

NETWORK DESIGN PROPOSAL FOR AIRPORT

A PROJECT REPORT

Submitted by

**TANYA AGGARWAL [RA1811003010250]
LAXMI ANUSRI PATTI [RA1811003010252]
SUJOY BAITALIK [RA1811003010263]
ANUSHKA RAY [RA1811003010266]**

Under the guidance of

Ms. S. Poornima

(Assistant Professor, Department of Computer Science & Engineering)

in partial fulfillment for the award of the degree

of

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE ENGINEERING

of

FACULTY OF ENGINEERING AND TECHNOLOGY



S.R.M. Nagar, Kattankulathur, Kancheepuram District

DECEMBER 2020

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

(Under Section 3 of UGC Act, 1956)

BONAFIDE CERTIFICATE

Certified that this project report titled “**NETWORK DESIGN PROPOSAL FOR AIRPORT**” is the bonafide work of **TANYA AGGARWAL [RA1811003010250]**, **LAXMI ANUSRI PATTI [RA1811003010252]**, **SUJOY BAITALIK [RA1811003010263]**, and **ANUSHKA RAY [RA1811003010266]** who carried out the project work under my supervision. Certified further, that to the best of my knowledge the work reported herein does not form any other project report or dissertation on the basis of which a degree or award was conferred on an earlier occasion on this or any other candidate.

SIGNATURE

Ms. S. Poornima

GUIDE

Assistant Professor

Dept. of Computer Science and Engineering

ABSTRACT

Designed a proposal for setting up a network in an airport which has three departments, i.e., the airport authority, flight service providers and guests. The airport authority maintains a server which handles the flight management controls. The flight service providers have access only to the specific server in the airport authority and not to any other systems. The guest users have access to a high-speed internet connection which is shared among all the users in all the departments, the wireless access also uses a common password. The guest users do not have any access to the other two departments and all users of every department obtain IP addresses automatically with the help of DHCP, enabled by the server they are connected to. The topology used to design the network is Hybrid Topology, it consists of different star topologies, which in turn can be connected to other smaller networks. A total of four VLANs are used in the network, one for the main switch and the Airport Authority Server, and the rest for Airport Authority, Flight Service Providers and Guests respectively. This sums up the basic infrastructure and network design for this project.

TABLE OF CONTENTS

ABSTRACT	iii
LIST OF FIGURES	vi
ABBREVIATIONS	vii
OBJECTIVE	viii
1 INTRODUCTION	1
2 NETWORKING REQUIREMENTS	3
3 NETWORK DESIGN STRATEGY	4
4 VLAN AND IP NETWORK DESIGN	6
4.1 VLAN DESIGN	6
4.2 IP DESIGN USING DHCP	8
5 REQUIREMENT ANALYSIS OF ACTIVE NETWORKING COMPONENTS	11
6 NETWORK IMPLEMENTATION PLAN	13
6.1 COMPONENTS	13
6.2 WORKING	14

7	NETWORK TOPOLOGY DIAGRAM	16
8	NETWORK CONFIGURATION AND GUIDELINES	18
8.1	SWITCH CONFIGURATION	18
8.2	ROUTER CONFIGURATION	21
8.3	DHCP CONFIGURATION	22
8.4	ACCESS POINTS AND CONFIGURATION GUIDELINES	24
9	HARDWARE INVENTORY LIST	25
10	CONCLUSION	31
11	REFERENCES	32

LIST OF FIGURES

3.1	PROPOSED NETWORK TOPOLOGY	5
4.1	VLAN SET UP	7
7.1	NETWORK TOPOLOGY DIAGRAM	16
8.1	AIRPORT AUTHORITY SWITCH VLAN INTERFACE	18
8.2	AIRPORT AUTHORITY SWITCH TRUNKING CONFIGURATION	19
8.3	FLIGHT SERVICES SWITCH VLAN INTERFACE	19
8.4	FLIGHT SERVICES SWITCH TRUNKING CONFIGURATION	20
8.5	GUESTS SWITCH VLAN INTERFACE	20
8.6	GUESTS SWITCH TRUNKING CONFIGURATION	21
8.7	ROUTER ACCESS CONFIGURATION LIST	21
8.8	ROUTER VLAN SUB-INTERFACES	22
8.9	AIRPORT AUTHORITY SERVER DHCP CONFIGURATION	23
8.10	GUEST SERVER DHCP CONFIGURATION	23

ABBREVIATIONS

IP	Internet Protocol
DHCP	Dynamic Host Configuration Protocol
VLAN	Virtual Local Area Network
UPOE	Universal Power over Ethernet
MLS	Multilayer Switch
ACL	Access List
OSI	Open System Intercommunication
ISP	Internet Service Provider
WEP	Wired Equivalent Privacy
WLC	Wireless LAN Controller
POE	Power over Ethernet
LAN	Local Area Network
DNS	Domain Name System
PC	Personal Computer
SD-WAN	Software-defined Wide Area Network

OBJECTIVE

The objective 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.

CHAPTER 1

INTRODUCTION

Airports are the most crucial and sensitive places around the world because they represent these gates through which millions of people travel each day from one country to another, one city to another. With millions of people flying in and out of these places every second and thousands of people working in this industry, governments, airlines, airport authorities, and the public have become aware of the vulnerability and need to safeguard passenger and freight transportation. This intense focus has drastically changed airport operations and is straining the already tight budgets of airport authorities which made the airport authorities, along with the airlines and government to actively seek out for cost-effective technology solutions to meet the challenges. Technology can be used to not only support the manual security processes but to also perform other activities that could be performed manually before. Computer networking is the most critical part of modern airports because this new technology takes the most important responsibilities, rather than people doing the tasks as in previous decades.

In an airport, it is important to have instantaneous, secure communications between airports, airlines, local authorities, as well as other external entities i.e. the passengers. This has created the need for an open, standards-based communications set-up that can be quickly and easily arranged while also supporting communications with external systems. Both the internal network and external connectivity must be designed with keeping the scalability, availability, and security in mind.

Internet access for public and/or private information is now and will remain a key deliverable in the future. Airports will want to provide flight and airport information to the general public as well as public Internet access in common areas and airline travel lounges. The network must support the ability to segment this traffic away from mission-critical

applications and provide a level of protection and security from external threats.

We installed and configured the network devices such as multilayer switches, routers, PCs, laptops, phones, and access points. We have used a hybrid topology consisting of 4-star topologies each interconnected to each other. The IP addresses are dynamically allocated using DHCP ensuring minimum wastage of IP addresses. This project also consists of two server machines, a combined server for the airport authority and flight services departments and a guest server, each of which are independent of each other. All the guests and other users have wireless access to the internet and will have no access to any other services. While staying in the airport, guest users will also have connectivity to the internet. The security benefits of our solution answer the need to increase safety for the flying public, our solution also provides quality service by proper management of bandwidth requirements, delays, jitters and other quality issues ensuring that the security of the airport is not compromised by other applications on the network. Our smart network service is able to identify and overcome failures while providing rerouting and redundancy for ensuring network availability. Airport and airline operations and communications functions thus gain from greater efficiency, reduced cost, minimized space requirements, simple installation, and ease of expansion.

CHAPTER 2

NETWORKING REQUIREMENTS

The technical requirements for this project are :

Four VLANs are configured to carry the data - VLAN 1 is the default VLAN, VLAN 2 carries the main Airport Authority server and can communicate with the Airport Authority and Flights Services department, VLAN 3 for the Airport Authorities, VLAN 4 for Flight services, and VLAN 5 for guests separately. The airport authority maintains a server which handles the flight management controls. The flight service providers have access only to the server in the airport authority network and not to any other systems. The flight service provider connects to the airport authority server using an access list which ensures that the flight services can connect to only the airport authority server.

The guest users have wireless access to a high speed internet connection, which is shared among all the users in all the departments. The wireless access uses a common password. The guest users cannot not communicate or have access to the other two departments.

Four switches will be mounted in the network to carry the data for Airport Authorities, Flight Services and Guest users. The main switch is a multilayer switch which works on 2 layers - one for routing and the other for switching.

The required number of users for each switch are following:

1. Airport Authorities Switch: 20 Users
2. Flight Services Switch: 40 Users
3. Guest User Switch: 100 Users

CHAPTER 3

NETWORK DESIGN STRATEGY

A network topology is a substantial arrangement of a network in which all the nodes are connected with each other using network links or connecting lines. Apart from just describing how the nodes are interconnected, network topology also explains how the data is transferred in a network.

Choosing the right network topology is important because it plays a fundamental role by giving us an insight into how the network will be set up, how well our network functions, cost factor analysis, maintenance and provisioning tasks. It helps in increasing the performance while making it easier to locate faults, troubleshoot errors, and more effectively allocate resources across the network to ensure optimal network health. A streamlined and properly managed network topology can increase energy and data efficiency, which can in turn help to reduce operational and maintenance costs.

For our project we have used a hybrid topology consisting of several star topologies. Despite having complex design, the main reason for choosing hybrid topology was the degree of flexibility it provides as it can be designed as per our requirements and can be further optimized too. It is also easy to increase the size of our network by adding more components anytime we want. Apart from that fault detection and troubleshooting is easier since the part in which fault has been detected can be isolated from the rest of the network and required corrective measures can be taken, without affecting the functioning of the rest of the network.

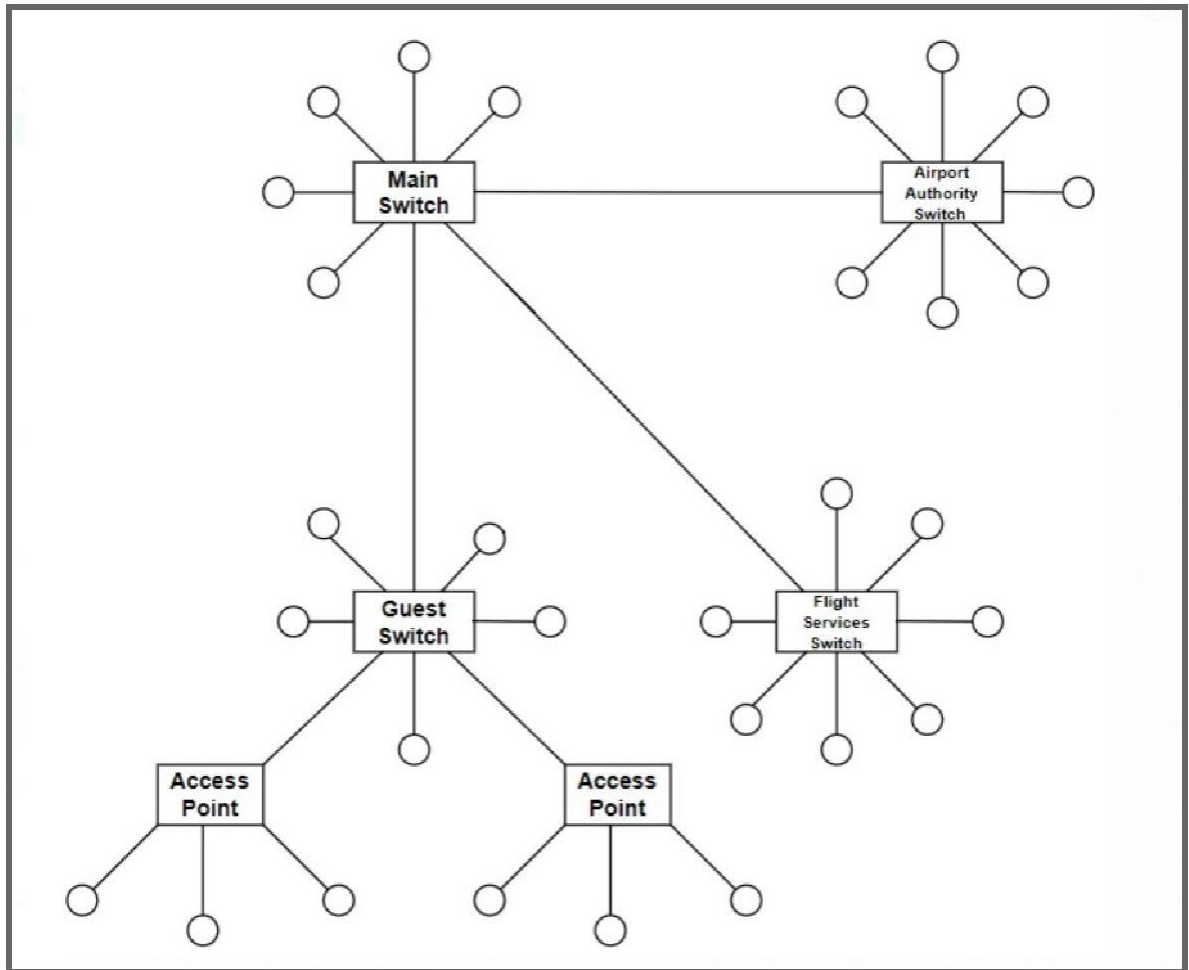


Figure 3.1: Proposed Network Topology

As seen in figure 3.1, the hybrid topology used in our project can be split into several star topologies. These individual star topologies are easy to design and implement. The use of the star topology reduces the impact of any faults that might occur by independently connecting each of the components to the switch. This results in the isolation of that component from all others, but the rest of the network will be unaffected.

CHAPTER 4

VLAN AND IP NETWORK DESIGN

4.1 VLAN DESIGN

A VLAN (virtual LAN) is a subnetwork which can group together collections of devices on separate physical local area networks (LANs). A LAN is a group of computers and devices that share a communications line or wireless link to a server within the same geographical area.

VLANs make it easy for network administrators to partition a single switched network to match the functional and security requirements of their systems without having to run new cables or make major changes in their current network infrastructure. VLANs are often set up by larger businesses to re-partition devices for better traffic management.

VLANs are also important because they can help improve the overall performance of a network by grouping together devices that communicate most frequently. VLANs also provide security on larger networks by allowing a higher degree of control over which devices have access to each other. VLANs tend to be flexible because they are based on logical connections, rather than physical.

Our network uses a total of 4 VLAN's, which contains the multilayer switch and the main server , Airport Authority , Flight Services and the Guest switch respectively.

As Ethernet interfaces can be configured either as access ports or a trunk ports, as follows:

- An access port can have only one VLAN configured on the interface; it can carry traffic for only one VLAN.

- A trunk port can have two or more VLANs configured on the interface; it can carry traffic for several VLANs simultaneously.

We set Access port for the VLAN 2 as it carries only 1 device , the main server while we set the Trunking port for VLAN 3,4 and 5.

A trunk is a point-to-point link between two network devices that carry more than one VLAN. With VLAN trunking, we can extend our configured VLAN across the entire network.

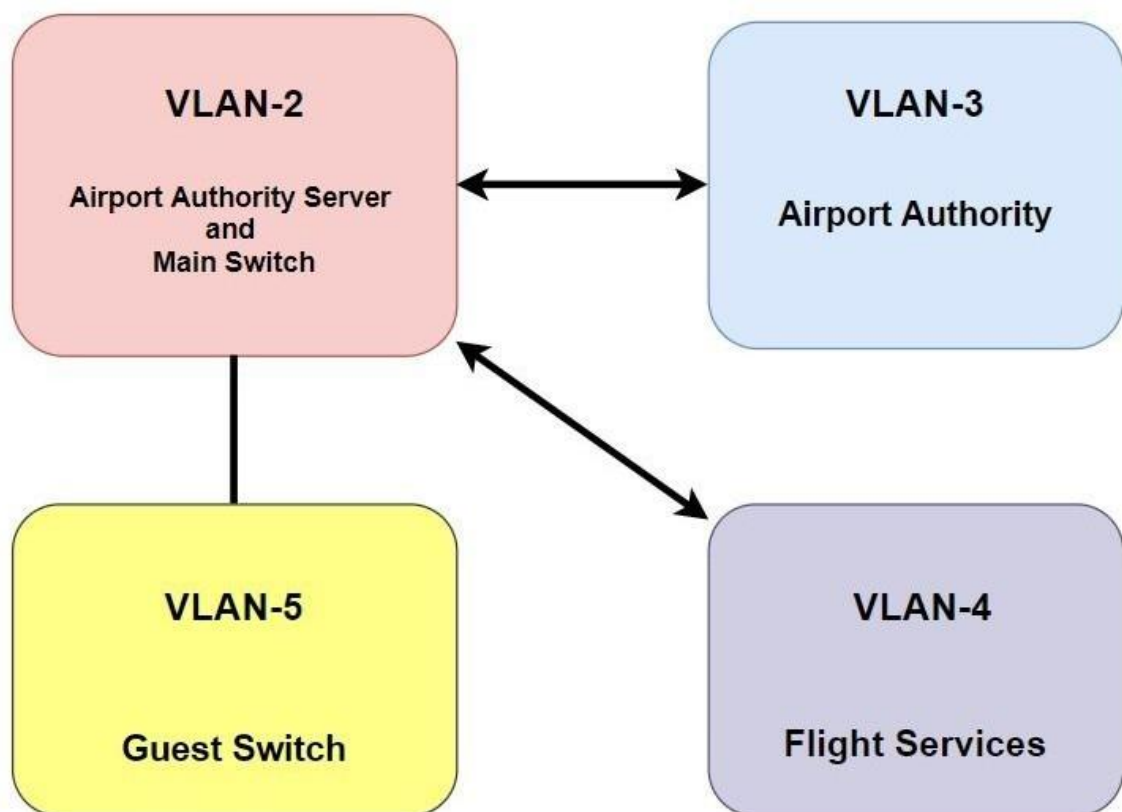


Figure 4.1 : VLAN set up

VLAN 1

Default VLAN

VLAN 2

Set to access mode as it carries only one device , the main server and can communicate with the Airport Authorities and Flight Services.

VLAN 3 AND VLAN 4

Every device in the Airport Authority has access to each other's data . Similarly , every device in Flight Services has access to each other's data. But devices of Airport Authority cannot access data of devices in Flight Services but can communicate to each other and the server. Both the vlans can communicate between each other with the help of trunking.

VLAN 5

The guest is connected to the multilayer switch using a vlan set to Trunking. Although the multilayer switch is a switch it functions like a router and helps in routing and we know that a VLAN needs to be set to trunking for it to work when connected between router and switch. The guest cannot communicate with any of the other components, i.e., Airport authorities, Flight Services and Main server and vice-versa due to access restriction.

4.2 IP DESIGN USING DHCP

DHCP stands for dynamic host configuration protocol and is a network protocol used on IP networks where a DHCP server automatically assigns an IP address and other information to each host on the network so they can communicate efficiently with other endpoints.

In addition to the IP address, DHCP also assigns the subnet mask, default gateway address, domain name server (DNS) address and other pertinent configuration parameters.

DHCP simplifies IP address management - The primary reason DHCP is needed is to simplify the management of IP addresses on networks. No two hosts can have the same IP address, and configuring them manually will likely lead to errors. Even on small networks manually assigning IP addresses can be confusing, particularly with mobile devices that require IP addresses on a non-permanent basis. Also, most users aren't technically proficient enough to locate the IP address information on a computer and assign it. Automating this process makes life easier for users and the network administrator.

Components of DHCP

When working with DHCP, it's important to understand all of the components. Below is a list of them and what they do:

- **DHCP server:** A networked device running the DHCP service that holds IP addresses and related configuration information. This is most typically a server or a router but could be anything that acts as a host, such as an SD-WAN appliance.
- **DHCP client:** The endpoint that receives configuration information from a DHCP server. This can be a computer, mobile device, IoT endpoint or anything else that requires connectivity to the network. Most are configured to receive DHCP information by default.
- **IP address pool:** The range of addresses that are available to DHCP clients. Addresses are typically handed out sequentially from lowest to highest.
- **Subnet:** IP networks can be partitioned into segments known as subnets. Subnets help keep networks manageable.
- **Lease:** The length of time for which a DHCP client holds the IP address information. When a lease expires, the client must renew it.
- **DHCP relay:** A router or host that listens for client messages being broadcast on that network and then forwards them to a configured server. The server then sends responses back to the relay agent that passes them along to the client. This can be used to centralize DHCP servers instead of having a server on each subnet.

Usage of DHCP in Airport Network

1. **Airport Authority Server** - It uses DHCP to dynamically allocate IP addresses for the airport authority as well as the flight services in such a manner that the the airport authority will communicate with the flight services and vice versa only using the airport authority server. This server doesn't have any connection to the Guest.

2. **Guest Server** - As the Guest doesn't have any connection with the other components of the network like the airport authority and flight services it uses Guest server to provide dynamic IP addresses using DHCP. The guest server first allocates IP addresses to the in-house devices used in the airport like monitors, screens etc using DHCP . It also allocates IP addresses to the visitor's or guest devices such as phones or laptops dynamically, these devices are connected wirelessly via the access point after authentication, it is only after authentication that a device is allocated an IP address. So once a guest device is authenticated the Guest Server provides orderly distribution of IP addresses till it's limit gets over using DHCP .

CHAPTER 5

REQUIREMENT ANALYSIS OF ACTIVE NETWORKING COMPONENTS

In our project we have 3 main networks or departments :

- Flight Services
- Airport Authority
- Guests

1. Switches

Switches are key building blocks for any network. They connect multiple devices, such as computers, printers, and servers; on the same network within a building or campus and also enable connected devices to share information and talk to each other. In our prototype we have used 3 switches, 2 same for airport authority and flight services and 1 different for guests.

Why not hub?

As a switch is able to handle the data and knows the specific addresses to send the message.

2. Multilayer Switch

A multilayer switch is a network device that has the ability to operate at higher layers of the OSI reference model. To further connect these 3 switches we have used a main multilayer switch. It not only can do all the job that Layer 2 switches do, it has a routing function as well, including static routing and dynamic routing.

3. Server

For our network we have used 2 DHCP servers. A DHCP Server is a network server that automatically provides and assigns IP addresses, default gateways and other network parameters to client devices. It relies on the standard protocol known as Dynamic Host Configuration Protocol or DHCP to respond to broadcast queries by clients.

4. Access Points

An access point is a wireless network device that acts as a portal for devices to connect to a local area network. Access points are used for extending the wireless coverage of an existing network and for increasing the number of users that can connect to it.

5. CAT6 and CAT6A Cables

As the sixth generation of twisted pair Ethernet cabling, CAT6 cable is mainly used in home and business networks. These cables are standardized twisted pair cables for Ethernet and other network physical layers that are backward compatible with the Category 5/5e and Category 3 cable standards.

CHAPTER 6

NETWORK IMPLEMENTATION PLAN

6.1 COMPONENTS

- **Multilayer Switch** -The multilayer switch (MLS) consists of a 10 gbe switch and a Gigabit Ethernet switch. This network device enables operations at multiple layers of the OSI model. The OSI model is a reference model that describes seven layers that computer systems use to communicate over a network. These seven layers include the physical layer (layer 1), data link layer (layer 2), network layer (layer 3), transport layer (layer 4), session layer (layer 5), presentation layer (layer 6) and application layer (layer 7). The multilayer switch performs functions up to almost Application Layer. For instance, it can do the context based access control, which is a feature of layer 7. Unlike the traditional switches, multilayer switches also can bear the functions of routers at incredibly fast speeds. In addition, the Layer 3 switch is a type of very commonly used multilayer switch.
- **Access List** -Access-list (ACL) is a set of rules defined for controlling the network traffic and reducing network attack. ACLs are used to filter traffic based on the set of rules defined for the incoming or outgoing of the network.

ACL features –

1. The set of rules defined are matched serial wise i.e matching starts with the first line, then 2nd, then 3rd and so on.
2. The packets are matched only until it matches the rule. Once a rule is matched then no further comparison takes place and that rule will be performed.

3. There is an implicit deny at the end of every ACL, i.e., if no condition or rule matches then the packet will be discarded.

6.2 WORKING

Main Switch used in our network for the airport is a multilayer switch . A multilayer switch operates at 2 different layers , the first layer for routing and the second layer for switching which is the reason for selection of multilayer switch as the main switch .

Requirement for Network -

Flight Services should only connect to the Airport authority server and it uses the access list for fulfilling this requirement .

Extended access list is enabled for the main switch which checks the IP address and applies the restrictions. It denies flight services to connect to any other network apart from the airport authority server.

Airport Authority Server -

IP addresses for Airport authority and flight services are dynamically allocated with the help of DHCP.

The airport authority will communicate with the flight services and vice versa only with the help of the airport authority server. The airport authority server has a separate local area network.

Guest -

The guest cannot communicate to the main switch and it has nothing to do with the main switch, the guest server is aware of the existence of the main server and vice versa , however they cannot communicate with each other as it doesn't know the next hop to reach the main server and vice versa.

The guests and other departments of the airport access the internet using the ISP router which is provided by the internet service providers like Airtel, Vodafone etc. It is a type of

a Gateway router. Gateway routers are a special type of routers which are used by enterprises to connect smaller networks to larger networks. In this case, it connects the basic internet infrastructure to the larger network of the ISP which in turn helps in connection to the Internet.

Guest Server -

As the Guest doesn't have any connection with the other components of the network like the airport authority and flight services it uses Guest server to provide dynamic IP addresses using DHCP.

The guest server first allocates IP addresses to the in-house devices used in the airport like monitors, screens etc using DHCP. It also allocates IP addresses to the visitor's or guest devices such as phones or laptops dynamically, these devices are connected wirelessly via the access point after authentication, it is only after authentication that a device is allocated an IP address. So once a guest device is authenticated the Guest Server provides orderly distribution of IP addresses till it's limit gets over using DHCP.

The Access Point has 2 ports , wireless and wired ports.

→ **Port 0** - Ethernet port , it has no IP address and it connects to the guest switch.

→ **Port 1** - Wireless Port , it can connect with any number of devices with an encryption for which WEP is used where the password is a set of 10 digits in hexadecimal form.

Since we are presenting a working prototype of the network infrastructure, the access points are directly connected to the guest switch, but if there are more number of access points spread over the region, wireless controllers can be used. These WLCs serve as a gateway between the guest switch and the different access points.

CHAPTER 7

NETWORK TOPOLOGY DIAGRAM

Building a topology for any network is very important. For our prototype we wanted to set up a resilient, secure, and easy-to-maintain topology. There are several different types of network topology and all are suitable for different purposes, depending on the overall network size and one's objectives. Our strategy was micro segmentation, that is, dividing networks into multiple micro segments and applying separate access privileges. This helps in securing each specific segment.

Keeping that in mind, we decided to build a hybrid topology which can be divided into multiple star topologies.

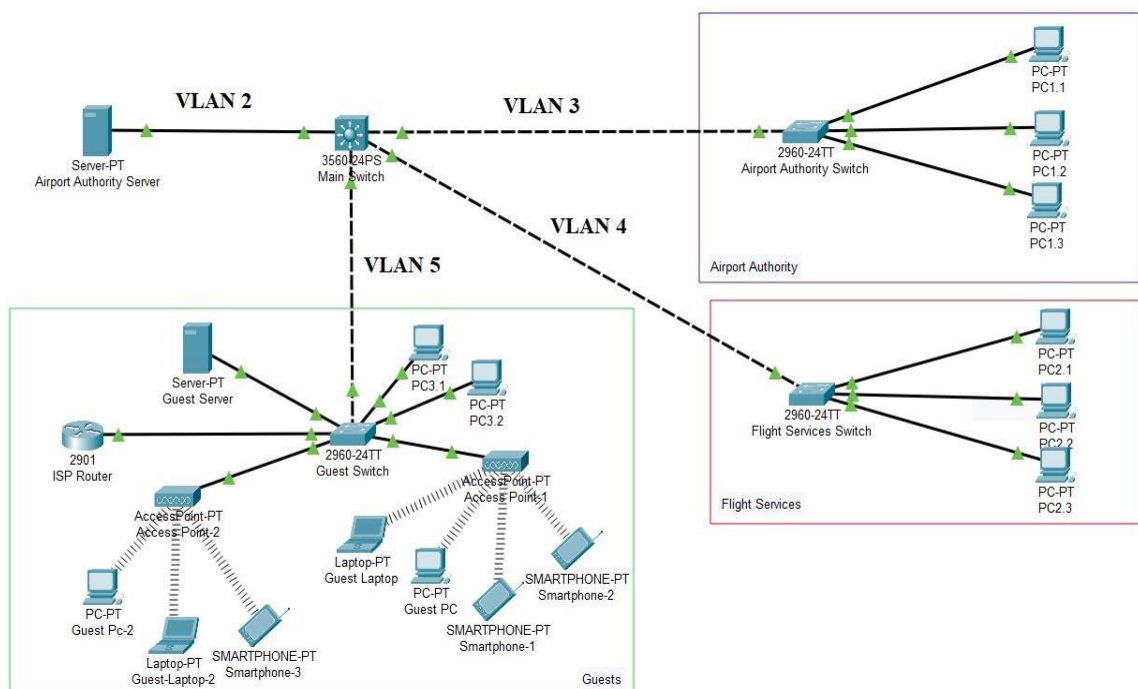


Figure 7.1 : Network Topology Diagram

This topology conveniently manages each segment of the network from a single location. Because each of the nodes is independently connected to the switches, should one go down, the rest of the network will continue functioning unaffected, making the topology a stable and secure network layout. Devices can also be added, removed, and modified without taking the entire network offline. Also it provides the degree of flexibility, as there are few limitations on the network structure itself that this hybrid setup can't accommodate.

On the physical side of things, the structure of the topology uses relatively little cabling to fully connect the network, which allows for both straightforward setup and management over time as the network expands or contracts. The simplicity of the network design makes life easier for administrators, too, because it's easy to identify where errors or performance issues are occurring.

CHAPTER 8

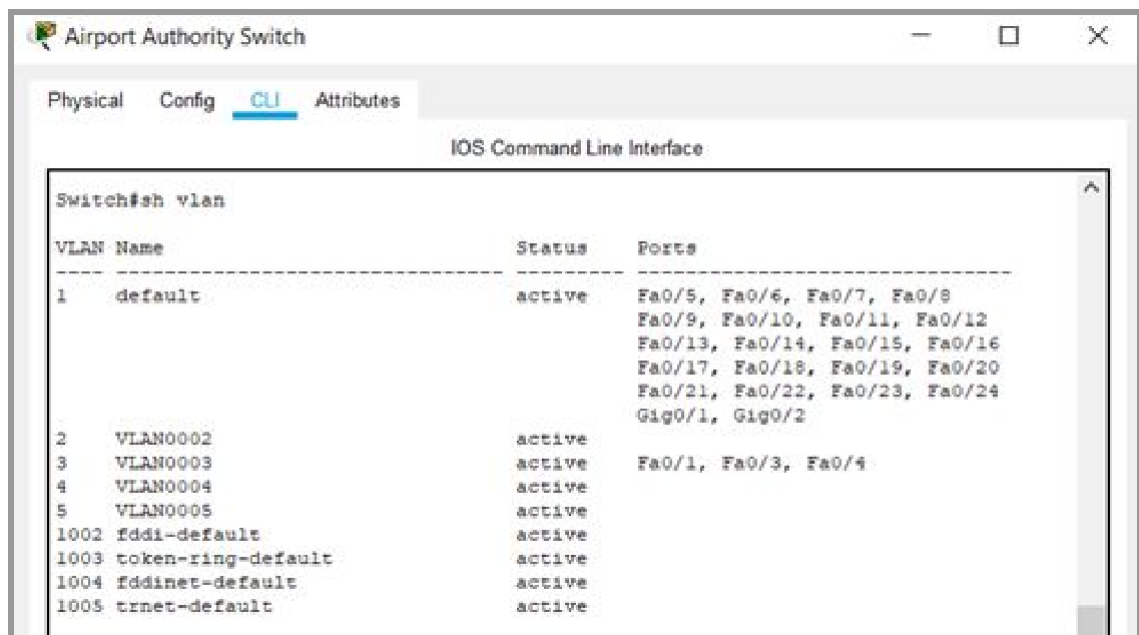
NETWORK CONFIGURATION AND GUIDELINES

Network configuration is the process of setting a network's controls, flow and operation to support the network communication in an organization. This is usually done by configuring the different interfaces and devices among which a connection is established to restrict and monitor the network. For a successful and efficient set-up of the network, some guidelines must be followed as well.

8.1 SWITCH CONFIGURATION

This network uses mainly 3 switches.

i) Airport Authority switch



The screenshot shows the 'show vlan' command output on a switch. The output is a table with three columns: VLAN Name, Status, and Ports. The table lists several VLANs, including the default VLAN 1 and several other VLANs with their respective ports.

VLAN Name	Status	Ports
1 default	active	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
2 VLAN0002	active	
3 VLAN0003	active	Fa0/1, Fa0/3, Fa0/4
4 VLAN0004	active	
5 VLAN0005	active	
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

Figure 8.1 : Airport Authority Switch VLAN interface

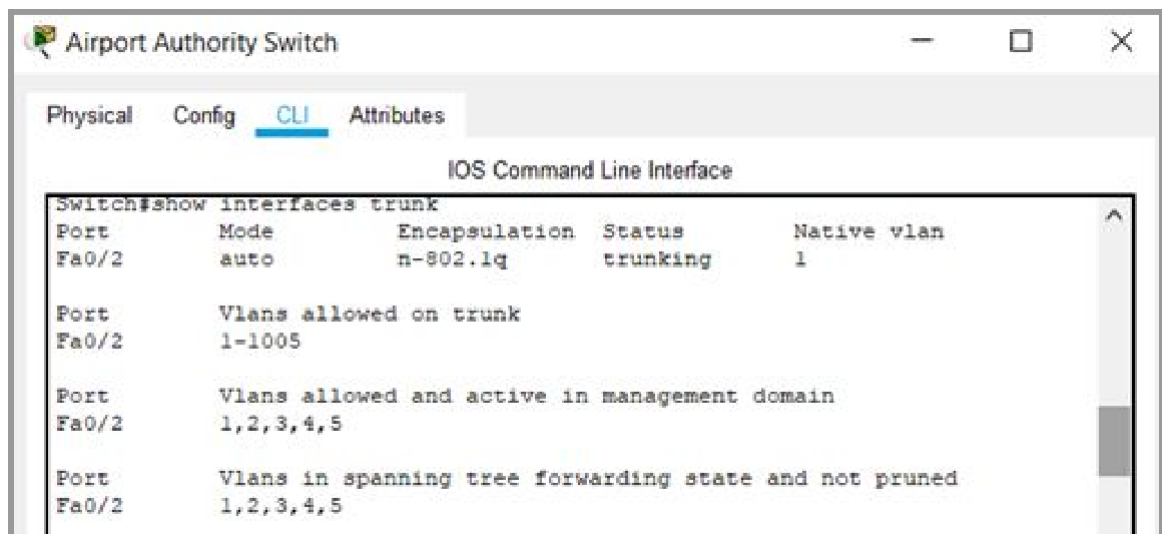


Figure 8.2 : Airport Authority Switch trunking configuration

ii) Flight services switch

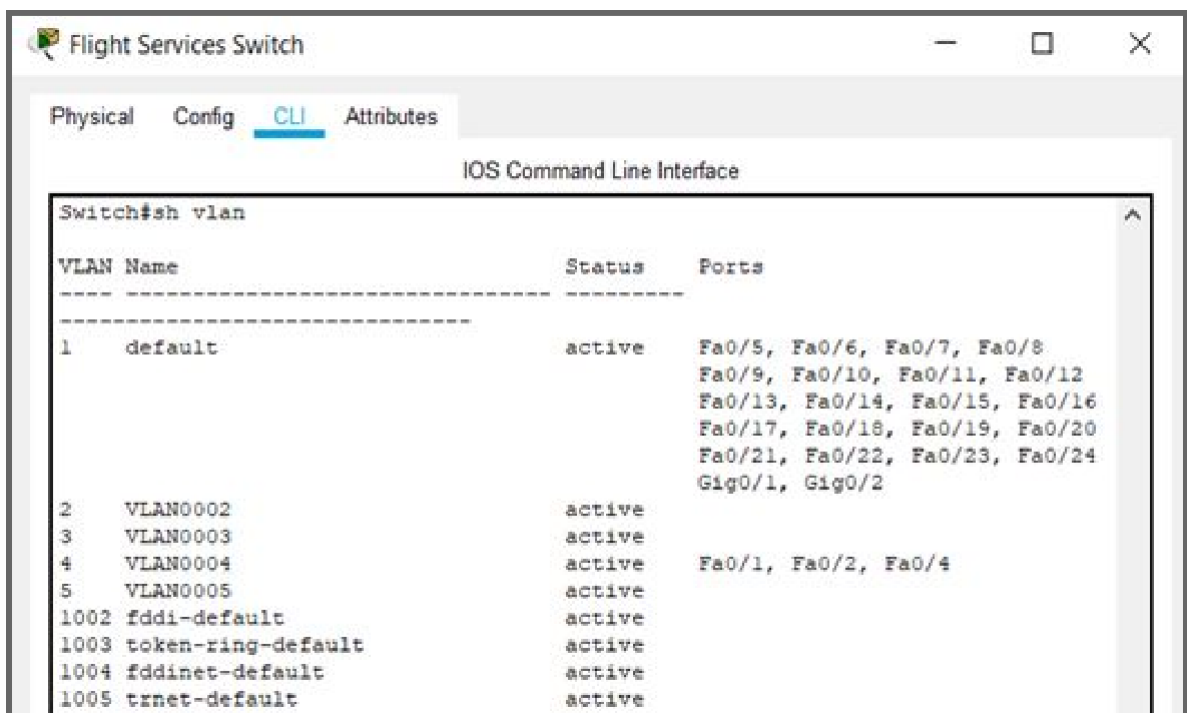


Figure 8.3 : Flight Services Switch VLAN interface

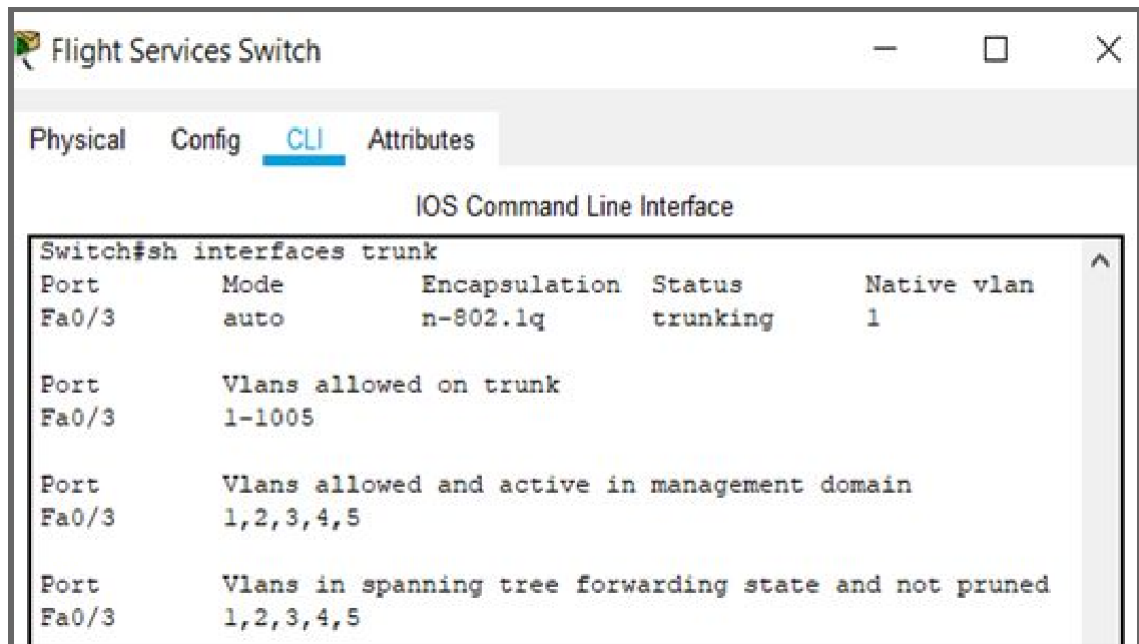


Figure 8.4 : Flight Services Switch trunking configuration

iii) Guest switch

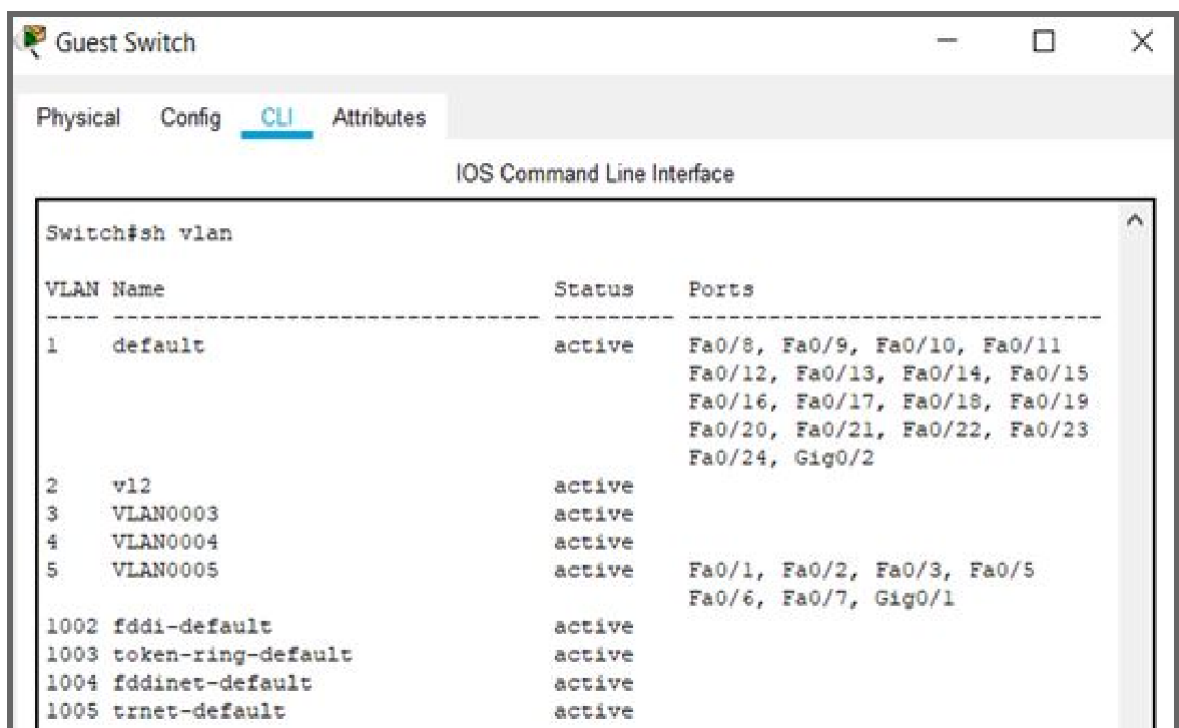


Figure 8.5 : Guest Switch VLAN interface

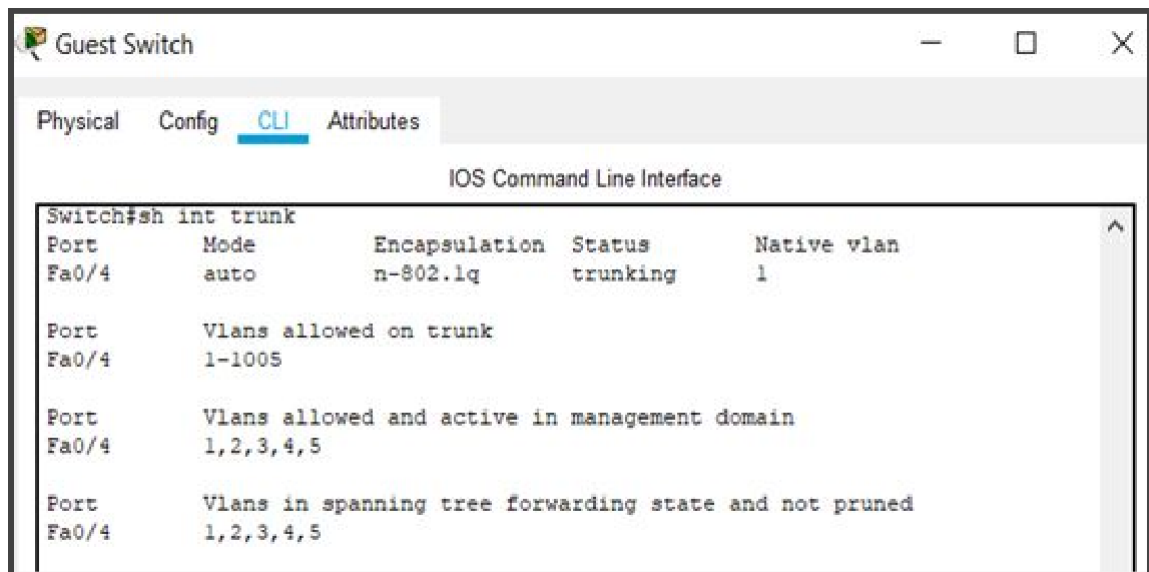


Figure 8.6 : Guest Switch trunking configuration

8.2 ROUTER CONFIGURATION

Instead of a router we use a multilayer switch which can act both as a switch and router.
(Named as main switch)

i) Access Configuration List

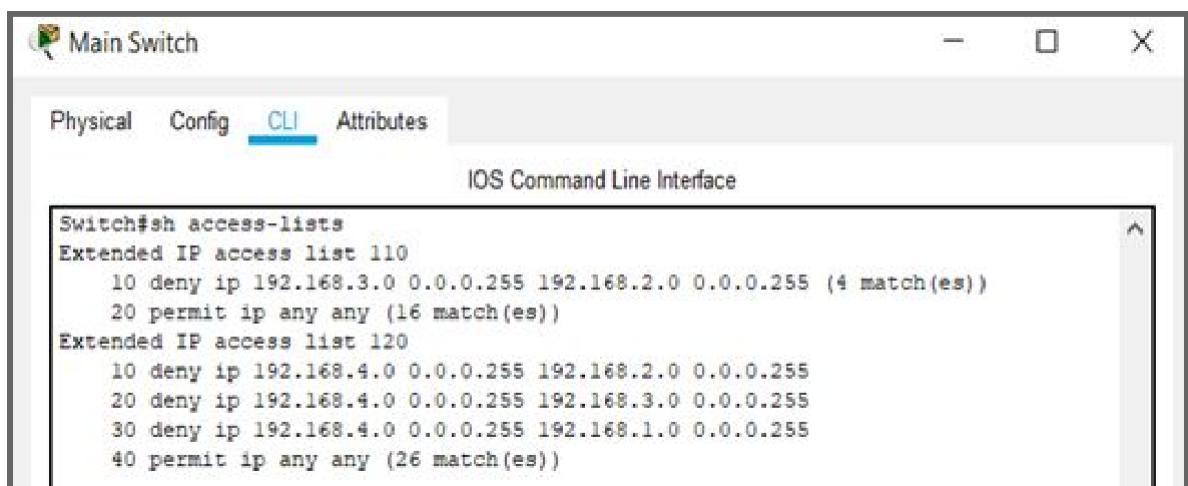
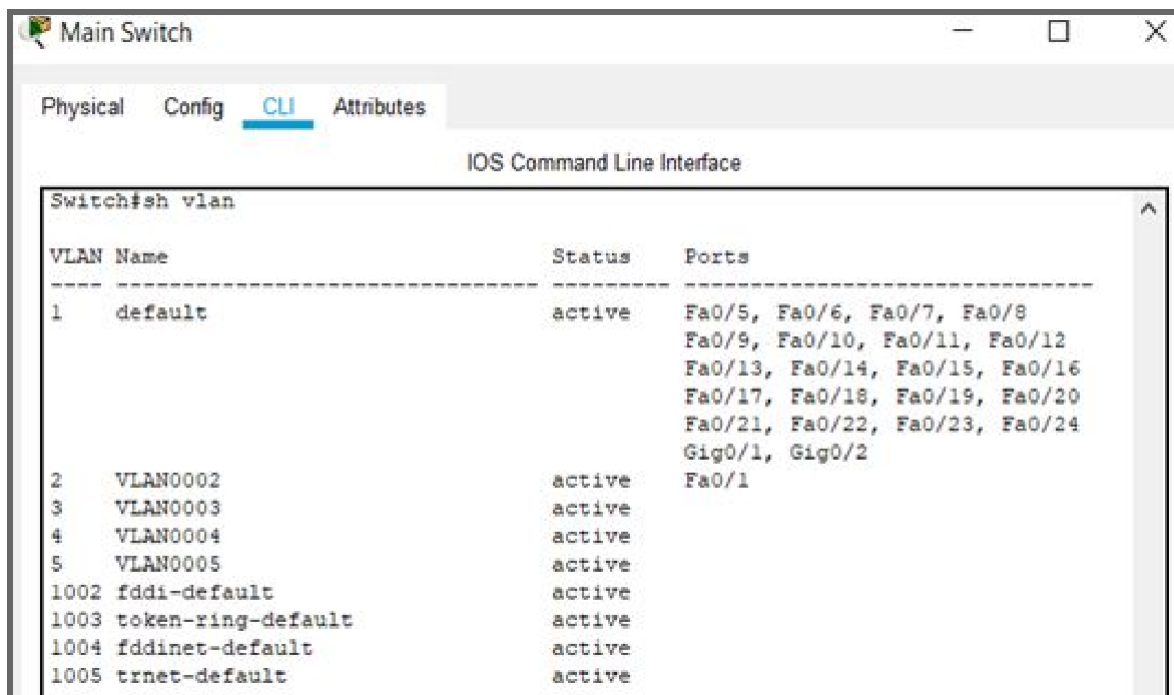


Figure 8.7 : Router Access Configuration List

ii) VLAN sub-interfaces



The screenshot shows a network switch's CLI interface. At the top, there are tabs for 'Physical', 'Config', 'CLI' (which is selected), and 'Attributes'. Below the tabs, the title 'IOS Command Line Interface' is displayed. The main area shows the output of the 'Switch#sh vlan' command. The output is a table with three columns: 'VLAN Name', 'Status', and 'Ports'. The table lists several VLANs, including the default VLAN (1) and several other VLANs (2-5, 1002-1005) with their respective ports and status.

VLAN	Name	Status	Ports
1	default	active	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
2	VLAN0002	active	Fa0/1
3	VLAN0003	active	
4	VLAN0004	active	
5	VLAN0005	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Figure 8.8 : Router VLAN sub- interfaces

8.3 DHCP CONFIGURATION

A DHCP server dynamically assigns an IP address and other network configuration parameters to each device on a network so they can communicate efficiently with other IP networks. This helps with any IP address conflicts that might occur. The use of DHCP also makes it very easy to change addresses, scopes or endpoints. This network has two servers.

- Airport Authority Server
- Guest Server

i) Airport Authority Server

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP**
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DHCP

Interface: FastEthernet0 Service: ☒ On ☐ Off

Pool Name: v4

Default Gateway: 192.168.3.1

DNS Server: 8.8.8.8

Start IP Address: 192.168.3.2

Subnet Mask: 255.255.255.0

Maximum Number of Users: 40

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Buttons: Add Save Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
Airport Authority Server	192.168.1.1	8.8.8.8	192.168.1.3	255.255.255.0	250	0.0.0.0	0.0.0.0
v4	192.168.3.1	8.8.8.8	192.168.3.2	255.255.255.0	40	0.0.0.0	0.0.0.0
v3	192.168.2.1	8.8.8.8	192.168.2.2	255.255.255.0	20	0.0.0.0	0.0.0.0

Top

Figure 8.9 : Airport Authority Server DHCP Configuration

ii) Guest Server

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP**
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DHCP

Interface: FastEthernet0 Service: ☒ On ☐ Off

Pool Name: serverPool

Default Gateway: 192.168.4.1

DNS Server: 8.8.8.8

Start IP Address: 192.168.4.6

Subnet Mask: 255.255.255.0

Maximum Number of Users: 160

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Buttons: Add Save Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	192.168.4.1	8.8.8.8	192.168.4.6	255.255.255.0	160	0.0.0.0	0.0.0.0

Top

Figure 8.10 : Guest Server DHCP Configuration

8.4 ACCESS POINTS AND CONFIGURATION GUIDELINES

An access point is a device that creates a wireless local area network, or WLAN, usually in an office or large building. An access point connects to a wired router, switch, or hub via an Ethernet cable, and projects a Wi-Fi signal to a designated area.

For this network we have used 2 access points, but more switches can be connected and we can connect different access points to them to spread the Wi-Fi signal over the area. Both are WEP encrypted and require a 10-digit password. This password can be given to the Guests upon their arrival in the airport terminal, and can be changed from time to time.

Some configuration guidelines that must be followed are:

1. Determining the most appropriate network configuration to ensure adequate security and performance for the Airport.
2. The organization should choose products that support security management solutions on a network level.
3. The organization shall document the hardware configuration and the software configuration of the network.
4. There should be documented standards / procedures for configuring network devices (e.g., routers, hubs, bridges, concentrators, switches, and firewalls), which cover device configuration and security architecture principles.
5. The organization should validate and audit standards with integrity check and documentation review.
6. All the planning, design and implementation must be done by trained and appointed professionals. Thorough reviews before final decisions play an important role.

CHAPTER 9

HARDWARE INVENTORY LIST

Our airport model is divided into three major sectors namely

- Airport Authority
- Flight Services
- Guests

The above three sectors are made into 3 different VLANs and consist of two servers, one is the airport authority server and other is the guest server. Also, here every VLAN is connected to each other through a multilayer switch. Such that VLAN 3 and 4 cannot communicate with VLAN5.

HARDWARE COMPONENTS

1. Switches

Switches are key building blocks for any network. They connect multiple devices, such as computers, printers, and servers on the same network within a building or campus and also enable connected devices to share information and talk to each other. As a switch is able to handle the data and knows the specific addresses to send the message.

For the Airport Authority and Flight services we will be using 2 units of same switches and for guest have used 1 unit of a different switch:

i. **c9300 48T-48 data ports (flight services and airport authority)**

- The Cisco Catalyst 9300 Series Switches are Cisco's lead stackable enterprise
- Switching platform built for security, IoT, mobility, and cloud.
- At 480 Gbps, they are the industry's highest density stacking bandwidth solution with the most flexible uplink architecture.

- Default AC power supply: 350WAC.
- RAM: 8 GB
- Total 10/100/1000 or Multi Gigabit copper ports: 48 (data ports are normal ports that carry data)
- Price: ₹206,500
- These switches are also ready for the future, with an x86 CPU architecture and more memory, enabling them to host containers and run third-party applications and scripts natively within the switch.

ii. **c9300 48U 48 UPOE ports (Guests)**

- As one of the major purposes of the guest network is to enable the host device to access the internet
- Thus, we have used UPOE (Universal Power over Ethernet).
- It is a CISCO technology which apart from performing the basic functionalities of switches also contains universal ports.
- In this ethernet cables can be used to transfer electricity and power up devices hence, it can be used to power up routers and etc.

2. Multi-Layer Switch

A multilayer switch is a network device that has the ability to operate at higher layers of the OSI reference model. multilayer switches not only can do all the job that Layer 2 switches do, it has a routing function as well, including static routing and dynamic routing.

To further connect the switches, a multi-layer switch is used such that only airport authority and flight services network can communicate with each other, while the guests network though knows the existence of VLAN 3 and 4 but will not be able to communicate with them in any way.

c9404r -1 96 UPOE ports

The Catalyst 9400 series chassis is enterprise optimized with efficient side-to-side airflow and full front accessibility for all removable components, including supervisors, line cards, power supplies and fan tray.

- Provides per port power consumption measurement
- Enables you to specify maximum power consumption on every port
- Supports PoE Power Configuration

3. Servers

A server is a computer that provides data to other computers. It may serve data to systems on a local area network (LAN) or a wide area network (WAN) over the Internet. Many types of servers exist, including web servers, mail servers, and file servers. Each type runs software specific to the purpose of the server.

In our project we have used two servers, one common for both flight services and airport authority and then other in the guest department.

i) Dell PowerEdge mx840c with iDRAC8 (Flight services and airport authority)

- The Integrated Dell Remote Access Controller (iDRAC) is designed for secure
- Local and remote server management.
- It also helps IT administrators deploy, update and monitor Dell EMC PowerEdge servers anywhere, anytime.
- So iDrac is basically management software. iDRAC8 requires setting up the DHCP manually

ii) Dell PowerEdge mx840c with iDRAC9 (Guests)

- This Guest server is different from iDRAC8, it has zero touch setup of DHCP.
- Up to four times more performance with integrated Dell Remote Access Controller 9 (iDRAC9) for easy lifecycle management from deployment to retirement.
- Integrates innovation to maximize longevity and minimize disruption

4. Access Points

An access point is a device that creates a wireless local area network, or WLAN, usually in an office or large building. An access point connects to a wired router, switch, or hub via an Ethernet cable, and projects a Wi-Fi signal to a designated area. Since this is only a prototype, we have used 2 access points in the guest department. If more access points are required, then wireless controllers can be used.

i) AX3600 Wi-Fi 6 Dual-Band Unified Access Point

The DWL-X8630AP AX3600 Wi-Fi 6 Dual-Band Unified Access Point brings next-generation Wi-Fi technology to small and midsize businesses as well as larger enterprises. By combining high-speed 802.11ax Wi-Fi with dual-band technology and 2.5G Ethernet, it provides lightning-fast access to bandwidth-intensive applications such as data, voice and video streaming, even in highly congested environments

- Latest 802.11ax Wi-Fi 6 wireless standard with increased connection speeds
- Up to 3.6 Gbps combined throughput²
- 4 x 4 MU-MIMO with 4 spatial streams
- Better performance in highly congested areas
- Optimised encoding, packing

ii) Wireless AC2600 Wave 2 Dual-Band Unified Access Point DWL-8620AP

The D-Link DWL Series Unified AC Wave 2 Wireless Access Points are specially designed for small to medium businesses or enterprises, providing unparalleled bandwidth and flexibility for administrators looking to deploy a medium to large scale Wi-Fi network with manageable dual-band wireless LAN options and utilizing the cutting-edge speed of Wireless AC Wave 2. Highly manageable and capable of blazing speeds, the Unified AC Wave 2 Wireless Access Points integrate seamlessly into any existing network infrastructure and can be easily scaled to meet future demands. the DWL Series supports Link Aggregation, which allows two Gigabit Ethernet ports to be linked together and act as a single port to double the available bandwidth and maximize the overall throughput of the access point.

The DWL-8620AP is designed for medium to large-scale Wi-Fi networks, delivering fast Wave 2 wireless speeds. It's highly manageable, it fits into any existing network, and can be scaled to meet future wireless demands

Both the devices can be ceiling mounted or wall mounted to provide the best wireless coverage. The built-in Power over Ethernet (PoE) port makes deployments faster and means it can be installed in areas without power outlets.

5. Wireless Controller (if required)

A wireless controller manages wireless network access points that allow wireless devices to connect to the network. It takes the bandwidth coming from a router and stretches it so that many devices can go on the network from farther distances away.

i) Cisco Catalyst 9800-L Wireless Controller

- The Cisco® Catalyst® 9800-L is a fixed wireless controller with seamless software updates for small and midsize enterprises.
- Built from the ground up for intent-based networking, the Cisco Catalyst 9800-L brings together Cisco IOS® XE Software and Cisco RF excellence to create a best-in-class wireless experience for your evolving and growing organization.
- The Cisco Catalyst 9800-L is feature rich and enterprise ready to power your business-critical operations and transform end-user experiences:
- SD-Access. The controller comes with built-in security: Secure Boot, runtime defenses, image signing, integrity verification, and hardware authenticity.
- Built on a modular operating system, the controller features open and programmable APIs that enable automation of day-0 to day-N network operations. Model-driven streaming telemetry provides deep insights into your network and client health.
- Cisco User Defined Network, a feature available in Cisco DNA Center, allows IT to give end users control of their very own wireless network partition on a shared network. End users can then remotely and securely deploy their devices on this network. It grants both device security and control, allowing each user to choose who can connect to their network.

6. Dell PCs (as required)

7. Ethernet Cable

Ethernet cables are standard wires that connect computers to a network. These cables are specifically designed to facilitate easy communication between disparate electronic equipment. An Ethernet cable facilitates communication between the internet servers and your personal computer. The cable provides stable internet connection.

i) CAT6A

CAT6A is capable of supporting data transfer rates of up to 10Gbps at a maximum bandwidth of 500MHz. CAT6A has additional and tighter twists, with additional insulation to reduce crosstalk. CAT6A is also backwards compatible with CAT6 and CAT5E, however, speeds are always limited and will perform to the lowest category cable or connector that is installed in the link. CAT6A is fast becoming the most cost effective solution as it is seen as a future-proof cable system. CAT6A components are used in Class EA networks as defined in ISO/IEC 11801 and TIA/EIA 568.

One of the perceived disadvantages of CAT6A is the actual size and weight of the cable. CAT6A was 50% larger when it originally appeared in 2008. Since then, cable sizes have been reduced and slimmed down by 10%. The additional weight increase also reduces the amount of cable that can fit into a cable tray and where you can place them. This results in a larger cable tray and conduits and smaller bundle size. The increased room is also required for the cable bend radius in the cable tray, patch panel and behind wall outlets.

CHAPTER 10

CONCLUSION

Over the years and even more with increasing globalization, the civil aviation industry became one of the central axes of the trade, which also allows the interconnection of all countries, to the point that airports, especially international, have become the gateways or borders of a country. The aviation industry relies on a quite complex infrastructure integrated in multiple systems that need to be individually and holistically protected.

Through this working prototype of the airport network infrastructure we have tried to overcome all the challenges that are there and make this industry more safe and secure. We have overcome the challenges faced in the past by implementing a streamlined end-to-end security. Our strategy was micro segmentation, that is, dividing networks into multiple micro segments and applying separate access privileges. This approach helps contain any compromise or data breach to its specific segment.

REFERENCES

- [1] www.community.cisco.com
- [2] www.packettracernetwork.com
- [3] www.instructables.com
- [4] www.computernetworking747640215.wordpress.com
- [5] www.tcpipguide.com
- [6] <https://youtu.be/HmtxH5UIIS8> (Văn Phạm Hoài)
- [7] www.stackoverflow.com
- [8] www.netmanias.com
- [9] www.cisco.com
- [10] www.academia.edu
- [11] www.ciscopress.com
- [12] www.netacad.com
- [13] cyberstartupobservatory.com/aviation-cybersecurity-understanding-the-airport-ecosystem
- [14] techgenix.com/network-topology/
- [15] www.networkworld.com
- [16] www.cisco.com/c/en/us/products/index.html
- [17] www.oreilly.com/library/view/packet-guide-to/9781449311315/ch04.html
- [18] Packet Tracer Network Simulator by Jesin A
- [19] The VIRL BOOK by Jack Wang