

**TEXAS COLLEGE OF MANAGEMENT AND IT**

***Bachelors in Information Technology***

**Project I of Advanced Computer Network**

**Project Title**: Secure Campus Network Design with Multi-Department Connectivity

**SUBMITTED BY: SUBMITTED TO:**

Merry Subedi Kripesh Shrestha Sir

BIT 1st year 2nd SEM Department of Computer Network

SECTION: “E” Date of Submission:15th July, 2025

LCID:LC00017003482

**TABLE OF CONTENTS**

Contents

[**1.** **INTRODUCTION** 3](#_Toc204197804)

[**2.** **OBJECTIVE** 4](#_Toc204197805)

[**3.** **TOOLS and TECHNOLOGIES USED** 4](#_Toc204197806)

[**4.** **NETWORK DESIGN OVERVIEW** 5](#_Toc204197807)

[**5.** **IMPLEMENTATION PLAN** 13](#_Toc204197808)

[**5.1 Phase 1: Basic Infrastructure Setup** 13](#_Toc204197809)

[**5.2 Phase 2: Distribution Layer Design** 13](#_Toc204197810)

[**5.3 Phase 3: Access Layer Implementation** 14](#_Toc204197811)

[**5.4 Phase 4: Advanced Features Deployed** 14](#_Toc204197812)

[**5.5 Phase 5: Security and Management** 14](#_Toc204197813)

[**6. SECURITY POLICIES** 15](#_Toc204197814)

[**Traffic Segmentation and Control** 15](#_Toc204197815)

[**Inter-Department Security Policies** 15](#_Toc204197816)

[**Device-Level Security** 16](#_Toc204197817)

[**Authentication and Access Control** 16](#_Toc204197818)

[**Remote Access Protection** 17](#_Toc204197819)

[**Port-Level Security** 17](#_Toc204197820)

[**Physical Access Control** 17](#_Toc204197821)

[**6.** **NETWORK MONITORING SETUP** 17](#_Toc204197822)

[**SNMP Security Implementation** 17](#_Toc204197823)

[**Centralized Logging and Time Synchronization** 18](#_Toc204197824)

[**Why This Security Approach Works** 18](#_Toc204197825)

[**8. TROUBLESHOOTING STRATEGY** 18](#_Toc204197826)

[**8.1 Common Network Issues and Solutions** 18](#_Toc204197827)

[**9. TESTING AND RESULTS** 26](#_Toc204197828)

[**10. CHALLENGES AND RESOLUTIONS** 28](#_Toc204197829)

[**11. CONCLUSION** 34](#_Toc204197830)

[**12. REFERENCES** 37](#_Toc204197831)

[**13. APPENDIX** 38](#_Toc204197832)

[**DECLARATION OF ORIGINALITY** 60](#_Toc204197833)

# **INTRODUCTION**

This project illustrates secure, scalable Campus Area Network (CAN) solution deployment in Texas College of Management and IT. The network integrates four important departments: Administrative Block, Academic Block, Library and Hostel into one campus and provides reliable communications and internet access along with security at all levels.

The network structure assumes the use of OSPF (Open Shortest Path First) dynamic routing, as well as NAT (Network Address Translation) for the path Internet, Access Control Lists (ACL) for traffic filtrations, and monitors network work by the protocol SNMP and Syslog. The topology is hierarchical with three layers model (Core, Distribution, Access), in order to scale and manage the architecture.

It tackles real-life networking issues such as inter-department security policy, network monitoring, time synchronization, and fault tolerance, giving navigational experience to enterprise network design as well as cybersecurity.

# **OBJECTIVE**

**Primary Objectives:**

* Design and simulate secure hierarchical campus network for all major departments.
* Deploy OSPF routing protocol for optimized and dynamic intra-campus routing.
* NAT service deployment for internet access with controlled security requirements
* Use full ACL policies to control and secure inter-department traffic
* Create a network monitoring system with SNMP and Syslog
* Deploy NTP services for network wide time sync

**Secondary Objectives:**

* Show how they can use VLANs for segmentation for each department.
* Enable device security in the form of password and SSH encryption.
* Design a network with redundant paths to avoid point of failure
* Create extensive documentation and troubleshooting articles
* Emulate and remediate typical network weaknesses

# **TOOLS and TECHNOLOGIES USED**

**Software Tools:**

* Cisco Packet Tracer 8.2+ - The main network simulator used for the course
* Draw. io - Draw network topology diagrams online!

**Network Protocols and Technologies:**

* OSPF (Open Shortest Path First) - A dynamic routing protocol
* NAT/PAT: Internet access (network address translation/port address translation)
* Vlans- Aka network Segmentation
* ACLs - Traffic Filtering and Security
* SNMP - Network monitoring.
* Syslog - Centralized logging
* NTP is used for time synchronization.
* SSH (Secure Shell) - Secure Access to Remote Session

**Hardware Components (Simulated):**

* Cisco 2811 Routers - Core and distribution layer routing
* Cisco 2960 Switches - Access layer switching
* Cisco ASA 5505 - Firewall and security appliance
* Servers - DHCP, DNS, Web, Syslog, NTP servers

# **NETWORK DESIGN OVERVIEW**

**4.1 Network Topology**

The network within the campus is a three-tier network, comprising:

***Core Layer:***

* Backbone router (Router-Core) to which all distribution routers are attached
* High-speed backbone connectivity
* Redundant paths for fault tolerance

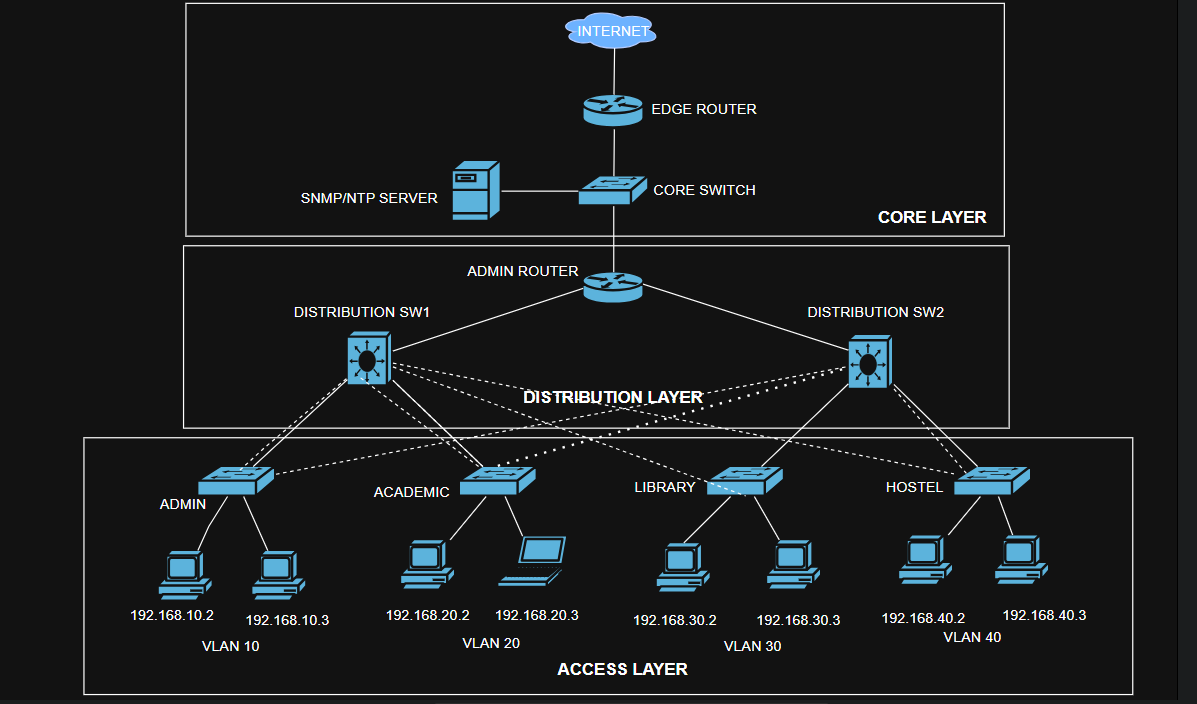
***Distribution Layer:***

* Department Level Routers (Router-Admin, Router-Academic, Router-Library, Router-Hostel)
* Inter-VLAN routing capabilities
* Policy enforcement points

***Access Layer:***

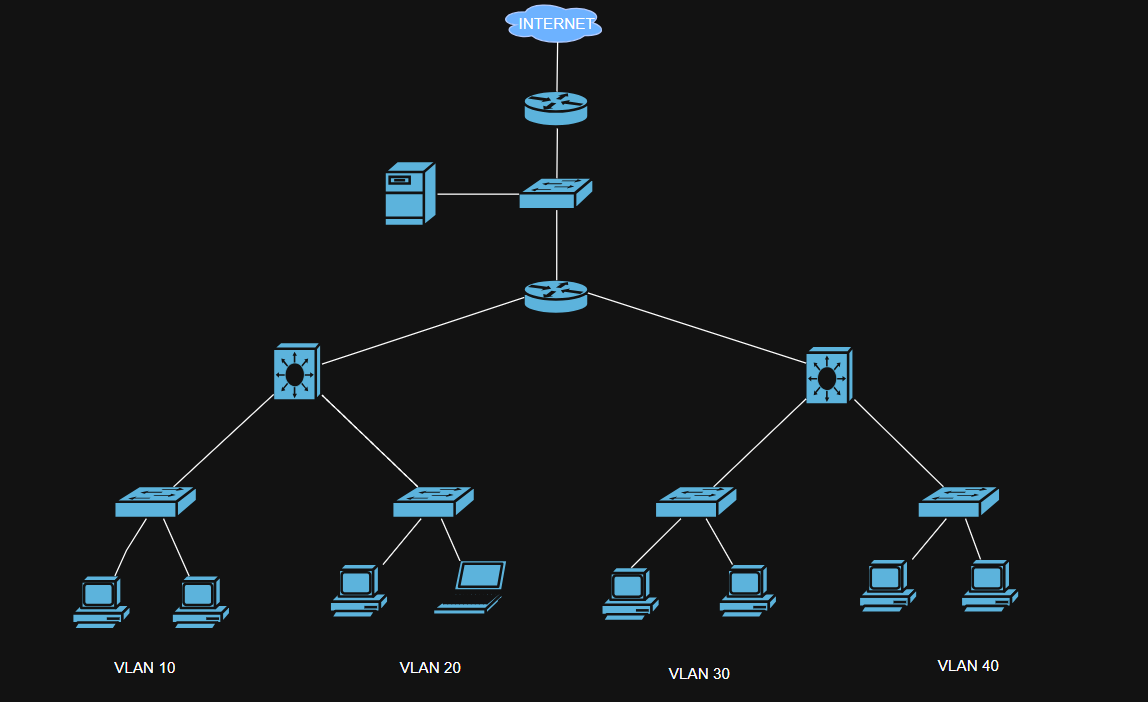
* Access switches for end-user connectivity
* VLAN assignment and port security
* PoE for IP phones and access points

**Here’s the logical topology**

****

*Built using draw.io*

**Here’s the physical topology**

****

**4.2 IP Addressing Scheme**

**Network Allocation:**

**Core Network Infrastructure:**

* **Edge Router to Internet**: DHCP assigned (simulated public IP)
* **Edge Router to Core**: 10.0.0.1/30 (10.0.0.0/30 subnet)
* **Core Switch**: 10.0.0.2/30

**Point-to-Point Links:**

* **Edge Router ↔ Core Switch**: 10.0.0.0/30
  + Edge Router G0/0/1: 10.0.0.1/30
  + Core Switch: 10.0.0.2/30
* **Core ↔ Admin Router**: 10.0.0.4/30
  + Core: 10.0.0.5/30
  + Admin Router G0/0: 10.0.0.6/30
* **Admin Router ↔ Distribution SW1**: 10.0.0.8/30
  + Admin Router G0/1: 10.0.0.9/30
  + Distribution SW1: 10.0.0.10/30
* **Admin Router ↔ Distribution SW2**: 10.0.0.12/30
  + Admin Router G0/2: 10.0.0.13/30
  + Distribution SW2 G0/1: 10.0.0.14/30

**VLAN Networks:**

* **VLAN 10 (Admin Block)**: 192.168.10.0/24
  + Gateway: 192.168.10.1
  + Usable range: 192.168.10.2-192.168.10.254
* **VLAN 20 (Academic Block)**: 192.168.20.0/24
  + Gateway: 192.168.20.1
  + Usable range: 192.168.20.2-192.168.20.254
* **VLAN 30 (Library Block)**: 192.168.30.0/24
  + Gateway: 192.168.30.1
  + Usable range: 192.168.30.2-192.168.30.254
* **VLAN 40 (Hostel Block)**: 192.168.40.0/24
  + Gateway: 192.168.40.1
  + Usable range: 192.168.40.2-192.168.40.254
* **VLAN 99 (Management)**: 192.168.99.0/24
  + Gateway: 192.168.99.1
  + Management servers: 192.168.99.10-192.168.99.50

**Server Assignments:**

* **SNMP/NTP Server**: 192.168.99.10/24
* **Syslog Server**: 192.168.99.20/24
* **DNS Server**: 192.168.99.30/24
* **DHCP Server**: 192.168.99.40/24

**4.3 VLAN DESIGN**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| VLAN ID | Department | Network | Gateway | Subnet Mask | Description |
| 10 | Admin | 192.168.10.0/24 | 192.168.10.1 | 255.255.255.0 | Administrative staff and servers |
| 20 | Academic | 192.168.20.0/24 | 192.168.20.1 | 255.255.255.0 | Faculty and academic resources |
| 30 | Library | 192.168.30.0/24 | 192.168.30.1 | 255.255.255.0 | Library systems and public access |
| 40 | Hostel | 192.168.40.0/24 | 192.168.40.1 | 255.255.255.0 | Student residential network |
| 99 | Management | 192.168.99.0/24 | 192.168.99.1 | 255.255.255.0 | Network management and monitoring |

**4.4 Device IP Assignments**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Device | Interface | IP Address | Subnet Mask | VLAN | Description |
| Edge Router | G0/0/0 | DHCP | - | - | To Internet |
| Edge Router | G0/0/1 | 10.0.0.1 | 255.255.255.252 | - | To Core Switch |
| Core Switch | - | 10.0.0.2 | 255.255.255.252 | - | Management IP |
| Admin Router | G0/0 | 10.0.0.6 | 255.255.255.252 | - | To Core |
| Admin Router | G0/1 | 10.0.0.9 | 255.255.255.252 | - | To Dist SW1 |
| Admin Router | G0/2 | 10.0.0.13 | 255.255.255.252 | - | To Dist SW2 |
| Distribution SW1 | G0/1 | 10.0.0.10 | 255.255.255.252 | - | To Admin Router |
| Distribution SW2 | G0/1 | 10.0.0.14 | 255.255.255.252 | - | To Admin Router |
| Admin Switch | VLAN 99 | 192.168.99.11 | 255.255.255.0 | 99 | Management |
| Academic Switch | VLAN 99 | 192.168.99.12 | 255.255.255.0 | 99 | Management |
| Library Switch | VLAN 99 | 192.168.99.13 | 255.255.255.0 | 99 | Management |
| Hostel Switch | VLAN 99 | 192.168.99.14 | 255.255.255.0 | 99 | Management |

**4.5 OSPF Area Design**

* **Area 0 (Backbone):** All routers participate in single area design
* **Router IDs:** Manually configured using loopback interfaces
* **Network Types:** Point-to-point for WAN links, broadcast for LAN segments

# **IMPLEMENTATION PLAN**

The network implementation follows a hierarchical three-tier architecture for Texas College, providing structured connectivity across four main building blocks: Admin, Academic, Library, and Hostel areas.

## **5.1 Phase 1: Basic Infrastructure Setup**

The **Edge Router** serves as the primary gateway, handling internet connectivity through DHCP on the external interface while maintaining internal connectivity via static IP addressing (10.0.0.1/30). NAT overload enables internet access for all internal networks, with OSPF providing dynamic routing throughout the campus. Security measures include SSH access only, encrypted passwords, and comprehensive logging to a centralized server.

The **Core Switch** functions as the central switching hub, configured as a VTP server managing five VLANs (Admin-10, Academic-20, Library-30, Hostel-40, Management-99). It maintains trunk connections to all distribution layer devices and handles VLAN propagation across the network. The management VLAN (99) provides dedicated administrative access with the subnet 192.168.99.0/24.

## **5.2 Phase 2: Distribution Layer Design**

An **Admin Router** creates redundant connectivity between the core and distribution switches, implementing OSPF with router-id 3.3.3.3. This device ensures high availability by providing dual paths to critical network segments.

**Distribution Switch 1** connects to Admin and Academic areas using EtherChannel technology (Port-channels 1 and 2) for increased bandwidth and redundancy. It operates as a VTP client and implements Rapid Spanning Tree Protocol with priority 4096 for optimal traffic flow.

**Distribution Switch 2** services the Library and Hostel blocks through similar EtherChannel configurations (Port-channels 3 and 4). It maintains VTP client status and uses RSTP priority 8192, creating a balanced load distribution with the first distribution switch.

## **5.3 Phase 3: Access Layer Implementation**

Each building block has dedicated access switches configured identically in structure but customized for their specific VLAN assignments:

**Admin Switch** provides 20 access ports on VLAN 10 with port security limiting each port to 2 MAC addresses. Dual trunk connections (Fa0/23-24) ensure redundancy to the distribution layer.

**Academic Switch** mirrors the admin configuration but assigns ports to VLAN 20, supporting classroom and faculty connectivity requirements.

**Library Switch** connects library resources to VLAN 30, maintaining the same redundancy and security standards as other access switches.

**Hostel Switch** serves student residential areas on VLAN 40, implementing identical security policies and redundant uplinks.

## **5.4 Phase 4: Advanced Features Deployed**

**VTP (VLAN Trunking Protocol)** maintains consistent VLAN information across all switches, with the core switch serving as the authoritative server and all others as clients receiving updates automatically.

**EtherChannel (LACP)** combines multiple physical links into logical channels, doubling bandwidth between distribution and access layers while providing automatic failover capabilities.

**OSPF Routing** enables dynamic path selection and automatic rerouting during link failures, with each router maintaining unique router-ids for network identification.

**Port Security** prevents unauthorized device connections by limiting MAC addresses per port and taking restrictive action against violations.

**Spanning Tree Protocol** (Rapid-PVST+) eliminates switching loops while maintaining redundant paths, with carefully planned priority settings ensuring optimal traffic flows.

## **5.5 Phase 5: Security and Management**

All devices implement standardized security including encrypted enable passwords, local user accounts, SSH-only remote access, and domain-based authentication. Comprehensive monitoring sends logs to 192.168.99.20, SNMP data to 192.168.99.10, and synchronizes time with NTP server 132.163.96.1.

The management VLAN (99) provides dedicated administrative access to all network devices, isolated from user traffic for enhanced security and reliable network administration.

This implementation creates a robust, scalable network infrastructure supporting current needs while providing foundation for future expansion across the Texas College campus.

# **6. SECURITY POLICIES**

When securing this network, we implemented a multi-layered security approach that controls traffic flow, protects device access, and monitors network activity. Here's what we put in place and why each policy matters.

## **Traffic Segmentation and Control**

The backbone of our security strategy revolves around **Access Control Lists (ACLs)** that act like digital security guards, controlling which departments can communicate with each other.

### **Inter-Department Security Policies**

We created specific security zones for each department with carefully crafted rules:

**Admin Block Security** - The administrative network has the most restrictive policies since it handles sensitive college data. We completely blocked admin users from accessing the hostel network (students shouldn't reach administrative systems), but allowed them to communicate with academic and library resources since they need to coordinate with faculty and access educational materials. The policy permits admin traffic to reach the internet for external communications while denying everything else by default.

**Hostel Block Security** - Student networks have limited access by design. We blocked students from reaching administrative systems entirely (they don't need access to payroll or student records systems), but allowed them to access library resources for research and studying. Students can still reach the internet for educational and personal use, but the default deny rule prevents unauthorized access to other internal networks.

**Academic Block Security** - Faculty and classroom systems have broader access since education requires coordination across departments. Academic users can reach administrative systems for grade submission and student information, access library resources for research, and connect to external educational resources. This reflects the collaborative nature of academic work.

**Library Access Policy** - The library network has unique requirements since it serves both internal users and potentially public access. We implemented service-specific rules allowing HTTP (port 80) and HTTPS (port 443) for web browsing, FTP (port 21) for file transfers, and SSH (port 22) for secure remote access. ICMP is permitted for network diagnostics, but everything else is blocked to prevent misuse of public access points.

**How ACLs Work in Practice**

These ACLs are applied to VLAN interfaces as either inbound or outbound filters. For example, when someone in the admin network (VLAN 10) tries to send traffic, the outbound ACL checks each packet against the ADMIN-SECURITY rules. If a packet matches a "permit" rule, it's allowed through. If it matches a "deny" rule, it's dropped. The final "deny ip any any" ensures that anything not explicitly permitted is blocked.

## **Device-Level Security**

### **Authentication and Access Control**

Every network device implements multiple layers of access security:

**Privileged Access** - We configured encrypted enable secrets that administrators must enter to gain full device control. The secret "cisco123" is hashed using strong encryption, making it nearly impossible for someone to discover the password even if they gain access to the configuration file.

**User Account Management** - We created role-based accounts: the "admin" user has full privileges (level 15) for complete device management, while the "operator" user has limited privileges (level 1) for basic monitoring tasks. This follows the principle of least privilege - users only get the access they actually need.

**Console Security** - Physical access to devices is protected with console passwords and automatic timeouts. After 10 minutes of inactivity, the console session automatically terminates, preventing unauthorized access if someone walks away from a logged-in session.

## **Remote Access Protection**

**SSH-Only Access** - We disabled insecure telnet completely and configured SSH version 2 for all remote management. SSH encrypts all communication between administrators and network devices, preventing password interception and session hijacking.

**Domain-Based Authentication** - By setting the domain name to "texascollege.edu" and generating RSA keys, we created a secure foundation for SSH that's tied to the college's identity.

**Session Management** - VTY lines (virtual terminal sessions) automatically timeout after 10 minutes of inactivity, and logging synchronous prevents command output from interrupting typed commands, reducing administrative errors.

## **Port-Level Security**

### **Physical Access Control**

On every access switch, we implemented **port security** that learns and remembers the MAC addresses of connected devices:

**MAC Address Limiting** - Each port can only learn a maximum of 2 MAC addresses. This prevents someone from connecting an unauthorized hub or switch to multiply their network access.

**Sticky MAC Learning** - Once a device connects, its MAC address is "stuck" to that port and saved in the configuration. This means authorized devices maintain their access, but unauthorized devices are automatically blocked.

**Violation Response** - When someone tries to connect more devices than allowed, the port enters "restrict" mode, dropping packets from unauthorized MAC addresses while keeping legitimate traffic flowing. This prevents network disruption while maintaining security.

# **NETWORK MONITORING SETUP**

## **SNMP Security Implementation**

We implemented both SNMP v2c and v3 for different monitoring needs:

**Community-Based Security (v2c)** - We used read-only community strings for basic monitoring and separate read-write communities for configuration changes. The "public" community provides read-only access for general monitoring, while "private" allows configuration changes for authorized management systems.

**Enhanced Security (v3)** - For sensitive monitoring, we configured SNMP v3 with strong authentication and encryption. The v3user account requires SHA authentication with "authpass123" and AES-128 encryption with "privpass123". This ensures that even if monitoring traffic is intercepted, it cannot be read or modified.

## **Centralized Logging and Time Synchronization**

**Syslog Security** - All devices send logs to 192.168.99.20, creating a centralized audit trail. Timestamps are synchronized via NTP to ensure accurate correlation of events across all devices.

**Management Network Isolation** - The management VLAN (99) provides a separate, secure channel for all administrative traffic, isolated from user networks.

## **Why This Security Approach Works**

This layered security model creates multiple barriers that potential attackers must overcome. Even if one security measure fails, others remain in place to protect the network. The policies reflect real-world usage patterns - administrators need broad access to do their jobs, students need limited access appropriate to their role, and public access points have the most restrictive policies.

The combination of network-level ACLs, device-level authentication, port-level security, and comprehensive monitoring creates a robust security posture that protects the college's digital infrastructure while allowing legitimate users to accomplish their educational and administrative goals efficiently.

# **8. TROUBLESHOOTING STRATEGY**

Effective troubleshooting is essential for maintaining a robust and reliable campus network. This section outlines common issues encountered in routing, VLANs, ACLs, and connectivity, along with their corresponding commands and resolution approaches.

## **8.1 Common Network Issues and Solutions**

**A. OSPF Troubleshooting**

**Common Issues and Real-World Scenarios:**

**1. OSPF Neighbor Adjacency Not Forming**

* **Symptoms**: Neighbors stuck in Init, 2-Way, or ExStart states
* **Common Causes**:
  + Interface administratively down or physically disconnected
  + Subnet mask mismatch between neighbors
  + OSPF network statement missing or incorrect
  + MTU mismatch between interfaces
* **Resolution Steps**:

//Check interface status

show ip interface brief

//Verify OSPF is enabled on interface

show ip ospf interface

//Check network statements

show running-config | section router ospf

//Fix example:

router ospf 1

network 192.168.10.0 0.0.0.255 area 0

**2. Area Mismatch**

* **Symptoms**: Neighbors appear in neighbor table but LSA exchange fails
* **Cause**: Different area IDs configured on connected interfaces
* **Resolution**:

! Check current area configuration

show ip ospf interface

! Correct area configuration

router ospf 1

network 192.168.10.0 0.0.0.255 area 0 ! Ensure same area

**3. Network Type Mismatch**

* **Symptoms**: DR/BDR election issues, neighbor state problems
* **Resolution**:

// Check current network type

show ip ospf interface

// Set matching network type

interface serial 0/0/0

ip ospf network point-to-point

**OSPF Verification Commands:**

show ip ospf neighbor

show ip ospf neighbor detail

show ip ospf interface

show ip ospf interface brief

show ip ospf database

show ip ospf database router

show ip route ospf

show ip protocols

debug ip ospf hello

debug ip ospf adj

**B. VLAN Troubleshooting**

**Common Issues and Solutions:**

**1. Port Not Assigned to VLAN**

* **Symptoms**: Device gets wrong IP via DHCP, can't reach gateway
* **Resolution**:

//Assign port to access VLAN

interface fastethernet 0/1

switchport mode access

switchport access vlan 10

! Verify port assignment

show interface fa0/1 switchport

**3. Trunk Port Misconfiguration**

* **Symptoms**: Inter-VLAN communication fails, some VLANs not passing
* **Common Issues**:
  + Trunk not enabled on both ends
  + VLAN pruning blocking required VLANs
  + Native VLAN mismatch
* **Resolution**:

// Configure trunk port

interface fastethernet 0/24

switchport mode trunk

switchport trunk allowed vlan 10,20,30,40

switchport trunk native vlan 99

// Verify trunk configuration

show interface trunk

show interface fa0/24 switchport

**VLAN Verification Commands:**

show vlan brief

show vlan id 10

show interface trunk

show interface fa0/1 switchport

show vtp status

show spanning-tree

show spanning-tree vlan 10

show mac address-table

**C. ACL Troubleshooting**

**Common Issues and Solutions:**

**1. Implicit Deny All Rule**

* **Symptoms**: Legitimate traffic being blocked
* **Resolution**:

// Always end ACL with explicit permit if needed

access-list 100 permit tcp 192.168.10.0 0.0.0.255 any eq 80

access-list 100 permit tcp 192.168.10.0 0.0.0.255 any eq 443

access-list 100 permit icmp any any

access-list 100 deny ip any any

**ACL Verification Commands:**

show access-lists

show access-lists 10

show access-lists ADMIN\_ACL

show ip interface

show ip access-lists interface fa0/0

debug ip packet detail

show logging

* 1. **Network Connectivity Testing**

A.Basic Connectivity

Use the ping command to verify reachability between routers and end devices:

ping 192.168.10.1 ! Admin Gateway

ping 192.168.20.1 ! Academic Gateway

ping 192.168.30.1 ! Library Gateway

ping 192.168.40.1 ! Hostel Gateway

B. Internet Access Simulation via NAT

ping 8.8.8.8

ping google.com

C. Traceroute to Diagnose Routing Paths

traceroute 192.168.30.1

traceroute 8.8.8.8

D. Interface and Neighbor Discovery

show ip interface brief

show interface status

show cdp neighbors

show lldp neighbors

**8.3 Performance Monitoring**

A. Interface Utilization

Monitor traffic flow and errors on interfaces:

show interface fastethernet 0/1

show interface counters

show interface summary

B. CPU & Memory Utilization

Check device resource usage:

show processes cpu

show memory

show version

C. EtherChannel Status

show etherchannel summary

show etherchannel port-channel

**8.4 Troubleshooting Log Example**

|  |  |  |  |
| --- | --- | --- | --- |
| **Issue** | **Cause** | **Resolution** | **Command Used** |
| OSPF not forming neighbors | Subnet mismatch | Corrected subnet mask | show ip ospf neighbor |
| No inter-VLAN communication | Missing trunk configuration | Configured switchport mode trunk | show interface trunk |
| Admin can't access Library | ACL blocking all traffic | Modified ACL to permit necessary traffic | show access-lists |
| NAT not working | Incorrect inside/outside interface | Configured NAT direction properly | show ip nat translations |
| Time not syncing | NTP server unreachable | Adjusted NTP IP and verified connectivity | show ntp associations (if CLI) |

# **9. TESTING AND RESULTS**

**9.1 OSPF Routing Verification**

***OSPF Neighbor Relationships***

EDGE-ROUTER#show ip ospf neighbor

ADMIN-ROUTER#show ip ospf neighbor

***Routing Table Verification***

EDGE-ROUTER#show ip route

**9.2 VLAN and Trunk Verification**

***VLAN Status***

CORE-SWITCH#show vlan brief

***Trunk Status***

CORE-SWITCH#show interface trunk

**9.3 ACL Testing Results**

***Admin to Hostel Access Test***

Admin-PC#ping 192.168.40.10

***Admin to Academic Access Test***

Admin-PC#ping 192.168.20.10

**9.4 NAT Functionality Testing**

***NAT Translation Table***

EDGE-ROUTER#show ip nat translations

***Internet Access Test***

Admin-PC#ping 8.8.8.8

**9.5 EtherChannel Status**

***EtherChannel Summary***

DISTRIBUTION-SW1#show etherchannel summary

**9.6 Network Monitoring Results**

***SNMP Monitoring***

SNMP-SERVER#show snmp

***NTP Synchronization***

CORE-SWITCH#show ntp status

CORE-SWITCH#show ntp associations

# **10. CHALLENGES AND RESOLUTIONS**

**10.1 Technical Challenges Encountered**

***Challenge 1: OSPF Neighbor Adjacency Issues***

Problem: OSPF neighbors were not forming adjacencies between Edge Router and Admin Router.

Root Cause: Mismatched subnet masks and incorrect network statements in OSPF configuration.

Solution:

* Verified interface IP addresses and subnet masks
* Corrected network statements in OSPF configuration
* Used debug ip ospf hello to troubleshoot adjacency formation

Resolution Steps:

! Verification commands used

show ip ospf interface

show ip ospf neighbor

debug ip ospf hello

! Corrected configuration

router ospf 1

network 10.0.0.0 0.0.0.3 area 0

network 10.0.0.4 0.0.0.3 area 0

***Challenge 2: Inter-VLAN Routing Not Working***

Problem: Devices in different VLANs could not communicate despite proper VLAN configuration.

Root Cause: SVIs (Switched Virtual Interfaces) were not configured on the Layer 3 device.

Solution:

* Configured VLAN interfaces on the core switch
* Enabled IP routing on the Layer 3 device
* Verified routing table entries

Resolution Steps:

! Enable IP routing

ip routing

! Configure VLAN interfaces

interface vlan 10

ip address 192.168.10.1 255.255.255.0

no shutdown

interface vlan 20

ip address 192.168.20.1 255.255.255.0

no shutdown

interface vlan 30

ip address 192.168.30.1 255.255.255.0

no shutdown

interface vlan 40

ip address 192.168.40.1 255.255.255.0

no shutdown

***Challenge 4: NAT Overload Configuration Issues***

Problem: Internal hosts could not access the internet through NAT.

Root Cause: Incorrect interface designation as NAT inside/outside and missing access-list for NAT.

Solution:

* Properly configured inside and outside NAT interfaces
* Created appropriate access-list for NAT translation
* Verified NAT translations

Resolution Steps:

! Configure NAT interfaces

interface GigabitEthernet0/0/0

ip nat outside

interface GigabitEthernet0/0/1

ip nat inside

! Configure NAT overload

ip nat inside source list 1 interface GigabitEthernet0/0/0 overload

access-list 1 permit 192.168.0.0 0.0.255.255

access-list 1 permit 10.0.0.0 0.0.255.255

***Challenge 6: EtherChannel Formation Issues***

Problem: EtherChannel was not forming between distribution switches and access switches.

Root Cause: Mismatched EtherChannel protocols and port configuration inconsistencies.

Solution:

* Standardized on LACP protocol for all EtherChannels
* Ensured consistent port configuration across channel members
* Verified channel-group configuration

Resolution Steps:

! Remove existing configuration

no interface port-channel 1

! Reconfigure with LACP

interface range FastEthernet0/1-2

channel-group 1 mode active

switchport mode trunk

switchport trunk allowed vlan 10,20,30,40,99

***Challenge 7: SSH Access Configuration***

Problem: SSH access was not working for remote management.

Root Cause: RSA keys not generated and SSH version not specified.

Solution:

* Generated RSA keys with appropriate key size
* Configured SSH version 2 for security
* Set up proper user authentication

Resolution Steps:

! Configure domain name

ip domain-name texascollege.edu

! Generate RSA keys

crypto key generate rsa general-keys modulus 1024

! Configure SSH

ip ssh version 2

line vty 0 15

login local

transport input ssh

***Challenge 8: SNMP Security Configuration***

Problem: SNMP was not secure and providing too much access.

Root Cause: Using default community strings and no access restrictions.

Solution:

* Changed default community strings
* Implemented proper read-only and read-write access
* Configured SNMP host restrictions

Resolution Steps:

! Remove default communities

no snmp-server community public

no snmp-server community private

! Configure secure communities

snmp-server community TexasCollege\_RO RO

snmp-server community TexasCollege\_RW RW

snmp-server host 192.168.99.10 TexasCollege\_RO

***Challenge 10: Network Monitoring Gaps***

Problem: Network monitoring was not comprehensive enough.

Root Cause: Insufficient SNMP traps and syslog configuration.

Solution:

* Enabled comprehensive SNMP traps
* Configured detailed syslog levels
* Implemented centralized monitoring

Resolution Steps:

//Enable comprehensive SNMP traps

snmp-server enable traps

snmp-server enable traps config

snmp-server enable traps hsrp

snmp-server enable traps interface

! Configure detailed syslog

logging trap debugging

logging facility local0

service timestamps log datetime msec localtime

# **11. CONCLUSION**

Secure Campus Network Design-MISSION ACCOMPLISED The Secure Campus Network Design project has successfully developed a complete enterprise campus network solution for the Texas School of Business and IT. The project met all its main goals and was an excellent experience in terms of practical exposure to state-of-the-art network technologies and security configurations.

**11.1 Key Achievements**

Network: Designed, implemented and configured a scalable 3-tier Hierarchical network for four significant departments (Admin, Academic, Library and Hostel blocks) with proper segmentation and scalability.

Implementation of Routing: OSPF was successfully implemented on all network equipment, creating dynamic network routing with fast convergence and fault tolerance. The one-area schema also minimized operation complexity and guaranteed routing efficiency.

Security Measures: There were adequate security arrangements such as:

* Extended ACL for between department traffic filtering
* SSH access with encrypted device and strong password policies
* Port security on access switches to deny unauthorized access.
* Implementation NAT for restricting internet access

Control Monitoring: Created solid monitoring infrastructure Network monitoring using:

* SNMP: Management of the device, information collection, performance analysis and monitoring.
* Syslog (remote) for centralized logging and troubleshooting
* NTP for network-wide time synchronization
* Comprehensive alerting and notification systems

Redundancy and High Availability: Realization of several redundancy methods such as:

* EtherChannel for link aggregation and redundancy
* HSRP for gateway redundancy
* Rapid Spanning Tree Protocol for fast convergence
* Multiple uplink paths to prevent single points of failure

**11.2 Learning Outcomes**

This project provided extensive practical experience in:

* Enterprise network design principles and best practices
* Cisco IOS configuration and troubleshooting
* Network security implementation and policy enforcement
* Performance monitoring and network management
* Fault tolerance and redundancy planning
* Documentation and project management skills

**11.3 Real-World Applications**

The implemented network design closely mirrors real-world campus and enterprise network deployments, providing valuable experience that directly translates to professional networking environments. The security policies and monitoring systems implemented follow industry best practices and regulatory compliance requirements.

**11.4 Future Enhancements**

Potential improvements and expansions to the current implementation include:

* Implementation of wireless infrastructure with proper security controls
* Integration of VoIP systems with QoS policies
* Enhanced security with next-generation firewall features
* Network automation and orchestration capabilities
* IPv6 dual-stack implementation for future-proofing
* Advanced monitoring with network analytics and AI-driven insights

**11.5 Project Impact**

This project has successfully prepared participants for real-world network engineering roles by providing hands-on experience with enterprise-grade networking technologies. The comprehensive documentation and troubleshooting procedures developed will serve as valuable reference materials for future network implementations and maintenance activities.

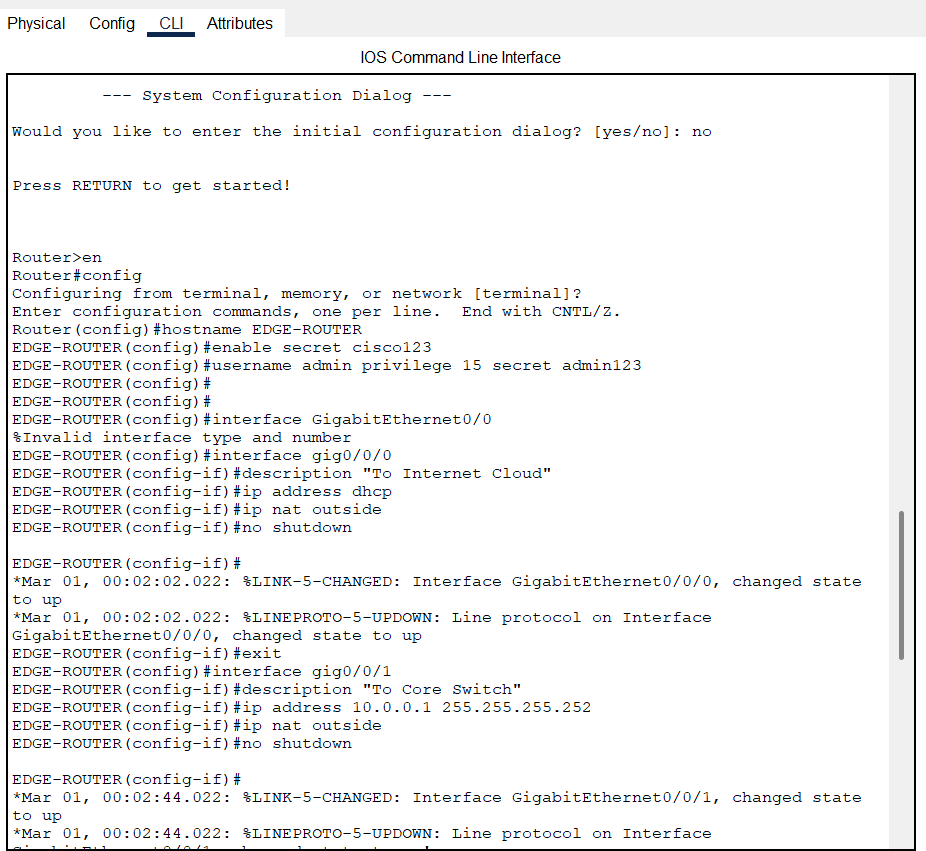
The successful completion of this project demonstrates proficiency in advanced networking concepts and practical implementation skills essential for careers in network engineering, cybersecurity, and IT infrastructure management.

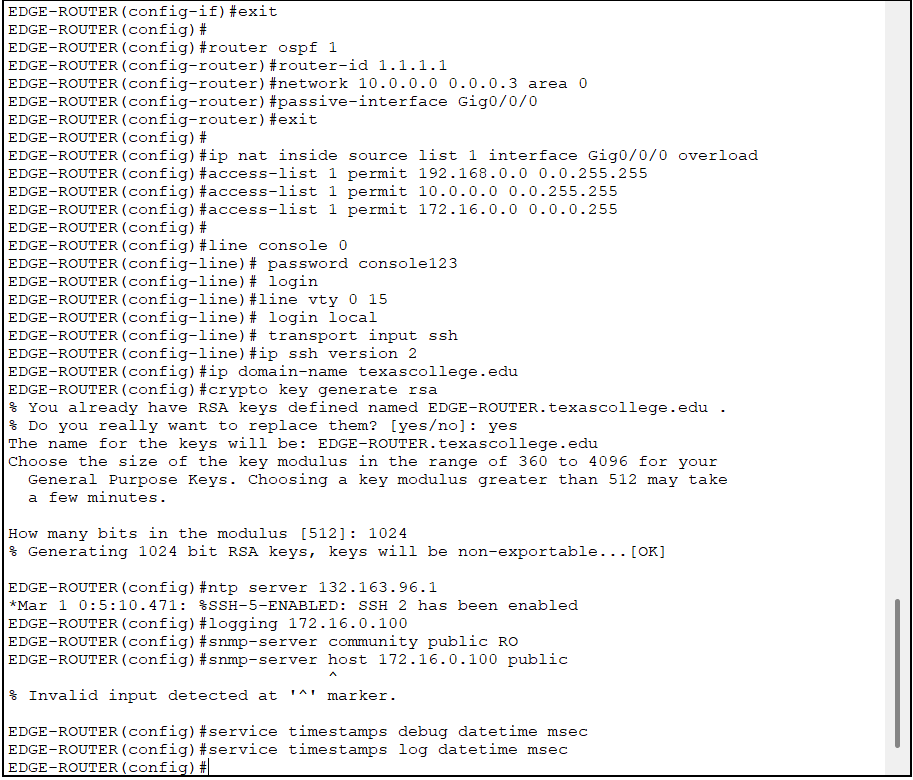
# **12. REFERENCES**

1. **Cisco Networking Academy Materials** 
   * CCNA Routing and Switching Curriculum
   * CCNA Security Curriculum
   * Cisco Packet Tracer Learning Materials
2. **Technical Documentation** 
   * Cisco IOS Configuration Guides
   * Cisco Catalyst Switch Configuration Guide
   * Cisco Router Configuration Guide
   * OSPF Configuration and Troubleshooting Guide
3. **Academic Resources** 
   * "Advanced Computer Network" by Rahul Sharma, Manmohan Singh
   * "Network Security Essentials" by William Stallings
   * "Computer Networks" by Andrew S. Tanenbaum
4. **Online Resources** 
   * Cisco Learning Network: <https://learningnetwork.cisco.com/>
   * Cisco Documentation: <https://www.cisco.com/c/en/us/support/docs/>
   * RFC Documents: <https://www.rfc-editor.org/>
   * IEEE Standards: <https://standards.ieee.org/>

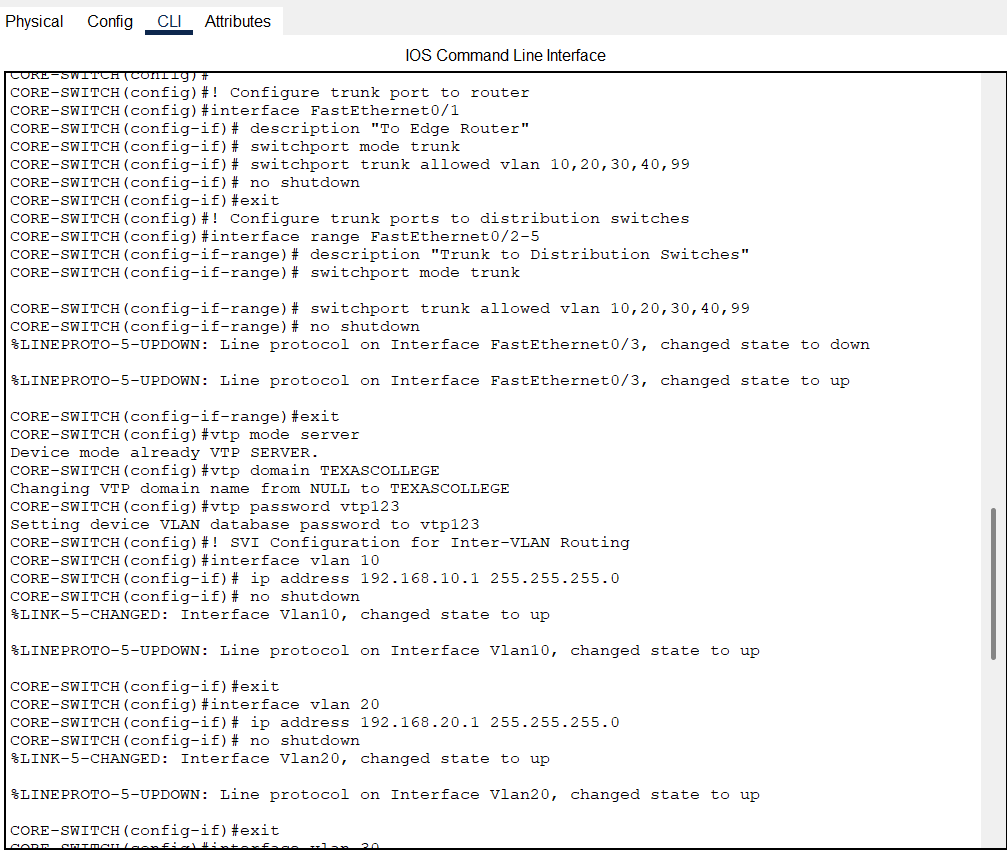
# **13. APPENDIX**

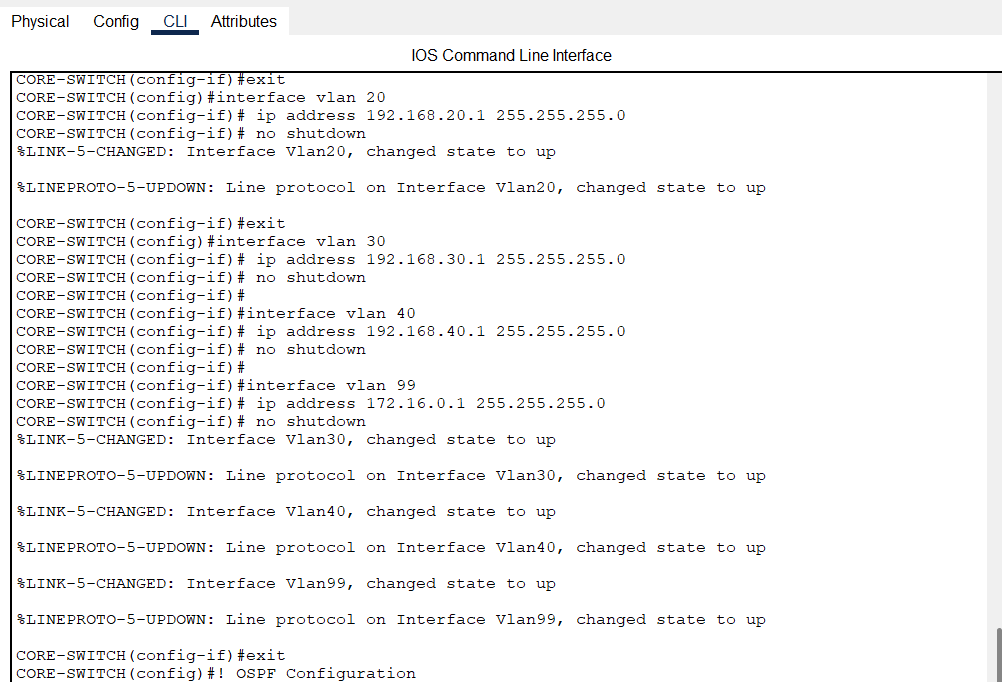
**Edge Router Configuration**

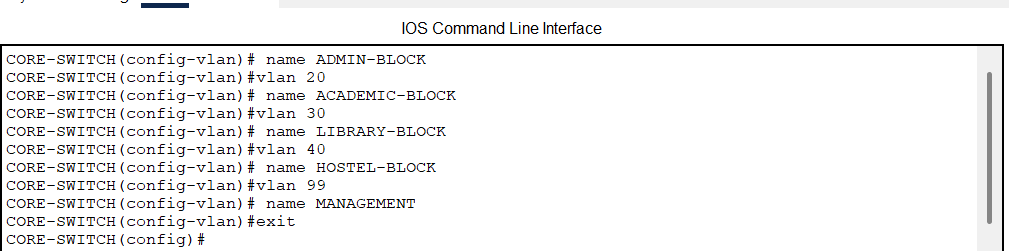
****

****

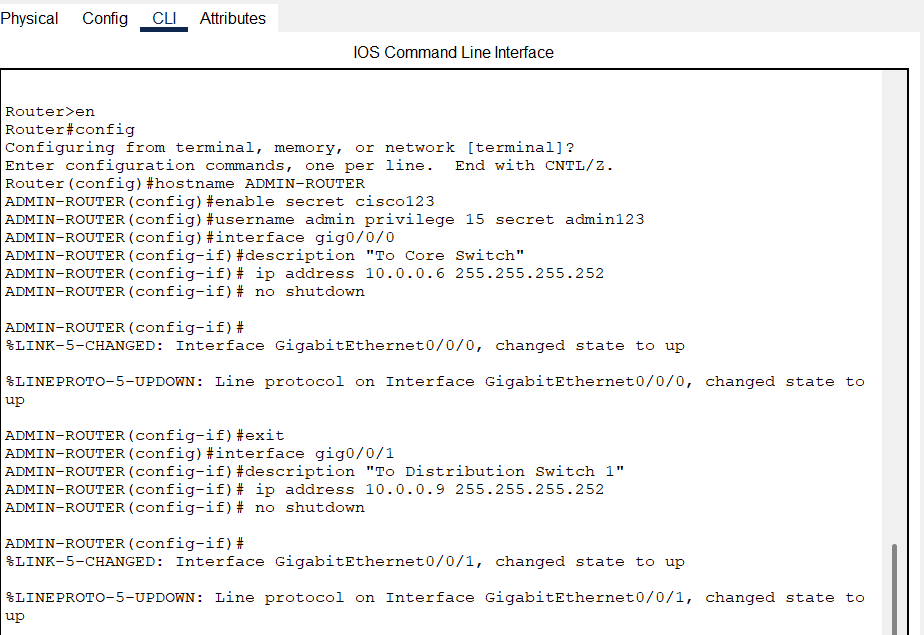
**Core Switch Configuration**

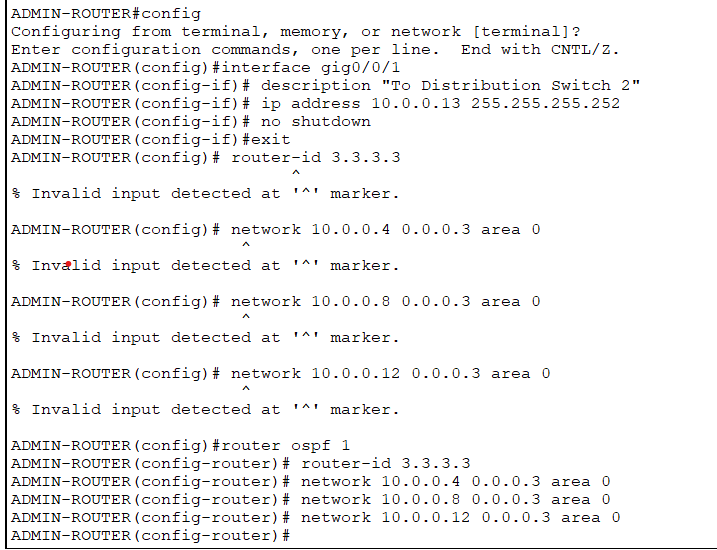
****

****

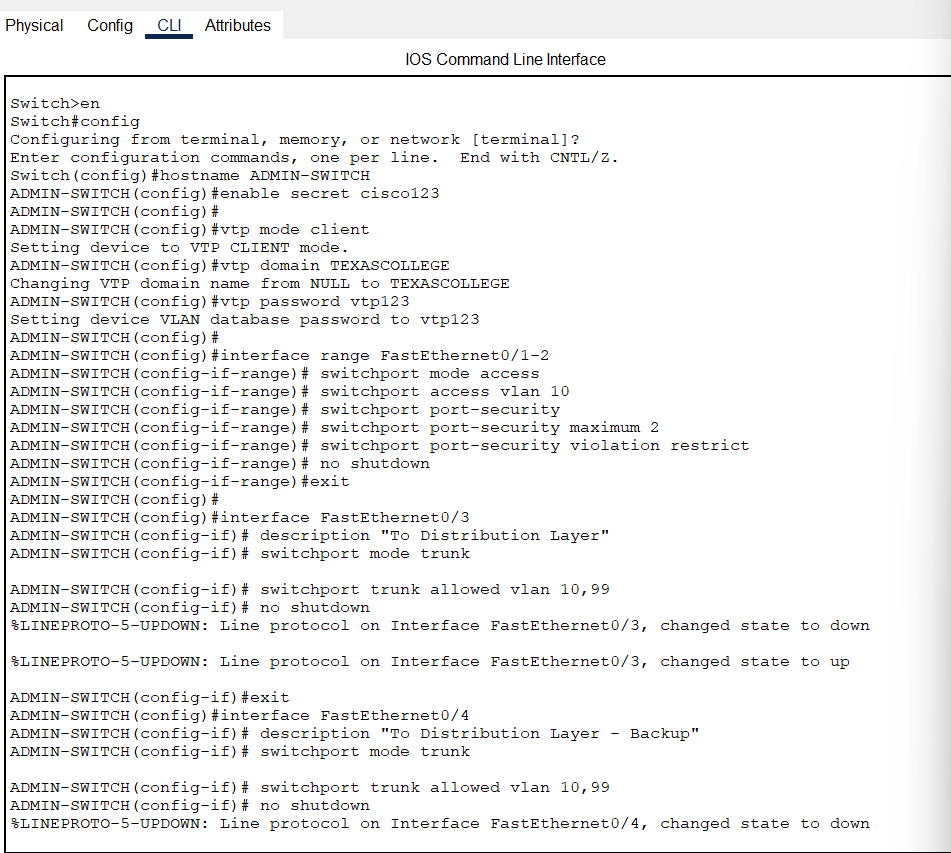
****

**Admin Router Configuration**

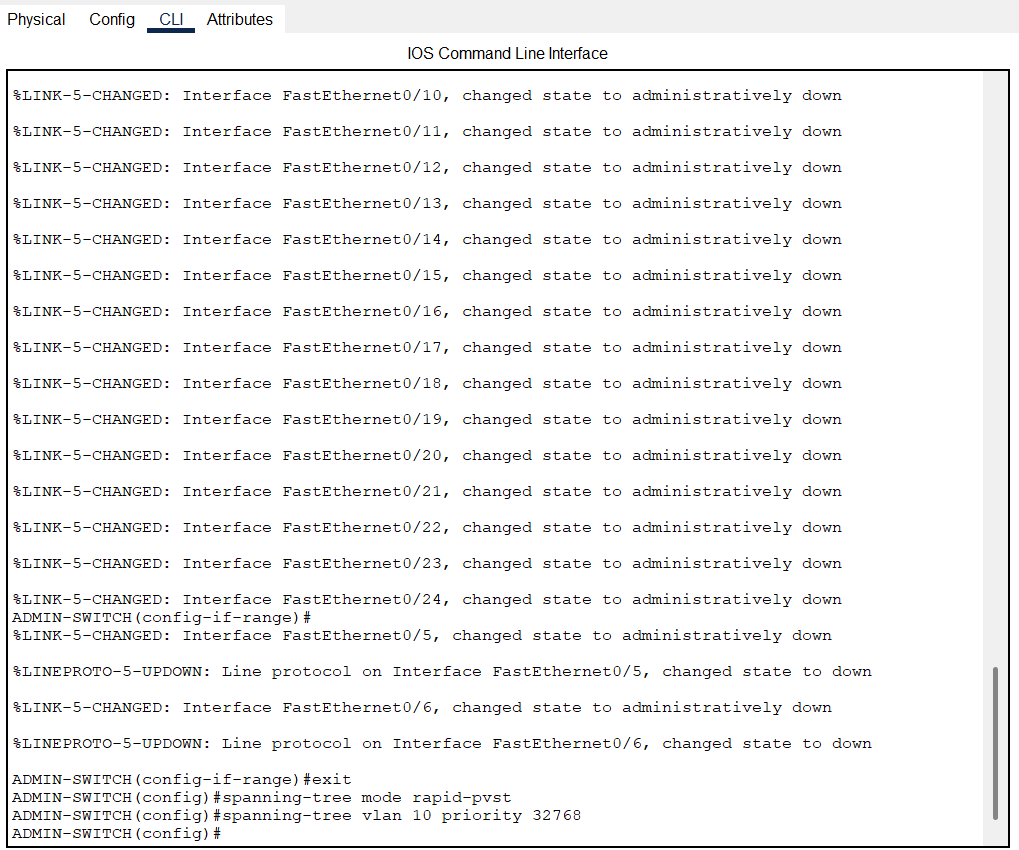
****



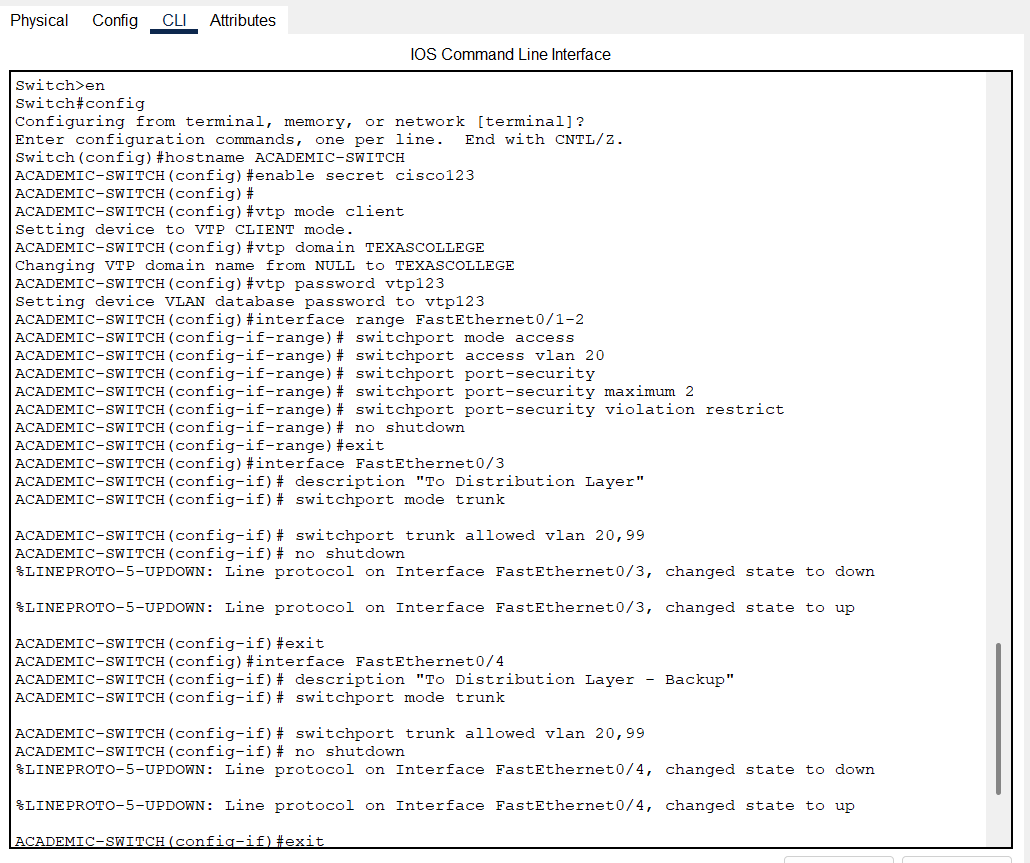
**Admin-Switch Configuration**

****

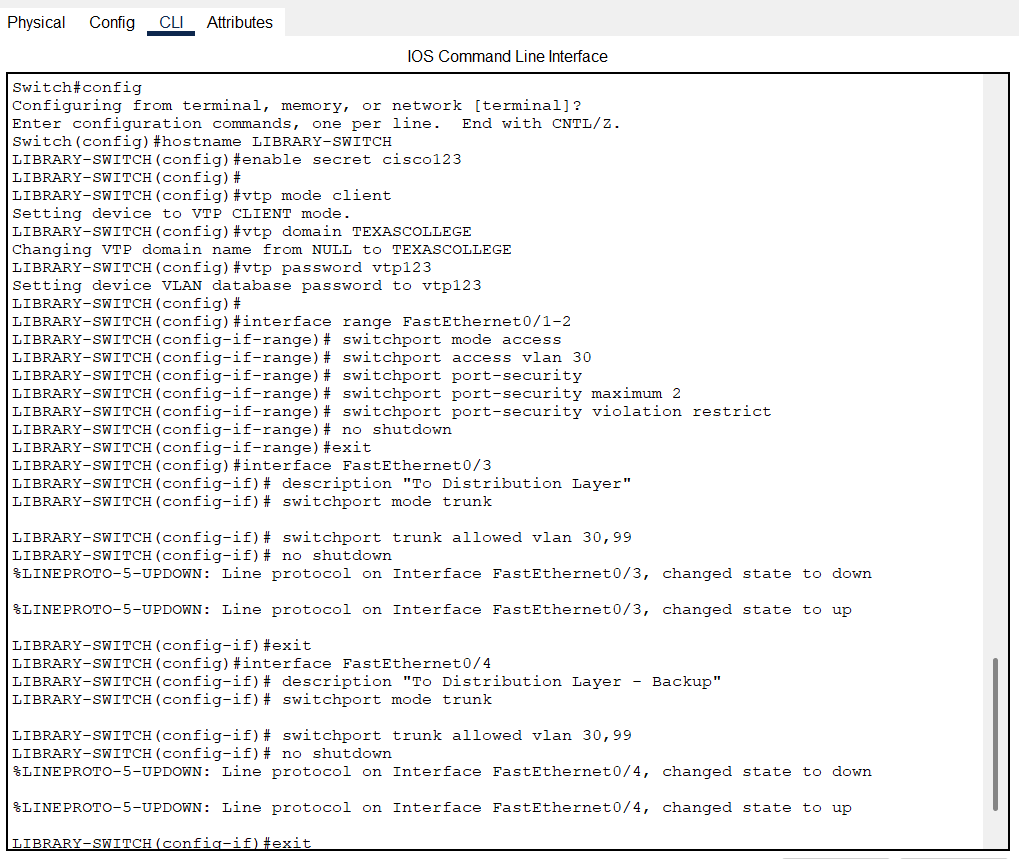
****



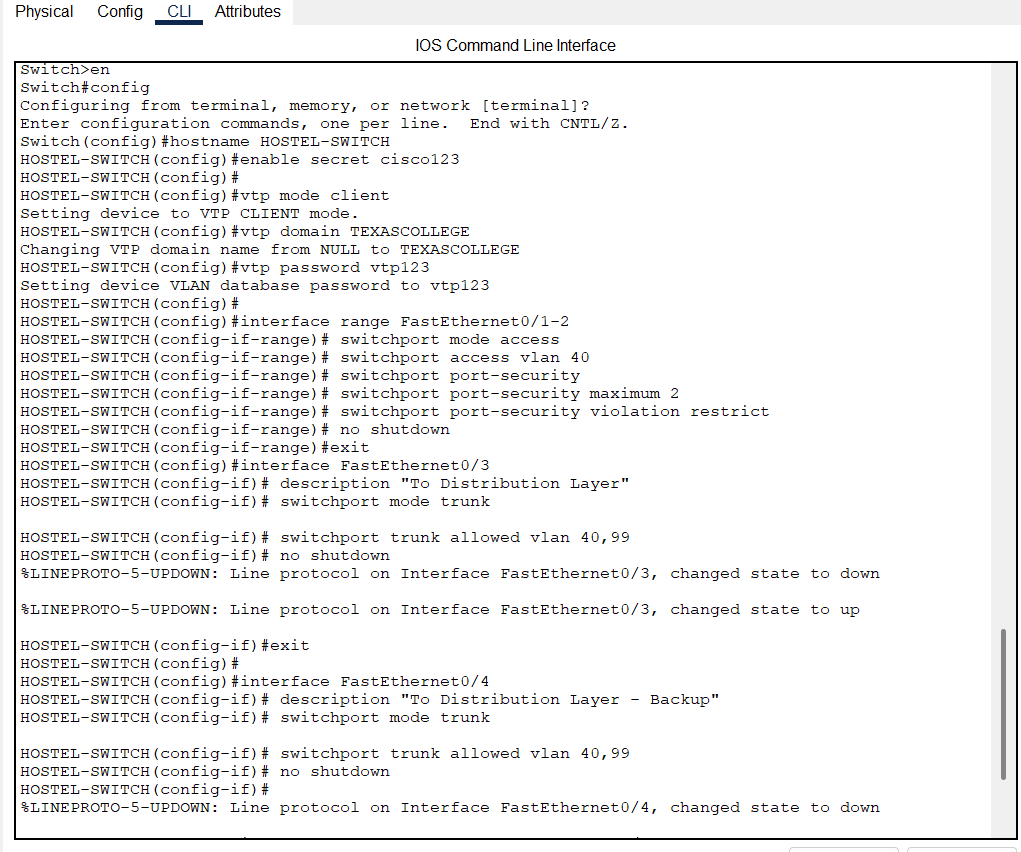
**Academic-Switch**

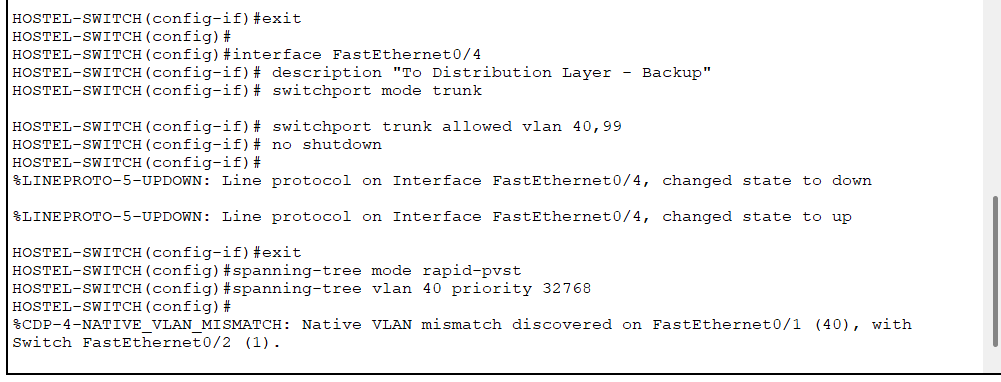
****

**Library- Switch**

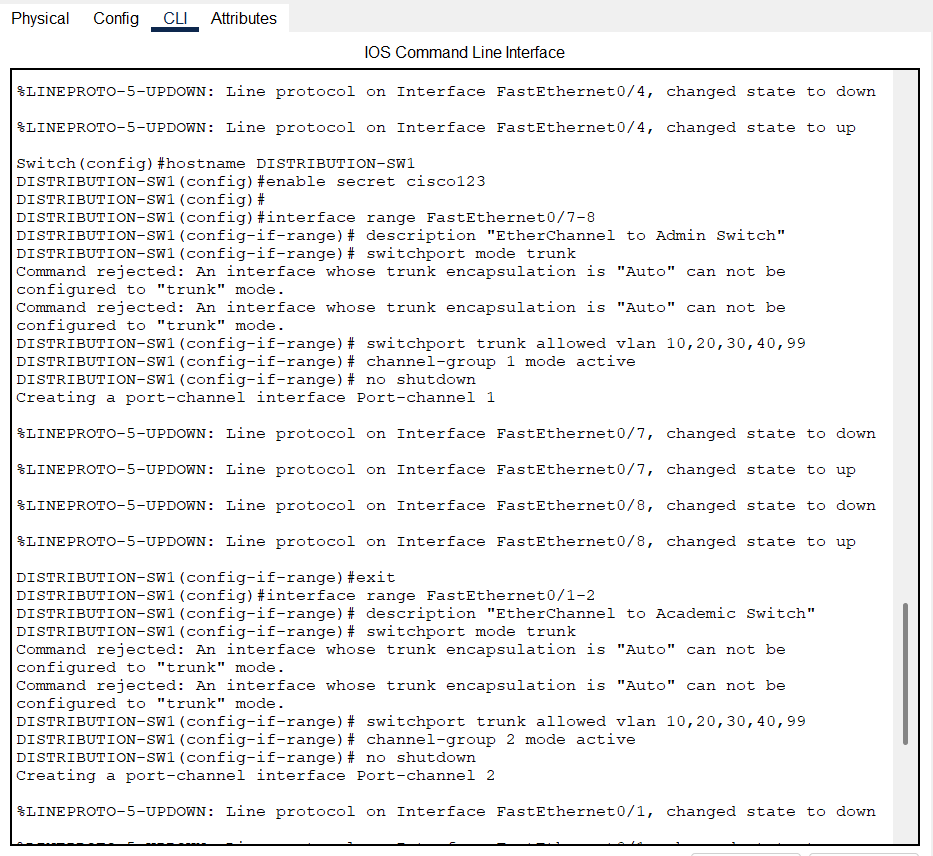
****

**Hostel-Switch**

****

****

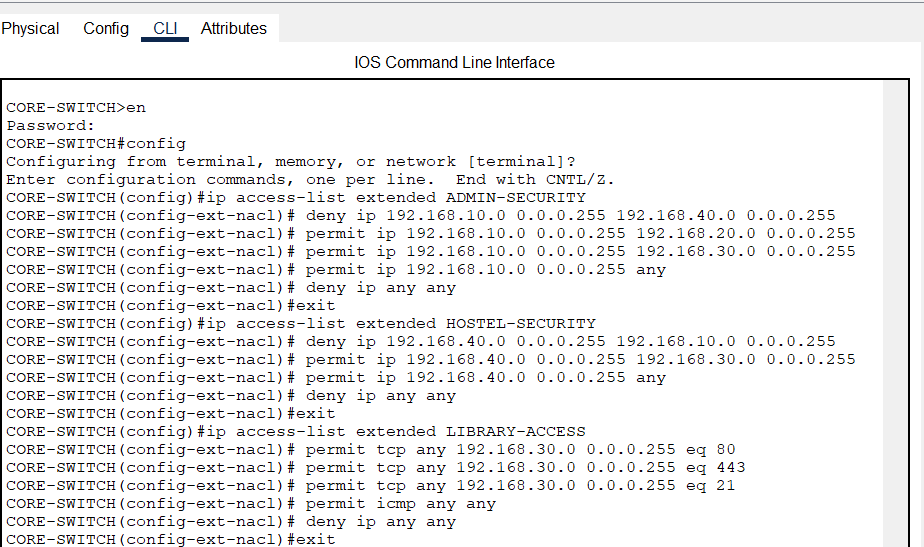
**Distribution Switch Configuration**

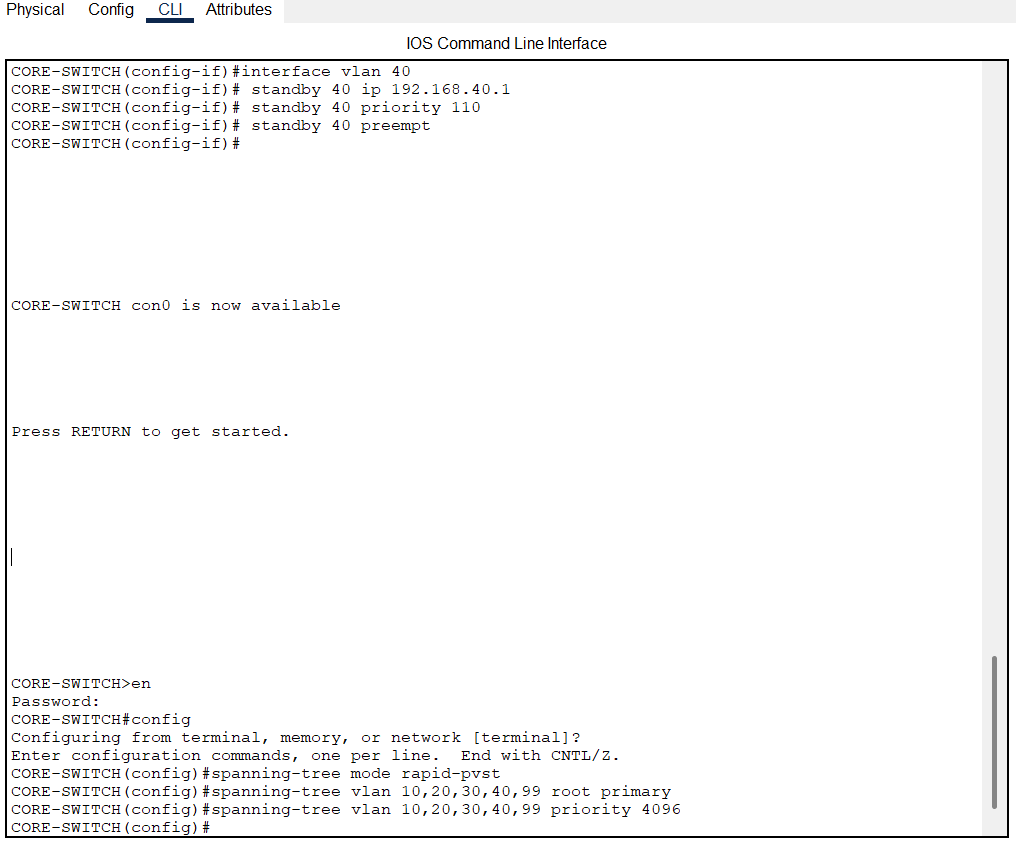
****

****

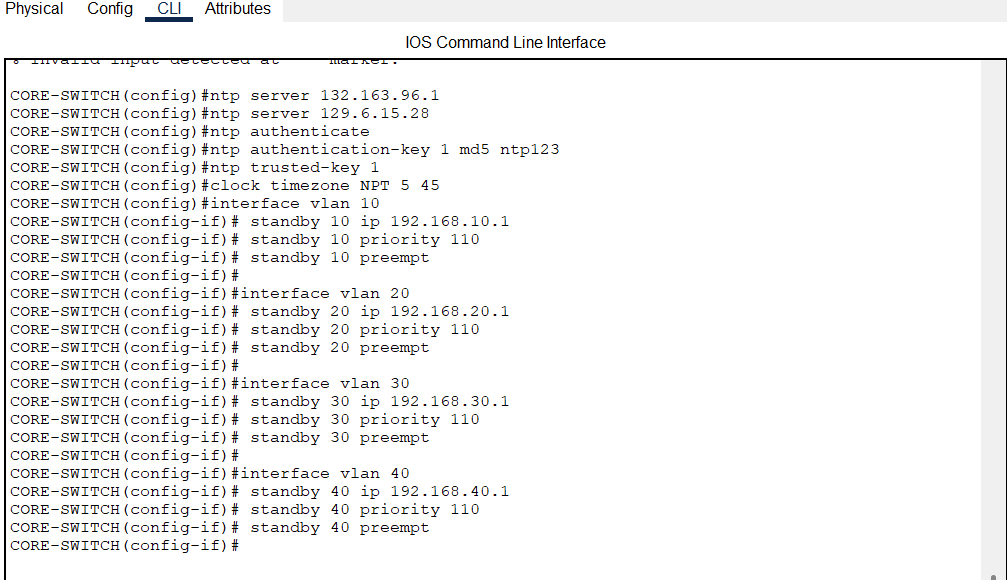
****

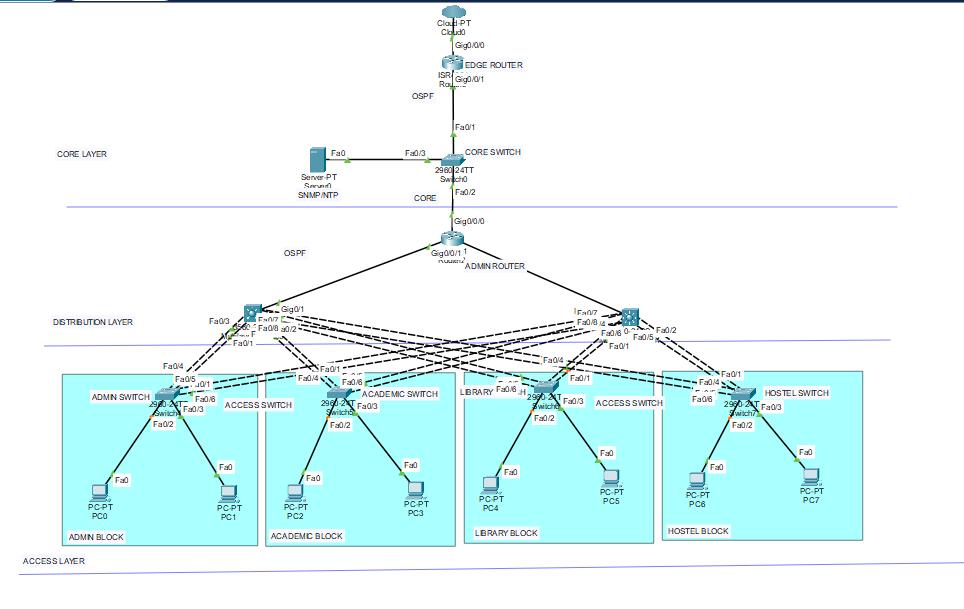
**Core switch security**

****

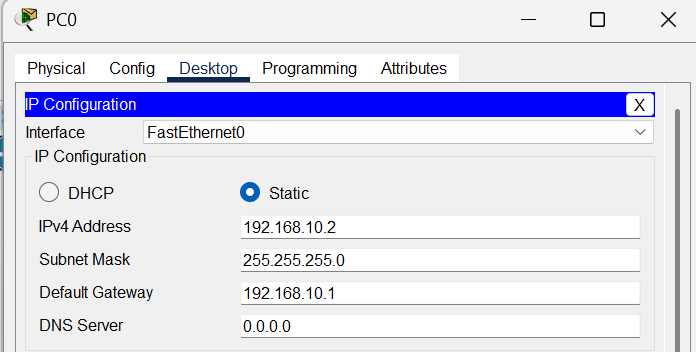
****

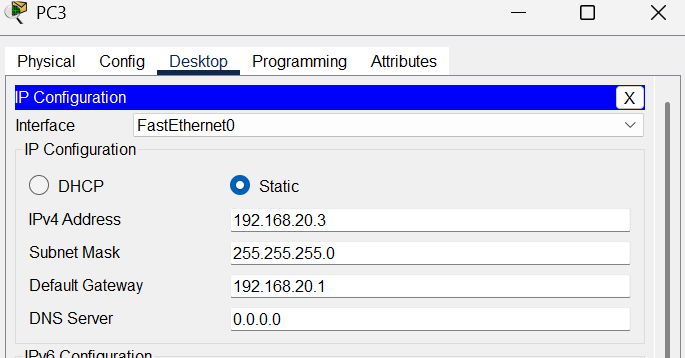
**NTP Configurations**



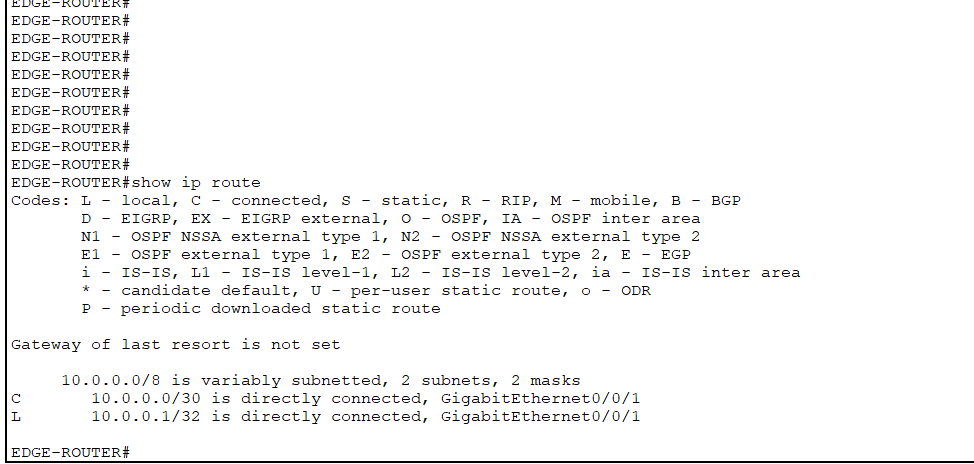


**IP Address Assignment**

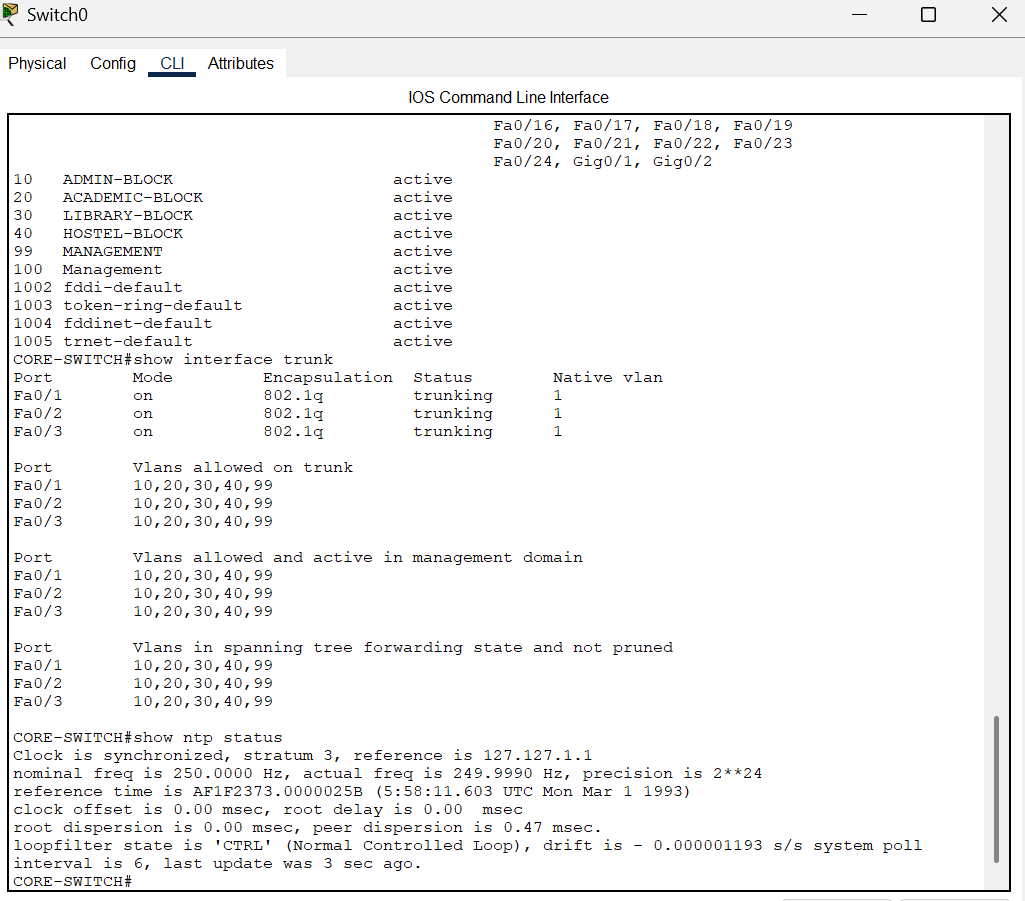
****

****

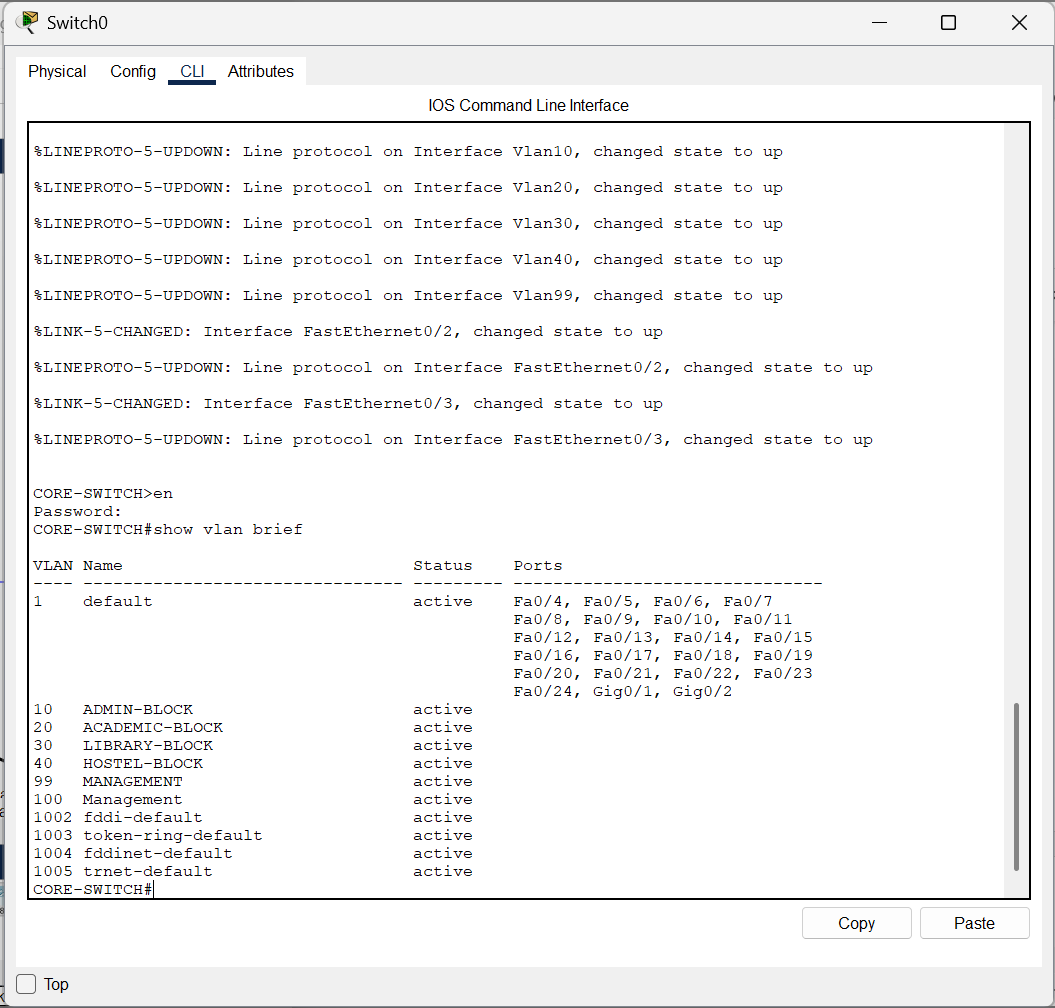
**Routing Table Verification**

****

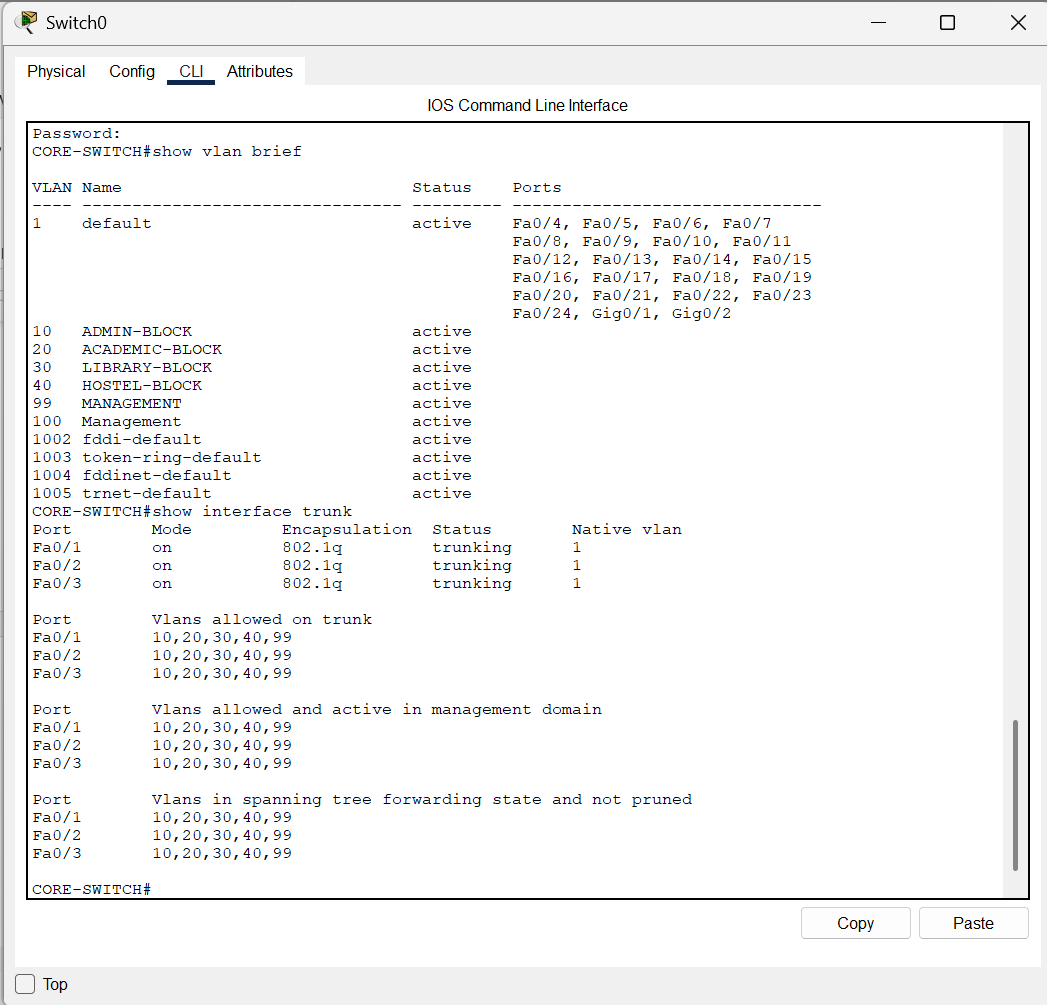
**NTP Synchronization**

****

**VLAN Configuration**



**TRUNK Configuration**

****

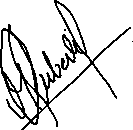
# **DECLARATION OF ORIGINALITY**

I hereby declare that this assignment is my original work, and I have referenced all sources as required. I understand that failure to adhere to academic integrity will result in disciplinary action.

Student Name: Merry Subedi

Student ID: LC00017003482

Signature:



Date: 15th July, 2025