Project 3: Network Design Proposal for Airport

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

Introduction

The aim of this project would be to design and implement communication network for airports with performance parameters being security, quality and reliability. The project will explore various utilities to construct a highly secure network for airport which includes crucial operations ranging from flight timing control, airplanes coordination, passenger services etc.

The potential utilities for such a network would include hardware firewalls, IP access control, MAC address port security, domain servers, proxy servers, failover firewall utility, Pre-boot Execution Environment (PXE) server, a Dynamic Host Configuration Protocol (DHCP) server, a Domain Name System (DNS) and cabled connections. These utilities will have to be 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 will aim to establish a communication network for an airport. The network will be able to facilitate three groups namely Airport Authority, Flight Service Providers (FSP's) and Guest Members. Each group will be assigned appropriate network privileges and functionality to perform relevant tasks and will be allocated appropriate service over the network. The Airport Authority and Flight Service Provider will have their respective servers while the guests would only be allowed to connect to the internet using either Wireless or Ethernet based connectivity. The project will implement appropriate yet scaled-down measures of cybersecurity, such as cabled connections, virtual LANs, subnetting, firewall 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.

For our project, we intend to cater the above 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.

Project Description

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.

Networking Requirements are as follows:

1. The active networking components (Routers, switches, wireless access points etc.) with quantity.
2. The IP network design for each department.
3. Creating and mapping IP networks with VLAN's.

4. Analysis, identification and explanation of methodologies to use for access restriction and internet sharing.
5. Dynamic IP addressing design for all the networks.
6. Identify the configuration and features, wherever appropriate, which is required on the active components to setup the network.
7. Network topology diagram.

Networking Requirement

1) Airport Authority: It will be responsible for maintaining the flight management protocols and will also be 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 will be regulated by Airport Authority. There should total be 20 users in this VLAN.
2) Flight Service Providers: This department will be responsible for handling the details of passengers, incoming/outgoing flights and arrival/departure times. There should be total of 40 users in this VLAN.
3) Guest Members: These will be 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 will be most limited to the internal network, which will comprise the flight service providers and airport authority networks. They will virtually only connect to the Internet and not the internal network of the airport. There should be a maximum of 100 users in this VLAN.

Network Design strategy

1) The active networking components will include 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 will already be creating network IDs with suitable subnet [3] masks according to the number of nodes within a network. For example, the different departments can be assigned different private network IDs and private IP addresses. To ensure no communication between the departments, we can configure different VLANs. The IP addresses of the routers in the network will be default gateways for the nodes in the VLANs.
3) The network must 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.

VLAN and IP Network Design

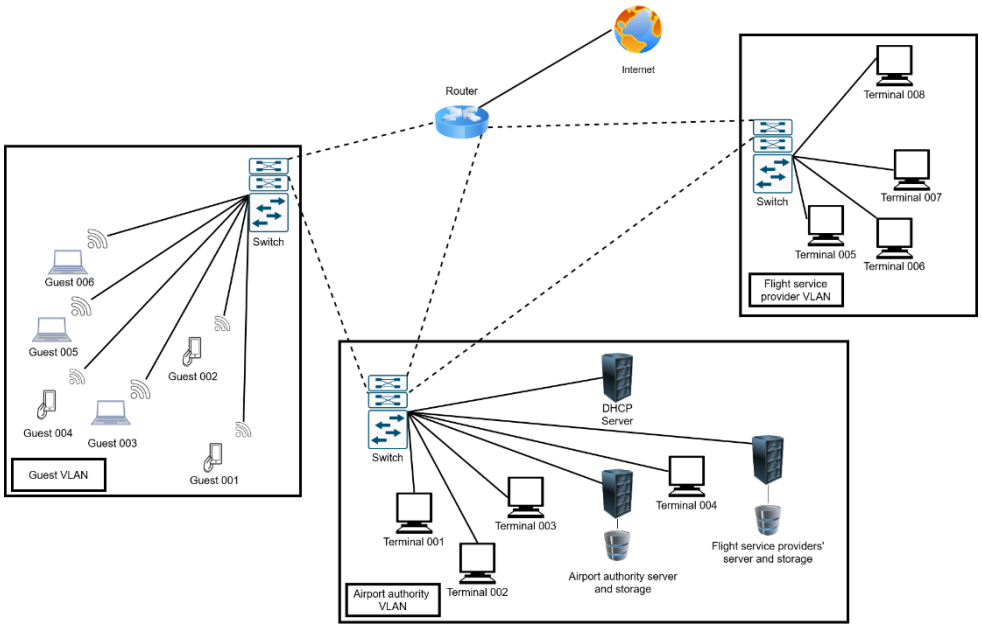
Since we will have three different VLANs, we will require three different network IDs. To create and map those IDs and corresponding IP addresses, we must configure a DHCP server to assign IP addresses with the relevant network ID, to the relevant VLAN nodes.

Requirement analysis of active networking components (Routers, switches, access points, DHCP Server)

As stated above, the network devices will consist of routers, switches, and WAPs for the guest area (since most nodes will most certainly have either smartphones or laptop joining in through Wi-Fi). Furthermore, the network will require routers for internet access, and a DHCP server to allocate network IDs and IP addresses to the VLANs.

Network Topology Diagram

The diagram below shows the first draft of the network topology. It displays the conceptual layout of the topology. The routing to the internet is shown by a single router, although in the final simulation this will be represented by a router. Similarly, the VLAN's are delineated by a single switch, although in the final topology more than one switch may be present in a VLAN.



Network Configuration and guidelines

a. **Switch configuration (VLAN, Trunking)**

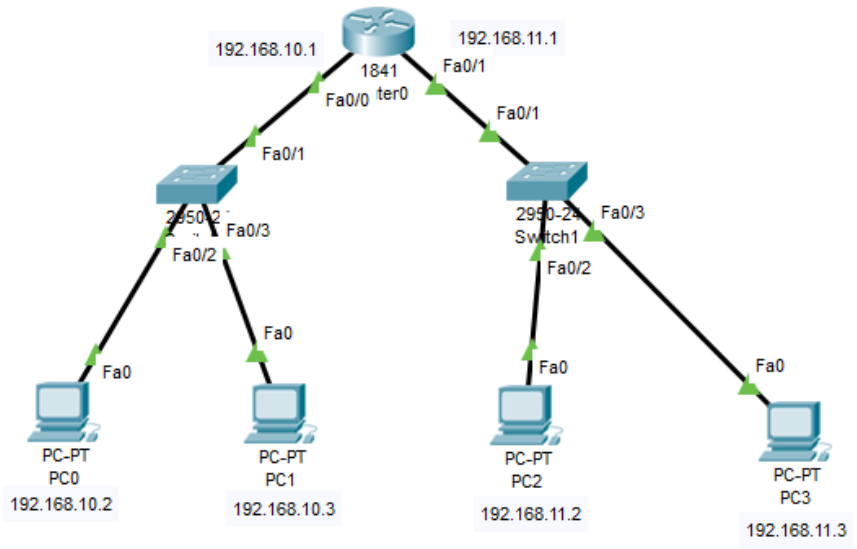
VLAN will allow the administrator, Airport Authority, to subdivide the physical network into individual logical domains to isolate the Guests from the Flight Service Providers. This will be achieved by configuration of Switch to let multiple users in the same VLAN to be able to communicate with each other while different switches will be interconnected using trunk port to connect multiple switches. This configuration will let administrator to logically split the switch for Guests and Flight Service Providers using same hardware while maintaining isolation, security, performances and integrity of network. Typical VLAN configuration for switch will be as follow where VLAN will assigned on particular interface along with their status.

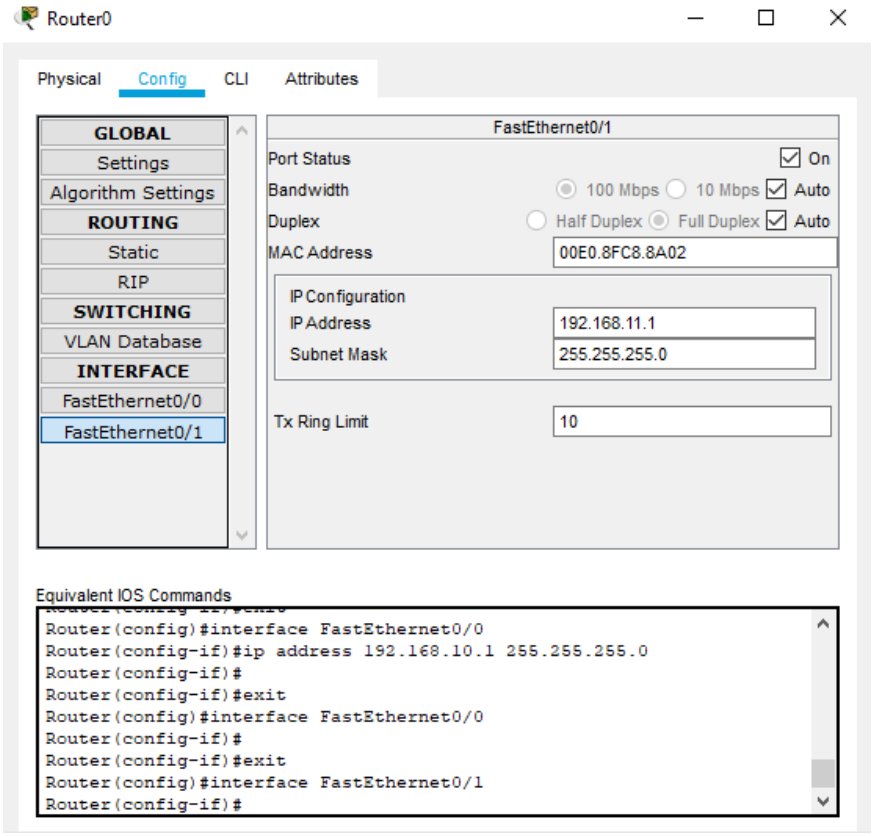
```
Switch#show Vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/4, Fa0/5, Fa0/6, Fa0/7
                                                 Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                 Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                 Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                 Fa0/24, Gig0/1, Gig0/2
10   sales                             active    Fa0/1
20   admin                             active    Fa0/2
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

```
Switch#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/3       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/3       10,20

Port        Vlans allowed and active in management domain
Fa0/3       10,20

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/3       10,20
```

b. **Router configuration (VLAN sub interface, Access lists)**

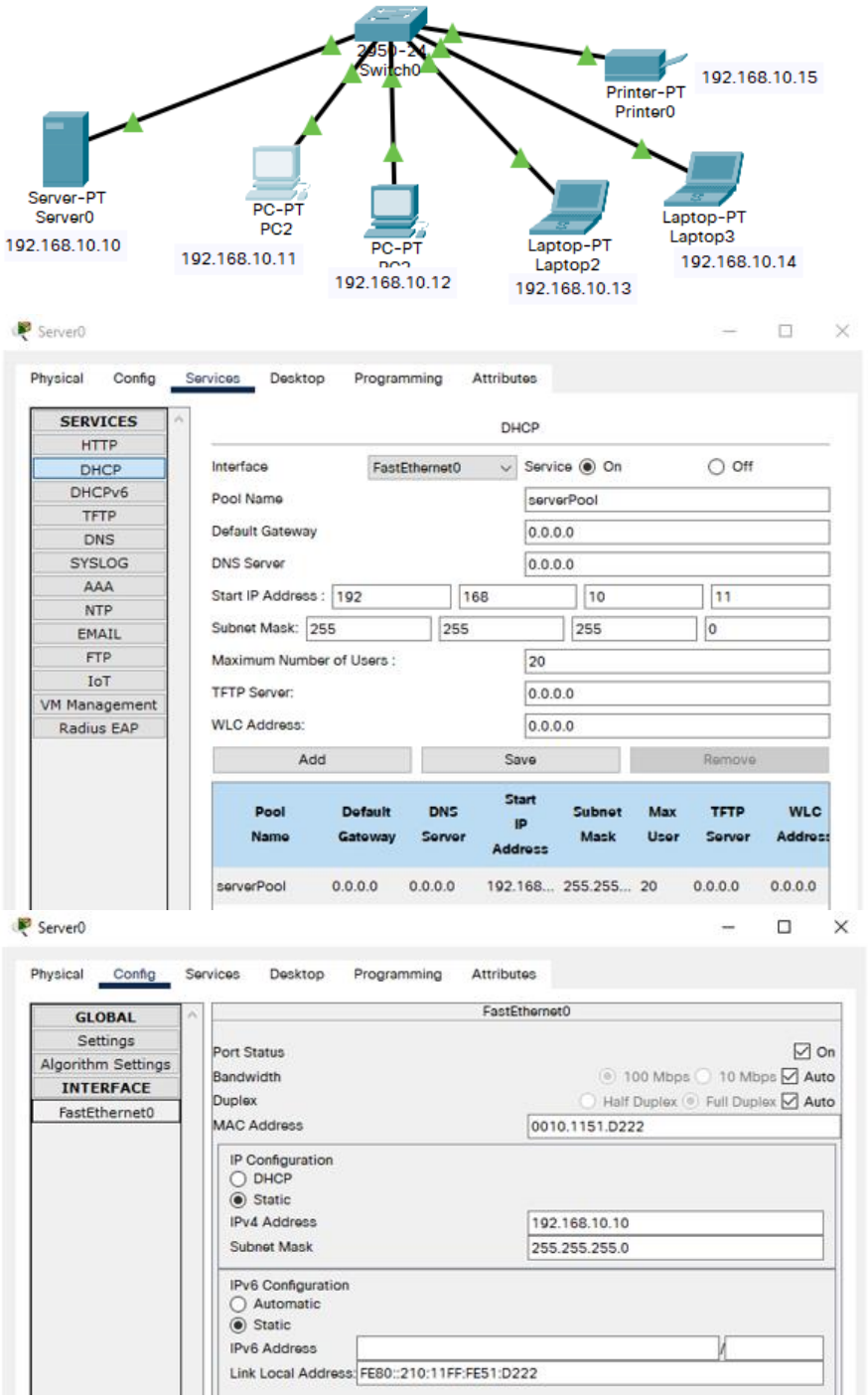
Router can be configured to connect multiple switches, VLANs or networks. We can assign Static routing or Dynamic routing using Routing Information Protocol (RIP) to interconnect multiple networks. We will have to configure the IP address and Subnet Mast for each network on specific FastEthernet port and also configure for Static or RIP routing along with bandwidth and mode of communication. A typical network containing router along with its configuration will be as follow:





c. **DHCP configuration (Scope creation with screen shot)**

DHCP server can be configured to assign IPs to user automatically. It has to be connected to a specific switch on which it will be assigning the IP addresses to connected devices. We have to state the Port Status, Bandwidth, Duplex, MAC address, IPv4 address, Subnet Mask etc. on the FastEthernet interfaces. A typical example of DHCP configuration would be as follow:



d. **Access point, server configuration guidelines**
The access point capability will be enabled through wireless access points (WAP), and they will be most likely present in the Guest network for reasons stated above. The server configuration of the DHCP server is also highlighted above.

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].