📌 PROJECT REPORT

Project Title:

Design and Implementation of a Secure and Scalable Network Infrastructure for Lakeview Hospital

Prepared By:

Enock Odongo

Network Engineering Student

Moi University

Student Registration Number: IS/2**2/23

Submitted To:

Praphul Mishra

Department of Information Technology

University of Wollongong in Dubai

Project Location:

Lakeview Hospital

Kisumu Town, Kisumu County, Kenya

Date of Submission:

23RD June, 2025

Academic Year:

2024/2025

Lakeview Hospital Enterprise Network Infrastructure Design & Implementation

This project showcases the design and implementation of a scalable, secure and highly available enterprise network infrastructure for Lakeview Hospital, a growing healthcare facility located in Kisumu, Kenya. The network is engineered using the three-tier hierarchical model; Core, Distribution and Access layers, to ensure performance, redundancy, manageability and future scalability for over 200 end-users across 10 departments, including Administration, Doctors, Nurses, Pharmacy, Laboratory, Radiology, Billing, Reception, IT and Management.

At the core of this architecture are two high-performance Layer 3 Core Routers configured for redundancy and load balancing. These core routers form the backbone of the network, connecting to two Distribution switches that facilitate inter-VLAN routing, segmentation and policy enforcement. The Access layer comprises multiple Layer 2 switches, each serving two distinct departments, ensuring efficient traffic management and broadcast containment using department-specific VLANs ranging from VLAN 10 to VLAN 100. In addition, a dedicated Management VLAN (VLAN 999) is deployed across all switches to centralize device administration securely via SSH and SNMP, isolated from user traffic.

For secure external communication, the network is protected by a Cisco ASA Firewall that connects to two redundant ISPs using static routing with priority-based failover. The ASA also manages traffic to a DMZ segment (VLAN 200) that hosts public-facing services like the clinic's website, patient portal and email servers. The DMZ is directly connected to the firewall via a dedicated access switch, with static NAT configured to translate internal private IPs to public IPs securely.

To support internal hospital systems such as Electronic Medical Records (EMR), Lab Information Systems (LIS) and radiology image storage, an additional internal server segment (VLAN 150) is connected to the distribution switches. This segment ensures isolated and fast access to critical applications for staff, while maintaining a layered security posture. Each device in the infrastructure; routers, switches and firewalls, is hardened using best security practices including SSH-only access, disabled unused services, secure password policies, banner warnings and logging. And other security measured to prevent modern evolving cyber threats

This professional-grade hospital network design not only meets the current operational needs of the clinic but also lays the groundwork for future expansion, such as cloud integration, IoT-based medical devices and advanced network monitoring. It exemplifies modern networking principles, security-focused architecture and industry-aligned documentation, making it a cornerstone project in my professional portfolio as a network engineer.

Network Requirements and Objectives

The design of the Lakeview Hospital enterprise network is driven by a comprehensive set of functional, technical and security requirements aimed at supporting the current operational needs of the clinic while providing scalability for future growth. The primary objective is to establish a robust, secure and highly available infrastructure that ensures uninterrupted access to critical healthcare applications, supports over 200 users across 10 departments and adheres to industry best practices for network design and data protection.

Functional Requirements

The network must provide seamless connectivity across all departments; Administration, Doctors, Nurses, Pharmacy, Laboratory, Radiology, Billing, Reception, IT and Management, ensuring that each department operates within its own isolated VLAN for optimized performance and security. Internal applications such as Electronic Medical Records (EMR), lab information systems and imaging systems must be reliably accessible from various departmental endpoints. The network must support both wired and potentially wireless users, with clear traffic segmentation and Quality of Service (QoS) to prioritize time-sensitive healthcare data and VoIP communication.

Scalability and Redundancy

The design must accommodate growth beyond the initial 200 users, allowing easy addition of new departments, users and services without major redesign. Redundant links between the core and distribution layers, as well as failover mechanisms for Internet connectivity via dual ISPs, are essential to minimize downtime and ensure high availability. The use of modular switches and hierarchical structure ensures scalability and maintainability as the clinic expands.

Security Requirements

Given the sensitive nature of patient data and healthcare systems, the network must implement strong security measures at every layer. Each department is logically segmented via VLANs to contain broadcast traffic and minimize potential internal threats. A dedicated DMZ, protected by a Cisco ASA Firewall, hosts public-facing servers such as the clinic's website and email services, segregated from internal systems. The firewall enforces access control policies, performs NAT and provides intrusion prevention capabilities. Device hardening techniques are implemented on all routers and switches to prevent unauthorized access and reduce attack surfaces.

Management and Monitoring

A dedicated Management VLAN is used to manage network devices, accessible only by the IT department. SSH, SNMP and syslog are configured for secure administration, remote logging and performance monitoring. The network must support centralized monitoring tools and future integration with Network Access Control (NAC) and endpoint security solutions.

This requirements phase forms the blueprint for the subsequent design, configuration and testing of the Lakeview Hospital network infrastructure.

DEVICES USED IN THE PROJECT

1. Cisco ASA Firewall – Qty: 1

Function- Acts as the network’s perimeter defense, connecting to two ISPs and enforcing security policies between internal networks, the DMZ and the internet. Handles NAT, ACLs, VPNs and DMZ segregation.

2. ISP Routers – Qty: 2

Function- Represent two independent Internet Service Providers (Primary and Secondary) for redundancy and load balancing. Connect to the ASA firewall and simulate internet access.

3. Core Routers (Cisco ISR Series) – Qty: 2

Function- Provide Layer 3 routing and inter-VLAN communication between distribution switches. Implement HSRP for gateway redundancy and route traffic between internal and external networks.

4. Distribution Layer Switches (Cisco Catalyst L3) – Qty: 2

Function- Aggregate and route traffic between access switches and core routers. Handle inter-VLAN routing, DHCP relay, redundancy (HSRP) and policy-based routing for departments.

5. Access Layer Switches – Qty: 7

- Departmental Access Switches (Qty: 5)

Function- Connect end devices (PCs, printers, etc.) from 10 departments to the network. Apply VLAN segmentation and port security.

- DMZ Access Switch (Qty: 1)

Function- Hosts public-facing servers (e.g., web, portal and email) in the DMZ, connecting directly to the ASA.

- Internal Server Access Switch (Qty: 1)

Function- Connects internal servers (EMR, DHCP, DNS, etc.) in the secure server room to the distribution layer.

6. End Devices – Qty: 200+

Function- Departmental PCs and printers used by hospital staff. Receive IPs dynamically from DHCP and communicate within segmented VLANs.

7. Servers – Qty: 6+

Function- Includes DHCP, DNS, EMR system, Database, Web and Mail servers. Internal servers use static IPs and are secured behind the firewall; DMZ servers are publicly accessible with restricted ACLs.

8. DHCP Server – Qty: 1

Function- Located in the server room, assigns IP addresses dynamically to end devices across all VLANs via DHCP relay.

9. Network Administrator Workstation – Qty: 1

Function- Used for managing network devices remotely via SSH through the Management VLAN. Also used for monitoring, configuration backups and updates.

Logical and Physical Network Design

The Logical and Physical Network Design section presents a clear, structured and professional view of how the network is architected to meet the clinic's requirements. It explains both the abstract (logical) connectivity, such as IP addressing, VLAN structure and routing domains and the physical layout, including device roles, cabling and interface connections.

1. Logical Network Design

The logical design is based on the three-tier hierarchical model: Core, Distribution and Access layers. This model ensures separation of concerns, scalability and simplified troubleshooting. (**Cisco Packet Tracer & GNS3**)

Core Layer

Composed of two high-availability Layer 3 core routers (Core1 and Core2) responsible for fast, fault-tolerant backbone routing. They interconnect all distribution switches and route inter-VLAN traffic.

Distribution Layer

Includes two multilayer switches (Dist1 and Dist2) that aggregate access layer traffic and perform routing between VLANs. Redundant links to the core layer ensure resiliency using routed point-to-point links (/29 subnets).

Access Layer

Comprises six access switches

Five switches connect end-users from 10 departments (2 departments per switch).

One switch connects internal servers (VLAN 150).

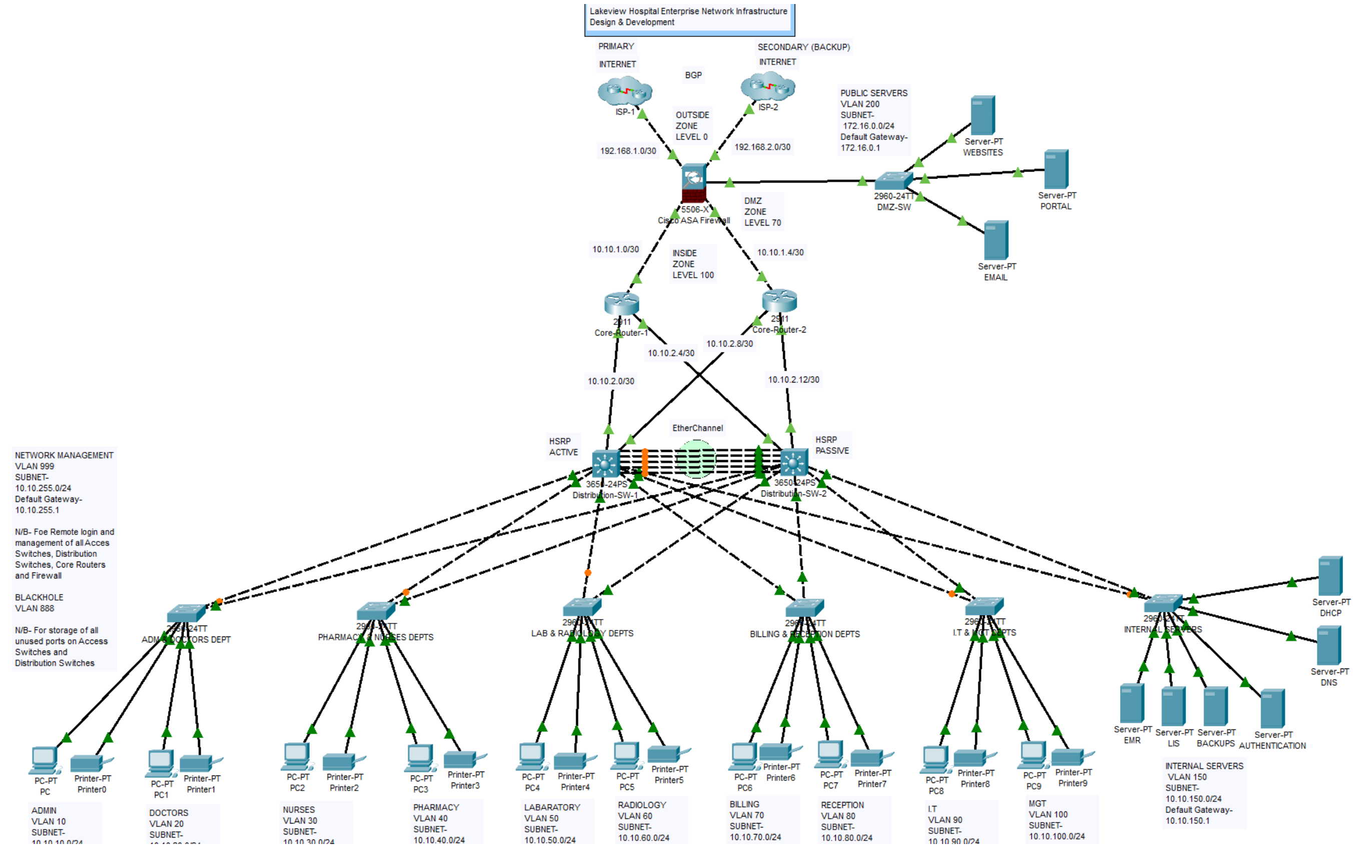
Another access switch connected directly to the ASA firewall handles DMZ services (VLAN 200).

VLANs and Subnets

Each department is assigned a dedicated VLAN with a /24 subnet. Inter-VLAN routing is handled by the distribution layer. A management VLAN (999) and two additional VLANs for DMZ (200) and internal servers (150) are included.

Firewall and ISPs

A Cisco ASA Firewall connects the internal network to two ISPs using static routing with primary/secondary failover. It also segments the DMZ using a dedicated interface and VLAN.


Lakeview Hospital Enterprise Network Infrastructure Design & Development
PRIMARY
INTERNET
SECONDARY (BACKUP)
INTERNET
BGP
ISP-1
ISP-2
OUTSIDE ZONE LEVEL 0
192.168.1.0/30
192.168.2.0/30
PUBLIC SERVERS VLAN 200 SUBNET- 172.16.0.0/24 Default Gateway- 172.16.0.1
Server-PT WEBSITES
Server-PT PORTAL
Server-PT EMAIL
2960-24TT DMZ-SW
5506-X Cisco ASA Firewall
DMZ ZONE LEVEL 70
10.10.1.0/30
INSIDE ZONE LEVEL 100
10.10.1.4/30
2911 Core-Router-1
2911 Core-Router-2
10.10.2.4/30
10.10.2.8/30
10.10.2.0/30
10.10.2.12/30
EtherChannel
HSRP ACTIVE
HSRP PASSIVE
3650-24PS Distribution-SW-1
3650-24PS Distribution-SW-2
NETWORK MANAGEMENT VLAN 999 SUBNET- 10.10.255.0/24 Default Gateway- 10.10.255.1
N/B- Foe Remote login and management of all Acces Switches, Distribution Switches, Core Routers and Firewall
BLACKHOLE VLAN 888
N/B- For storage of all unused ports on Access Switches and Distribution Switches
2960-24TT ADMIN & DOCTORS DEPT
2960-24TT PHARMACY & NURSES DEPTS
2960-24TT LAB & RADIOLOGY DEPTS
2960-24TT BILLING & RECEPTION DEPTS
2960-24TT I.T & MGT DEPTS
2960-24TT INTERNAL SERVERS
Server-PT DHCP
Server-PT DNS
Server-PT EMR
Server-PT LIS
Server-PT BACKUPS
Server-PT AUTHENTICATION
PC-PT PC
Printer-PT Printer0
PC-PT PC1
Printer-PT Printer1
PC-PT PC2
Printer-PT Printer2
PC-PT PC3
Printer-PT Printer3
PC-PT PC4
Printer-PT Printer4
PC-PT PC5
Printer-PT Printer5
PC-PT PC6
Printer-PT Printer6
PC-PT PC7
Printer-PT Printer7
PC-PT PC8
Printer-PT Printer8
PC-PT PC9
Printer-PT Printer9
ADMIN VLAN 10 SUBNET- 10.10.10.0/24
DOCTORS VLAN 20 SUBNET- 10.10.20.0/24
NURSES VLAN 30 SUBNET- 10.10.30.0/24
PHARMACY VLAN 40 SUBNET- 10.10.40.0/24
LABARATORY VLAN 50 SUBNET- 10.10.50.0/24
RADIOLOGY VLAN 60 SUBNET- 10.10.60.0/24
BILLING VLAN 70 SUBNET- 10.10.70.0/24
RECEPTION VLAN 80 SUBNET- 10.10.80.0/24
I.T VLAN 90 SUBNET- 10.10.90.0/24
MGT VLAN 100 SUBNET- 10.10.100.0/24
INTERNAL SERVERS VLAN 150 SUBNET- 10.10.150.0/24 Default Gateway- 10.10.150.1

2. Physical Network Design

Core routers are placed centrally in the main server room, connected via fiber to both distribution switches.

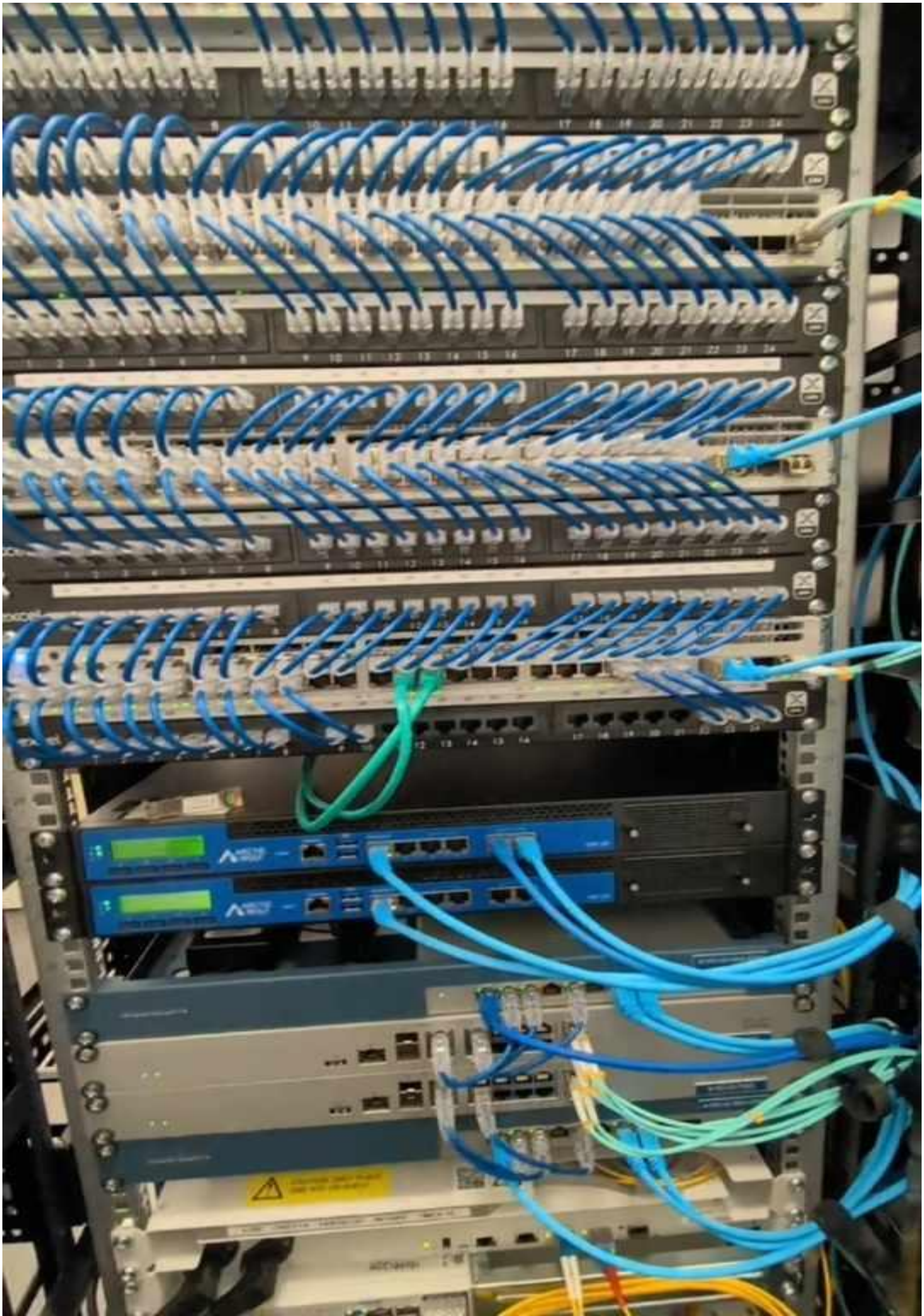
Distribution Switches are housed in the same data center rack and connected to all access switches via redundant uplinks (copper or fiber depending on distance).

Access Switches are distributed across different floors or wings of the clinic, each serving user endpoints in their assigned departments.

Firewall is placed at the network perimeter, directly connected to the core and ISP routers. The DMZ switch physically connects to a dedicated ASA interface.

Servers are located in a secure data center room and connected to their own access switch, which uplinks to both distribution switches.

This clean, modular design ensures high performance, resilience and future scalability while aligning with Cisco best practices and industry standards for healthcare network.


excel

Subnetting, IP Addressing and VLAN Design

This section outlines the structured IP addressing scheme and VLAN architecture used in the Lakeview Medical Clinic network. A well-organized VLAN and subnetting strategy ensures logical segmentation, efficient traffic management, enhanced security and simplified network administration. Each department is assigned a unique VLAN with a corresponding /24 subnet, providing up to 254 usable IP addresses per department, more than sufficient for current needs and future growth. Additionally, specialized VLANs are designated for servers, management and the DMZ.

1. Subnetting Strategy

A private IP addressing scheme (RFC 1918) is used throughout the internal network to conserve public IPs and enhance security. Subnets are assigned based on department functions and network roles. The structure allows for logical grouping and simplifies access control.

VLAN ID	Department	Subnet	Default Gateway	Notes
10	Administration	10.10.10.0/24	10.10.10.1	Staff computers, printers
20	Doctors	10.10.20.0/24	10.10.20.1	Medical PCs, tablets
30	Nurses	10.10.30.0/24	10.10.30.1	Nurse stations
40	Pharmacy	10.10.40.0/24	10.10.40.1	POS, drug inventory systems
50	Laboratory	10.10.50.0/24	10.10.50.1	Lab terminals, analyzers
60	Radiology	10.10.60.0/24	10.10.60.1	Imaging systems, PACS
70	Billing	10.10.70.0/24	10.10.70.1	Billing and finance devices
80	Reception	10.10.80.0/24	10.10.80.1	Front desk workstations
90	IT Department	10.10.90.0/24	10.10.90.1	Admin PCs, tools
100	Management	10.10.100.0/24	10.10.100.1	Executive offices
150	Internal Servers	10.10.150.0/24	10.10.150.1	EMR, LIS, backup systems
200	DMZ (Public Servers)	172.16.0.0/24	172.16.0.1	Website, portal, email
999	Network Management	10.10.255.0/24	10.10.255.1	Switch/router/firewall access
888	**BLACKHOLE**	*****	****	**Storing all unused ports**

2. Point-to-Point Subnetting

To support routing and redundancy between layers, smaller subnets (/30 or /29) are used for point-to-point links

Link Segment	Subnet	Interface IPs	Notes
ISP1 ↔ ASA Firewall	192.168.1.0/30	ISP1- 192.168.1.1 ASA- 192.168.1.2	Primary Internet connection
ISP2 ↔ ASA Firewall	192.168.2.0/30	ISP2- 192.168.2.1 ASA- 192.168.2.2	Secondary (backup) connection
ASA Firewall ↔ Core1 Router	10.10.1.0/30	ASA- 10.10.1.1 Core1- 10.10.1.2	Trusted zone uplink
ASA Firewall ↔ Core2 Router	10.10.1.4/30	ASA- 10.10.1.5 Core2- 10.10.1.6	Trusted zone uplink (redundant)
Core1 ↔ Dist1 Switch	10.10.2.0/30	Core1- 10.10.2.1 Dist1- 10.10.2.2	Core to distribution path
Core1 ↔ Dist2 Switch	10.10.2.4/30	Core1- 10.10.2.5 Dist2- 10.10.2.6	Redundant core-to-distribution path
Core2 ↔ Dist1 Switch	10.10.2.8/30	Core2- 10.10.2.9 Dist1- 10.10.2.10	Redundant core-to-distribution path
Core2 ↔ Dist2 Switch	10.10.2.12/30	Core2- 10.10.2.13 Dist2- 10.10.2.14	Core to distribution path

3. VLAN Naming Convention

Each VLAN is assigned a descriptive name for clarity in configuration and troubleshooting

VLAN ID	VLAN Name
10	ADMIN
20	DOCTORS
30	NURSES
40	PHARMACY
50	LAB
60	RADIOLOGY
70	BILLING
80	RECEPTION
90	IT
100	MANAGEMENT
150	SERVERS
200	DMZ
999	MGMT
888	**BLACKHOLE (UNUSED SWITCH PORTS)**

Device Configuration and Implementation

This section details the structured, secure and scalable configuration of all critical network devices, core routers, distribution and access switches, the ASA firewall and VLAN infrastructure. Following Cisco best practices, the implementation ensures high availability, effective segmentation and robust security for Lakeview Hospital's three-tier network.

End-user devices across all departmental VLANs will obtain **IP addresses dynamically** through a centralized DHCP server located in the internal server room. This server resides within the SERVERS VLAN (VLAN 150) and is connected to the internal access switch, which uplinks to the distribution layer. DHCP relay (IP helper address) is configured on the distribution switches to forward DHCP requests from all VLANs to the server. This setup ensures centralized IP management, simplifies administration and supports scalability as new devices join the network.

All server devices located in the internal server room and the DMZ are to be configured with **static IP addresses**. This ensures reliability, ease of access and consistency in network services such as DNS, DHCP, EMR systems and web applications. Static IP configuration eliminates the risk of IP address changes that can interrupt critical hospital operations or external accessibility. Servers in the SERVERS VLAN (VLAN 150) and DMZ VLAN (VLAN 200) will each be assigned fixed IPs within their subnet range, ensuring proper routing, NAT and firewall policy application. These settings will be documented for ongoing maintenance and disaster recovery.

In this project, devices were configured using a combination of manual **CLI configuration**, best practice templates and layered security policies. All routers, switches, and the ASA firewall were accessed via console (terminal) using PuTTY or SSH and configured using Cisco IOS and ASA OS commands. A structured approach was followed, starting with interface setup, VLAN creation, IP addressing, routing, DHCP relay and HSRP for redundancy. Security was implemented through port security, ACLs, SSH access, password encryption and service hardening. Management access was centralized via a dedicated Management VLAN. Each configuration step adhered to Cisco network design and security standards for enterprise-level environments.

############ CONFIG STEPS ############

1. Basic settings to all devices plus ssh on the routers and L3 switches.

2. VLAN assignment plus all access and trunk ports on L2 and L3 switches.

3. EtherChannel between the distribution switches.

4. Switchport security to all departmental switches.

5. Subnetting and IP addressing.

6. OSPF on the routers and L3 switches.

7. Static IP address to Server-Room devices.

8. DHCP server device configurations.

9. Inter-VLAN routing on the L3 switches plus ip dhcp helper-address.

10. Firewall configurations

11. Port Address Translation (PAT) + Access Control List (ACL).

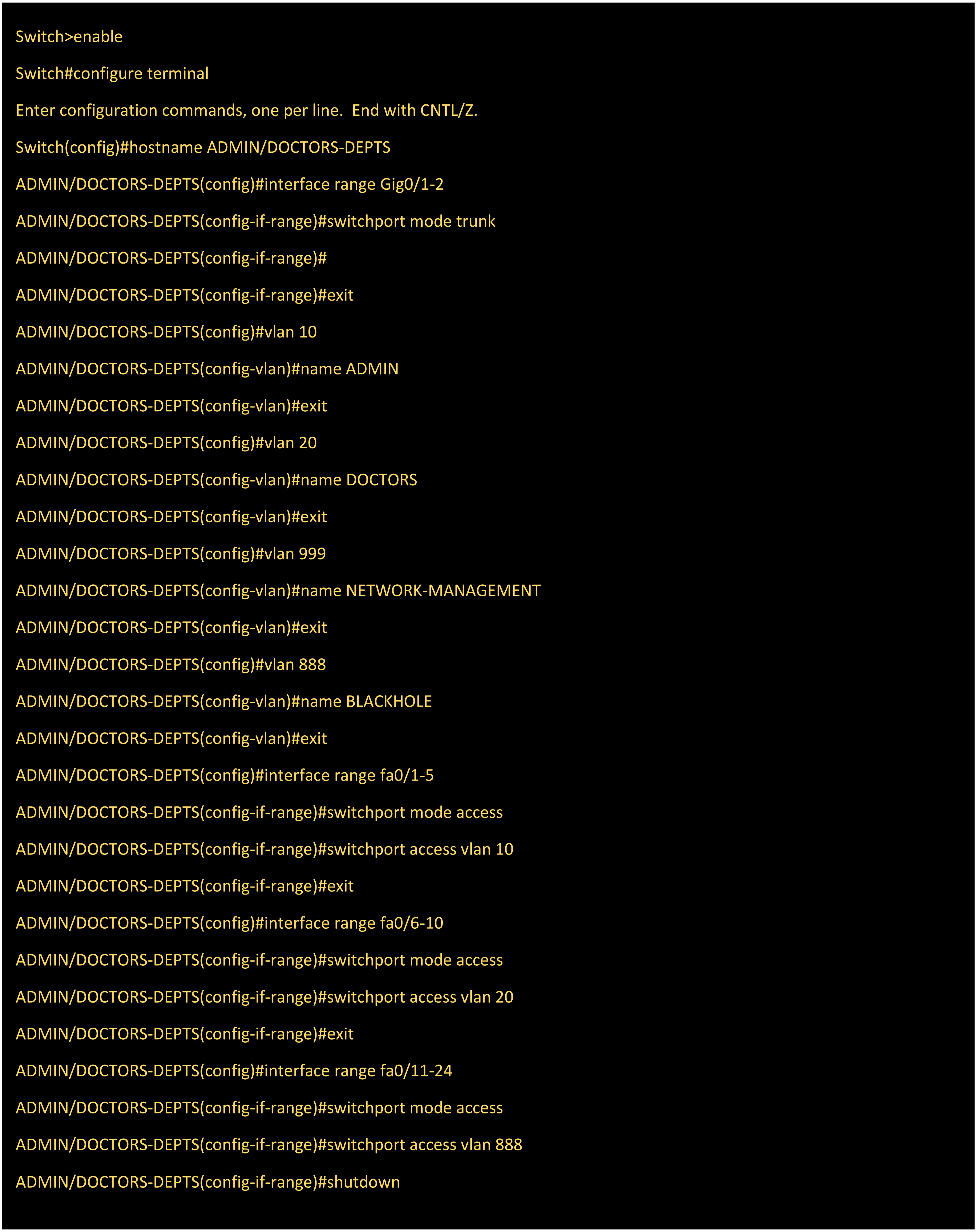
12. Default static route to the internet

13. Network security and device hardening

14. Verifying and Testing Configurations.

VLAN assignment plus all access and trunk ports on access and distribution switches

VLANs are assigned per department, isolating traffic and improving security. Access ports on access switches are configured for specific VLANs, while trunk ports connect access to distribution switches, allowing multiple VLANs. Distribution switches aggregate traffic and also use trunks to interconnect, ensuring VLAN propagation and efficient Layer 2 communication across the network. For this project, I have demonstrated with 1 access switch and 1 distribution switch only.



```
Switch>enable

Switch#configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Switch(config)#hostname ADMIN/DOCTORS-DEPTS

ADMIN/DOCTORS-DEPTS(config)#interface range Gig0/1-2

ADMIN/DOCTORS-DEPTS(config-if-range)#switchport mode trunk

ADMIN/DOCTORS-DEPTS(config-if-range)#

ADMIN/DOCTORS-DEPTS(config-if-range)#exit

ADMIN/DOCTORS-DEPTS(config)#vlan 10

ADMIN/DOCTORS-DEPTS(config-vlan)#name ADMIN

ADMIN/DOCTORS-DEPTS(config-vlan)#exit

ADMIN/DOCTORS-DEPTS(config)#vlan 20

ADMIN/DOCTORS-DEPTS(config-vlan)#name DOCTORS

ADMIN/DOCTORS-DEPTS(config-vlan)#exit

ADMIN/DOCTORS-DEPTS(config)#vlan 999

ADMIN/DOCTORS-DEPTS(config-vlan)#name NETWORK-MANAGEMENT

ADMIN/DOCTORS-DEPTS(config-vlan)#exit

ADMIN/DOCTORS-DEPTS(config)#vlan 888

ADMIN/DOCTORS-DEPTS(config-vlan)#name BLACKHOLE

ADMIN/DOCTORS-DEPTS(config-vlan)#exit

ADMIN/DOCTORS-DEPTS(config)#interface range fa0/1-5

ADMIN/DOCTORS-DEPTS(config-if-range)#switchport mode access

ADMIN/DOCTORS-DEPTS(config-if-range)#switchport access vlan 10

ADMIN/DOCTORS-DEPTS(config-if-range)#exit

ADMIN/DOCTORS-DEPTS(config)#interface range fa0/6-10

ADMIN/DOCTORS-DEPTS(config-if-range)#switchport mode access

ADMIN/DOCTORS-DEPTS(config-if-range)#switchport access vlan 20

ADMIN/DOCTORS-DEPTS(config-if-range)#exit

ADMIN/DOCTORS-DEPTS(config)#interface range fa0/11-24

ADMIN/DOCTORS-DEPTS(config-if-range)#switchport mode access

ADMIN/DOCTORS-DEPTS(config-if-range)#switchport access vlan 888

ADMIN/DOCTORS-DEPTS(config-if-range)#shutdown
```

VLANs verifications

```
ADMIN/DOCTORS-DEPTS(config)#do show vlan brief

VLAN Name                          Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
10   ADMIN                            active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5
20   DOCTORS                          active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10
888  BLACKHOLE                        active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24
999  NETWORK-MANAGEMENT               active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Distribution switches 1 & 2

```
Switch>enable

Switch#configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Switch(config)#hostname DISTRIBUTION-SW-2

DISTRIBUTION-SW-2(config)#interface range gig1/0/3-8

DISTRIBUTION-SW-2(config-if-range)#switchport mode trunk

DISTRIBUTION-SW-2(config-if-range)#switchport trunk allowed vlan
10,20,30,40,50,60,70,80,90,100,150,999

DISTRIBUTION-SW-2(config-if-range)#exit
```

VLANs Verification

```
DISTRIBUTION-SW-1(config)#do show vlan brief

VLAN Name                             Status    Ports

---- -------------------------------- --------- -------------------------------

1    default                          active    Gig1/0/1, Gig1/0/2, 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   ADMIN                            active

20   DOCTORS                          active

30   NURSES                           active

40   PHARMACY                         active

50   LABORATORY                       active

60   RADIOLOGY                        active

70   BILLING                          active

80   RECEPTION                        active
```

EtherChannel on the distribution switches

EtherChannel is a technology that allows you to combine multiple physical Ethernet links into a single logical link to increase bandwidth and provide redundancy. It prevents STP from blocking individual links by treating them as one logical interface. If one link fails, traffic continues on the remaining links without disruption. EtherChannel supports load balancing and is commonly used between switches, routers and servers

On distribution switch 1

```
DISTRIBUTION-SW-1>enable

DISTRIBUTION-SW-1#configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

DISTRIBUTION-SW-1(config)#interface range gig1/0/9-13

DISTRIBUTION-SW-1(config-if-range)#channel-group 1 mode active

DISTRIBUTION-SW-1(config-if-range)#exit

DISTRIBUTION-SW-1(config)#interface port-channel 1

DISTRIBUTION-SW-1(config-if)#switchport mode trunk

DISTRIBUTION-SW-1(config-if)#exit

DISTRIBUTION-SW-1(config)#do write

Building configuration...

Compressed configuration from 7383 bytes to 3601 bytes[OK]
```

On distribution switch 2

```
DISTRIBUTION-SW-2>enable

DISTRIBUTION-SW-2#configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

DISTRIBUTION-SW-2(config)#interface range gig1/0/9-13

DISTRIBUTION-SW-2(config-if-range)#channel-group 1 mode passive

DISTRIBUTION-SW-2(config-if-range)#exit

DISTRIBUTION-SW-2(config)#interface port-channel 1

DISTRIBUTION-SW-2(config-if)#switchport mode trunk

DISTRIBUTION-SW-2(config-if)#exit

DISTRIBUTION-SW-2(config)#do write

Creating a port-channel interface Port-channel 1
```

SUBNETTING & IP ADDRESSING

The hospital network is subnetted using a structured and scalable approach based on departmental VLANs and point-to-point links. Each department is assigned a unique /24 subnet, ensuring 254 usable IP addresses per VLAN for user devices. The DHCP server in the internal server room dynamically assigns IPs to end-user devices, while all servers in VLAN 150 (INTERNAL SERVERS) and VLAN 200 (DMZ) use static IP addressing. Point-to-point links between ASA, core routers and distribution switches use /30 subnets for efficient address utilization. Management VLAN (999) and BLACKHOLE VLAN (888) are reserved for device control and security enforcement, respectively.

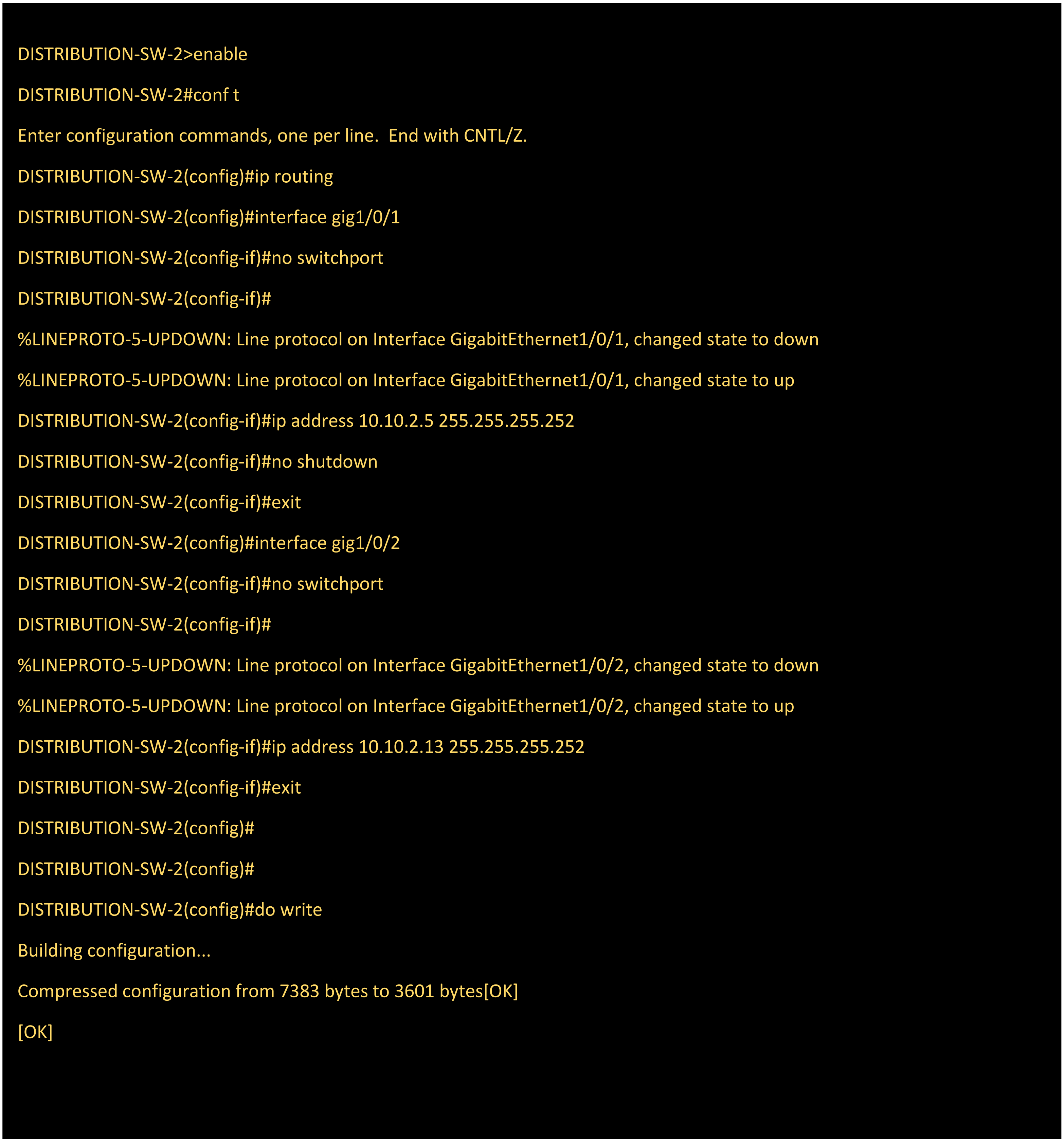
Management VLAN IP address (from VLAN 999) will be configured on each Access switch, Distribution switches, Core routers and ASA firewall devices as a Switched Virtual Interface (SVI) or management interface each having a unique IP Address. This IP allows centralized SSH remote access for administrative tasks.

```
interface vlan 999
 ip address 10.10.255.X 255.255.255.0   ! Assign a unique IP for each device
 no shutdown
ip default-gateway 10.10.255.1          ! Gateway on distribution switch/router
```

Verification

```
DISTRIBUTION-SW-2(config)#do show ip interface brief | exclude unassigned
Interface            IP-Address      OK?  Method   Status             Protocol
Vlan999              10.10.255.10    YES  manual   up                 up
```

Configuring IP Address on the Distribution Switch interfaces



```
DISTRIBUTION-SW-2>enable

DISTRIBUTION-SW-2#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

DISTRIBUTION-SW-2(config)#ip routing

DISTRIBUTION-SW-2(config)#interface gig1/0/1

DISTRIBUTION-SW-2(config-if)#no switchport

DISTRIBUTION-SW-2(config-if)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to up

DISTRIBUTION-SW-2(config-if)#ip address 10.10.2.5 255.255.255.252

DISTRIBUTION-SW-2(config-if)#no shutdown

DISTRIBUTION-SW-2(config-if)#exit

DISTRIBUTION-SW-2(config)#interface gig1/0/2

DISTRIBUTION-SW-2(config-if)#no switchport

DISTRIBUTION-SW-2(config-if)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/2, changed state to up

DISTRIBUTION-SW-2(config-if)#ip address 10.10.2.13 255.255.255.252

DISTRIBUTION-SW-2(config-if)#exit

DISTRIBUTION-SW-2(config)#

DISTRIBUTION-SW-2(config)#

DISTRIBUTION-SW-2(config)#do write

Building configuration...

Compressed configuration from 7383 bytes to 3601 bytes[OK]

[OK]
```

Interface Verification on the Distribution Switches

```
DISTRIBUTION-SW-2(config)#do show ip interface brief | exclude unassigned
Interface              IP-Address      OK? Method   Status          Protocol
GigabitEthernet1/0/1   10.10.2.5       YES manual   up              up
GigabitEthernet1/0/2   10.10.2.13      YES manual   up              up
Vlan999                10.10.255.10    YES manual   up              up
```

Configuring IP Address on the Core Routers interfaces

```
Router>enable

Router#configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)#hostname CORE-ROUTER-2

CORE-ROUTER-2(config)#interface Loopback1

CORE-ROUTER-2(config-if)#

%LINK-5-CHANGED: Interface Loopback1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up

CORE-ROUTER-2(config-if)#ip address 10.10.255.12 255.255.255.0

CORE-ROUTER-2(config-if)#exit

CORE-ROUTER-2(config)#interface gig0/0

CORE-ROUTER-2(config-if)#ip address 10.10.1.5 255.255.255.252

CORE-ROUTER-2(config-if)#exit

CORE-ROUTER-2(config)#interface gig0/1

CORE-ROUTER-2(config-if)#ip address 10.10.2.10 255.255.255.252

CORE-ROUTER-2(config-if)#exit

CORE-ROUTER-2(config)#interface gig0/2

CORE-ROUTER-2(config-if)#ip address 10.10.2.14 255.255.255.252

CORE-ROUTER-2(config-if)#no shutdown

CORE-ROUTER-2(config-if)#exit

CORE-ROUTER-2(config)#do write

Building configuration...

[OK]
```

Interface Verification on the Core Routers

```
CORE-ROUTER-2(config)#do show ip interface brief | exclude unassigned

Interface              IP-Address      OK?   Method Status          Protocol

GigabitEthernet0/0     10.10.1.5       YES    manual up              up

GigabitEthernet0/1     10.10.2.10      YES    manual up              up

GigabitEthernet0/2     10.10.2.14      YES   manual up               up

Loopback1              10.10.255.12    YES   manual up               up
```

Configuring IP Address on the ASA Firewall interfaces

```
ciscoasa>enable

Password:

ciscoasa#configure terminal

ciscoasa(config)#interface gig1/1

ciscoasa(config-if)#no shutdown

ciscoasa(config-if)#ip address 192.168.1.1 255.255.255.252

ciscoasa(config-if)#nameif OUTSIDE1

INFO: Security level for "OUTSIDE1" set to 0 by default.

ciscoasa(config-if)#security-level 0

ciscoasa(config-if)#exit

ciscoasa(config)#interface gig1/2

ciscoasa(config-if)#no shutdown

ciscoasa(config-if)#ip address 192.168.2.1 255.255.255.252

ciscoasa(config-if)#nameif OUTSIDE2

INFO: Security level for "OUTSIDE2" set to 0 by default.

ciscoasa(config-if)#security-level 0

ciscoasa(config-if)#exit

ciscoasa(config)#interface gig1/3

ciscoasa(config-if)#no shutdown

ciscoasa(config-if)#ip address 172.16.0.1 255.255.255.0

ciscoasa(config-if)#nameif DMZ

INFO: Security level for "DMZ" set to 0 by default.

ciscoasa(config-if)#security-level 70

ciscoasa(config-if)#exit

ciscoasa(config)#interface gig1/4

ciscoasa(config-if)#no shutdown

ciscoasa(config-if)#ip address 10.10.1.2 255.255.255.252

ciscoasa(config-if)#nameif INSIDE1

INFO: Security level for "INSIDE1" set to 0 by default.

ciscoasa(config-if)#security-level 100

ciscoasa(config-if)#exit

ciscoasa(config)#interface gig1/5

ciscoasa(config-if)#no shutdown

ciscoasa(config-if)#ip address 10.10.1.6 255.255.255.252
```

Configuring IP Address on the ISP interfaces

```
Router>enable

Router#configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)#hostname ISP-2

ISP-2(config)#interface Loopback1

ISP-2(config-if)#

%LINK-5-CHANGED: Interface Loopback1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up

ISP-2(config-if)#ip address 8.8.8.8 255.255.255.255

ISP-2(config-if)#no shutdown

ISP-2(config-if)#exit

ISP-2(config)#interface gig0/0

ISP-2(config-if)#ip address 192.168.2.2 255.255.255.252

ISP-2(config-if)#no shutdown

ISP-2(config-if)#exit

ISP-2(config)#do write

Building configuration...

[OK]
```

Interface verification

```
ISP-2(config)#do show ip interface brief | exclude unassigned
Interface              IP-Address      OK?    Method Status           Protocol
GigabitEthernet0/0     192.168.2.2     YES     manual up              up
Loopback1              8.8.8.8         YES     manual up              up
```

HSRP and Inter-VLAN routing on the layer 3 switches plus ip dhcp helper addresses

Hot Standby Router Protocol (HSRP) provides gateway redundancy on Layer 3 switches by allowing one switch to act as active and another as standby. Inter-VLAN routing enables communication between VLANs by assigning SVIs (Switched Virtual Interfaces) on the Layer 3 switch. To support DHCP for VLAN clients, IP helper addresses are configured on each SVI to forward DHCP requests to a centralized DHCP server. This setup ensures high availability, proper inter-VLAN communication and dynamic IP address allocation across VLANs. HSRP uses a virtual IP as the default gateway for clients, providing seamless failover if the active switch goes down.

N/B: I have demonstrated with 2 vlans, but the rest have been configured in the lab.

```
DISTRIBUTION-SW-1(config)#interface vlan 10

DISTRIBUTION-SW-1(config-if)#no shutdown

DISTRIBUTION-SW-1(config-if)#ip address 10.10.10.3 255.255.255.0

DISTRIBUTION-SW-1(config-if)#standby 10 ip 10.10.10.1

DISTRIBUTION-SW-1(config-if)#ip helper-address 10.10.150.5

DISTRIBUTION-SW-1(config-if)#exit

DISTRIBUTION-SW-1(config)#interface vlan 20

DISTRIBUTION-SW-1(config-if)#no shutdown

DISTRIBUTION-SW-1(config-if)#ip address 10.10.20.3 255.255.255.0

DISTRIBUTION-SW-1(config-if)#standby 20 ip 10.10.20.1

DISTRIBUTION-SW-1(config-if)#ip helper-address 10.10.150.5

DISTRIBUTION-SW-1(config-if)#exit
```

OSPF on the Firewall, Core Routers and Distribution Switches

OSPF (Open Shortest Path First) is a link-state routing protocol used within an autonomous system to dynamically exchange routing information between routers. It calculates the shortest and most efficient path to each destination using Dijkstra's algorithm. OSPF organizes networks into areas for scalability and supports fast convergence, load balancing and classless routing. It uses cost-based metrics based on bandwidth and sends routing updates through Link-State Advertisements (LSAs) and routes stored in the Link-State Database (LSDB) on each of the participating device.

On L3-SW-1 and L3-sw-2

```
DISTRIBUTION-SW-1>enable

DISTRIBUTION-SW-1#configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

DISTRIBUTION-SW-1(config)#router ospf 10

DISTRIBUTION-SW-1(config-router)#router-id 1.1.1.1

DISTRIBUTION-SW-1(config-router)#network 10.10.2.0 0.0.0.3 area 0

DISTRIBUTION-SW-1(config-router)#network 10.10.2.8 0.0.0.3 area 0

DISTRIBUTION-SW-1(config-router)#network 10.10.10.0 0.0.0.255 area 0

DISTRIBUTION-SW-1(config-router)#network 10.10.20.0 0.0.0.255 area 0

DISTRIBUTION-SW-1(config-router)#network 10.10.30.0 0.0.0.255 area 0

DISTRIBUTION-SW-1(config-router)#network 10.10.40.0 0.0.0.255 area 0

DISTRIBUTION-SW-1(config-router)#network 10.10.50.0 0.0.0.255 area 0

DISTRIBUTION-SW-1(config-router)#network 10.10.60.0 0.0.0.255 area 0

DISTRIBUTION-SW-1(config-router)#network 10.10.70.0 0.0.0.255 area 0

DISTRIBUTION-SW-1(config-router)#network 10.10.80.0 0.0.0.255 area 0

DISTRIBUTION-SW-1(config-router)#network 10.10.90.0 0.0.0.255 area 0

DISTRIBUTION-SW-1(config-router)#network 10.10.100.0 0.0.0.255 area 0

DISTRIBUTION-SW-1(config-router)#network 10.10.150.0 0.0.0.255 area 0

DISTRIBUTION-SW-1(config-router)#exit

DISTRIBUTION-SW-1(config)#do write

Building configuration...

Compressed configuration from 7383 bytes to 3601 bytes[OK]

[OK]
```

On Core Routers

```
Router>enable

Router#configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)#router ospf 10

Router(config-router)#router-id 1.1.1.3

Router(config-router)#network 10.10.2.0 0.0.0.3 area 0

Router(config-router)#network 10.10.2.4 0.0.0.3 area 0

Router(config-router)#network 10.10.1.0 0.0.0.3 area 0

Router(config-router)#exit

Router(config)#do write

Building configuration...

[OK]
```

OSPF on the firewall

```
ciscoasa(config)#router ospf 10

ciscoasa(config-router)#router-id 1.1.1.5

ciscoasa(config-router)#network 192.168.1.0 255.255.255.252 area 0

ciscoasa(config-router)#network 192.168.2.0 255.255.255.252 area 0

ciscoasa(config-router)#network 10.10.1.4 255.255.255.252 area 0

ciscoasa(config-router)#network 10.10.1.0 255.255.255.252 area 0

ciscoasa(config-router)#network 172.16.0.0 255.255.255.0 area 0

ciscoasa(config-router)#exit

ciscoasa(config)#write memory

Building configuration...

Cryptochecksum: 0c864a0e 69be0d04 3aa25024 467c490d


1571  bytes copied in 1.492 secs (1052 bytes/sec)

[OK]
```

ISP

```
ISP-2>enable

ISP-2#configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

ISP-2(config)#router ospf 10

ISP-2(config-router)#router-id 1.1.1.6

ISP-2(config-router)#network 192.168.2.0 0.0.0.3 area 0

ISP-2(config-router)#exit

ISP-2(config)#do write

Building configuration...

[OK]

ISP-2(config)#

00:05:30: %OSPF-5-ADJCHG: Process 10, Nbr 1.1.1.5 on GigabitEthernet0/0 from
LOADING to FULL, Loading Done
```

Firewall object networks

```
ciscoasa(config)#object network INSIDE1-OUTSIDE1

ciscoasa(config-network-object)#subnet 10.10.10.0 255.255.255.0

ciscoasa(config-network-object)#subnet 10.10.20.0 255.255.255.0

ciscoasa(config-network-object)#subnet 10.10.30.0 255.255.255.0

ciscoasa(config-network-object)#subnet 10.10.40.0 255.255.255.0

ciscoasa(config-network-object)#subnet 10.10.50.0 255.255.255.0

ciscoasa(config-network-object)#subnet 10.10.60.0 255.255.255.0

ciscoasa(config-network-object)#subnet 10.10.70.0 255.255.255.0

ciscoasa(config-network-object)#subnet 10.10.80.0 255.255.255.0

ciscoasa(config-network-object)#subnet 10.10.90.0 255.255.255.0

ciscoasa(config-network-object)#subnet 10.10.100.0 255.255.255.0

ciscoasa(config-network-object)#nat (INSIDE1,OUTSIDE1) dynamic interface

ciscoasa(config-network-object)#exit
```

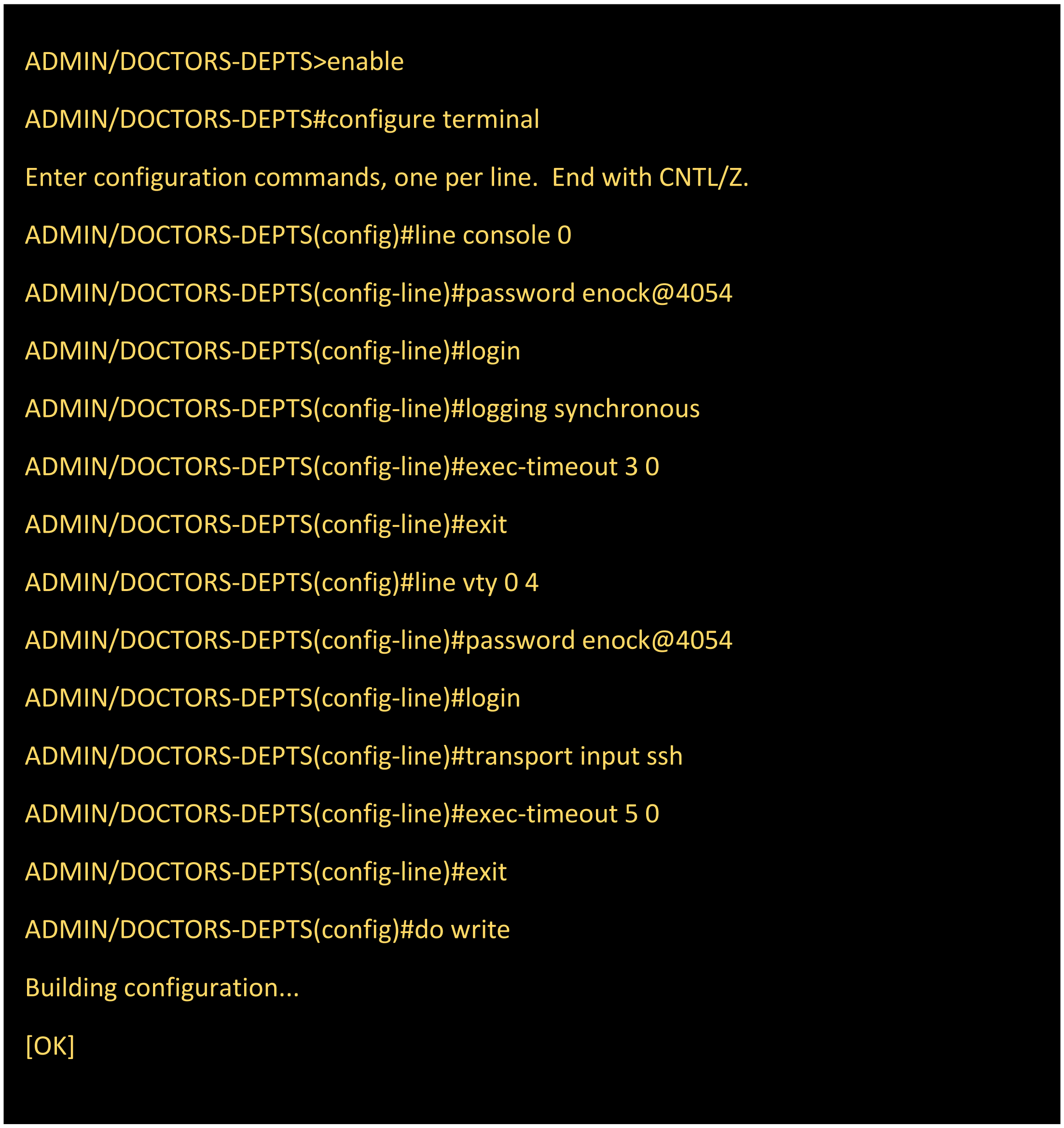
```
ciscoasa(config)#object network DMZ-OUTSIDE1

ciscoasa(config-network-object)#subnet 172.16.0.0 255.255.255.0

ciscoasa(config-network-object)#nat (DMZ,OUTSIDE1) dynamic interface

ciscoasa(config-network-object)#exit
```

Network Security and Devices Hardening

🔒 General Security Best Practices (All Cisco IOS Devices)

Apply to: Routers, Layer 3 Switches, Access Switches

1. Securing Console and VTY Access



```
ADMIN/DOCTORS-DEPTS>enable

ADMIN/DOCTORS-DEPTS#configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

ADMIN/DOCTORS-DEPTS(config)#line console 0

ADMIN/DOCTORS-DEPTS(config-line)#password enock@4054

ADMIN/DOCTORS-DEPTS(config-line)#login

ADMIN/DOCTORS-DEPTS(config-line)#logging synchronous

ADMIN/DOCTORS-DEPTS(config-line)#exec-timeout 3 0

ADMIN/DOCTORS-DEPTS(config-line)#exit

ADMIN/DOCTORS-DEPTS(config)#line vty 0 4

ADMIN/DOCTORS-DEPTS(config-line)#password enock@4054

ADMIN/DOCTORS-DEPTS(config-line)#login

ADMIN/DOCTORS-DEPTS(config-line)#transport input ssh

ADMIN/DOCTORS-DEPTS(config-line)#exec-timeout 5 0

ADMIN/DOCTORS-DEPTS(config-line)#exit

ADMIN/DOCTORS-DEPTS(config)#do write

Building configuration...

[OK]
```

2. Setting Strong Enable Secret

```
ADMIN/DOCTORS-DEPTS(config)#enable secret enock@4054

ADMIN/DOCTORS-DEPTS(config)#do write

Building configuration...

[OK]
```

3. Banner Message Of The Day

```
User Access Verification


Password:

ADMIN/DOCTORS-DEPTS>enable

Password:

ADMIN/DOCTORS-DEPTS#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

ADMIN/DOCTORS-DEPTS(config)#banner motd &

Enter TEXT message.  End with the character '&'.

########################################################################################

WARNING! Unauthorized access is prohibited. This device is restricted to

authorized personnel only. Remote login is permitted only from the management

network and strictly by prior authorization. All access is monitored and logged.

Disconnect immediately!

########################################################################################

&

ADMIN/DOCTORS-DEPTS(config)#no ip domain-lookup

ADMIN/DOCTORS-DEPTS(config)#service password-encryption

ADMIN/DOCTORS-DEPTS(config)#exit

ADMIN/DOCTORS-DEPTS#
```

4. Configuring SSH for Secure Remote Access

```
PHARMACY/NURSES-DEPT(config)#username enock password enock@4054
PHARMACY/NURSES-DEPT(config)#ip domain-name lakeview.local
PHARMACY/NURSES-DEPT(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: PHARMACY/NURSES-DEPT.lakeview.local

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 0:14:29.164: %SSH-5-ENABLED: SSH 1.99 has been enabled
PHARMACY/NURSES-DEPT(config)#ip ssh version 2
PHARMACY/NURSES-DEPT(config)#do write
Building configuration...
[OK]
PHARMACY/NURSES-DEPT(config)#access-list 1 permit 10.10.255.0 0.0.0.255
PHARMACY/NURSES-DEPT(config)#access-list 1 deny any
PHARMACY/NURSES-DEPT(config)#line vty 0 4
PHARMACY/NURSES-DEPT(config-line)#access-class 1 in
PHARMACY/NURSES-DEPT(config-line)#exit
PHARMACY/NURSES-DEPT(config)#
```

Access Switch Security

Apply to: Cisco Catalyst 2960, 9200, etc.

1. Port Security

```
ADMIN/DOCTORS-DEPTS>enable
Password:
ADMIN/DOCTORS-DEPTS#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ADMIN/DOCTORS-DEPTS(config)#interface range fa0/1 - 24
ADMIN/DOCTORS-DEPTS(config-if-range)#switchport mode access
ADMIN/DOCTORS-DEPTS(config-if-range)#switchport port-security
ADMIN/DOCTORS-DEPTS(config-if-range)#switchport port-security maximum 1
ADMIN/DOCTORS-DEPTS(config-if-range)#switchport port-security mac-address sticky
ADMIN/DOCTORS-DEPTS(config-if-range)#switchport port-security violation restrict
ADMIN/DOCTORS-DEPTS(config-if-range)#exit
ADMIN/DOCTORS-DEPTS(config)#do write
Building configuration...
[OK]
```

2. Prevention of spanning tree protocol

```
ADMIN/DOCTORS-DEPTS>enable

ADMIN/DOCTORS-DEPTS#configure terminal

ADMIN/DOCTORS-DEPTS(config)#interface range fa0/1-24

ADMIN/DOCTORS-DEPTS(config-if-range)#spanning-tree portfast

%Portfast has been configured on FastEthernet0/24 but will only

have effect when the interface is in a non-trunking mode.

ADMIN/DOCTORS-DEPTS(config-if-range)#spanning-tree bpduguard enable

ADMIN/DOCTORS-DEPTS(config-if-range)#exit

ADMIN/DOCTORS-DEPTS(config)#do write

Building configuration...

[OK]
```

3. Disabling Unused Ports

```
ADMIN/DOCTORS-DEPTS>enable

ADMIN/DOCTORS-DEPTS#configure terminal

ADMIN/DOCTORS-DEPTS(config)#interface range fa0/11-24

ADMIN/DOCTORS-DEPTS(config-if-range)#shutdown
```

🛡 Layer 3 Switch Security

Apply to: Catalyst 9300, 3850, etc.

Layer 3 switches combine switch and routing functionality.

🔐 Router Security

Apply to: Cisco ISR 4321, 2900, etc.

Routing Protocol Authentication (OSPF)

```
Core-Router-1(config)#interface range gig0/0-2
Core-Router-1(config-if-range)#ip ospf message-digest-key 1 md5 SecureOspfKey
Core-Router-1(config-if-range)#ip ospf authentication message-digest
Core-Router-1(config-if-range)#exit
Core-Router-1(config)#do write
Building configuration...
[OK]
```

🔥 Cisco ASA Firewall Security

Apply to: ASA 5505, 5506, 5510, PA-220 Replacement

1. Basic Hardening

```
ciscoasa>enable

Password:

ciscoasa#configure terminal

ciscoasa(config)#hostname ASA-FW

ASA-FW(config)#enable password Str0ngEnable@123 encrypted

ASA-FW(config)#username admin password Admin@123

ASA-FW(config)#no service telnet global
```

Access control lis

```
ciscoasa#conf t

ciscoasa(config)#access-list RES extended permit icmp any any

ciscoasa(config)#access-list RES extended permit tcp any any eq 80

ciscoasa(config)#access-list RES extended permit tcp any any eq 53

ciscoasa(config)#access-list RES extended permit udp any any eq 53

ciscoasa(config)#access-group RES in interface DMZ

ciscoasa(config)#access-group RES in interface OUTSIDE1

ciscoasa(config)#access-group RES in interface OUTSIDE2

ciscoasa(config)#

ciscoasa(config)#

ciscoasa(config)#write memory

Building configuration...

Cryptochecksum: 0c864a0e 69be0d04 3aa25024 467c490d


2492  bytes copied in 1.45 secs (1718 bytes/sec)

[OK]
```

📌 This project presents a professionally designed, secure and scalable three-tier network architecture for Lakeview Hospital, featuring VLAN segmentation, redundant links, centralized security using a Cisco ASA firewall and high availability for over 200 users across multiple departments.

- Disclaimer:
  This document is a student research and academic project prepared for educational purposes only. All network designs, configurations and recommendations contained herein are theoretical and simulated using Cisco Packet Tracer. While care has been taken to align the design with real-world industry standards, Lakeview Hospital and the student(s) involved assume no liability for any misuse or direct implementation in live production environments without professional evaluation.

- Confidentiality Notice:
  This report contains proprietary information belonging to Lakeview Hospital and the undersigned author(s). It may not be reproduced, distributed or disclosed in any form without prior written permission from the project supervisor or the hospital's management.

*********************THANK YOU AND HIRE ME!*********************