National University
Of Computer and Emerging Sciences

Final Project

Campus Network with Multi-Department Subnetting

An Assignment presented to

Ma'am Anum Mehmood

In partial fulfillment
of the requirement for the course of

Computer Networks

By

Arban Arfan
22i-0981
CS-E

Campus Network with Multi-Department Subnetting

Project Details:

Network Designed using Cisco Packet Tracer for a campus with departments like Administration, Faculty, and Student Labs for Computer-Science and Business Department. Each department has its own subnet, configured with DHCP for dynamic IP allocation. NAT is implemented to allow internet access, while routing enables inter-departmental communication.

Table of Contents

Objective

The primary objective of this project was to design a robust and secure network architecture using Cisco Packet Tracer. This architecture was tailored to enable seamless and secure communication between various departments, such as the **Department of Computer Science** and the **Department of Business Administration (BBA)**, with the administrative unit.

Key goals included:

- Ensuring efficient and automated IP allocation for departmental servers using **Dynamic Host Configuration Protocol (DHCP)**.
- Implementing advanced techniques such as **Network Address Translation (NAT)** and routing protocols like **Routing Information Protocol (RIP)** and **Open Shortest Path First (OSPF)** to achieve fast, reliable, and secure communication.
- Utilizing **subnetting** and other strategic methodologies to establish an optimized, scalable, and secure network design.

This project aimed to provide a well-structured, high-performing network that fulfills the requirements of secure and reliable communication while maintaining operational efficiency.

Technologies Used

This project utilized a range of tools, protocols, and frameworks to design and implement the network architecture effectively. The key technologies employed include:

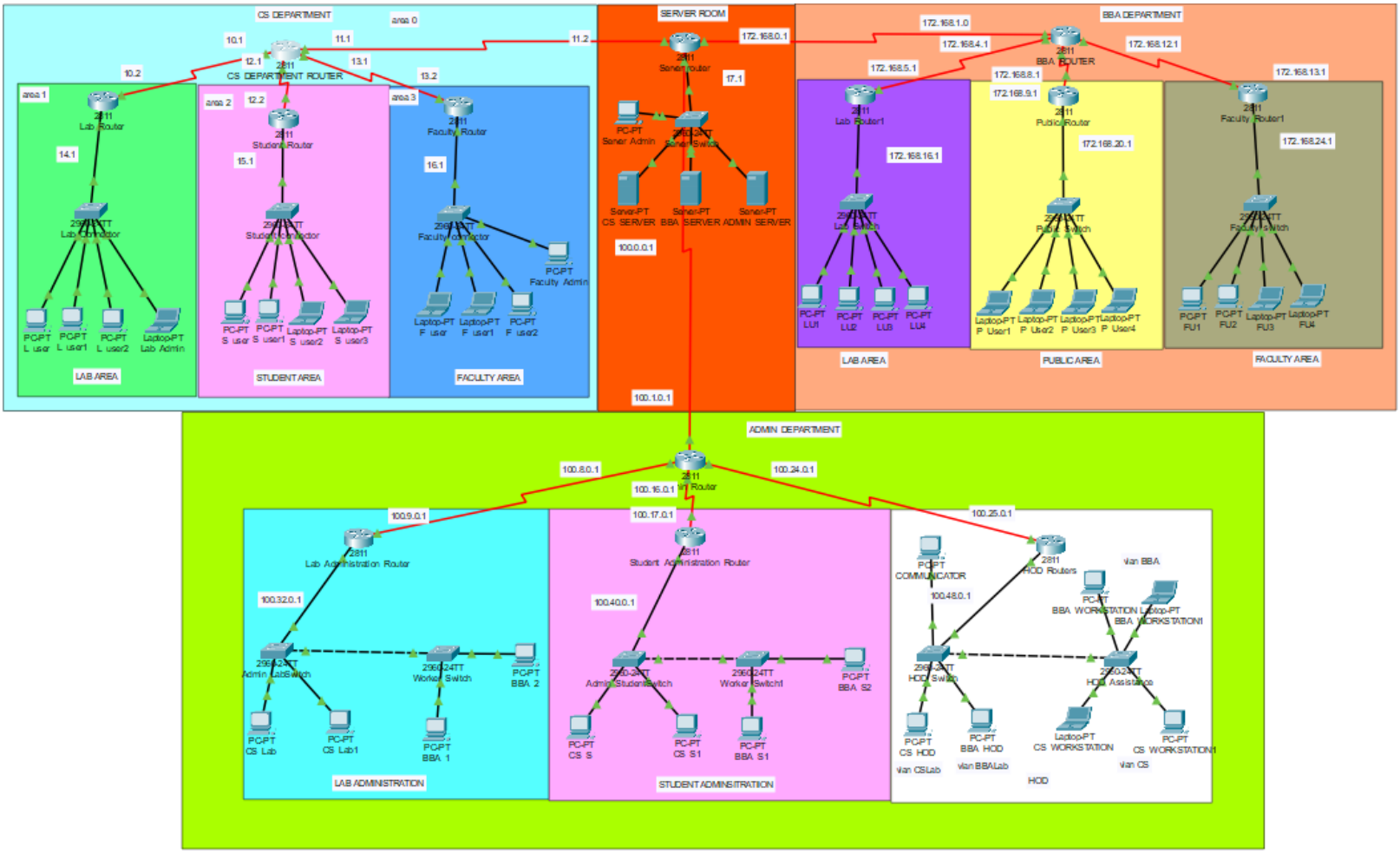
1. **Cisco Packet Tracer**
    - A powerful network simulation tool used for designing, configuring, and testing the network architecture.
2. **Dynamic Host Configuration Protocol (DHCP)**
    - Automated IP allocation for departmental devices and servers to ensure efficient network management.
3. **Network Address Translation (NAT)**
    - Secured communication by conserving IP addresses and enabling seamless internal-to-external network connectivity.
4. **Routing Protocols**
    - **Routing Information Protocol (RIP)** and **Open Shortest Path First (OSPF)** were implemented to enable dynamic routing, optimize paths, and enhance communication speed and reliability.
5. **Subnetting**
    - Applied to divide the network into smaller, manageable segments to improve efficiency, security, and scalability.
6. **Virtual Local Area Networks (VLANs)**
    - VLANs were configured for the **Head of Departments (HODs)** of the Computer Science and Business Administration (BBA) departments to communicate securely and directly with their workers, ensuring logical segmentation of the network.
7. **Access Control Lists (ACLs)**
    - ACLs were applied to prevent unauthorized communication, such as restricting direct interaction between students and the administrative unit, thereby enhancing network security.

Implementation Details

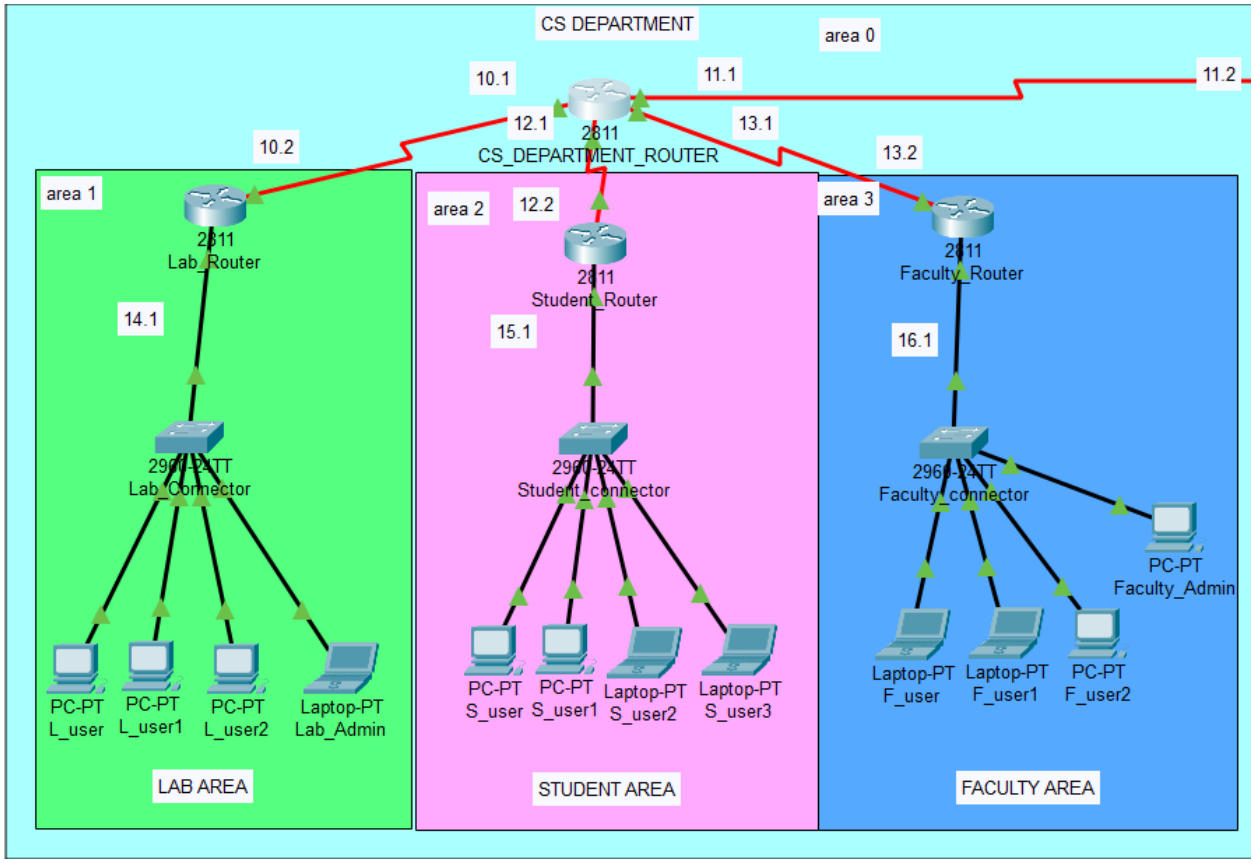
Network Architecture:

There are four major departments that are listed below and will be further explained in the document later.

1. **Computer Science Department (CS)**
2. **Business Administration Department (BBA)**
3. **Server Room**
4. **Administration Department**



Computer Science Department:



Network Design: One main router **'CS_DEPARTMENT_ROUTER'** is connected with Lab, student and Faculty router to provide secure and reliable communication to the entire network and monitor the department's activity and access. Besides that, Class C subnet and IP addresses are used for better **OSPF** and **NAT** configuration.

IP Addresses Assigned to Sub-Networks:

Name	IP Addresses
Lab Area	192.168.14.0
Student Area	192.168.15.0
Faculty Area	192.168.16.0
Main Router to Lab Area	192.168.10.0
Main Router to Students Area	192.168.12.0
Main Router to Faculty Area	192.168.13.0
Main Router to Server Room	192.168.11.0

Routing Protocols: Open Shortest Path First (OSPF) was implemented to enable dynamic routing, optimize paths, and enhance communication speed and reliability.

```
router ospf 1
 log-adjacency-changes
 network 192.168.10.0 0.0.0.255 area 1
 network 192.168.12.0 0.0.0.255 area 2
 network 192.168.13.0 0.0.0.255 area 3
 network 192.168.11.0 0.0.0.255 area 0
```

Dynamic Host Configuration Protocol (DHCP): Automated IP allocation for departmental devices and servers to ensure efficient network management. The IP addresses for all of the end-systems are provided by ***'CS_SERVER'*** which is attached in the **Server Room**.

Network Address Translation (NAT): Secured communication by conserving IP addresses and enabling seamless internal-to-external network connectivity.

```
interface Serial0/0/0
 ip address 192.168.10.1 255.255.255.0
 ip nat inside
 clock rate 2000000
!
interface Serial0/1/0
 ip address 192.168.13.1 255.255.255.0
 ip nat inside
 clock rate 2000000
!
interface Serial0/2/0
 ip address 192.168.11.1 255.255.255.0
 ip nat outside
 clock rate 2000000
!
interface Serial0/3/0
 ip address 192.168.12.1 255.255.255.0
 ip nat inside
 clock rate 2000000
```

```
ip nat pool CS_DEPARTMENT 192.168.11.4 192.168.11.8 netmask 255.255.255.0
ip nat inside source list 1 pool CS_DEPARTMENT
ip classless
```

Access Control Lists (ACLs): ACLs were applied to prevent unauthorized communication, such as restricting direct interaction between students and the administrative unit, thereby enhancing network security.

```
access-list 1 deny 192.168.15.0 0.0.0.255
access-list 1 permit any
```

NAT and Access Control Configuration Code:

access-list 1 deny 192.168.15.0 0.0.0.255

access-list 1 permit any

ip nat pool CS_DEPARTMENT 192.168.11.4 192.168.11.8 netmask 255.255.255.0

ip nat inside source list 1 pool CS_DEPARTMENT

int se0/2/0

ip nat outside

int se0/3/0

ip nat inside

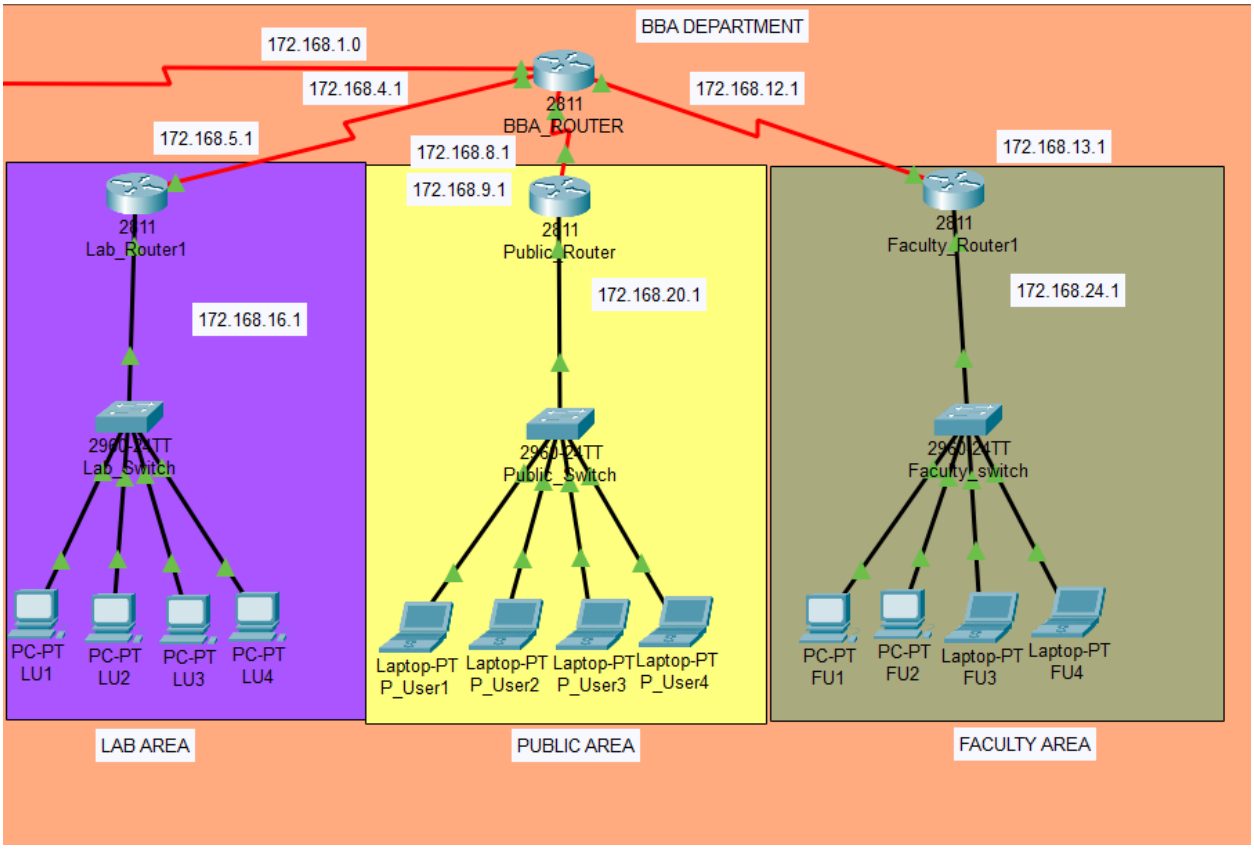
int se0/0/0

ip nat inside

int se0/1/0

ip nat inside

Business Administration Department (BBA):



Network Design: One main router **'BBA_ROUTER'** is connected with Lab, Public and Faculty router to provide secure and reliable communication to the entire network and monitor the department's activity and access. Besides that, **Subnetting** is implemented to divide the network into smaller, manageable segments to improve efficiency, security, and scalability. Whereas, for routing **RIP** is used.

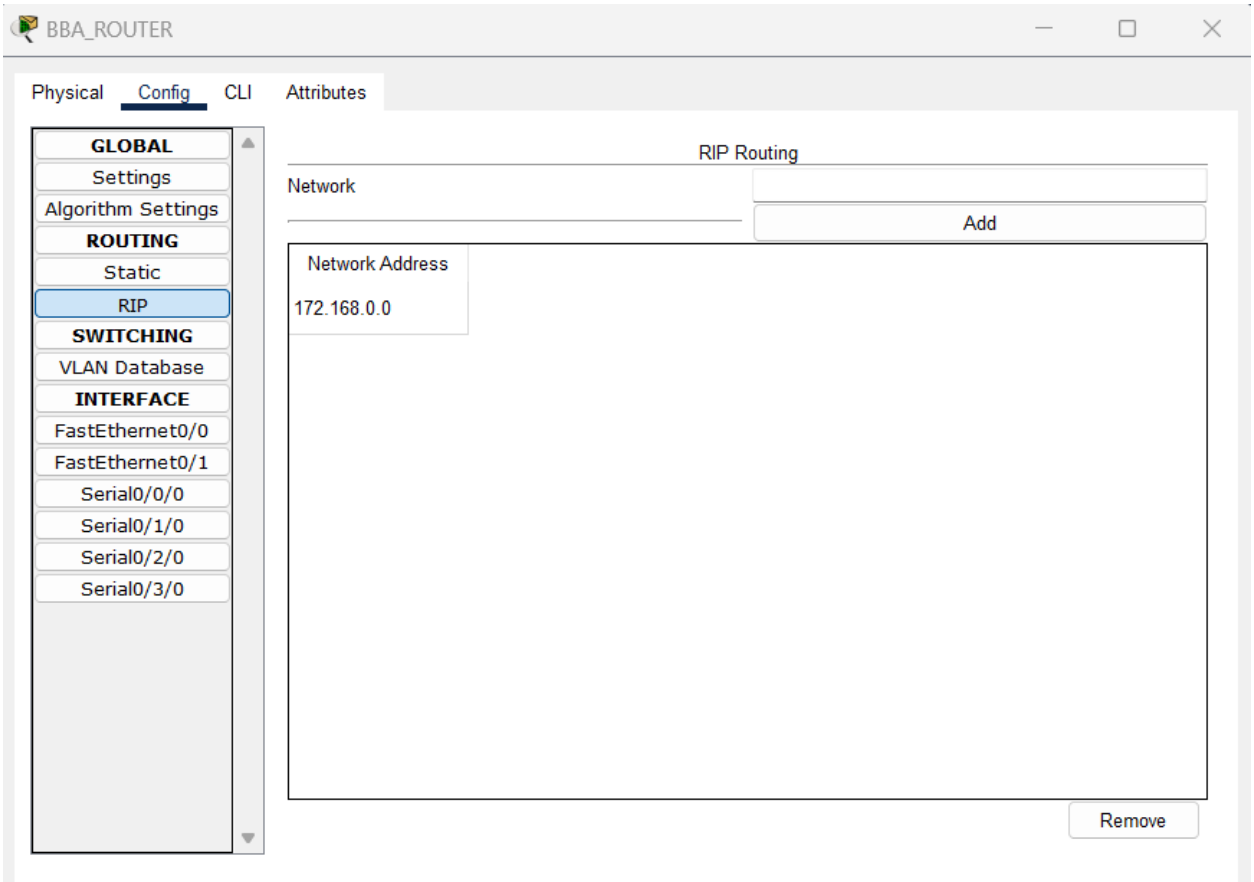
Subnetting Method Used:

Methods	Assignments
IP Address	172.168.1.0
Class	B
Number of Required Hosts	160
Number of Required Subnets	64
Subnet Mask	255.255.252.0
Range	4
Network	172.168.0.0

IP Addresses Assigned to Sub-Networks:

Name	IP Addresses
Lab Area	172.168.16.0
Public Area	172.168.20.0
Faculty Area	172.168.24.0
Main Router to Lab Area	172.168.4.0
Main Router to Public Area	172.168.8.0
Main Router to Faculty Area	172.168.12.0
Main Router to Server Room	172.168.0.0

Routing Protocols: Routing Information Protocol (RIP) was implemented to enhance communication speed and reliability.

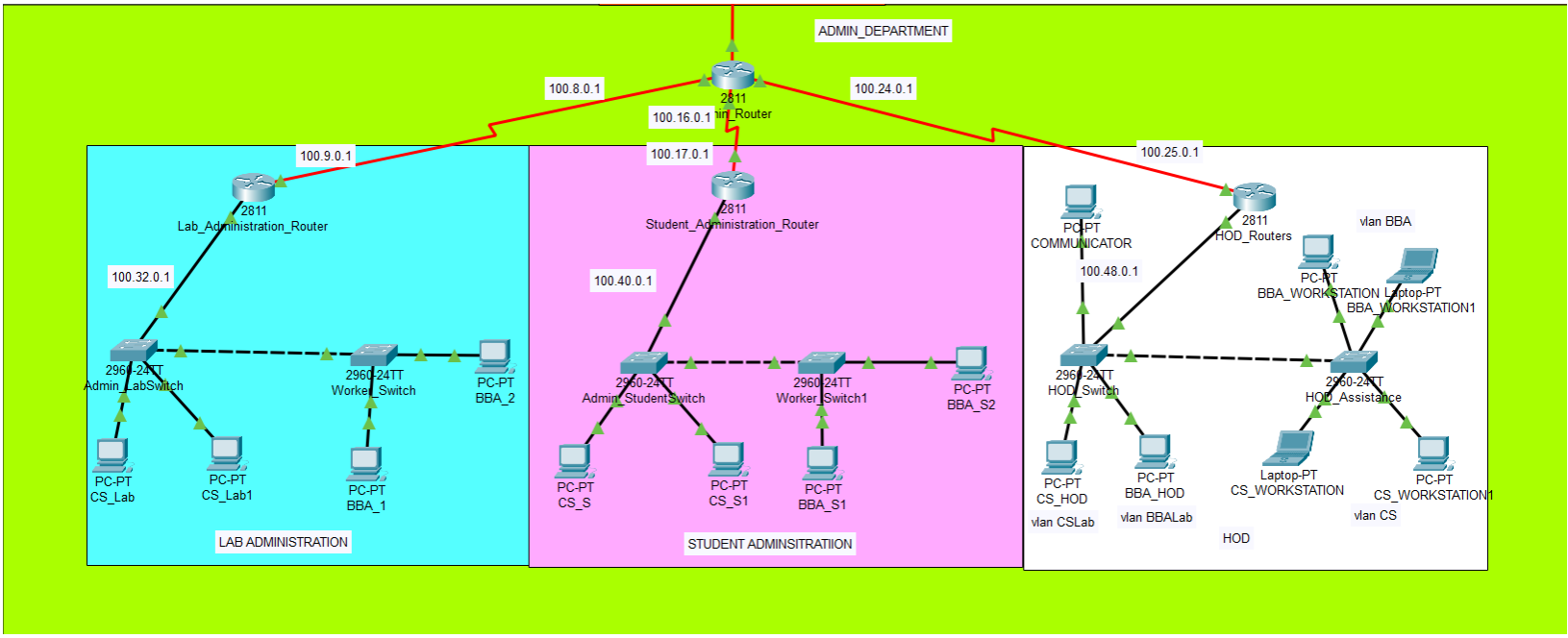


Dynamic Host Configuration Protocol (DHCP): Automated IP allocation for departmental devices and servers to ensure efficient network management. The IP addresses for all of the end-systems are provided by ***'BBA_SERVER'*** which is attached in the **Server Room**.

Access Control Lists (ACLs): ACLs were applied to prevent unauthorized communication, such as restricting direct interaction between **Public Area** and the administrative unit, thereby enhancing network security.

```
access-list 1 deny 100.0.0.0 0.255.255.255
access-list 1 permit any
```

Administration Department:



Network Design: One main router **'ADMIN_ROUTER'** is connected with Lab, Public and Faculty router to provide secure and reliable communication to the entire network and monitor the department's activity and access. Besides that, **Subnetting** is implemented to divide the network into smaller, manageable segments to improve efficiency, security, and scalability. Whereas, for routing **RIP** is used. In addition to **Virtual Local Area Networks (VLANs)** is also used for **Head of Departments (HODs)** of the Computer Science and Business Administration (BBA) departments to communicate securely and directly with their workers, ensuring logical segmentation of the network.

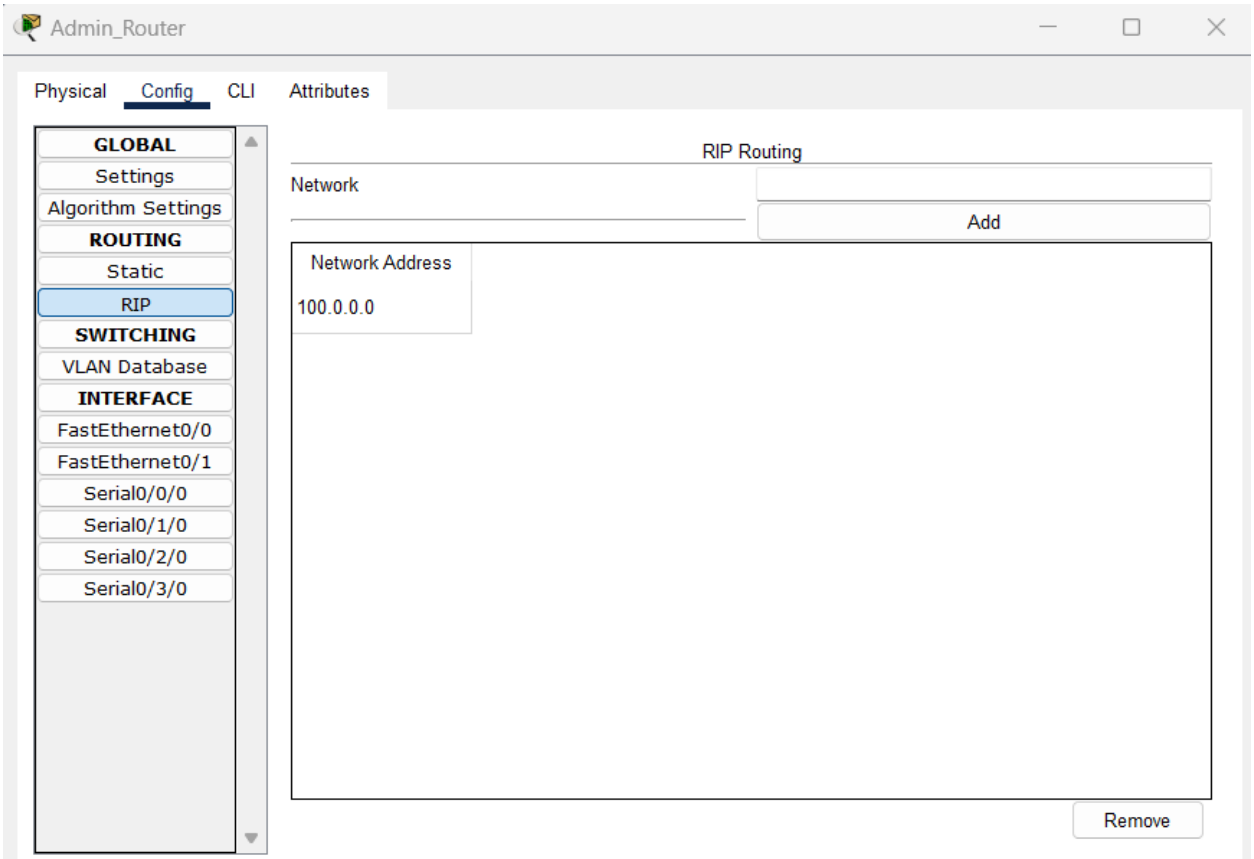
Subnetting Method Used:

Methods	Assignments
IP Address	100.0.0.0
Class	A
Number of Required Hosts	128
Number of Required Subnets	32
Subnet Mask	255.248.0.0
Range	8
Network	100.0.0.0

IP Addresses Assigned to Sub-Networks:

Name	IP Addresses
Lab Administration	100.32.0.0
Student Administration	100.40.0.0
HOD	100.48.0.0
Main Router to Lab Administration	100.8.0.0
Main Router to Student Administration	100.16.0.0
Main Router to HOD	100.24.0.0
Main Router to Server Room	100.0.0.0

Routing Protocols: Routing Information Protocol (RIP) was implemented to enhance communication speed and reliability.

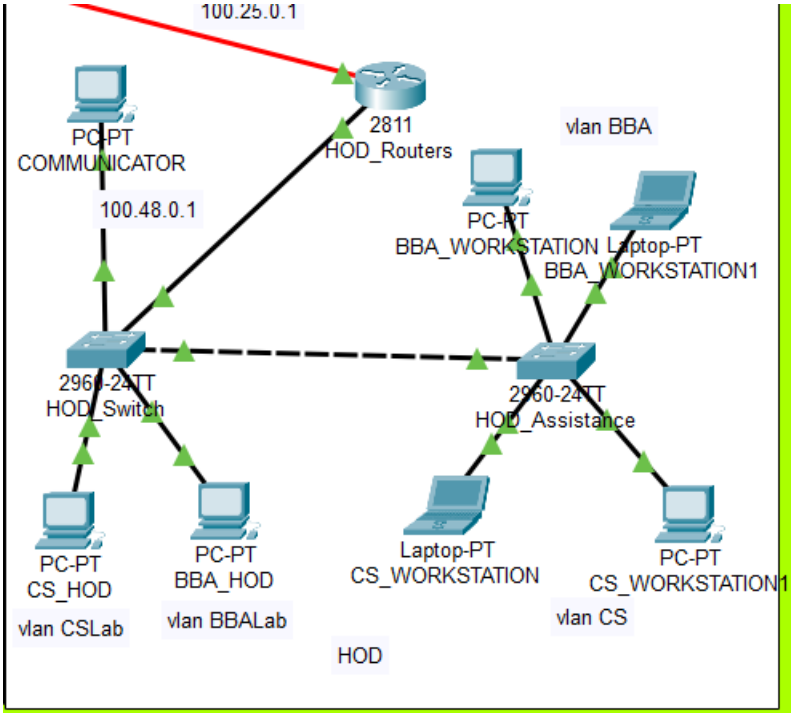


Dynamic Host Configuration Protocol (DHCP): Automated IP allocation for departmental devices and servers to ensure efficient network management. The IP addresses for all of the end-systems are provided by ***'ADMIN_SERVER'*** which is attached in the **Server Room**.

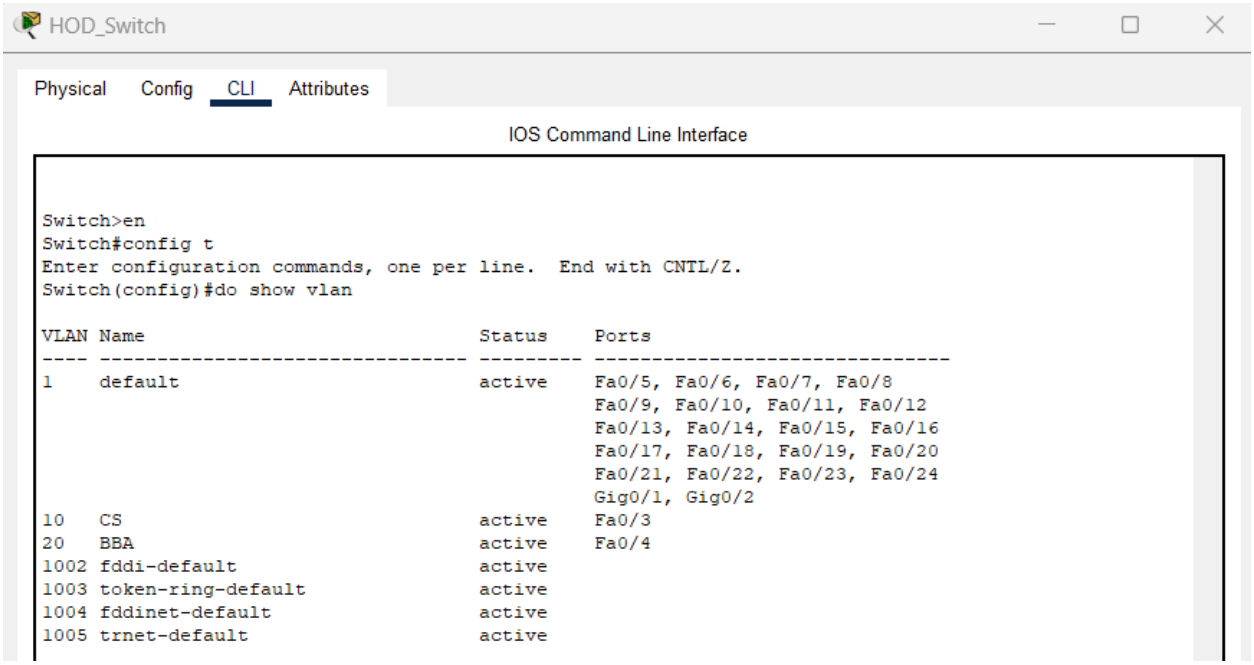
Access Control Lists (ACLs): ACLs were applied to prevent unauthorized communication, such as restricting direct interaction between students and the administrative unit, thereby enhancing network security.

```
access-list 1 deny 192.168.15.0 0.0.0.255
access-list 1 permit any
access-list 1 deny 172.168.1.0 0.0.0.255
```

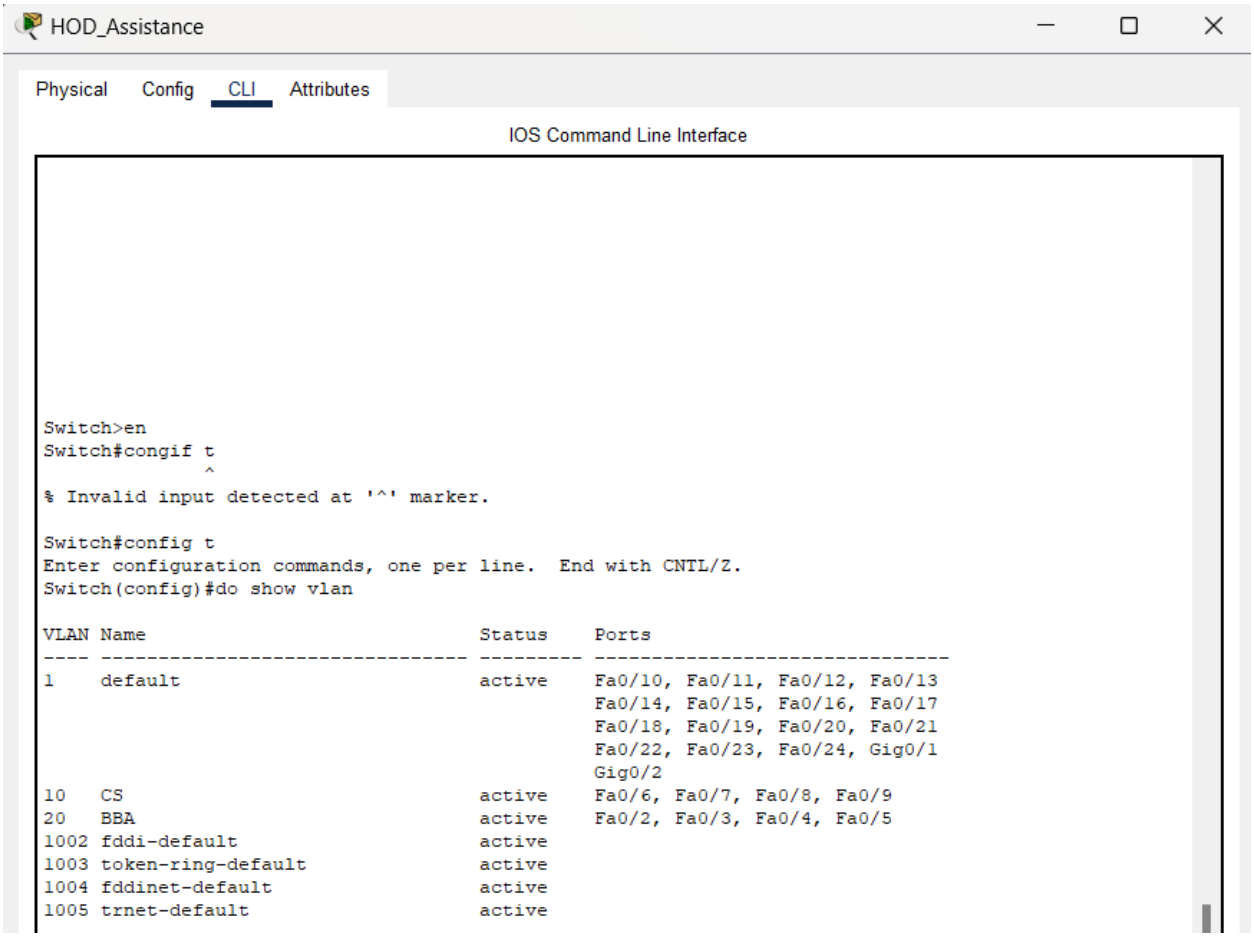
Virtual Local Area Networks (VLANs): VLANs were configured for the **Head of Departments (HODs)** of the Computer Science and Business Administration (BBA) departments to communicate securely and directly with their workers.



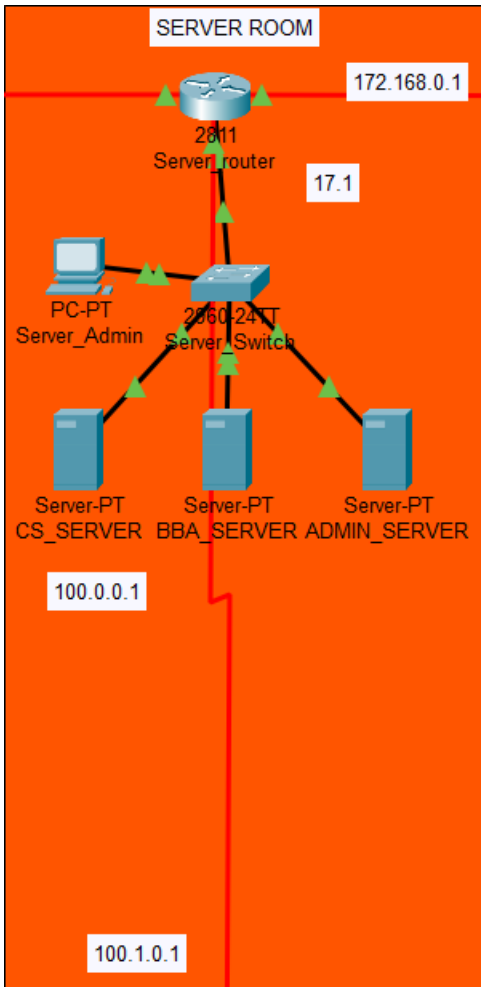
HOD Switch Configuration



Worker Switch Configuration



Server Room:



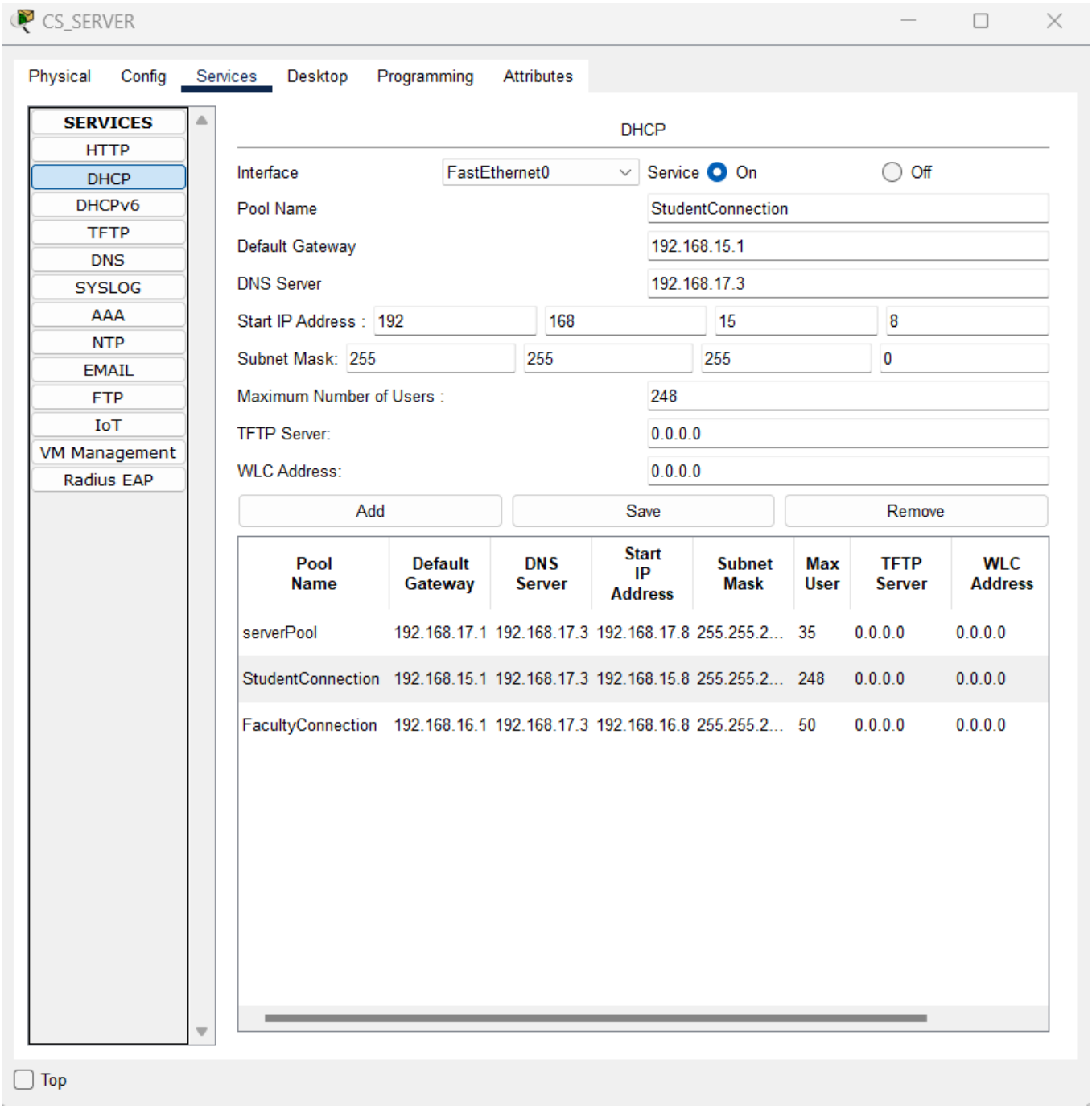
Network Design: One main router **'SERVER_ROUTER'** is connected with Lab, Public and Faculty router to provide secure and reliable communication to the entire network and monitor the department's activity and access. Besides that, its main purpose t to allocate IP addresses to the end-systems of the entire department through **DHCP**.

Three Servers are attached as mentioned below

1. **CS_SERVER** *: Assigning IP addresses to **CS DEPARTMENT***
2. **BBA_SERVER** *: Assigning IP addresses to **BBA DEPARTMENT***
3. **ADMIN_SERVER** *: Assigning IP addresses to **ADMINISTRATION DEPARTMENT***

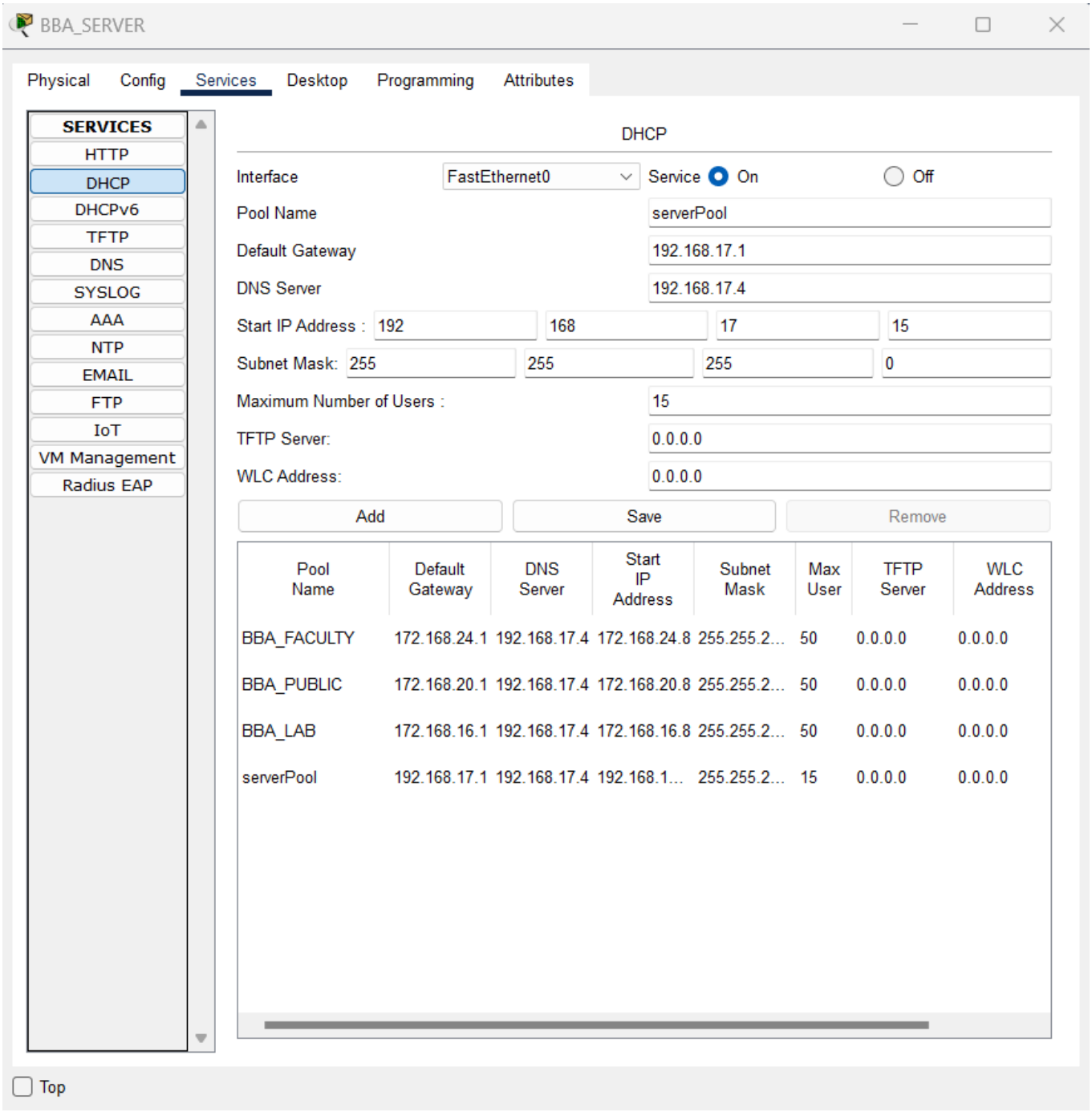
Besides that, a *Server_Admin* end system is also attached to handle and monitor the Server Room.

DHCP Allocation of CS Department via CS SERVER

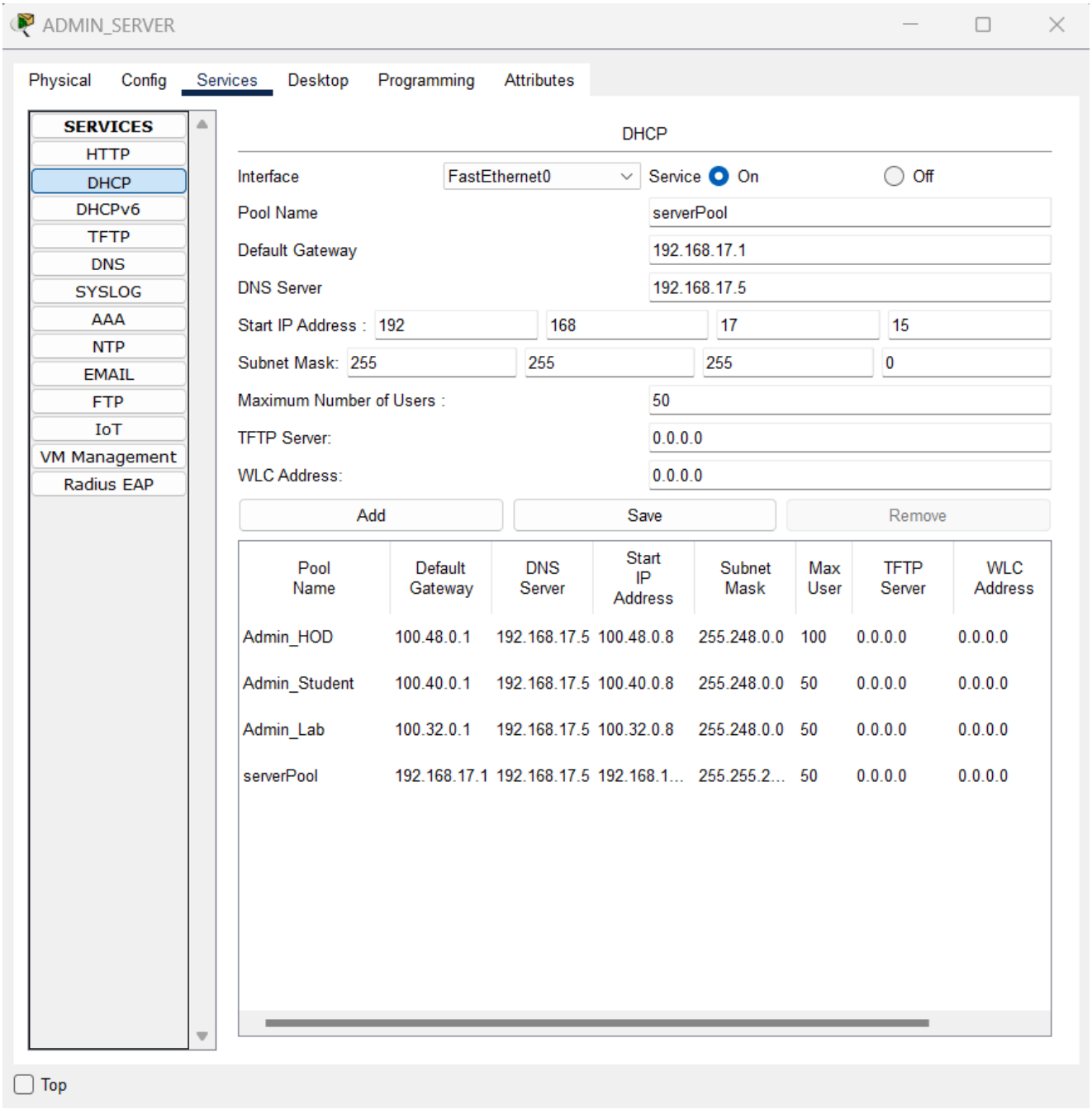


The lab Area of Students were connected through Static IP Addresses allocation approach.

DHCP Allocation of BBA Department via BBA SERVER



DHCP Allocation of ADMINISTRATION Department via ADMIN SERVER



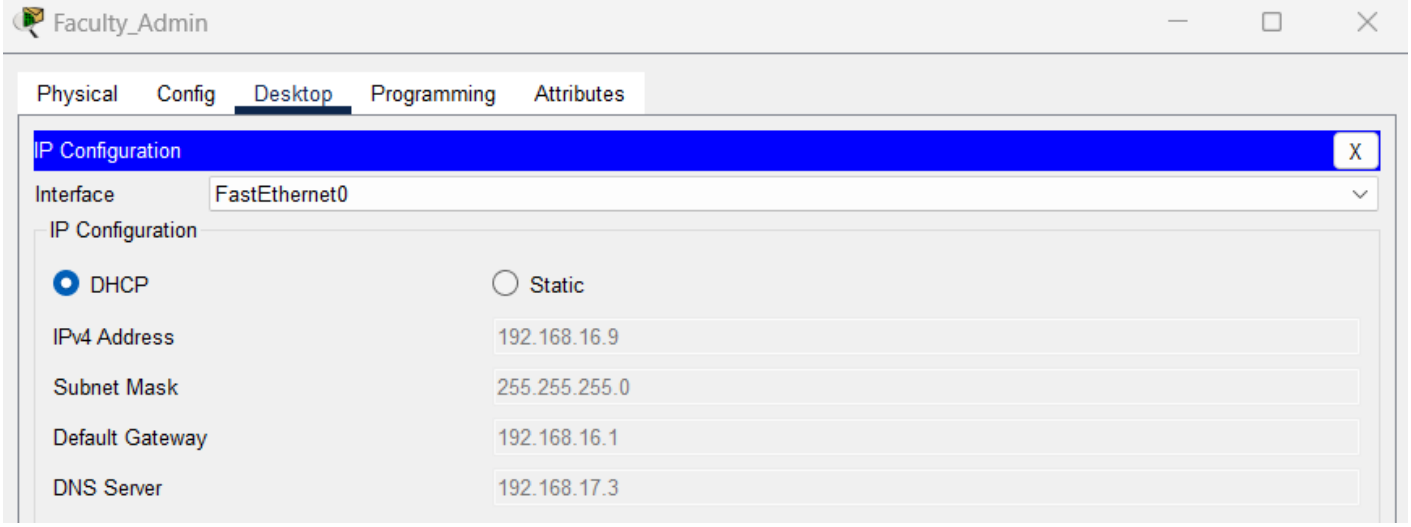
Results and Testing

Overall Network Testing

Scenario 0 | New | Delete | Toggle PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Faculty_Admin	Server_Admin	ICMP		0.000	N	0	(edit)	(delete)
	Successful	Faculty_Admin	FU1	ICMP		0.000	N	1	(edit)	(delete)
	Successful	F_user2	Lab_Admin	ICMP		0.000	N	2	(edit)	(delete)
	Successful	Faculty_Admin	CS_S	ICMP		0.000	N	3	(edit)	(delete)

DHCP Testing



Access Control Testing

Scenario 0 | New | Delete | Toggle PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Failed	S_user	CS_Lab	ICMP		0.000	N	0	(edit)	(delete)
	Failed	P_User1	BBA_S2	ICMP		0.000	N	1	(edit)	(delete)
	Failed	CS_HOD	S_user	ICMP		0.000	N	2	(edit)	(delete)
	Failed	BBA_HOD	P_User4	ICMP		0.000	N	3	(edit)	(delete)

Admin VLAN Testing

Scenario 0 | New | Delete | Toggle PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	CS_HOD	CS_WORKSTATION	ICMP		0.000	N	0	(edit)	(delete)
	Failed	CS_HOD	BBA_WORKSTATION	ICMP		0.000	N	1	(edit)	(delete)
	Successful	BBA_HOD	BBA_WORKSTATION	ICMP		0.000	N	2	(edit)	(delete)
	Failed	BBA_HOD	CS_WORKSTATION	ICMP		0.000	N	3	(edit)	(delete)

Challenges and Learning

During the implementation of the **Campus Network with Multi-Department Subnetting**, several challenges were encountered, each of which provided valuable learning opportunities:

1. **Configuring NAT for Multiple Departments**
    - **Challenge**: While implementing Network Address Translation (NAT) for CS Department, ensuring accurate mapping of internal to external IPs within the given address pool proved complex. Misconfigurations led to connectivity issues between departments and the internet.
    - **Learning**: A systematic approach to configuring NAT pools and associated ACLs ensured seamless internal and external communications. Properly defining access rules and conducting iterative testing mitigated errors.
2. **Subnetting Large and Small Networks**
    - **Challenge**: Balancing the allocation of IP addresses for departments with varying size and traffic requirements was intricate. Misaligned subnet masks initially resulted in inefficient IP utilization and connectivity problems.
    - **Learning**: Advanced planning and iterative subnet calculations using binary math ensured optimal IP allocation for departments. Tools like IP subnet calculators proved invaluable.
3. **Routing Protocol Integration**
    - **Challenge**: Integrating RIP for some departments and OSPF for others required careful coordination to prevent routing loops and ensure compatibility.
    - **Learning**: Understanding the operational differences between RIP and OSPF, including metric computation and convergence time, enabled smoother protocol integration and enhanced network reliability.
4. **Access Control Lists (ACLs) for Security**
    - **Challenge**: Designing ACLs to allow authorized communication while blocking unauthorized access was a meticulous task. Initial ACL configurations inadvertently blocked legitimate traffic.

- **Learning**: A layered approach to ACL design—starting with broader rules and refining them—ensured secure yet flexible communication. Testing scenarios highlighted the importance of sequential rule application in ACLs.

5. **VLAN Configuration**
    - **Challenge**: Setting up VLANs for the HODs of different departments and ensuring proper inter-VLAN routing required precise configuration. Misconfigured VLAN tags initially disrupted communication.
    - **Learning**: Understanding VLAN tagging and applying trunk ports effectively established logical segmentation and enhanced security for departmental heads.

Conclusion

The successful completion of the **Campus Network with Multi-Department Subnetting** project resulted in a robust and scalable network architecture tailored to the requirements of a multi-departmental campus. Key outcomes include:

- **Efficient Communication**: Implementation of OSPF and RIP ensured reliable inter-departmental communication with optimized routing paths.
- **Enhanced Security**: ACLs and VLANs provided a secure environment by restricting unauthorized access and logically segmenting the network.
- **Seamless Management**: Centralized DHCP servers automated IP allocation, reducing administrative overhead and improving operational efficiency.
- **Scalable Design**: Subnetting and VLAN configurations support future expansions, accommodating additional users and departments without significant redesigns.