elements:

User

- Can see the device status, establish guidelines and control other smart devices.
- Example: The owner using the tablet to observe the house
- **Includes:** Username, access level.

Device

- Consists of any device like a motion detector, fan as well as siren.
- **Includes:** The smart device name, the type (Light, Sensor, Appliance), Status (On or Off).

Automation Rule:

- Done through the tablet.
- Communicates with the system: " If motion detector detects motion, The siren turns on"
- **Includes:** Sensor device (Motion detector), Action Device (Siren) , Condition (On=true)

4.3 Network Diagram

The below diagram shows the network topology of our secure smart home network. The design combines IoT devices from many rooms into a unified network structure to guarantee transparency, control and layered security.

Our network structure contains the following essential components:

- **Core Switch and Router:** The main part of the network, located in the control room, which controls the traffic between devices and internet access. All IoT devices run through this.
- **Firewall:** Located between the router and the internet gateway, the firewall allows for filtering of incoming and outgoing traffic restrictions on the internet for unauthorized access.
- **VLAN Segmentation:** The devices are logically separated by room, or by function (i.e., security devices, smart lighting, HVAC systems) with VLANs in order to reduce the attack surface and to contain the threat.
- **IoT Devices:** Installed throughout the house - smart light bulbs, cameras, motion detectors, thermostats, and smart locks. Each room has smart devices relevant to that room, and smart devices are connected via wireless connectivity.
- **Central Server:** Houses a management dashboard and serves to allow real time monitoring, logging of data, and rule-based automation. The central server is isolated within a secured VLAN with administrative access only.
- **Tablet and End Users Dynamics**: Located in the kitchen, two tablets are used by homeowners to either interact with the system through the UI, issue commands, or receive alerts.

4.4 Three Alternative Solutions and Comparisons

When creating a secure smart home structure, there are a couple of planning options to contemplate. Below, we compared three different plan solutions before we made a decision on what to select.

Option 1: Basic Home Router Setup

A straightforward wireless router which has WPA2 security connecting all devices at once. They all share the same network.

Pros:

- Easy to work with and manage.
- Not expensive and is available everywhere.
- Works with most devices.

Cons:

- There is no Isolation between devices (If one of the devices is hacked, others are at risk as well)
- Won't be able to control traffic as much.
- Least logging and monitoring.

Option 2: VLAN-Based Segmentation with Central Control (Our Choice)

Devices are combined into VLANs based on function (sensors,alarms,lighting). A router which contains static IPs and firewall policies to separate traffic, and the tablet can control devices with conditions.

Pros:

- Devices are separated by type.
- It's safer.
- Conditions can be done easily from a central location.
- It can take a high scale of devices.

Cons:

- Hard to configure.
- Requires an understanding of networking.
- May require additional (switches and servers)

Option 3: Flat Network with Manual Control (No Automation Rules)

All IoT devices are connected to the same network but it is only controlled individually through a tablet or PC. No automation or any conditions that are implemented , devices are manually controlled by turning them on/off by the owner as he needs.

Pros:

- It's simple to work with (configure)
- No need for automation or conditions.
- Great for quick testings of how a device works.

Cons:

- No automation, which will be more work for the owner or the user.
- Not reliable for emergencies.
- All devices share the same network with no separation.

Our Choice

We Chose option 2 because it has a counterbalance between security, managing and flexibility. It allows us to work with procedures like (motion = siren on) as well for fans and much more stuff while having isolation with the help of VLANs and encryption. This design can last for a long term security and segmentation of a smart home.

Chapter 5: Development

5.1 Solution Overview

Our Smart Home Network project was established with security and segmentation as an integral part of the design. The Network design and topology was through use of Cisco Packet Tracer, implementing routers, Layer 2 switches, an ASA firewall, servers, and end devices including IoT technology, PCs for admins, and laptops for the guests. Ultimately, the final topology has become a realistic small-scale home automation network, tasked with function and privilege in mind, by using VLANs, ACLs, and firewall policies.

The Smart Home Network thought process was as follows:

- VLAN usage: Devices were placed into their respective VLANs, those being Admin on VLAN 10, IoT on VLAN 20, Guest on VLAN 30, and User on VLAN 40. Trunk and access ports were correctly configured on the switch.
- Router on a Stick: Our home router interface (G0/1) was used to create sub-interfaces meant for each VLAN with IP addressing and DHCP relay services.
- DHCP setup: The home router was utilized as the DHCP server, providing different IP pools for each VLAN, and for the wireless points to access. When we set up DHCP exclusions it prevented devices from obtaining already used IPs.
- Sticky Port preventive measures: We implemented port security on vital switch ports. These ports utilized sticky MAC addresses and violation counters to monitor and prevent individuals from compromising the system

- DHCP Snooping: DHCP snooping was used on the link from the switch to the router, in the Smart Home Network's case it was just one router, and one switch, therefore just on interface fa0/1. The interface was set using DHCP snooping trust command, and thus was defined to mitigate rogue DHCP server attacks.
- ACLs: VLAN 30 (Guest) was limited to HTTP/HTTPS and DNS. our VLAN 20 setup was intentionally prevented from communicating with VLAN 10.
- Logging and Email Simulation: A syslog and email server received logs and test messages from the network infrastructure.
- DNS and HTTP Services: A central server provided name resolution and hosted the IoT control interface.
- ASA Firewall: Configured with NAT and WebVPN, requiring external users to log in (test/test) to access internal resources via secure bookmarks.

5.2 Outputs

The key deliverables and functional outputs of the project include:

- VLAN Segmentation: Isolated traffic and devices to contain potential breaches and organize the network logically.
- Successful DHCP Distribution: End devices across VLANs received dynamic IPs from the router.
- Rogue DHCP Server Prevention: A test rogue server failed to issue addresses when DHCP snooping was active

- Restricted Guest Access: ACLs prevented VLAN 30 users from accessing admin services or using ICMP, enforcing HTTP/HTTPS only.
- Syslog and Email Logging: Events such as port violations and DHCP issues were logged and simulated email alerts were sent.
- Remote Access via WebVPN: External users accessed the IoT interface only through login and ASA bookmark.

Demonstrable evidence of these outputs includes command-line outputs (e.g., show ip dhcp snooping, show mac address-table, show access-lists, show running-config), successful pings (or denied pings), and GUI-based verifications via browser-based HTTP services and ASA login prompts.

5.3 User Manual

Accessing VLAN Devices

- VLAN 10 (Admin): For secure admin PCs. Use SSH or direct access.
- VLAN 20 (IoT): Hosts the central smart home server (192.168.20.100).
- VLAN 30 (Guest): Limited to browsing HTTP/HTTPS.
- VLAN 40 (Users): Standard user access.

Testing DHCP Snooping

1. Plug a rogue DHCP server into a non-trusted port (e.g., Fa0/2).
2. Shut down the router's DHCP pool for the VLAN.
3. Observe failure in IP assignment on the end device (IP Configuration -> DHCP).
4. Confirm via show ip dhcp snooping binding and lack of IP.

Port Security Demonstration

- Reconnect a device with a different MAC to a sticky-enabled port.
- Observe port shutdown (show port-security interface Fa0/x).

ACL Verification

- From VLAN 30, attempt to ping or SSH into 192.168.10.1 (should fail).
- Attempt HTTP access to 192.168.20.100 (should succeed).

Syslog and Email

- Trigger a violation (e.g., unauthorized MAC).
- Check Syslog server for new entry.
- View simulated email in the admin's mailbox.

Remote Access

1. From an outside PC, access https://203.0.113.1.
2. Login with test/test.
3. Click on SmartHomeNetwork bookmark to access http://203.0.113.10/home.html.

Chapter 6: Evaluation and Conclusion

6.1 Solution Testing

The network of the smart home was tested in a laboratory using Cisco Packet Tracer. Testing included:

- **Device Connectivity:** That all the IoT devices would be able to communicate within VLANs defined but appropriately isolated in other segments (e.g., IoT, trusted users, guest).
- **Security Testing:** Verified the firewall rules, VPN remote access, and WPA3 wireless encryption configurations.
- **Monitoring Utilities:** Used Wireshark to capture network traffic and confirm encryption and access control mechanisms were correctly preventing unauthorized access.
- **Failover Testing:** Simulated device disconnections and network loss to test system response and ensure resilience without significant downtime.

Testing confirmed the necessary security controls were operating as designed and the network could handle standard cyber attacks in an emulated smart home environment.

6.2 Verification

Verification was to make sure that the network met the technical requirements and project objectives as defined in the scope:

- **VLAN Segmentation:** Successfully implemented with segmented traffic.
- **WPA3 Encryption:** Wireless network established and verified to be running WPA3 encryption.
- **Firewall and ACLs:** Firewall configuration and Access Control Lists (ACLs) were confirmed to be blocking unauthorized traffic effectively.
- **VPN Access:** Remote access via Cisco AnyConnect VPN was working and encrypted.
- **Compliance:** The minimum GDPR and CCPA data protection standards were achieved in design and implementation.

All the system elements were installed and verified against the original design specifications for technical correctness.

6.3 Validation

Testing confirmed that the final network configuration not only met technical requirements but also served end-client requirements:

- **Usability:** The network offered easy access for authorized clients without requiring time-consuming manual configurations.
- **Performance:** Network speed and reliability were measured, with the security features having little effect on system performance.

- **Security:** Simulated penetration testing and traffic monitoring validated that common attack vectors like wireless unauthorized access and internal attacks were effectively thwarted.
- **User Feedback:** The users who tested the system reported hassle-free access to devices like smart thermostats, cameras, and lights without experiencing network interruptions, demonstrating that the system was user-friendly.

Overall, the final network solution was verified to be efficient, secure, and user-appropriate.

6.4 Team Conclusions

Helly Patel- The Secure Smart Home Networking project successfully accomplished its mission of developing and deploying a secure and stable smart home network environment. Utilizing Cisco technologies, VLAN segmentation, firewall settings, WPA3 encryption, and VPN remote access, the team developed a highly effective network that is resistant to common cyber attacks and easy to use for end-users.Extensive testing and validation guaranteed the network was secure, stable, with compliance to standards like GDPR and the NIST Cybersecurity Framework, and performance-optimized. Generally speaking, the project highlighted the importance of having strong cybersecurity capabilities included in smart home networks and the team's ability to offer a professional-level, scalable solution.

Jared Collazo- Our Smart Home Network infrastructure we developed has proven the effectiveness of the design and practicality of what a secure home network should look like.

We accomplished this using integral networking principles like VLAN segmentation, ACL integration, DHCP snooping, and sticky port/sticky MAC. Through brainstorming and planning and testing, we were able to prevent unwanted access, protect the network, and only allow those devices that are approved to connect and communicate with our network. This small form secure home network we created is scalable, efficient, and a secure place that uses industry methodologies, and showcases the importance of active defense in modern homes.

Fadi Meleika- Working on the Secure Smart Home Network project helped me strengthen my skills in networking by managing infrastructure as well as configuring router, switches, VLANs and wireless access points. Also adding conditions for IoT devices for motion detectors and sirens which insures a secured home network structure. Making sure that all smart devices are secured correctly within the network. These gave me hands-on experience applying security measures in a sensible home network.

Jesus Calvo- Our smart home has successfully met the scope and features we had set out to meet. We used VLANs, ACLs, DHCP snooping, and sticky MAC to make our network secure. We also connected all the IoTs to a server to control all the devices from a portal.We also set up a clientless vpn so that the IoTs could be access from anywhere as long as you have the right login information. We made sure to follow proper security practices when we set everything up.