ENTERPRISE NETWORK DESIGN AND IMPLEMENTATION FOR AIRPORTS

Table of Contents

Table of Contents 1
Tables Figures 2
1. Executive Summary 3
2. Introduction 3
3. Project Scope 3
4. Project Statement 4
5- Project Requirements 4
6. Network Topology 5
7. Required Configuration 7
8. Planning 7
9. Development Plan: 8
10. IP addressing 8
10.1 VLANs 9
10.2 VTP – VLAN Trunking Protocol 10
10.3 DHCP – Dynamic Host Configuration Protocol 11
10.4 EIGRP – Enhanced Interior Gateway Routing Protocol 14
10.5 NAT – Network Address Translation 14
10.6 ACL – Access Control List 15
10.7 Testing 16
10.8 Connectivity 18
11. Conclusion 20
12. References 20

Tables Figures

Figure 1 Network Diagram 5
Figure 2 Network Topology 6
Figure 3 Figure 4 Work Breakdown Structure of Project 7
Figure 5 Development plan IP Addressing 8
Figure 6 IP Addressing on Switches 8
Figure 7. IP Addresses Access Switches 9
Figure 8 IP Addresses Access Points 9
Figure 9 VLAN Status 10
Figure 10 VTP status 11
Figure 11 DHCP pool 12
Figure 12 Ping test 13
Figure 13 EIGRP Status 14
Figure 14 NAT Show 14
Figure 15 show ports status 15
Figure 16 ACL Access Control List 15
Figure 17 Pinging Internet router, R1, R2. 16
Figure 18 Testing 17
Figure 19 Connectivity 18
Figure 20 Preview 19

1. Executive Summary

In this project we design and implement a secure network for modern airport in which we maintain the security, quality, and safety of systems. The project has been provided with different utilities to introduce a network with a high security level for the airport. These utilities are hardware firewalls, an IP access control list, Mac address port security, a domain server and s proxy server. All of these utilities have been configured to provide a secure environment for the entire network and to prevent hackers from entering sensitive departments like the flight management and service providers departments. The total cost of this project 45,000$ [1]

2. Introduction

Airports are the sensitive places around the world. Technology plays many different roles to protect and represent a high quality of services for these places. Computer networking is the most crucial part of modern airports because this new technology takes the most important responsibilities, rather than people doing the tasks as in previous decades.

We installed and configure the network devices such as switches, routers, computers, IP Phones, & APs. We made topology and created IP address with minimum wastage of IP addresses. This project also consists of hardware-based firewalls, an IP access control list, MAC address control, a domain server and a proxy server are the tools that applied to prevent the hackers accessing the flight management department, which is the important department for any airport.

The network is designed to be scalable based upon requirements because scalability has been the most important consideration during the planning phase. Further security appliances such as IPS, IDS, NGFW etc. can be added to improve security and make the network bullet proof.

3. Project Scope

The project calls for the design and implementation of a secure network for a modern airport based in South Asia in which we maintain the security, quality, and safety of systems

4. Project Statement

The project goals and objectives include:

1. Building a highly resilient Network used in large airports and used by millions of uses per year.
2. Building a high throughput network
3. Providing a high security level for the airport's network
4. Providing a high quality of service for the airport's network
5. Maintaining the passengers' safety
6. Maintaining passengers' info
7. Supporting the FMS (flight management system)

In this project we will implement the security for servers and internal network as well. The project is design to secure the network from the following threats:

1- Unauthorized access devices.
2- Unencrypted or plaintext information.
3- DHCP Snooping.
4- Internal Access.

5- Project Requirements

Requirements for the network are:

1. All 100 employees be interconnected whether its LAN or WLAN.
2. We've to accommodate about 200 IP addresses, since everyone has smartphone and requires internet connectivity.
3. Employees need internet access
4. Only Cisco Networking devices will be used.
5. The network must be secure, redundant and fast.

6. Network Topology

The network is connected to the internet with a Firewall and the servers are in a DMZ (Demilitarized Zone). In this way, the outside world can access the servers but cannot access the internal network. [2]

3 Wireless Access Points are also used for accommodating employees' smartphones/laptops.

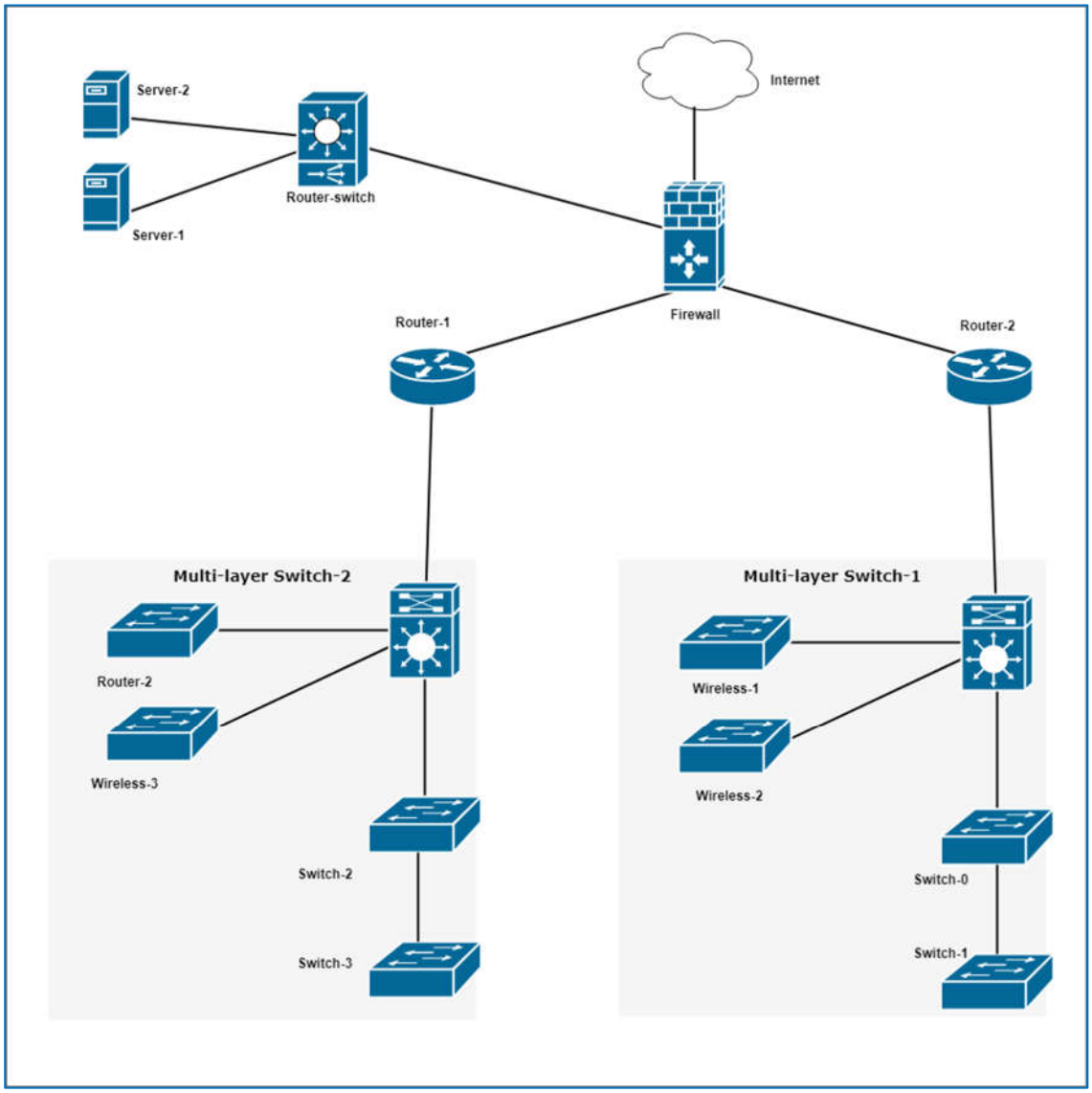


Figure 1 Network Diagram

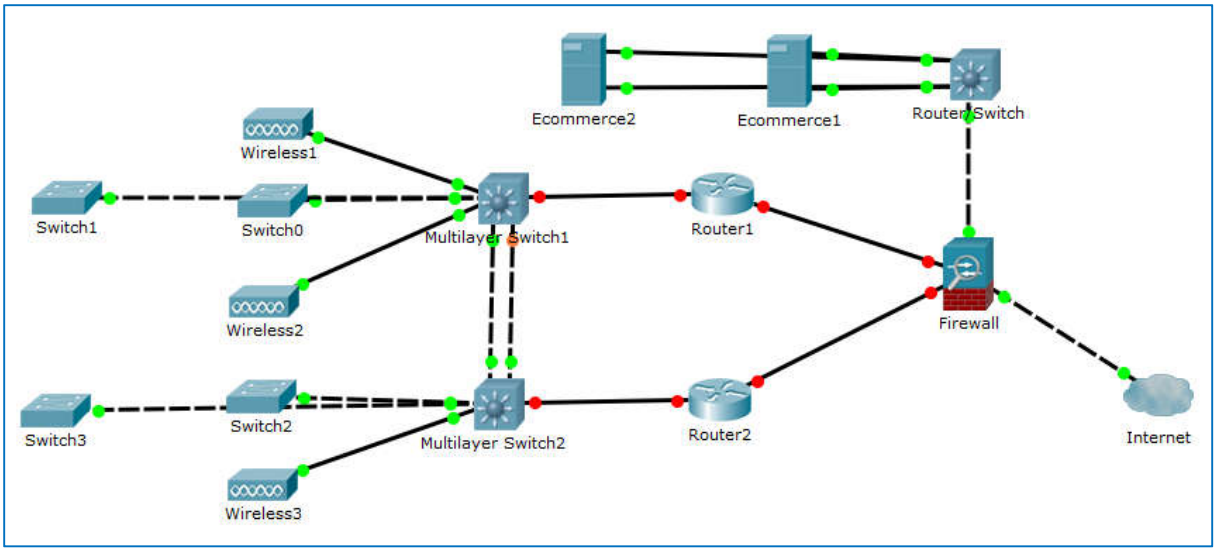


Figure 2 Network Topology

Cisco 2951 routers for Internet Connectivity. [3]

Cisco Catalyst 2960x 48TS Access layer switches. [4]

Cisco WS-C3850-12S will be used as multilayer-switches in distribution.

Cisco LinkSys EA9300 routers WLAN. [5]

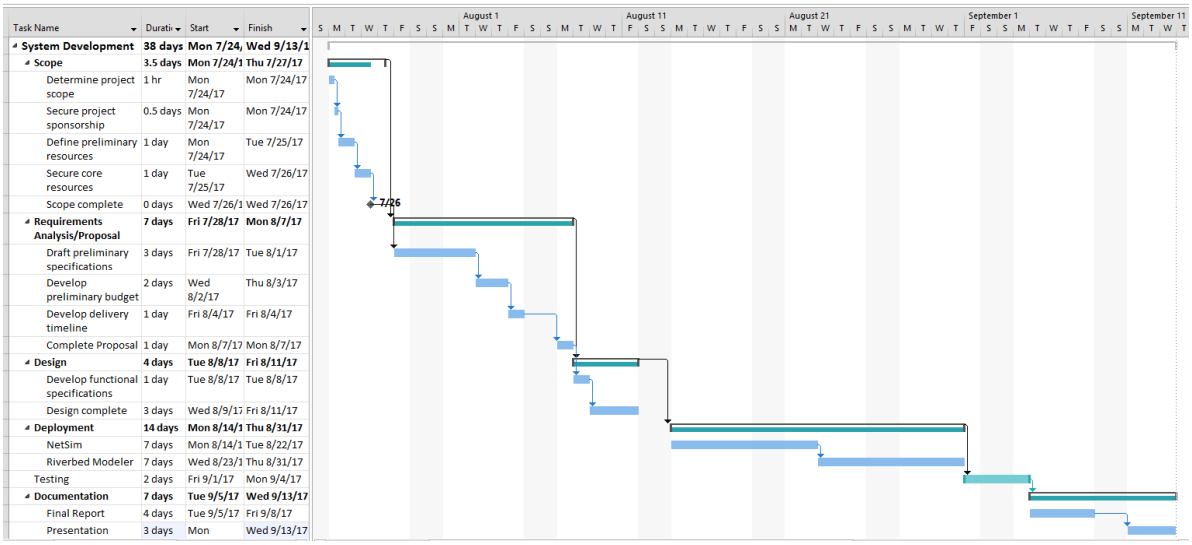
7. Required Configuration

Routers, Switches and firewall will have to be configured with at least the following technologies:

1. IP addresses, Basic Security
2. DHCP
3. Routing protocol preferably EIGRP
4. NAT (Network Address Translation
5. ACL (Access Control Lists)

8. Planning

Work Breakdown Structure of project:



Task Name	Durati	Start	Finish
System Development	**38 days**	**Mon 7/24,**	**Wed 9/13/1**
Scope	**3.5 days**	**Mon 7/24/1**	**Thu 7/27/17**
Determine project scope	1 hr	Mon 7/24/17	Mon 7/24/17
Secure project sponsorship	0.5 days	Mon 7/24/17	Mon 7/24/17
Define preliminary resources	1 day	Mon 7/24/17	Tue 7/25/17
Secure core resources	1 day	Tue 7/25/17	Wed 7/26/17
Scope complete	0 days	Wed 7/26/1	Wed 7/26/17
Requirements Analysis/Proposal	**7 days**	**Fri 7/28/17**	**Mon 8/7/17**
Draft preliminary specifications	3 days	Fri 7/28/17	Tue 8/1/17
Develop preliminary budget	2 days	Wed 8/2/17	Thu 8/3/17
Develop delivery timeline	1 day	Fri 8/4/17	Fri 8/4/17
Complete Proposal	1 day	Mon 8/7/17	Mon 8/7/17
Design	**4 days**	**Tue 8/8/17**	**Fri 8/11/17**
Develop functional specifications	1 day	Tue 8/8/17	Tue 8/8/17
Design complete	3 days	Wed 8/9/17	Fri 8/11/17
Deployment	**14 days**	**Mon 8/14/1**	**Thu 8/31/17**
NetSim	7 days	Mon 8/14/1	Tue 8/22/17
Riverbed Modeler	7 days	Wed 8/23/1	Thu 8/31/17
Testing	2 days	Fri 9/1/17	Mon 9/4/17
Documentation	**7 days**	**Tue 9/5/17**	**Wed 9/13/17**
Final Report	4 days	Tue 9/5/17	Fri 9/8/17
Presentation	3 days	Mon	Wed 9/13/17

Figure 3 Figure 4 Work Breakdown Structure of Project

9. Development Plan:

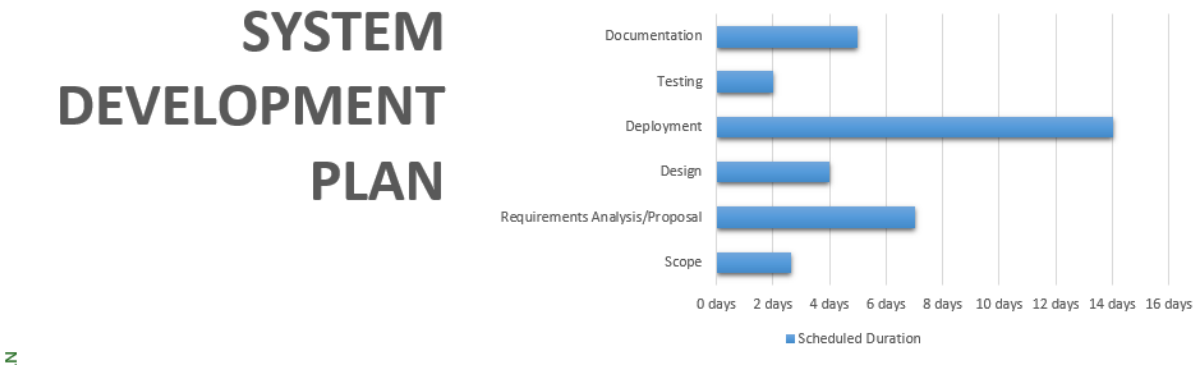


Figure 5 Development plan IP Addressing

10. IP addressing

Switch1 and Switch2:

Device	IP Address	Description
Switch1	192.168.1.1/26	Gateway For VLAN 10
	192.168.1.65/26	Gateway For VLAN 20
	192.168.1.129/26	Gateway For VLAN 30
	192.168.1.193/26	Gateway For VLAN 40
Switch2	192.168.1.2/26	Gateway For VLAN 10
	192.168.1.66/26	Gateway For VLAN 20
	192.168.1.130/26	Gateway For VLAN 30
	192.168.1.194/26	Gateway For VLAN 40

Figure 6 IP Addressing on Switches

The IP Addresses on MLSwitch2 were assigned as proposed, however the interfaces were closed because there was unidentified problem in communicating between VLANs.

Access Switches:

Device	IP Address	Description
Switch1	192.168.1.4/26	Switch Access (SSH)
Switch2	192.168.1.68/26	Switch Access (SSH)
Switch3	192.168.1.132/26	Switch Access (SSH)
Switch4	192.168.1.196/26	Switch Access (SSH)

Figure 7. IP Addresses Access Switches

Access Points:

The same mistake was made for access points however, since APs are not available in NETSIM, no problem arose.

Device	IP Address	Description
AP1	192.168.1.5/26	Wireless VLAN10
AP2	192.168.1.69/26	Wireless VLAN20
AP3	192.168.1.133/26	Wireless VLAN30
AP4	192.168.1.197/26	Wireless VLAN40

Figure 8 IP Addresses Access Points

10.1 VLANs

Switchport mode access makes the port an access port or a port that can be connected to only a PC or 1 VLAN. Switchport access vlan 10 assigns the port to vlan 10 and creates vlan 10 if it doesn't exist.

```
Access-Switch-1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Fa0/25, Fa0/26
                                                Fa0/27, Fa0/28, Fa0/29, Fa0/30
                                                Fa0/31, Fa0/32, Fa0/33, Fa0/34
                                                Fa0/35, Fa0/36, Fa0/37, Fa0/38
                                                Fa0/39, Fa0/40, Fa0/41, Fa0/42
                                                Fa0/43, Fa0/44, Fa0/45, Fa0/46
                                                Fa0/47, Fa0/48, Gi0/1, Gi0/2
10   VLAN0010                         active    Fa0/2
20   VLAN0020                         active
30   VLAN0030                         active
40   VLAN0040                         active
```

Figure 9 VLAN Status

Here we can see that it is trunking and mode is desirable which means if a PC is connected to it, it'll act as access port and if a switch is connected, it'll act as trunk port.

10.2 VTP – VLAN Trunking Protocol

Following screenshot shows output of show vtp status before and after creating a new vlan on switch ML1.

```
ML1#show vtp stat
VTP Version                     : 2
Configuration Revision          : 4
Maximum VLANs supported locally : 64
Number of existing VLANs        : 9

VTP Operating Mode              : Server
VTP Domain Name                 : ABC
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xEE 0xB3 0xDC 0x9F 0xE2 0xE0 0x25 0xDF
Configuration last modified by 0.0.0.0 at 3-1-2012 04:55:57
Local updater ID is 0.0.0.0 (no valid interface found)

ML1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ML1(config)#vlan 100
VLAN 100 added:
    Name:VLAN0100
ML1(config-vlan)#do show vtp stat
VTP Version                     : 2
Configuration Revision          : 5
Maximum VLANs supported locally : 64
Number of existing VLANs        : 10

VTP Operating Mode              : Server
VTP Domain Name                 : ABC
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xEE 0xB3 0xDC 0x9F 0xE2 0xE0 0x25 0xDF
Configuration last modified by 0.0.0.0 at 3-1-2012 04:55:57
Local updater ID is 0.0.0.0 (no valid interface found)
```

Figure 10 VTP status

Following screenshot from Switch1 shows output of show vtp status and show vlan brief before creation of Vlan100 on ML1.

10.3 DHCP – Dynamic Host Configuration Protocol

DHCP servers were created on MLSwitch1 and MLSwitch2 but were reduced to only MLSwitch2 because of problem in communication.

```
ip dhcp excluded-address 192.168.0.1 192.168.0.20
ip dhcp excluded-address 192.168.1.1 192.168.1.2
ip dhcp excluded-address 192.168.1.65 192.168.1.66
ip dhcp excluded-address 192.168.1.129 192.168.1.130
ip dhcp excluded-address 192.168.1.193 192.168.1.194
!
ip dhcp pool VLAN10
 network 192.168.1.0 255.255.255.192
 default-router 192.168.1.1
ip dhcp pool VLAN20
 network 192.168.1.64 255.255.255.192
 default-router 192.168.1.65
ip dhcp pool VLAN30
 network 192.168.1.128 255.255.255.192
 default-router 192.168.1.129
ip dhcp pool VLAN40
 network 192.168.1.192 255.255.255.192
 default-router 192.168.1.193
ip dhcp pool VLAN1
 network 192.168.0.0 255.255.255.0
 default-router 192.168.0.1
```

Figure 11 DHCP pool

PC in VLAN 40

As soon as PC is set to get IP Address from DHCP, it gets its IP Address. The following screenshot shows successful ping from VLAN40 to its gateway, VLAN10's gateway, VLAN20's gateway.

```
%DHCP-6-ADDRESS_ASSIGN: Interface Ethernet0 assigned DHCP address 192.168.1.195, mask 255.255.255.192,

C:>ping 192.168.1.193

Pinging 192.168.1.193 with 32 bytes of data:
Reply from 192.168.1.193: bytes=32 time=64ms TTL=241
Reply from 192.168.1.193: bytes=32 time=70ms TTL=241
Reply from 192.168.1.193: bytes=32 time=51ms TTL=241
Reply from 192.168.1.193: bytes=32 time=68ms TTL=241
Reply from 192.168.1.193: bytes=32 time=51ms TTL=241

Ping statistics for 192.168.1.193:
     Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
     Minimum = 51ms, Maximum =  70ms, Average =  61ms

C:>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=51ms TTL=241
Reply from 192.168.1.1: bytes=32 time=53ms TTL=241
Reply from 192.168.1.1: bytes=32 time=66ms TTL=241
Reply from 192.168.1.1: bytes=32 time=60ms TTL=241
Reply from 192.168.1.1: bytes=32 time=59ms TTL=241

Ping statistics for 192.168.1.1:
     Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
     Minimum = 51ms, Maximum =  66ms, Average =  58ms

C:>ping 192.168.1.65

Pinging 192.168.1.65 with 32 bytes of data:
Reply from 192.168.1.65: bytes=32 time=60ms TTL=241
Reply from 192.168.1.65: bytes=32 time=69ms TTL=241
Reply from 192.168.1.65: bytes=32 time=67ms TTL=241
Reply from 192.168.1.65: bytes=32 time=53ms TTL=241
Reply from 192.168.1.65: bytes=32 time=64ms TTL=241

Ping statistics for 192.168.1.65:
     Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
     Minimum = 53ms, Maximum =  69ms, Average =  63ms
```

Figure 12 Ping test

10.4 EIGRP – Enhanced Interior Gateway Routing Protocol

Following screenshot shows EIGRP's parameters and neighbors.

```
ML1#show ip protocols
Routing Protocol is "eigrp 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing:
  Automatic network summarization is not in effect
  Routing for Networks:
    192.168.1.0 0.0.0.255
    192.168.2.12 0.0.0.3
    192.168.0.0 0.0.0.255
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.2.13           90      04:09:13
  Distance: internal 90 external 170

ML1#show ip eigrp nei

EIGRP-IPv4 Neighbors for AS(10)
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   192.168.2.13            Fa0/1             13 04:10:49  216  1296  0  10
```

Figure 13 EIGRP Status

10.5 NAT – Network Address Translation

The following command shows translation of 192.168.1.195 which is VLAN40 PC to 100.1.1.2 which is R1's outside interface.

```
R1#show ip nat translation
Pro  Inside global     Inside local       Outside local      Outside global
icmp 100.1.1.2:9392    192.168.1.195:9392 100.1.1.1:9392     100.1.1.1:9392
icmp 100.1.1.2:9393    192.168.1.195:9393 100.1.1.1:9393     100.1.1.1:9393
icmp 100.1.1.2:9394    192.168.1.195:9394 100.1.1.1:9394     100.1.1.1:9394
icmp 100.1.1.2:9395    192.168.1.195:9395 100.1.1.1:9395     100.1.1.1:9395
icmp 100.1.1.2:9396    192.168.1.195:9396 100.1.1.1:9396     100.1.1.1:9396
```

Figure 14 NAT Show

10.6 ACL – Access Control List

All unused ports on switches were shut down.

```
FastEthernet0/1        unassigned      YES unset  up                    up
FastEthernet0/2        unassigned      YES unset  up                    up
FastEthernet0/3        unassigned      YES unset  administratively down down
FastEthernet0/4        unassigned      YES unset  administratively down down
FastEthernet0/5        unassigned      YES unset  administratively down down
FastEthernet0/6        unassigned      YES unset  administratively down down
FastEthernet0/7        unassigned      YES unset  administratively down down
FastEthernet0/8        unassigned      YES unset  administratively down down
FastEthernet0/9        unassigned      YES unset  administratively down down
FastEthernet0/10       unassigned      YES unset  administratively down down
FastEthernet0/11       unassigned      YES unset  administratively down down
FastEthernet0/12       unassigned      YES unset  administratively down down
FastEthernet0/13       unassigned      YES unset  administratively down down
FastEthernet0/14       unassigned      YES unset  administratively down down
FastEthernet0/15       unassigned      YES unset  administratively down down
FastEthernet0/16       unassigned      YES unset  administratively down down
FastEthernet0/17       unassigned      YES unset  administratively down down
FastEthernet0/18       unassigned      YES unset  administratively down down
FastEthernet0/19       unassigned      YES unset  administratively down down
FastEthernet0/20       unassigned      YES unset  administratively down down
FastEthernet0/21       unassigned      YES unset  administratively down down
FastEthernet0/22       unassigned      YES unset  administratively down down
FastEthernet0/23       unassigned      YES unset  administratively down down
FastEthernet0/24       unassigned      YES unset  administratively down down
FastEthernet0/25       unassigned      YES unset  administratively down down
FastEthernet0/26       unassigned      YES unset  administratively down down
FastEthernet0/27       unassigned      YES unset  administratively down down
FastEthernet0/28       unassigned      YES unset  administratively down down
FastEthernet0/29       unassigned      YES unset  administratively down down
FastEthernet0/30       unassigned      YES unset  administratively down down
FastEthernet0/31       unassigned      YES unset  administratively down down
FastEthernet0/32       unassigned      YES unset  administratively down down
FastEthernet0/33       unassigned      YES unset  administratively down down
FastEthernet0/34       unassigned      YES unset  administratively down down
FastEthernet0/35       unassigned      YES unset  administratively down down
FastEthernet0/36       unassigned      YES unset  administratively down down
```

Figure 15 show ports status

Enable Secret on all devices was set to cisco123.

ACL

The following access-list was configured on R1 and R2.

```
access-list 100 permit tcp any 192.168.2.1 0.0.0.3 eq www
access-list 100 permit eigrp any any
access-list 100 permit ip any host 100.1.1.2
access-list 100 deny   ip any any
!
```

Figure 16 ACL Access Control List

10.7 Testing

Pinging Internet router, R1, R2.

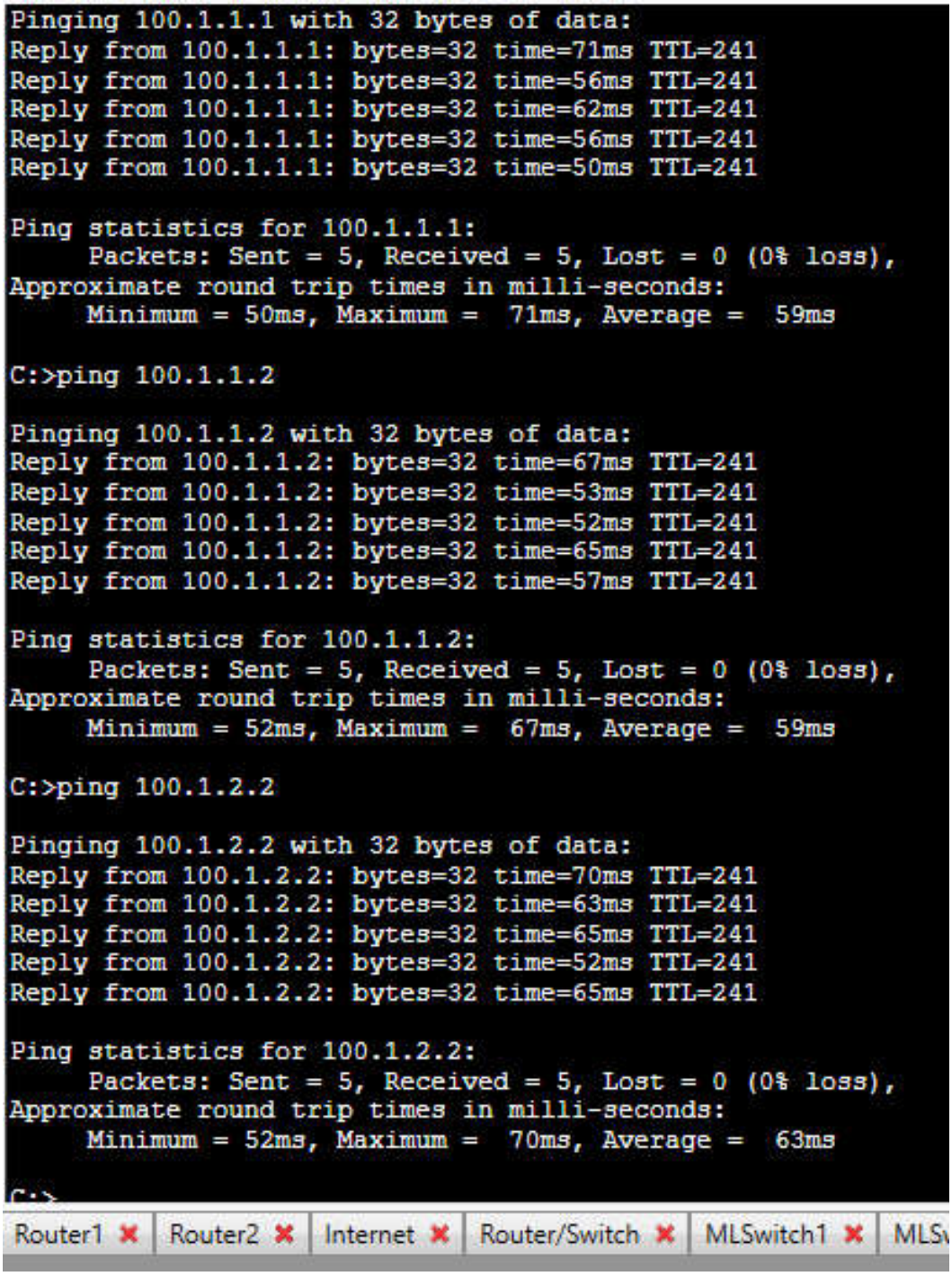


Figure 17 Pinging Internet router, R1, R2.

Pinging Router/Switch and both servers.

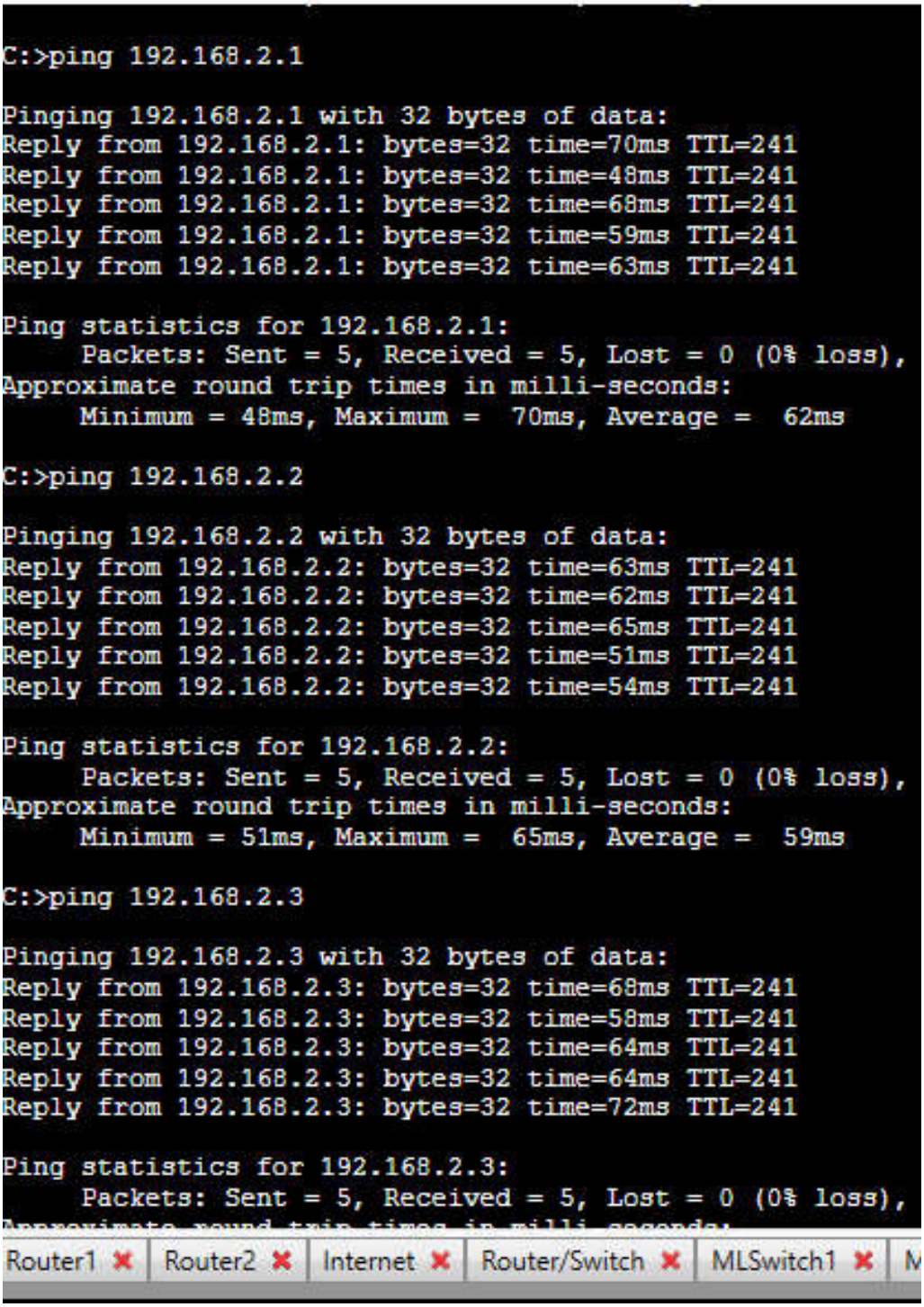


Figure 18 Testing

10.8 Connectivity

There is a feature of pinging all nodes from all nodes in Riverbed Modeler. Following graph was obtained as a result:

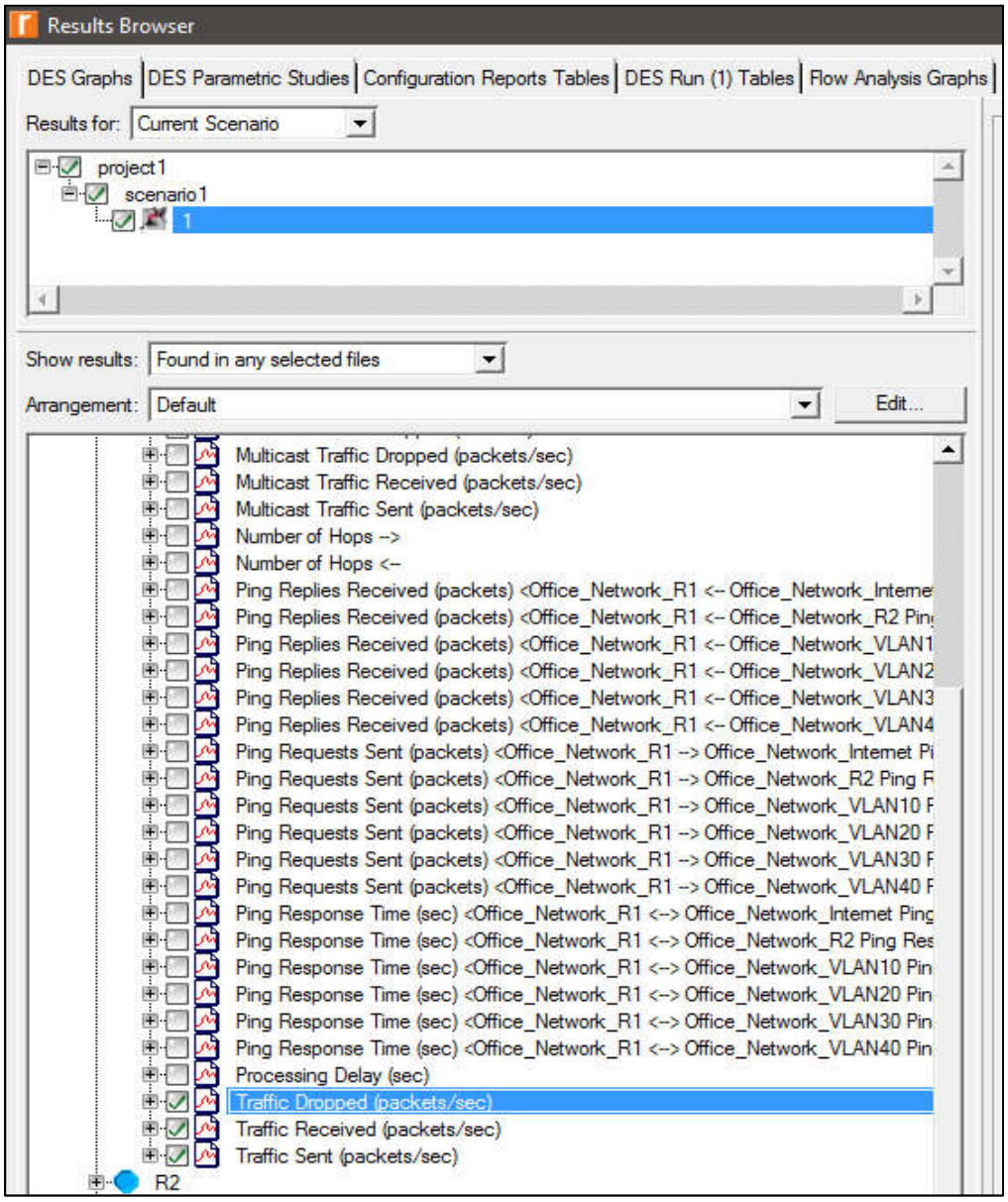


Figure 19 Connectivity

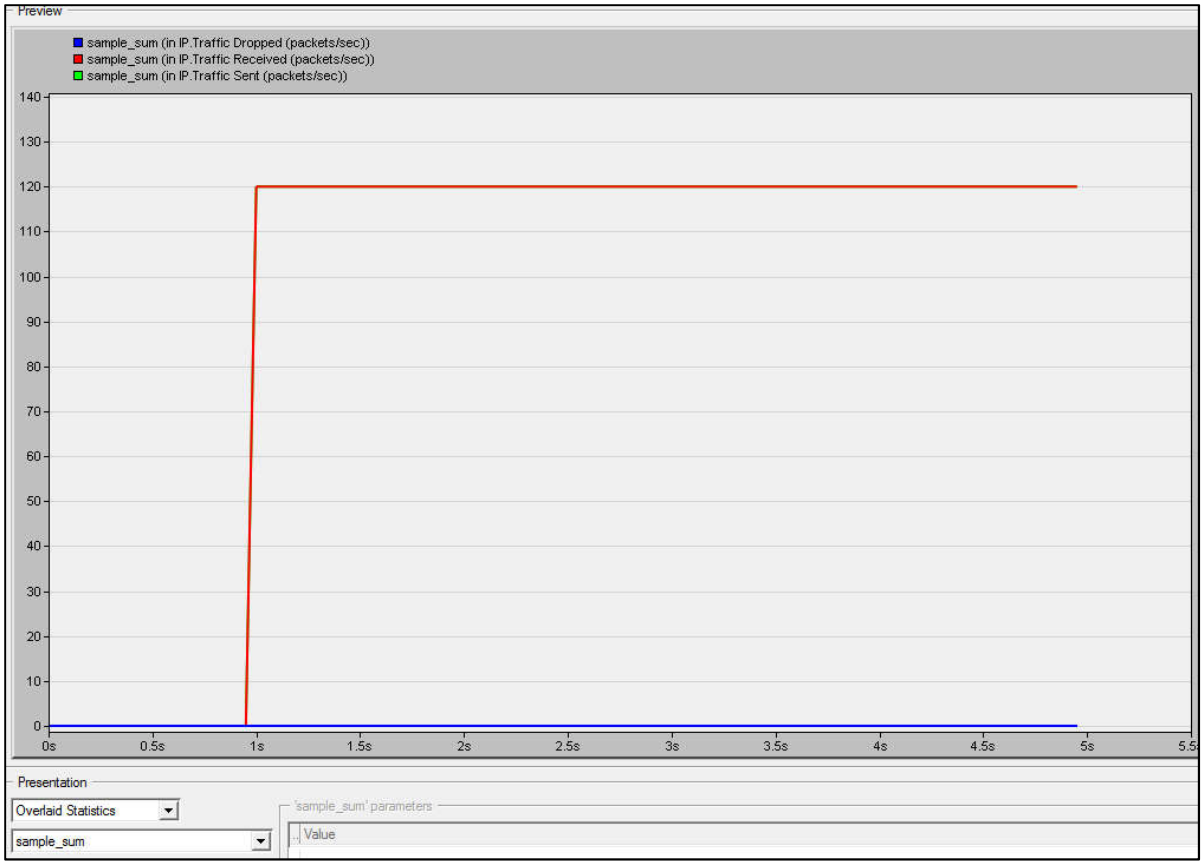


Figure 20 Preview

The top line shows the number of packets sent and received whereas the bottom blue line represents the number of packets lost which is 0. All devices are able to communicate with each other successfully and same graph was obtained from all devices.

11. Conclusion

In this report, we present the design and deployment of a secure network for airport. In this project we configured VLANs, Access and trunk ports, VTP, NAT, EIGRP routing protocol and DHCP on switches & provide screenshots and test connectivity in depth. The documentation & configuration are the part of project. The proposed system will provide enhanced security, scalability and high availability and will satisfy employees in better way.

12. References

[1] Ashraf H. Ali, ""Enterprise Network Design and Implementation for Airports" by Ashraf," 27 April 2016. [Online]. Available: https://scholar.valpo.edu/ms_ittheses/2/. [Accessed 5 May 2019].

[2] W. Staff, "DMZ - demilitarized zone," WEBOPEDIA, N.D N.D N.D. [Online]. Available: http://www.webopedia.com/TERM/D/DMZ.html. [Accessed 4 April 2019].

[3] Cisco, "Cisco 2951 Integrated Services Router," Cisco, N.D N.D N.D. [Online]. Available: http://www.cisco.com/c/en/us/products/routers/2951-integrated-services-router-isr/index.html. [Accessed 4 April 2019].

[4] Cisco, "Cisco Catalyst 2960X-48TS-L Switch," Cisco, N.D N.D N.D. [Online]. Available: http://www.cisco.com/c/en/us/support/switches/catalyst-2960x-48ts-l-switch/model.html. [Accessed 4 April 2019].

[5] Linksys, "LINKSYS EA9300 MAX-STREAM AC4000 TRI-BAND WI-FI ROUTER," Linksys, N.D N.D N.D. [Online]. Available: https://www.linksys.com/us/p/EA9300/. [Accessed 7 April 2019].