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:

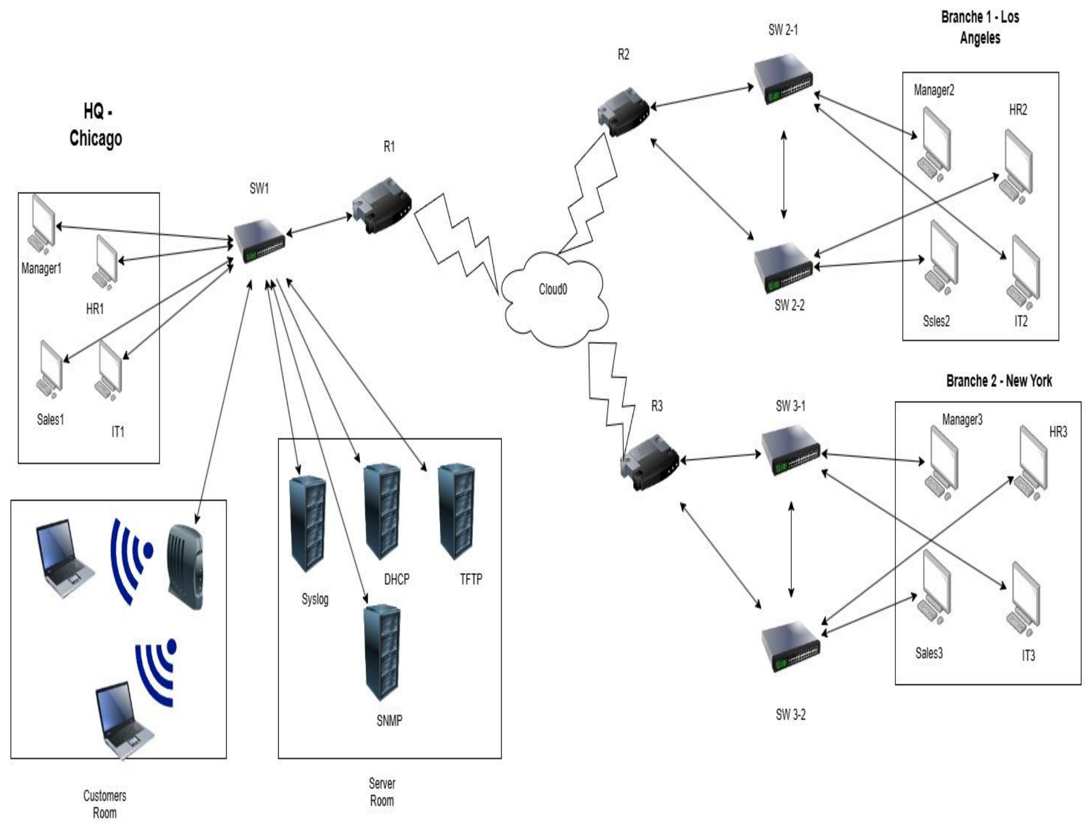
- **Headquarters (HQ):** Chicago, USA
- **Branch 1:** Los Angeles, USA
- **Branch 2:** New York, USA

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.**


HQ - Chicago
Manager1
HR1
Sales1
IT1
SW1
R1
Syslog
DHCP
TFTP
SNMP
Customers Room
Server Room
Cloud0
R2
SW 2-1
SW 2-2
Branche 1 - Los Angeles
Manager2
HR2
Ssles2
IT2
R3
SW 3-1
SW 3-2
Branche 2 - New York
Manager3
HR3
Sales3
IT3

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."

```
SW-1>en
SW-1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, 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, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, 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
```

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)

1 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.

---

2 Set Enable Password (Privilege Mode Access)
R1(config)# enable password 0236

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

---

3 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.

---

4 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.

---

5 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
1 Enable the Physical Interface
R1(config)# interface fastEthernet 0/0
R1(config-if)# no shutdown
R1(config-if)# no ip address

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

---

2 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 fastEthernet0/0.2
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. 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.

```
R1#sh ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES unset  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 unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
R1#
```

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

1 router rip – Enables the RIP routing protocol on the router.
2 version 2 – Activates RIP version 2, which supports classless routing (CIDR) and subnet masks, unlike version 1 which is classful.
3 network 192.168.1.0 – Advertises the 192.168.1.0 network and all of its subnets within RIP updates.
4 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 version2 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.

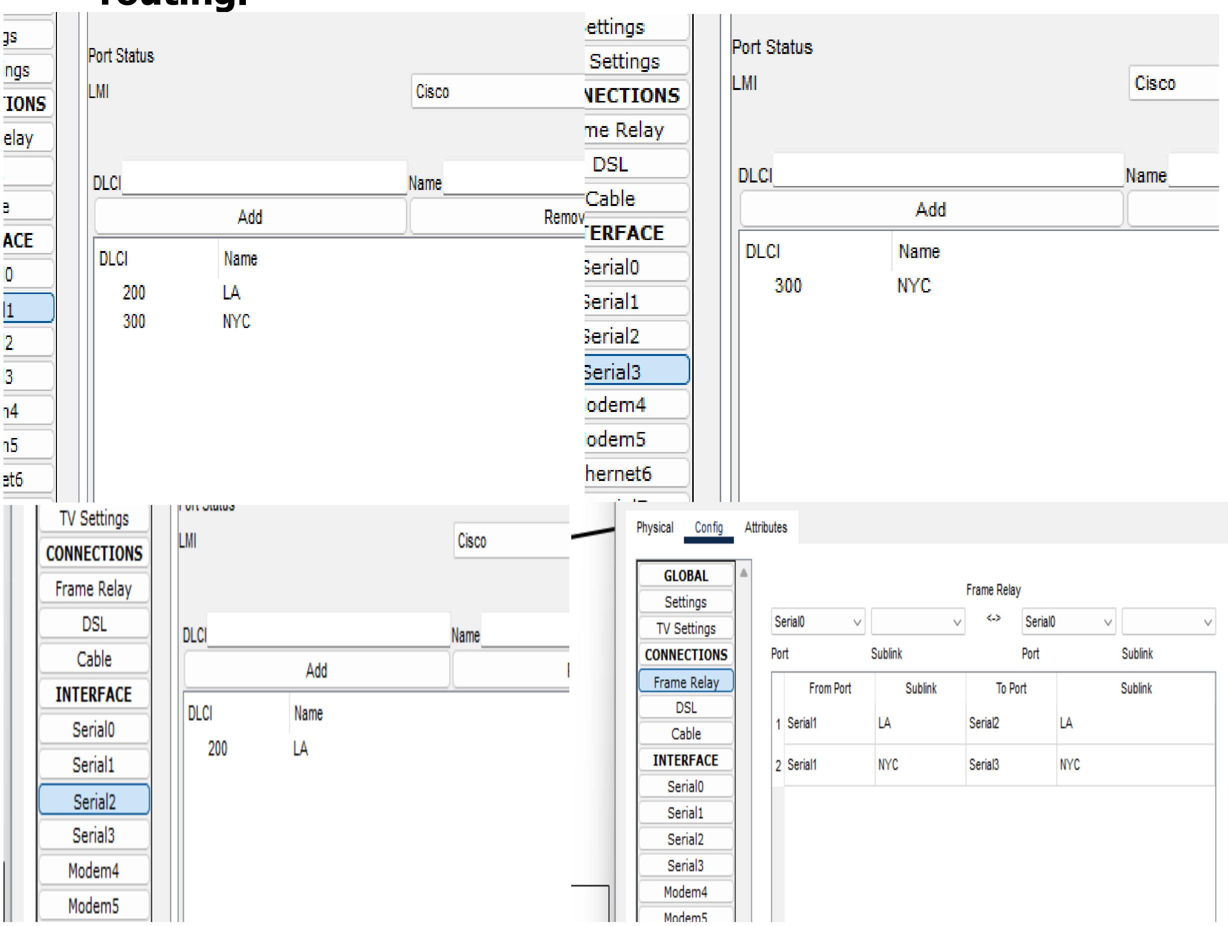
```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       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 not set

     192.168.1.0/24 is variably subnetted, 12 subnets, 2 masks
C       192.168.1.8/29 is directly connected, GigabitEthernet0/0/0.2
L       192.168.1.9/32 is directly connected, GigabitEthernet0/0/0.2
C       192.168.1.16/29 is directly connected, GigabitEthernet0/0/0.3
L       192.168.1.17/32 is directly connected, GigabitEthernet0/0/0.3
C       192.168.1.24/29 is directly connected, GigabitEthernet0/0/0.4
L       192.168.1.25/32 is directly connected, GigabitEthernet0/0/0.4
C       192.168.1.32/29 is directly connected, GigabitEthernet0/0/0.5
L       192.168.1.33/32 is directly connected, GigabitEthernet0/0/0.5
C       192.168.1.72/29 is directly connected, GigabitEthernet0/0/0.10
L       192.168.1.73/32 is directly connected, GigabitEthernet0/0/0.10
C       192.168.1.112/29 is directly connected, GigabitEthernet0/0/0.15
L       192.168.1.113/32 is directly connected, GigabitEthernet0/0/0.15
```

**WAN Connectivity

- **WAN Setup in Packet Tracer:**
- ***"The Frame Relay cloud in the lab was configured first by:**
- **Opening the Cloud and selecting Frame Relay as the connection type.**
- **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 (HQ Router)
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

- Two point-to-point Frame Relay sub-interfaces were configured on R1: **S0/0/0.2** for the **LA branch** and **S0/0/0.3** for the **NYC branch**.
- Each link uses a dedicated **/30 subnet** for router-to-router communication.
- Each sub-interface is mapped to the correct **DLCI** for proper WAN connectivity.

Note

"Frame Relay point-to-point sub-interfaces were configured on R1 to connect HQ with the LA and NYC branches. Each interface has its own IP address and matching DLCI, enabling WAN communication and RIP routing."

◈ Branch Routers – Frame Relay Configuration (R2 & R3)
R2 – LA 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 – NYC 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

- Serial interfaces on LA and NYC routers were enabled.
- Each branch router uses the DLCI assigned by the HQ router (R1).
- /30 IP addressing ensures simple, point-to-point WAN links.

Note

"The LA (R2) and NYC (R3) branch routers were configured with Frame Relay DLCIs that map to their HQ connection. The /30 addressing provides efficient routing and reliable WAN operation with RIP."

🔷 **Site-to-Site Tunnel Configuration (R2 ↔ R3)**

R2 – LA

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 – NYC

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

- A GRE tunnel connects the LA and NYC branches.
- The **serial interface** is used as the tunnel source.
- Each router points the tunnel destination to the **remote serial IP**.
- The tunnel network uses the **50.0.0.0/24** subnet.

Note

"Site-to-site tunnels were configured to provide secure communication between the LA and NYC branches using the existing Frame Relay WAN. Each tunnel has a unique IP and correct source/destination, enabling routing and data sharing between the two sites."

🔷 **Access-List Configuration – R1**

ACL – IT

ip access-list extended Acl_IT
 permit ip 192.168.1.8 0.0.0.7 any

ACL – Sales

ip access-list extended Acl_Sales
 permit ip 192.168.1.16 0.0.0.7 10.10.10.16 0.0.0.7
 permit ip 192.168.1.16 0.0.0.7 10.10.20.16 0.0.0.7
 permit ip 192.168.1.16 0.0.0.7 192.168.1.16 0.0.0.7
 deny   ip 192.168.1.16 0.0.0.7 any

ACL – HR

ip access-list extended Acl_HR
 permit ip 192.168.1.24 0.0.0.7 192.168.1.24 0.0.0.7
 permit ip 192.168.1.24 0.0.0.7 10.10.10.24 0.0.0.7

```
 permit ip 192.168.1.24 0.0.0.7 10.10.20.24 0.0.0.7
 permit ip 192.168.1.24 0.0.0.7 192.168.1.16 0.0.0.7
 permit ip 192.168.1.24 0.0.0.7 10.10.10.16 0.0.0.7
 permit ip 192.168.1.24 0.0.0.7 10.10.20.16 0.0.0.7
 deny   ip 192.168.1.24 0.0.0.7 any
```

ACL – Manager

```
ip access-list extended Acl_Manager
 permit ip 192.168.1.32 0.0.0.7 192.168.1.32 0.0.0.7
 permit ip 192.168.1.32 0.0.0.7 192.168.1.24 0.0.0.7
 permit ip 192.168.1.32 0.0.0.7 192.168.1.16 0.0.0.7
 permit ip 192.168.1.32 0.0.0.7 10.10.10.16 0.0.0.7
 permit ip 192.168.1.32 0.0.0.7 10.10.10.24 0.0.0.7
 permit ip 192.168.1.32 0.0.0.7 10.10.10.32 0.0.0.7
 permit ip 192.168.1.32 0.0.0.7 10.10.20.16 0.0.0.7
 permit ip 192.168.1.32 0.0.0.7 10.10.20.24 0.0.0.7
 permit ip 192.168.1.32 0.0.0.7 10.10.20.32 0.0.0.7
 deny   ip 192.168.1.32 0.0.0.7 any
```

ACL – Customer

```
ip access-list extended Acl_Customer
 permit tcp 192.168.1.72 0.0.0.7 any eq 80
 deny   ip 192.168.1.72 0.0.0.7 any
```

� Applying ACLs to Sub-Interfaces (R1)

```
int f0/0.2
 ip access-group Acl_IT in

int f0/0.3
 ip access-group Acl_Sales in

int f0/0.4
 ip access-group Acl_HR in

int f0/0.5
 ip access-group Acl_Manager in

int f0/0.10
 ip access-group Acl_Customer in
```

� Explanation

"Extended ACLs were applied on R1 sub-interfaces to enforce department-based security policies:

- **IT VLAN** – Full access to all internal/external networks
- **Sales VLAN** – Access only to Sales networks in HQ, LA, and NYC
- **HR VLAN** – Access only to HR and Sales

- **Manager VLAN** – Access to all networks except IT
- **Customer VLAN** – Only HTTP (port 80) Internet access

These ACLs ensure proper segmentation and enforce organizational security across all VLANs."

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."

EtherChannel Configuration (LA & NYC Branches)
LA Branch:

```
SW-LA1(config)# interface range f0/21-24
SW-LA1(config-if-range)# switchport mode trunk
SW-LA1(config-if-range)# channel-group 1 mode active

SW-LA2(config)# interface range f0/21-24
SW-LA2(config-if-range)# switchport mode trunk
SW-LA2(config-if-range)# channel-group 1 mode passive
```

NYC Branch:

```
SW-NYC1(config)# interface range f0/21-24
SW-NYC1(config-if-range)# switchport mode trunk
SW-NYC1(config-if-range)# channel-group 1 mode active

SW-NYC2(config)# interface range f0/21-24
SW-NYC2(config-if-range)# switchport mode trunk
SW-NYC2(config-if-range)# channel-group 1 mode passive
```

Explanation

- EtherChannel was created between the switches in each branch to aggregate ports, increase bandwidth, and improve redundancy.
- LACP was used with Active/Passive mode to form a single logical channel between each pair of switches.

Note:

"EtherChannel was configured on the access switches in both LA and NYC 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."

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.SS

Explanation:

- SSH was enabled on R1 to secure remote access to the VTY lines instead of using insecure Telnet.
- A **1024-bit RSA key** was generated to encrypt SSH sessions.
- A **local admin user** with full privileges (15) was created to authenticate SSH logins.
- VTY lines were configured for **local login only** and restricted to **SSH protocol**.

Note:

"SSH was configured on R1 to provide secure remote management. Each branch router (R2 – LA and R3 – NYC) was configured similarly: a local RSA key was generated, a privileged user account created, and VTY lines restricted to SSH only. This ensures encrypted and authenticated access to all routers."

◈ 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:

- The running configuration of R1 was backed up to the TFTP server to ensure configuration safety.
- Syslog was enabled to send debugging messages to a central syslog server, allowing real-time monitoring and troubleshooting.

Note:
"All routers had their running configurations backed up to the TFTP server. Syslog logging was enabled on each router to send debugging messages to a central server, providing centralized network monitoring and troubleshooting."

R2 & R3 – Branch Routers (LA & NYC):
R2# copy running-config tftp:
Address or name of remote host []? 192.168.1.114
Destination filename [R2-confg]? R2-Backup.cfg

R2(config)# logging 192.168.1.117
R2(config)# logging trap debugging

R3# copy running-config tftp:
Address or name of remote host []? 192.168.1.114
Destination filename [R3-confg]? R3-Backup.cfg

R3(config)# logging 192.168.1.117
R3(config)# logging trap debugging

Note:
"The same backup and syslog configuration steps were applied on the LA branch router (R2) and the NYC branch router (R3). Each router's running configuration was saved to the TFTP server, and debugging messages were sent to the central syslog server to facilitate monitoring and troubleshooting."

Testing & Verification

After completing the network setup, a series of tests were performed to ensure everything is working correctly:

---

1. **Connectivity Tests**

- Ping between branches (HQ ↔ LA ↔ NYC) to verify successful Frame Relay WAN connectivity.
- Ping between devices within the same VLAN to verify Inter-VLAN routing is functioning properly.

---

2. Routing Verification

- show ip route confirmed that all networks were correctly learned via RIP version 2.
- show ip interface brief verified that all interfaces are up with the correct IP addresses.

---

3. VLAN & Switch Configuration Verification

- show vlan brief confirmed that all VLANs are defined and assigned to the correct ports.
- show etherchannel summary verified that all EtherChannel links between switches were successfully established.

---

4. Security Testing

- Port Security: Connecting an unauthorized device triggers automatic port shutdown.
- ACLs: Verified access restrictions based on VLAN roles:
  - IT VLAN → Full access
  - Sales VLAN → Access only to Sales networks
  - HR VLAN → Access to HR and Sales networks
  - Manager VLAN → Access to all except IT
  - Customer VLAN → HTTP only

---

5. Services Verification

- Sales VLAN can communicate only with other Sales devices.
- HR VLAN can communicate with HR and Sales devices.
- Customer VLAN is limited to HTTP access only.
- Configuration Backup: Verified TFTP server backups of running-**config for** all routers.
- Syslog: Verified event logging on the central syslog server.
- SNMP Monitoring: Configured SNMP community strings for monitoring via NMS.

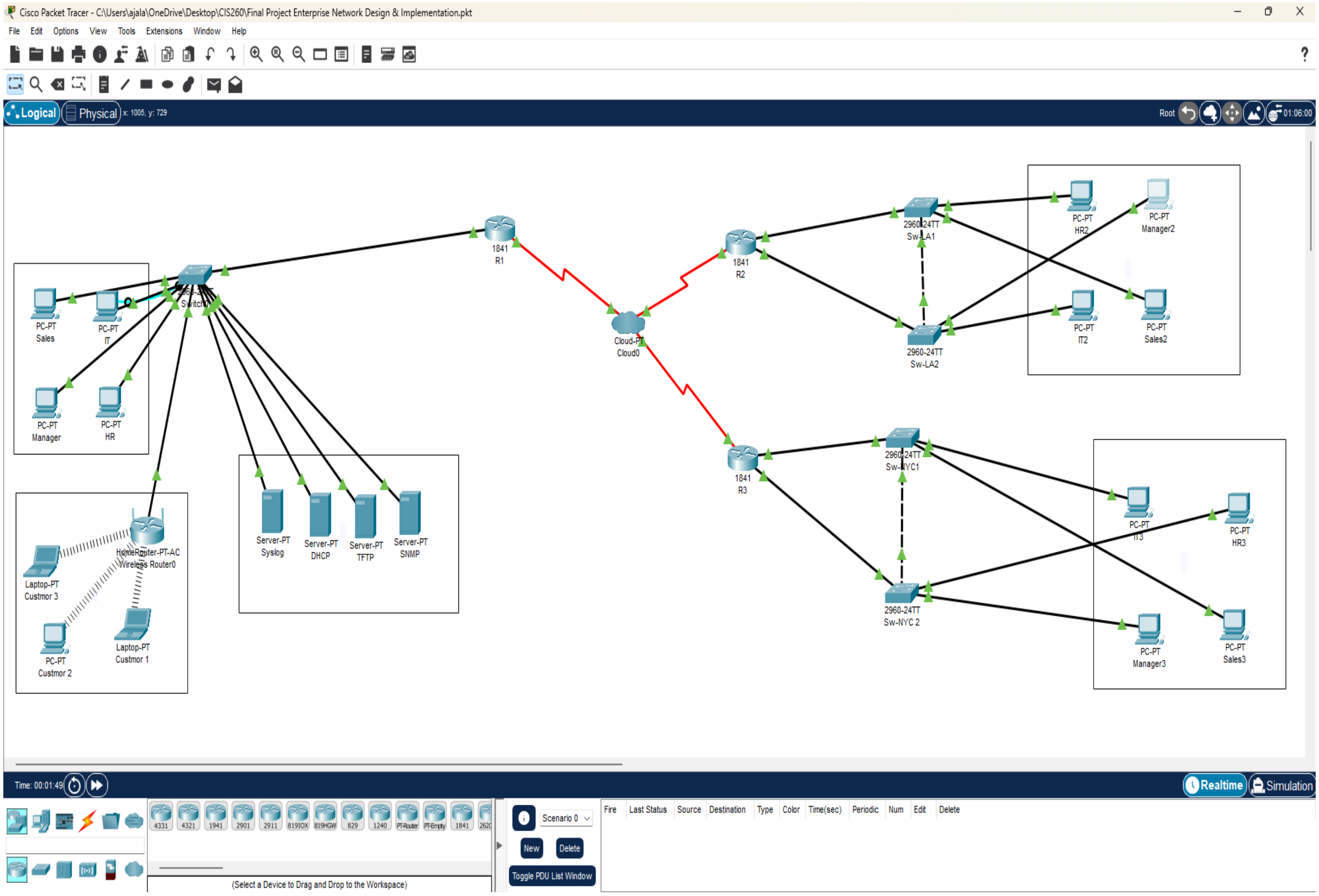
Executive Summary – Final Lab Project

This project demonstrates the design and implementation of a complete enterprise network connecting three company branches (**Chicago HQ, LA, and NYC**). The network includes **LAN, WAN, security, redundancy, and network management services**. Below is a summary of the main achievements:

Category	Key Achievements
Segmentation	VLANs implemented for IT, Sales, HR, Managers, Customers, and Servers. Router-on-a-Stick configuration enabled Inter-VLAN routing. DHCP pools were configured per VLAN for automated IP assignment.
Security	SSH enabled for secure remote access using RSA keys. Extended ACLs enforced department-specific policies. Port Security with sticky MAC addresses was configured; ports shut down on violation. Password encryption implemented for router access.
Redundancy & Performance	EtherChannel with LACP was configured for link aggregation. Frame Relay WAN with site-to-site tunnels between **LA and NYC** branches. Dynamic routing implemented using RIP v2 with no auto-summary.
Monitoring & Management	SNMP server configured for network monitoring. Syslog server enabled for centralized logging. TFTP server used for configuration backup. Connectivity and security tests verified functionality.

Summary:

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



Cisco Packet Tracer - C:\Users\ajala\OneDrive\Desktop\CIS260\Final Project Enterprise Network Design & Implementation.pkt
File Edit Options View Tools Extensions Window Help
Logical
Physical
x: 1005, y: 729
Root
01:06:00
1841
R1
Cloud-PT
Cloud0
1841
R2
2960-24TT
Sw-LA1
2960-24TT
Sw-LA2
PC-PT
HR2
PC-PT
Manager2
PC-PT
IT2
PC-PT
Sales2
1841
R3
2960-24TT
Sw-NYC1
2960-24TT
Sw-NYC 2
PC-PT
IT3
PC-PT
HR3
PC-PT
Manager3
PC-PT
Sales3
PC-PT
Sales
PC-PT
IT
PC-PT
Manager
PC-PT
HR
HomeRouter-PT-AC
Wireless Router0
Laptop-PT
Custmor 3
PC-PT
Custmor 2
Laptop-PT
Custmor 1
Server-PT
Syslog
Server-PT
DHCP
Server-PT
TFTP
Server-PT
SNMP
Time: 00:01:49
Realtime
Simulation
4331 4321 1941 2901 2911 819IOX 819HGW 829 1240 PTRouter PTEmpty 1841
Scenario 0
New
Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete
(Select a Device to Drag and Drop to the Workspace)