**Final Lab Project**

# Enterprise Network Design Implementation

Prepared by: Mohammed AJALA

# Project Idea

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

**Branches:**

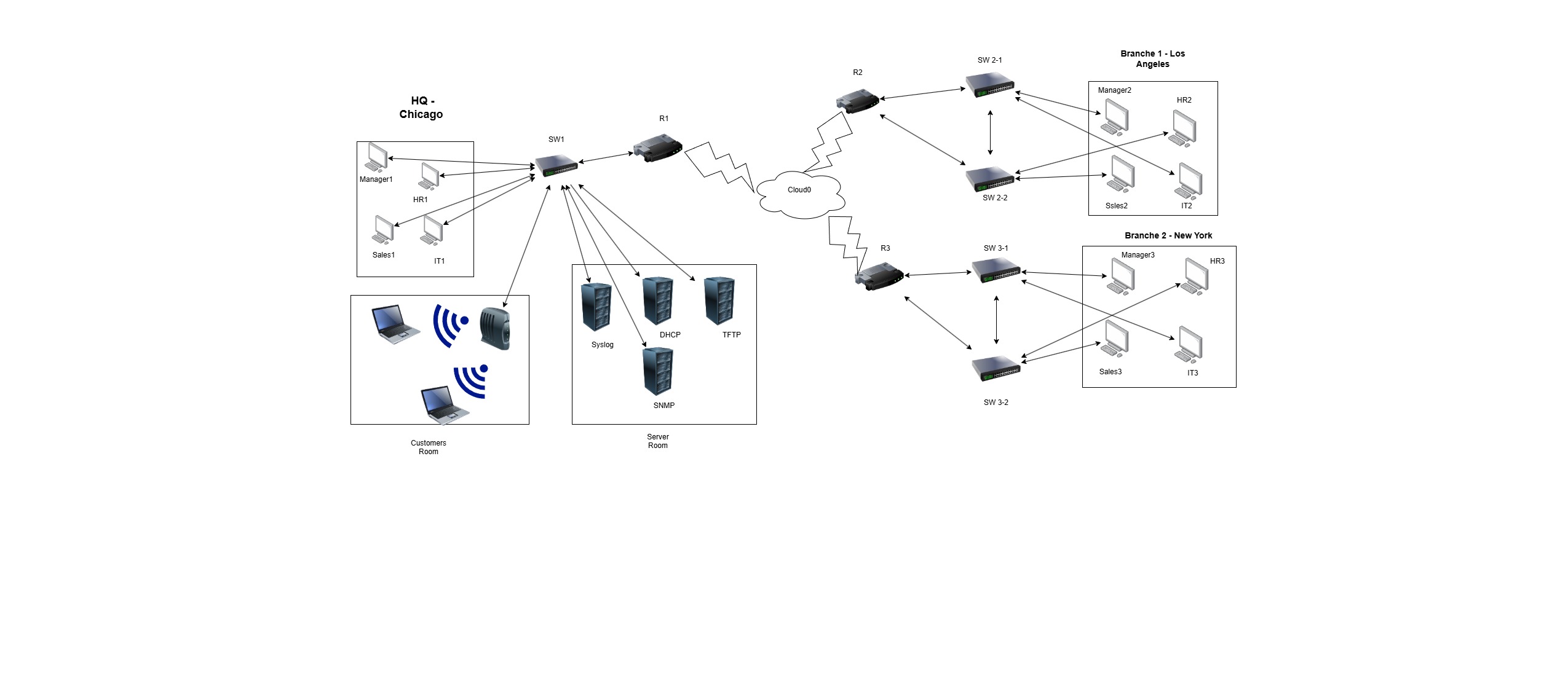
* **Headquarters (HQ):** Chicago, USA
  + **Branch 1:** Los Angeles, USA
  + **Branch 2:** New York, USA

**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.**



**What Has Been Implemented**

 **Configuration of Switches and Routers**

** Creating VLANs and Inter-VLAN Routing**

** DHCP for IP distribution**

** Routing using RIP v2**

** WAN Connection via Frame Relay to link the branches**

** Security using Access Lists, Port Security, and SSH**

** Running servers (DHCP, TFTP, Syslog, SNMP)**

** Backup of configurations for each router on a TFTP Server**

## 🔹 Network Summary

|  |  |  |  |
| --- | --- | --- | --- |
| **Device** | **Hostname** | **Role** | **Main Configurations / Services** |
| **Router 1** | R1 | HQ Router (Chicago) | Sub-Interfaces (VLAN 2,3,4,5,10,15) – DHCP – ACLs – SSH – RIP – SNMP –  Syslog – TFTP Backup – Frame Relay |
| **Router 2** | R2 | Branch Router  (LA) | Sub-Interfaces – DHCP – SSH – RIP – SNMP – Syslog – TFTP Backup – Frame  Relay |
| **Router 3** | R3 | Branch Router  (NYC) | 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 (Chicago ↔ LA ↔ NYC) |

**Configuration Steps**

🔹 **SW-1 Configuration**

**Changing Hostname**

Switch> enable

Switch# configure terminal

Switch(config)# hostname SW-1

**Creating VLANs**

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

**Assigning Ports to each VLAN:  
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

Enable the **trunk port** for connecting to **Router 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."**

A screenshot of a computer

AI-generated content may be incorrect.

**Enable Port Security on SW-1**

**Purpose:**  
Prevent connecting more than one device to the same port — for example, a user connecting a small hub/switch to allow more than one device to access the network.  
Also, configure the port to automatically learn the MAC address (sticky) and shut down if a violation occurs.

**Configuration:**

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

On port **F0/3 (Sales)**

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

On port **F0/4 (HR)**

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

On port **F0/5 (Manager)**

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

On **Server Ports F0/21 – F0/24**

**Explanation:**

* Port Security was enabled on the designated ports **(F0/2–F0/5)** and **server ports (F0/21–F0/24)**.
* Each port allows **only one device**, automatically learns the MAC address, and stores it in the **running-config** using **sticky**.
* If a **violation** occurs, the port will automatically **shut down**.

**Router Basic Security Configuration (R1)**

1️⃣ Change Hostname

Router> enable

Router# configure terminal

Router(config)# hostname R1

Description:  
The router hostname was changed from the default name to R1 for easier identification.

2️⃣ Set Enable Password (Privilege Mode Access)

R1(config)# enable password 0236

Description:  
An enable password was configured to secure privileged EXEC mode access.

3️⃣ Secure the Console Line

R1(config)# line console 0

R1(config-line)# password asd

R1(config-line)# login

Description:  
A console line password was set to control physical access to the router.

4️⃣ Secure the VTY (Telnet) Lines

R1(config)# line vty 0 4

R1(config-line)# password qwe

R1(config-line)# login

Description:  
VTY lines (0–4) were secured with a password to control remote Telnet access.

5️⃣ Enable Password Encryption

R1(config)# service password-encryption

Description:  
The service password-encryption command was enabled to encrypt all passwords in the configuration file.

**📝 Note:**

On router R1, basic security was applied by setting an enable password, configuring console and VTY line authentication, and enabling password encryption.  
This ensures that all passwords are stored in an encrypted format in the running configuration.

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

1️⃣ Enable the Physical Interface

R1(config)# interface gigabitEthernet 0/0

R1(config-if)# no shutdown

R1(config-if)# no ip address

Description:  
The GigabitEthernet 0/0 interface was activated and prepared for subinterface configuration.

2️⃣ Create Subinterfaces and Assign VLANs

Each VLAN is assigned a subinterface with a unique IP address to serve as the default gateway for that VLAN.

R1(config)# interface gigabitEthernet 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 gigabitEthernet 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 gigabitEthernet 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 gigabitEthernet 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 gigabitEthernet 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 gigabitEthernet 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.  
Subinterfaces were created for each VLAN, each assigned an IP address that serves as the default gateway.  
This configuration allows inter-VLAN communication, enabling devices on different VLANs to communicate through the router.

A screenshot of a computer program

AI-generated content may be incorrect.

**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

R1(dhcp-config)# dns-server 8.8.8.8

**📝 Note:**

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

**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**

1️⃣ router rip – Enables the RIP routing protocol on the router.  
2️⃣ version 2 – Activates RIP version 2, which supports classless routing (CIDR) and subnet masks, unlike version 1 which is classful.  
3️⃣ network 192.168.1.0 – Advertises the 192.168.1.0 network and all of its subnets within RIP updates.  
4️⃣ no auto-summary – Disables automatic route summarization to ensure that each subnet (/29) is advertised individually, allowing accurate routing between VLANs and networks.

**📝 Note:**

RIP version 2 was configured on R1 to enable dynamic routing between subnets.  
The no auto-summary command ensures that all subnets are properly advertised without being summarized, maintaining accurate inter-VLAN and WAN connectivity.

**📝 Additional 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 to the branch routers in LA (R2) and NYC (R3), along with their connected switches.  
This ensures consistent VLAN segmentation, IP address allocation, and routing across all sites.

