**WIRELESS NETWORK OPTIMIZATION-PERFORMANCE AND COVERAGE IN CAMPUS NETWORKS**

**A CASE STUDY REPORT**

***Submitted by***

**SARANSH SINGH**

# ABSTRACT

This case study report examines the design, configuration, and performance of a campus network architecture implemented in Cisco Packet Tracer. The network setup connects a campus, a affiliated campus, and an external email server located on the cloud. The primary objective was to establish end-to-end connectivity across all devices while enabling secure access to internal servers and external resources. Both campuses are organized into separate buildings and departments, each assigned its own IP network to ensure efficient traffic segmentation and secure communication. To manage and control traffic flow, VLANs were configured on switches within each campus, segmenting the network based on departmental needs and enhancing security through logical isolation of departments. Core devices, such as routers and switches, were configured to support these VLANs and enable seamless connectivity between departments and buildings. The internal routing between routers across both campuses is handled by RIPv2, optimizing data transmission across the network. For external connectivity, static routing was implemented to manage access to the cloud-hosted email server, allowing secure external communication without compromising internal network security. Additionally, a DHCP server configured on a central router in one of the campus buildings dynamically assigns IP addresses to devices, ensuring efficient IP management and simplifying device configuration. This dynamic IP addressing improves network flexibility by enabling easier device onboarding. The report evaluates the network's performance, scalability, and coverage, analyzing the benefits of the implemented VLANs, routing protocols, and security configurations. Through this case study, we illustrate how a well-structured campus network with logically segmented VLANs and tailored routing protocols can provide a secure, reliable, and highly scalable solution for multi-campus environments, meeting the demands of both internal and external connectivity.

**Table of Contents**

Abstract………………………………………………………………………………………...i

1. Introduction………………………………………………………………………………..1
2. Network Design and Topology……………………………….…………………….………2
3. Overview of the Network Components…………………………………………………….5
4. IP Addressing Scheme of the Devices……………………………………………..……….8
5. VLAN Configuration………………...…………………………………………………….9
6. RIP v2 and Dynamic Host Configuration Protocol…………..……………..…………….11
7. Security Measures…………………………………………………………...……………14
8. Quality of Service (QoS) ……………….………………………….…………………….15
9. Monitoring and Management………………………….………………………...……….16
10. Testing and Validation…………………………………………………………………….17
11. Conclusion…………………………………………………………………….………….20
12. References………………………………………………………….…………………….21
13. Appendices……………………………………………………………………………….22

**Table of Figures:**

1. Topology of the Network………………………………………………………………….2
2. Network Components…………………………………………………………..…………7
3. Successful VLAN configurations………………………………………….……………..10
4. RIPv2 and DHCP Commands……………………………………………...……………..12
5. Ping Commands from PCs…………………………………………………..……………18
6. **Introduction**
   1. **Background**

This case study explores the design and implementation of a network infrastructure for a university campus, encompassing both a campus and an affiliated campus, as well as an external email server hosted in the cloud. With the increasing need for streamlined communication and access to cloud-based services, a robust and scalable network architecture was crucial. Cisco Packet Tracer, a widely used network simulation tool, was selected to model and simulate the university's network. This tool enabled the configuration and testing of various network components, allowing us to create a realistic representation of the proposed infrastructure. The network design includes a structured approach to segmenting traffic and securing communication channels through the use of VLANs, RIPv2 for dynamic routing within the internal network, and static routing for the external email server. Additionally, DHCP was implemented in designated buildings on the campus for efficient IP address management.

* 1. **Objective**

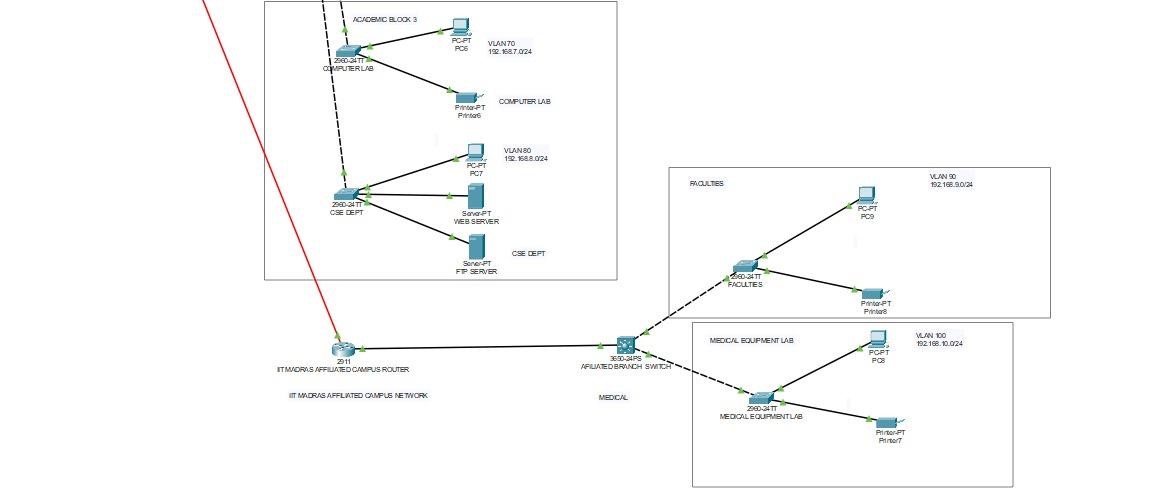
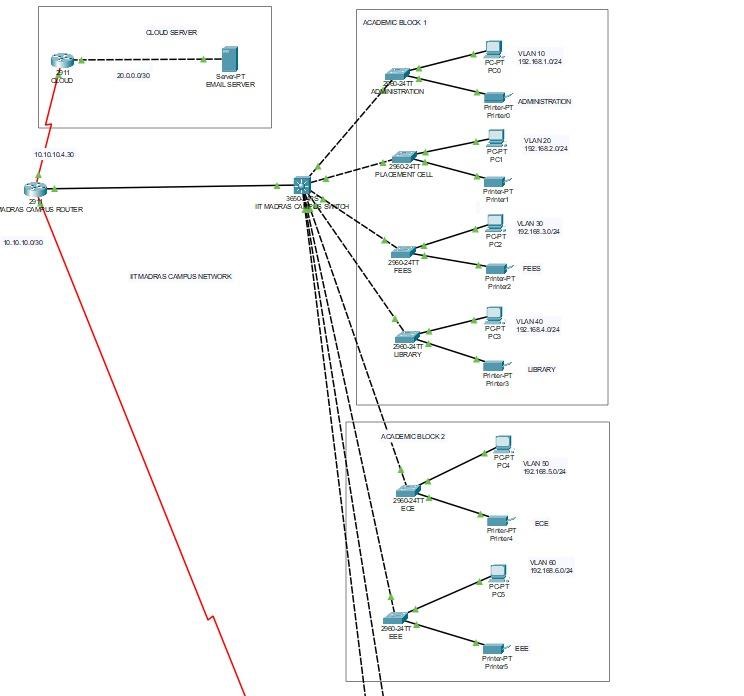
The primary objective of this project was to design and implement a secure, scalable, and high-performance campus network for the university. Key objectives included:

1. Establishing end-to-end connectivity between campuses and enabling secure access to an external cloud-hosted email server.
2. Segmenting network traffic across departments using VLANs, thus enhancing security and reducing unnecessary broadcast traffic.
3. Configuring dynamic routing within the internal network using RIPv2 to allow efficient communication between different parts of the campus.
4. Enabling DHCP for dynamic IP allocation in specific campus buildings to simplify network management and reduce administrative overhead.
5. Optimizing network performance through Quality of Service (QoS) settings, prioritizing critical applications to prevent network congestion.

This report outlines the design process, configuration details, testing procedures, and evaluation of the network’s performance, illustrating how the solution meets the university's operational requirements for connectivity, security, and scalability.

**2. Network Design and Topology**

The topology consists of two primary campuses — the Campus and the Affiliated campus — connected by a WAN link. Each campus hosts multiple departments, structured as individual sub-networks. These departmental networks are configured with VLANs for security, and all campus segments are connected through switches and routers, ensuring centralized management and efficient traffic handling.

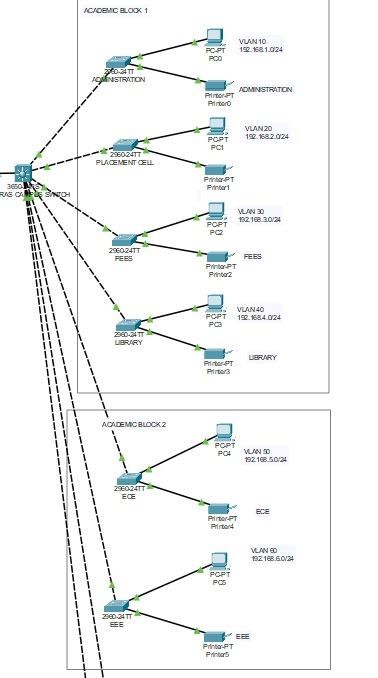


The campus hosts a variety of buildings, each representing specific departments, and has a centralized core network infrastructure. This includes the following key components:

* Core Router and Layer 3 Switch: The core router connects the campus to the affiliated campus and the external cloud-hosted email server. A Layer 3 switch is used to manage VLANs and provide inter-VLAN routing within the campus.
* Departmental VLANs: Each building or department (such as Administration, PLACEM-

CELL, Fees, Library, and others) is assigned a unique VLAN. These VLANs are segmented with unique IP address ranges for security and traffic isolation. For instance:

* VLAN 10 (Administration): 192.168.1.0/24
* VLAN 20 (PLACEM-CELL): 192.168.2.0/24
* VLAN 30 (Fees): 192.168.3.0/24
* VLAN 40 (Library): 192.168.4.0/24
* Additional VLANs for technical and student labs in the Academic block 2 and Academic block 3 buildings.
* DHCP Configuration: In the campus, a router-based DHCP server was implemented to assign IP addresses dynamically to devices in designated buildings. This simplifies IP management and supports the mobile needs of faculty and students.



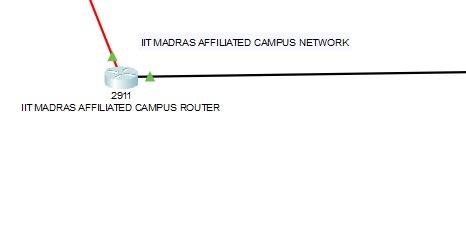
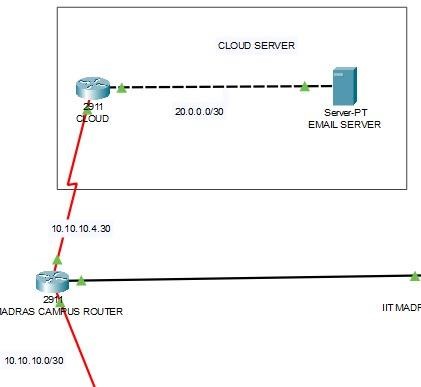
The affiliated campus network is connected to the campus via a WAN link, providing seamless connectivity between the two sites. The affiliated campus network is structured similarly to the campus, with its own Layer 3 switch and core router.

Affiliated campus Router and Layer 3 Switch: The branch router manages connections between the affiliated campus and the campus, while the Layer 3 switch manages VLANs within the affiliated campus.

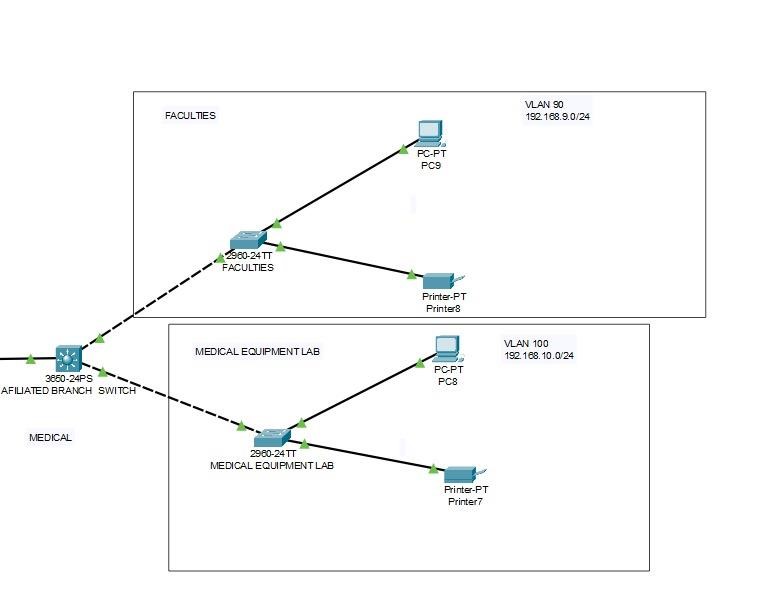
Departmental VLANs: The affiliated campus has separate VLANs for departments such as Medical, Faculties, and Student Library. For example:

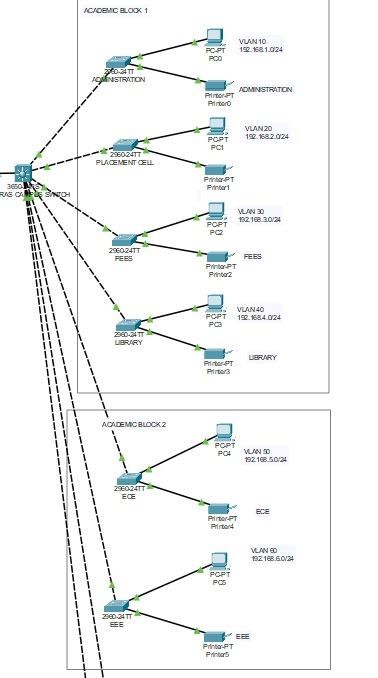
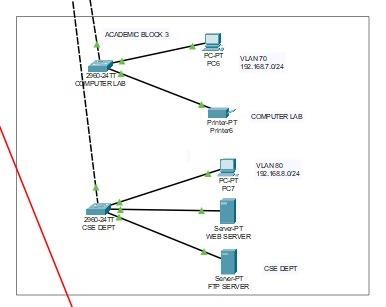
i) VLAN 90 (Faculties): 192.168.9.0/24 ii) VLAN 100 (Student Library): 192.168.10.0/24

Internal Routing and Inter-VLAN Communication: The Layer 3 switch at the affiliated campus handles inter-VLAN routing for internal communication within departments.



The university campus network includes integration with a cloud-hosted email server to provide efficient and scalable communication services for Faculties and students. This cloud server is connected to the campus via a secure WAN link, and static routing is used to direct traffic between the internal network and the cloud service. By hosting the email server in the cloud, the university gains the advantages of high availability, reduced on-premises hardware requirements, and scalability to support a growing user base. This setup ensures that email communications remain accessible from both the main and affiliated campuses, enhancing collaboration and communication across departments.





Each department includes end devices such as PCs and printers, configured to operate within their respective VLANs. In addition to academic and administrative devices, the Academic block 3 building houses web and FTP servers dedicated to the IT department, with these servers assigned a unique VLAN for additional security. The topology includes security features such as VLAN segmentation to isolate departmental traffic and limit broadcast domains. This reduces congestion and enhances security by ensuring that data from each department remains contained within its own network segment. Additional security settings are applied on core routers and switches to prevent unauthorized access.

**3. Overview of the Network Components:**

**i) Routers**

* Campus Router (2911):
* Interface Configuration:
* GigabitEthernet 0/0: Connected to the cloud with the external IP 10.10.10.4/30.
* GigabitEthernet 0/1: Connected to the core switch (Campus L3 Switch).
* Routing Protocol: RIPv2 for internal routing.
* Static Route: Configured for communication with the external email server through the cloud.
* Affiliated campus Router (2911):
* Interface Configuration:
* GigabitEthernet 0/0: Connected to Campus Router with IP 10.10.10.0/30.
* GigabitEthernet 0/1: Connected to Affiliated campus L3 Switch.
* Routing Protocol: RIPv2 for internal routing.

**ii) Switches**

* Campus Layer 3 Switch (3650-24PS)
* Serves as the core switch for VLAN routing within the campus.
* VLANs and Subnets:
* VLAN 10 (Administration): 192.168.1.0/24
* VLAN 20 (PLACEM-CELL): 192.168.2.0/24
* VLAN 30 (Fees): 192.168.3.0/24
* VLAN 40 (Library): 192.168.4.0/24
* VLAN 50 (ECE): 192.168.5.0/24
* VLAN 60 (EEE): 192.168.6.0/24
* VLAN 70 (Comp-lab): 192.168.7.0/24
* VLAN 80 (Cse-dept): 192.168.8.0/24
* DHCP: The router for this campus handles DHCP for specific buildings (such as IT and Student Labs) within the campus.
* Affiliated campus Layer 3 Switch (3650-24PS)
* Manages VLANs for separate departments in the affiliated campus.
* VLANs and Subnets:
* VLAN 90 (Faculties): 192.168.9.0/24
* VLAN 100 (Student Library): 192.168.10.0/24
* Access Switches (2960-24TT) (Campus)
* Each building (Administration, PLACEM-CELL, Fees, Library, ECE, EEE, Comp-lab, and Cse-dept) has dedicated access switches.
* Configuration: Access ports configured for respective VLANs as per departmental networks.
* Access Switches (2960-24TT) (Affiliated campus)
* The Faculties and Student Library sections are connected placem-cell access switches.
* Configuration: Ports set for VLAN 90 and VLAN 100, respectively, to provide network segmentation. **iii) Servers**
* Email Server (Cloud-based)
* IP Address: 20.0.0.2/30
* Serves email functions for the university, accessible from both the main and affiliated campuses via the cloud link. - Internal Servers (Campus)
* Web Server: Connected in the Cse-dept VLAN with IP Address 192.168.8.2
* FTP Server: Also in the Cse-dept VLAN with IP Address 192.168.8.3
* These servers provide web and file-sharing services internally for Faculties and students within the campus.

**iv) Workstations and Printers**

Each department or building has its own workstations and printers assigned IP addresses within their respective VLAN subnets. Below is a breakdown of the devices by department:

* Academic block 1 (Campus)
* Administration (VLAN 10): Workstation (PC0) 192.168.1.2, Printer 192.168.1.10
* PLACEM-CELL (VLAN 20): Workstation (PC1) 192.168.2.2, Printer 192.168.2.10
* Fees (VLAN 30): Workstation (PC2) 192.168.3.2, Printer 192.168.3.10
* Library (VLAN 40): Workstation (PC3) 192.168.4.2, Printer 192.168.4.10
* Academic block 2 (Campus)
* ECE (VLAN 50): Workstation (PC4) 192.168.5.2, Printer 192.168.5.10
* EEE (VLAN 60): Workstation (PC5) 192.168.6.2, Printer 192.168.6.10
* Academic block 3 (Campus)
* Comp-lab (VLAN 70): Workstation (PC6) 192.168.7.2, Printer 192.168.7.10
* Cse-dept (VLAN 80): Workstation (PC7) 192.168.8.4, Web Server 192.168.8.2, FTP Server

192.168.8.3

* Affiliated campus
* Medical (VLAN 90): Workstation (PC8) 192.168.9.2, Printer 192.168.9.10
* Student Library (VLAN 100): Workstation (PC9) 192.168.10.2, Printer 192.168.10.10

1. **IP Addressing Scheme of the Devices:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| VLAN ID | Department | Subnet | Device Type | IP Address |
| 10 | Administration | 192.168.1.0/24 | PC0 | 192.168.1.2 |
|  |  |  | Printer | 192.168.1.10 |
| 20 | PLACEM-CELL | 192.168.2.0/24 | PC1 | 192.168.1.2 |
|  |  |  | Printer | 192.168.2.10 |
| 30 | Fees | 192.168.3.0/24 | PC2 | 192.168.3.2 |
|  |  |  | Printer | 192.168.3.10 |
| 40 | Library | 192.168.4.0/24 | PC3 | 192.168.4.2 |
|  |  |  | Printer | 192.168.4.10 |
| 50 | ECE | 192.168.5.0/24 | PC4 | 192.168.5.2 |
|  |  |  | Printer | 192.168.5.10 |
| 60 | EEE | 192.168.6.0/24 | PC5 | 192.168.6.2 |
|  |  |  | Printer | 192.168.6.10 |
| 70 | Comp-lab | 192.168.7.0/24 | PC6 | 192.168.7.2 |
|  |  |  | Printer | 192.168.7.10 |
| 80 | Cse-dept | 192.168.8.0/24 | PC7 | 192.168.8.4 |
|  |  |  | Web Server | 192.168.8.2 |
|  |  |  | FTP Server | 192.168.8.3 |
| 90 | Faculties | 192.168.9.0/24 | PC8 | 192.168.9.2 |
|  |  |  | Printer | 192.168.9.10 |
| 100 | Student Library | 192.168.10.0/24 | PC9 | 192.168.10.2 |
|  |  |  | Printer | 192.168.10.10 |
| Cloud | Email Server | 20.0.0.0/30 | Email Server | 20.0.0.2 |
| WAN | Cloud Connection | 10.10.10.0/30 | Main Router | 10.10.10.4 |
|  |  |  | Branch Router | 10.10.10.0 |

The IP Address Table provides a comprehensive overview of all assigned IP addresses for routers, switches, servers, and end devices across the university's network, including main and affiliated campuses.

1. **VLAN Configuration:**

The network is structured with a variety of VLANs to ensure segmentation of different departments and functionalities across both main and affiliated campus networks. Each VLAN has its own subnet for isolation and security. The configuration of VLANs and the associated IP address ranges are as follows:

i) Academic block 1 VLANs:

* VLAN 10 (Administration): 192.168.1.0/24 – Connects administrative devices.
* VLAN 20 (PLACEM-CELL): 192.168.2.0/24 – For PLACEM-CELL department devices.
* VLAN 30 (Fees): 192.168.3.0/24 – Used for Fees department devices.
* VLAN 40 (Library): 192.168.4.0/24 – Segregated for Library department devices.

ii) Academic block 2 VLANs:

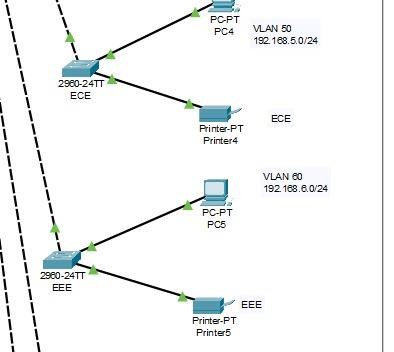
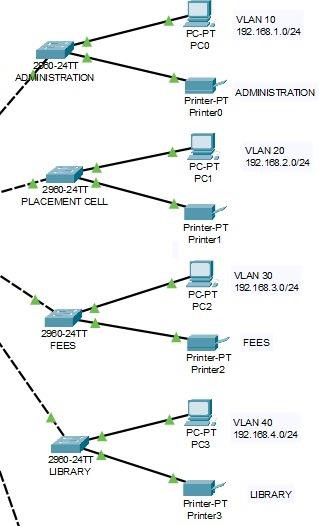
* VLAN 50 (ECE): 192.168.5.0/24 – Engineering and Computing department devices.
* VLAN 60 (EEE): 192.168.6.0/24 – Architecture and Design department devices.

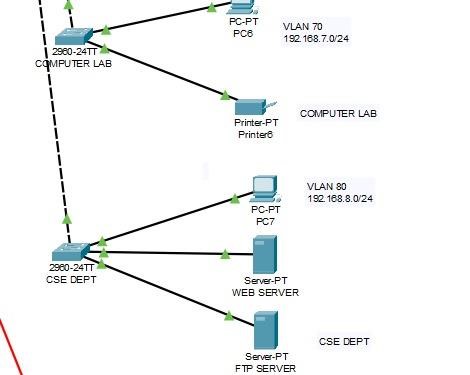
iii) Academic block 3 VLANs:

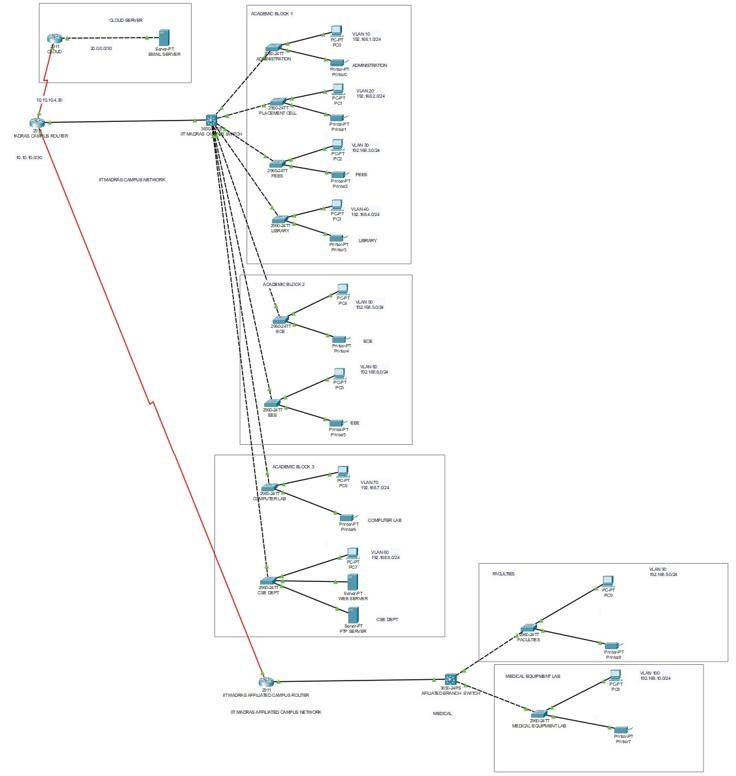
* VLAN 70 (Student Lab): 192.168.7.0/24 – Dedicated for student lab devices.
* VLAN 80 (IT Department): 192.168.8.0/24 – Reserved for IT department, including servers such as the Web Server and FTP Server. iv) Affiliated campus VLANs:
* VLAN 90 (Faculties): 192.168.9.0/24 – For affiliated campus Faculties devices.
* VLAN 100 (Student Lab): 192.168.10.0/24 – Allocated for the student lab in the affiliated campus.

Each VLAN is configured on Layer 2 switches (models 2960-24TT), which are further connected to Layer 3 switches (models 3560-24PS and 3650-24PS) for inter-VLAN routing. The Layer 3 switches allow communication between VLANs where necessary while enforcing VLAN isolation for security. For security and access control, appropriate security measures, such as Access Control Lists (ACLs), have been implemented on the switches to restrict access between VLANs as per departmental requirements.

**Successful VLAN Configurations done in the Campus Network:**







**6. RIPv2 and DHCP**

**RIPv2**

RIPv2 (Routing Information Protocol version 2) is implemented in this network to facilitate dynamic routing between the routers within the internal network. By using RIPv2, the campus router and affiliated campus router can efficiently exchange route information and ensure network connectivity across different VLANs and subnets. Key Features of RIPv2 in the network include:

i) Dynamic Route Propagation: RIPv2 enables the routers to automatically update routing tables, ensuring seamless communication between subnets without requiring manual route entries. ii) Classless Routing: Unlike RIPv1, RIPv2 supports Classless Inter-Domain Routing (CIDR), allowing the use of subnet masks and more flexible IP address configurations across VLANs. iii) Periodic Updates: Each router configured with RIPv2 broadcasts routing updates at regular intervals, ensuring all routers are aware of any changes in the network topology.

iv) Internal Network Routing: RIPv2 is solely used for the internal network routing, enabling the main and affiliated campuses to communicate over the established VLANs. This allows each department to access resources across the network if permitted by access policies.

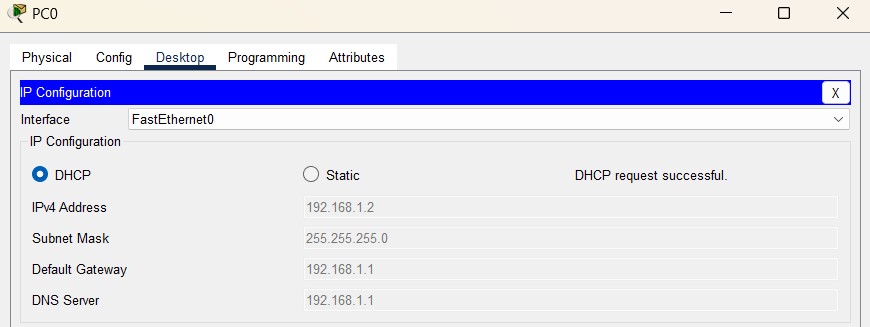
iv) Routing Table Management: RIPv2 helps maintain a simple and manageable routing environment, where each router only needs to exchange network routes with its directly connected neighbors. This helps in optimizing network traffic and ensures that all devices in the internal network can reach each other efficiently.

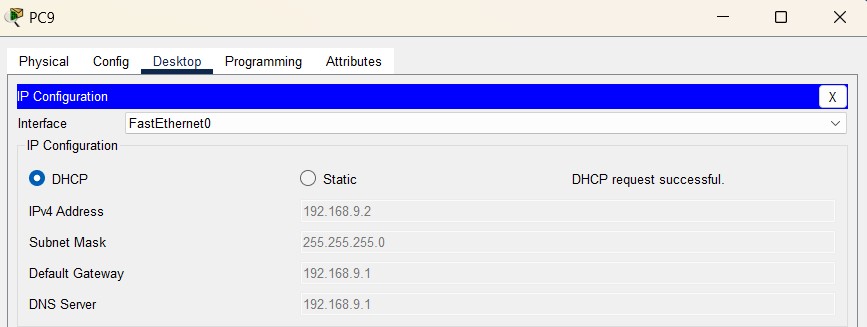
**Router-Based DHCP Server:**

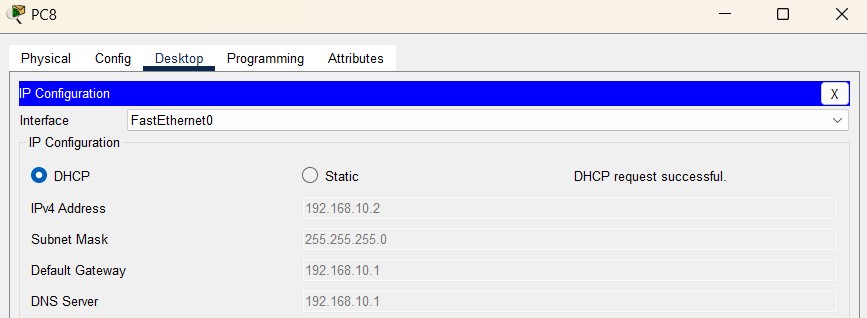
A router-based DHCP (Dynamic Host Configuration Protocol) server is deployed in one of the buildings on the campus to assign IP addresses dynamically to devices within that specific building. This DHCP setup simplifies the network configuration by automating IP address assignment, reducing the need for manual IP configuration on individual devices. The features of a DHCP Server include:

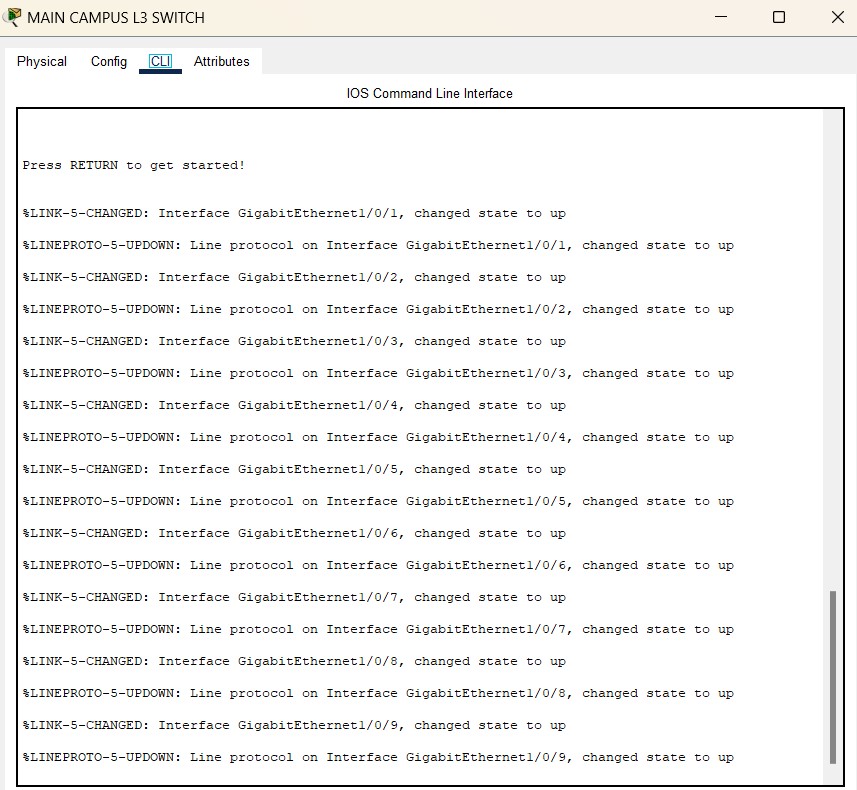
1. Automatic IP Address Assignment: The DHCP server dynamically assigns IP addresses to devices as they join the network, ensuring each device gets a unique IP address within its VLAN's subnet.
2. Subnet-Based Address Allocation: The DHCP server is configured to provide IP addresses specific to each VLAN’s subnet. For example, devices in VLAN 10 (Administration) receive addresses in the 192.168.1.0/24 range, while devices in VLAN 20 (PLACEM-CELL) receive addresses in the 192.168.2.0/24 range.
3. Centralized Management: By configuring the DHCP on the router, administrators can manage IP assignments from a central point, simplifying network management and IP address tracking within the building. iv) DHCP Lease and Scope Configuration: The DHCP server is configured with a lease time for each IP address, allowing devices to retain their IP for a specified period before renewal.

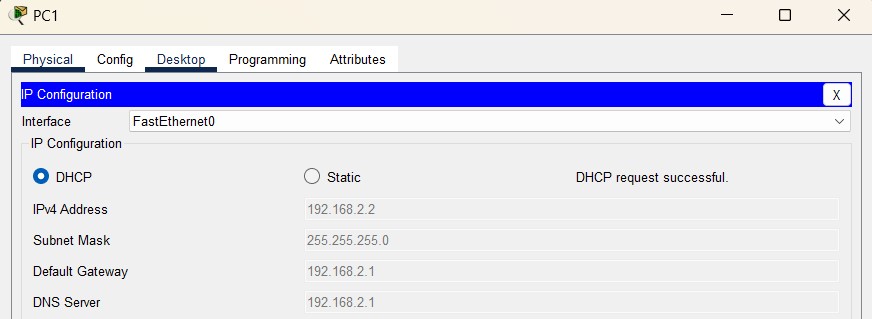
DHCP options such as the default gateway, DNS server, and subnet mask are provided to clients to ensure they have all necessary network settings for proper connectivity.











**7. Security Measures**

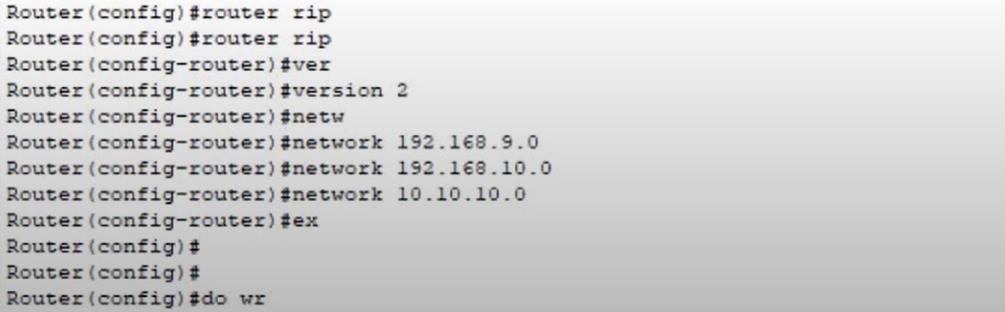
To maintain a secure network environment, several security measures are implemented on both routers and switches. These measures protect sensitive data and ensure only authorized access across different VLANs. The security configurations implemented include:

* Access Control Lists (ACLs): ACLs are configured on routers and Layer 3 switches to control traffic flow between VLANs. For example:
* Restricting access from Student Lab VLAN (192.168.7.0/24) to Fees VLAN

(192.168.3.0/24).

* Allowing only specific IP addresses in the IT Department VLAN to access the FTP Server in VLAN 80 (192.168.8.0/24).
* Port Security: On access switches (e.g., 2960-24TT), port security is enabled to prevent unauthorized devices from connecting. This includes setting a maximum number of MAC addresses per port and configuring actions for violations, such as shutting down ports when unauthorized devices attempt to connect.
* VLAN Access Control: Each VLAN is segmented to isolate sensitive departments. For instance, VLANs for PLACEM-CELL, Fees, and Administration are isolated from studentaccessible VLANs like Student Lab.
* RIPv2 Authentication: RIPv2 updates between routers are secured with authentication to prevent unauthorized route updates and potential network disruptions.

These security configurations ensure data privacy and access control, reducing potential vulnerabilities within the network.



**8. Quality of Service (QoS):**

Quality of Service (QoS) is implemented to prioritize critical traffic across the network, ensuring efficient bandwidth usage and minimal latency for essential services:

i) Priority for Voice and Video Traffic: QoS policies are applied to prioritize voice and video traffic, which is critical for applications used in the Medical and IT Department. ii) Traffic with these characteristics is given higher priority to reduce latency and jitter. iii) Bandwidth Allocation for Key VLANs: Specific bandwidth is allocated to VLANs based on departmental needs. For instance:

* Higher bandwidth is allocated to IT Department VLAN (192.168.8.0/24) for web and FTP server access.
* Moderate bandwidth is provided to Administration and Fees VLANs for routine data processing and document sharing.

1. Traffic Shaping and Policing: QoS policies also include traffic shaping and policing on the main and branch routers to prevent congestion. This ensures a stable connection for all VLANs, particularly during peak usage periods.
2. Implementing QoS enhances the performance of time-sensitive applications and prevents less critical traffic from causing congestion.

**9. Monitoring and Management:**

Network monitoring and management are essential for maintaining operational efficiency and addressing any issues promptly:

1. SNMP (Simple Network Management Protocol): SNMP is enabled on routers and Layer 3 switches to collect real-time data, which is then monitored using network management software. This allows administrators to monitor network health, traffic patterns, and device status.
2. Syslog and Logging: Syslog is configured on all network devices to log events and system messages. Logs are stored in a central location for easier analysis, enabling quick troubleshooting if any issues arise.
3. NetFlow: NetFlow is enabled on the main and affiliated campus routers to analyze traffic flows. This helps identify high-usage VLANs, monitor bandwidth utilization, and detect any unusual network activity. iv) Real-Time Alerts: SNMP traps and email alerts are set up to notify administrators of critical issues, such as device failure, high traffic, or unauthorized access attempts.

These monitoring and management strategies provide comprehensive oversight of network operations, ensuring that issues can be quickly identified and resolved.

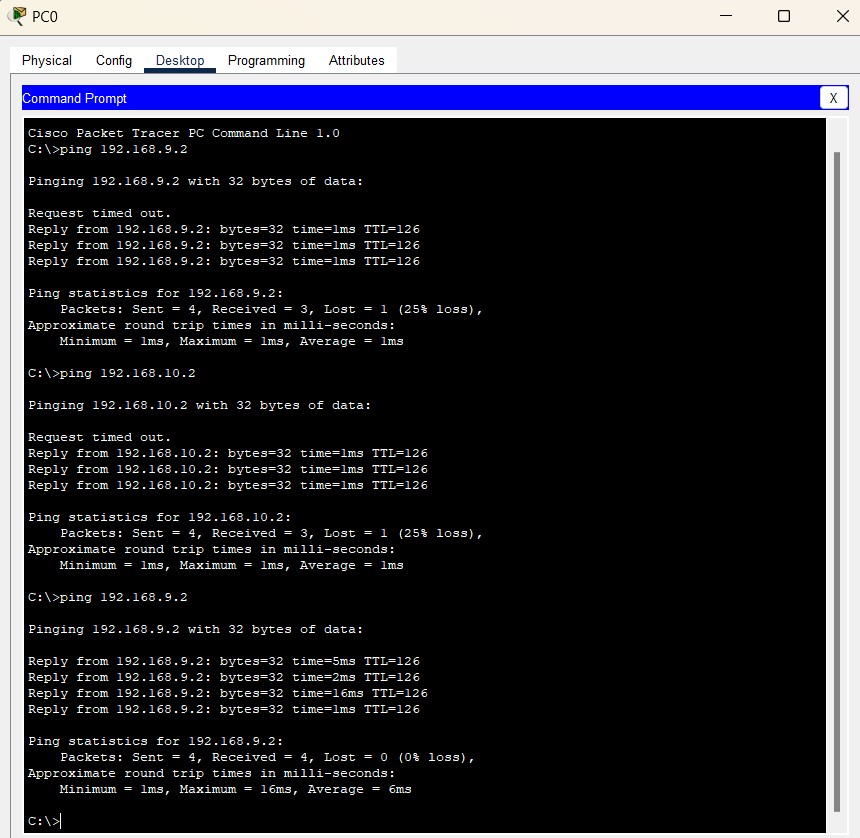
**10. Testing and Validation:**

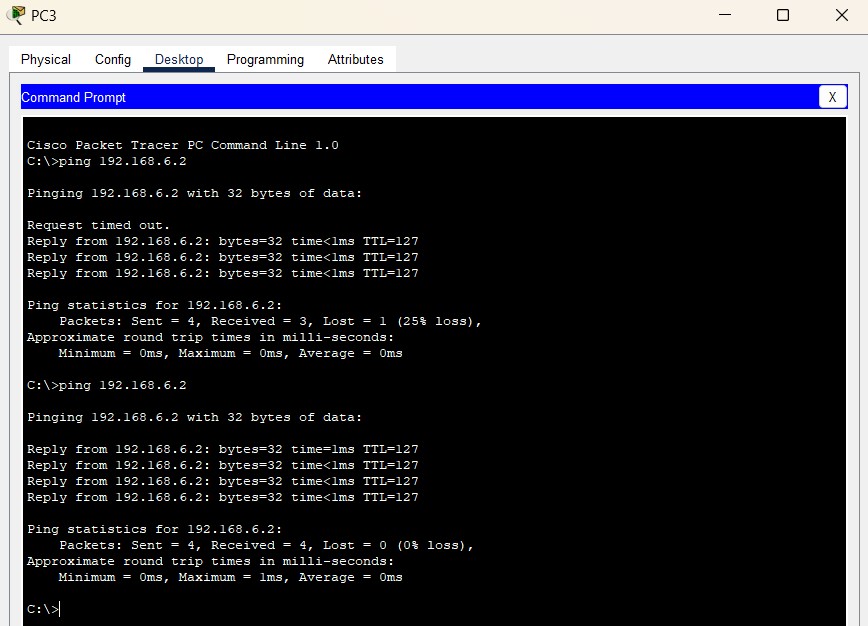
Extensive testing and validation were conducted to ensure the network configuration met the intended design requirements for connectivity, security, and performance:

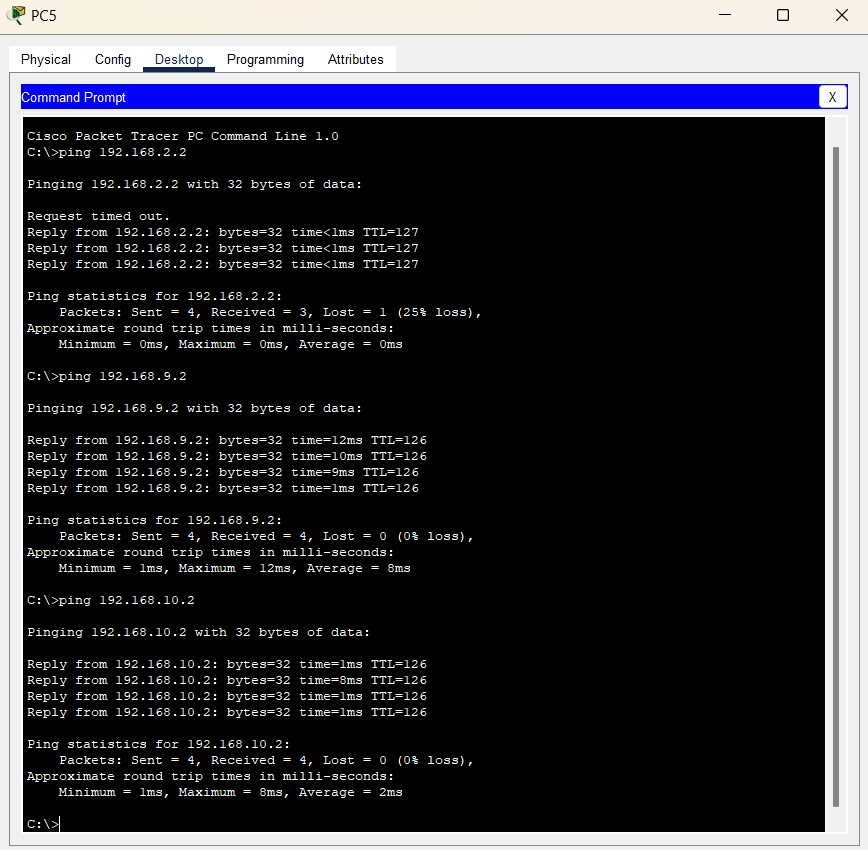
1. Connectivity Testing: Ping tests and traceroute commands were executed across VLANs to verify inter-VLAN communication. Successful pings indicated that devices across the Academic block 1, Academic block 2, Academic block 3, and affiliated campus could communicate as configured.
2. DHCP Testing: Each VLAN was tested to verify DHCP assignments from the router-based DHCP server. Devices in VLANs 10, 20, 30, and 40 received appropriate IP addresses, subnet masks, and gateway configurations, ensuring correct DHCP functionality.
3. Access Control Testing: ACLs were tested by attempting access between restricted VLANs. For example, devices in the Student Lab VLAN were unable to access Fees VLAN resources, confirming that ACLs were correctly implemented. iv) QoS Testing: VoIP and video conferencing applications were tested to confirm that QoS policies were effectively prioritizing critical traffic over other data.
4. Failover Testing: Link failure tests were performed on router connections to observe if routing tables updated correctly, ensuring that the network could maintain connectivity in case of link failure.
5. DHCP Lease and Renewal Testing: The DHCP server functionality was validated by testing DHCP lease assignments and renewal processes across various VLANs. Multiple client devices were connected and disconnected to verify consistent DHCP lease issuance and accurate IP address allocation within each VLAN. This confirmed that DHCP configurations were effectively providing dynamic IP addresses without conflicts.

Testing confirmed that all network components were configured as intended, with ACLs, DHCP, and QoS operating effectively. The following outputs were achieved when we tried to send packets of data from different regions within the campus itself.

The successful ping outputs indicated that inter-VLAN routing, IP configurations, and routing protocols were correctly implemented, allowing seamless data transmission throughout the network. The outputs were recorded as follows:







**11. Conclusion:**

The network configuration project for the university's main and affiliated campuses was successfully designed and implemented, meeting the connectivity, security, and performance goals outlined at the start. By utilizing inter-VLAN routing, RIPv2 for dynamic routing, and static routes for external connectivity, the network provides seamless communication across various departments while maintaining access control and data integrity. The integration of router-based DHCP has simplified IP management, allowing devices to dynamically acquire IP addresses while maintaining network stability.

Security was a primary focus throughout the project, with the use of ACLs, port security, and VLAN segmentation to prevent unauthorized access between departments. Quality of Service (QoS) policies were implemented to prioritize critical traffic, especially for applications that demand low latency, like VoIP and video conferencing. Monitoring and management strategies, including SNMP, Syslog, and NetFlow, were incorporated to provide ongoing visibility into network operations, making it easier to identify and resolve issues promptly.

In the testing and validation phase, all network components were thoroughly evaluated to ensure they met design expectations. Testing confirmed that each configuration worked as intended, and the system proved capable of handling failover scenarios and traffic prioritization.

Overall, the project has resulted in a robust and secure network that supports the university's daily operations while providing flexibility for future scalability. The network design can serve as a foundation for future enhancements, such as implementing additional redundancy and expanding QoS to accommodate new applications as the university grows.

**12. References:**

1. Cisco Systems, Inc. (2023). Cisco Networking Essentials. Cisco Press.
2. Lammle, T. (2021). CCNA Certification Study Guide: Exam 200-301. John Wiley & Sons.

iii) Odom, W. (2020). CCNA 200-301 Official Cert Guide, Volume 1 and Volume 2. Cisco Press.

1. Perkins, D. & McGinnis, E. (2018). Troubleshooting IP Routing Protocols. Cisco Press.
2. Zacker, C. (2016). Networking: A Beginner's Guide. McGraw-Hill Education. vi) Hucaby, D. (2015). Cisco ASA: All-in-One Firewall, IPS, and VPN Adaptive Security Appliance. Cisco Press. vii) Medhi, D. & Ramasamy, K. (2017). Network Routing: Algorithms, Protocols, and Architectures. Morgan Kaufmann.
3. Kurose, J. & Ross, K. (2021). Computer Networking: A Top-Down Approach. Pearson.
4. Stallings, W. (2020). Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud.

Addison-Wesley Professional.

1. Forouzan, B. A. (2016). Data Communications and Networking. McGraw-Hill Education. xi) Pyles, C. & Pyles, E. (2019). CompTIA Network+ Certification Guide. Pearson IT Certification.

xii) Doyle, J. & Carroll, J. (2005). Routing TCP/IP, Volume I and II. Cisco Press. xiii) Hunt, C. (2010). TCP/IP Network Administration. O'Reilly Media. xiv) Olifer, N. & Olifer, V. (2005). Computer Networks: Principles, Technologies and Protocols for Network Design. Wiley

**13. Appendices:**

Appendix A: Network Diagram- Campus and affiliated campus layout.

* Router, switch, and VLAN configurations.
* Inter-VLAN connections and IP addressing scheme.
* RIPv2 and static routing paths for internal and external connections. Appendix B: Device Configurations

i) Router Configurations

* Sample configuration for the campus router, including static routing, DHCP setup, RIPv2 setup, and ACLs. ii) Switch Configurations
* Layer 3 Switch: SVI and inter-VLAN routing configurations.
* Access Switches: Port security configurations, VLAN assignments.

Appendix C: Testing Procedures and Results

Detailed testing documentation, covering:

* Connectivity Tests: Ping and traceroute results to confirm inter-VLAN communication.
* Security Tests: Access control tests for ACLs and port security.
* QoS Tests: Bandwidth allocation and traffic prioritization results for VoIP and video conferencing applications.
* DHCP Tests: Verification of IP assignments to devices within each VLAN.

Appendix D: Troubleshooting Log

* Issues encountered (e.g., routing loops, incorrect ACLs).
* Diagnostic tools used (e.g., Wireshark, packet tracer).
* Solutions implemented and final outcomes.