**Building and Securing a Small Network**

**Project 1**

**Team Members:**

|  |  |  |
| --- | --- | --- |
| Name | email | Student ID |
| Ahmed Ahmed Abdelhaleem elattar | Elattar.ahmedahmed@gmail.com |  |
| Ahmed Mohamed Mohamed Mostafa |  |  |
| Ibrahim Yasser Ibrahim |  |  |
| Mohamed Fetouh |  |  |

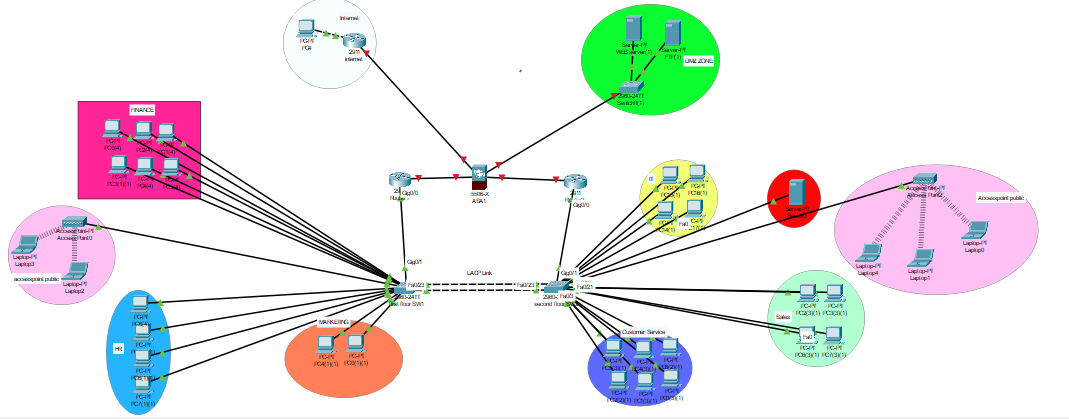
**Network Development Summary**

In this project, we designed and implemented a **secure and redundant network infrastructure** for a company with **two floors**, each housing different departments, including **HR, Finance, Marketing, Sales, Customer Service, and IT**. To ensure seamless wireless connectivity, **access points were deployed on each floor**.

The network includes **a web server and an FTP server**, accessible from the external network, and an **internal server**, which is restricted to internal access only. To achieve **high security and redundancy**, the following key components were implemented:

* **Inter-VLAN Routing:** Used to enable communication between different departments.
* **Redundancy:** Implemented using **two routers with HSRP**, ensuring load balancing by prioritizing certain VLANs on **Router 1** and others on **Router 2**. Additionally, **EtherChannel** was configured between the two switches for **high-speed connectivity and fault tolerance**.
* **Firewall Security:** A firewall was configured with **three security zones**:
  + **DMZ** (for public-facing services like web and FTP servers)
  + **Internal Network** (for company resources)
  + **Internet** (external access)
  + ACLs were used to **control access between zones** and **restrict unwanted services** in the DMZ.
* **Routing:** Implemented **OSPF** for efficient dynamic routing.
* **NAT:**
  + **Dynamic NAT** enabled internal devices to access the internet securely.
  + **Static NAT** ensured public accessibility for the **web and FTP servers**.
* **DHCP:** Used for **automatic IP assignment** to internal clients.
* **Layer 2 Security Enhancements:**
  + **Port Security** to prevent unauthorized device connections.
  + **DTP (switchport nonegotiate)** to disable unnecessary trunking.
  + **DHCP Snooping** to prevent rogue DHCP servers.
  + **Dynamic ARP Inspection (DAI)** to block ARP spoofing attacks.
  + **PortFast & BPDU Guard** to protect against spanning tree attacks.

This **network design ensures high availability, performance, and security**, meeting the company’s operational requirements while **protecting against potential threats**.



|  |  |  |  |
| --- | --- | --- | --- |
| Device | Interface | IP Address | Global IP |
| R1 | Gig0/0.10 | 192.168.10.2 | 209.165.200.226 |
| Gig0/0.20 | 192.168.20.2 |
| Gig0/0.30 | 192.168.30.2 |
| Gig0/0.40 | 192.168.40.2 |
| Gig0/0.50 | 192.168.50.2 |
| Gig0/0.60 | 192.168.60.2 |
| Gig0/0.70 | 192.168.70.2 |
| Gig0/0.80 | 192.168.80.2 |
| Gig0/0.90 | 192.168.90.2 |
| Gig0/0.99 | 192.168.99.1 |
| Gig0/1 | 10.1.2.2/30 |
| R2 | Gig0/0.10 | 192.168.10.3 |
| Gig0/0.20 | 192.168.20.3 |
| Gig0/0.30 | 192.168.30.3 |
| Gig0/0.40 | 192.168.40.3 |
| Gig0/0.50 | 192.168.50.3 |
| Gig0/0.60 | 192.168.60.3 |
| Gig0/0.70 | 192.168.70.3 |
| Gig0/0.80 | 192.168.80.3 |
| Gig0/0.90 | 192.168.90.3 |
| Gig0/0.99 | 192.168.99.2 |
| Gig0/1 | 10.1.1.2/30 |
| SW1 | Vlan 90 | 192.168.90.2 |
| SW2 | Vlan 90 | 192.168.90.3 |
| ASA Firewall | Gig1/1 | 10.1.2.1/30 |
| Gig1/2 | 10.1.1.1 255…252 |
| Gig1/3 | 192.168.100.1 |
| Gig1/4 | 209.165.200.226 255.255.255.248 |
| File Server |  | 192.168.80.4 | N/A |
| FTP Server |  | 192.168.100.2 | 209.165.200.228 |
| Web Server |  | 192.168.100.3 | 209.165.200.227 |

|  |  |  |  |
| --- | --- | --- | --- |
| VLan | Name | Network | Interface |
| 10 | Hr | 192.168.10.0/24 | SW1: fa0/1-5 |
| 20 | Finance | 192.168.20.0/24 | SW1: fa0/6-15 |
| 30 | Marketing | 192.168.30.0/24 | SW1: fa0/16-20 |
| 40 | Sales | 192.168.40.0/24 | SW2: fa0/1-5 |
| 50 | Customer service | 192.168.50.0/24 | SW2: fa0/6-15 |
| 60 | IT | 192.168.60.0/24 | SW2: fa0/16-19 |
| 70 | Access point | 192.168.70.0/24 | SW1: fa0/21 & SW2: fa0/21 |
| 80 | File server | 192.168.80.0/24 | SW2: fa0/20 |
| 90 | Management vlan | 192.168.90.0/24 | N/A |
| 99 | Native vlan | 192.168.99.0/24 | N/A |

ASA Firewall Enable Password = group$1

Configuration

///////////////////////////////////////////////On Sw1 & SW2//////////////////////////////////////////////

conf t

vlan 10

name HR

vlan 20

name Finance

vlan 30

name Marketing

vlan 40

name Sales

vlan 50

name CustomerService

vlan 60

name IT

vlan 70

name AccessPoint

vlan 80

name FileServer

vlan 90

name Manegment

vlan 99

name Native

/////////////////////////////////////////////////////On Sw1/////////////////////////////////////////////////

interface range fa0/1 - 5

switchport mode access

switchport access vlan 10

interface range fa0/6 - 15

switchport mode access

switchport access vlan 20

interface range fa0/16 - 20

switchport mode access

switchport access vlan 30

interface range fa0/21 - 22

switchport mode access

switchport access vlan 70

interface vlan 90

ip address 192.168.90.2 255.255.255.0

no shutdown

ip default-gateway 192.168.90.1

interface range gi0/1-2, fa0/23-24

switchport mode trunk

/////////////////////////////////////////////////////On Sw2/////////////////////////////////////////////////

interface range fa0/1 - 5

switchport mode access

switchport access vlan 40

interface range fa0/6 - 15

switchport mode access

switchport access vlan 50

interface range fa0/16 - 19

switchport mode access

switchport access vlan 60

interface fa0/20

switchport mode access

switchport access vlan 80

interface range fa0/21 - 22

switchport mode access

switchport access vlan 70

interface vlan 90

ip address 192.168.90.3 255.255.255.0

no shutdown

ip default-gateway 192.168.90.1

interface range gi0/1-2, fa0/23-24

switchport mode trunk

//////////////////////////////////////////////////On Router1 Intervlan//////////////////////////////////////

Ip routing

Interface GigabitEthernet0/0

No shutdown

interface GigabitEthernet0/0.99

encapsulation dot1Q 99 native

ip address 192.168.99.1 255.255.255.0

interface GigabitEthernet0/0.10

encapsulation dot1Q 10

ip address 192.168.10.2 255.255.255.0

standby 10 ip 192.168.10.1

standby 10 priority 110

standby 10 preempt

interface GigabitEthernet0/0.20

encapsulation dot1Q 20

ip address 192.168.20.2 255.255.255.0

standby 20 ip 192.168.20.1

standby 20 priority 110

standby 20 preempt

interface GigabitEthernet0/0.30

encapsulation dot1Q 30

ip address 192.168.30.2 255.255.255.0

standby 30 ip 192.168.30.1

standby 30 priority 110

standby 30 preempt

interface GigabitEthernet0/0.40

encapsulation dot1Q 40

ip address 192.168.40.2 255.255.255.0

standby 40 ip 192.168.30.1

standby 40 priority 90

standby 40 preempt

interface GigabitEthernet0/0.50

encapsulation dot1Q 50

ip address 192.168.50.2 255.255.255.0

standby 50 ip 192.168.50.1

standby 50 priority 90

standby 50 preempt

interface GigabitEthernet0/0.60

encapsulation dot1Q 60

ip address 192.168.60.2 255.255.255.0

standby 60 ip 192.168.60.1

standby 60 priority 90

standby 60 preempt

interface GigabitEthernet0/0.70

encapsulation dot1Q 70

ip address 192.168.70.2 255.255.255.0

standby 70 ip 192.168.70.1

standby 70 priority 110

standby 70 preempt

interface GigabitEthernet0/0.80

encapsulation dot1Q 80

ip address 192.168.80.2 255.255.255.0

standby 80 ip 192.168.80.1

standby 80 priority 90

standby 80 preempt

interface GigabitEthernet0/0.90

encapsulation dot1Q 90

ip address 192.168.60.2 255.255.255.0

standby 90 ip 192.168.90.1

standby 90 priority 110

standby 90 preempt

interface GigabitEthernet0/1

ip address 10.10.10.1 255.255.255.0

no shutdown

exit

interface GigabitEthernet0/2

ip address 10.10.20.1 255.255.255.0

no shutdown

exit

int range g0/1-2

ip address 10.1.2.2 255.255.255.252

no shutdown

exit

//////////////////////////////////////////On Router 2 intervlan ////////////////////////////////////////////

Ip routing

Interface GigabitEthernet0/0

No shutdown

interface GigabitEthernet0/0.99

encapsulation dot1Q 99 native

ip address 192.168.99.2 255.255.255.0

interface GigabitEthernet0/0.10

encapsulation dot1Q 10

ip address 192.168.10.3 255.255.255.0

standby 10 ip 192.168.10.1

standby 10 priority 90

standby 10 preempt

interface GigabitEthernet0/0.20

encapsulation dot1Q 20

ip address 192.168.20.3 255.255.255.0

standby 20 ip 192.168.20.1

standby 20 priority 90

standby 20 preempt

interface GigabitEthernet0/0.30

encapsulation dot1Q 30

ip address 192.168.30.3 255.255.255.0

standby 30 ip 192.168.30.1

standby 30 priority 90

standby 30 preempt

interface GigabitEthernet0/0.40

encapsulation dot1Q 40

ip address 192.168.40.3 255.255.255.0

standby 40 ip 192.168.30.1

standby 40 priority 110

standby 40 preempt

interface GigabitEthernet0/0.50

encapsulation dot1Q 50

ip address 192.168.50.3 255.255.255.0

standby 30 ip 192.168.50.1

standby 50 priority 110

standby 50 preempt

interface GigabitEthernet0/0.60

encapsulation dot1Q 60

ip address 192.168.60.3 255.255.255.0

standby 60 ip 192.168.60.1

standby 60 priority 110

standby 60 preempt

interface GigabitEthernet0/0.70

encapsulation dot1Q 70

ip address 192.168.70.3 255.255.255.0

standby 70 ip 192.168.70.1

standby 70 priority 90

standby 70 preempt

interface GigabitEthernet0/0.80

encapsulation dot1Q 80

ip address 192.168.80.3 255.255.255.0

standby 80 ip 192.168.80.1

standby 80 priority 110

standby 80 preempt

interface GigabitEthernet0/0.90

encapsulation dot1Q 90

ip address 192.168.60.3 255.255.255.0

standby 90 ip 192.168.90.1

standby 90 priority 90

standby 90 preempt

interface GigabitEthernet0/1

ip address 10.10.30.1 255.255.255.0

no shutdown

exit

interface GigabitEthernet0/2

ip address 10.10.20.2 255.255.255.0

no shutdown

exit

int range g0/1-2

ip address 10.1.1.2 255.255.255.252

no shutdown

exit

///////////////////////////SW1 ETHERCHANNEL///////////////////////////////////////////////////////////

Interface range fa0/23-24

Channel group 1 mode active

Exit

Interface port-channel 1

Switchport mode trunk

Switchport trunk allowed vlan 10,20,30,40,50,60,70,80,90,99

///////////////////////////SW2 ETHERCHANNEL///////////////////////////////////////////////////////////

Interface range fa0/23-24

Channel group 1 mode on

Exit

Interface port-channel 1

Switchport mode trunk

Switchport trunk allowed vlan 10,20,30,40,50,60,70,80,90,99

///////////////////////////ASA fIREWALL///////////////////////////////////////////////////////////////////

Conf t

Hostname TipoFirewall

Domain-name groupone.com

Enable password group$1

Clock set 02:42:00 8 feb 2025

Int g1/1

Nameif inside1

Security-level 100

Ip address 10.1.2.1 255.255.255.252

No sh

Int g1/2

Nameif inside

Security-level 100

Ip address 10.1.1.1 255.255.255.252

No sh

Int g1/3

Nameif dmz

Security-level 50

Ip address 192.168.100.1 255.255.255.0

No sh

Int g1/4

Nameif outside

Security-level 0

Ip address 209.165.200.226 255.255.255.248

No sh

Access-list outsideto-dmz permit icmp any host 192.168.100.3

Access-list outsideto-dmz permit tcp any host 192.168.100.3 eq 80

Access-list outsideto-dmz permit icmp any host 192.168.100.2

Access-list outsideto-dmz permit tcp any host 192.168.100.2 eq 20

Access-list outsideto-dmz permit tcp any host 192.168.100.2 eq 21

access-list outsideto-dmz extended permit icmp any any echo-reply

access-group outside-icmp in interface dmz

access-group outside-icmp in interface outside

Route Outside 0.0.0.0 0.0.0.0 209.165.200.225

router ospf 1

router-id 3.3.3.3

network 10.1.2.0 255.255.255.252 area 0

network 10.1.1.0 255.255.255.252 area 0

network 192.168.100.0 255.255.255.0 area 0

object network inside-nat

subnet 192.168.0.0 255.255.0.0

nat (inside,outside) dynamic interface

object network insideone-nat

subnet 192.168.0.0 255.255.0.0

nat (insideone,outside) dynamic interface

Object network WEB-SERVER

Host 192.168.100.3

Nat (DMZ,OUTSIDE) static 209.165.200.227

Exit

Object network FTP-SERVER

Host 192.168.100.2

Nat (DMZ,OUTSIDE) static 209.165.200.228

Exit

//////////////////////////////////////////Router 1 and Router 2////////////////////////////////////////////

R1

Int g0/1

Ip address 10.1.2.2 255.255.255.252

No sh

R2

Int g0/1

Ip address 10.1.1.2 255.255.255.252

No sh

ip dhcp excluded-address 192.168.10.1 192.168.10.3

ip dhcp excluded-address 192.168.20.1 192.168.20.3

ip dhcp excluded-address 192.168.30.1 192.168.30.3

ip dhcp excluded-address 192.168.40.1 192.168.40.3

ip dhcp excluded-address 192.168.50.1 192.168.50.3

ip dhcp excluded-address 192.168.60.1 192.168.60.3

ip dhcp excluded-address 192.168.70.1 192.168.70.3

ip dhcp pool HR

network 192.168.10.0 255.255.255.0

default-router 192.168.10.1

exit

ip dhcp pool FINANCE

network 192.168.20.0 255.255.255.0

default-router 192.168.20.1

exit

ip dhcp pool MARKETING

network 192.168.30.0 255.255.255.0

default-router 192.168.30.1

exit

ip dhcp pool SALES

network 192.168.40.0 255.255.255.0

default-router 192.168.40.1

exit

ip dhcp pool CUSTOMERSERVICE

network 192.168.50.0 255.255.255.0

default-router 192.168.50.1

exit

ip dhcp pool IT

network 192.168.60.0 255.255.255.0

default-router 192.168.60.1

exit

ip dhcp pool ACCESSPOINT

network 192.168.70.0 255.255.255.0

default-router 192.168.70.1

exit

///////////////////////////////////////OSPF configuration R1/////////////////////////////////////////////

Conf t

router ospf 1

Router-id 1.1.1.1

passive-interface GigabitEthernet0/0

network 192.168.10.0 0.0.0.255 area 0

network 192.168.20.0 0.0.0.255 area 0

network 192.168.30.0 0.0.0.255 area 0

network 192.168.40.0 0.0.0.255 area 0

network 192.168.50.0 0.0.0.255 area 0

network 192.168.60.0 0.0.0.255 area 0

network 192.168.70.0 0.0.0.255 area 0

network 192.168.80.0 0.0.0.255 area 0

network 192.168.90.0 0.0.0.255 area 0

network 192.168.99.0 0.0.0.255 area 0

! Advertise connection to ASA Firewall

network 10.1.2.0 0.0.0.3 area 0

exit

ip route 0.0.0.0 0.0.0.0 10.1.2.1

///////////////////////////////////////////////////OSPF configuration R2///////////////////////////////////

Conf t

router ospf 1

Router-id 2.2.2.2

passive-interface GigabitEthernet0/0

network 192.168.10.0 0.0.0.255 area 0

network 192.168.20.0 0.0.0.255 area 0

network 192.168.30.0 0.0.0.255 area 0

network 192.168.40.0 0.0.0.255 area 0

network 192.168.50.0 0.0.0.255 area 0

network 192.168.60.0 0.0.0.255 area 0

network 192.168.70.0 0.0.0.255 area 0

network 192.168.80.0 0.0.0.255 area 0

network 192.168.90.0 0.0.0.255 area 0

network 192.168.99.0 0.0.0.255 area 0

! Advertise connection to ASA Firewall

network 10.1.2.0 0.0.0.3 area 0

exit

ip route 0.0.0.0 0.0.0.0 10.1.1.1

///////////////////////////////////////////OSPF ASA Firewall////////////////////////////////////////////////

Conf t

Router ospf 1

Router-id 3.3.3.3

network 10.1.2.0 255.255.255.252 area 0

network 10.1.1.0 255.255.255.252 area 0

network 192.168.100.0 255.255.255.0 area 0

//////////////////////////////////////SW1 and SW2 Security////////////////////////////////////////////////

interface range fa0/1 – 20 , fa0/22 , gig0/2

switchport port-security

switchport port-security maximum 2

switchport port-security violation restrict

switchport port-security mac-address sticky

switchport port-security aging time 60

int range fa0/23-24 , fa0/22 , gig0/2

switchport nonegotiate

ip dhcp snooping

ip dhcp snooping vlan 10,20,30,40,50,60,70

interface range fa0/23-24 , gig0/1

ip dhcp snooping trust

exit

interface range fa0/1 – 20 , fa0/22

lp dhcp snooping limit rate 5

interface fa0/21

lp dhcp snooping limit rate 15

exit

Ip arp inspection validate src-mac dst-mac ip

ip arp inspection vlan 10,20,30,40,50,60,70

interface range fa0/23-24, gi0/1

ip arp inspection trust

show ip arp inspection interfaces

Spanning-tree portfast default

Spanning tree portfast bpduguard default

