NETWORK DESIGN PROPOSAL FOR AIRPORT

A CASE STUDY REPORT

Submitted by

PIYUSH PRAKASH WAKPAIJAN (RA2211003011274)
HARSHINI KASTURI (RA2211003011299)
NAGA LATHIKA KOMMINENI (RA2211003011310)
CHETNA RAJEEV(RA2211003011314)

for the course

21CSC302J – COMPUTER NETWORKS

in partial fulfillment of the requirements for the degree of

BACHELOR OF TECHNOLOGY

SRM
INSTITUTE OF SCIENCE & TECHNOLOGY
Deemed to be University u/s 3 of UGC Act, 1956

DEPARTMENT OF COMPUTING TECHNOLOGIES
SCHOOL OF COMPUTING
FACULTY OF ENGINEERING AND TECHNOLOGY
SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
KATTANKULATHUR - 603 203.

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
KATTANKULATHUR – 603 203

BONAFIDE CERTIFICATE

Certified that Computer Network A Case Study Report titled "**Network Design Proposal for Airport**" is the bonafide work of "**Piyush Prakash Wakpaijan" [RA2211003011274]**, "**Harshini Kasturi" [RA2211003011299]**, "**Naga Lathika Kommineni" [RA2211003011310]**, "**Chetna Rajeev" [RA2211003011314]** who carried out the case study under my supervision. Certified further, that to the best of my knowledge the work reported herein does not form any other work.

SIGNATURE OF FACULTY NAME

DR. A. JEYASEKAR
ASSOCIATE PROFESSOR
Department of Computing Technologies

Date :

ABSTRACT

Airports are critical infrastructures that demand high security and robust connectivity to support various operations, including administrative control, flight services, and guest services. This project proposes a comprehensive network design for an airport setting with three departments: Airport Authority, Flight Service Providers, and Guests. Each department has specific access needs, with the Airport Authority managing flight management servers, the Flight Service Providers requiring access to specific airport servers, and Guests needing high-speed wireless internet access.The network design includes layered security and access controls to ensure that each department operates independently, minimizing the risk of unauthorized access while facilitating seamless connectivity. The Airport Authority's network is configured to handle the secure management of flight operations, accessible only to authorized personnel and the Flight Service Providers. For guest users, a high-speed wireless network with a shared password ensures ease of access while remaining isolated from the sensitive departments. Automated IP address allocation via DHCP will be implemented to streamline device connections across all user categories. This setup provides a balanced approach to accessibility, security, and operational efficiency, ensuring that airport networking infrastructure supports modern demands and the sensitive nature of airport environments.

Table of Contents

Abstract.. iii

1. Introduction.. 1

1.1 Background...1

1.2 Objectives..1

2. Network Design...2

2.1 Topology...2

2.2 Requirement Analysis of Active Networking Components..3

2.3 Network Implementation Plan...4

2.4 VPN Design and Integration...6

3. Network Configuration and Guidelines...8

3.1 Switch Configuration..8

3.2 Router Configuration..9

3.3 DHCP Configuration..11

3.4 VPN Configuration..13

4. Security Measures...15

7. Testing and Validation.. 16

8. Results and Evaluation.. 18

9. Conclusion..19

10. References.. 20

11. Appendices... 20

TABLE OF FIGURES

FIGURE 1:TOPOLOGY OF FULL NETWORK..2

FIGURE 2: VLAN FOR SWITCH 2...5

FIGURE 3: DHCP IP ADDRESSING..12

FIGURE 4: DHCP SERVER POOL.. 12

FIGURE 5: DHCP GATEWAY...13

FIGURE 6: TRACEROUTE SUCCESSFUL..16

FIGURE 7: IP ALLOCATION..17

FIGURE 8: PERFORMANCE MEASURE THROUGH PING TIME..................................18

1. INTRODUCTION

1.1 Background

Airports are complex, high-security environments that rely on sophisticated networking solutions to ensure efficient operations and data security across multiple departments. As critical infrastructure, they depend on technology to manage administrative functions, flight operations, and guest services. This project outlines a network proposal for an airport with three main user groups: Airport Authority, Flight Service Providers, and Guests. Each has distinct needs: the Airport Authority requires a secure network for managing flight operations; Flight Service Providers need controlled access to specific airport resources; and Guests require high-speed wireless internet that is isolated from the other networks. Automatic IP allocation through DHCP and a shared password for guest Wi-Fi ensure ease of use while maintaining security. This network structure balances security, accessibility, and performance, supporting modern airport functions.

1.2 Objectives

The primary objective of this project is to design a secure and efficient network infrastructure tailored to the needs of an airport environment.

- **Design a Secure Network Architecture**: Establish a secure network for the Airport Authority to manage flight operations, ensuring that only authorized personnel have access to critical servers.
- **Implement Controlled Access for Flight Service Providers**: Provide Flight Service Providers with restricted access to specific resources within the Airport Authority's network, preventing unauthorized access to other systems.
- **Provide High-Speed Internet for Guests**: Set up a high-speed wireless network with a shared password for guests, allowing easy access while isolating it from the secured networks of the other departments.
- **Enable Automatic IP Allocation**: Configure DHCP for automatic IP assignment across all user groups, streamlining connectivity and network management.
- **Ensure Network Scalability and Performance**: Design the network to support the varying demands of each department, balancing security, accessibility, and performance for an efficient airport network infrastructure.

2. NETWORK DESIGN

2.1 Topology

The network topology primarily follows a hybrid structure, combining features of both star and extended bus topologies to enhance security, facilitate segmented traffic flow, and ensure scalability.
Star Topology: Each switch creates a star topology for its respective department, with all connected PCs and devices within that VLAN linked directly to the switch.

Extended bus Topology: The core router extends this bus layout by connecting all switches through trunk links, allowing each VLAN to maintain its distinct traffic channel but still interconnect for cross-departmental communication.

This hybrid topology is ideal for an airport setup because it promotes both scalability and security while segmenting network traffic based on departmental needs. Each VLAN remains isolated with controlled intercommunication, adhering to airport security protocols and ensuring efficient management of resources across departments.

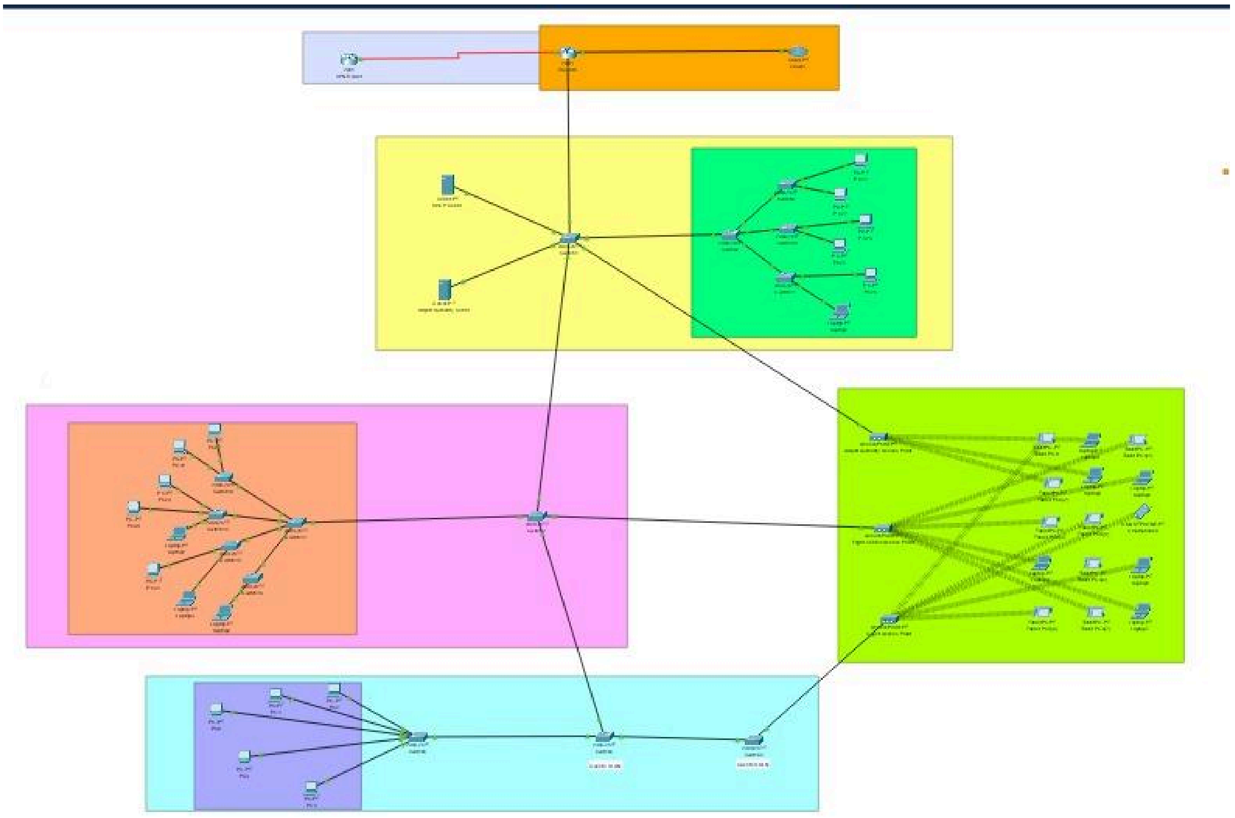


Figure 1: Topology of full networking

2.2 Requirement Analysis of Active Networking Components

Switches:

Switches play a pivotal role in the Airport Project by segmenting and managing different departmental networks, organized into VLANs. We have configured VLANs to logically separate traffic between Airport Authority (VLAN 2), Flight Services (VLAN 3), and Guest users (VLAN 4), ensuring efficient and secure traffic management. These switches allow for controlled inter-VLAN routing through trunk links to the router, enhancing network performance and security by isolating department-specific traffic.

Router:

The router enables inter-VLAN communication and acts as a central node for routing traffic between departments as per configured access control policies. With sub-interfaces configured for each VLAN, the router directs departmental traffic efficiently and applies IP helper addresses to relay DHCP requests to the server. The router also interfaces with external networks, managing NAT for internet access, thus acting as both an internal and external gateway, ensuring secure, managed connectivity.

Access Points:

The wireless access point provides connectivity for guest users, enabling them to access the internet using a shared password. The access point connects to the VLAN assigned to guest users, with DHCP dynamically assigning IP addresses to guest devices. This setup ensures guests have high-speed internet access while isolating them from critical resources of other departments, following the network's security policies.

DHCP Server:

The DHCP server automates IP address assignment across VLANs, crucial for scalability and management of a large number of devices. Configured with separate pools for each VLAN, it allocates IP addresses dynamically to Airport Authority, Flight Services, and Guest VLANs. This server ensures all devices in the network obtain appropriate IP configurations for seamless inter-departmental and internet connectivity, thus facilitating efficient network management.

VPN :

The VPN Router in the network serves as a secure gateway that enables remote access to the airport's internal network. It is responsible for encrypting and routing traffic from authorized remote users, ensuring that sensitive data transmitted between remote locations and the network remains secure. In the context of the Airport Project, the VPN router allows secure access to the

Airport Authority network (VLAN 2) for remote workers or stakeholders, ensuring that only authorized users from specific VLANs can connect. The VPN functionality is crucial for enhancing network security, particularly for users who need to access internal systems remotely without compromising the integrity of the overall network.

2.3 Network Implementation Plan

To organize network segmentation across different departments, VLAN technology will be employed. Each department will be associated with a unique IP network and mapped to a designated VLAN, allowing for efficient network separation and management. Access control lists (ACLs) will be implemented to enforce appropriate restrictions between departments, ensuring security and controlled access.

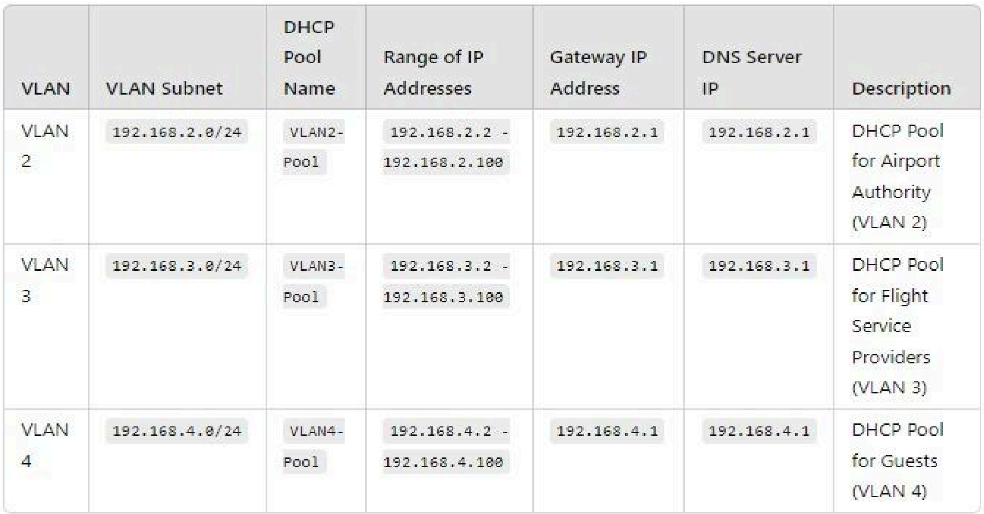
A DHCP server will be utilized to dynamically assign IP addresses to devices on the network, simplifying IP management and reducing manual configuration.

VLAN and IP Network Design:

VLANs will be configured for each department and mapped accordingly:

- VLAN 2 – Assigned to the Airport Authority department.
- VLAN 3 – Assigned to Flight Service Providers.
- VLAN 4 – Reserved for Guest users.

For each VLAN, a specific IP network will be created and mapped to the corresponding VLAN, defining an IP address range suitable for users and devices within each department. This design provides dedicated IP ranges for each VLAN, allowing efficient and controlled communication within departments and across the network where permitted.

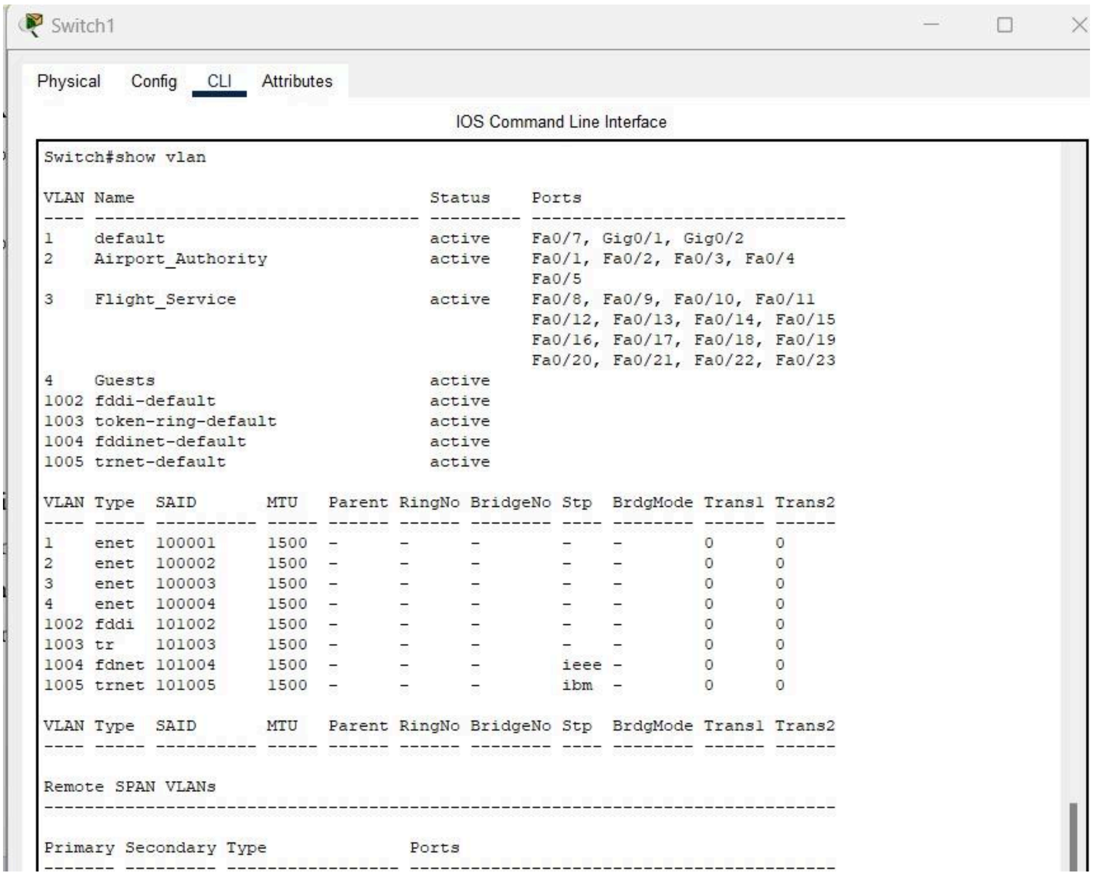


VLAN	VLAN Subnet	DHCP Pool Name	Range of IP Addresses	Gateway IP Address	DNS Server IP	Description
VLAN 2	192.168.2.0/24	VLAN2-Pool	192.168.2.2 - 192.168.2.100	192.168.2.1	192.168.2.1	DHCP Pool for Airport Authority (VLAN 2)
VLAN 3	192.168.3.0/24	VLAN3-Pool	192.168.3.2 - 192.168.3.100	192.168.3.1	192.168.3.1	DHCP Pool for Flight Service Providers (VLAN 3)
VLAN 4	192.168.4.0/24	VLAN4-Pool	192.168.4.2 - 192.168.4.100	192.168.4.1	192.168.4.1	DHCP Pool for Guests (VLAN 4)

Table 1: DHCP VLAN POOL Configuration

Switch ports are configured as members of their respective VLANs, with each department's computers connected to the appropriate VLAN-designated ports on the switches. Inter-VLAN routing is set up on the router to enable controlled communication between VLANs. To enforce security policies, access control lists (ACLs) are applied to restrict inter-departmental communication in alignment with the project requirements.
Access points are connected to switch ports assigned to VLAN 4, which is designated as the guest VLAN, ensuring guest traffic remains isolated. The DHCP server is set up on VLAN 2, the Airport Authority VLAN, and configured with multiple DHCP scopes. These scopes allow the DHCP server to provide IP addresses specific to each VLAN, thereby supporting dynamic IP allocation across departments.

To facilitate DHCP functionality across VLANs, the router is configured with the IP Helper-Address feature. This enables users in the Flight Services Provider VLAN and Guest VLAN to obtain dynamic IP addresses from the DHCP server located within the Airport Authority VLAN. This setup ensures seamless IP address assignment for users across all network segments.



```
Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/7, Gig0/1, Gig0/2
2    Airport_Authority                active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5
3    Flight_Service                   active    Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
4    Guests                           active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
2    enet  100002     1500  -      -      -        -    -        0      0
3    enet  100003     1500  -      -      -        -    -        0      0
4    enet  100004     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------

Remote SPAN VLANs
------------------------------------------------------------------------------

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

Figure 2. VLAN for Switch 1

It shows all the Ports that are configured for the specific VLANs for appropriate Inter-VLAN routing.

2.4 VPN Design and Integration

In this airport network project, the VPN (Virtual Private Network) serves to provide secure, encrypted communication over the network for authorized users, particularly when connecting remotely or accessing sensitive systems within the airport's network infrastructure. The VPN enhances security and ensures data privacy, especially for remote users from the Airport Authority or authorized personnel accessing the flight management controls.

Objectives of VPN Integration:

1. Secure Remote Access: VPN will enable authorized users, such as airport officials and flight service providers, to access the airport's internal network securely from remote locations. This is essential for critical operations, that may need to be accessed offsite.

2. Data Confidentiality and Integrity: By encrypting data traffic, VPN prevents unauthorized access or interception of sensitive information, especially in an environment with shared networks for multiple departments and guests.

3. Network Segmentation and Access Control: The VPN will allow network traffic segregation, limiting access to sensitive areas of the network for external users or other departments.

Design Considerations for VPN Integration

For this setup, the following design choices and network adjustments are implemented to support VPN functionality:

1. Two-Router Approach:

- We use two routers to manage internal and external connections. One router serves the main network, connecting internal VLANs (Airport Authority, Flight Services, and Guests) with different access control policies.
- The second router handles VPN configurations and links to the primary router, allowing external users to connect securely to the internal network.

2. VPN Gateway Configuration:

- The VPN gateway will be configured on the external router, which is directly connected to the internet.

- The gateway authenticates users attempting to connect to the network, ensuring that only authorized users gain access.

3. Tunnel Interface for VPN:

- A tunnel interface is created to establish a secure, encrypted pathway between the external and internal routers.
- This interface ensures that data transmitted over the VPN remains private and secure by encrypting data packets before they leave the internal network.

4. IPSec Encryption:

- IPSec is configured on the VPN tunnel interface to provide encryption and integrity for the data packets.
- IPSec prevents unauthorized access and ensures that any data accessed remotely is secure.

3. NETWORK CONFIGURATION AND GUIDELINES

The IP address of the DHCP Server is 192.168.2.2 and the IP address of the Airport Authority Server is 192.168.2.3. The access point is configured with IP addresses belonging to the VLAN 4 network address range.

3.1 Switch Configuration:

The following configuration details the actual setup which needs to be performed on a Cisco switch.

a. Create VLAN's, VLAN 2, VLAN 3 AND VLAN 4 with respective names on the switch.

```
switch(config)#vlan 2
switch(config-vlan)#name Airport_Authority
switch(config-vlan)#exit
switch(config)#vlan 3
switch(config-vlan)#name Flight_Service
switch(config-vlan)#exit
switch(config)#vlan 4
switch(config-vlan)#name Guests
switch(config-vlan)#exit
```

b. Configure appropriate ports on the switch as members of respective VLAN. Only two ports for each vlans are displayed. This can be added based on requirement.

```
 switch(config)#interface fastethernet 0/2
switch(config-if)#switchport mode access
if)#switchport access vlan 2
switch(config
switch(config-if)#exit
switch(config)#interface fastethernet 0/3
switch(config-if)#switchport mode access
if)#switchport access vlan 2
switch(config
switch(config-if)#exit
switch(config)#interface fastethernet 0/10
switch(config-if)#switchport mode access
```

```
if)#switchport access vlan 3
switch(config-if)#exit
switch(config)#interface fastethernet 0/11
switch(config-if)#switchport mode access
if)#switchport access vlan 3
switch(config-if)#exit
switch(config)#interface fastethernet 0/20   switch(conf ig-if)#switchport mode access
switch(config if)#switchport access vlan 4 switch(config-if)#exit
switch(config)#interface fastethernet 0/21
switch(config-if)#switchport mode access
if)#switchport access vlan 4
switch(config-if)#exit
```

c. Configure the port connected to the router (Port 1) as a trunk.

This is for allowing the traffic from all the vlans to the router, where appropriate routing and access restrictions are performed.

```
switch(config)#interface fastethernet 0/1  switch(config-if)#switchport mode trunk
 switch(config-if)#switchport trunk allowed vlan all
switch(config-if)#exit
```

3.2 Router Configuration:

The following configuration details the actual setup which needs to be performed on a Cisco router.

a. Sub interfaces on the router on the physical interface fastethernet 0/0 are mapped with appropriate VLAN and IP address. The IP address configured on the router, would be the default gateway address for users belonging to the respective vlan. IP addresses 192.168.2.1, 192.168.3.1 and 192.168.4.1 are mapped with the VLAN's, VLAN 2,3,4.

```
router(config)#interface fastethernet 0/0.1
router(conf ig-subif)#encapsulation dot1Q 2
router(config-subif)#ip address 192.168.2.1 255.255.255.0
router(config-subif)#no shutdown
router(config-subif)#exit
router(config)#interface fastethernet 0/0.2
router(config-subif)#encapsulation dot1Q 3
subif)#ip address 192.168.3.1 255.255.255.0
subif)#no shutdown
```

```
router(config-subif)#exit
router(config)#interface fastethernet 0/0.3
router(config-subif)#encapsulation dot1Q 4
subif)#ip address 192.168.4.1 255.255.255.0
subif)#no shutdown
router(config-subif)#exit
```

b. The IP Helper –address is configured on the VLAN 3 and VLAN 4 interfaces of the router. This is configured for users belonging to the respective vlans, to reach the DHCP server for obtaining dynamic IP addresses. The configurations are shown below. The IP address of the DHCP server is 192.168.2.2.

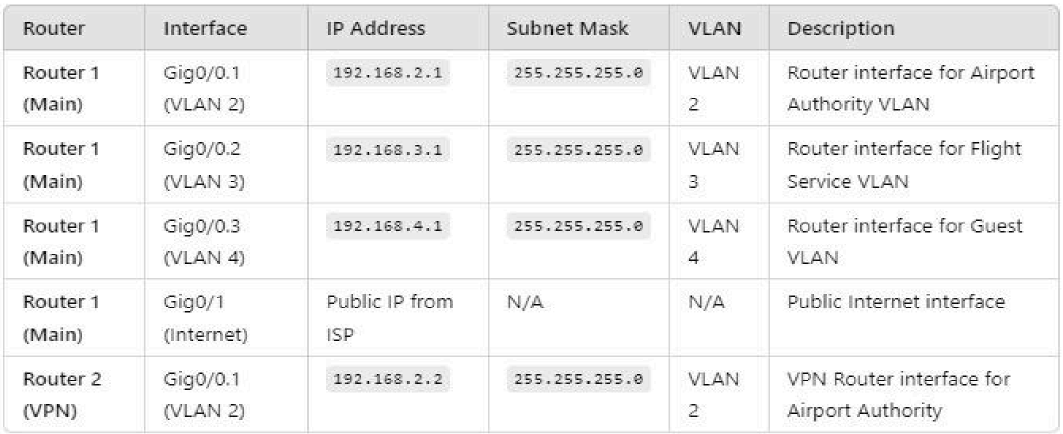
```
router(config)#interface fastethernet 0/0.2
router(config subif)#ip helper-address 192.168.2.2   router(config-subif)#exit
router(config)#interface fastethernet 0/0.3
router(config subif)#ip helper-address 192.168.2.2   router(config-subif)#exit
```

c. Appropriate access control lists are configured on the router. To deny access from the guest network to the other two networks an extended ACL is configured. The configuration is shown below. The first two lines would deny the access from the guest network to the airport authority and flight service provider networks. The third entry would allow all other traffic. This is for the internet connection. The access control list is applied in the guest vlan interface on the router as inbound.

```
router(config)#access-list 101 deny ip 192.168.4.0 0.0.0.255
192.168.2.0  0.0.0.255
router(config)#access-list 101 deny ip 192.168.4.0 0.0.0.255
192.168.3.0 0.0.0.255
router(config)#access-list 101 permit ip any any
router(config)#interface fastethernet 0/0.3
subif)#ip access-group 101 inbound
router(config subif)#ip access-group 101 inbound
```

d. Access control lists are configured to restrict access from the flight service network to the airport authority network. The first line allows the flight service provider network to access the airport authority server. The second line denies all other communication to the airport authority network as per the requirement. The third line allows all other communication, which would be the internet. The access list is applied as inbound on the VLAN interface corresponding to the airport authority network. router(config)#access-list 102 permit ip 192.168.3.0 0.0.0.255 host 192.168.2.3

```
router(config)#access-list 102 deny ip 192.168.3.0 0.0.0.255
192.168.2.0 0.0.0.255
router(config)#access-list 101 permit ip any any
router(config)#interface fastethernet 0/0.2
subif)#ip access-group 102 inbound
```



Router	Interface	IP Address	Subnet Mask	VLAN	Description
Router 1 (Main)	Gig0/0.1 (VLAN 2)	192.168.2.1	255.255.255.0	VLAN 2	Router interface for Airport Authority VLAN
Router 1 (Main)	Gig0/0.2 (VLAN 3)	192.168.3.1	255.255.255.0	VLAN 3	Router interface for Flight Service VLAN
Router 1 (Main)	Gig0/0.3 (VLAN 4)	192.168.4.1	255.255.255.0	VLAN 4	Router interface for Guest VLAN
Router 1 (Main)	Gig0/1 (Internet)	Public IP from ISP	N/A	N/A	Public Internet interface
Router 2 (VPN)	Gig0/0.1 (VLAN 2)	192.168.2.2	255.255.255.0	VLAN 2	VPN Router interface for Airport Authority

Table 2: Router Configuration

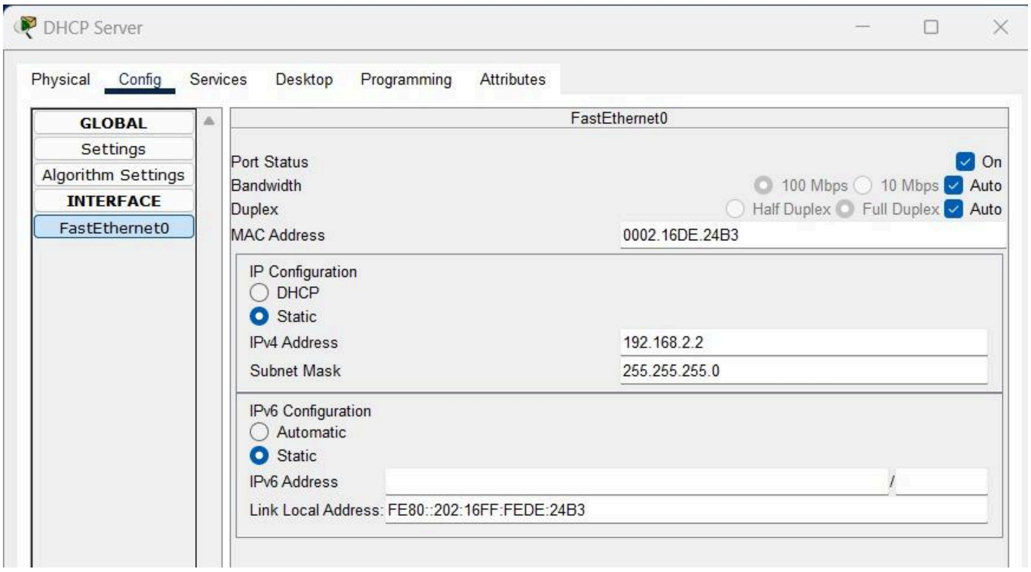
The Router Configuration table outlines the IP addressing and subinterface configuration for each VLAN on the router. It ensures that each VLAN has a proper gateway for devices in that VLAN, enabling inter-VLAN communication and proper routing between the Airport Authority, Flight Service, and Guest networks.

3.3 DHCP Configuration

Three separate DHCP scopes are created, each corresponding to one of the three VLANs. The DHCP server is configured to allocate IP addresses for the Airport Authority, Flight Services, and Guest VLANs, with each scope tailored to meet the specific needs of the respective VLAN.

- The DHCP scope for the Airport Authority VLAN allocates IP addresses to 20 users.
- The Flight Services VLAN DHCP scope provides IP addresses to 40 users.
- The Guest VLAN DHCP scope assigns IP addresses to 100 users.

The DHCP server is responsible for managing these IP pools, ensuring that the correct number of IP addresses is dynamically assigned to users within each VLAN, based on their network segment. The corresponding screenshots below illustrate the setup of these DHCP scopes.



FastEthernet0

Port Status ☑ On

Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address 0002.16DE.24B3

IP Configuration

○ DHCP

● Static

IPv4 Address 192.168.2.2

Subnet Mask 255.255.255.0

IPv6 Configuration

○ Automatic

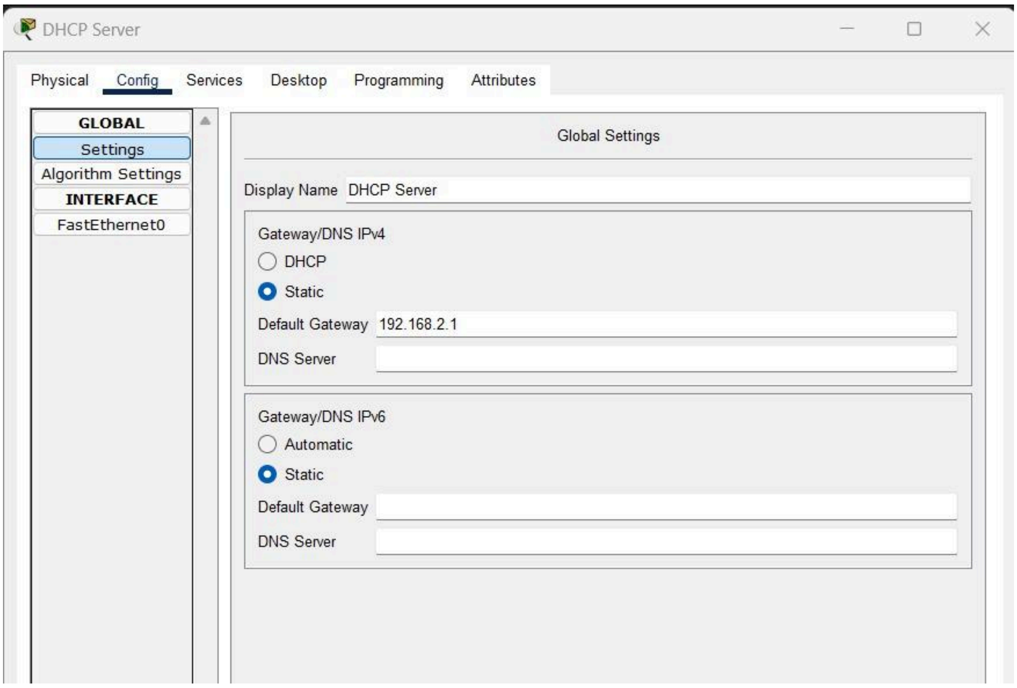
● Static

IPv6 Address /

Link Local Address: FE80::202:16FF:FEDE:24B3

Figure 3. DHCP IP Addressing

Figure 3 shows the IP configuration of the DHCP Server, connected within VLAN-2 (Airport Authority). This is needed for the router to forward all DHCP requests properly.



Global Settings

Display Name DHCP Server

Gateway/DNS IPv4

○ DHCP

● Static

Default Gateway 192.168.2.1

DNS Server

Gateway/DNS IPv6

○ Automatic

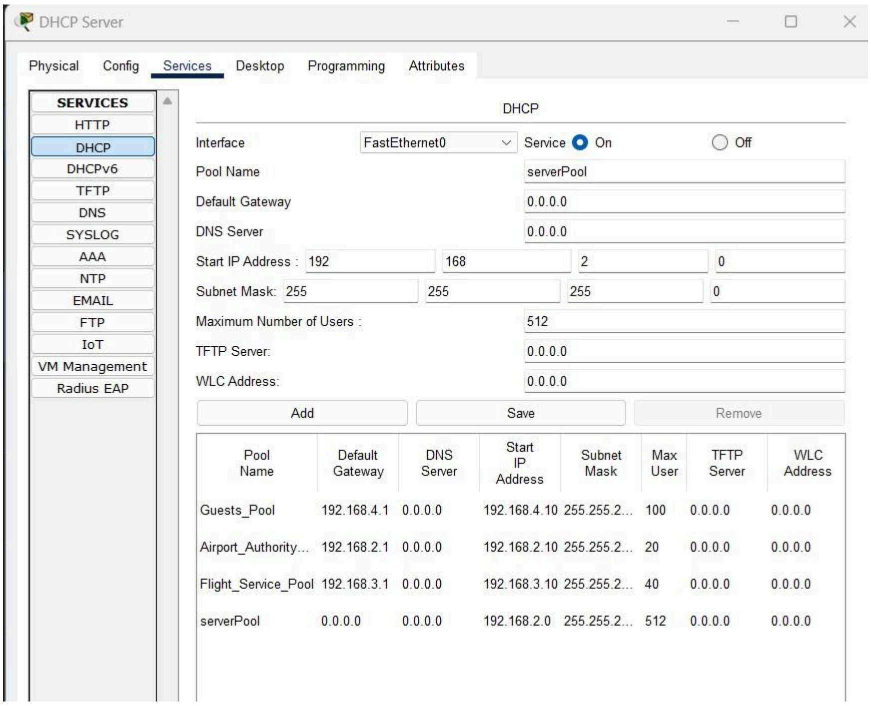
● Static

Default Gateway

DNS Server

Figure 4. DHCP Server Pool

DHCP Server Pool displays the DHCP server's address pool configuration, detailing the allocation of IP address ranges for the users in each VLAN (Airport Authority, Flight Services, and Guest).



DHCP

Interface: FastEthernet0 — Service ● On ○ Off

Pool Name: serverPool

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

Start IP Address : 192 168 2 0

Subnet Mask: 255 255 255 0

Maximum Number of Users : 512

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
Guests_Pool	192.168.4.1	0.0.0.0	192.168.4.10	255.255.2...	100	0.0.0.0	0.0.0.0
Airport_Authority...	192.168.2.1	0.0.0.0	192.168.2.10	255.255.2...	20	0.0.0.0	0.0.0.0
Flight_Service_Pool	192.168.3.1	0.0.0.0	192.168.3.10	255.255.2...	40	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	192.168.2.0	255.255.2...	512	0.0.0.0	0.0.0.0

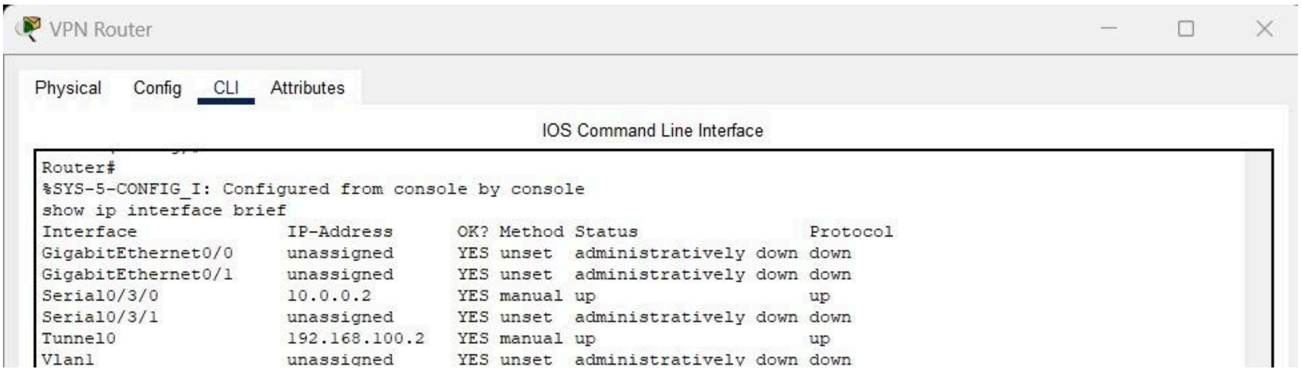
Figure 5. DHCP Gateway

The above image illustrates the DHCP gateway configuration, where the default gateway addresses are assigned to devices in each VLAN, enabling communication with other network segments and external resources.

3.4 VPN CONFIGURATION

1. Configure the VPN Router as a Gateway:

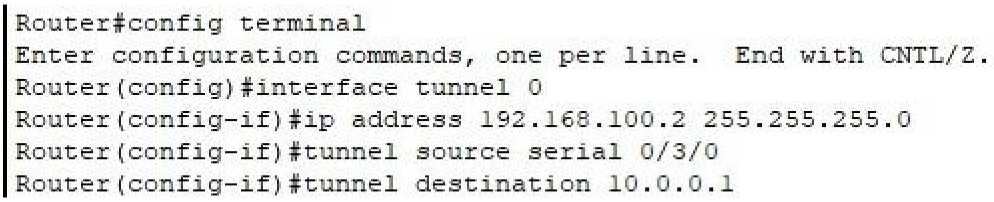
- Set up the VPN router to act as the entry point for remote connections.
- Configure a public facing IP address on the VPN router's external interface to accept VPN connections.



```
Router#
%SYS-5-CONFIG_I: Configured from console by console
show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  administratively down down
GigabitEthernet0/1     unassigned      YES unset  administratively down down
Serial0/3/0            10.0.0.2        YES manual up                    up
Serial0/3/1            unassigned      YES unset  administratively down down
Tunnel0                192.168.100.2   YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
```

2. Create VPN Tunnel:

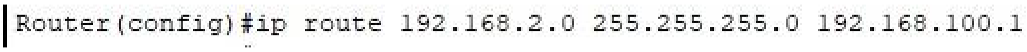
- Define a tunnel interface on the VPN router.
- Assign an IP address and enable IPSec encryption on this interface.
- Set up the corresponding tunnel interface on the internal router for traffic forwarding.



```
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface tunnel 0
Router(config-if)#ip address 192.168.100.2 255.255.255.0
Router(config-if)#tunnel source serial 0/3/0
Router(config-if)#tunnel destination 10.0.0.1
```

3. Configure Access Lists:

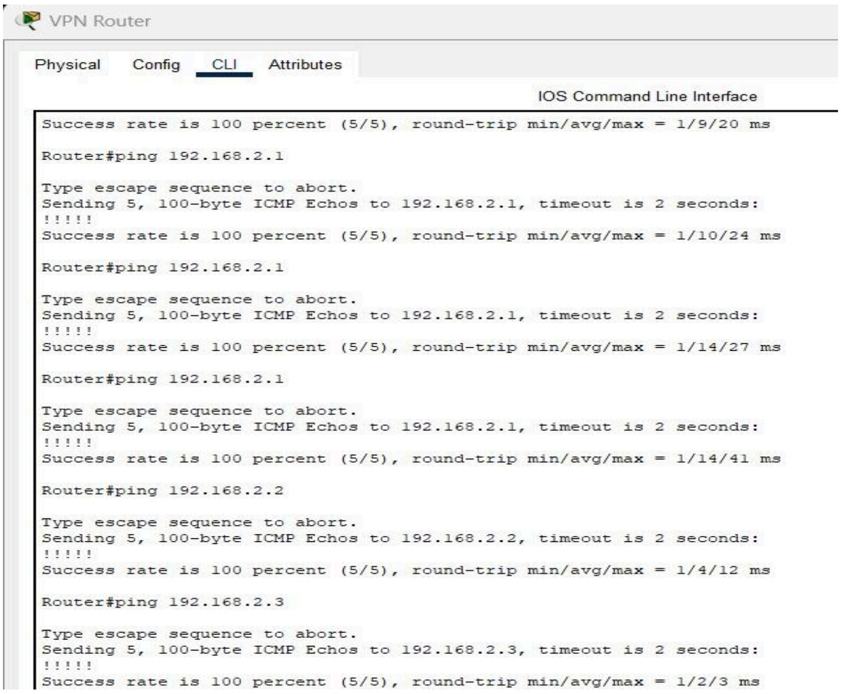
- Establish ACLs (Access Control Lists) on both the VPN and internal routers to restrict the network areas that can be accessed by VPN users.
- Implement rules to ensure that VPN users only access the flight management systems or other essential resources, following the project requirements.



```
Router(config)#ip route 192.168.2.0 255.255.255.0 192.168.100.1
```

4. Testing and Validation:

- Test the VPN connection to ensure remote users can connect securely to the VPN gateway.
- Verify that authenticated users can access the Airport Authority network or specific resources while being restricted from other areas, such as the Guest network or unrelated systems.



```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/9/20 ms

Router#ping 192.168.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/10/24 ms

Router#ping 192.168.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/14/27 ms

Router#ping 192.168.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/14/41 ms

Router#ping 192.168.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/12 ms

Router#ping 192.168.2.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/3 ms
```

4. SECURITY MEASURES

IEEE 802.1Q encapsulation has been implemented on the network switches as a means of enhancing security and managing traffic effectively. This method tags VLAN traffic on trunk links, enabling the separation and isolation of data based on VLAN identifiers. By doing so, it ensures that traffic is confined to its assigned VLAN, preventing unauthorized access across different network segments and reducing the risk of broadcast storms affecting the entire network.

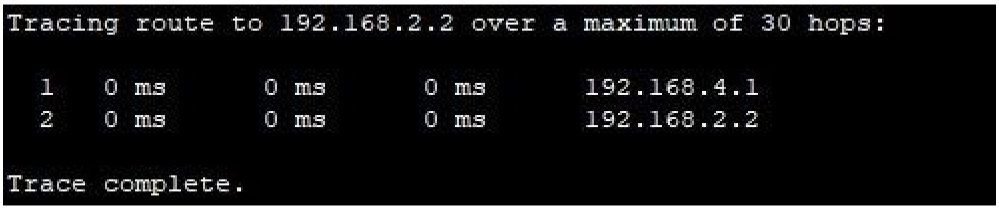
Beyond traffic segmentation, 802.1Q encapsulation also aids in enforcing network policies at the switch level. It allows network administrators to control access and strengthen security measures. Isolating traffic within each VLAN ensures that any potential security threats are contained within the affected VLAN, minimizing their impact on the broader network. This configuration is particularly beneficial in a campus network environment, where multiple departments or buildings require secure and controlled access to shared resources.

5. TESTING AND VALIDATION

5.1 Simulation

Packet Tracer was utilized to simulate and test the designed network. Packet Tracer is a network simulation tool that provides a virtual environment for designing, configuring, and testing network scenarios. The simulation process involves:

- **Network Topology Design:** The network topology, including routers, switches, PCs, servers, and other devices, was designed within Packet Tracer based on the specified requirements.
- **Configuration Implementation:** Using the designed topology, configurations were implemented on routers, switches, and other network devices according to the provided guidelines. Cisco Packet Tracer allows users to configure devices with a user-friendly interface similar to actual Cisco devices.
- **Traffic Simulation:** Packet Tracer allows the simulation of network traffic and communication between devices. This involves generating traffic, testing connectivity, and ensuring that data flows as expected.
- **Verification of Redundancy and Failover:** The hierarchical design with redundancy at every layer, including multiple routers, multilayer switches, and ISP connections, was tested to verify failover mechanisms and ensure network resilience.



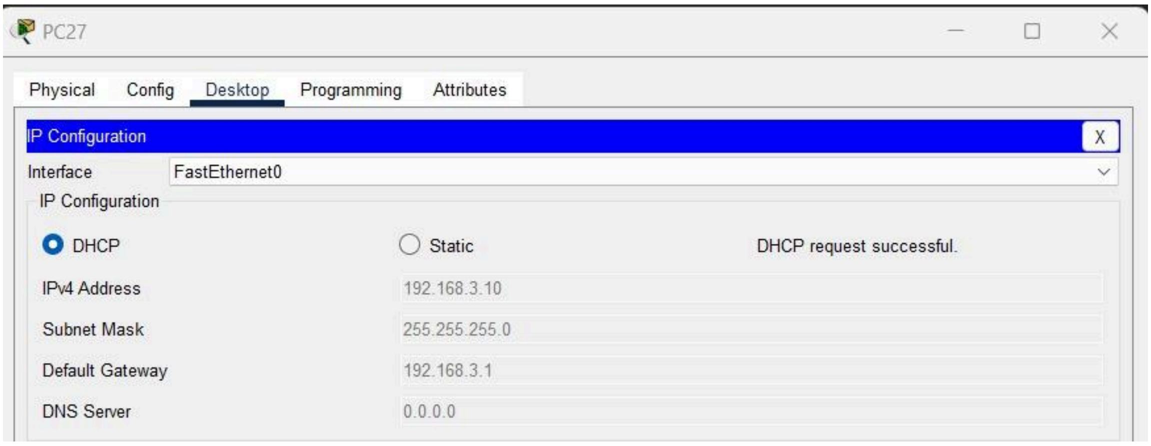
```
Tracing route to 192.168.2.2 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      192.168.4.1
  2   0 ms      0 ms      0 ms      192.168.2.2

Trace complete.
```

Figure 6. traceroute successful

- DHCP and IP Address Allocation: Dynamic Host Configuration Protocol (DHCP) functionality and IP address allocation were tested to ensure that devices received the correct IP addresses dynamically and that devices in the server room had static IP assignments.



Interface: FastEthernet0

IP Configuration

● DHCP ○ Static DHCP request successful.

IPv4 Address 192.168.3.10

Subnet Mask 255.255.255.0

Default Gateway 192.168.3.1

DNS Server 0.0.0.0

Figure 7. DHCP IP allocation

5.2 Troubleshooting

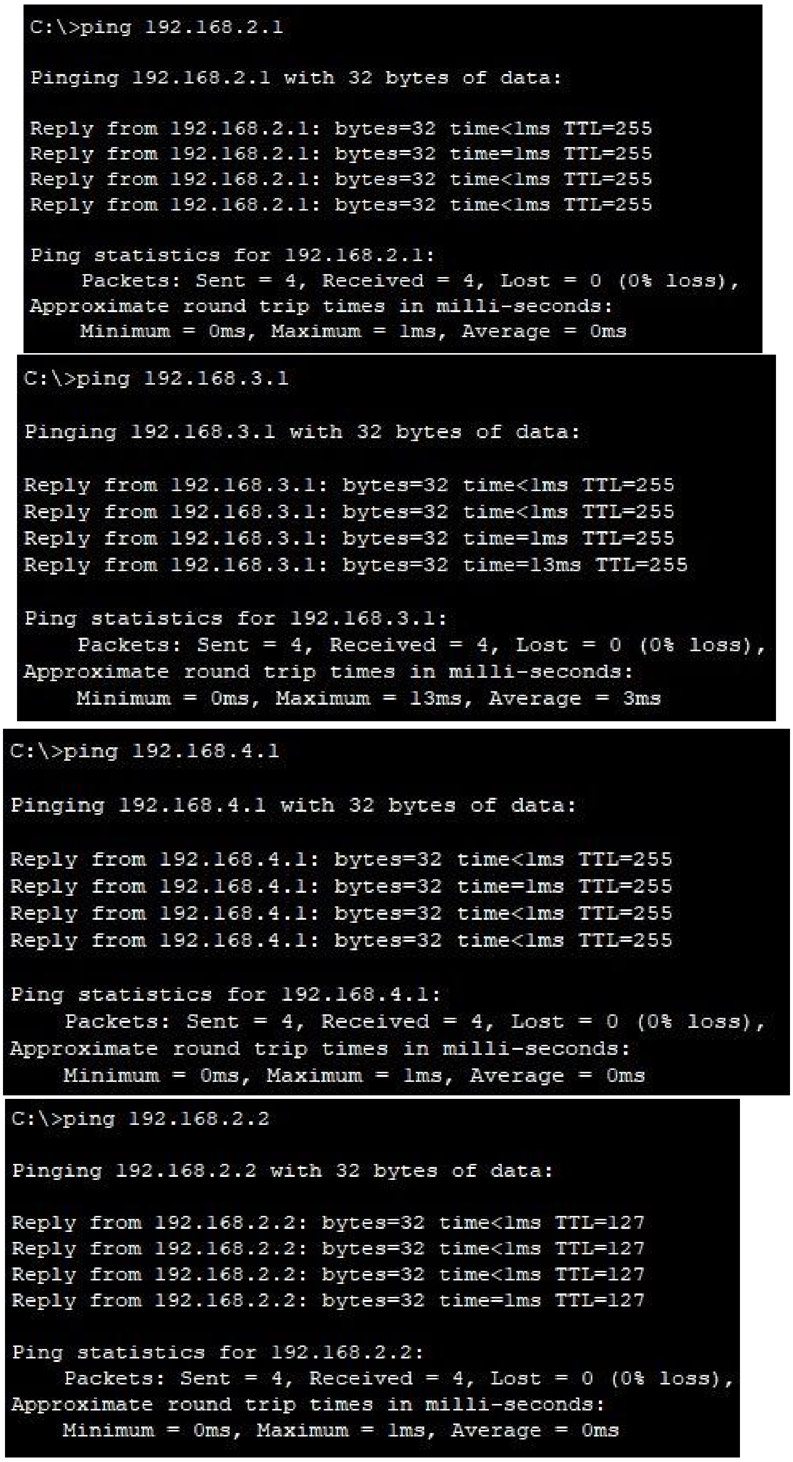
During the testing phase, several common troubleshooting steps were taken to address issues:

- Device Connectivity: Ensured that all devices could communicate within their respective VLANs and across different departments. Verified inter-VLAN routing configurations on multilayer switches.
- DHCP Issues: Investigated and resolved any DHCP-related issues, ensuring that DHCP servers were reachable and capable of assigning IP addresses to devices dynamically.
- Routing Configuration: Verified the Open Shortest Path First (OSPF) routing configurations on routers and multilayer switches, ensuring proper routing table updates and communication between different departments.
- Access Control Issues: Reviewed and adjusted Access Control Lists (ACLs) to allow necessary traffic and deny unauthorized access.
- Port Security: Verified the configuration of port security on the Finance department's switchports to ensure that only one device could connect per port and that MAC addresses were correctly learned.

6. RESULTS AND EVALUATION

6.1 Performance Metrics

Performance metrics, including network latency, throughput, redundancy testing, DHCP response time, security, QoS, and NAT/PAT functionality, were measured during testing to ensure optimal network operation.



```
C:\>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time<1ms TTL=255
Reply from 192.168.2.1: bytes=32 time=1ms TTL=255
Reply from 192.168.2.1: bytes=32 time<1ms TTL=255
Reply from 192.168.2.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

```
C:\>ping 192.168.3.1

Pinging 192.168.3.1 with 32 bytes of data:

Reply from 192.168.3.1: bytes=32 time<1ms TTL=255
Reply from 192.168.3.1: bytes=32 time<1ms TTL=255
Reply from 192.168.3.1: bytes=32 time=1ms TTL=255
Reply from 192.168.3.1: bytes=32 time=13ms TTL=255

Ping statistics for 192.168.3.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 13ms, Average = 3ms
```

```
C:\>ping 192.168.4.1

Pinging 192.168.4.1 with 32 bytes of data:

Reply from 192.168.4.1: bytes=32 time<1ms TTL=255
Reply from 192.168.4.1: bytes=32 time=1ms TTL=255
Reply from 192.168.4.1: bytes=32 time<1ms TTL=255
Reply from 192.168.4.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.4.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

```
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time<1ms TTL=127
Reply from 192.168.2.2: bytes=32 time<1ms TTL=127
Reply from 192.168.2.2: bytes=32 time<1ms TTL=127
Reply from 192.168.2.2: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Figure 8: performance measure through ping time

7. CONCLUSION

7.1 Summary

The proposed network design for the airport achieves a secure, scalable, and efficient infrastructure tailored to the needs of a high-security environment. By utilizing a hybrid topology combining star and extended star layouts, the network ensures both isolated and interconnected departmental traffic flow, essential for managing airport operations. VLAN segmentation across the Airport Authority, Flight Service Providers, and Guests provides clear separation and control, with each department assigned a unique IP range to maintain security and network management simplicity. Access Control Lists (ACLs) further reinforce security by controlling interdepartmental communication, adhering to strict airport protocols.Automatic IP assignment through a centralized DHCP server simplifies network configuration, allowing devices to connect effortlessly across all departments. The combination of a dedicated VLAN and IP network for each department enhances security while supporting easy management and scalability. This network design meets current needs and supports future growth, ensuring reliable performance, data security, and high-speed connectivity.

7.2 Lessons Learned

This project underscored key principles for designing secure, efficient networks in high-security environments:

1. **Importance of Network Segmentation:** VLANs and ACLs are crucial for securing and isolating departmental traffic, allowing each department to operate independently while preventing unauthorized access.
2. **Scalable and Flexible Topology:** The hybrid star and extended star topology provided an adaptable framework, ensuring the network could grow with the airport's needs without disruption.
3. **Efficient IP Management with DHCP:** Automating IP assignment through DHCP simplifies management and minimizes manual errors, especially in high-traffic areas like guest networks.
4. **Balancing Security and Accessibility:** Creating a secure network for internal operations while allowing guest access highlighted the need to balance robust security with user convenience.
5. **Future-Proof Design:** Structuring the network with scalability in mind ensures it can meet current demands and adapt to future requirements, avoiding costly redesigns.

8. REFERENCES

- Cisco Systems, Inc. (2020). Cisco Networking Basics: A Comprehensive Guide to Networking Fundamentals. Cisco Press.
- Tan, K. (2021). Network Design and Implementation: A Guide to Best Practices. Wiley & Sons.
- Cisco Systems, Inc. (2019). Configuring VLANs and Inter-VLAN Routing in Cisco Packet Tracer. Cisco Networking Academy.
- Cisco Systems, Inc. (2022). Configuring DHCP on Cisco Routers and Switches. Cisco Documentation. Retrieved from: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/xe-3s/iad-xe-3s-book/
- Baker, P. (2018). Designing Enterprise Networks: Principles and Best Practices. Pearson Education.
- Cai, D., & Li, Y. (2020). Implementing Secure Network Infrastructure: A Practical Guide to Security Protocols and Strategies. Springer.

- Cisco Systems, Inc. (2022). Configuring DHCP on Cisco Routers and Switches. Cisco Documentation. Retrieved from: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/xe-3s/iad-xe-3s-book/

- Hughes, C., & Stepanek, M. (2019). Understanding and Implementing Network Security Solutions. McGraw-Hill Education.

APPENDICES

Abbreviations:

DHCP - Dynamic Host Configuration Protocol

IP - Internet Protocol

VLAN - Virtual Local Area Network

VPN - Virtual Private Network