كلية التقنية الالكترونية
College of Electronic Technology - Tripoli
طرابلس

“Communication department”

Course Title : LAN Switching and Wireless
Case study : Network design for Rockford PLC

Name: Masara Ali Ganbour
Registration No:162027
Subject: CCNA 3
recipient: Eng. Hider swaih

Abstract:

This report presents a network design project for the company Rockford PLC , by using the Cisco Packet Tracer v7.2, 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. 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 remotely 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 = 172.22.0.0/21 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) .

Content list:

Tables list:

Figure list :

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:

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.

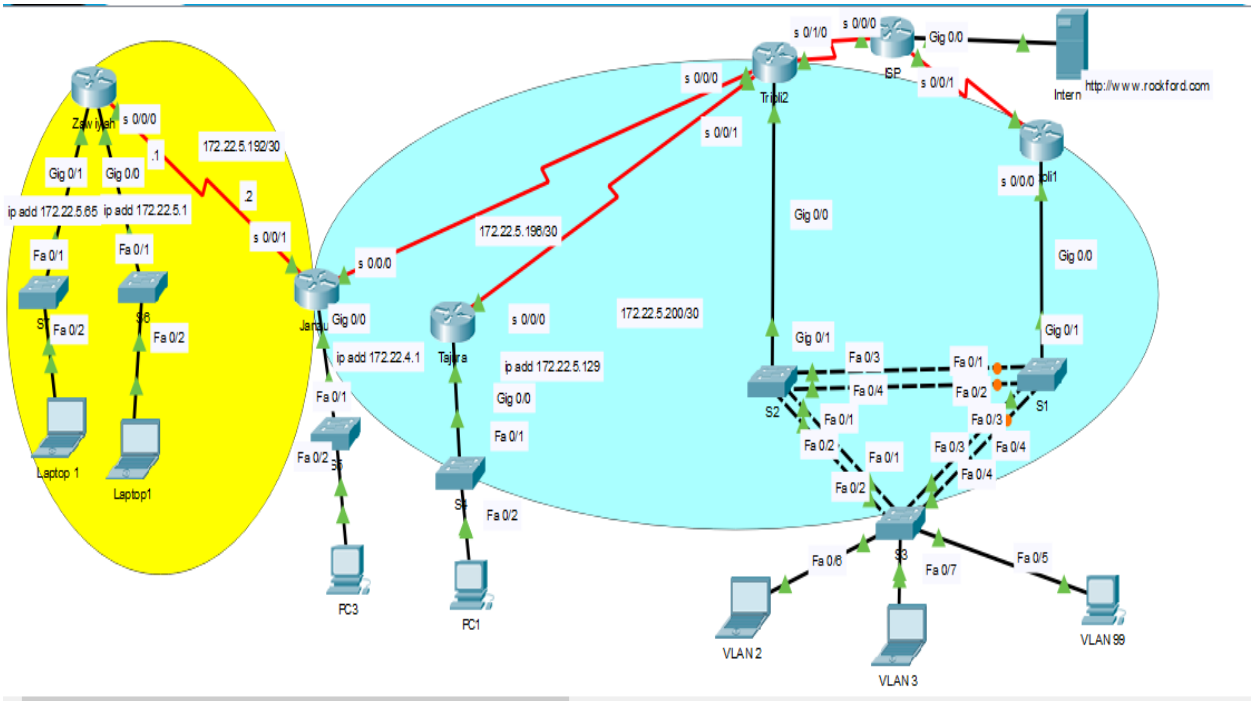
Phase 5: Configuring ACLs .

Phase 6: Configuring DHCP .

Phase 7: NAT .

Phase 8: Verification and Testing .

Topology:



Figure(1) "Network Topology"

Phase 1

1.1 Addressing WAN and LAN

In this company the address is 172.16.0.0/30 will be used distributed to networks and the next table shows addresses used in this phase

LANs	Needed Size	Network	Hosts Range	Broadcast	Subnet Mask	Prefix
Tripoli-Vlans	560	172.22.0.0	172.22.0. 1 - 172.22.3.254	172.22.3.255	255.255.255.0	/22
Tajura	60	172.22.5.128	172.22.5.129 - 172.22.5.190	255.255.255.192	172.22.5.191	/26
Janzur	200	172.22.4.0	172.22.4.1 - 172.22.4.254	255.255.255.0	172.22.4.255	/24
Zawiya (Lan1+Lan2)	120	172.22.5.0	172.22.5.1 - 172.22.5.126	255.255.255.128	172.22.5.127	/25

Table (1) shows Block ip addressing used to allocates for each LANs

Table (2) shows Addressing used to allocates for each Zawiyah (lan1) and Zawiyah (lan2)

LANs Allocated size	Allocated size	Network	Host Range	Broadcast	Subnet Mask	Prefix
Zawiyah LAN1	60	172.22.5.0	172.22.5.1 - 172.22.5.63	172.22.5.63	255.255.255.192	/26
Zawiyah LAN2	60	172.22.5.64	172.22.5.65 - 172.22.5.127	172.22.5.127	255.255.255.192	/26

Table (3) shows Addressing used to allocates for each WANs

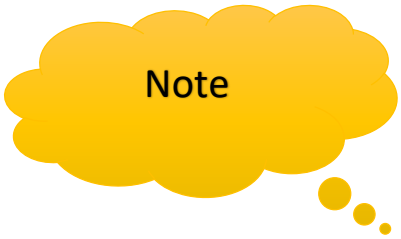
WAN	Allocated size	Network	Host Range	Broadcast	Subnet Mask	Prefix
WAN 1	2	172.22.5.192	172.22.5.193 - 172.22.5.194	172.22.5.195	255.255.255.252	/30
WAN 2	2	172.22.5.196	172.22.5.197 - 172.22.5.198	172.22.5.199	255.255.255.252	/30
WAN 3	2	172.22.5.200	172.22.5.201 - 172.22.5.202	172.22.5.203	255.255.255.252	/30

Table (4) shows Addressing used to allocates for each VLAN

LANS	VLAN Number	Needed Size	Network	Host range	Broadcast	Subnet Mask	Prefix
Tripoli 1 & 2	Vlan 2	400	172.22.0.0	172.22.0.1 - 172.22.1.254	172.22.1.255	255.255.254.0	/23
	Vlan 3	150	172.22.2.0	172.22.2.1 - 172.22.2.254	172.22.2.255	255.255.255.0	/25
	Vlan 99	10	172.22.3.0	172.22.3.1 - 172.22.3.14	172.22.3.15	255.255.255.240	/28

Table(5) shows the PCs and Server device that are assigned statically

Device	IPV4 Address	Subnet Mask	DNS Server	Default Getaway
PC3(Junzur)	172.22.4.254	255.255.255.0	209.1.1.2	172.22.4.1
PC4(Tajura)	172.22.5.190	255.255.255.192	209.1.1.2	172.22.5.129
PC7(VLAN99)	172.22.3.14	255.255.255.240	209.1.1.2	172.22.3.1
DNS server	209.1.1.2	255.255.255.252	209.1.1.2	209.1.1.1



other devices (PCS) will be assigned dynamically for the rest of the LANS **(Vlan2,3 , Zawiyah LANs)**, look at DHCP configuration in Phase 6

Phase 2

2 Basic Router and Switch configuration

In this phase we apply basic configuration in each router and switch in the Network Topology

2.1 Basic router configuration

- Step 1 : Router name (changing host name in each router) .
- Step 2 : creating Line console 0 to give password for user mode (cisco)
- Step 3 : creating Password for Privileged mode (class)
- Step 4 : enabling banner message as **# Authorized Access Only #** .
- Step 5: encrypt all passwords by using (**service password-encryption**) command.
- Step 6 : enabling SSH protocol for secure and encrypted remote management with (cisco.com) domain name and (admin/cisco) as a user information.
- Step 7 : give ip address for all the interfaces on routers
- Step 8 : Configure descriptions in point-to-point interfaces
- Step 9 : Configure descriptions in LAN interfaces

```
Press RETURN to get started!



Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Tripolil
Tripolil(config)#line console 0
Tripolil(config-line)#pass
Tripolil(config-line)#password cisco
Tripolil(config-line)#exit
Tripolil(config)#enable s
Tripolil(config)#enable secret class
Tripolil(config)#banner motd # Authorized Access Only #
Tripolil(config)#ser
Tripolil(config)#service pass
Tripolil(config)#service password-encryption
Tripolil(config)#
```

Figure(2) basic configuration in Tripoli1 and all routers

```
Tripolil(config)#ip domain-name cisco.com
Tripolil(config)#user
Tripolil(config)#username admin pass
Tripolil(config)#username admin password cisco
Tripolil(config)#crypto ke
Tripolil(config)#crypto key g
Tripolil(config)#crypto key generate r
Tripolil(config)#crypto key generate rsa
The name for the keys will be: Tripolil.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for
your
  General Purpose Keys. Choosing a key modulus greater than 512 may
take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Tripolil(config)#line vty 0 4
*Mar 1 0:3:12.517: %SSH-5-ENABLED: SSH 1.99 has been enabled
Tripolil(config-line)#transport input ssh
Tripolil(config-line)#login local
Tripolil(config-line)#exit
Tripolil(config)#ip ssh v 2
Tripolil(config)#
```

Figure(3) enable SSH to all routers

```
Tripolil(config)#int gig 0/0.2
Tripolil(config-subif)#ip add 172.22.0.3 255.255.254.0

% Configuring IP routing on a LAN subinterface is only allowed if
that
subinterface is already configured as part of an IEEE 802.10, IEEE
802.1Q,
or ISL vLAN.

Tripolil(config-subif)#no sh
Tripolil(config-subif)#int gig 0/0.3
Tripolil(config-subif)#ip add 172.22.2.3 255.255.255.128

% Configuring IP routing on a LAN subinterface is only allowed if
that
subinterface is already configured as part of an IEEE 802.10, IEEE
802.1Q,
or ISL vLAN.

Tripolil(config-subif)#int gig 0/0.99
Tripolil(config-subif)#ip add 172.22.3.3 255.255.255.240

% Configuring IP routing on a LAN subinterface is only allowed if
that
subinterface is already configured as part of an IEEE 802.10, IEEE
```

```
Tripolil(config-subif)#int gig 0/0
Tripolil(config-if)#no sh

Tripolil(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0.2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.2,
changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0.3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.3,
changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0.99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0.99, changed state to up
```

```
Tripolil(config-if)#int se 0/0/0
Tripolil(config-if)#ip add 10.4.0.2 255.255.255.252
Tripolil(config-if)#no sh

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
Tripolil(config-if)#
```

```
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
Tripolil(config-if)#int gig 0/0
Tripolil(config-if)#des
Tripolil(config-if)#description Link to S1
Tripolil(config-if)#int se 0/0/0
Tripolil(config-if)#description Link to ISP
Tripolil(config-if)#
```

Figure(4) assign ip address and descriptions to all interfaces in Tripoli1 and all routers

Note

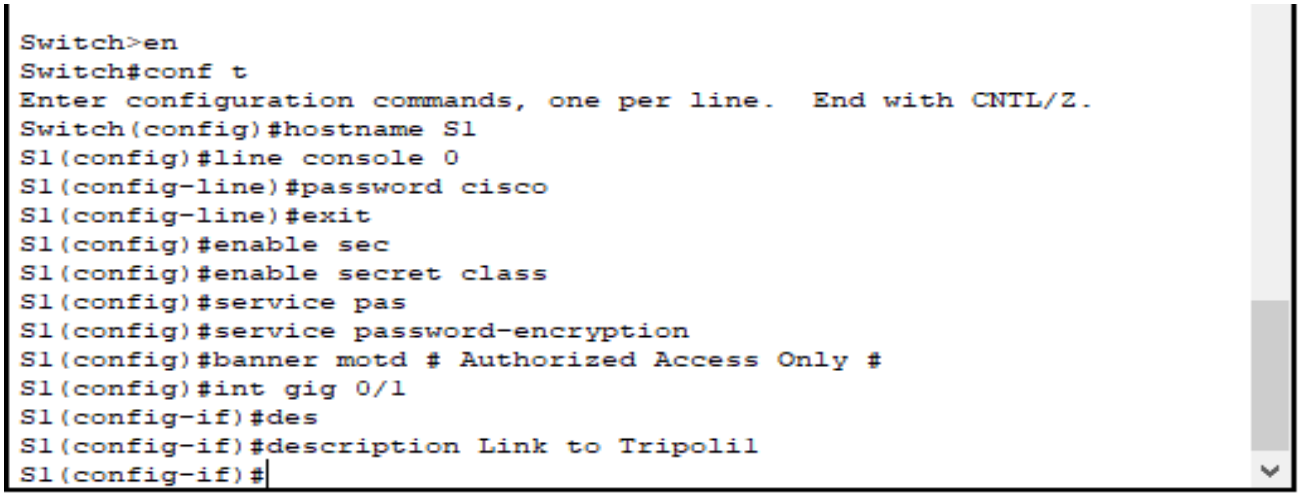
The IP of other interfaces on the Routers as displayed in the table “ 7 “.

Table (6) shows the IP and the subnet Mask for each Interfaces in the Routers devices

Device	Interfaces	IPV4 Addresses	Subnet Mask	Prefix
Tripoli 2	G 0/0.2	172.22.0.2	255.255.254.0	/23
	G 0/0.3	172.22.2.2	255.255.255.128	/25
	G 0/0.99	172.22.3.2	255.255.255.240	/28
	S 0/1/0	10.4.0.6	255.255.255.252	/30
	S 0/0/1	172.22.5.202	255.255.255.252	/30
	S 0/0/0	172.22.5.198	255.255.255.252	/30
Tripoli 1	G 0/0.2	172.22.0.3	255.255.254.0	/23
	G 0/0.3	172.22.2.3	255.255.255.128	/25
	G 0/0.99	172.22.3.3	255.255.255.240	/28
	S 0/0/0	10.4.0.2	255.255.255.252	/30
Tajura	G 0/0	172.22.5.129	255.255.255.192	/26
	S 0/0/0	172.22.5.201	255.255.255.252	/30
Janzur	G 0/0	172.22.4.1	255.255.255.0	/24
	S 0/0/0	172.22.5.197	255.255.255.252	/30
	S 0/0/1	172.22.5.194	255.255.255.252	/30
Zawiyah	G 0/0	172.22.5.1	255.255.255.192	
	G 0/1	172.22.5.65	255.255.255.192	
	S 0/0/1	172.22.5.193	255.255.255.252	/30
ISP	G 0/0	209.1.1.1	255.255.255.252	/30
	S 0/0/0	10.4.0.5	255.255.255.252	/30
	S 0/0/1	10.4.0.1	255.255.255.252	/30

2.2 Basic Switch Configuration

Step 1 : Configure hostname in each switch.
Step 2 :Create line console 0 password (cisco).
Step 3 : Enable secret password (cisco).
Step 4 : Encrypt all password using command (Service password-encryption).
Step 5 : create banner motd (#Authorized Access Only #) .
Step 6 : create remotely management.
Step 7 : enabling SSH protocol for secure and encrypted remote management with (cisco.com) domain name and (admin/cisco) as a user information.
Step 8 : Configure interfaces description that connected to routers



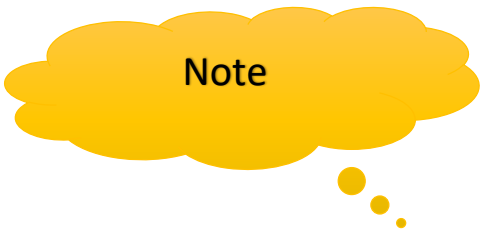
Figure(5) Basic switch configuration

```
S1(config-if)#
S1(config-if)#ip domain-name cisco.com
S1(config)#username admin password cisco
S1(config)#crypto key generate rsa
The name for the keys will be: S1.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for
your
  General Purpose Keys. Choosing a key modulus greater than 512 may
take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

S1(config)#ip ssh v 2
*Mar 1 0:6:25.459: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config)#line vty 0 4
S1(config-line)#transport input ssh
S1(config-line)#login local
S1(config-line)#
```

figure(6) Assign SSH on S1 and all switches

```
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#int vlan 99
S1(config-if)#ip address 172.22.3.4 255.255.255.240
S1(config-if)#
S1(config-if)#no sh
S1(config-if)#
```

Figure(7) Assign Management vLan on all switches



Management VLANs will be assigned as displayed in table " 7 " below.

Table(7) shows the IP and the subnet Mask for each VLANs in the Switches devices

Device	Interface	IPV4 Address	Subnet Mask	Prefix	Default Getaway
S1	VLAN 99	172.22.3.4	255.255.255.240	/28	172.22.3.1
S2	VLAN 99	172.22.3.5	255.255.255.240	/28	172.22.3.1
S3	VLAN 99	172.22.3.6	255.255.255.240	/28	172.22.3.1
S4	VLAN1	172.22.5.130	255.255.255.192	/26	172.22.5.129
S5	VLAN1	172.22.4.2	255.255.255.0	/24	172.22.4.1
S6	VLAN1	172.22.5.2	255.255.255.128	/25	172.22.5.1
S7	VLAN1	172.22.5.66	255.255.255.128	/25	172.22.5.65

Phase 3

3 Configure Default Routes, OSPF Routing and HSRP

3.1 Default routes

We use default route with Routers Tripoli-1 and Tripoli-2, to defines the packet forwarding rule to use when no specific route can be determined for a given Internet Protocol (IP) destination address .

```
Tripoli2#
Tripoli2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Tripoli2(config)#ip route 0.0.0.0 0.0.0.0 10.4.0.5
Tripoli2(config)#
```

Figure(8) configure default route in Tripoli2

```
Tripolil#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Tripolil(config)#ip route 0.0.0.0 0.0.0.0 10.4.0.1
Tripolil(config)#
```

Figure(9) configure default route in Tripoli1

```
ISP(config)#
ISP(config)#ip route 0.0.0.0 0.0.0.0  10.4.0.6
ISP(config)#ip route 0.0.0.0 0.0.0.0  10.4.0.2
ISP(config)#
```

Figure(10) configure default route in ISP router

3.2 Configure OSPF

First Step :

Configure router OSPF process ID **(Process ID is 10 on all routers)**.

second Step :

Configure router ID (Every router must be given an ID , if it is not it will assign an ID automatically depending on the highest interface, we do not want that to happen because the interfaces are not stable and can go down at any moment which will make the router go out of service)

Third Step :

Configure Network Advertisement (In each router must be advertise all directly connected networks considering area number as required)

Fourth Step :

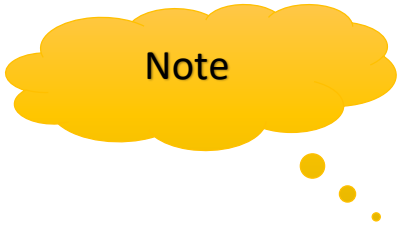
Configure a summary (Type 3) for area 1 , To minimize the size of routing table , must be configure summary type 3 and this configuration applied in R-janzur because its (ABR) (Area Border Router)

```
R-Tajura(config)#router ospf process-id
R-Tajura(config-router)#router-id ip-add
R-Tajura(config-router)#network Network ID waild-card area area-id
R-Tajura(config-router)#passive-interface g#/#
```

Figure (11) OSPF configuration

Table (8) Information needs to apply OSPF

Router	Process-ID	Network	Wildcard Mask	Area-ID	Passive interface
Tripoli2	4.4.4.4	172.22.0.0	0.0.1.255	0	G 0/0.2
	4.4.4.4	172.22.2.0	0.0.0.127	0	G 0/0.3
	4.4.4.4	172.22.3.0	0.0.0.15	0	G 0/0.99
	4.4.4.4	172.22.5.196	0.0.0.3	0	S 0/0/0
	4.4.4.4	172.22.5.200	0.0.0.3	0	S 0/0/1
Tripoli 1	*5.5.5.5*	172.22.0.0	0.0.1.255	0	*G 0/0.2*
	5.5.5.5	172.22.2.0	0.0.0.127	0	*G 0/0.3*
	5.5.5.5	172.22.3.0	0.0.0.15	0	*G 0/0.99*
Janzur	2.2.2.2	172.22.4.0	0.0.0.255	0	G 0/0
	2.2.2.2	172.22.5.192	0.0.0.3	1	S 0/0/0
	2.2.2.2	172.22.5.196	0.0.0.3	0	S 0/0/1
Tajura	3.3.3.3	172.22.5.128	0.0.0.63	0	G 0/0
	3.3.3.3	172.22.5.200	0.0.0.3	0	S 0/0/0
Zawiyah	1.1.1.1	172.22.5.0	0.0.0.63	1	G 0/0
	1.1.1.1	172.22.5.64	0.0.0.63	1	G 0/1
	1.1.1.1	172.22.5.192	0.0.0.3	1	S 0/0/0



default-information originate will be applied only in Tripoli1 and 2 routers because they are connected to the ISP to be able to propagate other networks and make them able to access the internet as displayed in figure(12).

```
Tripoli2(config)#router ospf 10
Tripoli2(config-router)#default
Tripoli2(config-router)#default-information originate
```

Figure(12)

3.3Configure HSRP :

PC1,PC2 and PC3 can connect to outside network by one ip getway, to insure availability of the network should configure HSRP.

In this case (Tripoli 2) have chosen to be the active router because It connect most network devices, this solution is better than giving the active state to Tripoli 1 router because all traffic will across the network to the ISP to reach Zawiyah or Janzur routers, this traffic will make overlay on the network . So the active router (Tripoli 2) configured as figure () .

Table (9) R – Active / Standby & Virtual

interfaces	Group Number	R-Tripoli 2 Activ	R-Tripoli 1 Standby	IP R-Virtual
G 0/0.2	1	172.22.0.2	172.22.0.3	172.22.0.1
G 0/0.3	1	172.22.2.2	172.22.2.3	172.22.2.1
G 0/0.99	1	172.22.3.2	172.22.3.3	172.22.3.1

```
Tripoli2(config)#int gig 0/0.2
Tripoli2(config-subif)#standby 1 ip 172.22.0.1
Tripoli2(config-subif)#standby 1 pr
Tripoli2(config-subif)#standby 1 prio
Tripoli2(config-subif)#standby 1 priority 150
Tripoli2(config-subif)#standby 1 preempt
Tripoli2(config-subif)#int gig 0/0.3
Tripoli2(config-subif)#standby 1 ip 172.22.2.1
Tripoli2(config-subif)#standby 1 priority 150
Tripoli2(config-subif)#standby 1 preempt
Tripoli2(config-subif)#int gig 0/0.99
Tripoli2(config-subif)#standby 1 ip 172.22.3.1
Tripoli2(config-subif)#standby 1 priority 150
Tripoli2(config-subif)#standby 1 preempt
Tripoli2(config-subif)#
```

Figure (13) configure HSRP in Active router "Tripoli2"

```
Tripoli1(config)#int gig0/0.2
Tripoli1(config-subif)#standby 1 ip 172.22.0.1
Tripoli1(config-subif)#standby 1 preempt
Tripoli1(config-subif)#int gig0/0.3
Tripoli1(config-subif)#standby 1 ip 172.22.2.1
Tripoli1(config-subif)#standby 1 preempt
Tripoli1(config-subif)#int gig0/0.99
Tripoli1(config-subif)#standby 1 ip 172.22.3.1
Tripoli1(config-subif)#standby 1 preempt
Tripoli1(config-subif)#
```

Figure (14) configure HSRP in Standby router "Tripoli1"

Phase 4

4. Configure VLANs

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
```

Figure (15) configure STP & VTP

4.2 Creating VLANS on server switch

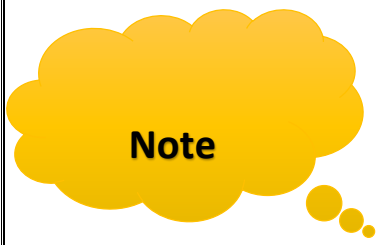
Create and name two Data VLANs and one Management VLAN

– VLAN 99: Management

– VLAN 100: Native

– VLAN 2: Production.

it configured as displayed in figure (16)



in this step every switch will be configured separately, SW1 will be the server switch, so the VLANS will be created just on this switch, and it will automatically send to other switches those has been configured as a client (S2&S3).

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

Figure (16) insert VLANs

Configure three switches (S1,S2&S3) assign :

- assign G0/1 ports as Trunks on S1&S2.
- assign fast Ethernet ports 1-4 as Trunks (802.1Q).
- configure Ether channel.

```
S1(config)#int gig 0/1
S1(config-if)#switch
S1(config-if)#switchport mode trunk
S1(config-if)#interface range fa 0/1-4
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#
```

Figure (17) configure trunks

4.3 Assigning Ports:

These ports on switch 3 will configured as access ports as follows

- Port 5 to Vlan 99
- Ports 6-15 to Vlan 2
- Port 16-20 to Vlan 3
- Disable all unused ports and put them in Garbage VLAN (VLAN98)

```
S3(config)#int fa 0/5
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 99
S3(config-if)#int range fa 0/6-15
S3(config-if-range)#switchport mode access
S3(config-if-range)#switchport access vlan 2
S3(config-if-range)#int range fa 0/16-20
S3(config-if-range)#switchport mode access
S3(config-if-range)#switchport access vlan 3
S3(config-if-range)#
```

```
S3(config-vlan)#int range fa 0/21-24
S3(config-if-range)#switchport mode access
S3(config-if-range)#switchport access vlan 98
S3(config-if-range)#int range fa 0/21-24
S3(config-if-range)#sh

%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to
administratively down
S3(config-if-range)#
```

Figure (18) assign VLANs

Phase 5

an access control lists are used For security purposes, ACL can deny or permit packets based on source and destination IP address, port numbers and upper layer protocols.

5.1 Configure Standard ACL to filter traffic:

The ACL should Deny only the Zawiyah LANs access to VLAN 2 (Production), permit all others as in figure ().

5.2Configure Named Standard ACL to filter traffic:

Prevent all networks to access Tajura network , except for VLAN2 and Janzur network they have the permission to access Tajura network , This list applied to Tajura router as follows.

5.3Use an ACL to control SSH access to all routers

Allow SSH session to all routers from the Management VLAN (VLAN99) only; SSH sessions from all other networks should be denied.

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

```
Tripoli2(config)#access-list 1 deny 172.22.5.0 0.0.0.63
Tripoli2(config)#access-list 1 deny 172.22.5.64 0.0.0.63
Tripoli2(config)#access-list 1 permit any
Tripoli2(config)#int gig 0/0
Tripoli2(config-if)#ip access-group 1 out
Tripoli2(config-if)#
```

Figure (19) ACL applied in Tripoli 1 & 2

```
Tajura(config)#ip access-list standard ACL1
Tajura(config-std-nacl)# permit 172.22.2.0 0.0.0.255
Tajura(config-std-nacl)#permit 172.22.4.0 0.0.0.255
Tajura(config-std-nacl)#deny any
Tajura(config-std-nacl)#int gig 0/0
Tajura(config-if)#ip access-group ACL1 out
Tajura(config-if)#
Tajura(config-if)#
Tajura(config-if)#
```

Figure (20) ACL applied in Tajura

Phase 6

Dynamic Host Configuration Protocol (DHCP) is a network management protocol used on UDP/IP networks where by a DHCP server dynamically assigns an IP address and other network configuration parameters to each device on a network to save time/work especially in large network.

6.1 DHCP should provide services to the following LANs hosts:

– Tripoli's VLAN 2, VLAN 3
– Janzur's LAN
– Zawiyah's LANs

6.2 Janzur router will be the DHCP server who is the responsible for distributing IP addresses .

6.3 pass the following parameters to the hosts :

– IP address and Subnet Mask .
– Default Gateway.
– DNS address (209.1.1.2).

6.4 Exclude the first 10 IP addresses from each pool (to be used for printers, servers, and so on)

Note

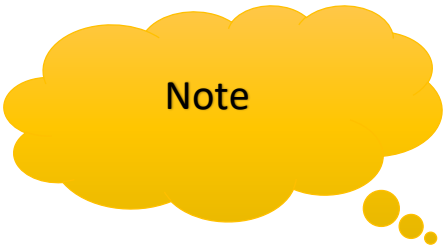
To get the addresses from DHCP Janzur and to forward the packet (Broadcast) for all LANs needs IP from DHCP serve, must be configured Tripoli1 & Tripoli 2 as Relay agent by assigning the ip helper address. As shown below:

```
ip dhcp excluded-address 172.22.4.1 172.22.4.10
ip dhcp excluded-address 172.22.5.1 172.22.5.10
ip dhcp excluded-address 172.22.5.65 172.22.5.75
ip dhcp excluded-address 172.22.0.1 172.22.0.10
ip dhcp excluded-address 172.22.2.1 172.22.2.10
```

Figure (21) DHCP pool in Janzur router

```
Zawiyah(config)#ip dhcp pool LAN1-Zawiyah
Zawiyah(dhcp-config)#network 172.22.5.0 255.255.255.192
Zawiyah(dhcp-config)#default-router 172.22.5.1
Zawiyah(dhcp-config)#dns-server 209.1.1.2
Zawiyah(dhcp-config)#ip dhcp pool LAN2-Zawiyah
Zawiyah(dhcp-config)#network 172.22.5.64 255.255.255.192
Zawiyah(dhcp-config)#default-router 172.22.5.65
Zawiyah(dhcp-config)#dns-server 209.1.1.2
Zawiyah(dhcp-config)#int range gig 0/0-1
Zawiyah(config-if-range)#ip helper-address 172.22.5.194
Zawiyah(config-if-range)#
```

Figure(22) assign helper address in Zawiyah router



When assign helper address in figure (22) it should assign to VLAN2 , VLAN 3 and Zawiyah .

Phase 7

NAT

Network Address Translator (NAT) commonly refers to a box that interconnects a local network to the public Internet, where the local network runs on a block of private IPv4 addresses.

In the original design of the Internet architecture, each IP address was defined to be globally unique and globally reachable. In contrast, a private IPv4 address is meaningful only within the scope of the local network behind a NAT and, as such, the same private address block can be reused in multiple local networks, as long as those networks do not directly talk to each other. Instead, they communicate with each other and with the rest of Internet through NAT boxes

7.1 The Tripoli's (1) routers will perform NAT. Configure the routers as follows:

- 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.

```
Tripolil(config)#ip nat pool NAT1 200.198.10.138 200.198.10.190
netmask 255.255.255.192
Tripolil(config)#access-list 3 permit 172.22.0.0 0.0.15.255
Tripolil(config)#ip nat inside source list 3 pool NAT1 overload
Tripolil(config)#int se 0/0/0
Tripolil(config-if)#ip nat outside
Tripolil(config-if)#int gig 0/0.2
Tripolil(config-subif)#ip nat inside
Tripolil(config-subif)#int gig 0/0.3
Tripolil(config-subif)#ip nat inside
Tripolil(config-subif)#int gig 0/0.99
Tripolil(config-subif)#ip nat inside
Tripolil(config-subif)#
```

Figure(23) Configure NAT in Tripoli1

```
Tripoli2(config)#ip nat pool NAT1 200.198.10.138 200.198.10.190
netmask 255.255.255.192
Tripoli2(config)#access-list 3 permit 172.22.0.0 0.0.15.255
Tripoli2(config)#ip nat inside source list 3 pool NAT1 overload
Tripoli2(config)#int se 0/1/0
Tripoli2(config-if)#ip nat outside
Tripoli2(config-if)#int se 0/0/0
Tripoli2(config-if)#ip nat inside
Tripoli2(config-if)#int se 0/0/1
Tripoli2(config-if)#ip nat inside
Tripoli2(config-if)#int gig 0/0.2
Tripoli2(config-subif)#ip nat inside
Tripoli2(config-subif)#int gig 0/0.3
Tripoli2(config-subif)#ip nat inside
Tripoli2(config-subif)#int gig 0/0.99
Tripoli2(config-subif)#ip nat inside
Tripoli2(config-subif)#
```

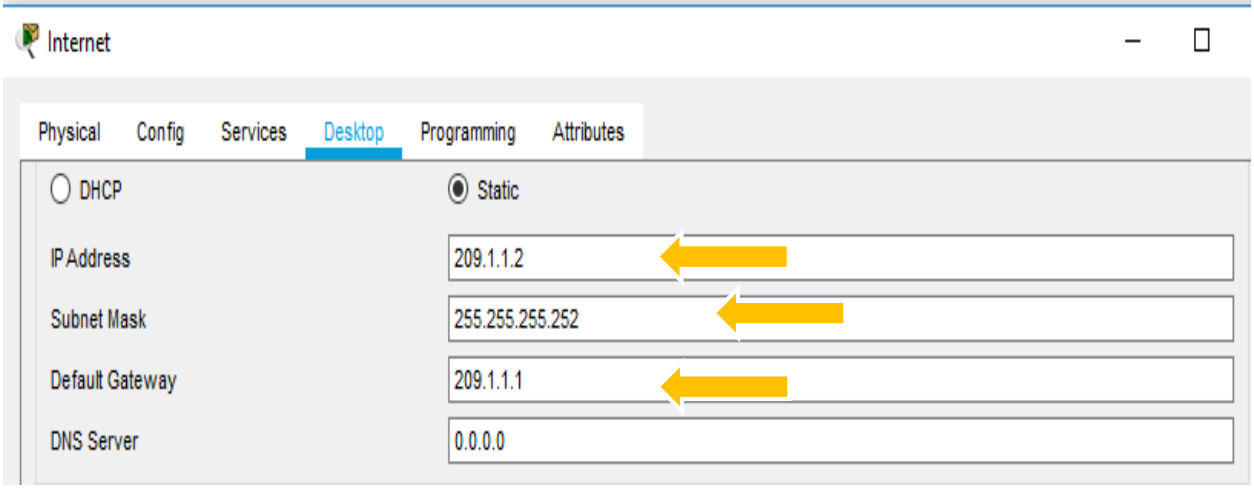
Figure(24) Configure NAT in Tripoli2

7.2 Connect a Server to the ISP's G1/1 port to simulate an ISP server.

Configure this Server as follows:

– Configure the IP address and subnet mask as 209.1.1.2/30.

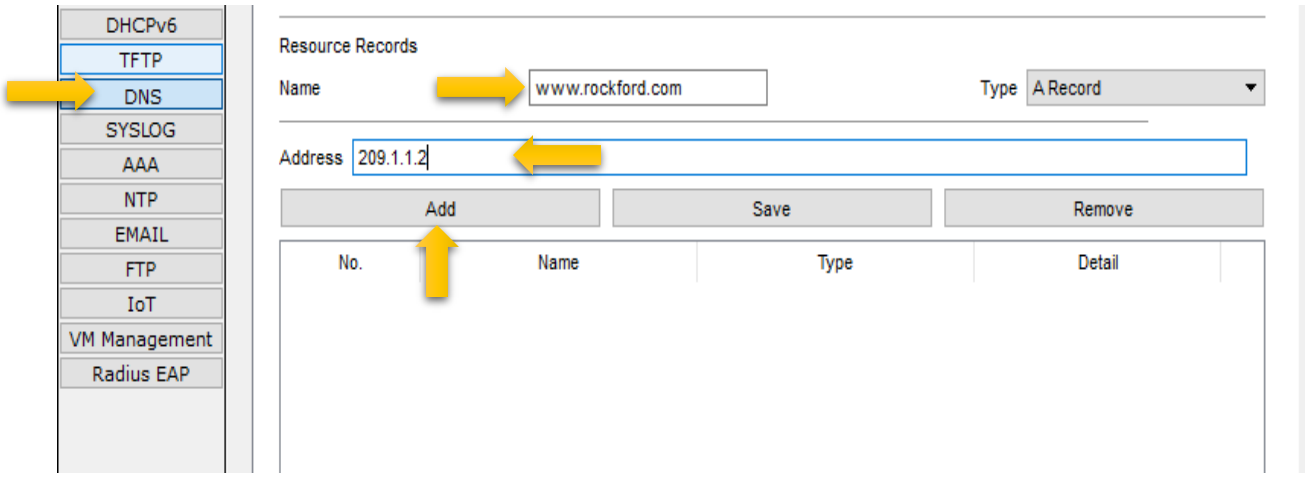
– Configure the default gateway to be 209.1.1.1.



Figure(25) Assign IP to DNS server

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(26) configure web server

Phase 8

Verification and Testing

8.1 Test remotely access from Vlan2 to Janzur as in figure (27).

Some hosts can't reach another network because it denied by ACL like :

- Zawyiah LANs can't reach Vlan2
- Vlan3 , Vlan 99 & Zawyah can't reach Tajura Lan
-remotely management to all routers just from Vlan99

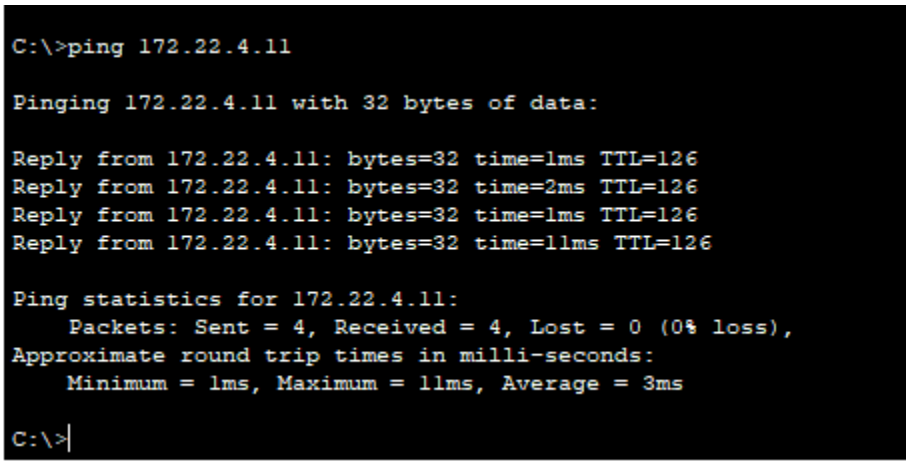
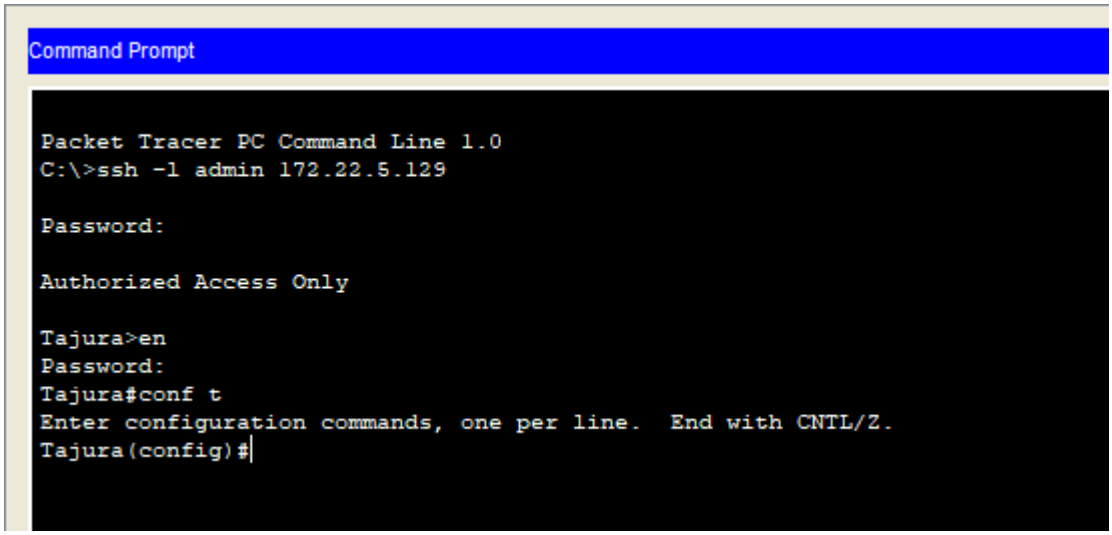
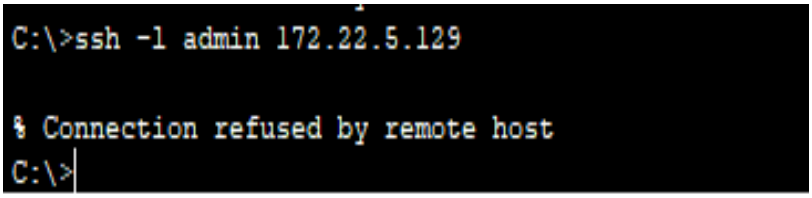


figure (27) access test from Vlan 2 to Janzur PC

8.2 Test with (SSH)



Figure(28) remotely management from Vlan 99 to Tajura



Figure(29) remotely management from Vlan 3 to Tajura

Note

When the remotely manage from Vlan 3 to any Router it will be denied because ACL permit from just VLAN99

8.3 Test from Vlan 3 PC to DNS server .

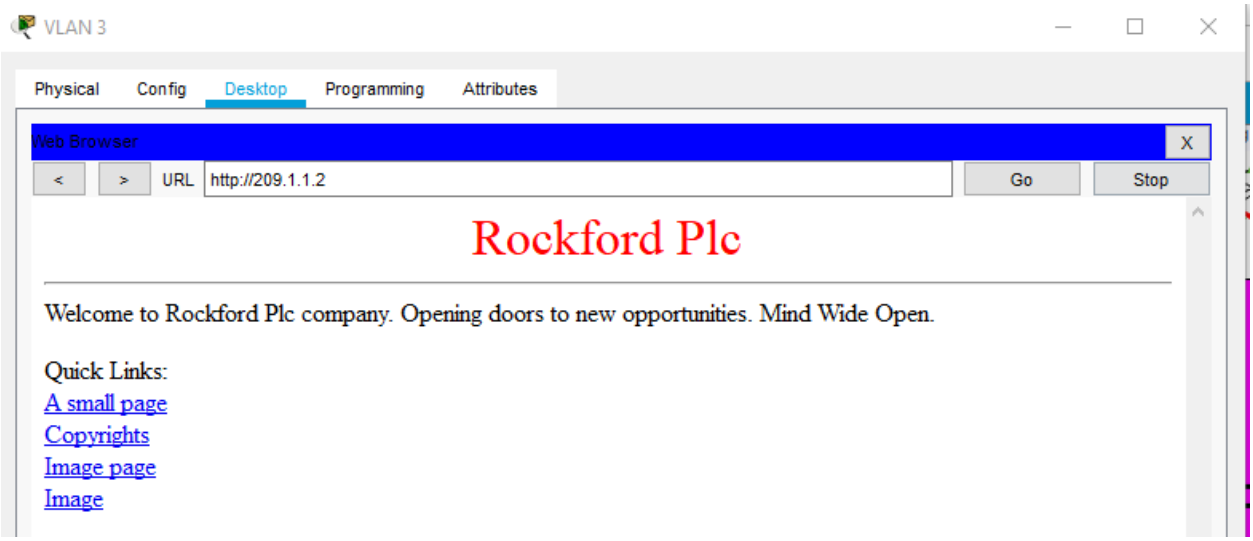


Figure (30) test to DNS server from Vlan 3

Note

Also when shutdown the LAN interface for (R-Tripoli2/Active) , the Network is working without any problem , because (R-Tripoli1) transition from standby to Active state and had become forwarding data over Network

8.4 Verification (show standby brief in Tripoli 2 to make Shure its Active router)

```
Tripoli2#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby
Virtual IP
Gig         1    150 P Active   local           172.22.0.3
172.22.0.1
Gig         1    150 P Active   local           172.22.2.3
172.22.2.1
Gig         1    150 P Active   local           172.22.3.3
172.22.3.1
Tripoli2#
```

Figure(31) show standby brief

8.5 Verification (show ip route to know routing table in Janzur router)

```
Janzur#sh 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 172.22.5.198 to network 0.0.0.0

     10.0.0.0/30 is subnetted, 2 subnets
O       10.4.0.0/30 [110/129] via 172.22.5.198, 00:39:37, Serial0/0/0
O       10.4.0.4/30 [110/128] via 172.22.5.198, 00:40:07, Serial0/0/0
     172.22.0.0/16 is variably subnetted, 13 subnets, 6 masks
O       172.22.0.0/23 [110/65] via 172.22.5.198, 00:39:37,
Serial0/0/0
O       172.22.2.0/24 [110/65] via 172.22.5.198, 00:39:37,
Serial0/0/0
O       172.22.3.0/28 [110/65] via 172.22.5.198, 00:39:37,
Serial0/0/0
C       172.22.4.0/24 is directly connected, GigabitEthernet0/0
L       172.22.4.1/32 is directly connected, GigabitEthernet0/0
O       172.22.5.0/26 [110/65] via 172.22.5.193, 00:40:12,
Serial0/0/1
O       172.22.5.64/26 [110/65] via 172.22.5.193, 00:40:12,
Serial0/0/1
O       172.22.5.128/26 [110/129] via 172.22.5.198, 00:40:07,
Serial0/0/0
C       172.22.5.192/30 is directly connected, Serial0/0/1
L       172.22.5.194/32 is directly connected, Serial0/0/1
C       172.22.5.196/30 is directly connected, Serial0/0/0
L       172.22.5.197/32 is directly connected, Serial0/0/0
O       172.22.5.200/30 [110/128] via 172.22.5.198, 00:40:07,
Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.22.5.198, 00:40:07, Serial0/0/0

Janzur#
```

Figure(32) Show ip route

References :

- Eng. Haider Swaih ppt slides