Final CCNA Lab Project

Enterprise Network Design & Implementation

Prepared by: Marwan Adel

Project Idea

connecting three company branches through a secure and segmented network using **Routing, Switching, VLANs, WAN, Security, and Network Services**.

Branches:

- **Headquarters (HQ):** Cairo, Egypt
- **Branch 1:** Jeddah, Saudi Arabia
- **Branch 2:** Riyadh, Saudi Arabia

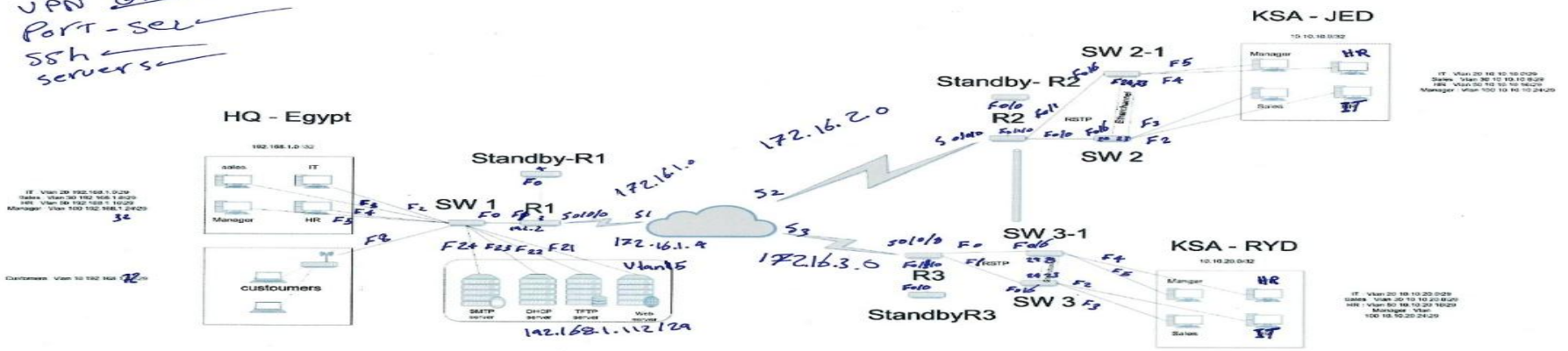
Topology:

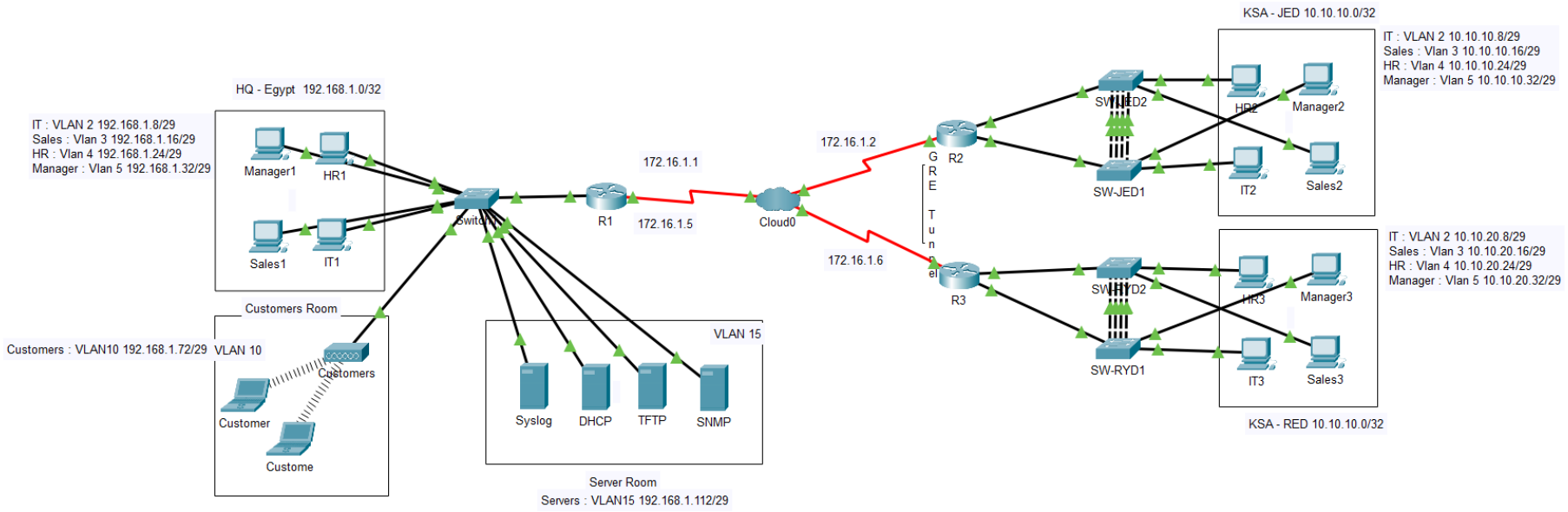
Network Design and Planning

At the beginning, I used draw.io to design and plan the network topology for my final lab. This step was very important for several reasons:

1. **Simplifying the design process: Having a clear topology diagram helped me visualize the entire network (HQ, branches, routers, and switches).**
2. **Interface mapping: The diagram allowed me to easily identify which interfaces should be connected to specific devices, reducing configuration errors.**
3. **Subnetting and VLAN planning: It made it easier to allocate IP addresses and assign VLANs to different departments.**
4. **Clear overall view: By drawing the complete network before implementing it on Cisco Packet Tracer, I saved time and effort during the configuration phase.**

Vlans
inter vlan
DHCP
Routing: RIP
Wan:
VPN Gre
Port-Sec
SSH
servers





What Has Been Implemented

- Configurationللـ Switches & Routers.
- إنشاءVLANs + Inter-VLAN Routing
- DHCPلتوزيع الـIP.
- Routingباستخدام RIP v2.
- WAN Connectionعن طريق Frame Relay لربط الفروع.
- Securityباستخدام Access-Lists +Port Security + SSH.
- تشغيل السيرفرات (DHCP, TFTP, Syslog, SNMP).
- Backupللـ Configurations لكل Router على TFTP Server.

◆ Network Summary

Device	Hostname	Role	Main Configurations / Services
Router 1	R1	HQ Router (Cairo)	Sub-Interfaces (VLAN 2,3,4,5,10,15) – DHCP – ACLs – SSH – RIP – SNMP – Syslog – TFTP Backup – Frame Relay
Router 2	R2	Branch Router (Jeddah)	Sub-Interfaces – DHCP – SSH – RIP – SNMP – Syslog – TFTP Backup – Frame Relay
Router 3	R3	Branch Router (Riyadh)	Sub-Interfaces – DHCP – SSH – RIP – SNMP – Syslog – TFTP Backup – Frame Relay
Switch 1	SW-1	HQ Switch	VLANs (2,3,4,5,10,15) – Port Security – Trunk
Switch 2	SW-2	Branch Switch	VLANs + Access Ports – Port Security – Trunk
Switch 3	SW-3	Branch Switch	VLANs + Access Ports – Port Security – Trunk
Server 1	TFTP	Backup Server	Stores router configurations
Server 2	Syslog	Logging Server	Receives and stores logs from routers
Server 3	SNMP	Monitoring Server	Network monitoring via SNMP
Frame Relay	CLOUD	WAN Connectivity	Provides inter-branch connection (Cairo ↔ Jeddah ↔ Riyadh)

Configuration Steps

◆ SW-1 Configuration

تغيير الـHostname

```
Switch> enable
Switch# configure terminal
Switch(config)# hostname SW-1
```

إنشاء الـVLANs

```
SW-1(config)# vlan 2
SW-1(config-vlan)# vlan 3
SW-1(config-vlan)# vlan 4
SW-1(config-vlan)# vlan 5
SW-1(config-vlan)# vlan 10
SW-1(config-vlan)# vlan 15
```

تخصيص الـ Ports لكلVLAN

Port F0/2 → VLAN 2 (IT)

Port F0/3 → VLAN 3 (Sales)

Port F0/4 → VLAN 4 (HR)

Port F0/5 → VLAN 5 (Manager)

Port F0/8 → VLAN 10 (Customers)

Ports F0/21 – F0/24 → VLAN 15 (Servers)

```
SW-1(config)# interface f0/2
SW-1(config-if)# switchport access vlan 2
SW-1(config-if)# switchport mode access

SW-1(config)# interface f0/3
SW-1(config-if)# switchport access vlan 3
SW-1(config-if)# switchport mode access

SW-1(config)# interface f0/4
SW-1(config-if)# switchport access vlan 4
SW-1(config-if)# switchport mode access

SW-1(config)# interface f0/5
SW-1(config-if)# switchport access vlan 5
SW-1(config-if)# switchport mode access

SW-1(config)# interface f0/8
SW-1(config-if)# switchport access vlan 10
SW-1(config-if)# switchport mode access

SW-1(config)# interface range f0/21-24
SW-1(config-if-range)# switchport access vlan 15
```

```
SW-1(config-if-range)# switchport mode access
```

◆ تفعيل الـ Trunk Port للاتصال بالراوتر R1

```
SW-1(config)# interface f0/1
SW-1(config-if)# switchport mode trunk
```

◆ Note

"In this step, we configured VLANs on switch SW-1 and assigned the appropriate interfaces for each department, in addition to configuring the trunk port towards Router R1."

```
SW-1#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/6, Fa0/7, Fa0/9, Fa0/10
                                                 Fa0/11, Fa0/12, Fa0/13,
Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17,
Fa0/18
                                                 Fa0/19, Fa0/20, Gig0/1,
Gig0/2
2    VLAN0002                          active    Fa0/2
3    VLAN0003                          active    Fa0/3
4    VLAN0004                          active    Fa0/4
5    VLAN0005                          active    Fa0/5
10   VLAN0010                          active    Fa0/8
15   VLAN0015                          active    Fa0/21, Fa0/22, Fa0/23,
Fa0/24
```

◆ تفعيل Port Security على SW-1

الغرض: منع توصيل أكثر من جهاز على نفس البورت مثلاً مستخدم يركب Hub/Switch صغير ويخلي أكتر من جهاز يدخل على الشبكة كمان بنخلي البورت يتعلم الـ MAC Address أوتوماتيك (sticky) ويغلق نفسه (shutdown) لو حصلViolation

Configuration

على بورت F0/3 (Sales)

```
SW-1(config)# interface f0/3
SW-1(config-if)# switchport port-security
SW-1(config-if)# switchport port-security maximum 1
SW-1(config-if)# switchport port-security violation shutdown
SW-1(config-if)# switchport port-security mac-address sticky
```

على بورت F0/4 (HR)

```
SW-1(config)# interface f0/4
SW-1(config-if)# switchport port-security
SW-1(config-if)# switchport port-security maximum 1
SW-1(config-if)# switchport port-security violation shutdown
SW-1(config-if)# switchport port-security mac-address sticky
```

على بورت F0/5 (Manager)

```
SW-1(config)# interface f0/5
SW-1(config-if)# switchport port-security
SW-1(config-if)# switchport port-security maximum 1
SW-1(config-if)# switchport port-security violation shutdown
```

SW-1(config-if)# switchport port-security mac-address sticky

على منافذ السيرفراتF0/21 – F0/24

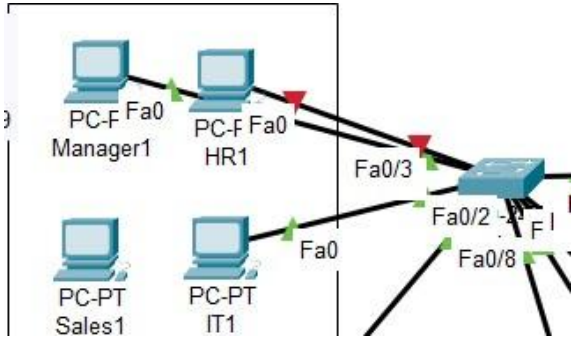
SW-1(config)# interface range f0/21-24
SW-1(config-if-range)# switchport port-security
SW-1(config-if-range)# switchport port-security maximum 1
SW-1(config-if-range)# switchport port-security violation shutdown
SW-1(config-if-range)# switchport port-security mac-address sticky

Explanation:

- تم تفعيل **Port Security** على البورتات المخصصة (F0/2-F0/5) ولبورتات السيرفرات.(F0/21-F0/24)
- كل بورت يسمح **بجهاز واحد فقط،** ويتعلم عنوان MAC تلقائيًا ويخزنه في الـ.(sticky) running-config
- في حالة أي انتهاك(Violation) ، البورت يتوقف تلقائيًا.(shutdown)

◆ Note

"To enhance security, port-security was configured on all access ports to allow only one device per port. The MAC address of the connected device is learned dynamically (sticky) and saved in the running configuration. If any violation occurs (e.g., an unauthorized device is connected), the port will automatically shut down to prevent unauthorized access."



◆ **Router Basic Security (R1)**

Configuration

1. تغيير الـ **Hostname:**

```
Router> enable
Router# configure terminal
Router(config)# hostname R1
```

2. إضافة **Enable Password** عشان الدخول لـprivilege mode

```
R1(config)# enable password 0236
```

3. حماية الـ **Console Line:**

```
R1(config)# line console 0
R1(config-line)# password asd
R1(config-line)# login
```

4. حماية الـ **VTY (Telnet) Lines:**

```
R1(config)# line vty 0 4
R1(config-line)# password qwe
R1(config-line)# login
```

6. تفعيل (**Service Password Encryption** لتشفير كل الباسوردات في الـ:(config

```
R1(config)# service password-encryption
```

◆ Note

"On router R1, basic security was applied by setting an enable password, configuring console and VTY line access with authentication, and creating a local user account. Additionally, the service password-encryption command was enabled to ensure that all passwords are stored in encrypted format in the running configuration."

```
User Access Verification

Password:
Password:
Password:

R1>ena
Password:
R1#
```

◆ **Router-on-a-Stick (Inter-VLAN Routing) – R1**

Configuration

1. تفعيل الـPhysical Interface:

```
R1(config)# interface fastEthernet 0/0
R1(config-if)# no shutdown
R1(config-if)# no ip address
```

2. إنشاء الـSub-Interfaces وربط كل واحدة بـ VLAN ID معين+IP Address

```
R1(config)# interface fastEthernet 0/0.2
R1(config-subif)# encapsulation dot1Q 2
R1(config-subif)# ip address 192.168.1.9 255.255.255.248
```

```
R1(config)# interface fastEthernet 0/0.3
R1(config-subif)# encapsulation dot1Q 3
R1(config-subif)# ip address 192.168.1.17 255.255.255.248

R1(config)# interface fastEthernet 0/0.4
R1(config-subif)# encapsulation dot1Q 4
R1(config-subif)# ip address 192.168.1.25 255.255.255.248

R1(config)# interface fastEthernet 0/0.5
R1(config-subif)# encapsulation dot1Q 5
R1(config-subif)# ip address 192.168.1.33 255.255.255.248

R1(config)# interface fastEthernet 0/0.10
R1(config-subif)# encapsulation dot1Q 10
R1(config-subif)# ip address 192.168.1.73 255.255.255.248

R1(config)# interface fastEthernet 0/0.15
R1(config-subif)# encapsulation dot1Q 15
R1(config-subif)# ip address 192.168.1.113 255.255.255.248
```

◆ Note

"On router R1, a Router-on-a-Stick configuration was implemented. Sub-interfaces were created for each VLAN, and an IP address was assigned as the default gateway for each subnet. This allows devices from different VLANs to communicate with each other through inter-VLAN routing."

```
R1#sh ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES NVRAM  up                    up
FastEthernet0/0.2      192.168.1.9     YES manual up                    up
FastEthernet0/0.3      192.168.1.17    YES manual up                    up
FastEthernet0/0.4      192.168.1.25    YES manual up                    up
FastEthernet0/0.5      192.168.1.33    YES manual up                    up
FastEthernet0/0.10     192.168.1.73    YES manual up                    up
FastEthernet0/0.15     192.168.1.113   YES manual up                    up
FastEthernet0/1        unassigned      YES NVRAM  up                    down
Serial0/0/0            unassigned      YES manual up                    up
Serial0/0/0.2          172.16.1.1      YES manual up                    up
Serial0/0/0.3          172.16.1.5      YES manual up                    up
Serial0/0/1            unassigned      YES NVRAM  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
```

◆ **DHCP Configuration – R1**

- **VLAN 2:**

  R1(config)# ip dhcp pool vlan2

  R1(dhcp-config)# network 192.168.1.8 255.255.255.248

  R1(dhcp-config)# default-router 192.168.1.9

  R1(dhcp-config)# dns-server 8.8.8.8

- **VLAN 3:**
  R1(config)# ip dhcp pool vlan3
  R1(dhcp-config)# network 192.168.1.16 255.255.255.248
  R1(dhcp-config)# default-router 192.168.1.17
  R1(dhcp-config)# dns-server 8.8.8.8
- **VLAN 4:**
  R1(config)# ip dhcp pool vlan4
  R1(dhcp-config)# network 192.168.1.24 255.255.255.248
  R1(dhcp-config)# default-router 192.168.1.25
  R1(dhcp-config)# dns-server 8.8.8.8
- **VLAN 5:**
  R1(config)# ip dhcp pool vlan5
  R1(dhcp-config)# network 192.168.1.32 255.255.255.248
  R1(dhcp-config)# default-router 192.168.1.33
  R1(dhcp-config)# dns-server 8.8.8.8
- **VLAN 10:**
  R1(config)# ip dhcp pool vlan10
  R1(dhcp-config)# network 192.168.1.72 255.255.255.248
  R1(dhcp-config)# default-router 192.168.1.73
  R1(dhcp-config)# dns-server 8.8.8.8
- **VLAN 15:**
  R1(config)# ip dhcp pool vlan15
  R1(dhcp-config)# network 192.168.1.112 255.255.255.248
  R1(dhcp-config)# default-router 192.168.1.113

◆ Note

"DHCP pools were configured on R1 for each VLAN to dynamically assign IP addresses to client devices. Each pool specifies the network, default gateway, and DNS server, allowing hosts to obtain the correct IP configuration automatically."

```
R1(config-subif)#do sh ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
192.168.1.10     0005.5EB4.51A2           --                     Automatic
192.168.1.18     00D0.FF4E.61D4           --                     Automatic
192.168.1.26     0001.9686.4C12           --                     Automatic
192.168.1.34     0030.F264.4D76           --                     Automatic
192.168.1.74     0001.9742.CA04           --                     Automatic
192.168.1.75     0006.2A2C.D24D           --                     Automatic
192.168.1.114    0002.160B.C088           --                     Automatic
192.168.1.116    0060.7097.B358           --                     Automatic
192.168.1.117    00D0.972A.A9DA           --                     Automatic
192.168.1.115    0010.1181.3443           --                     Automatic
R1(config-subif)#
```

◆ RIP Routing Configuration – R1

Configuration Commands:

```
R1(config)# router rip
R1(config-router)# version 2
R1(config-router)# network 192.168.1.0
R1(config-router)# no auto-summary
```

Explanation:

1. **router rip** لتفعيل بروتوكول RIP على الراوتر.
2. **version 2** يستخدمRIP v2 ، يدعم Subnet Mask Classless ضروري للشبكات غير الـClassful
3. **network 192.168.1.0** يعلن الشبكة 192.168.1.0 وجميع الـ subnets التابعة لها ضمن تحديثات.RIP
4. **no auto-summary** يمنع تجميع الشبكات (Automatic Summarization) ويضمن أن كل Subnet يعلن على حدة، وهو مهم مع الـ /29 subnets

◆ Note

"RIP version 2 was configured on R1 to enable dynamic routing between subnets. The no auto-summary command ensures proper advertisement of all subnets without summarization, allowing correct inter-VLAN and WAN connectivity."

◆ Note:

"The same configurations implemented on R1, including Router-on-a-Stick for inter-VLAN routing, DHCP pools for each VLAN, RIP version 2 dynamic routing, and basic security settings, were also applied on the branch routers in Jeddah (R2) and Riyadh (R3), along with their connected switches. This ensures consistent VLAN segmentation, IP address allocation, and routing across all sites."

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, 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 not set

     10.0.0.0/29 is subnetted, 8 subnets
R       10.10.10.8 [120/1] via 172.16.1.2, 00:00:04, Serial0/0/0.2
R       10.10.10.16 [120/1] via 172.16.1.2, 00:00:04, Serial0/0/0.2
R       10.10.10.24 [120/1] via 172.16.1.2, 00:00:04, Serial0/0/0.2
R       10.10.10.32 [120/1] via 172.16.1.2, 00:00:04, Serial0/0/0.2
R       10.10.20.8 [120/1] via 172.16.1.6, 00:00:29, Serial0/0/0.3
R       10.10.20.16 [120/1] via 172.16.1.6, 00:00:29, Serial0/0/0.3
R       10.10.20.24 [120/1] via 172.16.1.6, 00:00:29, Serial0/0/0.3
R       10.10.20.32 [120/1] via 172.16.1.6, 00:00:29, Serial0/0/0.3
     172.16.0.0/30 is subnetted, 2 subnets
C       172.16.1.0 is directly connected, Serial0/0/0.2
C       172.16.1.4 is directly connected, Serial0/0/0.3
     192.168.1.0/29 is subnetted, 6 subnets
C       192.168.1.8 is directly connected, FastEthernet0/0.2
C       192.168.1.16 is directly connected, FastEthernet0/0.3
C       192.168.1.24 is directly connected, FastEthernet0/0.4
C       192.168.1.32 is directly connected, FastEthernet0/0.5
C       192.168.1.72 is directly connected, FastEthernet0/0.10
```

◆ Advice

When working on a large-scale project or a Final CCNA Lab, it’s always better to complete all Router and Switch configurations for each branch first (VLANs, Inter-VLAN Routing, DHCP, Security, etc.).
After that, move on to configuring the WAN and interconnecting the branches.

This approach keeps the work organized and makes troubleshooting much easier, since you ensure that each branch is fully functional internally before integrating it with the others.

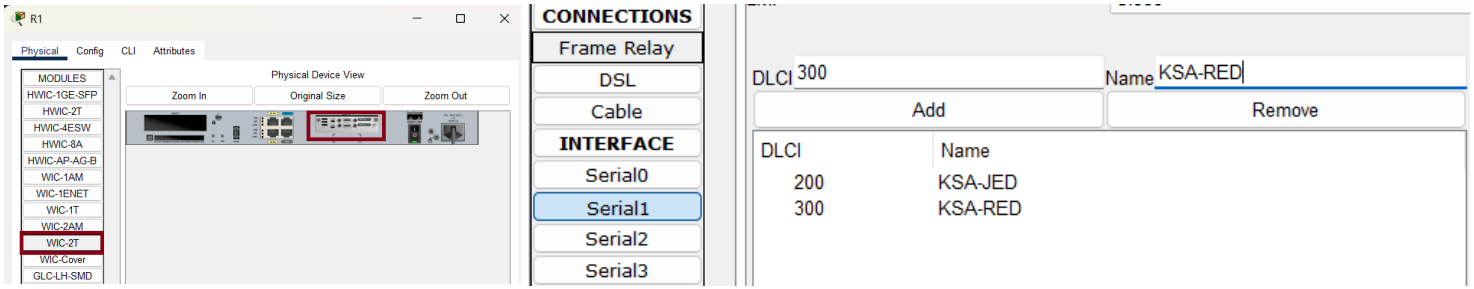
◆ WAN Connectivity

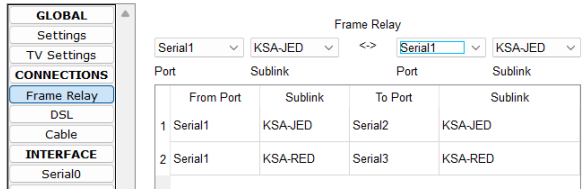
WAN Setup in Packet Tracer:

***"The Frame Relay cloud in the lab was configured first by:**

1. **Opening the Cloud and selecting Frame Relay as the connection type.**
2. **Adding the appropriate DLCIs for each point-to-point connection.**

After that, each branch router and HQ router was configured with a WIC-2T module to enable serial connectivity, allowing the DCE/DTE cables to be connected correctly. This setup ensures that each router can communicate over the Frame Relay WAN with the correct timing and IP addressing for RIP routing."*





◆ **Frame Relay Configuration (R1)**

Configuration Commands:

```
R1(config)# interface s0/0/0.2 point-to-point
R1(config-subif)# ip address 172.16.1.1 255.255.255.252
R1(config-subif)# frame-relay interface-dlci 200

R1(config)# interface s0/0/0.3 point-to-point
R1(config-subif)# ip address 172.16.1.5 255.255.255.252
R1(config-subif)# frame-relay interface-dlci 300
```

Explanation:

1. **Sub-Interfaces S0/0/0.2 & S0/0/0.3** لإنشاء خطوط WAN Point-to-Point لكل فرع.(Jeddah & Riyadh)
2. **IP Address** تم تخصيص /30 لكل رابط لضمان التواصل بين الراوترات فقط.
3. **frame-relay interface-dlci** ربط كل Sub-Interface بالـ DLCI الخاص بالفرع المقابل.

◆ Note

"Frame Relay point-to-point sub-interfaces were configured on R1 to connect HQ with the Jeddah and Riyadh branches. Each sub-interface has a dedicated IP address and is mapped to its corresponding DLCI, enabling WAN communication and integration with RIP routing."

◆ WAN Connectivity – Frame Relay (R2 & R3)

Branch Routers Configuration:

R2 – Jeddah Branch:

```
R2(config)# interface s0/0/0
R2(config-if)# no shutdown
R2(config-if)# frame-relay interface-dlci 200
R2(config-if)# ip address 172.16.1.2 255.255.255.252
```

R3 – Riyadh Branch:

```
R3(config)# interface s0/0/0
R3(config-if)# no shutdown
R3(config-if)# frame-relay interface-dlci 300
R3(config-if)# ip address 172.16.1.6 255.255.255.252
```

Explanation:

- تم تفعيل (Serial)لكل راوتر فرعي.
- كل راوتر مربوط بـ **DLCI**المقابل للـ Sub-Interface في.(R1) HQ
- تم تخصيص IP /30 لكل رابط لضمان اتصال مباشر فقط بين الراوترات.

◆ Note

"The Jeddah (R2) and Riyadh (R3) branch routers were configured with Frame Relay interfaces, assigned DLCIs corresponding to their connections with HQ (R1). Each interface received a dedicated /30 IP address to enable WAN connectivity and RIP routing across the enterprise network."

◆ Site-to-Site Tunnel Configuration (R2 & R3)

R2 – Jeddah Branch:

```
R2(config)# interface tunnel 1
R2(config-if)# ip address 50.0.0.2 255.255.255.0
R2(config-if)# tunnel source s0/0/0
R2(config-if)# tunnel destination 172.16.1.6
```

R3 – Riyadh Branch:

```
R3(config)# interface tunnel 1
R3(config-if)# ip address 50.0.0.3 255.255.255.0
R3(config-if)# tunnel source s0/0/0
R3(config-if)# tunnel destination 172.16.1.1
```

Explanation:

- تم إنشاء **IP Tunnel** بين الفروع لتأمين الاتصال بين المواقع عبر شبكة الـ Frame Relay.
- كل Tunnel يستخدم الـ Serial Interface كمصدر (tunnel source) و IP وجهة الراوتر الآخر (tunnel destination).
- تم تخصيص **Subnet 50.0.0.0/24** للـ Tunnel Interfaces لتسهيل التوجيه بين الفروع.

```
     50.0.0.0/24 is subnetted, 1 subnets
C       50.0.0.0 is directly connected, Tunnel1
```

◆ Note

"Site-to-Site tunnels were configured on the branch routers to provide secure communication between Jeddah and Riyadh branches over the existing Frame Relay WAN. Each tunnel interface was assigned a unique IP address and mapped to the correct source and destination serial interfaces, allowing routing and data flow between remote sites."

◆ Access-Lists Configuration – R1

```
R1(config)#ip access-list extended Acl_IT
R1(config-ext-nacl)#permit ip 192.168.1.8 0.0.0.7 any

R1(config-ext-nacl)#ip access-list extended Acl_Sales
R1(config-ext-nacl)#permit ip 192.168.1.16 0.0.0.7 10.10.10.16 0.0.0.7
R1(config-ext-nacl)#permit ip 192.168.1.16 0.0.0.7 10.10.20.16 0.0.0.7
R1(config-ext-nacl)#permit ip 192.168.1.16 0.0.0.7 192.168.1.16 0.0.0.7
R1(config-ext-nacl)#deny ip 192.168.1.16 0.0.0.7 any

R1(config-ext-nacl)#ip access-list extended Acl_HR
R1(config-ext-nacl)#permit ip 192.168.1.24 0.0.0.7 192.168.1.24 0.0.0.7
R1(config-ext-nacl)#permit ip 192.168.1.24 0.0.0.7 10.10.10.24 0.0.0.7
R1(config-ext-nacl)#permit ip 192.168.1.24 0.0.0.7 10.10.20.24 0.0.0.7
R1(config-ext-nacl)#permit ip 192.168.1.24 0.0.0.7 192.168.1.16 0.0.0.7
R1(config-ext-nacl)#permit ip 192.168.1.24 0.0.0.7 10.10.10.16 0.0.0.7
R1(config-ext-nacl)#permit ip 192.168.1.24 0.0.0.7 10.10.20.16 0.0.0.7
R1(config-ext-nacl)#deny ip 192.168.1.24 0.0.0.7 any

R1(config-ext-nacl)#ip access-list extended Acl_Manager
R1(config-ext-nacl)#permit ip 192.168.1.32 0.0.0.7 192.168.1.32 0.0.0.7
R1(config-ext-nacl)#permit ip 192.168.1.32 0.0.0.7 192.168.1.24 0.0.0.7
R1(config-ext-nacl)#permit ip 192.168.1.32 0.0.0.7 192.168.1.16 0.0.0.7
R1(config-ext-nacl)#permit ip 192.168.1.32 0.0.0.7 10.10.10.16 0.0.0.7
R1(config-ext-nacl)#permit ip 192.168.1.32 0.0.0.7 10.10.10.24 0.0.0.7
R1(config-ext-nacl)#permit ip 192.168.1.32 0.0.0.7 10.10.10.32 0.0.0.7
R1(config-ext-nacl)#permit ip 192.168.1.32 0.0.0.7 10.10.20.16 0.0.0.7
```

```
R1(config-ext-nacl)#permit ip 192.168.1.32 0.0.0.7 10.10.20.24 0.0.0.7
R1(config-ext-nacl)#permit ip 192.168.1.32 0.0.0.7 10.10.20.32 0.0.0.7
R1(config-ext-nacl)#deny ip 192.168.1.32 0.0.0.7 any
R1(config-ext-nacl)#ip access-list extended Acl_Customer
R1(config-ext-nacl)#permit tcp 192.168.1.72 0.0.0.7 any eq 80
R1(config-ext-nacl)#deny ip 192.168.1.72 0.0.0.7 any
```

◆ Apply ACLs on Sub-Interfaces

```
R1(config)#int f0/0.2
R1(config-subif)#ip access-group Acl_IT in

R1(config-subif)#int f0/0.3
R1(config-subif)#ip access-group Acl_Sales in

R1(config-subif)#int f0/0.4
R1(config-subif)#ip access-group Acl_HR in

R1(config-subif)#int f0/0.5
R1(config-subif)#ip access-group Acl_Manager in

R1(config-subif)#int f0/0.10
R1(config-subif)#ip access-group Acl_Customer in
```

Explanation

"تم تطبيق الـ (Extended ACLs) على كل Sub-Interface في الراوتر R1 لكل VLAN لتطبيق سياسات الأمان. كل VLAN لها قواعد مخصصة حسب دورها:

- **VLAN IT** مسموح لها الوصول الكامل لكل الشبكات الداخلية والخارجية.
- **VLAN Sales** مسموح لها التواصل فقط مع شبكات Sales الأخرى في الفروع.
- **VLAN HR** مسموح لها التواصل مع HR و Sales فقط.
- **VLAN Manager** مسموح لها الوصول لكل الشبكات باستثناء VLAN IT.
- **VLAN Customer** مسموح له الوصول لها على الإنترنت عبر HTTP فقط.

◆ Note

"Based on organizational security policies, each VLAN was restricted according to its role: IT has full access, Sales communicates only with Sales across branches, HR can communicate with HR and Sales, Managers have access to all except IT, and Customers are limited to Internet access via HTTP. These rules were enforced using Extended ACLs applied on router R1 sub-interfaces."

Fire	Last Status	Source	Destination	Type	Color
	Failed	HR1	IT1	ICMP	
	Successful	IT1	Sales2	ICMP	
	Successful	HR1	HR2	ICMP	

◆ **EtherChannel Configuration (Jeddah & Riyadh Branches)**

Jeddah Branch:

```
SW-JED1(config)# interface range f0/21-24
SW-JED1(config-if-range)# switchport mode trunk
SW-JED1(config-if-range)# channel-group 1 mode active

SW-JED2(config)# interface range f0/21-24
SW-JED2(config-if-range)# switchport mode trunk
SW-JED2(config-if-range)# channel-group 1 mode passive
```

Riyadh Branch:

```
SW-RYD1(config)# interface range f0/21-24
SW-RYD1(config-if-range)# switchport mode trunk
SW-RYD1(config-if-range)# channel-group 1 mode active

SW-RYD2(config)# interface range f0/21-24
SW-RYD2(config-if-range)# switchport mode trunk
SW-RYD2(config-if-range)# channel-group 1 mode passive
```

Explanation:

- تم إنشاء EtherChannel بين السويتشات في كل فرع لتجميع البورتات وزيادة الـ (Bandwidth) وتحسين .(Redundancy)
- تم استخدام بروتوكول LACP مع وضع Active/Passive لتحقيق قناة افتراضية واحدة لكل زوج من السويتشات.

◆ Note:

"EtherChannel was configured on the access switches in both Jeddah and Riyadh branches to aggregate multiple physical links into a single logical link. LACP was used to ensure link Redundancy and load balancing between the connected switches, enhancing overall network performance and reliability."

```
SW-JED1#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------
+-----------------------------------------------

1      Po1(SU)           LACP   Fa0/21(P) Fa0/22(P) Fa0/23(P) Fa0/24(P)
```

◆ SSH Configuration – R1 (HQ Router)

R1(config)# ip domain-name final-lab.com
R1(config)# crypto key generate rsa
How many bits in the modulus [512]: 1024
R1(config)# username admin privilege 15 secret P@$$word123
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# do show ip ssh
SSH Enabled - version 1.99

Explanation:

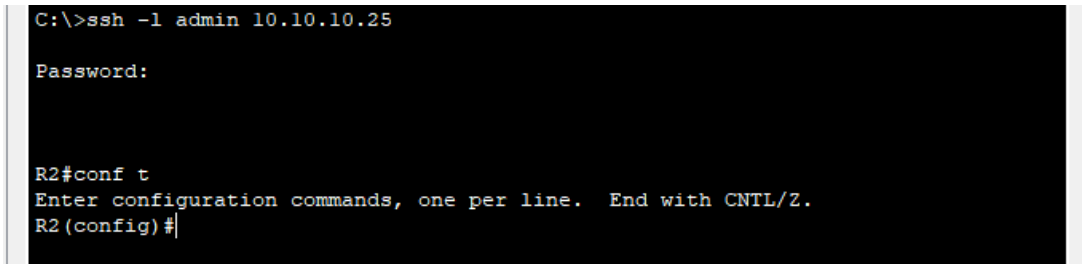
- تم تفعيل SSH على الراوتر R1 لتأمين الوصول عن بعد إلى الـ VTY بدلاً من Telnet غير الآمن.
- تم إنشاء مفتاح RSA بطول 1024 بت لتشفير جلسات SSH.
- تم إنشاء حساب مستخدم بصلاحيات كاملة (privilege 15) لتسجيل الدخول باستخدام SSH.
- الـ VTY lines تم إعدادها لاستخدام تسجيل الدخول المحلي فقط مع السماح ببروتوكول SSH فقط.

◆ Note

"SSH was configured on R1 to provide secure remote management access. A 1024-bit RSA key was generated, and a local admin user with full privileges was created. VTY lines were restricted to SSH access, ensuring encrypted and authenticated connections to the router."

◆ Note

"The same SSH configuration was applied on the branch routers R2 and R3 (Jeddah and Riyadh) to secure remote access. Each router had a local RSA key generated, a privileged user account created, and the VTY lines were configured to allow SSH only, just like on the main router R1."



◆ Configuration Backup & Syslog – R1, R2 & R3

R1 – HQ Router:

R1# copy running-config tftp:
Address or name of remote host []? 192.168.1.114
Destination filename [R1-confg]? R1-Backup.cfg
R1(config)# logging 192.168.1.117
R1(config)# logging trap debugging

Explanation:

- تم عمل نسخة احتياطية من الـ Running Configuration لكل راوتر على الـ TFTP Server لضمان سلامة الإعدادات.
- تم تمكين Syslog على جميع الراوترات لإرسال رسائل الـ Debugging إلى سيرفر مركزي، مما يسهل مراقبة أداء الشبكة والكشف عن أي مشاكل بشكل فوري.

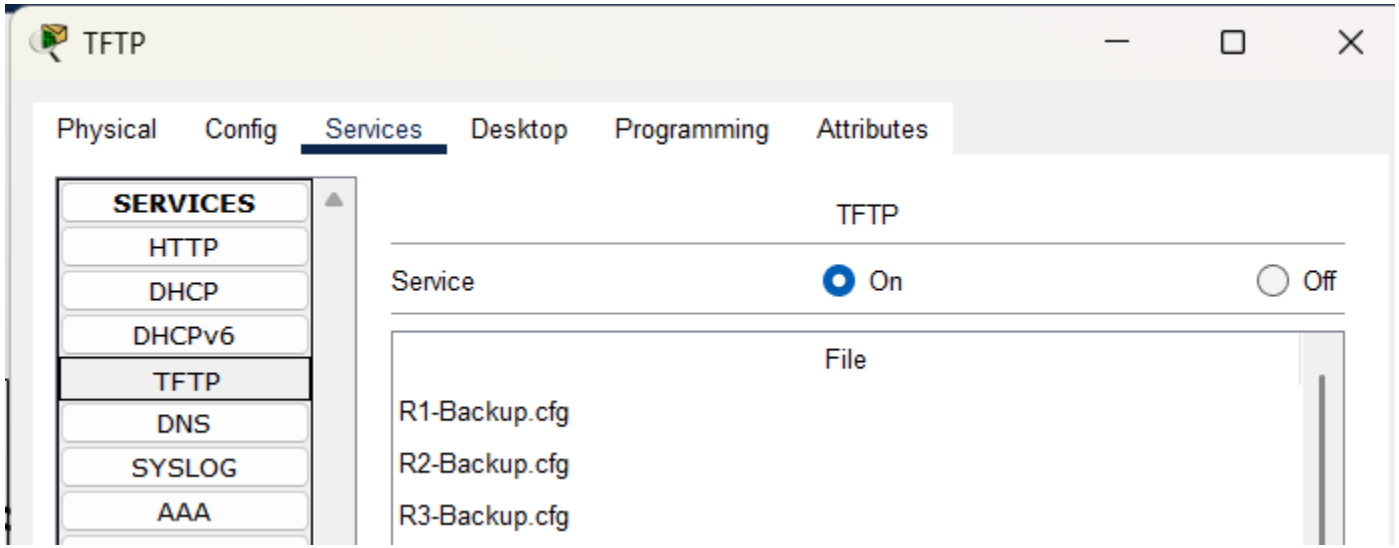
◆ Note

"All routers had their running configurations backed up to the TFTP server to ensure configuration safety. Additionally, syslog logging was enabled on each router to send debugging messages to the central syslog server, providing centralized monitoring and troubleshooting capabilities."

◆ Note

R2 & R3 – Branch Routers:

"The same steps were applied on the Jeddah branch router (R2) and the Riyadh branch router (R3) to back up their running configurations to the TFTP server and enable Syslog to send debugging messages to the central server for network monitoring and troubleshooting."




```
R2#show logg
R2#show logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited,
          0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.


No Inactive Message Discriminator.


    Console logging: level debugging, 10 messages logged, xml disabled,
          filtering disabled
    Monitor logging: level debugging, 10 messages logged, xml disabled,
          filtering disabled
    Buffer logging:  disabled, xml disabled,
          filtering disabled

    Logging Exception size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled

No active filter modules.

ESM: 0 messages dropped
    Trap logging: level debugging, 10 message lines logged
        Logging to 192.168.1.117  (udp port 514,  audit disabled,
              authentication disabled, encryption disabled, link up),
              10 message lines logged,
              0 message lines rate-limited,
```

◆ Testing & Verification

بعد الانتهاء من إعداد الشبكة، تم إجراء مجموعة من الاختبارات للتأكد من أن كل شيء يعمل بشكل صحيح:

1. **Connectivity Tests**
   - Pingبين فروع الشركة (HQ ↔ Jeddah ↔ Riyadh) للتأكد من نجاح الربط عبر الـ Frame Relay.
   - Pingبين الأجهزة داخل نفس الـ VLAN للتأكد من الـ Inter-VLAN Routing.
2. **Routing Verification**
   - `show ip route`أظهر أن كل الشبكات تم إضافتها من خلال بروتوكول RIP v2.
   - `show ip interface brief`للتأكد من أن جميع الواجهات مفعلة وبالعناوين الصحيحة.
3. **VLAN & Switch Configuration**
   - `show vlan brief`يوضح أن جميع الـ VLANs معرفة وتم ربطها بالمنافذ الصحيحة.
   - `show etherchannel summary`للتأكد من نجاح تجميع الـ Links بين السويتشات.
4. **Security Testing**
   - تجربة :Port Security توصيل جهاز غير مصرح به ← يتم إغلاق الـ Port تلقائيًا.
   - تجربة:ACLs
     - الـ Sales يمكنه الاتصال فقط بـ Sales.
     - الـ HR يمكنه الوصول لـ Sales وأجهزتهم.
     - الـ Customer لديه صلاحية HTTP فقط.
5. **Services Verification**
   - **TFTP**تم استخدام `copy running-config tftp:`لحفظ إعدادات الراوترات على السيرفر.
   - **Syslog**التحقق من تسجيل الأحداث Logs على السيرفر المركزي.
   - **SNMP**إعداد SNMP Community strings لتوفير المراقبة عبر NMS.

⬘ Executive Summary – Final CCNA Lab Project

This project demonstrates the design and implementation of a complete enterprise network connecting three company branches (Cairo HQ, Jeddah, and Riyadh). It includes LAN, WAN, security, redundancy, and network management services. Below is a summary of the main achievements.

Category	Key Achievements
Segmentation	Implemented VLANs for IT, Sales, HR, Managers, Customers, Servers. Router-on-a-Stick enabled Inter-VLAN routing. DHCP pools per VLAN for automated IP assignment.
Security	SSH for secure remote access (RSA keys). Extended ACLs enforcing department-specific policies. Port Security with sticky MAC & shutdown on violation. Password encryption for router access.
Redundancy & Performance	- EtherChannel (EtherChannel with LACP for link aggregation. Frame Relay WAN with site-to-site tunnels between Jeddah & Riyadh. Dynamic routing using RIP v2 with no auto-summary.
Monitoring & Management	- SNMP Server SNMP server for network monitoring. Syslog server for centralized logging. TFTP server for configuration backup. Connectivity & Security tests verified functionality

The project successfully integrates all CCNA topics into a practical enterprise environment, demonstrating a secure, scalable, and well-managed network design suitable for real-world deployment.