19CSE301 - COMPUTER NETWORKS

Case Study

Smart Home Automation System

Group Number - 13

Registration No	Name	Email ID	Contribution
CB.EN.U4CSE 21617	Veda Sai G	cb.en.u4cse21617 @ cb.students.amrita.edu	IP Addressing, DNS Server
CB.EN.U4CSE 21649	Joel P	cb.en.u4cse21649 @ cb.students.amrita.edu	Cell Tower Configuration
CB.EN.U4CSE 21657	Shenthan Marru	cb.en.u4cse21657 @ cb.students.amrita.edu	VLAN, IoT Devices Configuring
CB.EN.U4CSE 21670	Y Sri Bhargav	cb.en.u4cse21670 @	Subnetting, IoT Server

		cb.students.amrita.edu	

Problem Statement

The smart home automation project entails the integration of four distinct houses—Veda House, Shenthan House, Joel House, and Bhargav House—each featuring an array of IoT devices. Noteworthy aspects during the design and implementation phase involve the allocation of static IP addresses and subnetting for each house.

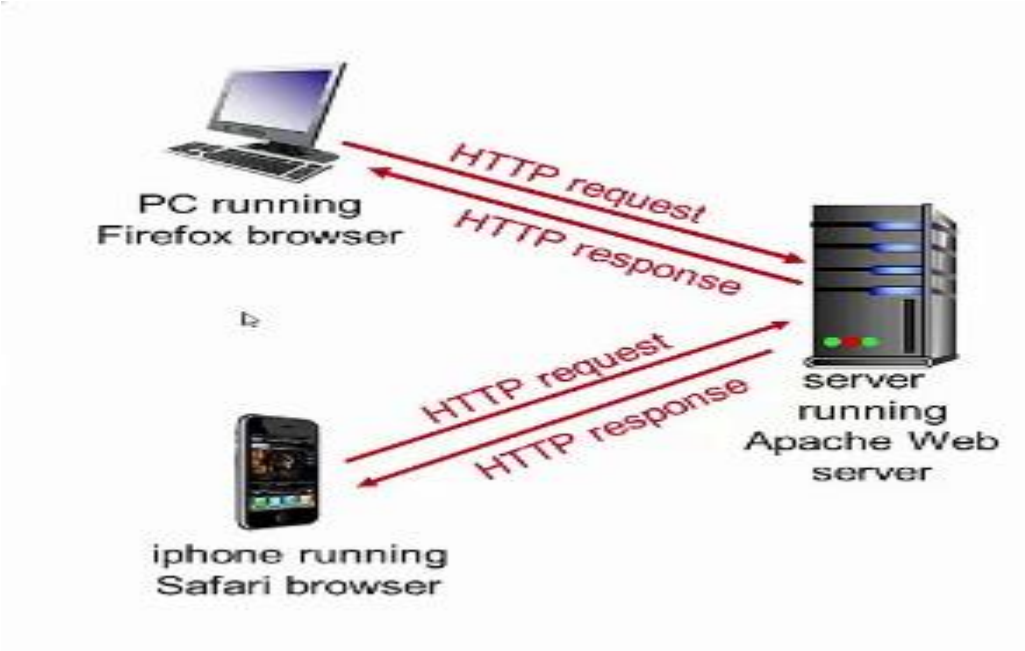
Specifically, Veda House adopts the subnet 172.17.68.1/26, Shenthan House utilizes 172.17.68.65/26, Joel House operates on 172.17.68.129/26, and Bhargav House employs 172.17.68.203/26.

Wi-Fi networks are established in each house to facilitate IoT device connectivity. Further organization involves VLANs, with each department assigned to a respective VLAN and designated IP address range. For routing, OSPF is implemented, ensuring efficient communication among devices.

The project mandates static IP address assignment, foregoing DHCP, for all devices. Additionally, SSH is configured on routers for remote login, fostering secure monitoring and control. This comprehensive approach aims to create a secure, interconnected smart home ecosystem across the four houses with statically assigned IP addresses for enhanced control and monitoring.

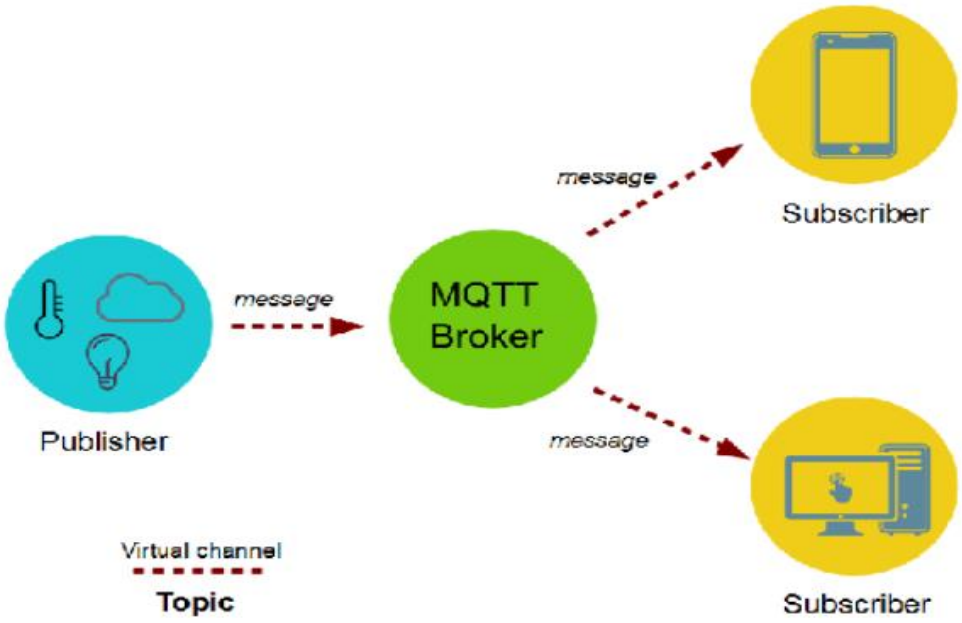
Protocols Used and Their Analysis

1.) HTTP:



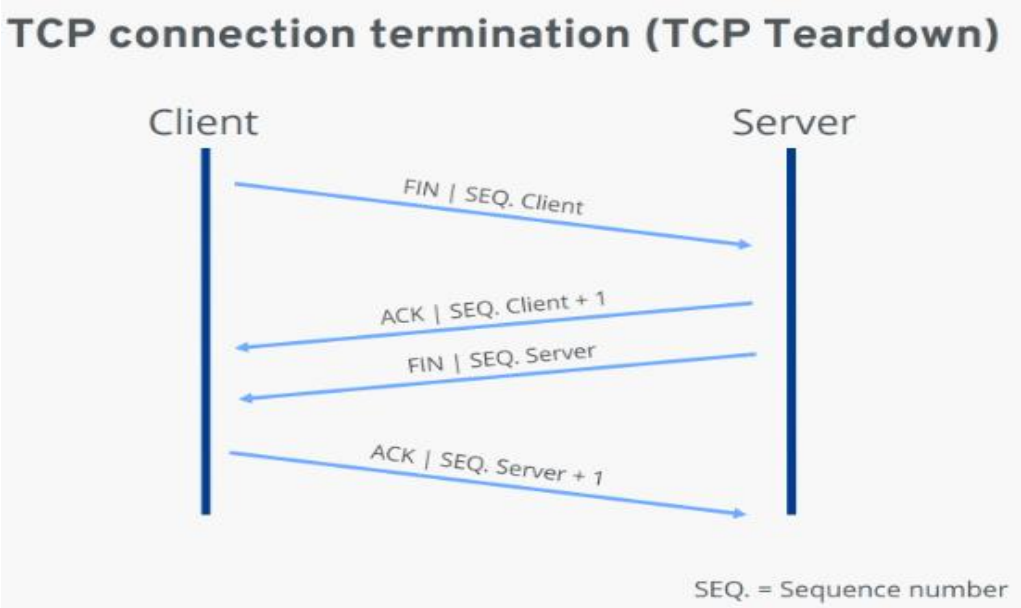
The Hypertext Transfer Protocol (HTTP) serves as the fundamental communication protocol for the World Wide Web. Operating on a request-response model, HTTP enables clients, such as web browsers, to send requests to servers, which respond with the requested data or error messages. Characterized by its connectionless and stateless nature, each client request is treated independently. HTTP employs various methods (GET, POST, etc.) to signify actions on resources, identified by Uniform Resource Identifiers (URIs). Headers in requests and responses convey essential information, while status codes communicate the outcome of requests. Security considerations advocate for HTTPS to encrypt data during transmission. Despite its stateless design, mechanisms like cookies or sessions are often employed for maintaining continuity across multiple requests. The protocol has evolved, with HTTP/3 aiming to enhance performance in contemporary web application

2.)MQTT:



The Message Queuing Telemetry Transport (MQTT) protocol plays a pivotal role in the Internet of Things (IoT) communication landscape. Operating on a publish-subscribe model, IoT devices, such as sensors, publish messages to specific topics, acting as channels. An MQTT broker receives and routes these messages to subscribers interested in corresponding topics, which can include web servers or other devices. Web servers, acting as MQTT clients, subscribe to relevant topics, enabling them to receive real-time updates from devices. The bidirectional nature of MQTT allows servers to not only receive data but also send commands to devices by publishing messages to specific topics. Quality of Service (QoS) levels ensure message delivery reliability, ranging from at most once to exactly once. Security considerations involve implementing Transport Layer Security (TLS) to encrypt communication between devices and the MQTT broker, safeguarding sensitive data. In summary, MQTT facilitates lightweight, efficient, and real-time communication in IoT scenarios, employing a flexible publish-subscribe architecture.

3.)TCP:



The Transmission Control Protocol (TCP) stands as a foundational protocol in network communication, providing reliable and connection-oriented data transfer. Operating at the transport layer of the Internet Protocol (IP) suite, TCP ensures the integrity and ordered delivery of data between devices. Utilizing a three-way handshake, TCP establishes a connection before data exchange, enhancing reliability. Once the connection is established, data is transmitted in the form of streams, with each segment acknowledged to ensure successful delivery. In the event of lost or corrupted segments, TCP employs mechanisms such as retransmission to guarantee data integrity. Flow control mechanisms prevent overwhelming the receiver, optimizing data transfer rates. TCP is instrumental in supporting various application layer protocols, including HTTP, MQTT, and many others. Its reliability, error recovery features, and widespread adoption make it a cornerstone of modern network communication.

Why networking is required for the application?

Networking is integral to smart home automation projects as it enables communication and coordination among diverse devices, facilitating centralized control and automation logic. It allows for remote access and data collection, empowering users to monitor and control their homes from anywhere. Additionally, networking supports firmware updates, maintenance, and scalability, ensuring the seamless integration of new devices and the adaptability of the system. The ability to integrate with external services, optimize energy efficiency, and enhance the overall user experience underscores the significance of networking in creating intelligent and interconnected smart home environments.

Furthermore, networking plays a pivotal role in enhancing the security and reliability of smart home automation systems. With secure communication protocols, such as encrypted data transmission and authentication mechanisms, networking helps safeguard sensitive information and prevents unauthorized access to smart devices. Redundancy and fault tolerance features inherent in networking protocols contribute to the reliability of smart home systems, ensuring consistent operation even in the face of network disruptions or device failures. The synergy between networking and smart home automation not only empowers users with advanced control and monitoring capabilities but also establishes a foundation for innovation, enabling the integration of emerging technologies and the continuous evolution of intelligent home environments.

Why do we need to measure network performance?

Measuring network performance in a smart home automation system is crucial for several reasons. Firstly, it ensures that all connected devices, such as smart thermostats, security cameras, and voice assistants, function optimally. By monitoring network performance, homeowners can identify and address any issues that may arise, such as slow connectivity or dropped signals, which could disrupt the seamless operation of their smart home.

Secondly, measuring network performance allows for the optimization of the system's overall efficiency. By analyzing metrics like bandwidth usage, latency, and packet loss, homeowners can make informed decisions about network upgrades or adjustments to ensure that their smart home operates at its full potential.

Furthermore, monitoring network performance is essential for ensuring the security of the smart home system. By tracking data traffic and identifying any anomalies, homeowners can detect potential security breaches or unauthorized access to their network, thereby safeguarding their personal information and privacy.

In addition, measuring network performance provides valuable insights for troubleshooting and maintenance. By regularly assessing the performance of the network, homeowners can proactively address any issues before they escalate, minimizing downtime and disruptions to their smart home automation system.

Overall, measuring network performance in a smart home automation system is essential for ensuring seamless operation, optimizing efficiency, enhancing security, and facilitating proactive maintenance. By staying vigilant and proactive in monitoring network performance, homeowners can enjoy the full benefits of their smart home while minimizing potential drawbacks.

Performance parameters:

Parameter	Meaning	Formula
Bandwidth	Bandwidth is the capacity of a wired or wireless network communications link to transmit the maximum amount of data from one point to another over a computer network or internet connection in a given amount of time	Expressed as bits per second (bps), modern network links have greater capacity, which is typically measured in millions of bits per second (megabits per second, or Mbps) or billions of bits per second (gigabits per second, or Gbps).

Throughput	Throughput measures the percentage of data packets that are successfully being sent; a low throughput means there are a lot of failed or dropped packets that need to be sent again.	
Packet Loss	Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination.Due to network congestion	Efficiency = 100% * (transferred - retransmitted) / transferred Network Loss = 100 - Efficiency

Transmission time	The time required for transmission of a message depends on the size of the message and the bandwidth of the channel.	Transmission time=Message size / Bandwidth
Propagation Time	Propagation time measures the time required for a bit to travel from the source to the destination. The propagation time is calculated by dividing the distance by the propagation speed.	Propagation time = Distance /Propagation speed
Processing Delay	Time taken by the processor to process the data packet is called processing delay.	
Queuing Delay	Time spent by the data packet waiting in the queue before it is taken for execution is called queuing delay.	

Jitter	Jitter is defined as the variation in time delay for the data packets sent over a network. This variable represents an identified disruption in the normal sequencing of data packets. Jitter is related to latency, since the jitter manifests itself in increased or uneven latency between data packets, which can disrupt network performance and lead to packet loss and network congestion. Although some level of jitter is to be expected and can usually be tolerated, quantifying network jitter is an important aspect of comprehensive network	Latency=sum of all delays To measure Jitter, we take the difference between samples, then divide by the number of samples (minus 1).

Technologies Implemented:

1. Creating a network topology using Cisco Packet Tracer.
2. Connecting IoT devices with Correct cabling, and setting them up to communicate with the Home Gateway for them to be Remotely Controlled/ Automated

3. Creating VLANs and assigning ports VLAN numbers.
4. Subnetting and IP Addressing.
5. Configuring Inter-VLAN Routing (Router on a stick).
6. Configuring DHCP Server (Router as the DHCP Server).
7. Configuring switchport security or Port-Security on the switches.
8. Configuring WLAN or wireless network (Cisco Access Point).
9. Host Device Configurations.
10. Test and Verifying Network Communication.

Routing Algorithms

In the case of Inter-Device communication between the IoT devices within the home, the following routing algorithms are involved:

1) Static Routing: The home gateway can use static routing tables to direct traffic between devices within the home network. This involves manually configuring the routing paths, making it suitable for smaller, less dynamic networks like a typical smart home setup.

2) Link-State Routing: In a more sophisticated smart home network with a larger number of interconnected devices, a link-state routing algorithm could be employed by the home gateway to maintain a detailed map of the network and calculate optimal paths based on this information.

This works by:

- each router in the network maintains a detailed map of the network topology, including information about its directly connected neighbors and the cost of the links to reach them.
- periodically exchange link-state advertisements (LSAs) to inform each other about their local network topology and link costs, allowing every router to build a complete and consistent view of the network.

- Using the received link-state information, each router independently creates a routing table that contains the best path to reach each destination.

Implementing VLANs:

A VLAN, or Virtual Local Area Network, is a technology that enables the creation of logical, isolated networks within a physical network infrastructure.

Security: Through VLANs, we're adding an additional layer of network security by isolating traffic within specific VLANs. Devices such as Motion Detectors, Security WebCams, Fire Detectors within one VLAN typically cannot communicate directly with devices in another VLAN without explicit configuration, helping to contain the impact of security breaches or unauthorized access.

Implementation:

We're designing our smart home automation in homes that're part of a community. Each home would be having critical devices like fire detectors, smoke detectors, fire sprinklers, webcams etc for security.

However, adding a separate switch and router for each of the houses would be very expensive, and hence we've connected these devices of all the houses to one single switch, through which we implement VLAN by assigning all the devices of a single home IP addresses from a single pre-defined subnet.

Within the subnet, the VLANs (Operating at level 2 of OSI, communicating using MAC addresses)

BENEFITS OF WIRELESS NETWORKING COMPARED TO WIRED NETWORKING

The choice between wireless and wired networking in a smart home project involves trade-offs, and the benefits of wireless networking in the context of the smart home automation project include:

Flexibility and Mobility:

Wireless networking allows for greater flexibility in device placement and mobility. Smart home devices can be easily moved or added without the constraints of physical cables, providing more adaptable and user-friendly configurations.

Ease of Installation:

Setting up a wireless network is generally simpler and less time-consuming than installing wired infrastructure. This is particularly advantageous in a smart home context, where ease of deployment is crucial for user adoption.

Wireless networks are easily scalable, allowing for the addition of new devices without the need to lay or adjust physical cables. This scalability is beneficial as smart home ecosystems often grow over time with the introduction of new devices and functionalities.

Cost Savings on Infrastructure:

Wired networks require the installation of physical cables, conduits, and connectors, which can contribute to higher installation costs. Wireless networks eliminate the need for these components, potentially resulting in cost savings, especially in retrofitting existing homes.

Wireless connectivity is almost universally supported by modern smart home devices. Most IoT devices are designed with built-in Wi-Fi or Bluetooth capabilities, making them inherently compatible with wireless networks. Wireless networks enable convenient remote access to smart home devices. Users can control and monitor their devices from anywhere within the range of the wireless

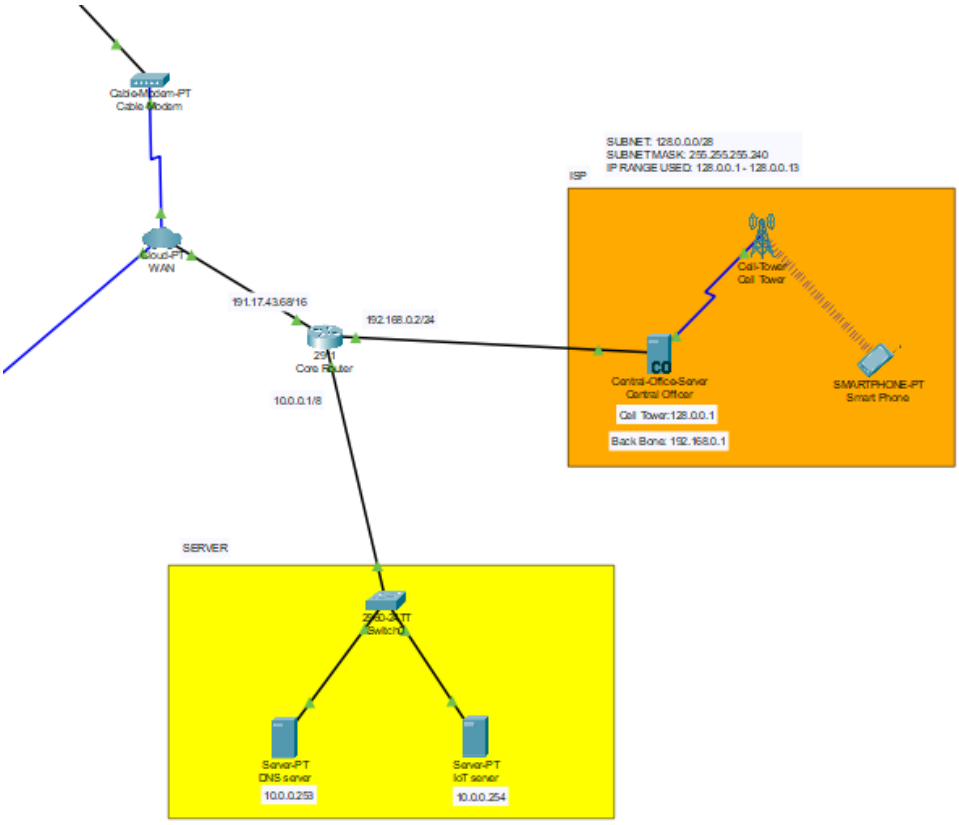
network, enhancing accessibility and convenience. The absence of physical cables reduces visual clutter in the smart home environment. This contributes to a cleaner and more aesthetically pleasing living space, aligning with the modern design preferences of smart home enthusiasts.

Easier Integration of Mobile Devices:

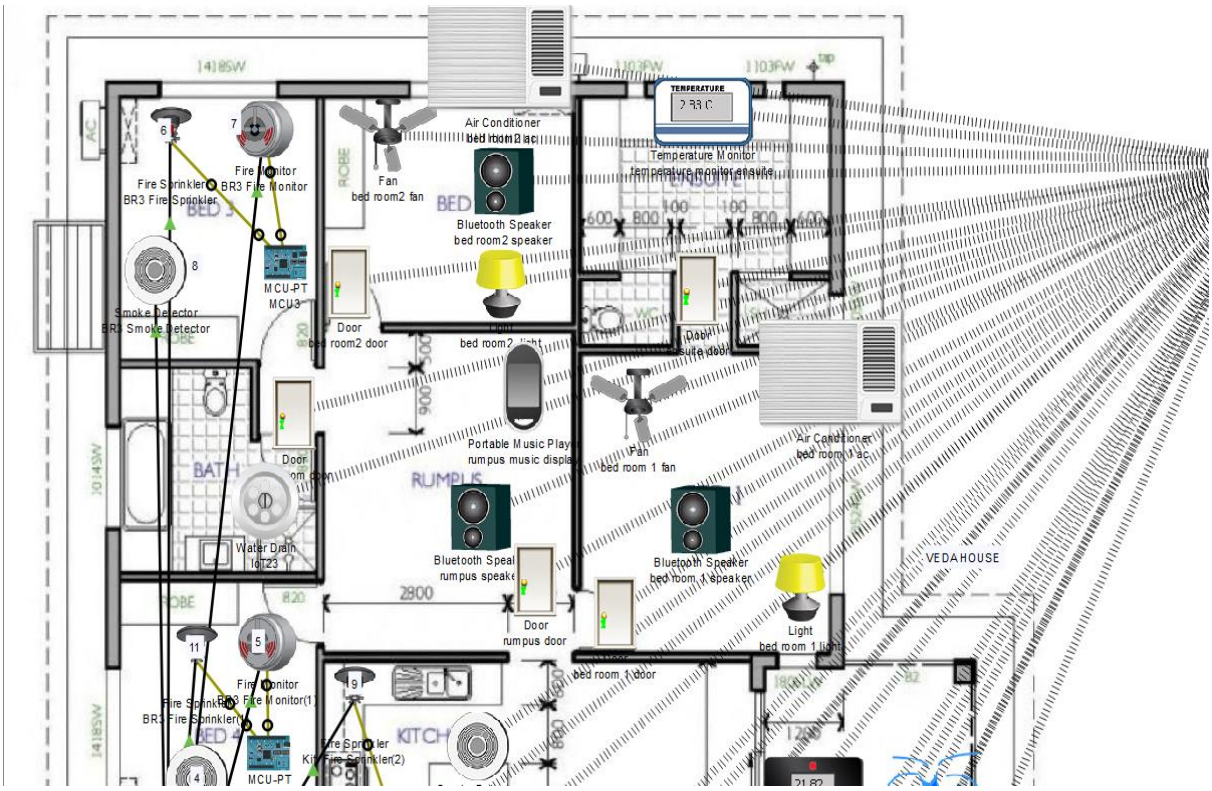
Wireless networking seamlessly integrates with mobile devices, such as smartphones and tablets, which are often central to smart home control. Users can interact with their smart home ecosystem from the convenience of their mobile devices without being tethered to a physical connection.

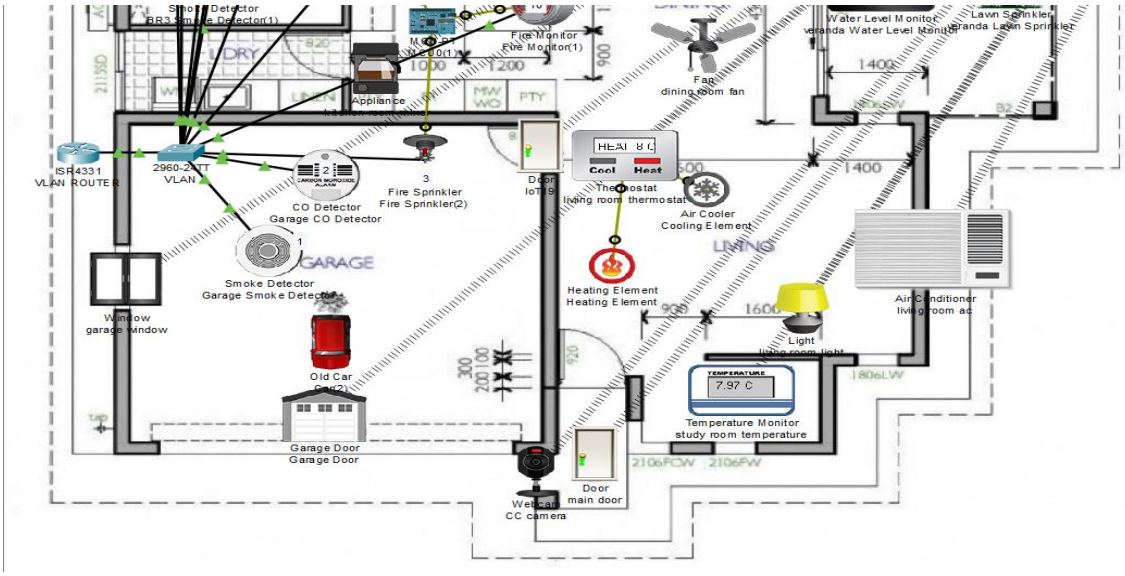
ARCHITECTURE DIAGRAM(CISCO PACKET TRACER):

Server side:

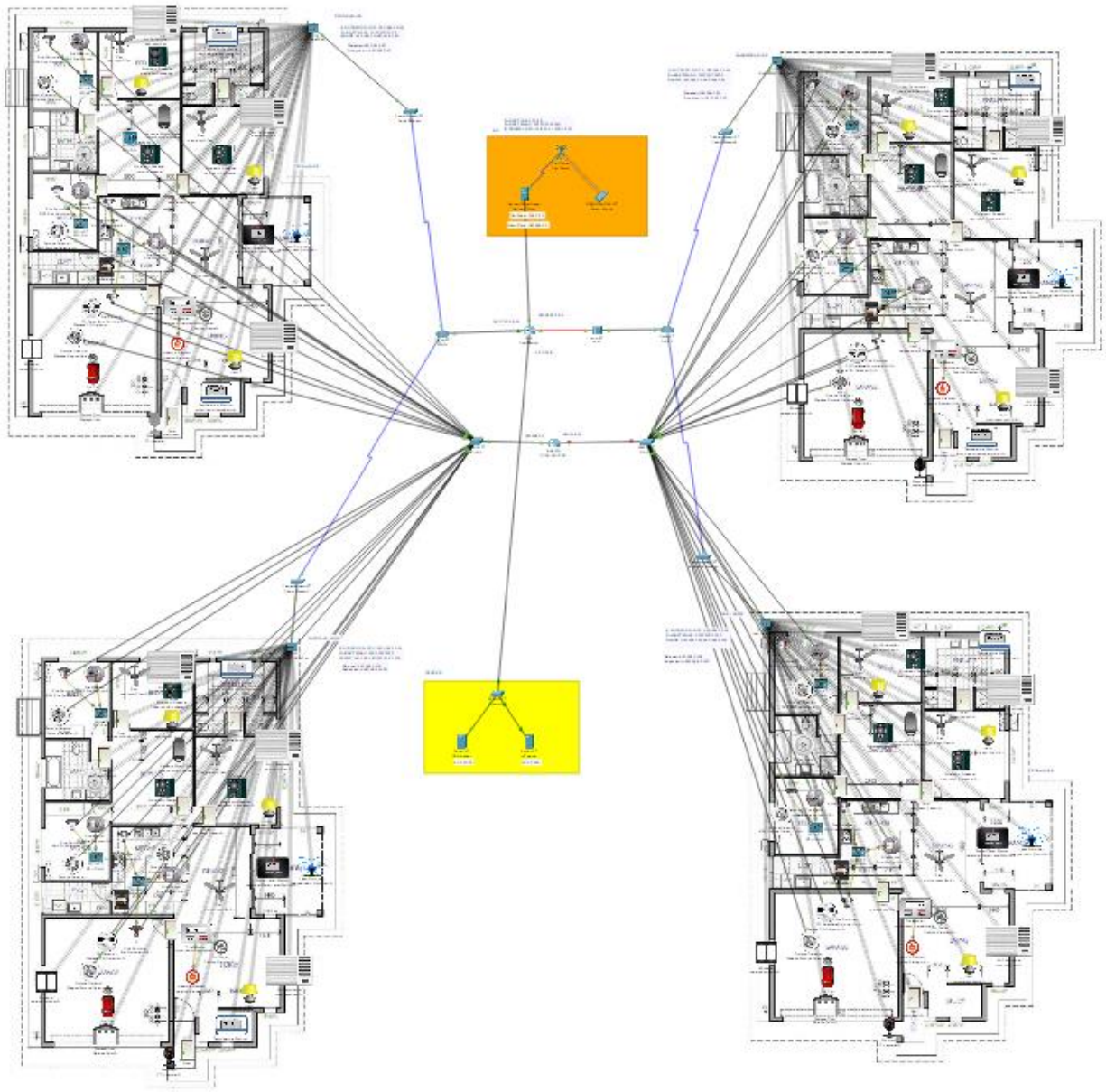

Cable-Modem-PT
Cable Modem
Cloud-PT
WAN
191.17.43.68/16
2911
Core Router
192.168.0.2/24
10.0.0.1/8
SUBNET: 128.0.0.0/28
SUBNETMASK: 255.255.255.240
IP RANGE USED: 128.0.0.1 - 128.0.0.13
ISP
Cell-Tower
Cell Tower
CO
Central-Office-Server
Central Office
Cell Tower:128.0.0.1
Back Bone: 192.168.0.1
SMARTPHONE-PT
Smart Phone
SERVER
2960-24TT
Switch0
Server-PT
DNS server
10.0.0.253
Server-PT
IoT server
10.0.0.254

Client Side:


Air Conditioner
bed room2 ac
Fan
bed room2 fan
Temperature Monitor
temperature monitor ensuite
Fire Sprinkler
BR3 Fire Sprinkler
Fire Monitor
BR3 Fire Monitor
Bluetooth Speaker
bed room2 speaker
MCU-PT
MCU3
Smoke Detector
BR3 Smoke Detector
Door
bed room2 door
bed room2 light
Door
ensuite door
Portable Music Player
rumpus music player
Fan
bed room 1 fan
Air Conditioner
bed room 1 ac
Water Drain
IoT23
Bluetooth Speaker
rumpus speaker
Bluetooth Speaker
bed room 1 speaker
VEDA HOUSE
Door
rumpus door
Light
bed room 1 light
bed room 1 door
Fire Monitor
BR3 Fire Monitor(1)
Fire Sprinkler
BR3 Fire Sprinkler(1)
Fire Sprinkler
Kitchen Fire Sprinkler(2)
MCU-PT
MCU4


Smoke Detector
BR3 Smoke Detector(1)
Fire Monitor
Fire Monitor(1)
Water Level Monitor
veranda Water Level Monitor
Lawn Sprinkler
veranda Lawn Sprinkler
Fan
dining room fan
Appliance
kitchen appliance
ISR4331
VLAN ROUTER
2960-24TT
VLAN
CO Detector
Garage CO Detector
Fire Sprinkler
Fire Sprinkler(2)
Door
IoT19
Thermostat
living room thermostat
Air Cooler
Cooling Element
Smoke Detector
Garage Smoke Detector
Heating Element
Heating Element
Window
garage window
Air Conditioner
living room ac
Light
living room light
Old Car
Car(2)
Temperature Monitor
study room temperature
Garage Door
Garage Door
Door
main door
WebCam
CC camera

The whole topology and connectivity:



User authentication web page:

Ping command to check connectivity with Iot server:

```
C:\>ping iot

Pinging 10.0.0.254 with 32 bytes of data:

Reply from 10.0.0.254: bytes=32 time=7ms TTL=126
Reply from 10.0.0.254: bytes=32 time=25ms TTL=126
Reply from 10.0.0.254: bytes=32 time=19ms TTL=126
Reply from 10.0.0.254: bytes=32 time=30ms TTL=126

Ping statistics for 10.0.0.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 30ms, Average = 20ms
```

Assigned passwords and usernames for different clients:

User veda:

Username: veda

Password: veda@iot

User Shenthan:

Username: shenthan

Password: shenthan@iot

User joel:

Username: joel

Password: joel@iot

User bhargav:

Username: bhargav

Password: bhargav@iot

Ip address configuration used for veda house:

IP ADDRESS BLOCK: 192.168.1.0/24
SUBNET MASK: 2255.255.255.0
RANGE: 192.168.1.1-192.168.1.62

Ip address configuration used for shenthan house:

IP ADDRESS BLOCK: 192.168.1.0/24
SUIBNET MASK: 255.255.255.0
RANGE: 192.168.1.65-192.168.1.126

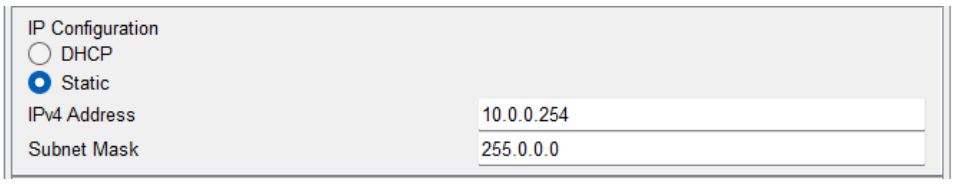
Ip address configuration used for bhargav house:

IP ADDRESS BLOCK: 192.168.2.0/24
SUBNET MASK: 255.255.255.0
RANGE: 192.168.2.1-192.168.2.62

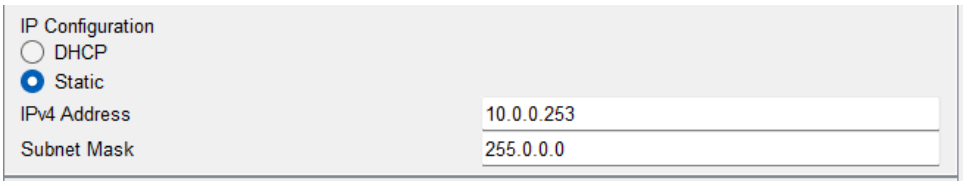
Ip address configuration used for joel house:

IP ADDRESS BLOCK: 192.168.2.0/24
SUBNET MASK: 255.255.255.0
RANGE: 192.168.2.65-192.168.2.126

Iot server:



DNS server:



Conclusion:

In summary, our IoT-based smart house simulation in Cisco Packet Tracer successfully integrated VLANs, subnetting, and routers to create a robust and secure network infrastructure. The implementation of VLANs facilitated the logical segmentation of devices, ensuring efficient management and enhanced security. Subnetting was employed to allocate distinct IP address ranges for each subnet, promoting organized communication among devices. The utilization of routers enabled inter-subnet communication and ensured the seamless flow of data. Additionally, a user-friendly HTTP web app was incorporated, allowing residents to conveniently control their appliances and interact with the smart home ecosystem. This simulation serves as a practical and educational tool, showcasing the effective integration of networking concepts to create an IoT-driven smart home environment within the confines of Cisco Packet Tracer.

References:

1. https://www.youtube.com/results?search_query=cisico+packet+tarcer+iot+devices
2. https://www.youtube.com/watch?v=KwhrRyWPv64
3. https://www.youtube.com/watch?v=EdYOZbX3r7s