**Bachelor of Computer Applications**

**NETWORKING PROJECT**

**[SSJUPS2201070005]**



**(2025-26) DEPARTMENT OF COMPUTER SCIENCE**

**Soban Singh Jeena University**

**Submitted to Submitted by**

**Dr. Ravindera Pathak Sachin negi**

**Assistant Professor Roll.no;-[2201070019]**

**INDEX**

|  |  |
| --- | --- |
| **1.** | **Acknowledgment** |
| **2.** | **PROJECT AIM** |
| **3.** | **TECHNICAL REQUIREMENT** |
| **4.** | **NETWORK DESIGN** |
| **5.** | **BASIC SETTING TO ALL DEVICES + SSH + STANDARD ACL FOR SSH** |
| **6.** | **VLAN ASSIGNMENT PLUS ALL ACCESS AND TRUNK PORT ON 12 AND 13 SWITCHES** |
| **7.** | **STP portfast and BPDUguard configuration an all access ports** |
| **8.** | **Etherchannel** |
| **9.** | **SUBnetting and ip addressing** |
| **10.** | **HSRP and inter-vlan routing on the 13 switches plus ip dhcp helper addresses** |
| **11.** | **STATIC ip address to DMZ/ server farm devices** |
| **12.** | **DHCP server device configuration** |
| **13.** | **OSPF on the firewall, router,and switches** |
| **14.** | **Firewall interface security zone and levels** |
| **15.** | **Firewall routing ospf + static routes** |
| 16. | **FIREWALL inspection policy configuration** |
| 17. | **VoIP Configuration** |
| 18. | **Network window management** |

**Acknowledgment**

I would like to express my sincere gratitude to Dr. Ravindra Pathak , whose invaluable guidance, encouragement, and continuous support played a vital role in the successful completion of my project, **Enterprise company Network *Design***

His insightful suggestions and expert knowledge helped me gain a deeper understanding of computer networks including LAN, WAN, VLAN ,DHCP ,OSPF ,LACP ,HSRP , VoIP, Wireless network

I am also thanks to my family, friends, and faculty member who supported me throughout this journey.

**PROJECT AIM**

**Neta solution pvt Ltd** is a dynamic and forward-thinking company specializing in providing innovative cloud solutions to clients worldwide. Leveraging cutting-edge technology and a team of highly skilled professionals, Neta solution focuses on developing and implementing cloud-based solutions tailored to meet the evolving needs of businesses across various industries. With a strong emphasis on creativity, agility, and customer-centricity, **Neta solution** aims to empower organizations to enhance their operational efficiency, scalability, and competitiveness in today's digital landscape . With a workforce of 600 staff, **Neta solution Ltd** recently expanded and is preparing to move to a new building. The new building, comprising three floors, will house various departments, including Sales and Marketing. Human Resources and Logistics, Finance and Accounts, Administrator and Public Relations, ICT, and Server Room. The ICT department further hosts Software Developers, Cloud Engineers, Cybersecurity Engineers, Network Engineers, System Administrators, IT Support Specialists, Business Analysts and Project Managers

Prior to the move, a new network service needs to be designed and implemented in the new building. To ensure robust security, **Neta solution** will implement several security measures to protect the network from internal and external threats. The firewall will have outside, inside, and DMZ security zones, with essential servers strategically housed within the fortified zone. Additionally. Active Directory (AD) servers, responsible for managing and authenticating users, computers, and resources within the internal network, will be placed on the Inside zone of the firewall- this implies that servers such as DHCP, DNS, and Radius will all be on the inside zone, while other servers such as FTP, WEB. Email. APP, and NAS storage will be located in the DMZ-the zone can be attached to any firewall as of now. This meticulous planning and deployment of security measures will safeguard the network and ensure smooth operations for Cytoun Innovation Ltd in its new building

As an integral part of the ICT infrastructure, the following components have been incorporated:

**Internet Services Provider (ISP):** The University has established a subscription with two ISPs (SEACOM & Safaricom) to ensure redundant internet connectivity.

**Network Security:** Two Cisco ASA Firewalls from the 5500-X series have been acquired to enhance

network security and redundancy.

**c) Network Routing:** Both the firewalls and the core switches will be used instead of a router.

**Switching Infrastructure**: The network includes two Catalyst 3850 48-Port Switches, and Catalyst 2960 48-Port Switches to ensure robust local network connectivity.

**Server Hardware and Virtualization:** Two physical servers will be utilized for virtualization through the hypervisor to achieve multiple virtual machines for various services.

**Wireless Infrastructure:** A Cisco Wireless LAN Controller (WLC) and various Lightweight Access Points (LAPs) will centralize the management of the wireless network.

**VoIP or IP Phones:** A Cisco Voice Gateway will be used to enable telephony service in the network:

Cloud computing as an important technology is used to connect clients across the world to the company services and resources thus the proposed network should allow the team access to these resources.

Therefore, as a key member of the Networks Team, you have been tasked to design a network for the new building. At this stage, logical design is required, which shows the measures that you would put in place to ensure that the new network meets the current business need and is future-proofed.

**Technical Requirements**

**1. Design Tool**: Utilize Cisco Packet Tracer for designing and implementing the network solution.

**2. Hierarchical Design:** Implement a hierarchical model that incorporates redundancy for enhanced network resilience.

**3. ISPs:** Establish connectivity to the two ISPs within the network infrastructure.

**4. WLC:** Ensure that each department is equipped with a Wireless Access Point (WAP) to provide WIFI access to employees, corporate users, external auditors, and guests, all centrally managed by the Wireless LAN Controllers (WLC).

**5. VLAN:** Maintain VLANs with the following IDs: 10 for Management, 20 for LAN, 50 for WLAN, 70 for VoIP, and finally, 199 for Blackhole in which all unused ports are placed.

**6. EtherChannel:** Implement the Link Aggregation Control Protocol (LACP) for EtherChannel configuration, enhancing link aggregation efficiency.

**7. Telephony Service:** Configure VoIP on the voice gateway router and allocate dial numbers in format (4..).

**8. STP PortFast and BPDUguard:** Configure Spanning Tree Protocol (STP) PortFast and BPDUguard to expedite port transitions from blocking to forwarding states.

**9. Subnetting:** Utilize subnetting techniques to allocate the appropriate number of IP addresses to each network group. I

**10. Basic Settings:** Configure fundamental device settings, including hostnames, and console passwords, enable passwords, banner messages, password encryption, and disable IP domain lookup.

**11. Inter-VLAN Routing:** Enable devices in all departments to communicate with one another by configuring the respective multilayer switch for inter-VLAN routing

**12. Core Switch:** Assign IP addresses to Multilayer switches to enable both routing and switching functionalities.

**13. DHCP Server:** Ensure that all devices in the network obtain IP addresses dynamically from the DHCP servers located at the server farm site.

**14. HSRP:** Implement high-availability router protocols such as HSRP to achieve redundancy, load balancing, and failover capabilities.

**15. Static Addressing:** Allocate static IP addresses to devices located in the server room.

**16. Routing Protocol:** Utilize Open Shortest Path First (OSPF) as the routing protocol to advertise routes on the firewall, routers, and multilayer switches.

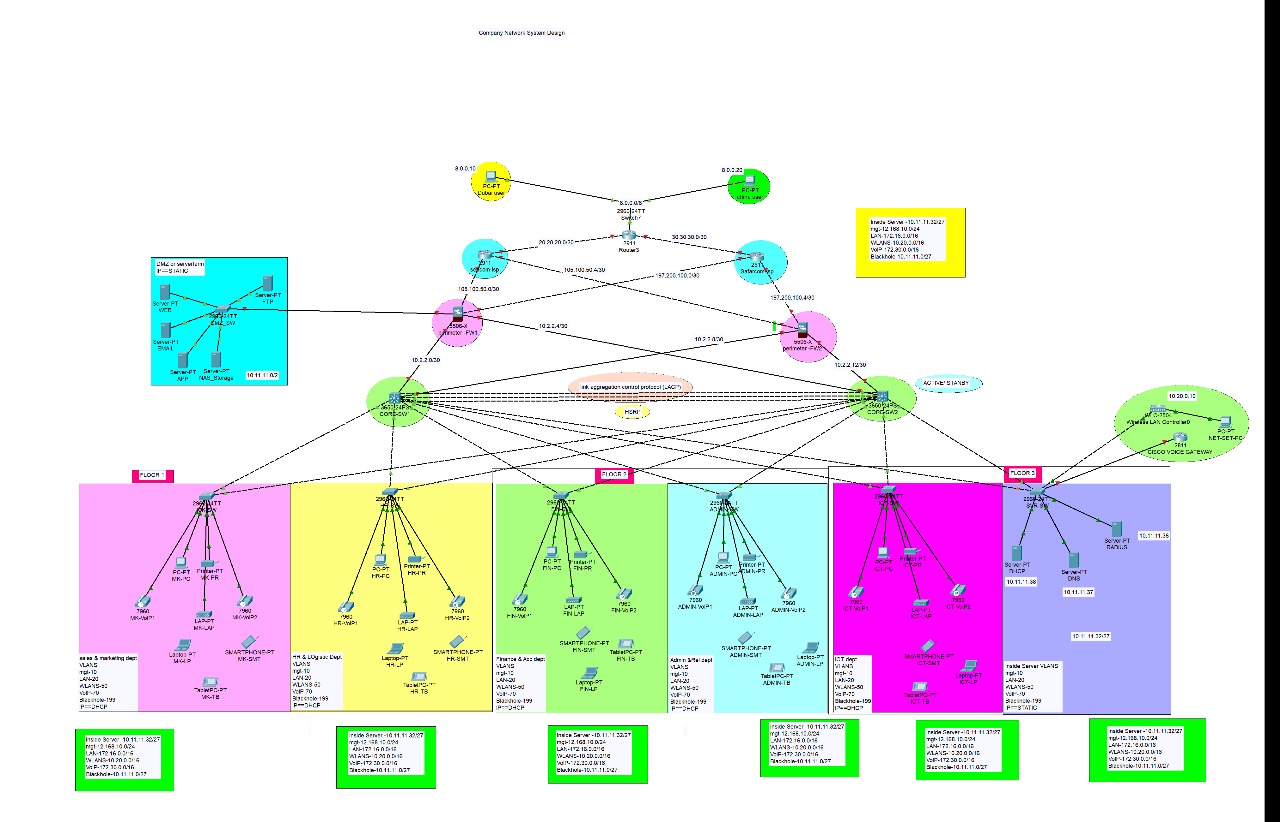
**17. Standard ACL for SSH:** Establish a simple standard Access Control List (ACL) on the VTY line to permit remote administrative tasks via SSH only for the Senior Network Security Engineer PC

**18. Cisco ASA Firewall:** Configure default static routes, basic settings, security levels, zones, and policies on the Cisco ASA Firewall to define access control and resource utilization within the

network.

**19. Final Testing:** Conduct thorough testing to verify proper communication and ensure that all configured elements function as intended.

**NETWORK DESIGN**



**1-BASIC SETTING TO ALL DEVICES + SSH + STANDARD ACL FOR SSH**

* SSH full form is Secure Shell, a cryptographic network protocol used for secure remote access, file transfers, and command execution.

**SM-SW**

En

Config t

Hostname SM-SW

Line console 0

Password cisco

Login

Exec-timeout 3 0

Logging synchronous

Enable password cisco

Banner motd &no unauthorised access!!!&

No ip domain-lookup

Service password-encryption

Username cisco password cisco

Ip domain-name cisco.com

Crypto key generate rsa general-key modulus 1024

Ip ssh version 2

Line vty 0 15

Login local

Transport input ssh

Exit

Do wr

Access-list 1 permit 192.168.10.0 0.0.0.255

Access-list 1 deny any

Line vty 0 15

Access-class 1 in

Exit

Do wr

**HR-SW**

En

Config t

Hostname HR-SW

Line console 0

Password cisco

Login

Exec-timeout 3 0

Logging synchronous

Enable password cisco

Banner motd &no unauthorised access!!!&

No ip domain-lookup

Service password-encryption

Username cisco password cisco

Ip domain-name cisco.com

Crypto key generate rsa general-key modulus 1024

Ip ssh version 2

Line vty 0 15

Login local

Transport input ssh

Exit

Do wr

Access-list 1 permit 192.168.10.0 0.0.0.255

Access-list 1 deny any

Line vty 0 15

Access-class 1 in

Exit

Do wr

**FIN-SW**

En

Config t

Hostname FIN-SW

Line console 0

Password cisco

Login

Exec-timeout 3 0

Logging synchronous

Enable password cisco

Banner motd &no unauthorised access!!!&

No ip domain-lookup

Service password-encryption

Username cisco password cisco

Ip domain-name cisco.com

Crypto key generate rsa general-key modulus 1024

Ip ssh version 2

Line vty 0 15

Login local

Transport input ssh

Exit

Do wr

Access-list 1 permit 192.168.10.0 0.0.0.255

Access-list 1 deny any

Line vty 0 15

Access-class 1 in

Exit

Do wr

**ADMIN-SW**

En

Config t

Hostname ADMIN-SW

Line console 0

Password cisco

Login

Exec-timeout 3 0

Logging synchronous

Enable password cisco

Banner motd &no unauthorised access!!!&

No ip domain-lookup

Service password-encryption

Username cisco password cisco

Ip domain-name cisco.com

Crypto key generate rsa general-key modulus 1024

Ip ssh version 2

Line vty 0 15

Login local

Transport input ssh

Exit

Do wr

Access-list 1 permit 192.168.10.0 0.0.0.255

Access-list 1 deny any

Line vty 0 15

Access-class 1 in

Exit

Do wr

**ICT-SW**

En

Config t

Hostname ICT-SW

Line console 0

Password cisco

Login

Exec-timeout 3 0

Logging synchronous

Enable password cisco

Banner motd &no unauthorised access!!!&

No ip domain-lookup

Service password-encryption

Username cisco password cisco

Ip domain-name cisco.com

Crypto key generate rsa general-key modulus 1024

Ip ssh version 2

Line vty 0 15

Login local

Transport input ssh

Exit

Do wr

Access-list 1 permit 192.168.10.0 0.0.0.255

Access-list 1 deny any

Line vty 0 15

Access-class 1 in

Exit

Do wr

**SVR-SW**

En

Config t

Hostname SVR-SW

Line console 0

Password cisco

Login

Exec-timeout 3 0

Logging synchronous

Enable password cisco

Banner motd &no unauthorised access!!!&

No ip domain-lookup

Service password-encryption

Username cisco password cisco

Ip domain-name cisco.com

Crypto key generate rsa general-key modulus 1024

Ip ssh version 2

Line vty 0 15

Login local

Transport input ssh

Exit

Do wr

Access-list 1 permit 192.168.10.0 0.0.0.255

Access-list 1 deny any

Line vty 0 15

Access-class 1 in

Exit

Do wr

**DMZ-SW**

En

Config t

Hostname DMZ-SW

Line console 0

Password cisco

Login

Exec-timeout 3 0

Logging synchronous

Enable password cisco

Banner motd &no unauthorised access!!!&

No ip domain-lookup

Service password-encryption

Username cisco password cisco

Ip domain-name cisco.com

Crypto key generate rsa general-key modulus 1024

Ip ssh version 2

Line vty 0 15

Login local

Transport input ssh

Exit

Do wr

Access-list 1 permit 192.168.10.0 0.0.0.255

Access-list 1 deny any

Line vty 0 15

Access-class 1 in

Exit

Do wr

**CORE-SW1**

En

Config t

Hostname CORE-SW1

Line console 0

Password cisco

Login

Exec-timeout 3 0

Logging synchronous

Enable password cisco

Banner motd &no unauthorised access!!!&

No ip domain-lookup

Service password-encryption

Username cisco password cisco

Ip domain-name cisco.com

Crypto key generate rsa general-key modulus 1024

Ip ssh version 2

Line vty 0 15

Login local

Transport input ssh

Exit

Do wr

Access-list 1 permit 192.168.10.0 0.0.0.255

Access-list 1 deny any

Line vty 0 15

Access-class 1 in

Exit

Do wr

**CORE-SW2**

En

Config t

Hostname CORE-SW2

Line console 0

Password cisco

Login

Exec-timeout 3 0

Logging synchronous

Enable password cisco

Banner motd &no unauthorised access!!!&

No ip domain-lookup

Service password-encryption

Username cisco password cisco

Ip domain-name cisco.com

Crypto key generate rsa general-key modulus 1024

Ip ssh version 2

Line vty 0 15

Login local

Transport input ssh

Exit

Do wr

Access-list 1 permit 192.168.10.0 0.0.0.255

Access-list 1 deny any

Line vty 0 15

Access-class 1 in

Exit

Do wr

**2- VLAN ASSIGNMENT PLUS ALL ACCESS AND TRUNK PORT ON 12 AND 13 SWITCHES**

* Virtual LAN (VLAN) is a concept in which we can divide the devices logically on layer 2 (data link layer). Generally, layer 3 devices divide the broadcast domain but the broadcast domain can be divided by switches using the concept of VLAN.

**configuration**

Int range fa0/1-2

Switchport mode trunk

Ex

Vlan 10

Name MGT

Vlan 20

Name LAN

Vlan 50

Name WLAN

Vlan 70

Name VoIP

Vlan 199

Name BLACKHOLE

Ex

Int range fa0/3-4

Switchport mode access

Switchport access vlan 20

Ex

Int range fa0/5-6

Switchport mode access

Switchport access vlan 70

Ex

Int range fa0/7

Switchport mode access

Switchport access vlan 50

Ex

Int range fa0/8-24 , gig0/1-2

Switchport mode access

Switchport access vlan 199

Shut

Ex

Do wr

**SW-SVR**

Int range fa0/1-2 , fa0/7

Switchport mode trunk

Ex

Vlan 10

Name MGT

Vlan 20

Name LAN

Vlan 50

Name WLAN

Vlan 70

Name VoIP

Vlan 90

Name inside-server

Ex

Int range fa0/3-5

Switchport mode access

Switchport access vlan 90

Ex

Int fa0/6

Switchport mode access

Switchport access vlan 50

Ex

Do wr

**Core sw-1**

Int range gig1/0/3-8

Switchport mode trunk

Ex

Vlan 10

Name MGT

Vlan 20

Name LAN

Vlan 50

Name WLAN

Vlan 70

Name VoIP

Vlan 90

Name inside-server

Ex

Do wr

**Mk -sw , hr-sw ,fin-sw ,admin-sw, ict-sw**

Int range fa0/5-6

No switchport access vlan 70

Switchport voice vlan 70

Ex

Do wr

**3- STP portfast and BPDUguard configuration an all access ports**

Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) are switching mechanisms that prevent a LAN with redundant links to forward Ethernet frames to loop in an indefinite time in a network.

Bridge protocol data unit (BPDU) is a data message forwarded across a Local Area Network (LAN) to detect loops in a spanning tree topology. A BPDU contains information about ports, switches, port priority, and addresses.

**SERVER-SW**

Int range fa0/3-6,fa0/8-24

Spanning-tree portfast

Spanning-tree bpduguard enable

Ex

Do wr

**IN (sw-mk,hr,fin,ict,admin)**

Int range fa0/3-24

Spanning-tree portfast

Spanning-tree bpduguard enable

Ex

Do wr

**Dmz-sw**

Int range fa0/1-24

Se portfast

Spanning-tree bpduguard enable

Ex

Do wr

**4- Etherchannel**

Ethernet connecting computers together with cable so the computers can share information. Within each main branch of the network, "Ethernet" can connect up to 1,024 personal computers and workstations.

**configuration**

**Core sw-1**

Int range gig1/0/9-11

Channel-group 1 mode active

Ex

Interface port-channel 1

Switchport mode trunk

Ex

Do wr

**Core sw-2**

Int range gig1/0/9-11

Channel-group 1 mode passive

Ex

Interface port-channel 1

Switchport mode trunk

Ex

Do wr

**5- SUBnetting and ip addressing**

A subnet is like a smaller group within a large network. It is a way to split a large network into smaller networks so that devices present in one network can transmits data more easily.

An IP address is a numerical label assigned to a device connected to a network that uses the Internet Protocol for communication

**Configuration**

**Core SW-1**

Ip routing

Int gig1/0/1

No switchport

No shut

Ip add 10.2.2.1 255.255.255.252

Int gig1/0/2

No switchport

No shut

Ip add 10.2.2.5 255.255.255.252

Ex

Do wr

**Core SW-2**

Ip routing

Int gig1/0/1

No switchport

No shut

Ip add 10.2.2.9 255.255.255.252

Int gig1/0/2

No switchport

No shut

Ip add 10.2.2.13 255.255.255.252

Ex

Do wr

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Category** | **Network &**  **Subnet mask** | **Valid Host**  **Addresses** | **Default Gateway** | **Broadcast**  **Address** |
| Management | 192.168.10.0/24 | 192.168.101.to  192.168.10.254 | 192.168.10.1 | 192.168.10.255 |
| WLAN | 10.20.0.0/16 | 10.20.0.1 to  10.20.255.254 | 10.20.0.1 | 10.20.255.254 |
| LAN | 172.16.0.0/16 | 172.16.0.1 to  172.16.255.254 | 172.16.0.1 | 172.16.255.255 |
| VOIP | 172.16.0.0/16 | 172.30.0.1 to  172.30.255.254 | 172.30.0.1 | 172.30.255.255 |
| DMZ | 10.11.11.0/27 | 10.11.11.1 to  10.11.11.30 | 10.11.11.1 | 10.11.11.31 |
| INSIDE SERVERS | 10.11.11.32/27 | 10.11.11.33 to  10.11.11.62 | 10.11.11.33 | 10.11.11.63 |

**Advanced Company Network**

**Between the cloud igsp farewell rotators and layer 3 switch**

|  |  |
| --- | --- |
| **No.** | **Network Address** |
| CLOUD Area | 8.0.0.0/8 |
| ISP1- Internet | 20.20.20.0/30 |
| ISP2- Internet | 30.30.30.0/30 |
| ISP1-FWL1 | 105.100.50.0/30 |
| ISP1-FWL2 | 105.100.50.4/30 |
| ISP2-FWL1 | 205.200.100.0/30 |
| ISP2-FWL2 | 205.200.100.4/30 |
| FWL1 to -MLSW1 | 10.2.2.0/30 |
| FWL1 to - MLSW2 | 10.2.2.4/30 |
| FWL2 to - MLSW1 | 10.2.2.8/30 |
| FWL2 to - MLSW2 | 10.2.2.12/30 |

**6- HSRP and inter-vlan routing on the 13 switches plus ip dhcp helper addresses**

* Hot Standby Router Protocol (HSRP) is a CISCO proprietary protocol, which provides redundancy for a local subnet. In HSRP, two or more routers gives an illusion of a virtual router. HSRP allows you to configure two or more routers as standby routers and only a single router as an active router at a time.

**CORE SW-1**

Int vlan 10

No shut

Ip address 192.168.10.3 255.255.255.0

Standby 10 ip 192.168.10.1

Ip helper-address 10.11.11.38

Ex

Int vlan 20

No shut

Ip address 172.16.0.3 255.255.0.0

Standby 20 ip 172.16.0.1

Ip helper-address 10.11.11.38

Ex

Int vlan 50

No shut

Ip address 10.20.0.2 255.255.0.0

Standby 50 ip 10.20.0.1

Ip helper-address 10.11.11.38

Ex

Int vlan 90

No shut

Ip address 10.11.11.34 255.255.255.224

Standby 90 ip 110.11.11.33

**CORE SW-2**

Int vlan 10

No shut

Ip address 192.168.10.2 255.255.255.0

Standby 10 ip 192.168.10.1

Ip helper-address 10.11.11.38

Ex

Int vlan 20

No shut

Ip address 172.16.0.2 255.255.0.0

Standby 20 ip 172.16.0.1

Ip helper-address 10.11.11.38

Ex

Int vlan 50

No shut

Ip address 10.20.0.3 255.255.0.0

Standby 50 ip 10.20.0.1

Ip helper-address 10.11.11.38

Ex

Int vlan 90

No shut

Ip address 10.11.11.35 255.255.255.224

Standby 90 ip 110.11.11.33

Ex

Do wr

**7- STATIC ip address to DMZ/ server farm devices**

**DHCP**

IPv4 Address -10.11.11.38

Subnet Mask-255.255.255.224

Default Gateway-10.11.11.33

DNS Server-10.11.11.37

**DNS**

IPv4 Address -10.11.11.37

Subnet Mask-255.255.255.224

Default Gateway-10.11.11.33

DNS Server-10.11.11.37

**RADIUS**

IPv4 Address -10.11.11.36

Subnet Mask-255.255.255.224

Default Gateway-10.11.11.33

DNS Server-10.11.11.37

**FTP**

IPv4 Address -10.11.11.10

Subnet Mask-255.255.255.224

Default Gateway-10.11.11.1

DNS Server-10.11.11.37

**WEB**

IPv4 Address -10.11.11.11

Subnet Mask-255.255.255.224

Default Gateway-10.11.11.1

DNS Server-10.11.11.37

**EMAIL**

IPv4 Address -10.11.11.12

Subnet Mask-255.255.255.224

Default Gateway-10.11.11.1

DNS Server-10.11.11.37

**APP**

IPv4 Address -10.11.11.13

Subnet Mask-255.255.255.224

Default Gateway-10.11.11.1

DNS Server-10.11.11.37

**NASS-STORAGE**

IPv4 Address -10.11.11.14

Subnet Mask-255.255.255.224

Default Gateway-10.11.11.1

DNS Server-10.11.11.37

**8. DHCP server device configuration**

DHCP is a network protocol that automates the process of assigning IP addresses and other network configuration parameters to devices on a network

**A screenshot of a computer

AI-generated content may be incorrect.**

**9- OSPF on the firewall, router,and switches**

OSPF (Open Shortest Path First) is an Interior Gateway Protocol (IGP). It is a link-state routing protocol that uses the Shortest Path First (SPF) algorithm to calculate the best route.

**CORE SW-1**

Router ospf 35

Router-id 1.1.1.1

Network 10.2.2.0 0.0.0.3 area 0

Network 10.2.2.4 0.0.0.3 area 0

Network 192.168.10.0 0.0.0.255 area 0

Network 172.16.0.0 0.0.255.255 area 0

Network 10.20.0.0 0.0.255.255 area 0

Network 10.11.11.32 0.0.0.31 area 0

Ex

Do wr

**CORE SW-2**

Router ospf 35

Router-id 1.1.2.2

Network 10.2.2.8 0.0.0.3 area 0

Network 10.2.2.12 0.0.0.3 area 0

Network 192.168.10.0 0.0.0.255 area 0

Network 172.16.0.0 0.0.255.255 area 0

Network 10.20.0.0 0.0.255.255 area 0

Network 10.11.11.32 0.0.0.31 area 0

Ex

Do wr

**Seascom-isp**

Router ospf 35

Router-id 1.1.3.3

Network 105.100.50.0 0.0.0.3 area 0

Network 105.100.50.4 0.0.0.3 area 0

Network 20.20.20.0 0.0.0.3 area 0

Ex

Do wr

**Seascom-isp**

Router ospf 35

Router-id 1.1.4.4

Network 30.30.30.0 0.0.0.3 area 0

Network 197.200.100.0 0.0.0.3 area 0

Network 197.20.100.4 0.0.0.3 area 0

Ex

Do wr

**Cluster- router**

Router ospf 35

Router-id 1.1.5.5

Network 8.0.0.0 0.255.255.255 area 0

Network 20.20.20.0 0.0.0.3 area 0

Network 30.30.30.0 0.0.0.3 area 0

Ex

Do wr

**10-firewall interface security zone and levels**

**FWL-1**

Hostname FWL1

Int gig1/3

No shut

Ip address 10.2.2.2 255.255.255.252

Nameif INSIDE1

Security-level 100

Ex

Int gig1/4

No shut

Ip address 10.2.2.10 255.255.255.252

Nameif INSIDE2

Security-level 100

Ex

Int gig1/5

No shut

Ip address 10.11.11.1 255.255.255.224

Nameif DMZ

Security-level 70

Ex

Int gig1/1

No shut

Ip address 105.100.50.2 255.255.255.252

Nameif outside1

Security-level 0

Ex

Int gig1/2

No shut

Ip address 197.200.100.2 255.255.255.252

Nameif outside2

Security-level 0

Ex

Do wr

Wr MEM

**FWL-2**

Hostname FWL2

Int gig1/3

No shut

Ip address 10.2.2.6 255.255.255.252

Nameif INSIDE1

Security-level 100

Ex

Int gig1/4

No shut

Ip address 10.2.2.14 255.255.255.252

Nameif INSIDE2

Security-level 100

Ex

Int gig1/1

No shut

Ip address 105.100.50.6 255.255.255.252

Nameif outside1

Security-level 0

Ex

Int gig1/2

No shut

Ip address 197.200.100.6 255.255.255.252

Nameif outside2

Security-level 0

Ex

Do wr

Wr MEM

**11-firewall routing ospf + static routes**

**FWL1**

Route outside1 0.0.0.0 0.0.0.0 105.100.50.1

Route outside2 0.0.0.0 0.0.0.0 197.200.100.1 70

Router ospf 35

Router-id 1.1.8.8

Network 105.100.50.0 255.255.255.252 area 0

Network 197.200.100.0 255.255.255.252 area 0

Network 10.11.11.0 255.255.255.224 area 0

Network 10.2.2.0 255.255.255.252 area 0

Network 10.2.2.8 255.255.255.252 area 0

Ex

Do wr

Wr MEM

**FWL2**

Route outside1 0.0.0.0 0.0.0.0 105.100.50.5

Route outside2 0.0.0.0 0.0.0.0 197.200.100.5

Router ospf 35

Router-id 1.1.9.9

Network 105.100.50.4 255.255.255.252 area 0

Network 197.200.100.4 255.255.255.252 area 0

Network 10.2.2.4 255.255.255.252 area 0

Network 10.2.2.12 255.255.255.252 area 0

Ex

Do wr

Wr MEM

**12- FIREWALL inspection policy configuration**

**FWL1**

Access-list RES extended permit icmp any any

Access-list RES extended permit tcp any any eq 80

Access-list RES extended permit tcp any any eq 53

Access-list RES extended permit udp any any eq 53

Access-group RES in interface DMZ

Access-group RES in interface OUTSIDE1

Access-group RES in interface OUTSIDE2

DO WR

WR MEM

**FWL2**

Access-list RES extended permit icmp any any

Access-list RES extended permit tcp any any eq 80

Access-list RES extended permit tcp any any eq 53

Access-list RES extended permit udp any any eq 53

Access-group RES in interface OUTSIDE1

Access-group RES in interface OUTSIDE2

DO WR

WR MEM

**14- VoIP Configuration**

**ROUTER-3**

Int fa0/0

No shut

Ex

Int fa0/0.70

Ip add 172.30.0.1 255.255.0.0

Encapsulation dot1Q 70

Ip add 172.30.0.1 255.255.0.0

Ex

Service dhcp

Ip dhcp pool voip-pool

Network 172.30.0.0 255.255.0.0

Default-router 172.30.0.1

Option 150 ip 172.30.0.1

Ex

Telephony-service

Max-ephone 30

Max-dn 30

Ip source-address 172.30.0.1 port 2000

Auto assign 1 to 30

Ex

Ephone-dn 1

Number 401

Ex

Ephone-dn 2

Number 402

Exephone-dn 3

Number 403

Exephone-dn 4

Number 404

Exephone-dn 5

Number 405

Exephone-dn 6

Number 406

Exephone-dn 7

Number 407

Exephone-dn 8

Number 408

Exephone-dn 9

Number 409

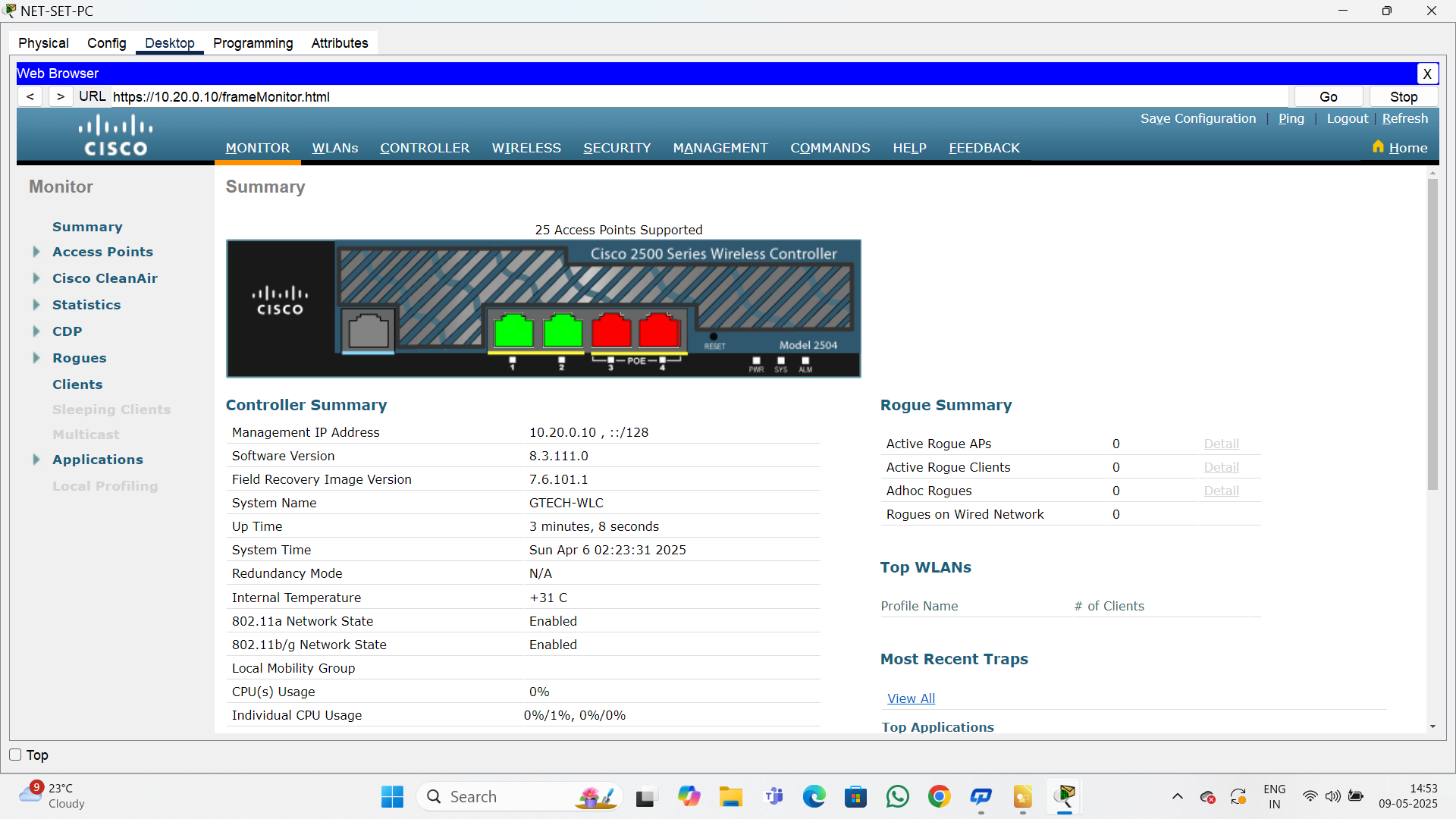
Exephone-dn 10

Number 410

Ex

Do wr

**Network window management**

 **Final Note**

Completing this Project on Enterprise Network *Design* has been a challenging yet deeply rewarding experience. It has not only expanded my technical understanding but also enhanced my analytical and problem-solving skills.

As I conclude this work, I am filled with gratitude for the journey of learning and growth it has offered. I hope this project serves as a valuable contribution and a useful reference for others interested in the field of enterprise networking.

Thank you for taking the time to engage with my work.