Green University of Bangladesh

Department of Computer Science and Engineering (CSE)
Semester: (Spring, Year: 2025), B.Sc. in CSE (Day)

Hotel Management System

Course Title: Computer Networking Lab
Course Code: CSE 312
Section: 223 D5

Students Details

Name	ID
Anisur Rahaman Maruf	222902078
Ammar Bin Anwar Fuad	222902083

Submission Date: 15/05/2025
Course Teacher's Name: Rusmita Halim Chaity

[For teachers use only: Don't write anything inside this box]

Lab Project Status	
Marks:	**Signature:**
Comments:	**Date:**

Contents

Chapter 1

Chapter 01

1.1 Abstract

This project proposes a **Cisco-Based Hotel Management System**, focusing on efficient networking infrastructure to support various departments within a hotel. The system ensures seamless communication, data transfer, security, and automation across multiple floors and VLAN-segmented departments. The architecture incorporates IoT devices, wireless access points, VLANs for segmentation, and centralized control mechanisms. The network is designed to handle daily hotel operations effectively, ensuring reliability, scalability, and security.

1.2 Introduction

In the hospitality industry, a well-structured network infrastructure is crucial for smooth operations, customer satisfaction, and security. This project aims to design and implement a hotel network using Cisco devices and technologies to ensure a high-performance system. The proposed system integrates different departments, IoT devices, and essential services such as security, administration, guest services, and automation.

The primary objectives of this project include:

- Ensuring seamless communication between different departments.
- Implementing a VLAN-based network for better security and efficiency.
- Integrating IoT devices for automation and security monitoring.
- Providing secure guest access and hotel management functionalities.

1.3 Body Content

1.3.1 Network Architecture Overview

The hotel consists of multiple floors, each with designated departments, connected via Cisco switches and routers. The network follows a layered approach, incorporating VLANs for segmentation and efficient traffic management.

1.3.2 Floor and Department Layout

Admin Room (Main Network Control Center)

- Core router and server integration
- Network monitoring and management using tools like Syslog and SNMP
- VLANs for departmental segregation
- SMTP and FTP servers for internal email and file transfers
- Static routing for efficient inter-VLAN communication

1st Floor: Guest and IT Services

- VLAN 10: IT Department (Guest Services and Maintenance)
- VLAN 20: Guest Internet Access
- IoT devices (Smoke detectors, webcams, access points, smart fans, and lights)

2nd Floor: Business and Hotel Operations

- VLAN 30: Sales Department
- VLAN 40: HR Department
- VLAN 50: Finance Department
- Multiple workstations and printers with static and DHCP IPs

3rd Floor: Logistics and Guest Services

- VLAN 70: Logistics and Backend Operations
- VLAN 80: Store and Reception
- IoT devices (Air conditioners, fire alarms, CCTV cameras, home speakers)

1.3.3 Devices and Components Used

Networking Hardware:

- Cisco 2960-24TT Switches for VLAN segmentation and port security
- Cisco Routers configured for inter-VLAN routing, static routing, ACLs, and firewall
- Cisco Access Points for wireless connectivity and roaming

End Devices:

- PCs, Laptops, Tablets, Smartphones (with static and DHCP IP assignments)

IoT Devices:

- Security cameras for surveillance
- Smoke detectors and fire sprinklers for safety
- Smart fans and lights for automation
- Access control systems (e.g., RFID readers, electronic door locks)

Servers:

- SMTP Server for internal email communication
- FTP Server for file sharing
- DNS Server for domain name resolution
- DHCP Server for dynamic IP addressing

1.3.4 VLAN Configuration

Each department is assigned a VLAN to ensure security and network performance:

- VLAN 10 – IT Department (Guest Services and Maintenance)
- VLAN 20 – Guest WiFi and Room Services
- VLAN 30 – Sales Department
- VLAN 40 – HR Department
- VLAN 50 – Finance Department
- VLAN 70 – Logistics and Backend Operations
- VLAN 80 – Store and Reception

1.3.5 Security Implementation

To ensure network security, the following measures are implemented:

- Access Control Lists (ACLs) to restrict unauthorized access between VLANs and devices
- Firewalls to protect against cyber threats
- VLAN segmentation to isolate traffic and prevent unauthorized data access
- Regular monitoring and logging of network activity via SNMP and Syslog servers
- Static routing for controlled and secure traffic flow between VLANs

1.4 Future Network Implementations

To enhance the network infrastructure and prepare for future demands, the following implementations are proposed:

- **Network Automation and Orchestration:** Utilize tools like Ansible or Cisco DNA Center to automate network device configuration and management.
- **Software Defined Networking (SDN):** Implement SDN for centralized and flexible network control.
- **Advanced Threat Detection:** Deploy Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to improve security.
- **Cloud Integration:** Enable hybrid cloud connectivity for data backup, application hosting, and additional services.
- **IPv6 Deployment:** Transition to IPv6 addressing to support future network scalability.
- **Network Access Control (NAC):** Enforce endpoint compliance policies before granting network access.
- **Quality of Service (QoS):** Prioritize critical traffic such as VoIP and video conferencing for better performance.
- **Backup and Disaster Recovery:** Implement redundant network links, backup servers, and failover strategies to ensure high availability.
- **Enhanced Wireless Security:** Adopt WPA3 and 802.1X authentication for improved wireless security.
- **Network Analytics and Artificial Intelligence:** Use AI/ML-based tools for predictive maintenance and anomaly detection.

- **VPN and Remote Access Solutions:** Provide secure remote connectivity for mobile and teleworking users.

- **Zero Trust Architecture:** Apply continuous verification principles and strict access controls to enhance security.

- **Blockchain for Security:** Integrate blockchain technology for immutable logging and enhanced security auditing.

Chapter 2

Chapter 02

2.1 Network Design

This network is designed to provide efficient, secure, and scalable connectivity across multiple floors and departments of an organization, integrating both traditional IT infrastructure and IoT devices for enhanced automation and security.

2.1.1 Design Overview

- The **Admin Room** acts as the main network control center, housing core routers and servers responsible for overall network management and monitoring.
- Each floor is segmented into VLANs to isolate traffic, improve security, and optimize network performance:
  - **1st Floor:** Focused on IT services and guest internet access, with VLANs dedicated to IT and guest users.
  - **2nd Floor:** Supports business operations such as Sales, HR, and Finance with separate VLANs for departmental data segregation.
  - **3rd Floor:** Handles logistics, guest services, and store operations, with VLANs for backend operations and reception, incorporating various IoT devices like fire alarms, AC, and CCTV.

2.1.2 Key Components and Configurations

- **Switches:** Cisco 2960-24TT switches are deployed for effective VLAN segmentation and layer 2 switching.
- **Routers:** Cisco routers manage inter-VLAN routing and firewall rules, ensuring secure and efficient data flow between VLANs.
- **Wireless Access Points:** Provide WiFi connectivity across floors, supporting mobile devices and IoT endpoints.

- **End Devices:** The network supports a variety of endpoints including PCs, laptops, tablets, and smartphones.
- **IoT Integration:** Security cameras, smoke detectors, fire sprinklers, smart fans, and lighting systems are integrated into the network for automation and enhanced safety.
- **Network Services:** Servers are configured to provide FTP, SMTP, DNS, and other essential services required for smooth business operations.
- **Static IP Addressing and DHCP:** A mix of static and dynamic IP addressing schemes ensure stable connectivity for critical devices like servers and access points.
- **Security:** Implementation of Access Control Lists (ACLs), firewalls, and VLAN segmentation restrict unauthorized access and control network traffic.

2.1.3 Workflow & Management

- Devices communicate across VLANs through router configurations ensuring departmental isolation yet allowing necessary inter-department access.
- IoT devices communicate with control servers through designated VLANs, enabling monitoring and management from the Admin room.
- Servers such as SMTP and FTP servers support internal and external communications and file sharing.
- Network monitoring tools provide visibility into traffic patterns and potential security threats, facilitating proactive maintenance.

2.1.4 Network IP Address Configuration

Device/Department	**IP Address**	**Subnet Mask**	**Gateway**
Admin Room Router	192.168.1.1	255.255.255.0	N/A
FTP Server	192.168.1.60	255.255.255.0	192.168.1.1
DNS Server	192.168.1.10	255.255.255.0	192.168.1.1
SMTP Server	192.168.1.30	255.255.255.0	192.168.1.1
Laptop (IT Dept)	192.168.1.17	255.255.255.0	192.168.1.1
Printer (IT Dept)	192.168.1.15	255.255.255.0	192.168.1.1
Router 1 (Inter-VLAN)	192.168.4.1	255.255.255.0	N/A
Sales PC	192.168.2.3	255.255.255.0	192.168.2.1
HR PC	192.168.2.5	255.255.255.0	192.168.2.1
Finance PC	192.168.2.7	255.255.255.0	192.168.2.1
Logistics Server	192.168.6.24	255.255.255.0	192.168.6.1
Store Access Point	192.168.3.60	255.255.255.0	192.168.3.1

Table 2.1: IP Address, Subnet Mask, and Gateway Information

2.1.5 Network Infrastructure Overview of Smart Hotel Management System

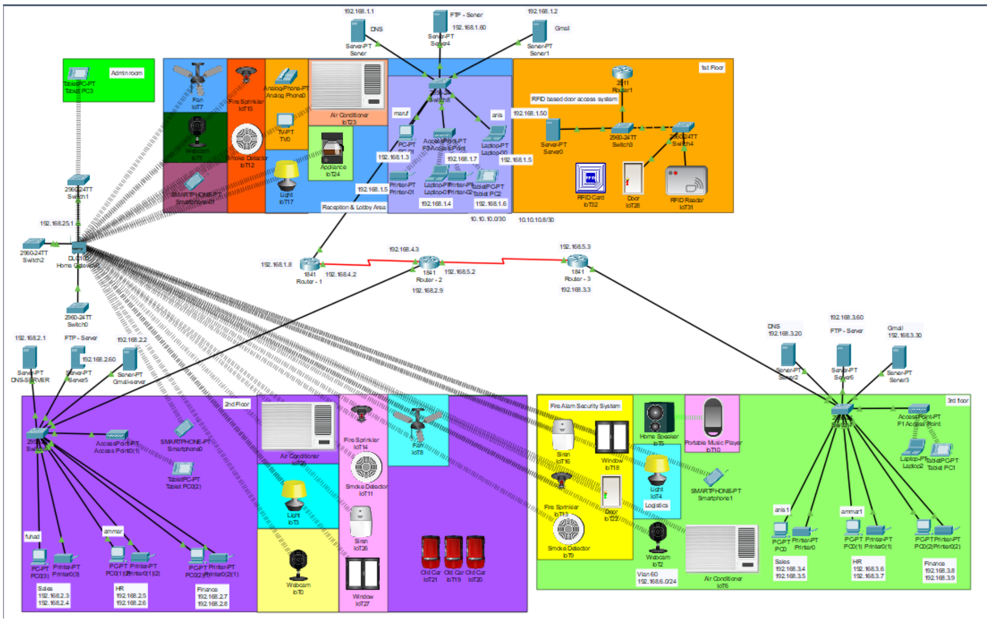


Figure 2.1: This is Full Project.

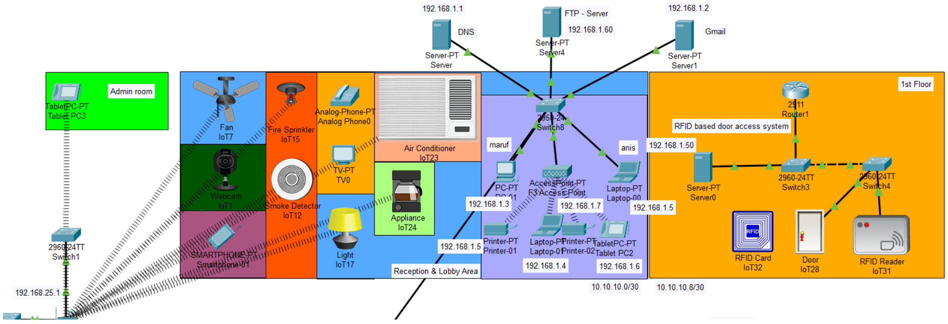


Figure 2.2: This is 1st Floor Design.

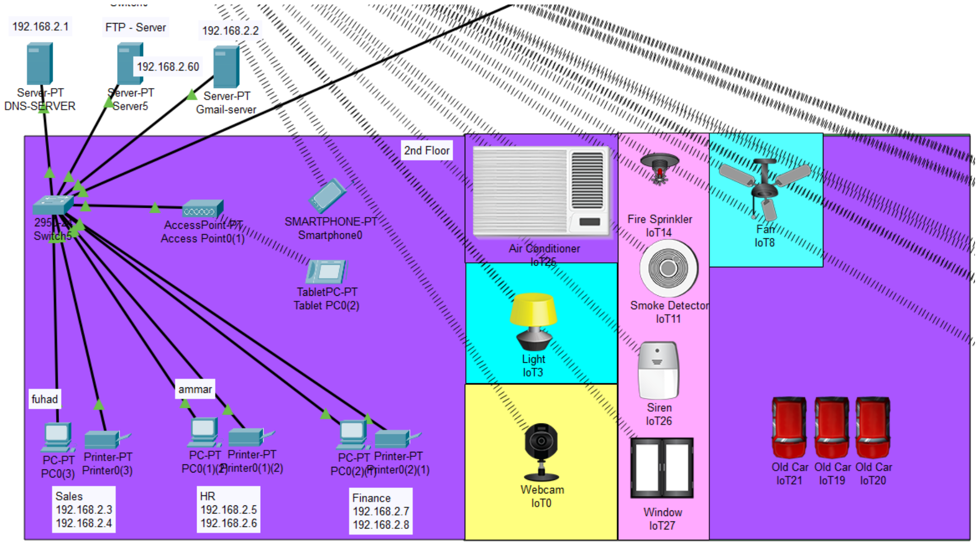


Figure 2.3: This is 2nd Floor Design.

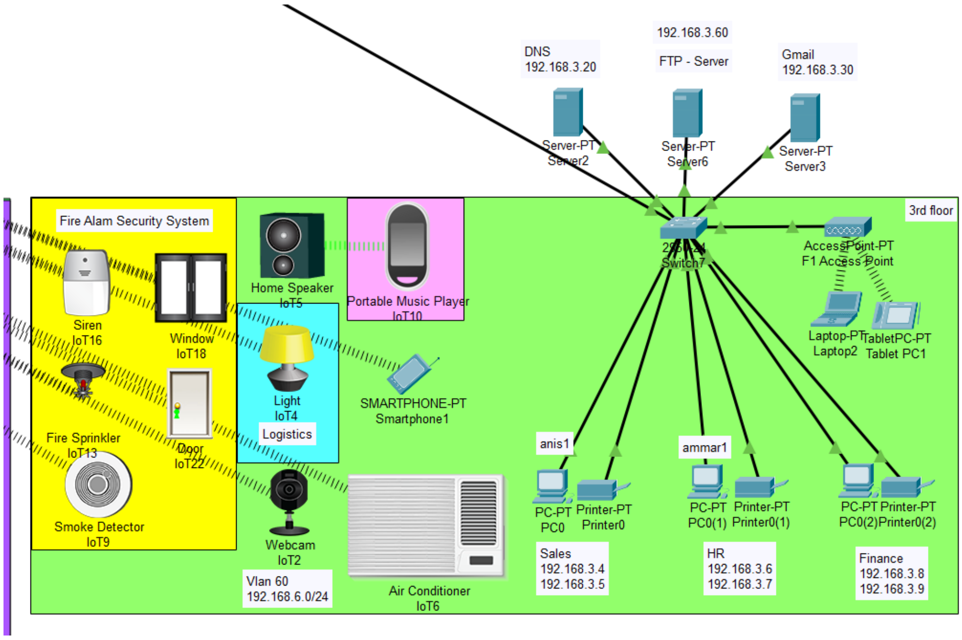


Figure 2.4: This is 3th Floor Design.

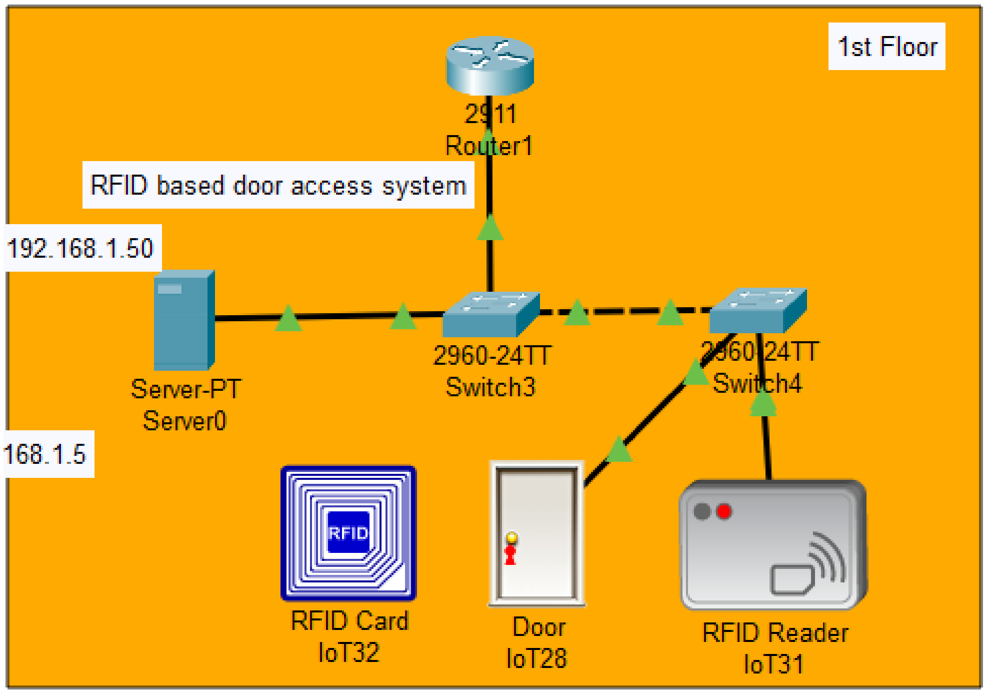
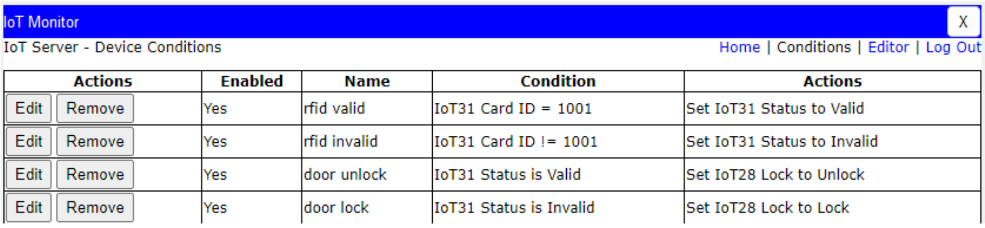


Figure 2.5: Now I can show how to work RFID-based door access system. When i Swap card on RFID Reader then automated unlock the door. Because i already create a condition on server.


IoT Monitor
X
IoT Server - Device Conditions
Home | Conditions | Editor | Log Out

Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	rfid valid	IoT31 Card ID = 1001	Set IoT31 Status to Valid
Edit Remove	Yes	rfid invalid	IoT31 Card ID != 1001	Set IoT31 Status to Invalid
Edit Remove	Yes	door unlock	IoT31 Status is Valid	Set IoT28 Lock to Unlock
Edit Remove	Yes	door lock	IoT31 Status is Invalid	Set IoT28 Lock to Lock

Figure 2.6: create a condition on the server.

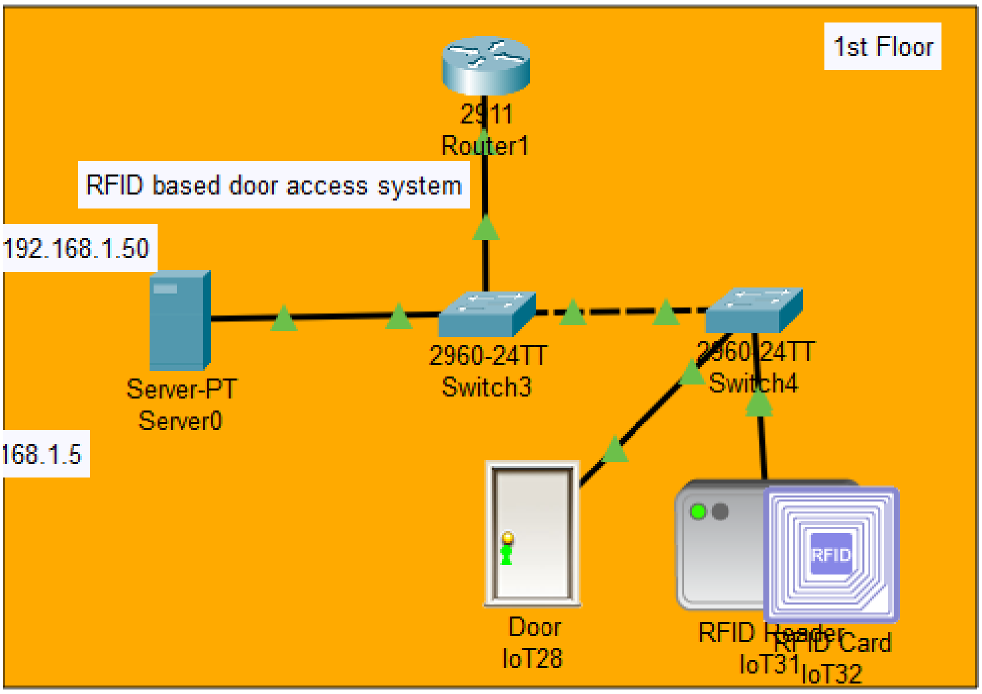


Figure 2.7: RFID-based door access system. UNLOCK

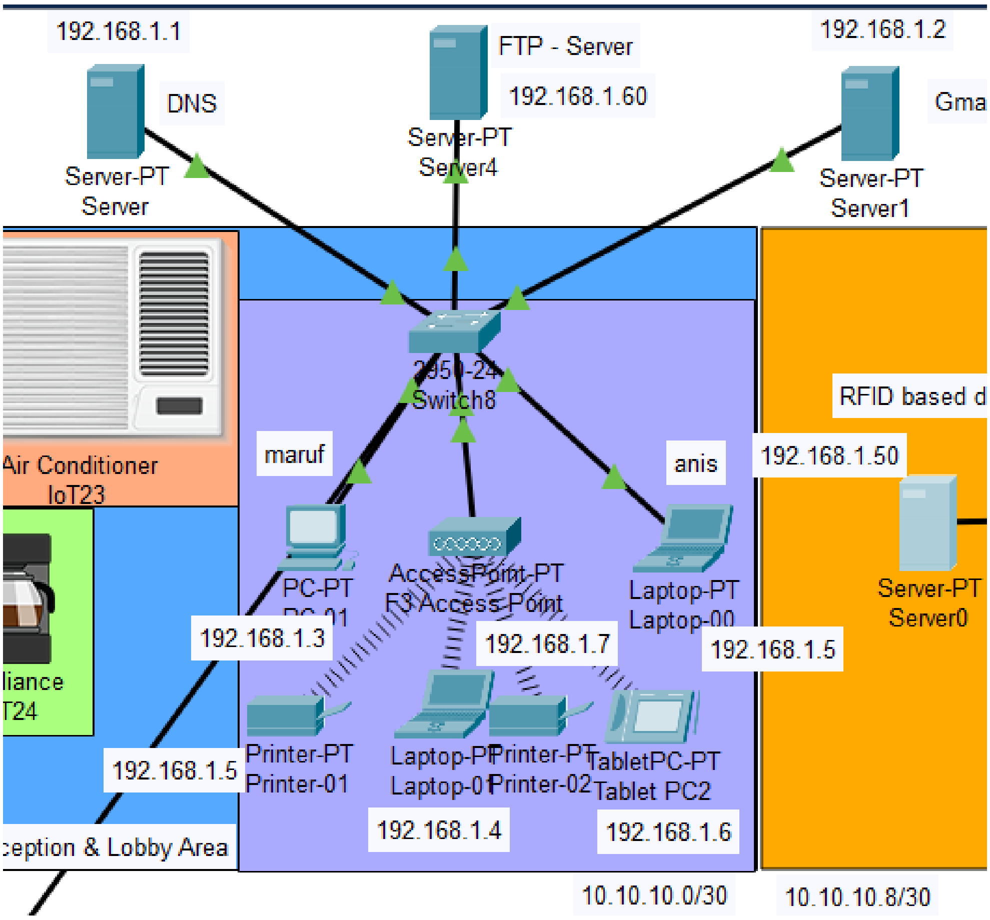
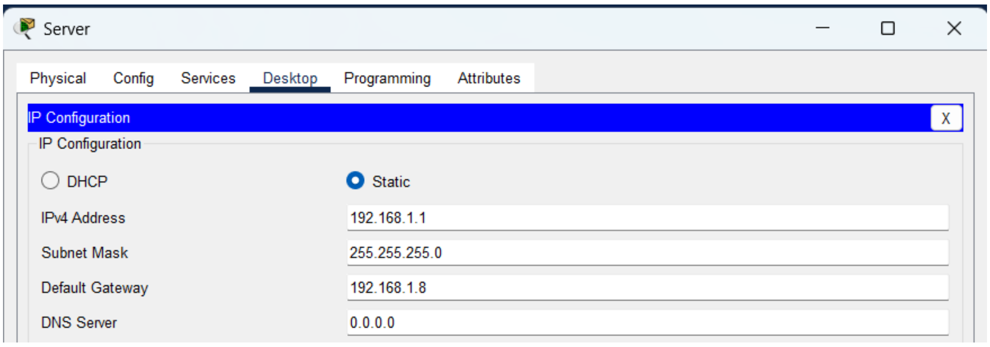


Figure 2.8: This is 1st Floor SMTP, FTP, DNS Server Configuration.



IP Configuration

○ DHCP ● Static

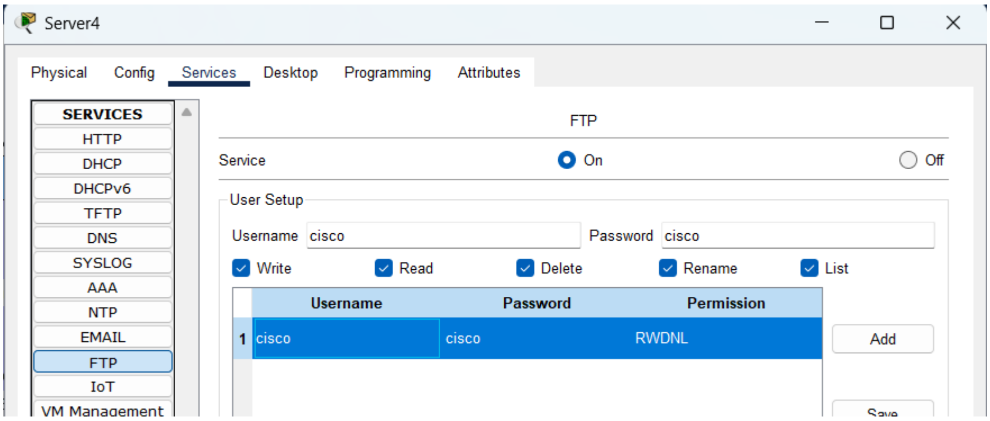
IPv4 Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.8

DNS Server: 0.0.0.0

Figure 2.9: DNS Server IP Configuration.



FTP

Service ● On ○ Off

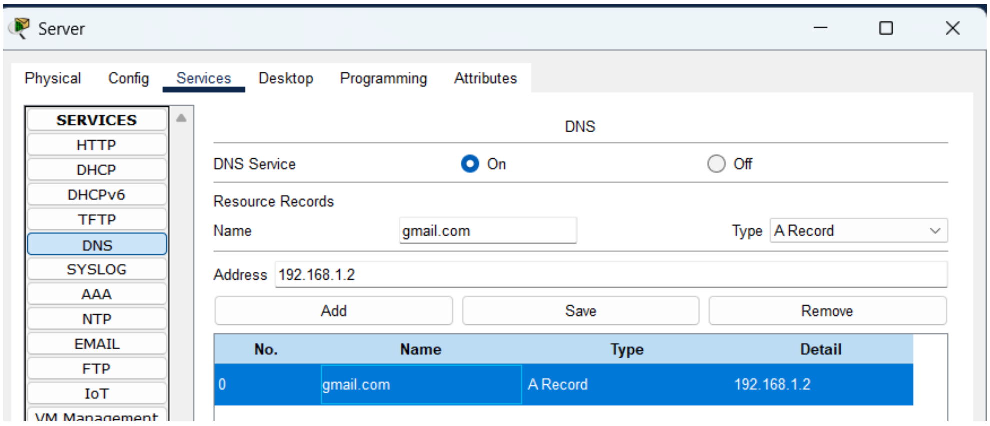
User Setup

Username: cisco Password: cisco

☑ Write ☑ Read ☑ Delete ☑ Rename ☑ List

	Username	Password	Permission
1	cisco	cisco	RWDNL

Figure 2.10: Create FTP Server.



DNS

DNS Service ● On ○ Off

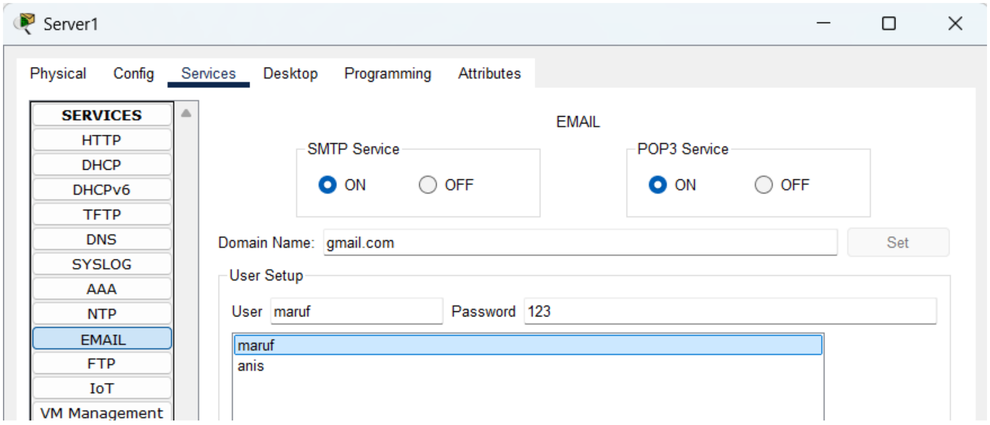
Resource Records

Name: gmail.com Type: A Record

Address: 192.168.1.2

No.	Name	Type	Detail
0	gmail.com	A Record	192.168.1.2

Figure 2.11: Create DNS For Gmail.



SMTP Service ● ON ○ OFF

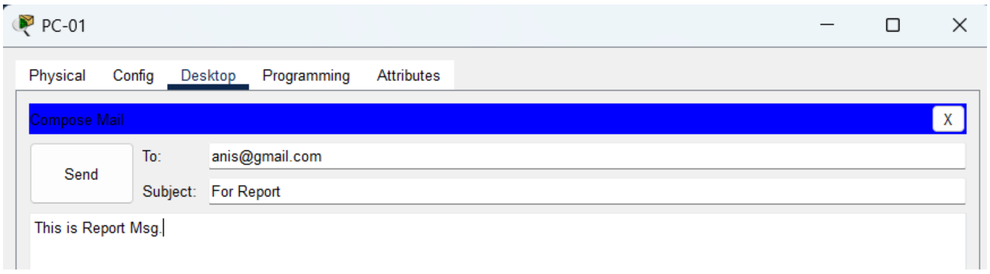
POP3 Service ● ON ○ OFF

Domain Name: gmail.com

User maruf Password 123

maruf
anis

Figure 2.12: Create Gmail Username Password.

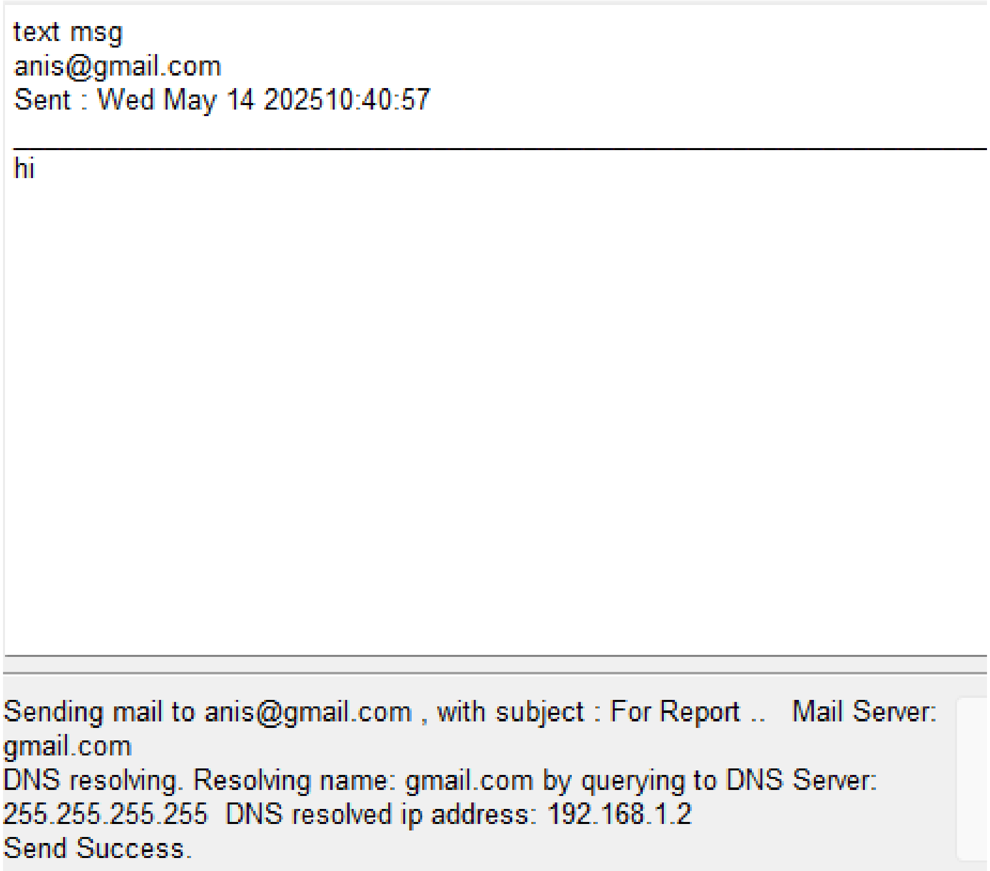


To: anis@gmail.com

Subject: For Report

This is Report Msg.

Figure 2.13: Send Gmail anis to maruf email address.

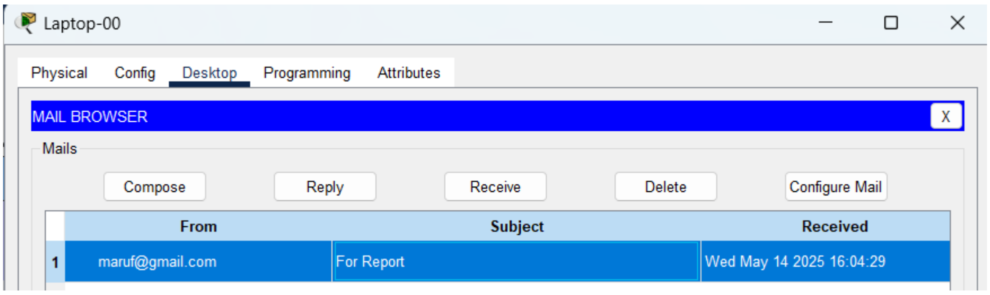


```
text msg
anis@gmail.com
Sent : Wed May 14 202510:40:57

hi
```

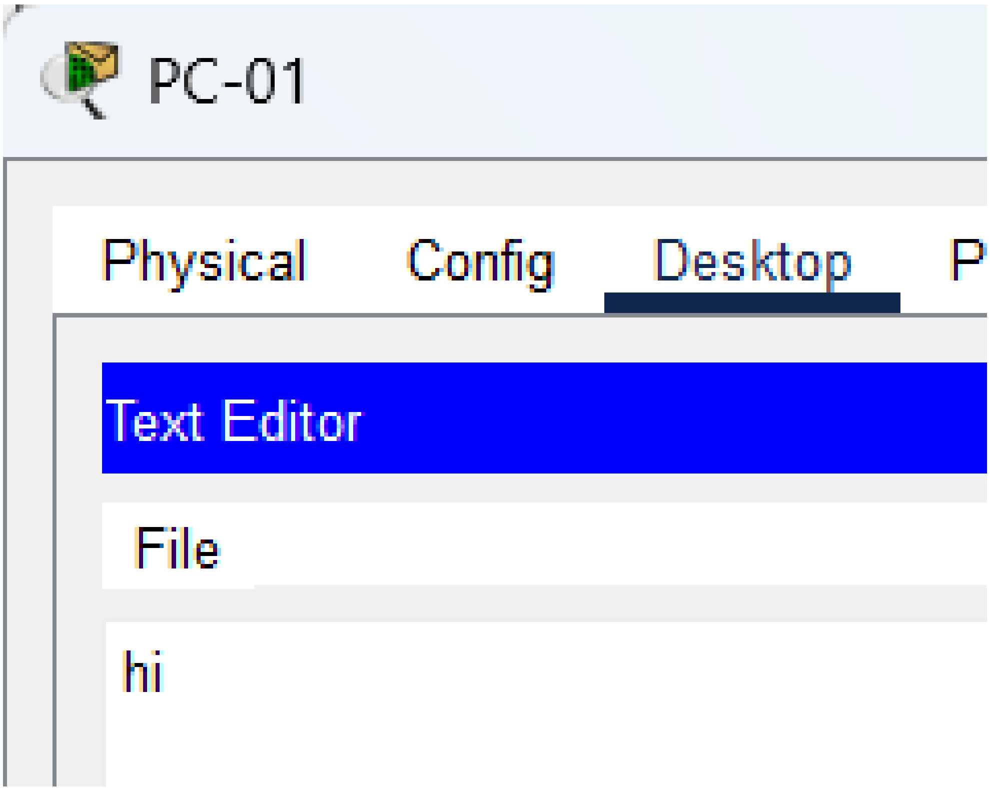
```
Sending mail to anis@gmail.com , with subject : For Report ..   Mail Server:
gmail.com
DNS resolving. Resolving name: gmail.com by querying to DNS Server:
255.255.255.255  DNS resolved ip address: 192.168.1.2
Send Success.
```

Figure 2.14: Successfully send.



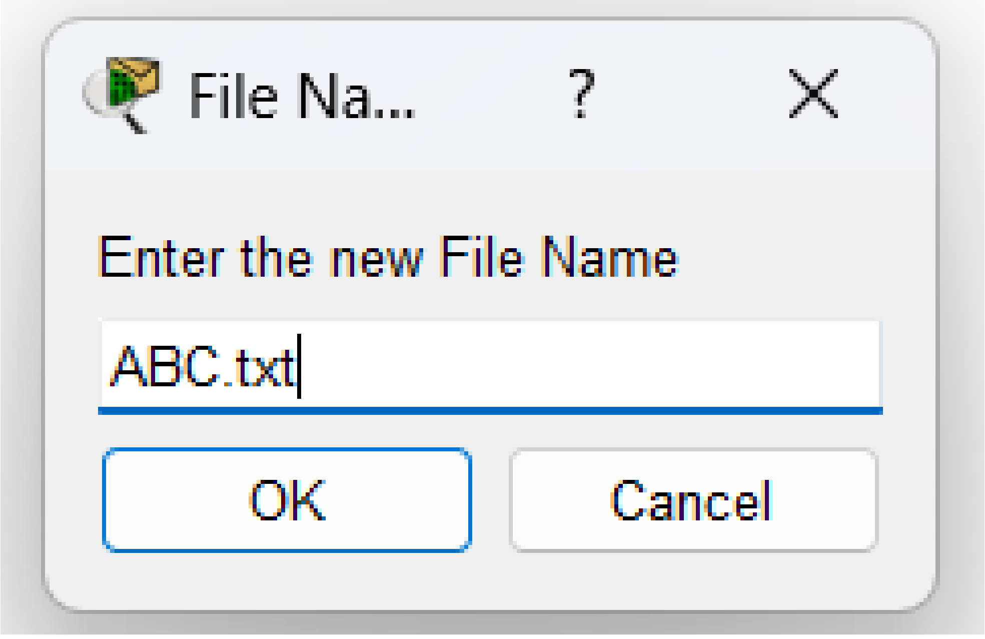
	From	Subject	Received
1	maruf@gmail.com	For Report	Wed May 14 2025 16:04:29

Figure 2.15: Receive The Mail.



hi

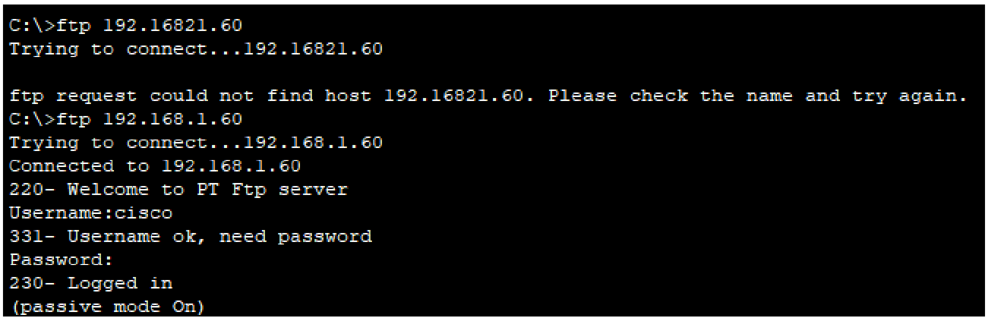
Figure 2.16: Create a txt file.



Enter the new File Name

ABC.txt

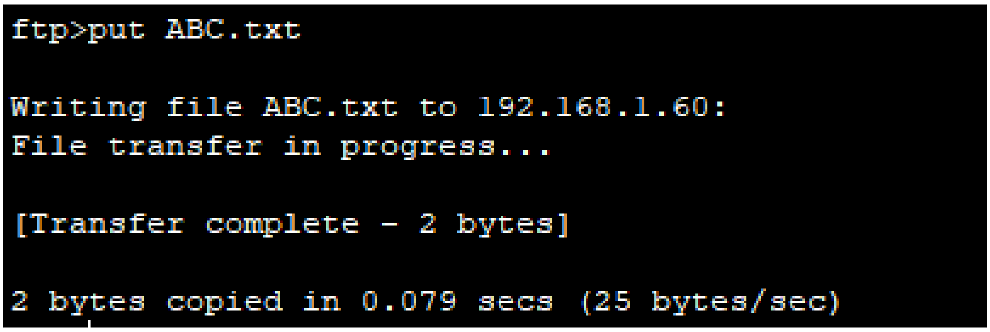
Figure 2.17: Save the file.



```
C:\>ftp 192.16821.60
Trying to connect...192.16821.60

ftp request could not find host 192.16821.60. Please check the name and try again.
C:\>ftp 192.168.1.60
Trying to connect...192.168.1.60
Connected to 192.168.1.60
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
```

Figure 2.18: Login the FTP Server from PC's Command Prompt.



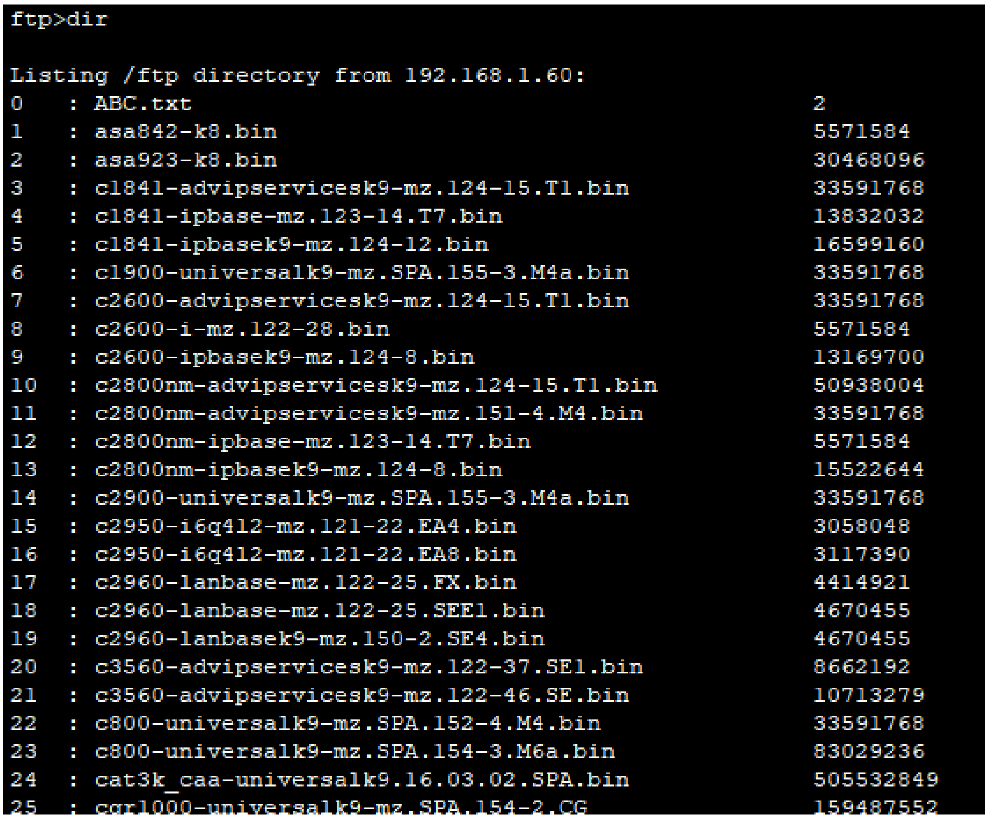
```
ftp>put ABC.txt

Writing file ABC.txt to 192.168.1.60:
File transfer in progress...

[Transfer complete - 2 bytes]

2 bytes copied in 0.079 secs (25 bytes/sec)
```

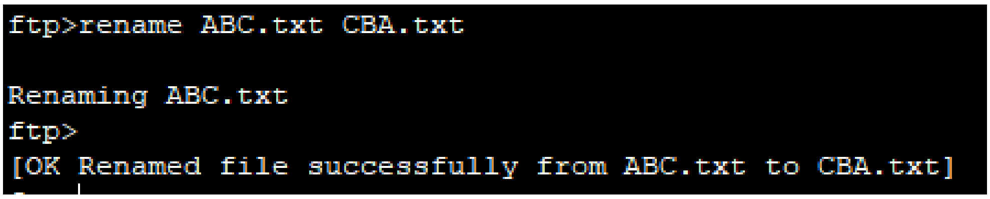
Figure 2.19: Upload a File to the FTP Server. put Comment



```
ftp>dir

Listing /ftp directory from 192.168.1.60:
0   : ABC.txt                                            2
1   : asa842-k8.bin                                      5571584
2   : asa923-k8.bin                                      30468096
3   : c1841-advipservicesk9-mz.124-15.T1.bin             33591768
4   : c1841-ipbase-mz.123-14.T7.bin                      13832032
5   : c1841-ipbasek9-mz.124-12.bin                       16599160
6   : c1900-universalk9-mz.SPA.155-3.M4a.bin             33591768
7   : c2600-advipservicesk9-mz.124-15.T1.bin             33591768
8   : c2600-i-mz.122-28.bin                              5571584
9   : c2600-ipbasek9-mz.124-8.bin                        13169700
10  : c2800nm-advipservicesk9-mz.124-15.T1.bin           50938004
11  : c2800nm-advipservicesk9-mz.151-4.M4.bin            33591768
12  : c2800nm-ipbase-mz.123-14.T7.bin                    5571584
13  : c2800nm-ipbasek9-mz.124-8.bin                      15522644
14  : c2900-universalk9-mz.SPA.155-3.M4a.bin             33591768
15  : c2950-i6q4l2-mz.121-22.EA4.bin                     3058048
16  : c2950-i6q4l2-mz.121-22.EA8.bin                     3117390
17  : c2960-lanbase-mz.122-25.FX.bin                     4414921
18  : c2960-lanbase-mz.122-25.SEE1.bin                   4670455
19  : c2960-lanbasek9-mz.150-2.SE4.bin                   4670455
20  : c3560-advipservicesk9-mz.122-37.SE1.bin            8662192
21  : c3560-advipservicesk9-mz.122-46.SE.bin             10713279
22  : c800-universalk9-mz.SPA.152-4.M4.bin               33591768
23  : c800-universalk9-mz.SPA.154-3.M6a.bin              83029236
24  : cat3k_caa-universalk9.16.03.02.SPA.bin             505532849
25  : cgr1000-universalk9-mz.SPA.154-2.CG                159487552
```

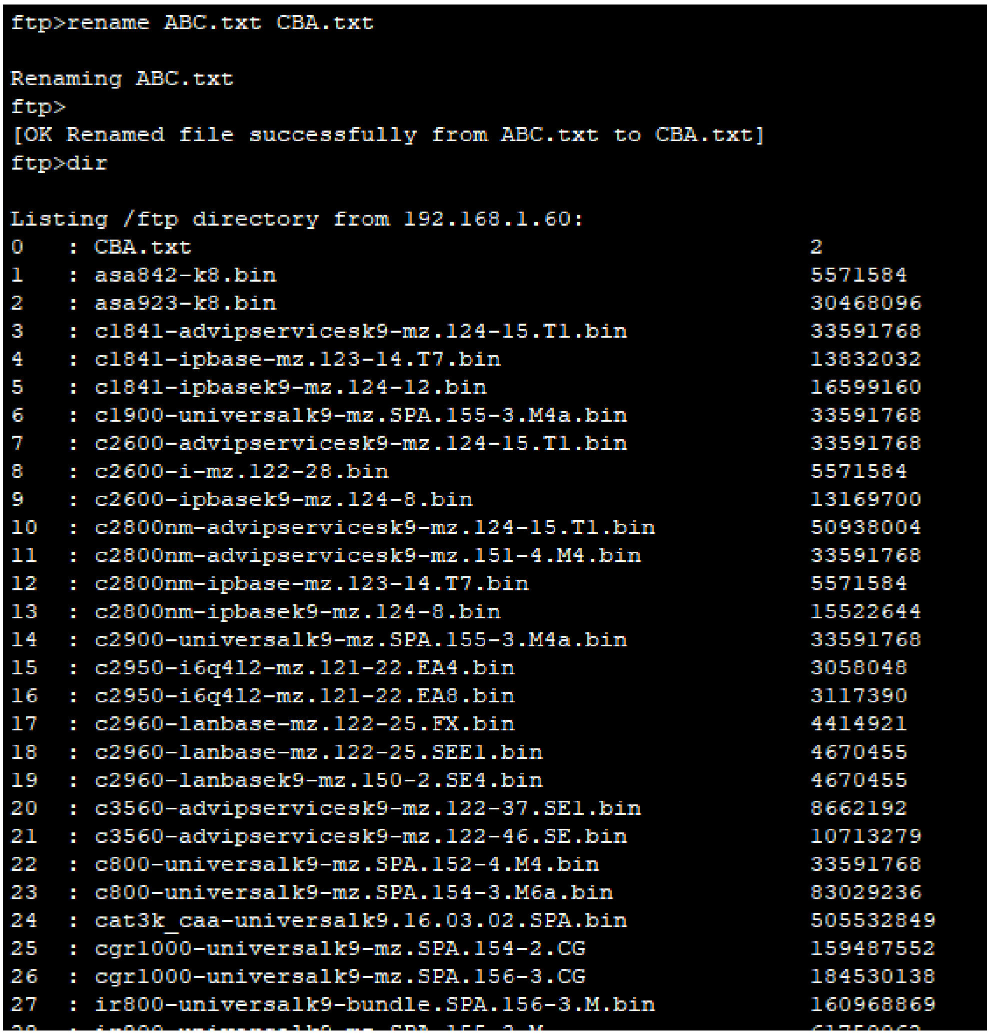
Figure 2.20: After uploading the file to the server, verify the transfer of the file by typing dir. The ABC.txt file is now listed in the file directory.



```
ftp>rename ABC.txt CBA.txt

Renaming ABC.txt
ftp>
[OK Renamed file successfully from ABC.txt to CBA.txt]
```

Figure 2.21: File Rename [old Name] [New Name]

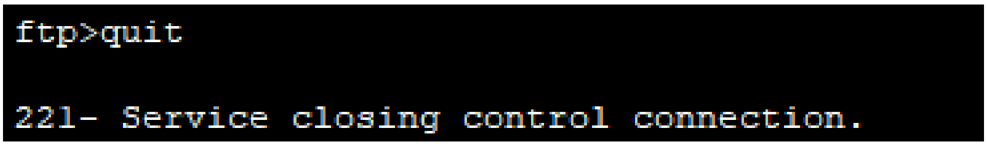


```
ftp>rename ABC.txt CBA.txt

Renaming ABC.txt
ftp>
[OK Renamed file successfully from ABC.txt to CBA.txt]
ftp>dir

Listing /ftp directory from 192.168.1.60:
0    : CBA.txt                                          2
1    : asa842-k8.bin                                    5571584
2    : asa923-k8.bin                                    30468096
3    : c1841-advipservicesk9-mz.124-15.T1.bin           33591768
4    : c1841-ipbase-mz.123-14.T7.bin                    13832032
5    : c1841-ipbasek9-mz.124-12.bin                     16599160
6    : c1900-universalk9-mz.SPA.155-3.M4a.bin           33591768
7    : c2600-advipservicesk9-mz.124-15.T1.bin           33591768
8    : c2600-i-mz.122-28.bin                            5571584
9    : c2600-ipbasek9-mz.124-8.bin                      13169700
10   : c2800nm-advipservicesk9-mz.124-15.T1.bin         50938004
11   : c2800nm-advipservicesk9-mz.151-4.M4.bin          33591768
12   : c2800nm-ipbase-mz.123-14.T7.bin                  5571584
13   : c2800nm-ipbasek9-mz.124-8.bin                    15522644
14   : c2900-universalk9-mz.SPA.155-3.M4a.bin           33591768
15   : c2950-i6q4l2-mz.121-22.EA4.bin                   3058048
16   : c2950-i6q4l2-mz.121-22.EA8.bin                   3117390
17   : c2960-lanbase-mz.122-25.FX.bin                   4414921
18   : c2960-lanbase-mz.122-25.SEE1.bin                 4670455
19   : c2960-lanbasek9-mz.150-2.SE4.bin                 4670455
20   : c3560-advipservicesk9-mz.122-37.SE1.bin          8662192
21   : c3560-advipservicesk9-mz.122-46.SE.bin           10713279
22   : c800-universalk9-mz.SPA.152-4.M4.bin             33591768
23   : c800-universalk9-mz.SPA.154-3.M6a.bin            83029236
24   : cat3k_caa-universalk9.16.03.02.SPA.bin           505532849
25   : cgr1000-universalk9-mz.SPA.154-2.CG              159487552
26   : cgr1000-universalk9-mz.SPA.156-3.CG              184530138
27   : ir800-universalk9-bundle.SPA.156-3.M.bin         160968869
```

Figure 2.22: Successfully Rename.



```
ftp>quit

221- Service closing control connection.
```

Figure 2.23: Close the FTP client by typing quit.

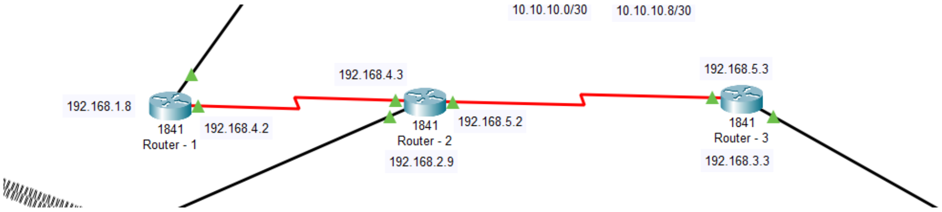


Figure 2.24: Router connect 3 Floor.

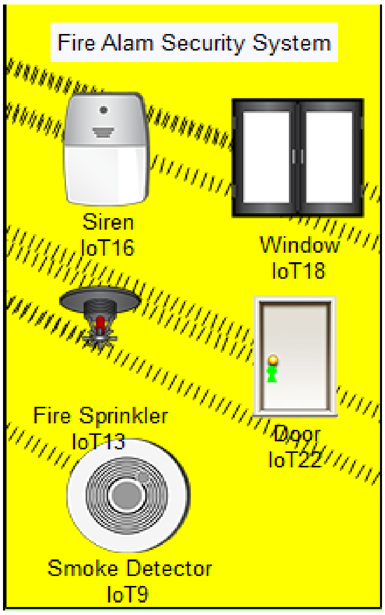


Figure 2.25: Design Fire Alam Security System.

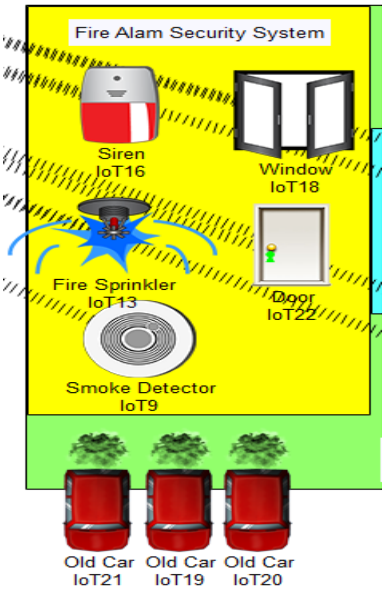
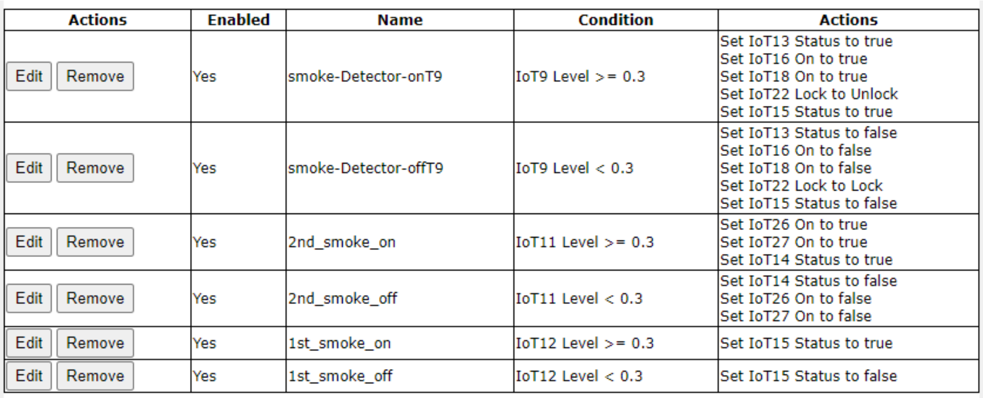
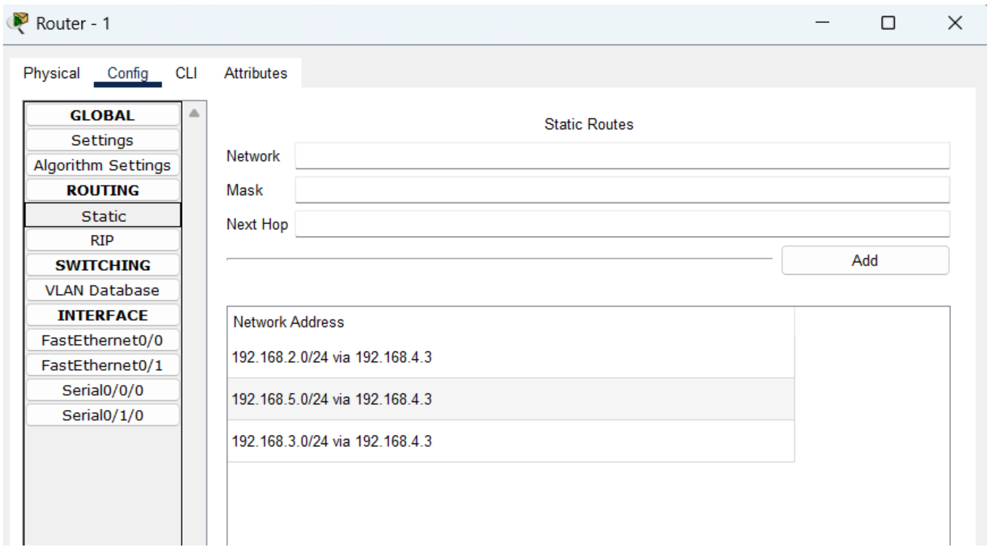


Figure 2.26: When the sensor detects smoke automatically Then The fire alarm on



Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	smoke-Detector-onT9	IoT9 Level >= 0.3	Set IoT13 Status to true Set IoT16 On to true Set IoT18 On to true Set IoT22 Lock to Unlock Set IoT15 Status to true
Edit Remove	Yes	smoke-Detector-offT9	IoT9 Level < 0.3	Set IoT13 Status to false Set IoT16 On to false Set IoT18 On to false Set IoT22 Lock to Lock Set IoT15 Status to false
Edit Remove	Yes	2nd_smoke_on	IoT11 Level >= 0.3	Set IoT26 On to true Set IoT27 On to true Set IoT14 Status to true
Edit Remove	Yes	2nd_smoke_off	IoT11 Level < 0.3	Set IoT14 Status to false Set IoT26 On to false Set IoT27 On to false
Edit Remove	Yes	1st_smoke_on	IoT12 Level >= 0.3	Set IoT15 Status to true
Edit Remove	Yes	1st_smoke_off	IoT12 Level < 0.3	Set IoT15 Status to false

Figure 2.27: All condition.



Static Routes

Network

Mask

Next Hop

Network Address

192.168.2.0/24 via 192.168.4.3

192.168.5.0/24 via 192.168.4.3

192.168.3.0/24 via 192.168.4.3

Figure 2.28: Static Networking Address Configur.

Chapter 3

Chapter 03

3.0.1 Results and Discussion

The Cisco-Based Hotel Management Network System was designed with scalability, security, and high performance in mind. The implementation results and observed benefits are outlined below:

- **Improved Communication and Segmentation:** Through the use of multiple VLANs (VLAN 10 to VLAN 80), inter-department communication is streamlined while maintaining strict logical separation. Each floor and department operates within its own VLAN, significantly reducing broadcast traffic and increasing performance.
- **Enhanced Network Security:** Access Control Lists (ACLs) and inter-VLAN routing configured via Cisco routers help restrict unauthorized access between sensitive departments (e.g., Finance, HR). The firewall provides an additional layer of protection from external threats. Furthermore, VLAN segmentation and regular logging help identify and prevent internal security breaches.
- **Effective Use of Protocols (SMTP, FTP, Static Routing):** SMTP is used for internal and external email communication between departments and clients. FTP is implemented for secured file transfers between HR, Finance, and Admin departments. Static routing ensures predictable routing behavior, minimizing complexity and ensuring faster route resolution for fixed network paths.
- **Guest Satisfaction and Internet Isolation:** A dedicated VLAN for guest services ensures that their internet access is isolated from the hotel's internal business network. This not only improves user experience but also protects internal data from potential exposure or misuse.
- **IoT Device Integration:** IoT devices such as smart fans, smoke detectors, fire alarms, webcams, access control systems, and CCTV cameras have been successfully integrated into the network. These contribute to safety, automation, and energy efficiency, enhancing overall hotel operations and the guest experience.
- **Operational Efficiency Across Departments:** With dedicated workstations and printers on each floor, employees across Sales, HR, Finance, Logistics, and Re-

ception have quick and reliable access to essential resources. Inter-VLAN routing allows seamless communication while maintaining security standards.

- **Centralized Monitoring and Administration:** The Admin Room, acting as the main control center, hosts core routers and servers. Network administrators can monitor traffic, manage bandwidth allocation, and troubleshoot issues in real time, increasing reliability and reducing downtime.
- **Scalability and Future Expansion:** The modular design allows future integration of cloud services, VoIP, intrusion detection systems (IDS), and centralized guest data management. The infrastructure supports future VLANs, allowing more departments or service layers without disrupting existing operations.
- **Compliance and Documentation:** Proper VLAN mapping, IP addressing, and device documentation ensure the network complies with best practices. Subnetting, gateway configurations, and port allocations follow a structured approach, which aids in troubleshooting and maintenance.

In summary, the designed hotel management system using Cisco Packet Tracer not only supports current operational needs but is also ready for future technological enhancements. This project demonstrates how layered security, protocol implementation, and smart design principles can transform traditional hospitality networks into efficient digital ecosystems.

Chapter 4

Chapter 04

4.0.1 Results and Discussion

The design and implementation of the Cisco-Based Hotel Management Network has yielded a secure, scalable, and efficient digital infrastructure that supports the diverse needs of a modern hotel environment. Key findings and operational benefits include:

- **Departmental Network Segmentation:** By deploying VLANs (VLAN 10 to VLAN 80), the network achieves logical isolation between departments such as IT, HR, Finance, Sales, and Guest Services. This not only improves bandwidth efficiency but also enhances data security.

- **Integrated Protocols for Functionality:** SMTP is configured to handle internal and external communication. FTP is used for secure document exchange across departments. Static routing ensures low-latency communication between VLANs, making data flow efficient and reliable.

- **Enhanced Network Security:** ACLs and firewall configurations are enforced at the router level to block unauthorized access between VLANs. VLAN segmentation itself acts as a major security boundary. Real-time network monitoring and logging are carried out from the Admin Control Room.

- **Guest Connectivity and Isolation:** A dedicated VLAN for guest internet access prevents exposure to the core business network. This improves user satisfaction while ensuring hotel data remains secure and isolated.

- **IoT-Based Automation and Monitoring:** The deployment of IoT devices like smart fans, fire alarms, CCTV, and smoke detectors contributes to automation, energy efficiency, and increased guest and staff safety.

- **Reliable Communication and Operational Access:** Floor-wise device distribution (PCs, printers, smart devices) ensures easy access to services. The network supports multiple platforms including tablets, laptops, and smartphones.

- **Centralized Control and Maintenance:** The Admin Room houses the core router, FTP/SMTP servers, and monitoring systems. This centralization reduces maintenance overhead and enables real-time management.

- **Scalability for Future Needs:** The network has been structured to accommodate future upgrades like cloud integration, centralized backup, VoIP communication, and even AI-driven automation for predictive monitoring and alert systems.
- **Professional Documentation and Planning:** IP addressing, subnetting, VLAN configurations, and routing tables are well-documented to maintain clarity and ease of future troubleshooting or upgrades.

In summary, this project demonstrates how a carefully segmented, protocol-integrated, and IoT-enhanced network architecture can significantly elevate the technological standards of hotel operations.

4.0.2 Conclusion

This project successfully demonstrates the planning, design, and implementation of a comprehensive Cisco-Based Hotel Management Network System. The approach integrates VLAN segmentation, secure protocol usage (SMTP, FTP, Static Routing), IoT device automation, and centralized monitoring to meet the critical demands of a dynamic hotel environment.

The system enhances communication, strengthens data security, improves guest services, and enables energy-efficient operation. Core technologies like Cisco switches, routers, and access points form the backbone of this reliable and scalable infrastructure.

Moreover, the modular nature of the design makes it future-ready. Potential future enhancements include:

- Cloud-based data storage and service management
- AI-driven network traffic analysis and threat detection
- Implementation of Voice over IP (VoIP) systems
- Integration of centralized mobile management (MDM)
- Deployment of redundancy and failover mechanisms

Overall, this project lays the groundwork for a secure, efficient, and smart hotel network system aligned with modern networking standards and future innovations.

4.0.3 References

1. Cisco Networking Academy. *CCNA: Introduction to Networks.* Cisco Systems, 2025.
2. Tanenbaum, A. S. *Computer Networks*, 6th Edition. Pearson Education, 2023.
3. IEEE. “Hotel IT Infrastructure Guidelines.” In: *IEEE International Conference on Smart Hospitality Networks*, 2024.

4. Cisco Systems. *Enterprise Networking Solutions – White Paper*. Accessed online at: https://www.cisco.com

5. Cisco Systems. *Best Practices for VLAN and ACL Implementation*. Cisco Technical Documentation, n.d.