Smart Office Network Project: Independent Implementation A Scalable IoT-Enabled Network Design and Simulation

Author:
Nor Aslinawati Binti Abdul Majid
Smart IT Technician Bootcamp October 2025

Executive Summary

This project demonstrates the design, implementation, and testing of a smart office network that integrates both traditional office devices and IoT systems. I independently expanded the scope to include a satellite office, showcasing scalability, network management, and automation capabilities. The network supports wired and wireless communication, employs both static and dynamic IP configurations, and enables IoT device management through a dedicated server and mobile application. This project was entirely planned, designed, and tested independently to demonstrate a practical understanding of modern smart office network infrastructure using Cisco Packet Tracer.

Project Objectives

- Design and implement a smart office network for 8 staff members with IoT devices.
- Extend the network to a satellite office with 6 staff on a separate subnet.
- Test network functionality using PING, TRACERT, and PDU methods.
- Develop a user-friendly guide for onboarding new staff.

Tools & Technologies

Tool / Technology	Purpose
Cisco Packet Tracer	Network simulation and configuration
Gantt Chart & Kanban Boards	Planning and project monitoring
IoT Monitor App	IoT device management
Network Devices	Switches, Routers, PCs, Laptops, Printers, IoT Server, IoT Devices
Protocols	DHCP, Static IP, Wireless SSID configuration

Table 1: Tools & Technologies

Planning

The project was scheduled over four days using Gantt charts and Kanban boards. Key milestones included network design, configuration, IoT integration, and testing phases.

Gantt Chart

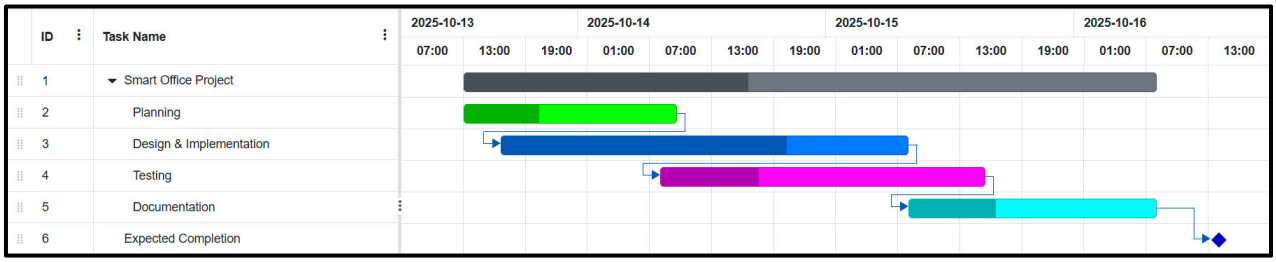


Figure 1: Gantt Chart Overview

Kanban Boards

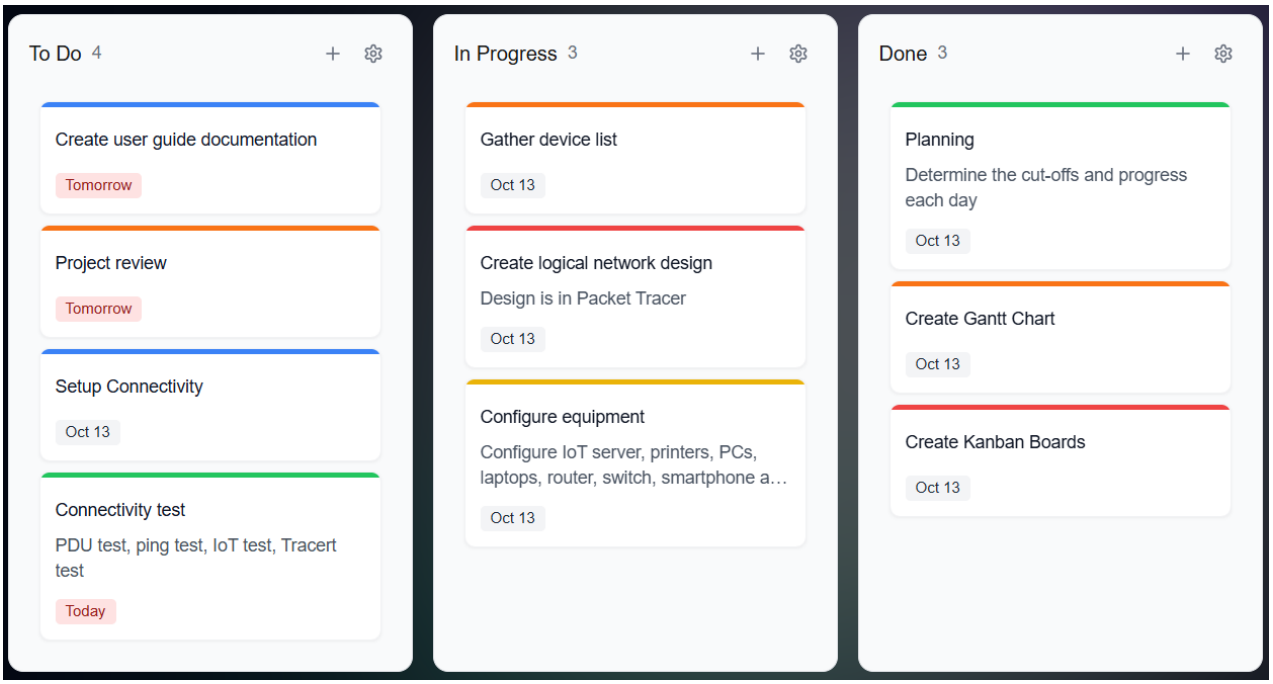


Figure 2: Kanban Boards Overview

Design

Design Brief

The new office space requires the following: A total of 8 members of staff, 4 who are permanently in the office and 4 who are only in the office occasionally (4 hot desks will therefore need to be set up for their devices). Each staff member requires a smartphone (you only need to include one in this project), and the ability to print using both a wireless and a wired printer. The business also wants you to add IoT devices to the network, such as, a coffee machine, a fan, a motion detector and a light. The IoT devices need to be connected to the IoT Server and managed via IoT Monitor App.

Each device configuration (static or dynamic) was chosen based on network efficiency and ease of management. For instance, servers and key PCs were configured with static IPs, while portable devices used DHCP.

The network needs to consist of:

4 desktop PCs (CLIENTS) - 2 with static IP addresses and 2 with DHCP IP addresses	2 printers (one must be wireless)
4 laptops with wireless connections to the network	1 switch
All staff need wireless connections for their phones	1 wireless router with DHCP enabled SSID: SmartOffice Passphrase: Office123
1 IoT Server	4 IoT devices

Table 2: Device listings for Corporate Office

The company are opening another satellite office with 3 office-based staff and 3 remote staff. Replicate what you have done for the first office for this satellite office; including the IoT devices, server and app. This network must be on a different sub-net.

Implementation

The network topology was organized to ensure minimal latency between IoT devices and the core server while maintaining a secure subnet structure for the satellite office.

Logical topology

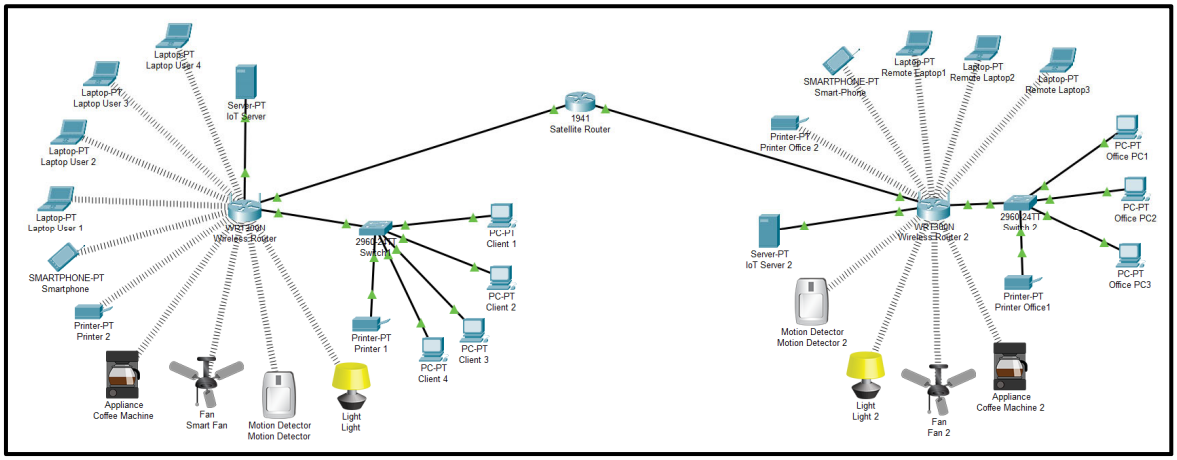


Figure 3: Logical Topology

Physical Topology

Figure 4: Physical Topology

Figure 5: Physical Topology - Corporate Office

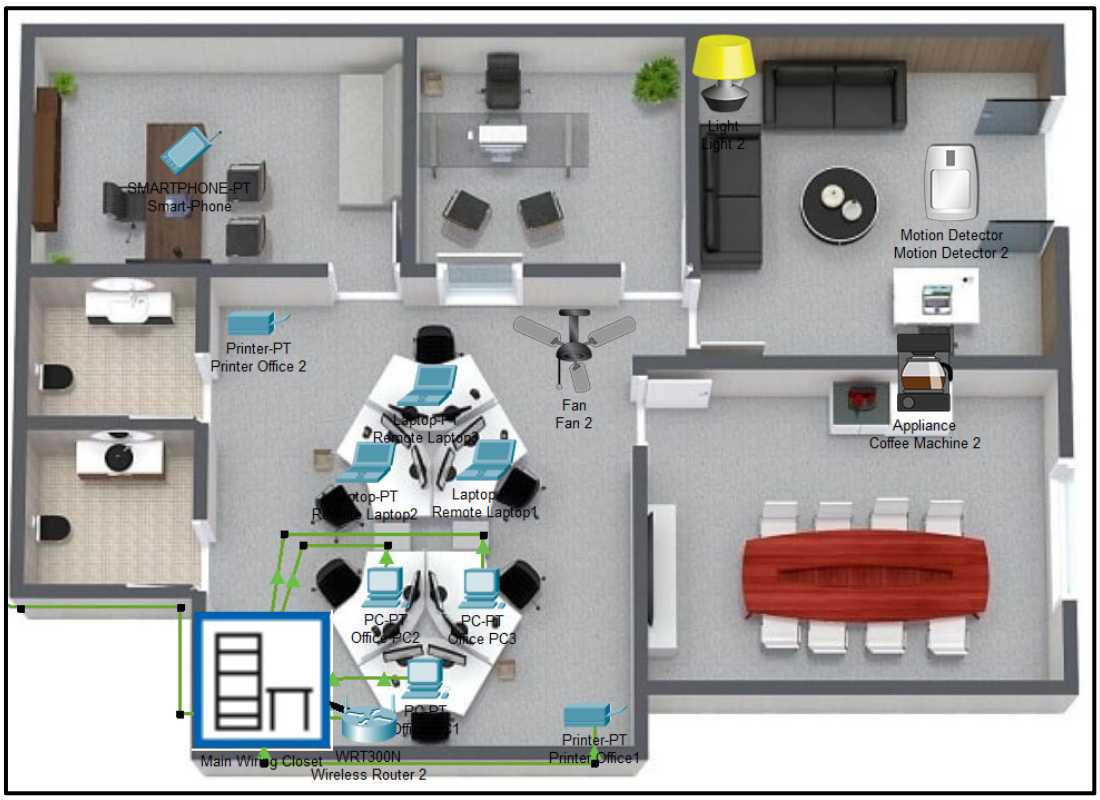


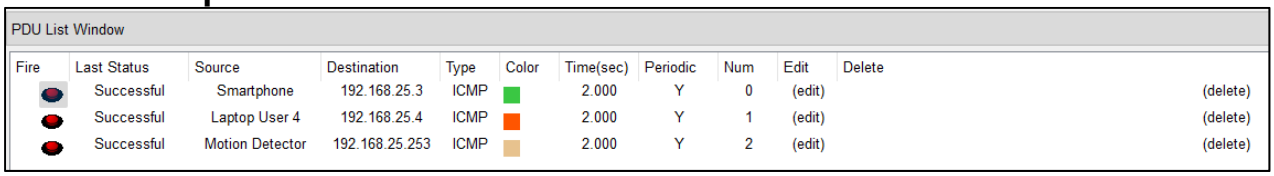
Figure 6: Physical Topology - Satellite Office

Testing

Network functionality was tested using:

- ✓ PING Test: Confirmed device reachability
- ✓ TRACERT Test: Verified routing across subnets
- ✓ PDU Test: Validated data packet delivery
- ✓ IoT Device Test: Ensured devices were properly added, configured, and controlled via the IoT Monitor App

PDU Test Corporate Office

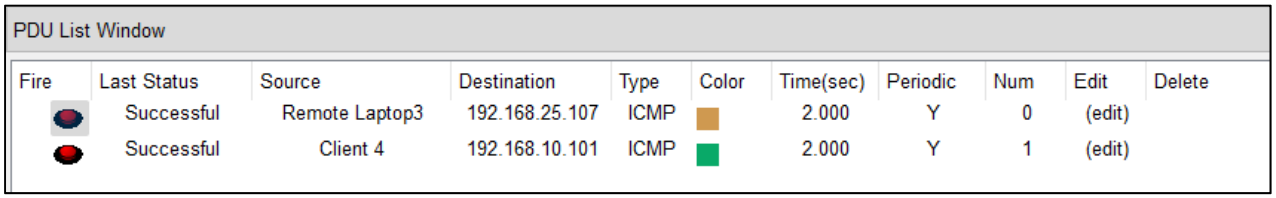


PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Smartphone	192.168.25.3	ICMP		2.000	Y	0	(edit)	(delete)
	Successful	Laptop User 4	192.168.25.4	ICMP		2.000	Y	1	(edit)	(delete)
	Successful	Motion Detector	192.168.25.253	ICMP		2.000	Y	2	(edit)	(delete)

Figure 7: PDU test for Corporate Office results

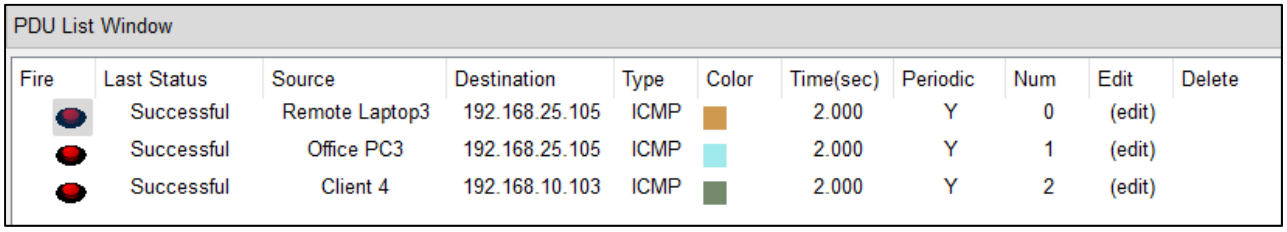
PDU Test Overall



PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Remote Laptop3	192.168.25.107	ICMP		2.000	Y	0	(edit)	
	Successful	Client 4	192.168.10.101	ICMP		2.000	Y	1	(edit)	

Figure 8: PDU test for Corporate Office and Satellite Office results



PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Remote Laptop3	192.168.25.105	ICMP		2.000	Y	0	(edit)	
	Successful	Office PC3	192.168.25.105	ICMP		2.000	Y	1	(edit)	
	Successful	Client 4	192.168.10.103	ICMP		2.000	Y	2	(edit)	

Figure 9: PDU test for Corporate Office and Satellite Office results

Ping Test Corporate Office

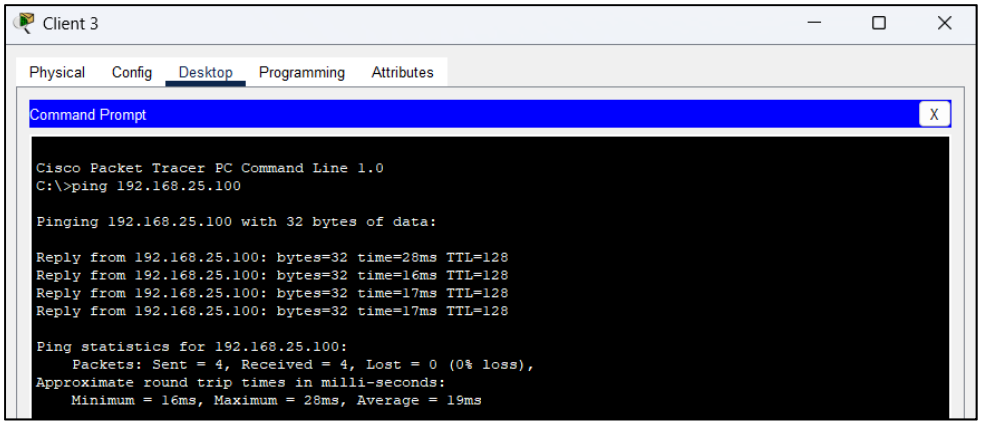


Figure 10: Ping test Corporate Office results

Ping Test Overall

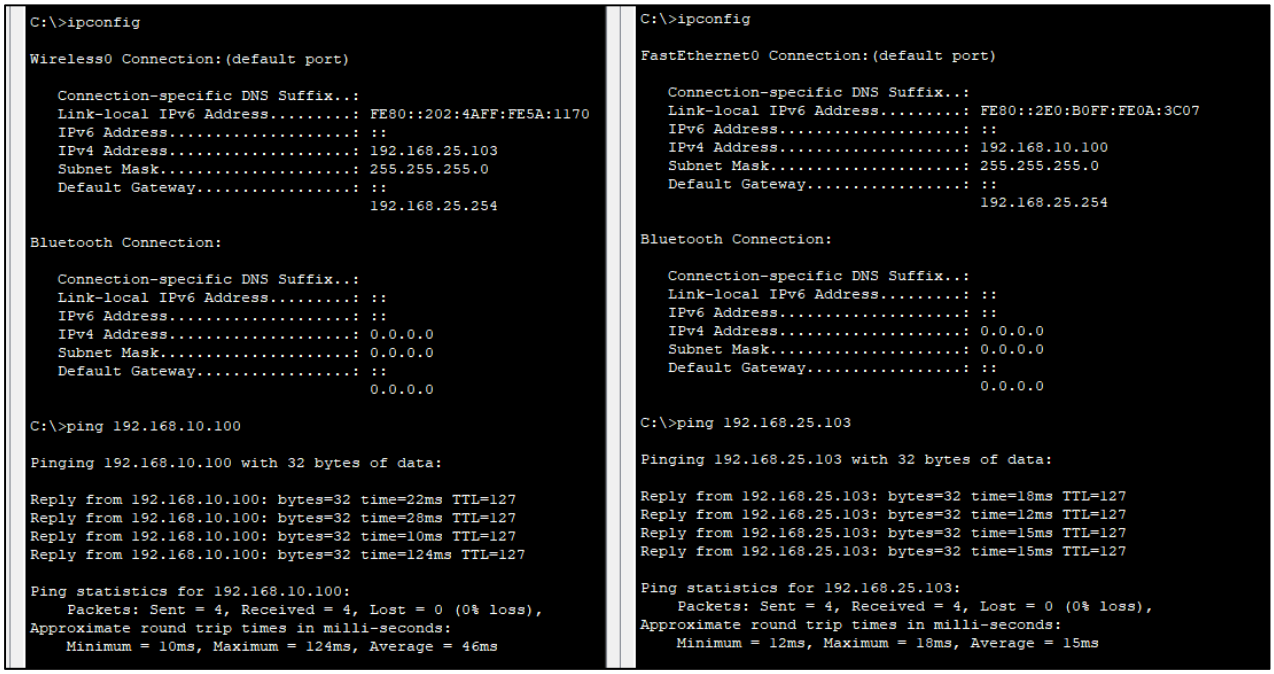


Figure 11: Ping test Corporate Office and Satellite Office results

IoT Test Corporate Office

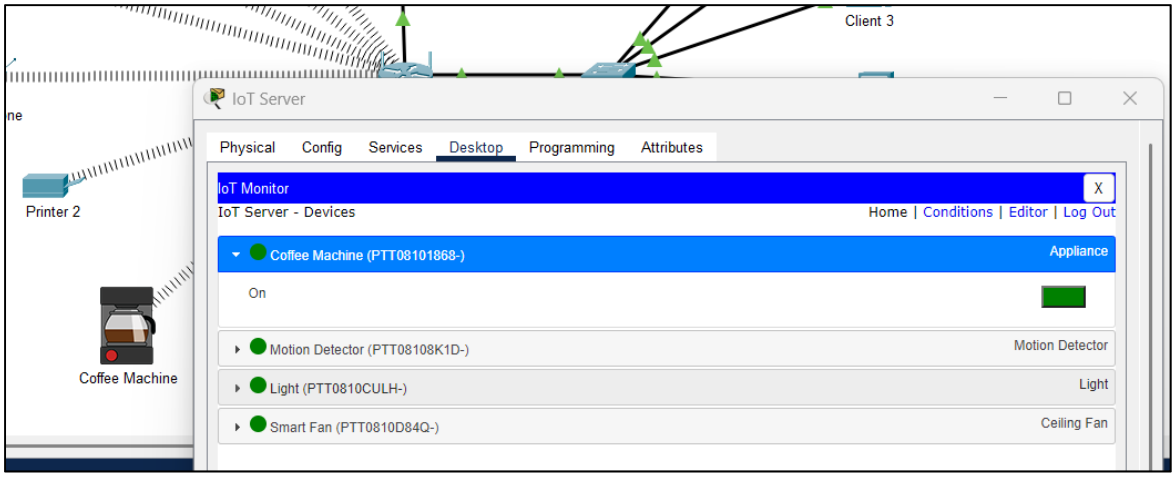


Figure 12: IoT test Corporate Office results

IoT Test Overall

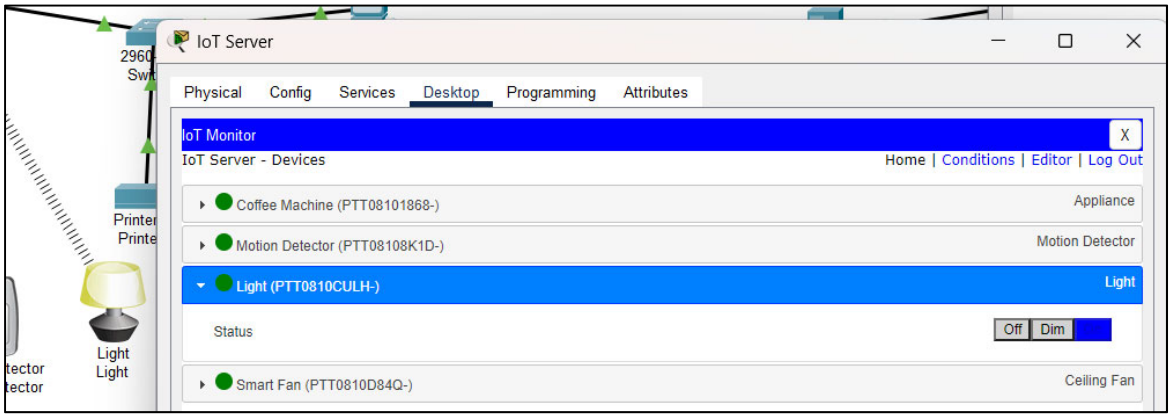


Figure 13: IoT test Corporate Office and Satellite Office results

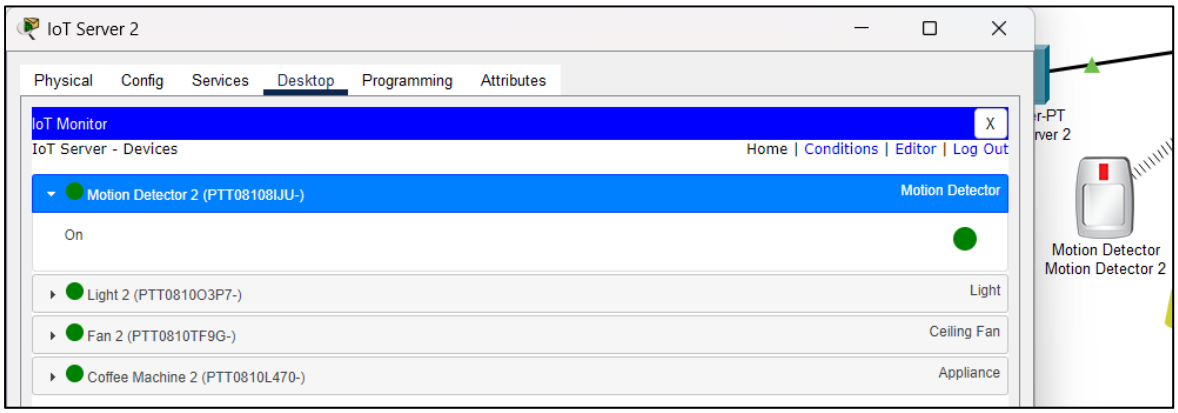


Figure 14: IoT test Corporate Office and Satellite Office results

Tracert Corporate Office

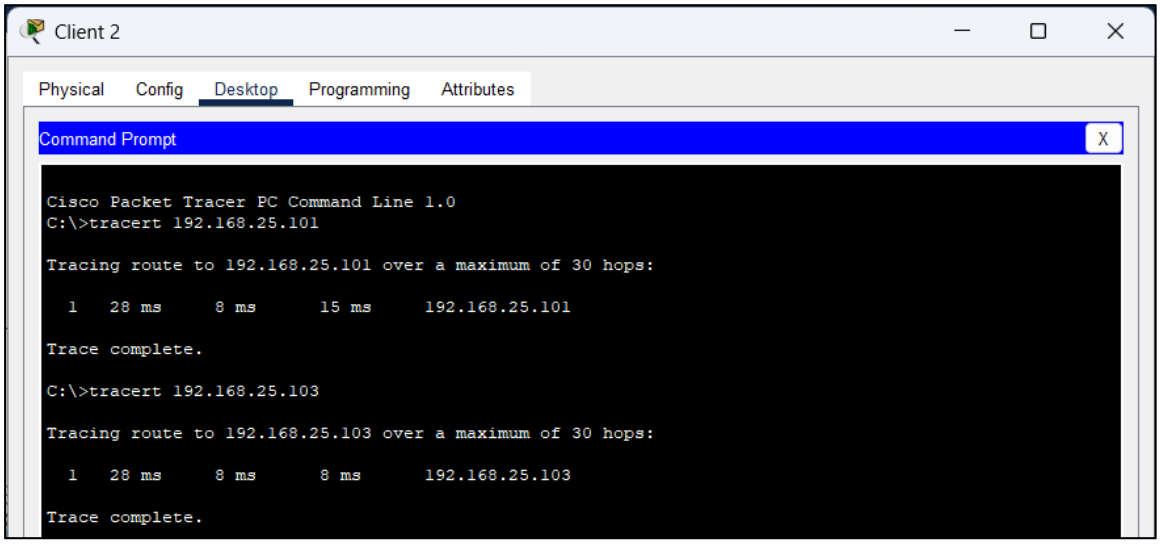


Figure 15: Tracert Corporate Office results

Tracert Overall

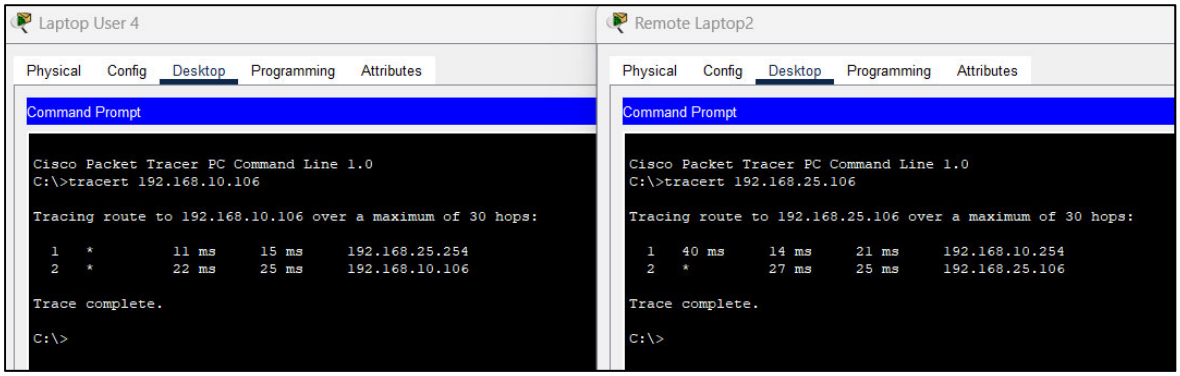


Figure 16: Tracert Corporate Office and Satellite Office results

Documentation

A separate Packet Tracer User Guide document was developed to accompany this project. The guide provides step-by-step instructions for new users or team members to understand, configure, and manage the smart office network.

The documentation covers:

- ✧ Adding devices using static and dynamic IP configuration methods
- ✧ Establishing wired and wireless connections across devices
- ✧ Setting up network access via SSID “SmartOffice” and passphrase “Office123”
- ✧ Adding and configuring IoT devices connected to the IoT Server
- ✧ Operating devices through the IoT Monitor App for real-time management

The guide was designed to serve as a training and reference manual, ensuring that any staff member can confidently operate or modify the network within Cisco Packet Tracer. It also reflects real-world practices such as structured configuration, IP management, and secure wireless setup, making it both educational and practical.

Monitor & Control

Project tracking was updated using Gantt charts and Kanban boards to show task completion.

Gantt Chart

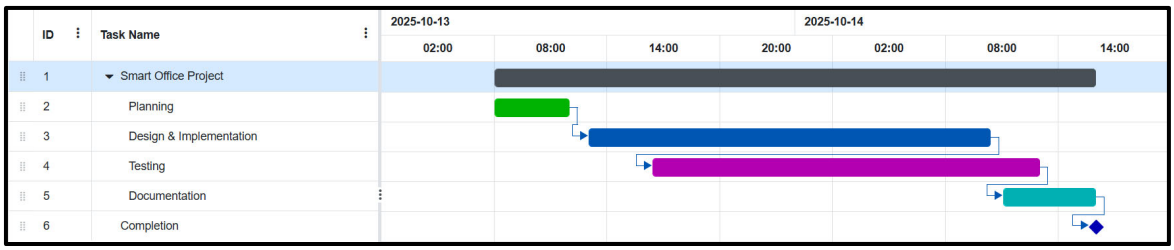


Figure 17: Completed Gantt Chart

Kanban Boards

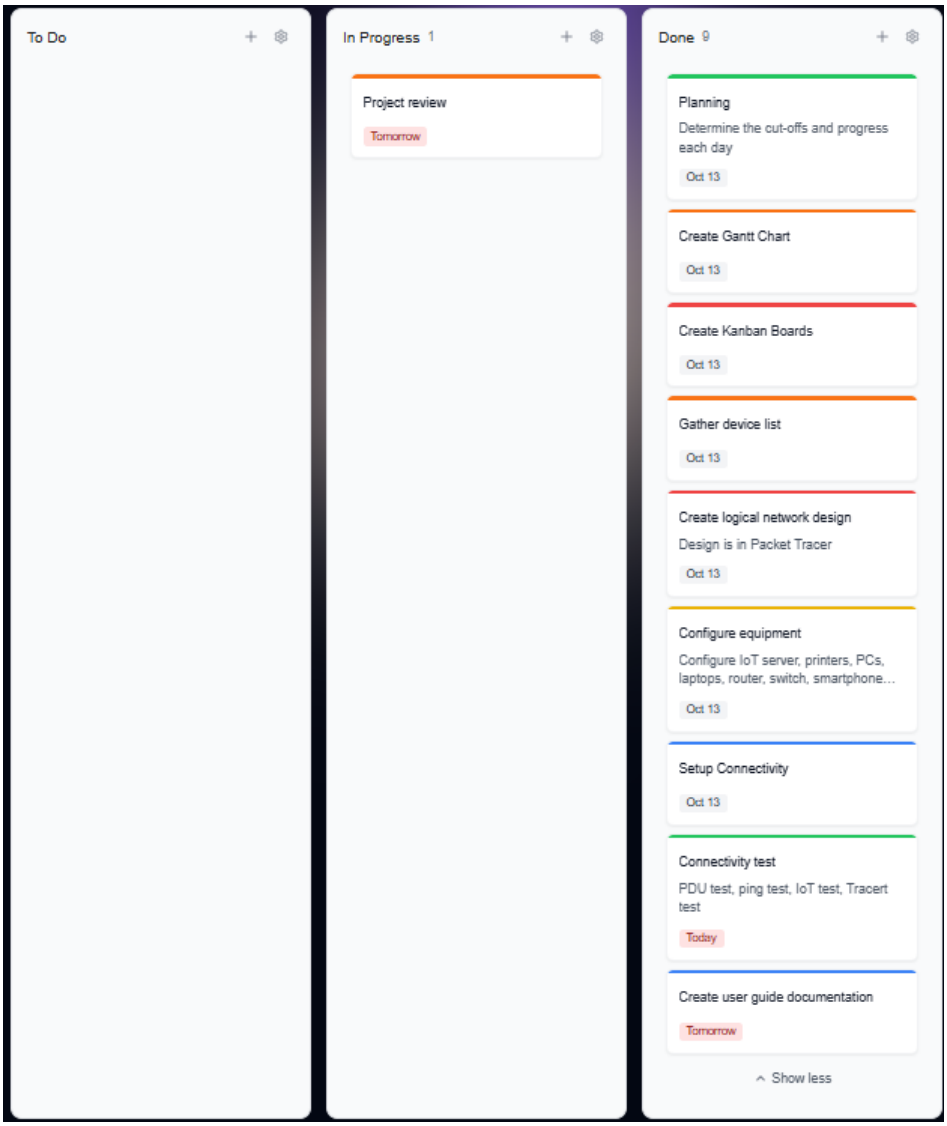


Figure 18: Completed Kanban Board

Post Project Evaluation

1. Client Requirements

The client's requirements for setting up a new corporate office network with both traditional and IoT devices have been successfully met.

Here's how each requirement was achieved:

Client Requirement	How It Was Met
Setup of 4 desktop PCs (2 static IPs, 2 DHCP)	Two PCs were manually assigned static IP addresses, while the other two obtained IPs dynamically through the DHCP-enabled wireless router.
Two printers (one wireless)	One printer was connected via Ethernet cable, and the second printer was configured using the SmartOffice SSID and passphrase "Office123." Both were tested with successful print simulations.
Four laptops with wireless connectivity	All laptops were connected to the wireless router using WPA2-PSK security with SSID "SmartOffice." Successful ping and file transfer tests confirmed connectivity.
Wireless access for staff mobile devices	Mobile devices connected to the WLAN using the same SSID and passphrase, allowing secure access across the network.
Wireless router with DHCP enabled	Configured DHCP pool assigned IPs automatically to wireless clients within the defined subnet. Verified using ipconfig /renew and ping tests.
IoT Server and 4 IoT devices	IoT Server was configured with active Home Gateway service. Four IoT devices (e.g., lamp, fan, sensor) were connected wirelessly and successfully controlled via the IoT Management App.
Network testing and connectivity	All devices responded to pings within the LAN. Traceroute confirmed proper internal routing. The network demonstrated full functionality and device-to-device communication.

Table 3: Client's Requirements meet.

Conclusion: All key client requirements were fully met. The network supports both traditional devices and IoT integration, allowing secure wired and wireless communication across all nodes.

2. Strengths

The strengths of the project are:

1. Successful Network Implementation
The entire network was successfully designed, configured, and tested within the required timeframe. All devices, including PCs, laptops, printers, and IoT devices were able to communicate seamlessly.

2. Effective Use of DHCP and Static IP Configuration
Both static and dynamic IP configurations were correctly implemented and verified, demonstrating flexibility in managing different types of devices.

3. Strong Wireless Configuration and Security
The wireless network was secured using WPA2 with a unique SSID (SmartOffice) and passphrase (Office123), ensuring authorized access and data protection.

4. Functional IoT Integration
The IoT Server and devices were successfully connected and controlled using the IoT Management App, showing an understanding of modern smart office setups.

5. Comprehensive Testing and Troubleshooting
Connectivity tests using ping and tracert confirmed that all wired and wireless devices could communicate efficiently within the local network.

6. Organized Planning and Documentation
The use of Gantt charts and Kanban boards helped structure the project timeline effectively, while proper documentation ensured that configuration steps could be easily repeated or audited.

7. Scalability and Flexibility
The network design allows easy expansion for additional devices or new subnets, such as the satellite office setup.

3. Areas for Development

The areas for development of the project are:

1. Internet Connectivity Simulation
The network currently operates only within a local environment. Future improvements could include simulating external internet access or cloud connectivity for a more realistic enterprise setup.

2. Advanced Security Configuration
While basic WPA2 security and passwords were implemented, additional measures such as MAC filtering, network segmentation (VLANs), and firewall rules could enhance protection.

3. IoT Device Monitoring and Automation
The IoT devices were successfully added and controlled, but the project could be developed further by enabling automation rules or integrating real-time monitoring dashboards.

4. Documentation Detail and Clarity
Although documentation was completed, it could be improved with clearer screenshots, configuration command outputs, and troubleshooting guides for new staff.

5. Scalability Testing
The project could include performance testing under higher traffic or when adding more IoT devices, to ensure network stability as the office grows.

6. Remote Access and VPN Configuration
Implementing VPN or secure remote access for remote staff would enhance flexibility and make the system suitable for hybrid working environments.

7. Backup and Redundancy
No failover or backup router/switch configuration was included. Adding redundancy would improve reliability in case of device or connection failure.

4. Own improvements

If I were to complete this project again, I would focus on improving several key areas:

1. Time Management
I would allocate more specific time slots for testing and documentation to avoid rushing these steps at the end. Creating daily milestones in the Gantt chart would help track progress more effectively.

2. Upskilling and Research
I would take extra time to deepen my understanding of advanced Cisco configurations and IoT automation features to make the network more efficient and secure.

3. Communication and Collaboration
If this were a team project, I would ensure more regular progress updates and clearer task delegation to improve coordination and avoid duplicated effort.

4. Documentation Quality
I would include more screenshots, configuration outputs, and troubleshooting tips to make the user guide easier for beginners to follow.

5. Testing and Troubleshooting
I would carry out more extensive testing scenarios, including stress tests, to identify potential bottlenecks or weaknesses before final submission.

6. Project Presentation
I would improve the visual presentation of diagrams and reports to make the design and results easier for clients and non-technical users to understand.

Overall, this project strengthened my skills in network design, testing, and documentation, while providing hands-on experience with IoT integration and multi-office scalability.