كلية التقنية الالكترونية
طرابلس
College of Electronic Technology - Tripoli

" Communication Department "

Course Title : LAN Switching and Wireless

Case study : Network design for Rockford PLC

Prepared :Yassen Ahmed Aweli

recipient: Eng. Hider swaih

delivery date : 12 Jul 2018

Abstract

This report presents a network design project for the company Rockford PLC , by using the Cisco Packet Tracer v7.1 , this network consists of group local networks distributed in different location in Libya , All networks will use Link state Routing protocol (OSPF) to enable these local networks to communicate with each other. Also, default static route must be used to access the internet. a local network Tripoli is the main network has been divided into more than VLAN for several purposes, including the administration on the network by more security ,management and improve the performance of the network at the division broadcast domain, and will be used HSRP Protocol between Tripoli's routers to do one as active router and one as standby to achieve more availability . for test the connectivity give each device IP dynamically by using Janzur router as DHCP server, which divided the main network ID = 172.16.0.0/20 to size of each LAN Network and create pooling for each local network in DHCP server , for the security and management aspect of the network, Will be used Access control lists (ACLs) on the level (Layer3) .

- Contents List :

- Tables list :

1.Introduction

This case study allows students fully Design a complex network using skills gained throughout the course but build and configure only a prototype as seen in the following diagram .

Rockford PLC is a large company who specialize in the manufacture of several models of cars. The company has been actively new employees throughout the year. Rockford realises that to aggressively compete in its market, the company needs change to its infrastructure that will support new models of cars and Internet access, allowing them to increase their productivity and to follow market trends. Rockford wants to use the internet to gain clients and find new opportunities.

Network Requirements is broken into a number of phases, **as following :**

Phase 1: Addressing the WAN & LANs .

Phase 2: Basic Router and Switch Configuration .

Phase 3: Configuring Default Routes, OSPF Routing and HSRP.

Phase 4: Configure VLANs .

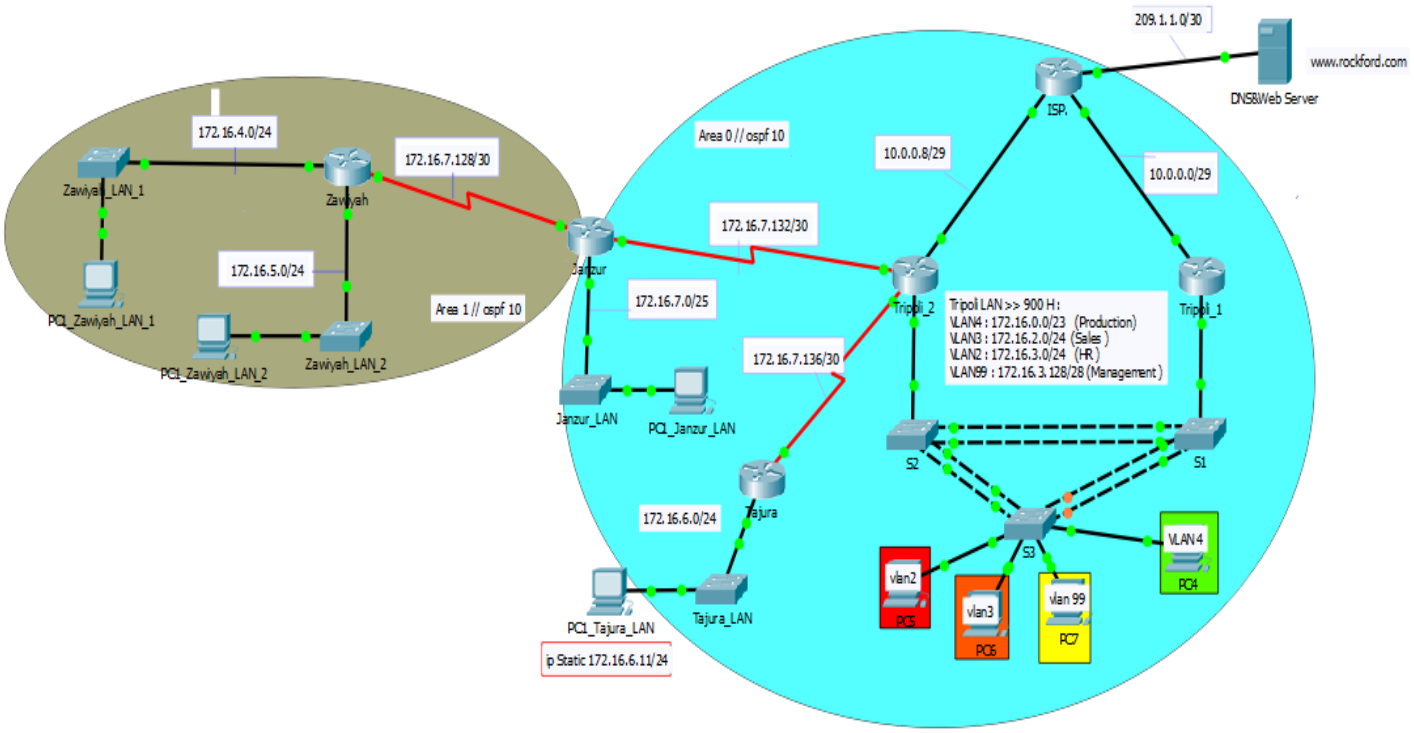
Phase 5: Configuring ACLs .

Phase 6: Configuring DHCP .

Phase 7: NAT .

Phase 8: Verification and Testing .

1.1 NETWORK TOPOLOGY :



Figure(1)

2.Methods :

2.1 phase 1 : Addressing the WAN & LANs :

2.1.1 the main address 172.16.0.0/20 sub-netting :

Table (1) (Addresses of routers)

Routers	Number of Hosts	Addresses
Tripoli_LANs	900 Hosts	N.ID : 172.16.0.0/22 S.M : 255.255.252.0 F.H : 172.16.0.1 /22 L.H : 172.16.3.254 /25 B.C : 172. 16.3.255 /25
Zawiyah_LAN_1	200 Hosts	N.ID : 172.16.4.0/24 S.M : 255.255.255.0 F.H : 172.16.4.1 /24 L.H : 172.16.4.254 /24 B.C : 172. 16.4.255 /24
Zawiyah_LAN_2	200 Hosts	N.ID : 172.16.5.0/24 S.M : 255.255.255.0 F.H : 172.16.5.1 /24 L.H : 172.16.5.254 /24 B.C : 172. 16.5.255 /24
Tajura_LAN	200 Hosts	N.ID : 172.16.6.0/24 S.M : 255.255.255.0 F.H : 172.16.6.1 /24 L.H : 172.16.6.254 /24 B.C : 172. 16.6.255 /24
Janzur_LAN	100 Hosts	N.ID : 172.16.7.0/25 S.M : 255.255.255.128 F.H : 172.16.7.1 /25 L.H : 172.16.7.126 /25 B.C : 172. 16.7.127 /25

*** NOTE :**

N.ID =Network ID ,F.H = First usable IP , L.H =Last usable IP , B.C = Broadcast IP , S.M = Subnet Mask .

2.1.2 Tripoli's VLANs :

Table (2) Addresses of VLANs

Routers	Number of Hosts	Addresses
VLAN 99 (Management)	10 Hosts	**N.ID : 172.16.3.144/28** **S.M : 255.255.255.240** **F.H : 172.16.3.145/28** **L.H : 172.16.3.158/28** **B.C : 172. 16.3.159/28**
VLAN 2 (HR)	120 Hosts	**N.ID : 172.16.3.0/25** **S.M : 255.255.255.128** **F.H : 172.16.3.1/25** **L.H : 172.16.3.126/25** **B.C : 172. 16.3.127/25**
VLAN 3 (Sales)	250 Hosts	**N.ID : 172.16.2.0/24** **S.M : 255.255.255.0** **F.H : 172.16.2.1 /24** **L.H : 172.16.2.254 /24** **B.C : 172. 16.2.255 /24**
VLAN 4 (production)	490 Hosts	**N.ID : 172.16.0.0/23** **S.M : 255.255.254.0** **F.H : 172.16.0.1 /23** **L.H : 172.16.1.254 /23** **B.C : 172. 16.1.255 /23**

2.1.3 Serial Links :

Table (3). Addresses of Serial Links

Link	Addresses
Zawiyah - Janzur	N.ID : 172.16.7.128/30 S.M : 255.255.255.252 F.H : 172.16.7.129 /30 L.H : 172.16.7.130 /30 B.C : 172. 16.7.131 /30
Janzur - Tripoli_2	N.ID : 172.16.7.132/30 S.M : 255.255.255.252 F.H : 172.16.7.133 /30 L.H : 172.16.7.134 /30 B.C : 172. 16.7.135 /30
Tripoli_2 - Tajura	N.ID : 172.16.7.136/30

S.M : 255.255.255.252
F.H : 172.16.7.137 /30
L.H : 172.16.7.138 /30
B.C : 172. 16.7.139 /30

2.2 phase 2 : Basic Router and Switch Configuration :

2.2.1 Basic Router Configuration :

- Zawiyah Router :

```
Router(config)#hostname Zawiyah
Zawiyah(config)#line consol 0
Zawiyah(config-line)#password cisco
Zawiyah(config-line)#login
Zawiyah(config-line)#exit
Zawiyah(config)#enable secret class
Zawiyah(config)#banner motd # Authorized Access Only#
Zawiyah(config)#service password-encryption
Zawiyah(config)#ip domain-name cisco.com
Zawiyah(config)# crypto key generate rsa

How many bits in the modulus [512]: 1024
Zawiyah(config)#username admin secret cisco
Zawiyah(config)#line vty 0 4
Zawiyah(config-line)#login local
Zawiyah(config-line)#exit
Zawiyah(config)#ip ssh version 2

Zawiyah(config)#interface serial 0/0/0
Zawiyah(config-if)#ip address 172.16.7.129 255.255.255.252
Zawiyah(config-if)#no shutdown
Zawiyah(config-if)#description Link to Janzur
Zawiyah(config-if)#exit
Zawiyah(config)#interface gigabitEthernet 0/1
Zawiyah(config-if)#ip address 172.16.4.1 255.255.255.0
Zawiyah(config-if)#no shutdown
Zawiyah(config-if)#description Link to Zawiyah LAN_1
Zawiyah(config-if)#exit
Zawiyah(config)#interface gigabitEthernet 0/0
Zawiyah(config-if)#ip address 172.16.5.1 255.255.255.0
Zawiyah(config-if)#no shutdown
Zawiyah(config-if)#description Link to Zawiyah LAN_2
```

NOTE : all another routers are configured by the same commands , but the difference between them is in misleading orders in blue, and Table (4) shows a summary of the different configuration of the rest of the routers .

Table (4). Summary of the configuration for another routers

Router name	Hostname	IPs of Interfaces	Description of interfaces
Janzur	Janzur	Se0/0/0 : 172.16.7.130/30 Se0/0/1 : 172.16.7.133/30	Se0/0/0 : Link to Zawiyah Se0/0/1 : Link to Tripoli_2 Gig0/0 : Link to Janzur LAN
Tajura	Tajura	Se0/0/0 : 172.16.7.138/30 Gig0/0 : 172.16.6.1/24	Se0/0/0 : Link to Tripoli_2 Gig0/0 : Link to Tajura LAN
Tripoli_2	Tripoli_2	Se0/0/0 : 172.16.7.134/30 Se0/0/1 : 172.16.7.137/30 Gig0/0 : 10.0.0.10/29	Se0/0/0 : Link to Janzur Se0/0/1 : Link to Tajura Gig0/0 : Link to ISP
Tripoli_1	Tripoli_1	Gig0/0 : 10.0.0.1/29	Gig0/0 : Link to ISP
ISP	ISP	Gig0/0 : 10.0.0.2/29 Gig0/1 : 10.0.0.9/29 Gig0/2 : 209.1.1.1/30	Gig0/0 : Link to Tripoli_1 Gig0/1 : Link to Tripoli_2 Gig0/2 : Link to DNS&Web Server

2.2.2 Basic Switch Configuration :

```
Switch(config)#hostname Tajura_LAN
Tajura_LAN(config)#line consol 0
Tajura_LAN(config-line)#password cisco
Tajura_LAN(config-line)#login
Tajura_LAN(config-line)#exit
Tajura_LAN(config)#enable secret class
Tajura_LAN(config)#banner motd # Authorized Access Only#
Tajura_LAN(config)#service password-encryption
Tajura_LAN(config)#ip domain-name cisco.com
Tajura_LAN(config)#crypto key generate rsa
How many bits in the modulus [512]: 1024
Tajura_LAN(config)#username admin secret cisco
Tajura_LAN(config)#line vty 0 4
Tajura_LAN(config-line)#login local
Tajura_LAN(config-line)#exit
Tajura_LAN(config)#ip ssh version 2
Tajura_LAN(config)#INTerface gigabitEthernet 0/1
Tajura_LAN(config-if)#description Link to Tajura
```

NOTE : all another switches are configured by the same commands , but the difference between them is in misleading orders in blue, and Table (5) shows a summary of the different configuration of the rest of the switches.

NOTE : also configure ip to vlan management in all switches , and the default getaway in global configuration . **as shown in table (9) in appendices .**

Table (5). Summary of the configuration for another switches

Switch name	Hostname	Description of interfaces
Zawiyah	Zawiyah_LAN_1	Gig0/1 : Link to Zawiyah
Zawiyah	Zawiyah_LAN_2	Gig0/1 : Link to Zawiyah
Janzur_LAN	Janzur_LAN	Gig0/1 : Link to Janzur
Tajura_LAN	Tajura_LAN	Gig0/1 : Link to Tajura
ISP	ISP	Gig0/0 : Link to Tripoli_1 Gig0/1 : Link to Tripoli_2 Gig0/2 : Link to DNS&Web Server

2.3. phase 3 : Configuring Default Routes , OSPF Routing and HSRP :

2.3.1 Configure Multi-area OSPF on Routers (Zawiyah, Janzur, Tajura, and Tripoli) a summary (type 3) for area 1.

```
Zawiyah(config)#router ospf 10
Zawiyah(config-router)#router-id 1.1.1.1
Zawiyah(config-router)#network 172.16.4.0 0.0.1.255 area 1
Zawiyah(config-router)#network 172.16.7.128 0.0.0.3 area 1

Zawiyah(config-router)#passive-interface gigabitEthernet 0/0
Zawiyah(config-router)#passive-interface gigabitEthernet 0/1
```

Manual Summarization between two networks:

172.16.4.0/24

172.16.5.0/24

```
Tripoli_2(config)#router ospf 10
Tripoli_2(config-router)#router-id 4.4.4.4
Tripoli_2(config-router)#network 172.16.0.0 0.0.3.255 area 0
Tripoli_2(config-router)#network 172.16.7.132 0.0.0.3 area 0
Tripoli_2(config-router)#network 172.16.7.136 0.0.0.3 area 0
Tripoli_2(config-router)#passive-interface gigabitEthernet 0/1
Tripoli_2(config-router)#passive-interface gigabitEthernet 0/0
Tripoli_2(config-router)#default-information originate
```

To redistribute the default route into the OSPF process.

```
Tripoli_1(config)#router ospf 10
Tripoli_1(config-router)#router-id 5.5.5.5
Tripoli_1(config-router)# network 172.16.0.0 0.0.3.255 area 0
Tripoli_1(config-router)#passive-interface gigabitEthernet 0/1
Tripoli_1(config-router)#passive-interface gigabitEthernet 0/0
Tripoli_1(config-router)#default-information originate
Tripoli_2(config-router)#default-information originate
```

Table (6) shows a summary of the ospf configuration on another routers.

commands	Janzur	Tajura
Process ID	10	10
router-id	2.2.2.2	3.3.3.3
networks	172.16.7.0/25 area 0 172.16.7.132/30 area 0 172.16.7.128/30 area 1	172.16.6.0/24 area 0 172.16.7.136/30 area 0
passive interfaces	Gig0/0	Gig0/0
OSPF Route Summarization	**area 1 range 172.16.4.0 255.255.252.0** **area 0 range 172.16.0.0 255.255.248.0**	N/A

Summarization all network on area 0 & area 1

- Configure **MD5** authentication between OSPF routers across all WAN links ,and Adjust the Hello timer to **40 sec** and Dead timers to **160 sec** on the link between Janzur and Zawiyah .

```
Zawiyah(config)#interface serial 0/0/0
Zawiyah(config-if)#ip ospf authentication message-digest
Zawiyah(config-if)#ip ospf message-digest-key 1 md5 cisco
Janzur(config)#interface serial 0/0/0
Janzur(config-if)#ip ospf authentication message-digest
Janzur(config-if)#Zawiyah(config-if)#ip ospf message-digest-key 1 md5 cisco
```

```
Zawiyah(config)#interface serial 0/0/0
Zawiyah(config-if)#ip ospf hello-interval 40
Zawiyah(config-if)#ip ospf dead-interval 160
          ==========  ============
Janzur(config)#interface serial 0/0/0
Janzur(config-if)#ip ospf hello-interval 40
Janzur(config-if)#ip ospf dead-interval 160
```

-Static routing :

```
ISP(config)#ip route 200.10.10.64 255.255.255.192 10.0.0.10
ISP(config)#ip route 200.10.10.64 255.255.255.192 10.0.0.1

ISP(config)#ip route 209.1.1.2 255.255.255.255 GigabitEthernet0/2

Tripoli_2(config)#ip route 0.0.0.0 0.0.0.0 10.0.0.9

Tripoli_1(config)#ip route 0.0.0.0 0.0.0.0 10.0.0.2
```

****NOTE**** : **in misleading orders in blue, was used Public network for routing because it is more secure than default route .**

2.3.2 HSRP :

```
Tripoli_2(config)#interface gigabitEthernet 0/1.2
Tripoli_2(config-subif)#encapsulation dot1Q 2
Tripoli_2(config-subif)#ip address 172.16.3.3 255.255.255.128
Tripoli_2(config-subif)#standby 1 ip 172.16.3.1
Tripoli_2(config-subif)#standby  1 preempt
```

```
Tripoli_2(config)#interface gigabitEthernet 0/1.3
Tripoli_2(config-subif)#encapsulation dot1Q 3
Tripoli_2(config-subif)#ip address 172.16.2.3 255.255.255.0
Tripoli_2(config-subif)#standby 2 ip 172.16.2.1
Tripoli_2(config-subif)#standby 2 preempt
```

```
Tripoli_1(config)#interface gigabitEthernet 0/1.99
Tripoli_1(config-subif)#encapsulation dot1Q 99
Tripoli_1(config-subif)#ip address 172.16.3.130 255.255.255.240
Tripoli_1(config-subif)#standby 4 ip 172.16.3.129
Tripoli_1(config-subif)#standby  4  preempt
Tripoli_1(config-subif)#standby 4  priority 50
```

NOTE : priority configured on Tripoli_1 =50 , and by default The priority of Tripoli_2 router =100 , then Tripoli_2 will be active router & Tripoli_1 standby router .

Table (7) shows a summary of the HSRP configuration on another interfaces.

configuration of Tripoli_2	gigabitEthernet 0/1.4	GigabitEthernet 0/1.99
encapsulation dot1Q ….	4	99
ip address	172.16.0.3/23	172.16.3.131/28
standby group number	3	4
standby ip	172.16.0.1/23	172.16.3.129/28
preempt	YES	**YES**

NOTE : configure HSRP on the Tripoli_1 by the same way with different IPs .

2.4. Phase 4 : Configure VLANs .

2.4.1 . Apply the switch configuration as follows:

- STP (PVST +) - VTP Server (S1) -VTP Client (S2,S3)

```
S1(config)#spanning-tree mode pvst

S1(config)#vtp domain cisco
S1(config)#vtp password cisco
```

S1 : Vtp mode is server by default

```
S2(config)#spanning-tree mode pvst

S2(config)#vtp mode client
S2(config)#vtp domain cisco
S2(config)#vtp password cisco
```

```
S3(config)#spanning-tree mode pvst

S3(config)#vtp mode client
S3(config)#vtp domain cisco
S3(config)#vtp password cisco
```

2.4.2. Configure the Tripoli's LAN (2 routers and 3 switches) as follows:

Create and name three Data VLANs and one Management VLAN
– VLAN 99: Management
– VLAN 100: Native
– VLAN 2: HR
– VLAN 3: Sales
– VLAN 4: Production.

```
S1(config)#vlan 99
S1(config-vlan)#name
S1(config-vlan)#name Management
S1(config-vlan)#exit
S1(config)#vlan 100
S1(config-vlan)#name Native
S1(config-vlan)#exit
S1(config)#vlan 2
S1(config-vlan)#name HR
S1(config-vlan)#exit
S1(config)#vlan 3
S1(config-vlan)#name Sales
S1(config-vlan)#exit
S1(config)#vlan 4
S1(config-vlan)#name Production
```

- Configure switches S1, S2 and S3; assign:
- FastEthernet ports 1-4 & Gig0/1as trunks (802.1Q).
- Configure Etherchannel when appropriate.

```
S2(config)#interface range fastEthernet 0/1-4 , gigabitEthernet 0/1
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#switchport trunk allowed vlan 2,3,4,99,100
S2(config-if-range)#switchport trunk native vlan 100
```

```
S2(config)#interface range fastEthernet 0/1-2
S2(config-if-range)# channel-protocol lacp
S2(config-if-range)#channel-group 1 mode active
S2(config-if-range)#exit
S2(config)#interface range fastEthernet 0/3-4
S2(config-if-range)# channel-protocol lacp
S2(config-if-range)#channel-group 2 mode active
S2(config-if-range)#exit
```

NOTE: S1&S2 switches are configured by the same commands , but the difference between them is in misleading orders in blue, and Table (8) shows a summary of the different configuration of the rest of the switches.

Table (8) shows a summary of the Etherchannel configuration on another interfaces.

Switches	interfaces	channel-group
S1	fastEthernet 0/1-2	1
	fastEthernet 0/3-4	3
S3	fastEthernet 0/1-2	3
	fastEthernet 0/3-4	2

2.3.3 Configure access layer switch S3; assign:

- Port 6 to VLAN 99
- Ports 7-10 to VLAN 2
- Ports 11-14 to VLAN 3
- Ports 14-20 to VLAN 4
- Disable all unused ports and put them in Garbage VLAN.

```
S3(config)#interface fastEthernet 0/6
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 99
S3(config)#interface range fastEthernet 0/7-10
S3(config-if-range)#switchport mode access
S3(config-if-range)#switchport access vlan 2
S3(config)#interface range fastEthernet 0/11-14
S3(config-if-range)#switchport mode access
S3(config-if-range)#switchport access vlan 3
S3(config)#interface range fastEthernet 0/14-20
S3(config-if-range)#switchport mode access
S3(config-if-range)#switchport access vlan 4

S1(config)#vlan 20
S1(config-vlan)#name Garbage_VLAN

S3(config)#interface range fastEthernet 0/21-24 , gigabitEthernet 0/1-2
S3(config-if-range)#switchport access vlan 20
S3(config-if-range)#shutdown
```

Create Garbage vlan in the S1 (Server)

NOTE : all another switches configured by the same commands ,

2.5. Phase 5: Configuring ACLs.

2.5.1. Configure a Standard ACL to filter traffic.
The ACL should:
- Deny only the Zawiyah LANs access to VLAN 3 (Sales), permit all others .

```
Tripoli_2(config)#access-list 1 deny 172.16.4.0 0.0.1.255

Tripoli_2(config)#access-list 1 permit any

Tripoli_2(config)#interface gigabitEthernet 0/1.3
Tripoli_2(config-subif)#ip access-group 1 out
```

summarization

2.5.2. Configure a Named Standard ACL to filter traffic. The ACL should:
Permit the HR (VLAN 2) and Janzur LAN users to access the Tajora LAN, deny all others.

```
Tajura (config)#ip access-list standard (HR&Janzur_LANs)_to_access
Tajura (config-std-nacl)#permit 172.16.3.0 0.0.0.127
Tajura (config-std-nacl)#permit 172.16.7.0 0.0.0.127
Tajura (config-std-nacl)#deny any
Tajura (config-std-nacl)#exit
Tajura (config)#interface Gig0/0
Tajura (config-if)#ip access-group (HR&Janzur_LANs)_to_access out
```

2.5.3. Use an ACL to control SSH access to all routers. The ACL should:
Allow SSH session to all routers from the Management VLAN (VLAN99) only; SSH sessions from all other networks should be denied.

```
Zawiyah(config)#ip access-list extended SSH_Session
Zawiyah(config-ext-nacl)#permit tcp 172.16.3.128 0.0.0.15 any eq 22
Zawiyah(config-ext-nacl)#deny tcp any any eq 22
Zawiyah(config-ext-nacl)#permit ip any any

Zawiyah(config)#interface range gigabitEthernet 0/0-1
Zawiyah(config-if-range)#ip access-group SSH_Session in
Zawiyah(config)#interface serial 0/0/0

Zawiyah(config-if)#ip access-group SSH_Session in
Zawiyah(config-if)#exit
```

NOTE :configure this ACL on all routers, and activated on all interfaces in the router .

2.6. Phase 6: Configuring DHCP

DHCP Services DHCP should provide services to the following LANs hosts:

– Tripoli's VLAN 2, VLAN 3 and VLAN 4

– Janzur's LAN

– Zawiyah's LANs

DHCP should pass the following parameters to the hosts:
– IP address and Subnet Mask
– Default Gateway
– DNS address (209.1.1.2)
The Janzur router will perform the DHCP services. Configure Janzur using the DHCP pools documented in Phase 1.

Configure DHCP services on the Janzur router as follows:
– Exclude the first 10 IP addresses from each pool (to be used for printers, servers, and so on) .

```
Janzur(config)#ip dhcp excluded-address 172.16.0.1 172.16.0.10
Janzur(config)#ip dhcp excluded-address 172.16.2.1 172.16.2.10
Janzur(config)#ip dhcp excluded-address 172.16.3.1 172.16.3.10
Janzur(config)#ip dhcp excluded-address 172.16.4.1 172.16.4.10
Janzur(config)#ip dhcp excluded-address 172.16.5.1 172.16.5.10
Janzur(config)#ip dhcp excluded-address 172.16.7.1 172.16.7.10
```

```
Janzur(config)#ip dhcp pool Zawiyah_LAN_1
Janzur(dhcp-config)#network 172.16.4.0 255.255.255.0
Janzur(dhcp-config)#default-router 172.16.4.1
Janzur(dhcp-config)#dns-server 209.1.1.2
```

```
Janzur(config)#ip dhcp pool Zawiyah_LAN_2
Janzur(dhcp-config)#network 172.16.5.0 255.255.255.0
Janzur(dhcp-config)#default-router 172.16.5.1
Janzur(dhcp-config)#dns-server 209.1.1.2
```

```
Janzur(config)#ip dhcp pool Janzur
 Janzur(dhcp-config)#network 172.16.7.0 255.255.255.128
Janzur(dhcp-config)#default-router 172.16.7.1
Janzur(dhcp-config)#dns-server 209.1.1.2
```

```
Janzur(config)#ip dhcp pool Production_LAN
Janzur(dhcp-config)#network 172.16.0.0 255.255.254.0
Janzur(dhcp-config)#default-router 172.16.0.1
Janzur(dhcp-config)#dns-server 209.1.1.2
```

```
Tripoli_2(config)#interface gigabitEthernet 0/1.99
Tripoli_2(config-subif)#ip helper-address 172.16.7.133
Tripoli_2(config-subif)#exit
```

```
Zawiyah(config)#interface gigabitEthernet 0/0
Zawiyah(config-if)#ip helper-address 172.16.7.130

Zawiyah(config)#interface gigabitEthernet 0/1
Zawiyah(config-if)#ip helper-address 172.16.7.130
```

```
Tripoli_2(config)#interface range gigabitEthernet 0/1.2 , gigabitEthernet 0/1.3 ,
gigabitEthernet 0/1.4 , gigabitEthernet 0/1.99 , gigabitEthernet 0/1.100
Tripoli_2(config-subif)#ip helper-address 172.16.7.133
Tripoli_2(config-subif)#exit
```

NOTE : used IP helper command to the router interfaces , to be able to forward the packet (Broadcast) for all LANs needs IP from DHCP server.

2.7. Phase 7: NAT :

2.7.1 The Tripoli's (2) routers will perform NAT. Configure the routers as follows:

- Define the NAT pool. The pool consists of public network address 200.10.10.64/26. Exclude first 10 addresses from this pool (to be use for servers, when required).
- Define an access control list, which will translate for all internal (172.16.0.0/20) addresses, and deny all other traffic.

Establish dynamic source translation, specifying the NAT pool and the ACL defined in the previous steps.

Specify the inside and the outside NAT interfaces.

```
Tripoli_1(config)#ip nat pool Public_IP 200.10.10.74 200.10.10.126 netmask 255.255.255.192
Tripoli_1(config)#ip access-list standard NAT
Tripoli_1(config-std-nacl)# permit 172.16.0.0 0.0.15.255
Tripoli_1(config-std-nacl)# deny any

Tripoli_1(config)#ip nat inside source list NAT pool Public_IP

Tripoli_1(config-if)#interface gigabitEthernet 0/0
Tripoli_1(config-if)#ip nat outside
Tripoli_1(config-if)#exit
Tripoli_1(config)#interface range gigabitEthernet 0/1.2 , gigabitEthernet 0/1.3 , gigabitEthernet 0/1.4 ,
gigabitEthernet 0/1.99 , gigabitEthernet 0/1.100
Tripoli_1(config-if-range)#ip nat inside
```

```
Tripoli_2(config)#ip nat pool Public_IP 200.10.10.74 200.10.10.126 netmask 255.255.255.192
Tripoli_2(config)#ip access-list standard NAT
Tripoli_2(config-std-nacl)# permit 172.16.0.0 0.0.15.255
Tripoli_2(config-std-nacl)# deny any

Tripoli_2(config)#ip nat inside source list NAT pool Public_IP

Tripoli_2(config-if)#interface  se 0/0/0
Tripoli_2(config-if)#ip nat inside
Tripoli_2(config-if)#exit

Tripoli_2(config-if)#interface  se 0/0/1
Tripoli_2(config-if)#ip nat inside
Tripoli_2(config-if)#exit

Tripoli_2(config-if)#interface gigabitEthernet 0/0
Tripoli_2(config-if)#ip nat outside
Tripoli_2(config-if)#exit
Tripoli_2(config)#interface range gigabitEthernet 0/1.2 , gigabitEthernet 0/1.3 , gigabitEthernet 0/1.4 ,
gigabitEthernet 0/1.99 , gigabitEthernet 0/1.100
Tripoli_1(config-if-range)#ip nat inside
```

2.7.2 . Connect a Server to the ISP's G0/0 port to simulate an ISP server. Configure this Server as follows:
– Configure the IP address and subnet mask as 209.1.1.2/30.
– Configure the default gateway to be 209.1.1.1.

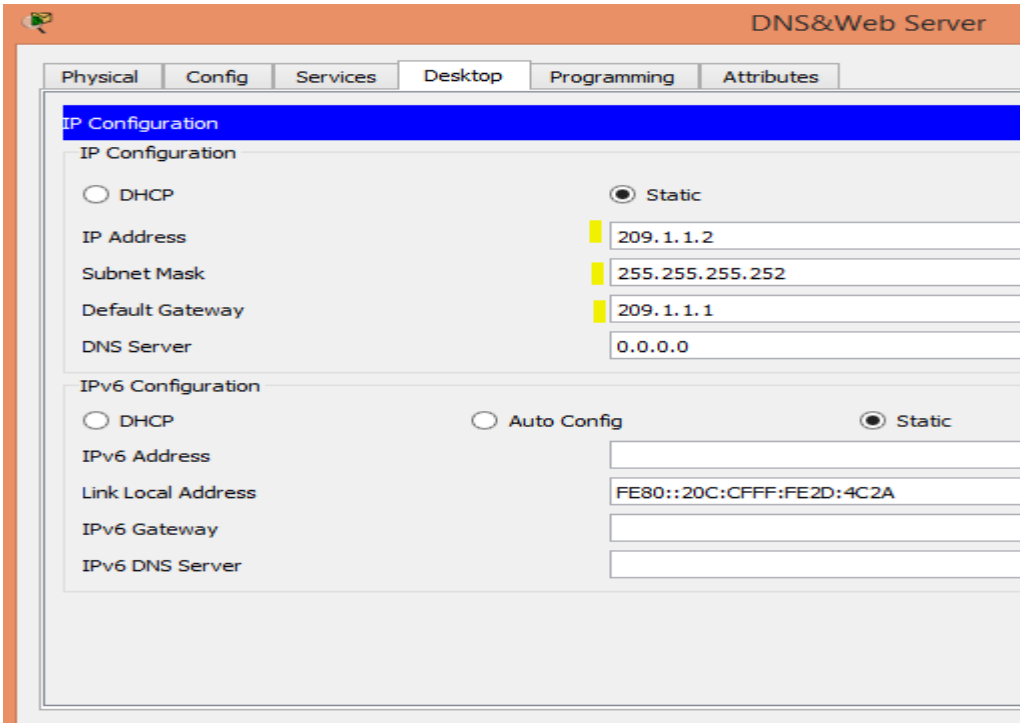


Figure (2)

2.7.3. Configure the server to act as a web server. Enable a simple web page (www. rockford.com) that will tell users that they have reached the ISP.

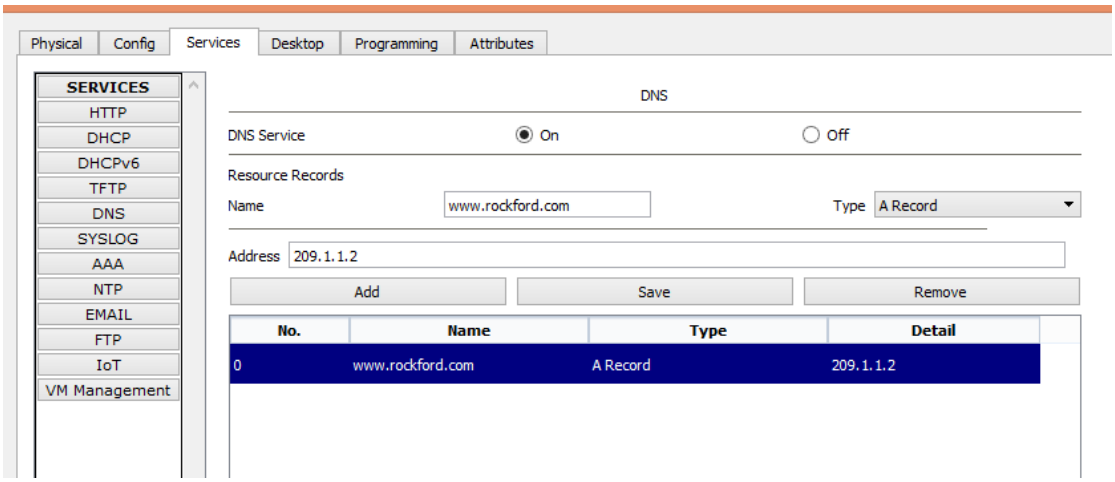


Figure (3)

2.8 .Verification and Testing .

- Test remotely access from VLAN99(management) to Zawiyah router…. (ssh) :

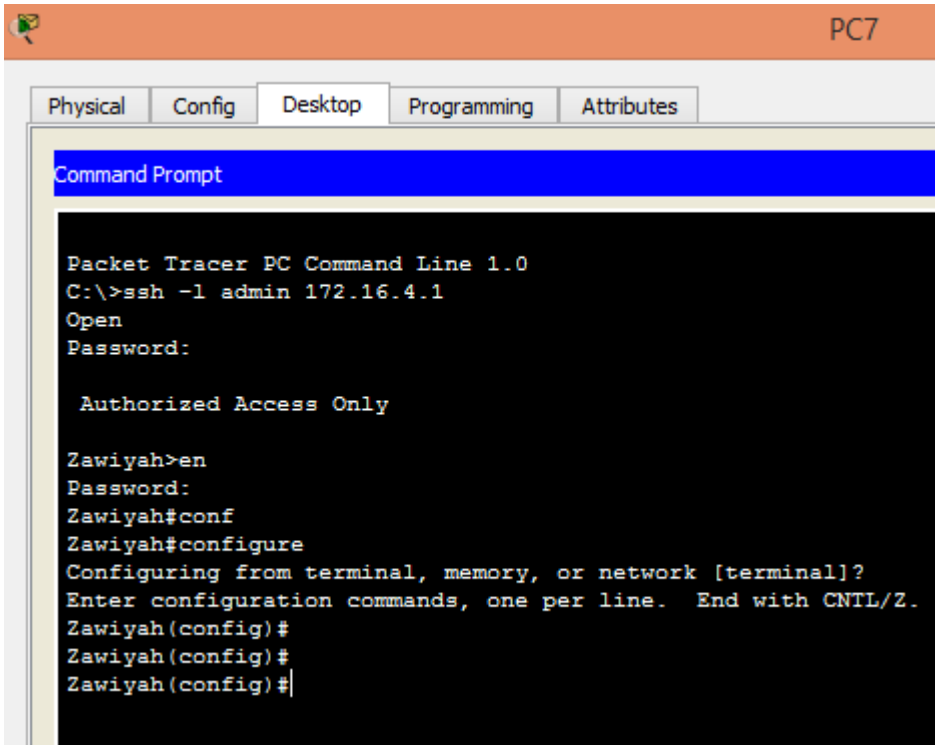


Figure (4)

NOTE : Test remotely access from any another LAN is not successful because it denied by ACLs , as shown in figure (5) :

-Test remotely access from PC in VLAN3 to Zawiyah router…. (ssh) :

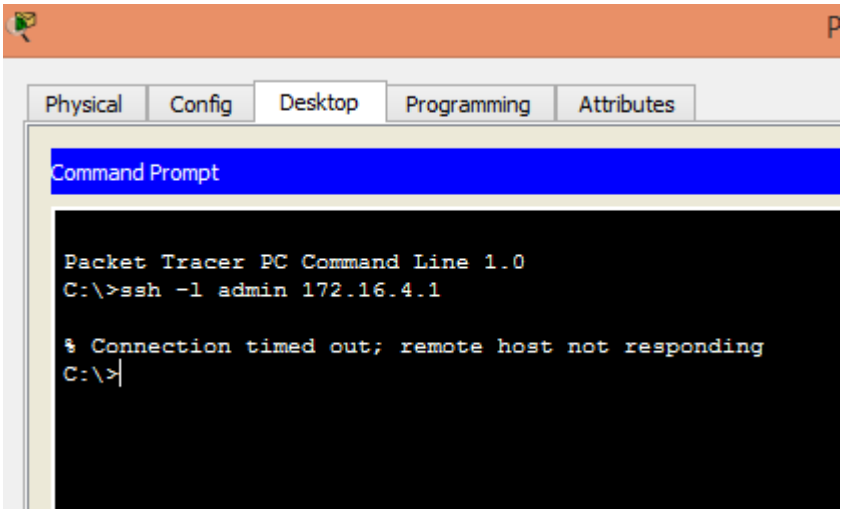


Figure (5)

- Test connection from PC in Zawiyah_LAN_1 to DNS&Web Server :

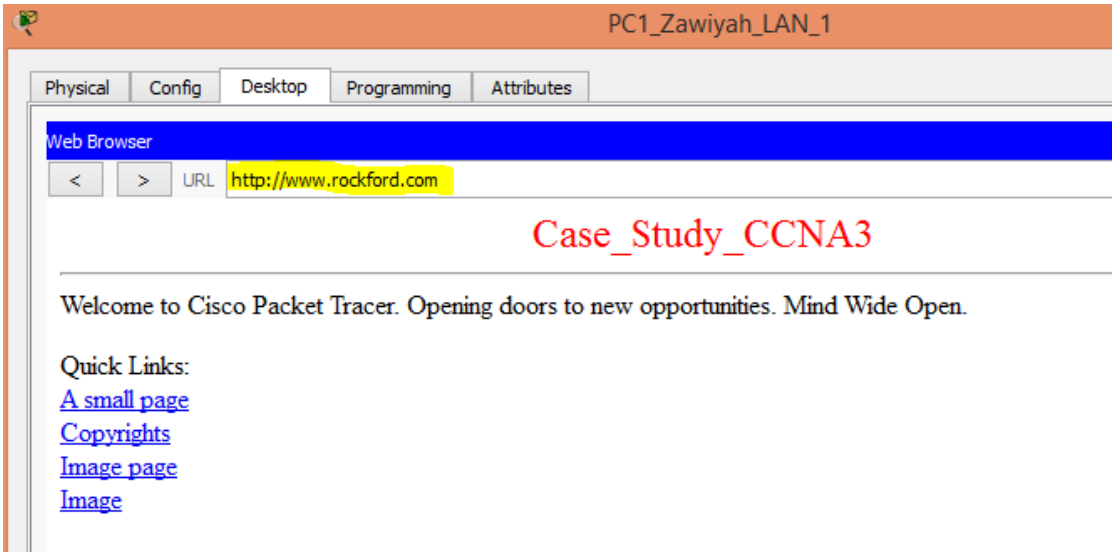


Figure (6)

-Ping command :

*All commands of ping supposed are successful Except the devices Access denied by using ACLs.

- Test connection from Janzur_LAN to Tajura_LAN :

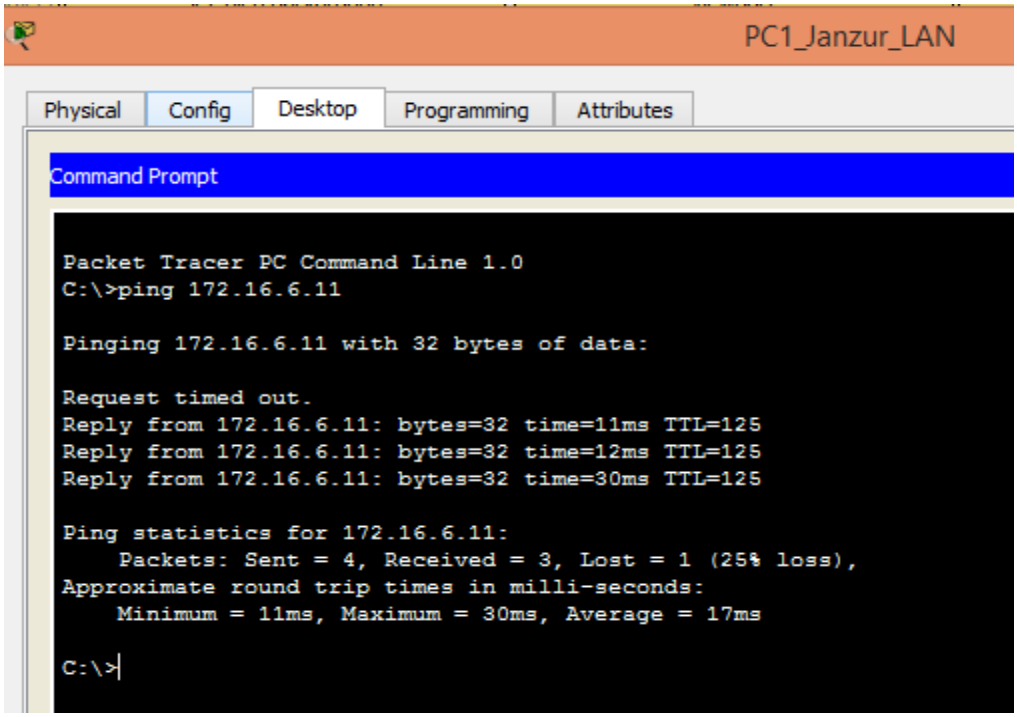


Figure (7)

- traceroute command :

- Tripoli_2 router to PC1_Janzur_LAN :

```
Tripoli_2#traceroute 172.16.5.11
Type escape sequence to abort.
Tracing the route to 172.16.5.11

  1   172.16.7.133    1 msec    2 msec    0 msec
  2   172.16.7.129    2 msec    2 msec    1 msec
  3   172.16.5.11     5 msec    13 msec   14 msec
Tripoli 2#
```

Figure (8)

- Zawiyah router to PC1_ Tajura_LAN :

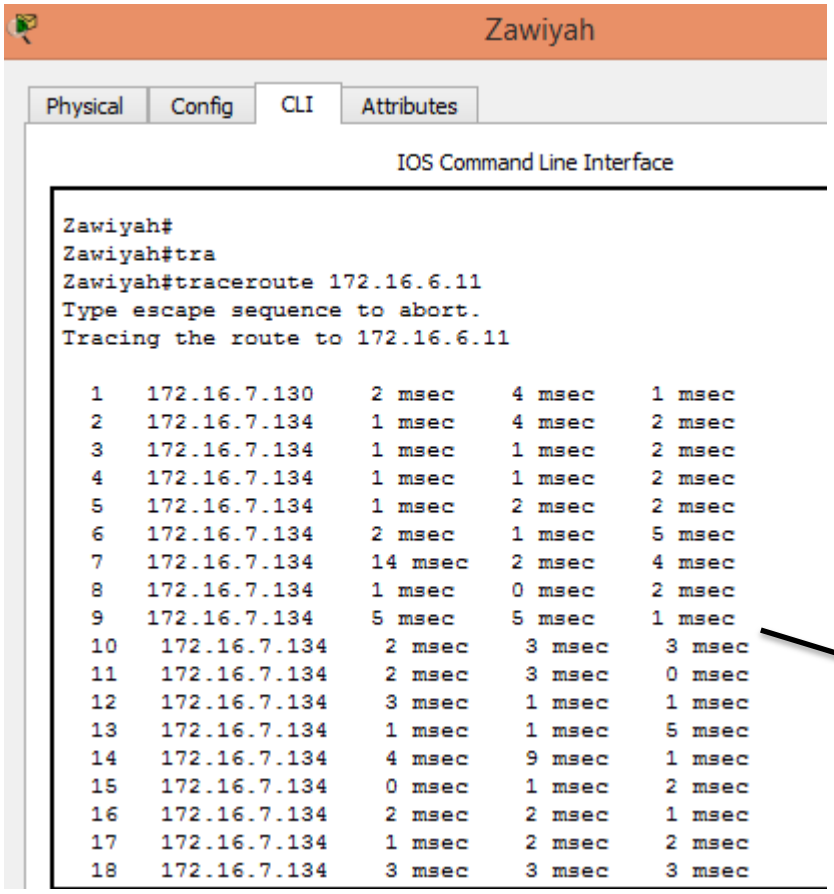
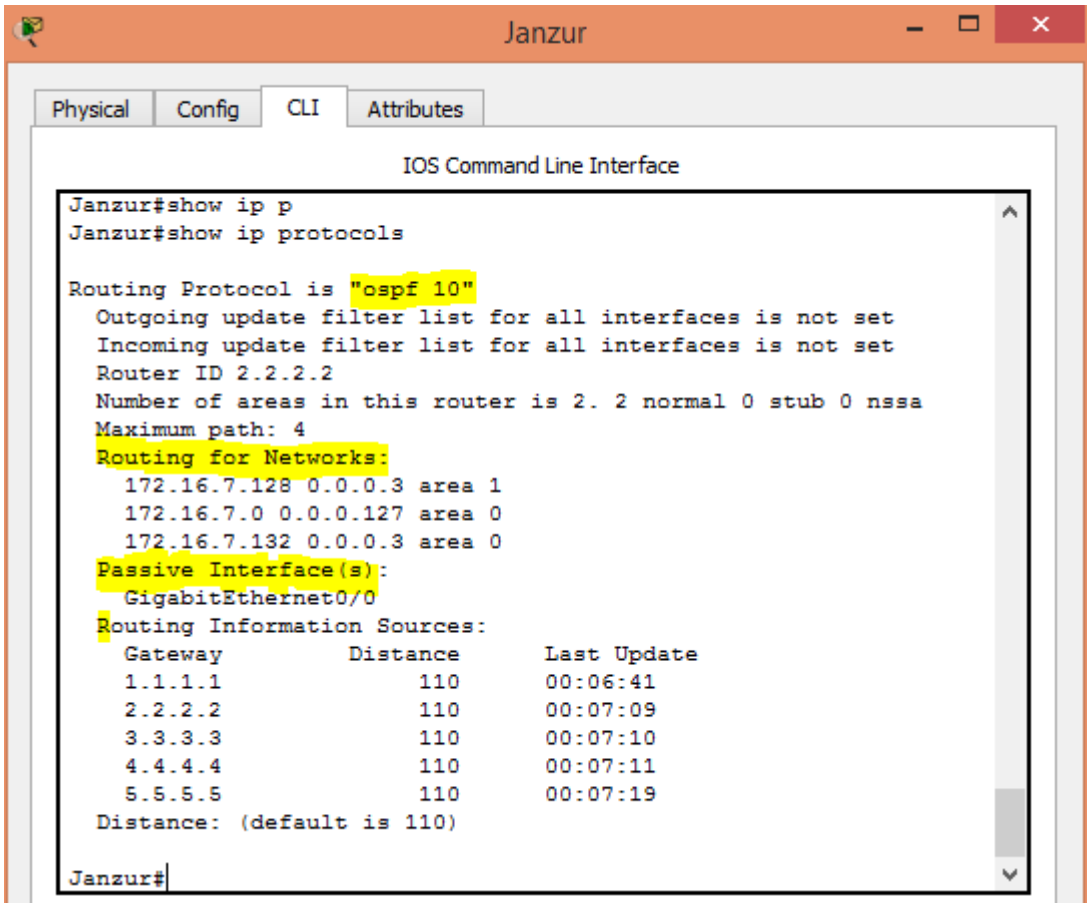


Figure (9)

3. some of Show commands :

3.1 Janzur :




```
Janzur#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P
- Phone
Device ID    Local Intrfce   Holdtme    Capability   Platform
Port ID
Janzur_LAN   Gig 0/0          127            S       2960
Gig 0/1
Zawiyah      Ser 0/0/0        127            R       C1900
Ser 0/0/0
Tripoli_2    Ser 0/0/1        127            R       C1900
Ser 0/0/0
Janzur#
```

3.2 Zawiyah :

```
Zawiyah#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile,
B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter
area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E -
EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 172.16.7.130 to network 0.0.0.0

     172.16.0.0/16 is variably subnetted, 7 subnets, 4 masks
O IA    172.16.0.0/21 [110/65] via 172.16.7.130, 00:07:33,
Serial0/0/0
C       172.16.4.0/24 is directly connected, GigabitEthernet0/1
L       172.16.4.1/32 is directly connected, GigabitEthernet0/1
C       172.16.5.0/24 is directly connected, GigabitEthernet0/0
L       172.16.5.1/32 is directly connected, GigabitEthernet0/0
C       172.16.7.128/30 is directly connected, Serial0/0/0
L       172.16.7.129/32 is directly connected, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.16.7.130, 00:08:03, Serial0/0/0
```

3.3 S2 :

```
S2#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Po1         on           802.1q         trunking      100
Po2         on           802.1q         trunking      100
Gig0/1      on           802.1q         trunking      100

Port        Vlans allowed on trunk
Po1         2-4,99-100
Po2         2-4,99-100
Gig0/1      2-4,99-100

Port        Vlans allowed and active in management domain
Po1         2,3,4,99,100
Po2         2,3,4,99,100
Gig0/1      2,3,4,99,100

Port        Vlans in spanning tree forwarding state and not
pruned
Po1         2,3,4,99,100
Po2         2,3,4,99,100
Gig0/1      2,3,4,99,100
```

4.1. Plans recommended in the future for improvement network performance and security :

1. Disable all unused ports and put them in Garbage VLAN in other switches as (Zawiyah_LAN_1 , Zawiyah_LAN_2 , Janzur_LAN ….) , also using port security in them .

2.Change all **standard & Extended** numbered ACLs to Named ACLs, because it gives more flexibility in the troubleshooting In the event of an error in the order of the commands.

4.2. Lessons learned from Case Study :

1. How to install and work configuration for the network , beginning with the physical layer and up to network layer (L3 security by ACLs & L3 Routing) . and, how troubleshooting this network , by using Cisco packet tracer version 7.1 .

2.How to document the network using Microsoft word 2010.

3. Working under pressure, and organizing time to comply with the date of delivery of this report .

* **Appendices** :

Table (9). Summary of the configuration for assign ip to switches

Switches	Vlans	IP Address / prefix	Default getaway
Zawiyah_LAN_1	1	172.16.4.2/24	**172.16.4.1**
Zawiyah_LAN_2	1	172.16.5.2/24	**172.16.5.1**
Janzur_LAN	1	172.16.7.2 /25	**172.16.7.1**
Tajura_LAN	1	172.16.6.2 /24	**172.16.6.1**
S1	99	172.16.3.132/28	**172.16.3.129**
S2	99	172.16.3.133/28	**172.16.3.129**
S3	99	172.16.3.134/28	**172.16.3.129**

Table (10). Shows Shortcut

SSH	Secure Shell
ACLs	Access Control List .
VLAN	Virtual Local Area Network .
RIP	Routing Information Protocol.
OSPF	. Open Shortest Path First.

1. Zawiyah router :

```
Zawiyah#show running-config
Building configuration...

Current configuration : 1745 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Zawiyah
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
```

```
no ip cef
no ipv6 cef
!
username admin secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
license udi pid CISCO1941/K9 sn FTX1524DKIK
!
ip ssh version 2
ip domain-name cisco.com
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
description Link to Zawiyah LAN_2
ip address 172.16.5.1 255.255.255.0
ip helper-address 172.16.7.130
ip access-group SSH_Session in
duplex auto
speed auto
!
interface GigabitEthernet0/1
description Link to Zawiyah LAN_1
ip address 172.16.4.1 255.255.255.0
ip helper-address 172.16.7.130
ip access-group SSH_Session in
duplex auto
speed auto
!
interface Serial0/0/0
description Link to Janzur
ip address 172.16.7.129 255.255.255.252
ip helper-address 172.16.7.130
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 cisco
ip ospf hello-interval 40
ip ospf dead-interval 160
ip access-group SSH_Session in
!
interface Serial0/0/1
no ip address
clock rate 2000000
shutdown
!
interface Vlan1
no ip address
shutdown
!
router ospf 10
router-id 1.1.1.1
log-adjacency-changes
passive-interface GigabitEthernet0/0
```

```
passive-interface GigabitEthernet0/1
network 172.16.4.0 0.0.1.255 area 1
network 172.16.7.128 0.0.0.3 area 1
!
ip classless
!
ip flow-export version 9
!
ip access-list extended SSH_Session
permit tcp 172.16.3.128 0.0.0.15 any eq 22
deny tcp any any eq 22
permit ip any any
!
banner motd ^C Authorized Access Only^C
!
line con 0
password 7 0822455D0A16
login
!
line aux 0
!
line vty 0 4
login local
!
end
```

---

2. Zawiyah router :

```
Janzur#show running-config
Building configuration...

Current configuration : 2665 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Janzur
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
ip dhcp excluded-address 172.16.0.1 172.16.0.10
ip dhcp excluded-address 172.16.2.1 172.16.2.10
ip dhcp excluded-address 172.16.3.1 172.16.3.10
ip dhcp excluded-address 172.16.4.1 172.16.4.10
ip dhcp excluded-address 172.16.5.1 172.16.5.10
ip dhcp excluded-address 172.16.7.1 172.16.7.10
!
```

```
ip dhcp pool Production_LAN
network 172.16.0.0 255.255.254.0
default-router 172.16.0.1
dns-server 209.1.1.2
ip dhcp pool Zawiyah_LAN_1
network 172.16.4.0 255.255.255.0
default-router 172.16.4.1
dns-server 209.1.1.2
ip dhcp pool Zawiyah_LAN_2
network 172.16.5.0 255.255.255.0
default-router 172.16.5.1
dns-server 209.1.1.2
ip dhcp pool Janzur
network 172.16.7.0 255.255.255.128
default-router 172.16.7.1
dns-server 209.1.1.2
ip dhcp pool Sales_LAN
network 172.16.2.0 255.255.255.0
default-router 172.16.2.1
dns-server 209.1.1.2
ip dhcp pool HR_LAN
network 172.16.3.0 255.255.255.128
default-router 172.16.3.1
dns-server 209.1.1.2
!
no ip cef
no ipv6 cef
!
username admin secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
license udi pid CISCO1941/K9 sn FTX1524F7DU
!
ip ssh version 2
ip domain-name cisco.com
!
spanning-tree mode pvst
!
 interface GigabitEthernet0/0
ip address 172.16.7.1 255.255.255.128
ip access-group SSH_Session in
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/0/0
ip address 172.16.7.130 255.255.255.252
```

```
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 cisco
ip ospf hello-interval 40
ip ospf dead-interval 160
ip access-group SSH_Session in
clock rate 2000000
!
interface Serial0/0/1
ip address 172.16.7.133 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 cisco
ip access-group SSH_Session in
clock rate 2000000
!
interface Vlan1
no ip address
shutdown
!
router ospf 10
router-id 2.2.2.2
log-adjacency-changes
area 0 range 172.16.0.0 255.255.248.0
area 1 range 172.16.4.0 255.255.252.0
passive-interface GigabitEthernet0/0
network 172.16.7.0 0.0.0.127 area 0
network 172.16.7.132 0.0.0.3 area 0
network 172.16.7.128 0.0.0.3 area 1
!
ip classless
!
ip flow-export version 9
!
ip access-list extended SSH_Session
permit tcp 172.16.3.128 0.0.0.15 any eq 22
deny tcp any any eq 22
permit ip any any
!
banner motd ^C Authorized Access Only^C
!
line con 0
password 7 0822455D0A16
login
!
line aux 0
!
line vty 0 4
login local
!
end
```

3. Tripoli_2 router :

```
Tripoli_2#show running-config
Building configuration...

Current configuration : 3134 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Tripoli_2
!

enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
no ip cef
no ipv6 cef
!
username admin secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
license udi pid CISCO1941/K9 sn FTX1524WIK7
!
ip ssh version 2
ip domain-name cisco.com
!
 spanning-tree mode pvst
!
interface GigabitEthernet0/0
ip address 10.0.0.10 255.255.255.248
ip nat outside
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
!
interface GigabitEthernet0/1.2
encapsulation dot1Q 2
ip address 172.16.3.3 255.255.255.128
ip helper-address 172.16.7.133
ip access-group SSH_Session in
ip nat inside
standby 1 ip 172.16.3.1
standby 1 preempt
!
```

```
interface GigabitEthernet0/1.3
encapsulation dot1Q 3
ip address 172.16.2.3 255.255.255.0
ip helper-address 172.16.7.133
ip access-group SSH_Session in
ip access-group 1 out
ip nat inside
standby 2 ip 172.16.2.1
standby 2 preempt
!
interface GigabitEthernet0/1.4
encapsulation dot1Q 4
ip address 172.16.0.3 255.255.254.0
ip helper-address 172.16.7.133
ip access-group SSH_Session in
ip nat inside
standby 3 ip 172.16.0.1
standby 3 preempt
!
interface GigabitEthernet0/1.99
encapsulation dot1Q 99
ip address 172.16.3.131 255.255.255.240
ip helper-address 172.16.7.133
ip access-group SSH_Session in
ip nat inside
standby 4 ip 172.16.3.129
standby 4 preempt
!
interface GigabitEthernet0/1.100
encapsulation dot1Q 100 native
no ip address
ip access-group SSH_Session in
ip nat inside
!
interface Serial0/0/0
ip address 172.16.7.134 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 cisco
ip access-group SSH_Session in
ip nat inside
!
interface Serial0/0/1
ip address 172.16.7.137 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 cisco
ip access-group SSH_Session in
ip access-group (HR&Janzur_LANs)_to_access out
ip nat inside
clock rate 2000000
!
interface Vlan1
```

```
no ip address
shutdown
!
router ospf 10
router-id 4.4.4.4
log-adjacency-changes
passive-interface GigabitEthernet0/0
passive-interface GigabitEthernet0/1
network 172.16.0.0 0.0.3.255 area 0
network 172.16.7.132 0.0.0.3 area 0
network 172.16.7.136 0.0.0.3 area 0
default-information originate
!
ip nat pool Public_IP 200.10.10.74 200.10.10.126 netmask 255.255.255.192
ip nat inside source list NAT pool Public_IP
ip classless
ip route 0.0.0.0 0.0.0.0 10.0.0.9
!
ip flow-export version 9
!
access-list 1 deny 172.16.4.0 0.0.1.255
access-list 1 permit any
ip access-list extended SSH_Session
permit tcp 172.16.3.128 0.0.0.15 any eq 22
deny tcp any any eq 22
permit ip any any
ip access-list standard (HR&Janzur_LANs)_to_access
permit 172.16.3.0 0.0.0.255
permit 172.16.7.0 0.0.0.127
deny any
ip access-list standard NAT
permit 172.16.0.0 0.0.15.255
deny any
!
banner motd ^C Authorized Access Only^C
!
line con 0
password 7 0822455D0A16
login
!
line aux 0
!
line vty 0 4
login local
!
end
```

4. Tajura router :

```
Tajura#show running-config
Building configuration...

Current configuration : 1567 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Tajura
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
no ip cef
no ipv6 cef
!
license udi pid CISCO1941/K9 sn FTX1524ZH5X
!
ip ssh version 2
ip domain-name cisco.com
!
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
description Link to Tajura LAN
ip address 172.16.6.1 255.255.255.0
ip access-group SSH_Session in
duplex auto
speed auto
!
interface GigabitEthernet0/1
description Link to Tajura LAN
no ip address
duplex auto
speed auto
!
interface Serial0/0/0
description Link to Tripoli_2
ip address 172.16.7.138 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 cisco
ip access-group SSH_Session in
!
interface Serial0/0/1
no ip address
clock rate 2000000
shutdown
```

```
!
interface Vlan1
no ip address
shutdown
!
router ospf 10
router-id 3.3.3.3
log-adjacency-changes
passive-interface GigabitEthernet0/0
network 172.16.6.0 0.0.0.255 area 0
network 172.16.7.136 0.0.0.3 area 0
!
ip classless
!
ip flow-export version 9
!
ip access-list standard permit(HR&Janzur_LANs)_to_access
permit 172.16.3.0 0.0.0.255
permit 172.16.7.0 0.0.0.127
deny any
ip access-list extended SSH_Session
permit tcp 172.16.3.128 0.0.0.15 any eq 22
deny tcp any any eq 22
permit ip any any
!
banner motd ^C Authorized Access Only^C
!
line con 0
password 7 0822455D0A16
login
!
line aux 0
!
line vty 0 4
login local
!
end
```

---

* Reference :

(Routing and Switching Essentials Companion Guide , Published by: Paul Boger , 800 East 96th Street Indianapolis, IN 46240 USA , First Printing February 2014 , Available from https://drive.google.com/drive/folders/0B8gUkGgrt_vqVFB2Tzh3dmd1VFU , [Accessed 18th March 2018]).