

# Graduation Project

## Securing a Small Business Network

### Cisco Cybersecurity Engineer (ONL2\_ISS5\_S2)

#### Made by

Ezz-Eldein Ali Hanafy	21088600
Mohammed Alaa Hamada	21073442
Mohammed Ibrahim Gomaa	21092169
Ahmed Mohammed Ali	21091026
Mohammed Khaled Abdalla	21072330

#### Supervised by

Eng. Amr Adel

## Content

VLSM Table .....	2
IP Address Table .....	3
Port Channel Table .....	4
IP Phone Table .....	5
VLAN Table .....	5
VTP Table .....	6
Introduction .....	6
Network Design Overview .....	6
Implemented Features & Technologies .....	7
Download Project .....	16

### VLSM Table

Subnet (VLAN)	Hosts	Net ID	Subnet Mask	Usable Range	Broadcast
<b>192.168.1.0/24</b>					
<b>Default/IT (1)</b>	64	192.168.1.0/26	255.255.255.192	192.168.1.1 192.168.1.62	192.168.1.63
<b>Development (10)</b>	32	192.168.1.64/27	255.255.255.224	192.168.1.65 192.168.1.94	192.168.1.95
<b>Legal Affairs (20)</b>	32	192.168.1.96/27	255.255.255.224	192.168.1.97 192.168.1.126	192.168.1.127
<b>Marketing (30)</b>	32	192.168.1.128/27	255.255.255.224	192.168.1.129 192.168.1.158	192.168.1.159
<b>Financial (40)</b>	32	192.168.1.160/27	255.255.255.224	192.168.1.161 192.168.1.190	192.168.1.191
<b>HR (50)</b>	32	192.168.1.192/27	255.255.255.224	192.168.1.193 192.168.1.222	192.168.1.223
<b>Customer Service (60)</b>	32	192.168.1.224/27	255.255.255.224	192.168.1.225 192.168.1.254	192.168.1.255
<b>Administration (2)</b>	16	192.168.2.0/28	255.255.255.240	192.168.2.1 192.168.2.14	192.168.2.15
<b>Voice (3)</b>	16	192.168.2.16/28	255.255.255.240	192.168.2.17 192.168.2.30	192.168.2.31
<b>Guest Wi-Fi (111)</b>	4	192.168.2.32/30	255.255.255.252	192.168.2.33 192.168.2.34	192.168.2.35
<b>10.0.0.0/24</b>					
<b>INSIDE 0 &amp; 3</b>	8	10.0.0.0/29	255.255.255.248	10.0.0.1 10.0.0.6	10.0.0.7
<b>INSIDE 1 &amp; 2</b>	8	10.0.0.8/29	255.255.255.248	10.0.0.9 10.0.0.15	10.0.0.16
<b>60.0.0.0/24</b>					
<b>DMZ</b>	8	60.0.0.0/29	255.255.255.248	60.0.0.1 60.0.0.6	60.0.0.7
<b>20.0.0.0/24</b>					
<b>OUTSIDE 0</b>	4	20.0.0.0/30	255.255.255.252	20.0.0.1 20.0.0.2	20.0.0.3
<b>OUTSIDE 1</b>	4	20.0.0.4/30	255.255.255.252	20.0.0.5 20.0.0.6	20.0.0.7
<b>OUTSIDE 2</b>	4	20.0.0.8/30	255.255.255.252	20.0.0.9 20.0.0.10	20.0.0.11
<b>OUTSIDE 3</b>	4	20.0.0.12/30	255.255.255.252	20.0.0.13 20.0.0.14	20.0.0.15

**IP Address Table**

Device	Interface	IP Address/Prefix	Default Gateway
<b>MLS0</b>	VLAN 1	192.168.1.1/26	N/A
	VLAN 2	192.168.2.1/28	N/A
	VLAN 3	192.168.2.17/28	N/A
	VLAN 10	192.168.1.65/27	N/A
	VLAN 20	192.168.1.97/27	N/A
	VLAN 100	10.0.0.2/29	N/A
	VLAN 111	192.168.2.33/30	N/A
<b>MLS1</b>	VLAN 3	192.168.2.19/28	N/A
	VLAN 30	192.168.1.129/27	N/A
	VLAN 40	192.168.1.161/27	N/A
	VLAN 50	192.168.1.193/27	N/A
	VLAN 60	192.168.1.225/27	N/A
	VLAN 200	10.0.0.10/29	N/A
<b>Admin-IT-Sw</b>	VLAN 1	DHCP	192.168.1.1
<b>Dev-Sw</b>	VLAN 1	192.168.1.6/26	192.168.1.1
<b>Legal-Sw</b>	VLAN 1	192.168.1.5/26	192.168.1.1
<b>Market-Sw</b>	VLAN 30	192.168.1.132/27	192.168.1.129
<b>Finan-Sw</b>	VLAN 40	192.168.1.164/27	192.168.1.161
<b>HR-Sw</b>	VLAN 50	192.168.1.196/27	192.168.1.193
<b>CS-Sw</b>	VLAN 60	192.168.1.228/27	192.168.1.225
<b>DMZ-Sw</b>	VLAN 1	60.0.0.5/29	60.0.0.1
<b>R0</b>	G0/0	100.0.0.1/30	N/A
	G0/1	20.0.0.2/30	N/A
	G0/2	20.0.0.10/30	N/A
<b>R1</b>	G0/0	100.0.0.5/30	N/A
	G0/1	20.0.0.14/30	N/A
	G0/2	20.0.0.6/30	N/A
<b>R2</b>	G0/0	100.0.0.6/30	N/A
	G0/1	100.0.0.2/30	N/A
	S0/0/0	209.111.44.1/30	N/A
<b>R3</b>	G0/0	172.16.1.1/24	N/A
	S0/0/0	209.111.44.2/30	N/A
<b>VoIP</b>	F0/0	192.168.2.18/28	N/A
<b>Server0</b>	F0	192.168.1.7/26	192.168.1.1
<b>HTTP</b>	F0	60.0.0.2/29	60.0.0.1
<b>Email</b>	F0	60.0.0.3/29	60.0.0.1
<b>External DNS</b>	F0	60.0.0.4/29	60.0.0.1
	G1/management (IT)	192.168.1.4/26	192.168.1.1
	Administration	192.168.2.6/28	192.168.2.1
	Development	192.168.1.70/27	192.168.1.65

<b>WiLAN Controller</b>	Marketing	192.168.1.134/27	192.168.1.129
	HR	192.168.1.198/27	192.168.1.193
	Customer Service	192.168.1.230/27	192.168.1.224
<b>ASA0</b>	G1/1	20.0.0.13/30	N/A
	G1/2	20.0.0.9/30	N/A
	G1/3	10.0.0.3/29	N/A
	G1/4	10.0.0.11/29	N/A
<b>ASA1</b>	G1/1	20.0.0.1/30	N/A
	G1/2	20.0.0.5/30	N/A
	G1/3	10.0.0.9/29	N/A
	G1/4	10.0.0.1/29	N/A
	G1/5	60.0.0.1/29	N/A
<b>PC72</b>	F0	172.16.1.10/24	172.16.1.1
<b>Smartphone0</b>	Wireless	192.168.2.34/30	192.168.2.33
<b>Other PCs, Printers and IP Phones</b>	Wired or Wireless	DHCP	Based on VLAN

**Port Channel Table**

Location	Group	Ports	Protocol
<b>Left Side</b>	1	Finan-Sw: <b>F0/13-15</b> MLS1: <b>F0/4-6</b>	PAGP
	2	Market-Sw: <b>F0/2-4</b> MLS1: <b>F0/1-3</b>	LACP
	3	HR-Sw: <b>F0/2-4</b> MLS1: <b>F0/7-9</b>	LACP
	4	CS-Sw: <b>F0/2-4</b> MLS1: <b>F0/10-12</b>	PAGP
<b>Right Side</b>	1	Legal-Sw: <b>F0/13-15</b> MLS0: <b>F0/1-3</b>	PAGP
	2	Dev-Sw: <b>F0/2-4</b> MLS0: <b>F0/4-6</b>	PAGP
	3	Admin-IT-Sw: <b>F5/1, F6/1, F7/1</b> MLS0: <b>F0/7-9</b>	PAGP

### IP Phone Table

Phone	Line Number	VLAN	IP Address	TFTP Server
0	2	Administration	DHCP	R0 192.168.2.20
1	1	IT		
2	60	Customer-Service		
3	50	HR		
4	40	Financial		
5	30	Marketing		
6	20	Legal-Affairs		
7	10	Development		

### VLAN Table

VLAN Number	VLAN Name	Interface Assigned
1	Default	Admin-IT-Sw: <b>F0/1, G3/1</b> DMZ-Sw: <b>F0/1-3</b> Another-Site: <b>F0/1</b>
2	Administration	Admin-IT-Sw: <b>F1/1, G2/1</b>
3	Voice	Admin-IT-Sw: <b>F0/1, F1/1</b> Dev-Sw: <b>F0/1</b> Legal-Sw: <b>F0/1</b> Market-Sw: <b>F0/1</b> Finan-Sw: <b>F0/1</b> HR-Sw: <b>F0/1</b> CS-Sw: <b>F0/1</b>
10	Development	Dev-Sw: <b>F0/1</b>
20	Legal-Affairs	Legal-Sw: <b>F0/1-12</b>
30	Marketing	Market-Sw: <b>F0/1</b>
40	Financial	Finan-Sw: <b>F0/1-12</b>
50	HR	HR-Sw: <b>F0/1</b>
60	Customer-Service	CS-Sw: <b>F0/1</b>
111	Guest	MLS0: <b>F0/10</b>
404	Black-Hole	Dev-Sw: <b>F0/5-24, G0/2</b> Legal-Sw: <b>F0/16-24, G0/1-2</b> Market-Sw: <b>F0/5-24, G0/2</b> Finan-Sw: <b>F0/16-24, G0/1-2</b> HR-Sw: <b>F0/5-24, G0/2</b> CS-Sw: <b>F0/5-24, G0/2</b> MLS0: <b>F0/15-24</b> MLS1: <b>F0/18-24</b> DMZ-Sw: <b>F0/4-24, G0/2</b>

## VTP Table

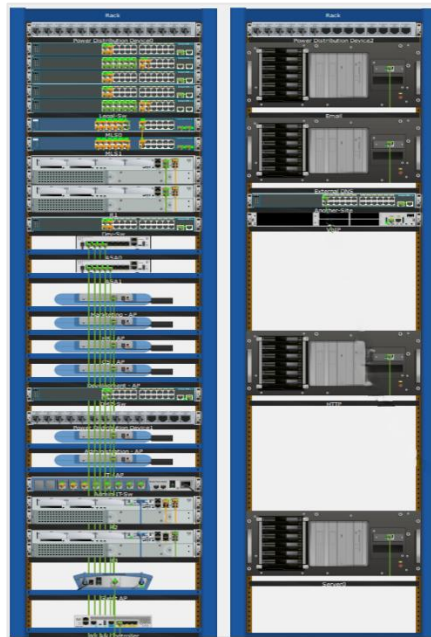
Device	Mode	Domain (Password)
MLS1	Server	reals (123)
MLS0		
Admin-IT-Sw	Client	
Dev-Sw		
Legal-Sw		
Market-Sw		
Finan-Sw		
HR-Sw		
CS-Sw		

## Introduction

The purpose of this project is to design and implement a secure and reliable network infrastructure for a small business (For Real Estate Company) with more than 30 employees. The network will support essential business operations by connecting employee workstations, printers, a small server, and guest Wi-Fi while ensuring secure remote access and strong protection against cyber threats. To enhance performance and security, the network will be segmented into multiple zones—such as internal, guest, and server segments—using VLANs and proper IP addressing. Security measures including firewall rules, Intrusion Detection and Prevention Systems (IDPS), and VPN access will be implemented to guard against unauthorized access and malware. This setup will enable employees to work efficiently, access resources securely, and maintain the confidentiality and integrity of sensitive business data.

## Network Design Overview

The design includes VLAN segmentation by department, dedicated infrastructure services (HTTP, HTTPS, DNS, DHCP, NTP, SYSLOG, TFTP), wireless access for employees and guests, secured remote access via VPN, and centralized security policies with AAA and firewall implementations.







### **Rapid-PVST**

Rapid Per-VLAN Spanning Tree (Rapid-PVST) has been implemented to provide accelerated convergence times for the spanning-tree protocol within the switched network topology. This enhancement significantly improves overall network availability by rapidly adapting to network changes and mitigating potential disruptions caused by spanning-tree convergence delays.

### **Port Fast**

To expedite the connectivity of end-user devices connected via access ports, the PortFast feature has been implemented. This optimization allows these designated ports to bypass the standard Spanning Tree Protocol (STP) listening and learning stages, thereby enabling immediate data forwarding upon link establishment.

### **BPDU Guard**

To enhance the security posture of the network infrastructure, the Bridge Protocol Data Unit (BPDU) Guard feature has been implemented. This security mechanism actively protects against potential BPDU attacks by automatically disabling any port that receives unexpected or unauthorized BPDU frames, thereby preventing malicious manipulation of the spanning-tree topology.

### **Port Security**

To further fortify network access control, Port Security has been implemented on access ports. This security feature restricts the number of permissible MAC addresses that can be associated with a given port, effectively preventing the connection of unauthorized devices and mitigating potential security breaches.

### **LACP & PAgP**

Link Aggregation Control Protocol (LACP) and Port Aggregation Protocol (PAgP) have been implemented to establish EtherChannels between network switches.<sup>1</sup> These link aggregation protocols serve to aggregate multiple physical links into a single logical channel, thereby providing both enhanced bandwidth capacity and improved redundancy in the inter-switch connections.

### **VLANs With VTPv2**


The network infrastructure employs Virtual Local Area Networks (VLANs) to logically segment network resources based on departmental affiliation. These VLANs, including those designated for Marketing, Finance, Legal, Administration, Development, and Guest access, are centrally managed through the VLAN Trunking Protocol version 2 (VTPv2). This centralized approach streamlines VLAN configuration, ensures consistency across network devices, and simplifies the administration of network segmentation.

## Inter-VLAN Routing

To facilitate secure and controlled inter-VLAN communication, a Layer 3 switching infrastructure has been implemented. This strategic deployment of a Layer 3 switch enables the establishment of defined routing pathways, thereby allowing for the necessary exchange of data between disparate Virtual Local Area Networks while maintaining robust security protocols and network segmentation.

## Wireless Connectivity

Wireless Access Points (APs) provide Wi-Fi connectivity for both employees and guests. To ensure network security, visitor traffic is segregated from the corporate network through the implementation of Virtual Local Area Networks (VLANs). This isolation is facilitated by Lightweight Access Points (LWAPs) operating under the management of a Wireless LAN Controller (WLC) via the Control and Provisioning of Wireless Access Points (CAPWAP) protocol.



150 Access Points Supported

### Controller Summary

Management IP Address	192.168.1.4 , ::/128
Software Version	8.3.111.0
Field Recovery Image Version	7.6.101.1
System Name	Real-Estate
Up Time	45 minutes, 58 seconds
System Time	Fri Mar 7 19:50:10 2025
Redundancy Mode	N/A
Internal Temperature	+31 C
802.11a Network State	Enabled
802.11b/g Network State	Enabled
Local Mobility Group	
CPU(s) Usage	0%
Individual CPU Usage	0%/1%, 0%/0%
Memory Usage	46%
Fan Status	3800 rpm

### Access Point Summary

	Total	Up	Down	
802.11a/n/ac Radios	6	6	0	<a href="#">Detail</a>
802.11b/g/n Radios	6	6	0	<a href="#">Detail</a>
Dual-Band Radios	0	0	0	<a href="#">Detail</a>
All APs	6	6	0	<a href="#">Detail</a>

802.1x Wireless Access

For enhanced security in the wireless network environment, 802.1x authentication has been implemented in conjunction with the RADIUS server. This industry-standard port-based network access control protocol requires users and devices to be authenticated and authorized before gaining access to the wireless network, with the RADIUS server providing centralized authentication and authorization services. This combination ensures that only verified and authorized entities can connect to the wireless infrastructure.

RADIUS Authentication Servers > Edit

Server Index

1

Server Address(Ipv4/Ipv6)

192.168.1.7

Shared Secret Format

ASCII

Shared Secret

...

Confirm Shared Secret

...

Key Wrap

☐ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

Port Number

1645

Server Status

Enabled

Support for CoA

Disabled

Server Timeout

2 seconds

Network User

☒ Enable

Management

☒ Enable

Management Retransmit Timeout

2 seconds

Realm List

IPSec

☐ Enable

Password Encryption Service

To enhance the security of stored credentials, a password encryption service has been implemented. This service utilizes the **service password-encryption** command to encrypt service passwords, thereby protecting sensitive authentication information from unauthorized access.

SYSLOG Service

A centralized SYSLOG service has been implemented to provide comprehensive logging and monitoring capabilities for network events. This service aggregates system messages from various network devices, facilitating efficient analysis, troubleshooting, and proactive identification of potential issues.

Syslog

Service

On

Off

Time	HostName	Message
1 05.12.2025 08:34:05.808 AM	192.168.2.18	%SYS-5-CONFIG_I: Configured from console by console

## DHCPv4 Service

A Dynamic Host Configuration Protocol (DHCP) server automatically assigns IP addresses and other network configuration parameters (like subnet masks and default gateways) to client devices. This reduces the need for manual IP configuration and ensures that devices in a network can communicate efficiently.

DHCP				
Interface	FastEthernet0			
Pool Name	VLAN 1			
Default Gateway	192.168.1.1			
DNS Server	192.168.1.7			
Start IP Address :	192	168	1	9
Subnet Mask:	255	255	255	192
Maximum Number of Users :	55			
TFTP Server:	192.168.1.7			
WLC Address:	192.168.1.4			

## DNS Service

A Domain Name System (DNS) server resolves human-readable domain names (like www.example.com) into machine-readable IP addresses. This process is essential for web browsing and network operations, as it allows devices to locate and communicate with others over the internet or internal networks.

DNS	
DNS Service	<input checked="" type="radio"/> On <input type="radio"/> Off
Resource Records	
Name	www.real.com
Type	A Record
Address	192.168.1.7

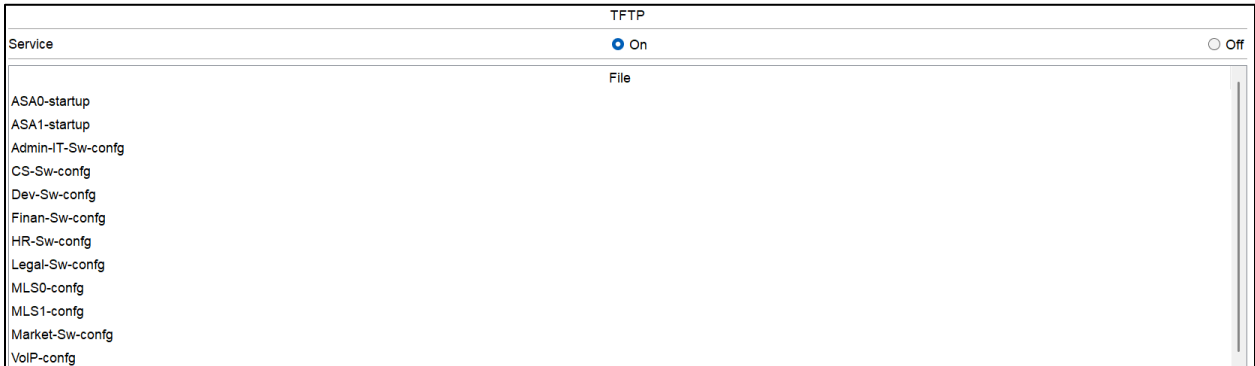
## NTP Service

To maintain temporal consistency across all network devices, the Network Time Protocol (NTP) service has been implemented. This protocol ensures accurate time synchronization throughout the network infrastructure, which is crucial for coordinated logging, security protocols, and overall system operation.

NTP						
Service	<input checked="" type="radio"/> On <input type="radio"/> Off					
Authentication	<input checked="" type="radio"/> Enable <input type="radio"/> Disable					
Key:	1		Password: 123			
May, 2025 03:53:13PM						
Sun	Mon	Tue	Wed	Thu	Fri	Sat
27	28	29	30	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

TFTP Service

A Trivial File Transfer Protocol (TFTP) service has been established to provide a centralized repository for the storage of network device configuration backups and Cisco IOS software images. This centralized storage solution simplifies the management of critical system files, facilitating efficient backup procedures, streamlined device restoration, and consistent software deployment across the network infrastructure.

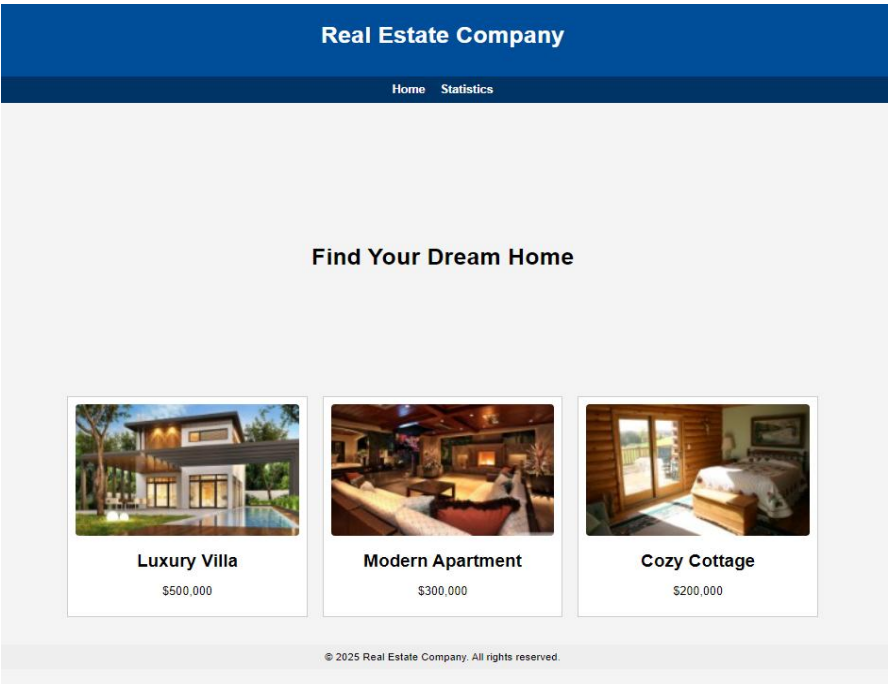


Timestamps Log & Debug Services

To facilitate more effective troubleshooting and analysis of network events, both system logs and debugging output are configured with precise timestamps. This inclusion of temporal information enables administrators to more accurately correlate events, trace issues chronologically, and gain a clearer understanding of the sequence of operations during diagnostic procedures.

Web Service

A web server hosts and delivers websites or web-based applications to users over the internet or intranet. It processes incoming HTTP/HTTPS requests, interprets them, and sends the appropriate content (web pages, images, scripts).



## **Email Service**

An email server handles the sending, receiving, and storage of emails. It allows users to communicate using email protocols such as SMTP (Simple Mail Transfer Protocol) for outgoing mail, and IMAP (Internet Messaging Access Protocol)/POP3 (Post Office Protocol) for incoming mail. Popular email servers include Microsoft Exchange and Postfix.

## **IP Phone Configurations**

To ensure optimal Quality of Service (QoS) and maintain the integrity of voice communications, dedicated voice VLANs have been implemented for IP phone configurations. This network segmentation strategy isolates voice traffic from data traffic, prioritizing voice packets to guarantee clear and reliable telephony services.

## **Shutdown Unused Ports**

As a proactive security measure, all switch ports that are not actively in use have been administratively shut down. This practice effectively mitigates the risk of unauthorized access to the network infrastructure through dormant physical connections.

## **Unused VLAN for Unused Ports**

To further enhance security and network isolation, all administratively disabled switch ports are assigned to a designated black-hole VLAN. This VLAN is configured with no routing capabilities or network access, ensuring that any inadvertent or unauthorized connection to these ports will not result in network connectivity or potential security breaches.

## **Disable Negotiation on Unused Ports**

To ensure operational stability and prevent potential security vulnerabilities on inactive network interfaces, the speed and duplex settings on all unused ports have been manually configured. Furthermore, the Dynamic Trunking Protocol (DTP) has been disabled on these ports, eliminating the possibility of unintended trunk negotiation and maintaining a secure and predictable port configuration.

## **Disable CDP & LLDP on Unused Ports**

To further minimize the network's attack surface and prevent potential reconnaissance activities, both Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP) have been disabled on all unused switch ports. This measure prevents the advertisement of device information on these inactive interfaces, thereby hindering attackers from easily mapping the network topology.

## **No IP Domain Lookup**

As previously stated, to further minimize the network's attack surface and prevent potential reconnaissance activities, both Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP) have been disabled on all unused switch ports. This measure prevents the advertisement of device information on these inactive interfaces, thereby hindering attackers from easily mapping the network topology.

### **Logging Synchronous**

To ensure a consistent and uninterrupted command-line interface experience, the **logging synchronous** command has been implemented. This configuration prevents unsolicited log messages from interrupting command input, thereby improving the efficiency and clarity of administrative tasks performed via the console.

### **Port Address Translation (PAT)**

To facilitate Internet access for multiple internal hosts while efficiently utilizing public IP address resources, Port Address Translation (PAT) has been implemented. This network address translation technique allows numerous private IP addresses within the internal network to be mapped to a single public IP address by using distinct port numbers, thereby enabling simultaneous communication with external networks.

### **Cisco ASA Firewall**

Cisco Adaptive Security Appliance (ASA) is a security device that combines firewall, and other network security services in a single platform. It provides advanced threat defence, intrusion prevention, and protects the network from attacks by monitoring, controlling, and filtering traffic.

### **Access Control Lists (ACLs)**

To enhance network security by implementing granular traffic control, Access Control Lists (ACLs) have been strategically deployed. These ACLs are configured to restrict both inter-VLAN communication and traffic destined for the Internet, thereby enforcing defined security policies and preventing unauthorized network access or data flow.

### **Open Shortest Path First (OSPF) Routing**

OSPF has been implemented as the dynamic routing protocol for internal routing operations between network routers and geographically dispersed sites. This link-state routing protocol facilitates the efficient and automatic determination of optimal routing paths based on network topology and link costs, ensuring resilient and scalable inter-site connectivity.

### **Static Route & Default Route**

To ensure predictable and controlled routing for specific network destinations, static routes have been configured. Additionally, a default route has been established to direct all traffic destined for the Internet, providing a gateway for external communication. This combination of static and default routing strategies allows for both precise traffic management and seamless access to external networks.

### **Site-to-Site VPN**

To establish a secure communication channel with a remote office location, a Site-to-Site Virtual Private Network (VPN) has been implemented utilizing the IP Security (IPsec) protocol. This VPN tunnel encrypts all network traffic traversing the public internet, ensuring the confidentiality and integrity of data exchanged between the primary and remote sites.

## SSHv2 Access

Secure Shell version 2 (SSHv2) has been implemented to provide encrypted remote Command-Line Interface (CLI) access to network devices. This secure protocol replaces the less secure Telnet, ensuring the confidentiality and integrity of management sessions conducted remotely.

## Session Timeout

To enhance security and optimize resource utilization, inactive management sessions on network devices are automatically terminated after a predefined period of inactivity. This session timeout policy helps to prevent unauthorized access through unattended sessions and ensures efficient allocation of system resources.

## AAA with RADIUS

For enhanced security and streamlined administration, a centralized Authentication, Authorization, and Accounting (AAA) framework has been implemented utilizing a Remote Authentication Dial-In User Service (RADIUS) server. This centralized system manages user authentication, enforces access control policies, and tracks user activity, providing a robust and auditable security solution.

AAA				
Service <input checked="" type="radio"/> On <input type="radio"/> Off		Radius Port 1645		
Network Configuration				
Client Name MLS1		Client IP 10.0.0.10		
Secret 123		ServerType Radius		
	Client Name	Client IP	Server Type	Key
1	MLS1	10.0.0.10	Radius	123
2	Market-Sw	192.168.1.132	Radius	123
3	Finan-Sw	192.168.1.164	Radius	123
4	HR-Sw	192.168.1.196	Radius	123
5	MLS0	192.168.1.1	Radius	123
6	CS-Sw	192.168.1.228	Radius	123
7	WLC	192.168.1.1	Radius	123
User Setup				
Username		Password		
	Username	Password		
1	alaa	1234		
2	ali	1234		
3	ezz	1234		
4	gomaa	1234		
5	khaled	1234		

## Console & VTY Login via RADIUS

To ensure consistent and centralized access control, all Command-Line Interface (CLI) login attempts, whether via the console port or virtual terminal lines (VTY) such as SSH, are authenticated through the designated RADIUS server. This unified authentication mechanism enforces consistent security policies across all management interfaces.

## Enable Secret Password

To enhance the security of privileged access, an encrypted secret password has been enabled for accessing the privileged EXEC mode on network devices. This robust encryption method



protects the administrative password from unauthorized disclosure, ensuring that only authorized personnel can gain elevated command-line privileges.

### **Logging Login Success/Failure**

To facilitate comprehensive security auditing and monitoring, all login attempts to network devices, including both successful and failed authentication attempts, are meticulously logged. This detailed logging provides valuable insights into access patterns and potential security incidents.

### **Account Lockout After Failed Attempts**

To mitigate the risk of brute-force password attacks, an account lockout policy has been implemented. This security measure automatically blocks user accounts for a specified duration after a predefined number of consecutive failed login attempts, thereby hindering automated attempts to compromise user credentials.

### **Minimum Password Length**

To bolster password security and reduce the likelihood of easily compromised credentials, a minimum password length requirement has been enforced across all user accounts on network devices. This policy mandates that passwords meet a specific character count, encouraging the use of stronger and more resilient authentication strings.

**To Download Project:** [Drive Link](#)