

4-27-2016

Enterprise Network Design and Implementation for Airports

Ashraf H. Ali

Valparaiso University, ashraf.ali@valpo.edu

Follow this and additional works at: http://scholar.valpo.edu/ms_ittheses

 Part of the [Aviation Commons](#), [Computer Engineering Commons](#), and the [Computer Sciences Commons](#)

Recommended Citation

Ali, Ashraf H., "Enterprise Network Design and Implementation for Airports" (2016). *Information Technology Master Theses*. Paper 2.

This Thesis is brought to you for free and open access by the Department of Computing and Information Sciences at ValpoScholar. It has been accepted for inclusion in Information Technology Master Theses by an authorized administrator of ValpoScholar. For more information, please contact a ValpoScholar staff member at scholar@valpo.edu.



VALPARAISO UNIVERSITY

Enterprise Network Design and Implementation for Airports

By

ASHRAF H. ALI

MASTER'S THESIS

Submitted to the Graduate School of Valparaiso University

Valparaiso, Indiana in the United States of America

In partial fulfillment of the requirements

For the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY

May 2016

VALPARAISO  UNIVERSITY
GRADUATE SCHOOL

Thesis Approval Form

Date: 4/27/2016

This form is to certify that the thesis:

Enterprise Network Design and Implementation for Airports

By:

ASHRAF H. ALI

Has been reviewed and approved by the thesis committee.



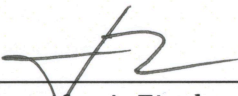
Shiv Yadav, M.S.
Thesis Advisor and Committee Chair



Nicholas S. Rosasco, D.Sc.
Member, Thesis Committee



James Caristi, Ph.D.
Graduate Program Director, Information Technology



Jennifer A. Ziegler, Ph.D.
Dean of the Graduate School and Continuing Education

© Copyright
Ashraf H. Ali, 2016
All rights reserved

Abstract

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

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

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

The dual internet service providers' role was to provide the flight management department, which helps to confirm the backup operation for the Air Traffic Control Complex (BATCX) system to outside the local network. This is achieved by using Windows servers backup (iSCSI initiators and iSCSI target) servers which helps to keep the Air Traffic Control systems' information in a safe place. Also, for passengers' personal information safety, the web server has been placed in the local network, which provides a secure environment for any network's element.

Acknowledgement

First and foremost I would like to thank God. You have given me the power to believe in myself and pursue my dreams. I could never have done this without the faith I have in you, the Almighty.

I want to thank my thesis advisor Shiv Yadav and my deep thanks to Dr. Nicholas Rosasco for the trust, the insightful discussion, offering valuable advice, for your support during the period of the project, and especially for your patience and guidance during the writing process.

I also thank professor Dr. James Caristi for his guidance for the thousand moments of kindhearted advice and support that I will take with me wherever I go. Moreover, my deep thanks for Jason Kellerman for his technical advising during the practical work, professors Kevin Steele and Mark DeMateo for their moral support during this my project.

I want to thank my parents for their love and encouragement, without which I would never have enjoyed so many opportunities.

Furthermore, my lovely wife who has never stopped to supporting me during this project, our great American friends.

My sincere thanks and appreciation to the Valparaiso University, College of Science and Technology for granting me opportunity to study for a Master's degree. I am also thankful to office of Human Resources at the Resources at the Ministry of Post and Communication in Iraqi Kurdistan for making provision the opportunity to study at developer countries.

Also to anyone whom I might have forgotten while I was writing these sentences, with all my respect and appreciation.

Table of Contents

1	Introduction.....	1
1.1	Background & context.....	1
1.2	Problem description.....	2
1.3	Related Work.....	3
2	Security.....	4
2.1.1	Firewalls Design.....	6
2.1.2	Configurations of Firewalls.....	9
2.1.3	Firewalls advantages.....	13
2.2	IP access control list (standard or extended) design.....	14
2.2.1	The access list configuration.....	15
2.2.2	Results.....	20
2.3	MAC address port security.....	22
2.3.1	MAC address port security design.....	23
2.3.2	MAC address port security configurations.....	25
2.3.3	Results.....	27
2.4	Domain Controller Server.....	29
2.4.1	Design.....	30
2.4.2	Active Directory Domain Services and Domain Controller Configurations.....	32
2.5.1	Squid Proxy Server.....	48
3	Quality.....	56
3.1	Failover Design.....	57
3.1.1	Failover configuration.....	58
3.2	PXE Sever (Pre-boot Execution Environment).....	63
3.2.1	PXE Server Design.....	66
3.2.2	PXE Server Configurations.....	67
3.3	Dynamic Host Configuration Protocol (DHCP) Server.....	74
3.3.1	DHCP Position in Overall Network.....	76
3.3.2	DHCP Sever Installation and Configuration.....	78
3.4	Domain Name System (DNS) Server.....	83
3.4.1	DNS Server Network Location.....	84
3.4.2	DNS Server's installation and configuration.....	86

3.5	Airport's Network Cabling	90
3.5.1	Airport's Network Cabling Design.....	91
3.5.2	Airport's Network Cabling Configurations.....	93
4	Safety.....	94
4.1	Web server	94
4.1.1	Web Server Design.....	95
4.1.2	Webserver configurations	97
4.2	Dual Internet Service Providers (ISPs)	101
4.2.1	Dual Internet Service Providers (ISPs) Design	102
4.2.2	Dual Internet Service Providers (ISPs) Configurations	104
5	Conclusions.....	110
5.1	Research Questions	110
5.2	Future Questions/Future Research Directions	111
5.3	Summary	112
	References	113

Table of figures

Figure 1. Firewalls design.....	8
Figure 2. Flight management firewall design.....	9
Figure 3. Assign inside and outside security level.....	10
Figure 4. Assign inside interfaces for VLAN.	11
Figure 5. Assign outside interfaces for VLAN.	11
Figure 6. Assign VLANs and security levels for flight management department.....	12
Figure 7. Standard access list range.....	15
Figure 8. . Deny arrivals, departures and guests' department form accessing the service providers' department.	16
Figure 9. Deny service providers department from accessing flight management department.	16
Figure 10. Outband access-list configuration for arrivals, departures and guests' department.....	17
Figure 11. Permit access-list for other departments.	18
Figure 12. Deny the service providers' department from accessing flight management department.	18
Figure 13. Deny service providers department from access to the flight management department.....	19
Figure 14. Service provider's network accessing the by TCP protocol.	20
Figure 15. Result of deny arrivals, departures, guests' department from accessing other departments..	21
Figure 16. Result of denying arrivals, departures and guests' department form accessing flight management department.....	21
Figure 17. Result of accessing service provider's department can access with TCP protocol.....	22
Figure 18. Switch port security options.	25
Figure 19. Switch port security sticky option.....	25
Figure 20. Assign mac-address to sticky option.....	26
Figure 21. Assign mac- address for each device.	26
Figure 22. Port-security violation mode.	26
Figure 23. Port-security shutdown.	27
Figure 24. Port security policy.....	27
Figure 25. Result of not matching mac address.....	28
Figure 26. Port-security policy report.	28
Figure 27. Violation for authorized device recorded.	29
Figure 28. Domain control server design.	31
Figure 29. Active Directory Domain add roles and features.....	33
Figure 30. Role-based installation.....	33
Figure 31. Sever pool.	34
Figure 32. Active directory roles.	34
Figure 33. NET framework role.	35
Figure 34. Active directory installation.	35
Figure 35. Promoting the active directory.	36
Figure 36. Specify Domain information.	37
Figure 37. Domain controller options.....	37

Figure 38. Verify NetBIOS name.	38
Figure 39. Domain server path.	38
Figure 40. Review the selections.	39
Figure 41. Prerequisite domain controller installation.	39
Figure 42. Airport domain controller directory.	40
Figure 43. Airport domain controller directory options.	40
Figure 44. Organization unit for flight management department.	42
Figure 45. Organization unit name.	43
Figure 46. Organization unit for service providers department.	43
Figure 47. Assign group policy management departments.	44
Figure 48. Flight management policy.	44
Figure 49. Service providers' policy.	45
Figure 50. Hide add programs from Microsoft.	45
Figure 51. Hide control panel.	46
Figure 52. Proxy server design.	49
Figure 53. Update Ubuntu system.	50
Figure 54. Root user.	51
Figure 55. Install squid.	51
Figure 56. Squid IP address.	51
Figure 57. Connect Squid to the internet.	52
Figure 58. Block website.	52
Figure 59. Squid restart service.	53
Figure 60. Proxy server websites access deny.	53
Figure 61. Proxy server access websites.	54
Figure 62. Squid monitoring tool.	55
Figure 63. Failover location design.	58
Figure 64. PXE Server location design.	67
Figure 65. PXE network LAN adapters.	68
Figure 66. PXE operating system image.	68
Figure 67. Connect PXE to Putty tool.	69
Figure 68. PXE directories.	69
Figure 69. Mounting operating systems.	70
Figure 70. Install git.	70
Figure 71. Clone repo for PXE.	71
Figure 72. Moving PXE directory.	71
Figure 73. PXE server URLs.	72
Figure 74. Virtual client adapter configurations.	72
Figure 75. Accessing PXE server through LAN.	73
Figure 76. Operating systems options.	73
Figure 77. Operating system CentOS.	74
Figure 78. DHCP Sever location design.	76
Figure 79. Arrival, departure, and guests' department DHCP server location.	77
Figure 80. Roles DHCP installation.	79
Figure 81. DHCP related features.	79

Figure 82. DHCP scope option.	80
Figure 83. DHCP flight management scope.	80
Figure 84. Scope name.	81
Figure 85. Scope IP address range.	81
Figure 86. DHCP scope lease duration.	82
Figure 87. Scope default gateway.	82
Figure 88. DNS server example.	83
Figure 89. DNS server location design.	85
Figure 90. DNS roles and features.	86
Figure 91. Roles and features type.	86
Figure 92. Server roles installation.	87
Figure 93. Setup new DNS zone.	87
Figure 94. DNS zone name.	88
Figure 95. DNS zone file.	88
Figure 96. DNS dynamic update.	89
Figure 97. DNS record server.	90
Figure 98. Airport's Network Cabling design.	93
Figure 99. Web Server location design.	96
Figure 100. Web server roles and features.	97
Figure 101. Web server (IIS) role installation.	98
Figure 102. Web server (IIS) installation requirements.	98
Figure 103. Web Server (IIS) requirements.	99
Figure 104. Web Server tool manager.	100
Figure 105. Web Server local host.	100
Figure 106. Airport home page.	101
Figure 107. Dual ISPs Design.	103
Figure 108. Add roles and features for Backup Server	105
Figure 109. Windows Server backup tool.	105
Figure 110. Add roles for a backup tool.	106
Figure 111. Backup Server installation type.	106
Figure 112. iSCSI Target Server roles	107
Figure 113. Backup Server disk space.	107
Figure 114. iSCSI virtual disk size	108
Figure 115. Target Server name.	108
Figure 116. iSCSI initiators server IP address.	109
Figure 117. Air Traffic Control system virtual disk.	109

1 Introduction

In most countries around the world, there are many places that represent the main gates for entrance and exit. Because of the importance of these places, each country takes many necessary measures to provide them with the best technology. Airports are the most sensitive places around the world because they represent these gates. Technology plays many different roles to protect and represent a high quality of services for these places. Computer networking is the most crucial part of modern airports because this new technology takes the most important responsibilities, rather than people doing the tasks as in previous decades. The following thesis sheds light on three main parts which are improved during the practical work: security, quality, and safety.

1.1 Background & context

The majority of the airports around the world have three main departments: the flight management controls, flight service, and arrivals, departures, guests' department. These departments in airports are connected, and huge amounts of data are transferred between them each and every day. Not only is transferring data between these departments important in the project, but saving peoples' lives is important too. Also, the quality of service in this project is critical because of the difficulty of the networks' tasks. However, in each network, there are many weak points which should be dealt with to avoid many issues that might lead to huge losses in the realms of economy and humanity. This project provides a scheme for using two main tools that can help to avoid these common problems: design and implementation. The network design offered concentrates on the positions of each element in the network and how these components and capability can solve these issues.

1.2 Problem description

In this thesis, there were many issues that have been solved technically. The first concern was security, the second concern was quality and the third concern was safety.

In the security centered analysis, the airport's network provides services for different people, including passengers and staff, so there may be some people who cannot be trusted to connect to the inside network. However, there are many techniques to prevent people who are planning terrorist attacks from having access to the sensitive departments in the network. The tools that have been used to provide a high security level to the airport's network are hardware firewalls, an IP access control list, MAC address port security, a DNS server and a proxy server. These techniques have been used to prevent these people from stealing data from the flight management department, the most safety critical department. Nevertheless, these techniques must provide a high security level for the network and stop the hackers infiltrating the network because the more the security techniques are increased, the more hackers' techniques will increase in response. Moreover, the security rules have been designed to prevent any outside hackers sneaking into the network and getting what they want.

Improving the performance of any network needs a high quality of techniques and services that help to improve the general function of the network. Airport networks need to have a high quality of services that should be presented immediately in order to keep the airport activities on track. In this section the quality of network services has been provided by new techniques to improve the quality of service. These techniques are represented by failover firewalls utility, a Pre-boot Execution Environment server (PXE), Dynamic Host Configuration Protocol Server (DHCP), Domain Name System Server (DNS) and cabling. The network includes everything necessary to provide a high quality of service.

Protecting passenger safety was the most important part of the project's design. To insure the availability of service, the airport should have two internet service providers that help guarantee the outside connection remains active during the airport operations. The Internet support for the flight management department needs continuous Internet service, especially the Air Traffic Control system, which manages the aircraft movement in the airport. Also, saving people's information in the airport is important, and that was the second strategy for saving people's lives. All of this support has been provided by using Dual ISPs Design to provide the Air Traffic Control system (ATC) and ATC Backup configurations.

The aim of this project is to demonstrate an example of an airport's network design and implementation:

- Providing a high security level for the airport's network
- Providing a high quality of service for the airport's network
- Maintaining the passengers' safety in the airport
- Maintaining passengers' information
- Supporting the flight management system

1.3 Related Work

In general, airports' networks should not be as simple as any other organizations because of the safety and general visibility of the facility, so these need to be protected and supported by technology that introduce design and defense in departments. Prior work in this area includes as a proposal by Sachin (2013) which was presented as a very simple network. The report did not discuss the main drivers for any airport's network, which are security, quality and safety. {However, the proposal report can apply for small organizations or coffee shops}. Also, it just

introduced the main departments in the airport's network and devices that are used to provide the service for any small network. In the airport, the network needs to be protected and has a high quality to ensure the safety of passengers. In the security section, the report proposal does not contain a sufficient level of protection like hardware firewalls, domain Windows servers, an IP access control list, Mac address port security, and a proxy server. All these tools have been applied in this project, and the result is more secure than the original report proposal. In the service quality section the report proposal was not supported by devices that provide the network a high quality of service, which is critical in airports. This extensive work ensures a high quality of service by providing the airport's network with the following services: failover firewalls, a PXE server (Pre-boot Execution Environment) and a DNS server (Domain Name System). The third and most important part that was not supported in the earlier work was safety, which is represented by supporting the flight management department through the use of dual ISPs (internet service providers). Otherwise, these services have been applied in this project to keep the Internet connection continuous in the flight management department, making the process of backup in the Air Traffic Control System permanent. All these techniques have been combined to make this project appropriate for any airport's network.

2 Security

Network security is the most important attribute of any computer network, especially in with the increasing reliance on neighborhood systems for key functions and operations. People communicate in different ways with each other with emails, social websites and other tools that make the communication very easy. As these tools improve, the danger will be finding against the computers networks around the world. From ongoing threats and international companies which spend a lot of money for network security on their local network to protect it from hackers.

Despite this destination, the risk is across the whole system since these departments could be involved in the data transfer through network elements. It is difficult to control any computer network from outside attacks unless this network is isolated from the outside world. In this design, the arrival, departure, and guests' department represents the most untrusted and least secure department on account of the diversity of users. Moreover, as these departments are connected by the same network, persons from each one of these departments can become an inside threat. According to Canavan (2001), "Canavan's first rule of security is to safeguard physically systems and networks. Are your systems, communications equipment, and media located in a secure facility? Central Hosts and Servers should be kept in secure rooms that can only be entered by authorized personnel" (p.14).

Security risks in this situation could lead to a hack from the outside of the airport's network or in the inside (between main departments) network. Reliving required capabilities in to this a complex challenge for the network.

2.1 Firewalls

Firewalls are the first step toward a high security level, and a primary mechanism for the design presented here. These devices are a well-known security system for any computer network. They are used for controlling the packets and data that create a zone inside and outside the network. The firewall allows for a higher degree of trust for systems behind it, as external hosts are generally excluded.

In standard configuration, firewalls will trust the inside activity, and the configuration of the device will give a low level of security because of the trusted people inside the organization. Otherwise, the outside activity like internet connections or the connections that establish outside

the local network will be untested. Therefore, the network administrative team responsible for managing the network inside any organization will give a high level of security for the outside connections to inside, some of these levels reach to 100% of security. For that reason, these firewalls filter packets from hosts the outside and deny any untrusted connection depending on created rules. According to Semeria (1996), "Internet firewalls manage access between the Internet and an organization's private network Without a firewall, each host system on the private network is exposed to attacks from other hosts on the Internet" (p.2).

By functioning as gateways, firewalls can control all the communication in to an act of the network by appliance rules for each packets which protect the network from any attack. In this project, the use of firewalls took two stages: design and configuration.

2.1.1 Firewalls Design

In the design stage, this project end covered to determine the optimal location through firewalls. It is assumed airport network has been supported with two ISPs (Internet service providers), with both connections of them are going through the main firewall.

The ASA1 firewall position design takes a very important location because it works as police check point on the bridge. With this strategy, no data can be exchanged without it passing through the firewalls. For the most network designs, network engineers take prominent role for the design of the network before anything. This step represents the first step in establishing an integrated any deploy system as well as the all practical work that benefits the design, especially the overall technology. The first importance of firewalls location design is to ensure it can be the control checkpoint and the question mechanism. According to Kaur (2012), some of the queries traffic control and the network activity in case of having two firewalls in the same network are:

- Any outside to inside activity in the network should be inspected.
- Compare the firewalls' configuration with each other to ensure the similarity in the policy rules.
- Inspect for the activation of each firewall in the same network.
- Check the impact of a port compromise to interface for the firewall.
- Assuring the policy configuration setups for the firewalls to meet the organization requirements.
- Making sure of disabling the unused open ports especially the closes one from the used ports.
- Depending on the organization's equipment the used ports should be mentioned as a part of the policy rules.
- The firewall policy rules, which should be trusted on every update.

As a result of these steps, the location for the firewalls does not introduce all policy rules for exchanging the information inside and outside the network. The local network have been configured to limit the access from outside, this task has been assigned to the by proxy server which has already been installed for the Airport network. The rule set the project's firewalls follows a design structure that reflect security for each position.

1. The internet service providers (ISPs) was connected to the firewall to control the data exchange from outside to inside the airport network (the Internet to the local network).
2. The second firewall was placed in the Flight Management Database Server as shown in the figure 1.
3. This firewall was attached to one of the flight management switch ports.

As a result of this design the security level for all network and specifically in the Flight Management Department was increased dramatically because of the security policy which installed for each firewall.

The first result of the design was filtering the transmitted data through the internet. Each device inside the airport's network can be accessed through any website from the Internet because the outside security level was set up with zero security level. Otherwise, the inside network set up with high security level to prevent the outside activities entering the local network. As a final result, this will protect the inside network from any hackers and untrusted connections as shown in figure 1.

The second result of the design was configuring the failover tool in the main firewall. This tool allowed the firewall to switch ISP1 to ISP2 or ISP2 to ISP1 when one of the ISPs fail, figure 1 illustrates the connection setup.

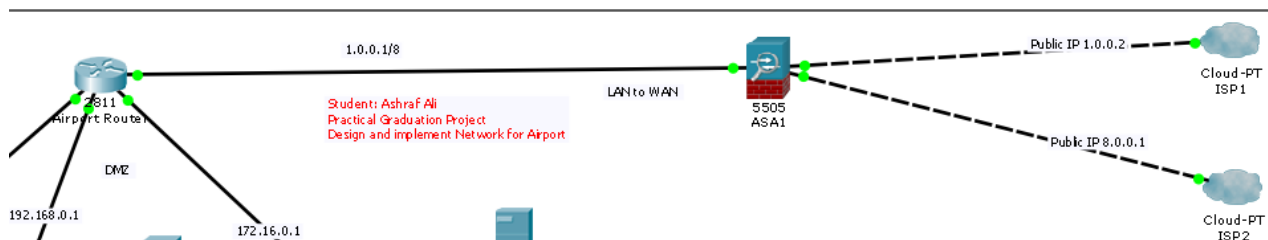


Figure 1. Firewalls design.

The third result of the design was greater protection for the Flight Management Department, which is the highest risk department for the airport's network. This department requires a database server for the flight management departments (as shown in figure 2). The firewalls designed for this over of the network which protected the server not only from the outside the network but also

from the inside (other departments). This firewall restricts access to for the flight management department's technicians and engineers, members of the flight management department. This firewall ensured controls access to flight management database server, providing a high security level for the data in that department. Also, the firewall access ports have been designed assigned for one switch port which connected to the flight management's users. There are some configurations designed for the switch device to allow these users to pass through the device to the firewall port; these configurations will be mentioned in the next steps of the project. Figure 2 shows how the firewall is connected to the switch with the other department's network elements.

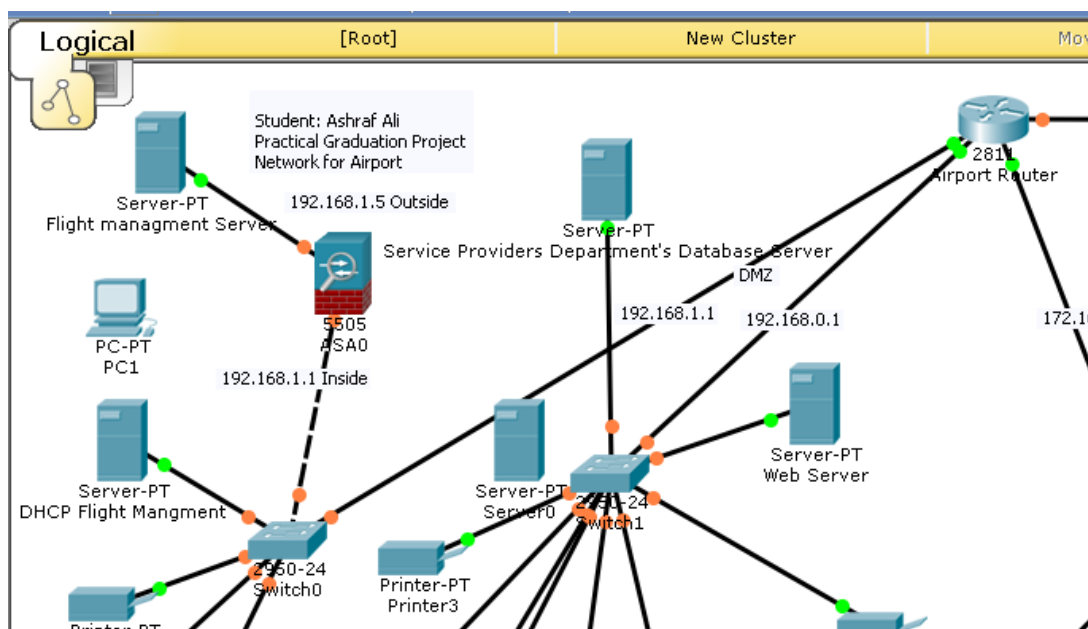


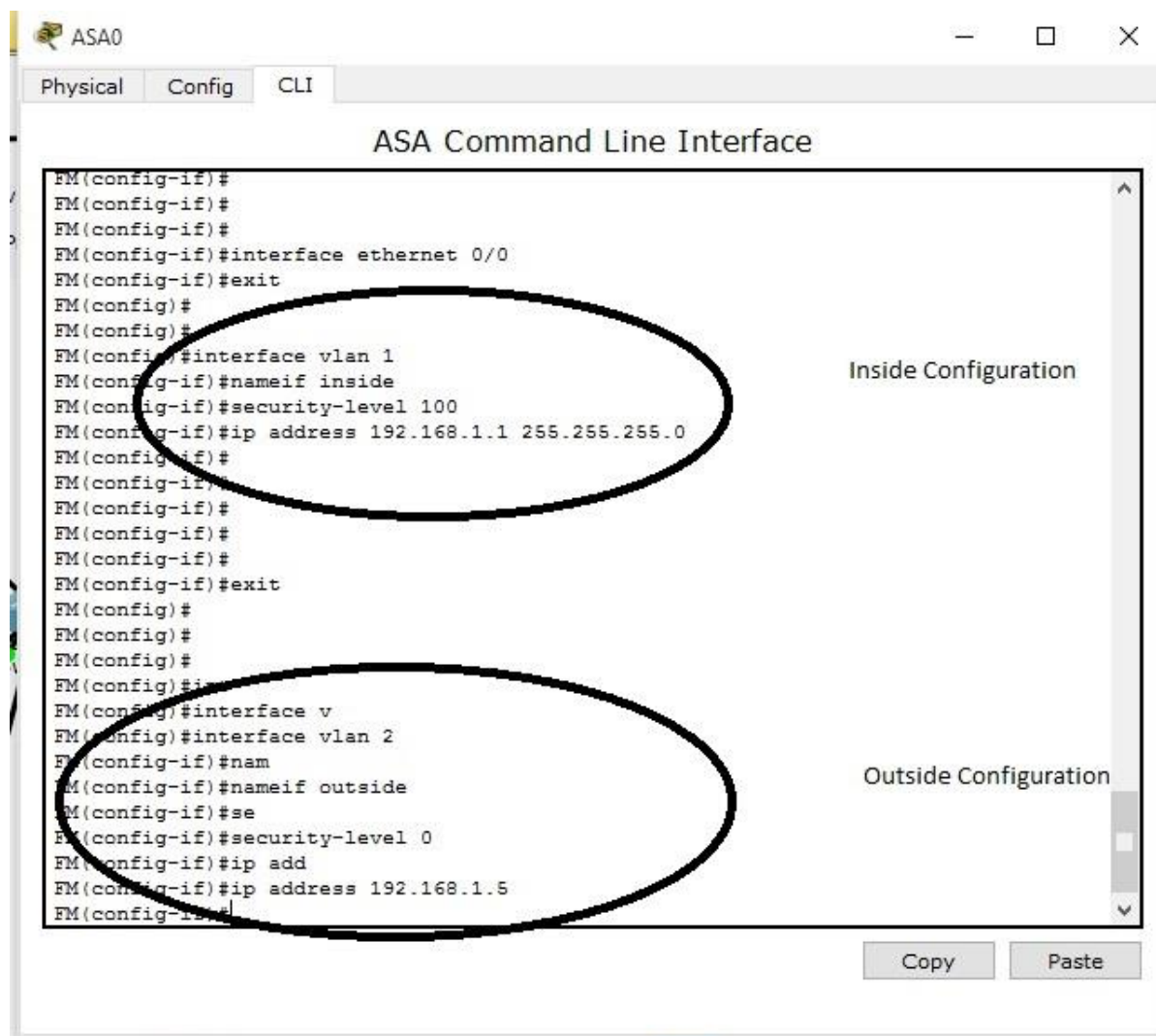
Figure 2. Flight management firewall design.

2.1.2 Configurations of Firewalls

The Airport's network as mentioned before must be protected because of the sensitivity of this operation. Otherwise, the devices which have been used to protect the network were hardware firewalls, the hardware part has a little rule in this security task. Firewalls devices implement a rule set, these configurations took many steps to provide a high quality of service to the network.

However, there was a problem before the security policy configured which was the DHCP configuration in the firewall. The configuration part will explain the steps that were taken to set up these devices and prepare them to against potential intrusions and response to them which has been configured according to Sequeira (2012).

The firewall configuration begins with the main firewalls which create in the main gate of the airport's network. This firewall links the internal network to outside connection. In the first step of configuring the firewalls was link the inside and outside ports to the network internet protocols (IPs) with their security level as shown in figure 3.



The screenshot shows the ASA Command Line Interface (CLI) window. The window title is "ASA0" and it has tabs for "Physical", "Config", and "CLI". The main content area is titled "ASA Command Line Interface" and displays the following configuration commands:

```
FM(config-if)#
FM(config-if)#
FM(config-if)#
FM(config-if)#interface ethernet 0/0
FM(config-if)#exit
FM(config)#
FM(config)#
FM(config)#interface vlan 1
FM(config-if)#nameif inside
FM(config-if)#security-level 100
FM(config-if)#ip address 192.168.1.1 255.255.255.0
FM(config-if)#
FM(config-if)#
FM(config-if)#
FM(config-if)#
FM(config-if)#exit
FM(config)#
FM(config)#
FM(config)#
FM(config)#
FM(config)#interface v
FM(config)#interface vlan 2
FM(config-if)#nam
FM(config-if)#nameif outside
FM(config-if)#se
FM(config-if)#security-level 0
FM(config-if)#ip add
FM(config-if)#ip address 192.168.1.5
FM(config-if)#
```

Two sections of the configuration are circled in black. The first circle highlights the configuration for the "inside" interface, including the command `FM(config-if)#security-level 100`. The second circle highlights the configuration for the "outside" interface, including the command `FM(config-if)#security-level 0`. To the right of the terminal output, the text "Inside Configuration" and "Outside Configuration" are visible. At the bottom right of the window, there are "Copy" and "Paste" buttons.

Figure 3. Assign inside and outside security level.

Also, each port is assigned to specific VLAN (Virtual Local Area Network) inside port (interface Ethernet 0/0) with high security level (100) and outside ports (interface Ethernets 0/1, 0/2, 0/3, 0/4, 0/5, 0/6, 0/7) VLANs with 0 security level, as illustrated in figure 4 and figure 5.

```
AirportFirewall(config)#
AirportFirewall(config)#int
AirportFirewall(config)#interface v
AirportFirewall(config)#interface vlan 1
AirportFirewall(config-if)#nam
AirportFirewall(config-if)#nameif in
AirportFirewall(config-if)#nameif ins
AirportFirewall(config-if)#nameif inside
AirportFirewall(config-if)#se
AirportFirewall(config-if)#se
AirportFirewall(config-if)#security-level 100
AirportFirewall(config-if)#ip add
AirportFirewall(config-if)#ip address 1.0.0.1 255.0.0.0
AirportFirewall(config-if)#By Ashraf ALi MS Project Airports
```

Inside Vlan, Local Network

Copy Paste

Figure 4. Assign inside interfaces for VLAN.

```
AirportFirewall(config)#
AirportFirewall(config)#int
AirportFirewall(config)#interface v
AirportFirewall(config)#interface vlan 2
AirportFirewall(config-if)#se
AirportFirewall(config-if)#nam
AirportFirewall(config-if)#nameif outside
AirportFirewall(config-if)#se
AirportFirewall(config-if)#security-level 0
AirportFirewall(config-if)#ip add
AirportFirewall(config-if)#ip address 8.0.0.1 255.0.0.0
AirportFirewall(config-if)#
```

Outside VLAN, Internet Service Providers

Copy Paste

Figure 5. Assign outside interfaces for VLAN.

VLANs also make the data available for the other ports which help to having a high security level. In the Airports' network, the main firewall has been configured with two VLANs as shown previously in figure 4 and 5.

The second firewall configure is the one further flight management department. These configuration steps were similar to the main firewall, but the number of users inside the network was limited. However, the inside ports (Interface Ethernet 0/0,) have been connected to five computers in the flight management department through the department's switch device, and the outside port (Interface Ethernet 0/1) has been connected to the flight management department's database server as shown in figure 6.

```

ASA0
Physical Config CLI
ASA Command Line Interface
FM(config-if)#
FM(config-if)#
FM(config-if)#
FM(config-if)#interface ethernet 0/0
FM(config-if)#exit
FM(config)#
FM(config)#
FM(config)#interface vlan 1
FM(config-if)#nameif inside
FM(config-if)#security-level 100
FM(config-if)#ip address 192.168.1.1 255.255.255.0
FM(config-if)#
FM(config-if)#
FM(config-if)#
FM(config-if)#
FM(config-if)#exit
FM(config)#
FM(config)#
FM(config)#
FM(config)#int
FM(config)#int
FM(config)#interface vlan 2
FM(config-if)#nam
FM(config-if)#nameif outside
FM(config-if)#se
FM(config-if)#security-level 0
FM(config-if)#ip add
FM(config-if)#ip address 192.168.1.5
FM(config-if)#
  
```

Inside VLAN, Flight Management Department's Users

Outside VLAN, Flight Mangmant Department's Database Server

Copy Paste

Figure 6. Assign VLANs and security levels for flight management department.

2.1.3 Firewalls advantages

As mentioned before, the security represents the main part of any network because any network with a low security level cannot be trusted for any organizational or governmental locations. Also, the protectable part of any network is taken care of by the firewalls; these devices have many advantages which in general prevent untrusted activities from inside or outside the network by using filtering algorithms and IP check tools.

According to Chadwick's study in (2001) firewalls have some advantages:

They can stop incoming requests to inherently insecure services, e.g. you can disallow login, or RPC services such as NFS. They can control access to other services e.g. Bar callers from certain IP addresses, filter the service operations (both incoming and outgoing), e.g. stop FTP writes hide information e.g. by only allowing access to certain directories or systems. They are more cost-effective than securing each host on the corporate network since there is often only one or a few firewall systems to concentrate on.

They are more secure than securing each host due to:

The complexity of the software on the host - this makes it easier for security loopholes to appear. In contrast, firewalls usually have simplified operating systems and don't run complex application software, the number of hosts that need to be secured (the security of the whole is only as strong as the weakest link). (p.151)

Therefore, the advantages of firewalls cannot just be illustrated on an individual device, or they cannot show that firewalls protect individual devices the whole idea in this case is to protect all networks. In the airport's network not only should the user's devices should be protected but also the servers which contain the whole network's information.

2.2 IP access control list (standard or extended) design.

Several strategies are needed to protect the network from untrusted users like people from outside the network and unemployed people for any organization. In the airport's network, the flight management department can be trusted because all the users are the main employees for supporting this department. The second department for the airport's network is service provider department which contains employee's forms, and unauthorized people cannot enter to use the department's technology for the personal purpose. Moreover, this department's employees can also be trusted depending on the network structure and rules. The arrival, departure, and guests' department contain different users from different countries that may include terrorist. These people contain a percentage of untrusted people or terrorists whose activities in the network can be very dangerous. Therefore, the main router in the arrival, departure, guest's department has been configured in list access control to prevent the users in this department accessing the other departments. For this purpose, the control access list tool has been configured on the router's Interface Ethernet for the guest department. The access control list used to control and to filter the packet during the network's activities. This tool provided a high security level to the network and determined the network traffic. Moreover, this tool can help to prevent the hackers from entering the other departments in the network and stealing data or damaging them.

According to Sedayao (2001) in his study about Cisco routers found the following benefits of access-list technology:

On the Internet, high-profile web servers are constantly probed for potential security vulnerabilities and opportunities for crackers to penetrate a web server and alter its contents. These web servers can be substantially protected from this and other kinds of attacks by limiting the type of packet a router passes on to the servers. With this policy

tool, also known as packet filtering, we define in our policy sets the kinds of IP packets that can pass through router interfaces. Packet filtering with access lists is a very common use of Cisco routers, particularly as part of firewalls. Although the primary concern here is security, robustness and business policy are also considerations, since an organization may find that certain kinds of packets cause problems. It may decide that it doesn't want a certain type of network traffic passing through, thus conserving bandwidth or reducing costs.

As a result, the ACL can be used to filter the packets and control the packets inside the local network. This tool helped to present a high-security level for the airport's network by protecting it from any outside and inside attacks.

2.2.1 The access list configuration

There are many types of configuration access list control deepening on the security and quality rules for each network. The first type is Standard access-list; this type tests the guests' department's packets or activities (the source packets). This was helping to stop the packets and restrict them inside (172.16.0.0) close to the destination which is the arrival, departure, and guest's department. Otherwise, for other activities like Talent (control the router from other devices in the network) this tool was active because of the network needs and it will be visible to the network administrator. Also, the standard access list has a standards number 1-99 which indicates and notifies the router that this is a standard access list configuration as shown in figure 7.

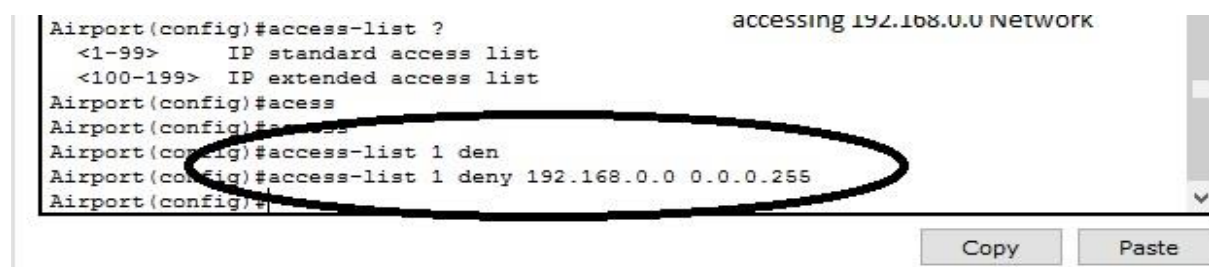


```
Airport(config)#acc
Airport(config)#access-list ?
<1-99>      IP standard access list
<100-199>  IP extended access list
Airport(config)#access-list
```

Figure 7. Standard access list range.

Moreover, in this type of access-list control, the whole traffic is blocked by default, so there are not any possibilities to allow any of data to pass on to the other departments. The protocols that have been prevented include IP (Internet Protocol), ICMP (Internet Control Message Protocol), TCP (Transmission Control Protocol), and UDP (User Datagram Protocol). Several configurations steps have been assigned according to Wilkins 2013. The standard access-list configurations for the arrival, departure, and guests' department was going through these states:

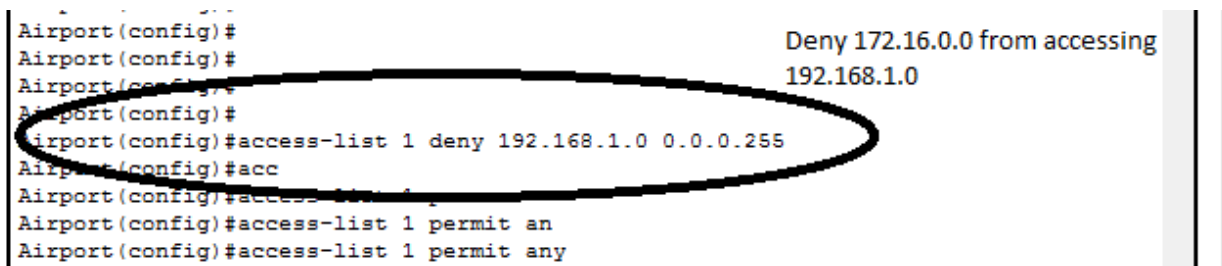
The first step was denying the arrival, departure, guest department with IP (172.16.0.0) from accessing the service providers department with IP (192.168.0.0) as shown in figure 8.



```
Airport(config)#access-list ?                                accessing 192.168.0.0 NETWORK
<1-99>      IP standard access list
<100-199>   IP extended access list
Airport(config)#access
Airport(config)#access-list 1 deny
Airport(config)#access-list 1 deny 192.168.0.0 0.0.0.255
Airport(config)#
```

Figure 8. . Deny arrivals, departures and guests' department from accessing the service providers' department.

The second step was denying the same department from accessing the flight management department with IP (192.168.1.0) as shown in figure 9.



```
Airport(config)#
Airport(config)#
Airport(config)#
Airport(config)#
Airport(config)#access-list 1 deny 192.168.1.0 0.0.0.255
Airport(config)#acc
Airport(config)#access-list 1
Airport(config)#access-list 1 permit an
Airport(config)#access-list 1 permit any
```

Figure 9. Deny service providers department from accessing flight management department.

The third step was controlling the arrival, departure, and guests' department (192.168.0.0) network range to make packets go from high security level to low security level. This allowed this department in the inside network to connect to the outside the Internet, so this configuration allowed the direction of this department to the router interface and directly to the routers interface that connected to the internet. Figure 10 the outgoing access-list configuration for the interface 1\0 for the arrival, departure, and guest' department.

```
Airport (config)#
Airport (config)#
Airport (config)#int
Airport (config)#interface f
Airport (config)#interface fastEthernet 1/0
Airport (config-if)#ip acc
Airport (config-if)#ip access-group 1 out
Airport (config-if)#
Airport (config-if)#
Airport (config-if)#
Airport (config-if)#
```

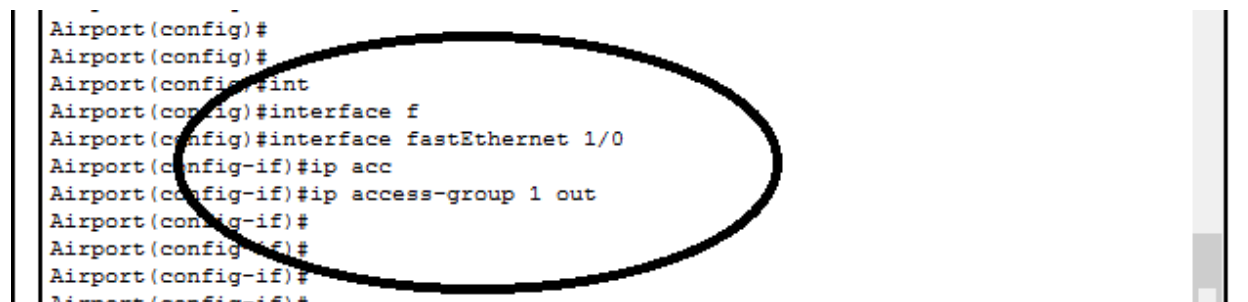


Figure 10. Outband access-list configuration for arrivals, departures and guests' department.

On the other hand, this department is should be configured to be accessible by other departments. The flight management department and service providers, for example obtain internet service from the arrival, departure, and guest department's wireless access points. To obtain successful access to the arrival, departure, guest department the access-list has been configuring as permit access as shown in figure 11.

```

Airport(config)#access-list 1 deny 192.168.0.0 0.0.0.255
Airport(config)#
Airport(config)#
Airport(config)#
Airport(config)#
Airport(config)#
Airport(config)#
Airport(config)#access
Airport(config)#access-list 1 per
Airport(config)#access-list 1 permit any
Airport(config)#
Airport(config)#

```

192.168.0.0 Network permit
for other Airport's Network

Figure 11. Permit access-list for other departments.

The second type is an extended access-list; this type is used to deny the service providers' department from accessing flight management department, the rules are based on the source and destination IP. Also, the port number has been specified depending on the user's needs. Also, this configuration has many protocol options, and the network administrator can choose to depend on the network access policy, as shown in figure 12.

```

Airport(config)#acc
Airport(config)#access-list 100?
<100-199>
Airport(config)#access-list 100 de *
Airport(config)#access-list 100 deny ?
  ahp   Authentication Header Protocol
  eigrp Cisco's EIGRP routing protocol
  esp   Encapsulation Security Payload
  gre   Cisco's GRE tunneling
  icmp  Internet Control Message Protocol
  ip    Any Internet Protocol

```

Copy Paste

Figure 12. Deny the service providers' department from accessing flight management department.

As mentioned before, the standard access list can deny and permit all the packets and protocols in the network together. In this way, there should be other tools to permit transferring

specific protocols, this can happen by using the extended access list. The list access control for the service provider department has been configured to deny access to flight management department, excepting for the TCP protocol (Transmission Control Protocol) which permitted for the service providers department. The aim from allowing the service provider department to access the server is to permit the flow of the flight time and other information regarding their needs. As shown in figure 13, the service providers department has been blocked from accessing the flight management department.

```
Airport(config)#access-list 100 deny ip 192.168.0.0 0.0.0.255 192.168.1.0
0.0.0.255
Airport(config)#acc
Airport(config)#access-list 100 per
Airport(config)#access-list 100 permit any any          Deny 192.168.0.0 accessing 192.168.1.0
% Invalid input detected at '^' marker.

Airport(config)#access-list 100 permit ip any any
Airport(config)#int
Airport(config)#interface f
Airport(config)#interface fastEthernet 0/1
Airport(config-if)#ip acc
Airport(config-if)#ip access-group 100 in
Airport(config-if)#
```

Figure 13. Deny service providers department from access to the flight management department.

Otherwise, figure 14 shows how the service providers' network has been permitted to access only the data server place in the flight management department network, referring the security policy.

```
Airport#  
Airport#conf  
Airport#configure t  
Airport#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Airport(config)#  
Airport(config)#  
Airport(config)#  
Airport(config)#  
Airport(config)#access-list 100 permit tcp 192.168.0.0 0.0.0.255 host 192.168.1.30  
eq 80  
Airport(config)#  
Airport(config)#
```

Copy Paste

Figure 14. Service provider's network accessing the by TCP protocol.

The access-list's TCP port configuration has been configured with (matched only packets on a given port number) which means that the only matched TCP protocol is going with the port number 80. After the configurations are placed on the router, the following steps will show which departments communicate with each other and which cannot.

2.2.2 Results

The first test conducted between the arrivals, departures and guests' department with the other departments is shown in figure 15 and 16.

```

Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 192.168.0.23

Pinging 192.168.0.23 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.0.23:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

```

Figure 15. Result of deny arrivals, departures, guests' department from accessing other departments.

```

Ping statistics for 192.168.1.7:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>ping 192.168.1.7

Pinging 192.168.1.7 with 32 bytes of data:

Request timed out.
Request timed out.

```

Also, cannot ping flight management department

Figure 16. Result of denying arrivals, departures and guests' department from accessing flight management department.

Also, the service providers' department can access just to the server with IP 192.168.1.30 in the flight management department and TCP protocol has been used to establish this connection as shown in figure 17.


```

PC>ping 192.168.1.30

Pinging 192.168.1.30 with 32 bytes of data:

Reply from 192.168.1.30: bytes=32 time=1ms TTL=127
Reply from 192.168.1.30: bytes=32 time=0ms TTL=127
Reply from 192.168.1.30: bytes=32 time=0ms TTL=127
Reply from 192.168.1.30: bytes=32 time=3ms TTL=127

Ping statistics for 192.168.1.30:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 1ms

PC>

```

Figure 17. Result of accessing service provider's department can access with TCP protocol.

The reason for placing the service provider's server in flight management department was to provide a high security level for the server. This server contains the service provider's department information, which includes this information is passenger's information, so the importance of this server is similar to the flight management server. The, access-list control plays a large role in the security plan and helped to protect the network's elements from any renditions packets.

2.3 MAC address port security

In this step of security, the strategy was taking place of layer two, this layer include the switching device and the physical connections. In the OSI model (Open Systems Interconnection model), also, layer two is represented by Data Link layer. The most important and practical way to protect the network in layer two is with the port security tools. This tool works with the MAC address of any device that is connected to the Ethernet-based network.

2.3.1 MAC address port security design

In this project, this tool has been used with more than one department, depending on their importance and unique needs, some departments will shut down services when presented with an unknown device. On the other hand, the rest of the departments have been designed to deal with unknown devices as a violation. In the arrivals, departure and guests' department many public devices have been placed for numerous users; these devices provide a variety of services. The port security policy can take more than one direction; the security configuration can be for individual devices, or it could be for a group of devices depending on their first connect to the network with this network, the configuration must implement the security policy up to each department. According to Cisco Systems, Inc. (1999–2004):

After you have set the maximum number of secure MAC addresses on a port, the secure addresses are included in an address table in one of these ways:

- You can configure all secure MAC addresses by using the switch port `port-security mac-address mac_address` interface configuration command for access, private VLAN host, and private VLAN promiscuous ports.
- You can configure all secure MAC addresses by using the `port-security mac-address VLAN range` configuration command for trunk and private VLAN trunk ports.
- You can allow the port to configure dynamically secure MAC addresses with the MAC addresses of connected devices.

- You can configure some addresses and allow the rest to be dynamically configured.
- You can configure MAC addresses to be sticky. These can be dynamically learned or manually configured, stored in the address table, and added to the running configuration. If these addresses are saved in the configuration file, the interface does not need to relearn them dynamically when the switch restarts. Although sticky secure addresses can be manually configured, it is not recommended.

All the options of configuring port security can provide granular security but each one of them will have specific reporting. This technique allows the network administrator to set up the security policies regarding the network design and security aspect. In the airport's network the arrivals, departures, and guests' department switch, the port security should be configured as sticky port security because of the high security level for the future. Sticky port security can learn all the MAC addresses of the connected devices which helps to track all the connected devices in that department. Distinctly, the service provider department has violation modes; this configuration will report each unauthorized connection in that department. The reason for using this configuration was the service provider's department is more reliable than the arrivals, departures, and guests' departments. Port security with shutdown configuration can cause many problems during serving the customer, the most important one is to delay the passenger's process, when the network administrator is not available. In the flight management department, the security port has been configured manually because of the department has few devices and this range should be tightly controlled. Also, this department contains important devices which

contain the control tower information and flight scheduling. Soon, the port security has been designed for maximum reliability and safety.

2.3.2 MAC address port security configurations

The configuration steps started from the arrivals, departure and guests' department because this department is untested department depending on the project's design roles. Knowing that, these configurations have been designed with relevance to Stretch (2010). These configurations were assigned for the public computers with taking the maximum rate for protection. Accordingly, any connection for unknown devices will shut-down the service from that port. This is implemented by applying the following steps.

- The first step was checking the port security configurations options and chose the appropriate one for this department as shown in figure 18.

```
Switch(config-if)#switchport port-security ?
  mac-address  Secure mac address
  maximum     Max secure addresses
  violation    Security violation mode
  <cr>
```

Figure 18. Switch port security options

- The second step was configuring the 'sticky' because of the utility that allowed the switch to learn the all connected devices from the first step of the connected machines startup as mentioned in previously, figure 19 and 20 show that.

```
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#
Switch(config-if)#
```

Figure 19. Switch port security sticky option.

```

interface FastEthernet0/2
  switchport mode access
  switchport port-security
  switchport port-security mac-address sticky
  switchport port-security mac-address sticky 00D0.589B.53E4
!

```

Figure 20. Assign mac-address to sticky option.

- The third step was assigning the maximum number of the devices that can be learned automatically. For this setup each device has been assigned for one MAC address not to offer any other connections possibility, as shown in figure 21.

```

Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#

```

Figure 21. Assign mac- address for each device.

- The fourth step was choosing and defining the violation policy for each port. In this case, the shutdown option has been chosen to ensure that each unknown device will not have the opportunity to try connection more than once and also gives an automatic alert to the network administrator. This option was placed in the public use computers, figure 22 and 23 show the option of establishing this task.

```

Switch(config-if)#switchport port-security violation ?
protect Security violation protect mode
restrict Security violation restrict mode
shutdown Security violation shutdown mode
Switch(Config-if)#switchport port-security violation

```

Copy Paste

Figure 22. Port-security violation mode.

```
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#
```

Figure 23. Port-security shutdown.

- The fifth was defining an IP address which refers to the same IP on the authorized machine to ensure the port security policy; figure 24 shows the authorized machine's IP setup.

Figure 24. Port security policy.

2.3.3 Results

The same IP has been placed on other machines but still cannot access because the mac address was not matching the switch authorized number as shown in figure 25.

```

Command Prompt

Packet Tracer PC Command Line 1.0
PC>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>

```

Figure 25. Result of not matching mac address.

Immediately, the port went down because of the unauthorized device connection as shown in figure 26.

```

Switch#show interfaces fastEthernet 0/2
FastEthernet0/2 is down, line protocol is down (err-disabled)
  Hardware is Lance, address is 000b.beab.aa02 (bia 000b.beab.aa02)
  1000000 Kbit, DLY 1000 usec,
    reliability 100/100, tx load 0/0, rx load 1/100
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo

```

Figure 26. Port-security policy report.

Also, the violation logging for this authorized device has been recorded in the switch's memory, as shown in figure 27.

```

Switch#show port-security interface fastEthernet 0/2
Port Security          : Enabled
Port Status            : Secure-shutdown
Violation Mode         : Shutdown
Aging Time             : 0 mins
Aging Type             : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses  : 1
Total MAC Addresses    : 1
Configured MAC Addresses : 0
Sticky MAC Addresses   : 1
Last Source Address:Vlan : 0000 5674 374C:1
Security Violation Count : 1
Switch#

```

Copy Paste

Figure 27. Violation for authorized device recorded.

At the end of the above steps, the airport's network includes another security tool which can stop specific types of attacks from inside and outside the network. While not all types of attacks can be stopped by this tool, this tool still counts towards creating a high level of security.

2.4 Domain Controller Server

The domain controller server is a special kind of computer that has specific properties for special tasks. This server is a part of Microsoft Corporation suite which is designed for security and other services inside any network. On the networking side, this server is used to establish a login and other security permissions. Also, this server is usually placed inside the computer network and can provide a high storage space. According to Mark et al (2013),

Domain is a collection of objects that share the same database. That means that in our workgroup example you would create one Joe in the central Active Directory database and connect workgroup computers 1 and 2 to this database domain. Why you use a domain? If all objects are managed centrally, you don't need to connect to or walk to each computer to change the user's password.

Like it, many common computers which are located in the local network can be controlled by the Windows Server specifically the active directory tool in the server. The active directory contains many services but in this part, all the configurations focus on the domain controller utility depending on the project scope. As Mark also states, the Active Directory Domain Services (AD DS) represent a specific service that is placed in the Windows server operating system as a part of the server's software. To configure and enable this service any network administrator or advanced user needs to create the Active Directory Domain Services on the system with other important configuration requirements to have a complete domain environment like DNS service. At the same time, this tool can be stopped and started at any time because it is a service that runs in the background. Therefore, the administrator does not need to boot to the recovery mode each time to stop or start the service. Moreover, the Active Directory has another copy on the server which helps to recover the files during the process; this can help to save the file in a safe place when the system goes down (p. 258). On the other hand, it is better to have the Windows Storage Server in the same location of the domain service. This utility will allow the users to keep their files in specific partition when they log in to the domain.

2.4.1 Design

This airport's network domain as planned to provide two services: security and storage. The services took advantages of the distinctive computer network design in the two departments of the airport's local network, as shown in figure 28.

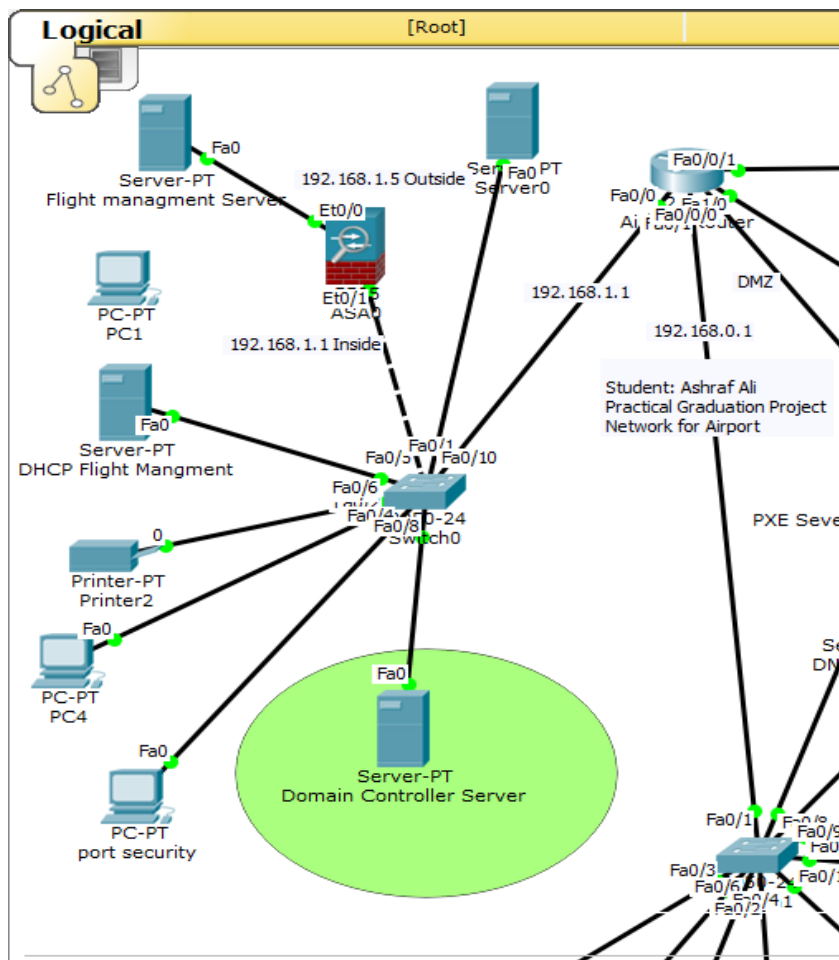


Figure 28. Domain control server design.

The storage service contains a physical device which has been placed in the flight management department and connected directly to the domain controller server. This can help each user in the network to have his own partition when he logged in to the domain.

Also, these services are contacted under specific security rules. The service provider's department employees can access the domain service. However, the domain active directory placed security policy for each user depending on her/his position in the airport's network. For example, the services provider's department employees can read only from the data storage server which is placed in the flight management department. Also, the service flight management department's employees have all permissions in the data storage server like read, write and

execute. Otherwise, some of the information technology department's employees have all permissions for all computers in the airport's local network. They can remove, install, configure, maintain and set up programs on the all connected computers. Moreover, each employee must have his unique username and password to join to the domain for accessing the machine which will has an available storage portions spaces. On the other hand, the arrivals, departures, and guests' department cannot access to the domain controller server and the domain storage service. The domain controller server are hosted in secure placed which provide high security level for the network as a general. The reason for that is, the arrivals, departures, and guests' department has been designed and configured to provide internet service and some computers for public use only. As mentioned before arrivals, departures, guest's department cannot access to the other two departments because of the airport's network security policy, so the service in this department configured for limited purposes.

2.4.2 Active Directory Domain Services and Domain Controller Configurations

First, of all the domain controller server 2012 R2, was assigned with two organization units. Each unit has been configured for the separate department in the airport's network. The flight management department has its own unite which has been configured with specific security policy depending on the department's roles. Also, the service providers department has assigned with different roles which help the employees to access certain servers in the network. This stratgies of design has been taken because each department of the airport's network has been designed with a different IP address. For the flight management department, the domain controller unit server was installed on the virtual box which has the IP (192.168.1.2). In another side, the second virtual box's was assigned to the service providers' department with IP address (192.168.0.2).

2.4.3 Active Directory Domain Services

The first step was creating an active directory to manage the domain controller and install the Domain Name System (DNS) as a default of active directory configurations. This configuration started by adding roles and features to the domain controller server. This utility allowed the system administrator to have all the needed features for installing the active directory domain server. Figures 29 and 30 show the first step of configuring the active directory and adding roles with needed features by going to the server manager and chose Add roles and features. This was taking the roles- based or feature based installation.

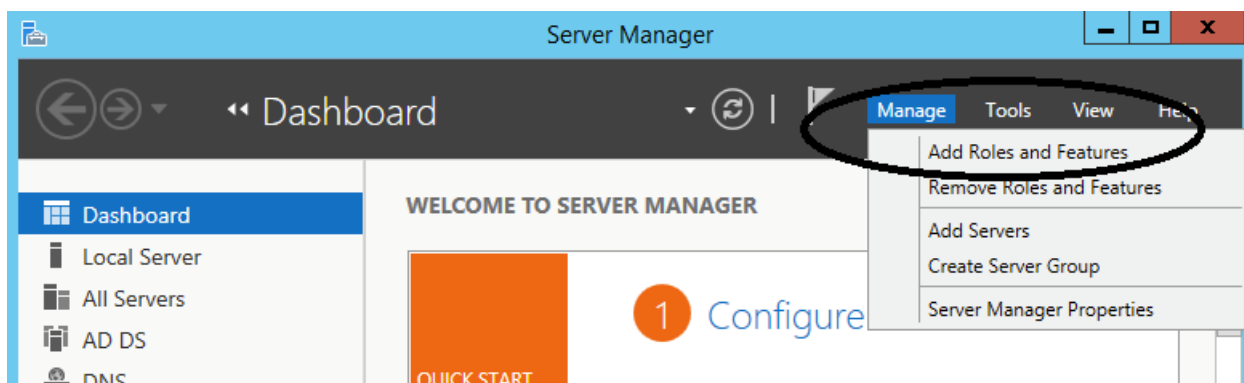


Figure 29. Active Directory Domain add roles and features



Figure 30. Role-based installation

The second step was selecting the destination's storage to place the roles and features. For the airport's network, the virtual hard disk storage has been chosen as a primary storage space which is the Windows server data center. This is configured in this way because the admin

server is installed on two different machines, so it is more powerful to install each domain separately as shown in figure 31.

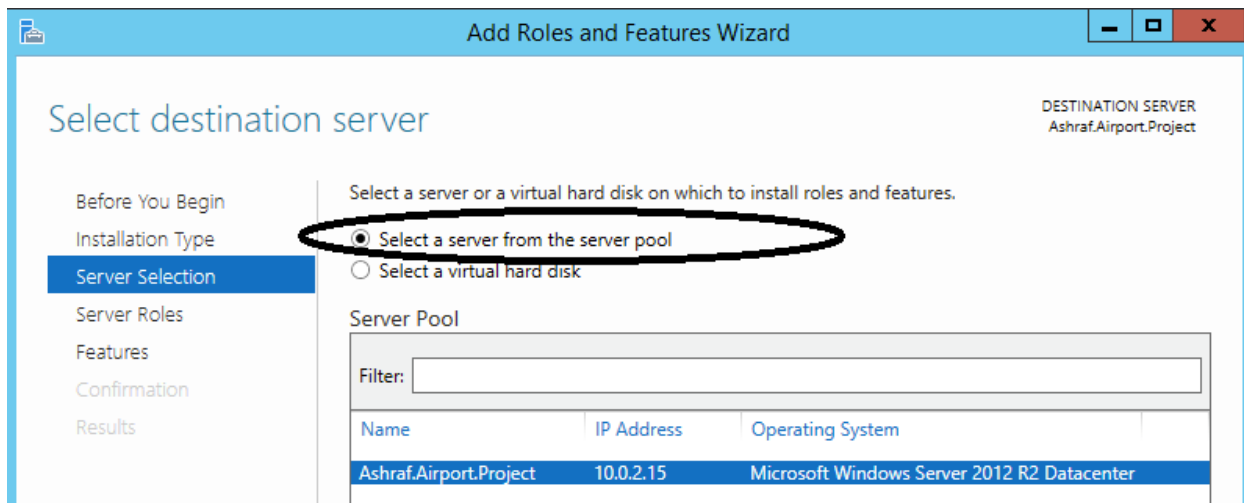


Figure 31. Sever pool

The third step was choosing the roles and services that were needed to complete the domain controller server directory. The Active Directory Domain Service and DNS service were the two most important services for completing the domain service installation. As shown in figure 32 and 33, there are other roles and features that were chosen automatically which were required for completing the installation.

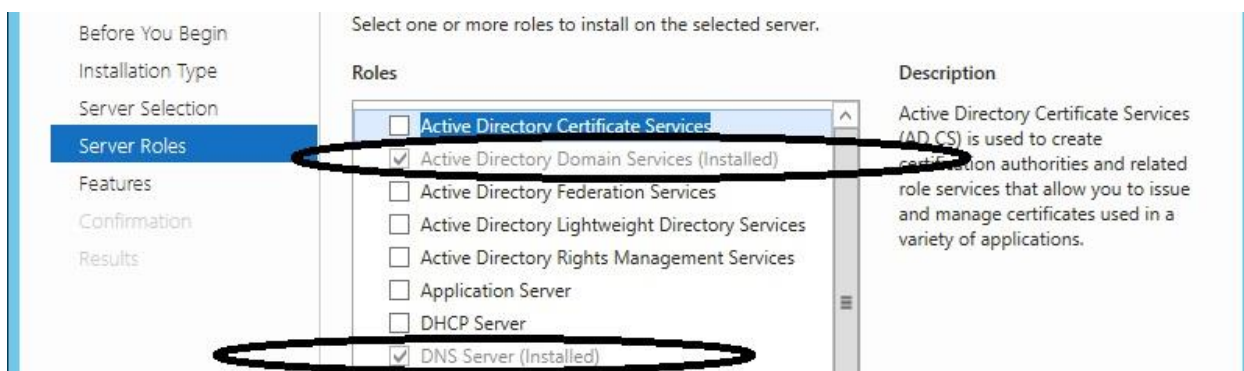


Figure 32. Active directory roles

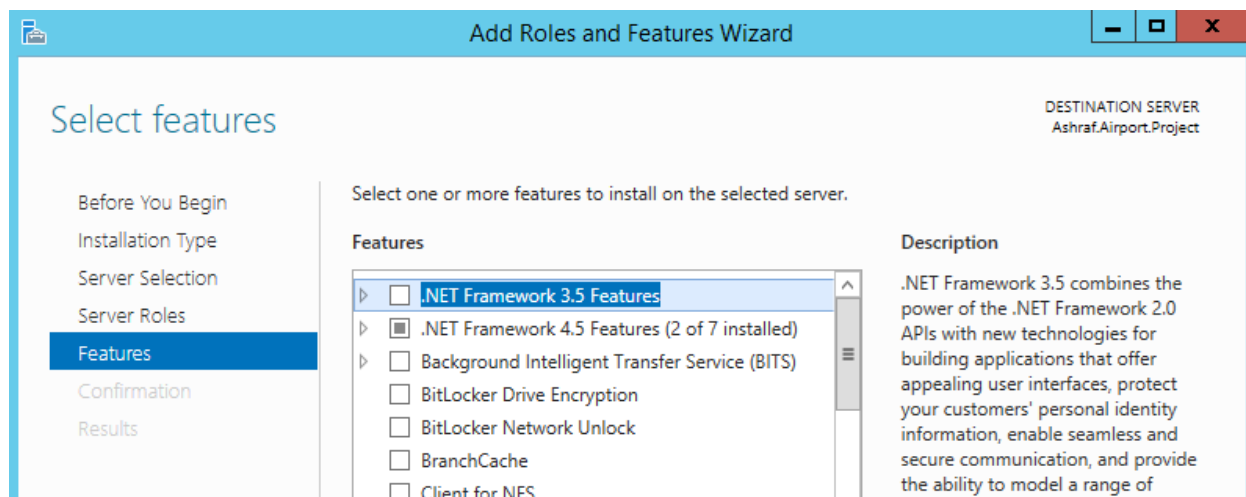


Figure 33. NET framework role.

The fourth step was the confirmation step which confirmed the configurations to continue the installing steps. It also included the option of restarting the server automatically if required and the install button to start the installations with the assigned roles and features as shown in figure 34.

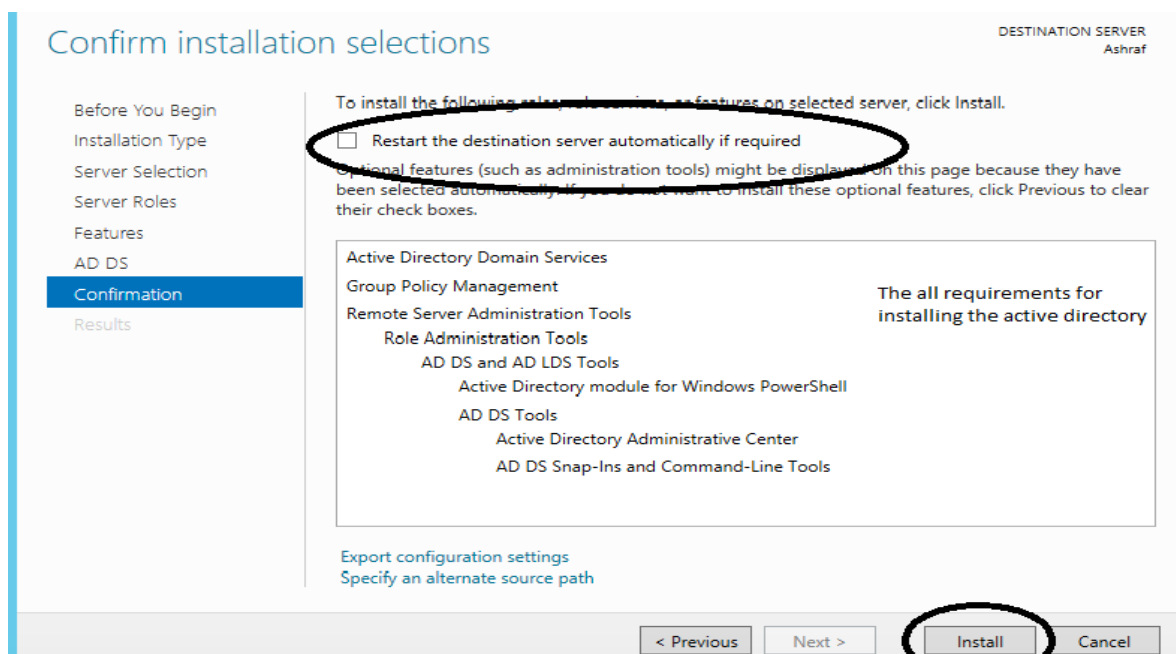


Figure 34. Active directory installation.

After these steps the server was ready to join the devices that connected to the network and define security policy for each devices' group.

2.4.4 Domain Controller

After installing all roles and features for the ADDS (Active Directory Domain Services), the following configuration set on the AD (domain controller) which is the main aim for the airport's network. The following steps include the steps that have been taken to configure the domain controller and to add the users to the domain.

The first step of domain controller setup was promoted the serve to active directory in the domain controller as shown in figure 35.

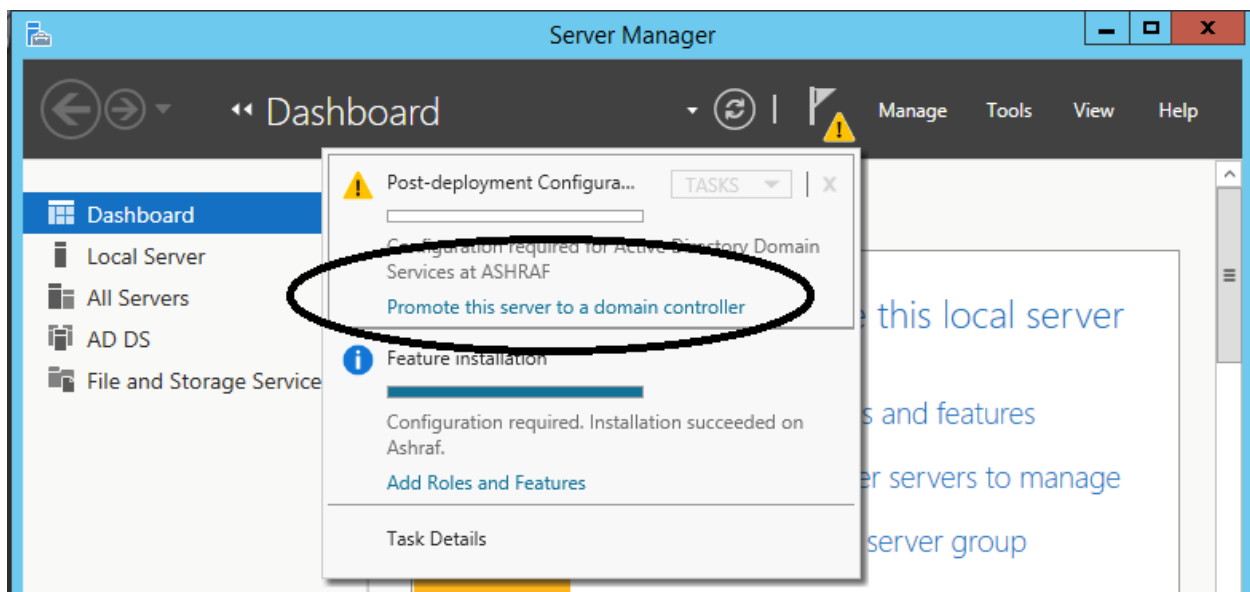


Figure 35. Promoting the active directory

Next the domain controller is setup and called (Airprt.Project) depending on the airport's network project as shown in figure 36.

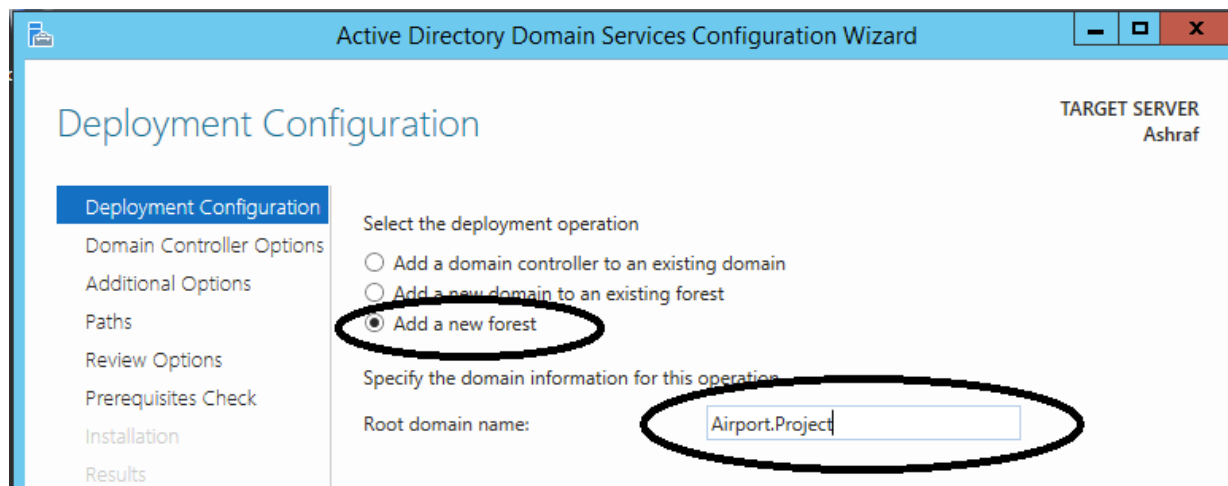


Figure 36. Specify Domain information

The third step was assigning the domain functional level, and 'forest' functional level and specify the domain controller capabilities by installing the DNS server. At the same time, it was important to assign the security policy to the domain; this was helping to assign the connected computers in both departments to the domain. The network administrator can add and remove machines in the local network. Therefore, the the directory services restore mode (DSRM) password has been assigned for this purpose, as shown in figure 37.

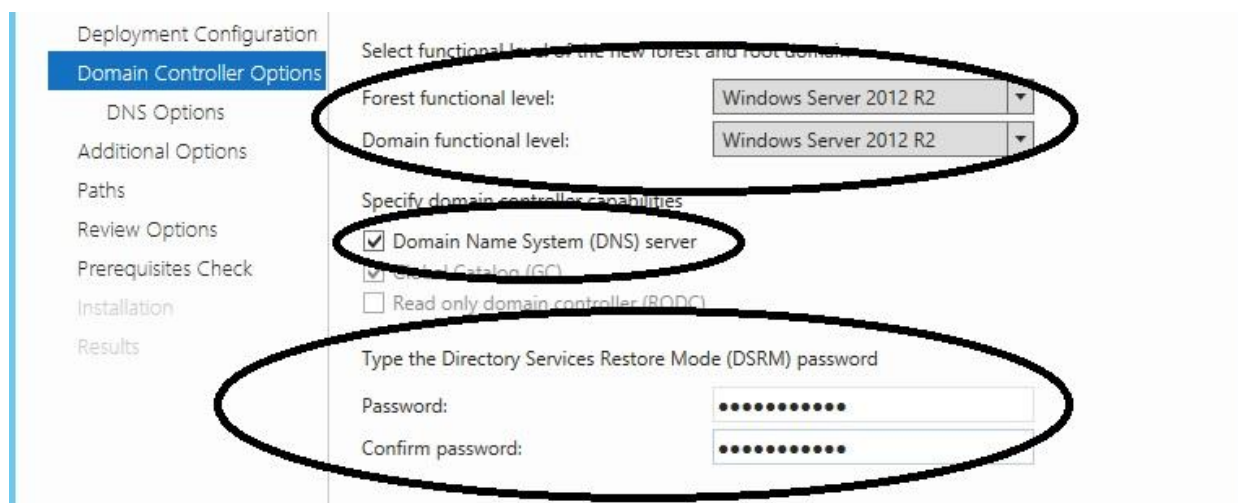


Figure 37. Domain controller options.

The fourth step of configuring the domain controller was checking the NetBIOS name and making sure that the name was verified with the assigned name in the previous steps of the configurations and changing it if that was necessary for the administrator needs, as shown in figure 38.



Figure 38. Verify NetBIOS name.

The fifth step was checking the path for the active directory which should be in the C: drive which is the default path for Windows installation as shown in figure 39.

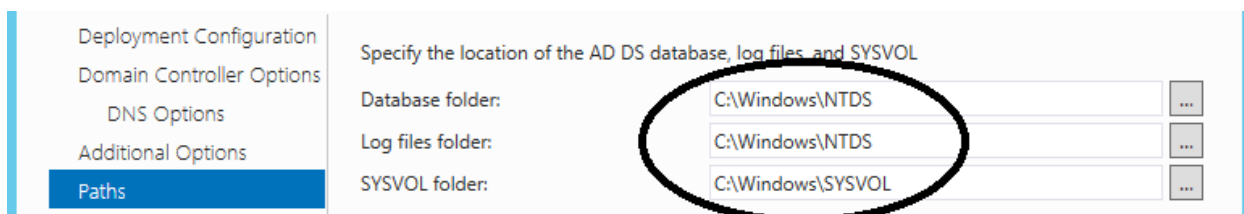


Figure 39. Domain server path.

The sixth step was reviewing all options that have been configured during the installation process and making sure that all services that were required to configure the Domain Controller are available before the installation as shown in figure 40.

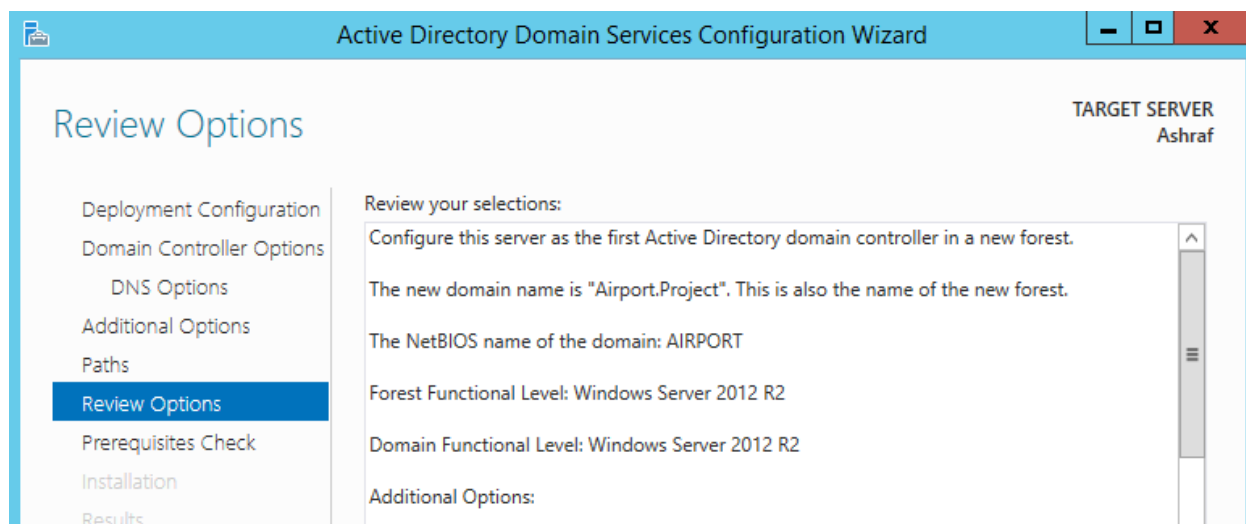


Figure 40. Review the selections.

The last step of the installation was making sure that all installation requirements have been passed successfully and are ready to request the required files for the installation and start the installation progress as shown in figure 41.

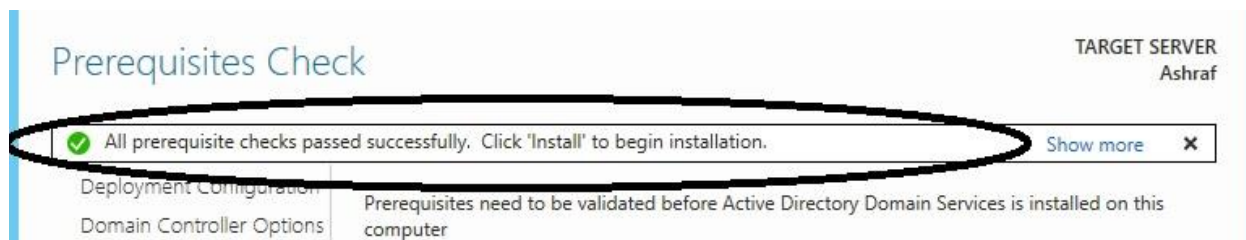


Figure 41. Prerequisite domain controller installation.

The final stage was obtaining a Domain Controller Directory that contains containers as shown in figure 42 and 43.

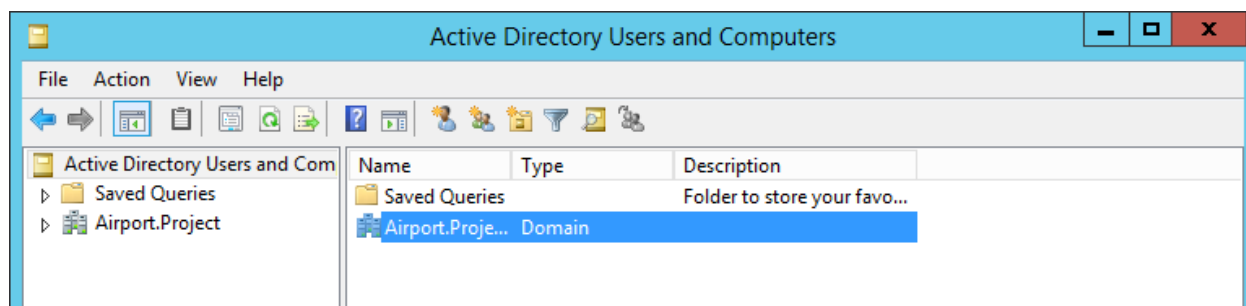


Figure 42. Airport domain controller directory.

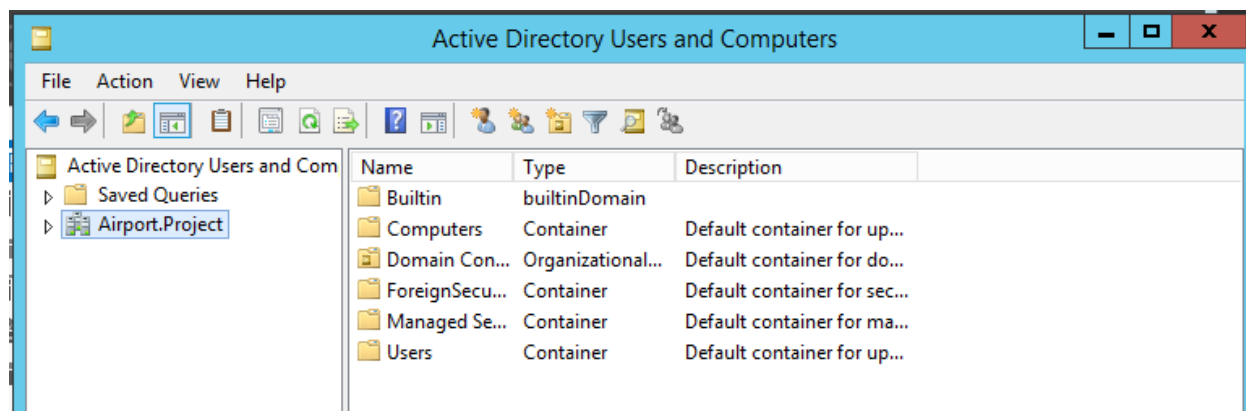


Figure 43. Airport domain controller directory options.

With this of configurations, the domain service was ready to support to any machine in the flight management department and service providers department. Each machine was able to join the domain changing the domain name of the machine as shown in figure 44.

After configuring the domain controller on the Windows server 2012 R2, it is necessary to assign security policy for each member or group in the airport. These policies help to protect software and hardware problem from end users community with limited technology skills. Each security level has been assigned to a specific organization and with limited permissions through

use of the group policy object tool. The following steps will show the strategies that have been taken and assigned to each group of users with their departments in the airport's network. Moreover, each department has been assigned specific origination units (containers) which contain all devices' permissions for each department. These domains represented individually and all organizational units are part of the main domain controller, but they are configured to act like separated domains. Also, these departments have been assigned to different groups which compatible with the network communications authorizations. For example, the flight management department has more access the airport's network in general, versus other departments which provide granular permissions access. Stanek's (2012) project found the following:

Computers are assigned to sites based on their location in a subnet or a set of subnets. If computers in subnets can communicate efficiently with one another over the network, they're said to be well connected. Ideally, sites consist of subnets and computers that are all well connected. If the subnets and computers aren't well connected, you might need to set up multiple sites. Being well connected gives sites several advantages:

- When clients log on to a domain, the authentication process first searches for domain controllers that are in the same site as the client. This means that local domain controllers are used first, if possible, which localizes network traffic and can speed up the authentication process.
- Directory information is replicated more frequently within sites than between sites. This reduces the network traffic load caused by replication while ensuring that local domain controllers get up-to-date information quickly. You can also use site links to customize how directory information is replicated between sites.

A domain controller designated to perform intersite replication is called a *bridgehead server*. By designating a bridgehead server to handle replication between sites, you place the bulk of the intersite replication burden on a specific server rather than on any available server in a site. (p. 229)

As a result, the above advantages domain controller sites subnet, which represented as containers in the server can provide a high level of security and limitation for the users in any position. The following steps will show how each department has been assigned to the airport's network departments and how their security policy was placed in each group.

Step one, assign the flight management to the specific group was creating an organization unit and calling it Flight management as shown in the following figures 45 and 46.

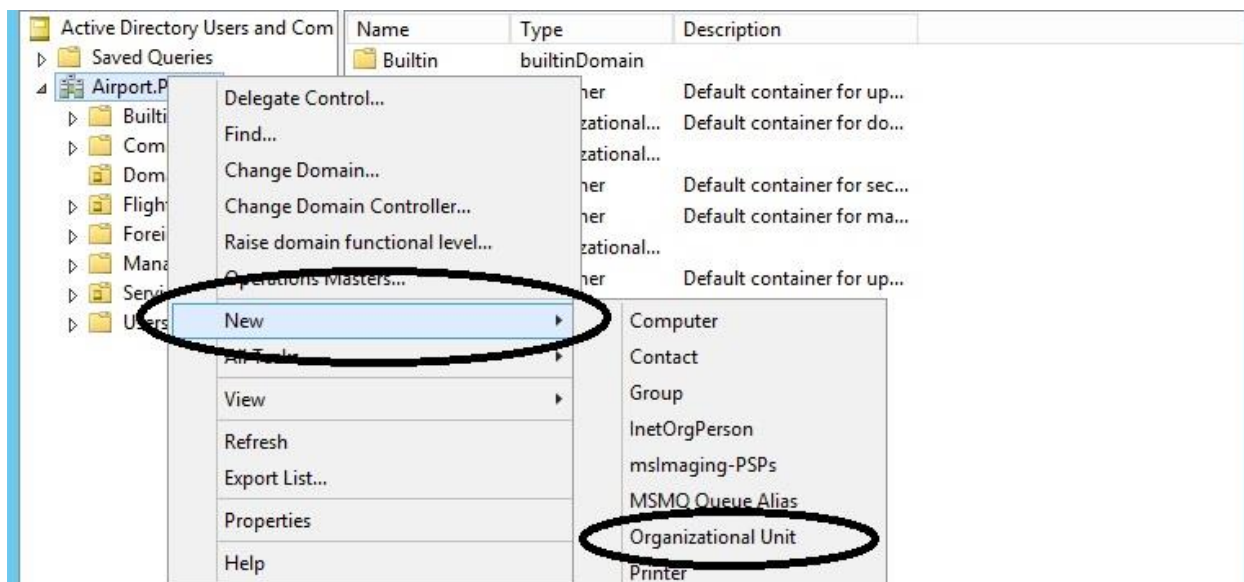


Figure 44. Organization unit for flight management department.

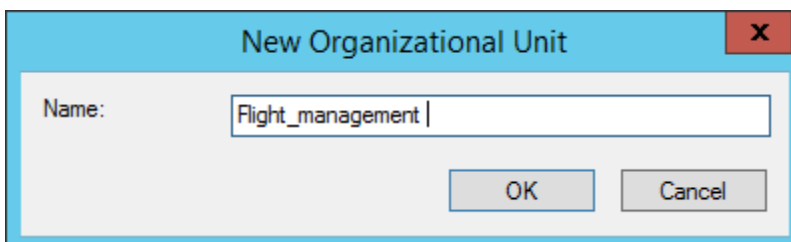


Figure 45. Organization unit name.

On the other side, the service provider's department has assigned for another organization unit on the same domain because there is a single Windows server which handles all the domain security services and is installed on the virtual machine (for example virtual box) as mentioned before. However, this department has a limited policy because of the network's security policies authorizations; figure 47 shows the organization unit name for this department that is assigned to the service providers' department.

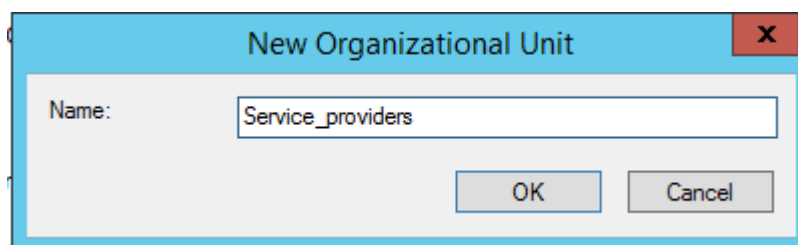


Figure 46. Organization unit for service providers' department.

After assigning each department to a specific origination's unit (group), these departments have been linked to different security policy membership. In this point the power of the group policy tool, as the Group Policy Management Console is the powerful way to define policy conditions. In the airport's network both departments have been linked to the group policy management tool, as shown in figure 48.

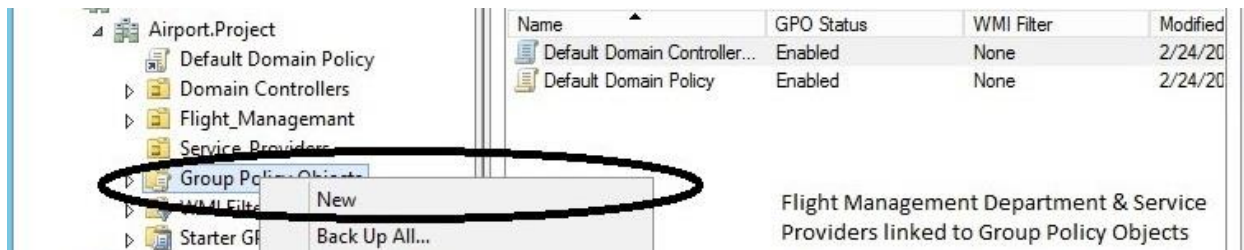


Figure 47. Assign group policy management departments.

Both departments have been linked to different policy objects, this was creates unit setting for each department, for example: the flight management department has named by **(Flight_management_policy)**. Note underscore used here because spaces can lead to issues. Similarly, the service provider’s department has named by **(Service_Porviders_policy)** as shown in Figures 49 and 50.

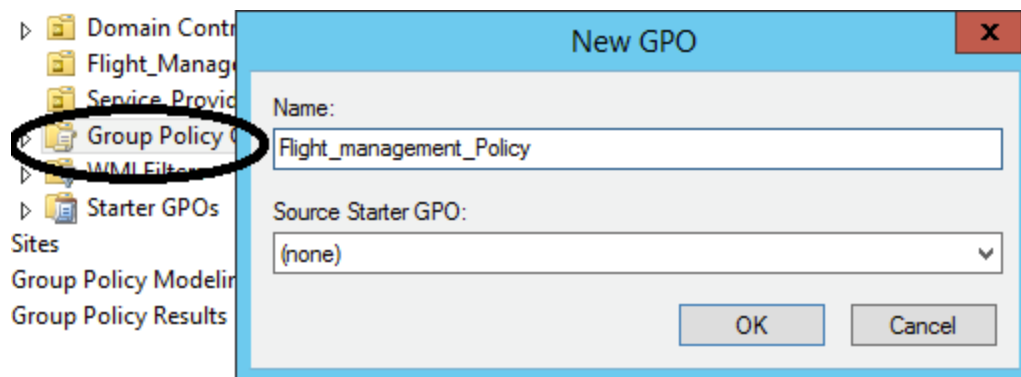


Figure 48. Flight management policy

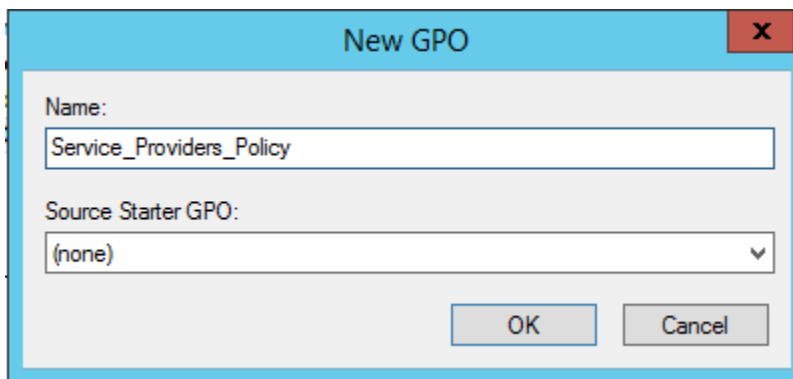


Figure 49. Service providers' policy.

The edit tool can be used to set up the policy permissions for each user in the network. In the airport's network, the most powerful permissions have been assigned to or the flight management department because the important service and flight control devices are here, so any changes cannot be obtained without help from this department. Very few permissions have been granted to the service providers department because all of the machines are placed in the departure area which can contain unreliable users, figures 51 and 52 show how edit tool used to change the user's permission.

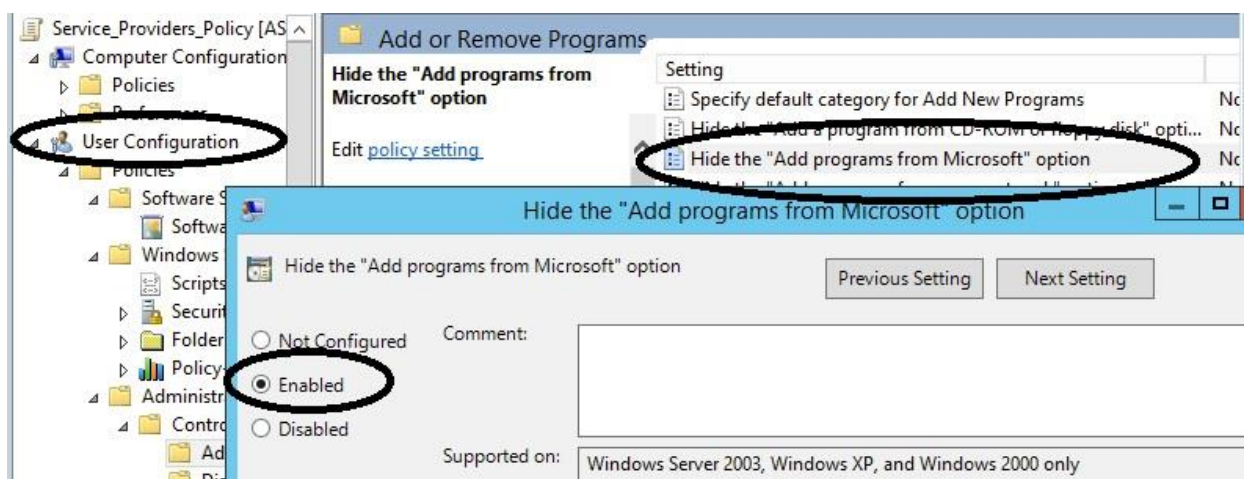


Figure 50. Hide add programs from Microsoft

As shown in figure 51, the group policy management object has placed specific permissions for the service provider's department. In this step, the users in this department cannot add programs to any machine in the network. This option has been hidden by using the group policy management editor. This means each user can use the programs that were installed by the system administrator or the information technology (IT) department who have all the permissions on the network machines. This configuration can help to avoid many software issues that can be caused by the end users. Also, any user on these machines cannot install programs that may be used to attack the network or the database server. Many other software options for each device have been hidden from the users in this department, these are related to the operating system for each computer as shown in figure 52.

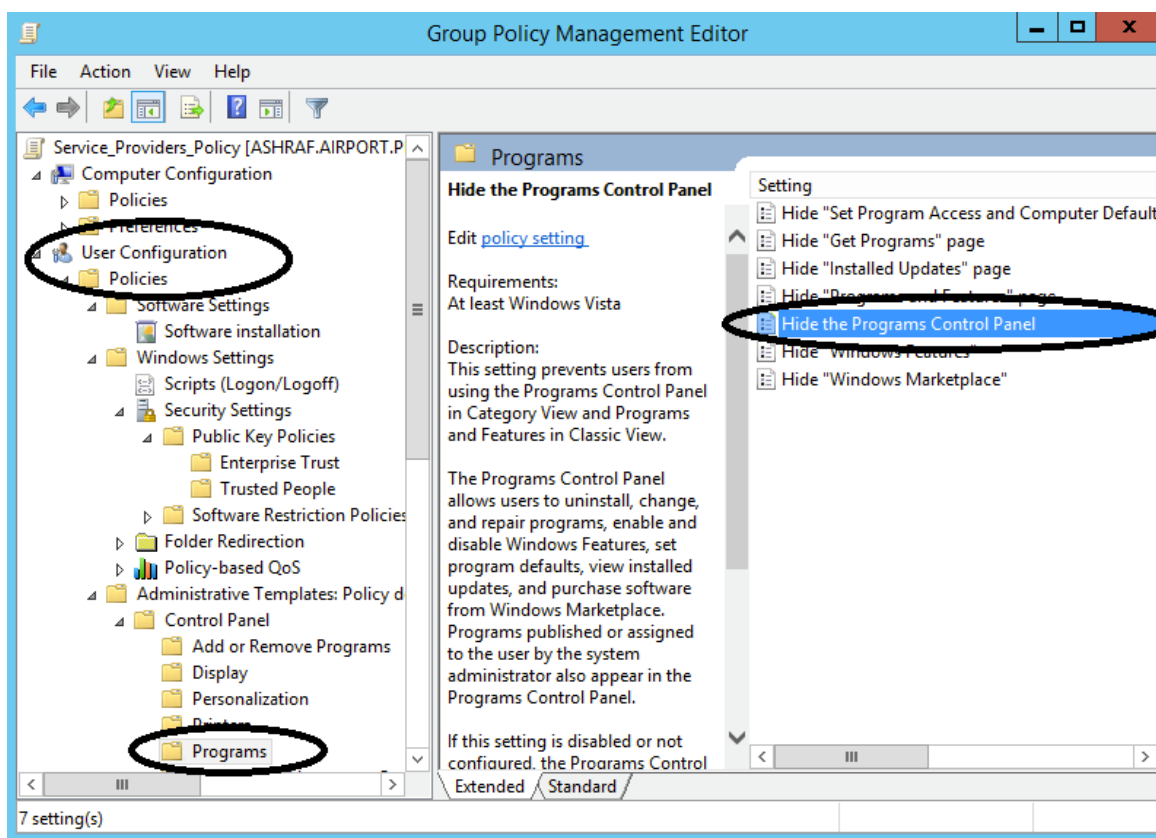


Figure 51. Hide control panel.

2.5 Proxy Server

The proxy server usually designs to hold the resources that come from the internet and save them until the users request them again. This tool allows prioritization based on user needs. Also, this server can hold the information that is requested from Internet by users and save them on its his hard disk. In many companies that have a lot of computers with different operating systems, this server helps to save the first updating request for any user in the local network and offer in immediately for the other users in the fastest way. This server provide redundancy through the return of cached data even when links are clean. According to Tsozen and Yenlin (2012), the proxy server has been used commonly because it rteduce time for requesting web sites for any external site. On the user side, this server is designed to serve many users inside the local network at the same time. In the general configurations, this server is configured to deal with the users together or separately. In case of overload request information that is not valid, the request will be sent to the proxy server to be processed, and when the proxy server has a valid copy, it will send it directly to the user. Also, if the proxy server's cache lucks the Internet, it will connect the source web server. After the proxy server receives the new information, it will send it to the user. In either situation, the client has to wait until the server collects the requested information, and store them in the cache reducing time for future requests.

The proxy server can also be used for security purposes. This server acts like a filter, all packets can be checked when they passing the proxy server. This securing layer is designed to prevent outside attack through encryption (SSL). According to Patrick (2012), all the traffic that passes through the proxy server wherever it is located will be encrypted in a proxy tunnel which links the user and the Internet. If an a hatcher attempts to listen to the communication and tries to see translation packets that transferred to or from the use's machine, he will not be able to read

the exchanged packets which pass through the server because everything has been encrypted. This provides a strong mechanism combining the proxy server except the header SSL tool. It is clear that, the security level will increase dramatically when using the proxy server on any network design.

2.5.1 Squid Proxy Server

This design a specific example of proxy server proudest called the (Squid) proxy server. This application can also websites filter or block depending on the organizational needs. Squid can managed multiple protocols including Transport Protocol (HTTP), File Transfer Protocol (FTP), Cache Protocol (ICP), Hyper Text Caching Protocol (HTCP), Cache Array Routing Protocol (CARP), and Web Cache Coordination Protocol (WCCP) among others. All these protocols are in standard of as a part of the data flows internet connectivity. This tool uses the Internet protocol (IP) address for the source and destination user's system request with their TCP port number. Checked against on access control list tool. By employing a proxy server it is possible to prevent the unauthorized communications from penetration the local network (airport's network).

2.5.2 Squid proxy server placement

Properly placed server can protect the entire network from outside attacks and to restrict inside users. For maximum impact, this server has been placed alogside the internet service providers (ISP) and the main router in the airport's network. The reason for that is that all the packets that are going from the local network and coming from outside to inside the instructions are passing through this main connection. As shown in figure 53 the squid proxy server also backs steps by the firewalls which have similar security principles but not exactly, so if some

unauthorized connection could pass the firewalls, the Squid proxy server will block them immediately.

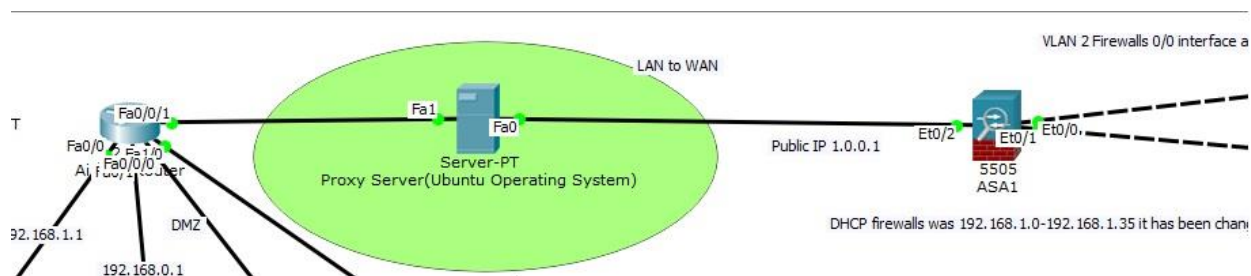


Figure 52. Proxy server design.

This double arrangement to protect the network with a focus on the internet protocol (IP) 172.16.0.1 because of this IP represent the arrival, departure, and guests' department which is the most untrusted department in the airport's network. This is because of the unknown users can access too many different websites that could be very dangerous to the airport's network as a general. In addition, this department has been provided by internet services thought out wireless access point devices which connected to the switch and the main router a high convenience with high risk capability. Without watching and controlling the users activities inside and outside this department many attacks possibilities could happen every day. On the other hand, the flight management department has its own privacy requirements including data related to the flight control system and control tower. Also, service providers' department contain passenger's information that is exchanged by the main airport's website especially when passengers provide their information from outside the network to the web server in the airport's local network. In both sides of the data transfer, squid proxy server provides the SSL mechanism which can prevent anyone from snooping your information. Therefore, this design can help to protect transferring the packets in the airport's network.

2.5.3 Squid proxy server configurations

Squid is an application that will need to be installed on a proxy server to create the necessary functionality. In the airport's network this system should run on the OS Linux family system can provide a high security level. In this design the software that has been used as mention previously was Packet Tracer, so in this software, there is no Ubuntu operating system to install a proxy server on it. Therefore, a virtual machines powered by virtual box has been used to install either configuration this service. The following step has been applied for Ubuntu operating system which installed on the VM machine.

First, the following command has been used to update the operating system, as shown in figure 54 ensuring the OS is fully patched.

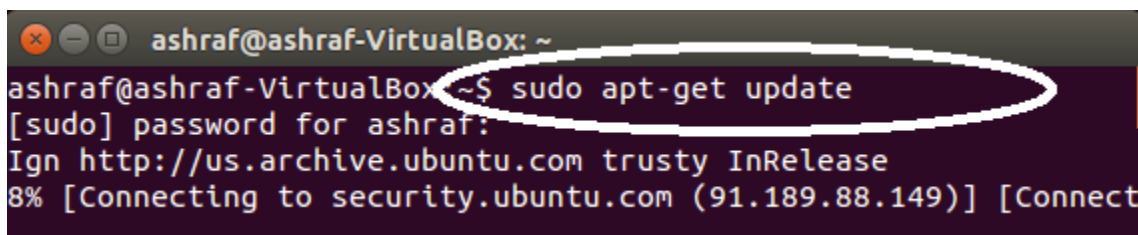
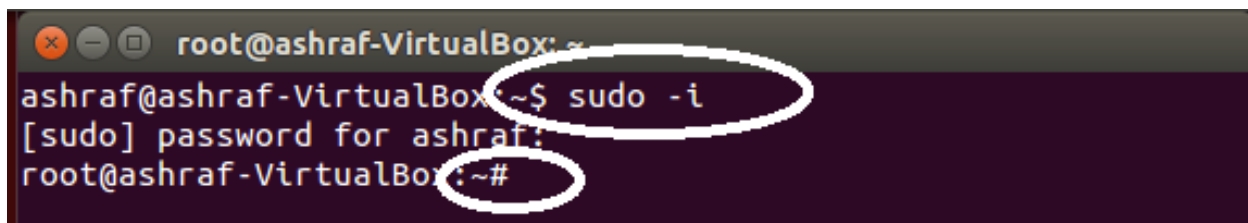
A terminal window screenshot from a virtual machine. The window title is 'ashraf@ashraf-VirtualBox: ~'. The terminal shows the command 'sudo apt-get update' being entered and executed. The prompt changes to '[sudo] password for ashraf:' and then the output shows 'Ign http://us.archive.ubuntu.com trusty InRelease' and '8% [Connecting to security.ubuntu.com (91.189.88.149)] [Connect'. The command 'sudo apt-get update' is circled in white.

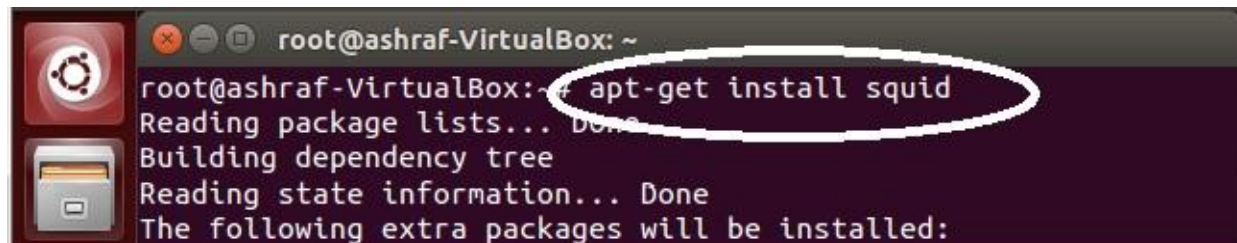
Figure 53. Update Ubuntu system.

The second step was install the Squid proxy server on the Ubuntu operating system by using the installing squid command. Before that it is possible to avoid using so before each command, by logging in as a root on your own operating system or as the system administrator for any organization by using `sudo -i` as shown in figure 55. At the same time, figure 56 shows the command that has been used to install Squid proxy server.



```
root@ashraf-VirtualBox: ~  
ashraf@ashraf-VirtualBox:~$ sudo -i  
[sudo] password for ashraf:  
root@ashraf-VirtualBox:~#
```

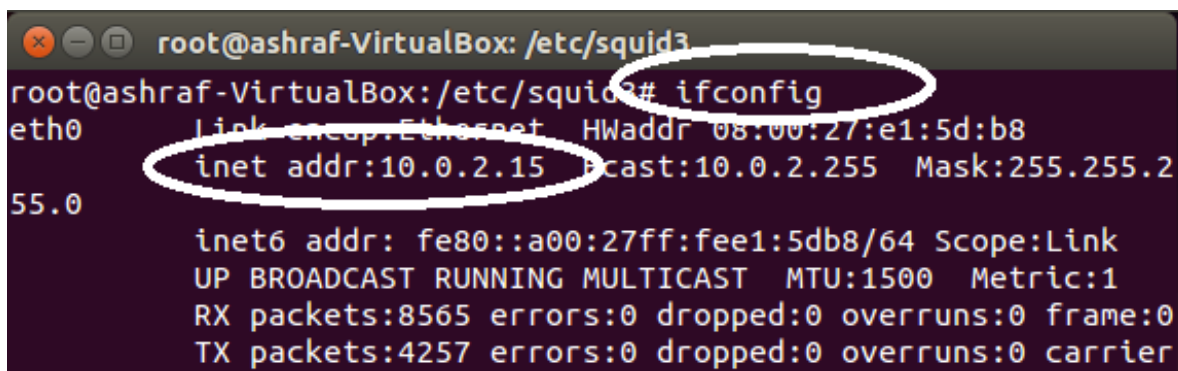
Figure 54. Root user.



```
root@ashraf-VirtualBox:~# apt-get install squid  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following extra packages will be installed:
```

Figure 55. Install squid.

The third step was testing the squid proxy server using server's internet protocol (IP) and adding it (with the port number) to the squid proxy server's web browser. This located in the proxy configuration's web browser as shown in figures 57 and 58.



```
root@ashraf-VirtualBox: /etc/squid3  
root@ashraf-VirtualBox:/etc/squid3# ifconfig  
eth0      link encap:Ethernet  HWaddr 08:00:27:e1:5d:b8  
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fee1:5db8/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:8565 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:4257 errors:0 dropped:0 overruns:0 carrier
```

Figure 56. Squid IP address.

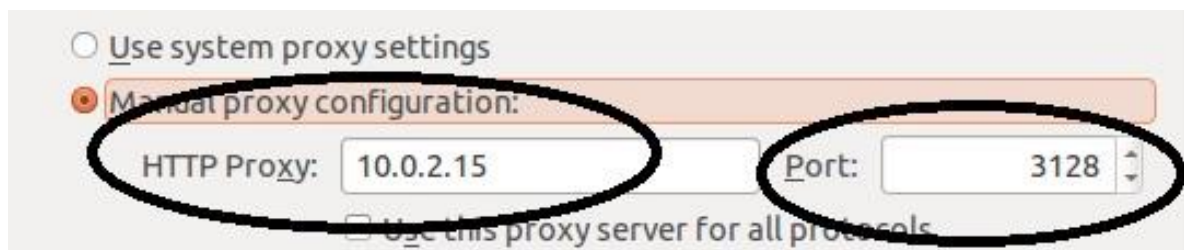


Figure 57. Connect Squid to the internet.

The fourth step was editing the squid.conf which defines for the policies in the Squid server. Any configuring steps to block websites are located in this file. Also, each Squid version has a different Squid file name. For this project the file was named squid3.conf. In the airport's network some websites have been blocked from the network because of the network administration policy. One of the blocked websites is YouTube; this configuration is applied for the squid3.config file by removing the hash sign, which allowed enabling the command configuration as shown in figure 59.

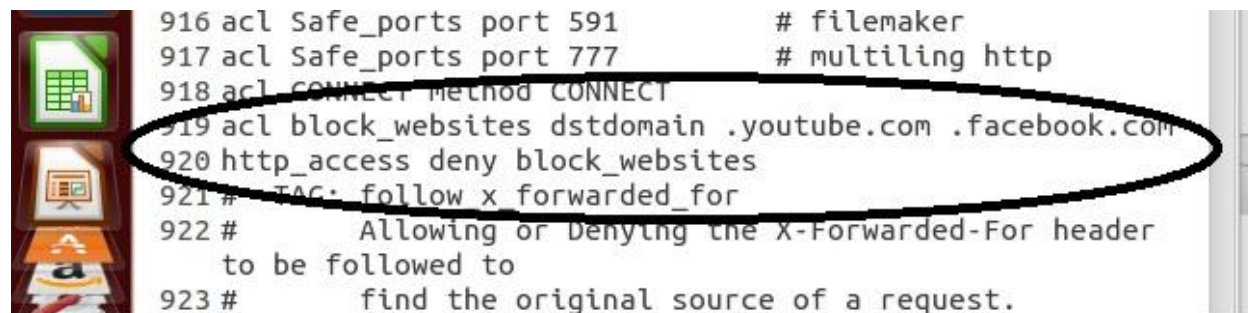


Figure 58. Block website

The above configurations were applied by restarting the squid proxy server as shown in figure 60.

```

root@ashraf-VirtualBox: /etc/squid3
root@ashraf-VirtualBox:/etc/squid3# service squid3 restart
squid3 stop/waiting
squid3 start/running, process 2833
root@ashraf-VirtualBox:/etc/squid3#

```

Figure 59. Squid restart service.

The fifth step was testing the squid proxy server and making sure that the blocked website (YouTube) cannot access the internet, which is the main aim of this server as shown in figure 61.

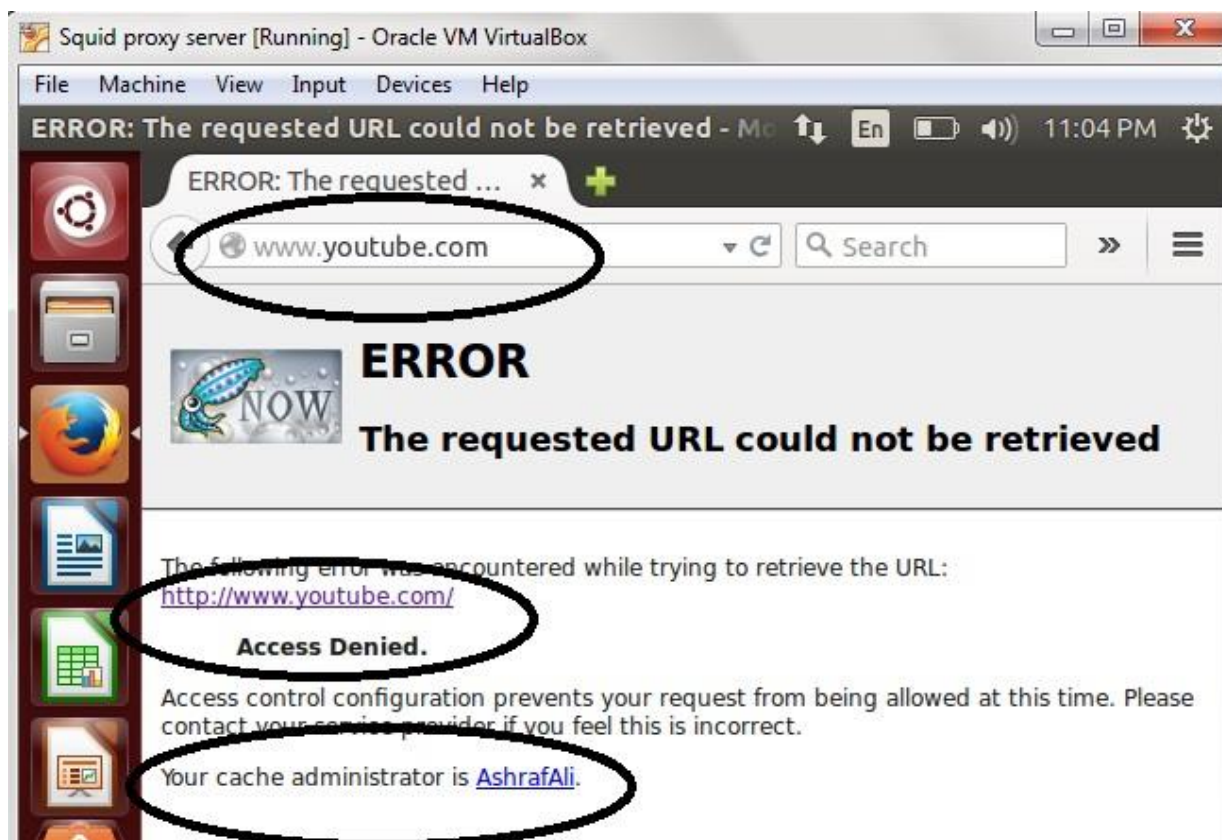


Figure 60. Proxy server websites access deny.

As shown in figure 61, the system administrator was responsible for allowing and blocking any website for the local network. In this case, the cache administrator is Ashraf Hasan Ali, who is the author for this project. However, any other websites can be accessed in these configurations, the squid3.Config file was responsible for blocking this website and allowed any other websites to be accessed from the local airport's network as shown in figure 62.

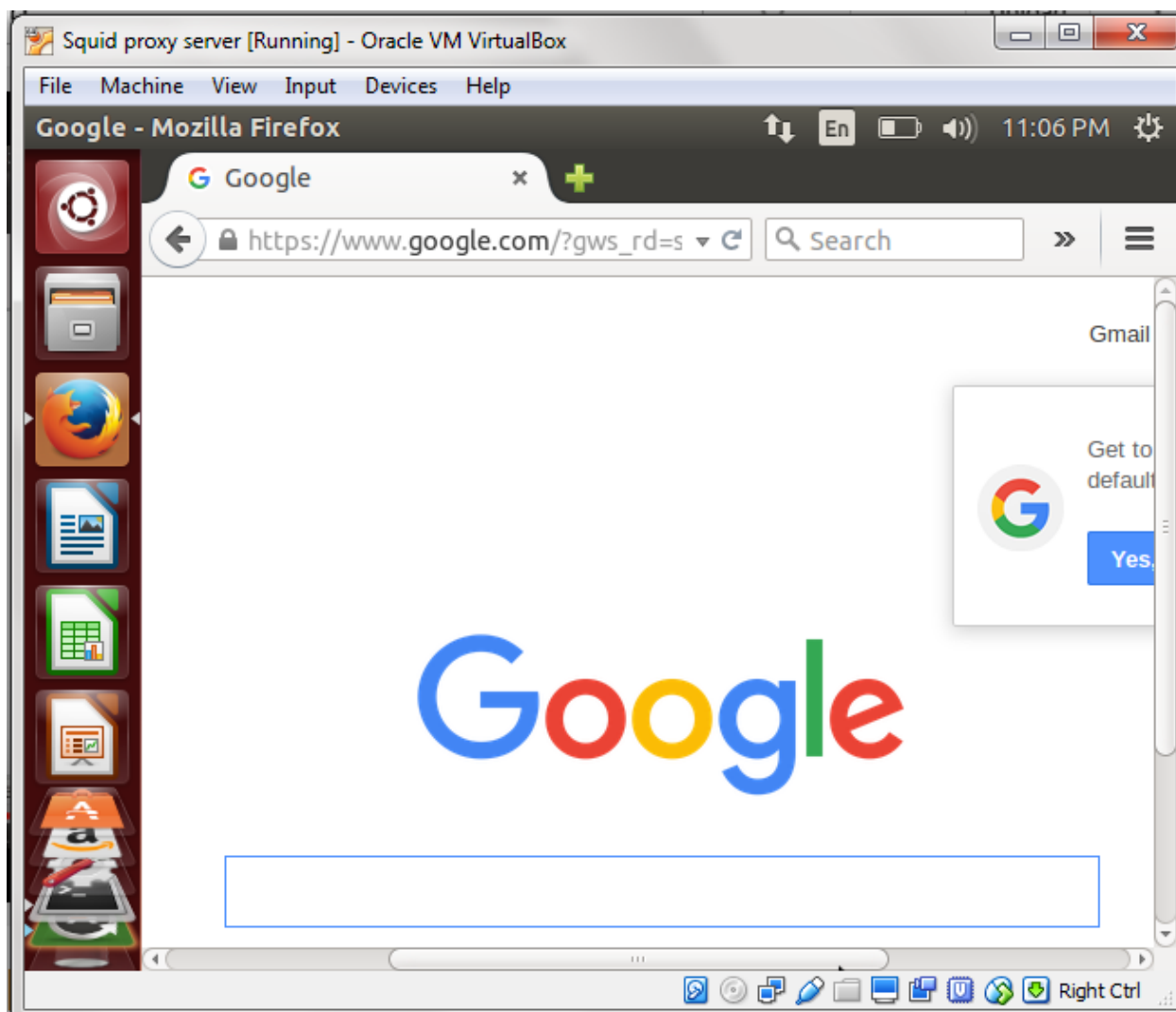
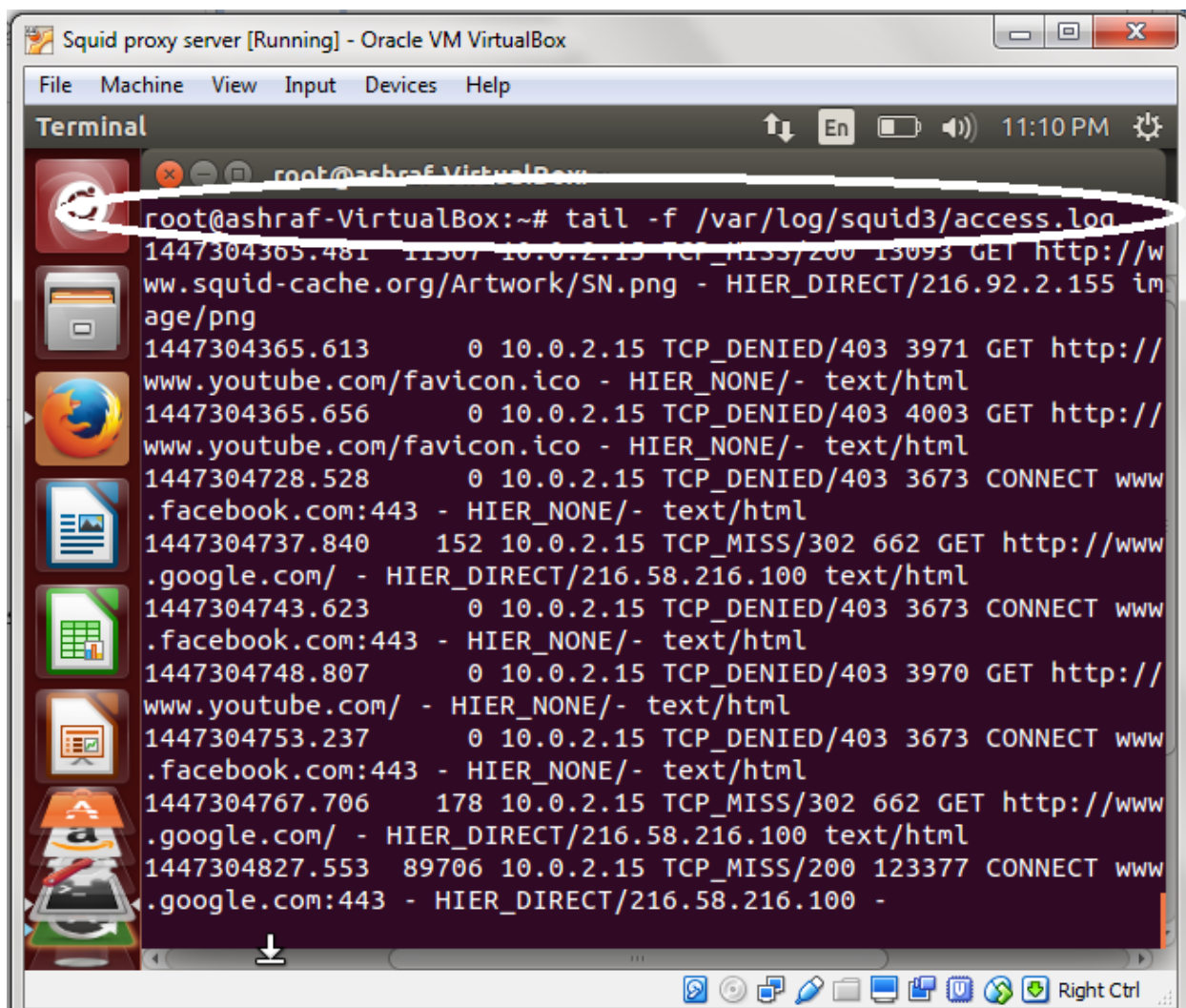


Figure 61. Proxy server access websites.

The final step was checking the monitoring service that tracks the users' activities inside the network. As a system administrator, it is very important to know which websites are accessed

every day by the users in the airport's network. This helps to decide which websites need to be available and which are blocked by using a special command as shown in figure 63. The user's activities can show if there are untrusted people using the internet to attack or plane for the terrorist attack at the airport. Nowadays many terrorist groups are using social websites like Facebook, Twitter, and others to attack any organizations around the world. As mentioned before, Squid proxy server can help to watch these people and put limitations on their activities even if they use the network for a short time during their coexisting in the airport.



```
root@ashraf-VirtualBox:~# tail -f /var/log/squid3/access.log
1447304365.481 11507 10.0.2.15 TCP_MISS/200 13093 GET http://www.squid-cache.org/Artwork/SN.png - HIER_DIRECT/216.92.2.15 image/png
1447304365.613 0 10.0.2.15 TCP_DENIED/403 3971 GET http://www.youtube.com/favicon.ico - HIER_NONE/- text/html
1447304365.656 0 10.0.2.15 TCP_DENIED/403 4003 GET http://www.youtube.com/favicon.ico - HIER_NONE/- text/html
1447304728.528 0 10.0.2.15 TCP_DENIED/403 3673 CONNECT www.facebook.com:443 - HIER_NONE/- text/html
1447304737.840 152 10.0.2.15 TCP_MISS/302 662 GET http://www.google.com/ - HIER_DIRECT/216.58.216.100 text/html
1447304743.623 0 10.0.2.15 TCP_DENIED/403 3673 CONNECT www.facebook.com:443 - HIER_NONE/- text/html
1447304748.807 0 10.0.2.15 TCP_DENIED/403 3970 GET http://www.youtube.com/ - HIER_NONE/- text/html
1447304753.237 0 10.0.2.15 TCP_DENIED/403 3673 CONNECT www.facebook.com:443 - HIER_NONE/- text/html
1447304767.706 178 10.0.2.15 TCP_MISS/302 662 GET http://www.google.com/ - HIER_DIRECT/216.58.216.100 text/html
1447304827.553 89706 10.0.2.15 TCP_MISS/200 123377 CONNECT www.google.com:443 - HIER_DIRECT/216.58.216.100 -
```

Figure 62. Squid monitoring tool.

As can be shown in the above figure, the most accessed websites are YouTube, Facebook, and Google. This allows a network administrator to watch the network activities and each users' access. This information can be used to control and monitor access, and maintain a high security posture.

3 Quality

A second offbeat that is need is reliability; accordingly, this design incorporates looks for failover. Failover utility is very powerful and was used to provide constant communication service during the network operations. This utility was located in the Cisco firewalls and routers network's devices. Usually, this configuration is used when the network has two outside connections to one device. Each link connection has a special task, the main link connection (ISP1) named primary as a default and the second named as a secondary link connection (ISP2). According to Cisco Systems, Inc. (2012):

The firewall allows a router to continue processing and forwarding firewall session packets after a planned or unplanned outage occurs. A backup (secondary) router automatically takes over the tasks of the active (primary) router if the active router loses connectivity for any reason. This process is transparent and requires neither adjustment nor reconfiguration of any remote peer.

As described above, the active link is the main provider (Active) for the network and the second one is the spare (standby) provider. In this configuration there is one supporter for the network and when it fails the second link will provide the service. Also, the failover utility deals with the internet protocols (IPs) and media access control (MAC) for each connectivity. These two sources help to give the directions to the firewall's command table, and this device takes the

actions depending on this information. When the failure happens to one of the links the negotiations will start between the both links and the configuration policy, which is address resolution protocol (ARP), will be involved in this comparison.

3.1 Failover Design

In the airport's network, this configuration has been applied to the main firewall which is connected directly to the internet service providers. At the same time, ASA was the device that has been chosen which are required configurations for this configurations part. These requirements were related to the active connection and the spare connection in the device. According to Cisco Systems, Inc. (2012), Active/Standby failover has the following prerequisites:

- Both units must be identical ASAs that are connected to each other through a dedicated failover link and, optionally, a Stateful Failover link.
- Both units must have the same software configuration and the valid licenses.
- Both units must be in the same mode (single or multiple, transparent or routed).

As clarified previously, both links should connect to the same device, or if there is more than one device, all the devices should be from the same manufacturer type to ensure compatibility. Also, all the configuration that is applied for each device should be duplicated on the others, in this example all configurations have been applied to one device which is the main firewall. Not only the firewalls devices can provide this utility service but also the router devices can present the same utility. In this project, the configurations have been applied for the firewall as mentioned before because this device was located in the foreground of the gate of exchanging the data from inside to outside and vice versa. Also, this device was designed to accept two connections from outside and provide on for the inside. The main reason for that was keeping one connection

providing the service all the time and keeping the error handling outside the main connection, as shown in figure 64.

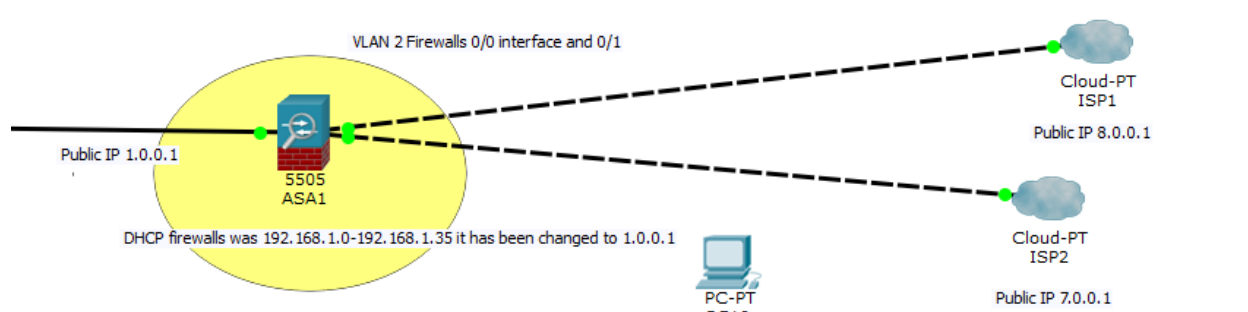


Figure 63. Failover location design.

The assigned configuration will be responsible for guiding the packets and recognizing which is the active link and which is the standby link.

3.1.1 Failover configuration

In the configuration steps there are different ways to achieve the main task of failover utility. This depends on the different types of configuration and setup of the devices. Many networks use two providers to increase performance of the communication, in this situation the failover configurations will be different, both links will be connected and when one of them cannot provide the required level the secondary provider will start to support the service until the speed reaches the required level. This represents unsuccessful technical steps because there will be collision data and the quality of service will decrease dramatically.

In this project, failover has been added to keep the airport's network reliably to the outside world, so that if one of the links goes down the other will work immediately. As mentioned before, this project used the Cisco Packet tracer simulated for design and implementation for the airport network, but unfortunately, the program has only ASA 5505 firewalls. This firewalls cannot support this configuration, or the network administrator cannot apply the following

configurations on it. The physical ASA 5505 accepts this configuration and many other Cisco firewalls. Also, the Cisco configuration document will be used as a main reference for the failover configurations. The following steps will show how the main firewall in the airport has been configured with failover utility depending on Cisco configuration devices.

The first part of the configurations is configuring the primary unit which represents the active link (service provider) in the network. Before starting the configuration steps, Cisco has some recommendations to ensure the quality of service. According to Cisco Systems, Inc. (2012), "Do not configure an IP address in interface configuration mode for the Stateful Failover link if you are going to use a dedicated Stateful Failover interface. You use the failover interface IP command to configure a dedicated Stateful Failover interface in a later step" (p. 50-8). As clearly the quote explained above, it is not recommended to assign IP for each interface that connected to the main (active) link to the service providers. According to Cisco Systems, Inc. (2012), these steps will be taken an example of configuring failover in this project.

The first step of the configuration of the primary unit is specifying the port as a primary (active) unit, as shown in the following command.

failover LAN unit primary

The second step is choosing the firewall interface to be the primary (active) link and should not be used for any other connections as shown.

failover LAN interface if_name interface_id

Example:

hostname(config)# failover LAN interface link GigabitEthernet0/3

The third step is to assign IPs for each failover link. In the airport's network, two ISPs have been providers: (8.0.0.1) and (7.0.0.1). These IPs will be used for these configurations steps as an example. As mentioned in the Cisco document both IPs should be on the same subnet and this what has been assigned for the project. Also, these IPs stay for each unit to ensure the connectivity. For example, the primary unit (active unit) will be assigned to the IP 8.0.0.1 and the secondary unit (standby unit) will be assigned with the IP 7.0.0.1. The following command shows how to assign the IPs for each unit according to the document configurations.

```
failover interface ip if_name [ip_address mask standby ip_address |  
ipv6_address/prefix standbyipv6_address]
```

Example:

```
hostname(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby  
172.27.48.2
```

```
hostname(config)# failover interface ip folink 2001:a0a:b00::a0a:b70/64 standby  
2001:a0a:b00::a0a:b71
```

The fourth step is to enable the configuring interfaces as shown in the following command.

```
interface interface_id no shutdown
```

Example:

The fifth step is enabling the failover utility as shown in the following command.

```
failover
```

Example:

hostname(config)# failover

The final step is saving the configurations to the firewall memory as shown in the following command.

copy running-config startup-config

Example:

hostname(config)# copy running-config startup config

The second part is configuring the secondary unit (Standby) to be recognized from the primary unit. Also, all the configurations will take the same steps, but only step 5 will be different because it mentions the secondary unit. These steps have been taken from the same source.

The first step is specifying the interface for the secondary unit.

failover lan interface if_name interface_id

Example:

hostname(config)# failover lan interface folink vlan100

The second step is assigning the active and standby to the failover link, the same for the primary configuration part.

**failover interface ip if_name [ip_address mask standby ip_address |
ipv6_address/prefix standbyipv6_address]**

Example:

hostname(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby

172.27.48.2

hostname(config)# failover interface ip folink 2001:a0a:b00::a0a:b70/64 standby

2001:a0a:b00::a0a:b71

The third step is enabling the secondary interface as shown in the following command.

interface interface_id no shutdown

Example:

hostname(config)# interface vlan100 hostname(config-if)# no shutdown

The fourth step is pointing this unit as secondary unit as shown in the following command.

failover lan unit secondary

Example:

hostname(config)# failover lan unit secondary

The fifth step is enabling the failover as shown in the following command.

failover

Example:

hostname(config)# failover

After this activation the primary unit sends the all running configurations which were saved in the early steps.

The final step is saving the configurations to the firewall memory, the same step for the previous configurations (primary unit) as shown in the following command.

copy running-config startup-config

Example:

hostname(config)# copy running-config startup-config

As a result, these configurations can apply for any Cisco firewalls devices to provide the failover utility.

3.2 PXE Sever (Pre-boot Execution Environment)

In the large companies that have more than 100 users on the same network, computers are the most facing devices with hardware and software malfunctions. In the software side, the end users represent the most causative aspect for damaging the computer's operating system. As a result, there should be a specific technique to solve the operating system issues because any operating system failure will affect the quality of service or it might delay the work process for each employee. In this case, the information technology department (IT technician) will have to resolve these problems as soon as possible to keep the work process safe. Also, most operating system problems could be solved by re-imaging the computers which are setting up new operating systems for these machines. If the IT technician need to install operating systems individually, how do they do it if there is more than one computer that lost its operating system at the same time sequentially? In this situation, there should be a tool that can support more than one task at the same time. A PXE server is the appropriate service to support operating systems to the clients on any local networks. This service can be provided by installing a PXE server on the local network, and the clients can access and obtain the operating systems by only connecting to the same network by using network cards. According to Cowan (2008):

By letting network administrators manage and configure client PCs over the network, PXE can help reduce the cost of ownership and simplify client management.

Administrators no longer need to visit clients to install a new operating system or update an existing system. The client can boot from the network and have the new software installed, regardless of the condition of the local hard drive. (p. 4)

Conclude with the above quote;

- a- PXE Boot can help to save the time for the technicians and the clients can get their new operating system in the fastest ways.
- b- This server can manage the computers on the network. Any user who wants to have a new operating system on their computer have to log in to the controller domain which has been configured in the earlier steps of this project.

The users who are usually from the IT department will log into the control domain and ask to set up a task to install a new operating system on any computer in the local network. The IT department will assign these permissions depending on the needs. Therefore, it is not allowed for any user in the airport's network to install a new operating system by using PXE server without getting permissions (setting task) from the IT department or the network administrator. Also, these permissions can refer to the tag numbers that's been assigned to each device on the local network. On the other hand, PXE server cannot be installed like any applications; there should be some protocols and other servers that help the communication to success and pass the packs to the right path. The main protocols that are used with the PXE server are TFTP protocol and DHCP. There are some other tools that are used with this server like Unified Extensible Firmware Interface (UEFI) standard and Network Bootstrap Program (NBP). For instance, the DHCP protocol that provided by the DHCP server specifies the location of the device that is

asking for the operating system. In other words, this protocol represents the identification and the exact location of each device in the local network. Also, it supports any device in the network with IP address dynamically with specific range depend on the subnet class for each network. According to Microsoft TechNet (2008),

When a Pre-Boot Execution Environment (PXE) boot is initiated, the PXE ROM requests an IP address from a Dynamic Host Configuration Protocol (DHCP) server, using the normal DHCP discovery process. As part of the initial DHCP discovery request, the client computer identifies itself as being PXE-enabled, which indicates to the PXE server that the client needs to be serviced. After the client has obtained a valid IP address from a DHCP server, the client attempts to locate and establish a connection with the PXE server to download a network boot program (NBP).

As clarified previously, DHCP server can provide the client an appropriate IP address which represents the clear signal to the client location in the network; the client locations are so difficult to reach especially in the huge organization, but with DHCP server, the task could be easier. The DHCP in this case (PXE server) does not represent the physical DHCP servers in the airport's network, the DHCP, in this case, is a required tool as many other tools that need to install and configure PXE server. The physical DHCP servers are located in the local network to provide dynamic IP addresses to all the clients.

3.2.1 PXE Server Design

This service should be placed in the big networks that handle many services in the same time, airports' network need to have high quality of service. If this service is provided in the network section that has a low-security level, it will put all the network in the risk. For this reason, the design should take a specific view for the network designer. For this project, the PXE server has been positioned between two high security levels departments which are the service provider's department and the flight management department; many networking security tools have protected both of the departments in the previous chapter from this project. Otherwise, the arrival, departure and guest's department have not been provided by this service because of the trusted users in this department regarding the concept of the airport's network. Also, this service has been configured with two main IPs addresses for the two departments which are (192.168.0.1) and (192.168.1.1). Both of the IPs can access the PXE server and obtain their operating systems. These IPs have been ranked in the PXE server depending on the computer's IPs in this department and their tag number. As shown in figure 65, this service has been connected to the main router and is configured to be accessed by both trusted departments.

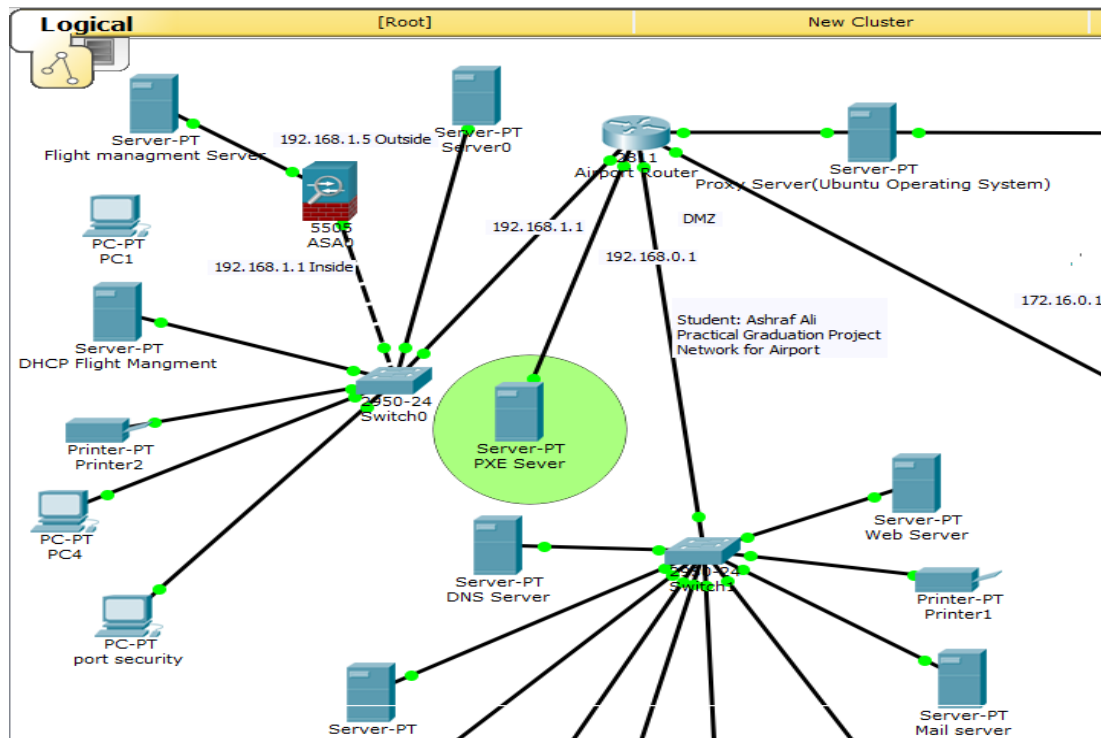


Figure 64. PXE Server location design.

As a result, this design can help to provide the operating systems to all users, which leads to an increase in the quality of the network services in the airport.

3.2.2 PXE Server Configurations

The configurations for the PXE server have been taken in more than one direction; many services were configured to establish this environment. The main tools that are:

- DHCP Server to provide dynamic IPs for users
- PXE boot server to provide operating system
- CentOS, as a bootable server
- Some packets that are needed to install like TFTP

All these requirements have been installed and configured to make the installation successful. These configurations have been placed on an Oracle virtual box. Before starting the configurations steps, there were some configurations for the virtual box specifically for the internet LANs to make it appropriate for installing the PXE server as shown in figure 66.

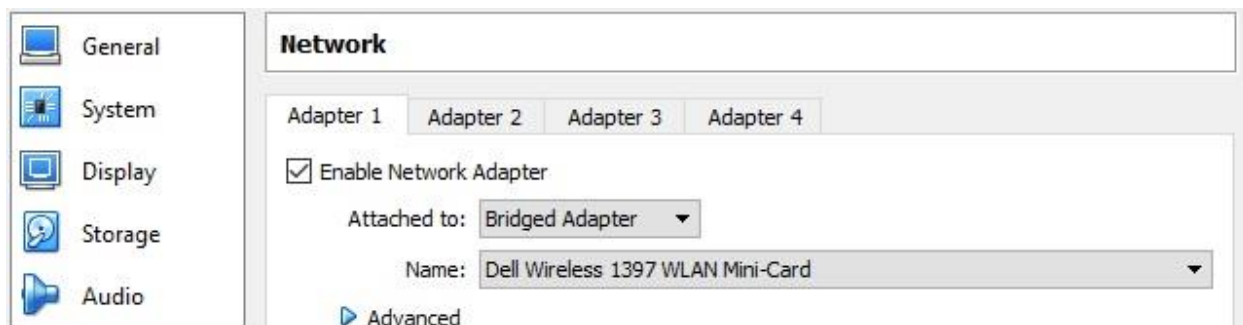


Figure 65. PXE network LAN adapters.

While most of the configurations have been assigned on the CentOS, the PXE server according to Cezar (2014). There should be two network adapters; the first one has been configured and bridged to obtain the internet from then actual computer adapter and the second one has been configured as an internal network which connects the users to obtain the operating systems.

The first step of the configurations was using both operating systems in the same virtual box as shown in figure 67, this to configure the PXE on the both systems.

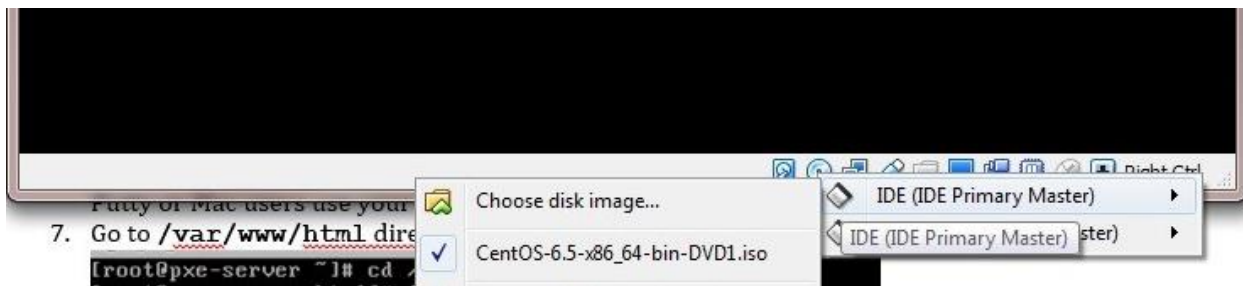
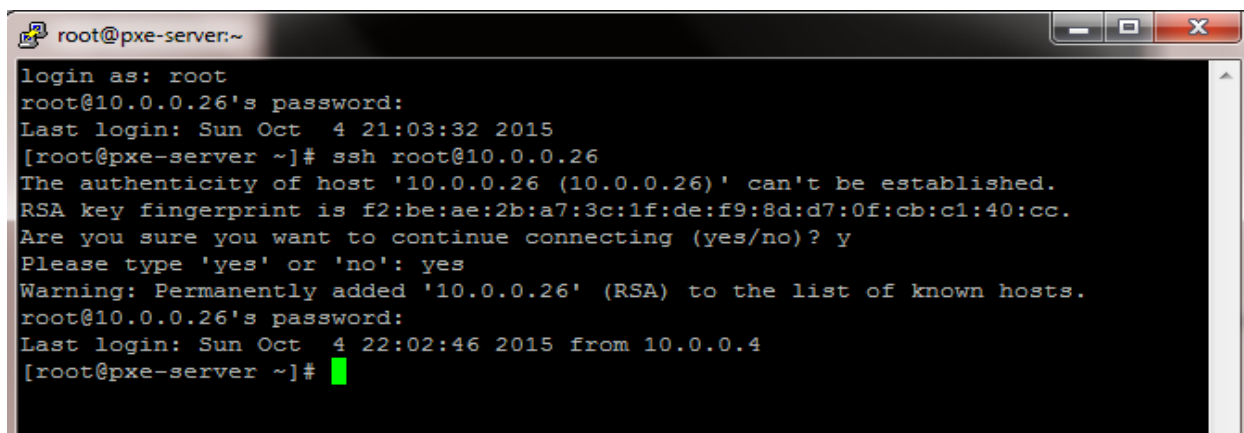


Figure 66. PXE operating system image.

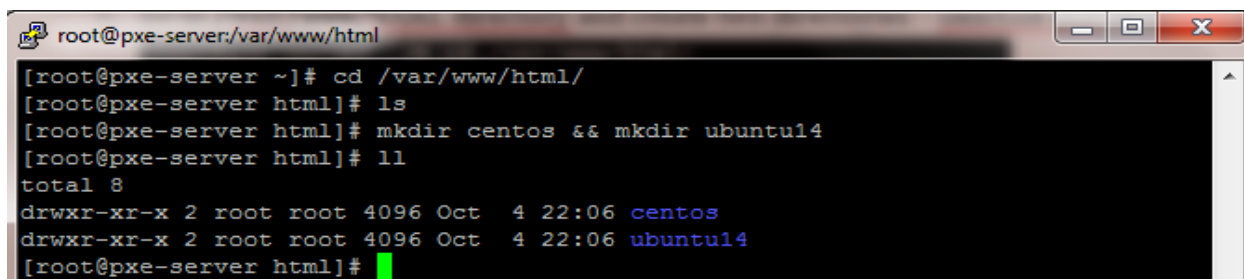
To type the command more easily and copy and paste from the same machine, the Putty tool (remote access tool) has been used. This connection is established (ssh connection) by using the server IP address in the putty tool as shown in figure 68.



```
root@pxe-server:~  
login as: root  
root@10.0.0.26's password:  
Last login: Sun Oct  4 21:03:32 2015  
[root@pxe-server ~]# ssh root@10.0.0.26  
The authenticity of host '10.0.0.26 (10.0.0.26)' can't be established.  
RSA key fingerprint is f2:be:ae:2b:a7:3c:1f:de:f9:8d:d7:0f:cb:c1:40:cc.  
Are you sure you want to continue connecting (yes/no)? y  
Please type 'yes' or 'no': yes  
Warning: Permanently added '10.0.0.26' (RSA) to the list of known hosts.  
root@10.0.0.26's password:  
Last login: Sun Oct  4 22:02:46 2015 from 10.0.0.4  
[root@pxe-server ~]#
```

Figure 67. Connect PXE to Putty tool.

The second step was creating two directories for both operating systems to mount the both operating systems in these directories, as shown in figure 69.



```
root@pxe-server:/var/www/html  
[root@pxe-server ~]# cd /var/www/html/  
[root@pxe-server html]# ls  
[root@pxe-server html]# mkdir centos && mkdir ubuntu14  
[root@pxe-server html]# ll  
total 8  
drwxr-xr-x 2 root root 4096 Oct  4 22:06 centos  
drwxr-xr-x 2 root root 4096 Oct  4 22:06 ubuntu14  
[root@pxe-server html]#
```

Figure 68. PXE directories.

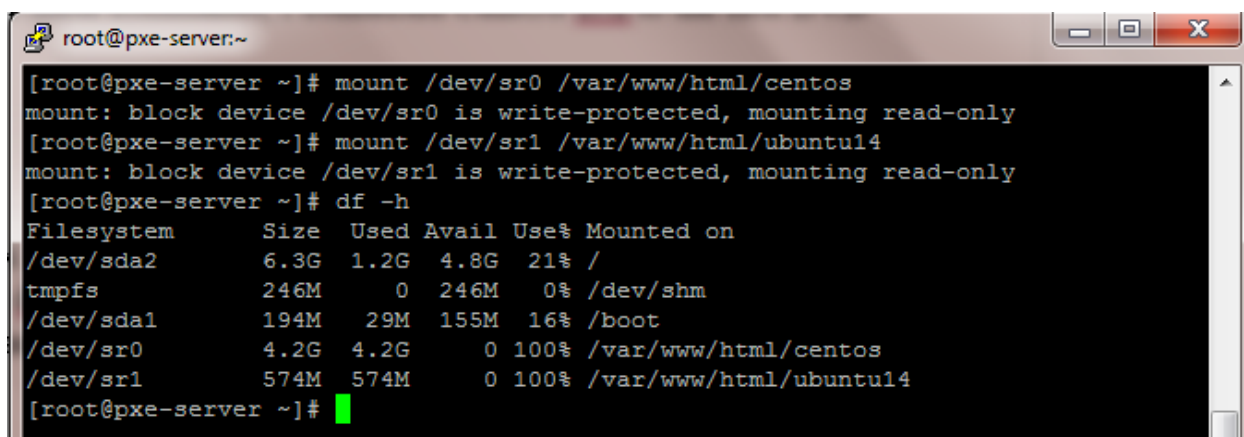
The third step was mounting the CDs that have been created to these directories by using the following commands.

```
# mount /dev/sr0 /var/www/html/centos
```



```
# mount /dev/sr1 /var/www/html/ubuntu14
```

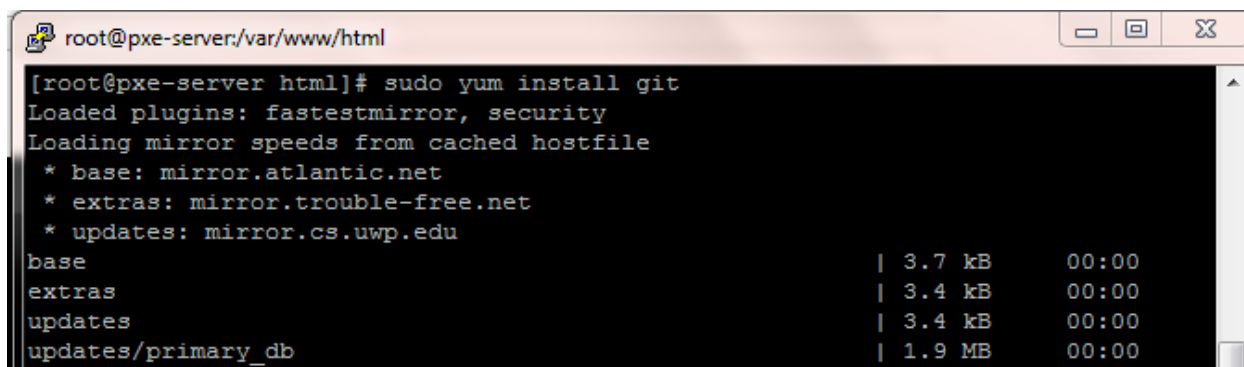
As show in the previous steps, the Centos operating system connected to the primary (first) IDE master and the Ubuntu operating system connected to the secondary IDE. After mounting the both operating systems, both systems should have specified the size as shown in figure 70.



```
root@pxe-server:~
[root@pxe-server ~]# mount /dev/sr0 /var/www/html/centos
mount: block device /dev/sr0 is write-protected, mounting read-only
[root@pxe-server ~]# mount /dev/sr1 /var/www/html/ubuntu14
mount: block device /dev/sr1 is write-protected, mounting read-only
[root@pxe-server ~]# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda2       6.3G  1.2G  4.8G  21% /
tmpfs           246M    0  246M   0% /dev/shm
/dev/sda1       194M   29M  155M  16% /boot
/dev/sr0        4.2G  4.2G    0 100% /var/www/html/centos
/dev/sr1        574M  574M    0 100% /var/www/html/ubuntu14
[root@pxe-server ~]#
```

Figure 69. Mounting operating systems.

The fourth step was downloading the kickstart files from the GitHub website. In this case, the kickstart files have been downloaded from the following link: <https://github.com/Ashraf-airport/airport.git>, which is the author of this project's account. Also, installing git and clone the repo to the following directory: /var/www/html as shown in figure 71 and 72.



```
root@pxe-server:/var/www/html
[root@pxe-server html]# sudo yum install git
Loaded plugins: fastestmirror, security
Loading mirror speeds from cached hostfile
* base: mirror.atlantic.net
* extras: mirror.trouble-free.net
* updates: mirror.cs.uwp.edu
base | 3.7 kB | 00:00
extras | 3.4 kB | 00:00
updates | 3.4 kB | 00:00
updates/primary_db | 1.9 MB | 00:00
```

Figure 70. Install git.

```
[root@pxe-server html]# ls -l
total 12
drwxr-xr-x 2 root root 4096 Oct  4 22:06 centos
drwxr-xr-x 3 root root 4096 Oct  4 23:44 pxe
drwxr-xr-x 2 root root 4096 Oct  4 22:06 ubuntu14
[root@pxe-server html]#
```

Figure 71. Clone repo for PXE.

The fifth step was moving the files that have been saved in the PXE directory to /var/www/html as shown in figure 73.

```
drwxr-xr-x 2 root root 4096 Oct  4 22:06 centos
-rw-r--r-- 1 root root 1079 Oct  4 23:44 ks.cfg
drwxr-xr-x 3 root root 4096 Oct  4 23:47 pxe
-rw-r--r-- 1 root root 121 Oct  4 23:44 README.md
-rw-r--r-- 1 root root 1228 Oct  4 23:44 ub14.ks
-rwxr-xr-x 1 root root 95 Oct  4 23:44 ubu14-fix.cfg
drwxr-xr-x 2 root root 4096 Oct  4 22:06 ubuntu14
```

Figure 72. Moving PXE directory.

The final step was testing the PXE server by accessing the URLs, which were saved already in the PXE directory, as mentioned in step four. The PXE server has been tested by typing the IP address, which was (10.0.0.26) of the server as step one. Therefore, this IP has been placed in a web browser to test the server if connecting to the DVD contents as shown in figure 74.

Index of /centos

Name	Last modified	Size	Description
Parent Directory		-	
CentOS_BuildTag	29-Nov-2013 05:52	14	
EFI/	29-Nov-2013 06:05	-	
EULA	27-Nov-2013 13:12	212	
GPL	27-Nov-2013 13:12	18K	
Packages/	29-Nov-2013 06:08	-	
RELEASE-NOTES-en-US.html	27-Nov-2013 13:13	1.3K	
RPM-GPG-KEY-CentOS-6	27-Nov-2013 13:12	1.7K	
RPM-GPG-KEY-CentOS-Debug-6	27-Nov-2013 13:12	1.7K	
RPM-GPG-KEY-CentOS-Security-6	27-Nov-2013 13:12	1.7K	
RPM-GPG-KEY-CentOS-Testing-6	27-Nov-2013 13:12	1.7K	
TRANS.TBL	29-Nov-2013 06:09	3.3K	
images/	29-Nov-2013 06:09	-	
isolinux/	29-Nov-2013 06:04	-	
repodata/	29-Nov-2013 06:09	-	

Apache/2.2.15 (CentOS) Server at 152.228.195.162 Port 80

Figure 73. PXE server URLs.

After these steps, the PXE server was working and ready to provide the users with operating systems.

Installing and configuring the PXE client was the second part of the configuration have process in this step the virtual client box has been configured with an internal network card to connect to the PXE server as shown in figure 75.



Figure 74. Virtual client adapter configurations.

The first step of the client configurations was accessing to the PXE server by using the network card which was the aim of the PXE server in the airport's network. As shown in figure 76 the client can access the server by booting from its network card.

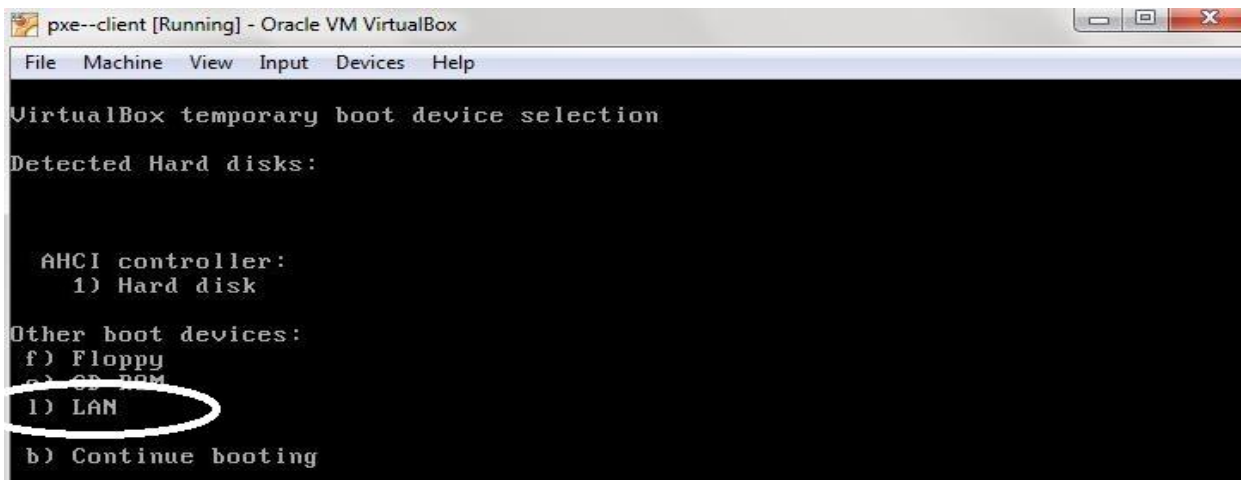


Figure 75. Accessing PXE server through LAN.

The second step from the client side was choosing the operating system that wanted to install on the machine, in this case, the CentOS 6.5 X64 chose for installation as shown in figure 77.

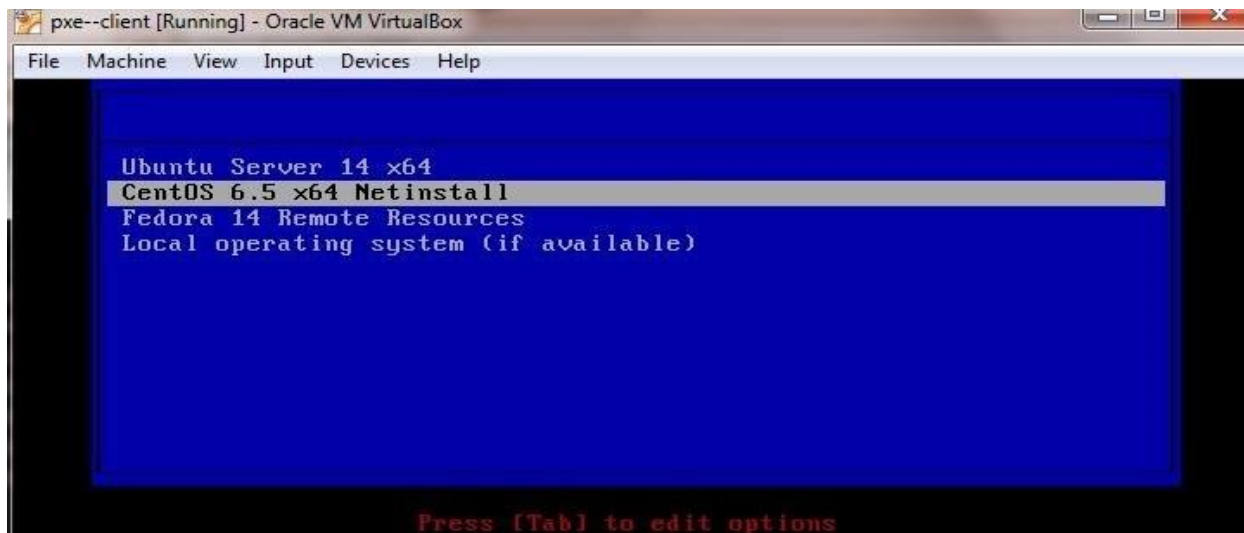


Figure 76. Operating systems options.

After many installations steps had been completed, the operating system was ready to use as shown in figure 78.

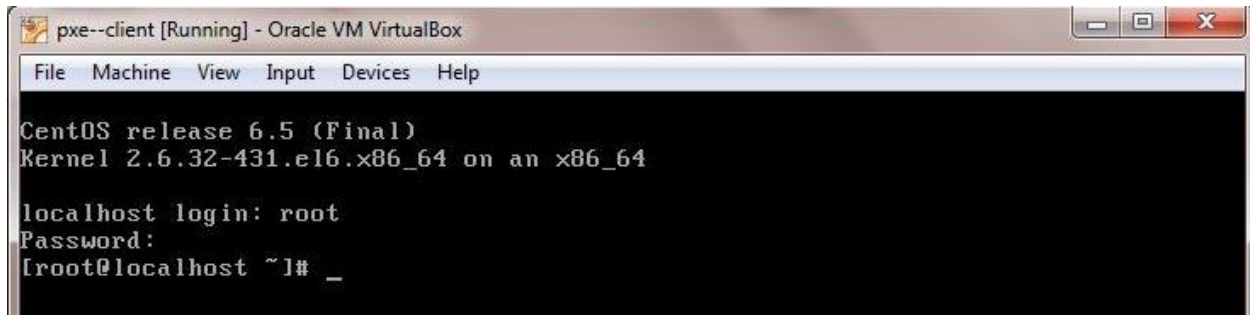


Figure 77. Operating system CentOS.

3.3 Dynamic Host Configuration Protocol (DHCP) Server

This server is responsible for assigning internet protocols (IP) automatically for all users on the internet. Situations without this service address, all the IPs need to assigned manually, situation which does not scale well. In this case, it is not possible to assign IP addressed for all clients manually. Also, if the user lost his IP, he would need to be assigned another one which it should not be used by another user in the same local network. According to (TechNet) (2005), a DHCP server provides the following benefits:

- Safe and reliable configuration. DHCP minimizes configuration errors caused by manual IP address configuration, such as typographical errors, as well as address conflicts caused by a currently assigned IP address accidentally being reissued to another computer.
- Reduced network administration.
 - TCP/IP configuration is centralized and automated.
 - Network administrators can centrally define global and subnet-specific TCP/IP configurations.

- Clients can be automatically assigned a full range of additional TCP/IP configuration values by using DHCP options.
- Address changes for client configurations that must be updated frequently, such as remote access clients that move around constantly, can be made efficiently and automatically when the client restarts in its new location.
- Most routers can forward DHCP configuration requests, eliminating the requirement of setting up a DHCP server on every subnet, unless there is another reason to do so.

This server can provide clients IPs even when they lose the IP that has been assigned to their devices, and the server will provide different IP for each request from the same subnet (range of IPs in the same network). The DHCP tool that handles this task is called pool, which is responsible for managing IP addresses on the local network. With this tool the enable devices (connected to the network) have specific IP but the disabled devices (not connect to the network) will lose the IP, and that will be given to the enabled device on the network. DHCP is not used only for providing IPs but also manage them on the network. In the airport's network, the DHCP server provides the users dynamic IPs and other services inside the local network. For example, data center, DSN server and Web server obtaining their IPs from DHCP automatically. On the other hand, the airport's departments have been assigned to a different class of IP addresses depending on the connected devices. The flight management department was designed with C class and the IP address (192.168.1.1). Also, the service providers' department was assigned to C class and the IP address (192.168.0.1). Also, the arrival, departure and guests' department assigned with B class and the IP address (172.16.0.1). Moreover, the class C can provide IPs for (254) clients, and class B can provide (32766) clients, class B can provide (65534) clients usually but in the

arrival, departure and guests' department this class has been subnetted depending on the needs. The IP range is available for any device in each department, and there are many limitations for users which were configured in the previous steps depending on the security policy.

3.3.1 DHCP Position in Overall Network

In the airport's network as mentioned before each department has been assigned to different IP address classes. However, this service was not provided from one server; there were two central servers which provided the entire network with dynamic IP addresses. The DHCP servers' design was applied regarding the security policy for each department. The flight management department and the service provider's departments were provided by two servers which are located in the department as shown in figure 79.

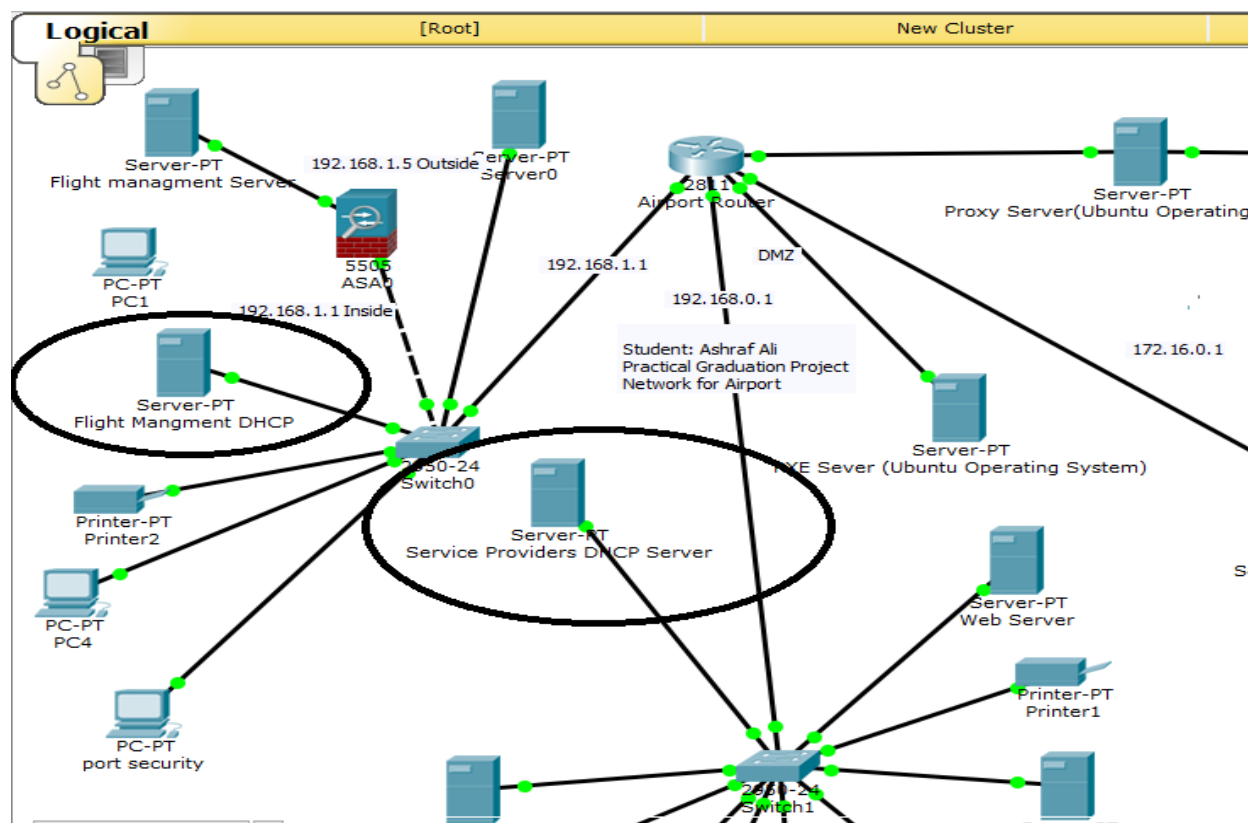


Figure 78. DHCP Sever location design.

From another aspect, the design of the DHCP server is required to place the arrival, departure, and guests' department server separately and connected directly with this department without any other connections from the neighboring departments. This was also one of the main requirements of the security policy that was assigned to the airport's network. In this case, this department has a private server which was supported by different devices with dynamic IP addresses as shown in figure 80.

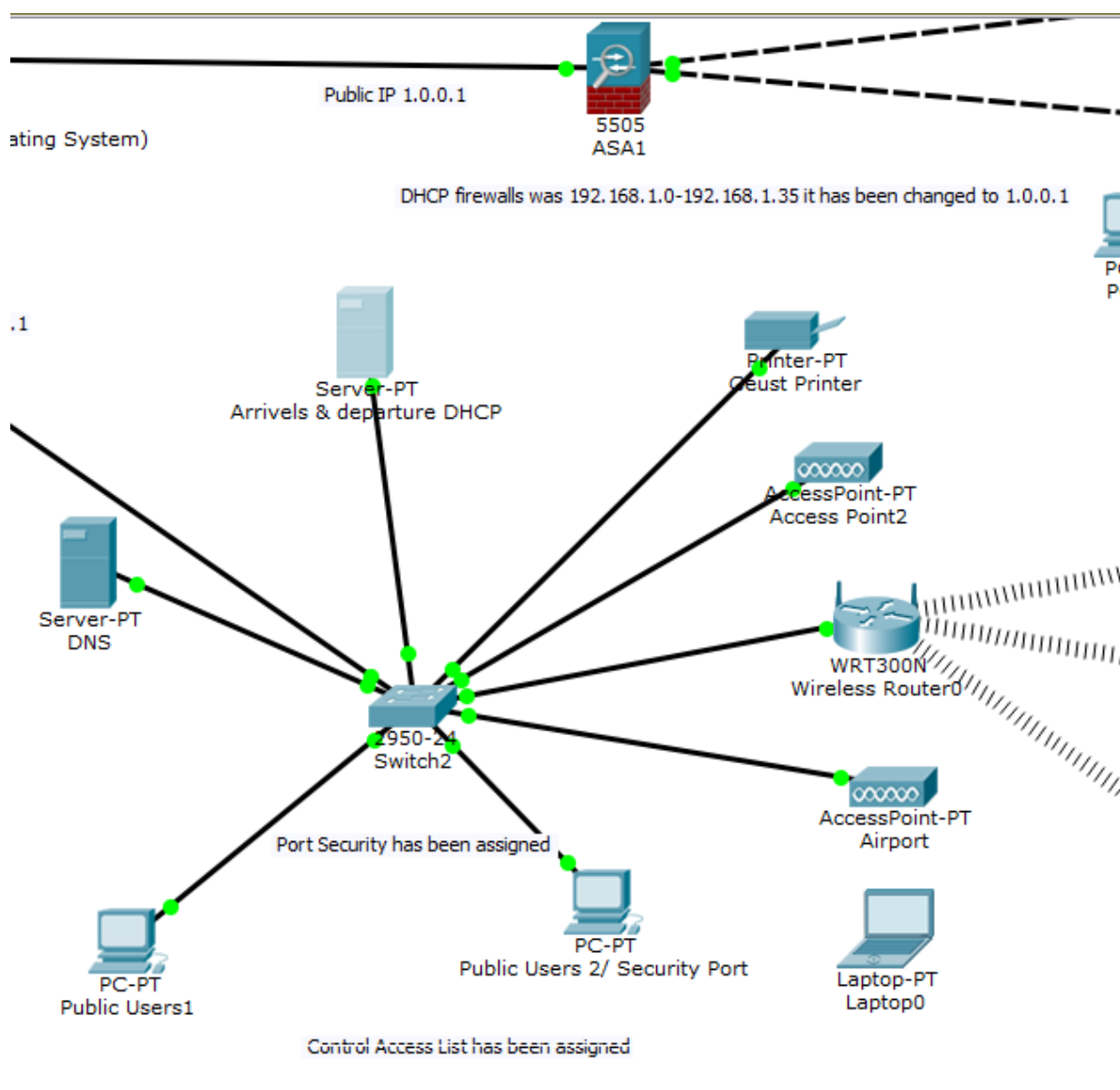


Figure 79. Arrival, departure, and guests' department DHCP server location.

This illustrates the network topology for the practical work in the project which was determined during the concrete steps. Furthermore, the server has been configured to take avoid data collision and obtain an IP address. According to (TechNet) (2005), The 80/20 design rule for using multiple DHCP servers in the same scope (network) to make balancing the address in the same area. Using more than one DHCP server in the same network subnet offers error allowance for the DHCP server that provides the network, if one of the servers is not ready to provide DHCP service for the network, the other server will fill the vacancy and restores supporting the connected clients. For the standard balancing strategy for using two DHCP server on the same network, is providing 80 percent from the clients by the first DHCP server and the other 20 percent by the second server. As the previous source explained, the DHCP server in the same network can avoid the faults that occurred when one of the servers goes down. This was an advantage of the design in the airport's network design when the flight management department and service providers department provided with two DHCP servers.

3.3.2 DHCP Sever Installation and Configuration

In the installations section, the DHCP server is installed on the Windows Server 2012, which is located in the flight management's department also this server has been configured for the Domain Controller Server service previously. However, the DHCP server that provides the service provider's department clients and arrival, departure and guest's department have been configured with the same configurations steps but on another physical box. On the other hand, some of following configurations have been placed according to Davis (2012).

The first step was adding the roles and features from the server manager and choosing the role-based installation to start configuring the DHCP server as shown in figure 81 and 82.

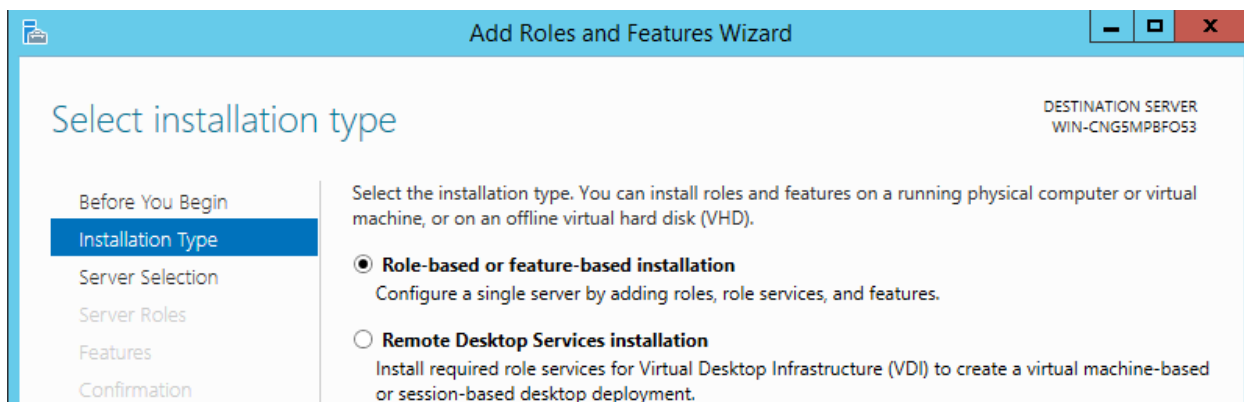


Figure 80. Roles DHCP installation.

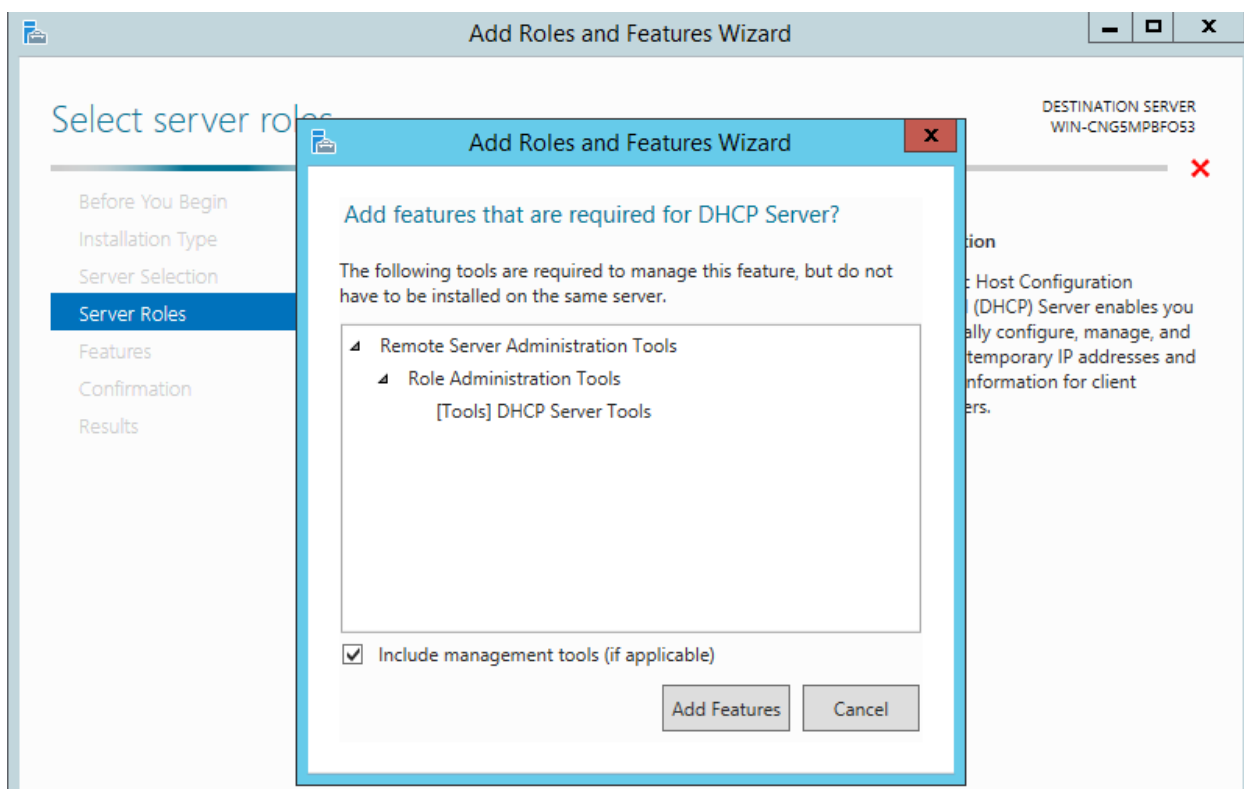


Figure 81. DHCP related features.

The second step was configuring the scope options by choosing to the server tool option and creating a new scope for the flight management department which is configured depending on the needs of this department as shown in figure 83 and 84.

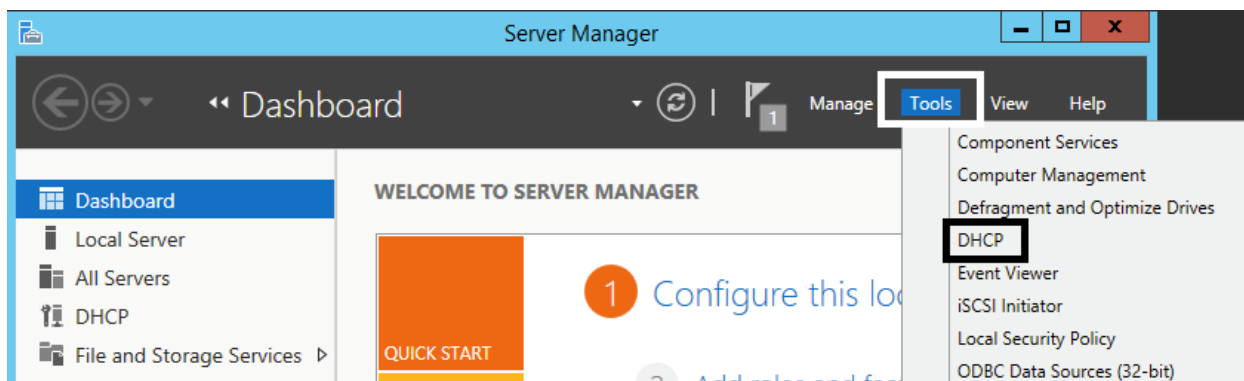


Figure 82. DHCP scope option.

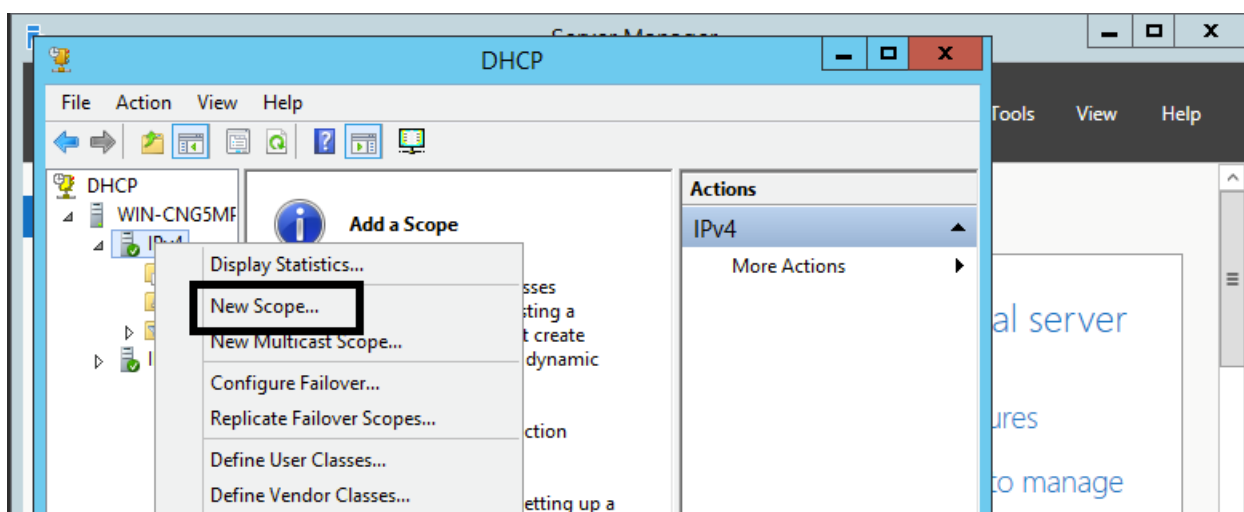



Figure 83. DHCP flight management scope.

The third step was naming the scope that covering the flight management department and assigning the IP address range. In the flight management department, the DHCP server provided the entire department with 60 IP addresses and this number can be increased depending on the department's need. The IP address range for this department has been configured to start from (192.168.1.5) to (192.168.1.60) as shown in figure 85 and 86.

New Scope Wizard

Scope Name 

You have to provide an identifying scope name. You also have the option of providing a description.


Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.

Name:

Description:

Figure 84. Scope name.

New Scope Wizard

IP Address Range 

You define the scope address range by identifying a set of consecutive IP addresses.

Enter the range of addresses that the scope distributes.

Start IP address:

End IP address:

Configuration settings that propagate to DHCP Client

Length:

Subnet mask:

Figure 85. Scope IP address range.

The fourth step was configuring the duration for the leases, for the flight management department the DHCP need support the dynamic IP address 24 hours, seven days a week because this department should be active all day to help and guide the airplanes to the right path as shown in figure 87.

New Scope Wizard

Lease Duration
The lease duration specifies how long a client can use an IP address from this scope.

Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

Set the duration for scope leases when distributed by this server.

Limited to:

Days: 7 Hours: 23 Minutes: 59

Figure 86. DHCP scope lease duration.

The final step was configuring the default gateway for the router that connects this department to the other parts and with the outside world as shown in figure 88.

New Scope Wizard

Router (Default Gateway)
You can specify the routers, or default gateways, to be distributed by this scope.

To add an IP address for a router used by clients, enter the address below.

IP address:

192.168.1.1

Add Remove

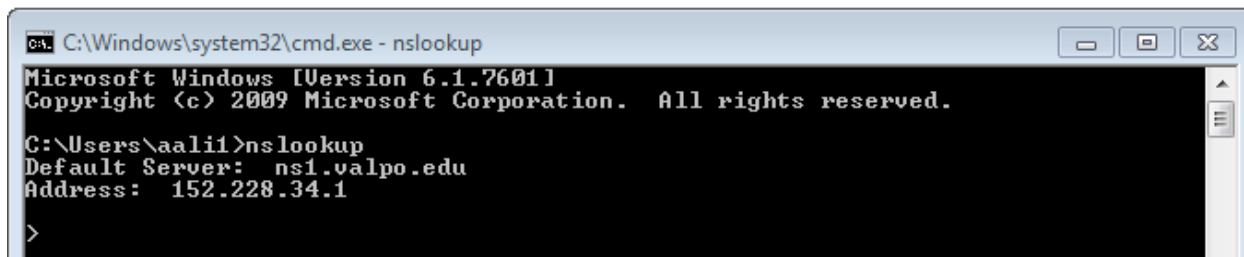
Figure 87. Scope default gateway.

As a result, the other departments have been configured by following the same steps except the IP address range. The service providers' department, has been assigned to the IP address range which started from (192.168.0.2) to (192.168.0.200). On the other side, the arrival,

departure and guests' department have been assigned with the IP address that started from (172.16.0.2) to (172.16.0.)

3.4 Domain Name System (DNS) Server

The numeric IP address is the mechanism that is used to help establish the communication between devices in the local network and Internet. Also, it is possible to reach the internet websites from the local network by using the IP address and passing them to the outside servers. However, this use of numbers is impractical for users. Therefore, there is a system that can translate a textual name to the numbers, the Domain Name system (DNS). By using it as lookup tool, it is possible to know what the DNS server's IP address on the network is. For example, the DNS server's address for Valparaiso University is (152.228.34.1) as shown in figure 89.



```
ca. C:\Windows\system32\cmd.exe - nslookup
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\aaali1>nslookup
Default Server: ns1.valpo.edu
Address: 152.228.34.1

>
```

Figure 88. DNS server example.

In addition, this server can provide the easiest ways for the users to access their websites.

According to Boyce (2000):

Host names provide a more “friendly” way to name hosts, making it easier to remember host addresses. For example, when you want to get the news, you can point your browser to www.newsmax.com instead of 64.29.200.227. Add a couple of hundred other addresses to your frequent site list, and you can see that host names are a lot easier on the brain than IP addresses.

As explained in the above quote, the primary task for a DNS server is translating the words to network-meaningful numbers that can be used to access to a particular destination. There are many steps for the DNS server to complete this process. Most of these steps are happen out on the local network, especially when the clients request information from outside the local network. In the airport's network, the DNS server has been positioned to help the users accessing the airport's website. Any user from the local network or from outside the network cannot access the website without translating his/her IP addresses to the website's extension link. This process has its own structure that provides each position depending on the location. According to TechNet (2003),

The Domain Name System is implemented as a hierarchical and distributed database containing various types of data, including host names and domain names. The names in a DNS database form a hierarchical tree structure called the domain namespace. Domain names consist of individual labels separated by dots, for example mydomain.microsoft.com.

As previously explained, the DNS service divided to names which separated to more than one part depending on the destinations or the way of saving the data.

3.4.1 DNS Server Network Location

The DNS server can be located in any positions which should have a high security level. In the airport's network, the DNS server has been placed in the service provider's department because the web server has been put in the same department as shown in figure 90.

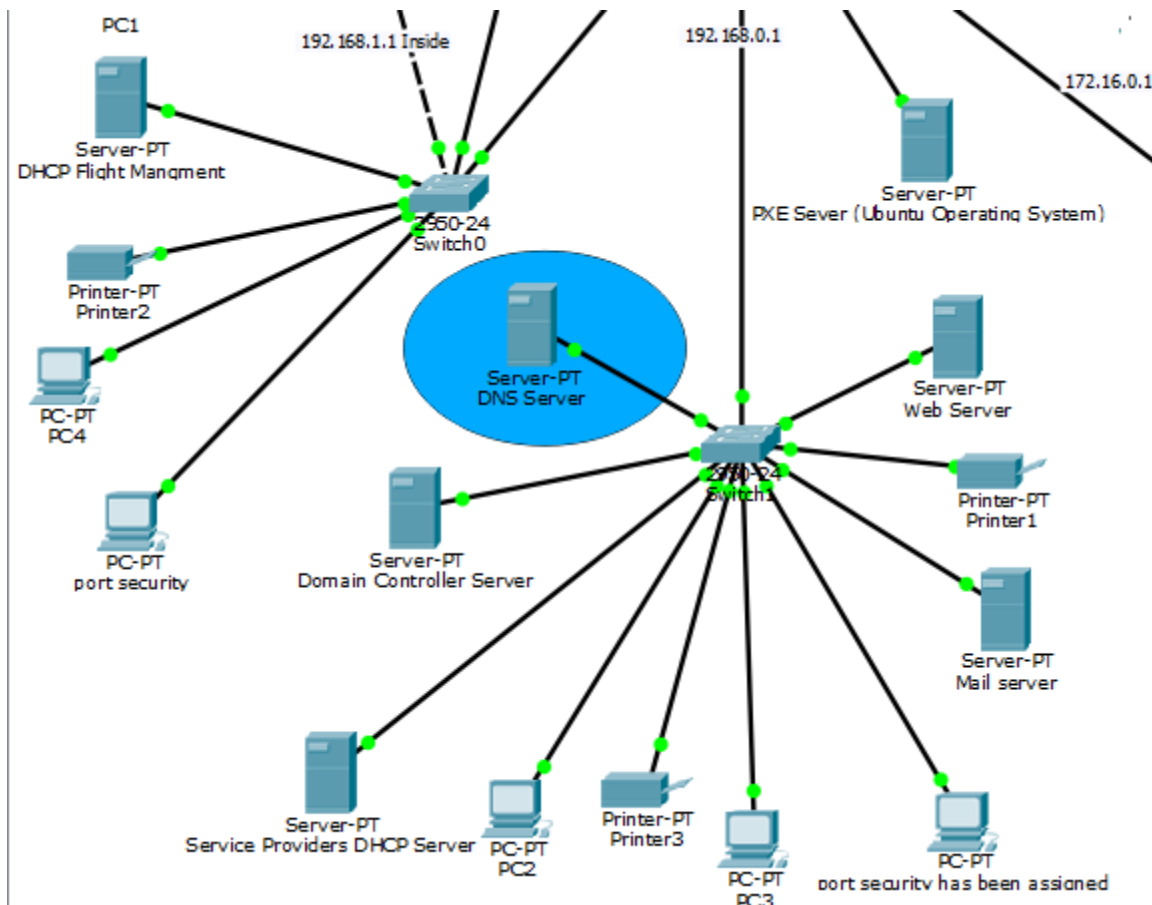


Figure 89. DNS server location design.

For the flight management department, the users can access the local DNS server and access the web server from the local network. Otherwise, the arrivals, departures and guests' department cannot access the local DNS server in order to access the internet server because of the untested users in this department as mentioned before, so this department can access the internet server through the web. As clearly explained in the earlier parts of the project, the arrivals, departures, guest's department has been supported with internet service as a general and few computers for local use that allow the user to obtain the DNS service from the cloud. The other reason for locating the DNS server in the service providers' department was the importance of service for the airline companies. This provides the airlines staff access to their services which is located in the same area.

3.4.2 DNS Server's installation and configuration

The DNS Sever installation and configuration have been placed on the service provider department's Windows Server, the same server that handles the DHCP service and has been installed and configured in the previous section. Also, the IP address for the airport's website has been set with (192.168.0.100), so any user can access the internet site by using the following link(www.kurdistanairport.com) which has been configured to translate to the IP address that mentioned before by using the DNS server. The following steps represent the installation and configurations for the DNS server according to Nelson (2014):

The Installation part:

The first step from DNS server installation was adding rules and features to the server manager to insert the requirements to the Windows Server as shown in figure 91.



Figure 90. DNS roles and features.

The second step was choosing the installation type for the DNS server. For this installation, the appropriate choice was Role-based or feature-based installation as shown in figure 92.

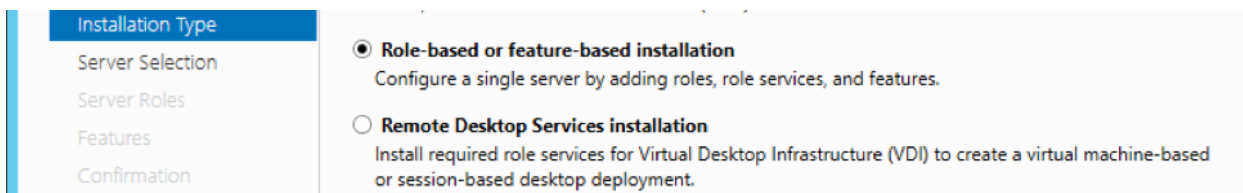


Figure 91. Roles and features type.

The third step was installing the roles for the server. In this setup DNS related server roles were required to complete the installation and adding all the configurations requirements depending on needs as shown in figure 93.

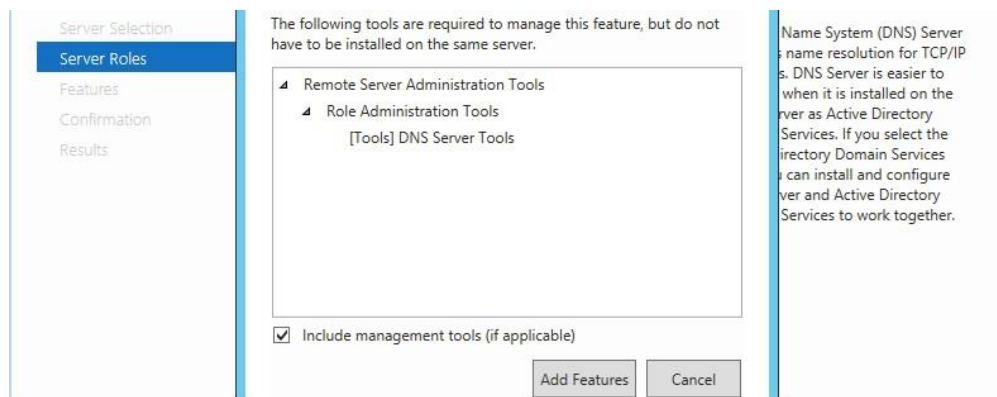


Figure 92. Server roles installation.

The final step of the installation was viewing the installation progress and making sure that all the requirements have been placed as shown in figure 94. The configurations part has been placed according to Geared (2012);

The first step of the configurations part was using the wizard to create a primary zone for the airport's website which can update on the server as shown in figure 95.

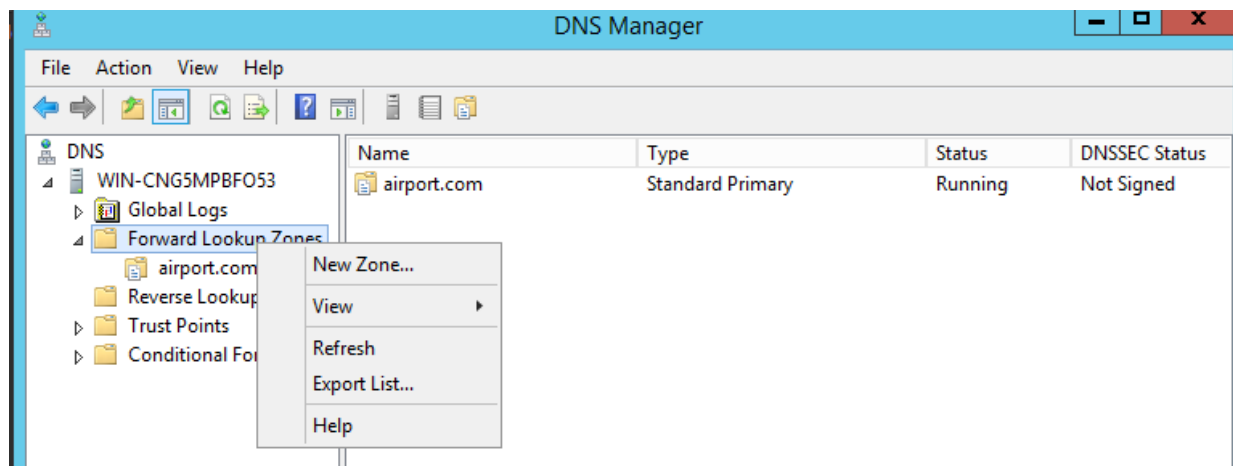


Figure 93. Setup new DNS zone.

The second step of the DNS server configurations was choosing a name for the zone (airport local network service) which specifies the portion of the authoritative server and create the zone file. In this case, the name of the zone has been configured with (airport.com) as shown in figure 96 and 97.

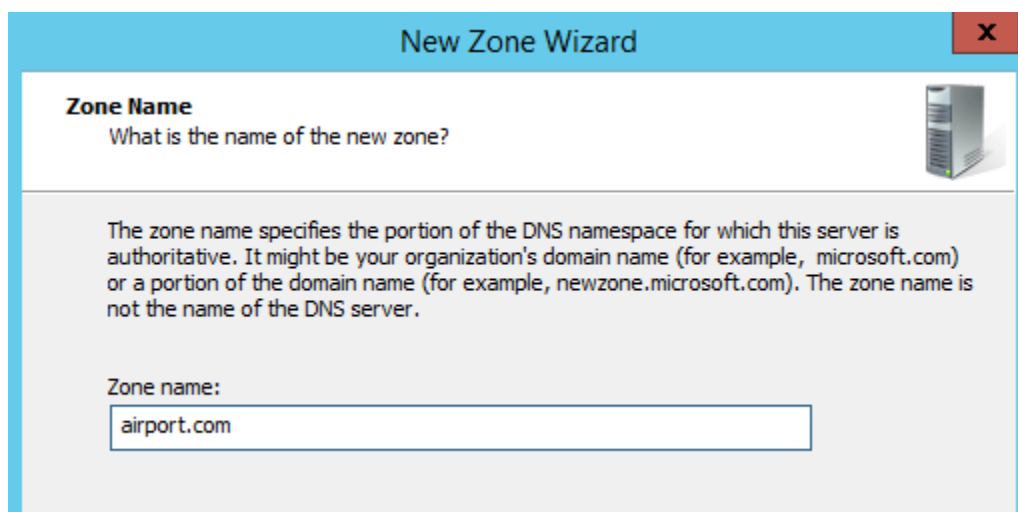


Figure 94. DNS zone name.

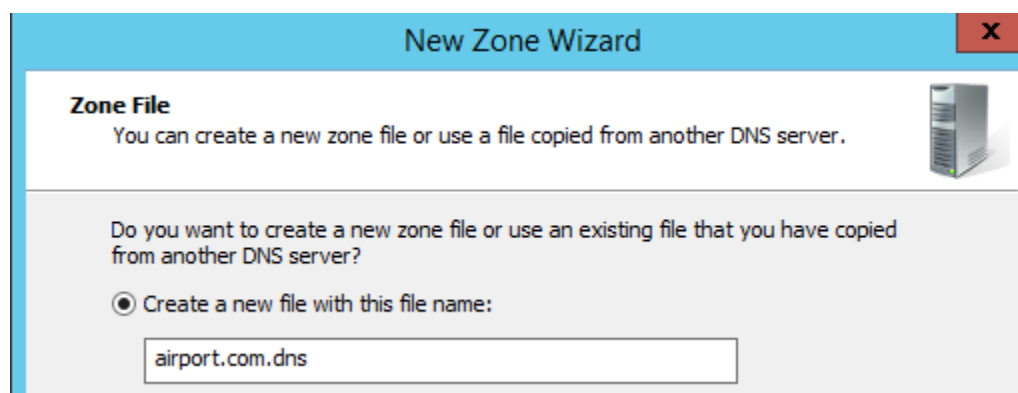


Figure 95. DNS zone file.

The third step was assigning the permission for the users to place their IP with the DNS server, in the airport's network policy, the network's administrator has the only permission to

add and remove IP addresses on the DNS server by choosing not to allow dynamic updates in the configurations progress as shown figure 98.

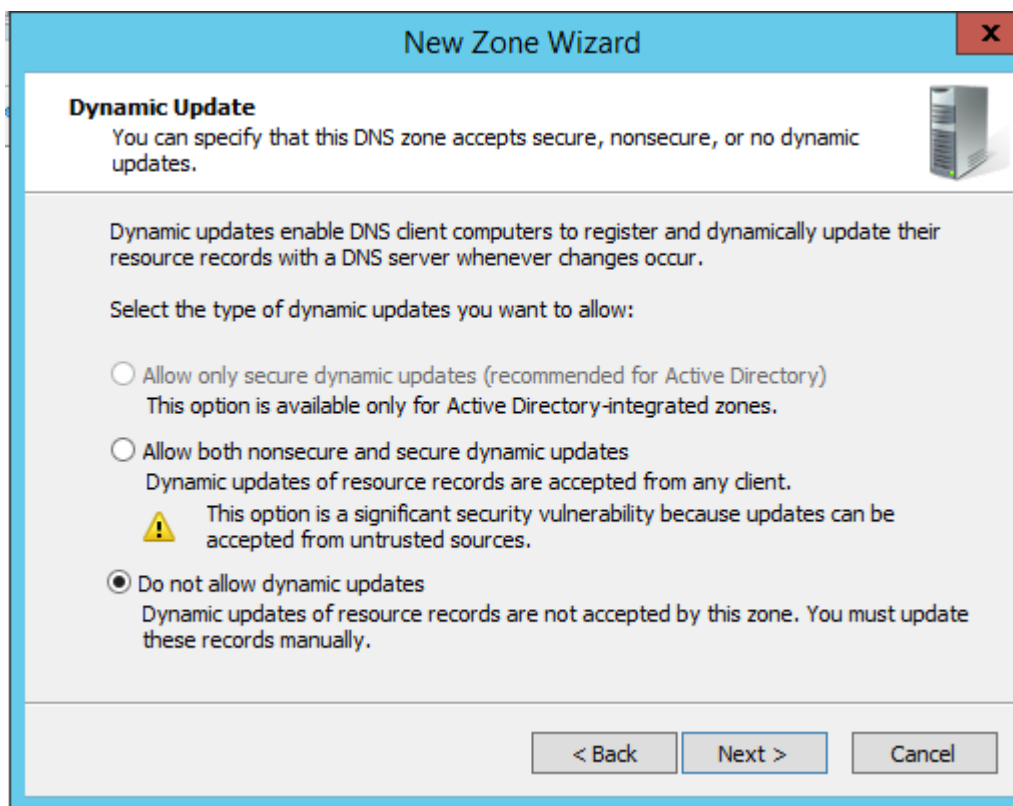
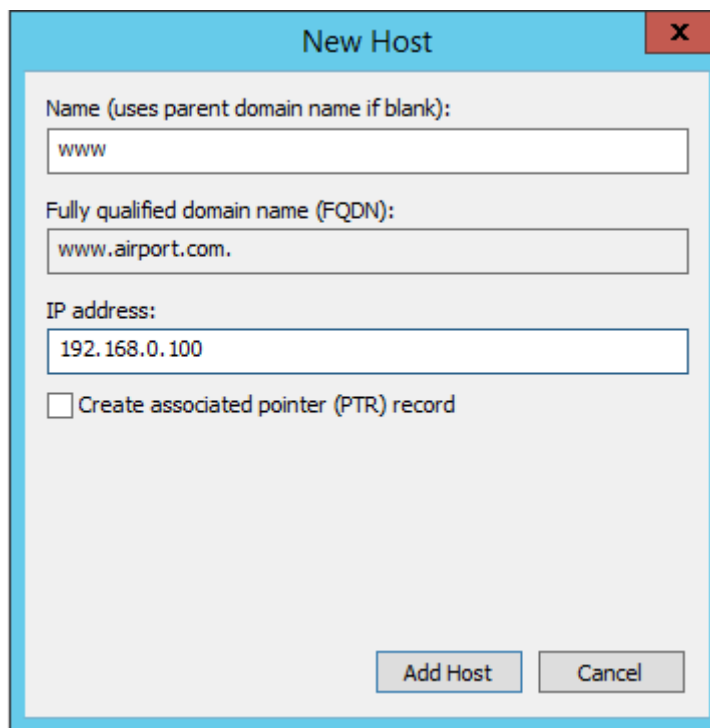


Figure 96. DNS dynamic update.

The final step was creating the record for the DNS server zone.com for the IP address (192.168.0.100) that has been chosen for the airport's website which represents the result of this DNS server as shown in figure 99.



The image shows a 'New Host' dialog box with the following fields and options:

- Name (uses parent domain name if blank):
- Fully qualified domain name (FQDN):
- IP address:
- Create associated pointer (PTR) record
- Buttons: Add Host, Cancel

Figure 97. DNS record server.

3.5 Airport's Network Cabling

In any successful network, there should be a high quality of connectivity to related hardware. Data exchange between the network's elements need to be chosen to support desired speed. In some areas the performance will be unacceptable when connectivity quality is not high. In this part the importance of the cabling system appears, many networks lose their quality of service when the cabling is not satisfactory. Therefore, the network technician, must take special care with the network cabling to ensure the quality of service. According to Peters (2012):

Data cables (also known as transmission media) are responsible for carrying messages back and forth between computers and other devices and as such are the foundation of your network. All other network equipment has to be compatible with your choice of data cable, so this decision constrains or determines many of your other options. While dozens

of cable variants are standardized and available for purchase, these variants fall into four main categories:

- 1- coaxial cable
- 2- twisted pair cables
- 3- optical fiber
- 4- wireless

In the airport's network, the cable type decision has been made depending on the distance and the type of data that transfers on the wires. In many parts, the security aspect has been taken because some connectivity types cannot be relabeled to transfer the data during the work operations and the quality of transferring these data. Therefore, the airport's network topology has been taken as the primary consideration for the cabling used in the airport.

3.5.1 Airport's Network Cabling Design

The network cabling design part in the airport network took two aspects of applying the wiring design on the buildings. In the flight management department, the quality and aspects have been considered as the main plane of placing the cables for the airport's network departments. The flight management department has been connected to the primary router with fiber optic (single mode) cable because this department manage the Airport Traffic Control Tower (ATCT) which is usually located in an area that is a long distance from the main building. In this case, the fiber optic has been chosen as a design plane to provide a high speed for transferring the data between the ATCT building, and the management building, this type of cabling can provide the service for long distance. According to McQuerry (2004):

Single-mode fiber-optic cable allows only one mode (or wavelength) of light to propagate through the fiber. This type of cable is capable of higher band-width and greater distances

than multimode and is often used for campus backbones. Single-mode cable uses lasers as the light-generating method and is more expensive than multimode cable. The maximum cable length of single-mode cable is 60+ km (37+ miles).

As detailed above quote, fiber optic cable provides long distance connectivity with a high quality of transferring the data; this was very critical for the ACTC department because of the importance of the data that transfer between the flight management and the mentioned department. Also, the flight management department, service providers department and arrival, departure and guests' department have been connected with the main router by fiber optic (multimode) because these departments are not too far from each other. According to McQuerry (2004):

Multimode fiber-optic cable allows multiple modes of light to propa-gate through the fiber. Multimode cable is often used for workgroup applications, using light emitting diodes (LEDs) as light-generating devices. The maximum length of multimode cable is 2 km (1.2 miles).

As clarified early, these types of cables are appropriate to connect the airport's departments together as long as they can provide less quality, but this will not affect the network quality in general. The reason for choosing this kind of cable for these departments was taking the total cost into consideration for designing the airport's network. In the result, the design takes an aspect of dividing each department to specific category depending on the department's location. On the other hand, the second aspect of the Airport's Network Cabling design was focusing on the security in the cabling area, this part illustrated the wireless services in the airport's network. As a result, the wireless connectivity service was assigned to provide the internet service only for the airport; no other data transformation was configured to exchange throughout network

wireless services. Each department has been connected with its computers and other devices by Ethernet cables (twisted pair) because of the short distance between devices and each switch device in the departments. Moreover, the workstation devices and other servers have been connected with other devices by Ethernet cables because the network card for them support this connection only. As a general of the cabling design for the airport's network, figure 100 shows how the departments have been connected and how the wireless connectivity is setup for the entire network.

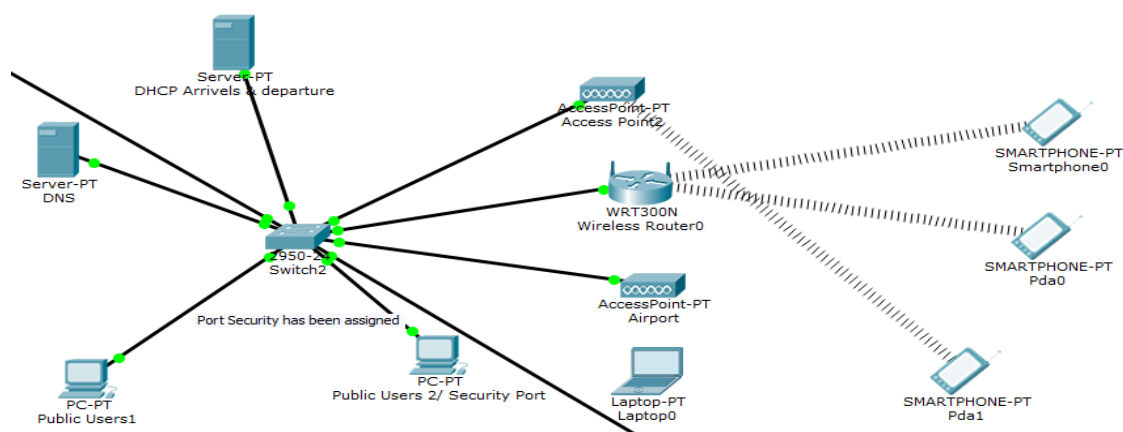


Figure 98. Airport's Network Cabling design.

3.5.2 Airport's Network Cabling Configurations

As mentioned before the airport's network design and implementation has been tested on Cisco Packet Tracer (network simulation software), so there were some parts of the project has been verified with other software programs. For the cabling part, the configurations have been taken from another source because the packet tracer cannot test this aspect.

The cabling section was included by connecting the fiber optic (single mode) which has been placed between the buildings in the airport. The first part was connecting the ATCT building with the main building which includes all the network devices. This connection is established by using fiber optic (single mode). Also, the flight management department, service

provider department, and arrival, departure and guests' department have been connected with fiber optic cable (multimode) depending on the distances as mentioned before. Moreover, all the computers and wireless access points devices have been connected by Ethernet cables (Twisted Pair). As a result, the fiber cables configurations have been applied according to National Electrical Contractors Association (an American National Standard), Standard for Installing and Testing Fiber Optic Cables. However, the Ethernet cables configurations which have been installed according to Cisco System, Inc.

4 Safety

4.1 Web server

In many networks, websites are often the most porous part of any network because this system retains all information for the users and customers from inside and outside the organization. Also, these websites can be protected and controlled easily when they are located in the local network; this can be achieved by providing a high-security level for all network in general. Not only the quality of websites is required but also the safety of the information can be more important. Therefore, to save the user's information on the website could not be secure without saving the hardware part that hosts these sites which are the web server. According to Kenner (2010):

The main issue is that when you run a Web server on your home PC, you're opening a port on your computer that allows entry from the outside world. Web servers may not be the easiest way to gain access to a computer, but they are a well-known method of intrusion, meaning that you raise your risk of having your computer attacked, your website defaced, and maybe even having your computer taken over completely by unscrupulous individuals.

As clarified above, a web server can be attacked from outside; this happens when the webserver opens a port on the computer for public uses. In addition, all the information in the computer will be at risk. If there is a database server on the same machine which includes all the users' information, this could represent a very big problem for any network around the world. In this project, the airport's network has been protected by many technical ways, which explained in the early steps of the project, to keep the entire network secure. Therefore, there is no danger to host the website server on the local network and keep the passengers' information safe which was the aim of this part of the project. As it happens in these days, airports are the most targeted placed for terrorist attacks. However, these attacks cannot be just suicide attacks but also could be technical attacks especially in these days. In this part of the project, the implementation, and design of the airport's network has been focused on the passengers' information as the essential scope of the airport's network safety. All the information required for the passengers during the flight progress like name, date of birth (DOB), gender, type of travel document (passport), expiration date, country of issue, destination address and other information depending on the passenger's country. All the information could make the way for the terrorist for their criminal operations against the civilians (passengers). Therefore, all the information for the user's needs to be safe and secure to ensure the safety of passenger's lives, this is what this part illustrated for the airport's network.

4.1.1 Web Server Design

The other important aspect of saving the website information was locating the web server in a secure place. The setup for the web server took advantages of the security tools which have been configured for the airport's network. The main beneficial tool for security was the accessed list utility; this tool prevented the unauthorized users from accessing other departments, such as

the arrivals, departures, and guests' department from accessing the service provider's department. For this reason, the web server has been placed in this department as shown in figure 101.

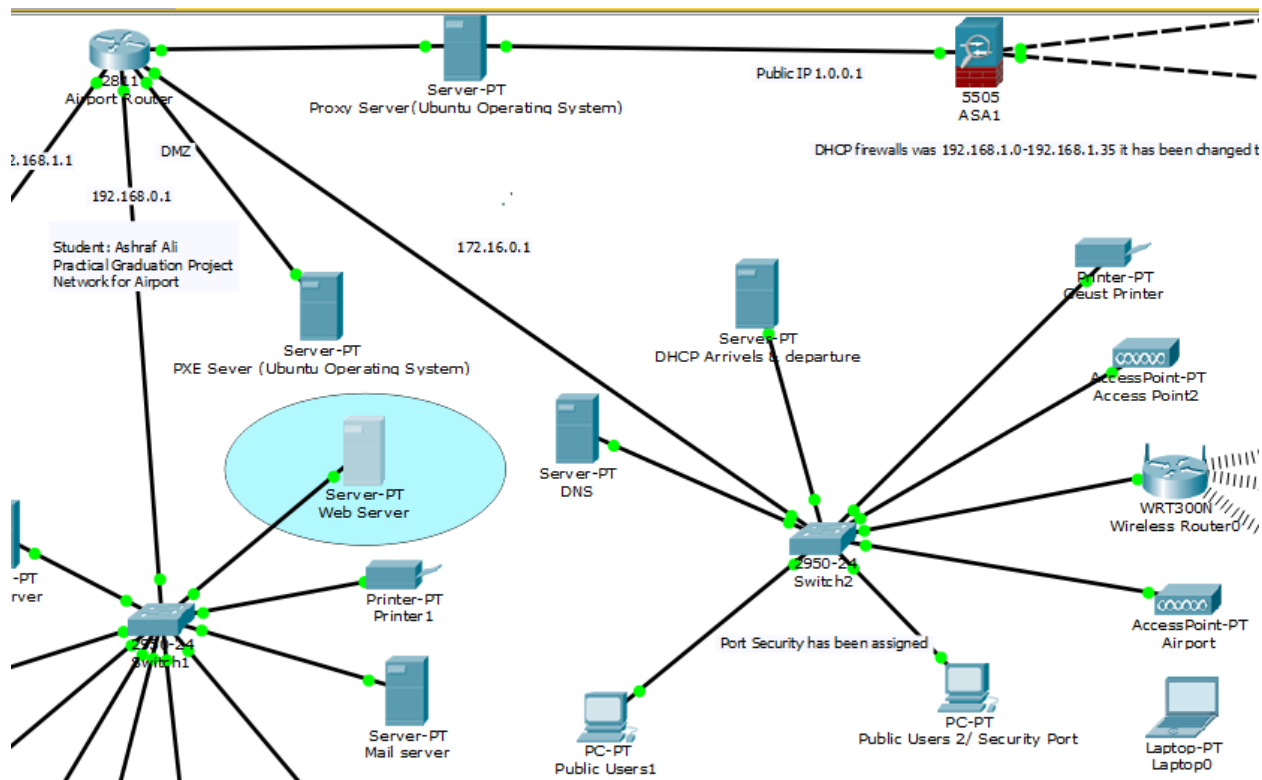


Figure 99. Web Server location design.

This design has been placed on the local network, which keeps the passengers' information safe from inside attacks by terrorists who are doing their activity inside the airport. Otherwise, the airport's network has taken precautions against the outside attacks by placing the firewalls and proxy server in the main internet service providers for the network. Nevertheless, providing a protected environment for the web server was more important than protecting the web server itself, this was provided by Internet Information Services (IIS) which is a web server for Microsoft server operating system and can provide a secure environment for the web server. According to the Microsoft Corporation (2006):

When you incorporate security features into your application's design, implementation, and deployment, it helps to have a good understanding of how attackers think. By thinking like attackers and being aware of their likely tactics, you can be more efficient when applying countermeasures.

As explained in the quote, the network designer or technician needs to have strong skills or hacking which help to cover all the weak points in his network and know how to prevent hackers from entering his network. The web server represents a part of the network like any other parts, but it is the most facing targeted device which should be surrounded by protection devices to keep the web server in protected surroundings. This is what the project design worked on, placing the web server in a protected environment which can secure the passenger's information. As a result, this design can offer safety for the passengers.

4.1.2 Webserver configurations

In this part, the configurations have been applied to MS Windows Server 2012 r2 and install MS Internet Information Services (IIS) which represent the web server for the airport's network. This web server has been chosen because of the high security that supports Windows Server 2012. Some of the configurations steps have been practiced according to Costantini (2015).

The first step of configurations was adding roles and features to the server as shown in figure 102.



Figure 100. Web server roles and features.

The second step was choosing the roles that need to be installed and add the required parts in order to install the Internet Information Services (IIS) on Windows Server; there were some steps which have been done by clicking next bottom on each part and finally getting the installing page as shown in figure 103 and 104.

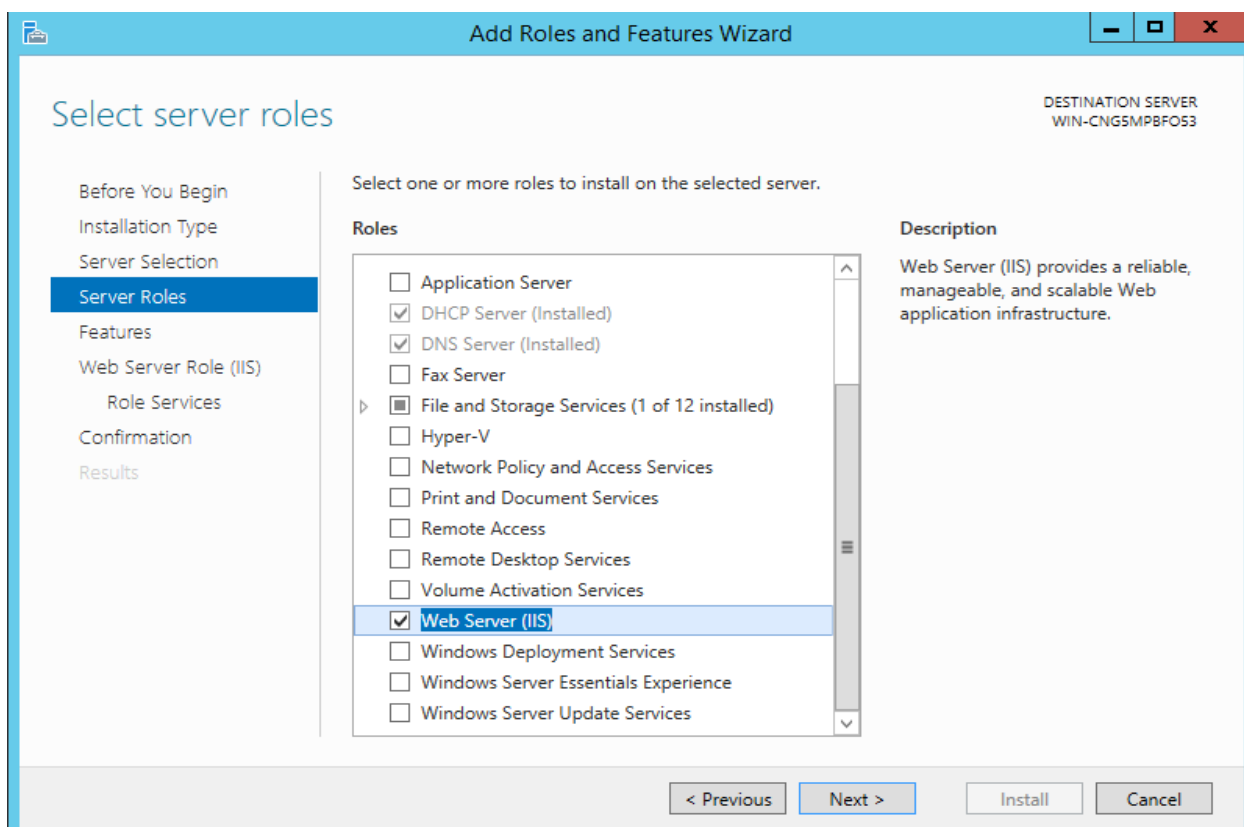


Figure 101. Web server (IIS) role installation.

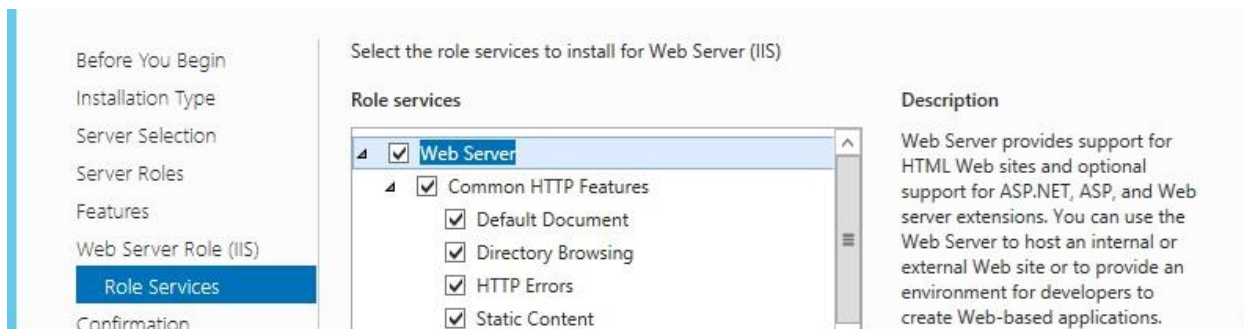


Figure 102. Web server (IIS) installation requirements.

As shown in figure 4, many required roles need to be installed to the web server. In a nutshell, this represents an integrated environmental tool to host websites and database connections which are what can be provided by other tools like Apache Server.

The third step was confirming the installation's process and making sure that all the requirements have been placed correctly and making sure that the server has been added to the Windows server tool as shown in figure 105 and 106.

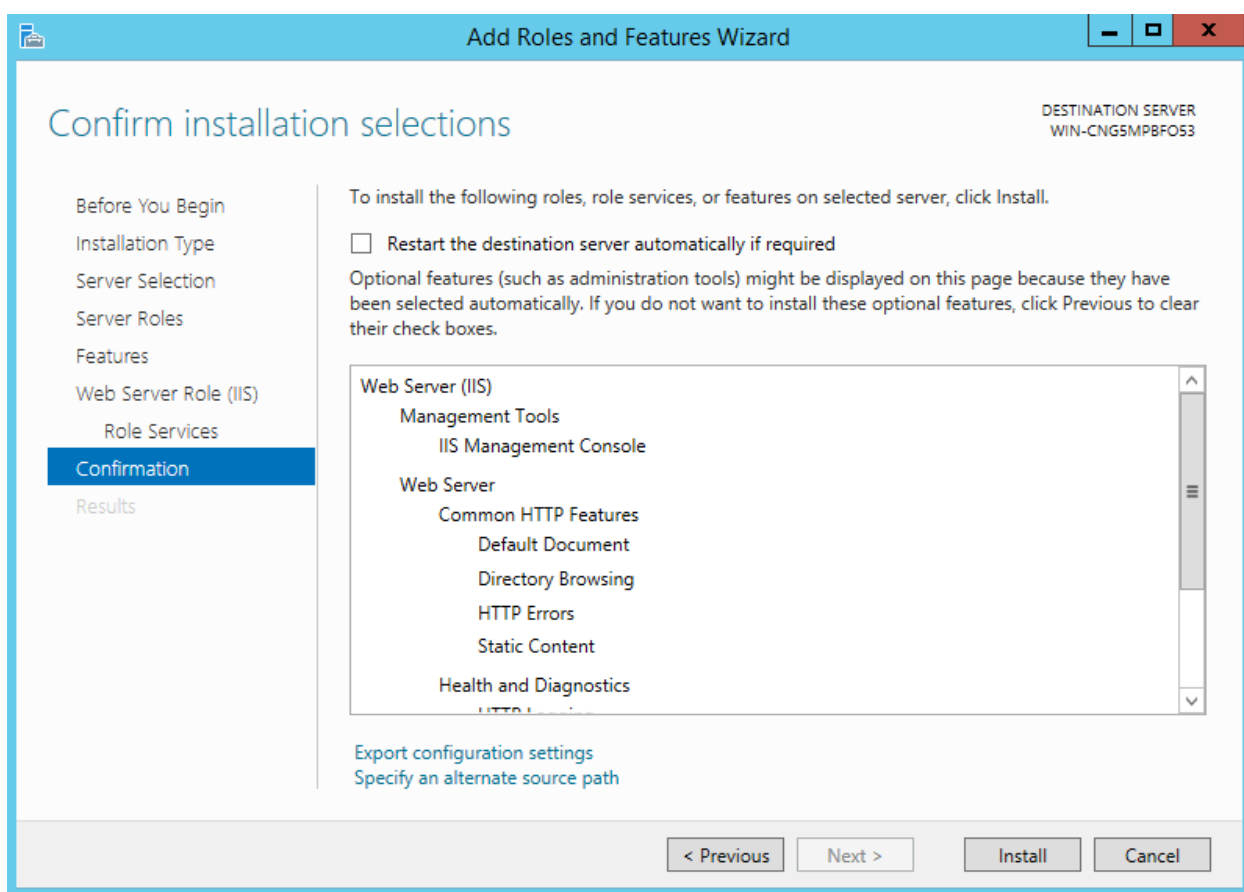


Figure 103. Web Server (IIS) requirements.

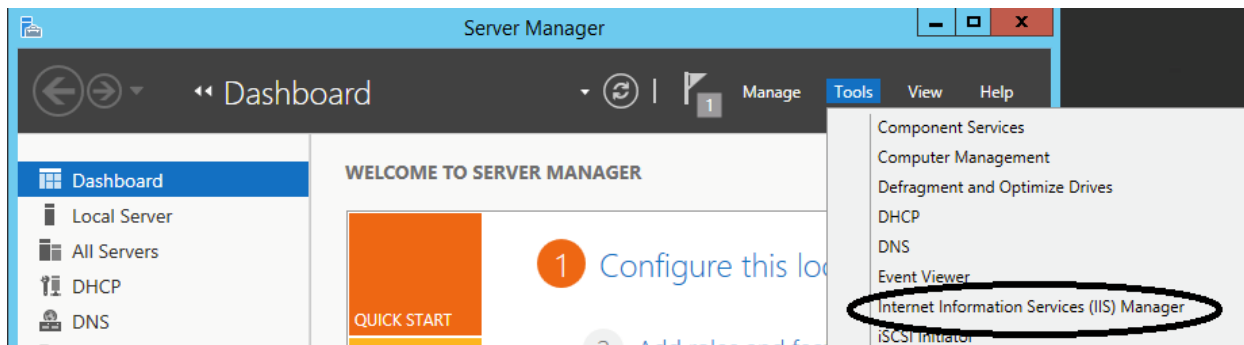


Figure 104. Web Server tool manager.

The final step was testing the web server by opening the local host webpage and start preparing the web server environment to locate the airport server website as shown in figure 107. Also, for test purposes, the internet page for the airport has been added to the web server and configured with the URL (www.airport.com) as a main page for the airport to support the users and people from different parts of the work information about the airport as shown in figure 108.

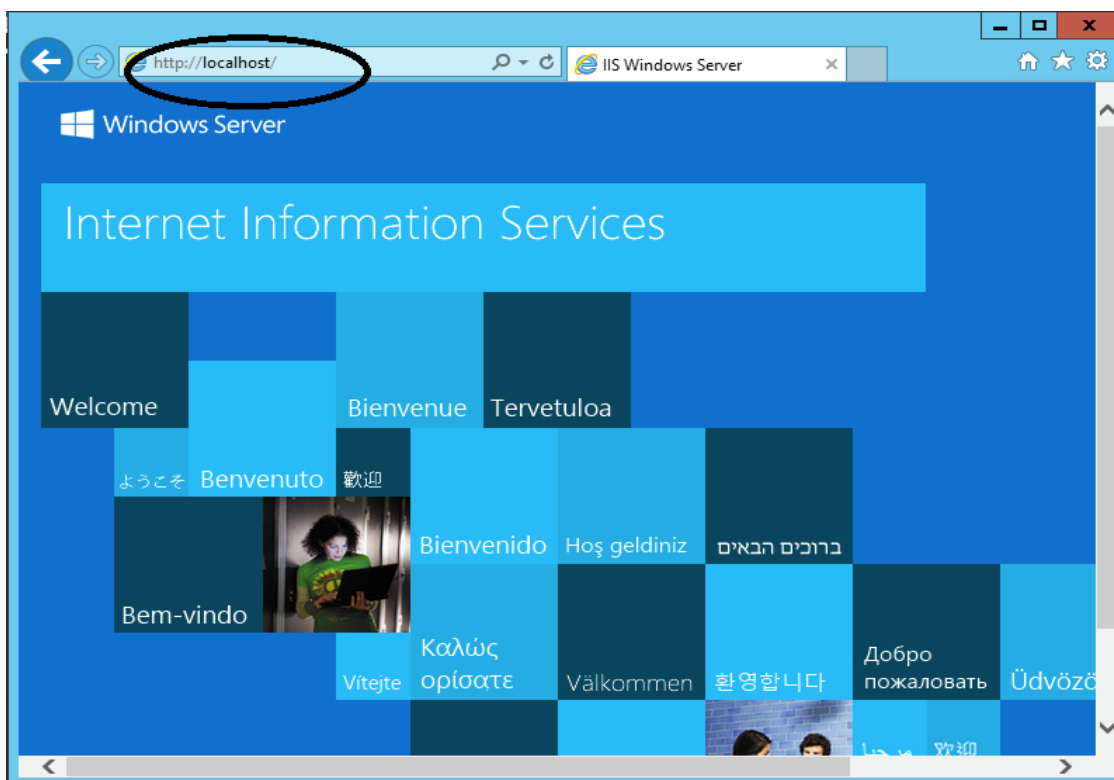


Figure 105. Web Server local host.

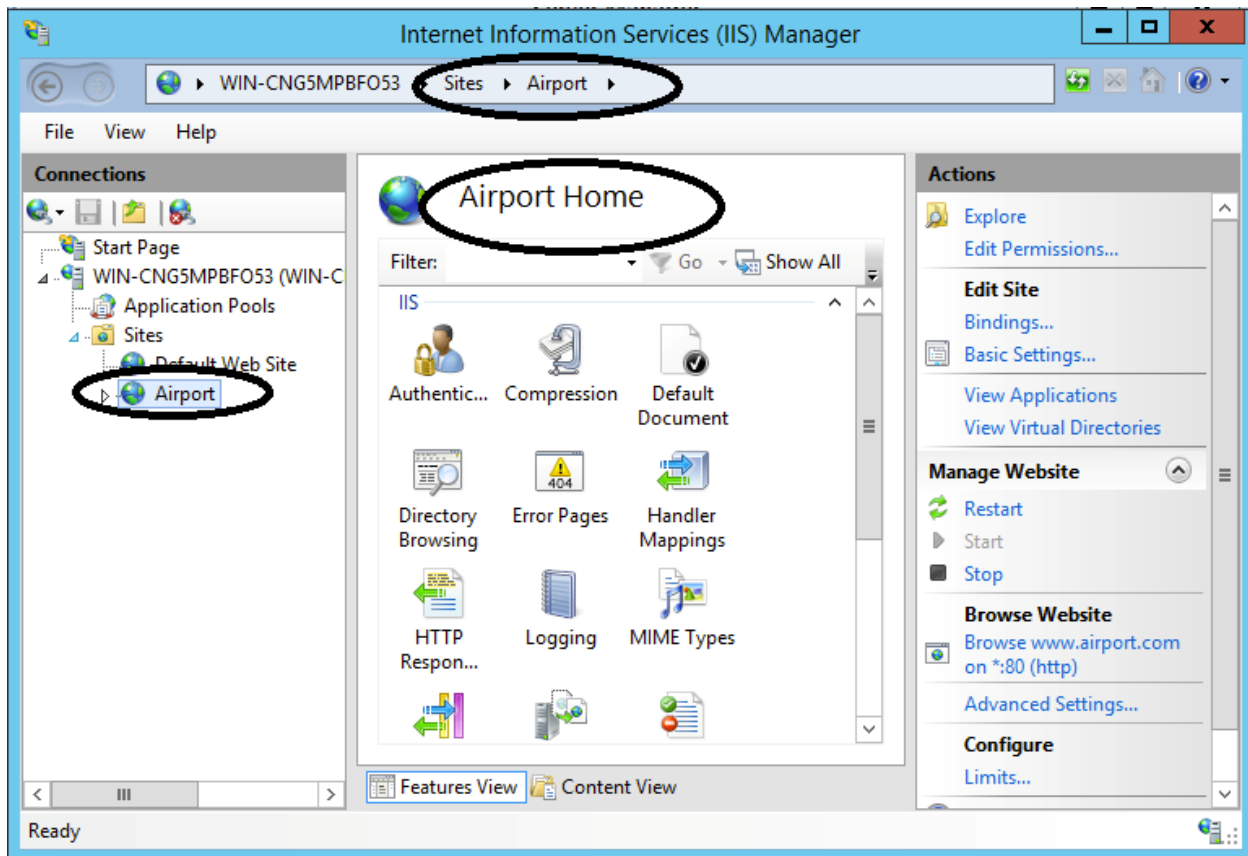


Figure 106. Airport home page.

All the above configurations were placed as a part of the network administrator responsibilities for the airport project, but creating a web page, and the coding part should be done by the web developer or web programmer as a significant aspect.

4.2 Dual Internet Service Providers (ISPs)

In the earlier parts of the project, the configurations part for failover utility in firewalls had shown the advantage of the having two internet services providers. In this section, the advantages of dual internet service providers will explain how the two ISPs can protect the flight system, which protects people's lives. In order to clarify more, the flight management department includes more than one system like datacenter and Air Traffic Control Centre, which are located in the Air Traffic Control Tower. So this part of the project focuses on the Air Traffic

Control Tower because it included the all flight control systems and is covered by the flight management department as a responsible department. According to Civil Aviation Department (2010):

In the event of a serious fire or hazardous incidents which render the Air Traffic Control Complex (ATCX) not able to perform its original function, normal air traffic control (ATC) services will be severely disrupted. To maintain the continuous ATC services, a Backup Air Traffic Control Complex (BATCX) equipped with all essential backup ATC facilities will be activated. These backup facilities can support about 30 percent air traffic control handling capacity to maintain a safe and orderly flow of air traffic.

As mentioned in the above quote, the ATCX system is the most important part of the Air Traffic Control Center which contain the flight control data. In addition, the BATCX system is responsible for the backup of the Air Traffic Control Center data which control the aircraft movement and provide the directions to the pilots to avoid aircraft collisions. Therefore, the data center in this department needs to be protected from loss. This is what the Air Traffic Control's complex system's task.

4.2.1 Dual Internet Service Providers (ISPs) Design

In the design part, the advantages of the dual Internet service providers are represented by providing 24 hours internet service for the Air Traffic Control Centre which have the all flight control systems as mentioned before. In most airports around the world, this system located in the flight management department as illustrated in figure 109.

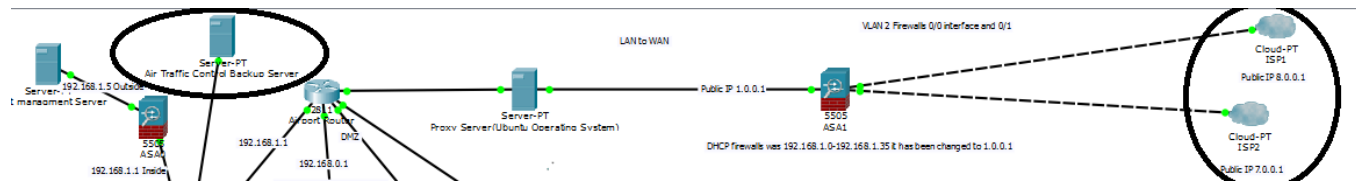


Figure 107. Dual ISPs Design.

Moreover, in the most airports, the Internet service is not one of the necessary requirements for the Air Traffic Control Centre because most of the information is generated in the Air Traffic Control Center. Also, the backup operation for the data in this system is supported by BATCX system which located in the same location. However, what will happen if this department had a fire or if an aircraft crashed in to the Air Traffic Control Center (Tower)? The expected result is losing the data or having system error like what happened in Chicago aurora airport. According to CBS News (2014):

Chicago's airports are already taxed due to a fire at the FAA Aurora facility on Friday, September 26 that caused more than 2,000 canceled flights. Brian Howard, 36, is charged with arson and sabotage. The Aurora facility handles high-altitude communications so that traffic was transferred to other nearby facilities.

As shown above, many flights were canceled in one day but other cases, if the Air Traffic Control system fails itself, it will lead to aircraft collision. In this project, the internet service has been placed to provide the Air Traffic Control system which is located in the flight management department. The Backup Air Traffic Control Complex (BATCX) was the main part that is involved in this part.

4.2.2 Dual Internet Service Providers (ISPs) Configurations

As mentioned in the design part, the flight management department has been provided by internet service providers and the aim of this service was back up the Air Traffic Control data to the cloud server which is a physical server but located out of the Air Traffic Control building (Tower). As mentioned in early steps from the project's sections, the airport's network has been provided by two ISPs which work alternately. Therefore, the configuration part for the main firewalls in the security section was configured to support the failover utility. Also, the other departments could support with one ISP without affecting the network functionality as a general. However, the main aim of using the two ISPs with failover configuration was supporting the flight management system with non-stop service. This can help the Backup Air Traffic Control Complex (BATCX) system which operates permanently, and sets the backup data in a safe location. The safe location is represented by a data center in another building and connected with the Air Traffic Control through internet services. In the configuration part, two targeted servers involved in data backup process especially the Backup Air Traffic Control Complex (BATCX) system. Wherefore, the server responsible for this process was Windows Server 2012. This server has been configured to make a backup for the BATCX system during the work operations and sent it by using the network and internet service to the target server. Both sides in Windows Server 2012 called (iSCSI initiators and iSCSI target). The iSCSI initiator's task was to backup the Air Traffic Control data and send them through the network to the storage (iSCSI target) which is located outside the airport's network. Both services configurations have been applied to the airport's network and will be explained in the following steps which used according to Bipin (2014).

In this step, the initiators server has been installed by adding roles and features to install the backup service (iSCSI initiators) on windows server 2012 as shown in Figures 110 and 111. This server can handle the backup task and sends the backup data to the target server which has been configured and will be explained in the following configurations' steps.

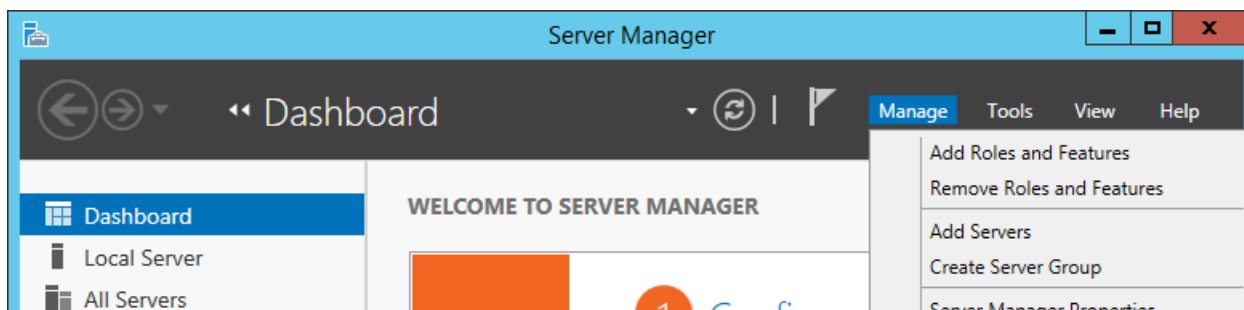


Figure 108. Add roles and features for Backup Server

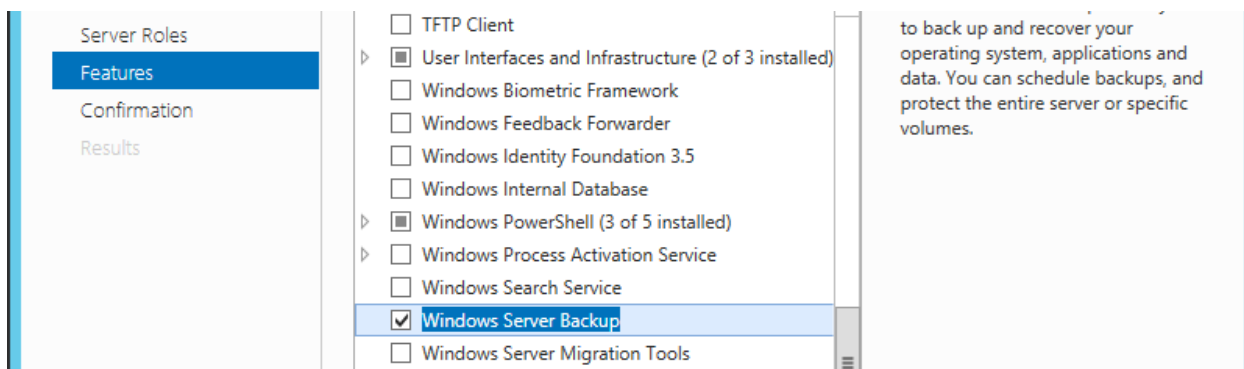


Figure 109. Windows Server backup tool.

The following steps show the configurations for the iSCSI target server which represents the storage server for the Air Traffic Control Complex's backup data which has many options for backup the data. According to Bipin:

Server 2012 now includes iSCSI software components, which means you can create SAN in server 2012. Two main components of iSCSI are iSCSI initiators and iSCSI target. iSCSI initiator is a client or system that will be using the storage from SAN. iSCSI target

is the SAN box or storage box or the server where iSCSI target component is installed. You can use Server 2012 iSCSI SAN feature to configure shared storage for fail-over clustering for Hyper V and VMware vSphere, and others.

As mentioned above, there are many ways for using the Windows Server 2012 backup utility. For this project, the VN ware has been used to host the Windows Server 2012 and use the backup role as a target server too.

The first step of installing the target server was adding roles and features to the Windows server 2012 as the (iSCSI initiators) server as shown in figure 112.

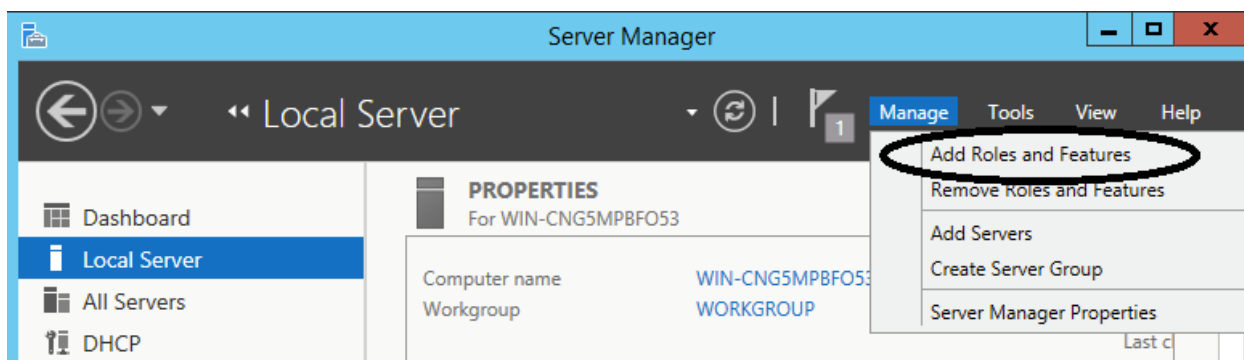


Figure 110. Add roles for a backup tool.

The second step was choosing the installation type to be appropriate for the target server as shown in figure 113.

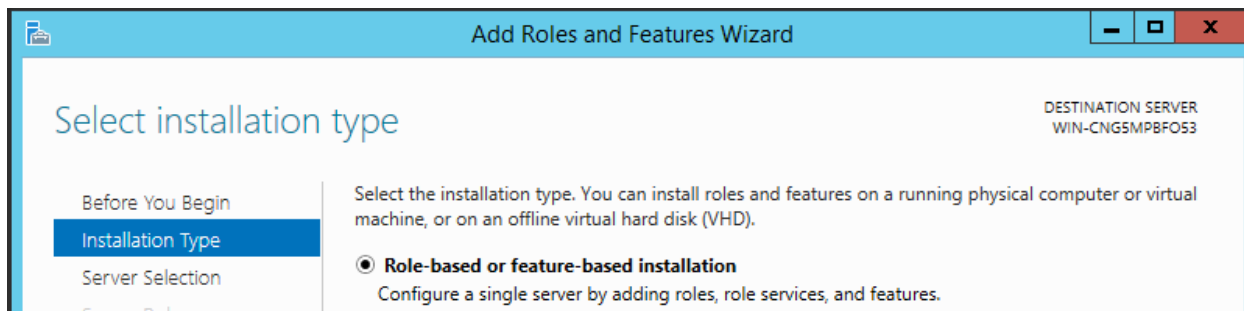


Figure 111. Backup Server installation type.

The third step was installing the iSCSI Target Server which hosts the backup storage for the Air Traffic Control system forms the Windows Server 2012 roles as shown in figure 114.

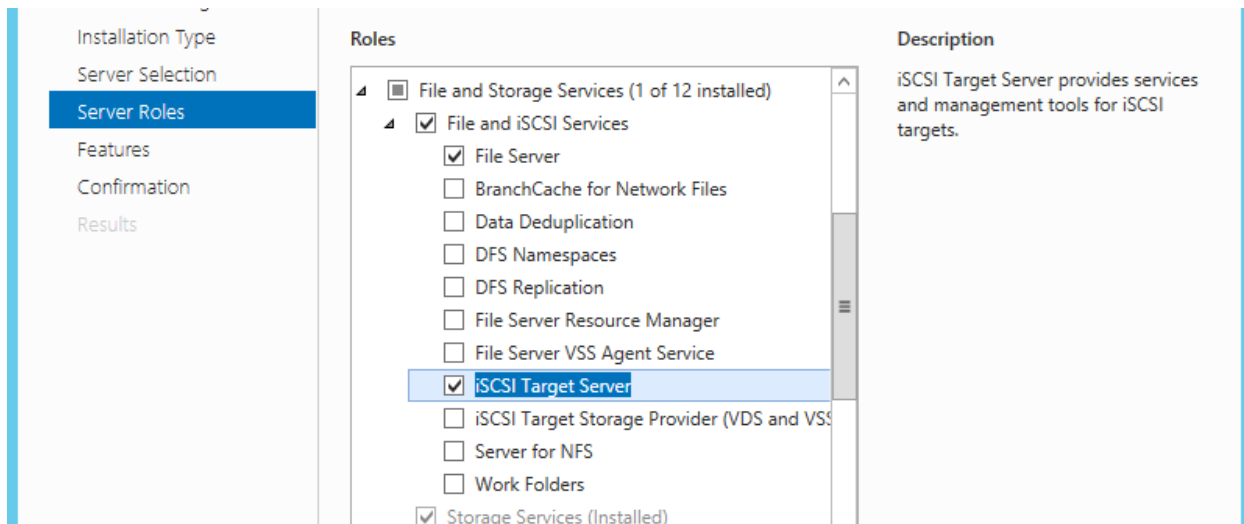


Figure 112. iSCSI Target Server roles

After installing the iSCSI target Server, the virtual disk for the Air Traffic Control has been created to host the backup data as mentioned in the following steps.

The first step of creating the virtual disk was preparing the available disks with NTFS format with the size of the storage. For the Air Traffic Control system, the size should be more than 5TB to provide enough storage space for the system. In this case, the presumed area was 5TB as shown in figure 115 and 116.

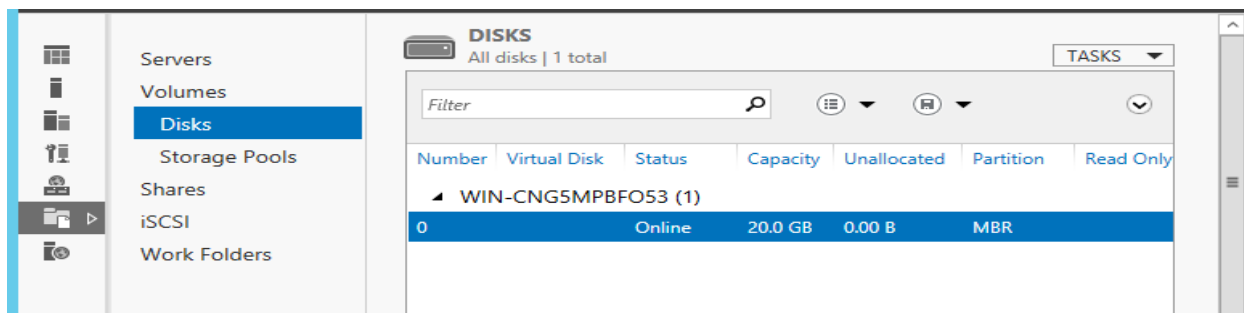


Figure 113. Backup Server disk space.

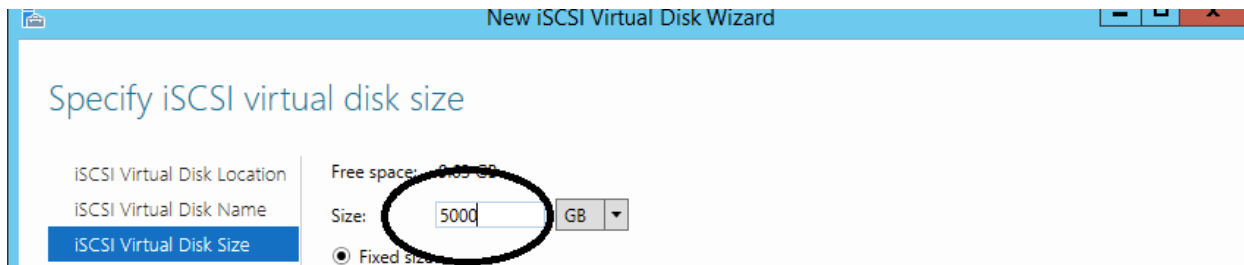


Figure 114. iSCSI virtual disk size

The second step of creating the disk portion was naming the hard drive portion to be recognized during the backup operations, and when calling the data in the emergency situations, these configurations have been done after some simple steps, including assigning the target name as show in figure 117.

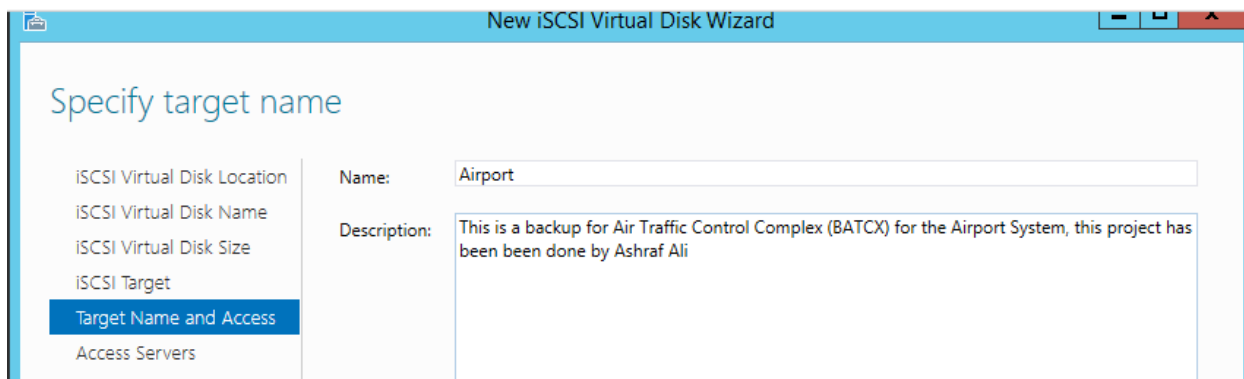


Figure 115. Target Server name.

The third step was assigning the IP address to the target server to identify the initiator server that uses the target storage disk. This can help the target server to identify the initiator server, which located in the airport's network, from outside and provided the backup data in case of need. As shown in figure 118, the IP that has been assigned for the initiator server was (192.168.1.10) which was in the flight management network.

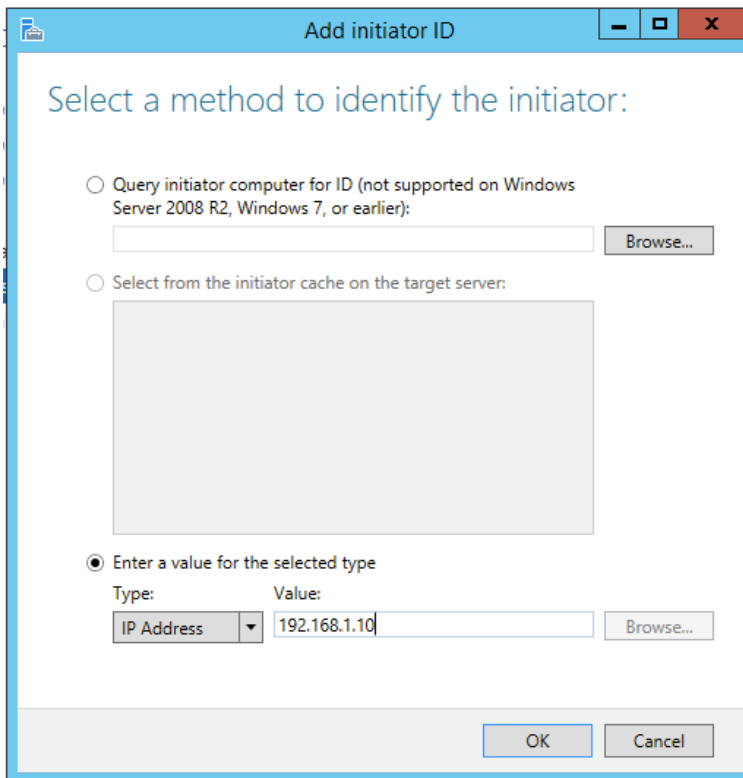


Figure 116. iSCSI initiators server IP address

After finishing the configurations, the target server was ready to receive the data from the initiator in the Air Traffic Control system as shown in figure 119.

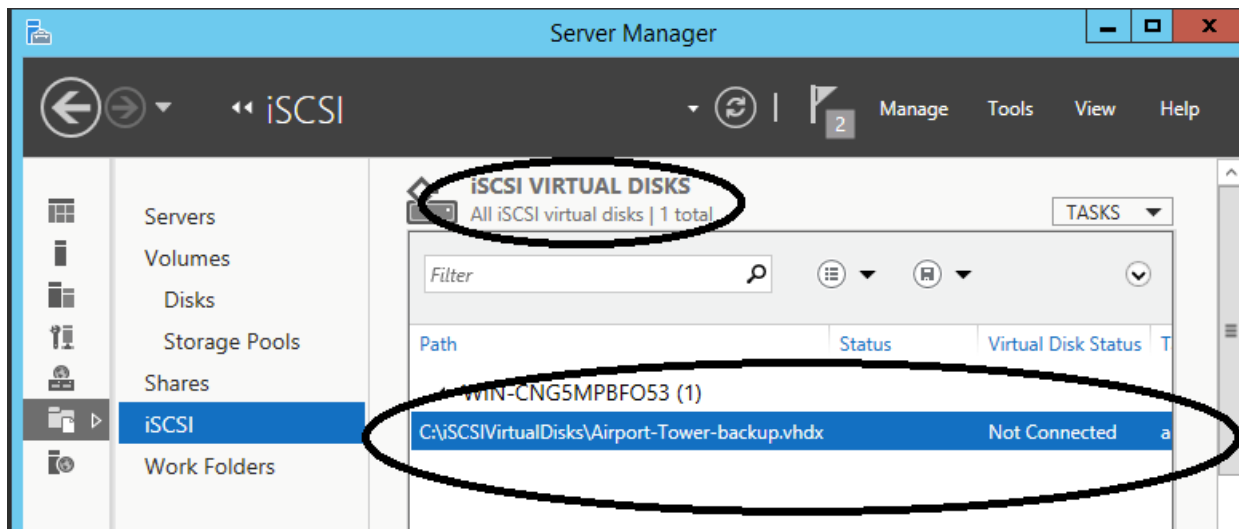


Figure 117. Air Traffic Control system virtual disk.

This server should be located outside the local network for safety purposes. Also, as mentioned before, the aim of this backup is keeping the Air Traffic Control system's data in a safe place which leads to saving the passengers' lives from aircraft collisions and many other problems when the system goes down. This part of configurations also shows the importance of having two internet providers on the network, which helps to enable the backup process from working permanently.

5 Conclusions

5.1 Research Questions

This project and the design focused on the security, quality and safety aspects that can be provided to an airport's network. Therefore, the thesis integrates multiple areas in the networking field to introduce the best technical options available. This thesis started with the idea of investigating the most common problems that happen in airports. As the world testifies, terrorist attacks over the Internet increase these days and this was the primary factor in providing the necessary protection to the airport's network. From this concept, the airport's network has been designed and configured to provide a high quality of service. Hardware based firewalls, an IP access control list, MAC address control, a domain server and a proxy server were the tools that applied to prevent the hackers accessing the flight management department, which is the most important department for any airport. The quality of service was another consideration used to help define a fully-featured network that is suitable for international airports. Failover firewalls utility, PXE server, DHCP server, DNS server and cabling design are the tools that help to provide a high quality of service to the airport's network. The last and most important side of the airport's network design and implementation was protecting passengers' lives. Dual ISPs were

the principal mechanism to back up the data from Air Traffic Control, which is the most sensitive system in terms of passengers' safety.

5.2 Future Questions/Future Research Directions

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

Additional effort on several questions is possible. These include:

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

5.3 Summary

As explained previously, airports are high risk and high exposure facilities. Therefore, this project has been informed by many technical means that can provide a high level of security and quality of service while preserving safety for passengers. The security part of the airport's network has been provided with security tools like hardware firewalls, an IP access control list, Mac address port security, a domain server and a proxy server to prevent unauthorized users from entering the flight management system and the service providers' department data. The quality part of the network has been enhanced through numerous tools. These include failover firewalls utility, PXE server, DHCP server, DNS server and cabling design. The safety part was focused on saving the airport's information and passengers. The airport's information has been protected by backing up the Air Traffic Control Systems' information to outside the local network with Windows server 2012 tools. The passengers' information has been supported by a secure environment with the local Webserver. As a result of these techniques, the airport's network is ready to provide a secure environment with a high quality of service and safety for the airport's system and passengers.

References

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

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

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

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

Bipin. (2014, April 01). Configure iSCSI SAN in Server 2012 R2. Retrieved April 01, 2016,

from <http://www.mustbegeek.com/configure-iscsi-san-in-server-2012-r2/>

Boyce, J. (2000, July 20). Understanding how DNS works, part 1 - TechRepublic. Retrieved

March 23, 2016, from <http://www.techrepublic.com/article/understanding-how-dns-works-part-1/>

Burns, S. F. GIAC Security Essentials Certification (GSEC) Practical Assignment v1. 4c January 5, 2005. Threat Modeling: A Process to Ensure Application Security.

C. D. (2012, October 01). Server 2012 DHCP Server Role • PC-Addicts. Retrieved March 19,

2016, from <http://pc-addicts.com/server-2012-dhcp-server-role/>

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

CBSNews. (2014, October 6). Chicago flights grounded for second time in two weeks. Retrieved

March 31, 2016, from <http://www.cbsnews.com/news/chicago-flights-grounded-for-second-time-in-two-weeks/>

- Cezar, M. (2014, October 16). Setting up a 'PXE Network Boot Server' for Multiple Linux Distribution Installations in RHEL/CentOS 7. Retrieved March 22, 2016, from <http://www.tecmint.com/install-pxe-network-boot-server-in-centos-7/>
- Chadwick, D. W. (2001). Network Firewall Technologies. *NATO SCIENCE SERIES SUB SERIES III COMPUTER AND SYSTEMS SCIENCES*, 178, 149-168.
- Cisco Systems, Inc. (2003, March 14). CCNA: Network Media Types. Retrieved March 26, 2016, from <http://www.ciscopress.com/articles/article.asp?p=31276>
- Cisco. (n.d.). Cisco IOS Classic Firewall Stateful Failover High Availability Solution. Retrieved March 24, 2016, from http://www.cisco.com/c/en/us/products/collateral/routers/3800-series-integrated-services-routers-isr/white_paper_c11_472858.html
- Civil Aviation Department. (2010, January 6). Functions of Various Air Traffic Control Equipment for the Airport. Retrieved March 30, 2016, from <http://www.cad.gov.hk/english/esd equip.html#backup>
- Costantini, D. (2015, March 27). How to install and configure IIS on Windows Server 2012 R2. Retrieved March 28, 2016, from <http://thesolving.com/server-room/how-to-install-and-configure-iis-on-windows-server-2012-r2/>
- Cowan, P. (2008). What is PXE?.
- Itgeared. (2012, December 15). How to Install the DNS Service on Server 2012 (Step by Step). Retrieved March 25, 2016, from https://www.youtube.com/watch?v=-5_KGCH1nzY
- Kaur, H., & Alm, M. A. (2012). Implementation of Portion Approach in Distributed Firewall Application for Network Security Framework. *arXiv preprint arXiv:1201.4555*.

- Kenner, A. (2010, January 1). Home Web Server Security Part 1. Retrieved March 27, 2016, from <http://www.htmlgoodies.com/beyond/security/article.php/3604136/Home-Web-Server-Security-Part-1.htm>
- Khalil, G. (2012, July 18). Configuring Active Directory (AD DS) in Windows Server 2012. Retrieved March 20, 2016, from <http://sharepointgeorge.com/2012/configuring-active-directory-ad-ds-in-windows-server-2012/>
- Lambert, P. (2012). The basics of using a proxy server for privacy and security. Tech Republic.
- McQuerry, S. (2004, April 9). CCNA Self-Study: Network Media (The Physical Layer). Retrieved March 25, 2016, from <http://www.ciscopress.com/articles/article.asp?p=169686>
- Microsoft Corporation. (2006, January). Chapter 2 – Threats and Countermeasures. Retrieved March 28, 2016, from <https://msdn.microsoft.com/en-us/library/ff648641.aspx>
- Microsoft, T. (n.d.). How DNS Works. Retrieved March 23, 2016, from [https://technet.microsoft.com/enus/library/cc772774\(v=ws.10\).aspx#w2k3tr_dns_how_e_hij](https://technet.microsoft.com/enus/library/cc772774(v=ws.10).aspx#w2k3tr_dns_how_e_hij)
- Minasi, M., Greene, K., Booth, C., Butler, R., McCabe, J., Panek, R., ... & Roth, S. (2013). Mastering Windows Server 2012 R2. John Wiley & Sons.
- National Electrical Contractors Association. (2004). Installing and Testing Fiber Optic Cables. Retrieved March 26, 2016, from http://www.westfield.in.gov/egov/documents/1202477639_843017.pdf

- Nelson, B. (2014, September 03). How to Setup and Configure DNS in Windows Server 2012 - Install and Configure DNS on Windows Server 2012. Retrieved March 24, 2016, from <http://www.tomsitpro.com/articles/configure-dns-windows-server-2012,2-793.html>
- Peters, C. (2012, March 27). Networking 101: Understanding Your Needs and Options. Retrieved March 25, 2016, from <http://www.techsoup.org/support/articles-and-how-tos/networking-101-understanding-networking-needs-and-options>
- Sachin, P. (2013, May 29). Network design proposal for airport. Retrieved April 05, 2016, from <http://projectsinnetworking.com/network-design-proposal-for-airport/>
- Sedayao, J. (2001). *Cisco IOS access lists*. " O'Reilly Media, Inc."
- Semeria, C. (1996). Internet firewalls and security: a technology overview. 3Com Corporation.
- Sequeira, A. (2012, October 24). CCNP Security Firewall Cert Guide: Configuring ASA Interfaces. Retrieved March 22, 2016, from <http://www.ciscopress.com/articles/article.asp?p=1924778>
- Stanek, W. (2012). Windows Server 2012 Pocket Consultant. Pearson Education.
- Stretch, J. (2010, May 3). Port Security. Retrieved March 21, 2016, from <http://packetlife.net/blog/2010/may/3/port-security/>
- Wilkins, S. (2013, June 27). Cisco ASA Access Lists Concepts and Configuration. Retrieved March 22, 2016, from <http://www.ciscopress.com/articles/article.asp?p=2104953>
- Windows Server. (n.d.). Retrieved March 11, 2016, from Windows Server. (n.d.). Retrieved March 11, 2016, from [https://technet.microsoft.com/en-us/library/cc732649\(v=ws.10\).aspx#BKMK_1](https://technet.microsoft.com/en-us/library/cc732649(v=ws.10).aspx#BKMK_1)

Yeh, T., & Pan, Y. (2012, February). Improving the performance of the web proxy server through group prefetching. In Proceedings of the 6th International Conference on Ubiquitous Information Management and Communication (p. 81). ACM.