**Telecommunication Company Network Design and Implementation**

**Problem:**

Cairo Telco is a fast-growing telecommunication company in Egypt, which offers IT solutions and services to its clients. The company is located in the Egyptian capital city, Cairo, and has occupied the fourth and fifth floors of Pharaoh’s Mega Plaza. The company has its fourth floor hosting HR and Finance(40), Product Brand and Marketing(45), and finally, Admin and Corporate departments(35). The fifth floor is designed for IT Network & Support(45), Software Engineering(36), and Cloud Engineering departments(32).

As part of ICT infrastructure, the company has subscribed to Seacom ISP for internet services and also has purchased one 5525-X Cisco ASA Firewall, one Catalyst 3850 48-Port Switch, 3 Catalyst 2960 48-Port Switches, 2 Catalyst 2960 24-Port Switches, 1 Cisco Voice Gateway, 1 Cisco WLC, and 6 LAPs. The company uses Windows Server 2022 to manage the Active Directory and Radius Server, the server is responsible for DNS services and for allocating IPv4 addresses to the DHCP hosts in the network. The company has an internally hosted ERP system, Email server, and File server. The company has settled on using Cisco Voice Gateways to provide VoIP or telephony services in the network and Cisco WLC to provide central management for Aps.

Cairo Telco leverages using Microsoft Azure cloud platform to facilitate service delivery thus this is one of the core business functions of the firm. The developers and cloud engineers use several MS Azure resources like VM, blob storage, networking, and security among others to ensure seamless business continuity. The proposed network should allow the team access to these resources.

Due to security requirements, it has been decided that all LAN, WLAN, and VoIP users will be on a separate network segment within the same local area network. The firewall will be used to set security zones and filter traffic that moves in and out of the zones based on the configured inspection policies. You have been hired as a network security engineer to design the network for Cairo Telco according to the requirements set by the senior management. You will consult an appropriate robust network design model to meet the design requirements. You are required to design and implement a secured, reliable, scalable, and robust network system that is paramount to safeguarding the Confidentiality, Integrity, and Availability of data and communication.

The company has emphasized high performance, redundancy, scalability, and availability, and hence you are required to provide a complete Cairo Telco network infrastructure design and implementation. The company will be using the following IP address: 10.20.0.0/16 for WLAN, 192.168.10.0/24 for LAN, 172.16.10.0/24 for Voice, 10.10.10.0/28 for DMZ and 197.200.100.0 for public addresses.

1. **Design Tool**: Use Cisco Packet Tracer to design and implement the network solution.
2. **Hierarchical Design**: Use a hierarchical model providing redundancy at every layer.
3. **ISPs**: The network is also expected to connect to a Seacom ISP Router.
4. **WLC**: Each department is required to have a WAP providing both employees and guest WIFI managed by WLC.
5. **VoIP**: Each department should have IP phones.
6. **VLAN**: The LAN, WLAN, and VoIP VLANs remain at 50, 60 & 101 respectively for the entire network.
7. **EtherChannel**: Use standard LACP as a method of link aggregation.
8. **STP PortFast and BPDUguard**: configure the two protocols to enable faster port transition from blocking to forwarding.
9. **Subnetting**: Provided the networks above, carry out subnetting to allocate the correct number of IP addresses to each department.
10. **Basic settings**: Configure basic device settings such as hostnames, and console passwords, enable passwords, and banner messages, encrypt all passwords, and disable IP domain lookup.
11. **Inter-VLAN Routing**: Devices in all the departments are required to communicate with each other with the respective multilayer switch configured for inter-VLAN routing.
12. **Core Switch**: The Multilayer switches are expected to carry out both routing and switching functionalities and thus will be assigned IP addresses.
13. **DHCP Server**: All devices in the network (except IP phones) are expected to obtain an IP address dynamically from the AD servers located at the server farm site.
14. **Cisco 2811 Router**: Ensure to have a router that can support telephony service i.e Cisco Catalyst 2811(the VoIP router should be connected to the l3-switch).
15. **Static Addressing**: Devices in the server room are to be allocated IP addresses statically.
16. **Telephony Service**: Configure VoIP on the voice gateway router and allocate dial numbers in format (1...).
17. **Routing Protocol**: Use OSPF as the routing protocol to advertise routes both on the routers and multilayer switches.
18. **Standard ACL for SSH**: configure a simple standard ACL on the line VTY to allow only the Senior Network Security Engineer to carry out all remote administrative tasks using SSH.
19. **Cisco ASA Firewall**: Configure security levels, zones, and policies to define how resources are accessed in the network
20. **Final**: Test Communication, ensure everything configured is working as expected.

**Technologies Implemented:**

1. Creating a network topology using Cisco Packet Tracer.
2. Hierarchical Network Design.
3. Connecting Networking devices with Correct cabling.
4. Configuring Basic device settings.
5. Creating VLANs and assigning ports VLAN numbers.
6. Creating both data and voice VLANs and assigning ports VLAN numbers.
7. Subnetting and IP Addressing.
8. Configuring Inter-VLAN Routing both on the Switches (SVI) and Routers (router-on-a-stick).
9. Configuring Dedicated DHCP Server device for Data to provide dynamic IP allocation.
10. Configuring Routers as DHCP server for Voice to provide IP Phones dynamic IP allocation.
11. Configuring Spanning-Tree Protocol - STP PortFast and BPDUGuard.
12. Configuring Active Directory as DHCP Server.
13. Configuring SSH for secure Remote access.
14. Configuring OSPF as the routing protocol.
15. Configuring Standard ACL for VTY interfaces to restrict remote Access using SSH.
16. Configuring VoIP or Telephony service configuration in all routers.
17. Configuring WLAN network- Wireless LAN Controller + Wireless Lighweight Access Points .
18. Configuring Cisco ASA Firewall Interface descriptions, zones and security levels.
19. Configuring Cisco ASA Firewall Object Network + Network Address Translation (NAT).
20. Configuring Cisco ASA Firewall OSPF + Default Static Routes.
21. Configuring Cisco ASA Firewall Inspection Policiesto filter traffic based on predetermined ACLs .
22. Host Device Configurations.
23. Test and Verifying Network Communication.

**Solution:**

**Note:**

**Subnetting:**

1. **WLAN**

* **Network ID**: 10.20.0.0/16
* **Usable IP Range**: 10.20.0.1 - 10.20.255.254
* **Broadcast Address**: 10.20.255.255
* **Subnet Mask**: 255.255.0.0
* **Hosts**: 65,534 (suitable for a large WLAN network)

1. **LAN**

* **Network ID**: 192.168.10.0/24
* **Usable IP Range**: 192.168.10.1 - 192.168.10.254
* **Broadcast Address**: 192.168.10.255
* **Subnet Mask**: 255.255.255.0
* **Hosts**: 254 (suitable for a medium-sized network)

1. **Voice Network**

* **Network ID**: 172.16.10.0/24
* **Usable IP Range**: 172.16.10.1 - 172.16.10.254
* **Broadcast Address**: 172.16.10.255
* **Subnet Mask**: 255.255.255.0
* **Hosts**: 254 (for VoIP phones and related devices)

1. **DMZ**

* **Network ID**: 10.10.10.0/28
* **Usable IP Range**: 10.10.10.1 - 10.10.10.14
* **Broadcast Address**: 10.10.10.15
* **Subnet Mask**: 255.255.255.240
* **Hosts**: 14 (suitable for limited DMZ devices

1. **Public Addresses**

* **Network ID**: 197.200.100.0/24
* **Usable IP Range**: 197.200.100.1 - 197.200.100.254
* **Broadcast Address**: 197.200.100.255
* **Subnet Mask**: 255.255.255.0
* **Hosts**: 254

1. **Firewall to Core Switch (Point-to-Point)**

* **Network ID**: 10.30.30.0/30
* **Usable IP Range**: 10.30.30.1 - 10.30.30.2
* **Broadcast Address**: 10.30.30.3
* **Subnet Mask**: 255.255.255.252
* **Hosts**: 2 (suitable for point-to-point link)

1. **Firewall to ISP (Public Address)**

* **Network ID**: 197.200.100.0/30
* **Usable IP Range**: 197.200.100.1 - 197.200.100.2
* **Broadcast Address**: 197.200.100.3
* **Subnet Mask**: 255.255.255.252
* **Hosts**: 2 (suitable for public IP address link to ISP)

1. **ISP to Cloud**

* **Network ID**: 20.20.20.0/30
* **Usable IP Range**: 20.20.20.1 - 20.20.20.2
* **Broadcast Address**: 20.20.20.3
* **Subnet Mask**: 255.255.255.252
* **Hosts**: 2 (suitable for point-to-point link)

1. **Cloud Network**

* **Network ID**: 30.0.0.0/8
* **Usable IP Range**: 30.0.0.1 - 30.255.255.254
* **Broadcast Address**: 30.255.255.255
* **Subnet Mask**: 255.0.0.0
* **Hosts**: 16,777,214 (for a large network or various cloud services)

**All Configuration**

**Firewall:**

ciscoasa>en

Password:

ciscoasa#conf t

**#Set the hostname**

ciscoasa(config)#hostname Firewall

**#Set enable secret password for privileged EXEC mode**

Firewall(config)#enable password firewall

**#Create a local user account with an encrypted password for management access**

Firewall(config)#username firewall password firewall

**#Set domain name**

Firewall(config)# domain-name cairo.com

Firewall(config)# exit

Firewall#write memory

**#Assign IP Address to interface**

**#Configure the DMZ Interface**

Firewall(config)#interface gig1/1

Firewall(config-if)#no shutdown

Firewall(config-if)#nameif dmz

Firewall(config-if)#security-level 50

Firewall(config-if)#ip address 10.10.10.1 255.255.255.240

Firewall(config-if)#exit

**#Configure the Inside (LAN) Interface**

Firewall(config)#interface gig1/2

Firewall(config-if)#no shutdown

Firewall(config-if)#nameif inside

Firewall(config-if)#security-level 100

Firewall(config-if)#ip address 10.30.30.1 255.255.255.252

Firewall(config-if)#exit

**#Configure the Outside (Public/ISP) Interface**

Firewall(config)#interface gig1/3

Firewall(config-if)#no shutdown

Firewall(config-if)#nameif outside

Firewall(config-if)#security-level 0

Firewall(config-if)#ip address 197.200.100.2 255.255.255.252

Firewall(config-if)#exit

Firewall(config)#wr mem

Firewall(config)#exit

**#Enable Routing Protocol (OSPF)**

Firewall(config)#router ospf 10

Firewall(config-router)#network 10.10.10.0 255.255.255.240 area 0

Firewall(config-router)#network 10.30.30.0 255.255.255.252 area 0

Firewall(config-router)#network 197.200.100.0 255.255.255.252 area 0

Firewall(config-router)#exit

**#Default Route to Reach the Internet via Outside Interface**

Firewall(config)#route outside 0.0.0.0 0.0.0.0 197.200.100.1

Firewall(config)#wr mem

Firewall(config)#exit

**#NAT Configuration**

Firewall(config)#object network inside-network-io

Firewall(config-network-object)#subnet 192.168.10.0 255.255.255.0

Firewall(config-network-object)#nat (inside,outside) dynamic interface

Firewall(config)#object network inside-wifi-network-io

Firewall(config-network-object)#subnet 10.20.0.0 255.255.0.0

Firewall(config-network-object)#nat (inside,outside) dynamic interface

Firewall(config)#object network dmz-network-do

Firewall(config-network-object)#subnet 10.10.10.0 255.255.255.240

Firewall(config-network-object)#nat (dmz,outside) dynamic interface

Firewall(config-network-object)#wr mem

Firewall(config-network-object)#exit

**#Configure access lists**

**# Allow ICMP (Ping)**

Firewall(config)#access-list DMZ-TO-INSIDE-ACL extended permit icmp any any

**# Allow DHCP (UDP/TCP port 67)**

Firewall(config)#access-list DMZ-TO-INSIDE-ACL extended permit udp any any eq 67

Firewall(config)#access-list DMZ-TO-INSIDE-ACL extended permit tcp any any eq 67

**# Allow DNS (UDP/TCP port 53)**

Firewall(config)#access-list DMZ-TO-INSIDE-ACL extended permit udp any eq 53 any

Firewall(config)#access-list DMZ-TO-INSIDE-ACL extended permit tcp any eq 53 any

**# Allow HTTP and HTTPS (TCP ports 80, 8080, 443, 8443)**

Firewall(config)#access-list DMZ-TO-INSIDE-ACL extended permit tcp any eq 80 any

Firewall(config)#access-list DMZ-TO-INSIDE-ACL extended permit tcp any eq 8080 any

Firewall(config)#access-list DMZ-TO-INSIDE-ACL extended permit tcp any eq 443 any

Firewall(config)#access-list DMZ-TO-INSIDE-ACL extended permit tcp any eq 8443 any

**# Allow Email services (SMTP, SMTPS, IMAP, IMAPS, POP3, POP3S)**

Firewall(config)#access-list DMZ-TO-INSIDE-ACL extended permit tcp any eq any 25

Firewall(config)#access-list DMZ-TO-INSIDE-ACL extended permit tcp any eq any 465

Firewall(config)#access-list DMZ-TO-INSIDE-ACL extended permit tcp any eq 143 any

Firewall(config)#access-list DMZ-TO-INSIDE-ACL extended permit tcp any eq 993 any

Firewall(config)#access-list DMZ-TO-INSIDE-ACL extended permit tcp any eq 110 any

Firewall(config)#access-list DMZ-TO-INSIDE-ACL extended permit tcp any eq 995 any

**# Allow File Sharing (TCP ports 445, 21)**

Firewall(config)#access-list DMZ-TO-INSIDE-ACL extended permit tcp any any eq 445

Firewall(config)#access-list DMZ-TO-INSIDE-ACL extended permit tcp any any eq 21

**# Apply ACL to the DMZ interface**

Firewall(config)#access-group DMZ-TO-INSIDE-ACL in interface dmz

Firewall(config)#wr mem

**# Allow ICMP (Ping)**

Firewall(config)#access-list INSIDE-TO-OUTSIDE-ACL extended permit icmp any any

**# Allow HTTP and HTTPS (TCP ports 80, 8080, 443, 8443)**

Firewall(config)#access-list INSIDE-TO-OUTSIDE-ACL extended permit tcp any eq 80 any

Firewall(config)#access-list INSIDE-TO-OUTSIDE-ACL extended permit tcp any eq 8080 any

Firewall(config)#access-list INSIDE-TO-OUTSIDE-ACL extended permit tcp any eq 443 any

Firewall(config)#access-list INSIDE-TO-OUTSIDE-ACL extended permit tcp any eq 8443 any

**# Apply ACL to the outside interface**

Firewall(config)#access-group INSIDE-TO-OUTSIDE-ACL in interface outside

Firewall(config)#wr mem

**Core-Switch:**

Switch>en

Switch#conf t

**#Set the hostname**

Switch(config)#hostname Core-Switch

**#Set console password**

Core-Switch(config)#line console 0

Core-Switch(config-line)#password coreswitch

Core-Switch(config-line)#login

Core-Switch(config-line)#exit

**#Set enable secret password for privileged EXEC mode**

Core-Switch(config)#enable secret coreswitch

**#Enable password encryption for all passwords**

Core-Switch(config)#service password-encryption

**#Configure banner for unauthorized access warning**

Core-Switch(config)#banner motd # Unauthorized access is prohibited. #

**#Disable domain name lookup to prevent delays caused by incorrect commands**

Core-Switch(config)#no ip domain-lookup

**#Configure SSH**

Core-Switch(config)#ip domain-name cairo.com

**#Generate RSA key pairs for SSH encryption**

Core-Switch(config)#crypto key generate rsa

How many bits in the modulus [512]: 1024

**#Enable SSH version 2**

Core-Switch(config)#ip ssh version 2

**#Create a local user for SSH access**

Core-Switch(config)#username coreswitch secret coreswitch

**#Configure VTY lines to accept only SSH connections**

Core-Switch(config)#line vty 0 4

Core-Switch(config-line)#transport input ssh

Core-Switch(config-line)#login local

Core-Switch(config-line)#exit

**#Set SSH time-out and retries to improve security**

Core-Switch(config)#ip ssh time-out 60

Core-Switch(config)#ip ssh authentication-retries 3

Core-Switch(config)#do wr

Core-Switch(config)#exit

**#Create Vlans**

Core-Switch(config)#vlan 50

Core-Switch(config-vlan)#name LAN

Core-Switch(config-vlan)#exit

Core-Switch(config)#vlan 60

Core-Switch(config-vlan)#name WLAN

Core-Switch(config-vlan)#exit

Core-Switch(config)#vlan 101

Core-Switch(config-vlan)#name VoIP

Core-Switch(config-vlan)#exit

**#Assign vlan to access port**

Core-Switch(config)#int gig1/0/3

Core-Switch(config-if)#switchport mode access

Core-Switch(config-if)#switchport access vlan 60

Core-Switch(config-if)#switchport nonegotiate

Core-Switch(config-if)#spanning-tree portfast

Core-Switch(config-if)#spanning-tree bpduguard enable

Core-Switch(config-if)#exit

Core-Switch(config)#int gig1/0/2

Core-Switch(config-if)#switchport mode trunk

Core-Switch(config-if)#switchport trunk allowed vlan 101

Core-Switch(config-if)#switchport nonegotiate

Core-Switch(config-if)#spanning-tree portfast

Core-Switch(config-if)#spanning-tree bpduguard enable

Core-Switch(config-if)#exit

**#EtherChannel configuration and make it trunk**

Core-Switch(config)#int range gig1/0/4-5

Core-Switch(config-if-range)#channel-group 1 mode active

Core-Switch(config-if-range)#exit

Core-Switch(config)#int port-channel 1

Core-Switch(config-if)#switchport mode trunk

Core-Switch(config-if)#exit

Core-Switch(config)#int range gig1/0/6-7

Core-Switch(config-if-range)#channel-group 2 mode active

Core-Switch(config-if-range)#exit

Core-Switch(config)#int port-channel 2

Core-Switch(config-if)#switchport mode trunk

Core-Switch(config-if)#exit

Core-Switch(config)#int range gig1/0/8-9

Core-Switch(config-if-range)#channel-group 3 mode active

Core-Switch(config-if-range)#exit

Core-Switch(config)#int port-channel 3

Core-Switch(config-if)#switchport mode trunk

Core-Switch(config-if)#exit

Core-Switch(config)#do wr

Core-Switch(config)#exit

**#Assign IP Address to interface**

Core-Switch(config)#int gig1/0/1

Core-Switch(config-if)#no switchport

Core-Switch(config-if)#ip address 10.30.30.2 255.255.255.252

Core-Switch(config-if)#exit

Core-Switch(config)#do wr

Core-Switch(config)#exit

**#Inter-Vlan Routing + IP DHCP Helper Address**

Core-Switch(config)#interface vlan 50

Core-Switch(config-if)#no shutdown

Core-Switch(config-if)#ip address 192.168.10.1 255.255.255.0

Core-Switch(config-if)#ip helper-address 10.10.10.5

Core-Switch(config-if)#exit

Core-Switch(config)#interface vlan 60

Core-Switch(config-if)#no shutdown

Core-Switch(config-if)#ip address 10.20.0.1 255.255.0.0

Core-Switch(config-if)#ip helper-address 10.10.10.5

Core-Switch(config-if)#exit

Core-Switch(config)#do wr

Core-Switch(config)#exit

**#Enable Routing Protocol (OSPF)**

Core-Switch(config)#ip routing

Core-Switch(config)#router ospf 10

Core-Switch(config-router)#network 192.168.10.0 0.0.0.255 area 0

Core-Switch(config-router)#network 10.20.0.0 0.0.255.255 area 0

Core-Switch(config-router)#network 10.30.30.0 0.0.0.3 area 0

Core-Switch(config-router)#exit

Core-Switch(config)#do wr

Core-Switch(config)#exit

**Switch-1:**

Switch>en

Switch#conf t

**# Set hostname**

Switch(config)#hostname Switch-1

**# Console password setup**

Switch-1(config)#line console 0

Switch-1(config-line)#password switch1

Switch-1(config-line)#login

Switch-1(config-line)#exit

**# Enable secret for privileged access**

Switch-1(config)#enable secret switch1

**# Create local user account**

Switch-1(config)#username switch1 secret switch1

**# Encrypt all plaintext passwords**

Switch-1(config)#service password-encryption

**# Unauthorized access warning**

Switch-1(config)#banner motd # Unauthorized access is prohibited. #

**# Disable DNS lookup for mistyped commands**

Switch-1(config)#no ip domain-lookup

**# Save configuration**

Switch-1(config)#do wr

Switch-1(config)#exit

**#Create Vlans + assign access port + STP PortFast configuration + BPDUguard configuration**

Switch-1(config)#vlan 50

Switch-1(config-vlan)#name LAN

Switch-1(config-vlan)#exit

Switch-1(config)#vlan 60

Switch-1(config-vlan)#name WLAN

Switch-1(config-vlan)#exit

Switch-1(config)#vlan 101

Switch-1(config-vlan)#name VoIP

Switch-1(config-vlan)#exit

Switch-1(config)#int range fa0/2-12

Switch-1(config-if-range)#switchport mode access

Switch-1(config-if-range)#switchport access vlan 50

Switch-1(config-if-range)#switchport voice vlan 101

Switch-1(config-if-range)#spanning-tree portfast

Switch-1(config-if-range)#spanning-tree bpduguard enable

Switch-1(config-if-range)#exit

Switch-1(config)#int fa0/1

Switch-1(config-if)#switchport mode access

Switch-1(config-if)#switchport access vlan 60

Switch-1(config-if)#spanning-tree portfast

Switch-1(config-if)#spanning-tree bpduguard enable

Switch-1(config-if)#exit

Switch-1(config)#int range fa0/14-24

Switch-1(config-if-range)#switchport mode access

Switch-1(config-if-range)#switchport voice vlan 50

Switch-1(config-if-range)#switchport voice vlan 101

Switch-1(config-if-range)#spanning-tree portfast

Switch-1(config-if-range)#spanning-tree bpduguard enable

Switch-1(config-if-range)#exit

Switch-1(config)#int fa0/13

Switch-1(config-if)#switchport mode access

Switch-1(config-if)#switchport access vlan 60

Switch-1(config-if)#spanning-tree portfast

Switch-1(config-if)#spanning-tree bpduguard enable

Switch-1(config-if-range)#exit

Switch-1(config)#do wr

Switch-1(config)#exit

**#EtherChannel configuration and make it trunk**

Switch-1(config)#int range gig0/1-2

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

Switch-1(config-if-range)#exit

Switch-1(config)#int port-channel 1

Switch-1(config-if)#switchport mode trunk

Switch-1(config-if)#exit

Switch-1(config)#do wr

Switch-1(config)#exit

**Switch-2:**

Switch>en

Switch#conf t

**# Set hostname**

Switch(config)#hostname Switch-2

**# Console password setup**

Switch-2(config)#line console 0

Switch-2(config-line)#password switch2

Switch-2(config-line)#login

Switch-2(config-line)#exit

**# Enable secret for privileged access**

Switch-2(config)#enable secret switch2

**# Create local user account**

Switch-2(config)#username switch2 secret switch2

**# Encrypt all plaintext passwords**

Switch-2(config)#service password-encryption

**# Unauthorized access warning**

Switch-2(config)#banner motd # Unauthorized access is prohibited. #

**# Disable DNS lookup for mistyped commands**

Switch-2(config)#no ip domain-lookup

**# Save configuration**

Switch-2(config)#do wr

Switch-2(config)#exit

**#Create Vlans + assign access port + STP PortFast configuration + BPDUguard configuration**

Switch-2(config)#vlan 50

Switch-2(config-vlan)#name LAN

Switch-2(config-vlan)#exit

Switch-2(config)#vlan 60

Switch-2(config-vlan)#name WLAN

Switch-2(config-vlan)#exit

Switch-2(config)#vlan 101

Switch-2(config-vlan)#name VoIP

Switch-2(config-vlan)#exit

Switch-2(config)#int range fa0/2-12

Switch-2(config-if-range)#switchport mode access

Switch-2(config-if-range)#switchport access vlan 50

Switch-2(config-if-range)#switchport voice vlan 101

Switch-2(config-if-range)#spanning-tree portfast

Switch-2(config-if-range)#spanning-tree bpduguard enable

Switch-2(config-if-range)#exit

Switch-2(config)#int fa0/1

Switch-2(config-if)#switchport mode access

Switch-2(config-if)#switchport access vlan 60

Switch-2(config-if)#spanning-tree portfast

Switch-2(config-if)#spanning-tree bpduguard enable

Switch-2(config-if)#exit

Switch-2(config)#int range fa0/14-24

Switch-2(config-if-range)#switchport mode access

Switch-2(config-if-range)#switchport access vlan 50

Switch-2(config-if-range)#switchport voice vlan 101

Switch-2(config-if-range)#spanning-tree portfast

Switch-2(config-if-range)#spanning-tree bpduguard enable

Switch-2(config-if-range)#exit

Switch-2(config)#int fa0/13

Switch-2(config-if)#switchport mode access

Switch-2(config-if)#switchport access vlan 60

Switch-2(config-if)#spanning-tree portfast

Switch-2(config-if)#spanning-tree bpduguard enable

Switch-2(config-if)#exit

Switch-2(config)#do wr

Switch-2(config)#exit

**#EtherChannel configuration and make it trunk**

Switch-2(config)#int range gig0/1-2

Switch-2(config-if-range)#channel-group 2 mode active

Switch-2(config-if-range)#exit

Switch-2(config)#int port-channel 2

Switch-2(config-if)#switchport mode trunk

Switch-2(config-if)#exit

Switch-2(config)#do wr

Switch-2(config)#exit

**Switch-3:**

Switch>en

Switch#conf t

**# Set hostname**

Switch(config)#hostname Switch-3

**# Console password setup**

Switch-3(config)#line console 0

Switch-3(config-line)#password switch3

Switch-3(config-line)#login

Switch-3(config-line)#exit

**# Enable secret for privileged access**

Switch-3(config)#enable secret switch3

**# Create local user account**

Switch-3(config)#username switch3 secret switch3

**# Encrypt all plaintext passwords**

Switch-3(config)#service password-encryption

**# Unauthorized access warning**

Switch-3(config)#banner motd # Unauthorized access is prohibited. #

**# Disable DNS lookup for mistyped commands**

Switch-3(config)#no ip domain-lookup

**# Save configuration**

Switch-3(config)#do wr

Switch-3(config)#exit

**#Create Vlans + assign access port + STP PortFast configuration + BPDUguard configuration**

Switch-3(config)#vlan 50

Switch-3(config-vlan)#name LAN

Switch-3(config-vlan)#exit

Switch-3(config)#vlan 60

Switch-3(config-vlan)#name WLAN

Switch-3(config-vlan)#exit

Switch-3(config)#vlan 101

Switch-3(config-vlan)#name VoIP

Switch-3(config-vlan)#exit

Switch-3(config)#int range fa0/2-12

Switch-3(config-if-range)#switchport mode access

Switch-3(config-if-range)#switchport access vlan 50

Switch-3(config-if-range)#switchport voice vlan 101

Switch-3(config-if-range)#spanning-tree portfast

Switch-3(config-if-range)#spanning-tree bpduguard enable

Switch-3(config-if-range)#exit

Switch-3(config)#int fa0/1

Switch-3(config-if)#switchport mode access

Switch-3(config-if)#switchport access vlan 60

Switch-3(config-if)#spanning-tree portfast

Switch-3(config-if)#spanning-tree bpduguard enable

Switch-3(config-if)#exit

Switch-3(config)#int range fa0/14-24

Switch-3(config-if-range)#switchport mode access

Switch-3(config-if-range)#switchport access vlan 50

Switch-3(config-if-range)#switchport voice vlan 101

Switch-3(config-if-range)#spanning-tree portfast

Switch-3(config-if-range)#spanning-tree bpduguard enable

Switch-3(config-if-range)#exit

Switch-3(config)#int fa0/13

Switch-3(config-if)#switchport mode access

Switch-3(config-if)#switchport access vlan 60

Switch-3(config-if)#spanning-tree portfast

Switch-3(config-if)#spanning-tree bpduguard enable

Switch-3(config-if)#exit

Switch-3(config)#do wr

Switch-3(config)#exit

**#EtherChannel configuration and make it trunk**

Switch-3(config)#int range gig0/1-2

Switch-3(config-if-range)#channel-group 3 mode active

Switch-3(config-if-range)#exit

Switch-3(config)#int port-channel 3

Switch-3(config-if)#switchport mode trunk

Switch-3(config-if)#exit

Switch-3(config)#do wr

Switch-3(config)#exit

**Central-WLC:**

**Static IP Configuration to Management Interface:**

**IP Address**: 10.20.0.2

**Subnet Mask**: 255.255.0.0

**Default Gateway**: 10.20.0.1

**DNS Server**: 10.10.10.5

**username**: cairo

**password**: Cairo@123

**System Name**: Cairo-WLC

**Management IP Address**: 10.20.0.2

**Subnet Mask**: 255.255.0.0

**Default Gateway**: 10.20.0.1

**Management VLAN ID**: 0

**Network Name**: Cairo-Management

**Password**: Management@123

**HR-Finance-AP:**

**HR Department:**

**Access Point Name**: HR-Fin-AP

**Network Name (SSID):** HR-WiFi

**Security Mode**: WPA2-PSK

**Passphrase**: HR@12345

**Associated VLAN**: 0

**Interface Name**: management

**VLAN Identifier**: 0

**IP Address**: 10.20.0.2

**Netmask**: 255.255.0.0

**Gateway**: 10.20.0.1

**Primary DHCP Server**: 10.10.10.5

**AP Group Name**: HR-Fin-Group

**Finance Department:**

**Access Point Name**: HR-Fin-AP

**Network Name (SSID):** Finance-WiFi

**Security Mode**: WPA2-PSK

**Passphrase**: Finance@12345

**Associated** VLAN: 0

**Interface Name**: management

**VLAN Identifier**: 0

**IP Address**: 10.20.0.2

**Netmask**: 255.255.0.0

**Gateway**: 10.20.0.1

**Primary DHCP Server**: 10.10.10.5

**AP Group Name**: HR-Fin-Group

**PB-Marketing-AP:**

**PB Department:**

**Access Point Name**: PB-Marketing-AP

**Network Name (SSID):** PB-WiFi

**Security Mode**: WPA2-PSK

**Passphrase**: PB@12345

**Associated VLAN**: 0

**Interface Name**: management

**VLAN Identifier**: 0

**IP Address**: 10.20.0.2

**Netmask**: 255.255.0.0

**Gateway**: 10.20.0.1

**Primary DHCP Server**: 10.10.10.5

**AP Group Name**: PB-Marketing-Group

**Marketing Department:**

**Access Point Name**: PB-Marketing-AP

**Network Name (SSID):** Marketing-WiFi

**Security Mode**: WPA2-PSK

**Passphrase**: Marketing@12345

**Associated VLAN**: 0

**Interface Name**: management

**VLAN Identifier**: 0

**IP Address**: 10.20.0.2

**Netmask**: 255.255.0.0

**Gateway**: 10.20.0.1

**Primary DHCP Server**: 10.10.10.5

**AP Group Name**: PB-Marketing-Group

**Admin-Corp-AP:**

**Admin Department:**

**Access Point Name**: Admin-Corp-AP

**Network Name (SSID):** Admin-WiFi

**Security Mode**: WPA2-PSK

**Passphrase**: Admin@12345

**Associated VLAN**: 0

**Interface Name**: management

**VLAN Identifier**: 0

**IP Address**: 10.20.0.2

**Netmask**: 255.255.0.0

**Gateway**: 10.20.0.1

**Primary DHCP Server**: 10.10.10.5

**AP Group Name**: Admin-Corp-Group

**Corporate Department:**

**Access Point Name**: Admin-Corp-AP

**Network Name (SSID):** Corporate-WiFi

**Security Mode**: WPA2-PSK

**Passphrase**: Corporate@12345

**Associated VLAN**: 0

**Interface Name**: management

**VLAN Identifier**: 0

**IP Address**: 10.20.0.2

**Netmask**: 255.255.0.0

**Gateway**: 10.20.0.1

**Primary DHCP Server**: 10.10.10.5

**AP Group Name**: Admin-Corp-Group

**IT-Support-AP:**

**IT Department:**

**Access Point Name**: IT-Support-AP

**Network Name (SSID):** IT-WiFi

**Security Mode**: WPA2-PSK

**Passphrase**: IT@12345

**Associated VLAN**: 0

**Interface Name**: management

**VLAN Identifier**: 0

**IP Address**: 10.20.0.2

**Netmask**: 255.255.0.0

**Gateway**: 10.20.0.1

**Primary DHCP Server**: 10.10.10.5

**AP Group Name**: IT-Support-Group

**Support Department:**

**Access Point Name**: IT-Support-AP

**Network Name (SSID):** Support-WiFi

**Security Mode**: WPA2-PSK

**Passphrase**: Support@12345

**Associated VLAN**: 0

**Interface Name**: management

**VLAN Identifier**: 0

**IP Address**: 10.20.0.2

**Netmask**: 255.255.0.0

**Gateway**: 10.20.0.1

**Primary DHCP Server**: 10.10.10.5

**AP Group Name**: IT-Support-Group

**Software-Engin-AP:**

**Software Engineering Department:**

**Access Point Name**: Software-Engin-AP

**Network Name (SSID):** Software-WiFi

**Security Mode**: WPA2-PSK

**Passphrase**: Software@12345

**Associated VLAN**: 0

**Interface Name**: management

**VLAN Identifier**: 0

**IP Address**: 10.20.0.2

**Netmask**: 255.255.0.0

**Gateway**: 10.20.0.1

**Primary DHCP Server**: 10.10.10.5

**AP Group Name**: Software-Group

**Cloud-Engin-AP:**

**Cloud Engineering Department:**

**Access Point Name**: Cloud-Engin-AP

**Network Name (SSID):** Cloud-WiFi

**Security Mode**: WPA2-PSK

**Passphrase**: Cloud@12345

**Associated VLAN**: 0

**Interface Name**: management

**VLAN Identifier**: 0

**IP Address**: 10.20.0.2

**Netmask**: 255.255.0.0

**Gateway**: 10.20.0.1

**Primary DHCP Server**: 10.10.10.5

**AP Group Name**: Cloud-Group

**DMZ-Switch:**

Switch>en

Switch#conf t

**# Set hostname**

Switch(config)#hostname DMZ-Switch

**# Console password setup**

DMZ-Switch(config)#line console 0

DMZ-Switch(config-line)#password dmz

DMZ-Switch(config-line)#login

DMZ-Switch(config-line)#exit

**# Enable secret for privileged access**

DMZ-Switch(config)#enable secret dmz

**# Create local user account**

DMZ-Switch(config)#username dmz secret dmz

**# Encrypt all plaintext passwords**

DMZ-Switch(config)#service password-encryption

**# Unauthorized access warning**

DMZ-Switch(config)#banner motd # Unauthorized access is prohibited. #

**# Disable DNS lookup for mistyped commands**

DMZ-Switch(config)#no ip domain-lookup

**# Save configuration**

DMZ-Switch(config)#do wr

DMZ-Switch(config)#exit

**AD-Server(DHCP and DNS Server):**

**Static IP Configuration:**

**IP Address**: 10.10.10.5

**Subnet Mask**: 255.255.255.240

**Default Gateway**: 10.10.10.1

**DNS Server**: 10.10.10.5

**DHCP Configuration:**

1. **WLAN (VLAN 60)**

* **Pool Name**: wlan\_pool
* **Network ID**: 10.20.0.0/16
* **Default Gateway**: 10.20.0.1
* **DNS Server**: 10.10.10.5
* **Starting IP Address**: 10.20.0.10
* **Subnet Mask**: 255.255.0.0
* **WLC Addresses**: 10.20.0.2
* **Maximum Number of Users**: 65,518

1. **Exclusions:**

* **Network Address:** 10.20.0.0
* **Default Gateway**: 10.20.0.1
* **Broadcast Address**: 10.20.255.255
* **Reserved for Core Network Devices**: 10.20.0.2 - 10.20.0.9
* **Reserved for Scalability**: 10.20.255.250 - 10.20.255.254
* **Usable IP Range**: 10.20.0.10 - 10.20.255.249

1. **LAN (VLAN 50)**

* **Pool Name**: lan\_pool
* **Network ID**: 192.168.10.0/24
* **Default Gateway**: 192.168.10.1
* **DNS Server**: 10.10.10.5
* **Starting IP Address**: 192.168.10.10
* **Subnet Mask**: 255.255.255.0
* **Maximum Number of Users**: 238

1. **Exclusions:**

* **Network Address**: 192.168.10.0
* **Default Gateway**: 192.168.10.1
* **Broadcast Address**: 192.168.10.255
* **Reserved for Core Network Devices**: 192.168.10.2 - 192.168.10.9
* **Reserved for Scalability**: 192.168.10.250 - 192.168.10.254
* **Usable IP Range**: 192.168.10.10 - 192.168.10.249

**DNS Configuration:**

**DNS Record:**

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Name | Type | Detail |
| 1. | pop.cairo.com | A Record | 10.10.10.7 |
| 2. | smtp.cairo.com | A Record | 10.10.10.7 |
| 3. | www.cairo.com | A Record | 10.10.10.6 |

**ERP-Server:**

**Static IP Configuration:**

**IP Address**: 10.10.10.6

**Subnet Mask**: 255.255.255.240

**Default Gateway**: 10.10.10.1

**DNS Server**: 10.10.10.5

**Web Page:**

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="UTF-8">

<meta name="viewport" content="width=device-width, initial-scale=1.0">

<title>Cairo Telco</title>

</head>

<body style="font-family: Arial, sans-serif; background-color: #f3f3f3; color: #333; text-align: center;">

<header style="background-color: #003366; padding: 20px; color: white;">

<h1>Cairo Telco</h1>

<p>A Fast-Growing Telecommunication Company in Egypt</p>

</header>

<main style="padding: 40px;">

<section>

<h2>Welcome to Cairo Telco</h2>

<p>

Cairo Telco is dedicated to providing top-notch IT solutions and services to businesses across Egypt. We specialize in telecommunication infrastructure, network security, cloud solutions, and managed IT services.

</p>

<p>

Our team of experienced professionals is committed to supporting our clients with reliable and secure technology solutions, helping them grow and achieve their business goals.

</p>

</section>

<section style="margin-top: 40px;">

<h3>Our Services</h3>

<ul style="list-style-type: none; padding: 0;">

<li>Telecommunication Infrastructure</li>

<li>Network Security Solutions</li>

<li>Cloud Computing Services</li>

<li>Managed IT Services</li>

</ul>

</section>

</main>

<footer style="background-color: #003366; color: white; padding: 10px;">

<p>&copy; 2024 Cairo Telco | All rights reserved</p>

</footer>

</body>

</html>

**Email-Server:**

**Static IP Configuration:**

**IP Address**: 10.10.10.7

**Subnet Mask**: 255.255.255.240

**Default Gateway**: 10.10.10.1

**DNS Server**: 10.10.10.5

**Set the Email Domain:**

**Domain Name**: cairo.com

**Users Email Tables:**

|  |  |  |  |
| --- | --- | --- | --- |
| HR | | | |
| No. | **Username** | **Password** | **Email** |
| 1. | hr | hr@12345 | hr@cairo.com |

|  |  |  |  |
| --- | --- | --- | --- |
| Finance | | | |
| No. | **Username** | **Password** | **Email** |
| 1. | finance | Finance@12345 | finance@cairo.com |

|  |  |  |  |
| --- | --- | --- | --- |
| Product Brand | | | |
| No. | **Username** | **Password** | **Email** |
| 1. | pb | PB@12345 | pb@cairo.com |

|  |  |  |  |
| --- | --- | --- | --- |
| Marketing | | | |
| No. | **Username** | **Password** | **Email** |
| 1. | marketing | Marketing@12345 | marketing@cairo.com |

|  |  |  |  |
| --- | --- | --- | --- |
| Administrator | | | |
| No. | **Username** | **Password** | **Email** |
| 1. | **admin** | **Admin@12345** | **admin@cairo.com** |

|  |  |  |  |
| --- | --- | --- | --- |
| Corporate | | | |
| No. | **Username** | **Password** | **Email** |
| 1. | corporate | Corporate@12345 | corporate@cairo.com |

|  |  |  |  |
| --- | --- | --- | --- |
| IT | | | |
| No. | **Username** | **Password** | **Email** |
| 1. | it | IT@12345 | it@cairo.com |

|  |  |  |  |
| --- | --- | --- | --- |
| Support | | | |
| No. | **Username** | **Password** | **Email** |
| 1. | support | Support@12345 | support@cairo.com |

|  |  |  |  |
| --- | --- | --- | --- |
| Software Engineering | | | |
| No. | **Username** | **Password** | **Email** |
| 1. | sde | SDE@12345 | sde@cairo.com |

|  |  |  |  |
| --- | --- | --- | --- |
| Cloud Engineering | | | |
| No. | **Username** | **Password** | **Email** |
| 1. | ce | CE@12345 | ce@cairo.com |

**Client Side Email Setting:**

**Your Name**: XYZ

**Email Address**: XYZ@cairo.com

**Incoming Server**: pop.cairo.com, Port 995 (SSL)

**Outgoing Server**: smtp.cairo.com, Port 465 (SSL)

**User Name**: XYZ@cairo.com

**Password**: XYZ@12345

**File-Storage-Server:**

**Static IP Configuration:**

**IP Address:** 10.10.10.8

**Subnet Mask**: 255.255.255.240

**Default Gateway**: 10.10.10.1

**DNS Server**: 10.10.10.5

**Voice-Gateway:**

Switch>en

Switch#conf t

**#Set the hostname**

Router(config)#hostname Voice-Gateway

**#Set console password**

Voice-Gateway(config)#line console 0

Voice-Gateway(config-line)#password voice

Voice-Gateway(config-line)#login

Voice-Gateway(config-line)#exit

**#Set enable secret password for privileged EXEC mode**

Voice-Gateway(config)#enable secret voice

**#Enable password encryption for all passwords**

Voice-Gateway(config)#service password-encryption

**#Configure banner for unauthorized access warning**

Voice-Gateway(config)#banner motd # Unauthorized access is prohibited. #

**#Disable domain name lookup to prevent delays caused by incorrect commands**

Voice-Gateway(config)#no ip domain-lookup

**#Configure SSH**

Voice-Gateway(config)#ip domain-name cairo.com

**#Generate RSA key pairs for SSH encryption**

Voice-Gateway(config)#crypto key generate rsa

How many bits in the modulus [512]: 1024

**#Enable SSH version 2**

Voice-Gateway(config)#ip ssh version 2

**#Create a local user for SSH access**

Voice-Gateway(config)#username voice secret voice

**#Configure VTY lines to accept only SSH connections**

Voice-Gateway(config)#line vty 0 4

Voice-Gateway(config-line)#transport input ssh

Voice-Gateway(config-line)#login local

Voice-Gateway(config-line)#exit

**#Set SSH time-out and retries to improve security**

Voice-Gateway(config)#ip ssh time-out 60

Voice-Gateway(config)#ip ssh authentication-retries 3

Voice-Gateway(config)#do wr

Voice-Gateway(config)#exit

**# Enable interface FastEthernet 0/0**

Voice-Gateway(config)#int fa0/0

Voice-Gateway(config-if)#no shut

Voice-Gateway(config-if)#exit

**# Configure sub-interface for VLAN 101 with IP address**

Voice-Gateway(config)#int fa0/0.101

Voice-Gateway(config-subif)#encapsulation dot1Q 101

Voice-Gateway(config-subif)#ip address 172.16.10.1 255.255.255.0

Voice-Gateway(config-subif)#exit

**# Enable DHCP and set up VoIP pool**

Voice-Gateway(config)#service dhcp

Voice-Gateway(config)#ip dhcp pool VoIP-pool

Voice-Gateway(dhcp-config)#network 172.16.10.0 255.255.255.0

Voice-Gateway(dhcp-config)#default-router 172.16.10.1

Voice-Gateway(dhcp-config)#option 150 ip 172.16.10.1

Voice-Gateway(dhcp-config)#exit

**# Configure telephony service for VoIP**

Voice-Gateway(config)#telephony-service

Voice-Gateway(config-telephony)#max-dn 20

Voice-Gateway(config-telephony)#max-ephone 20

Voice-Gateway(config-telephony)#ip source-address 172.16.10.1 port 2000

Voice-Gateway(config-telephony)#auto assign 1 to 20

Voice-Gateway(config-telephony)#exit

**# Assign phone numbers 1001-1010 to ephones**

Voice-Gateway(config)#ephone-dn 1

Voice-Gateway(config-ephone-dn)#number 1001

Voice-Gateway(config-ephone-dn)#exit

Voice-Gateway(config)#ephone-dn 2

Voice-Gateway(config-ephone-dn)#number 1002

Voice-Gateway(config-ephone-dn)#exit

Voice-Gateway(config)#ephone-dn 3

Voice-Gateway(config-ephone-dn)#number 1003

Voice-Gateway(config-ephone-dn)#exit

Voice-Gateway(config)#ephone-dn 4

Voice-Gateway(config-ephone-dn)#number 1004

Voice-Gateway(config-ephone-dn)#exit

Voice-Gateway(config)#ephone-dn 5

Voice-Gateway(config-ephone-dn)#number 1005

Voice-Gateway(config-ephone-dn)#exit

Voice-Gateway(config)#ephone-dn 6

Voice-Gateway(config-ephone-dn)#number 1006

Voice-Gateway(config-ephone-dn)#exit

Voice-Gateway(config)#ephone-dn 7

Voice-Gateway(config-ephone-dn)#number 1007

Voice-Gateway(config-ephone-dn)#exit

Voice-Gateway(config)#ephone-dn 8

Voice-Gateway(config-ephone-dn)#number 1008

Voice-Gateway(config-ephone-dn)#exit

Voice-Gateway(config)#ephone-dn 9

Voice-Gateway(config-ephone-dn)#number 1009

Voice-Gateway(config-ephone-dn)#exit

Voice-Gateway(config)#ephone-dn 10

Voice-Gateway(config-ephone-dn)#number 1010

Voice-Gateway(config-ephone-dn)#exit

Voice-Gateway(config)#do wr

Voice-Gateway(config)#exit

**Seacom-ISP:**

Router>en

Router#conf t

**#Assign hostname**

Router(config)#hostname Seacom-ISP

**#Assign IP Address to interface**

Seacom-ISP(config)#int gig0/0

Seacom-ISP(config-if)#no shutdown

Seacom-ISP(config-if)#ip address 197.200.100.1 255.255.255.252

Seacom-ISP(config-if)#exit

Seacom-ISP(config)#int gig0/1

Seacom-ISP(config-if)#no shutdown

Seacom-ISP(config-if)#ip address 20.20.20.1 255.255.255.252

Seacom-ISP(config-if)#exit

Seacom-ISP(config)#do wr

Seacom-ISP(config)#exit

**#Enable Routing Protocol (OSPF)**

Seacom-ISP(config)#router ospf 10

Seacom-ISP(config-router)#network 197.200.100.0 0.0.0.3 area 0

Seacom-ISP(config-router)#network 20.20.20.0 0.0.0.3 area 0

Seacom-ISP(config-router)#exit

Seacom-ISP(config)#do wr

Seacom-ISP(config)#exit

**Azure-Cloud:**

Router>en

Router#conf t

**#Assign hostname**

Router(config)#hostname Azure-Cloud

**#Assign IP Address to interface**

Azure-Cloud(config)#int gig0/0

Azure-Cloud(config-if)#no shutdown

Azure-Cloud(config-if)#ip address 20.20.20.2 255.255.255.252

Azure-Cloud(config-if)#exit

Azure-Cloud(config)#int gig0/1

Azure-Cloud(config-if)#no shutdown

Azure-Cloud(config-if)#ip address 30.0.0.1 255.0.0.0

Azure-Cloud(config-if)#exit

Azure-Cloud(config)#do wr

Azure-Cloud(config)#exit

**#Enable Routing Protocol (OSPF)**

Azure-Cloud(config)#router ospf 10

Azure-Cloud(config-router)#network 30.0.0.0 0.255.255.255 area 0

Azure-Cloud(config-router)#network 20.20.20.0 0.0.0.3 area 0

Azure-Cloud(config-router)#exit

Azure-Cloud(config)#do wr

Azure-Cloud(config)#exit

**Azure-Switch:**

Switch>en

Switch#conf t

**#Assign hostname**

Switch(config)#hostname Azure-Switch

**Result:**

