SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

KATTANKULATHUR- 603 203

JUNE 2022

NETWORK DESIGNING FOR AIRPORT

A COURSE PROJECT REPORT

18CSS202J - COMPUTER COMMUNICATIONS

Mini Project

Submitted by

KAMYA OJHA **(RA2111003010343)**

PALAASH SURANA **(RA2111003010319)**

Under the guidance of

Dr.R.S.Ponmagal

(Associate Professor, Department of Computer Science and Engineering)

BACHELOR OF TECHNOLOGY

in

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

of

FACULTY OF ENGINEERING AND TECHNOLOGY

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

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

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 diagram4

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. ADDRESSING TABLE

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 cicso 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 (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 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

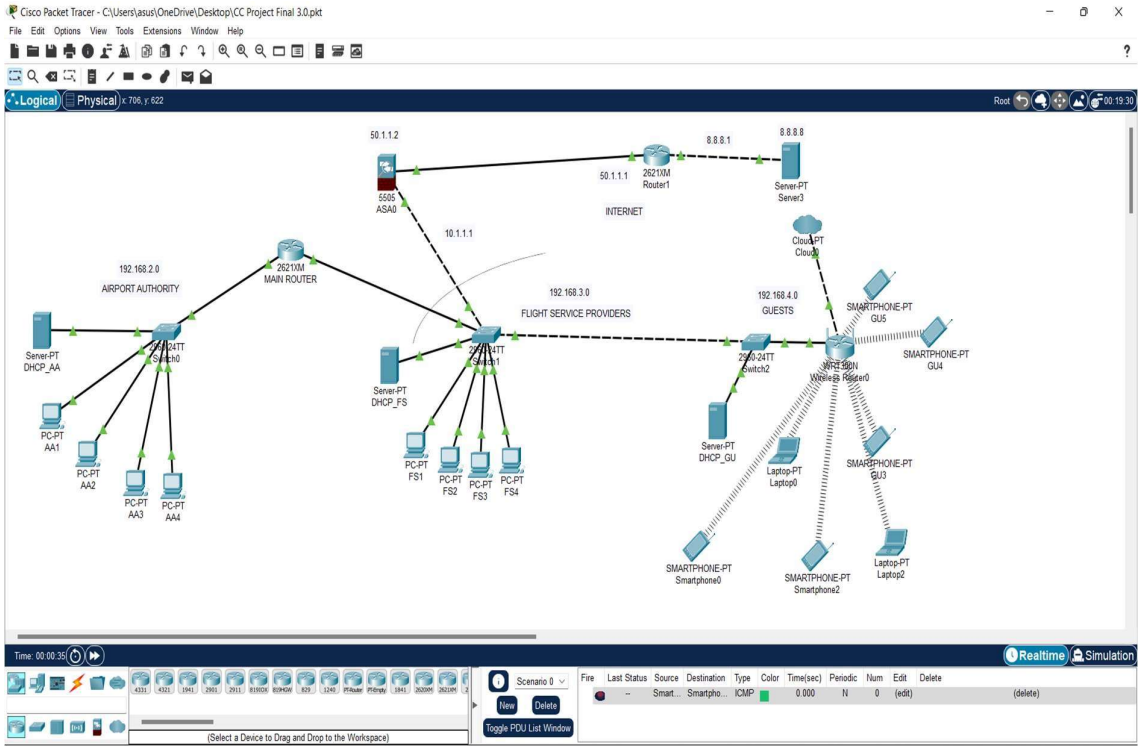
ip dhcp pool dv4

network 192.168.4.0 255.255.255.0

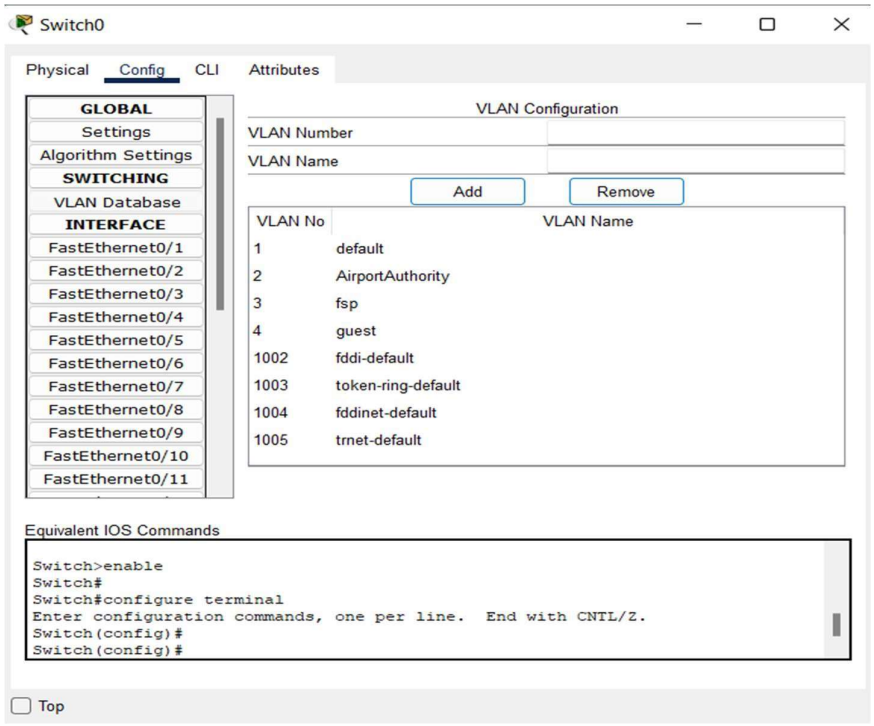
default-router 192.168.4.1

EXPERIMENT RESULTS & ANALYSIS

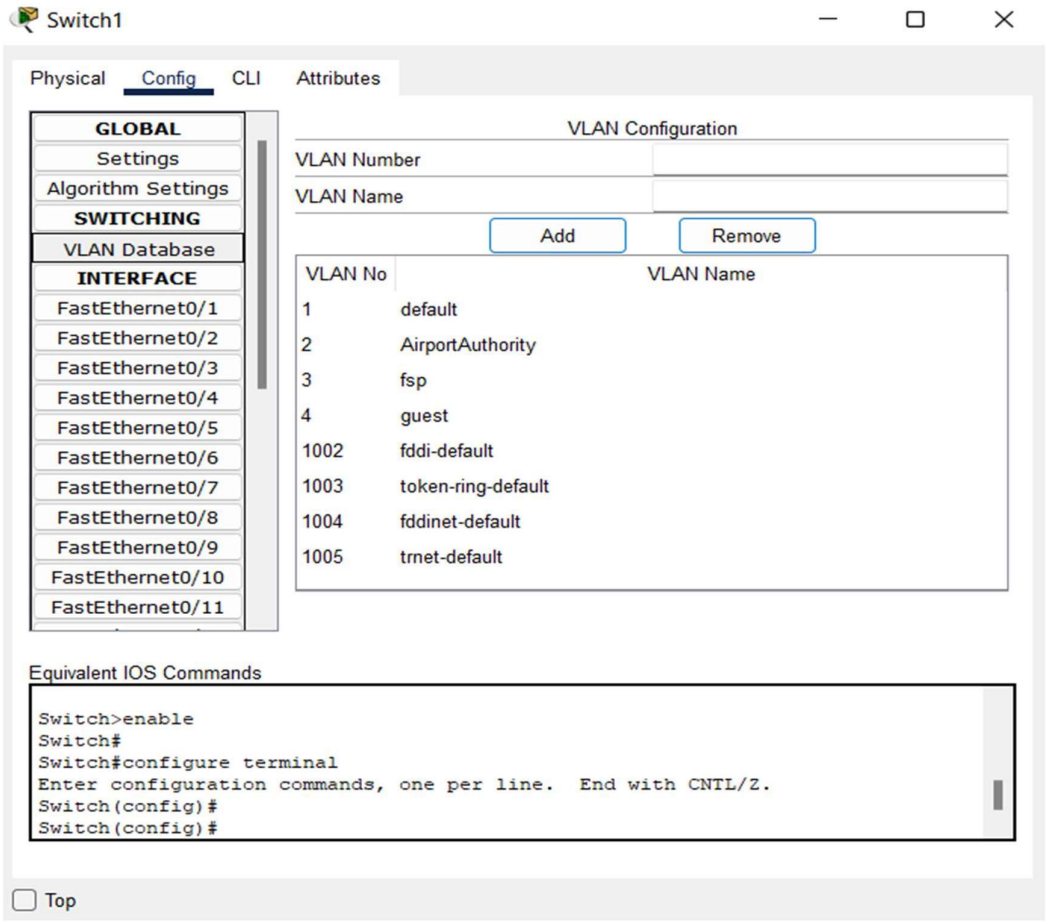
FINAL TOPOLOGY



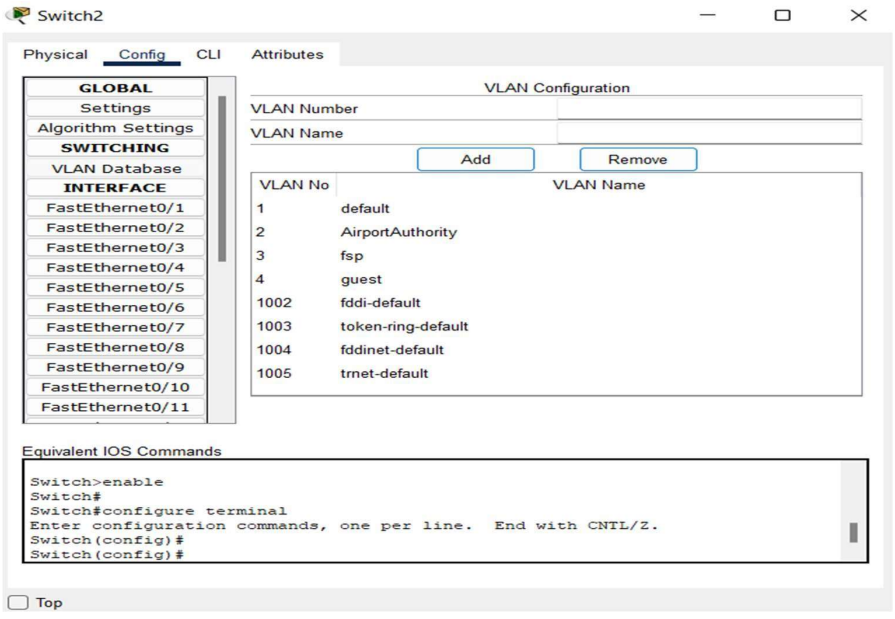
FOR AIRPORT AUTHORITY VLAN DATABASE



FOR FLIGHT SERVER PROVIDER VLAN DATABASE



FOR GUEST VLAN DATABASE



CONCLUSION AND FUTURE WORK

There should be further investigation of the technology in these places. Many technicals

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 f light 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.