CCNA Project
Cloud Architecture 46 - Smart Village

Enterprise Network Infrastructure Design for Information Technology Institute (ITI)

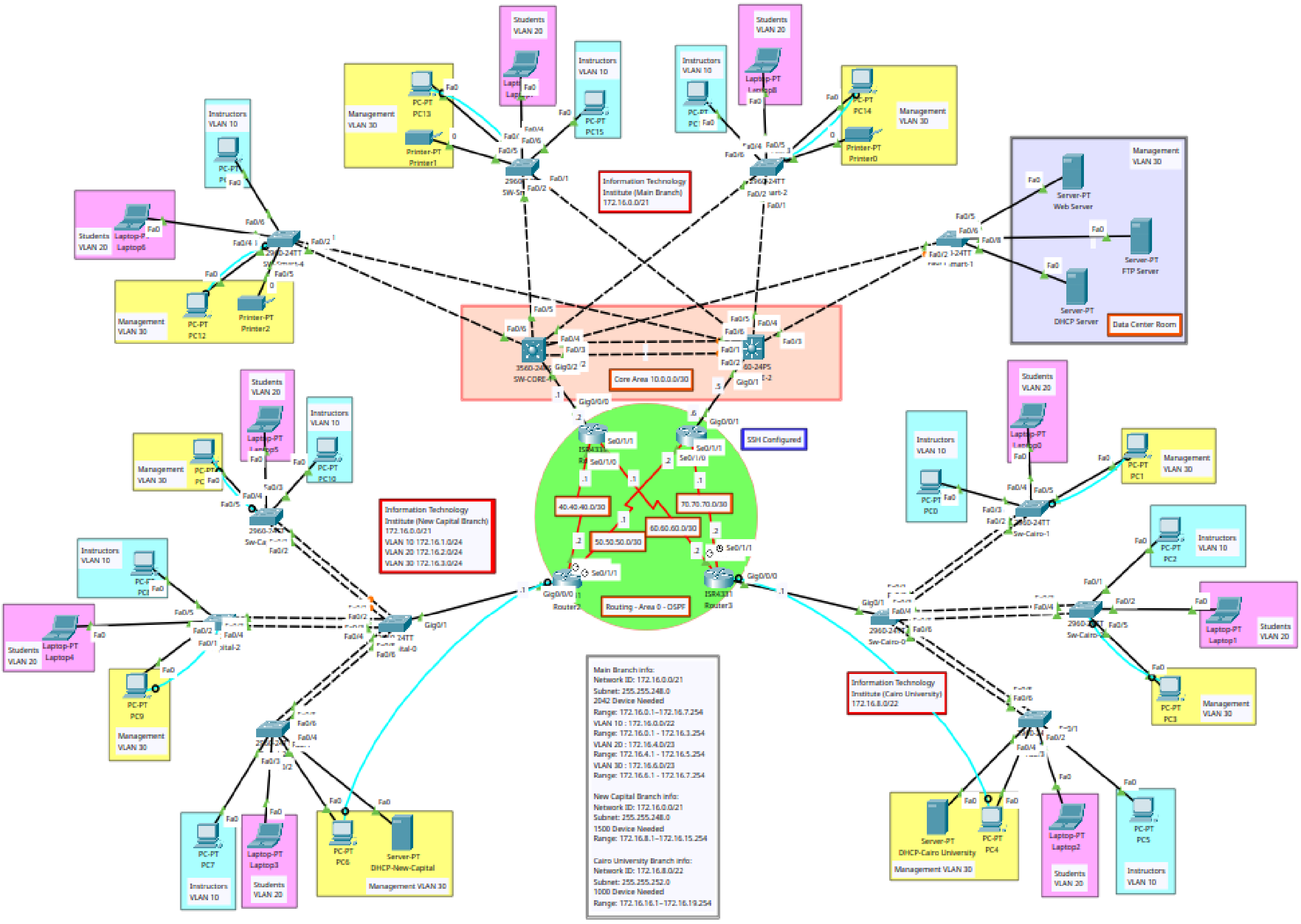
Prepared by:

Sara Hassan
Tuqa Kamel
Khaled Mahmoud

Eng. Ekram

Introduction

As the Information Technology Institute (**ITI**) continues to expand its educational footprint, the need for a robust, scalable, and secure network infrastructure becomes paramount. This project presents a comprehensive Wide Area Network (WAN) design connecting three strategic ITI branches: **Smart Village** Branch, the **New Capital** Branch, and the **Cairo University** Branch.



Main objective:

This documentation outlines the design and implementation of a multi-branch enterprise network for the Information Technology Institute (**ITI**). The topology integrates three geographically separated branches into a single, cohesive Autonomous System using **standard protocols**.

Key Design Features:

- **Optimized IP Addressing (VLSM):** A hierarchical IP addressing scheme was designed to maximize address conservation.
- **Inter-VLAN Routing:** Implemented using both **SVI** for high-performance core switching and **ROAS** for edge routing.
- **Link Aggregation (EtherChannel):** Bundled physical links to increase bandwidth and link redundancy.
- **High Availability (HSRP):** Deployed at the distribution layer to ensure gateway redundancy and zero downtime for end-users.
- **Dynamic Routing (OSPF):** utilized for fast convergence and efficient path selection between branches.
- **Automated Address Management (DHCP):** Centralized IP allocation using DHCP pools and Relay agents.
- **Internet Connectivity (NAT):** Configured to provide secure Internet access for private internal subnets, Accessing the **Web Serve**r through public IP.
- **Secure Management (SSH & AAA):** Implemented SSH encryption and AAA authentication to secure network devices against unauthorized access.
- **Disaster Recovery (FTP):** Established a backup solution for saving configurations and system images

Optimized IP Addressing (VLSM):

To efficiently manage the network for the organization, we designed a subnetting plan for three branches: **Main Branch**, **New Capital Branch**, and **Cairo University Branch**. The plan uses **Variable Length Subnet Masking (VLSM)** to allocate IP addresses according to the number of devices in each branch, ensuring optimal utilization of the available address space while leaving room for future growth.

Networks	*Network ID*	*First Usable IP*	*Last usable ip*	*broadcast ip*	*no. oF hosts*
Main Branch/Smart	**172.16.0.0/21**	**172.16.0.1**	**172.16.7.254**	**172.16.7.255**	**2042**
cairo university	**172.16.8.0 /21**	**172.16.8.1**	**172.16.15.254**	**172.16.15.255**	**1500**
New Capital	**172.16.16.0 /22**	**172.16.16.1**	**172.16.19.254**	**172.16.19.255**	**1000**

VLANs (Virtual Local Area Networks):

A VLAN (Virtual Local Area Network) is a logical grouping of devices within a network, even if they are not physically connected to the same switch. **VLANs are used to segment a network into smaller broadcast domains**, improving performance, security, and manageability.

By creating VLANs, network administrators can:

- Reduce broadcast traffic by limiting it to devices within the same VLAN.
- Enhance security by isolating sensitive devices or departments.
- Simplify network management by grouping devices logically, rather than physically.

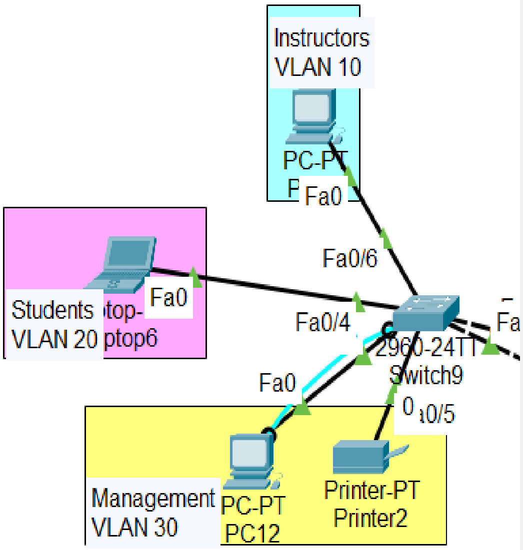
Each VLAN is assigned a unique subnet, and devices in the same VLAN can communicate directly with each other. However, to communicate with devices in a different VLAN, Inter-VLAN Routing is required.

VLANs are widely used in enterprise networks to efficiently manage large numbers of devices while maintaining network performance and security.

- ***Main Branch VLANs***

Networks	*Network ID*	*First Usable IP*	*Last usable ip*	*broadcast ip*	*no. oF hosts*
VLAN 10	**172.16.0.0 /22**	**172.16.0.1**	**172.16.3.254**	**172.16.3.255**	**1022**

VLAN 20	**172.16.4.0 /23**	**172.16.4.1**	**172.16.5.254**	**172.16.5.255**	**510**
VLAN 30	**172.16.6.0 /23**	**172.16.6.1**	**172.16.7.254**	**172.16.7.255**	**510**




```
interface FastEthernet0/1
 switchport mode trunk
!
interface FastEthernet0/2
 switchport mode trunk
!
interface FastEthernet0/3
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 10
 switchport mode access
!
```

These commands configure the interfaces **Fa0/1** and **Fa0/2** as **trunk ports** Because **each is connected to L3 switch**.

→**Trunk mode** allows the switch to carry traffic for **multiple VLANs** across a single link, typically used for connecting switches or routers.Fa0/1 and Fa0/2 each is connected to L3 switch.

interface FastEthernet0/3:

switchport access vlan 30→ Assigns the interface to **VLAN 30**.

switchport mode access→ Configures the port as an **access port** ,Typically used for connecting **end devices** (PCs or printers).

interface FastEthernet0/4:

switchport access vlan 20→ Assigns the interface to **VLAN 20**.

switchport mode access→ Configures the port as an **access port** ,Typically used for connecting **end devices** .

interface FastEthernet0/5:

switchport access vlan 30→ Assigns the interface to **VLAN 30**.

switchport mode access→ Configures the port as an **access port** .

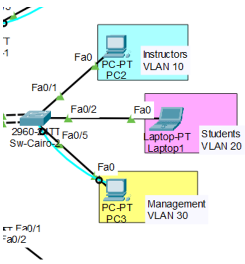
interface FastEthernet0/6:

switchport access vlan 10→ Assigns the interface to **VLAN 10**.

switchport mode access→ Configures the port as an **access port** ,Typically used for connecting **end devices** .

- ***Cairo University VLANs***

Networks	*Network ID*	*First Usable IP*	*Last usable ip*	*broadcast ip*	*no. oF hosts*
VLAN 10	**172.16.10.0 /24**	**172.16.10.1**	**172.16.10.254**	**172.16.10.255**	**254**
VLAN 20	**172.16.20.0 /24**	**172.16.20.1**	**172.16.20.254**	**172.16.20.255**	**254**
VLAN 30	**172.16.30.0 /24**	**172.16.30.1**	**172.16.30.254**	**172.16.30.255**	**254**




```
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 20
 switchport mode access
!
```

```
interface FastEthernet0/5
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/6
 switchport mode trunk
!
```

interface FastEthernet0/1:

switchport access vlan 10→ Assigns the interface to **VLAN 10**.

switchport mode access→ Configures the port as an **access port** ,Typically used for connecting **end devices** (PCs or printers).

interface FastEthernet0/2:

switchport access vlan 20→ Assigns the interface to **VLAN 20**.

switchport mode access→ Configures the port as an **access port** ,Typically used for connecting **end devices** .

interface FastEthernet0/5:

switchport access vlan 30→ Assigns the interface to **VLAN 30**.

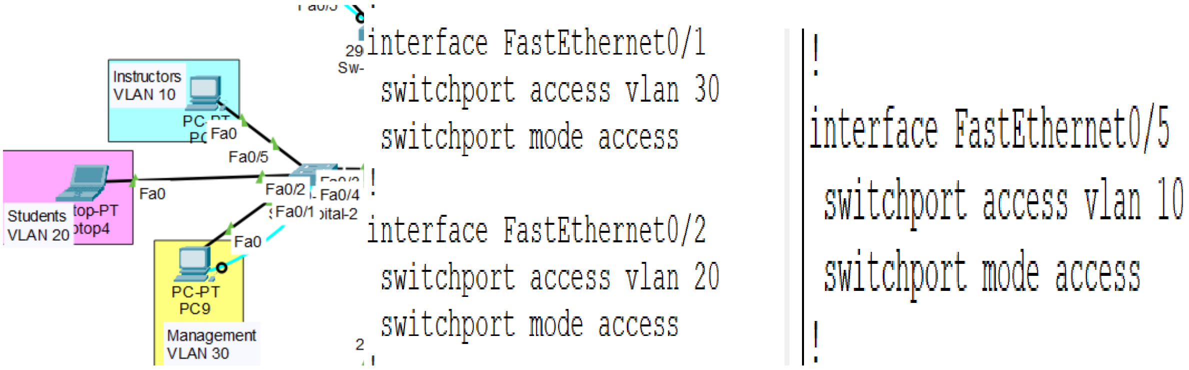
switchport mode access→ Configures the port as an **access port** .

interface FastEthernet0/6:

Trunk mode→ allows the switch to carry traffic for **multiple VLANs** across a single link

- ***New Capital VLANs***

Networks	*Network ID*	*First Usable IP*	*Last usable ip*	*broadcast ip*	*no. oF hosts*
VLAN 10	**172.16.1.0 /24**	**172.16.1.1**	**172.16.1.254**	**172.16.1.255**	**254**
VLAN 20	**172.16.2.0 /24**	**172.16.2.1**	**172.16.2.254**	**172.16.2.255**	**254**
VLAN 30	**172.16.3.0 /24**	**172.16.3.1**	**172.16.3.254**	**172.16.3.255**	**254**



interface FastEthernet0/1:

switchport access vlan 30→ Assigns the interface to **VLAN 30**.

switchport mode access→ Configures the port as an **access port** ,Typically used for connecting **end devices** (PCs or printers).

interface FastEthernet0/2:

switchport access vlan 20→ Assigns the interface to **VLAN 20**.

switchport mode access→ Configures the port as an **access port** ,Typically used for connecting **end devices** .

interface FastEthernet0/5:

switchport access vlan 10→ Assigns the interface to **VLAN 10**.

switchport mode access→ Configures the port as an **access port** .

Inter-VLAN Routing

VLANs (Virtual Local Area Networks) are used to segment a single physical network into multiple logical networks. VLANs improve security, reduce broadcast domains, and help organize network traffic based on departments or functions. However, by default, devices in different VLANs cannot communicate with each other because each VLAN is a separate broadcast domain.

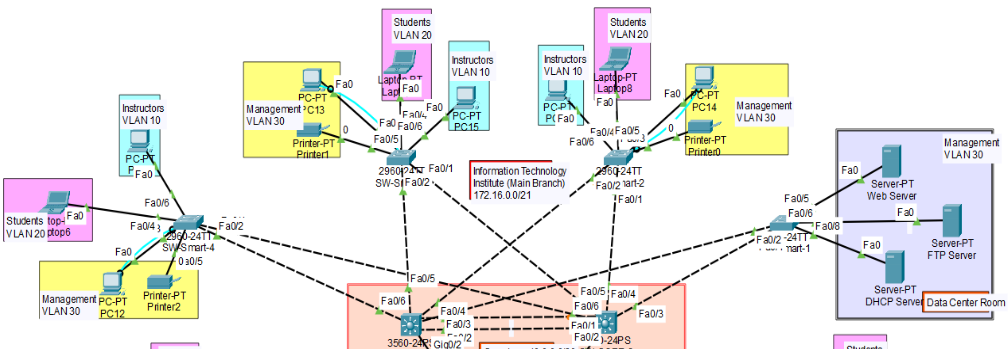
To enable communication between VLANs, a routing mechanism is required. **Inter-VLAN routing allows devices in different VLANs to exchange data**

- ***Main Branch:***

  we used **A Switched Virtual Interface (SVI)** which is a logical Layer 3 interface on a Layer 3 switch that represents a VLAN. SVIs allow the switch to **route traffic between VLANs without the need for an external router.**

Key Points:

- Each VLAN that requires routing gets its own SVI.
- The SVI IP address acts as the default gateway for devices in that VLAN.
- Inter-VLAN routing on a Layer 3 switch is done by configuring SVIs and enabling IP routing on the switch.



```
interface Vlan10
 mac-address 00d0.9703.0401
 ip address 172.16.0.3 255.255.252.0
 ip helper-address 172.16.6.60
 standby 10 ip 172.16.0.1
 standby 10 priority 150
 standby 10 preempt
!
interface Vlan20
 mac-address 00d0.9703.0402
 ip address 172.16.4.3 255.255.254.0
 ip helper-address 172.16.6.60
 standby 20 ip 172.16.4.1
 standby 20 priority 150
 standby 20 preempt
!
interface Vlan30
 mac-address 00d0.9703.0403
 ip address 172.16.6.3 255.255.254.0
 standby 30 ip 172.16.6.1
 standby 30 priority 150
 standby 30 preempt
```

VLAN 10 SVI:

interface **Vlan10**→ Logical interface for **VLAN 10.**

ip address **172.16.0.3 255.255.252.0**→ Default gateway IP for VLAN10 hosts.

VLAN 20 SVI:

interface **Vlan20**→ Logical interface for **VLAN 20.**

ip address **172.16.4.3 255.255.254.0**→ Default gateway IP for VLAN20 hosts.

VLAN 30 SVI:

interface **Vlan30**→ Logical interface for **VLAN 30.**

ip address **172.16.6.3 255.255.254.0**→ Default gateway IP for VLAN30 hosts.

Summary:

- Each **SVI provides a Layer 3 IP address** for its VLAN.
- These SVIs enable **inter-VLAN routing**, allowing devices in different VLANs to communicate through the Layer 3 switch.

Cairo University:

We used Router-on-a-Stick (**ROAS**) which is a method used to enable inter-VLAN routing using a single physical router interface. In this setup, the router interface is divided into subinterfaces, each assigned to a specific VLAN. The interface connected to the switch is configured as a trunk, allowing traffic from multiple VLANs to pass through one physical link.

Router-on-a-Stick (ROAS) Concept:

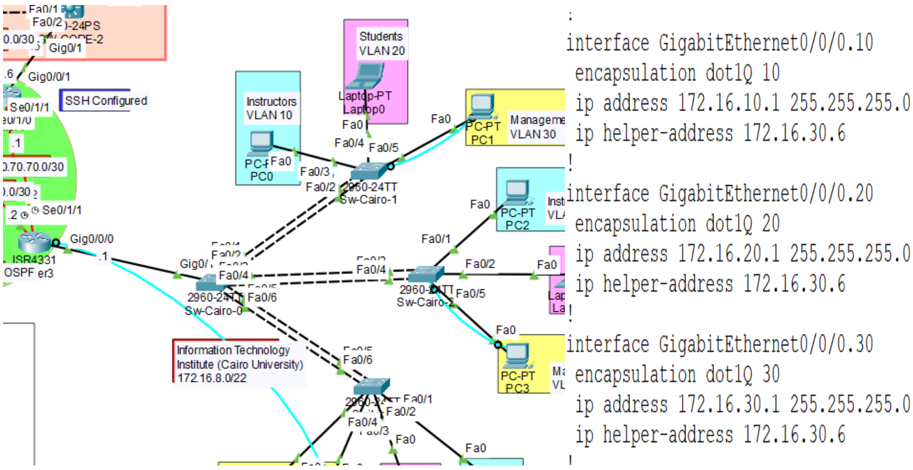
- **A single physical router interface** is used to route traffic between multiple VLANs.
- This interface is divided into **subinterfaces**, each assigned to a specific VLAN.
- Each subinterface has its own IP address, which **acts as the default gateway** for devices in that VLAN.
- The connection between the switch and router is configured as **a trunk link**, carrying traffic for all VLANs.

Benefits of ROAS:

- Efficient use of router interfaces (only one physical interface needed).

- Simplifies network design for small to medium networks.

- Provides centralized routing between VLANs.



VLAN 10 Subinterface

interface GigabitEthernet0/0/0.10→ Creates a **subinterface** on the physical router interface G0/0/0 for VLAN 10.

encapsulation dot1Q 10→ Configures **802.1Q encapsulation** and associates this subinterface with **VLAN 10**, so it can tag and route VLAN 10 traffic.

ip address **172.16.10.1 255.255.255.0**→Assigns a **Layer 3 IP address**, which acts as the **default gateway** for VLAN10 hosts.

VLAN 20 Subinterface

VLAN 20 Subinterface

interface GigabitEthernet0/0/0.20→ Creates a **subinterface** on the physical router interface G0/0/0 for VLAN 20.

encapsulation dot1Q 20→ Configures **802.1Q encapsulation** and associates this subinterface with **VLAN 20**, so it can tag and route VLAN 20 traffic.

ip address **172.16.20.1 255.255.255.0**→Assigns a **Layer 3 IP address**, which acts as the **default gateway** for VLAN20 hosts.

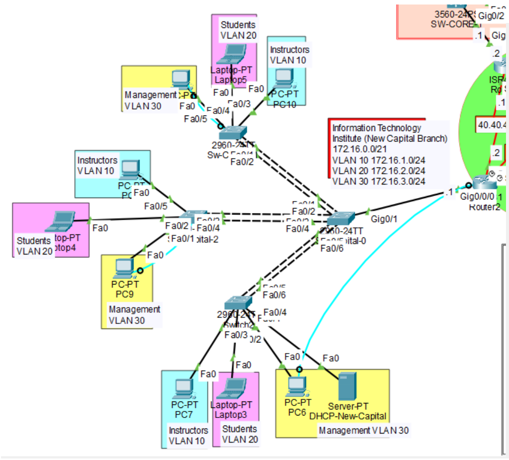
VLAN 30 Subinterface

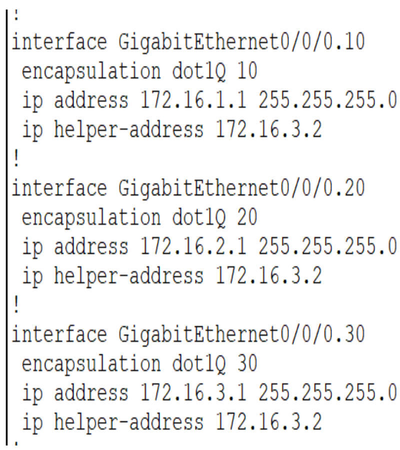
interface GigabitEthernet0/0/0.30→ Creates a **subinterface** on the physical router interface G0/0/0 for VLAN 30.

encapsulation dot1Q 30→ Configures **802.1Q encapsulation** and associates this subinterface with **VLAN 30**, so it can tag and route VLAN 30 traffic.

ip address **172.16.30.1 255.255.255.0**→Assigns a **Layer 3 IP address**, which acts as the **default gateway** for VLAN30 hosts.

New Capital:





```
!
interface GigabitEthernet0/0/0.10
 encapsulation dot1Q 10
 ip address 172.16.1.1 255.255.255.0
 ip helper-address 172.16.3.2
!
interface GigabitEthernet0/0/0.20
 encapsulation dot1Q 20
 ip address 172.16.2.1 255.255.255.0
 ip helper-address 172.16.3.2
!
interface GigabitEthernet0/0/0.30
 encapsulation dot1Q 30
 ip address 172.16.3.1 255.255.255.0
 ip helper-address 172.16.3.2
```

VLAN 10 Subinterface

interface GigabitEthernet0/0/0.10→ Creates a **subinterface** on the physical router interface G0/0/0 for VLAN 10.

encapsulation dot1Q 10→ Configures **802.1Q encapsulation** and associates this subinterface with **VLAN 10**, so it can tag and route VLAN 10 traffic.

ip address **172.16.1.1 255.255.255.0**→Assigns a **Layer 3 IP address**, which acts as the **default gateway** for VLAN10 hosts.
 VLAN 20 Subinterface

VLAN 20 Subinterface

interface GigabitEthernet0/0/0.20→ Creates a **subinterface** on the physical router interface G0/0/0 for VLAN 20.

encapsulation dot1Q 20→ Configures **802.1Q encapsulation** and associates this subinterface with **VLAN 20**, so it can tag and route VLAN 20 traffic.

ip address **172.16.2.1 255.255.255.0**→Assigns a **Layer 3 IP address**, which acts as the **default gateway** for VLAN20 hosts.

VLAN 30 Subinterface

interface GigabitEthernet0/0/0.30→ Creates a **subinterface** on the physical router interface G0/0/0 for VLAN 30.

encapsulation dot1Q 30→ Configures **802.1Q encapsulation** and associates this subinterface with **VLAN 30**, so it can tag and route VLAN 30 traffic.

ip address **172.16.3.1 255.255.255.0**→Assigns a **Layer 3 IP address**, which acts as the **default gateway** for VLAN30 hosts.

Summary:

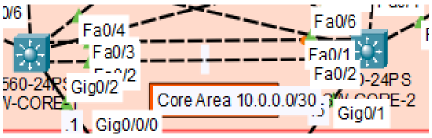
- Each subinterface allows the router to **route traffic between VLANs** using a single physical interface.
- The encapsulation dot1Q command ensures packets are properly tagged with their VLAN ID.
- The IP address on each subinterface serves as the **gateway** for its respective VLAN.

EtherChannel:

EtherChannel is a technique used to combine multiple physical links between switches or between a switch and a router into **a single logical link**. This provides:

- **Increased bandwidth** by aggregating the speed of all member links.
- **Redundancy**, because if one link fails, the others continue to carry traffic.
- Simplified management, as the multiple physical links appear as one interface in configuration.

Main Branch:



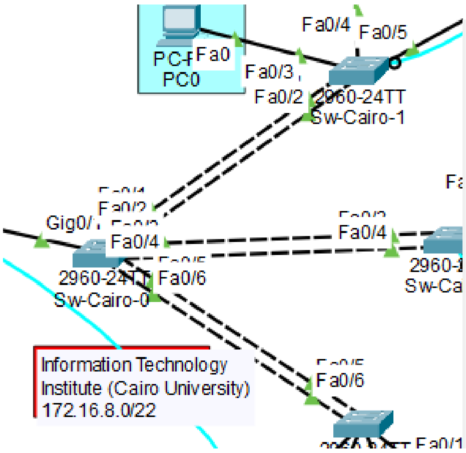

```
interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

interface Port-channel1→ Refers to the **logical EtherChannel interface**, which combines multiple physical links into a single logical link.

switchport trunk encapsulation dot1q→ Configures the trunk to use **802.1Q encapsulation**, allowing it to carry traffic from **multiple VLANs**.

switchport mode trunk→Sets the port-channel as a **trunk port**, so it can transmit VLAN-tagged traffic between switches.

Cairo university:




```
interface Port-channel1
 switchport trunk allowed vlan 1,10,20,30
 switchport mode trunk
!
interface Port-channel2
 switchport trunk allowed vlan 1,10,20,30
 switchport mode trunk
!
interface Port-channel3
 switchport trunk allowed vlan 1,10,20,30
 switchport mode trunk
!
```

interface Port-channel1→Logical EtherChannel interface combining multiple physical links.

switchport trunk allowed vlan 1,10,20,30→Only VLANs 1, 10, 20, and 30 are allowed on this trunk.

switchport mode trunk→ Configures the interface as a **trunk port**, carrying tagged VLAN traffic.

interface Port-channel2→Logical EtherChannel interface combining multiple physical links.

switchport trunk allowed vlan 1,10,20,30→Only VLANs 1, 10, 20, and 30 are allowed on this trunk.

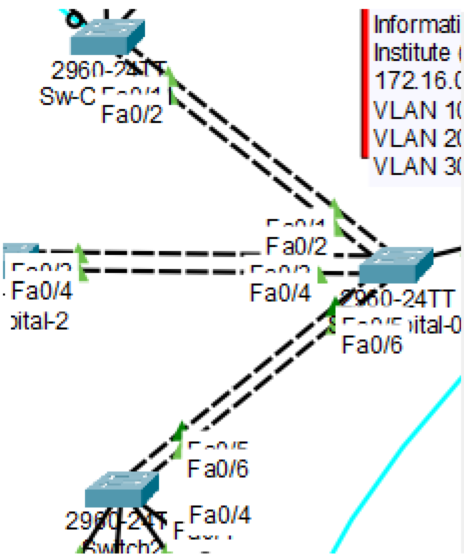
switchport mode trunk→ Configures the interface as a **trunk port**, carrying tagged VLAN traffic.

interface Port-channel3→Logical EtherChannel interface combining multiple physical links.

switchport trunk allowed vlan 1,10,20,30→Only VLANs 1, 10, 20, and 30 are allowed on this trunk.

switchport mode trunk→ Configures the interface as a **trunk port**, carrying tagged VLAN traffic.

New Capital:




```
interface Port-channel1
 switchport trunk allowed vlan 10,20,30
 switchport mode trunk
!
interface Port-channel2
 switchport trunk allowed vlan 10,20,30
 switchport mode trunk
!
interface Port-channel3
 switchport trunk allowed vlan 10,20,30
 switchport mode trunk
!
```

interface Port-channel1→Logical EtherChannel interface combining multiple physical links.

switchport trunk allowed vlan 1,10,20,30 → Only VLANs **1, 10, 20**, and **30** are allowed on this trunk.

switchport mode trunk→ Configures the interface as a **trunk port**, carrying tagged VLAN traffic.

interface Port-channel2 → Logical EtherChannel interface combining multiple physical links.

switchport trunk allowed vlan 1,10,20,30 → Only VLANs 1, 10, 20, and 30 are allowed on this trunk.

switchport mode trunk → Configures the interface as a **trunk port**, carrying tagged VLAN traffic.

interface Port-channel3 → Logical EtherChannel interface combining multiple physical links.

switchport trunk allowed vlan 1,10,20,30 → Only VLANs 1, 10, 20, and 30 are allowed on this trunk.

switchport mode trunk → Configures the interface as a **trunk port**, carrying tagged VLAN traffic.

Summary:

- Each **Port-Channel** is a logical trunk link carrying multiple VLANs.
- Limiting VLANs with `allowed vlan` ensures only the specified VLANs traverse the link.
- EtherChannel provides **increased bandwidth**, **redundancy**, and **simplified management** by combining physical links into one logical interface.

High Availability (HSRP)

To ensure continuous network uptime and fault tolerance, the Hot Standby Router Protocol (**HSRP**) was deployed at the **Core/Distribution layer**. This protocol provides gateway redundancy for all end devices (Students, Instructors, and Management) by virtualizing the Default Gateway IP address.

Design Strategy: Instead of relying on a single physical switch as a gateway, two Multilayer Switches (**Core-SW-1 and Core-SW-2**) work together in a group. They present a single **Virtual IP** (VIP) to the end clients. If the primary switch fails, the standby switch automatically takes over the VIP without requiring any reconfiguration on the client side.

Key Configuration Features:

- **VLAN-Based Load Balancing:** To utilize the full processing power of both core switches (Active/Active scenario from a system perspective), HSRP groups were configured to split traffic load:
  - **Core-SW-1** serves as the **Active Gateway** for **VLAN 10**.
  - **Core-SW-2** serves as the **Active Gateway** for **VLAN 20 & VLAN 30**.
  - This ensures that traffic is distributed across both physical links and devices during normal operation.
- **Priority & Election:**
  - The **Active** role was enforced by setting a higher priority value (**150**) on the primary switch for each respective VLAN.

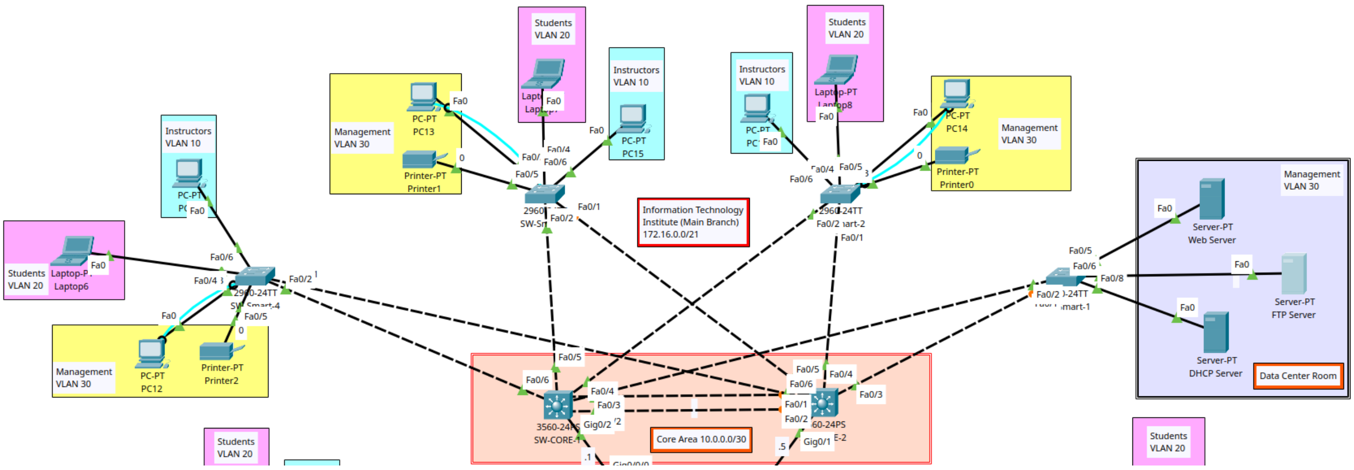
   - The **Standby** switch was configured with a lower priority (**100**) to remain in wait mode.

- **Preemption:**
   - The standby preempt command was enabled on all interfaces. This ensures that if a failed primary switch comes back online, it automatically reclaims its role as the Active Gateway, restoring the original load-balancing state.

HSRP Configuration Matrix

VLAN ID	HSRP GROUP	Virtual Gateway IP (VIP)	Active Switch (Priority 150)	Standby Switch (Priority 100)
VLAN 10	**10**	**172.16.0.1**	**SW-Core-1**	**SW-Core-2**
VLAN 20	**20**	**172.16.4.1**	**SW-Core-2**	**SW-Core-1**
VLAN 30	**30**	**172.16.6.1**	**SW-Core-2**	**SW-Core-1**

The topology above illustrates the High Availability (HA) design implemented within the Core Area. Two Multilayer Switches (**SW-CORE-1 and SW-CORE-2**) are configured with HSRP (Hot Standby Router Protocol) to function as a redundant gateway pair.



- ***Active Layer 3 Switch (SW-Core-1):***

```
SW-Core-1#show standby
Vlan10 - Group 10
  State is Active
    5 state changes, last state change 00:00:19
  Virtual IP address is 172.16.0.1
  Active virtual MAC address is 0000.0C07.AC0A
    Local virtual MAC address is 0000.0C07.AC0A (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.599 secs
  Preemption enabled
  Active router is local
  Standby router is 172.16.0.2
  Priority 150 (configured 150)
  Group name is hsrp-Vl1-10 (default)
Vlan20 - Group 20
  State is Active
    5 state changes, last state change 00:00:17
  Virtual IP address is 172.16.4.1
  Active virtual MAC address is 0000.0C07.AC14
    Local virtual MAC address is 0000.0C07.AC14 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.295 secs
  Preemption enabled
  Active router is local
  Standby router is 172.16.4.2, priority 100 (expires in 6 sec)
  Priority 150 (configured 150)
  Group name is hsrp-Vl2-20 (default)
Vlan30 - Group 30
  State is Active
    5 state changes, last state change 00:00:18
  Virtual IP address is 172.16.6.1
  Active virtual MAC address is 0000.0C07.AC1E
    Local virtual MAC address is 0000.0C07.AC1E (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.152 secs
  Preemption enabled
  Active router is local
  Standby router is 172.16.6.2, priority 100 (expires in 8 sec)
  Priority 150 (configured 150)
  Group name is hsrp-Vl3-30 (default)
```

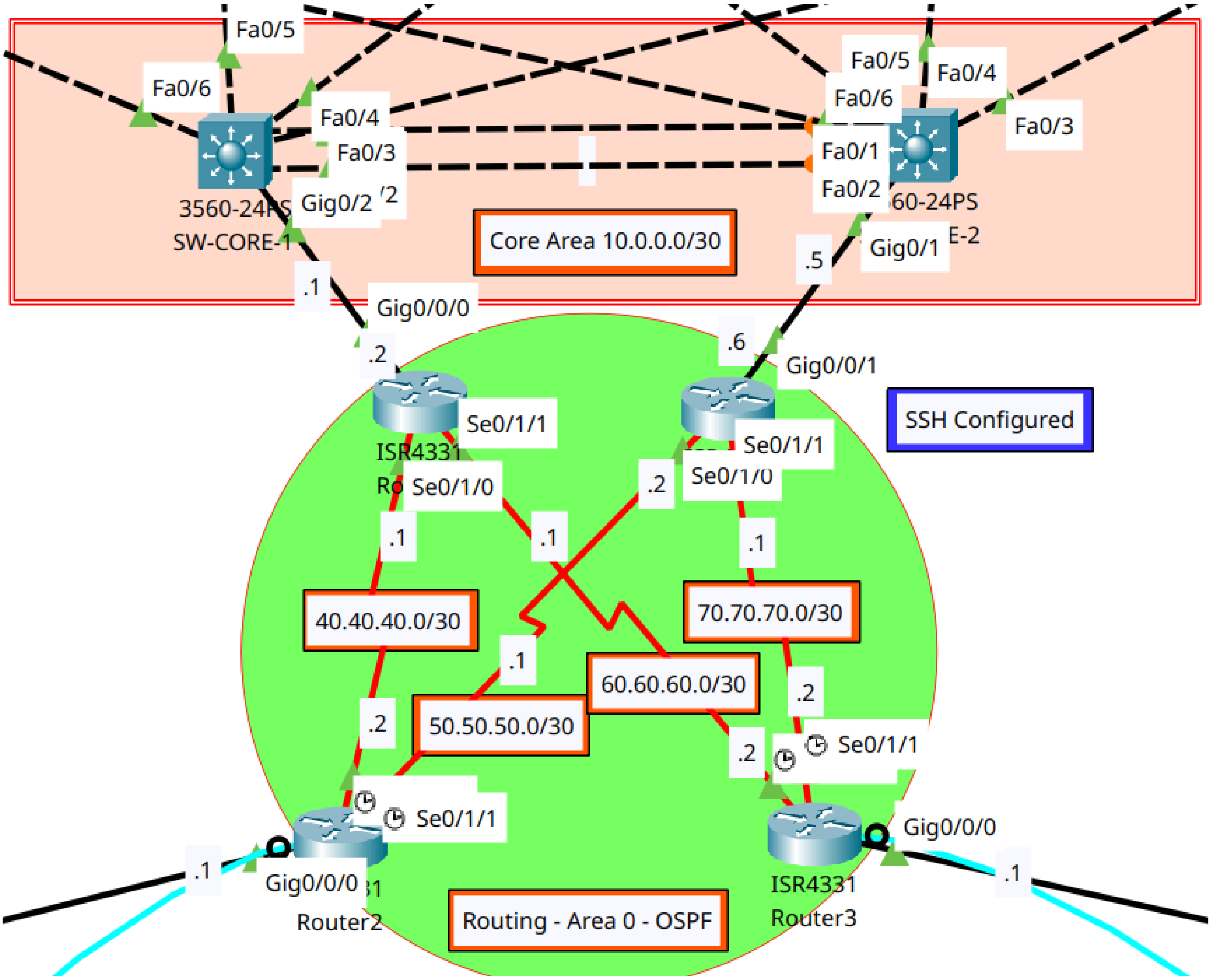
- ***Standby Layer 3 Switch (SW-Core-2):***

```
SW-Core-2#show standby
Vlan10 - Group 10
  State is Standby
    7 state changes, last state change 00:00:39
  Virtual IP address is 172.16.0.1
  Active virtual MAC address is 0000.0C07.AC0A
    Local virtual MAC address is 0000.0C07.AC0A (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.221 secs
  Preemption enabled
  Active router is 172.16.0.3
  Standby router is local
  Priority 100 (default 100)
  Group name is hsrp-Vl1-10 (default)
Vlan20 - Group 20
  State is Standby
    7 state changes, last state change 00:00:39
  Virtual IP address is 172.16.4.1
  Active virtual MAC address is 0000.0C07.AC14
    Local virtual MAC address is 0000.0C07.AC14 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.022 secs
  Preemption enabled
  Active router is 172.16.4.3, priority 150 (expires in 9 sec)
    MAC address is 0000.0C07.AC14
  Standby router is local
  Priority 100 (default 100)
  Group name is hsrp-Vl2-20 (default)
Vlan30 - Group 30
  State is Standby
    7 state changes, last state change 00:00:40
  Virtual IP address is 172.16.6.1
  Active virtual MAC address is 0000.0C07.AC1E
    Local virtual MAC address is 0000.0C07.AC1E (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.903 secs
  Preemption enabled
  Active router is 172.16.6.3, priority 150 (expires in 9 sec)
    MAC address is 0000.0C07.AC1E
  Standby router is local
  Priority 100 (default 100)
  Group name is hsrp-Vl3-30 (default)
```

Dynamic Routing Strategy (OSPF):

To manage the complex connectivity between the three branches and ensuring optimal path selection, **Open Shortest Path First (OSPFv2)** was implemented as the Interior Gateway Protocol (IGP). OSPF was chosen for its fast convergence, scalability, and vendor-neutral support, making it ideal for the ITI enterprise network.

Design Strategy: The network employs a **Single-Area OSPF (Area 0)** design, also known as the **Backbone** Area. All Routers and Multilayer Switches participate in this area, allowing them to share a complete topological map of the network. This ensures that if a primary link fails (e.g., between the Main Branch and the ISP), traffic is automatically rerouted through the backup serial links between branches.



Key Configuration Features:

- Routed Ports on **Core Switches**: Instead of using traditional **SVI-based** routing for uplinks, the physical interfaces connecting the Core Multilayer Switches to the Edge Routers were converted into Routed Ports (using the `no switchport` command). This creates efficient point-to-point Layer 3 links (`/30`), reducing broadcast domains and improving OSPF adjacency stability, One of the MLS were configured with **Default Route (0.0.0.0/0)**
- **Passive Interfaces:** To enhance security and bandwidth efficiency, **Passive Interfaces** were configured on all LAN-facing ports (SVIs for VLAN 10, 20, 30). This prevents OSPF Hello packets from being broadcasted to end-user devices, protecting the routing table from spoofing attacks and reducing unnecessary traffic.
- **Route Redundancy:** The topology utilizes dual links between routers. OSPF’s Dijkstra algorithm automatically calculates the cost of each link (based on Bandwidth) to determine the best path. In the event of a link failure, OSPF re-converges instantly to the alternative path.

OSPF Configuration Summary

Networks	***Value***	***Description***
Process ID	**1**	**Locally significant ID used to start the OSPF process.**
Area ID	**Backbone (0)**	**All devices reside in the backbone area for direct routing.**
Router ID	**Unique (e.g., 1.1.1.1)**	**Manually assigned Loopback IPs for stable identification.**

Routing Table of Multi-Layer-SW-1:

<SHOW IP ROUTE>

```
SW-Core-1#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

     10.0.0.0/30 is subnetted, 2 subnets
O       10.0.0.0 [110/2] via 172.16.0.2, 00:16:07, Vlan10
                 [110/2] via 172.16.4.2, 00:16:07, Vlan20
                 [110/2] via 172.16.6.2, 00:16:07, Vlan30
C       10.0.0.4 is directly connected, GigabitEthernet0/1
     40.0.0.0/30 is subnetted, 1 subnets
O       40.40.40.0 [110/66] via 172.16.0.2, 00:16:07, Vlan10
                   [110/66] via 172.16.4.2, 00:16:07, Vlan20
                   [110/66] via 172.16.6.2, 00:16:07, Vlan30
     50.0.0.0/30 is subnetted, 1 subnets
S       50.50.50.0 [1/0] via 10.0.0.6
     60.0.0.0/30 is subnetted, 1 subnets
O       60.60.60.0 [110/66] via 172.16.0.2, 00:16:07, Vlan10
                   [110/66] via 172.16.4.2, 00:16:07, Vlan20
                   [110/66] via 172.16.6.2, 00:16:07, Vlan30
     70.0.0.0/30 is subnetted, 1 subnets
O       70.70.70.0 [110/65] via 10.0.0.6, 00:16:07, GigabitEthernet0/1
     172.16.0.0/16 is variably subnetted, 9 subnets, 3 masks
C       172.16.0.0/22 is directly connected, Vlan10
O       172.16.1.0/24 [110/66] via 10.0.0.6, 00:16:07, GigabitEthernet0/1
O       172.16.2.0/24 [110/66] via 10.0.0.6, 00:16:07, GigabitEthernet0/1
O       172.16.3.0/24 [110/66] via 10.0.0.6, 00:16:07, GigabitEthernet0/1
C       172.16.4.0/23 is directly connected, Vlan20
C       172.16.6.0/23 is directly connected, Vlan30
O       172.16.10.0/24 [110/66] via 10.0.0.6, 00:16:07, GigabitEthernet0/1
O       172.16.20.0/24 [110/66] via 10.0.0.6, 00:16:07, GigabitEthernet0/1
O       172.16.30.0/24 [110/66] via 10.0.0.6, 00:16:07, GigabitEthernet0/1
```

Routing Table of Multi-Layer-SW-2:

<SHOW IP ROUTE>

```
SW-Core-2#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 0.0.0.0 to network 0.0.0.0

     10.0.0.0/30 is subnetted, 2 subnets
C       10.0.0.0 is directly connected, GigabitEthernet0/2
O       10.0.0.4 [110/2] via 172.16.0.3, 00:16:48, Vlan10
                 [110/2] via 172.16.4.3, 00:16:48, Vlan20
                 [110/2] via 172.16.6.3, 00:16:48, Vlan30
     40.0.0.0/30 is subnetted, 1 subnets
O       40.40.40.0 [110/65] via 10.0.0.2, 00:16:48, GigabitEthernet0/2
     50.0.0.0/30 is subnetted, 1 subnets
O       50.50.50.0 [110/66] via 172.16.0.3, 00:16:48, Vlan10
                   [110/66] via 172.16.4.3, 00:16:48, Vlan20
                   [110/66] via 172.16.6.3, 00:16:48, Vlan30
     60.0.0.0/30 is subnetted, 1 subnets
O       60.60.60.0 [110/65] via 10.0.0.2, 00:16:48, GigabitEthernet0/2
     70.0.0.0/30 is subnetted, 1 subnets
O       70.70.70.0 [110/66] via 172.16.0.3, 00:16:48, Vlan10
                   [110/66] via 172.16.4.3, 00:16:48, Vlan20
                   [110/66] via 172.16.6.3, 00:16:48, Vlan30
     172.16.0.0/16 is variably subnetted, 9 subnets, 3 masks
C       172.16.0.0/22 is directly connected, Vlan10
O       172.16.1.0/24 [110/66] via 10.0.0.2, 00:16:48, GigabitEthernet0/2
O       172.16.2.0/24 [110/66] via 10.0.0.2, 00:16:48, GigabitEthernet0/2
O       172.16.3.0/24 [110/66] via 10.0.0.2, 00:16:48, GigabitEthernet0/2
C       172.16.4.0/23 is directly connected, Vlan20
C       172.16.6.0/23 is directly connected, Vlan30
O       172.16.10.0/24 [110/66] via 10.0.0.2, 00:16:48, GigabitEthernet0/2
O       172.16.20.0/24 [110/66] via 10.0.0.2, 00:16:48, GigabitEthernet0/2
O       172.16.30.0/24 [110/66] via 10.0.0.2, 00:16:48, GigabitEthernet0/2
S*   0.0.0.0/0 is directly connected, GigabitEthernet0/2
```

Routers Area - Routing Table of R1-Main:

<SHOW IP ROUTE>

```
R1-Main#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

     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O       10.0.0.0/30 [110/3] via 10.0.0.5, 00:17:36, GigabitEthernet0/0/1
C       10.0.0.4/30 is directly connected, GigabitEthernet0/0/1
L       10.0.0.6/32 is directly connected, GigabitEthernet0/0/1
     40.0.0.0/30 is subnetted, 1 subnets
O       40.40.40.0/30 [110/67] via 10.0.0.5, 00:17:36, GigabitEthernet0/0/1
     50.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       50.50.50.0/30 is directly connected, Serial0/1/0
L       50.50.50.2/32 is directly connected, Serial0/1/0
     60.0.0.0/30 is subnetted, 1 subnets
O       60.60.60.0/30 [110/67] via 10.0.0.5, 00:17:36, GigabitEthernet0/0/1
     70.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       70.70.70.0/30 is directly connected, Serial0/1/1
L       70.70.70.1/32 is directly connected, Serial0/1/1
     172.16.0.0/16 is variably subnetted, 9 subnets, 3 masks
O       172.16.0.0/22 [110/2] via 10.0.0.5, 00:17:36, GigabitEthernet0/0/1
O       172.16.1.0/24 [110/65] via 50.50.50.1, 00:18:21, Serial0/1/0
O       172.16.2.0/24 [110/65] via 50.50.50.1, 00:18:21, Serial0/1/0
O       172.16.3.0/24 [110/65] via 50.50.50.1, 00:18:21, Serial0/1/0
O       172.16.4.0/23 [110/2] via 10.0.0.5, 00:17:36, GigabitEthernet0/0/1
S       172.16.6.0/23 [1/0] via 10.0.0.5
O       172.16.10.0/24 [110/65] via 70.70.70.2, 00:18:11, Serial0/1/1
O       172.16.20.0/24 [110/65] via 70.70.70.2, 00:18:11, Serial0/1/1
O       172.16.30.0/24 [110/65] via 70.70.70.2, 00:18:11, Serial0/1/1
```

Routers Area - Routing Table of R2-Main:

<SHOW IP ROUTE>

```
R2-Main#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

     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.0.0.0/30 is directly connected, GigabitEthernet0/0/0
L       10.0.0.2/32 is directly connected, GigabitEthernet0/0/0
O       10.0.0.4/30 [110/3] via 10.0.0.1, 00:19:01, GigabitEthernet0/0/0
     40.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       40.40.40.0/30 is directly connected, Serial0/1/0
L       40.40.40.1/32 is directly connected, Serial0/1/0
     50.0.0.0/30 is subnetted, 1 subnets
O       50.50.50.0/30 [110/67] via 10.0.0.1, 00:19:01, GigabitEthernet0/0/0
     60.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       60.60.60.0/30 is directly connected, Serial0/1/1
L       60.60.60.1/32 is directly connected, Serial0/1/1
     70.0.0.0/30 is subnetted, 1 subnets
O       70.70.70.0/30 [110/67] via 10.0.0.1, 00:19:01, GigabitEthernet0/0/0
     172.16.0.0/16 is variably subnetted, 9 subnets, 3 masks
O       172.16.0.0/22 [110/2] via 10.0.0.1, 00:19:01, GigabitEthernet0/0/0
O       172.16.1.0/24 [110/65] via 40.40.40.2, 00:19:36, Serial0/1/0
O       172.16.2.0/24 [110/65] via 40.40.40.2, 00:19:36, Serial0/1/0
O       172.16.3.0/24 [110/65] via 40.40.40.2, 00:19:36, Serial0/1/0
O       172.16.4.0/23 [110/2] via 10.0.0.1, 00:19:01, GigabitEthernet0/0/0
O       172.16.6.0/23 [110/2] via 10.0.0.1, 00:19:01, GigabitEthernet0/0/0
O       172.16.10.0/24 [110/65] via 60.60.60.2, 00:19:36, Serial0/1/1
O       172.16.20.0/24 [110/65] via 60.60.60.2, 00:19:36, Serial0/1/1
O       172.16.30.0/24 [110/65] via 60.60.60.2, 00:19:36, Serial0/1/1
```

Routers Area - Routing Table of Router-Cairo-Univ:

<SHOW IP ROUTE>

```
Cairo-Univ#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

     10.0.0.0/30 is subnetted, 2 subnets
O       10.0.0.0/30 [110/65] via 60.60.60.1, 00:19:32, Serial0/1/0
O       10.0.0.4/30 [110/65] via 70.70.70.1, 00:19:32, Serial0/1/1
     40.0.0.0/30 is subnetted, 1 subnets
O       40.40.40.0/30 [110/128] via 60.60.60.1, 00:20:12, Serial0/1/0
     50.0.0.0/30 is subnetted, 1 subnets
O       50.50.50.0/30 [110/128] via 70.70.70.1, 00:20:12, Serial0/1/1
     60.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       60.60.60.0/30 is directly connected, Serial0/1/0
L       60.60.60.2/32 is directly connected, Serial0/1/0
     70.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       70.70.70.0/30 is directly connected, Serial0/1/1
L       70.70.70.2/32 is directly connected, Serial0/1/1
     172.16.0.0/16 is variably subnetted, 12 subnets, 4 masks
O       172.16.0.0/22 [110/66] via 60.60.60.1, 00:19:32, Serial0/1/0
                      [110/66] via 70.70.70.1, 00:19:32, Serial0/1/1
O       172.16.1.0/24 [110/129] via 60.60.60.1, 00:20:02, Serial0/1/0
                      [110/129] via 70.70.70.1, 00:20:02, Serial0/1/1
O       172.16.2.0/24 [110/129] via 60.60.60.1, 00:20:02, Serial0/1/0
                      [110/129] via 70.70.70.1, 00:20:02, Serial0/1/1
O       172.16.3.0/24 [110/129] via 60.60.60.1, 00:20:02, Serial0/1/0
                      [110/129] via 70.70.70.1, 00:20:02, Serial0/1/1
O       172.16.4.0/23 [110/66] via 60.60.60.1, 00:19:32, Serial0/1/0
                      [110/66] via 70.70.70.1, 00:19:32, Serial0/1/1
O       172.16.6.0/23 [110/66] via 60.60.60.1, 00:19:32, Serial0/1/0
                      [110/66] via 70.70.70.1, 00:19:32, Serial0/1/1
C       172.16.10.0/24 is directly connected, GigabitEthernet0/0/0.10
L       172.16.10.1/32 is directly connected, GigabitEthernet0/0/0.10
C       172.16.20.0/24 is directly connected, GigabitEthernet0/0/0.20
L       172.16.20.1/32 is directly connected, GigabitEthernet0/0/0.20
C       172.16.30.0/24 is directly connected, GigabitEthernet0/0/0.30
L       172.16.30.1/32 is directly connected, GigabitEthernet0/0/0.30
```

Routers Area - Routing Table of Router-New-Capital:

<SHOW IP ROUTE>

```
New-Capital#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

     10.0.0.0/30 is subnetted, 2 subnets
O       10.0.0.0/30 [110/65] via 40.40.40.1, 00:20:14, Serial0/1/0
O       10.0.0.4/30 [110/65] via 50.50.50.2, 00:20:14, Serial0/1/1
     40.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       40.40.40.0/24 is directly connected, Serial0/1/0
L       40.40.40.2/32 is directly connected, Serial0/1/0
     50.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       50.50.50.0/24 is directly connected, Serial0/1/1
L       50.50.50.1/32 is directly connected, Serial0/1/1
     60.0.0.0/30 is subnetted, 1 subnets
O       60.60.60.0/30 [110/128] via 40.40.40.1, 00:20:49, Serial0/1/0
     70.0.0.0/30 is subnetted, 1 subnets
O       70.70.70.0/30 [110/128] via 50.50.50.2, 00:20:49, Serial0/1/1
     172.16.0.0/16 is variably subnetted, 12 subnets, 4 masks
O       172.16.0.0/22 [110/66] via 40.40.40.1, 00:20:14, Serial0/1/0
                      [110/66] via 50.50.50.2, 00:20:14, Serial0/1/1
C       172.16.1.0/24 is directly connected, GigabitEthernet0/0/0.10
L       172.16.1.1/32 is directly connected, GigabitEthernet0/0/0.10
C       172.16.2.0/24 is directly connected, GigabitEthernet0/0/0.20
L       172.16.2.1/32 is directly connected, GigabitEthernet0/0/0.20
C       172.16.3.0/24 is directly connected, GigabitEthernet0/0/0.30
L       172.16.3.1/32 is directly connected, GigabitEthernet0/0/0.30
O       172.16.4.0/23 [110/66] via 40.40.40.1, 00:20:14, Serial0/1/0
                      [110/66] via 50.50.50.2, 00:20:14, Serial0/1/1
O       172.16.6.0/23 [110/66] via 40.40.40.1, 00:20:14, Serial0/1/0
                      [110/66] via 50.50.50.2, 00:20:14, Serial0/1/1
O       172.16.10.0/24 [110/129] via 40.40.40.1, 00:20:49, Serial0/1/0
                       [110/129] via 50.50.50.2, 00:20:49, Serial0/1/1
O       172.16.20.0/24 [110/129] via 40.40.40.1, 00:20:49, Serial0/1/0
                       [110/129] via 50.50.50.2, 00:20:49, Serial0/1/1
O       172.16.30.0/24 [110/129] via 40.40.40.1, 00:20:49, Serial0/1/0
                       [110/129] via 50.50.50.2, 00:20:49, Serial0/1/1
```

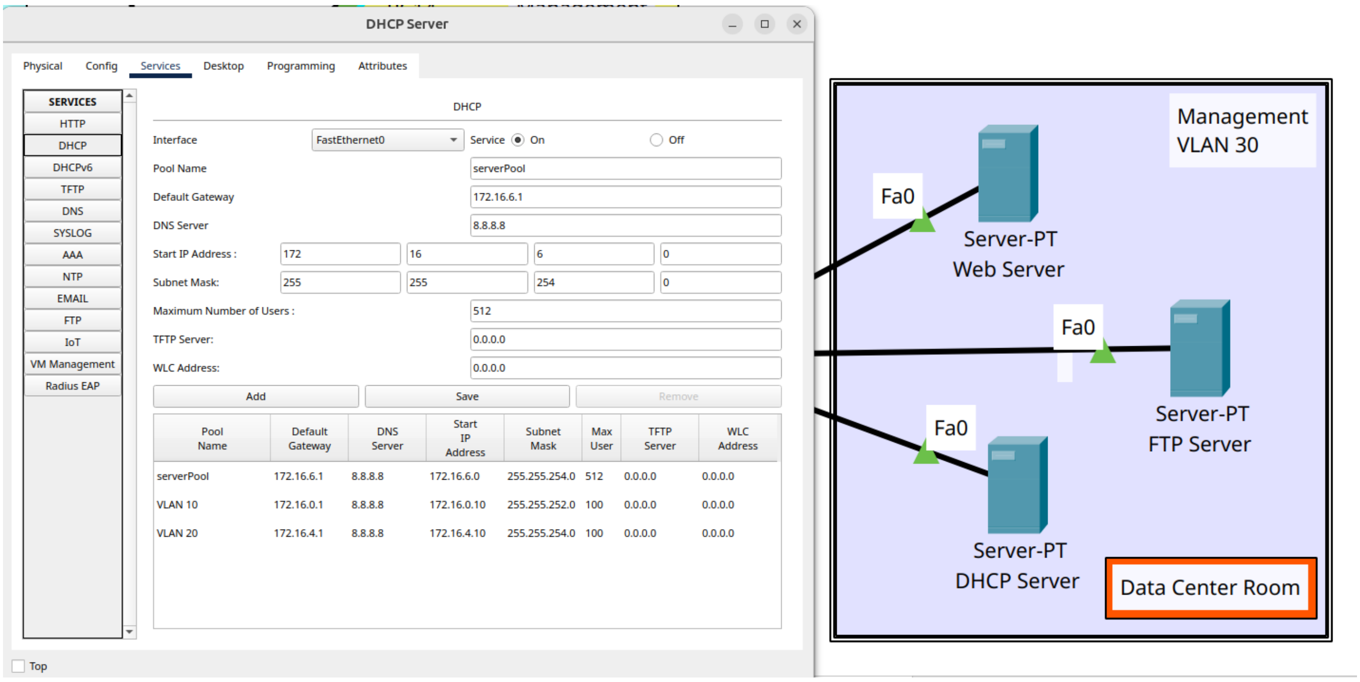
Automated Address Management: DHCP Strategy

To ensure branch autonomy and reduce traffic across the WAN links, a **Distributed DHCP Architecture** was implemented. Each branch hosts its own **local DHCP server** located within the Management VLAN (VLAN 30).

Design Strategy: Since the network is segmented into multiple VLANs (Broadcast Domains), a DHCP broadcast packet from a client cannot naturally reach the centralized server. To overcome this, the **DHCP Relay Agent feature** was implemented on the Core Multilayer Switches.

1. Main Branch: SVI & Layer 3 Switching

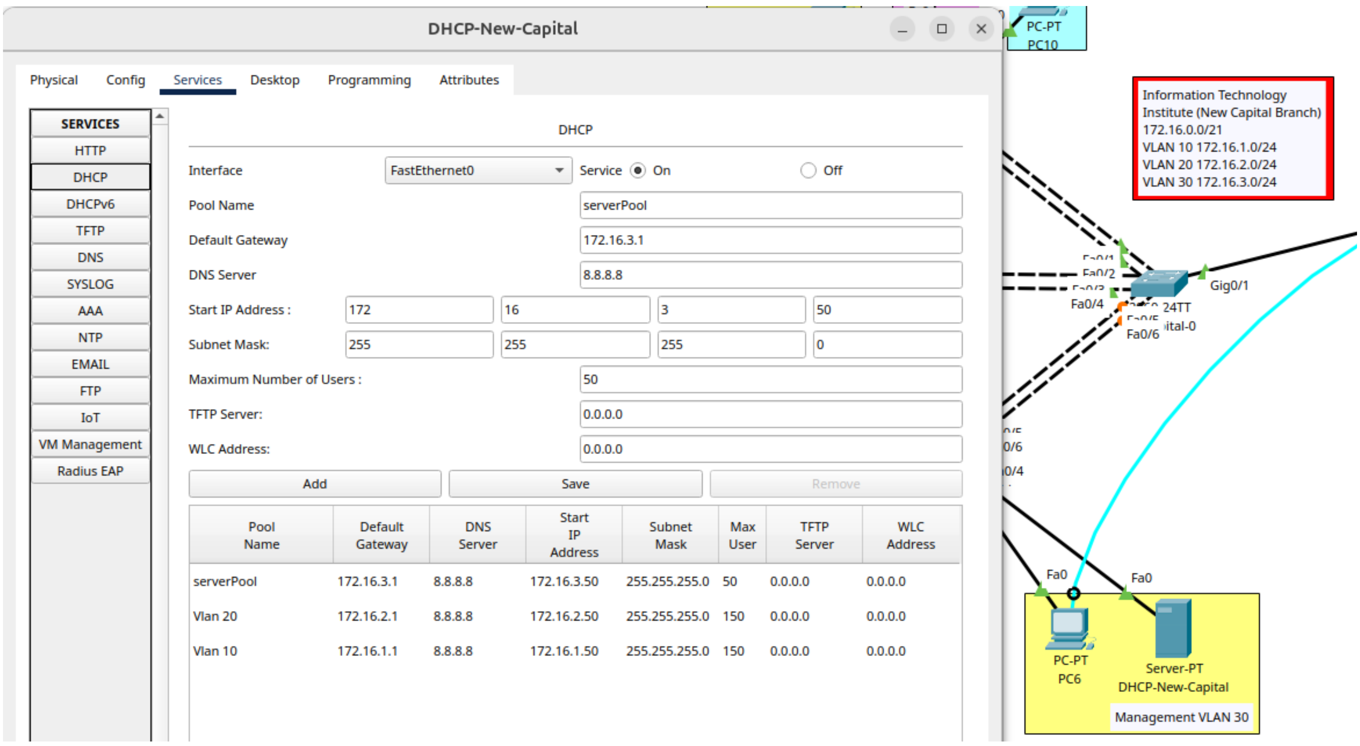
- **Routing Method: Switched Virtual Interfaces (SVI)** were used on the Core Multilayer Switches to perform hardware-based Inter-VLAN routing.
- **DHCP Relay:** The `ip helper-address` command was configured on the VLAN interfaces (SVI 10 & 20) to forward requests to the central DHCP server.



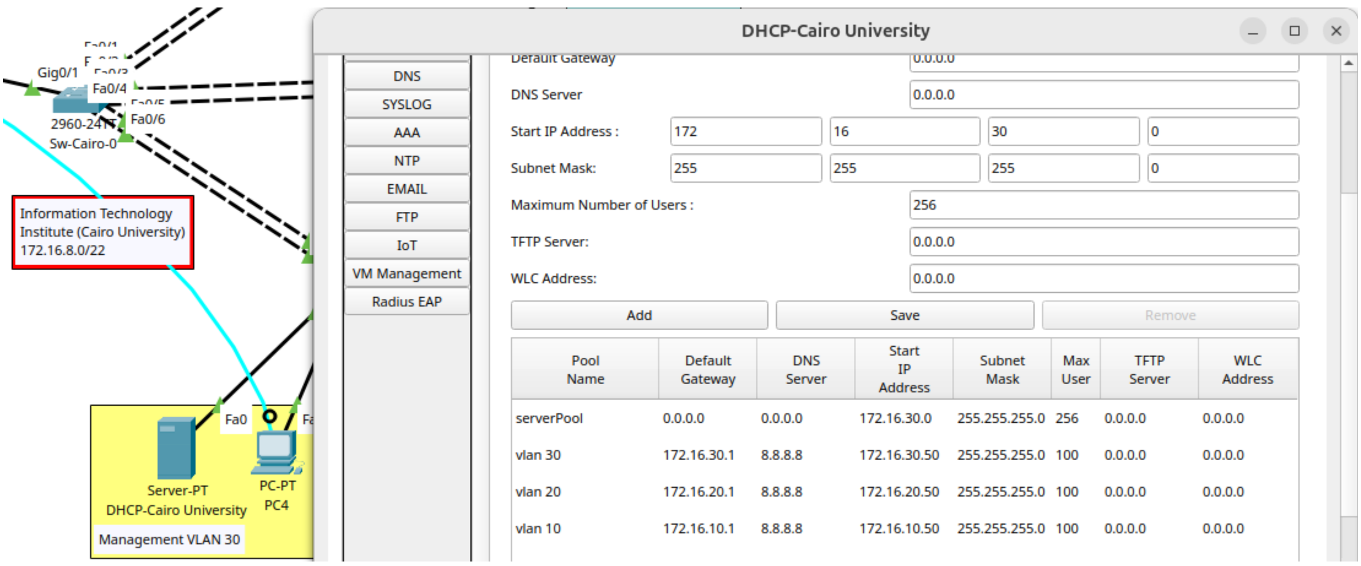
2. Remote Branches (New Capital & Cairo Univ): ROAS

- **Routing Method:** Due to the use of Layer 2 switches in these branches, **Router-on-a-Stick (ROAS)** was implemented on the Edge Routers.
    - **Configuration:** The router's physical interface connected to the switch is divided into logical **Sub-interfaces** (e.g., `G0/0.10`, `G0/0.20`).
    - **Encapsulation: IEEE 802.1Q** encapsulation was enabled on each sub-interface to tag and route traffic between VLANs.

2.1 New Capital Branch:



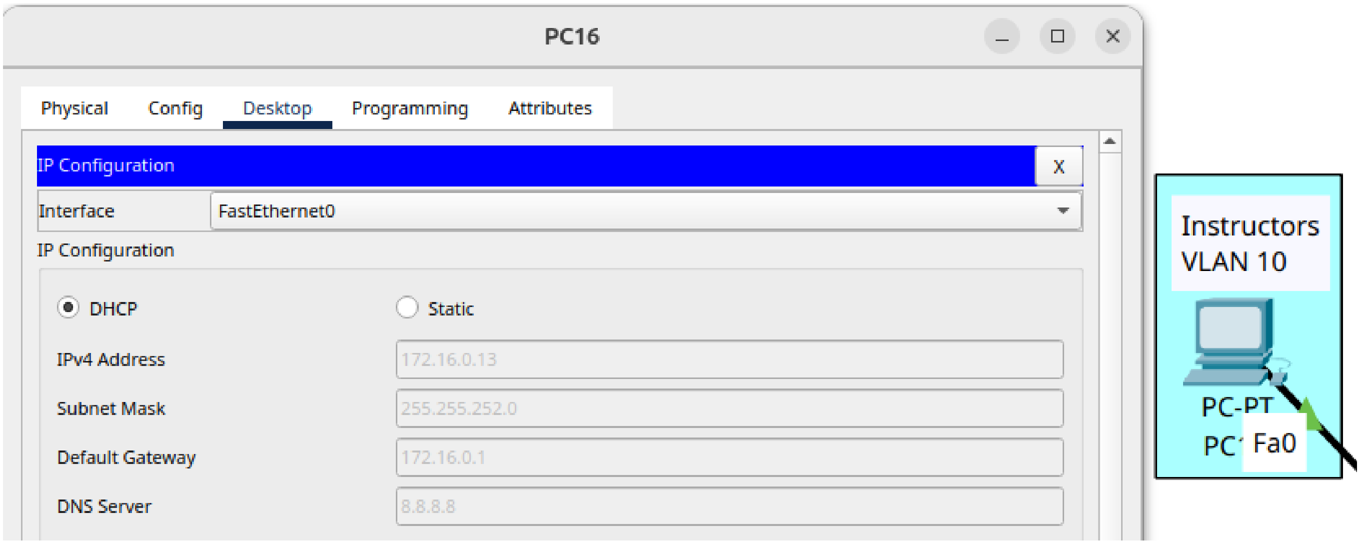
2.2 Cairo University Branch:



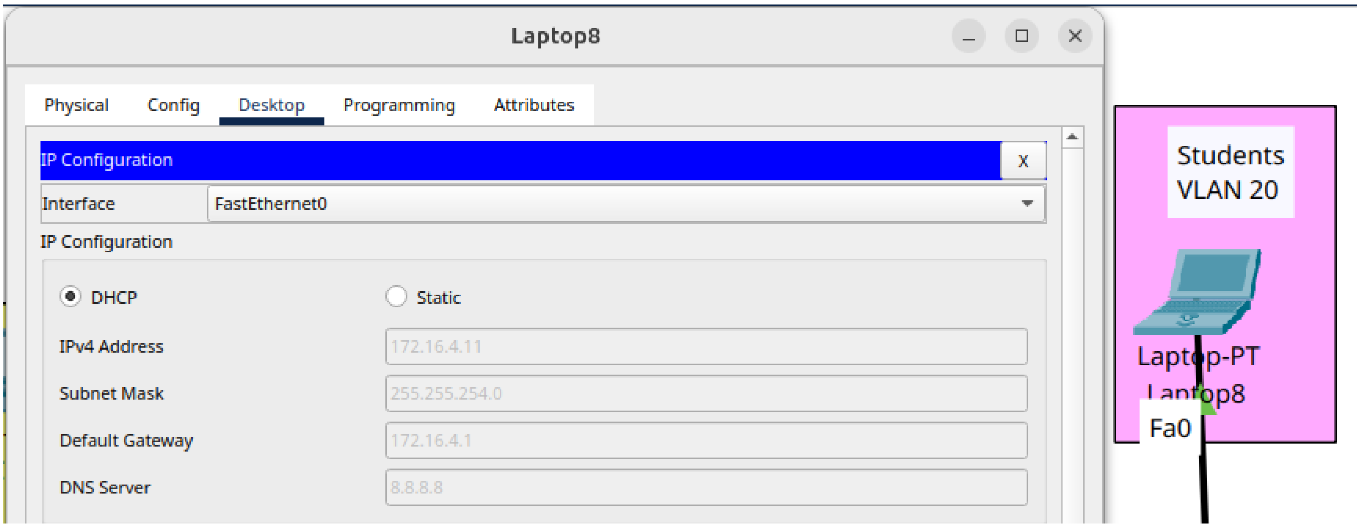
Comparison of Routing Implementations:

Feature	***Main Branch***	***Remote Branches (New Capital / Cairo)***
Routing Device	**Multilayer Switch (Core)**	**Edge Router (ISR)**
Method	**SVI (Interface VLAN)**	**Router-on-a-Stick (Sub-interfaces)**
DHCP Relay Point	**On SVI Interface**	**On Router Sub-interface**

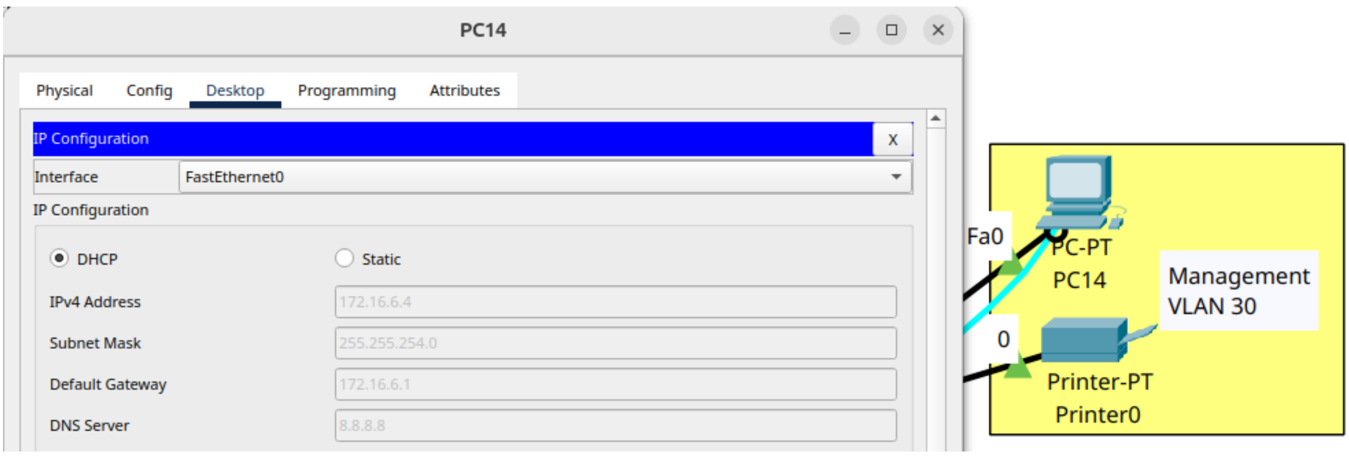
Assigning Dynamic Configuration for VLAN-10 (Instructors):



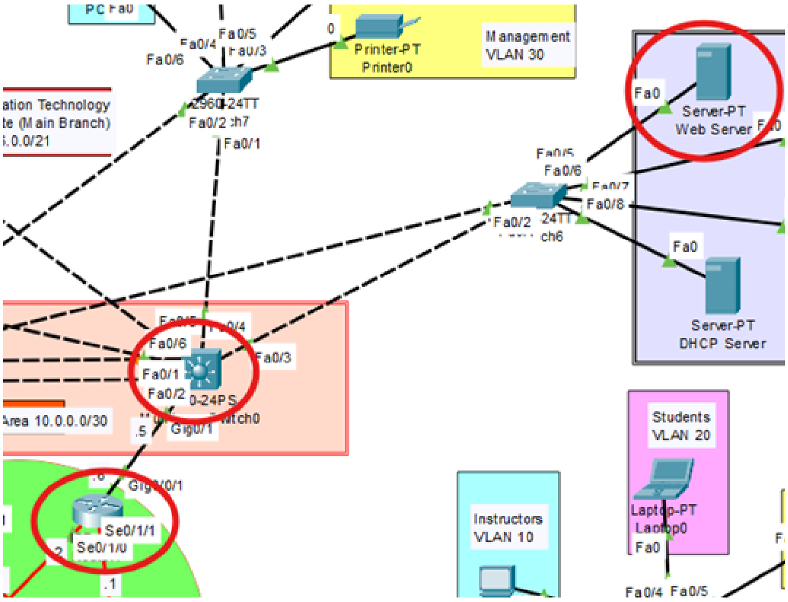
Assigning Dynamic Configuration for VLAN-20 (Students):



Assigning Dynamic Configuration for VLAN-30 (Management):



Static NAT Configuration



In this part of the project, we implemented static **Network Address Translation (NAT)** on the central core router to allow external access to the internal Web Server.The web server operates using a

Private IP: 172.16.6.5

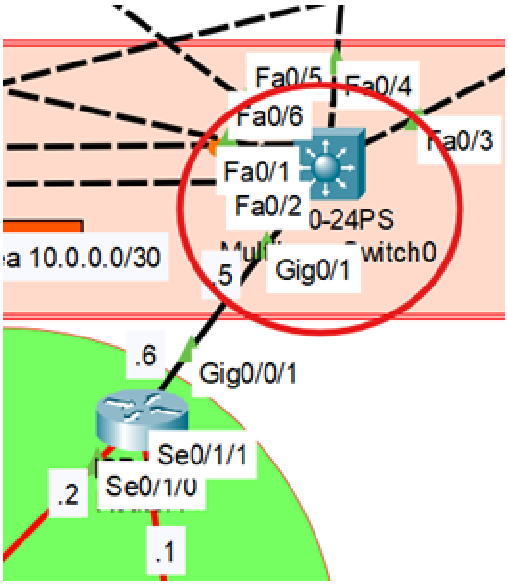
NetworkID: 172.16.6.0/23

Accessing the Internal Web Server After Configuring Static NAT The server is connected to an access switch, which uplinks to the multilayer core switch. From the core switch, traffic reaches Router R1.

Router R1 is the device connected to the outside world using a Public IP : **50.50.50.2.**

NetworkID: 50.50.50.0/30

MultiLayer Switch



The Multilayer Switch handles all internal VLAN routing for all branches. However, the public network **50.50.50.0/30**, which contains the router's public IP (50.50.50.2), does **not** exist inside the LAN.

The Multilayer Switch must know how to reach this public network so that traffic destined for the Web Server's NAT translation can reach Router R1 correctly.

Add a route in the Multilayer Switch

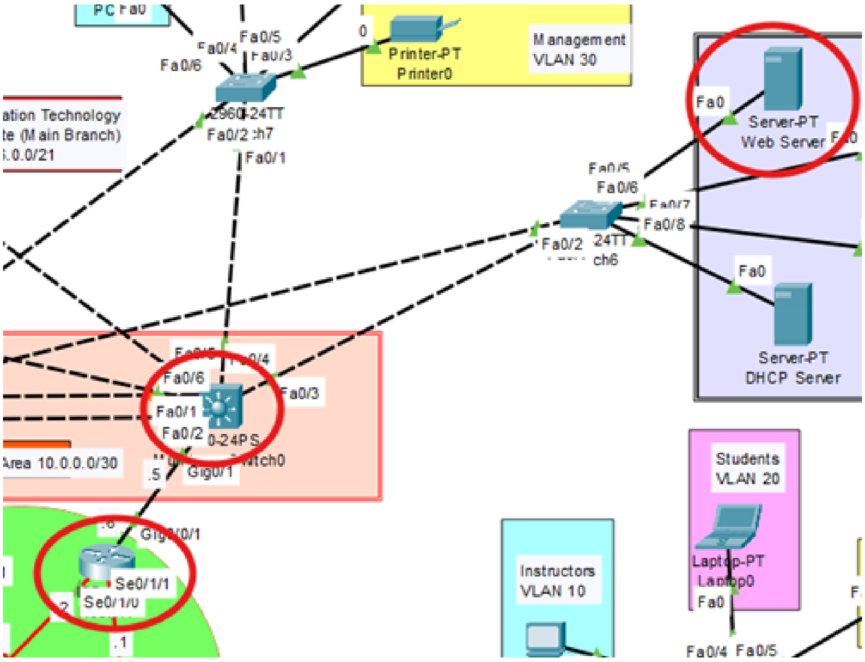
- We add this default route so that whenever the device receives traffic destined to a network that is not found in its routing table the MLS must forward traffic toward a next-hop device.

```
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/2
```

- Router R1 is connected to the MLS using an internal IP. The MLS reaches Router R1 through the next-hop **10.0.0.6**.

```
ip route 50.50.50.0 255.255.255.252 10.0.0.6
```

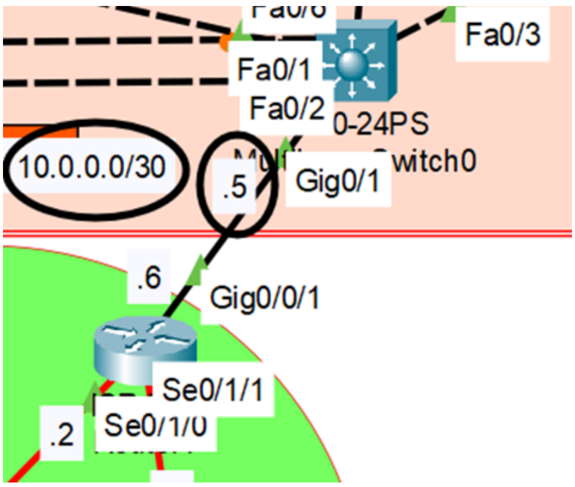
Router R1



The Server’s Network Is NOT Directly Connected to R1.

The server’s network is connected to: **Server → Switch → MLS → R1**

Since it’s not directly on R1’s interfaces so we need to give it the path to reach the server’s network.




```
ip route 172.16.6.0 255.255.254.0 10.0.0.5
```

172.16.6.0 is the network of the server I want to reach, 10.0.0.5 is the next hop of the MLS that will help me reach it.

Configure Static NAT Mapping on Router R1

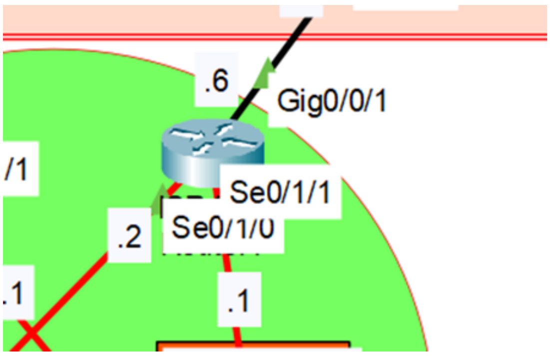
Now we are mapping the server's private IP to the router's public IP.

```
ip nat inside source static tcp 172.16.6.5 80 50.50.50.2 80
ip nat inside source static tcp 172.16.6.70 21 50.50.50.2 21
```

Any external user trying to access `50.50.50.2` on port 80 will be **forwarded to the internal server** `172.16.6.5` on port 80.

External users connecting to `50.50.50.2` on port 21 are forwarded to the internal FTP server at `172.16.6.70` on port 21.

Identify NAT Inside and Outside Interfaces on Router R1



When we configure NAT on a router, we must tell the router which interface is "inside" and which interface is "outside."

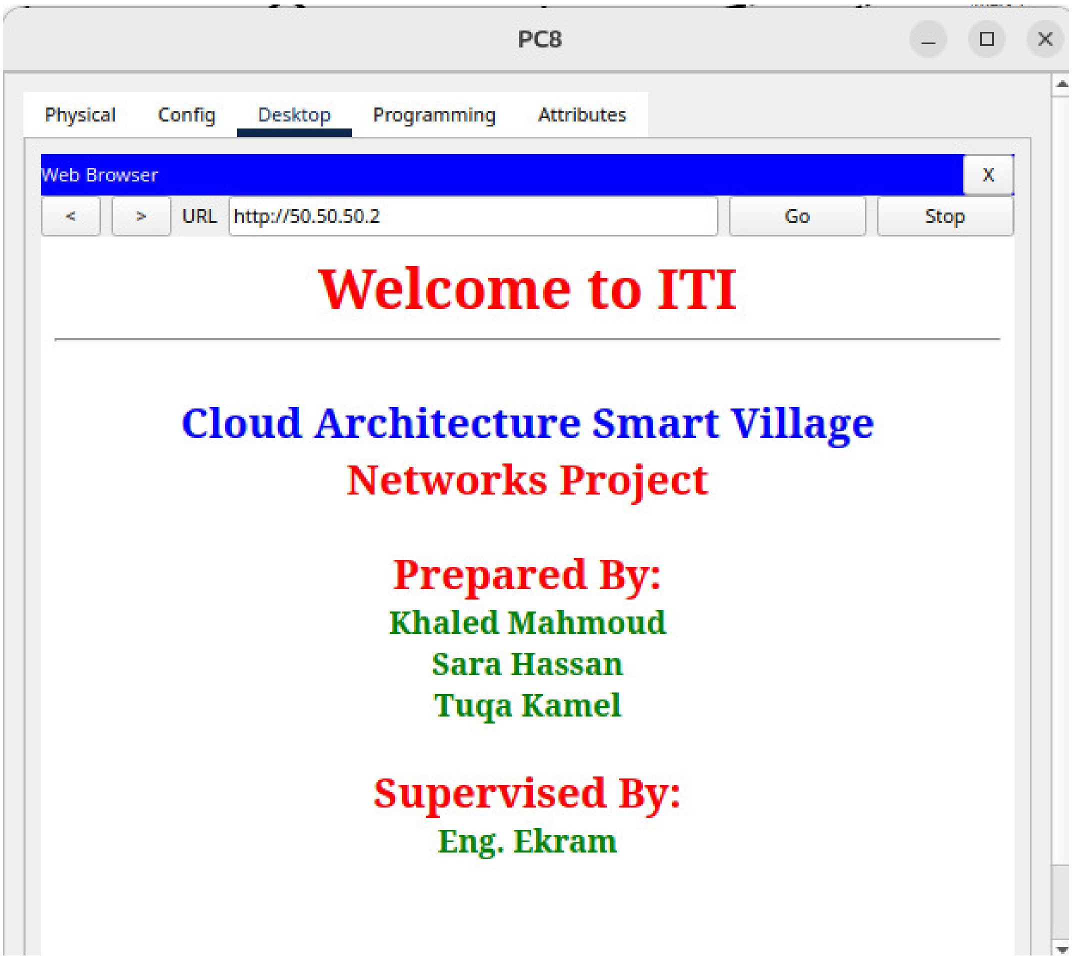
Inside Network → Private network

```
interface GigabitEthernet0/0/1
 ip address 10.0.0.6 255.255.255.252
 ip nat inside
```

Outside Network → Public network

```
interface Serial0/1/0
 ip address 50.50.50.2 255.255.255.252
 ip nat outside

interface Serial0/1/1
 ip address 70.70.70.1 255.255.255.252
 ip nat outside
```

Accessing the Internal Web Server After Configuring Static NAT



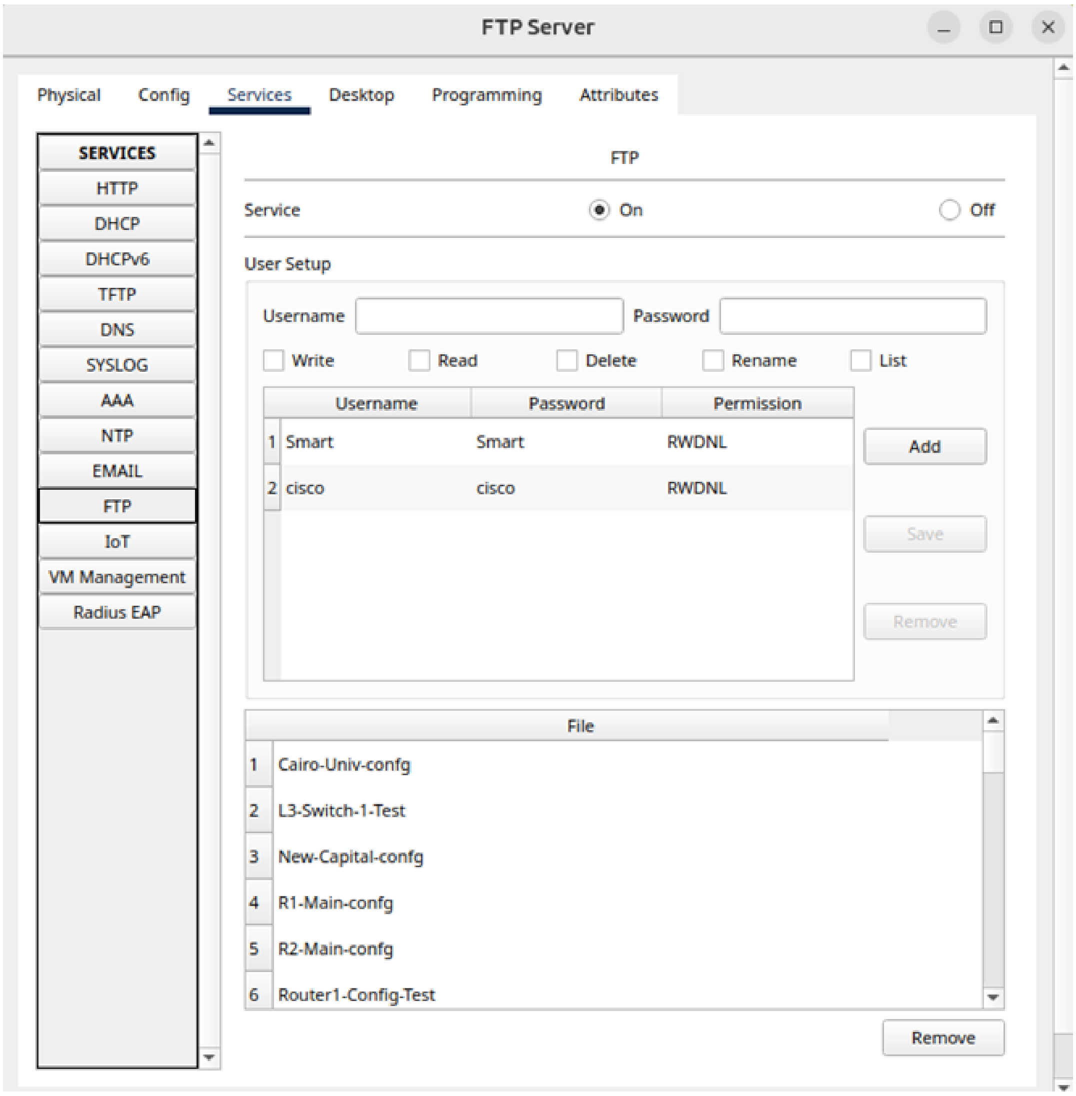
After configuring static NAT on the router, the internal web server became accessible using the public IP address.

When I typed http://50.50.50.2 into the browser, the router matched this request with the NAT rule that maps public IP **50.50.50.2** on port **80** to the internal server **172.16.6.5** on port **80**. The router translated the destination address, forwarded the request to the internal web server, and then translated the response back to the public IP before sending it to my PC.

As a result, the web page stored on the internal server successfully loaded, displaying the “Welcome to ITI” homepage. This confirms that the static NAT configuration and port-forwarding are functioning correctly.

FTP Configuration

To ensure that all device configurations in the ITI network can be saved, backed up, and restored easily, We configured FTP (File Transfer Protocol) on all four routers and the two multilayer switches. FTP provides a simple and reliable method to transfer configuration files between the network devices and the FTP server.



For authentication, I created a local FTP user account on each router and Multilayer Switch using the username **Smart** and password **Smart**. This user has the required privilege level to allow FTP file transfers.

<u>FTP Configuration Commands on all Routers</u>

```
ip ftp username Smart
ip ftp password Smart
```

<u>FTP Configuration Commands on all Multilayer switches</u>

```
ip ftp username Smart
ip ftp password Smart
```

Then, we enabled the FTP server function on the devices so they can act as FTP servers and accept incoming file transfers.

With this setup, any device in the network can save its configuration by using the **copy running-config ftp**: command on any Router or Multilayer switch.

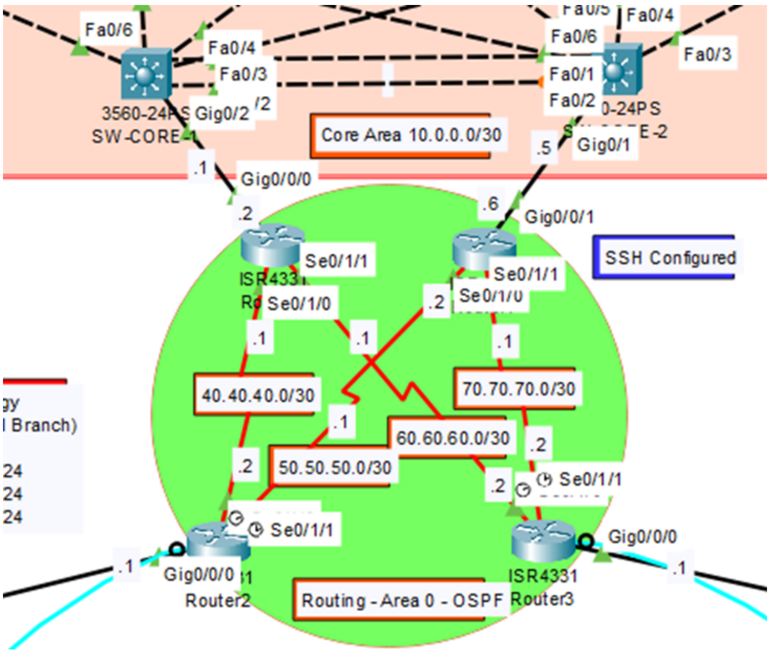
```
R1-Main#copy running-config ftp:
Address or name of remote host []? 172.16.6.70
Destination filename [R1-Main-confg]? Router1-Config-Test

Writing running-config...
[OK - 1768 bytes]

1768 bytes copied in 0.071 secs (24000 bytes/sec)
```

```
SW-Core-1#copy running-config ftp:
Address or name of remote host []? 172.16.6.70
Destination filename [SW-Core-1-confg]? L3-Switch-1-Test

Writing running-config...
[OK - 2677 bytes]

2677 bytes copied in 0.056 secs (47000 bytes/sec)
```

This approach ensures that if any router or switch fails, the saved configuration can be restored instantly without reconfiguring everything from the beginning. It also standardizes management across all branches **Smart, Cairo**, **and New Capital** by ensuring configuration backups are always available.

	File
1	Cairo-Univ-confg
2	L3-Switch-1-Test
3	New-Capital-confg
4	R1-Main-confg
5	R2-Main-confg
6	Router1-Config-Test

Enabling AAA Services



The first step in securing the network devices is enabling the AAA service on each router and multilayer switch.

Activating AAA means the device will no longer rely on simple console or vty passwords; instead, it will use a structured authentication system based on users, and methods.

By enabling AAA on all six devices, we are enforcing a unified authentication mechanism across the entire network to prevent unauthorized people from accessing or modifying device configurations.

Configuration for each of 6 devices

First, we need to enable the AAA feature on the device.

```
aaa new-model
```

Create local usernames and passwords

Since we're doing local authentication, we define users directly on the device:

```
username admin privilege 15 secret 5 $1$mERr$vTbHul1N28cEp8lkLqr0f/
```

privilege 15 → full admin access.

Username: admin

Password: admin

Apply AAA locally for login

```
aaa authentication login default local
```

Apply authentication to lines

To ensure anyone logging in either physically (console) or remotely (VTY) must enter the correct local username/password.

```
line con 0
 login authentication default
!
line aux 0
!
line vty 0 4
 login authentication default
 transport input ssh
```

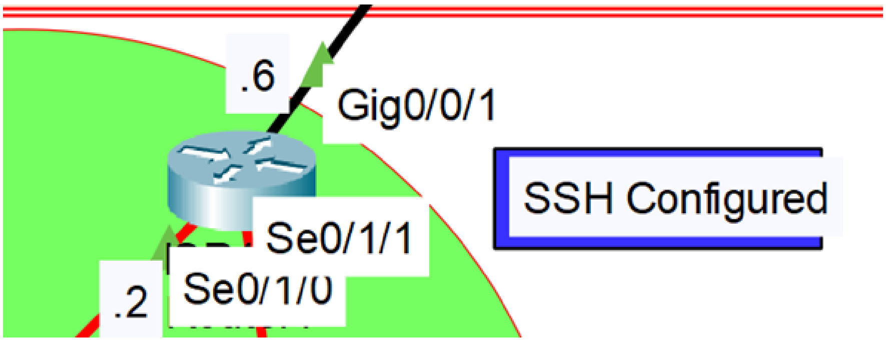
Now that the AAA is applied lets check it on **Router 2 (Cairo Branch)**

```
User Access Verification

Username: admin
Password:
Cairo-Univ>
```

Pc8 in New Capital Branch accessing Router 3

```
C:\>telnet 60.60.60.2
Trying 60.60.60.2 ...Open

User Access Verification

Username: admin
Password:
Cairo-Univ>
Cairo-Univ>
```

SSH on Router R1



To configure SSH we need to do those steps

- Enable secret enabled
- Username & password
- Encryption key generation
- Enabling SSH on the vty lines

We configured the username & password and enabled the ssh on vty lines in the AAA setup

Enable secret enabled

```
enable secret 5 $1$mERr$vTbHul1N28cEp8lkLqr0f/
```

Encryption key generation

```
hostname R1-Main
```

```
ip domain-name R1-Smart.local
```

The hostname and domain is used to identify the router

```
crypto key generate rsa
```

We used it to generate the key

Enable SSH Version 2

```
ip ssh version 2
```

Version 2 is more secure. This ensures encrypted communication.

Accessing Router R1 from pc 8 in New Capital Branch using SSH

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l admin 50.50.50.2

Password:
R1-Main>
R1-Main>en
Password:
R1-Main#
R1-Main#
```