



Enhancing Network Performance: Qos and Congestion Control In Campus Networks

Thesis

HARAMAYA UNIVERSITY

Submitted to Haramaya Institute of Technology

**In partial fulfillment of the requirements for the degree of Bachelor of Science
in Electrical and Computer Engineering (Computer Engineering)**

BY

Name

ID

- | | |
|-------------------|----------|
| 1. EBISA ACHAME | 1786/12 |
| 2. KENA BAYISA | 2203/12 |
| 3. YOSBEK ENDALU | 3087/12 |
| 4. TSIYON GEMECHU | 2950 /12 |

Declaration

We declare that this Thesis represents our work which has been done after registration for School of Electrical and Computer Engineering specialization in Computer Engineering at Haramaya University. We declared that the work contained in this thesis is our own, except where explicitly stated otherwise. In addition, this work has not been previously included in a thesis submitted to this or any other institution for qualifications. We have attempted to identify all the risks related to this project that may arise in conducting this project, obtained the relevant ethical and/or safety approval, and acknowledged our obligations and the rights of the participants

Name	Id	Signature
1. Ebisa Achame	1786/12	_____
2. Kena Bayisa	2203/12	_____
3. Yosbek Endalu	3087/12	_____
4. Tsiyon Gemechu	2950 /12	_____

Approval Page

This is to certify that Thesis entitled “Enhancing Network Performance: Qos And Congestion Control In Campus Networks” that is submitted by this group members in partial fulfillment of the requirement for the fulfillment of Final Thesis in the degree BSC in Electrical and Computer Engineering (Computer Engineering) of Haramaya University, is a record of the candidate own work carried out by him under my own supervision. The matter embodies in thesis is original and has not been submitted for the award of any other degree.

This thesis has been submitted for examination with approval of university advisor.

Advisor Name	Signature	Date
Mr. Wehib Abubeker	_____	_____
Department Dean Name		
Mr. Wehib Abubeker	_____	_____

Acknowledgement

We would like to express our deepest gratitude to the Almighty God, whose guidance and blessing have illuminated our path throughout the journey of this project. His unwavering support has been the cornerstone of our perseverance and success.

We extend our sincerest appreciation to our thesis advisor, Mr. Wehib Abubeker whose invaluable guidance, mentorship, and unwavering encouragement have been instrumental in shaping our understanding and approach towards this project. We are profoundly thankful to our families for their unconditional love, unwavering support, and understanding during the course of this endeavor. Their patience, encouragement, and sacrifices have been the driving force behind our pursuit of knowledge and academic achievement. We would also like to express our gratitude to School of Electrical and Computer Engineering in Haramaya University who provided assistance, resources, or support during the course of the project.

Lastly, we would like to express our gratitude to all those who have contributed, directly or indirectly, to the completion of this thesis. Your support and encouragement have been invaluable, and we are deeply grateful for your unwavering belief in our abilities.

With heartfelt appreciation!

Abstract

In today's increasingly interconnected world, the efficiency and reliability of network infrastructures within campus environments are paramount for facilitating seamless communication, collaboration, and access to digital resources. This thesis focuses on enhancing network performance through the strategic implementation and optimization of Quality of Service (QoS) and congestion control mechanisms within campus networks, leveraging the versatile simulation capabilities of Cisco Packet Tracer. The proposed thesis aims to address the multifaceted challenges faced by network administrators and stakeholders in orchestrating agile, resilient, and high-throughput networking infrastructures. By synthesizing existing literature, conducting empirical analyses, and leveraging Cisco Packet Tracer's simulation environment, this study seeks to elucidate the intricate interplay between QoS provisioning, congestion control, and network performance optimization within campus settings. The project encompassed the design of representative campus network topologies within Cisco Packet Tracer, configuration of QoS policies to prioritize traffic and allocate resources fairly, and deployment of congestion control mechanisms to mitigate adverse effects of network congestion. The anticipated findings hold significant implications for academia, industry, and network practitioners, providing actionable insights into the design, management, and optimization of campus network infrastructures. By advancing our understanding of effective network management strategies and leveraging innovative simulation methodologies, this project endeavors to foster a conducive ecosystem for seamless digital interactions, knowledge dissemination, and technological innovation within campus communities.

Key Words: Congestion, Quality Of Services, Redundancy, Congestion Control Mechanism, Network Performance

Table of Contents	
Declaration	i
Approval Page	ii
Acknowledgement	iii
List of figures	viii
List of Tables	ix
List of Acronyms	x
CHAPTER ONE	1
INTRODUCTION	1
1.1 Background	1
1.2 Statement of Problem	1
1.3 Objective	2
1.3.1 General Objective	2
1.3.2 Specific Objectives	3
1.4 Scope of the Study.....	3
1.5 Significance of the Study	4
1.6 Rationale for thesis.....	6
1.7 Feasibility Study.....	6
1.7.1 Operational Feasibility	6
1.7.2 Economic Feasibility	6
1.7.3 Technical Feasibility.....	6
1.8 Motivation of project.....	7
1.9 Risk Assessment.....	7
CHAPTER TWO	8
LITERATURE REVIEW	8
2.1 Introduction to Campus Area Network	8
2.1.1 The Components of a Campus Area Network.....	9
2.1.2 How Campus Area Network Work Functions.....	16
2.1.3 The Benefits of a Campus Area Network.....	17
2.2 Network Performance	18
2.2.1 Key metrics used to measure Network Performance.....	18

2.2.2 Quality of service.....	19
2.2.3 Network Congestion and Control Mechanism	20
2.2.4 The trade-off between congestion control and Quality of Service	20
2.3 Related Work.....	21
2.4 Existing Solutions and Limitations	24
2.5 Emerging Challenges	24
CHAPTER THREE	26
METHODOLOGY	26
3.1 Materials and tools	26
3.1.1 Materials	26
3.1.2 Designing tool.....	28
3.2 Campus Network Topology Design.....	29
3.2.1 Hierarchical network design model.....	30
3.3 Implementation.....	33
3.3.1 Basic configuration.....	33
3.3.2 STP port-fast and BPDU guard configuration on all access ports	34
3.3.3 Ether-channel or Link aggregation configuration	36
3.3.4 Sub-netting and ip addressing.....	37
3.3.5 Creating VLAN on Access, Distributions, and Core switches.....	41
3.3.6 Configuring Static ip address	41
3.3.7 HSRP configuration and Assigning Ip DHCP helper Address.....	43
3.3.8 Configuring OSPF	48
3.3.9 Configuring firewall interface security zones and levels	48
3.3.10 Wireless network configuration.....	51
3.3.11 QOS Configuration.....	52
CHAPTER FOUR.....	54
TESTING AND RESULT	54
4.1 Checking Status.....	54
4.2 Testing.....	55
CHAPTER FIVE	58
CONCLUSION AND RECOMMENDATION	58
5.1 Conclusion.....	58

5.2 Recommendation.....	59
References.....	61
Appendices.....	I
Appendix I. Basic Configuration	I
Appendix II. Configuration for creating VLAN	I
Appendix III HSRP CONFIGURATION	II
Appendix IV OSPF Configuration.....	VI
Appendix v Firewall interface security zones and levels configuration	VI
Appendix VI Firewall inspection policies configuration	VII

List of figures

FIGURE 2.1 ROUTER	9
FIGURE 2.2 MULTI-LAYER SWITCH	10
FIGURE 2.3 ACCESS SWITCH	11
FIGURE 2.4 FIREWALL	12
FIGURE 2.5 SERVER	13
FIGURE 2.6 WIRELESS LAN CONTROLLER	14
FIGURE 2.7 PACKET TRACER	16
FIGURE 3.1 DESIGN STEPS	30
FIGURE 3.2 ACCESS-LAYER	30
FIGURE 3.3 CORE AND DISTRIBUTION LAYER	31
FIGURE 3.4 INTERNAL NETWORK	32
FIGURE 3.5 EXTERNAL NETWORK	33
FIGURE 3.6 TOPOLOGICAL VIEW OF CAMPUS AREA NETWORK	33
FIGURE 4.1 ETHER-CHANNEL STATUS	54
FIGURE 4.2 HSRP STATUS	54
FIGURE 4.3 VLAN STATUS	55
FIGURE 4.4 DHCP ADDRESS	55
FIGURE 4.5 PINGING	56
FIGURE 4.6 WLAN TESTING	56
FIGURE 4.7 SSH TESTING	57

List of Tables

TABLE 3.1 EQUIPMENT LIST26

TABLE 3.2 IP ADDRESS39

List of Acronyms

QoS	-----	Quality of Service
RED	-----	Random Early Detection
NFV	-----	Network Function Virtualization
VLANs	-----	Virtual local Area Network
LANs	-----	Local Area Networks
WAN	-----	Wide Area Networks
TCP	-----	Transmission Control Protocol
RED	-----	Random Early Detection
CAN	-----	Campus Area Network
BGP	-----	Border Gateway Protocol
CLI	-----	Command-line Interface
IOS	-----	Internetworking Operating System
ACLs	-----	Access Control Lists
MAC	-----	Media Access Control
RSTP	-----	Rapid Spanning Tree Protocol
PoE	-----	Power over Ethernet
IP	-----	Internet Protocol
NAT	-----	Network Address Translation
VPN	-----	Virtual Private Network
IDS	-----	Intrusion Detection System
IPS	-----	Intrusion Prevention System
WLC	-----	Wireless LAN Controller

Aps ----- Access Points

WPA2 ----- Wi-Fi Protected Access 2

EAP ----- Extensible Authentication Protocol

AES ----- Advanced Encryption Standard

SNMP ----- Simple Network Management Protocol

HTTP ----- Hypertext Transfer Protocol

CPU ----- Central Processing Unit

OSI ----- Open Systems Interconnection

DMZ ----- Demilitarized Zone

DHCP ----- Dynamic Host Configuration Protocol

FTP ----- File Transfer Protocol

DNS ----- Domain Name System

SSH ----- secure shell

VTY ----- Virtual Terminal

STP ----- Spanning Tree Protocol

BPDU ----- Bridge Protocol Data Units

SVI ----- Switched Virtual Interface

HSRP ----- Hot Standby Router Protocol

OSPF ----- Open Shortest Path First

CHAPTER ONE

INTRODUCTION

1.1 Background

In the modern digital age, where information exchange is pivotal for every facet of academia and business, the efficacy of network infrastructures holds paramount importance. Within campus environments, the demand for reliable and high-performance networking capabilities has intensified exponentially with the proliferation of online learning platforms, collaborative thesis endeavors, and data-intensive applications. Consequently, the efficient management of Quality of Service (QoS) and congestion control mechanisms within campus networks emerges as a critical imperative to sustain seamless connectivity, optimize resource utilization, and ensure user satisfaction.

Campus Area Networks provide a simple way for organizations to control their network resources, centralize their security efforts and share data quickly. Let's explore how each of these benefits work within a campus area network. Campus environments serve as dynamic hubs of intellectual exchange, where students, faculty members, researchers, and administrative staff rely extensively on network infrastructures to facilitate communication, collaboration, and access to digital resources [1]. With the proliferation of diverse applications ranging from real-time video conferencing to cloud-based data analytics platforms, the demand for robust and high-performance networking capabilities within campus networks has escalated significantly in recent years.

1.2 Statement of Problem

Ideally when it comes to network performance, there are several key metrics you should consider. There is no Latency the time it takes for data to travel from the source to the destination is very small. This implies that network speed is very high. For copper wire the speed of data transfer is equal with electric signal speed. When we use fiber optic the speed of data transfer must be equal with speed of light. There is no Jitter, ideally since there is no latency, there is no variability in latency. Data transmission is consistent. There is no packet loss, ever packet sent from a source reaches it's destination. Throughput is the same

with bandwidth and it is the amount of data transferred per unit of time. Network is always available and operational. There is no downtime.

In practical throughput can't be equal with bandwidth. Due to noises and characteristics of network devices and links theoretically expected capacity of devices and network link bandwidth can't be achieved. Throughput is always less than bandwidth. Due to limited bandwidth of network links, when many users want to access network at the same time it leads to network traffic congestion. At this time if the amount of packet exceeds the storage capacity of network devices it leads to packet loss. Sometime networking devices accidentally stop its operation, so the network is down.

This project focuses on solving the existing problem in campus area network with available resource. To avoid single point of failure we used redundant links so that if one link fail we can access network through another link. This is achieved by using two distribution and two core Switches. At distribution layer when one switch is active the other is used as standby. If the operating switch fails and down the standby switch automatically up so that the network is available and the downtime is minimal. Multiple physical ethernet links of multilayer switches are combined together to create single logical link. This single logical link provides high bandwidth for network traffic. Priority is also configured for important traffic so that when network experience congestion the priority is given for high priority traffic. This is very important for applications that are sensitive to delay. The campus network is divided into multiple VLANs to minimize broadcast domain.

1.3 Objective

1.3.1 General Objective

The general objective of this thesis is to enhance network performance within campus environments through the strategic implementation and optimization of Quality of Service (QoS) and congestion control mechanisms using Cisco Packet Tracer.

1.3.2 Specific Objectives

- ✓ To design and implement representative campus network topologies within Cisco Packet Tracer, capturing the diverse network elements and traffic patterns characteristic of campus environments.
- ✓ To configure and evaluate Quality of Service (QoS) policies within the simulated campus network, prioritizing traffic, allocating bandwidth, and managing queues to meet predefined service level objectives.
- ✓ To conduct controlled experiments and performance evaluations within the simulated campus network, measuring key performance metrics such as throughput, latency, packet loss, and fairness under different network conditions and traffic scenarios.
- ✓ To analyze the effectiveness and efficiency of QoS and congestion control mechanisms in enhancing network performance, identifying optimal configurations and best practices for network optimization within campus environments.

1.4 Scope of the Study

The scope of the thesis on enhancing network performance through Quality of Service (QoS) and congestion control in campus environments encompasses several key dimensions, as outlined below:

Campus Network Infrastructure: This thesis will primarily focus on the network infrastructure deployed within campus environments, including wired and wireless networks, routers, switches, access points, and other networking devices. The investigation will encompass both local area networks (LANs) and wide area networks (WANs) interconnected across campus premises.

Traffic Characteristics: The Project will consider the diverse spectrum of traffic types traversing campus networks, including but not limited to data transfers, real-time multimedia streams, voice communications, video conferencing, and web browsing. The analysis will account for the varying QoS requirements, traffic patterns, and temporal dynamics associated with different types of network traffic.

QoS Mechanisms: The study will explore a range of QoS mechanisms and protocols aimed at prioritizing, shaping, and managing network traffic to meet predefined service level objectives. This includes techniques such as traffic classification, prioritization, traffic shaping, bandwidth allocation, and admission control, among others.

Congestion Control Strategies: The project will investigate congestion control mechanisms designed to regulate the flow of network traffic, prevent congestion-induced performance degradation, and ensure equitable resource allocation. This encompasses both reactive congestion control algorithms, such as TCP congestion avoidance and congestion control protocols like Random Early Detection (RED), as well as proactive congestion control strategies and traffic engineering approaches.

Evaluation Methodologies: Empirical analyses, simulation studies, and theoretical modeling will be employed to evaluate the performance, scalability, and effectiveness of proposed QoS and congestion control strategies within campus environments. The project will utilize relevant performance metrics such as throughput, latency, packet loss, fairness, and resource utilization to assess the impact of interventions and optimizations.

Limitations: It's important to acknowledge that while the scope of the study is comprehensive, certain limitations may exist. These include constraints related to access to proprietary network infrastructure, scalability of experimental setups, and generalization of findings across diverse campus environments. Efforts will be made to mitigate these limitations through rigorous experimental design, sensitivity analysis, and validation in multiple contexts where feasible.

1.5 Significance of the Study

The thesis on enhancing network performance through the optimization of Quality of Service (QoS) and congestion control mechanisms within campus environments carries significant implications and potential benefits across multiple dimensions:

Improved User Experience: By enhancing QoS provisioning and congestion control strategies, the thesis aims to elevate the overall quality of user experience within campus networks. This improvement will be particularly beneficial for students, faculty members, researchers, and administrative staff who rely extensively on network connectivity for

accessing educational resources, conducting research activities, and engaging in collaborative endeavors.

Enhanced Productivity and Collaboration: Optimal network performance facilitates seamless communication and collaboration among stakeholders within campus environments. By mitigating congestion-induced disruptions and ensuring equitable resource allocation, the thesis can foster a conducive ecosystem for interdisciplinary interactions, knowledge exchange, and collaborative research initiatives, thereby enhancing productivity and innovation across academic and administrative domains.

Resource Optimization and Cost Reduction: Effective QoS provisioning and congestion control mechanisms enable judicious utilization of network resources, thereby reducing wastage and optimizing operational efficiency. By minimizing network congestion and ensuring efficient resource allocation, the thesis has the potential to alleviate network bottlenecks, lower infrastructure costs, and enhance the cost-effectiveness of campus network management.

Support for Emerging Applications and Technologies: As campus environments embrace emerging technologies and innovative applications, the demand for adaptable and scalable networking infrastructures becomes increasingly pronounced. By investigating novel QoS paradigms and congestion control strategies, the thesis endeavors to address the evolving requirements of emerging applications such as Internet of Things (IoT), augmented reality (AR), and virtual reality (VR), thereby future-proofing campus networks and facilitating seamless integration of cutting-edge technologies.

Contribution to Knowledge and Best Practices: Through empirical analyses, theoretical modeling, and real-world deployment, the thesis seeks to generate new knowledge and best practices in the domain of campus network optimization. By elucidating the underlying dynamics of QoS provisioning and congestion control, the thesis aims to contribute to the advancement of networking theory and inform the development of practical guidelines and recommendations for network administrators and stakeholders.

1.6 Rationale for thesis

Against this backdrop, there exists a compelling imperative to undertake comprehensive thesis endeavors aimed at elucidating the intricate interplay between QoS provisioning, congestion control, and network performance optimization within campus environments. By leveraging advances in networking paradigms, algorithmic design, and empirical methodologies, this research seeks to unravel the underlying complexities, identify critical bottlenecks, and propose innovative solutions to bolster the resilience, efficiency, and scalability of campus network infrastructures.

1.7 Feasibility Study

1.7.1 Operational Feasibility

With the successful deployment and utilization of simulation software, the operational aspects of managing and maintaining the enhanced network performance have been proven viable. The research has demonstrated that the proposed enhancements can be integrated seamlessly into existing network infrastructure and effectively managed by network administrators.

1.7.2 Economic Feasibility

The cost-benefit analysis revealed that the long-term benefits, including improved network reliability, reduced downtime, and enhanced user experience, outweighed the initial investment in simulation software and hardware upgrades. The research has thus established the economic feasibility of enhancing network performance through QoS and congestion control in campus networks.

1.7.3 Technical Feasibility

A detailed technical feasibility analysis was conducted to evaluate the practicality and effectiveness of implementing QoS and congestion control mechanisms using simulation software. The research involved testing various network configurations and scenarios to ensure compatibility with existing software systems. The results demonstrated the technical feasibility of deploying the proposed enhancements, with the simulation software providing a reliable platform for testing and optimization.

1.8 Motivation of project

The motivation behind the project stems from the critical need to improve the efficiency and reliability of campus networks. By focusing on QoS and congestion control mechanisms, the thesis aims to develop innovative solutions that can optimize resource utilization, prioritize critical traffic types, and ensure consistent network performance even under heavy loads. The ultimate goal is to contribute to the advancement of network management strategies that can elevate the quality of service delivery in campus environments, meeting the evolving needs of users and enhancing overall network performance. This thesis is driven by the desire to address the existing challenges faced by campus networks and pave the way for a more efficient and resilient network infrastructure.

1.9 Risk Assessment

A thorough risk assessment was conducted to identify and mitigate potential risks associated with the implementation of network performance enhancements. Risks such as software compatibility issues, network disruptions during implementation, and user resistance to changes were identified and addressed through contingency planning.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction to Campus Area Network

A Campus Area Network (CAN) is a type of computer network that connects multiple buildings or sites within a limited geographic area, such as a university campus, corporate headquarters, or military base. It provides high-speed connectivity and enables communication and data sharing among various devices, systems, and users within the network.

A CAN typically consists of interconnected local area networks (LANs), which are individual networks within each building or site, and a backbone network that connects these LANs. The backbone network is responsible for carrying data traffic between different LANs and providing a centralized management system for the entire CAN.

At the heart of a campus area network is the main data center, where all the network equipment is located. This data center houses the core switches, routers, and servers that ensure seamless communication between different buildings. The core switches act as the central hub, connecting all the other switches and devices throughout the campus.

From the data center, the network equipment is distributed to various buildings through fiber optic cables. These cables carry large amounts of data at high speeds, ensuring fast and reliable connectivity. Each building is equipped with distribution switches that connect to the core switches in the data center, forming a hierarchical network architecture.

One of the main advantages of a CAN is its scalability. It can easily accommodate a large number of users and devices, allowing for seamless expansion as the network grows. Additionally, a CAN provides a secure and reliable network infrastructure, with multiple layers of security measures to protect sensitive data and prevent unauthorized access.

Common applications of a CAN include supporting educational institutions by connecting classrooms, libraries, and administrative buildings; facilitating communication and

collaboration within a corporate campus; and enabling efficient command and control operations in military complexes. By establishing a CAN, organizations can enhance their operational efficiency, improve communication and data sharing, and streamline their network management processes.

2.1.1 The Components of a Campus Area Network

1. Routers

Routers play a crucial role in a campus area network. They are responsible for directing network traffic and ensuring that data packets are delivered to their intended destinations. Routers are usually connected to multiple networks and use protocols such as Border Gateway Protocol (BGP) to communicate with other routers in order to determine the best path for data transmission



Figure 2.1 Router

Function of Router

Routing Functionality: Routers determine the best path for data packets to travel from the source to the destination network

Interface Connectivity: Routers have multiple interfaces, allowing them to connect to various types of networks such as LANs, WANs, and the Internet.

Configuration and Management: Routers are configured and managed through a command-line interface (CLI) using an operating system like Cisco IOS. Administrators can use commands to configure router interfaces, routing protocols, and network settings.

Routers offer security features such as access control lists (ACLs) and firewalls to protect networks from unauthorized access and attacks. Routers support QoS mechanisms to prioritize network traffic and ensure optimal performance for critical applications.

2. Switches

Switches are essential for connecting devices within a campus area network. They are responsible for creating a network connection between different devices, such as computers, servers, and printers. Switches can transmit data at high speeds and are capable of filtering and forwarding data packets based on MAC addresses.

a. Multilayer Switch

A multilayer switch is a high-capacity switch generally positioned within the backbone or physical core of a network. It serves as the gateway to a wide area network (WAN) or the Internet; they provide the final aggregation point for the network and allow multiple aggregation modules to work together [2].

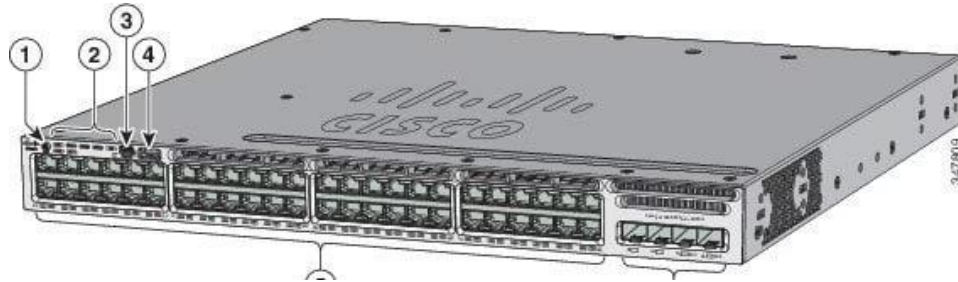


Figure 2.2 Multi-Layer Switch

Function of multilayer switch

Aggregation: multilayer switches aggregate network traffic from multiple access switches within a local area network (LAN) or a specific network segment. They consolidate traffic from various endpoints and distribute it to the core switch or other distribution switches for further routing.

Interconnection: multilayer switches serve as the primary connection point for access switches and core switches in the network topology. They facilitate communication between access switches within the same LAN and provide connectivity to the core switch for inter-VLAN routing and access to resources outside the local network.

VLAN Segmentation: Distribution switches often perform VLAN segmentation by assigning VLAN memberships to different ports or network segments.

Quality of Service (QoS): multilayer switches support QoS features to prioritize and manage network traffic effectively.

They may implement QoS policies to ensure that critical applications, such as voice and video communication, receive preferential treatment over less time-sensitive traffic.

Spanning Tree Protocol (STP): multilayer switches participate in STP or Rapid Spanning Tree Protocol (RSTP) to prevent network loops and ensure redundancy in the network topology

b. Access Layer switch

An access switch, also known as an edge switch, is a networking device that serves as a connection point for end-user devices, such as computers, printers, IP phones, and other networked devices, to the local area network (LAN). Its primary function is to provide network access to these devices while also facilitating communication between them and the rest of the network infrastructure [3].



Figure 2.3 Access Switch

Function of access switch

Device Connectivity: The primary function of an access switch is to provide connectivity for end-user devices to the network. It typically includes multiple Ethernet ports (e.g., Fast Ethernet, Gigabit Ethernet) that users can connect their devices to via Ethernet cables.

Port-Based Connectivity: Access switches operate at Layer 2 of the OSI model and use MAC addresses to forward data packets between connected devices within the same network segment. Each port on the switch represents a separate network segment, allowing devices to communicate with each other directly.

VLAN Assignment: Access switches often support VLANs (Virtual Local Area Networks) and can assign devices to different VLANs based on their port configuration or MAC addresses. VLANs help segment network traffic, improve network security, and facilitate network management by logically separating devices into distinct broadcast domains.

Power over Ethernet (PoE): Some access switches feature PoE functionality, allowing them to provide power to PoE-enabled devices such as IP phones, wireless access points, and security cameras over the Ethernet cable. This eliminates the need for separate power adapters and simplifies the deployment of powered devices.

Quality of Service (QoS): Access switches may implement QoS features to prioritize certain types of traffic over others, ensuring optimal performance for latency-sensitive applications such as voice and video communication. QoS mechanisms help manage bandwidth usage and maintain consistent network performance.

3. Firewalls

Firewalls are crucial for ensuring the security of a campus area network. They act as a barrier between the network and potential threats from the internet. Firewalls monitor and control incoming and outgoing network traffic based on predefined security rules. They can prevent unauthorized access, block malicious software, and protect sensitive data.



Figure 2.4 Firewall

Functions of firewall

Packet Filtering: Firewalls inspect data packets as they pass through the network, filtering them based on criteria such as source/destination IP addresses, ports, and protocols.

State full Inspection: Modern firewalls use state full inspection to track the state of active connections and make more intelligent filtering decisions.

Network Address Translation (NAT): Firewalls often include NAT functionality to translate private IP addresses used within a local network to a single public IP address when communicating with external networks

Virtual Private Network (VPN) Support: Many firewalls support VPN technologies to establish secure encrypted tunnels for remote access and site-to-site connectivity.

Intrusion Detection and Prevention (IDS/IPS): Some firewalls incorporate intrusion detection and prevention capabilities to detect and block suspicious or malicious network activity in real-time.

4. Servers

Servers are powerful computers that store and process data for the network. They can serve various purposes, such as hosting websites, managing databases, providing email services, and running applications. Servers are typically located in dedicated server rooms or data centers within the campus area network.



Figure 2.5 Server

5. Wireless LAN Controller

A WLC is a network device used in wireless networking to manage and control multiple wireless access points (APs) within a centralized management system. It serves as a centralized point of control for configuring, managing, and monitoring wireless networks.



Figure 2.6 Wireless LAN Controller

Functions of WLC

Access Point Management: The primary function of a WLC is to manage multiple wireless access points deployed throughout an organization. It provides centralized configuration and management of APs, allowing administrators to deploy, monitor, and troubleshoot wireless networks from a single interface.

Wireless Client Management: A WLC handles the authentication, association, and roaming of wireless clients (devices connecting to the wireless network). It manages client connections, assigns IP addresses, and enforces security policies to ensure secure and efficient communication between wireless clients and the network.

Radio Resource Management (RRM): WLCs perform RRM functions to optimize the performance of wireless networks. This includes dynamically adjusting radio power levels, channel assignments, and load balancing between APs to maximize coverage, minimize interference, and ensure optimal network performance.

Security Policies Enforcement: WLCs enforce security policies to protect the wireless network from unauthorized access and attacks. They support authentication methods such as WPA2-Enterprise, 802.1X/EAP, and captive portal authentication, as well as encryption protocols like WPA2-PSK and AES to secure wireless communications.

Quality of Service (QoS): WLCs support QoS mechanisms to prioritize and manage wireless traffic based on application requirements. They can prioritize critical traffic types such as voice and video over less time-sensitive traffic to ensure optimal performance and quality for real-time applications.

Guest Access Management: WLCs facilitate guest access to the wireless network by providing secure and controlled guest authentication and access policies. They can create separate guest VLANs, enforce captive portal authentication, and apply bandwidth restrictions to guest traffic.

Mobility and Roaming Support: WLCs enable seamless mobility and roaming for wireless clients as they move between different APs within the network. They coordinate the handoff of clients between APs and ensure uninterrupted connectivity and session persistence during roaming events.

6. Wireless Access point

Wireless access points enable wireless connectivity within a campus area network. They allow devices with wireless capabilities, such as laptops, smartphones, and tablets, to connect to the network without the need for physical cables. Wireless access points provide a reliable and convenient means of accessing network resources while on campus.

7. Network Security Appliances

Network security appliances are specifically designed to protect the campus area network from various security threats. These appliances include intrusion detection systems (IDS), intrusion prevention systems (IPS), virtual private network (VPN) gateways, and other advanced security technologies. They monitor network traffic, detect and mitigate potential attacks, and ensure the network's overall integrity.

8. Network Cabling

Network cabling is the physical infrastructure that allows data to be transmitted between devices within the campus area network. Common types of network cables include Ethernet cables, fiber optic cables, and coaxial cables. Properly installed and configured network cabling is crucial for ensuring fast and reliable data transmission within the network.

9. Network Monitoring and Management Tools

Network monitoring and management tools are used to oversee and control network operations within a campus area network. These tools allow network administrators to monitor network performance, identify and resolve issues, manage network devices, and ensure optimal network utilization. Examples of network monitoring and management tools include network analyzers, SNMP monitoring tools, and configuration management systems.

Cisco Packet Tracer

Cisco Packet Tracer 8.2.2 version serves as the primary simulation tool for modeling campus network environments, configuring network devices, and implementing QoS and congestion control mechanisms. Version compatibility and feature availability within Cisco Packet Tracer will be verified to ensure compatibility with the planned project. We used cisco packet tracer 8.2.2 version tool to configure routing protocols, VLANs, QoS policies, and congestion control mechanisms, allowing for hands-on learning and experimentation in network management and optimization.



Figure 2.7 Packet Tracer

Cisco Packet Tracer is a comprehensive, networking technology teaching and learning program that offers a unique combination of realistic simulation and visualization experiences, assessment and activity authoring capabilities, and opportunities for multiuser collaboration and competition.

2.1.2 How Campus Area Network Work Functions

Each building or area within the campus is equipped with network access points, which are connected to the core network infrastructure. These access points allow users in that building or area to connect their devices to the network and access shared resources, such as printers, servers, and internet connectivity. A campus area network also includes a network management system, which is responsible for monitoring and maintaining the network. This system allows network administrators to monitor traffic, track network

performance, and troubleshoot any issues that may arise. In addition to connecting buildings or areas, a campus area network may also provide connectivity to external networks, such as the internet or other corporate networks. This allows users within the campus to access external resources and communicate with users outside of the campus.

Overall, a campus area network works by providing a secure and efficient way for different departments or entities within a campus to communicate and share resources. It connects buildings or areas through a network infrastructure, enables user access through network access points, and is managed and maintained by a network management system.

2.1.3 The Benefits of a Campus Area Network

A Campus Area Network (CAN) offers numerous benefits to organizations and institutions. Here are some of the key advantages.

Enhanced Connectivity: A CAN provides high-speed, reliable connectivity across the entire campus, allowing students, faculty, and staff to access resources and information seamlessly. This ensures smooth communication and collaboration, improving overall productivity and efficiency.

Cost Savings: By consolidating resources into a single network infrastructure, organizations can save on costs related to equipment, maintenance, and support. A well-designed CAN optimizes network performance and reduces the need for multiple standalone networks, resulting in substantial cost savings.

Scalability: As organizations grow and expand, a CAN provides the flexibility to scale the network infrastructure easily and accommodate increasing user demands. This scalability ensures that the network can adapt to future requirements without disrupting operations or compromising performance.

Centralized Management: With a CAN, network administrators have centralized control, making it easier to monitor and manage network devices, security protocols, and user access. This centralized management streamlines troubleshooting, reduces the risk of security breaches, and simplifies network administration tasks.

Improved Security: A CAN allows for the implementation of robust security measures, including firewalls, intrusion detection systems, and access controls. This enhances the protection of sensitive data, ensuring confidentiality, integrity, and availability throughout the entire campus network.

Enhanced Learning and Collaboration: With a reliable and high-speed network, students and educators can leverage various digital tools and resources, enabling interactive learning experiences. CAN also fosters collaboration by facilitating easy communication and file sharing, enabling teamwork and knowledge exchange.

Overall, a well-designed Campus Area Network offers organizations and institutions the benefits of enhanced connectivity, cost savings, scalability, centralized management, improved security, and enhanced learning and collaboration opportunities.

2.2 Network Performance

In the realm of technology, network performance plays a crucial role in enhancing communication and data exchange amongst interconnected devices within an organization or even across the globe. Its primary purpose is to optimize and improve the efficiency of networks, thereby ensuring the smooth flow of information and mitigating potential hindrances that may arise due to faulty systems or congested bandwidths. Network performance monitoring and management tools help administrators to analyze, troubleshoot, and optimize network performance, ensuring continuous improvements, quick response to issues, and increased overall network stability.

2.2.1 Key metrics used to measure Network Performance

Key metrics used to measure Network Performance are throughput, latency, jitter, and packet loss.

Bandwidth: The term bandwidth defines the transmission capacity of an electronic line. Theoretically, it describes the range of possible transmission rates, or frequencies. In practice, it describes the size of the pipe that an application program needs in order to communicate over the network. The significance of a channel bandwidth is that it

determines the channel capacity, which is the maximum information rate that can be transmitted [4].

Throughput: Throughput is the number of messages successfully delivered per unit time. Throughput is controlled by available bandwidth, as well as the available signal-to-noise ratio and hardware limitations. Throughput is usually measured in bits per second (bit/s, sometimes abbreviated bps), and sometimes in data packets per second (p/s or pps) or data packets per time slot.

Latency: Network latency is the delay in network communication. It shows the time that data takes to transfer across the network. Networks with a longer delay or lag have high latency, while those with fast response times have low latency.

Jitter: jitter is a variance in latency, or the time delay between when a signal is transmitted and when it is received. This variance is measured in milliseconds (ms) and is described as the disruption in the normal sequence of sending data packets.

Packet Loss: Packet loss is another important QoS performance measure. Some applications may not function properly, or may not function at all, if the packet loss exceeded a specified number, or rate. For example, when streaming video frames, after certain number of lost frames, the video streaming may become useless. This number may be zero in certain cases [5].

2.2.2 Quality of service

Quality of service is particularly important for the transport of traffic with special requirements. In particular, developers have introduced Voice over IP technology to allow computer networks to become as useful as telephone networks for audio conversations, as well as supporting new applications with even stricter network performance requirements. The network Quality of Service (QoS) is the capability to control traffic-handling mechanisms in the network such that the network meets the service needs of certain applications and users subject to network policies. The notion of QoS came up as a response to the new demands imposed on the network performance by modern applications, especially multimedia real-time applications [6].

2.2.3 Network Congestion and Control Mechanism

Network Congestion occurs when the traffic flowing through a network exceeds its maximum capacity. In most cases, congestion is a temporary issue with the network caused due to a sudden upsurge of traffic, however, sometimes, a network is continually congested, indicating a deeper problem. End-users perceive network congestion as Network Slowdown or a very large delay in processing requests

Congestion control mechanism is called end-to-end flow control. In order for a host to be able to detect congestion, the routers must be able to provide the information that the network is currently (or is about to become) overloaded; this mechanism is called feedback. Flow control and feedback are conceptually related, so they are often referred to as feedback flow control [7].

2.2.4 The trade-off between congestion control and Quality of Service

The trade-off between congestion control and Quality of Service (QoS) in computer networks is a complex balancing act. Congestion control mechanisms aim to prevent network congestion by controlling the amount of data sent into the network, while QoS is concerned with ensuring reliable service delivery according to various metrics such as latency, jitter, and packet loss.

Congestion control operates by adjusting the rate at which hosts send data, often in response to network conditions. For example, TCP uses congestion control algorithms that increase data transmission rates until packet loss occurs, indicating congestion, and then decrease the rates accordingly. This reactive approach can lead to a temporary decrease in QoS due to increased latency or packet loss during periods of congestion.

On the other hand, QoS mechanisms prioritize traffic to provide better service to certain data flows. This is crucial for real-time applications like voice and video, which require timely and predictable data delivery. Implementing QoS often involves classifying traffic and providing different levels of service, potentially reserving bandwidth or applying priority queuing for high priority traffic.

The trade-off arises because aggressive congestion control can lead to underutilization of network resources, reducing throughput, which is a key component of QoS. Conversely, prioritizing QoS without adequate congestion control can lead to network instability and widespread packet loss, ultimately degrading the service quality for all users.

The trade-off between congestion control and QoS is about finding the right balance between efficiently utilizing network resources to maximize throughput while ensuring that the network can deliver data flows with the required service quality, especially for real-time applications. Effective network management requires a combination of both congestion control and QoS mechanisms to adapt to varying network conditions and application requirements.

2.3 Related Work

QoS Policies to Improve Performance in Academic Campus and SDN Networks given the evolution of technology and the growing demand for resources from users of campus networks that affect network performance, a solution based on SDN is proposed; a technology that differs from the paradigm of traditional networks that centers the administration of the network in a controller. With this new approach, the traffic in campus networks, its behavior, and the main treatment of QoS policies in conventional networks is studied; besides a model to define QoS policies in SDN and conventional networks is designed.

Performance is evaluated in three physical scenarios based on latency, jitter and bandwidth, taking an important step to introduce SDN networks in real environment. The D-TIG traffic generator is used for testing. The T-Student statistical method is applied for the analysis of the data [8].

Congestion is a major cause of energy wastage and Quality of Service (QoS) degradation in wireless communication systems. Saving energy and maintaining high QoS levels are especially important in Wireless Multimedia Sensor Networks (WMSN), due to the limited sensor node energy resources and QoS-related application requirements. This paper proposes an energy efficient and QoS-aware congestion control scheme for reliable communications over WMSNs (eqCC). The proposed solution makes use of QoS feedback and current battery energy levels of sensor nodes in order to adapt sending data rate. We employ reinforcement learning by formulating the problem in terms of a Markov Decision Process (MDP) and solve it using the Q-Learning technique. The proposed eqCC is validated using simulations and is compared with classic TCP and Flush, another congestion control algorithm for Wireless Sensor Networks (WSN). The results show how eqCC outperforms the other solutions under high and low network load [9].

Quality of service (QoS) is the set of techniques designed to manage network resources. QoS refers to the capability of a network to provide better service to selected network traffic over various LAN and WAN technologies. The primary goal of QoS is to provide flow priority, including dedicated bandwidth, controlled jitter and latency (required by

some interactive and delay-sensitive traffic), and improved loss characteristics. While QoS has become an essential technology for those organizations rolling out a new generation of network applications such as real-time voice communications and high-quality video delivery, most of the literature available on this foundation technology for current and future business applications focuses on IP QoS. Equally important is the application of QoS in the campus LAN environment, which is primarily responsible for delivering traffic to the desktop [3].

Myths about congestion control are examined, and an explanation of why the trend toward cheaper memory, higher-speed links, and higher-speed processors has intensified the need to solve the congestion problem is provided. A number of proposed solutions are described, and a classification of congestion problems as well as their solutions is presented. The reasons why the problem is so difficult are identified, and the protocol design decisions that affect the design of a congestion control scheme are discussed [10].

The study focuses on Enhancing Network Performance and Quality of Service (QoS) in a Wired Local Area Network (LAN). In today's interconnected landscape, the optimization of Local Area Networks (LANs) stands as a pivotal pursuit. The study aims to evaluate and discern the factors that significantly influence network performance and QoS utilizing the Optimized Network Engineering Tool (OPNET) Modeler. The key objectives are to design a network design that gives the best network performance and QoS; to evaluate link connections, connectivity, and effect on network performance, and to recommend and implement the best network designs, link connections, and connectivity that yield the best network performance and QoS. OPNET simulation software tool has been used to simulate the network design scenarios. The results highlighted the impact of link capacity on network performance, revealing that higher capacities led to lower HTTP response times. Conversely, lower capacity links struggled with simultaneous traffic, resulting in delayed responses [11].

Access Control List (ACL) is a set of commands grouped together to filter the traffic that enters and leaves the interface. The ACL commands allow the administrator to deny or permit traffic that enters the interface. ACL also performs other tasks such as restricting telnet, filtering routing information and prioritizing WAN traffic with queuing. A wildcard

mask allow to match the range of address in the ACL statements. A router makes two references to ACL such as numbered and named. These references support two types of filtering such as standard and extended. In this paper we have analyzed and simulated the network using Standard ACL and Extended ACL. The configuration is done using Cisco packet tracer [12].

Networks are encountering packet loss, high- frequency blockage, delays, and unnecessary retransmission of data with the increasing strain on the growth of digital infrastructure accompanied by millions of users. Nowadays, almost all real-time applications seek high-speed data transmission that contributes to making the networks more saturated and unresponsive. Such demands result in degradable data transmission, giving rise to congestion. To maintain a sustainable network with efficient performance, several mechanisms need to be taken into consideration to prevent networks from being congested. Congestion control plays an indispensable role to lengthen the lifetime of the network and improve its performance [13].

The issue of congestion can arise in any networked system and is a situation in which there is steep performance degradation due to the presence of a large number of packets in the subnet, which is beyond the handling capacity of the network. Congestion control is the mechanism of mitigating congestion and assuring the network resources like CPU time, buffer space, and bandwidth are optimally utilized maximizing the throughput. Its objective is to ensure that the system keeps on running to its capacity even with the worst scenarios of overloaded traffic.² Two major approaches to deal with the issue of congestion as per the control theory is closed-loop congestion control, which tries to alleviate congestion after it happens, and another one is open-loop congestion control, which is about preventive measures taken before congestion happens [14].

The advantage of using the research proposal title Enhancing Network Performance: QoS and Congestion Control in Campus Networks by Using Cisco Packet Tracer lies in its precise and focused articulation of the research objective, methodology, and tools employed. By explicitly stating the goal of enhancing network performance through the implementation of Quality of Service (QoS) and congestion control mechanisms within campus networks, the title effectively communicates the research's core focus to both

academic and industry audiences. Additionally, the inclusion of Cisco Packet Tracer in the title provides specificity regarding the technological platform utilized for experimentation and analysis, offering clarity on the tools and methodologies employed in the study. This clarity enhances the proposal's appeal to stakeholders interested in network optimization, network administrators seeking practical solutions, and researchers aiming to contribute to the advancement of network engineering. Furthermore, the title's succinctness facilitates easy comprehension and immediate recognition of the research's domain and objectives, potentially increasing its visibility and relevance within the academic and professional communities.

2.4 Existing Solutions and Limitations

Historically, network administrators have employed a spectrum of solutions to address QoS and congestion control challenges within campus networks. These solutions encompass traffic shaping techniques, such as prioritization and traffic policing, as well as congestion avoidance mechanisms, including Random Early Detection (RED) and Explicit Congestion Notification (ECN). While these approaches have demonstrated efficacy in certain scenarios, they often entail trade-offs between resource utilization, fairness, and scalability, thereby warranting further exploration and refinement.

By decoupling control plane functionalities from underlying hardware infrastructure and facilitating programmable network management, SDN and NFV offer the promise of dynamic QoS provisioning and adaptive congestion control mechanisms tailored to the evolving demands of diverse stakeholders.

2.5 Emerging Challenges

However, the burgeoning requirements imposed by modern digital workflows have introduced a plethora of challenges for network administrators and stakeholders. One of the foremost challenges pertains to ensuring consistent Quality of Service (QoS) across heterogeneous traffic types traversing the network infrastructure. The coexistence of delay-sensitive applications such as voice and video streaming alongside latency-tolerant data transfers necessitates the implementation of QoS mechanisms to prioritize and allocate network resources judiciously.

Moreover, congestion emerges as a recurrent bottleneck that can impede the flow of data, degrade network performance, and undermine user experience within campus environments. The inherent variability in traffic patterns, coupled with the finite capacity of network links and devices, exacerbates the risk of congestion occurrences, thereby necessitating proactive congestion control strategies to mitigate adverse effects and maintain optimal throughput.











CHAPTER THREE

METHODOLOGY

3.1 Materials and tools

3.1.1 Materials

Table 3.1 Equipment List

Designing Materials	image	type	Quantity
Routers		ISR4331	1
Firewalls		5506-X ASA	1
Core and Distribution switches		3650-24PS	2
Access switches		2960-24TT	25
Servers		Server-PT	6
Access points			
Printers		Printer-PT	23
WLC		WLC-PT	23
PC		PC-PT	46
Laptops		Laptop-PT	23
Smartphones		SMARTPHONE-PT	23
Cables and RJ-45	-	Straight through and cross over cable	-

a. Router

A router is a networking device that connects multiple networks together and routes data packets between them. It operates at Layer 3 (the network layer) of the OSI model and performs the function of packet forwarding based on IP addresses [15].

b. Firewall

A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between a trusted internal network and untrusted external networks, such as the Internet, to prevent unauthorized access and protect against malicious threat.

c. Core Switch

A core switch is a high-capacity switch generally positioned within the backbone or physical core of a network. Core switches serve as the gateway to a wide area network (WAN) or the Internet they provide the final aggregation point for the network and allow multiple aggregation modules to work together [2].

d. Distribution switch

A distribution switch is a networking device that serves as an intermediary between access switches and core switches in a hierarchical network architecture. It plays a crucial role in connecting end-user devices, such as computers, printers, and IP phones, to the network infrastructure, while also providing aggregation and distribution of network traffic [2].

e. Access switch

An access switch, also known as an edge switch, is a networking device that serves as a connection point for end-user devices, such as computers, printers, IP phones, and other networked devices, to the local area network (LAN). Its primary function is to provide network access to these devices while also facilitating communication between them and the rest of the network infrastructure [3].

f. Wireless LAN Controller

A WLC is a network device used in wireless networking to manage and control multiple wireless access points (APs) within a centralized management system. It serves as a centralized point of control for configuring, managing, and monitoring wireless networks.

g. End devices

End systems, also known as end devices or edge devices, are the various types of equipment that users directly interact with on a network. They can be sources or destinations in a networked system. These devices are desktops, laptops, smartphones, server and etc.

h. Cables

Cables are used to establish physical connections between network devices, enabling data transmission and communication within a network.

- ✓ A straight-through cable is a type of twisted pair cable that is used in local area networks to connect a computer to a network hub such as a router.
- ✓ An Ethernet crossover cable is a type of Ethernet cable used to connect computing devices together directly

3.1.2 Designing tool

Cisco Packet Tracer

Cisco Packet Tracer serves as the primary simulation tool for modeling campus network environments, configuring network devices, and implementing QoS and congestion control mechanisms. Version compatibility and feature availability within Cisco Packet Tracer will be verified to ensure compatibility with the planned project. We used cisco packet tracer 8.2.2 version tool to configure routing protocols, VLANs, QoS policies, and congestion control mechanisms, allowing for hands-on learning and experimentation in network management and optimization.

Here's a is some key aspects of Cisco Packet Tracer

- Simulation Environment
- Device Support
- Protocols and Technologies
- Visual Interface

- Learning Tool
- Assessment Capabilities

3.2 Campus Network Topology Design

A campus network is generally the portion of the network infrastructure that provides access to network communication services and resources to end users and devices that spread over a single geographic location. It might be a single floor, a building, or even a group of buildings spread over an extended geographic area. The steps to design the topology of Campus area network for our project as a follows.

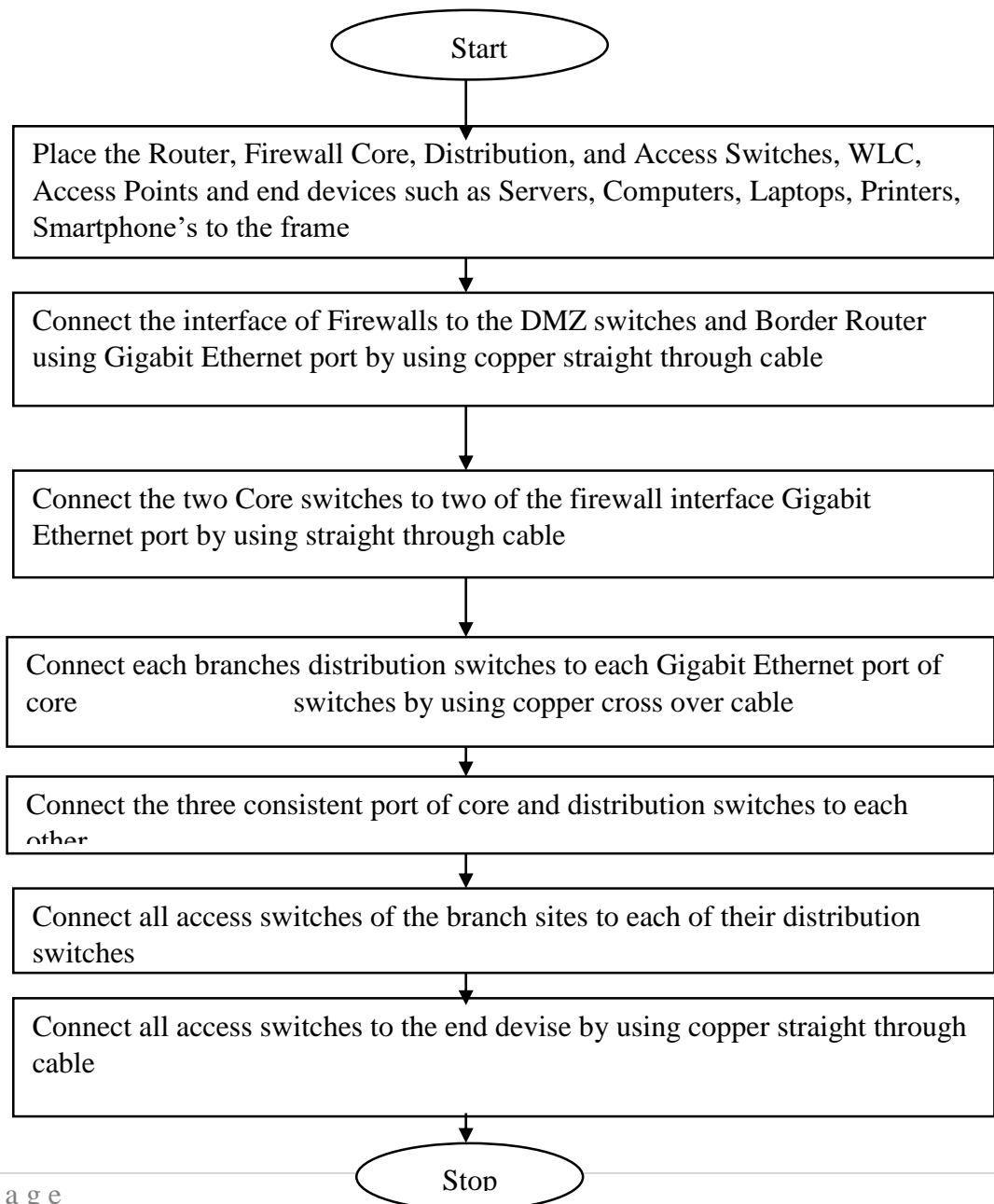


Figure 3.1 Design Steps

3.2.1 Hierarchical network design model

Hierarchical network design model breaks the complex problem of network design into smaller and more manageable. Each level in the hierarchy is focused on specific set of roles. This helps the network designer and architect to optimize and select the right network hardware, software and features to perform specific roles for that network layer

A typical enterprise hierarchical campus network design includes the following three layers:

- The Access layer that provides workgroup/user access to the network
- The Core layer that provides optimal transport between sites and high performance routing
- The Distribution layer that provides policy-based connectivity and control boundary between the access and core layers

a. Access layer design

An access layer is the part of a network infrastructure that connects end devices, such as computers, printers, and IP phones, to the network. The design of the access layer is crucial as it directly impacts the performance, security, and manageability of the network.

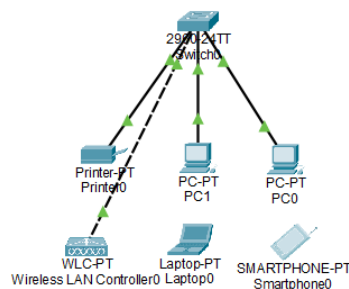


Figure 3.2 Access-Layer

b. Core Layer Design

The core layer serves as the central conduit, facilitating high-speed data transmission between various segments of the network. Its primary objective is to ensure rapid packet forwarding with minimal latency, catering to the substantial volume of traffic traversing

the network. Typically, the core layer employs advanced networking devices like routers and switches optimized for swift data processing. It prioritizes throughput over complex processing tasks and implements redundancy measures to bolster fault tolerance and maintain uninterrupted connectivity.

a. Distribution Layer Design

The distribution layer acts as an intermediary between the core and access layers, consolidating and distributing traffic to and from access layer devices such as switches and end-user terminals. It undertakes essential routing, filtering, and policy enforcement functions, segmenting the network into manageable broadcast domains while enforcing security measures like VLANs and access control lists. The distribution layer augments network efficiency by orchestrating traffic flow and prioritization, contributing to a robust, scalable, and secure networking infrastructure. Together, these layers harmonize to optimize network performance, reliability, and manageability in complex network environments.

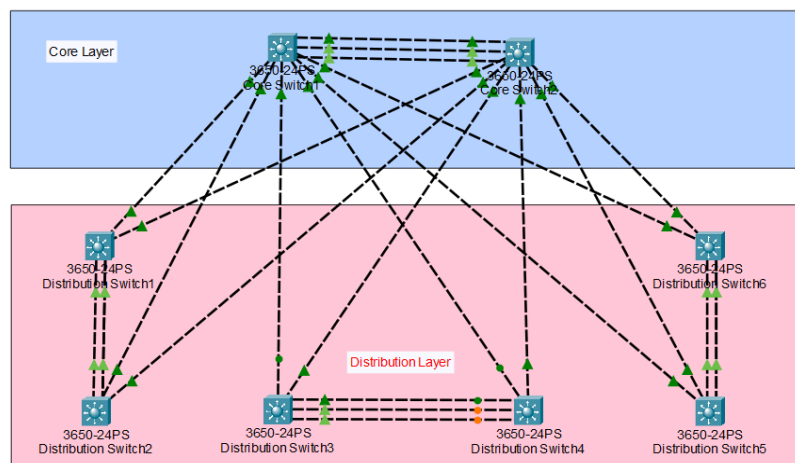


Figure 3.3 Core and Distribution Layer

b. Demilitarized zone, Internal and External network Design

DMZ

The DMZ is a network segment that sits between the internal network and the external network. The primary purpose of the DMZ is to host services and resources that need to be accessible from the internet while protecting the internal network from direct exposure to

external threats. The purpose of a DMZ is to add an additional layer of security to the network by segregating and isolating certain services and systems that need to be accessed from the internet, such as web servers, email servers, DHCP servers, FTP servers or DNS servers.

Internal Networks

Internal network refers to the interconnected computers, and devices within a campus. It is typically protected by various security measures such as firewalls, access controls, and encryption mechanisms. The internal network is where sensitive data, applications, and resources are stored and accessed by authorized users. It's considered a trusted environment because access to the internal network is usually restricted to employees or authorized personnel.

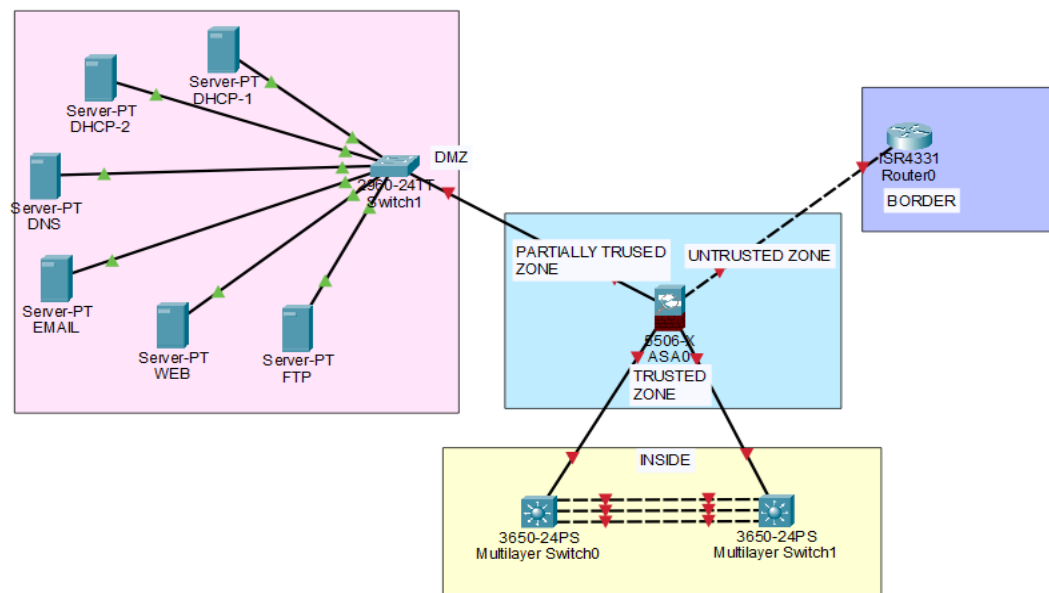


Figure 3.4 Internal Network

External Network

The external network refers to any network outside of the campus's internal network. This includes the broader internet, as well as other external networks such as those belonging to partner organizations or third-party service providers. The external network is considered untrusted because it is beyond the direct control of the organization, and it may contain potential security threats such as hackers, malware, and malicious actors. Access to the

external network is typically unrestricted and available to anyone with an internet connection.

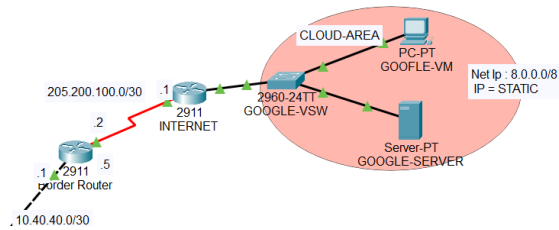


Figure 3.5 External Network

The overall combined hierarchically and geographically designed campus area network of the above is given as following figure.

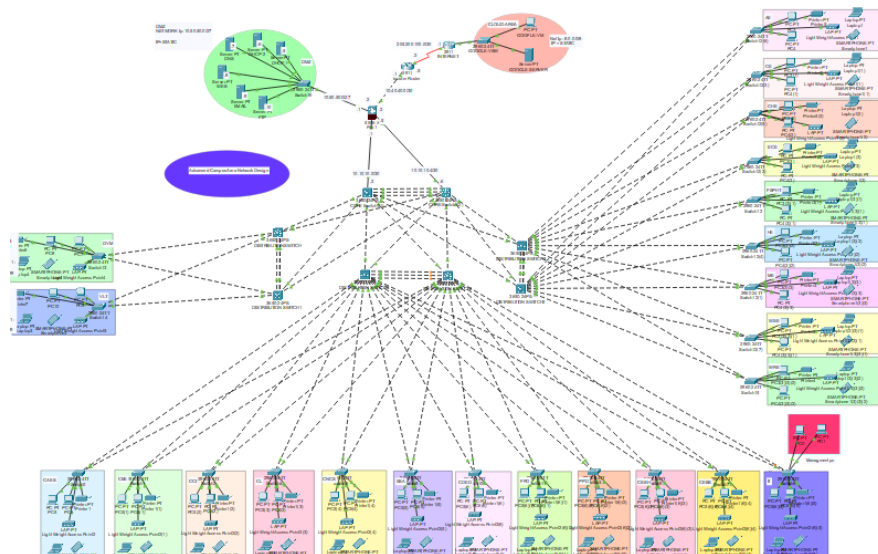


Figure 3.6 Topological view of Campus Area Network

3.3 Implementation

3.3.1 Basic configuration

Setting up basic configurations on networking devices involves several steps. Here's a simplified steps:

Step 1: Initial Configuration

- ✓ Assign a unique hostname to each device.
- ✓ Configure IP addresses for management interfaces.

- ✓ Set up basic parameters such as domain name, time settings, and console and VTY line passwords for administrative access.

Step 2: SSH Configuration

- ✓ Generate RSA/DSA keys for SSH encryption.
- ✓ Enable SSH server and specify version (SSHv2 recommended for security).
- ✓ Configure domain name and authentication parameters (local or external AAA server).
- ✓ Set up SSH version 2 for enhanced security.
- ✓ Specify the SSH timeout interval for idle sessions.

Step 3: Standard ACL for SSH

- ✓ Create an access control list (ACL) specifically for SSH traffic.
- ✓ Define the ACL permitting SSH traffic from trusted management hosts.
- ✓ Apply the ACL inbound on the VTY lines to restrict SSH access.

3.3.2 STP port-fast and BPDU guard configuration on all access ports

Implementing STP Port-Fast and BPDU Guard configurations on all access ports enhances network stability and security. Port-Fast allows access ports to transition directly from blocking to forwarding state, reducing network convergence time, especially when connecting end devices. Meanwhile, BPDU Guard provides an extra layer of protection by shutting down ports that receive Bridge Protocol Data Units (BPDUs), indicating the presence of unauthorized switches or misconfigurations. By configuring both features on access ports, network administrators ensure faster network convergence and mitigate the risks associated with unauthorized devices attempting to disrupt the network.

Throughout the network infrastructure, STP Port-Fast and BPDU Guard were configured on all access ports. This configuration streamlined the transition of access ports to the forwarding state, minimizing network convergence time and providing efficient connectivity for end devices. Additionally, BPDU Guard was enabled to promptly identify and disable ports receiving unexpected BPDUs, mitigating the potential risks posed by rogue switches or misconfigured devices. Together, these measures optimized network

performance, enhanced stability, and fortified network security against unauthorized access and disruptions.

Configuring STP Port-Fast and BPDU Guard on all access ports involves several steps to ensure network stability and security.

Step 1: Identify Access Ports

- ✓ Determine which ports connect to end devices such as computers, printers, or IP phones.
- ✓ These ports are typically configured as access ports in VLANs and don't participate in STP forwarding loops.

Step 2: Enable Port-Fast

Access ports are configured with Port-Fast to allow them to transition directly from blocking to forwarding state, bypassing the normal STP convergence process. This is crucial for access ports as they shouldn't be part of the STP topology changes since they connect directly to end devices. Port-Fast can be enabled globally for all access ports or individually on each port.

Step 3: Implement BPDU Guard

BPDU Guard is configured to protect against Layer 2 loops caused by unauthorized switches or misconfigured ports. When enabled on access ports, BPDU Guard monitors for incoming BPDUs. If a BPDU is detected on an access port, BPDU Guard shuts down the port to prevent potential network disruptions. BPDU Guard can be enabled globally for all access ports or individually on each port.

Step 4: Verification

After configuring Port-Fast and BPDU Guard, we verify the settings to ensure they have been applied correctly. Use show commands (e.g., show spanning-tree interface <interface-

id>) to check the Port-Fast and BPDU Guard status on each interface. Monitor the device logs for any BPDU Guard actions, such as port shutdowns triggered by unexpected BPDUs.

Step 5: Testing

Perform testing to confirm that Port-Fast and BPDU Guard configurations are functioning as intended. Test connectivity on access ports to verify that devices can establish network connections without delays caused by STP convergence.

Simulate scenarios where unauthorized devices attempt to connect to access ports to ensure that BPDU Guard triggers the appropriate actions to protect the network.

By following these steps, network administrators can effectively configure STP Port-Fast and BPDU Guard on all access ports, optimizing network performance while safeguarding against potential security threats.

3.3.3 Ether-channel or Link aggregation configuration

Ether-Channel, also known as Link Aggregation or Port Channel, was configured on switches to optimize network performance and enhance redundancy. By bundling multiple physical links into a single logical interface, Ether-Channel allowed for increased bandwidth and improved fault tolerance between switches. This aggregation of links provided higher throughput, reduced congestion, and enhanced load balancing across the network. The configuration process involved several steps

Step 1: Identifying Member Interfaces

Network administrators selected the physical interfaces to be grouped together into the Ether-Channel.

Step 2: Configuring Ether-Channel Interface

They created a logical Ether-Channel interface and assigned it a unique identifier (channel-group number) and a port-channel interface name.

Step 3: Selecting Ether-Channel Mode

We choose the appropriate Ether-Channel mode based on the network requirements.

Common modes included:

"On" mode: All configured member interfaces formed the Ether-Channel immediately.

"Desirable/Auto" mode: Used for negotiating Ether-Channel membership with the neighboring switch.

"Active/Passive" mode: Similar to Desirable/Auto, but with one side actively negotiating and the other passively waiting for negotiation.

Step 4: Applying Configuration to Member Interfaces

They applied the Ether-Channel configuration to the selected member interfaces.

This involved assigning them to the corresponding Ether-Channel interface and ensuring consistency in settings such as speed, duplex, and VLAN membership.

Step 5: Verification and Testing

After configuring Ether-Channel, administrators verified its status and functionality. They used commands like show Ether-channel summary to check the status of the Ether-Channel bundle and member interfaces. Testing involved validating load balancing across member links and verifying failover behavior in case of link failures. Once configured, Ether-Channel provided several benefits to the network, including increased aggregate bandwidth, improved fault tolerance, and enhanced scalability. It optimized switch-to-switch and switch-to-router connections, ensuring efficient data transmission across the network infrastructure.

3.3.4 Sub-netting and ip addressing

Sub-netting and IP addressing are fundamental concepts in computer networking, crucial for effectively managing and organizing IP networks.

Sub-netting involves dividing a large IP network into smaller, more manageable sub-networks, known as subnets, while IP addressing involves assigning unique IP addresses to devices within those subnets. Here's an overview of both concepts:

a. Sub-netting

Sub-netting is the process of breaking down a larger network into smaller, more efficient sub-networks, known as subnets. It helps in organizing and managing network resources more effectively, improving performance and security. Sub-netting is typically done based on network requirements, such as the number of devices per subnet, geographical locations, or security considerations. It allows for better utilization of IP addresses and reduces the broadcast domain size, minimizing network congestion and improving network performance.

Sub-netting is achieved by borrowing bits from the host portion of the IP address and using them to create subnet addresses.

b. IP Addressing

IP addressing involves assigning unique IP addresses to devices connected to a network, enabling them to communicate with each other.

An IP address consists of two parts, the network portion and the host portion. The network portion identifies the network to which the device belongs, while the host portion identifies the specific device within that network.

IP addresses can be assigned statically (manually) or dynamically (using DHCP - Dynamic Host Configuration Protocol). IPv4 addresses are 32 bits long and are typically expressed in dotted-decimal notation.

IP addresses are assigned based on the sub-netting scheme used, ensuring that each device has a unique address within its subnet. Subnet masks are used to determine the network portion and host portion of an IP address. They are represented in dotted-decimal notation.

Network devices are configured by using the following ip addresses.

Wireless local area network: 10.60.0.0/16. This ip address has 65,536 valid addresses.

1. Network address: 10.60.0.0/16.
2. Default gateway address: 10.60.0.1/16.
3. Broadcast address: 10.60.255.255/16.
4. Host address: 10.60.0.2/16 to 10.60.255.254/16.

For all LAN users 192.168.0.0/17 is used. This ip address has 32,768 valid ip addresses. To minimize broadcast domains, we divided this network into 32 sub-nets.

Table 3.2 Ip address

No	Network address	Broadcast address	Host addresses	Vlan Id	Default gateway
1	192.168.0.0	192.168.3.255	192.168.0.2 to 192.168.3.254	5	192.168.0.1
2	192.168.4.0	192.168.7.255	192.168.4.1 to 192.168.7.254	10	192.168.4.1
3	192.168.8.0	192.168.11.255	192.168.8.2 to 192.168.11.254	15	192.168.8.1
4	192.168.12.0	192.168.15.255	192.168.12.2 to 192.168.15.254	20	192.168.12.1
5	192.168.16.0	192.168.19.255	192.168.16.2 to 192.168.19.254	25	192.168.16.1
6	192.168.20.0	192.168.23.254	192.168.20.2 to 192.168.23.254	30	192.168.20.1
7	192.168.24.0	192.168.27.255	192.168.24.2 to 192.168.27.254	35	192.168.24.1
8	192.168.28.0	192.168.31.255	192.168.28.2 to 192.168.31.254	40	192.168.28.1
9	192.168.32.0	192.168.35.255	192.168.32.2 to 192.168.35.254	45	192.168.32.1
10	192.168.36.0	92.168.39.254	92.168.36.2 to	50	92.168.36.1

			92.168.39.254		
11	192.168.40.0	192.168.43.255	192.168.40.2 to 192.168.43.254	55	192.168.40.1
12	192.168.44.0	192.168.47.255	192.168.44.2 to 192.168.47.254	60	192.168.44.1
13	192.168.48.0	192.168.51.255	192.168.48.2 to 192.168.51.254	65	192.168.48.1
14	192.168.52.0	192.168.55.255	192.168.52.2 to 192.168.55.254	70	192.168.52.1
15	192.168.56.0	192.168.59.255	192.168.56.2 to 192.168.59.254	75	192.168.56.1
16	192.168.60.0	192.168.63.255	192.168.60.2 to 192.168.63.254	80	192.168.60.1
17	192.168.64.0	192.168.67.255	192.168.64.2 to 192.168.67.254	85	192.168.64.1
18	192.168.68.0	192.168.71.255	192.168.68.2 to 192.168.71.254	90	192.168.68.1
19	192.168.72.0	192.168.75.255	192.168.72.2 to 192.168.75.255	95	192.168.72.1 /22
20	192.168.76.0	192.168.79.255	192.168.76.2 to 192.168.79.254	100	192.168.76.1
21	192.168.80.0	192.168.83.255	192.168.80.2 to 192.168.83.254	105	192.168.80.1
22	192.168.84.0	192.168.87.255	192.168.84.2 to 192.168.87.254	110	192.168.84.1
23	192.168.88.0	192.168.91.255	192.168.88.2 to 192.168.91.254	115	192.168.88.1
24	192.168.92.0	192.168.95.255	192.168.92.2 to 192.168.95.254		192.168.92.1

Management VLAN network ip address: 172.16.10.0/24. This ip address has 256 valid addresses.

1. Default gateway: 172.16.10.1/24
2. Broadcast address: 172.16.10.255/24.
3. For user: from 172.16.10.2/24 to 172.16.10.254/24

Demilitarized network address: 10.50.50.0/27. We have 32 valid ip addresses.

1. Default ip address: 10.50.50.1/27
2. Usable ip addresses: from 10.50.50.2/27 to 10.50.50.32/27.

3.3.5 Creating VLAN on Access, Distributions, and Core switches

Step 1 Access Switch: Creates VLANs for device segregation, typically used for connecting end devices; no routing functions performed. It primarily connect end devices such as computers, printers, and IP phones. VLANs are typically assigned to access ports where end devices connect.

Step 2 Distribution Switch: Aggregates traffic from access switches, creates VLANs, and often performs inter-VLAN routing functions. It aggregate traffic from access switches and often perform routing functions. It may have Layer 3 interfaces (SVIs) configured for each VLAN to perform inter-VLAN routing.

Step 3 Core Switch: Acts as the backbone of the network, creates VLANs, assigns IP addresses as default gateways for each VLAN, and facilitates high-speed connectivity between distribution switches. It typically serve as the backbone of the network, providing high-speed connectivity between distribution switches and to the rest of the network.

3.3.6 Configuring Static ip address

1. DMZ/server farm devices

Assigning static IP addresses to DMZ (Demilitarized Zone) or server farm devices is essential for several reasons.

Continuous Accessibility: Devices in the DMZ or server farm, such as web servers or email servers, need to maintain constant accessibility from both internal and external networks. Static IP addressing ensures that these critical services are always reachable at a known address, enabling seamless communication with client's and users.

Predictable Network Configurations: Static IP addresses provide network administrators with a predictable and stable network infrastructure. Unlike dynamic IP addressing, where addresses may change over time, static IPs remain constant, simplifying network management tasks such as configuration, monitoring, and troubleshooting.

Enhanced Security: Static IP addressing helps bolster network security by reducing the risk of unauthorized access or network disruptions. With static IPs, administrators have greater control over which devices are allowed to communicate with each other, reducing the likelihood of unauthorized devices gaining access to sensitive resources in the DMZ or server farm.

Avoidance of IP Address Conflicts: By assigning static IP addresses, the risk of IP address conflicts is minimized. Conflicting IP addresses can cause network disruptions and downtime, especially in environments with critical services like those found in a DMZ or server farm. Static IPs ensure that each device has a unique address, preventing conflicts and maintaining network stability.

Assigning static IP addresses to DMZ or server farm devices ensures continuous accessibility, simplifies network management, enhances security, and mitigates the risk of IP address conflicts, making it a fundamental practice in network administration.

Firewall interfaces, router interfaces, and SVIs

Configuring static IP addresses for firewall interfaces, router interfaces, and virtual interfaces of switches is crucial for network stability, security, and ease of management. Assigning static IP addresses to firewall interfaces ensures consistent access control rules and allows for easier management of firewall configurations. Static IPs enable predictable firewall policies, ensuring that specific services or applications are allowed or denied based on predefined rules.

Static IP addressing for router interfaces ensures consistent routing behavior and predictable network paths. Configuring static IP addresses for SVIs ensures stable communication between VLANs and maintains consistent network segmentation. Static IPs on SVIs simplify network troubleshooting and management tasks, as they provide a fixed reference point for monitoring and configuration purposes.

3.3.7 HSRP configuration and Assigning Ip DHCP helper Address

HSRP

Hot Standby Router Protocol (HSRP) is a protocol used to provide high availability and failover for IP networks. It allows two or more routers to work together in a group, with one router acting as the active router and the others as standby routers. The active router forwards packets for the virtual IP address associated with the HSRP group, while the standby routers monitor the health of the active router and take over its role if it fails.

Key aspects of HSRP include:-

Step 1: Virtual IP Address (VIP)

- ✓ Each HSRP group is associated with a virtual IP address.
- ✓ This virtual IP address serves as the default gateway for hosts on the subnet.

Step 2: Active and Standby Routers

- ✓ Within an HSRP group, one router is elected as the active Router, and the others are in standby mode.
- ✓ The active router forwards traffic for the virtual IP address. If the active router fails, a standby router takes over and becomes the new active router.

Step 3: Hello Messages

- ✓ Routers in an HSRP group exchange hello messages to monitor each other's status.
- ✓ Hello messages are used to detect router failures and determine the active and standby routers.

Step 4: Preemption

- ✓ Preemption is the ability of a standby router with a higher priority to take over the active role if it becomes available.
- ✓ Without preemption, the active role remains with the current active router even if a standby router with a higher priority comes online.

Step 5: Priority

Each router in an HSRP group is assigned a priority value. The router with the highest priority becomes the active router. Priority values can be manually configured, allowing administrators to control the election process.

HSRP provides redundancy and fault tolerance for networks by ensuring continuous availability of the default gateway. It is commonly used in environments where network uptime is critical, such as enterprise networks, data centers, and service provider networks.

IP DHCP helper address

When DHCP clients are located in different subnets or VLANs from the DHCP server, DHCP broadcast messages cannot be forwarded by routers by default. As a result, DHCP requests from clients in remote subnets or VLANs cannot reach the DHCP server.

The "IP DHCP helper address" command solves this problem by instructing the router to forward DHCP broadcast messages received on a specified interface to a designated DHCP server. This command is typically configured on the Layer 3 interface (SVI - Switched Virtual Interface) of the router that is the default gateway for the DHCP clients. Here's how the command works.

DHCP Client Broadcasts: When a DHCP client broadcasts a DHCP Discover message to obtain an IP address, subnet mask, default gateway, DNS server, etc., it sends the broadcast to the local subnet's broadcast address.

Router Receives Broadcast: The router interface configured with the "IP DHCP helper address" command receives the DHCP broadcast message from the client.

DHCP Helper Address Forwarding: The router, upon receiving the DHCP broadcast, forwards it as a unicast packet to the IP address specified in the "IP DHCP helper address" command.

DHCP Server Response: The DHCP server receives the DHCP request from the router and responds with DHCP Offer, DHCP Acknowledgment, and other DHCP messages to assign the IP address and other network configuration parameters to the client.

By configuring the "IP DHCP helper address" command on a router interface, DHCP clients in remote subnets or VLANs can obtain IP address assignments from a DHCP server located elsewhere in the network. Assigning an IP DHCP helper address when configuring HSRP ensures that DHCP clients can successfully obtain IP address assignments from DHCP servers located in different subnets or VLANs, enhancing the functionality and flexibility of DHCP operations within the network.

Configuring HSRP (Hot Standby Router Protocol) along with DHCP (Dynamic Host Configuration Protocol) address assignment on a Layer 3 switch involves several steps to ensure both high availability and efficient IP address allocation. Here's how it can be done:

Step 1 Identify VLANs and Interfaces

- ✓ Determine which VLANs require HSRP redundancy and DHCP address assignment.
- ✓ Identify the Layer 3 interfaces (SVIs - Switched Virtual Interfaces) associated with these VLANs on the Layer 3 switch.

Step 2 HSRP Configuration

- ✓ Configure HSRP on the identified SVIs to provide redundancy for the default gateway within each VLAN.
- ✓ Specify the HSRP group number, virtual IP address, and priority on each SVI.
- ✓ Ensure consistent HSRP configuration (group number, virtual IP, etc.) across the switches participating in HSRP within the same VLAN.

Step 3 DHCP Helper Address Configuration

- ✓ Assign an IP DHCP helper address on each SVI participating in HSRP.
- ✓ Specify the IP address of the DHCP server to which DHCP broadcast messages will be forwarded.
- ✓ This allows DHCP requests from clients in the VLAN to reach the DHCP server, even if it is located in a different subnet or VLAN.

Step 4 Verification

- ✓ Verify the HSRP and DHCP helper address configurations on the Layer 3 switch.
- ✓ Use commands such as ``show standby`` to verify HSRP status and ``show ip DHCP snooping`` or ``show ip DHCP pool`` to verify DHCP helper address configuration and DHCP pool settings.

Step 5 Testing

- ✓ Test connectivity and failover behavior to ensure HSRP redundancy is functioning as expected.
- ✓ Verify that DHCP clients in the VLANs are successfully obtaining IP address assignments from the DHCP server specified in the DHCP helper address configuration.

Step 6 Monitoring and Maintenance

- ✓ Regularly monitor the HSRP status and DHCP address assignment functionality to ensure network reliability and availability.
- ✓ Update configurations as necessary to accommodate changes in network requirements or topology.

Configuring HSRP with DHCP address assignment on a Layer 3 switch, providing both redundancy for the default gateway and efficient IP address allocation for devices within the network.

Configuring a DHCP server device

Configuring a DHCP server device involves several steps and is essential for automating IP address assignment and network configuration for client devices. Here's how and why it's done:

Step 1: Activation

Activate the DHCP service to start offering IP addresses and configuration parameters to DHCP clients.

Step 2: Scope Configuration

Define DHCP address pools or scopes, specifying ranges of IP addresses to be assigned to DHCP clients. Configure additional parameters within each scope, such as subnet masks, default gateways, DNS servers, and lease durations.

Step 3: Exclusion Ranges

Exclude specific IP addresses from DHCP assignment within each scope to prevent conflicts with statically assigned addresses or reserved addresses for network infrastructure device.

Reasons for Configuring a DHCP Server

Automatic IP Address Assignment: DHCP automates the process of IP address assignment, eliminating the need for manual configuration on individual client devices. This saves time and reduces the risk of configuration errors.

Centralized Network Management: DHCP centralizes IP address management, allowing network administrators to efficiently allocate and manage IP addresses from a single location. This simplifies network administration tasks and ensures consistency across the network.

Scalability: DHCP scales easily to accommodate growing networks by dynamically allocating IP addresses as needed. This flexibility makes it well-suited for networks with changing device populations or temporary connections, such as guest networks or dynamic work environments.

Reduced IP Address Conflicts: DHCP helps prevent IP address conflicts by actively managing IP address assignments and detecting address conflicts before they occur. This improves network reliability and reduces downtime caused by address conflicts.

3.3.8 Configuring OSPF

Configuring OSPF (Open Shortest Path First) on the firewall, routers, and SVIs (Switched Virtual Interfaces) is crucial for dynamic routing, efficient traffic forwarding, and network scalability. Here's how and why it's done.

Firewall Configuration: Configuring OSPF on the firewall allows it to participate in dynamic routing and exchange routing information with other OSPF-enabled devices.

Router Configuration: OSPF enables routers to dynamically learn and update routing tables based on network topology changes, ensuring optimal path selection and efficient traffic forwarding.

SVI Configuration (Layer 3 Switches): Configuring OSPF on SVIs enables the switch to participate in dynamic routing and exchange routing information with other OSPF-enabled devices in the network.

Here are the necessary steps:

- ✓ Enable OSPF routing on the layer 3 device.
- ✓ Configure OSPF settings such as router ID, area assignments, and authentication.
- ✓ Advertise VLAN subnets or SVIs into OSPF.
- ✓ Establish OSPF neighbor relationships with adjacent routers or SVIs.

3.3.9 Configuring firewall interface security zones and levels

Configuring firewall interface security zones and levels involves categorizing network segments based on security requirements and assigning appropriate security policies to each zone. Here's how and why it's done:

Define Security Zones: Different parts of the network have varying security requirements based on factors like sensitivity of data, types of applications, and regulatory compliance. By defining security zones, we can segment the network and enforce appropriate security

policies to protect critical assets and mitigate potential threats. To Configure we Identify and categorize network segments into distinct security zones, such as internal, DMZ (Demilitarized Zone), and external/internet-facing zones.

Assign Security Levels: Security levels represent the relative trustworthiness of traffic originating from or destined to each security zone. Higher security levels indicate greater trust, while lower security levels indicate less trust. To Configure we Assign a numerical security level to each security zone, with higher numbers indicating higher trust levels. For example, internal zones may have higher security levels than DMZ or external zones.

Define Inter-Zone Policies: Firewall policies are used to control traffic flow between different security zones. Defining inter-zone policies ensures that only authorized traffic is allowed to traverse between zones, thereby minimizing the risk of unauthorized access or data breaches. Configure firewall rules or access control lists (ACLs) to permit or deny traffic between security zones based on specific criteria such as source/destination IP addresses, ports, protocols, and application types.

Implement Zone-Based Security Policies: Zone-based security policies allow administrators to apply consistent security policies across all interfaces within a security zone, simplifying policy management and enforcement. To Configure Implement zone-based security policies on the firewall by associating interfaces with their respective security zones and applying security policies to each zone. This involve defining inbound and outbound traffic rules, application inspection policies, and threat prevention measures.

By configuring firewall interface security zones and levels, we can establish a layered defense strategy, enforce granular access controls, and protect critical assets from unauthorized access or cyber threats. This approach helps maintain network integrity, confidentiality, and availability, thereby enhancing overall network security posture.

Configuring firewall inspection policies

Configuring firewall inspection policies is essential for ensuring comprehensive security enforcement and traffic inspection within a network. Here's why and how it's done:

Security Enforcement: Firewall inspection policies allow administrators to enforce security measures and inspect network traffic for potential threats, vulnerabilities, or policy violations. To Configure define inspection policies to examine different aspects of network traffic, including packet headers, payload content, and application behavior.

Threat Detection and Prevention: Inspection policies enable the firewall to detect and prevent various types of cyber threats, including malware, viruses, intrusions, and malicious activities. Configure firewall rules or policies to perform deep packet inspection (DPI), protocol analysis, and application-layer filtering to identify and block suspicious or unauthorized traffic.

Policy Compliance: Inspection policies help enforce compliance with organizational security policies, regulatory requirements, and industry standards. To Configure define rules and policies to ensure that network traffic adheres to predefined security guidelines, access controls, and acceptable use policies.

Application Visibility and Control: Inspection policies provide visibility into network applications and allow administrators to control application usage and behavior.

To Configure Implement application-aware inspection policies to identify and classify network applications, enforce bandwidth management, and regulate application access based on specific criteria.

Performance Optimization: Properly configured inspection policies can help optimize network performance by efficiently handling legitimate traffic while mitigating the impact of security threats. Fine-tune inspection policies to balance security requirements with performance considerations, ensuring that traffic inspection does not introduce excessive latency or degrade network throughput.

Threat Intelligence Integration: Inspection policies can leverage threat intelligence feeds and security analytics to enhance threat detection and response capabilities. To Configure Integrate threat intelligence sources with firewall inspection policies to enrich security context, identify emerging threats, and automate threat remediation actions.

By configuring firewall inspection policies, we can strengthen their overall security posture, proactively detect and mitigate security risks, ensure compliance with regulatory requirements, and optimize network performance. Inspection policies play a critical role in safeguarding network assets, preserving data confidentiality, and maintaining the integrity and availability of network resources.

3.3.10 Wireless network configuration

Wireless network configuration involves setting up access points, configuring wireless LAN controllers (WLCs), and connecting wireless devices. Here's a simplified step-by-step guide.

Step 1: Access Point Setup

- ✓ Drag and drop an access point (AP) from the Packet Tracer toolbar onto the workspace.
- ✓ Configure basic settings such as SSID (network name), security settings (WPA2, etc.), and channel settings.
- ✓ Assign an IP address to the access point if required.

Step 2: Wireless LAN Controller Configuration

- ✓ Add a wireless LAN controller (WLC) to the topology from the Packet Tracer toolbar.
- ✓ Access the WLC's console or web interface to configure it.
- ✓ Configure basic settings such as IP address, hostname, and management settings.
- ✓ Create WLANs (Wireless LANs) on the WLC and configure parameters such as SSID, security policies, VLAN mappings, etc.
- ✓ Associate access points with the WLC by specifying the WLC's IP address on the access point configuration.

Step 3: Connectivity Setup

- ✓ Connect the access points to switches using copper straight-through cables.
- ✓ Connect the switches to the router or other network devices as needed.
- ✓ Configure VLANs on switches if you plan to use VLAN segmentation for wireless clients.

Step 3: Device Configuration

- ✓ Place wireless devices (laptops, smartphones, etc.) onto the Packet Tracer workspace.
- ✓ Configure the wireless adapter settings on these devices to connect to the configured SSID.
- ✓ Enter the wireless network passphrase or security settings as configured on the WLC.

Step 4: Verification and Testing

- ✓ Verify connectivity between wireless devices and the network by attempting to ping other devices or access resources.
- ✓ Monitor the WLC and access point interfaces to ensure they are up and functioning correctly.
- ✓ Use Packet Tracer's simulation mode to troubleshoot any connectivity issues if they arise.

3.3.11 QoS Configuration

Configuring Quality of Service (QoS) involves prioritizing and managing network traffic to ensure that critical applications receive sufficient bandwidth and priority over less important traffic. Here's is how we configured QoS on a switch.

Step 1: Identify Traffic Classes

- ✓ Determine the types of traffic that require QoS prioritization, such as voice, video, or real-time applications.
- ✓ Classify traffic into different classes based on their importance and characteristics.

Step 2: Define QoS Policies

- ✓ Assign appropriate QoS parameters to each traffic class, including bandwidth limits, packet prioritization, and queueing strategies.
- ✓ Define QoS policies to enforce these parameters, specifying how traffic should be treated based on its classification.

Step 3: Enable QoS Features

- ✓ Enable QoS features on the network device, such as traffic shaping, policing, or queueing mechanisms.
- ✓ Configure QoS settings in accordance with your defined policies and requirements.

Step 4: Implement Traffic Classification

- ✓ Use classification methods such as access control lists (ACLs), Differentiated Services Code Point (DSCP) markings, or Layer 2 or Layer 3 markings to classify traffic into different classes.
- ✓ Map traffic classifications to corresponding QoS policies to ensure that each traffic class receives the appropriate treatment.

Step 5: Apply QoS Policies

- ✓ Apply QoS policies to relevant interfaces or VLANs on the network device to enforce traffic prioritization and management.
- ✓ Specify inbound and outbound QoS policies to control traffic in both directions.

Step 6: Monitor and Tune QoS Performance

- ✓ Monitor QoS statistics and performance metrics to ensure that QoS policies are effectively prioritizing and managing traffic.
- ✓ Fine-tune QoS settings as needed to optimize network performance and accommodate changes in traffic patterns or requirements.

CHAPTER FOUR

TESTING AND RESULT

In the ever-evolving landscape of network technologies, ensuring optimal performance and reliability is paramount, particularly within campus networks where diverse users and applications coexist.

4.1 Checking Status

Ether-channel status

After configuring the Ether-channel in the core and distribution switch the result we get is displayed as the following. This displayed by using the command “show ether-channel port-channel”.

```
CORE-SW1#show etherchannel port-channel
Channel-group listing:
-----
Group: 4
-----
Port-channels in the group:
-----
Port-channel: Po4 (Primary Aggregator)
-----
Age of the Port-channel = 00d:00h:0m:49s
Logical slot/port = 2/4 Number of ports = 3
EC = 0x00000000 HotStandby port = null
Port state = Port-channel
Protocol = LACP
Port Security = Disabled

Ports in the Port-channel:
-----
Index Load Port EC state No of bits
-----
0 00 Gg1/0/23Active 0
0 00 Gg1/0/23Active 0
0 00 Gg1/0/24Active 0
Time since last port bundled: 00d:00h:0m:49s Gg1/0/24
CORE-SW1#
```

```
CORE-SW2#show etherchannel port-channel
Channel-group listing:
-----
Group: 4
-----
Port-channels in the group:
-----
Port-channel: Po4 (Primary Aggregator)
-----
Age of the Port-channel = 00d:00h:0m:35s
Logical slot/port = 2/4 Number of ports = 3
EC = 0x00000000 HotStandby port = null
Port state = Port-channel
Protocol = LACP
Port Security = Disabled

Ports in the Port-channel:
-----
Index Load Port EC state No of bits
-----
0 00 Gg1/0/23Passive 0
0 00 Gg1/0/23Passive 0
0 00 Gg1/0/24Passive 0
Time since last port bundled: 00d:00h:0m:34s Gg1/0/24
CORE-SW2#
HSRP-6-STATECHANGE: Vlan70 Grp 70 state Speak -> Standby
HSRP-6-STATECHANGE: Vlan70 Grp 70 state Standby -> Active
```

Figure 4.1 Ether-Channel status

HSRP status

The Hot Standby Router Protocol is displayed by using command “show standby brief” in the core switch CLI.

```
Core Switch-1
Physical Config CLI Attributes
IOS Command Line Interface
Password: Password:
CORE-SW1#enable
CORE-SW1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CORE-SW1(config)#interface GigabitEthernet1/0/3
CORE-SW1(config-if)#
CORE-SW1#
VLANs - CONFIG_11 Configured from console by console
CORE-SW1#show standby brief
P indicates configured to preempt.
-----
Interface gtp pri p State Active Standby Virtual IP
V12 5 120 P Active local 192.168.10.3 192.168.10.1
V15 5 120 P Active local 192.168.0.3 192.168.0.1
V10 10 120 P Active local 192.168.4.3 192.168.4.1
V15 15 120 P Active local 192.168.8.3 192.168.8.1
V10 20 120 P Active local 192.168.12.3 192.168.12.1
V15 25 120 P Active local 192.168.16.3 192.168.16.1
V10 30 120 P Active local 192.168.20.3 192.168.20.1
V15 35 120 P Active local 192.168.24.3 192.168.24.1
V10 40 120 P Active local 192.168.28.3 192.168.28.1
V15 45 120 P Active local 192.168.32.3 192.168.32.1
V10 50 120 P Active local 192.168.36.3 192.168.36.1
V15 55 120 P Active local 192.168.40.3 192.168.40.1
V10 60 120 P Active local 192.168.44.3 192.168.44.1
V15 65 120 P Active local 192.168.48.3 192.168.48.1
V10 70 120 P Active local 192.168.52.3 192.168.52.1
V15 75 120 P Active local 192.168.56.3 192.168.56.1
V10 80 120 P Active local 192.168.60.3 192.168.60.1
V15 85 120 P Active local 192.168.64.3 192.168.64.1
V10 90 120 P Active local 192.168.68.3 192.168.68.1
V15 95 120 P Active local 192.168.72.3 192.168.72.1
V10 100 120 P Active local 192.168.76.3 192.168.76.1
V15 105 120 P Active local 192.168.80.3 192.168.80.1
V10 110 120 P Active local 192.168.84.3 192.168.84.1
V15 115 120 P Active local 192.168.88.3 192.168.88.1
V10 120 120 P Active local 192.168.92.3 192.168.92.1
CORE-SW1#
```

Figure 4.2 HSRP status

VLAN Status

The status of VLANs configured on core, distribution and access switch is displayed as the following by using command "show vlan brief" in their CLI.

CORE-SW1#show vlan br			
VLAN Name	Status	Ports	
1 default	active	Gig1/0/7, Gig1/0/8, Gig1/0/9, Gig1/0/11 Gig1/0/12, Gig1/0/13, Gig1/0/14, Gig1/0/15 Gig1/0/16, Gig1/0/17, Gig1/0/19, Gig1/0/20 Gig1/0/21, Gig1/1/1, Gig1/1/2, Gig1/1/3 Gig1/1/4	
2 Management	active		
5 DMZ-LAN	active		
10 VLT-LAN	active		
15 CAES-LAN	active		
20 CBE-LAN	active		
25 CCI-LAN	active		
30 CL-LAN	active		
35 CWS-LAN	active		
40 SSA-LAN	active		
45 CDED-LAN	active		
50 FPD-LAN	active		
55 CESH-LAN	active		
60 CESH-LAN	active		
65 CESH-LAN	active		
70 IT-LAN	active		
75 AE-LAN	active		
80 CE-LAN	active		
85 CSE-LAN	active		
90 ECE-LAN	active		
95 FFWHT-LAN	active		
100 RE-LAN	active		
105 RE-LAN	active		
110 RE-LAN	active		
115 WRE-LAN	active		
199 Blackhole	active		
200 WAN-VLAN	active	Gig1/0/10	
1002 fddi-default	active		
1003 token-ring-default	active		
1004 fddi-default	active		
1005 trnet-default	active		
CORE-SW1#			

CORE-SW2#			
VLAN Name	Status	Ports	
1 default	active	Gig1/0/7, Gig1/0/8, Gig1/0/9, Gig1/0/11 Gig1/0/12, Gig1/0/13, Gig1/0/14, Gig1/0/15 Gig1/0/16, Gig1/0/17, Gig1/0/19, Gig1/0/20 Gig1/0/21, Gig1/1/1, Gig1/1/2, Gig1/1/3 Gig1/1/4	
2 Management	active		
5 DMZ-LAN	active		
10 VLT-LAN	active		
15 CAES-LAN	active		
20 CBE-LAN	active		
25 CCI-LAN	active		
30 CL-LAN	active		
35 CWS-LAN	active		
40 SSA-LAN	active		
45 CDED-LAN	active		
50 FPD-LAN	active		
55 CESH-LAN	active		
60 CESH-LAN	active		
65 CESH-LAN	active		
70 IT-LAN	active		
75 AE-LAN	active		
80 CE-LAN	active		
85 CSE-LAN	active		
90 ECE-LAN	active		
95 FFWHT-LAN	active		
100 RE-LAN	active		
105 RE-LAN	active		
110 RE-LAN	active		
115 WRE-LAN	active		
199 Blackhole	active		
200 WAN-VLAN	active	Gig1/0/10	
1002 fddi-default	active		
1003 token-ring-default	active		
1004 fddi-default	active		
1005 trnet-default	active		
CORE-SW2#			

Figure 4.3 VLAN status

4.2 Testing

DHCP testing

Frist, we set the network interface of the PC to obtain an IP address automatically (DHCP enabled).

The DHCP server responds with a DHCPACK, confirming that the PC can use the offered IP address and providing any additional configuration parameters such as subnet mask, default gateway and DNS server address. Here is some example of the tested figure.

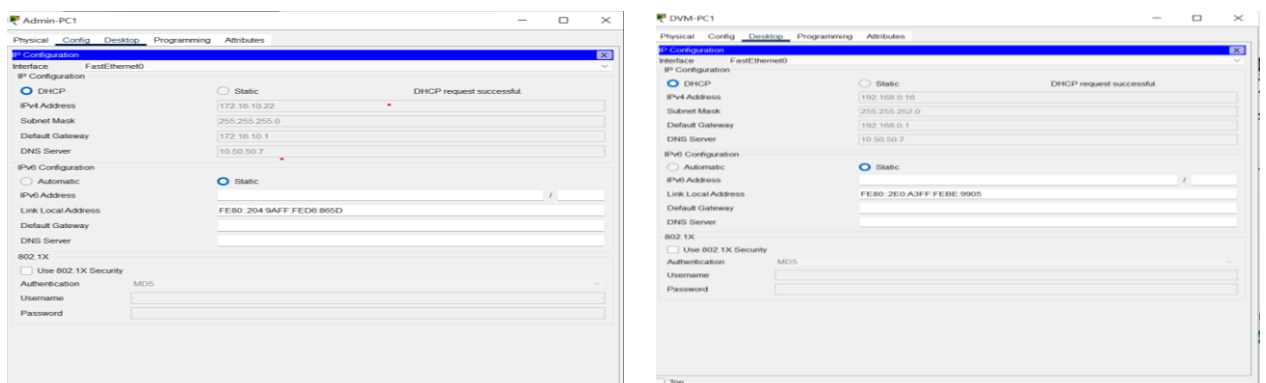


Figure 4.4 DHCP Address

Connection Testing

We performed connection testing between devices such as PCs, routers, switches, and gateways to ensure proper network communication. Here's how you can perform connection testing between devices.

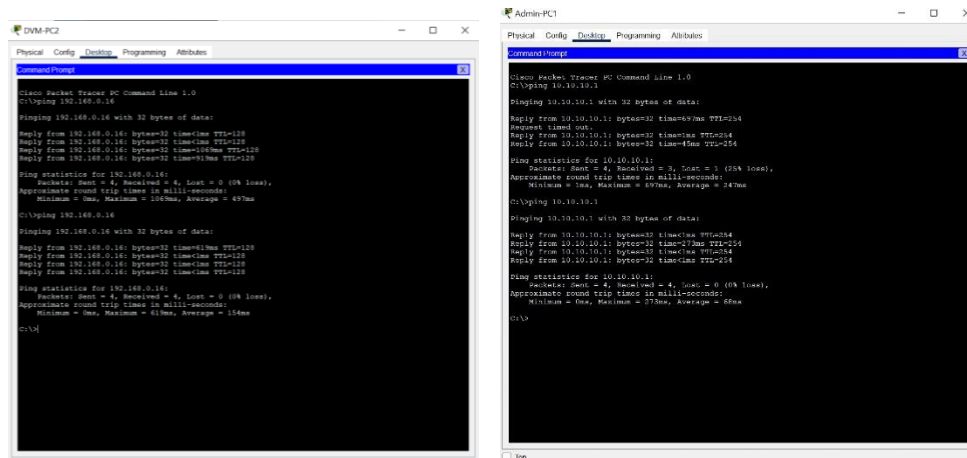


Figure 4.5 Pinging

WLAN Testing

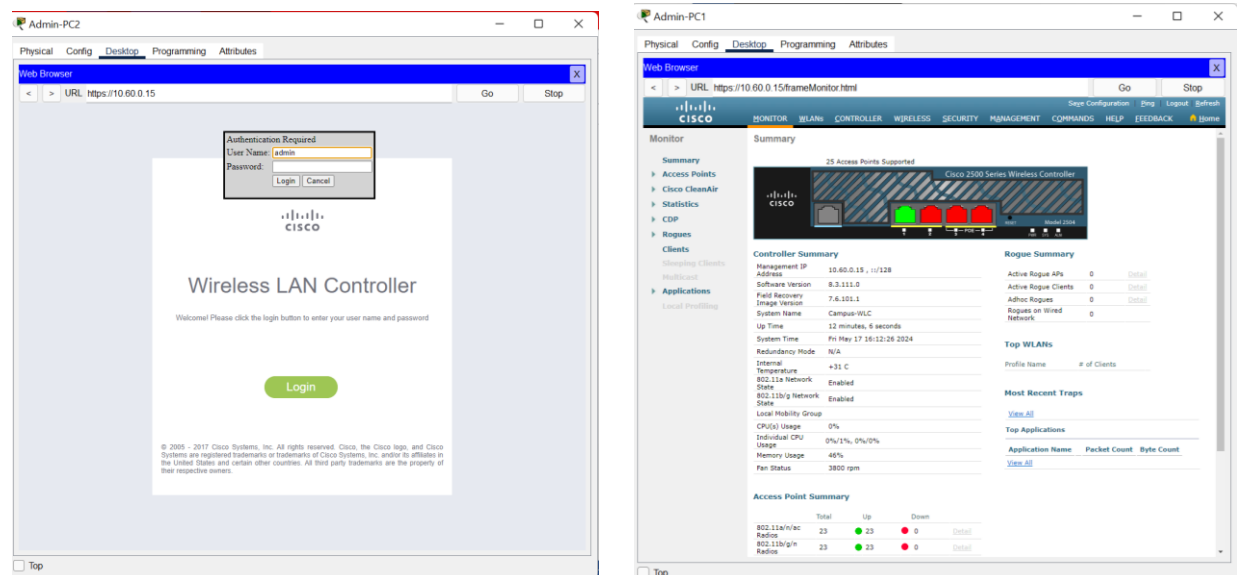
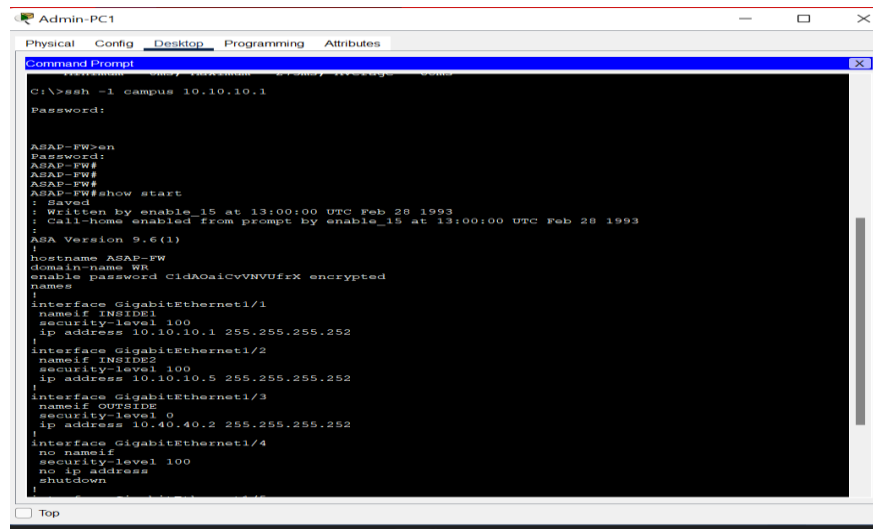


Figure 4.6 WLAN Testing

SSH testing



```
Admin-PC1
Physical  Config  Desktop  Programming  Attributes
Command Prompt
C:\>ssh -l campus 10.10.10.1
Password:
ASAP-FW#
ASAP-FW#
ASAP-FW#
ASAP-FW#
ASAP-FW#show start
! Saved
! Written by enable_15 at 13:00:00 UTC Feb 28 1993
! Call-home enabled from prompt by enable_15 at 13:00:00 UTC Feb 28 1993
2
ASA Version 9.6(1)
1
hostname ASAP-FW
domain-name WR
enable password CldAa1cVvNVUfrX encrypted
names
!
interface GigabitEthernet1/1
 nameif INSIDE1
 security-level 100
 ip address 10.10.10.1 255.255.255.252
!
interface GigabitEthernet1/2
 nameif INSIDE2
 security-level 100
 ip address 10.10.10.5 255.255.255.252
!
interface GigabitEthernet1/3
 nameif OUTSIDE
 security-level 0
 ip address 10.40.40.2 255.255.255.252
!
interface GigabitEthernet1/4
 no nameif
 security-level 100
 no ip address
 shutdown
!
```

Figure 4.7 SSH testing

CHAPTER FIVE

CONCLUSION AND RECOMMENDATION

5.1 Conclusion

The proposed campus area network design, leveraging redundant links, minimized broadcast domains, high-bandwidth cables, and departmental VLANs, provides a comprehensive solution to address the evolving needs of the educational institution. This approach ensures a reliable, efficient, and secure network infrastructure that can support the diverse requirements of students, faculty, and staff. The redundant link configuration enhances the availability and resilience of the network, minimizing the impact of potential failures and ensuring continuous access to critical resources. The segmentation of the network into smaller broadcast domains, using VLANs, improves overall performance by reducing the scope of broadcast traffic and enhancing security through better control and management of network resources.

The high-bandwidth cables, such as fiber optic or high-speed Ethernet, future-proof the campus network by providing ample capacity to accommodate the growing demands for bandwidth-intensive applications, including video conferencing, multimedia streaming, and large file transfers. This will enable a seamless and responsive user experience for the campus community. Furthermore, the implementation of departmental VLANs allows for the tailored configuration of network policies, access controls, and quality of service settings to meet the specific requirements of each department. This level of highly detailed control and segmentation promotes better network optimization, security, and resource allocation.

By adopting this comprehensive approach to campus area network design, the educational institution can establish a robust, scalable, and adaptable infrastructure that supports the evolving needs of the campus community. This will ultimately enhance the overall educational experience, foster collaboration, and enable the institution to maintain a competitive edge in the dynamic educational landscape.

5.2 Recommendation

Here is what we recommend a campus area network user based on the important parameters: using redundant link, minimizing broadcast domain, using high bandwidth cable, and using different VLANs for different departments. To build a robust and efficient campus area network, we would recommend the following.

Redundant Link: Implement a redundant network link to ensure high availability and reliable connectivity across the campus. This can be achieved by deploying a secondary, independent link that can automatically take over in the event of a failure in the primary link. This redundancy will help maintain uninterrupted access to critical resources and services, minimizing downtime and ensuring business continuity.

Minimizing Broadcast Domain: Divide the campus network into smaller, logical segments or broadcast domains using VLANs (Virtual Local Area Networks). By segmenting the network, you can reduce the scope of broadcast traffic, improve network performance, and enhance security. Each VLAN can be assigned to a specific department or function, allowing for better control and management of network resources.

High Bandwidth Cable: Utilize high-bandwidth network cables, such as fiber optic or high-speed Ethernet, to support the growing data demands of the campus environment. These high-performance cables can handle the increased bandwidth requirements for applications like video conferencing, multimedia streaming, and large file transfers. The enhanced bandwidth will ensure a smooth and responsive user experience for students, faculty, and staff.

Departmental VLANs: Assign different VLANs to the various departments within the campus. This will help segregate network traffic and minimize the potential for interference or unauthorized access between departments. Each VLAN can be configured with its own set of policies, access controls, and quality of service (QoS) settings to meet the specific needs of the respective department. This approach promotes better network segmentation, security, and optimization.

By implementing these recommendations, anyone can build a campus area network that is resilient, efficient, and tailored to the unique requirements of educational institution. The redundant link ensures high availability, the minimized broadcast domains improve performance and security, the high-bandwidth cables provide ample capacity, and the departmental VLANs enable better control and management of network resources. This comprehensive approach will help create a campus network that can support the evolving needs of your students, faculty, and staff while maintaining a secure and reliable connectivity infrastructure.

References

- [1] L. a. F. R. a. R. J. a. F. F. {Camarinha-Matos, "{Collaborative Networks: A Pillar of Digital Transformation}", " *Applied Sciences* }, Vols. {9}, {2019},.
- [2] M. Rouse, "Networking Hardware," *Techopedia*, 23 September 2014.
- [3] M. F. K. T. Richard Froom, "Cisco Catalyst QoS: Quality of Service in Campus Networks," *Cisco Press*, Jun 6, 2003.
- [4] M. {Kaur, "{AN OVERVIEW OF QUALITY OF SERVICE COMPUTER NETWORK}", " *Indian Journal of Computer Science and Engineering* }, Vols. {2}, pp. {471}, {2011},.
- [5] M. {Kaur, "{AN OVERVIEW OF QUALITY OF SERVICE COMPUTER NETWORK}", " *Indian Journal of Computer Science and Engineering* }, Vols. {2}, pp. {472}, {2011},.
- [6] M. {Kaur, "{AN OVERVIEW OF QUALITY OF SERVICE COMPUTER NETWORK}", " *Indian Journal of Computer Science and Engineering* }, Vols. {2}, pp. {470}, {2011},.
- [7] P. a. C. J. a. K. P. a. B. S. {Gevros, "{Congestion Control Mechanisms and the Best Effort Service Model}", " *Network, IEEE* }, Vols. {15}, pp. { 26}, {2001},.
- [8] R. G. a. C. M. a. A. N. a. M. C. a. S.-C. C. {Barba, "{QoS Policies to Improve Performance in Academic Campus and SDN Networks}", " in *{2018 IEEE 10th Latin-American Conference on Communications (LATINCOM)}*, IEEE, {2018},, pp. {1-6},.
- [9] B. T. a. M. L. a. M. G.-M. {Nguyen, "{Energy-Efficient QoS-Based Congestion Control for Reliable Communications in Wireless Multimedia Sensor Networks}", " in *{2018 IEEE International Conference on Communications Workshops (ICC Workshops)}*, IEEE, {2018},, pp. {1-6},.
- [10] R. {Jain, "{Congestion control in computer networks: issues and trends}", " *IEEE Network* }, Vols. {4}, pp. {24-30}, {1990},.
- [11] K. a. T. S. a. H. B. {Nzobokela, "{Enhancing Network Performance and Quality of Service (QoS) in a Wired Local Area Network (LAN)}", " *international Journal of Networks and Communications* , vol. {13}, pp. {1-14}, { 02, 2024},.

- [12] S. a. A. A. {Suman, "{IP Traffic Management With Access Control List Using Cisco Packet Tracer}},{", *{International Journal of Science, Engineering and Technology Research}*, Vols. {5},{, pp. {1556-1561}, {2016},{,.
- [13] S. a. M. A. a. A. S. a. P. S. {Sunassee, "{A Comprehensive Review on Congestion Control Techniques in Networking},{", in *{2021 5th International Conference on Computing Methodologies and Communication (ICCMC)}*, , IEEE, {2021},{, pp. {305-312},{,.
- [14] R. G. S. K. U. Haribansh Mishra, "Systematic review of congestion handling techniques for 802.11 wireless networks," *onlinelibrary.wiley.com*, 16 September 2019.
- [15] R. Lewis, "Cisco Systems," *Encyclopedia Britannica*, 29 Mar. 2024.
- [16]
- [17] Howard, "Driving Next Generation Data Centers Toward 400G," *Fast shipping to Ethiopia*, May 25, 2021.
- [18] Kinza Yasar, Technical WriterJohn Burke, "Nemertes Research," *TechTarget*, 2023.
- [19]
- [20] J. E. J. B. Linda Rosencrance, "software-defined networking (SDN)," *Nemertes Research*.

Appendices

Appendix I. Basic Configuration

Configuration for all access switch except IT-staff office

```
enable
configure terminal
int range gig1/0/3-24
spanning-tree portfast
spanning-tree bpduguard enable
ex
do wr
```

Access switch trunk interface configuration

```
enable
configure terminal
interface FastEthernet0/1-2
switchport mode trunk
ex
do wr
```

Station distribution switch trunk interface configuration

```
enable
configure terminal
interface GigabitEthernet0/1-4
switchport mode trunk
ex
do wr
```

Main branch distribution switch trunk interface configuration

```
enable
configure terminal
interface range GigabitEthernet0/1-14
switchport mode trunk
ex
do wr
```

Gendeje branch distribution switch trunk interface configuration

```
enable
configure terminal
interface range GigabitEthernet0/1-11
switchport mode trunk
ex
do wr
```

Etherchannel configuration in all core and distribution switch of each branch

```
enable
configure terminal
interface range GigabitEthernet1/0/22-24
switchport mode trunk
channel-group 2 mode active
ex
do wr
```

Appendix II. Configuration for creating VLAN

In all department access switch switches

```
vlan <department_LAN_vlan_id>
name <department_LAN_vlan_name>
vlan 2
name Management
vlan 200
name WLAN-VLAN
vlan 199
name Blackhole
```

EX

```
int range FastEthernet0/3-20
switchport mode access
switchport access vlan
<department_LAN_vlan_id>
exit
```

```
int range FastEthernet0/21-24
switchport mode access
switchport access vlan 200
exit
```

```
do wr
int range GigabitEthernet0/21-24
switchport mode access
switchport access vlan 199
shutdown
```

exit

do wr

In IT-staff access switch switch

```
vlan <department_LAN_vlan_id>
name <department_LAN_vlan_name>
vlan 2
name Management
vlan 200
```

```

name WLAN-VLAN
int range FastEthernet0/3-20
switchport mode access
switchport access vlan
<department_LAN_vlan_id>
exit
int range FastEthernet0/21-24
switchport mode access
switchport access vlan 200
exit
do wr
int range GigabitEthernet0/1-2
switchport mode access
switchport access vlan 2
no shutdown
exit
do wr

```

vlan creation in all layer 3 Station branch distribution switch

```

vlan <department_LAN_vlan_id>
name <department_LAN_vlan_name>
vlan 2
name Management
vlan 200
name WLAN-VLAN
vlan 199
name Blackhole
exit
do wr

```

Appendix III HSRP CONFIGURATION

Passive core switch

```

interface Vlan2
ip address 172.16.10.3 255.255.252.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 2 ip 172.16.10.1
standby 2 priority 110
standby 2 preempt
interface Vlan5
ip address 192.168.0.3 255.255.252.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 5 ip 192.168.0.1
standby 5 priority 110

```

```

standby 5 preempt
interface Vlan10
ip address 192.168.4.3 255.255.252.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 10 ip 192.168.4.1
standby 10 priority 110
standby 10 preempt
interface Vlan15
ip address 192.168.8.3 255.255.252.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 15 ip 192.168.8.1
standby 15 priority 110
standby 15 preempt
interface Vlan20
ip address 192.168.12.3 255.255.252.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 20 ip 192.168.12.1
standby 20 priority 110
standby 20 preempt
interface Vlan25
ip address 192.168.16.3 255.255.252.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 25 ip 192.168.16.1
standby 25 priority 110
standby 25 preempt
interface Vlan30
ip address 192.168.20.3 255.255.252.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 30 ip 192.168.20.1
standby 30 priority 110
standby 30 preempt
interface Vlan35
ip address 192.168.24.3 255.255.252.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 35 ip 192.168.24.1
standby 35 priority 110
standby 35 preempt
interface Vlan40
ip address 192.168.28.3 255.255.252.0
ip helper-address 10.50.50.5

```

```

ip helper-address 10.50.50.6
standby 40 ip 192.168.28.1
standby 40 priority 110
standby 40 preempt
interface Vlan45
ip address 192.168.32.3 255.255.252.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 45 ip 192.168.32.1
standby 45 priority 110
standby 45 preempt
interface Vlan50
ip address 192.168.36.3 255.255.252.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 50 ip 192.168.36.1
standby 50 priority 110
standby 50 preempt
interface Vlan55
ip address 192.168.40.3 255.255.252.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 55 ip 192.168.40.1
standby 55 priority 110
standby 55 preempt
interface Vlan60
ip address 192.168.44.3 255.255.252.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 65 ip 192.168.44.1
standby 65 priority 110
standby 65 preempt
interface Vlan65
ip address 192.168.48.3 255.255.252.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 65 ip 192.168.48.1
standby 65 priority 110
standby 65 preempt
interface Vlan70
ip address 192.168.52.3 255.255.252.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 70 ip 192.168.52.1
standby 70 priority 110
standby 70 preempt

```

```

interface Vlan75
ip address 192.168.56.3 255.255.252.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 75 ip 192.168.56.1
standby 75 priority 110
standby 75 preempt
interface Vlan80
ip address 192.168.60.3 255.255.252.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 80 ip 192.168.60.1
standby 80 priority 110
standby 80 preempt
interface Vlan85
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 85 ip 192.168.64.1
standby 85 priority 110
standby 85 preempt
interface Vlan90
ip address 192.168.68.3 255.255.252.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 90 ip 192.168.68.1
standby 90 priority 110
standby 90 preempt
interface Vlan95
ip address 192.168.72.3 255.255.252.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 95 ip 192.168.72.1
standby 95 priority 110
standby 95 preempt
interface Vlan100
ip address 192.168.76.3 255.255.252.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 100 ip 192.168.76.1
standby 100 priority 110
standby 100 preempt
interface Vlan105
ip address 192.168.80.3 255.255.252.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 105 ip 192.168.80.1

```

```

standby 105 priority 110
standby 105 preempt
interface Vlan110
ip address 192.168.84.3 255.255.252.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 110 ip 192.168.84.1
standby 110 priority 110
standby 110 preempt
interface Vlan115
ip address 192.168.88.3 255.255.252.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 115 ip 192.168.88.1
standby 115 priority 110
standby 115 preempt
For active core switch
interface Vlan2
ip address 172.16.10.2 255.255.252.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 2 ip 172.16.10.1
standby 2 priority 120
standby 2 preempt
interface Vlan5
ip address 192.168.0.2 255.255.252.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 5 ip 192.168.0.1
standby 5 priority 120
standby 5 preempt
interface Vlan10
ip address 192.168.4.2 255.255.252.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 10 ip 192.168.4.1
standby 10 priority 120
standby 10 preempt
interface Vlan15
ip address 192.168.8.2 255.255.252.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 15 ip 192.168.8.1
standby 15 priority 120
standby 15 preempt
interface Vlan20

```

```

ip address 192.168.12.2 255.255.252.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 20 ip 192.168.12.1
standby 20 priority 120
standby 20 preempt
interface Vlan25
ip address 192.168.16.2 255.255.252.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 25 ip 192.168.16.1
standby 25 priority 120
standby 25 preempt
interface Vlan30
ip address 192.168.20.2 255.255.252.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 30 ip 192.168.20.1
standby 30 priority 120
standby 30 preempt
interface Vlan35
ip address 192.168.24.2 255.255.252.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 35 ip 192.168.24.1
standby 35 priority 120
standby 35 preempt
interface Vlan40
ip address 192.168.28.2 255.255.252.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 40 ip 192.168.28.1
standby 40 priority 120
standby 40 preempt
interface Vlan45
ip address 192.168.32.2 255.255.252.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 45 ip 192.168.32.1
standby 45 priority 120
standby 45 preempt
interface Vlan50
ip address 192.168.36.2 255.255.252.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 50 ip 192.168.36.1

```

```

standby 50 priority 120
standby 50 preempt
interface Vlan55
ip address 192.168.40.2 255.255.252.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 55 ip 192.168.40.1
standby 55 priority 120
standby 55 preempt
interface Vlan60
ip address 192.168.44.2 255.255.252.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 65 ip 192.168.44.1
standby 65 priority 120
standby 65 preempt
interface Vlan65
ip address 192.168.48.2 255.255.252.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 65 ip 192.168.48.1
standby 65 priority 120
standby 65 preempt
interface Vlan70
ip address 192.168.52.2 255.255.252.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 70 ip 192.168.52.1
standby 70 priority 120
standby 70 preempt
interface Vlan75
ip address 192.168.56.2 255.255.252.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 75 ip 192.168.56.1
standby 75 priority 120
standby 75 preempt
interface Vlan80
mac-address 000b.be11.c511
ip address 192.168.60.2 255.255.252.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 80 ip 192.168.60.1
standby 80 priority 120
standby 80 preempt
interface Vlan85

```

```

mac-address 000b.be11.c512
ip address 192.168.64.2 255.255.252.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 85 ip 192.168.64.1
standby 85 priority 120
standby 85 preempt
interface Vlan90
ip address 192.168.68.2 255.255.252.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 90 ip 192.168.68.1
standby 90 priority 120
standby 90 preempt
interface Vlan95
ip address 192.168.72.2 255.255.252.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 95 ip 192.168.72.1
standby 95 priority 120
standby 95 preempt
interface Vlan100
ip address 192.168.76.2 255.255.252.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 100 ip 192.168.76.1
standby 100 priority 120
standby 100 preempt
interface Vlan105
ip address 192.168.80.2 255.255.252.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 105 ip 192.168.80.1
standby 105 priority 120
standby 105 preempt
interface Vlan110
ip address 192.168.84.2 255.255.252.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 110 ip 192.168.84.1
standby 110 priority 120
standby 110 preempt
interface Vlan115
mac-address 000b.be11.c518
ip address 192.168.88.2 255.255.252.0
ip helper-address 10.50.50.5

```

```

ip helper-address 10.50.50.6
standby 115 ip 192.168.88.1
standby 115 priority 120
standby 115 preempt
interface Vlan200
mac-address 000b.be11.c519
ip address 10.60.0.2 255.255.0.0
ip helper-address 10.50.50.5
ip helper-address 10.50.50.6
standby 200 ip 10.60.0.1
standby 200 priority 120
standby 200 preempt

```

Appendix IV OSPF Configuration

Core switch 1

```

router ospf 15
router-id 2.1.2.1
network 10.10.10.0 0.0.0.3 area 0
network 10.10.10.4 0.0.0.3 area 0
network 192.168.0.0 0.0.3.255 area 0
network 192.168.4.0 0.0.3.255 area 0
network 192.168.8.0 0.0.3.255 area 0
network 192.168.12.0 0.0.3.255 area 0
network 192.168.16.0 0.0.3.255 area 0
network 192.168.20.0 0.0.3.255 area 0
network 192.168.24.0 0.0.3.255 area 0
network 192.168.28.0 0.0.3.255 area 0
network 192.168.32.0 0.0.3.255 area 0
network 192.168.36.0 0.0.3.255 area 0
network 192.168.40.0 0.0.3.255 area 0
network 192.168.44.0 0.0.3.255 area 0
network 192.168.48.0 0.0.3.255 area 0
network 192.168.52.0 0.0.3.255 area 0
network 192.168.56.0 0.0.3.255 area 0
network 192.168.60.0 0.0.3.255 area 0
network 192.168.64.0 0.0.3.255 area 0
network 192.168.68.0 0.0.3.255 area 0
network 192.168.72.0 0.0.3.255 area 0
network 192.168.76.0 0.0.3.255 area 0
network 192.168.80.0 0.0.3.255 area 0
network 192.168.84.0 0.0.3.255 area 0
network 192.168.88.0 0.0.3.255 area 0
network 10.60.0.0 0.0.255.255 area 0
network 172.16.10.0 0.0.0.255 area 0

```

Core switch 2

```

router ospf 15
router-id 2.2.2.2
network 10.10.10.0 0.0.0.3 area 0
network 10.10.10.4 0.0.0.3 area 0
network 192.168.0.0 0.0.3.255 area 0
network 192.168.4.0 0.0.3.255 area 0
network 192.168.8.0 0.0.3.255 area 0
network 192.168.12.0 0.0.3.255 area 0
network 192.168.16.0 0.0.3.255 area 0
network 192.168.20.0 0.0.3.255 area 0
network 192.168.24.0 0.0.3.255 area 0
network 192.168.28.0 0.0.3.255 area 0
network 192.168.32.0 0.0.3.255 area 0
network 192.168.36.0 0.0.3.255 area 0
network 192.168.40.0 0.0.3.255 area 0
network 192.168.44.0 0.0.3.255 area 0
network 192.168.48.0 0.0.3.255 area 0
network 192.168.52.0 0.0.3.255 area 0
network 192.168.56.0 0.0.3.255 area 0
network 192.168.60.0 0.0.3.255 area 0
network 192.168.64.0 0.0.3.255 area 0
network 192.168.68.0 0.0.3.255 area 0
network 192.168.72.0 0.0.3.255 area 0
network 192.168.76.0 0.0.3.255 area 0
network 192.168.80.0 0.0.3.255 area 0
network 192.168.84.0 0.0.3.255 area 0
network 192.168.88.0 0.0.3.255 area 0
network 10.60.0.0 0.0.255.255 area 0
network 172.16.10.0 0.0.0.255 area 0

```

Appendix v Firewall interface security zones and levels configuration

```

interface GigabitEthernet1/1
nameif INSIDE1
security-level 100
ip address 10.10.10.1 255.255.255.252
interface GigabitEthernet1/2
nameif INSIDE2
security-level 100
ip address 10.10.10.5 255.255.255.252
interface GigabitEthernet1/3
nameif OUTSIDE
security-level 0
ip address 10.40.40.2 255.255.255.252

```



```
interface GigabitEthernet1/6
nameif DMZ-FW1
security-level 70
ip address 10.50.50.1 255.255.255.224
```

Appendix VI Firewall inspection policies configuration

```
object network INSIDE1-OUTSIDE
subnet 10.60.0.0 255.255.0.0
nat (INSIDE2,OUTSIDE) dynamic
interface
object network INSIDE10-OUTSIDE
subnet 192.168.32.0 255.255.252.0
nat (INSIDE1,OUTSIDE) dynamic
interface
object network INSIDE10a-OUTSIDE
subnet 192.168.32.0 255.255.252.0
nat (INSIDE2,OUTSIDE) dynamic
interface
object network INSIDE11-OUTSIDE
subnet 192.168.36.0 255.255.252.0
nat (INSIDE1,OUTSIDE) dynamic
interface
object network INSIDE11a-OUTSIDE
subnet 192.168.36.0 255.255.252.0
nat (INSIDE2,OUTSIDE) dynamic
interface
object network INSIDE12-OUTSIDE
subnet 192.168.40.0 255.255.252.0
nat (INSIDE1,OUTSIDE) dynamic
interface
object network INSIDE12a-OUTSIDE
subnet 192.168.40.0 255.255.252.0
nat (INSIDE2,OUTSIDE) dynamic
interface
object network INSIDE13-OUTSIDE
subnet 192.168.44.0 255.255.252.0
nat (INSIDE1,OUTSIDE) dynamic
interface
object network INSIDE13a-OUTSIDE
subnet 192.168.44.0 255.255.252.0
nat (INSIDE2,OUTSIDE) dynamic
interface
object network INSIDE14-OUTSIDE
subnet 192.168.48.0 255.255.252.0
```

```
nat (INSIDE1,OUTSIDE) dynamic
interface
object network INSIDE14a-OUTSIDE
subnet 192.168.48.0 255.255.252.0
nat (INSIDE2,OUTSIDE) dynamic
interface
object network INSIDE15-OUTSIDE
subnet 192.168.52.0 255.255.252.0
nat (INSIDE1,OUTSIDE) dynamic
interface
object network INSIDE15a-OUTSIDE
subnet 192.168.52.0 255.255.252.0
nat (INSIDE2,OUTSIDE) dynamic
interface
object network INSIDE16-OUTSIDE
subnet 192.168.56.0 255.255.252.0
nat (INSIDE1,OUTSIDE) dynamic
interface
object network INSIDE16a-OUTSIDE
subnet 192.168.56.0 255.255.252.0
nat (INSIDE2,OUTSIDE) dynamic
interface
object network INSIDE17-OUTSIDE
subnet 192.168.60.0 255.255.252.0
nat (INSIDE1,OUTSIDE) dynamic
interface
object network INSIDE17a-OUTSIDE
subnet 192.168.60.0 255.255.252.0
nat (INSIDE2,OUTSIDE) dynamic
interface
object network INSIDE18-OUTSIDE
subnet 192.168.64.0 255.255.252.0
nat (INSIDE1,OUTSIDE) dynamic
interface
object network INSIDE18a-OUTSIDE
subnet 192.168.64.0 255.255.252.0
nat (INSIDE2,OUTSIDE) dynamic
interface
object network INSIDE19-OUTSIDE
subnet 192.168.68.0 255.255.252.0
nat (INSIDE1,OUTSIDE) dynamic
interface
object network INSIDE19a-OUTSIDE
subnet 192.168.68.0 255.255.252.0
nat (INSIDE2,OUTSIDE) dynamic
interface
```

object network INSIDE1a-OUTSIDE
 subnet 10.60.0.0 255.255.0.0
 nat (INSIDE2,OUTSIDE) dynamic
 interface
 object network INSIDE2-OUTSIDE
 subnet 192.168.0.0 255.255.252.0
 nat (INSIDE1,OUTSIDE) dynamic
 interface
 object network INSIDE20-OUTSIDE
 subnet 192.168.72.0 255.255.252.0
 nat (INSIDE1,OUTSIDE) dynamic
 interface
 object network INSIDE20a-OUTSIDE
 subnet 192.168.72.0 255.255.252.0
 nat (INSIDE2,OUTSIDE) dynamic
 interface
 object network INSIDE21-OUTSIDE
 subnet 192.168.76.0 255.255.252.0
 nat (INSIDE1,OUTSIDE) dynamic
 interface
 object network INSIDE21a-OUTSIDE
 subnet 192.168.76.0 255.255.252.0
 nat (INSIDE2,OUTSIDE) dynamic
 interface
 object network INSIDE22-OUTSIDE
 subnet 192.168.80.0 255.255.252.0
 nat (INSIDE1,OUTSIDE) dynamic
 interface
 object network INSIDE22a-OUTSIDE
 subnet 192.168.80.0 255.255.252.0
 nat (INSIDE2,OUTSIDE) dynamic
 interface
 object network INSIDE23-OUTSIDE
 subnet 192.168.88.0 255.255.252.0
 nat (INSIDE1,OUTSIDE) dynamic
 interface
 object network INSIDE23a-OUTSIDE
 subnet 192.168.88.0 255.255.252.0
 nat (INSIDE2,OUTSIDE) dynamic
 interface
 object network INSIDE24-OUTSIDE
 object network INSIDE24a-OUTSIDE
 subnet 192.168.0.0 255.255.252.0
 nat (INSIDE2,OUTSIDE) dynamic
 interface
 object network INSIDE2a-OUTSIDE

subnet 192.168.0.0 255.255.252.0
 nat (INSIDE2,OUTSIDE) dynamic
 interface
 object network INSIDE3-OUTSIDE
 subnet 192.168.4.0 255.255.252.0
 nat (INSIDE1,OUTSIDE) dynamic
 interface
 object network INSIDE3a-OUTSIDE
 subnet 192.168.4.0 255.255.252.0
 nat (INSIDE2,OUTSIDE) dynamic
 interface
 object network INSIDE4-OUTSIDE
 subnet 192.168.8.0 255.255.252.0
 nat (INSIDE1,OUTSIDE) dynamic
 interface
 object network INSIDE4a-OUTSIDE
 subnet 192.168.8.0 255.255.252.0
 nat (INSIDE2,OUTSIDE) dynamic
 interface
 object network INSIDE5-OUTSIDE
 subnet 192.168.12.0 255.255.252.0
 nat (INSIDE1,OUTSIDE) dynamic
 interface
 object network INSIDE5a-OUTSIDE
 subnet 192.168.12.0 255.255.252.0
 nat (INSIDE2,OUTSIDE) dynamic
 interface
 object network INSIDE6-OUTSIDE
 subnet 192.168.16.0 255.255.252.0
 nat (INSIDE1,OUTSIDE) dynamic
 interface
 object network INSIDE6a-OUTSIDE
 subnet 192.168.16.0 255.255.252.0
 nat (INSIDE2,OUTSIDE) dynamic
 interface
 object network INSIDE7-OUTSIDE
 subnet 192.168.20.0 255.255.252.0
 nat (INSIDE1,OUTSIDE) dynamic
 interface
 object network INSIDE7a-OUTSIDE
 subnet 192.168.20.0 255.255.252.0
 nat (INSIDE2,OUTSIDE) dynamic
 interface
 object network INSIDE8-OUTSIDE
 subnet 192.168.24.0 255.255.252.0

```
nat (INSIDE1,OUTSIDE) dynamic
interface
object network INSIDE8a-OUTSIDE
subnet 192.168.24.0 255.255.252.0
nat (INSIDE2,OUTSIDE) dynamic
interface
object network INSIDE9-OUTSIDE
subnet 192.168.28.0 255.255.252.0
nat (INSIDE1,OUTSIDE) dynamic
interface
object network INSIDE9a-OUTSIDE
subnet 192.168.28.0 255.255.252.0
nat (INSIDE2,OUTSIDE) dynamic
interface
route OUTSIDE 0.0.0.0 0.0.0.0
10.40.40.1 1
access-list res-access extended permit
icmp any any
access-list res-access extended permit
udp any any eq bootps
access-list res-access extended permit
udp any any eq bootpc
access-list res-access extended permit
udp any any eq domain
access-list res-access extended permit
tcp any any eq domain
access-list res-access extended permit
tcp any any eq www
access-list res-access extended permit
tcp any any eq smtp
access-list res-access extended permit
tcp any any eq 20
access-list res-access extended permit
tcp any any eq ftp
access-group res-access in interface
DMZ-FW1
access-group res-access in interface
OUTSIDE
access-group res-access in interface
INSIDE1
aaa authentication ssh console LOCAL
```