**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:**

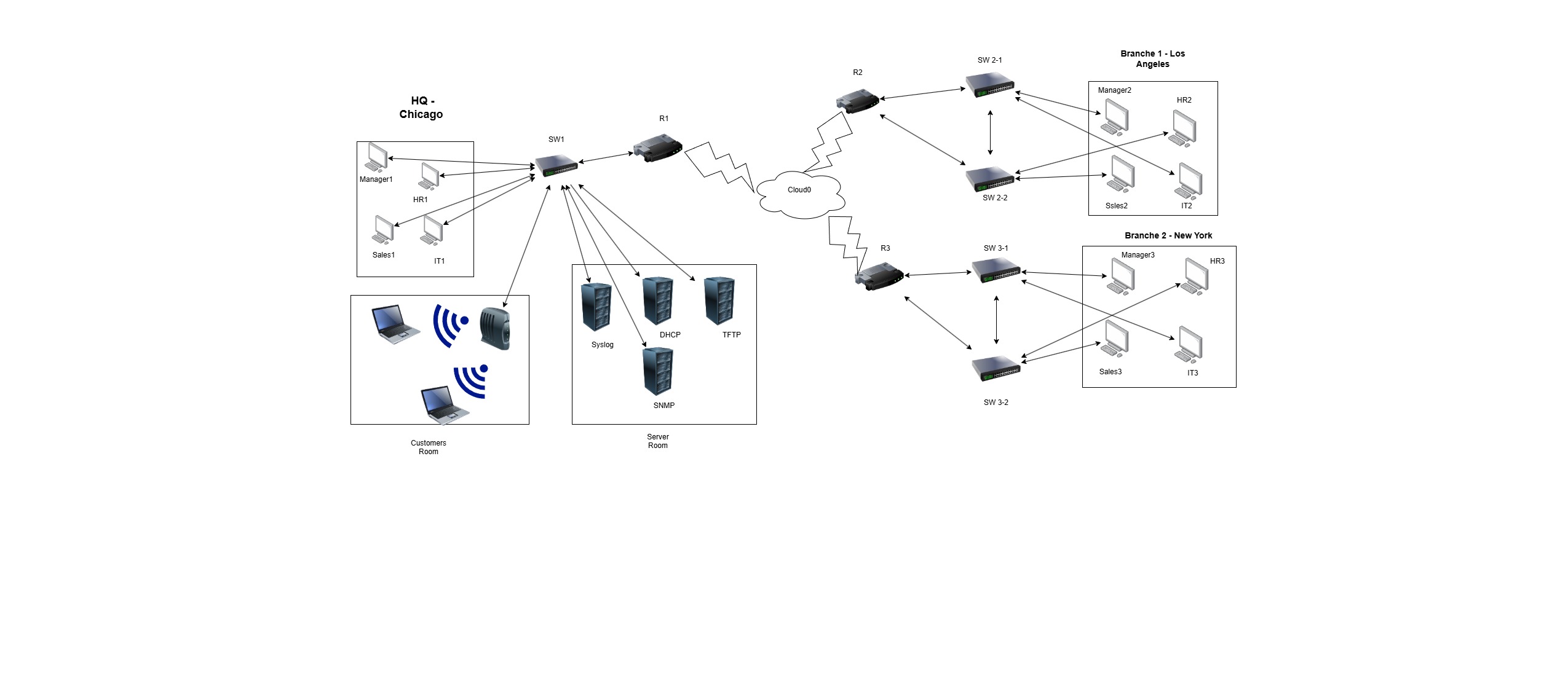
* **Headquarters (HQ):** Chicago, USA
  + **Branch 1:** Los Angeles, USA
  + **Branch 2:** New York, USA

**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**.