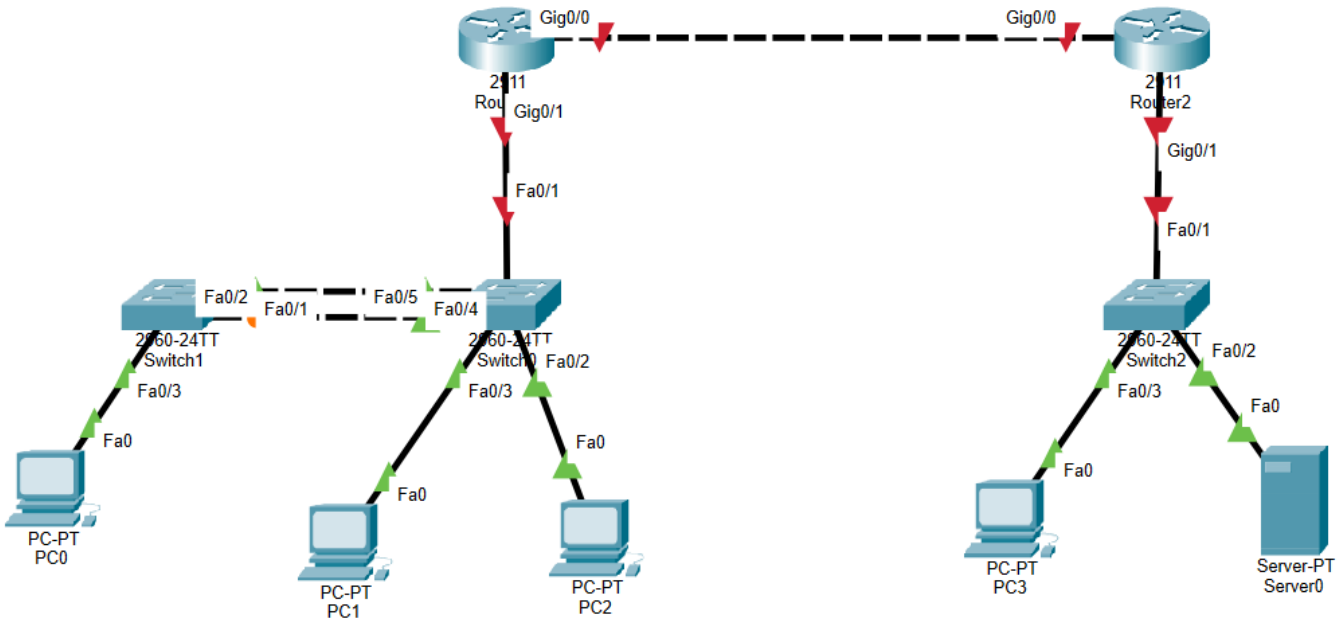
Final Lab Project (BCS-5A) **Dr Maryam Akbar**

Student Name: Kulsoom Khurshid **Student Reg # SP20-BCS-044**

Topology **Date: 1/07/2022**

Last Date of submission: 29/6/2022



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0/0	128.128.20.1	255.255.0.0	N/A
	G0/0/1	127.128.10.1	255.255.0.0	
R3	G0/0/0	128.128.20.2	255.255.0.0	N/A
	G0/0/1	127.128.30.1	255.255.0.0	
S1	VLAN 2 (CS Dept)			
S2	VLAN 3 (HR Dept)			
S3	VLAN 4 (Management)			

Assessment Objectives

Part 1: Initialize, Reload and Configure Basic Device Settings (*Using Class B IP scheme*) including VLans, VTP, Trunking & Etherchannel

Part 2: Configure Single Area OSPFv2

Part 3: Configure Access Control list, NAT, and perform configuration backup

Scenario

In this Skills Assessment (SA) you will configure the devices in a small network. You must configure a router, switch and PCs to support IPv4 connectivity for supported hosts. Your router and switch must also be managed securely. You will configure Single-Area OSPFv2, NAT, and access control lists.

Required Resources

- 2 Routers (Cisco 2911) & 3 Switches (Cisco 2960)
- 4 PCs & 1 Serve (Windows with a terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology
- Use public addresses between routers

Instructions

Part 1: Initialize, Reload and Configure Basic Device Settings

Step 1: Initialize and reload routers and switches.

Erase the startup configurations and VLANs from the router and switch and reload the devices.

Before proceeding.

In Routers 0 and 1, we write **erase start-config** and then **reload** command **in privilege mode** to erase the startup configurations from the routers and reload the devices.

In Switch 0,1 and 2 we write **erase start-config** and then **delete vlan.dat** to remove the VLANs and then **reload** command **in privilege mode** to erase the startup configurations from the switches and reload the devices.

Step 2: Configure the routers.

Configuration tasks for R1 and R3 include the following:

Task	Specification
Disable DNS lookup	Type **no ip domain-lookup** in configuration mode.
Router name with R1 & R3	Router0: **hostname R1** Router1: **hostname R3** in configuration mode.
Encrypted privileged EXEC password	In configuration mode : Type **enable password Ciscopass11**
Console access password	In configuration mode : Type **line console 0** **Password Ciscopass11** **login**
Create an administrative user in the local database	In configuration mode : Type **username admin password Cisco123**
Set login on VTY lines to use local database	In configuration mode : Type **line vty 0 4** **Login local** **Enable secret Cisco123**

Task	Specification
Set VTY lines to accept Telnet connections only	In privileged mode: **Type telnet 127.128.10.1 in R1** **Type telnet 127.128.30.1 in R3**
Encrypt the clear text passwords	In configuration mode : Type **service password-encryption**
Configure an MOTD Banner	In configuration mode : Type **banner motd # Welcome here!!! #**
Configure interface G0/0 for R1	In configuration mode : **Type int g0/0** **Ip add 127.128.10.1 255.255.0.0** **No shutdown**
Configure interface G0/1 for R1	In configuration mode : **Type int g0/0** **Ip add 128.128.20.1 255.255.0.0** **No shutdown**
Configure interface G0/0 for R3	In configuration mode : **Type int g0/0** **Ip add 128.128.20.2 255.255.0.0** **No shutdown**
Configure interface G0/1 for R1	In configuration mode : **Type int g0/0** **Ip add 127.128.30.1 255.255.0.0** **No shutdown**

Step 3: Configure S1, S2 and S3.

Configuration tasks for the switches include the following

Task	Specification
Disable DNS lookup	Type **no ip domain-lookup** in configuration mode.
Switch name must belong to its dept	In switch0 type **hostname Hr** and in switch1 type **hostname ComputerScience** in switch2 type **hostname Management** in configuration mode.
Encrypted privileged EXEC password	In configuration mode : Type **enable password Cisco1234**

Task	Specification
Console access password	In configuration mode : Type **line console 0** **Password Cisco1234** **login**
Shutdown all unused interfaces	In configuration mode : **Int range fa0/4-24** **Sh**
Create an administrative user in the local database	In configuration mode : Type **username admin password admin123**
Set login on VTY lines to use local database	In configuration mode : Type **line vty 0 4** **Login local** **Enable secret Cisco123**
Set VTY lines to accept Telnet connections only	In privileged mode: **Type telnet 127.128.10.5 in hr switch** **Type telnet 127.128.10.6 in computer science switch** **Type telnet 127.128.30.6 in management switch**
Encrypt the clear text passwords	In configuration mode : Type **service password-encryption**
Configure an MOTD Banner	In configuration mode : Type **banner motd # Welcome here!!! #**

Step4: Configure Network Infrastructure Settings (VLANs, Trunking, EtherChannel)

i) Configure S1 as Vtp Server.

In configuration mode :

Type vtp mode server

vtp domain cisco

vtp password 1234

Configuration tasks for S1 include the following:

Task	Specification
Create VLANs	In configuration mode : Type **VLAN 2, name CS** **VLAN 3, name HR** **VLAN 4, name Management** **VLAN 5, name Null**
Create 802.1Q trunks that use the native VLAN 1	In configuration mode : Type **Int fa0/1** **Switchport mode trunk** **ex** **Int fa0/3** **Switchport mode trunk** **ex** **Int fa0/2** **Switchport mode trunk** **ex**
Create a Layer 2 EtherChannel port group that uses interfaces F0/4 and F0/5	In configuration mode : Type **Int range fa0/3,fa0/2** **Sh** **Channel-group 2 mode desirable** **No sh** **ex** **Interface port-channel 2** **Switchport mode trunk** **ex**
Configure host access port for VLAN 2	In configuration mode : Type **Int fa0/5** **Switchport mode access** **Switchport access vlan 2**

Task	Specification
Secure all unused interfaces	In configuration mode : Type **Int range fa0/6-24** **Switchport mode access** **Switchport access vlan 5** **Sh** **Int range gig0/1-2** **Switchport mode access** **Switchport access vlan 5** **Sh**

ii) Configure S2 as VTP client.

In configuration mode :

Type vtp mode client

vtp domain cisco

vtp password 1234

Configuration tasks for S2 include the following:

Task	Specification
Create VLANs	In configuration mode : Type **VLAN 2, name CS** **VLAN 3, name HR** **VLAN 4, name Management** **VLAN 5, name Null**
Create 802.1Q trunks that use the native VLAN 1	In configuration mode : Type **Int fa0/1** **Switchport mode trunk** **ex** **Int fa0/2** **Switchport mode trunk** **ex**

Task	Specification
Create a Layer 2 Ether Channel port group that uses interfaces F0/1 and F0/2	In configuration mode : Type **Int range fa0/1,fa0/2** **Sh** **Channel-group 1 mode active** **No sh** **ex** **Interface port-channel 1** **Switchport mode trunk** **ex**
Configure host access port for VLAN 3	In configuration mode : Type **Int fa0/3** **Switchport mode access** **Switchport access vlan 3**
Secure all unused interfaces	In configuration mode : Type **Int range fa0/4-24** **Switchport mode access** **Switchport access vlan 5** **Sh** **Int range gig0/1-2** **Switchport mode access** **Switchport access vlan 5** **Sh**

ii) Configure S3.

Configuration tasks for S3 include the following:

Task	Specification
Create VLANs	In configuration mode : Type **VLAN 2, name CS** **VLAN 3, name HR** **VLAN 4, name Management** **VLAN 5, name Null**

Task	Specification
Create 802.1Q trunks that use the native VLAN 1	In configuration mode : Type **Int fa0/1** **Switchport mode trunk** **ex**
Configure host access port for VLAN 4	In configuration mode : Type **Int fa0/2** **Switchport mode access** **Switchport access vlan 4**
Secure all unused interfaces	In configuration mode : Type **Int range fa0/4-24** **Switchport mode access** **Switchport access vlan 5** **Sh** **Int range gig0/1-2** **Switchport mode access** **Switchport access vlan 5** **Sh**

Part 2: Configure Single Area OSPFv2

Configuration tasks for R1 and R3 include the following:

R1:
R1(config)#router ospf 1
R1(config-router)#network 128.128.20.0 0.0.0.3 area 0

R1(config-router)#network 127.128.10.0 0.0.0.255 area 0

R3:

R3(config)#router ospf 1
R3(config-router)#network 128.128.20.0 0.0.0.3 area 0
R3(config-router)#network 128.128.20.0 0.0.0.3 area 0

R3(config-router)#network 127.128.30.0 0.0.0.255 area 0

Task	Specification
Configure the OSPF routing process	Use process id 1

Task	Specification
Configure network statements	Configure a network statement for each locally attached network using a wild card mask that matches each network's subnet mask

Part 3: Configure Access Control List, NAT, and perform configuration backup

Step 1: Configure host computers.

Configure the host computers PC-A,PC-B,PC-C,PC-D with IPv4 addresses.

Description	PC-A	PC-B	PC-C	PC-D
IP Address	193.168.10.4	193.168.10.3	193.168.30.2	193.168.10.2
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Default Gateway	193.168.10.1	193.168.10.1	193.168.30.1	193.168.10.1

After configuring each host computer, perform the following tests:

Source	Target	Protocol	Expected Result
PC-A	PC-C	Ping	Success
PC-A	https:// (Web-server)	HTTPS	Success
PC-B	Switch1	Telnet	Success
PC-C	Router3	Telnet	Success

If you get different results, troubleshoot your OSPF and host configurations.

Step 2: Configure Access Control on R3.

Create and apply an access control list on R3 named **R3-SECURITY**to do the following:

Task	Specification
Create an access control list	**R3-SECURITY**
Control HTTP traffic	access-list 100 deny icmp host 192.168.10.4 host 192.168.30.4 access-list 100 deny tcp host 192.168.10.4 host 192.168.10.1 eq telnet
Permit traffic	access-list 100 permit icmp any any access-list 100 permit tcp any any
Apply the ACL	int gig0/1 ip access-group 100 out

After configuring and applying the ACL, perform the following tests:

Source	Target	Protocol	Expected Result
PC-A	PC-C	Ping	Success
PC-A	Web- Server	Ping	Failure
PC-A	https://	HTTPS	Success

Source	Target	Protocol	Expected Result
PC-A	Router1	Telnet	Failure
PC-D	Switch2	Telnet	Success

If you get different results, double check your ACL configuration and application.

Step 3: Configure NAT.

The decision has been made that the entire organization should be using addresses in the Class B network space. R1's LAN is out of compliance. There are applications and services running in the R1 LAN that cannot have their IP address changed without the entire system being rebuilt, so NAT is in order. Here are the configuration tasks at R1:

Task	Specification
Create an ACL to identify hosts allowed to be translated	In configuration mode : **Type int g0/0** **Ip add 172.168.10.1 255.255.0.0** **No shutdown** In configuration mode : **Type int g0/0** **Ip add 173.168.20.1 255.255.0.0** **No shutdown** In configuration mode : **Type int g0/0** **Ip add 173.168.20.2 255.255.0.0** **No shutdown** In configuration mode : **Type int g0/0** **Ip add 172.168.30.1 255.255.0.0** **No shutdown**
Configure Port Address Translation on the outside interface of R1	In Configuration mode : Type **Access-list 1 permit 172.168.10.0 0.0.255.255** **Ip nat inside source list 1 inteface gig0/1 overload**
Identify the interfaces involved in NAT	In Configuration mode : Type **Int gig0/1** **Ip nat outside** **Int gig0/0** **Ip nat inside**