Computer Communication & Networks: Project Report. Smart Office Solutions.

Project Members:

- Muhammad Ali Masroor Khan (01-134232-110)
- Ishmam Asim (01-134232-079)

Section:

BS CS 3D

Course Instructor:

Dr. Arshad Farhad

1. Introduction

In today's rapidly evolving technological landscape, **smart offices** play a pivotal role in enhancing efficiency, security, and connectivity. Businesses and organisations are increasingly relying on integrated networks to streamline operations and provide flexible work environments. A smart office combines automation, robust networking solutions, and centralised control systems to create a seamless and secure working environment for both physical and remote users.

The primary objectives of this project are to ensure **enhanced security** and reliable **connectivity** across multiple locations. To achieve this, the network restricts direct communication between devices using **Access Control Lists (ACLs)**, ensuring all data flow passes through designated servers, thereby enhancing safety.

Our network includes **two office environments** and **two home networks**, catering to the modern demand for **"work from home"** capabilities and remote accessibility. A **dedicated server house** located in a secure remote facility provides centralised services, including:

- **Dynamic Host Configuration Protocol (DHCP) Server** for automatic IP address assignment,
- **Domain Name System (DNS) Server** for resolving hostnames to IP addresses,
- **HyperText Transfer Protocol (HTTP) Server** for hosting web content,
- **File Transfer Protocol (FTP) Server** for secure file sharing and transfer, and
- **Simple Mail Transfer Protocol (SMTP) Server** for managing email communication.

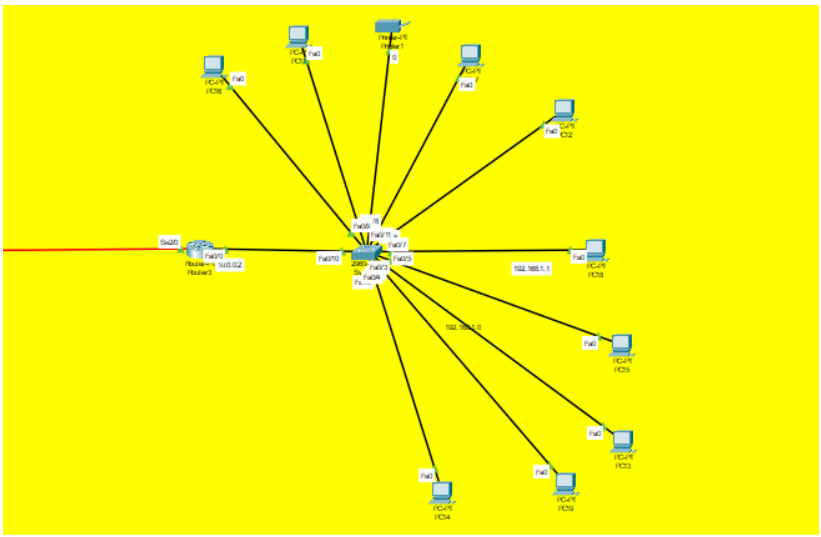
Additionally, **IoT integration** introduces advanced automation within the home networks, including RFID-enabled doors, motion-activated lighting, thermostats, air conditioning, and other smart devices, enabling an efficient and modern working environment.

This project adheres to the **core principles of Cisco networking** and demonstrates extensive implementation of configurations across network devices, ensuring secure, functional, and well-optimised communication.

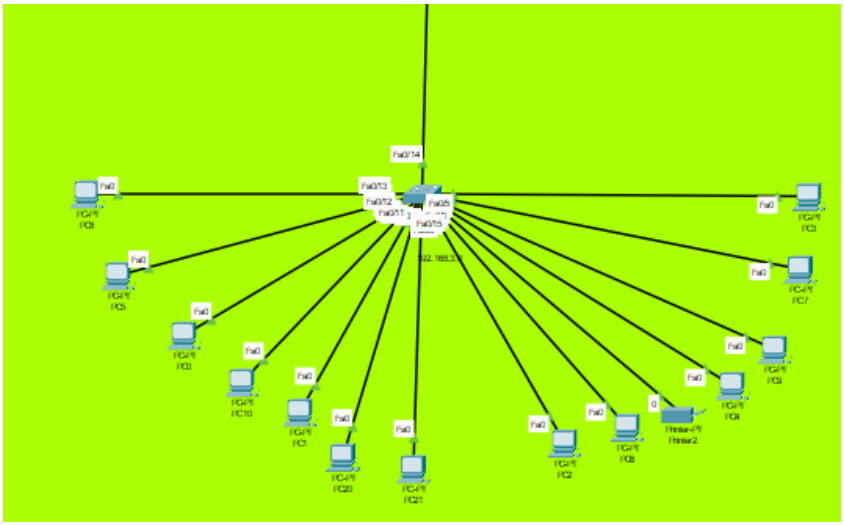
2. Network Design

The **smart office network** is designed to ensure **centralised communication** and **security** through a well-structured topology. The key components include two office networks, two home networks, a server network, and a VoIP system, all connected through a **main router (Router4)**.

Office Networks



Office: 1



Office: 2

Office 1 and **Office 2** share the same structure:

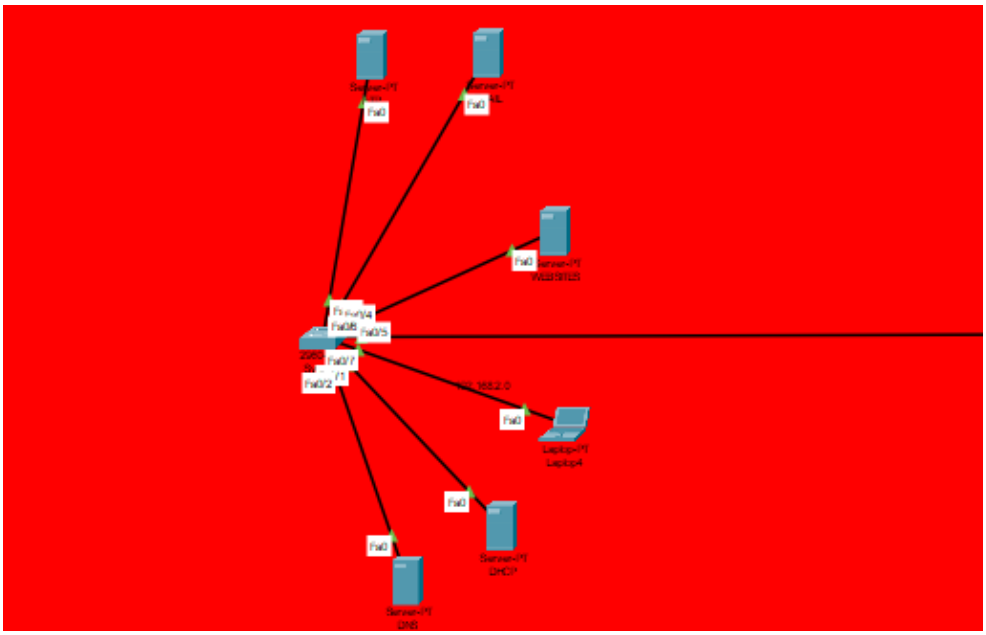
- **End Devices**: PCs and a network printer.
- **Switch**: Cisco Catalyst 2960 IOS 15 connects all devices.
- **Router**: Each office switch is connected to a **Router-PT**, which routes traffic to **Router4** (main router).

IP Addressing:

- **Office 1**: `192.168.1.0/24`
- **Office 2**: `192.168.3.0/24`

Each network has **254 usable IP addresses**, calculated as `2^8 - 2` for devices and the router interface.

Server Network

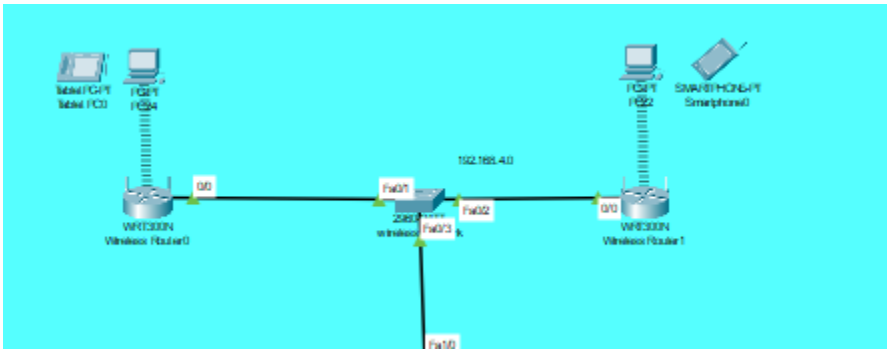


The **server room** is connected to **Router4** and acts as the central hub for all network traffic:

- **IP Address Scheme**: `192.168.2.0/24`
- **Usable IPs**: 254

All traffic between offices, home networks, and VoIP must pass through this network to ensure centralised routing and security.

Home Networks



The **two home networks** facilitate remote connectivity using a combination of wireless and wired devices:

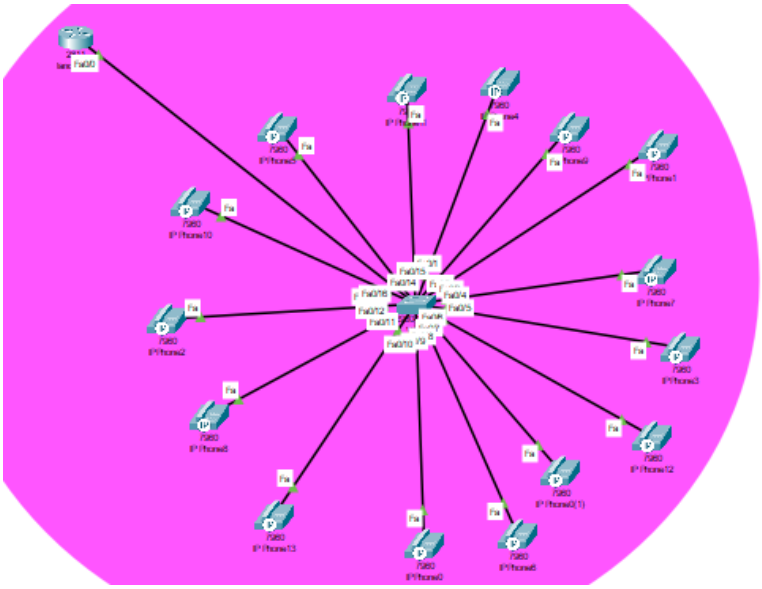
- **Wireless Router**: Linksys WRT300N connects devices wirelessly.
- **Switch**: Cisco Catalyst 2960 connects wired PCs and laptops.

IP Addressing:

- **Home Network 1**: `192.168.0.0/24`
- **Home Network 2**: `192.168.5.0/24`

Each network provides **254 usable IP addresses**.

VoIP Network



The VoIP system enables voice communication across the smart office network:

- **Switch**: Cisco Catalyst 2960 connects all IP phones.
- **Router**: The switch is connected to a dedicated **Router-PT**, which routes VoIP traffic to Router4.

IP Address Scheme: `192.168.10.0/24`

- **Usable IPs**: 254

Centralised Router (Router4)

Router4 acts as the main router, connecting all networks:

- **Office Routers**: Connected to Router4.
- **Home Routers and VoIP Routers**: Traffic passes through Router4.
- **Server Network**: Ensures all traffic flows through the server room.

Routing Table for Router4:

Type	Network	Port	Next Hop IP	Metric
C	10.0.0.0/8	Serial2/0	---	0/0
C	11.0.0.0/8	Serial3/0	---	0/0
R	192.168.1.0/24	Serial2/0	10.0.0.2	120/1
C	192.168.2.0/24	FastEthernet0/0	---	0/0
R	192.168.3.0/24	Serial3/0	11.0.0.2	120/1
C	192.168.4.0/24	FastEthernet1/0	---	0/0

Key Points:

1. All networks route traffic through **Router4**, ensuring centralised control.
2. **RIP Version 2** dynamically propagates routes between the connected subnets.
3. **Access Control Lists (ACLs)** on Router4 block direct communication between devices, requiring all traffic to pass through the server room for security.

Conclusion

The network design ensures **centralised routing** through Router4, enforces secure communication through the server network, and provides dynamic routing with **RIP Version 2**. This structure

guarantees seamless connectivity, scalability, and enhanced security across all offices, home networks, and VoIP systems.

3. Routing Protocols

The network utilises **Routing Information Protocol (RIP Version 2)** for dynamic routing across all subnets. RIP Version 2 ensures efficient routing by propagating route information dynamically to all routers.

RIP Configuration

Below are the commands configured on **Router4** to enable **RIP Version 2**:

```
scss
Copy code
Router> enable
Router# configure terminal
Router(config)# router rip
Router(config-router)# version 2
Router(config-router)# network 192.168.1.0
Router(config-router)# network 192.168.2.0
Router(config-router)# network 192.168.3.0
Router(config-router)# network 192.168.4.0
Router(config-router)# network 10.0.0.0
Router(config-router)# network 11.0.0.0
Router(config-router)# no auto-summary
Router(config-router)# exit
Router# write memory
```

Verification Outputs

The following outputs confirm that **RIP Version 2** has been successfully implemented on **Router4**:

1. `show ip route` Command

This output displays the routing table for Router4.

```
vbnet
Copy code
Codes: C - connected, R - RIP, S - static, O - OSPF, I - IGRP, B - BGP
Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, Serial2/0
C    11.0.0.0/8 is directly connected, Serial3/0
R    192.168.1.0/24 [120/1] via 10.0.0.2, 00:00:20, Serial2/0
C    192.168.2.0/24 is directly connected, FastEthernet0/0
```

```
R    192.168.3.0/24 [120/1] via 11.0.0.2, 00:00:22, Serial3/0
C    192.168.4.0/24 is directly connected, FastEthernet1/0
```

Explanation:

- **C**: Directly connected networks:
  - `10.0.0.0/8`, `11.0.0.0/8`, `192.168.2.0/24`, `192.168.4.0/24`.
- **R**: RIP-learned routes with a hop count of `1` (Metric 120):
  - `192.168.1.0/24` via **10.0.0.2** (Serial2/0).
  - `192.168.3.0/24` via **11.0.0.2** (Serial3/0).

---

2. `show ip route rip` Command

This command filters the routing table to display only RIP-learned routes.

```
less
Copy code
Router# show ip route rip
R    192.168.1.0/24 [120/1] via 10.0.0.2, 00:00:15, Serial2/0
R    192.168.3.0/24 [120/1] via 11.0.0.2, 00:00:17, Serial3/0
```

Explanation:

- RIP is dynamically learning routes to **192.168.1.0/24** and **192.168.3.0/24** via the next hop IPs:
  - `10.0.0.2` on Serial2/0.
  - `11.0.0.2` on Serial3/0.
- The **metric (120/1)** indicates a hop count of `1`, meaning these routes are one router away.

Traffic Flow Through Router4

1. **Central Role**: Router4 acts as the central hub for all routing, ensuring that all traffic flows through the **server network**.
2. **RIP Propagation**: Routes are dynamically learned and shared with all routers in the network, allowing seamless communication between:
   - **Office 1** (`192.168.1.0/24`)
   - **Office 2** (`192.168.3.0/24`)
   - **Server Network** (`192.168.2.0/24`)
   - **Home Networks** and **VoIP** systems.
3. **Direct and Learned Routes**: Directly connected routes (C) and RIP-learned routes (R) confirm that **Router4** maintains connectivity for all subnets.

Conclusion

The configuration and verification of **RIP Version 2** on **Router4** ensure dynamic and efficient routing between all network segments. Verification outputs demonstrate that routes are properly advertised and accessible, with **Router4** serving as the central point of control for all network traffic.

4. Server Configuration

The **server room** is configured to centralise all essential services, ensuring seamless communication and resource management across the network. Below are the details for each server:

---

1. DHCP Server

The **DHCP Server** dynamically assigns IP addresses to devices across the network.

- **IP Pool Ranges**:
  - **Office 1**: `192.168.1.10 - 192.168.1.100`
  - **Office 2**: `192.168.3.10 - 192.168.3.100`
  - **Home Network 1**: `192.168.0.10 - 192.168.0.100`
  - **Home Network 2**: `192.168.5.10 - 192.168.5.100`
  - **VoIP Network**: `192.168.10.10 - 192.168.10.100`

DHCP Configuration (Sample for Office 1 and VoIP Network):

```
scss
Copy code
Router> enable
Router# configure terminal

Router(config)# ip dhcp pool OFFICE1
Router(dhcp-config)# network 192.168.1.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.1.1
Router(dhcp-config)# exit

Router(config)# ip dhcp pool VOIP
Router(dhcp-config)# network 192.168.10.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.10.1
Router(dhcp-config)# exit

Router# write memory
```

---

2. DNS Server

The **DNS Server** resolves domain names to IP addresses, enabling devices to communicate using hostnames.

- **Domain Name**: `smartoffice.local`
- **Key IP Mappings**:
  - **Web Server**: `web.smartoffice.local` → `192.168.2.10`
  - **FTP Server**: `ftp.smartoffice.local` → `192.168.2.20`
  - **Email Server**: `mail.smartoffice.local` → `192.168.2.30`

This configuration ensures simplified name resolution within the network.

---

3. Web Server

The **Web Server** hosts a basic test page to verify connectivity and internal web services.

- **Hosted Page**: A simple HTML file titled **"Smart Office Test Page"**.
- **Purpose**: To confirm that the web server is operational and reachable from all networks.

---

4. FTP Server

The **FTP Server** allows secure file transfers across the network.

- **IP Address**: `192.168.2.20`
- **Directory Structure**:
  - `/uploads`: For uploading files.
  - `/downloads`: For accessing shared files.
- **Verification**: File transfers tested using standard FTP commands and clients like **FileZilla**.

---

5. Email Server

The **Email Server** enables internal email communication using **SMTP**.

- **Domain**: `smartoffice.local`
- **IP Address**: `192.168.2.30`
- **Purpose**: Handles mail delivery between users within the network.
- **Verification**: Email sending functionality tested using SMTP commands via Telnet.

Conclusion

The server configurations ensure effective resource management, with DHCP enabling dynamic IP allocation, DNS simplifying communication via hostnames, and web, FTP, and email servers providing essential services. These servers form the foundation for secure and reliable operations within the smart office network.

5. ACL Configuration

Access Control Lists (ACLs) have been configured on **Router4** to enhance network security by preventing direct communication between devices in different subnets. Traffic flows are explicitly defined, ensuring that only permitted communication can occur while all other traffic is denied by default.

Router4 Access List Configuration

The following **Extended Access List (ACL 101)** has been implemented on **Router4**:

```
scss
Copy code
Router> enable
Router# configure terminal
Router(config)# access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.2.0
0.0.0.255
Router(config)# access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.2.0
0.0.0.255
Router(config)# access-list 101 permit ip 192.168.4.0 0.0.0.255 192.168.2.0
0.0.0.255

Router(config)# access-list 101 deny ip 192.168.1.0 0.0.0.255 192.168.3.0
0.0.0.255
Router(config)# access-list 101 deny ip 192.168.1.0 0.0.0.255 192.168.4.0
0.0.0.255
Router(config)# access-list 101 deny ip 192.168.3.0 0.0.0.255 192.168.4.0
0.0.0.255
Router(config)# access-list 101 deny ip 192.168.4.0 0.0.0.255 192.168.1.0
0.0.0.255
Router(config)# access-list 101 deny ip 192.168.4.0 0.0.0.255 192.168.3.0
0.0.0.255

Router(config)# access-list 101 permit ip any any
Router(config)# exit
Router# write memory
```

Explanation of Rules

Rule	Source	Destination	Action	Purpose
Line 10	`192.168.1.0/24`	`192.168.2.0/24`	**Permit**	Allow Office 1 to communicate with servers.
Line 20	`192.168.3.0/24`	`192.168.2.0/24`	**Permit**	Allow Office 2 to communicate with servers.
Line 30	`192.168.4.0/24`	`192.168.2.0/24`	**Permit**	Allow VoIP network to communicate with servers.
Line 40-90	Various subnets	Various subnets	**Deny**	Block direct communication between devices.
Line 100	`any`	`any`	**Permit**	Allow all other traffic by default.

Traffic Examples

1. **Permitted Traffic**:
   - Devices in **192.168.1.0/24** (Office 1) can communicate with servers in **192.168.2.0/24**.
   - Devices in **192.168.3.0/24** (Office 2) can communicate with servers in **192.168.2.0/24**.
   - VoIP devices in **192.168.4.0/24** can communicate with servers in **192.168.2.0/24**.
2. **Denied Traffic**:
   - Devices in **192.168.1.0/24** cannot directly communicate with devices in **192.168.3.0/24**.
   - Devices in **192.168.4.0/24** cannot directly communicate with devices in **192.168.1.0/24** or **192.168.3.0/24**.

Verification of ACLs

```
Router# show access-lists
```

Output:

```
arduino
Copy code
Extended IP access list 101
  10 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
  20 permit ip 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255
  30 permit ip 192.168.4.0 0.0.0.255 192.168.2.0 0.0.0.255
  40 deny ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
  50 deny ip 192.168.1.0 0.0.0.255 192.168.4.0 0.0.0.255
  60 deny ip 192.168.3.0 0.0.0.255 192.168.4.0 0.0.0.255
  70 deny ip 192.168.4.0 0.0.0.255 192.168.1.0 0.0.0.255
  80 deny ip 192.168.4.0 0.0.0.255 192.168.3.0 0.0.0.255
```

```
100 permit ip any any
```

Conclusion

The Access Control List (ACL 101) implemented on **Router4** ensures that:

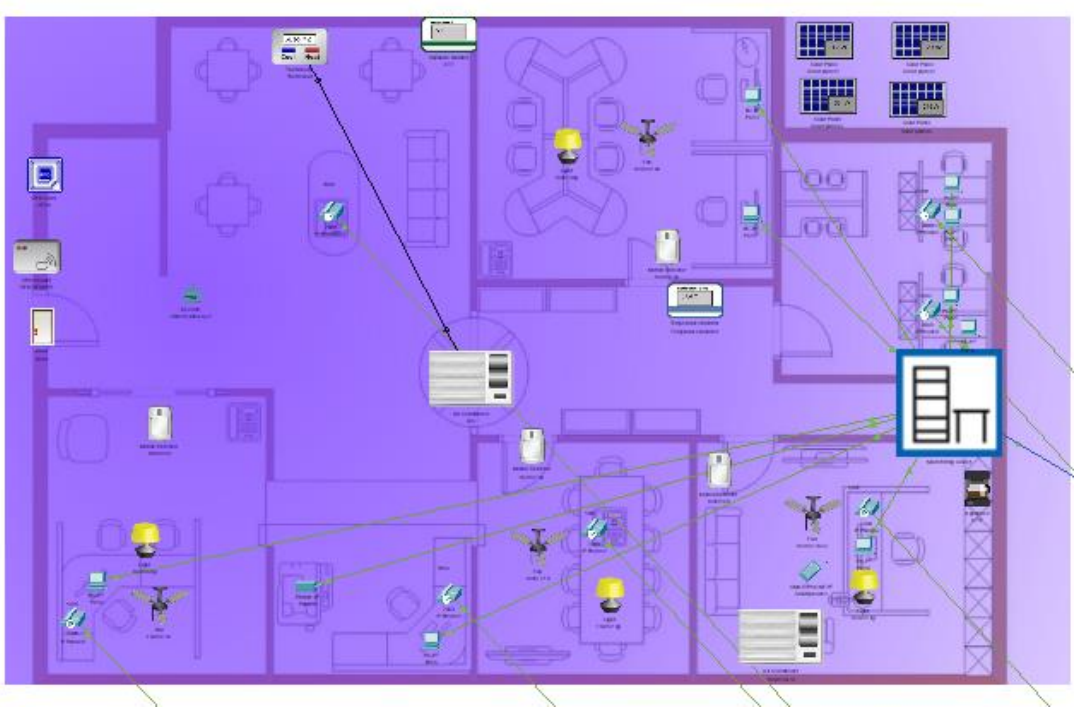
1. Communication between subnets is restricted to pass through the server network.
2. Direct device-to-device communication is blocked to enhance security.
3. Traffic intended for the server room is explicitly permitted.

The ACL configuration aligns with the **security goals** of the smart office network while allowing necessary traffic for seamless operations.

6. IoT Integration

The **IoT integration** in the smart office network enhances automation, energy efficiency, and user convenience. The IoT devices are deployed within the **home networks** and operate on a dedicated **LAN setup** to ensure smooth and reliable communication.

IoT Devices



The following IoT devices are integrated into the system:

- **Motion Sensors**: Detect movement to automatically turn on/off **fans** and **lights**.
- **RFID Doors**: Control door access for authorised users.
- **Coffee Machine**: Smart coffee machine that can be activated remotely.
- **Air Conditioning (AC)**: Integrated with a **thermostat** for temperature control.
- **IoT Monitor**: A **smartphone-based control panel** to view and manage all IoT devices.

---

2. LAN Setup for IoT Devices

The IoT devices are connected through a **home gateway** that facilitates wireless communication within the home networks. The setup includes:

- **IP Addressing**:
  - IoT devices operate on a dedicated LAN with a **gateway IP** of `192.168.25.1`.
  - The IP addresses for IoT devices are assigned dynamically via the **home gateway**.
- **Communication**:
  - IoT devices communicate over the **Local Area Network (LAN)**, ensuring minimal latency and reliable operation.
  - The **home gateway** enables wireless connectivity, allowing IoT devices to interact seamlessly.
- **Centralised Monitoring**:
  - All IoT devices can be monitored and controlled using a **smartphone IoT monitor**, providing a user-friendly interface for real-time control.

---

3. Summary of IoT Workflow

1. **Motion Sensors**: Detect activity → Send a signal to turn on fans and lights.
2. **RFID Doors**: Authenticate users → Unlock doors for authorised access.
3. **Coffee Machine**: Activated remotely using the smartphone monitor.
4. **AC Control**: Thermostat sends signals to the AC system to regulate temperature.
5. **Smartphone Integration**: All device statuses can be monitored and controlled remotely through the IoT monitor.

Conclusion

The IoT integration provides automation and centralised control of devices within the home network. Using a dedicated **LAN (192.168.25.1)** and wireless home gateways, the system ensures reliable connectivity and seamless management of IoT devices, improving convenience and efficiency in the smart office environment.

7. Conclusion and Future Improvements

Conclusion

The **smart office network** successfully achieves its goals of **centralised control**, **dynamic routing**, and **enhanced security**:

- All communication flows through the **server network** via Router4.
- **RIP Version 2** enables dynamic routing between offices, home networks, and VoIP.
- **Access Control Lists (ACLs)** restrict direct device communication, ensuring security.
- IoT devices provide automation and user convenience within a dedicated LAN.

Limitations

- **Scalability**: RIP Version 2 limits network growth due to its 15-hop restriction.
- **Redundancy**: A single point of failure exists at **Router4**.
- **Security**: Advanced measures like firewalls and encryption are absent.

Future Improvements

1. **Upgrade to VLANs** for better segmentation and traffic management.
2. Replace RIP with **OSPF** or **EIGRP** for improved scalability and performance.
3. Add **redundant routers** using **HSRP** to eliminate single points of failure.
4. Enhance security with **firewalls** and **IPsec encryption**.
5. Deploy **network monitoring tools** like SNMP for real-time management.

By addressing these limitations, the network can achieve greater **scalability**, **security**, and **reliability** for long-term performance.