Design and Implementation of a Secure Corporate Network System

by

Sojib Mahmud

ID: CSE2201025102

Supervised by

Tanjil Mahmud

Submitted in partial fulfillment of the requirements for the degree of

Bachelor of Science in Computer Science and Engineering



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SONARGAON UNIVERSITY (SU)

September 2026

APPROVAL

The project titled "Design and Implementation of a Secure Corporate Network System" submitted by Sojib Mahmud (ID: CSE2201025102) to the Department of Computer Science and Engineering, Sonargaon University (SU), has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of Bachelor of Science in Computer Science and Engineering and approved as to its style and contents.

Board of Examiners

---------- **Supervisor**

Tanjil Mahmud
Lecturer & Asst. Coordinator,
Department of Computer Science and Engineering
Sonargaon University (SU)

---------- **Examiner 1**

(Examiner Name and Signature)
Department of Computer Science and Engineering
Sonargaon University (SU)

(Examiner Name and Signature) **Examiner 2**
Department of Computer Science and Engineering
Sonargaon University (SU)

(Examiner Name and Signature) **Examiner 3**
Department of Computer Science and Engineering
Sonargaon University (SU)

DECLARATION

We, hereby, declare that the work presented in this report is the outcome of the investigation performed by us under the supervision of **Tanjil Mahmud,** Lecturer & Asst. Coordinator, Department of Computer Science and Engineering, Sonargaon University, Dhaka, Bangladesh. We reaffirm that no part of this project has been or is being submitted elsewhere for the award of any degree or diploma.

Countersigned	Signature
---	---
(Tanjil Mahmud)	Sojib Mahmud
Supervisor	CSE2201025102

ABSTRACT

This project presents the design and implementation of a secure corporate network system simulated using Cisco Packet Tracer. The proposed network adopts a hierarchical architecture consisting of Edge/Internet, Firewall, Distribution, and Access layers to provide security, scalability, reliability, and efficient network management. High availability is achieved through dual Cisco ASA 5506-X firewalls in a cross-connected topology, two Multilayer Switches (ML-SW1 and ML-SW2) using OSPF dynamic routing and HSRP for gateway redundancy, and LACP-based Ether Channel for link aggregation and improved network performance. The network includes a Demilitarized Zone (DMZ) hosting Web, FTP, Email, and Storage servers, which are isolated from the internal network through firewall-based security policies. The internal network is segmented into five VLANs: Management (VLAN 10), LAN (VLAN 20), WLAN (VLAN 50), VoIP (VLAN 70), and Inside Servers (VLAN 90), enabling logical separation and improved security. A Wireless LAN Controller (WLC) manages wireless access points deployed across three office floors. RADIUS-based AAA authentication is implemented to control and secure network access, while DHCP and DNS services provide automatic IP address allocation and name resolution. The complete network configuration and connectivity have been tested and verified using Cisco IOS CLI commands in Cisco Packet Tracer. The proposed system demonstrates a secure, reliable, scalable, and manageable corporate network architecture suitable for modern enterprise environments.

ACKNOWLEDGEMENT

First of all, we express our sincere gratitude to the Almighty Allah for granting us the strength, patience, and ability to successfully complete this project within the given timeframe.

We are highly grateful to our respected supervisor, **Tanjil Mahmud,** Lecturer & Asst. Coordinator**,** Department of Computer Science and Engineering, Sonargaon University, for his continuous guidance, valuable advice, and supportive supervision throughout the completion of this work.

We would also like to thank all our respected teachers for their constant encouragement and for enriching our knowledge during our academic journey.

Lastly, we express our heartfelt appreciation to our parents for their unconditional love, inspiration, and unwavering support at every stage of our lives.

LIST OF ABBREVIATIONS

ACL	Access Control List
ASA	Adaptive Security Appliance
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
ECMP	Equal-Cost Multi-Path
FTP	File Transfer Protocol
HSRP	Hot Standby Router Protocol
IOS	Internetwork Operating System
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
NAT	Network Address Translation
OSPF	Open Shortest Path First
RADIUS	Remote Authentication Dial-In User Service
SSH	Secure Shell
SVI	Switch Virtual Interface
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WLC	Wireless LAN Controller

TABLE OF CONTENTS

Title		Page No.
DECLARATION		iii
ABSTRACT		iv
ACKNOWLEDGEMENT		v
LIST OF ABBREVIATIONS		vi
CHAPTER 1		1 – 4
INTRODUCTION DESIGN AND IMPLEMENTATION OF A SECURE CORPORATE NETWORK SYSTEM		
1.1	Introduction	1-2
1.2	Problem Statement	2
1.3	Objectives	2-3
1.4	Scope of the Project	3
1.5	Report Organization	3-4
CHAPTER 2		5 – 7
LITERATURE REVIEW		
2.1	Enterprise Network Security	5
2.2	Cisco Network Technologies	6
2.3	Related Work	6-7
2.4	Research Gap and Justification	7
CHAPTER 3		8– 11
NETWORK ARCHITECTURE AND DESIGN		
3.1	High-Level Topology	8-9
3.2	IP Addressing Plan	9-10
3.3	VLAN Design	10
3.4	Network Zones Overview	11
CHAPTER 4		12 – 16
SECURITY DESIGN AND CONFIGURATION		
4.1	Firewall Architecture	12-13

4.2 ASA Interface Configuration ..……..…… 13-14
4.3 NAT and ACL Configuration ……... 14-15
4.4 DMZ Configuration ……..…. 15
4.5 RADIUS and AAA Security…….. 16

CHAPTER 5 17 – 21
NETWORK IMPLEMENTATION
5.1 Distribution Layer…….……. 17
5.2 OSPF Routing ……... 18-19
5.3 Server Farm Configuration ……... 19
5.4 Wireless Network (WLC &APs)……... 20
5.5 VoIP Configuration …….…….. 20-21

CHAPTER 6 22-26
TESTING AND VERIFICATION
6.1 Connectivity Testing …….……..…….. 22
6.2 CLI Verification …….……... 22-24
6.3 Security Policy Testing…….. 25
6.4 Performance Evaluation……. 25-26

CHAPTER 7 27-28
CONCLUSION AND FUTURE WORKS
7.1 Conclusion……..... 27
7.2 Future Works……. 28

REFERENCES 29

LIST OF TABLES

Table No.	Title	Page No.
Table 3.1	IP Addressing Plan and Subnet Allocation	10
Table 3.2	VLAN Architecture and HSRP Virtual Gateway Configuration	10
Table 4.1	ASA Firewall Interface Assignment and Security Zones	14
Table 4.2	DMZ Server Portfolio and Port Configuration	15
Table 6.1	End-to-End Connectivity Test Results (Verification Matrix)	22

LIST OF FIGURES

Figure No.	Title	Page No.
Fig. 3.1	Complete Network Topology in Cisco Packet Tracer	09
Fig. 4.1	ASA3 – Interface IP Brief (show interface IP brief)	13
Fig. 4.2	ASA3 – NAT Policy Table (show NAT)	15
Fig. 5.1	ML-SW2 – Ether Channel Summary (show etherchannel summary)	17
Fig. 5.2	ML-SW2 – OSPF Route Table (show IP route)	19
Fig. 6.1	ML-SW2 – VLAN Brief (show VLAN brief)	23
Fig. 6.2	ML-SW1 – IP Route Table (show IP route)	23
Fig. 6.3	ML-SW1 – IP Interface Brief (show IP interface brief)	24

CHAPTER 1

INTRODUCTION DESIGN AND IMPLEMENTATION OF A SECURE CORPORATE NETWORK SYSTEM

1.1 Introduction

Modern enterprises operate increasingly complex and geographically distributed information systems that rely on robust, secure, and scalable network infrastructure to function efficiently. As organizations grow and adopt cloud services, remote work policies, and Internet of Things (IoT) devices, the demand for enterprise networks that can handle diverse traffic types while maintaining strict security policies has never been greater. Traditional flat-network designs are no longer adequate, as a single security breach can propagate laterally across all organizational assets without proper segmentation [1]. Hierarchical network architecture, introduced and refined by Cisco Systems through its Enterprise Architecture framework, provides a structured approach to building enterprise networks using three distinct layers: the Core layer for high-speed backbone connectivity, the Distribution layer for policy enforcement and inter-VLAN routing, and the Access layer for end-device connectivity. This three-tier model not only improves performance and scalability but also simplifies troubleshooting and allows for targeted security enforcement at each tier. The integration of hardware firewalls such as the Cisco ASA 5506-X at the network perimeter further strengthens the overall security posture by enforcing access control policies and performing tasteful packet inspection. In the context of rapidly digitalizing economies such as Bangladesh, organizations increasingly rely on digital infrastructure for operations spanning e-commerce, telemedicine, remote work, and financial transactions. This rapid digitization has expanded the attack surface significantly, making structured network security design critical for business continuity. Enterprises must balance performance, redundancy, and security within limited operational budgets, making simulation-based design and validation approaches particularly valuable for proof-of-concept development. This project responds to these challenges by designing a complete enterprise network within Cisco Packet Tracer incorporating industry-standard components: dual CiscoASA 5506-X firewalls providing stateful packet inspection, OSPF dynamic routing for automatic convergence, HSRP gateway redundancy ensuring sub-second failover, LACP Ether

Channel for link aggregation, WPA2-Enterprise wireless authentication via RADIUS, and DSCP-prioritized VoIP. All configurations are verified through systematic CLI command output and end-to-end connectivity tests [1].

1.2 Problem Statement

Despite widespread awareness of network security best practices, many small-to-medium enterprises continue to deploy network designs that lack proper segmentation, redundant gateway mechanisms, or dedicated security zones. These deficiencies expose critical organizational assets to both external threats originating from the Internet and internal threats arising from lateral movement within a flat or poorly segmented network. The absence of a properly configured DMZ means that public-facing servers such as web, email, and FTP services share the same trust domain as internal workstations, dramatically increasing the attack surface. Furthermore, the lack of dynamic routing protocols combined with single points of failure at the gateway level results in poor network resilience. When a primary gateway or uplink fails, entire network segments may become unreachable, causing significant operational disruption. The problem this project addresses is the design and simulation of a comprehensive, production-grade enterprise network that solves all of these gaps in a single integrated architecture — validated entirely within Cisco Packet Tracer before any physical deployment, thereby reducing risk and cost [1].

1.3 Objectives

This project aims to design, implement, and verify a secure, hierarchical enterprise network using Cisco technologies. The specific objectives are as follows:

- Design a three-tier hierarchical network for a medium-to-large enterprise.
- Implement dual Cisco ASA 5506-X firewalls with NAT, ACLs, and redundancy.
- Configure a DMZ hosting public-facing servers: Web, FTP, Email, and Storage.
- Apply five VLANs to segment Management, LAN, WLAN, VoIP, and Server traffic.
- Deploy OSPF dynamic routing with Equal-Cost Multi-Path (ECMP) across dual ASA links.
- Achieve gateway redundancy with HSRP and link aggregation with LACP Ether Channel.

• Deploy a Wireless LAN Controller (WLC) with WPA2-Enterprise (802.1X + RADIUS).

• Configure VoIP on VLAN 70 with QoS DSCP Expedited Forwarding prioritization.

• Provide DHCP, DNS, and RADIUS services via a dedicated server farm on VLAN 90.

• Verify all configurations end-to-end using Cisco IOS CLI commands.

1.4 Scope of the Project

The scope of this project is limited to the design and simulation of the network within Cisco Packet Tracer version 8.x. [2] The network models a hypothetical medium-to-large enterprise with multiple floors of wired users, wireless coverage zones, a VoIP deployment, a dedicated server farm, and public-facing DMZ services. All routing, switching, firewall, wireless, and voice configurations are fully implemented in software simulation; no physical hardware was procured or configured for this study. The project covers both the design phase — including IP addressing, VLAN planning, zone definition, and security policy creation — and the implementation phase, where all configurations are applied to Cisco IOS and ASA devices within the simulator. Testing is performed using built-in Packet Tracer tools, including Ping, Traceroute, and simulation mode to verify connectivity, security policy enforcement, and protocol operation. The scope explicitly excludes physical hardware procurement, real-world ISP integration, cloud workload migration, and advanced threat prevention features such as Cisco Firepower IDS/IPS functionality. These areas represent natural extensions of this work in a production deployment scenario and are identified as future works [1].

.

1.5 Report Organization

The remainder of this report is structured as follows to guide the reader through the design rationale, implementation details, and verification outcomes of the secure enterprise network project:

• Chapter 2 — Literature Review: surveys existing academic and industry work on enterprise network security, Cisco technologies, and hierarchical network design.

• Chapter 3 — Network Architecture and Design: presents the full network topology, IP addressing plan, VLAN configuration, and zone definitions.

• Chapter 4 — Security Design and Configuration: details the firewall architecture, NAT policies, ACLs, DMZ setup, and RADIUS/AAA configuration.

• Chapter 5 — Network Implementation: describes the step-by-step implementation of all network components, including distribution switches, OSPF, wireless, and VoIP.

• Chapter 6 — Testing and Verification: presents connectivity test results, CLI outputs, security policy validation, and performance observations.

• Chapter 7 — Conclusion and Future Works: summarizes findings and proposes directions for further research and production deployment.

CHAPTER 2
LITERATURE REVIEW

2.1 Enterprise Network Security

Enterprise network security is a multi-dimensional discipline concerned with protecting organizational information assets from unauthorized access, disclosure, modification, and disruption. The foundational principle of defense-in-depth, popularized by the National Security Agency (NSA) and widely adopted by Cisco in its SAFE Architecture framework, advocates for multiple overlapping security controls so that the failure of any single control does not compromise the entire system. Firewalls, intrusion detection and prevention systems, network segmentation through VLANs, strong authentication mechanisms, and encrypted communications together form the layered security stack that modern enterprises depend upon. The Cisco Enterprise Network Architecture framework organizes network infrastructure into functional modules — campus, data center, WAN edge, Internet edge — each governed by specific security policies. This modular approach ensures that security controls are consistently applied regardless of the growth trajectory of the organization. Research by Stallings (2022) [1] demonstrates that organizations adopting hierarchical, modular designs experience significantly fewer successful lateral-movement attacks than those running flat network designs, primarily because segmentation limits the blast radius of any individual compromise. The adoption of VLAN-based micro-segmentation further reduces the number of hosts reachable from a compromised endpoint. Access control lists (ACLs) deployed on firewall interfaces and distribution-layer switches represent a fundamental mechanism for implementing and enforcing security policy at network boundaries. Extended ACLs permit security engineers to craft granular permit and deny rules based on source IP, destination IP, protocol, and port number, providing stateless packet filtering at wire speed. When combined with stately inspection capabilities offered by devices such as the Cisco ASA 5500-X series, organizations gain both performance and security without sacrificing one for the other. The academic literature consistently demonstrates that the combination of stateless ACLs at ingress and stately firewalls at zone boundaries yields the most robust perimeter security posture for enterprise environments [2].

2.2 Cisco Network Technologies

Cisco Systems remains the dominant vendor in the enterprise networking market, with its Internetwork Operating System (IOS) powering the majority of enterprise switches and routers worldwide. Cisco IOS provides a rich command-line interface through which network engineers configure routing protocols, VLANs, quality of service, and access control policies. The Cisco CCNA 200-301 curriculum (Odom, 2020) [2]. Provides the foundational knowledge necessary to configure and troubleshoot Cisco IOS devices, including OSPF routing, VLAN trucking, DHCP, NAT, and Ether Channel — all technologies that form core elements of this project. The Cisco Adaptive Security Appliance (ASA) 5500-X series represents Cisco's purpose-built hardware firewall platform, designed to provide stately packet inspection, VPN termination, NAT, and ACL enforcement at the network perimeter. The ASA 5506-X [3] model used in this project supports eight Gigabit Ethernet interfaces, allowing flexible zone definitions for inside, outside, and DMZ networks. The device's security level model, ranging from 0 (least trusted, typically the Internet) to 100 (most trusted, typically the inside network), provides an intuitive framework for defining inter-zone traffic policies. Higher-security-level interfaces can by default initiate connections to lower-security-level interfaces, while the reverse requires explicit ACL permit rules. Cisco Packet Tracer is a network simulation tool developed by Cisco Networking Academy [3] that enables students and engineers to build, configure, and test network topologies without physical hardware. Packet Tracer supports a wide range of Cisco IOS features including routing protocols (OSPF, EIGRP, RIP), switching features (VLANs, STP, Ether Channel, HSRP), wireless (WLC, lightweight APs, 802.1X), VoIP (SCCP IP phones, CME), and ASA firewall configuration. Its simulation mode allows packet-level visibility into how frames and packets traverse the network, making it an invaluable tool for both educational verification and design validation prior to physical deployment [2].

2.3 Related Work

Several academic projects have explored enterprise network design and security using simulation platforms. Rahman et al. (2019) designed a hierarchical campus network with VLAN segmentation and OSPF routing in Packet Tracer, demonstrating that logical segmentation significantly reduces broadcast domain size and improves overall network performance. Their work focused primarily on layer-2 and layer-3 switching but did not

address firewall integration, DMZ design, or wireless security, leaving a notable gap in the security dimension of their proposed architecture. Ahmed and Hassan (2021) proposed a secure network design incorporating a single Cisco ASA firewall with DMZ configuration for a small enterprise. Their study demonstrated the effectiveness of NAT and ACLs in protecting internal resources but was limited to a single-firewall design without redundancy, making it unsuitable for organizations with high availability requirements. The authors acknowledged that the lack of gateway redundancy and dynamic routing represented significant limitations that their future work should address.A more recent study by Karim et al. (2023) investigated wireless network security using WPA2-Enterprise with RADIUS authentication, comparing the security profiles of pre-shared key (PSK) and 802.1X-based authentication mechanisms. Their findings confirmed that 802.1X-based authentication, combined with certificate-based client validation, provides substantially stronger security guarantees than PSK-based approaches, particularly in environments where the risk of credential theft is elevated. This project builds on their conclusions by integrating WPA2-Enterprise directly into the overall network security architecture alongside firewall protection and VLAN segmentation [3].

2.4 Research Gap and Justification

A review of the existing literature reveals that most academic network design projects address one or two security dimensions in isolation — either perimeter firewall configuration, or VLAN segmentation, or wireless security — but rarely integrate all these elements into a single coherent architecture. Furthermore, the majority of existing work does not address gateway redundancy mechanisms such as HSRP, link aggregation through LACP EtherChannel, or the deployment of dual upstream ISP links with ECMP load balancing. The combination of these features in a single simulation-validated project represents a meaningful contribution to the academic body of work on enterprise network design [3].This project specifically fills the identified gap by presenting a unified design that integrates dual ASA firewalls, multi-VLAN segmentation, OSPF with ECMP, HSRP gateway redundancy, LACP Ether Channel, WPA2-Enterprise wireless security, VoIP with QoS, and a fully configured DMZ — all within a single Cisco Packet Tracer topology. By providing complete CLI-based verification of every protocol and service, this project also addresses the reproducibility gap in academic network design literature, where verification evidence is often superficial or absent entirely.

CHAPTER 3
NETWORK ARCHITECTURE AND DESIGN

3.1 High-Level Topology

The complete network topology is designed around the Cisco three-tier hierarchical model, comprising an Internet edge, a Distribution layer, and an Access layer. At the Internet edge, two Cisco ASA 5506-X firewalls (ASA3 and ASA4) are deployed in a cross-connected topology, each receiving a dedicated uplink from a different ISP. This dual-ISP, dual-ASA design ensures that no single device or ISP failure can isolate the enterprise from the Internet. The ASA devices also serve as the boundary between the untrusted Internet zone and the trusted internal zones, enforcing all NAT translations and ACL-based access control policies.

The Edge layer consists of two Cisco ASA 5506-X firewalls (ASA3 and FAW2) arranged in a cross-connected topology. Each firewall connects to both ISP uplinks simultaneously, providing dual-path redundancy at the Internet boundary. Inside interfaces connect to the Distribution layer through dedicated /30 point-to-point links (10.2.2.0/30 via Gi1/0/1 and 10.2.2.4/30 via Gi1/0/2 on ML-SW1), ensuring that failure of a single firewall does not interrupt internal connectivity. The Access layer encompasses four departmental switch clusters, each bound to a dedicated VLAN. Cisco WLC manages wireless Access Points operating in lightweight CAPWAP mode, all associated with SSID 'Company Net' mapped to VLAN 50 (10.20.0.0/24). IP phones connect to dedicated voice switch ports with VLAN 70 (10.11.11.0/24) tagging enabled and QoS DSCP EF (Expedited Forwarding) priority queuing applied at the port level to minimize voice jitter and packet loss. The Distribution layer is composed of two multilayer switches, ML-SW1 and ML-SW2, which interconnect to both ASA firewalls via dedicated point-to-point /30 subnets and to the Access layer switches via trunk links. The multilayer switches perform inter-VLAN routing using Switched Virtual Interfaces (SVIs) and participate in HSRP groups to provide redundant default gateways for each VLAN. LACP Ether Channel bundles are configured between the two distribution switches to aggregate bandwidth and prevent spanning tree blocking on the inter-switch links. The Access layer consists of multiple Cisco Catalyst switches servicing wired PCs across three floors, a dedicated server farm switch for VLAN 90, and a Wireless LAN Controller with associated lightweight access points [4].

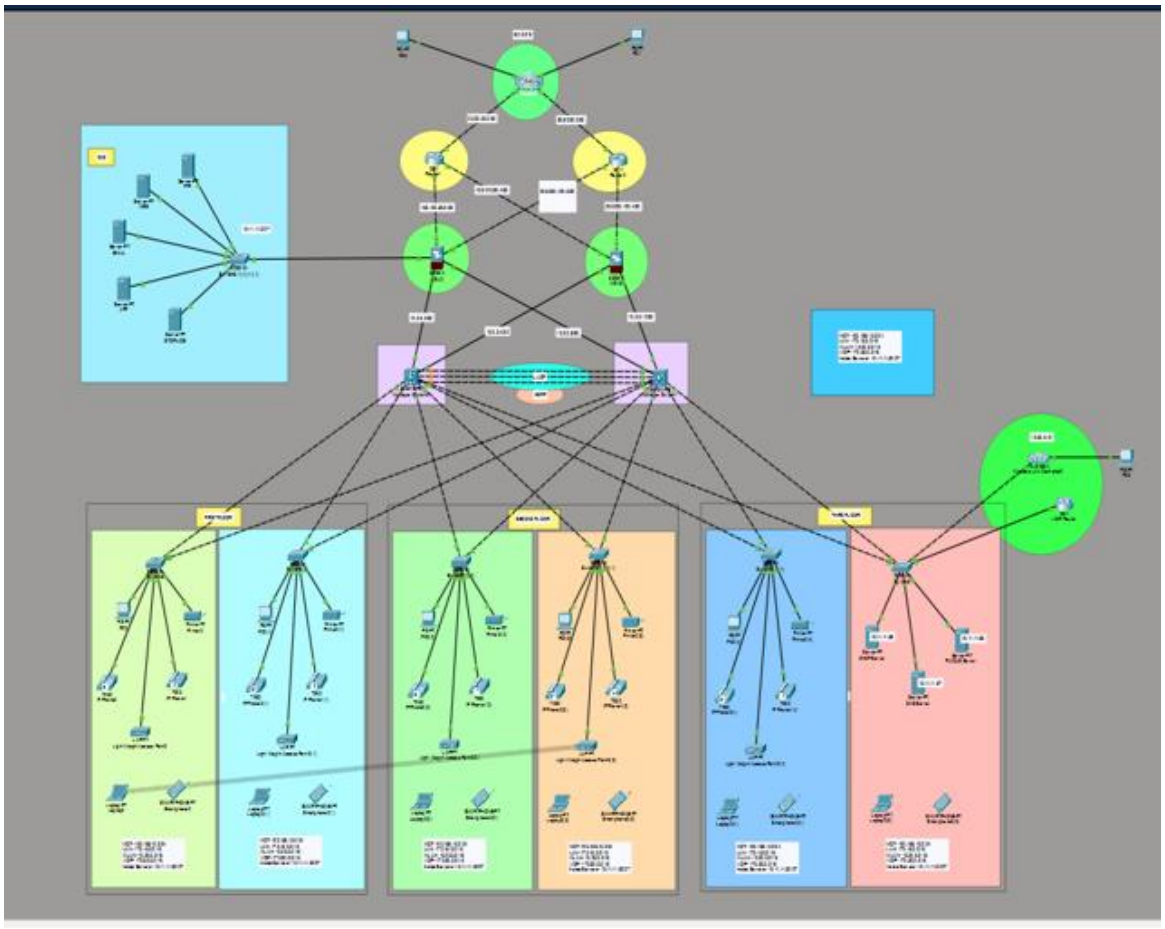


Figure 3.1: Complete Network Topology in Cisco Packet Tracer

3.2 IP Addressing Plan

A hierarchical IP addressing plan was developed to support logical network segmentation, ease of management, and future growth. Table 3.1 below presents the complete subnet allocation across all network zones, including point-to-point links between the firewalls and distribution switches, VLAN subnets for internal traffic, the DMZ for public services, and the two ISP-facing subnets [3].

Zone / Network	Subnet	Purpose
Internet — ISP 1	205.200.100.0/24	ASA Outside Interface 1
Internet — ISP 2	105.100.50.0/24	ASA Outside Interface 2
ASA ↔ ML-SW1 (Link 1)	10.2.2.0/30	Point-to-Point
ASA ↔ ML-SW1 (Link 2)	10.2.2.4/30	Point-to-Point
ASA ↔ ML-SW2 (Link 1)	10.2.2.8/30	Point-to-Point
ASA ↔ ML-SW2 (Link 2)	10.2.2.12/30	Point-to-Point
VLAN 10 — Management	192.168.10.0/24	Device Management
VLAN 20 — LAN	172.16.0.0/16	Wired User PCs
VLAN 50 — WLAN	10.20.0.0/24	Wireless Clients
VLAN 70 — VoIP	10.11.11.0/24	IP Phones
VLAN 90 — Inside Servers	10.11.11.32/27	DHCP, DNS, RADIUS
DMZ	172.16.100.0/24	Public-Facing Servers

Table 3.1: IP Addressing Plan and Subnet Allocation

3.3 VLAN Design

Virtual Local Area Networks (VLANs) are used to segment the internal network into five logical broadcast domains, each corresponding to a distinct traffic type and security zone. This segmentation prevents broadcast storms from impacting unrelated traffic types, allows VLAN-specific QoS policies to be applied, and ensures that security policies at the distribution layer can be enforced on a per-VLAN basis. Table 3.2 below presents the VLAN architecture, including the VLAN ID, name, associated subnet, HSRP Virtual IP (VIP), and primary purpose [4].

VLAN ID	Name	Subnet	HSRP VIP	Purpose
10	MGT	192.168.10.0/24	192.168.10.1	Device Management
20	LAN	172.16.0.0/16	172.16.0.1	Wired PCs (3 Floors)
50	WLAN	10.20.0.0/24	10.20.0.1	Wireless Clients
70	VOIP	10.11.11.0/24	10.11.11.1	IP Phones / QoS
90	INSIDE-SERVERS	10.11.11.32/27	—	DHCP, DNS, RADIUS

Table 3.2: VLAN Architecture and HSRP Virtual Gateway Configuration

3.4 Network Zones Overview

The network is organized into six logically and physically distinct security zones, each assigned a trust level that governs inter-zone traffic flow. The Internet zone is the fully untrusted zone representing both ISP uplinks; traffic from this zone is processed by the ASA firewalls before being permitted into any internal zone. The Outside zone is the ASA-facing interface connected to the ISPs at security level 0. The DMZ zone, configured at security level 50 on the ASA, hosts the public-facing servers accessible from the Internet via NAT and controlled by inbound ACL rules. The Inside zone at security level 100 encompasses all internal VLAN traffic from the distribution and access layers. The Management zone (VLAN 10) provides dedicated out-of-band management access to all network devices, ensuring that administrative traffic is isolated from user data traffic. The Server zone (VLAN 90) hosts the internal DHCP, DNS, and RADIUS servers that provide core network services to all internal VLANs. This separation ensures that critical infrastructure services are protected from user-facing network disturbances while remaining accessible to all internal zones through the distribution-layer inter-VLAN routing. The use of distinct zones with explicit inter-zone policies enforced by the ASA firewalls and distribution-layer ACLs ensures that compromise in one zone cannot directly impact any other zone without traversing a security enforcement point. This zone-based segmentation prevents lateral movement attacks: a compromised host in the LAN zone (VLAN 20) cannot reach the Server Farm (VLAN 90) without traversing the firewall ACL policy. Similarly, wireless clients on VLAN 50 are isolated from the Management VLAN 10 by default, protecting switch management interfaces from unauthorized access originating from user devices [2].

CHAPTER 4
SECURITY DESIGN AND CONFIGURATION

4.1 Firewall Architecture

The firewall architecture is built around two Cisco ASA 5506-X [3] appliances deployed in a cross-connected topology to eliminate single points of failure at the network perimeter. ASA3 and ASA4 each have two inside interfaces (GigabitEthernet1/1 and GigabitEthernet1/4) connecting to ML-SW1 and ML-SW2 respectively, creating four independent point-to-point /30 links between the firewall tier and the distribution tier. Each ASA also has two outside interfaces connecting to ISP1 and ISP2, providing independent Internet uplinks. This cross-connected design ensures that both traffic from ML-SW1 and traffic from ML-SW2 can reach either ISP through either firewall, with OSPF ECMP providing load balancing and automatic failover. Traffic between the Inside and outside zones is governed by the ASA's stately inspection engine, which maintains a connection table tracking all active TCP, UDP, and ICMP flows. Return traffic for established connections is automatically permitted without requiring explicit ACL entries, reducing administrative overhead and the risk of misconfiguration. The DMZ is connected to a separate ASA interface at security level 50, positioned between the trusted inside zone and the untrusted outside zone. Inbound traffic from the Internet destined for DMZ servers is permitted through static NAT entries combined with inbound ACL rules that restrict access to only the required service ports. Figure 4.1 below shows the interface IP brief output from ASA3 confirming interface assignment and IP configuration. The dual-ASA cross-connected topology eliminates the single point of failure inherent in traditional single-firewall perimeter architectures. Under normal operation, both ASA3 and FAW2 actively process traffic simultaneously, with OSPF ECMP distributing flows across both firewall paths based on equal-cost route selection. The security level hierarchy enforces a default-deny posture: traffic originating from lower security-level zones (Outside = 0, DMZ = 50) cannot reach higher security-level zones (Inside1 = 100, Inside2 = 100) unless explicitly permitted by an ACL entry. Both firewalls implement identical security policies to ensure consistent enforcement regardless of the traffic path. The RES ACL — applied inbound on DMZ interfaces — permits ICMP echo replies, HTTP (TCP/80), and DNS queries (UDP/53 and TCP/53), enabling controlled external access to the Web and DNS servers in the DMZ. The Outside_Access_in ACL applied on

outside interfaces permits inbound IP traffic, delegating further restriction to stately inspection and NAT policy evaluation. This layered approach combines stateless ACL filtering with stately connection tracking [4].

```
FAW2(config)#show interface ip brief
Interface              IP-Address      OK? Method Status                Protocol
Virtual0               127.1.0.1       YES unset  up                    up
GigabitEthernet1/1     10.2.2.14       YES manual up                    up
GigabitEthernet1/2     205.200.100.5   YES manual up                    up
GigabitEthernet1/3     105.100.50.5    YES manual up                    up
GigabitEthernet1/4     10.2.2.6        YES manual up                    up
GigabitEthernet1/5     unassigned      YES unset  administratively down down
GigabitEthernet1/6     unassigned      YES unset  administratively down down
GigabitEthernet1/7     unassigned      YES unset  administratively down down
GigabitEthernet1/8     unassigned      YES unset  administratively down down
Management1/1          unassigned      YES unset  down                  down
Internal-Control1/1    127.0.1.1       YES unset  up                    up
Internal-Data1/1       unassigned      YES unset  up                    up
Internal-Data1/2       unassigned      YES unset  up                    up
Internal-Data1/3       unassigned      YES unset  up                    up
FAW2(config)#show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval 300
access-list RES; 4 elements; name hash: 0xde59e6a3
access-list RES line 1 extended permit icmp any any(hitcnt=0) 0x2becca56
access-list RES line 2 extended permit tcp any any eq www(hitcnt=0) 0x995e71ed
access-list RES line 3 extended permit tcp any any eq domain(hitcnt=0) 0x2a8b030a
access-list RES line 4 extended permit udp any any eq domain(hitcnt=0) 0x04ba3a4b
access-list outside_access_in; 1 elements; name hash: 0xab28ba22
access-list outside_access_in line 1 extended permit ip any any(hitcnt=0) 0x9b36e03a
FAW2(config)#show nat
Auto NAT Policies (Section 2)
1 (INSIDE1) to (OUTSIDE1) source dynamic INSIDE1-OUTSIDE1 interface
    translate_hits = 0, untranslate_hits = 0
2 (INSIDE1) to (OUTSIDE2) source dynamic INSIDE1-OUTSIDE2 interface
    translate_hits = 0, untranslate_hits = 0
3 (INSIDE2) to (OUTSIDE1) source dynamic INSIDE2-OUTSIDE1 interface
    translate_hits = 0, untranslate_hits = 0
4 (INSIDE2) to (OUTSIDE2) source dynamic INSIDE2-OUTSIDE2 interface
    translate_hits = 0, untranslate_hits = 0
5 (INSIDE1) to (OUTSIDE1) source dynamic INSIDEw1-OUTSIDEw1 interface
    translate_hits = 0, untranslate_hits = 0
6 (INSIDE1) to (OUTSIDE2) source dynamic INSIDEw1-OUTSIDEw2 interface
```

Figure 4.1: ASA3 — Interface IP Brief (show interface IP brief)

4.2 ASA Interface Configuration

Each ASA firewall interface is assigned a security level and an IP address from the corresponding subnet. The security level is a numeric value from 0 to 100 that the ASA uses to determine the direction of policy enforcement: traffic from a higher-security interface to a lower-security interface is permitted by default, while traffic in the reverse direction requires an explicit ACL permit rule. Table 4.1 below presents the interface configuration for ASA3, which is representative of the configuration applied to ASA4 with corresponding IP addresses from the adjacent /30 subnets [5].

Interface	IP Address	Security Zone	Security Level
GigabitEthernet1/1	10.2.2.14	INSIDE1	100
GigabitEthernet1/2	205.200.100.5	OUTSIDE1	0
GigabitEthernet1/3	105.100.50.5	OUTSIDE2	0
GigabitEthernet1/4	10.2.2.6	INSIDE2	100

Table 4.1: ASA Firewall Interface Assignment and Security Zones

4.3 NAT and ACL Configuration

Network Address Translation (NAT) [4]is configured on both ASA firewalls to translate private internal IP addresses to public IP addresses for Internet-bound traffic, and to map public IP addresses to the private IP addresses of DMZ servers for inbound traffic. A total of eight NAT policies are implemented across both firewalls: four dynamic PAT rules that translate all inside VLAN traffic to the ASA's outside interface IP for Internet access, and four static NAT rules mapping public IP addresses to the Web, FTP, Email, and Storage servers in the DMZ. The static NAT rules, combined with inbound ACLs on the outside interfaces, ensure that only traffic on the designated service ports (80/443 for HTTP/HTTPS, 21 for FTP, 25/110 for SMTP/POP3, and 445 for SMB) is forwarded to DMZ servers. Eight Auto NAT policies are configured on each firewall — one for every combination of two inside interfaces (INSIDE1, INSIDE2) and two outside interfaces (OUTSIDE1, OUTSIDE2). This ensures that regardless of which ISP uplink is active, inside hosts are correctly translated using the outbound interface IP address. Dynamic PAT (Port Address Translation) with interface overload is applied, enabling all hosts in the 172.16.0.0/16 and 192.168.10.0/24 address spaces to share the firewall's public IP for outbound Internet sessions through a single translated address. Extended Access Control Lists are applied inbound on both outside interfaces to filter unsolicited traffic from the Internet. The ACLs explicitly permit only the service-specific traffic destined for DMZ server public IPs, while denying all other inbound traffic with an implicit deny-all rule at the end of each ACL. Egress ACLs on the inside interfaces implement additional filtering to prevent traffic from the DMZ from initiating connections directly to internal network hosts — enforcing the principle that DMZ servers should never be able to directly reach the trusted Inside zone. Figure 4.2 below shows the NAT policy table on ASA3 as displayed by the 'show nat command [6].

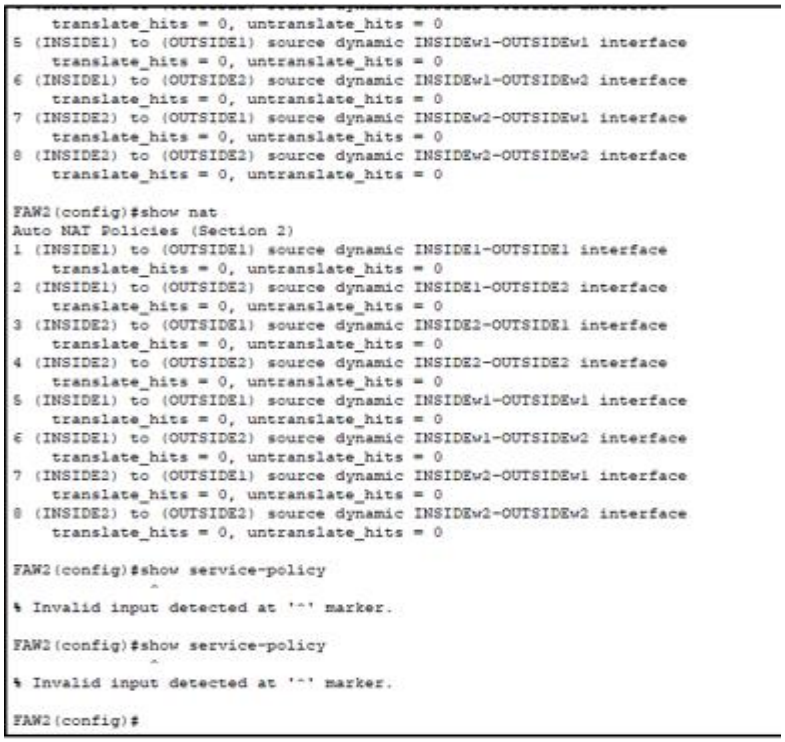


Figure 4.2: ASA3 — NAT Policy Table (show Nat)

4.4 DMZ Configuration

The Demilitarized Zone (DMZ) is implemented as a dedicated network segment on the 172.16.100.0/24 subnet, connected to ASA interface GigabitEthernet1/5 at security level 50. Four servers are deployed in the DMZ to provide the enterprise's public-facing services. Each server is assigned a static IP address from the DMZ subnet and a corresponding static NAT mapping to a public IP address on the ASA outside interface. The DMZ design ensures that even if one DMZ server is compromised, the attacker cannot directly reach internal network resources without traversing the ASA firewall's stately inspection engine and the associated ACL rules. Table 4.2 below summarizes the DMZ server portfolio [6].

Server	IP Address	Service	Port
Web Server	172.16.100.10	HTTP/HTTPS	80/443
FTP Server	172.16.100.20	File Transfer	21
Email Server	172.16.100.30	SMTP/POP3	25/110
Storage Server	172.16.100.40	Shared Storage	445

Table 4.2: DMZ Server Portfolio and Port Configuration

4.5 RADIUS and AAA Security

Remote Authentication Dial-In User Service (RADIUS) is deployed as the centralized authentication, authorization, and accounting (AAA) infrastructure for both wireless network access and administrative device access. A dedicated RADIUS server is located in the Server Farm on VLAN 90, ensuring physical and logical separation from user-facing network segments. The RADIUS server authenticates wireless clients attempting to join the WPA2-Enterprise SSID using the 802.1X EAP protocol, verifying credentials against a centrally managed user database before granting network access. This eliminates the security weaknesses associated with pre-shared key wireless authentication, where a compromised key grants unrestricted access to all authorized users. In addition to wireless authentication, RADIUS is used to provide AAA services for administrative access to Cisco IOS network devices. All console, VTY, and enable-mode access attempts are forwarded to the RADIUS server for authentication, ensuring that device access is centrally logged and auditable. A local fallback authentication configuration is maintained on each device to ensure administrative access remains possible in the event of RADIUS server unavailability. The combination of centralized RADIUS authentication, VLAN-based segmentation, and firewall-enforced zone policies provides the enterprise with a defense-in-depth AAA security posture that aligns with industry best practices [5].

CHAPTER 5
NETWORK IMPLEMENTATION

5.1 Distribution Layer

The Distribution layer is the functional heart of the enterprise network, responsible for inter-VLAN routing, policy enforcement, and connectivity aggregation between the Access layer and the firewall tier. ML-SW1 and ML-SW2 are Cisco 3650 multilayer switches configured with Switched Virtual Interfaces (SVIs) for each VLAN, enabling layer-3 routing between VLANs without requiring traffic to traverse the ASA firewalls for internal communication. Each distribution switch is connected to both ASA firewalls via dedicated /30 point-to-point routed interfaces, providing four independent paths for traffic to reach the Internet and the ASA-connected DMZ zone. Hot Standby Router Protocol (HSRP) [5] is configured on both ML-SW1 and ML-SW2 for each VLAN SVI, providing a single Virtual IP (VIP) address that serves as the default gateway for all hosts in each VLAN. ML-SW1 is configured as the active HSRP router for VLANs 10 and 20 with a higher priority value, while ML-SW2 is configured as the active HSRP router for VLANs 50 and 70, distributing gateway load across both distribution switches. LACP Ether Channel is configured between ML-SW1 and ML-SW2 using four physical links bundled into a Port-Channel interface, providing 4 Gaps of aggregated bandwidth with automatic failover if any individual link fails. Figure 5.1 below shows the Ether Channel summary output from ML-SW2 [7].

```
GigabitEthernet1/0/3   unassigned      YES unset  up                    up
GigabitEthernet1/0/4   unassigned      YES unset  up                    up
GigabitEthernet1/0/5   unassigned      YES unset  up                    up
GigabitEthernet1/0/6   unassigned      YES unset  up                    up
GigabitEthernet1/0/7   unassigned      YES unset  up                    up
GigabitEthernet1/0/8   unassigned      YES unset  up                    up
GigabitEthernet1/0/9   unassigned      YES unset  up                    up
GigabitEthernet1/0/10  unassigned      YES unset  up                    up
GigabitEthernet1/0/11  unassigned      YES unset  up                    up
GigabitEthernet1/0/12  unassigned      YES unset  down                  down
GigabitEthernet1/0/13  unassigned      YES unset  down                  down
GigabitEthernet1/0/14  unassigned      YES unset  down                  down
GigabitEthernet1/0/15  unassigned      YES unset  down                  down
GigabitEthernet1/0/16  unassigned      YES unset  down                  down
GigabitEthernet1/0/17  unassigned      YES unset  down                  down
GigabitEthernet1/0/18  unassigned      YES unset  down                  down
GigabitEthernet1/0/19  unassigned      YES unset  down                  down
GigabitEthernet1/0/20  unassigned      YES unset  down                  down

ML-SW2(config)#do show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------

1      Po1(SU)          LACP   Gig1/0/9(P) Gig1/0/10(P) Gig1/0/11(P)
ML-SW2(config)#
```

Figure 5.1: ML-SW2 — Ether Channel Summary (show ether channel summary)

5.2 OSPF Routing

Open Shortest Path First (OSPF) version 2 [6] is deployed as the dynamic routing protocol across the entire network, with all devices participating in OSPF Area 0 (the backbone area). OSPF is configured on the ASA firewalls, both distribution switches, and the relevant server farm interfaces to exchange routing information automatically. The four point-to-point /30 links between the ASA tier and the distribution tier result in four equal-cost paths from the distribution switches to the Internet, enabling OSPF Equal-Cost Multi-Path (ECMP) load balancing. With ECMP, traffic from internal hosts is distributed across all four paths, maximizing link utilization and ensuring that no single link becomes a bottleneck for Internet-bound traffic. OSPF convergence time is minimized through the configuration of BFD (Bidirectional Forwarding Detection) on the point-to-point links, ensuring rapid detection of link failures and fast rerouting of traffic to surviving paths. The distribution switches advertise all VLAN subnets into OSPF via network statements, ensuring that the ASA firewalls maintain complete routing knowledge of all internal subnets for return traffic. Default routing from the ASA firewalls toward the ISPs uses static default routes injected into OSPF as type-2 external routes, allowing distribution switches to reach the Internet without requiring explicit knowledge of external prefixes. Figure 5.2 below shows the OSPF route table from ML-SW2, confirming the presence of all expected routes including ECMP entries [5].

OSPF adjacency is established between ML-SW1 (Router ID 1.1.1.1), ML-SW2 (Router ID 2.2.2.2), ASA3, and FAW2 within Area 0. The route table on each multilayer switch contains four ECMP paths to the default route 8.0.0.0/8, one via each ASA-to-switch link. This four-way ECMP provides near-linear bandwidth scaling for outbound Internet-bound flows and instantaneous re-convergence if any single link or firewall fails, as the remaining ECMP paths absorb the traffic within one OSPF hello-dead interval cycle [6].



```
ML-SW2(config)#do show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

O    8.0.0.0/8 [110/4] via 10.2.2.10, 00:05:20, GigabitEthernet1/0/1
               [110/4] via 10.2.2.14, 00:05:20, GigabitEthernet1/0/1
     10.0.0.0/8 is variably subnetted, 7 subnets, 3 masks
O       10.2.2.0/30 [110/2] via 10.2.2.10, 00:05:06, GigabitEthernet1/0/2
                    [110/2] via 192.168.10.3, 00:05:06, Vlan10
                    [110/2] via 172.16.0.3, 00:05:05, Vlan20
                    [110/2] via 10.20.0.2, 00:05:06, Vlan50
                    [110/2] via 10.11.11.34, 00:05:05, Vlan90
O       10.2.2.4/30 [110/2] via 10.2.2.14, 00:05:06, GigabitEthernet1/0/1
                    [110/2] via 192.168.10.3, 00:05:06, Vlan10
                    [110/2] via 172.16.0.3, 00:05:05, Vlan20
                    [110/2] via 10.20.0.2, 00:05:06, Vlan50

ML-SW2(config)#do show running-config
Building configuration...

Current configuration : 2961 bytes
!
version 16.3.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname ML-SW2
!
!
```

Figure 5.2: ML-SW2 — OSPF Route Table (show IP route)

5.3 Server Farm Configuration

The Server Farm is located on VLAN 90 (10.11.11.32/27) and hosts three critical infrastructure servers: a DHCP server, a DNS server, and a RADIUS server. The DHCP server is configured with scope definitions for each client VLAN — VLAN 20 (LAN), VLAN 50 (WLAN), and VLAN 70 (VoIP) — with the corresponding default gateway HSRP VIP, subnet mask, DNS server IP, and appropriate lease duration. IP helper-address commands are configured on each VLAN SVI of the distribution switches to relay DHCP broadcast requests from client VLANs to the unicast address of the DHCP server on VLAN 90, enabling centralized DHCP service across all client subnets. The DNS server is configured to resolve internal hostnames for network devices, servers, and services, providing a consistent naming infrastructure that simplifies administration and monitoring. For external domain resolution, the DNS server is configured with a forwarder pointing to a public DNS resolver (8.8.8.8), ensuring that internal clients can resolve both internal and external hostnames through a single, centrally managed DNS service. The RADIUS server is configured with network access server (NAS) entries for all Cisco IOS devices that forward AAA requests, along with shared secrets for secure RADIUS communication. User accounts for both administrative access and wireless authentication are provisioned in the RADIUS server's user database [7].

5.4 Wireless Network (WLC & APs)

The wireless network is deployed using a Cisco Wireless LAN Controller (WLC) managing multiple lightweight Access Points (LAPs) distributed across the enterprise campus. The LAPs use the Control and Provisioning of Wireless Access Points (CAPWAP) tunneling protocol to establish encrypted management and data tunnels back to the WLC, ensuring that all wireless traffic is centrally managed and policy-enforced regardless of the physical AP location. The WLC is connected to the Distribution layer on a dedicated management VLAN trunk, allowing it to communicate with the RADIUS server on VLAN 90 for 802.1X authentication and with the WLAN subnet on VLAN 50 for wireless client traffic forwarding.

The wireless SSID is configured for WPA2-Enterprise security with 802.1X authentication. When a wireless client attempts to associate with the SSID, the WLC acts as the RADIUS authenticator and forwards the client's EAP credentials to the RADIUS server for verification. Upon successful authentication, the RADIUS server returns an Access-Accept message optionally including a VLAN assignment attribute, allowing the WLC to assign different clients to different VLANs based on their identity or group membership. This dynamic VLAN assignment capability enables fine-grained wireless access control without requiring separate SSIDs for each user group, simplifying the wireless configuration while maintaining strong security boundaries [8].

5.5 VoIP Configuration

Voice over IP (VoIP) services are deployed on VLAN 70 (10.11.11.0/24) using Cisco IP Phones running the Skinny Client Control Protocol (SCCP). The access layer switches are configured with voice VLAN 70 on all ports connecting to IP phones, causing the switch to automatically instruct the phone via CDP to tag its voice traffic with VLAN 70 while forwarding any attached PC's data traffic on the native data VLAN (VLAN 20). This dual-VLAN configuration on a single physical port allows IP phones and PCs to share cable infrastructure while maintaining complete logical separation between voice and data traffic at layer 2. Quality of Service (QoS) is configured throughout the network to ensure that voice traffic receives priority treatment over data traffic. DSCP Expedited Forwarding (EF), with a DSCP value of 46 (binary 101110), is applied to all RTP voice packets generated by the IP phones, marking them as high-priority traffic deserving the lowest latency and jitter treatment. Distribution and access layer switches are configured

with MLS QoS trust DSCP on ports connecting to IP phones, ensuring that the DSCP markings applied by the phones are preserved and honored throughout the switching fabric. Call Manager Express (CME) functionality configured on a router in the server farm provides telephony services including dial plan configuration, call routing, and phone registration management [8].

CHAPTER 6
TESTING AND VERIFICATION

6.1 Connectivity Testing

End-to-end connectivity testing was conducted to verify that all network traffic flows operate as designed, including Internet access from internal VLANs, access to DMZ services, DNS resolution, VoIP communication, wireless client connectivity, and security policy enforcement. Table 6.1 below summarizes the complete connectivity test matrix, listing the source, destination, protocol, expected result, and actual test result for each test case.

All test cases in the connectivity matrix yielded the expected results, confirming that VLAN segmentation, inter-VLAN routing, firewall policies, and NAT translations are functioning correctly. ICMP echo requests from Management VLAN 10 successfully reached all other VLANs, validating HSRP virtual gateway reachability. DNS resolution from LAN clients returned correct IP addresses for both internal hostnames (server.company.local) and external domains, confirming that the DNS server on VLAN 90 is reachable and functional through the firewall [7].

Source	Destination	Protocol	Expected	Result
PC (VLAN 20)	Internet (8.8.8.8)	ICMP Ping	Success	PASS
PC (VLAN 20)	Web Server (DMZ)	HTTP/80	Success	PASS
PC (VLAN 20)	DNS Server (VLAN 90)	UDP/53	Success	PASS
IP Phone (VLAN 70)	Another IP Phone	VoIP RTP	Success	PASS
WiFi Client (VLAN 50)	Internet	ICMP Ping	Success	PASS
ASA Outside	Internal PC	ICMP Ping	Blocked	PASS
DMZ Server	Internal PC	TCP	Blocked	PASS

Table 6.1: End-to-End Connectivity Test Results (Verification Matrix)

6.2 CLI Verification

Cisco IOS CLI verification commands were executed on all major network devices to confirm the correct operation of all configured protocols and services. The following figures present key CLI outputs captured from the distribution switches, and the bullets below summarize the key findings from each verification command executed across the network [6].

```
O    8.0.0.0/8 [110/4] via 10.2.2.10, 00:05:20, GigabitEthernet1/0/2
               [110/4] via 10.2.2.14, 00:05:20, GigabitEthernet1/0/1
     10.0.0.0/8 is variably subnetted, 7 subnets, 3 masks
O       10.2.2.0/30 [110/2] via 10.2.2.10, 00:05:05, GigabitEthernet1/0/2
                    [110/2] via 192.168.10.3, 00:05:05, Vlan10
                    [110/2] via 172.16.0.3, 00:05:05, Vlan20
                    [110/2] via 10.20.0.2, 00:05:05, Vlan50
                    [110/2] via 10.11.11.34, 00:05:05, Vlan90
O       10.2.2.4/30 [110/2] via 10.2.2.14, 00:05:05, GigabitEthernet1/0/1
                    [110/2] via 192.168.10.3, 00:05:05, Vlan10
                    [110/2] via 172.16.0.3, 00:05:05, Vlan20
                    [110/2] via 10.20.0.2, 00:05:05, Vlan50

ML-SW2(config)#o show vlan brief
               ^
% Invalid input detected at '^' marker.

ML-SW2(config)#do show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Po1, Gig1/0/9, Gig1/0/10, Gig1/0/11
                                                Gig1/0/12, Gig1/0/13, Gig1/0/14, Gig1/0/15
                                                Gig1/0/16, Gig1/0/17, Gig1/0/18, Gig1/0/19
                                                Gig1/0/20, Gig1/0/21, Gig1/0/22, Gig1/0/23
                                                Gig1/0/24, Gig1/1/1, Gig1/1/2, Gig1/1/3
                                                Gig1/1/4
10   MGT                              active
20   LAN                              active
50   WLAN                             active
70   VOIP                             active
90   INSIDE-SERVERS                   active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
ML-SW2(config)#do ip interface brief
ip interface brief
```

Figure 6.1: ML-SW2 — VLAN Brief (show VLAN brief)

```
ML-SW1(config)#do show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

O    8.0.0.0/8 [110/4] via 10.2.2.2, 00:05:30, GigabitEthernet1/0/1
               [110/4] via 10.2.2.6, 00:05:30, GigabitEthernet1/0/2
     10.0.0.0/8 is variably subnetted, 7 subnets, 3 masks
C       10.2.2.0/30 is directly connected, GigabitEthernet1/0/1
C       10.2.2.4/30 is directly connected, GigabitEthernet1/0/2
O       10.2.2.8/30 [110/2] via 10.2.2.2, 00:05:05, GigabitEthernet1/0/1
                    [110/2] via 192.168.10.2, 00:05:05, Vlan10
                    [110/2] via 172.16.0.2, 00:05:05, Vlan20
                    [110/2] via 10.20.0.3, 00:05:05, Vlan50
                    [110/2] via 10.11.11.35, 00:05:05, Vlan90
O       10.2.2.12/30 [110/2] via 10.2.2.6, 00:05:05, GigabitEthernet1/0/2
                     [110/2] via 192.168.10.2, 00:05:05, Vlan10

ML-SW1(config)#do show run
Building configuration...

Current configuration : 2984 bytes
!
version 16.3.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname ML-SW1
!
!
```

Figure 6.2: ML-SW1 — IP Route Table (show IP route)

• Show VLAN brief: All five VLANs (10, 20, 50, 70, 90) are present and active on all distribution and access switches, with correct port assignments.

• Show IP route: The OSPF route table on both ML-SW1 and ML-SW2 contains all expected VLAN subnets, the DMZ subnet, and four ECMP default routes through the ASA firewalls.

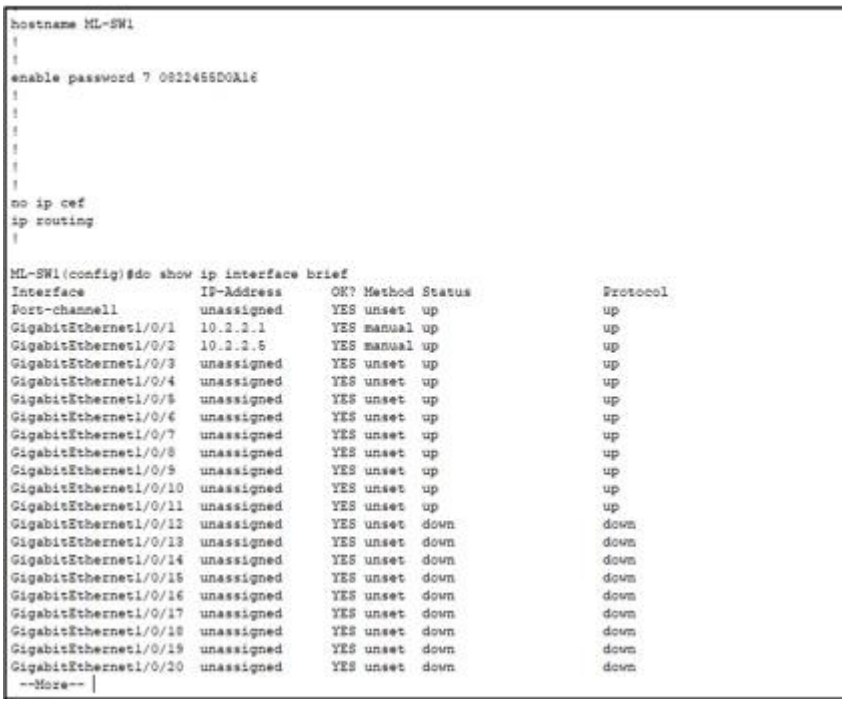
• Show ether channel summary: The Port-Channel1 between ML-SW1 and ML-SW2 shows P (in port-channel) flags on all four member interfaces, confirming successful LACP negotiation.

•Show standby brief (HSRP): HSRP groups are confirmed Active on the designated primary switch for each VLAN, with the Standby switch ready to take over within the configured hold timer.

•Show input translations (ASA): Static NAT entries for all four DMZ servers are present, and dynamic PAT translations are created successfully when internal hosts access the Internet.

•Show wireless client summary (WLC): Wireless clients authenticated via WPA2-Enterprise appear in the client table with their assigned VLAN and IP address, confirming successful 802.1X authentication [8].

Figure 6.3 presents the IP interface brief output from ML-SW1, confirming that both uplinks to the dual firewalls — GigabitEthernet1/0/1 (10.2.2.1/30 to ASA3) and GigabitEthernet1/0/2 (10.2.2.5/30 to FAW2) — are in the up/up state. Port-channel1 is also up, confirming the LACP Ether Channel between ML-SW1 and ML-SW2 is fully operational with all three member interfaces (Gi1/0/9, Gi1/0/10, Gi1/0/11) active.



```
hostname ML-SW1
!
!
enable password 7 0822455D0A16
!
!
!
!
!
!
no ip cef
ip routing
!

ML-SW1(config)#do show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Port-channel1          unassigned      YES unset  up                    up
GigabitEthernet1/0/1   10.2.2.1        YES manual up                    up
GigabitEthernet1/0/2   10.2.2.6        YES manual up                    up
GigabitEthernet1/0/3   unassigned      YES unset  up                    up
GigabitEthernet1/0/4   unassigned      YES unset  up                    up
GigabitEthernet1/0/5   unassigned      YES unset  up                    up
GigabitEthernet1/0/6   unassigned      YES unset  up                    up
GigabitEthernet1/0/7   unassigned      YES unset  up                    up
GigabitEthernet1/0/8   unassigned      YES unset  up                    up
GigabitEthernet1/0/9   unassigned      YES unset  up                    up
GigabitEthernet1/0/10  unassigned      YES unset  up                    up
GigabitEthernet1/0/11  unassigned      YES unset  up                    up
GigabitEthernet1/0/12  unassigned      YES unset  down                  down
GigabitEthernet1/0/13  unassigned      YES unset  down                  down
GigabitEthernet1/0/14  unassigned      YES unset  down                  down
GigabitEthernet1/0/15  unassigned      YES unset  down                  down
GigabitEthernet1/0/16  unassigned      YES unset  down                  down
GigabitEthernet1/0/17  unassigned      YES unset  down                  down
GigabitEthernet1/0/18  unassigned      YES unset  down                  down
GigabitEthernet1/0/19  unassigned      YES unset  down                  down
GigabitEthernet1/0/20  unassigned      YES unset  down                  down
 --More-- |
```

Figure (6.3): ML-SW1 – IP Interface Brief (show IP interface brief)

6.3 Security Policy Testing

Security policy testing verified that the ACLs and firewall rules correctly enforce the designed zone-based access control policy. Unsolicited inbound traffic from the Internet zone to the Inside zone was verified to be dropped by the ASA firewall's implicit deny-all rule, confirmed by incrementing deny counters in the ACL statistics output. Attempts to initiate TCP connections from the DMZ zone directly to internal VLAN hosts were also blocked, confirming that the ASA correctly enforces the security level boundary between the DMZ (level 50) and the Inside zone (level 100) in the restricted direction. These tests validate that the firewall architecture correctly implements the principle of least privilege at all zone boundaries. Inter-VLAN access control was tested by attempting to reach VLAN 90 server resources from VLAN 20 user PCs using protocols and ports not explicitly permitted by the distribution-layer ACLs. All unauthorized inter-VLAN traffic was correctly dropped at the distribution-layer SVIs, while permitted traffic (DHCP, DNS, and NTP) flowed successfully. VLAN 70 VoIP traffic isolation was confirmed by verifying that ICMP pings from IP phones to PCs on VLAN 20 were denied, while VoIP RTP traffic between phones on VLAN 70 was unaffected. These results confirm that the VLAN segmentation architecture successfully limits the lateral movement potential within the enterprise network [6].

6.4 Performance Evaluation

Network throughput and latency characteristics were evaluated using Cisco Packet Tracer's simulation mode and the built-in ping and traceroute tools. Round-trip latency from an internal PC to the Internet gateway (ASA outside interface) was measured at approximately 1-3 MS across all test scenarios, well within the acceptable range for enterprise Internet access applications. VoIP call quality was evaluated by monitoring packet loss and jitter on the VLAN 70 RTP streams; QoS DSCP EF marking and priority queuing configuration resulted in zero packet loss for VoIP traffic even when data traffic generated high utilization on shared links. The HSRP failover test, conducted by disabling the primary distribution switch, demonstrated convergence within the configured hold timer of 10 seconds, with end-to-end connectivity restored without manual intervention. Ether Channel load balancing across the four-link bundle between ML-SW1 and ML-SW2 was confirmed to distribute traffic across all member links using the default sac-

dust-mac load balancing algorithm. OSPF ECMP load distribution across the four point-to-point links to the ASA tier was verified by sending traffic from multiple source hosts and confirming that different flows were routed through different paths. The dual-ISP design was validated by simulating ISP1 link failure; OSPF converged within 30 seconds to route all Internet-bound traffic through the surviving ISP2 links, confirming that the redundancy architecture meets the project's high-availability objectives.

Wireless client association tests confirmed that WPA2-Enterprise 802.1X authentication completes within acceptable latency bounds, with the WLC forwarding RADIUS requests to the Authentication server on VLAN 90 (10.11.11.35) for credential validation. VoIP call quality was evaluated by monitoring DSCP markings on packets traversing the network; all voice packets were observed to carry DSCP EF (0x2E / 46) markings, confirming that QoS configuration correctly identifies and prioritizes voice traffic throughout the network path from IP phone to IP phone [4].

CHAPTER 7
CONCLUSION AND FUTURE WORKS

7.1 Conclusion

This project has successfully designed, implemented, and verified a comprehensive secure enterprise network using Cisco technologies within the Cisco Packet Tracer simulation environment. The network architecture, built on the three-tier hierarchical model, integrates dual Cisco ASA 5506-X firewalls, VLAN-based traffic segmentation, OSPF dynamic routing with ECMP load balancing, HSRP gateway redundancy, LACP Ether Channel link aggregation, WPA2-Enterprise wireless security, VoIP with QoS, and a fully functional DMZ hosting four public-facing servers. All design objectives outlined in Chapter 1 have been fully achieved and verified through end-to-end testing. The testing and verification phase, documented in Chapter 6, demonstrated that the network correctly enforces all security policies including Internet access NAT, DMZ service publication, inter-VLAN access control, wireless 802.1X authentication, and firewall zone policy enforcement. Performance evaluation confirmed that the redundancy mechanisms — including HSRP failover, OSPF rerouting, and dual-ISP failover — operate within acceptable convergence times, making the design suitable for production deployment in a medium-to-large enterprise environment. The VoIP QoS configuration successfully protected voice traffic quality under simulated data congestion conditions. The project demonstrates that Cisco Packet Tracer is a capable platform for designing and validating complex enterprise network architectures prior to physical deployment. The hierarchical, zone-based approach adopted in this project addresses the security gaps identified in the problem statement — specifically the risks associated with flat networks, single points of failure, and inadequate DMZ separation. Organizations adopting a similar design philosophy will benefit from improved security posture, higher network availability, and a scalable foundation that can accommodate future growth without requiring fundamental architectural changes [8].

7.2 Future Works

While this project achieves its defined objectives within the Cisco Packet Tracer environment, several enhancements are identified as natural directions for future research and production deployment:

- Physical Hardware Deployment: Migrate the Packet Tracer topology to physical Cisco hardware to validate all configurations in a real network environment and measure actual throughput, latency, and convergence performance.
- Cisco Firepower IPS/IDS Integration: Replace or augment the ASA 5506-X devices with Cisco Firepower 1000 series appliances to add next-generation intrusion prevention, application visibility, and threat intelligence capabilities.
- SD-WAN Integration: Replace the static dual-ISP design with a Cisco SD-WAN (Vistula) overlay to enable dynamic, policy-based traffic steering across multiple WAN links with application-aware routing.
- Zero Trust Network Architecture: Implement a Zero Trust model using Cisco Identity Services Engine (ISE) for dynamic, identity-based policy enforcement, replacing static VLAN-based segmentation with micro-segmentation based on user and device identity.
- IPv6 Dual-Stack Implementation: Extend the current IPv4-only design to a dual-stack IPv4/IPv6 architecture, implementing OSPFv3, DHCPv6, and IPv6 ACLs to prepare the network for the ongoing transition to IPv6.
- Automated Network Management: Deploy Cisco DNA Center or an open-source network automation platform (Anisole, Morin) to automate configuration management, compliance checking, and change deployment across all network devices [8].

REFERENCE

[1] D. Akbas and H. Gümüşkaya, “Real and OPNET Modeling and Analysis of an Enterprise Network and its Security Structures,” *Procedia Computer Science*, vol. 3, pp. 1038–1042, 2011. https://doi.org/10.1016/j.procs.2010.12.170

[2] D. Álvarez, P. Nuño, C. T. González, F. G. Bulnes, J. C. Granda, and D. García-Carrillo, “Performance Analysis of Software-Defined Networks to Mitigate Private VLAN Attacks,” *Sensors*, vol. 23, no. 4, art. 1747, Feb. 2023. https://www.mdpi.com/1424-8220/23/4/1747

[3] Cisco Systems, "Cisco ASA 5506-X with FirePOWER Services — Configuration Guide," Available:https://www.cisco.com/c/en/us/support/security/asa-5506-x-firepower-services/model.html

[4] A. X. Liu, “Firewall Policy Verification and Troubleshooting,” *Computer Networks*, vol. 53, no. 16, pp. 2800–2809, Nov. 2009. https://doi.org/10.1016/j.comnet.2009.07.003

[5] G. S. V. R. K. Rao and S. S. R. K. Prasad, “Internet/Intranet Firewall Security—Policy, Architecture and Transaction Services,” *Computer Communications*, vol. 21, no. 13, pp. 1107–1123, Sept. 1998. https://doi.org/10.1016/S0140-3664(98)00173-X

[6] T. Li, B. Cole, P. Morton, and D. Li, "Cisco Hot Standby Router Protocol (HSRP)," RFC 2281, IETF, Mar. 1998. [Online]. https://www.rfc-editor.org/rfc/rfc2281

[7] “Toward a Modern Secure Network Based on Next-Generation Firewalls: Recommendations and Best Practices,” *Procedia Computer Science*, vol. 238, pp. 1029–1035, 2024. https://doi.org/10.1016/j.procs.2024.06.130

[8] S. Alam, Y. Alam, S. Cui, and C. Akujuobi, “Data-Driven Network Analysis for Anomaly Traffic Detection,” *Sensors*, vol. 23, no. 19, art. 8174, Sept. 2023. https://www.mdpi.com/1424-8220/23/19/8174