Network Design for Airport Enterprise

Ahsan Ali (aa05201) and Muhammad Abeer Sohail (ms04406)

Introduction

The aim of this project is to design and implement communication network for airports with performance parameters being security, quality and reliability. The project has explored various utilities to construct a highly secure network for airport which includes crucial operations ranging from flight timing control, airplanes coordination, passenger services through servers and databases.

The potential utilities for such a network include hardware firewalls, IP access control, MAC address port security, domain servers, proxy servers, failover firewall utility, Inter VLAN Routing, a Dynamic Host Configuration Protocol (DHCP) server, a Domain Name System (DNS) and cabled connections. These utilities will have been configured to provide a secure and reliable environment for various parties such as Management Authority, Flight Service Provider and Guests to intercommunicate and prevents compromising of sensitive information such as flight management and service providers to potential attackers.

This project aims to establish a communication network for an airport. The network is able to facilitate three groups namely Airport Authority, Flight Service Providers (FSP's) and Guest Members. Each group is assigned appropriate network privileges and functionality to perform relevant tasks and is allocated appropriate service over the network. The Airport Authority and Flight Service Provider have their respective servers while the guests are only allowed to connect to the internet using either Wireless or Ethernet based connectivity. The project has implemented appropriate yet scaled-down measures of cybersecurity, such as cabled connections, virtual LANs, subnetting, firewall, access restriction and isolation to prevent unwanted access into the network.

Project Scope and Problem Description

As discussed above, the main features of an airport network include a highly secure network, flight timing control, airplanes coordination, and passenger services. They can, more generally, be divided into features associated with two types of interactions. Supervisory Control and Data Acquisition (SCADA) systems are critical infrastructure responsible maintaining electrical power systems, water, gas and other utilities in transportation systems as airport. They provide physical isolation and technical uniqueness against cyber-attacks by playing

crucial rule on enterprise and corporate networks. SCADA systems are now being integrated into information technology systems network using TCP/IP.

Developing technologies are giving rise to whole new arena of cyber-attacks and the need for robust privacy and security systems are ever great. For example, according to Chief IT Officer of Los Angeles airport, there were 6400 reported attempts to hack into file server after 2 days it was employed; and about 59,000 internet misuse cases and abuse attempts were reportedly block; and over one year period, about 2.9 million hacking attempts were blocked [1]. Most of these vulnerabilities lie in poor and partial configuration of Wireless Access Point (WAP), Network Access Points (NAP), unsecured SQL databases, poorly optimized and configured firewalls, interconnected peer networks with compromised security and several others.

In case of airports, most common cyberattacks takes place in form of Speak-Phishing emails containing malware packages like Sykipot that when is running target machine will establish an SSL connection to command and control server, where more malicious files are then downloaded and installed in victim's computer. Information of airport network layout, flight timings, routes, passengers' details and airport facilities are compromised. According to one of the studies [1], 77 percent of Airtight networks were non-hotspot out of which 80 percent were unsecured or using legacy WEP encryption, fatally flawed protocol.

Networking Requirement

1) Airport Authority: It is responsible for maintaining the flight management protocols and is also responsible for assigning dynamic IPs to the Guest users as well as controlling the limitation and access of Flight Service Providers. Both the servers mentioned above are regulated by Airport Authority. There are total of 20 users in this VLAN.
2) Flight Service Providers: This department is responsible for handling the details of passengers, incoming/outgoing flights and arrival/departure times. There are total of 40 users in this VLAN.
3) Guest Members: These are ordinary people or passengers who will likely browse the internet for their email, to look for hotel bookings, to book a taxi etc. Their access is most limited to the internal network, which comprise the flight service providers and airport authority networks. They virtually only connect to the Internet and not the internal network of the airport. There are maximum of 100 users in this VLAN.

Network Design Strategy

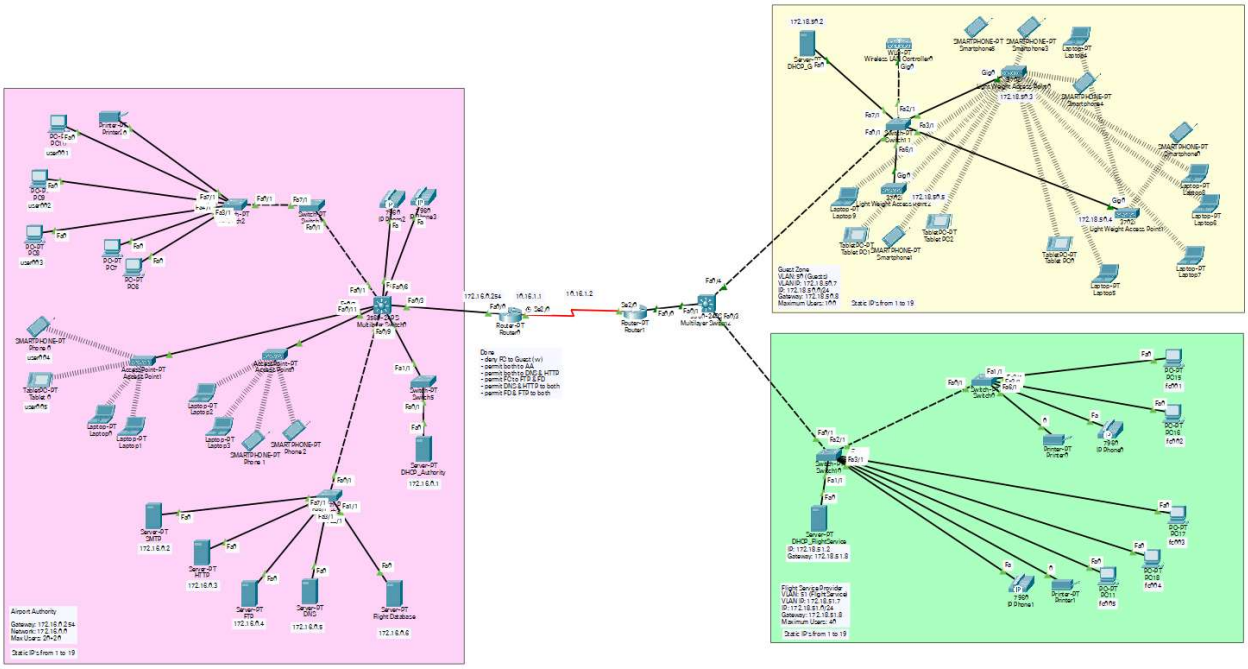
1) The active networking components includes the following:
    a) Routers (for connection to the internet).
    b) Switches (for connection of the PC nodes and workstations within a VLAN, and for the interconnection of VLAN's).
    c) Wireless Access Points (WAPs) for connecting nodes that do not seek a permanent connection, using a wireless medium.

2) The IP network design for each department. a) We have created network IDs with suitable subnet masks according to the number of nodes within a network. For example, the different departments are assigned different private network IDs and private IP addresses. To ensure no communication between the departments, we have configured different VLANs. The IP addresses of the routers in the network are default gateways for the nodes in the VLANs.

3) The network should support bandwidth sharing and restricted access for the different users in the network. This is especially true for the guest network, since the number of connecting nodes are very high, and any malicious agent can enter the core network of the airport from the guest network since the login details are public. This can be configured using the priority and bandwidth commands from the command-line-interface in Cisco devices.

Network Topology Diagram

The diagram below shows the final network topology. It displays the conceptual layout of the topology. The routing to the internet is performed by two routers and two multi-switches. Multi-switch is also used to create VLANs. Appropriate restrictions are composed in routers as well as discussed in later section. Multiple servers are also placed in Authority zone to provide services of database, emailing, browsing, DNS, HTTP etc.



Airport Authority Topology

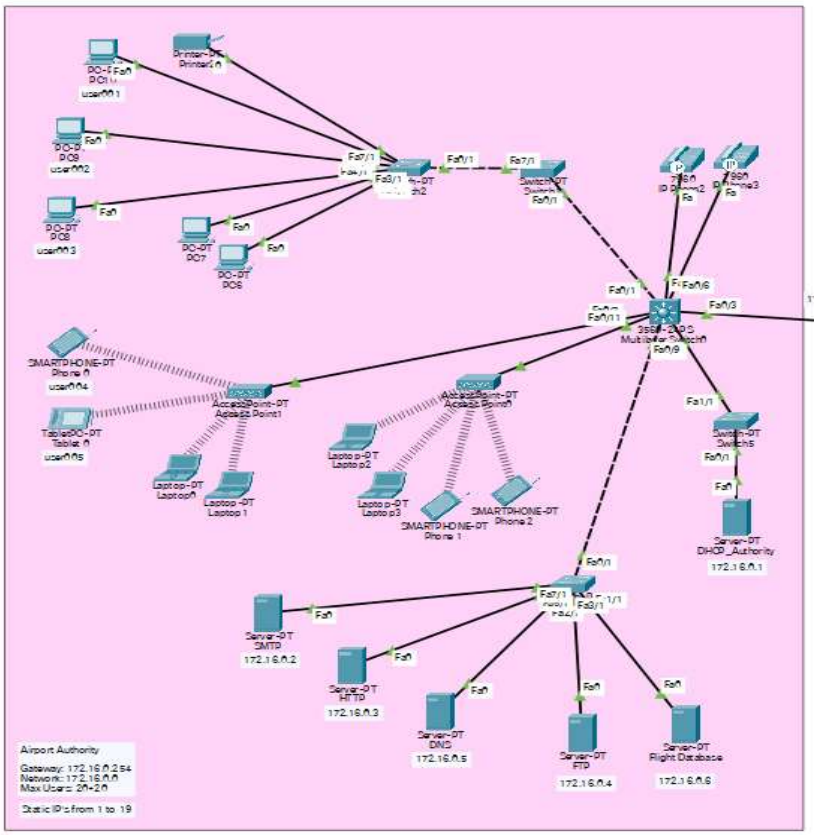
Network Address Table

Device	Network Zone	IP Interface	Gateway	User ID
SMTP Server	Airport Authority	172.16.0.2	172.16.0.254	-
HTTP Server	Airport Authority	172.16.0.3	172.16.0.254	-
DNS Server	Airport Authority	172.16.0.5	172.16.0.254	-
FTP Server	Airport Authority	172.16.0.4	172.16.0.254	-
Flight Database Server	Airport Authority	172.16.0.6	172.16.0.254	-
DHCP Authority Server	Airport Authority	172.16.0.1	172.16.0.254	-
DHCP Flight Service	Flight Service	172.18.51.2	172.18.51.8	-
DHCP Guests	Guests Zone	172.18.50.2	172.18.50.8	-
Router 1	Intermediate	Fa0/0 Se2/0 10.16.1.2	-	-
Router 0	Intermediate	Fa0/0 172.16.0.254 Se2/0 10.16.1.1	-	-
PC10	Airport Authority	Dynamic	172.16.0.254	User001
PC9	Airport Authority	Dynamic	172.16.0.254	User002
PC8	Airport Authority	Dynamic	172.16.0.254	User003
Smartphone 0	Airport Authority	Dynamic	172.16.0.254	User004

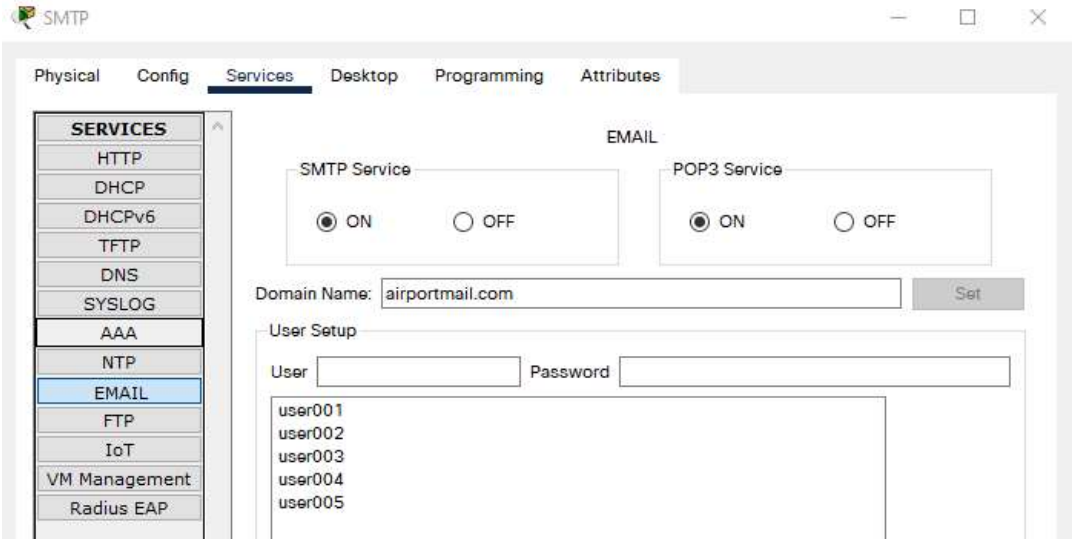
Tablet PC 0	Airport Authority	Dynamic	172.16.0.254	User005
PC15	Flight Service	Dynamic	172.18.51.8	Fc001
PC16	Flight Service	Dynamic	172.18.51.8	Fc002
PC17	Flight Service	Dynamic	172.18.51.8	Fc003
PC18	Flight Service	Dynamic	172.18.51.8	Fc004

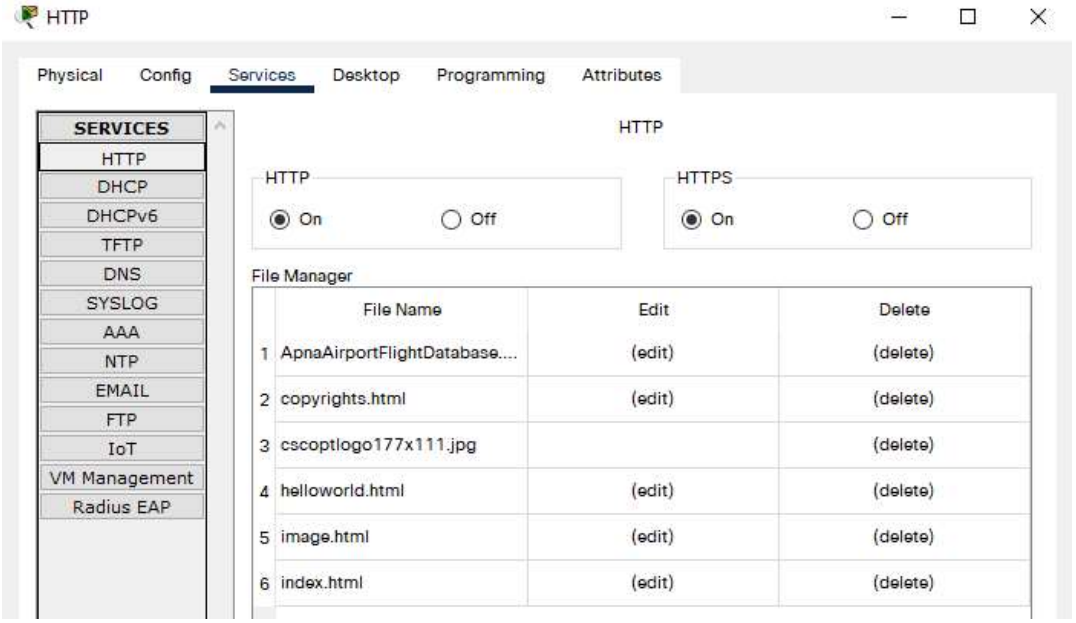
Network Configuration Details

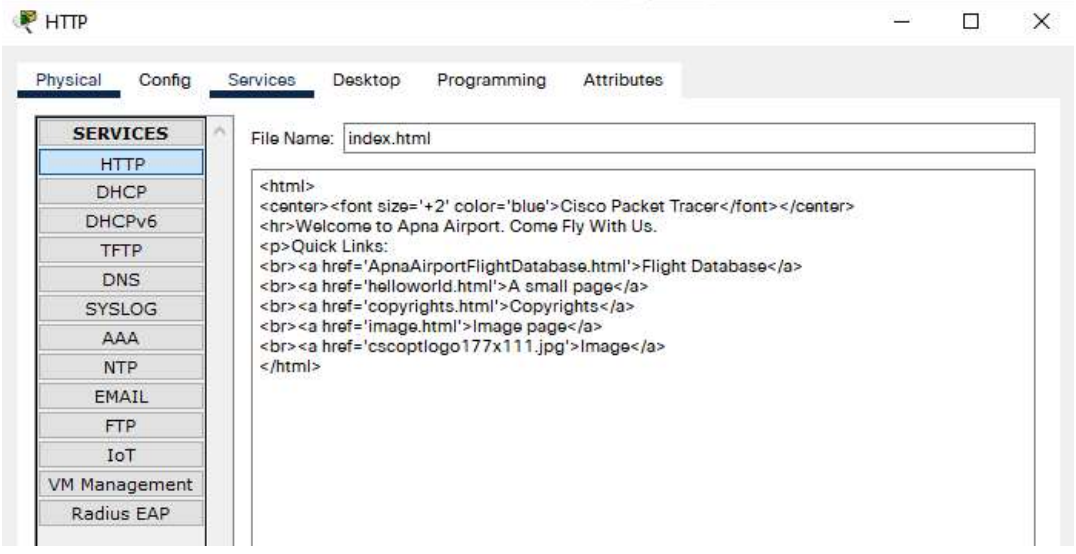
1. **Airport Authority**



Authority has absolute control and command over all the Servers, Users and Service Providers in any of the network. Each User in Authority network is assumed to be staff person and is assigned IP dynamically using DHCP Authority and have access to configure all the server configured as above in topology. The zone contains both wired and wireless devices controlled via same Multilayer Switch. The screenshots of configurations for this zone are attached below:


SMTP
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
EMAIL
SMTP Service
ON
OFF
POP3 Service
ON
OFF
Domain Name:
airportmail.com
Set
User Setup
User
Password
user001
user002
user003
user004
user005


HTTP
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
HTTP
HTTP
On
Off
HTTPS
On
Off
File Manager
File Name
Edit
Delete
1 ApnaAirportFlightDatabase.... (edit) (delete)
2 copyrights.html (edit) (delete)
3 cscoptlogo177x111.jpg (delete)
4 helloworld.html (edit) (delete)
5 image.html (edit) (delete)
6 index.html (edit) (delete)


HTTP
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
File Name:
index.html
<html>
Cisco Packet Tracer
<hr>Welcome to Apna Airport. Come Fly With Us.
<p>Quick Links:

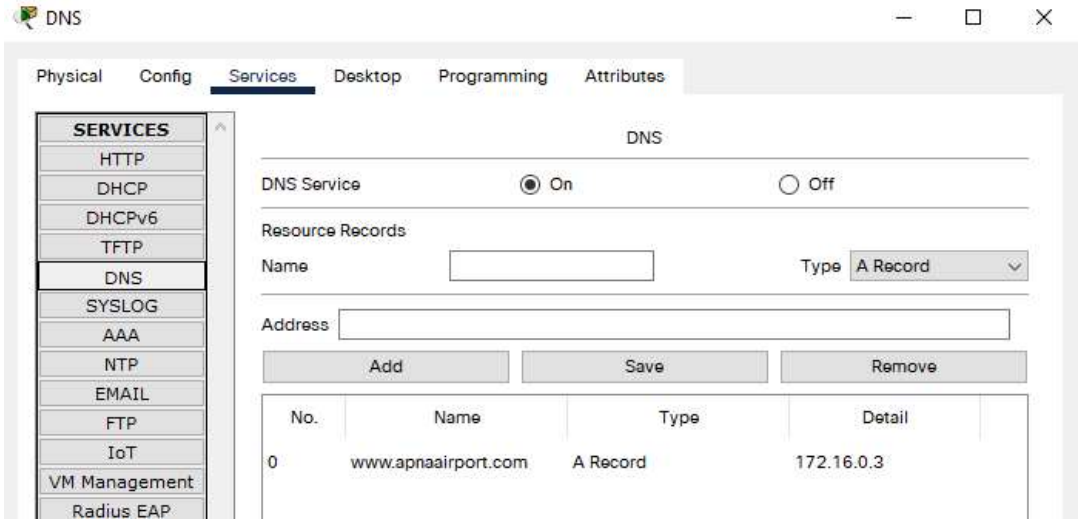
Flight Database

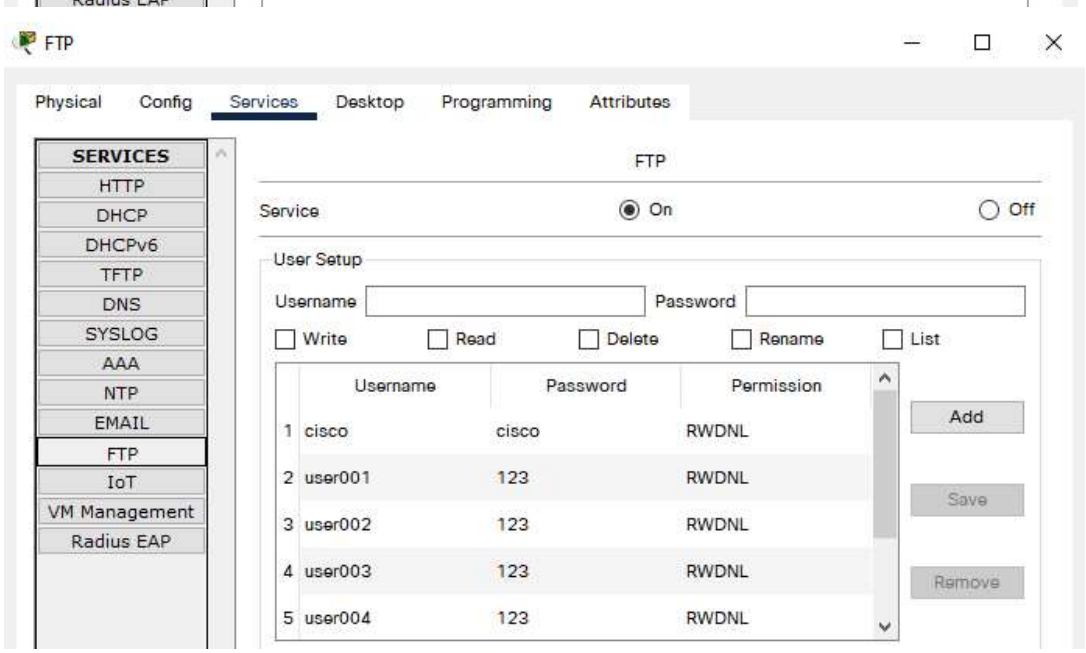
A small page

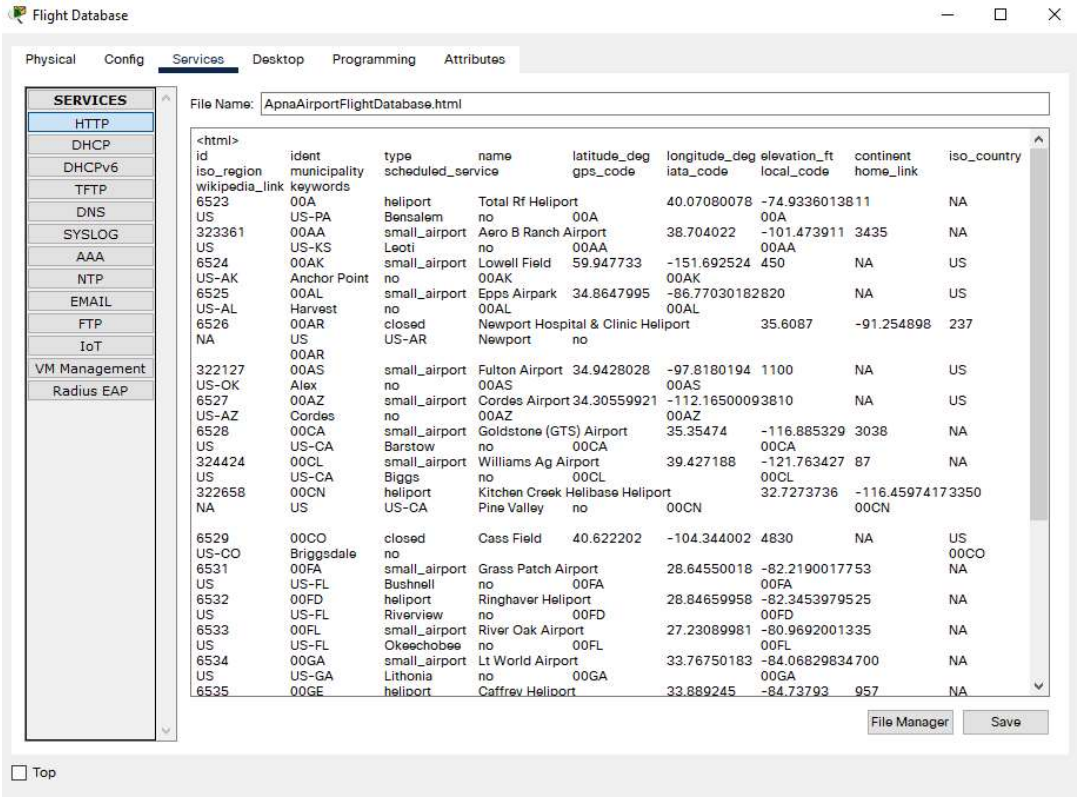
Copyrights

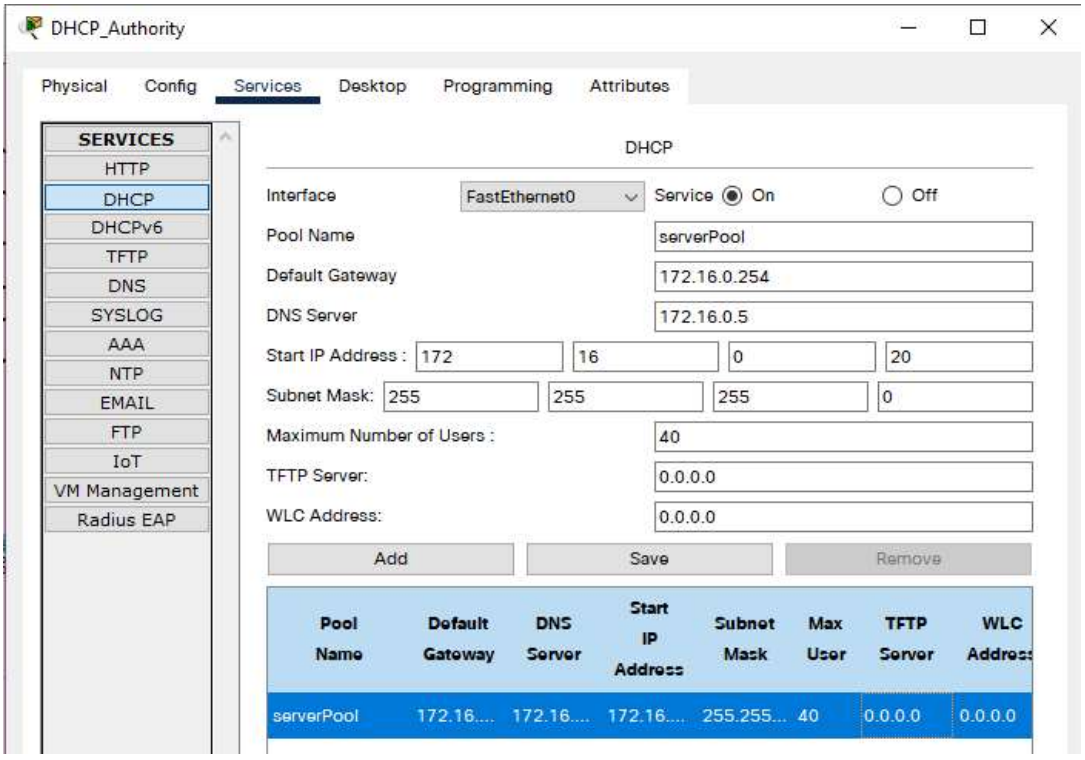
Image page

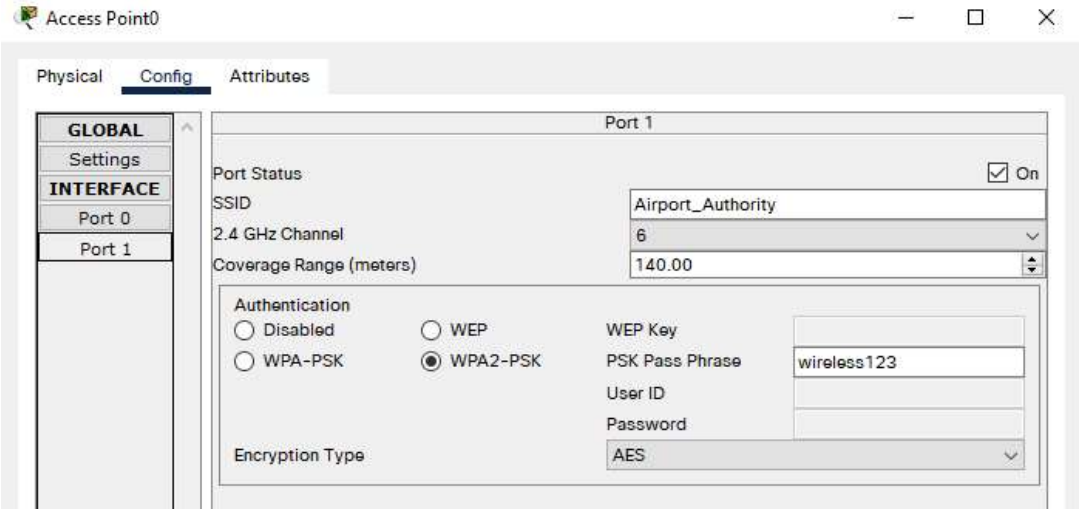
Image
</html>


DNS
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
DNS
DNS Service
On
Off
Resource Records
Name
Type
A Record
Address
Add
Save
Remove
No.
Name
Type
Detail
0
www.apnaairport.com
A Record
172.16.0.3

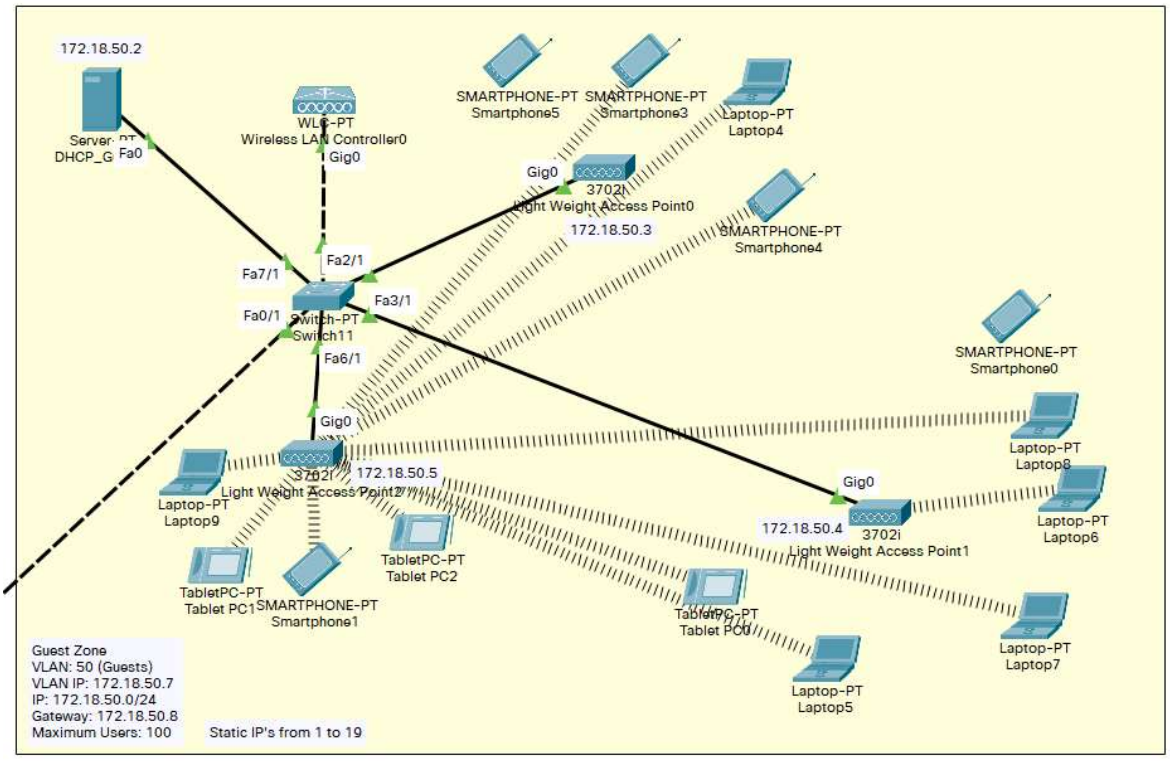

FTP
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
FTP
Service
On
Off
User Setup
Username
Password
Write
Read
Delete
Rename
List
Username
Password
Permission
1 cisco cisco RWDNL
2 user001 123 RWDNL
3 user002 123 RWDNL
4 user003 123 RWDNL
5 user004 123 RWDNL
Add
Save
Remove


Flight Database
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
File Name: ApnaAirportFlightDatabase.html
<html>
id ident type name latitude_deg longitude_deg elevation_ft continent iso_country
iso_region municipality scheduled_service gps_code iata_code local_code home_link
wikipedia_link keywords
6523 00A heliport Total Rf Heliport 40.07080078 -74.93360138 11 NA
US US-PA Bensalem no 00A 00A
323361 00AA small_airport Aero B Ranch Airport 38.704022 -101.473911 3435 NA
US US-KS Leoti no 00AA 00AA
6524 00AK small_airport Lowell Field 59.947733 -151.692524 450 NA US
US-AK Anchor Point no 00AK 00AK
6525 00AL small_airport Epps Airpark 34.8647995 -86.77030182 820 NA US
US-AL Harvest no 00AL 00AL
6526 00AR closed Newport Hospital & Clinic Heliport 35.6087 -91.254898 237
NA US US-AR Newport no
00AR
322127 00AS small_airport Fulton Airport 34.9428028 -97.8180194 1100 NA US
US-OK Alex no 00AS 00AS
6527 00AZ small_airport Cordes Airport 34.30559921 -112.1650009 3810 NA US
US-AZ Cordes no 00AZ 00AZ
6528 00CA small_airport Goldstone (GTS) Airport 35.35474 -116.885329 3038 NA
US US-CA Barstow no 00CA 00CA
324424 00CL small_airport Williams Ag Airport 39.427188 -121.763427 87 NA
US US-CA Biggs no 00CL 00CL
322658 00CN heliport Kitchen Creek Helibase Heliport 32.7273736 -116.4597417 3350
NA US US-CA Pine Valley no 00CN 00CN
6529 00CO closed Cass Field 40.622202 -104.344002 4830 NA US
US-CO Briggsdale no 00CO
6531 00FA small_airport Grass Patch Airport 28.64550018 -82.21900175 3 NA
US US-FL Bushnell no 00FA 00FA
6532 00FD heliport Ringhaver Heliport 28.84659958 -82.34539795 25 NA
US US-FL Riverview no 00FD 00FD
6533 00FL small_airport River Oak Airport 27.23089981 -80.96920013 35 NA
US US-FL Okeechobee no 00FL 00FL
6534 00GA small_airport Lt World Airport 33.76750183 -84.06829834 700 NA
US US-GA Lithonia no 00GA 00GA
6535 00GE heliport Caffrey Heliport 33.889245 -84.73793 957 NA
File Manager
Save
Top


DHCP_Authority
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 172.16.0.254
DNS Server 172.16.0.5
Start IP Address : 172 16 0 20
Subnet Mask: 255 255 255 0
Maximum Number of Users : 40
TFTP Server: 0.0.0.0
WLC Address: 0.0.0.0
Add
Save
Remove
Pool Name
Default Gateway
DNS Server
Start IP Address
Subnet Mask
Max User
TFTP Server
WLC Address
serverPool 172.16.... 172.16.... 172.16.... 255.255... 40 0.0.0.0 0.0.0.0

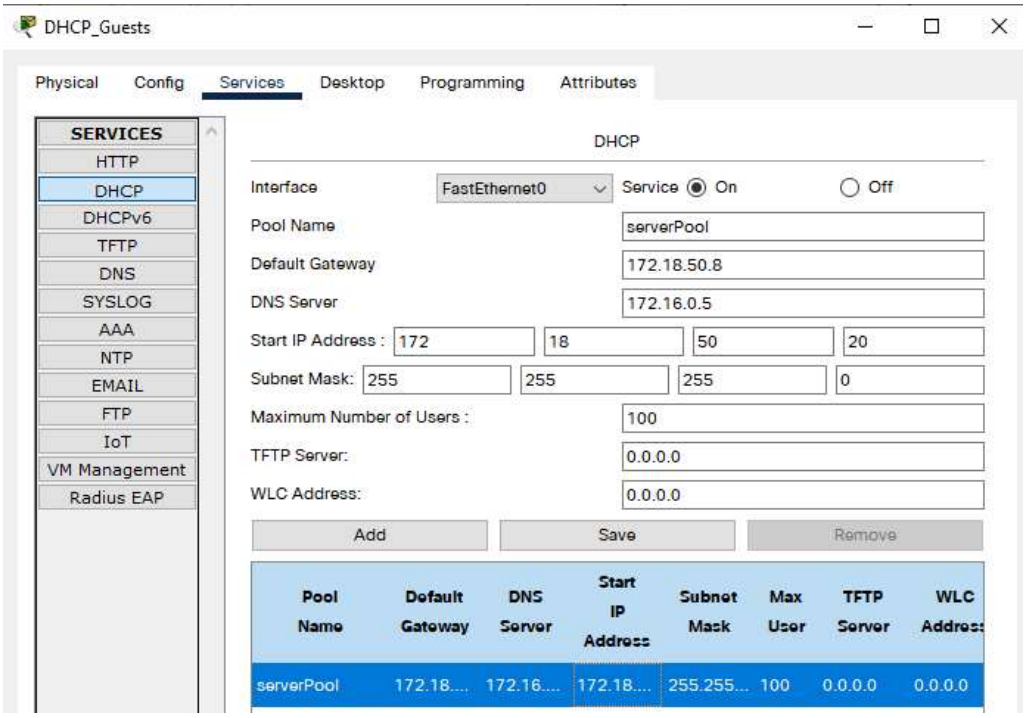


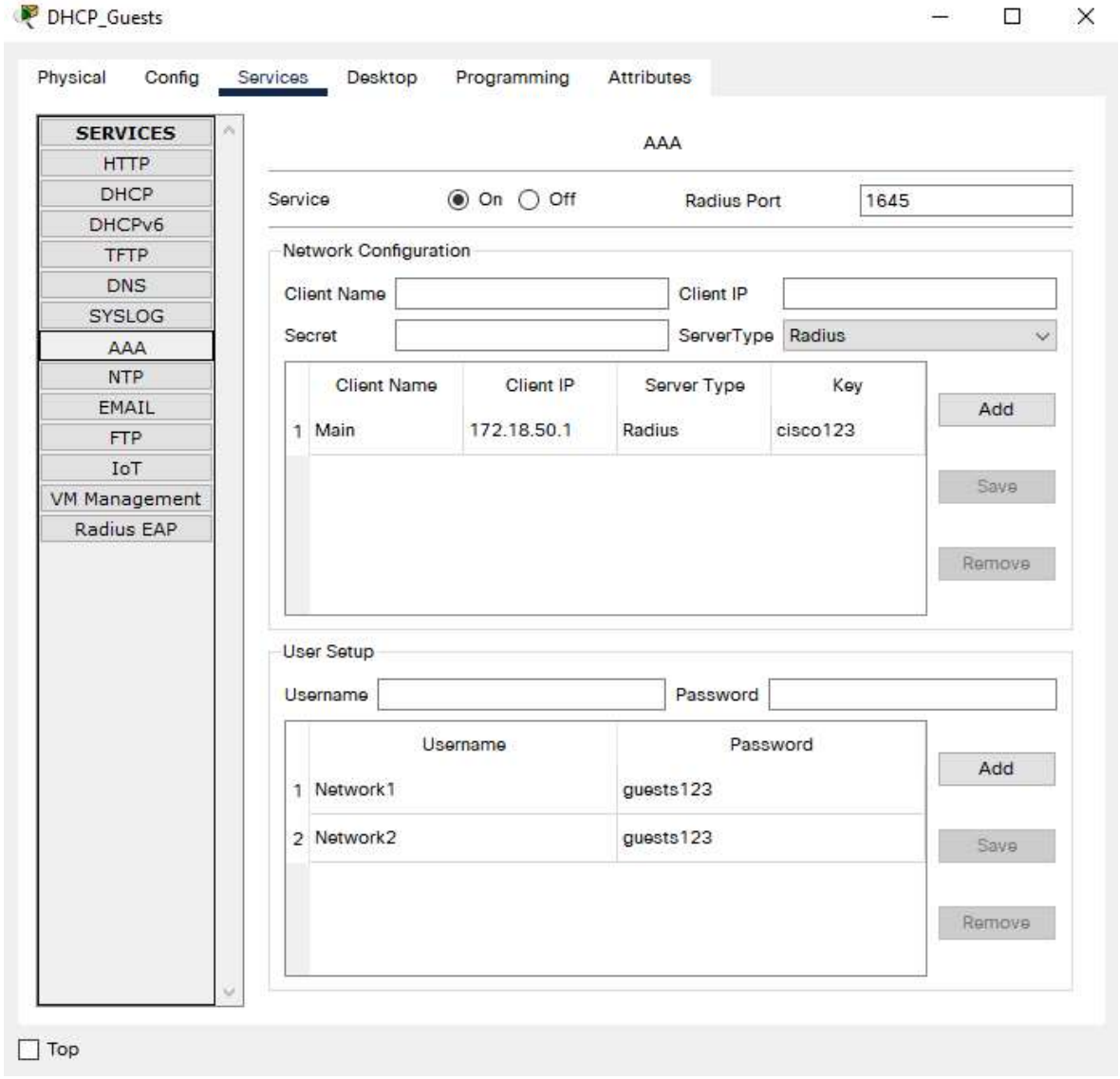
2. Guest Zone

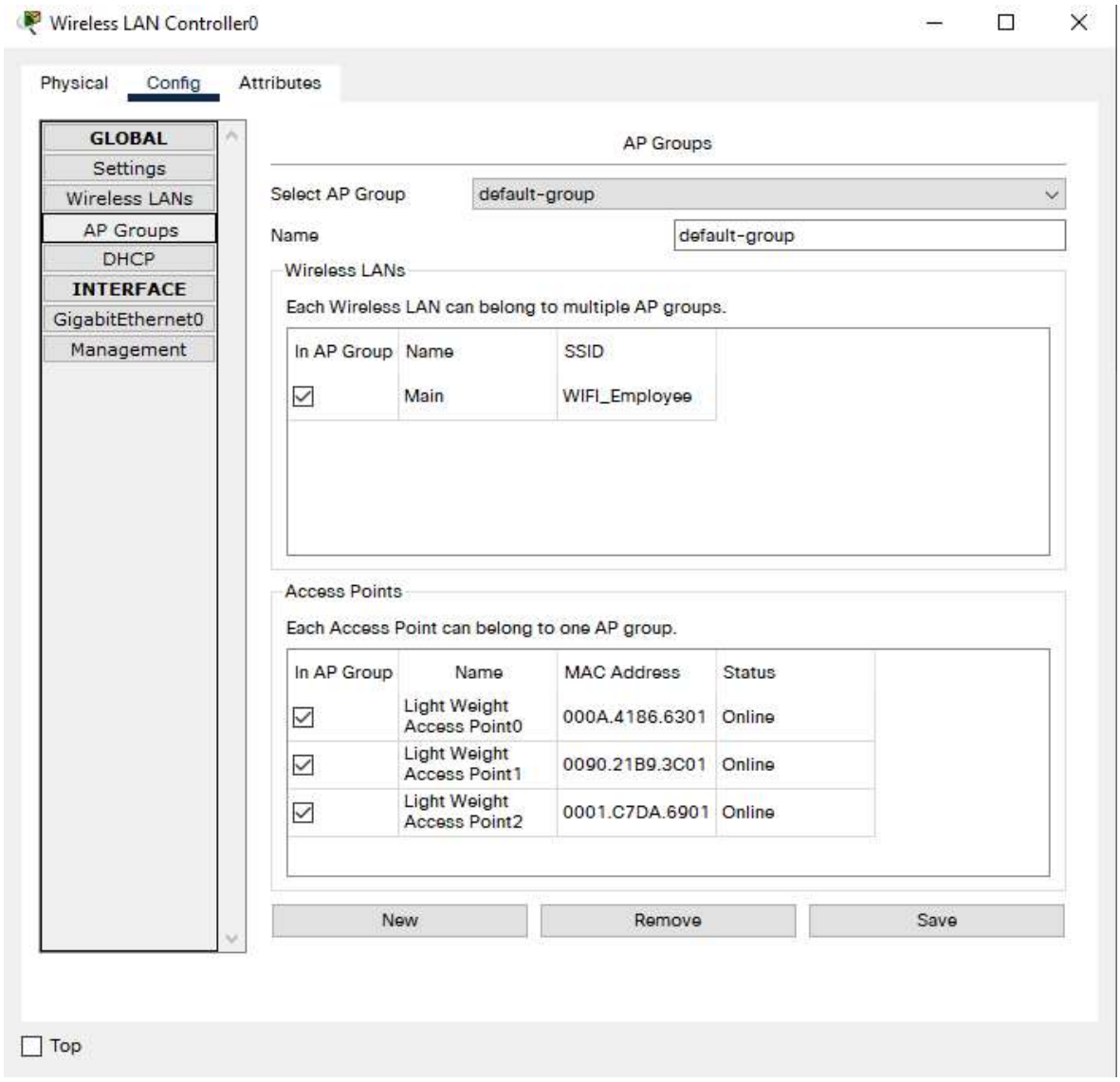


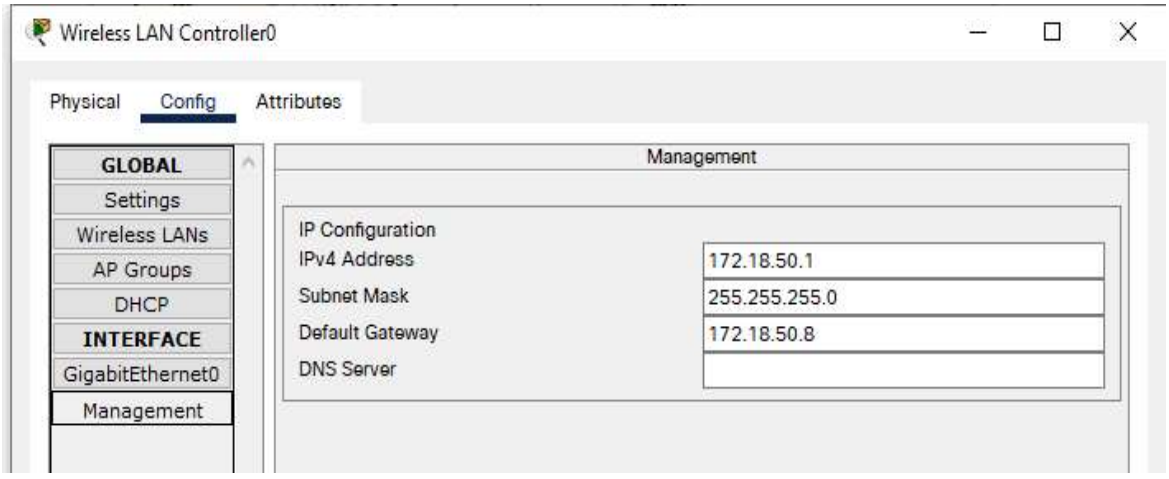
Guests are only permitted to access HTTP Server to access browsing within the Authority Zone. Guests are assigned IP using DHCP Guests. Single Wireless LAN Controller is used to control all the access points in Guest Zone, each of which have varying coverage and static IP assigned to it. Single Wireless LAN Controller allows to configure SSD, Pass, AAA Authentication, DHCP on single device. All devices in this

zone are wireless and are assumed to be simple passengers in the network. This network is created on VLAN 50 with other configuration details shown below:

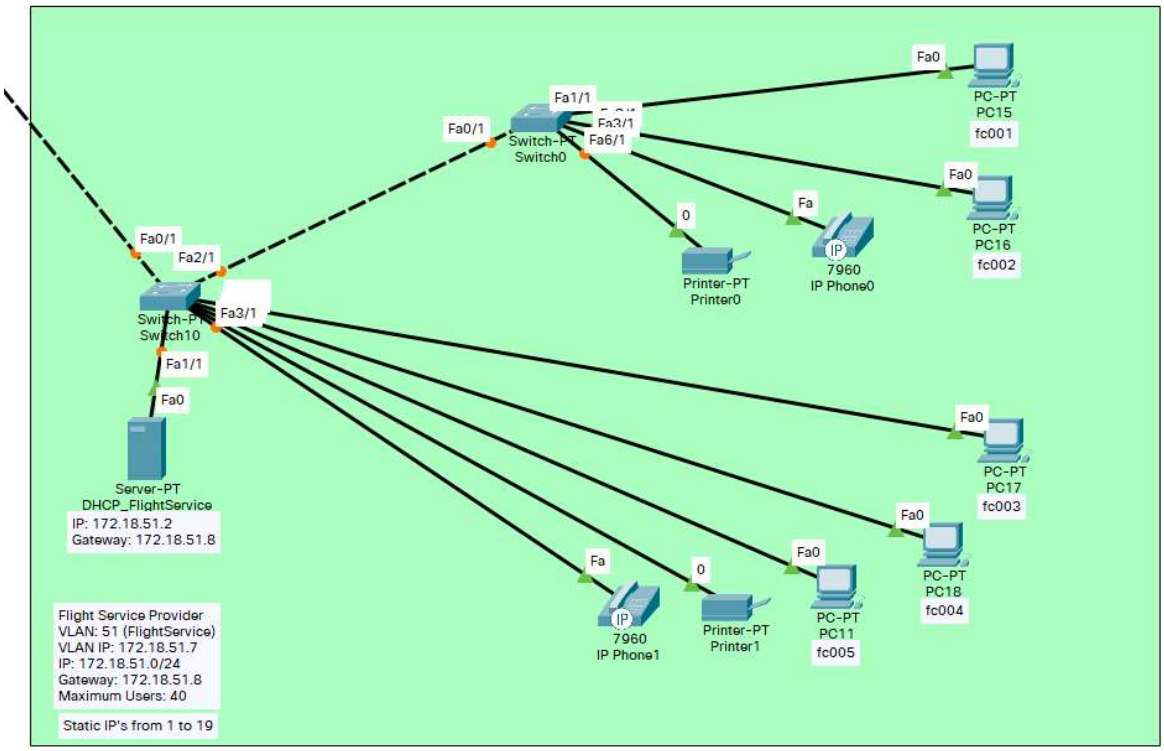



DHCP_Guests
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
AAA
Service
On
Off
Radius Port
1645
Network Configuration
Client Name
Client IP
Secret
ServerType
Radius
Client Name
Client IP
Server Type
Key
1
Main
172.18.50.1
Radius
cisco123
Add
Save
Remove
User Setup
Username
Password
Username
Password
1
Network1
guests123
2
Network2
guests123
Add
Save
Remove
Top

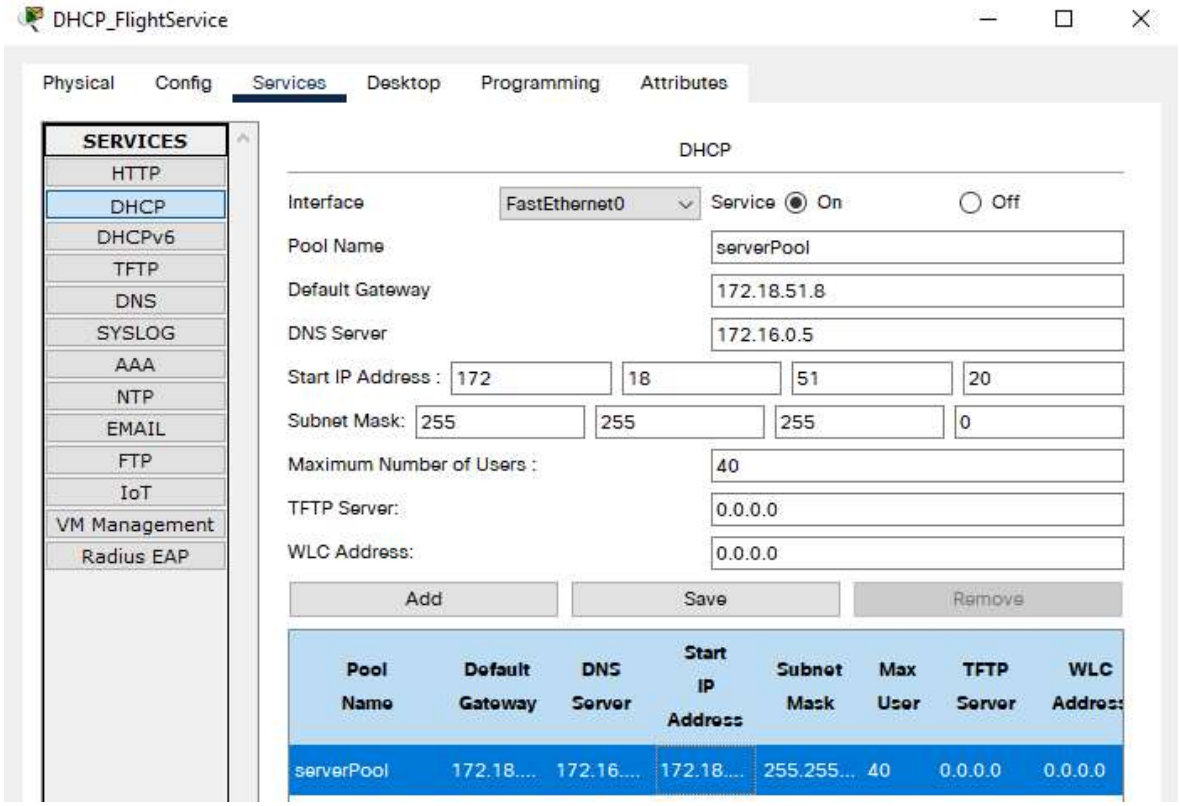




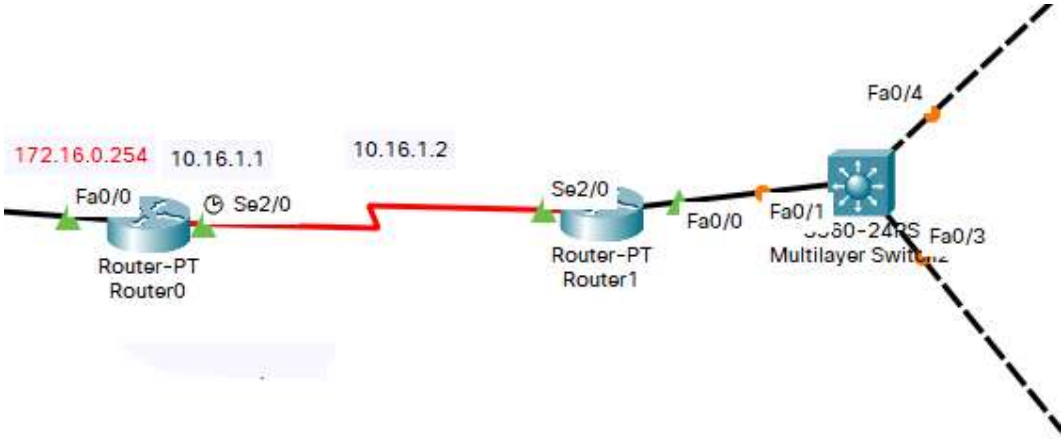
3. **Flight Service Provider**



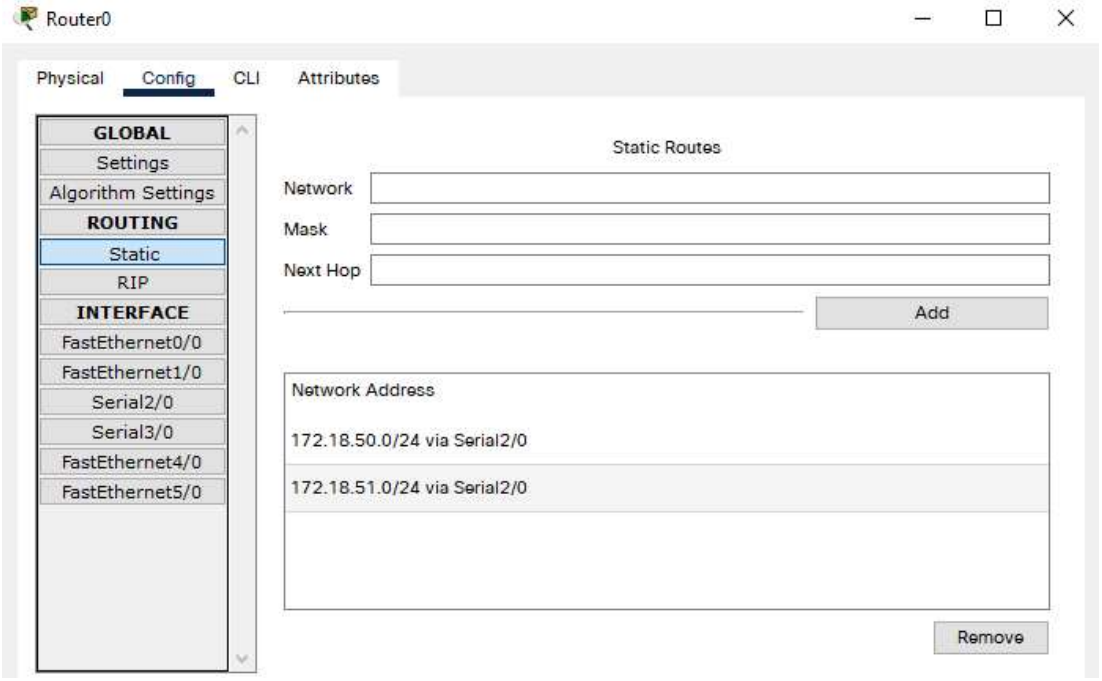
This zone contain staff responsible for managing Flight Database and should only have access to the Flight Database Server within Authority Network to access the Flight Schedules, Users Details, Departure Details, Routing etc. Multiple users in this network are assigned User Address by the Flight Database Server as FCuser001 etc. They are able to modify the Flight Database by having permission of read, write, delete, overwrite etc. This network is created on VLAN 51 with other configuration details attached below:

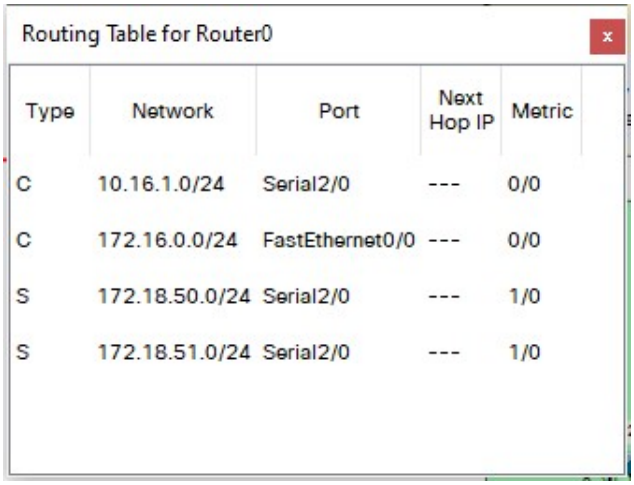

DHCP_FlightService
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
DHCP
Interface
FastEthernet0
Service
On
Off
Pool Name
serverPool
Default Gateway
172.18.51.8
DNS Server
172.16.0.5
Start IP Address :
172
18
51
20
Subnet Mask:
255
255
255
0
Maximum Number of Users :
40
TFTP Server:
0.0.0.0
WLC Address:
0.0.0.0
Add
Save
Remove
Pool Name
Default Gateway
DNS Server
Start IP Address
Subnet Mask
Max User
TFTP Server
WLC Address
serverPool
172.18....
172.16....
172.18....
255.255...
40
0.0.0.0
0.0.0.0

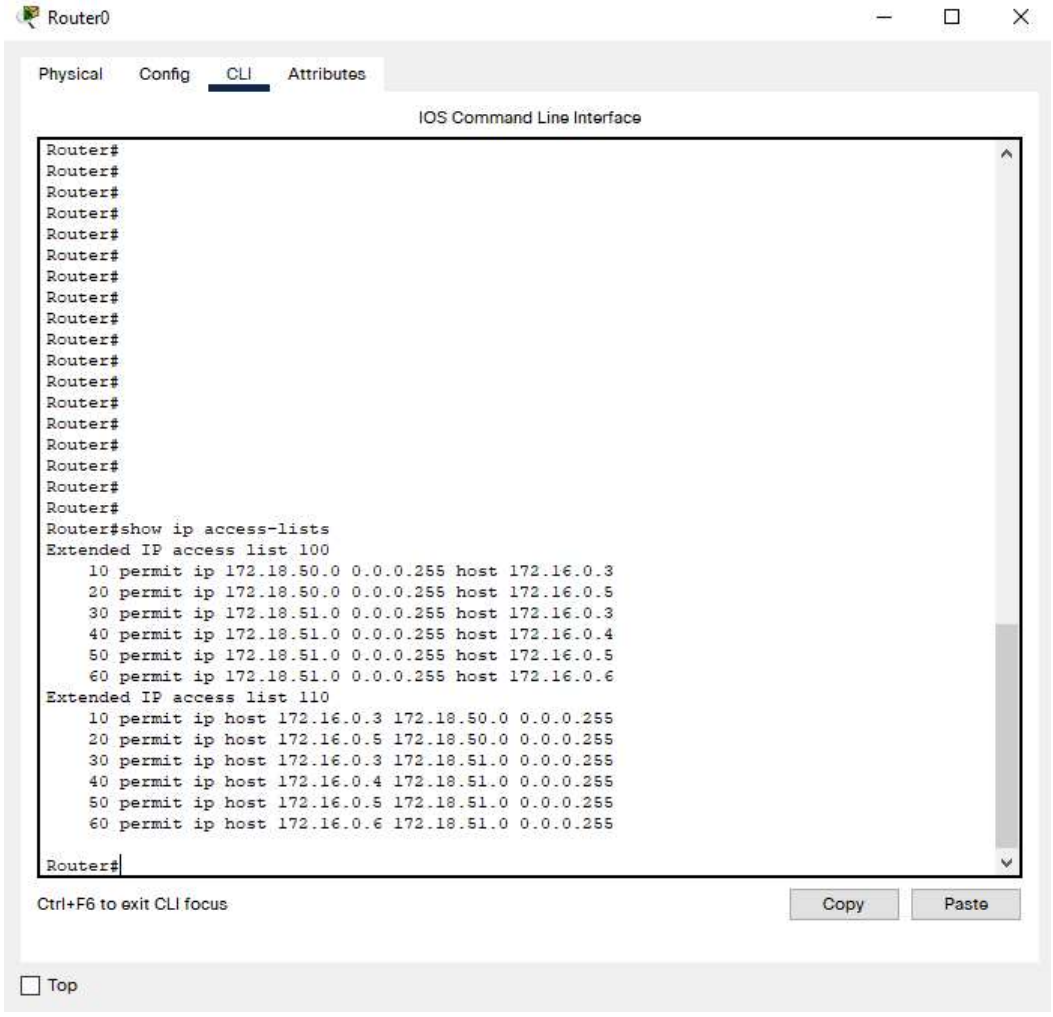
4. Intermediate Zone

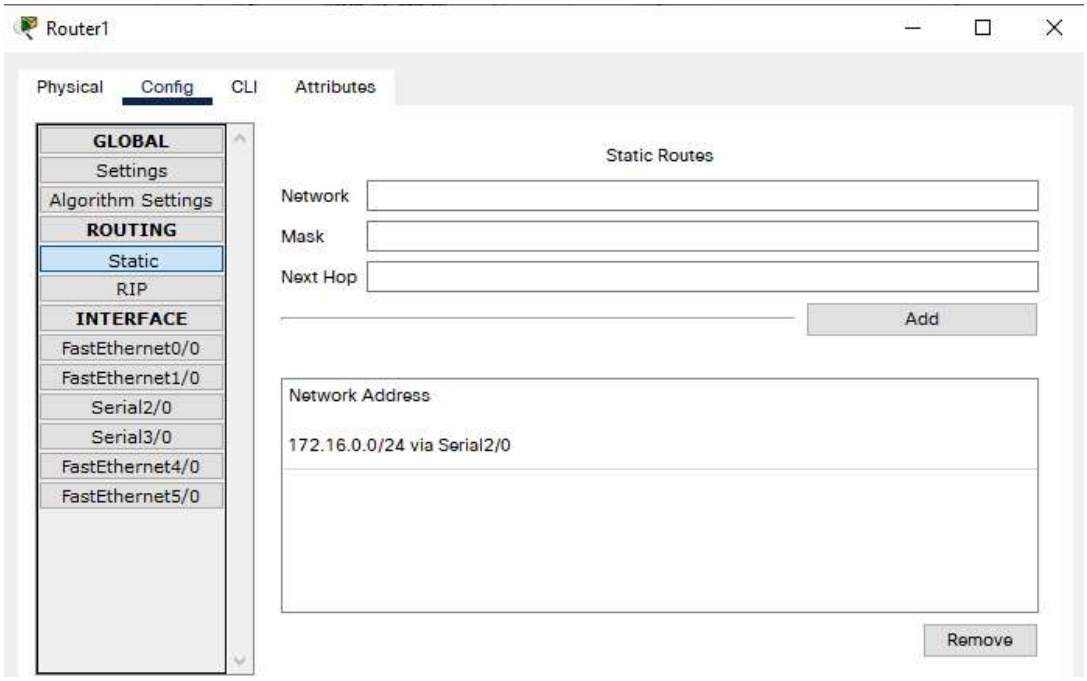


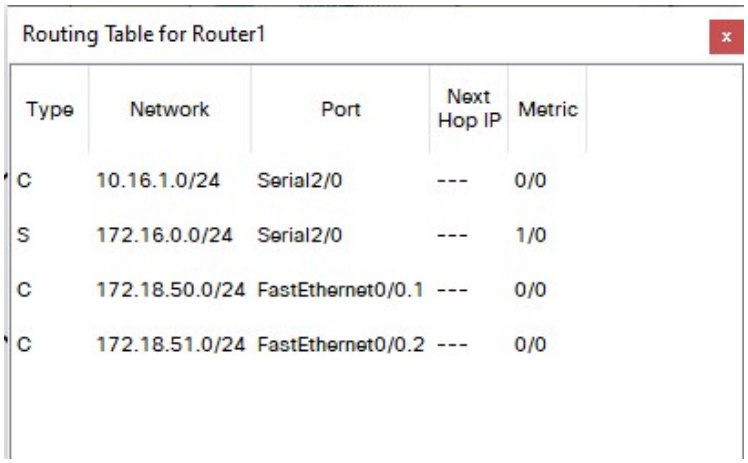
This Zone contains two routers and a Multilayer Switch and is responsible for interconnecting all the Zones together. The Gateways are configured on this network having own IP of 10.16.0.0. The VLANs 50 and 51 are configured here along with encapsulation dot1q for the Inter VLAN routing. The Static routing protocol is also defined here. The Access Control List (ACL) is also configured here which deny Flight Control Access to Guests, permits both the Flight Service and Guests to HTTP and DNS server and Flight Service is additionally permitted to Flight Database. No users in either of three networks are allowed to intercommunicate directly. The configuration for all the tasks are mentioned below with results and verification in next section:

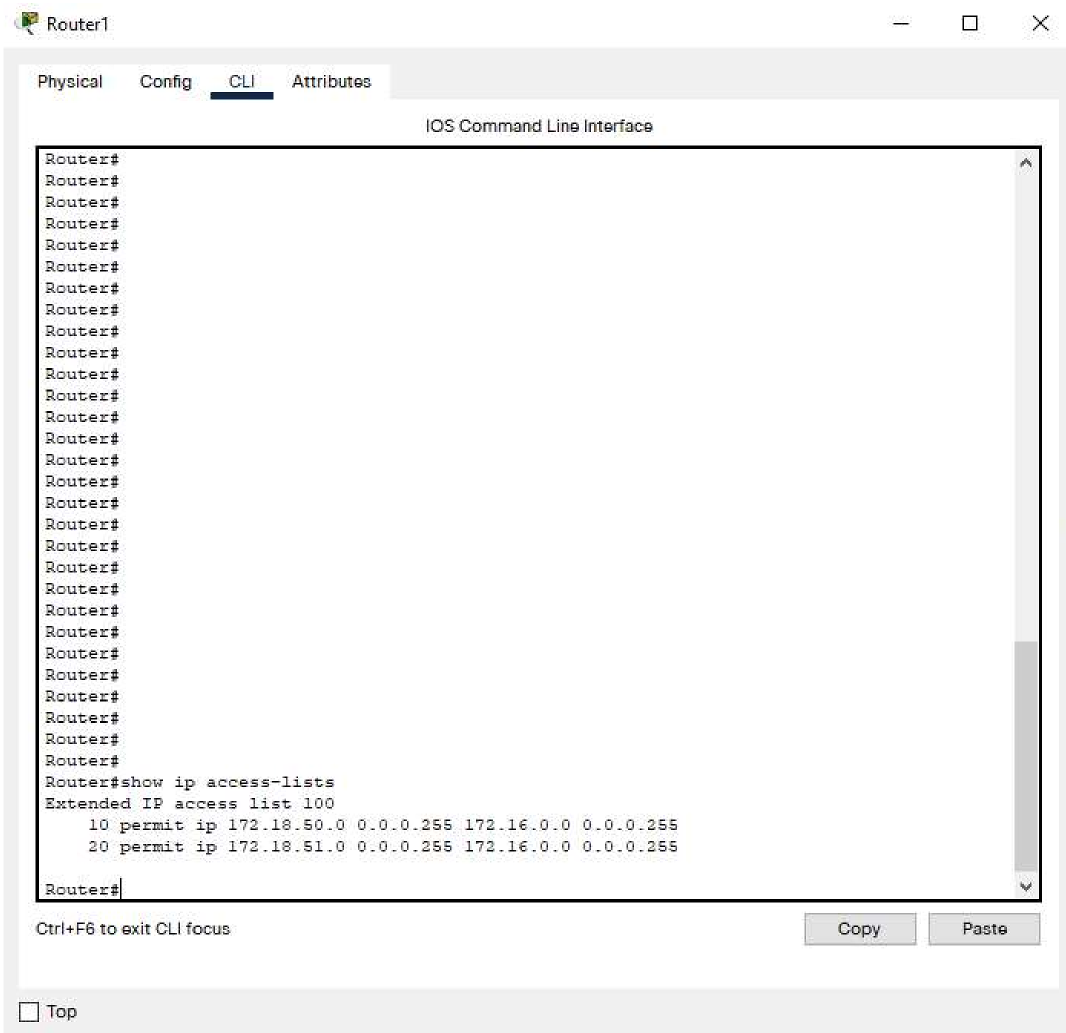

Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet1/0
Serial2/0
Serial3/0
FastEthernet4/0
FastEthernet5/0
Static Routes
Network
Mask
Next Hop
Add
Network Address
172.18.50.0/24 via Serial2/0
172.18.51.0/24 via Serial2/0
Remove

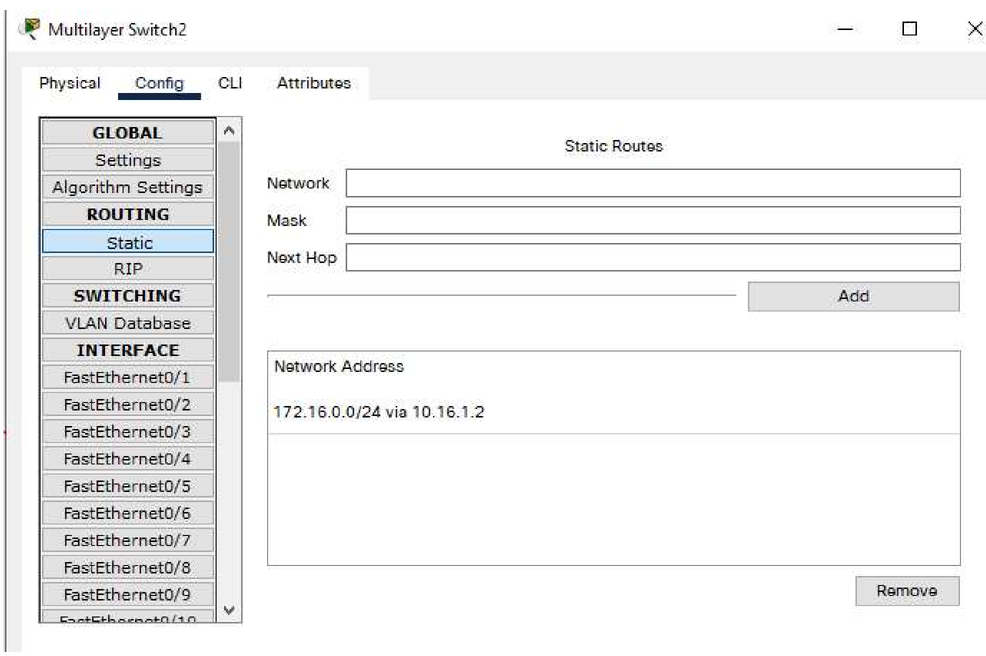

Routing Table for Router0
Type
Network
Port
Next Hop IP
Metric
C 10.16.1.0/24 Serial2/0 --- 0/0
C 172.16.0.0/24 FastEthernet0/0 --- 0/0
S 172.18.50.0/24 Serial2/0 --- 1/0
S 172.18.51.0/24 Serial2/0 --- 1/0

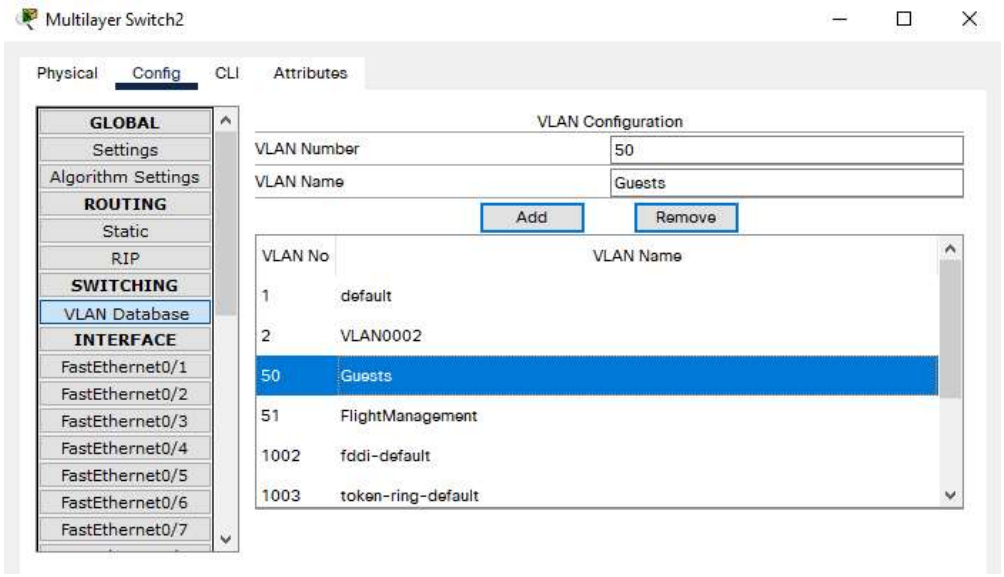

Router0
Physical
Config
CLI
Attributes
IOS Command Line Interface
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#show ip access-lists
Extended IP access list 100
10 permit ip 172.18.50.0 0.0.0.255 host 172.16.0.3
20 permit ip 172.18.50.0 0.0.0.255 host 172.16.0.5
30 permit ip 172.18.51.0 0.0.0.255 host 172.16.0.3
40 permit ip 172.18.51.0 0.0.0.255 host 172.16.0.4
50 permit ip 172.18.51.0 0.0.0.255 host 172.16.0.5
60 permit ip 172.18.51.0 0.0.0.255 host 172.16.0.6
Extended IP access list 110
10 permit ip host 172.16.0.3 172.18.50.0 0.0.0.255
20 permit ip host 172.16.0.5 172.18.50.0 0.0.0.255
30 permit ip host 172.16.0.3 172.18.51.0 0.0.0.255
40 permit ip host 172.16.0.4 172.18.51.0 0.0.0.255
50 permit ip host 172.16.0.5 172.18.51.0 0.0.0.255
60 permit ip host 172.16.0.6 172.18.51.0 0.0.0.255
Router#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top


Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet1/0
Serial2/0
Serial3/0
FastEthernet4/0
FastEthernet5/0
Static Routes
Network
Mask
Next Hop
Add
Network Address
172.16.0.0/24 via Serial2/0
Remove


Routing Table for Router1
Type
Network
Port
Next Hop IP
Metric
C 10.16.1.0/24 Serial2/0 --- 0/0
S 172.16.0.0/24 Serial2/0 --- 1/0
C 172.18.50.0/24 FastEthernet0/0.1 --- 0/0
C 172.18.51.0/24 FastEthernet0/0.2 --- 0/0


Router1
Physical
Config
CLI
Attributes
IOS Command Line Interface
Router#
Router#show ip access-lists
Extended IP access list 100
10 permit ip 172.18.50.0 0.0.0.255 172.16.0.0 0.0.0.255
20 permit ip 172.18.51.0 0.0.0.255 172.16.0.0 0.0.0.255
Router#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top


Multilayer Switch2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/1
FastEthernet0/2
FastEthernet0/3
FastEthernet0/4
FastEthernet0/5
FastEthernet0/6
FastEthernet0/7
FastEthernet0/8
FastEthernet0/9
Static Routes
Network
Mask
Next Hop
Add
Network Address
172.16.0.0/24 via 10.16.1.2
Remove

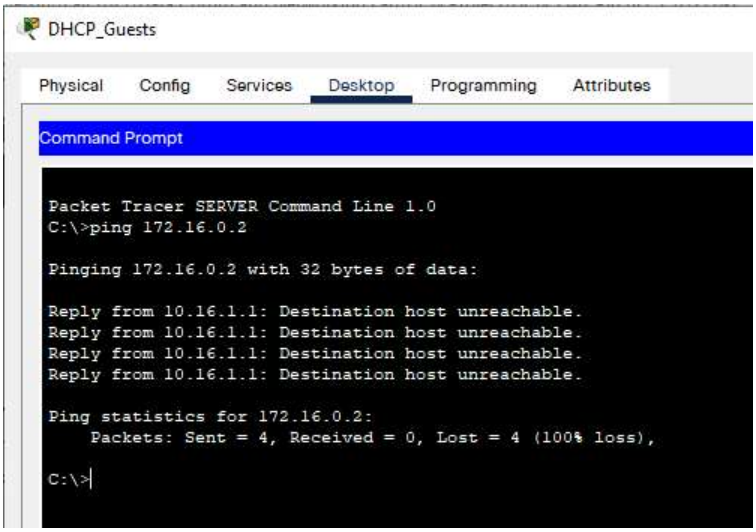

Multilayer Switch2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/1
FastEthernet0/2
FastEthernet0/3
FastEthernet0/4
FastEthernet0/5
FastEthernet0/6
FastEthernet0/7
VLAN Configuration
VLAN Number
50
VLAN Name
Guests
Add
Remove
VLAN No
VLAN Name
1
default
2
VLAN0002
50
Guests
51
FlightManagement
1002
fddi-default
1003
token-ring-default

Verification and Testing

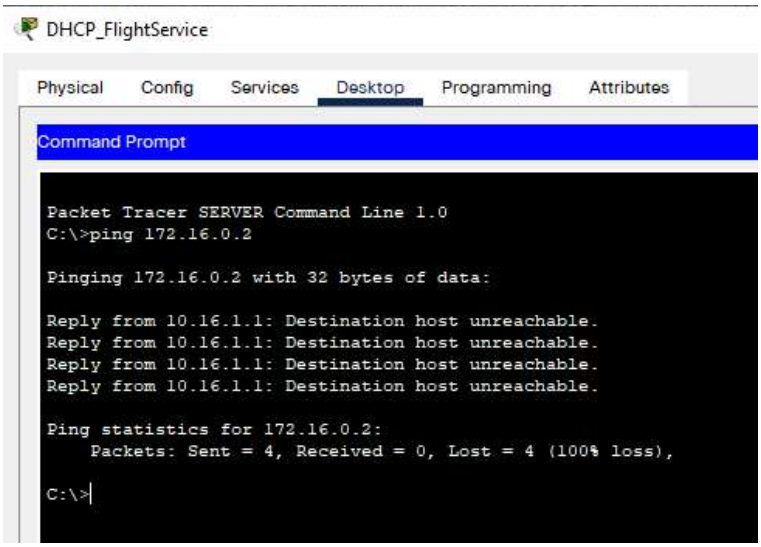
We must first demonstrate that no communication takes place between the Guest and Flight Service Provider (FSP) VLANs. This can be demonstrated by pinging two different workstations between the VLANs. For convenience, we will show the ping result between the DHCP server in the Guest VLAN and the DHCP server in the FSP VLAN.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)
	Failed	DHCP_FlightService	DHCP_Guests	ICMP		0.000

We can also demonstrate that, no workstation in the Guest and FSP VLAN can access the internal network of the Airport Authority (AA), except for the designated servers[1]. To demonstrate this, we shall show the ping result from the DHCP servers in Guest and FSP VLAN, to the Simple Mail Transfer Protocol (SMTP) server in the AA VLAN. The SMTP server manages the corporate email service in the AA only. The following result will demonstrate successful access restriction.

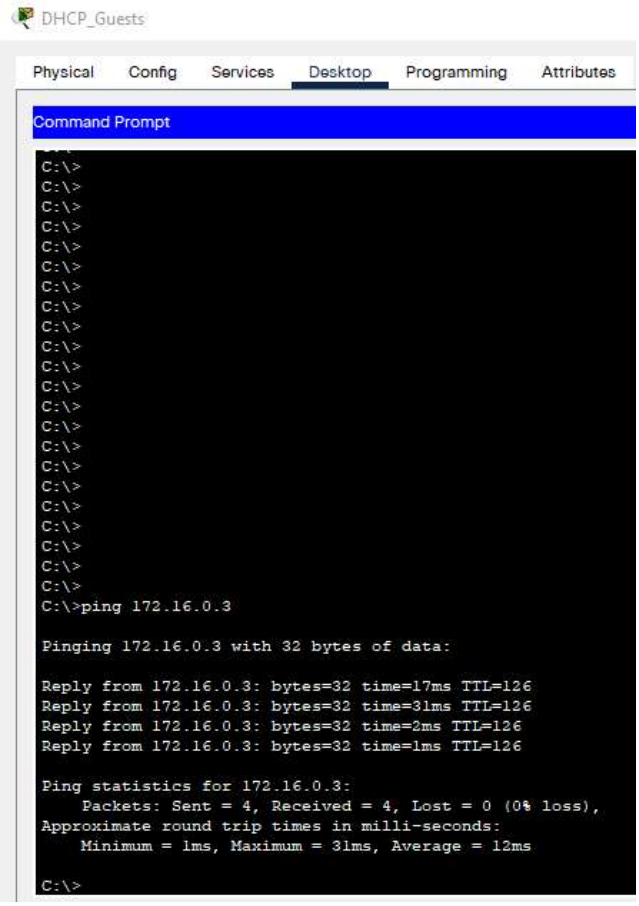


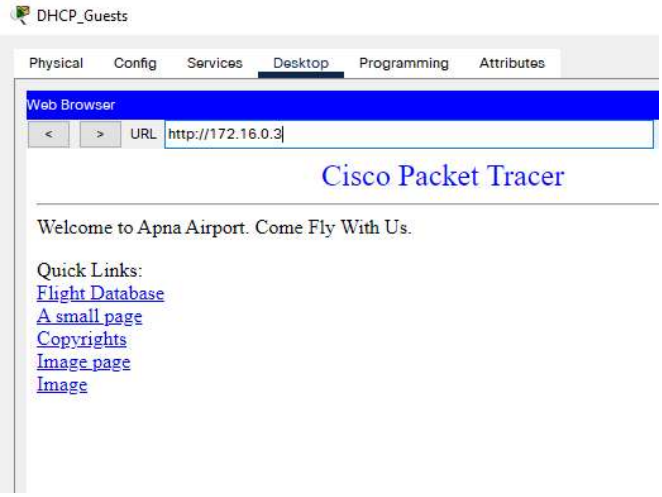
[1] To reiterate: the Guest VLAN can only access the DNS serve and HTTP server; the FSP VLAN can access DNS, HTTP, FTP and Flight Database server.



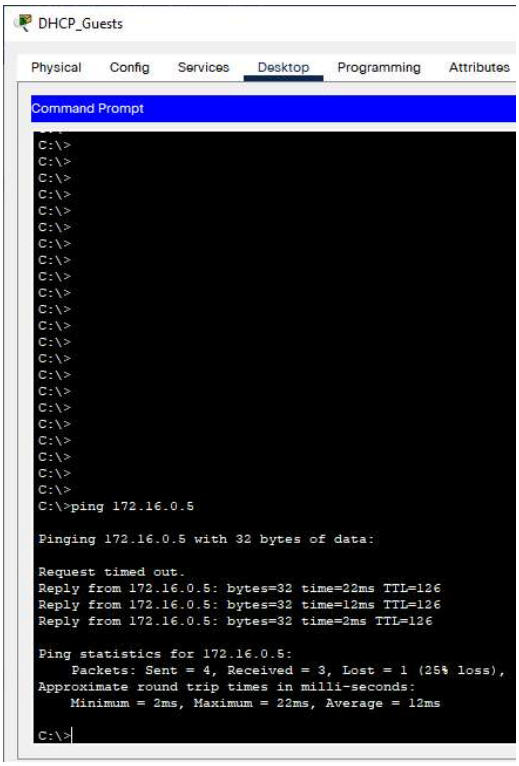
Communication between the designated servers and clients in all the VLAN's is happening successfully:

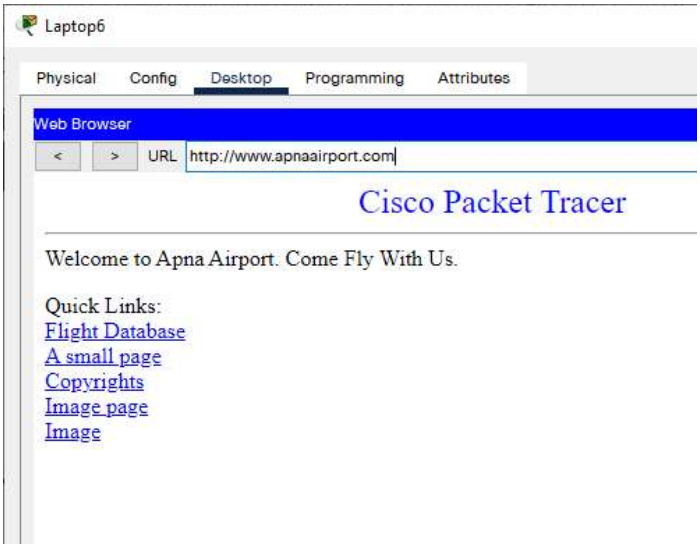
1. **Guest VLAN to HTTP**



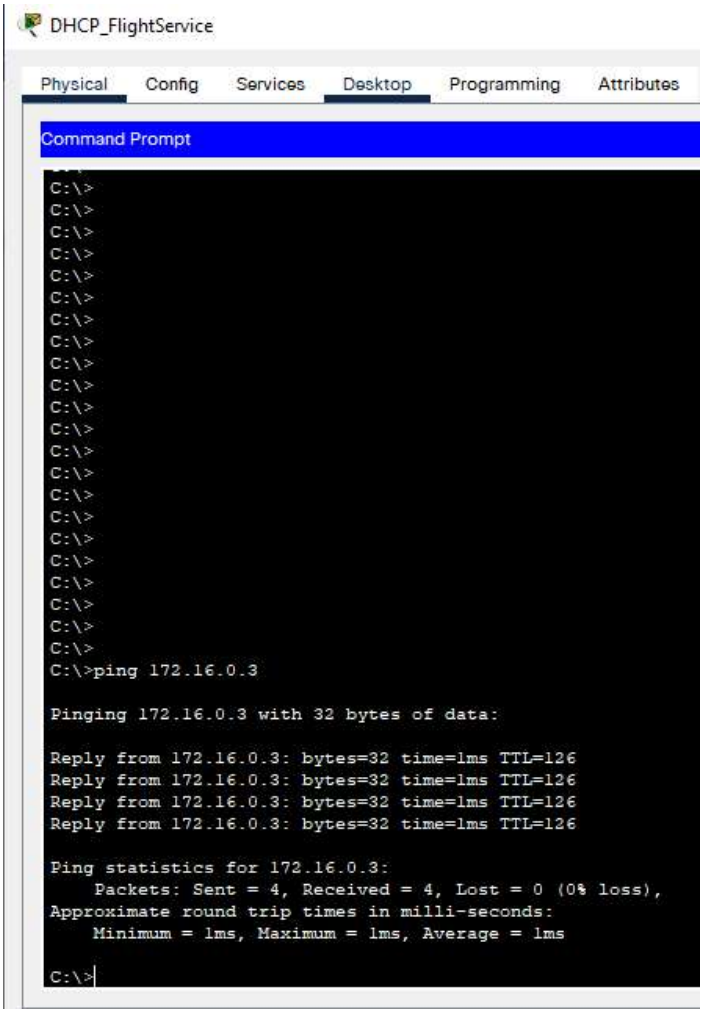


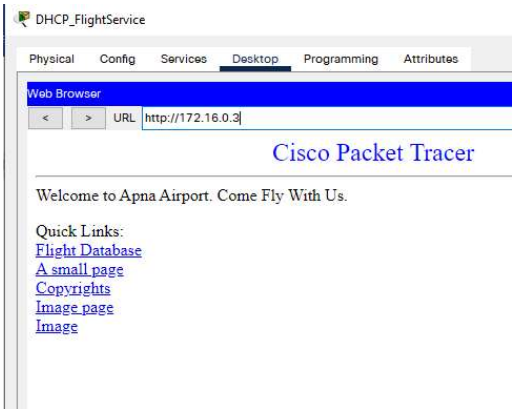
2. Guest VLAN to DNS



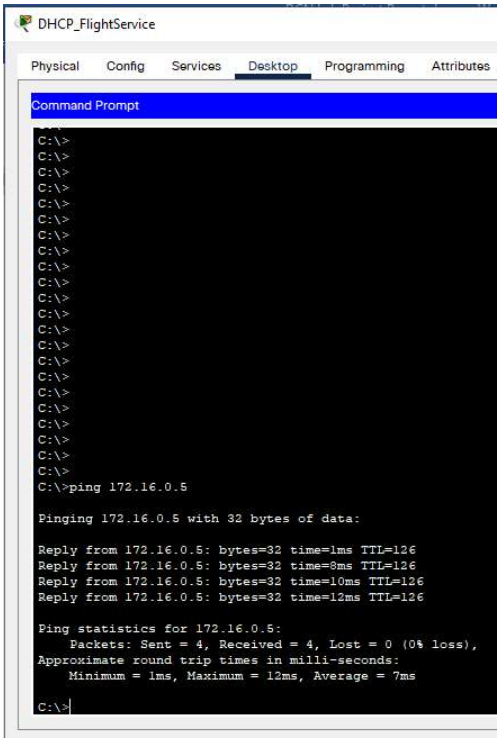


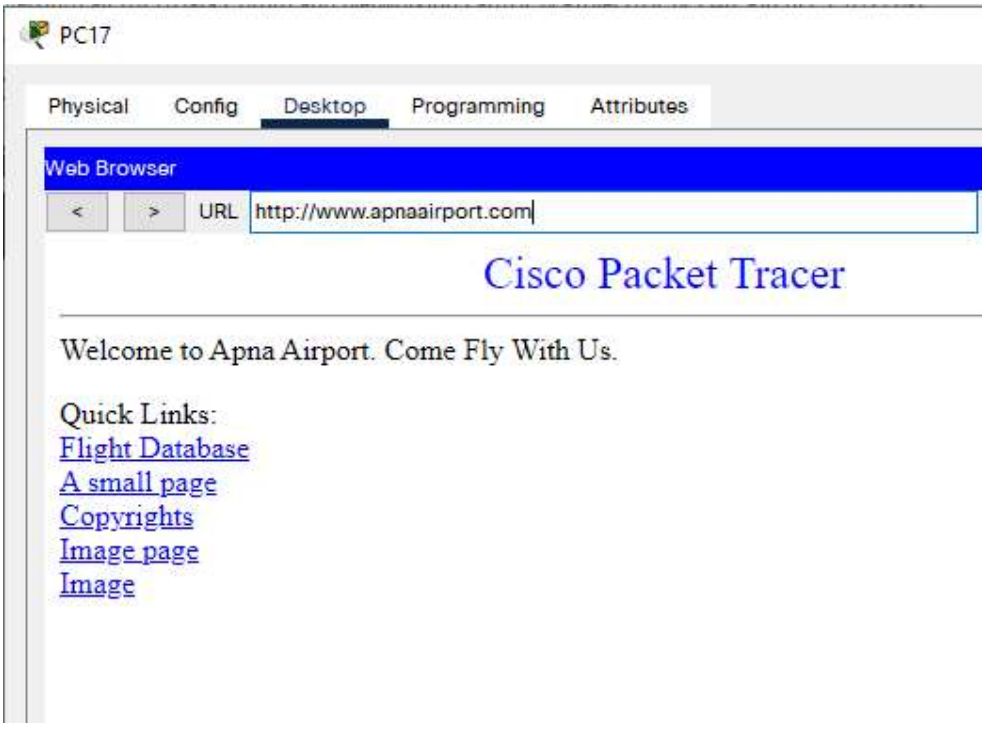
3. **FSP VLAN to HTTP**



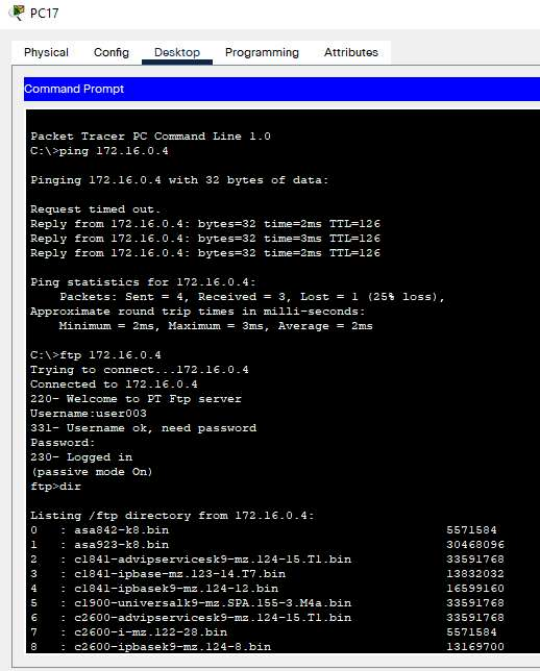


4. FSP VLAN to DNS

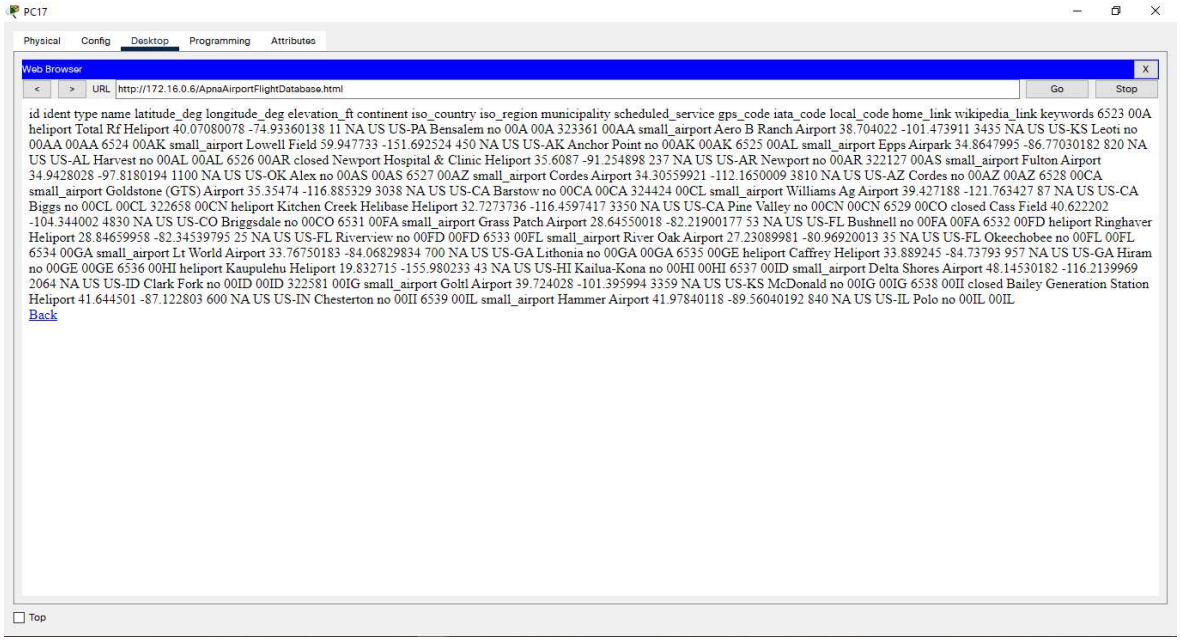




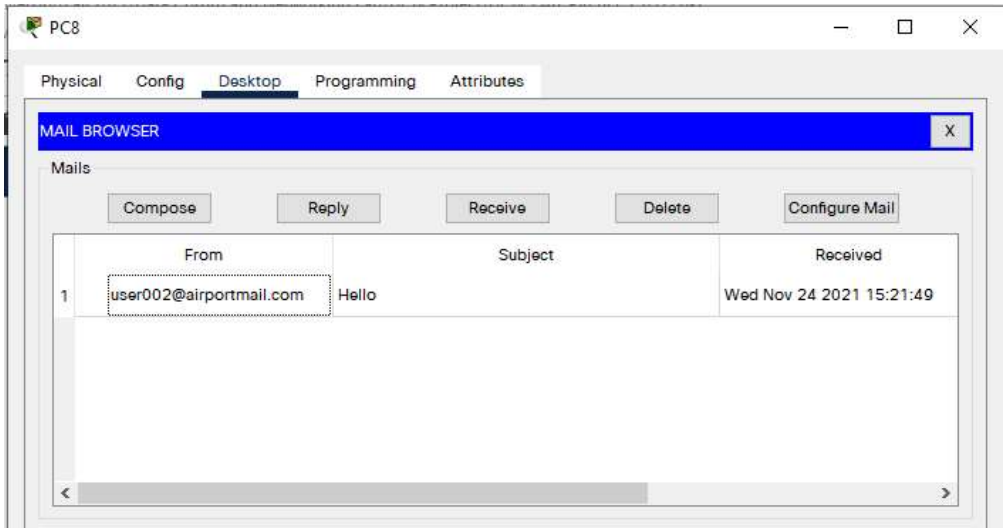
5. **FSP VLAN to FTP**



6. FSP VLAN to Flight Database server



The corporate email service is also online within the AA VLAN is also functional:



Thus, we have demonstrated the main services and access restriction as proposed in the proposal document.

Conclusion and Future Work

For this project, we intend to cater the potential SCADA threat at airports by establishing Internet connection in the airport for guests to be temporary by nature, and so the main challenge in catering to cater to providing around 100 guests access to the internet on-the-fly, would be through ad-hoc networks. In setting up those networks, two types of wireless access topologies can be implemented: the Basic Service Set (BSS) and the Extended Service Set (ESS), as laid out by the IEEE 802.11 standard. In an airport setting, ESS would be typically employed to increase the coverage area and reduce down-time during handover mode. Some key parameters to measure the reliability of the internet are [2]:

1. Average Packet Residence Time (APRT) in the network is the time a packet spends within a network.
2. Successfully received packets within a network.
3. Packet dropping probability.
4. Throughput.

These will be the network related parameters, and an analysis of these can ascertain a network's efficiency adequately, but there are other parameters that lie outside the scope of this project, like battery consumption of smartphones and laptops that guests use. In future, the above SCADA modelling can be performed in context of Airport Enterprise Network [4].

References

1. J. McCarthy and W. Mahoney, “SCADA threats in the modern airport,” International Journal of Cyber Warfare and Terrorism (IJCWT), vol. 3, no. 4, pp. 32–39, 2013.
2. I. E. Ahmed, B. R. Qazi and J. M. H. Elmirghani, "Performance Analysis of an Ad Hoc Network in the INtelligent Airport," 2010 Fourth International Conference on Next Generation Mobile Applications, Services and Technologies, 2010, pp. 198-202, doi: 10.1109/NGMAST.2010.47.
3. “Smart Airport Agile Network,” Huawei.com. [Online]. Available: https://e.huawei.com/ae/solutions/industries/transportation/smart-aviation/agile-network. [Accessed: 31-Oct-2021].
4. S. E. Zaharia and C. V. Pietreanu, “Challenges in airport digital transformation,” Transportation Research Procedia, vol. 35, pp. 90–99, 2018.