

NETWORK DESIGNING FOR A AIRPORT

A COURSE PROJECT REPORT

By

Saswata Lahiri (RA1911027010001)

P.Adithya (RA1911027010003)

Avinash reddy Vasipalli (RA1911027010007)

Aagam Shah (RA1911027010015)

Under the guidance of

**Dr. E.Sasikala, Associate Professor,
Data Science and Business System**

In partial fulfilment for the Course

of

18CSC302J - COMPUTER NETWORKS

in

Department Name



FACULTY OF ENGINEERING AND TECHNOLOGY

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

Kattankulathur, Chenpalattu District

NOVEMBER 2021

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

(Under Section 3 of UGC Act, 1956)

BONAFIDE CERTIFICATE

Certified that this project report " **Network design proposal for airport**"

is the bonafide work of *Saswata Lahiri* (RA1911027010001)

P.Adithya (RA1911027010003)

Avinash reddy Vasipalli (RA1911027010007)

Aagam Shah (RA1911027010015)

who carried out the project work under my supervision

SIGNATURE

Dr.E. Sasikala,
Course Coordinator
Associate Professor,
Data Science and Business Systems
SRM Institute of Science and Technology
Potheri, SRM Nagar, Kattankulathur,
Tamil Nadu 603203

TABLE OF CONTENTS

<u>CHAPTERS</u>	<u>CONTENTS PAGE NO</u>
1) <i>ABSTRACT</i>	4
2) <i>INTRODUCTION</i>	5
3) <i>PROBLEM STATEMENT</i>	6
4) <i>REQUIREMENT ANALYSIS</i>	7
4.1 <i>Objective</i>	
4.2 <i>Networking Requirements</i>	
4.3 <i>Requirement analysis of active networking component</i>	
5) <i>Network Topology</i>	9
5.1 <i>Network Design statutory</i>	
5.2 <i>WHY VLAN?</i>	
5.3 <i>VLAN and IP address Design</i>	
6) <i>IMPLEMENTATION</i>	11
7) <i>EXPERIMENT RESULTS & ANALYSIS</i>	16
8.1 <i>RESULTS</i>	
8.2 <i>RESULT ANALYSIS</i>	
8.3 <i>CONCLUSION & FUTURE WORK</i>	
8) <i>Hardware and Software inventory list</i>	19
9) <i>REFERENCES</i>	20

1.ABSTRACT

The aim of this project was airports network design and implementation and the introduction of a suitable network for most airports around the world. The following project focused on three main parts: security, quality, and safety.

The project has been provided with different utilities to introduce a network with a high security level for the airport. These utilities are hardware firewalls, an IP access control list, Mac address port security, a domain server and s proxy server. All of these utilities have been configured to provide a secure environment for the entire network and to prevent hackers from entering sensitive departments like the flight management and service providers departments

The project is design to secure the network from the following threats:

- Unauthorized access devices.
- Unencrypted or plaintext information.
- DHCP Snooping.
- Internal Access

Improving the performance of any network requires a high quality of techniques and services which help to improve the general task of the network. The technical services that have been placed in the airport's network are failover firewalls utility a Dynamic Host Configuration Protocol (DHCP) server, a Domain Name System (DNS) server and a cabling system. These tools can increase the performance of the network in general and provide a stable internet service for the Air Traffic Control System by using dual internet service providers and the failover utility.

2.INTRODUCTION

Airports are the sensitive places around the world. Network Security plays a major role on computer network, especially in where high quality of services are required. Modern technology takes edge over the primitive ones where lot of energy, resources and time were wasted.

Technology plays many different roles to protect and represent a high quality of services for these places. Computer networking is the most crucial part of modern airports because this new technology takes the most important responsibilities, rather than people doing the tasks as in previous decades. We installed and configure the network devices such as switches, routers, computers, IP Phones, & APs. We made topology and created IP address with minimum wastage of IP addresses.

This project also consists of hardware-based firewalls, an IP access control list, MAC address control, a domain server and a proxy server are the tools that applied to prevent the hackers accessing the flight management department, which is the important department for any airport.

The network is designed to be scalable based upon requirements because scalability has been the most important consideration during the planning phase. Further security appliances such as IPS, IDS, NGFW etc. can be added to improve security and make the network bullet proof.

3.PROJECT STATEMENT

The project is to design a proposal for setting up a network in an airport.

The airport has three departments.

1. Airport authority
2. Flight service providers
3. Guests.

The airport authority maintains a server which handles the flight management controls. The flight service providers should have access only to the specific server in the airport authority network and not to any other systems. The guest users should have wireless access to a high-speed internet connection, which should be shared among all the users in all the departments.

The wireless access should be using a common password. The guest users should not have access to the other two departments. The users should obtain IP addresses automatically. The airport authority has 20 users, the flight service providers have 40 users and the maximum numbers of guests are estimated to be 100.

Report Contents

1. Introduction
2. Networking Requirement
3. Network Design strategy
4. VLAN and IP Network Design
5. Requirement analysis of active networking components (Routers, switches, access points, DHCP Server)
6. Network implementation plan
7. Network Topology Diagram
8. Network Configuration and guidelines
 - a. Switch configuration (VLAN, Trunking)
 - b. Router configuration (VLAN sub interface, Access lists)
 - c. DHCP configuration (Scope creation with screen shot)
 - d. Access point, server configuration guidelines.
9. Hardware inventory list.

4. REQUIREMENT ANALYSIS

4.1 Objectives-

- The project goals and objectives include:
- To Build a highly resilient Network used in large airports and used by large uses per year.
- To Build a high throughput network
- To Provide a high security level for the airport's network
- To Provide a high quality of service for the airport's network
- To Prevent accidental damage to the network's private data, its users, or their devices
- To Maintain users' details in a secure way
- To Support the FMS (flight management system)

4.2 Networking Requirement

- The active networking components (Routers, switches, wireless access points etc.) with quantity.
- The IP network design for each department.
- Creating and mapping IP networks with vlans.
- Analysis, identification and explanation of methodologies to use for access restriction and internet sharing.
- Dynamic IP addressing design for all the networks.
- Identify the configuration and features, wherever appropriate, which is required on the active components to setup the network.
- Network topology diagram

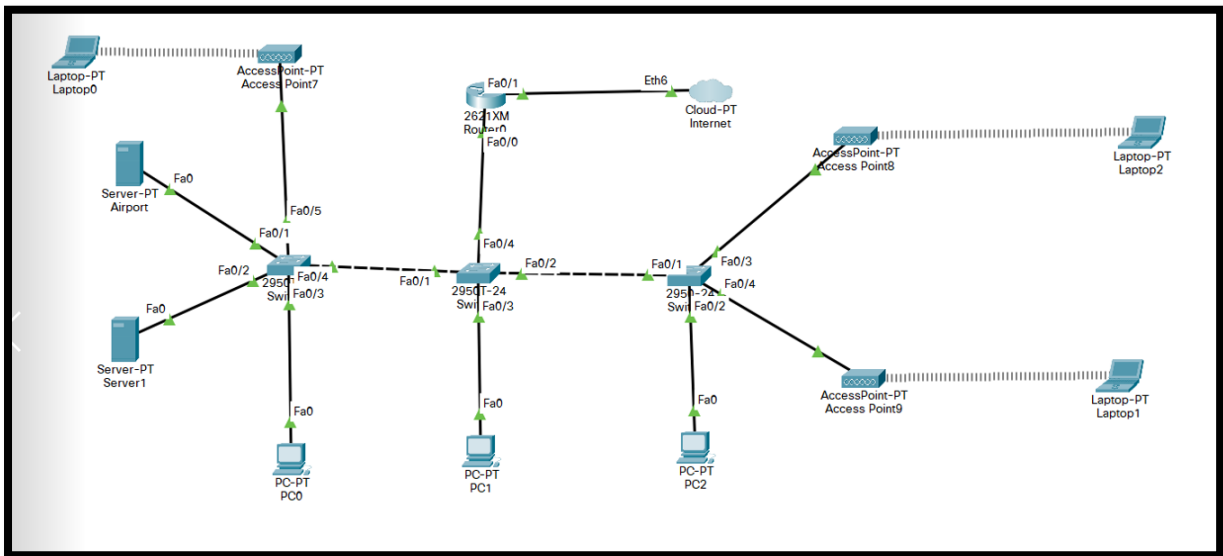
4.3 Requirement analysis of Active Networking Component

- **Switches** – The airport authority has 20 users; the flight service providers have 40 users and the maximum numbers of guests are estimated to be 100. The total number of LAN users is 60, which includes the airport authority and flight service providers. As the guests are on the wireless networks, 3 access points are proposed for accommodating the 100 users. This would require 60 ports for the LAN users, 3 ports for the access points, 1 port for the airport authority server and 1 port for the DHCP server. So, a total of 65 ports are required. Switches are available as 24 or 48 port capacity. So, 3 nos of 24 port switches, which support vlans are proposed.
- **Routers** – A router which supports high speed internet connection, with the appropriate interface is required. The router also requires an interface which supports 802.1q, which would be used for routing between vlans and access restriction between the vlans. 1 no's router is required.
- **Access points** – As the estimated number of guest users are 100, a total of 3 access points is proposed. This is proposed based on the load which can be shared on the access points.
- **DHCP Server** – A DHCP server is required for assigning dynamic IP addresses to users on the network. The DHCP server service on

Required Configuration

- Routers, Switches and firewall will have to be configured with at least the following technologies:
 - 1. IP addresses, Basic Security
 - 2. DHCP
 - 3. Routing protocol preferably EIGRP
 - 4. NAT (Network Address Translation)
 - 5. ACL (Access Control Lists)

5. Network Topology



The network topology diagram is as shown above. The DHCP server and the airport authority server are connected to ports on the switch, which are members of VLAN 2, the airport authority VLAN. The respective PC's belonging to the departments are connected to the appropriate ports on the switch. The access points are connected to ports on the switches, which are members of VLAN 4, which is associated with the guest VLAN. The guest users connect to the access points and are assigned IP address in the appropriate VLAN range.

5.1 Network Design strategy

VLAN (virtual local area network) is also known as a virtual LAN. This technology can logically partition and isolate one or more physical LANs into multiple broadcast domains. VLANs allow network administrators to automatically limit access to a specified group of users by dividing workstations into different isolated LAN segments.

VLAN technology would be used to create the networks associated with different departments. Every department would be associated with an IP network and mapped with a specific vlan. Appropriate restrictions would

be provided between the departments using access control lists. A DHCP server would use for providing dynamic IP addresses to the users on the network.

5.2 WHY VLAN?

A Virtual LAN can priorities data, separate private and public networks, or secure specific devices. Administrators can keep data from merging over into the voice traffic lane. Prioritizing using VLANs helps maintain the quality-of-service users expect. Another common use of VLANs is separating private and public networks.

- help with network efficiency by reducing extraneous traffic
- enhance security by creating a virtual boundary around that business unit
- improve bandwidth performance by limiting node-to-node and broadcast traffic
- save workplace disruption, as there is no need to physically match up ports and switches on a network.

5.3 VLAN and IP Network Design

VLAN's are created and mapped with each department.

1. VLAN 2 – Airport Authority
2. VLAN 3 – Flight Service Provider
3. VLAN 4 – Guests

IP networks are created for each VLAN and mapped with the same. The IP address range for users and systems which can be used on the specific department is also included.

VLAN	IP Network Address	IP Address range
VLAN 2	192.168.2.0/24	192.168.2.2-192.168.2.21
VLAN 3	192.168.3.0/24	192.168.3.2-192.168.3.41
VLAN 4	192.168.4.0/24	192.168.4.2-192.168.4.101

6. IMPLEMENTATION

1. The DHCP server is connected to port, which is a member of VLAN 2
The IP address of DHCP server of Flight server authority is 192.168.3.2
and IP address of airport authority server is 192.168.2.2
2. Access points are configured with IP address belonging to the VLAN 4 network address range.

3. Switch Configuration

Detailed configuration details on the switches in cisco switch is required.

- a. Create the VLAN's lines namely VLAN 2, VLAN 3, and VLAN 4 with respect to 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 providers
switch(config-vlan)#exit
```

```
switch(config)#vlan 4
switch(config-vlan)#name Guests
switch(config-vlan)#exit
```

- b. Now let's configure appropriate ports on the switch as members of respective VLAN. Only two ports for each vlans are displayed and that can be added based on requirement.

```
switch(config)#interface fa 0/2
switch(config-if)#switchport mode access
switch(config-if)#switchport access vlan 2
```

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

```
switch(config)#interface fa 0/4
switch(config-if)#switchport mode access
switch(config-if)#switchport access vlan 2
```

and config the other Fa interface to VLAN 2 as shown above from switch 0
Similarly for Switch 1 and 2 configuration is made with Vlan 3 and 4 respectively

For Switch 1

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

For all the Fa interface to VLAN 3 as shown above.

For Switch 2

```
switch(config)#interface fa 0/1
switch(config-if)#switchport mode access
switch(config-if)#switchport access vlan 4
```

For all the Fa interface to VLAN 4 as shown above.

- c. Configure the port connected to the router as trunk. This enables in allowing traffic from all the vlans to the router where appropriate routing and access restriction are performed.

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

4. Router configuration

The below configuration is for the router in the Packet diagram

- a. The interface connected to the internet is configured with the appropriate IP address.

```
router(config)#interface fa 0/0
router(config-if)#ip address 50.1.1.2 255.0.0.0
router(config-if)#no shutdown
router(config-if)#exit
router(config)#interface fa 0/1
router(config-if)#ip address 8.8.8.1 255.0.0.0
router(config-if)#no shutdown
```

- b. Sub interfaces on the router on physical interface Fa0/0 are mapped with appropriate VLAN and IP address. These configured address on router are default gateway address for users for respective VLAN.

```
router(config)#interface fa 0/0.1
router (config-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 fa 0/0.2
router(config-subif)#encapsulation dot1Q 3
```

```

router(config-subif)#ip address 192.168.3.1 255.255.255.0
router(config-subif)#no shutdown
router(config-subif)#exit
router(config)#interface fa 0/0.3
router(config-subif)#encapsulation dot1Q 4
router(config-subif)#ip address 192.168.4.1 255.255.255.0
router(config-subif)#no shutdown
router(config-subif)#exit

```

- c. The IP helper address is configured on VLAN 3 and 4 interface of router. This is configured for uses in their respective VLANs to reach DHCP server for obtaining dynamic IP address. The configuration is

```

router(config)#interface fa 0/0.1
router(config-subif)#ip helper-address 192.168.2.2
router(config-subif)#exit
router(config)#interface fa 0/0.7
router(config-subif)#ip helper-address 192.168.3.2
router(config-subif)#exit
router(config)#interface fa 0/0.3
router(config-subif)#ip helper-address 192.168.4.2
router(config-subif)#exit

```

- d. Appropriate access control list is configured on router. This is to deny access from guest network to other 2 networks which are an extended ACL. The first 2 lines deny access from guest network to airport authority and Flight server provider networks. Third entry allows all other traffic. This is for internet connection and the access control list is applied in guest vlan interface on 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 fa 0/0.2
router(config-subif)#ip access-group 101 inbound

```

- e. Access control list to restrict access from flight service network to airport authority network. The first line allows flight service provider network to access the airport authority. The second line denies all communication to airport authority network and third line allows all other communications that is for internet. Access list is applied inbound on VLAN interface corresponding to airport authority network.

```

router(config)#access-list 102 permit ip 192.168.2.0 0.0.0.255
host 192.168.3.2

```

```

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 fa 0/0.7
router(config-subif)#ip access-group 102 inbound

```

5. Firewall Configuration

We used ASA1 firewall in this design as it can work as a bridge between Vlan's when configured. Considering the restrictions of access between the Vlans this is best way to config and implement the design

```

ciscoasa(config)#interface vlan 2
ciscoasa(config)#nameif inside
ciscoasa(config-if)#security-level 100
ciscoasa(config-if)#ip address 192.168.2.0 255.255.255.0
ciscoasa(config-if)#exit
ciscoasa(config)#interface vlan 2
ciscoasa(config)#nameif outside
ciscoasa(config-if)#security-level 0
ciscoasa(config-if)#ip address 192.168.2.0 255.255.255.0
ciscoasa(config-if)#exit

```

Similarity we restrict the IP address such that no guest can access Flight service provider or Airport authority and Flight service can't access Airport authority only where as Airport authority has access to all the Vlans.

6. DHCP Configuration

DHCP configuration are made to assign IP automatically to the end devices. For this process we gave a pool of address encapsulated such that an IP address is assigned to end devices automatically.

```

Router#sh ip dhcp pool
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip dhcp pool dv2
Router(dhcp-config)#network 192.168.2.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.2.1
Router(dhcp-config)#%DHCPD-4-PING_CONFLICT: DHCP address
conflict: server pinged 192.168.2.1.
Router(dhcp-config)#ip dhcp pool dv3
Router(dhcp-config)#network 192.168.3.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.3.1
Router(dhcp-config)#ip dhcp pool dv4
Router(dhcp-config)#network 192.168.4.0 255.255.255.0

```

```
Router(dhcp-config)#network 192.168.4.0 255.255.255.0
%DHCPD-4-PING_CONFLICT: DHCP address confl
Router(dhcp-config)#default-router 192.168.4.1
Router(dhcp-config)#ex
Router(config)#ex
Router#%SYS-5-CONFIG_I: Configured from console by console
```

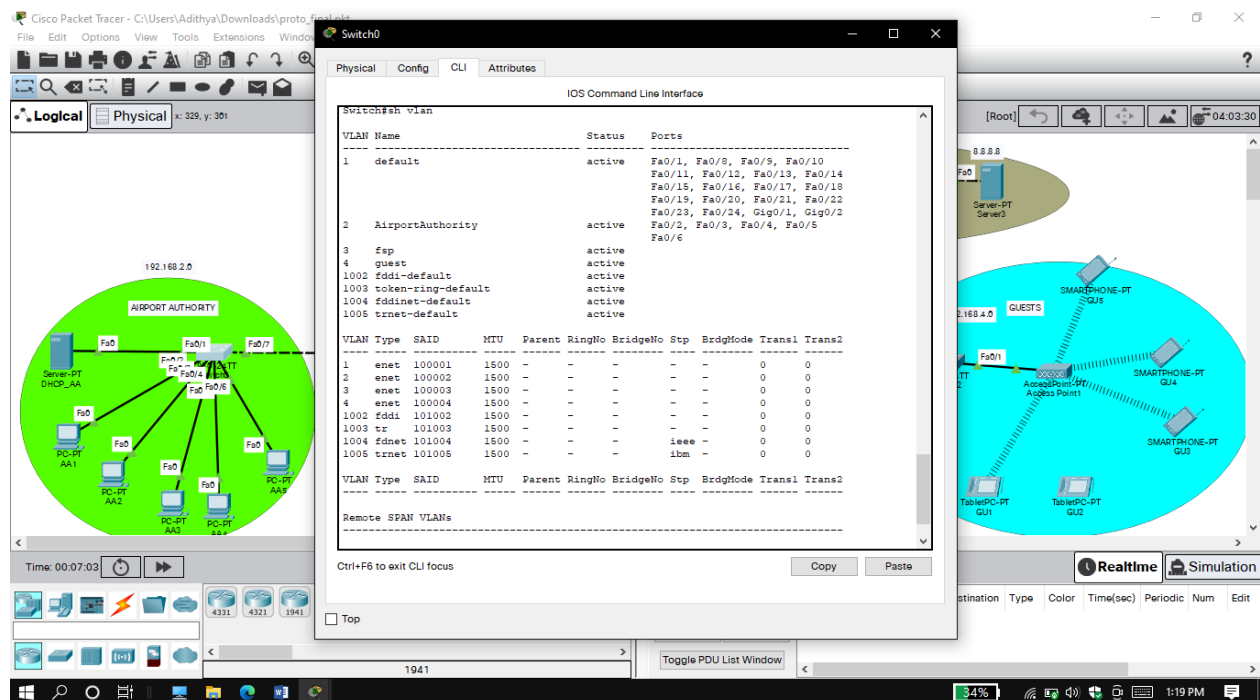
```
Router#sh run
Building configuration...
```

```
Current configuration : 989 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
!
ip dhcp pool dv2
network 192.168.2.0 255.255.255.0
default-router 192.168.2.1
ip dhcp pool dv3
network 192.168.3.0 255.255.255.0
default-router 192.168.3.1
ip dhcp pool dv4
network 192.168.4.0 255.255.255.0
default-router 192.168.4.1
```

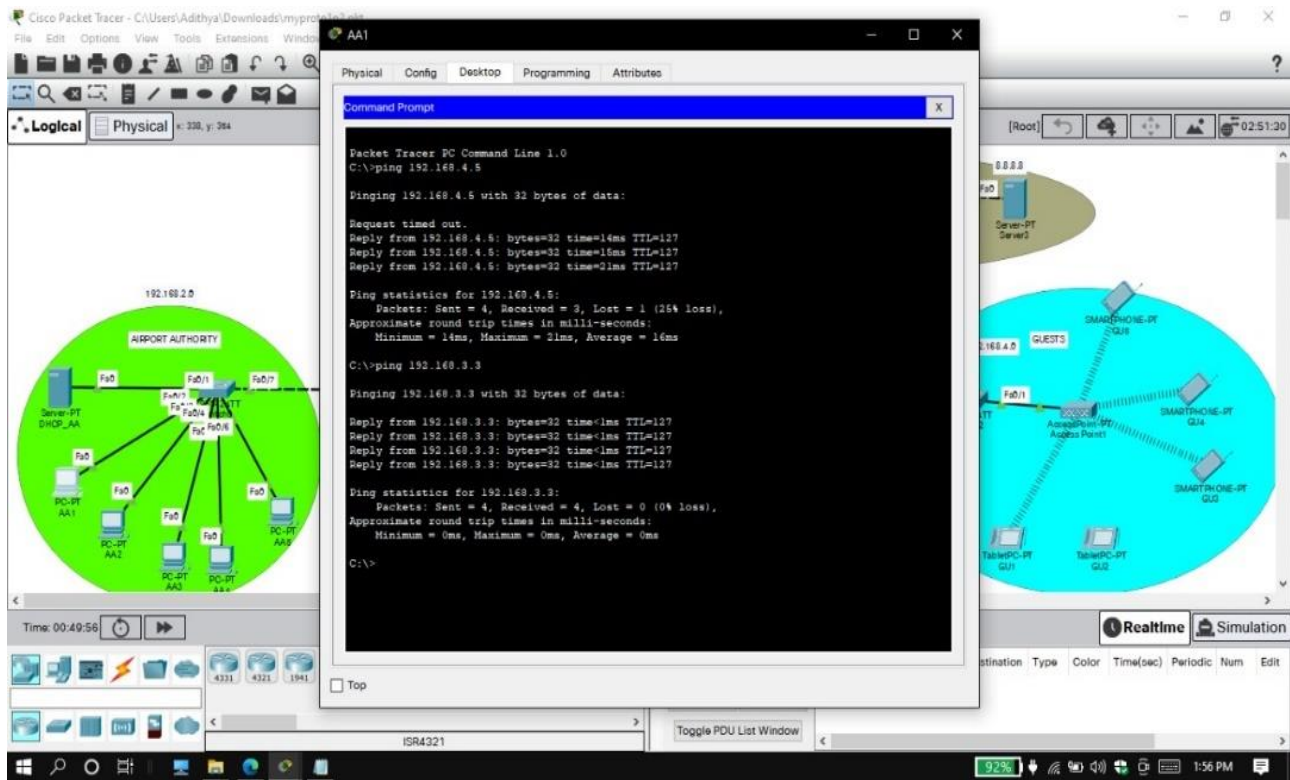
The screenshot shows the WinBox interface for configuring the FastEthernet0 interface. The 'IP Configuration' window is open, and the 'DHCP' tab is selected. The DHCP configuration shows a successful request, and the IPv4 address is set to 192.168.2.2 with a subnet mask of 255.255.255.0. The IPv6 configuration is set to static with a link local address of FE80::204:9AFF:FEEC:E989. The 802.1X security is disabled.

Field	Value
Interface	FastEthernet0
IP Configuration	DHCP (Selected)
Static	Static
DHCP request	DHCP request successful.
IPv4 Address	192.168.2.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.1
DNS Server	0.0.0.0
IPv6 Configuration	Static (Selected)
Automatic	Automatic
IPv6 Address	/
Link Local Address	FE80::204:9AFF:FEEC:E989
Default Gateway	
DNS Server	
802.1X	Use 802.1X Security (Disabled)
Authentication	MD5
Username	
Password	

DHCP SERVER SETUP

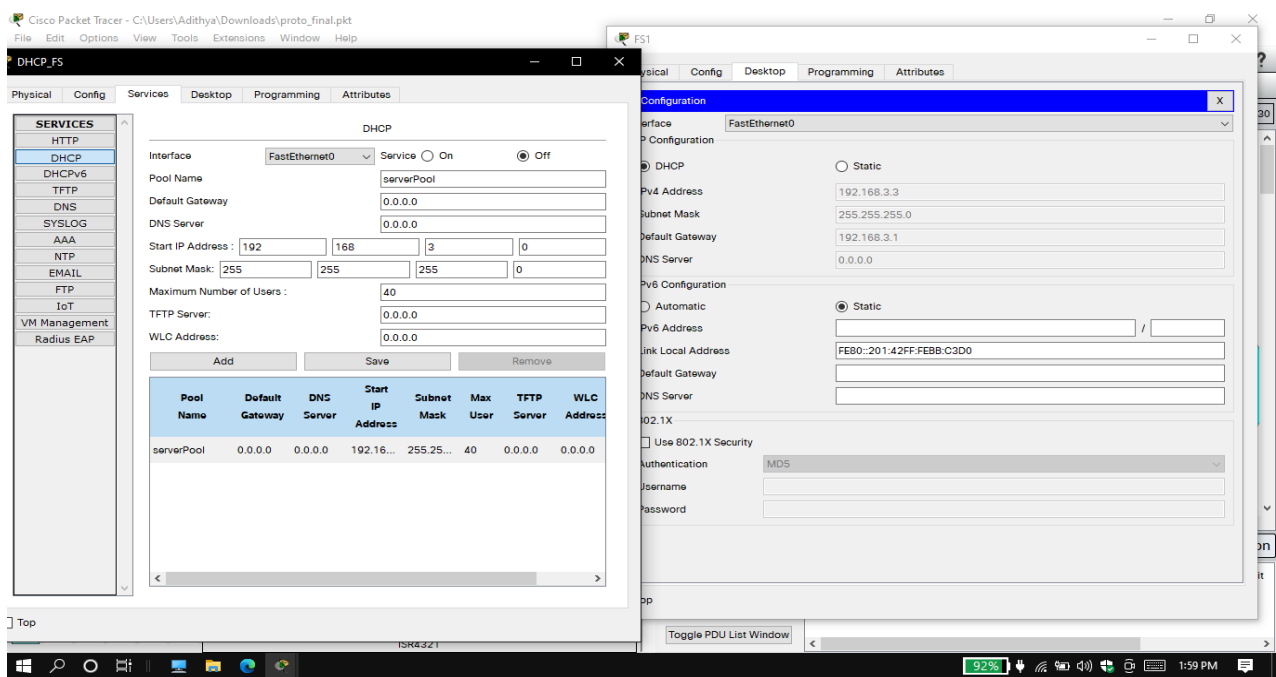


Successful PING in Airport Authority



2.For Flight Server Provider

DHCP SERVER SETUP



VLAN DATABASE

The image shows a Cisco Packet Tracer interface with a network diagram on the left and a CLI window for Switch1 on the right. The network diagram shows a central switch connected to several PCs and a server. The CLI window displays the following output:

```
Switch1
Switch>
Switch>en
Switch>sh vlan
```

VLAN Name	Status	Ports
1 default	active	Fa0/1, 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, Fa0/24, Gi0/1, Gi0/2
2 AirportAuthority fsp	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5
3 guest	active	Fa0/6
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnetr-default	active	

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

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

Remote SPAN VLANs

Ctrl+F6 to exit CLI focus

Successful PING in Flight Server Provider

The image shows a Cisco Packet Tracer interface with a network diagram on the left and a CLI window for FS2 on the right. The network diagram shows a central switch connected to several PCs and a server. The CLI window displays the following output:

```
FS2
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 = 0ms, Average = 0ms
```

```
C:\>ping 192.168.4.5
```

Pinging 192.168.4.5 with 32 bytes of data:

```
Reply from 192.168.4.5: bytes=32 time=16ms TTL=127
Reply from 192.168.4.5: bytes=32 time=26ms TTL=127
Reply from 192.168.4.5: bytes=32 time=32ms TTL=127
Reply from 192.168.4.5: bytes=32 time=36ms TTL=127
```

Ping statistics for 192.168.4.5:

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 16ms, Maximum = 36ms, Average = 24ms
```

```
C:\>ping 192.168.3.1
```

Pinging 192.168.3.1 with 32 bytes of data:

```
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
```

Ping statistics for 192.168.3.1:

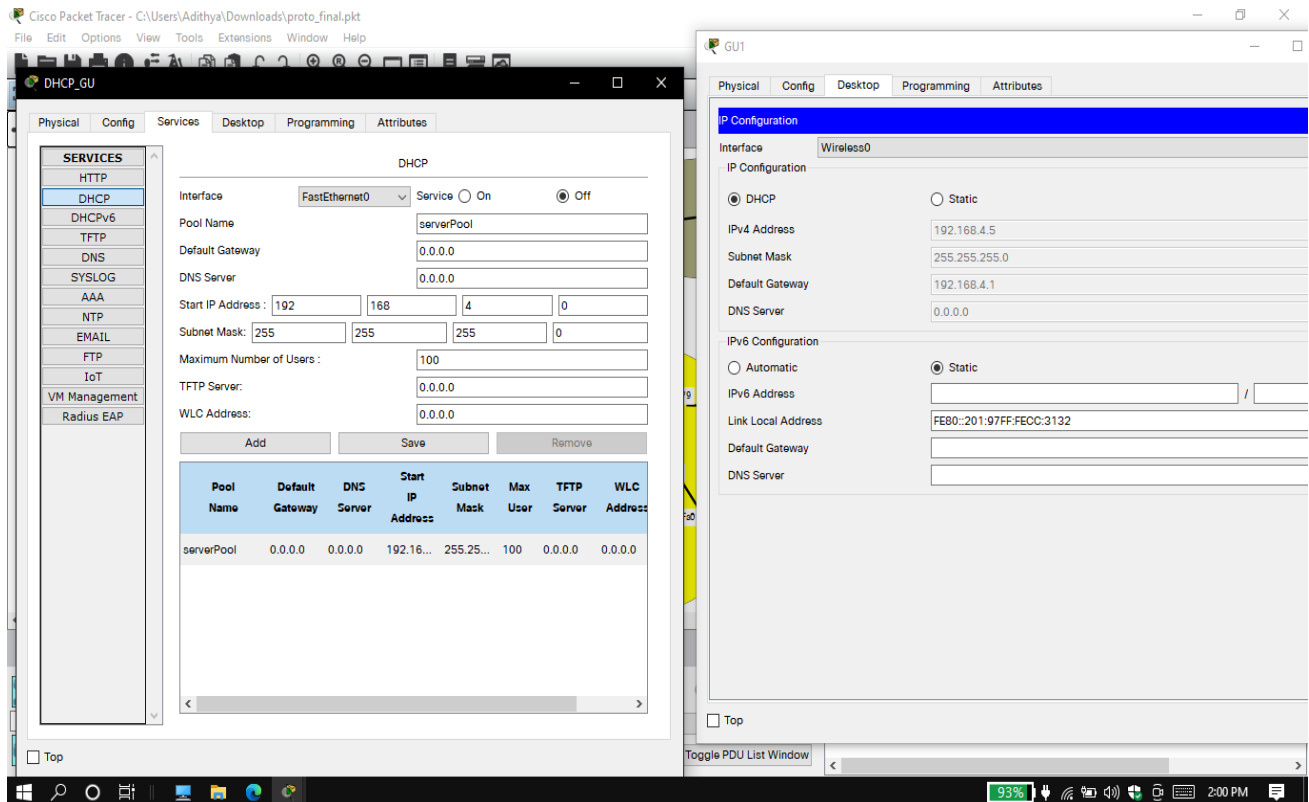
```
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

The output is annotated with red text:

- Able to access airport authority before implementing ACL** (next to the successful pings to 192.168.2.2 and 192.168.4.5)
- Not Able to access airport authority after implementing ACL** (next to the failed ping to 192.168.3.1)

3. For GUEST

DHCP SERVER SETUP



The image shows the DHCP server configuration in Cisco Packet Tracer. The DHCP_GU window is open, showing the configuration for the 'serverPool' interface. The configuration includes:

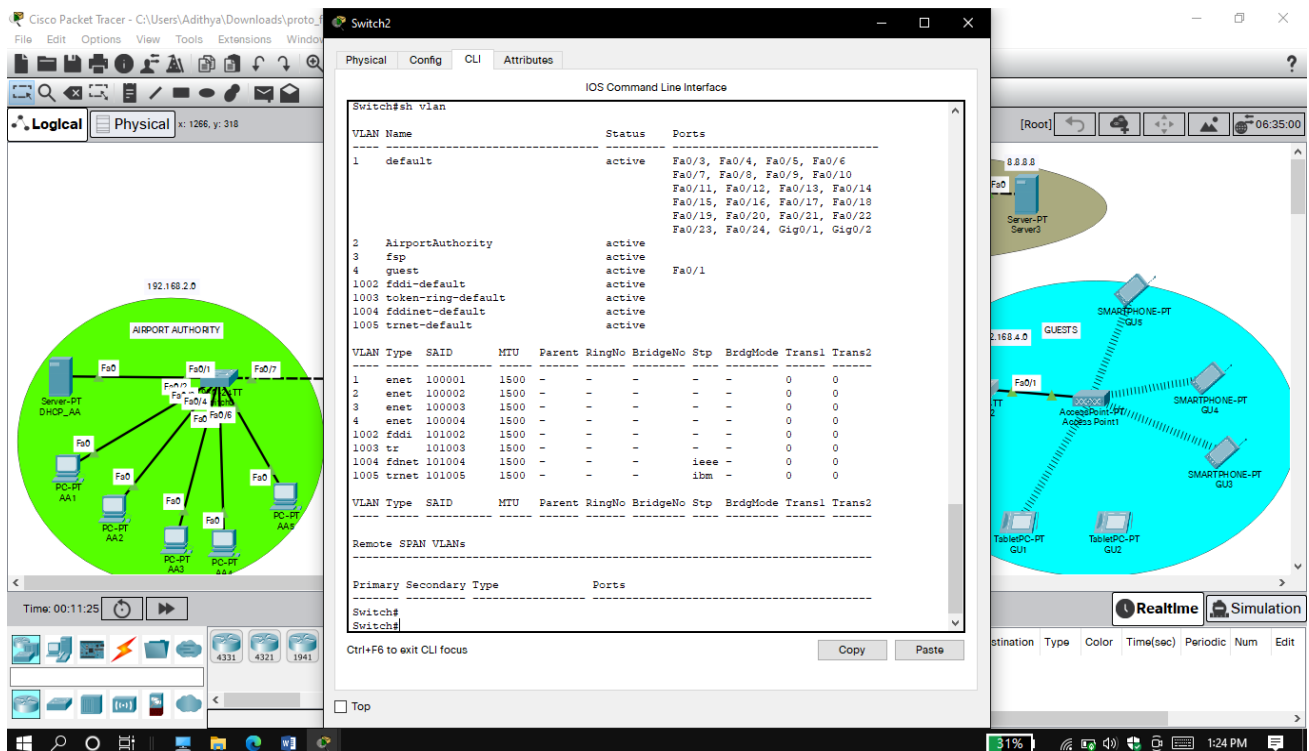
- Interface: FastEthernet0
- Service: Off
- Pool Name: serverPool
- Default Gateway: 0.0.0.0
- DNS Server: 0.0.0.0
- Start IP Address: 192.168.4.0
- Subnet Mask: 255.255.255.0
- Maximum Number of Users: 100
- TFTP Server: 0.0.0.0
- WLC Address: 0.0.0.0

The table below shows the configuration for the 'serverPool' interface:

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	0.0.0.0	0.0.0.0	192.168.4.0	255.255.255.0	100	0.0.0.0	0.0.0.0

The GU1 window shows the IP Configuration for the Wireless0 interface, configured with DHCP. The IPv4 Address is 192.168.4.5, Subnet Mask is 255.255.255.0, Default Gateway is 192.168.4.1, and DNS Server is 0.0.0.0. The IPv6 Configuration is set to Static, with IPv6 Address, Link Local Address, Default Gateway, and DNS Server fields.

VLAN DATABASE



The image shows the VLAN database configuration in Cisco Packet Tracer. The Switch2 window is open, showing the configuration for the 'default' VLAN. The configuration includes:

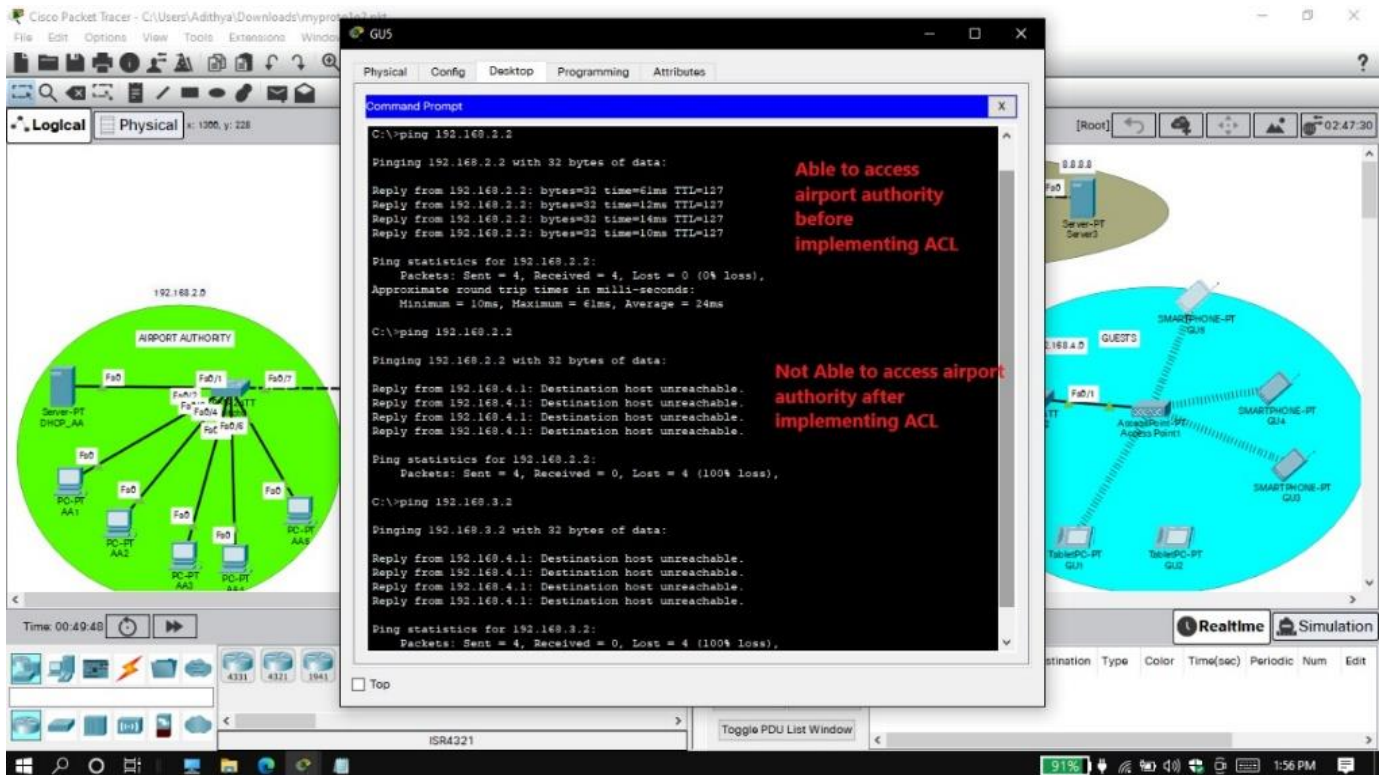
- VLAN Name: default
- Status: active
- Ports: Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Fa0/24, Gig0/1, Gig0/2

The table below shows the configuration for the 'default' VLAN:

VLAN Name	Status	Ports
default	active	Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7, 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, Fa0/24, Gig0/1, Gig0/2

The Logical window shows the network topology, including the 'AIRPORT AUTHORITY' and 'GUESTS' VLANs. The 'GUESTS' VLAN is highlighted in blue, and the 'AIRPORT AUTHORITY' VLAN is highlighted in green. The network includes a DHCP server, a switch, and various devices like PCs, servers, and access points.

Successful PING in Guest Interface



7.2 RESULT ANALYSIS

A final Network Topology is made from the requested problem from the basic topology from the start. Each VLAN is described along the switch. Considering 3 VLAN 2,3 and 4 where each VLAN has their own Server and output devices with IP address assigning randomly by using DHCP server. With three switches each component is divided such that they can be assessed from one another where guest server is denied of other server's access except for Internet.

A detailed topology was made from which airport network is made using the Cisco Packet software. With end users and server along with access points a fully functional network design for Airport is made. A public network needs security for this a firewall is installed along the router such that it can prevent people from accessing the information of servers without authentication. As requested, Airport server can access any information and

provide DHCP address to the PC whereas the Flight server provider can only access its information and guest info but not the airport authority. Guest server is made such that internet is available to the end users whereas the access for other 2 servers is denied completely. When pinged in end users' connections it provides the connections.

7.3 CONCLUSION & FUTURE WORK

There should be further investigation of the technology in these places. Many technical problems may be solved during the actual work period for the airports, particularly as technology evolves. Furthermore, many issues can be resolved and refined in further studies.

Additional effort on several questions is possible. These include:

- Limiting the outside connection by providing a high security level with firewall security policies and the proxy server filter to avoid the outside attack.
- Involve the Windows servers in the security aspect to filter the untested data that entered into the flight management system.
- Bootable operating system from different buildings or the cloud when the local system fails or in case of sudden fire in any department.
- Apply the failover configurations on the firewalls' user interface in a state of the terminal that has been used in the Packet Tracer program to ensure the configuration process steps.
- Use the IP subnet utility to limit the IPs in the network which allows the network to be organized more easily.
- Increase the target storage capacity for the Air Traffic Control System backup to make sure, that the target server has enough

space to store the data, especially in big airports which have a lot of traffic during work operations.

8. Hardware and software inventory list

ITEMS	MODEL	Quantity
ROUTER	Cisco 2600 Series 2621 Router with high-speed interface and internet connection	2
Switches	Cisco 2950 Catalyst Switch	3
Firewall	Cisco ASA0 firewall 5505	1
Assess Points	Cisco Aironet 1200 Access Point	1
Server	IBM/DELL	1
Operating systems	Windows	1
PC	DELL/HP	As per requirement

9. References

"DHCP Best Practices." Dynamic Host Configuration Protocol (DHCP). Web. 18Mar. 2016.

[https://technet.microsoft.com/en-us/library/cc780311\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc780311(v=ws.10).aspx)

Benefits of using DHCP. (n.d.). Retrieved March 17, 2016, from

[https://technet.microsoft.com/en-us/library/cc784893\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc784893(v=ws.10).aspx)

Bipin. (2014, April 01). Configure iSCSI SAN in Server 2012 R2.
Retrieved April 01, 2016, From
<http://www.mustbegeek.com/configure-iscsi-san-in-server-2012-r2/>

Boyce, J. (2000, July 20). Understanding how DNS works, part 1 -
TechRepublic. Retrieved
March 23, 2016, from
<http://www.techrepublic.com/article/understanding-how-dnsworks-part-1/>

C. D. (2012, October 01). Server 2012 DHCP Server Role • PC-
Addicts. Retrieved March 19,
2016, from
<http://pc-addicts.com/server-2012-dhcp-server-role/>

Canavan, J. E. (2001). *Fundamentals of network security*. Artech House.

Sachin, P. (2013, May 29). Network design proposal for airport. Retrieved
April 05, 2016, from
<http://projectsinnetworking.com/network-design-proposal-for-airport/>

Sedayao, J. (2001). *Cisco IOS access lists*. " O'Reilly Media, Inc."

[How to configure DHCP using a Server for Different Networks - YouTube](#)
Apr 27, 2018,from [Tech Acad](#)

[DHCP and DNS server configuration in cisco packet tracer - YouTube](#)
Apr 7, 2016 from [Rajesh Yadav](#)

Configuring a LAN with DHCP and VLANs
[Configuring a LAN with DHCP and VLANs \[Support\] - Cisco Systems](#)

Configuring VLANs

[swvlan.pdf \(cisco.com\)](#)

Access List Commands
[Access List Commands - Cisco](#)

[Extended Access List \(ACL\) for the Cisco CCNA - Part 1 - YouTube](#)
Feb 29, 2012 from [danscourses](#)

[Configuration of Cisco ASA Firewall - YouTube](#)
Feb 19, 2019 from [Saurabh IT Corporate Trainer](#)

Major Reference from SRM institute's PPTs and handouts provides on the topics like DNS, VLAN and DHCP server along with their suggested books like

- ❖ **DATA and Computer Communications written by William Stallings**
- ❖ **DATA Communication and Networking written by Behrouz A. Forouzan**
 - ❖ **Computer networks and Internets written by Douglas E. Comer**

Numerous Online Websites like stack overflow, Cisco and online information sites like techtarget.com and Open source from Wikipedia.

Online content creators and educational tutors mostly from YouTube who helped a lot in clarification of doubts on various topics from the start.

ACKNOWLEDGEMENT

We express our heartfelt thanks to our honorable **Vice Chancellor Dr. C. MUTHAMIZHCHELVAN**, for being the beacon in all our endeavors.

We would like to express my warmth of gratitude to our **Registrar**

Dr. S. Ponnusamy, for his encouragement

We express our profound gratitude to our **Dean (College of Engineering and Technology) Dr. T. V.Gopal**, for bringing out novelty in all executions.

We would like to express my heartfelt thanks to Chairperson, School of Computing **Dr. Revathi Venkataraman**, for imparting confidence to complete my course project

We wish to express my sincere thanks to **Course Audit Professor**

Dr.M.LAKSHMI, Professor and Head, Data Science and Business Systems and Course Coordinator Dr.E. Sasikala, Associate Professor, Data Science and Business Systems for their constant encouragement and support.

We are highly thankful to our my Course project Internal guide **Dr. E.Sasikala, Associate Professor, Data Science and Business System**, for **his/her** assistance, timely suggestion and

guidance throughout the duration of this course project.

We extend my gratitude to all my Departmental colleagues for their Support.

Finally, we thank our parents and friends near and dear ones who directly and indirectly contributed to the successful completion of our project. Above all, I thank the almighty for showering his blessings on me to complete my Course project
