4. Design and Implementation of a Secure Telecommunication Company Network

Objective

The main motive of this project is to design and implement a secure Telecommunication Company Network which has two floors of departments. One floor is hosting HR and Finance (40), Product Brand and Marketing (45), and Admin and Corporate departments (35). The second floor is hosting IT Network & Support (45), Software Engineering (36), and Cloud Engineering departments (32) departments. The company has subscribed to ISP for internet services and has purchased one Cisco ASA Firewall, Switches, 1 Cisco Voice Gateway, 1 Cisco WLC, and 6 LAPs. The company has Cisco Voice Gateways to provide VoIP or telephony services in the network and Cisco WLC to provide central management for Aps.

The company has emphasized high performance, redundancy, scalability, and availability, and hence it is 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.

Details of design

Hierarchical Design- Use a hierarchical model providing redundancy at every layer.

ISPs- The network is also expected to connect to a Seacom ISP Router.

WLC- Each department is required to have a WAP providing both employees and guest WIFI managed by WLC.

VoIP- Each department should have IP phones.

VLAN- The LAN, WLAN, and VoIP VLANs remain at 50, 60 & 101 respectively for the entire network.

EtherChannel- Use standard LACP as a method of link aggregation.

STP PortFast and BPDUguard- configure the two protocols to enable faster port transition from blocking to forwarding.

Subnetting- Provided the networks above, carry out subnetting to allocate the correct number of IP addresses to each department.

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.

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.

Core Switch- The Multilayer switches are expected to carry out both routing and switching functionalities and thus will be assigned IP addresses.

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.

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).

Static Addressing- Devices in the server room are to be allocated IP addresses statically.

Telephony Service- Configure VoIP on the voice gateway router and allocate dial numbers in format (1...).

Routing Protocol- Use OSPF as the routing protocol to advertise routes both on the routers and multilayer switches.

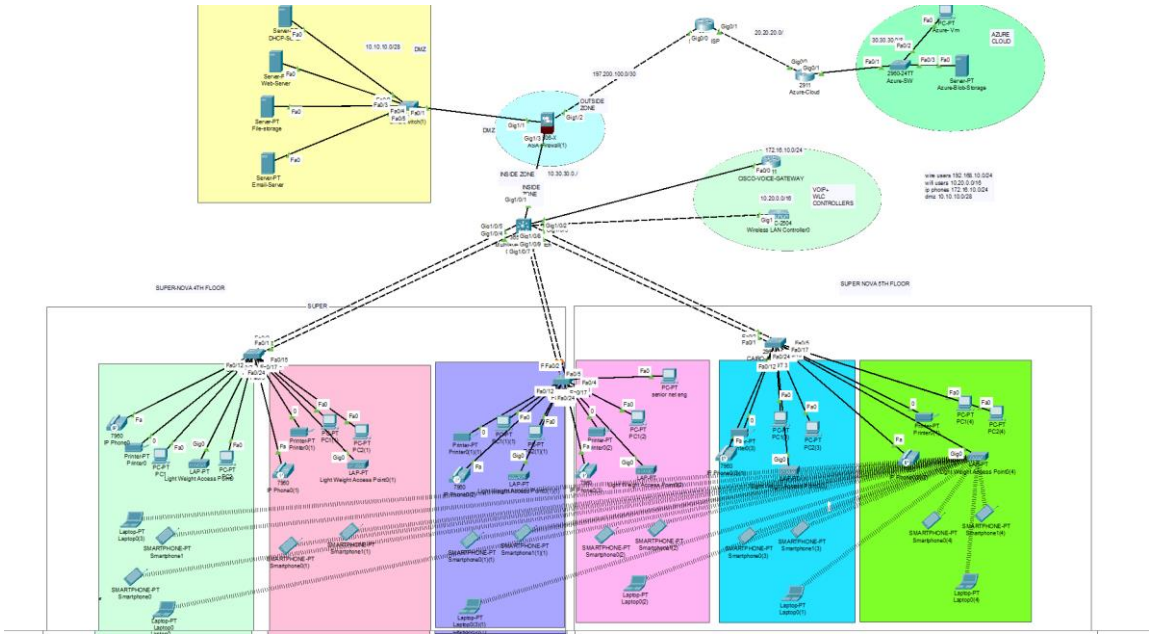
Cisco ASA Firewall- Configure security levels, zones, and policies to define how resources are accessed in the network

Final- Test Communication, ensure everything configured is working as expected.

Technologies Implemented

- Creating a network topology using Cisco Packet Tracer.
- Hierarchical Network Design.
- Connecting Networking devices with Correct cabling.
- Configuring Basic device settings.
- Creating VLANs and assigning ports VLAN numbers.
- Creating both data and voice VLANs and assigning ports VLAN numbers.
- Configuring Spanning-Tree Protocol - STP PortFast and BPDUGuard EtherChannel using LACP method.
- Subnetting and IP Addressing configuration.
- Configuring Inter-VLAN Routing both on the Switches (SVI) and Routers (router-on-a-stick).
- Configuring Dedicated DHCP Server device for Data to provide dynamic IP allocation.
- Configuring Routers as DHCP server for Voice to provide IP Phones dynamic IP allocation.
- Configuring Active Directory as DHCP Server.
- Configuring WLAN network- Wireless LAN Controller + Wireless Lightweight Access Points.
- Configuring SSH for secure Remote access to only Senior Network Security Engineer.
- Configuring OSPF as the routing protocol.
- Configuring Standard ACL for VTY interfaces to restrict remote Access using SSH.
- Configuring VoIP or Telephony service configuration in VoIP routers.
- Configuring Cisco ASA Firewall Interface descriptions, zones, and security levels.
- Configuring Cisco ASA Firewall Object Network + NAT + Default Static Routes.
- Configuring Cisco ASA Firewall OSPF.
- Configuring Cisco ASA Firewall Inspection Policies to filter traffic based on predetermined ACLs.
- Host Device Configurations.

Network Topology Diagram



Configuring Basic device settings

The basic settings have been made on DMZ Switch, 3 access layer switch, Azure switch, Multilayer switch and VoIP router.

DMZ-Switch

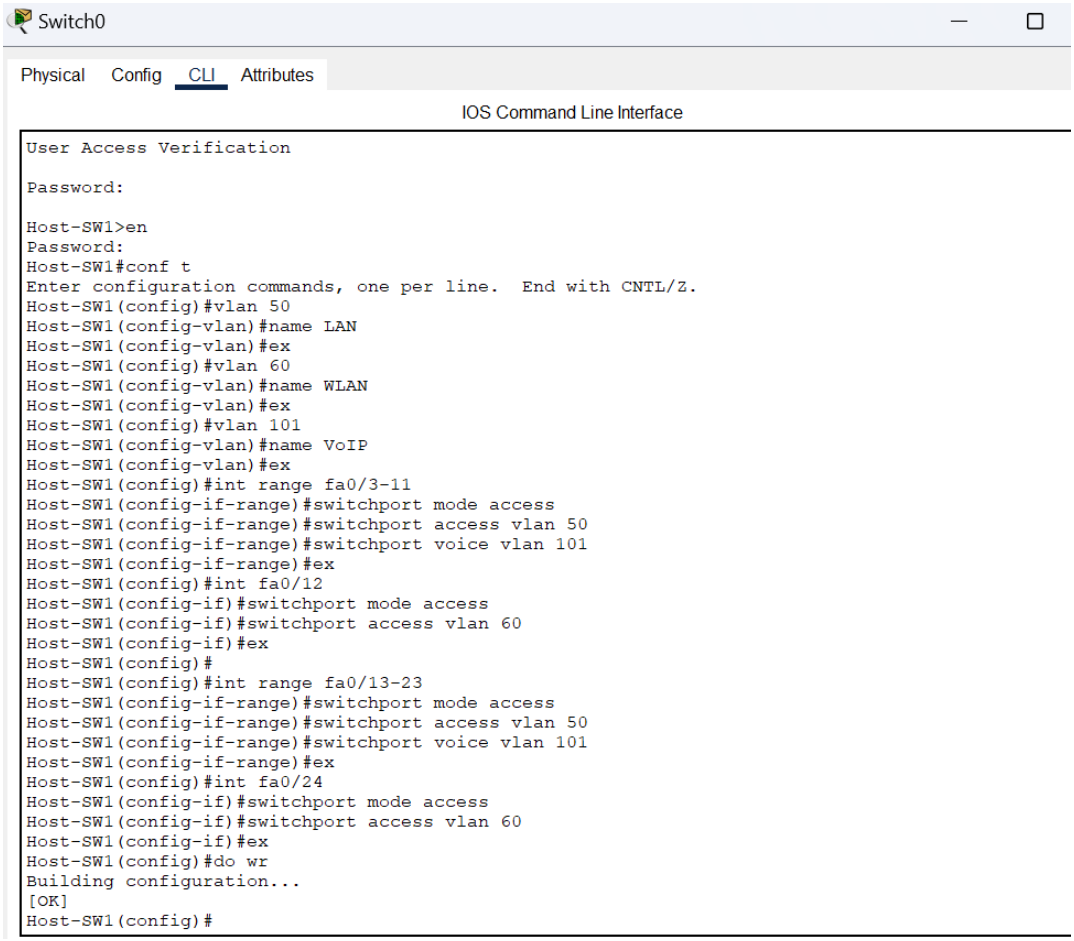
Physical Config CLI Attributes

IOS Command Line Interface

```
Switch>en
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname DMZ-SW
DMZ-SW(config)#enable password cisco
DMZ-SW(config)#banner motd *No unauthorized access*
DMZ-SW(config)#no ip domain lookup
DMZ-SW(config)#line console 0
DMZ-SW(config-line)#password cisco
DMZ-SW(config-line)#login
DMZ-SW(config-line)#
DMZ-SW(config-line)#service password-encryption
DMZ-SW(config)#
DMZ-SW(config)#ip domain name cisco.net
DMZ-SW(config)#username admin password cisco
DMZ-SW(config)#do wr
Building configuration...
[OK]
DMZ-SW(config)#
```

Creating VLANs and assigning ports VLAN numbers for wired, wireless and VoIP

All 3-access layer switch have been assigned VLANs.



Configuring Spanning Tree Protocol STP PortFast and BPDUGuard EtherChannel using LACP (Link Aggregation Control Protocol) method

1. STP PortFast and BPDU Guard

PortFast:

PortFast is a Cisco-specific feature that allows a switch port to bypass the usual Spanning Tree Protocol (STP) states (Listening, Learning) and go directly to the Forwarding state. This is useful for ports that connect to end devices like computers, where the STP process isn't necessary.

BPDU Guard:

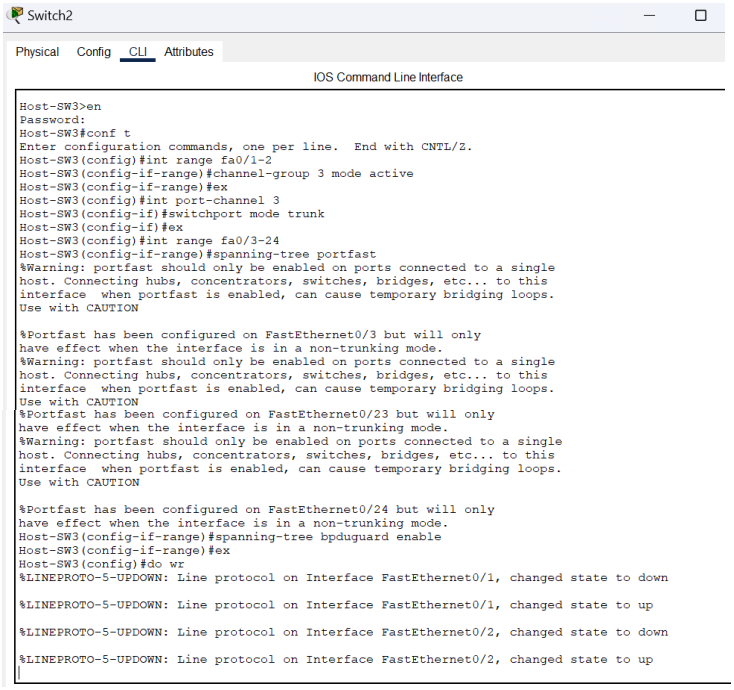
BPDU Guard is a security feature that disables a port if it receives Bridge Protocol Data Units (BPDUs). It's typically used on ports with PortFast enabled to prevent unintended STP changes if a switch is mistakenly connected.

2. EtherChannel using LACP

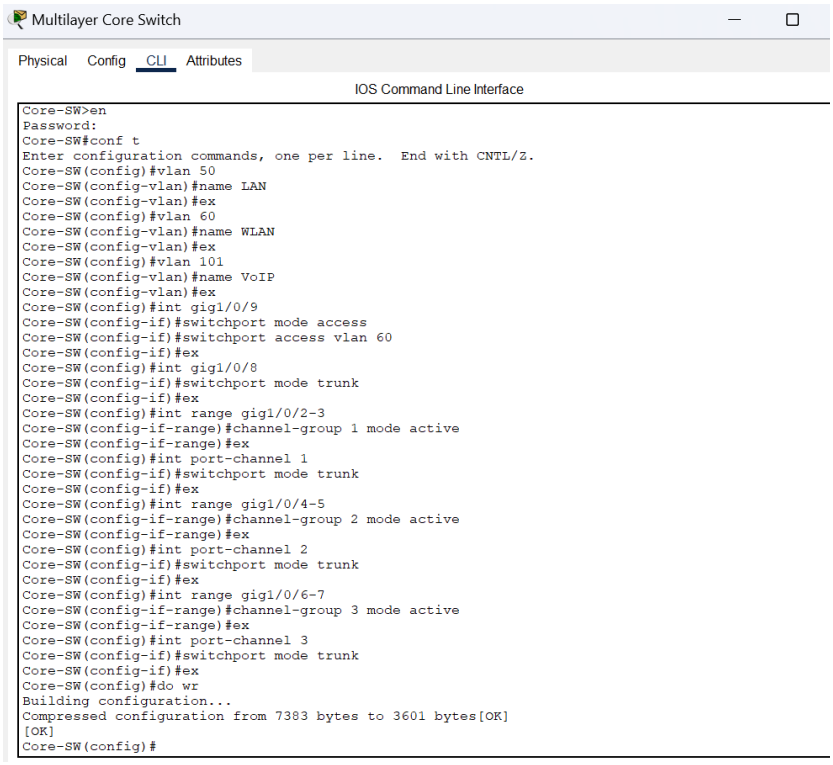
EtherChannel is a technology that allows the grouping of multiple physical Ethernet links to create a logical link for increased bandwidth and redundancy. LACP (Link Aggregation Control Protocol) is a dynamic protocol for automatically configuring and maintaining Ethernet channels.

These configurations enhance network performance and security, providing faster convergence and protection against certain network misconfigurations.

The channel-group 1, 2 and 3 are used for the three switches.



On L3 core switch,



Subnetting

Category	Network address	Broadcast address	Host range	Subnet Mask
WLAN	10.20.0.0/16	10.20.255.255/16	10.20.0.1 to 10.20.255.254	255.255.0.0

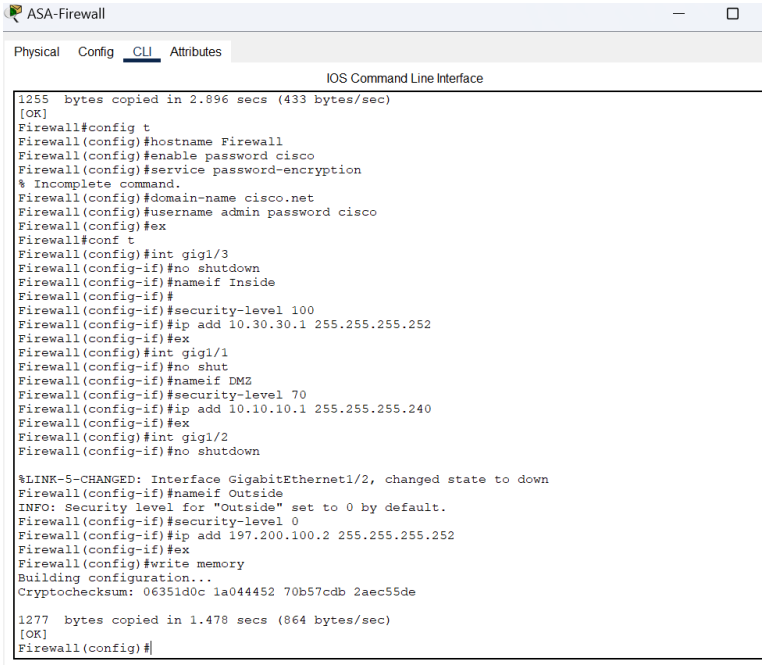
LAN	192.168.10.0/24	192.168.10.255/24	192.168.10.1 to 192.168.10.254	255.255.255.0
VoIP	172.16.10.0/24	172.16.10.255/24	172.16.10.1 to 172.16.10.254	255.255.255.0
DMZ	10.10.10.0/28	10.10.10.15/28	192.168.100.193 to 192.168.100.254	255.255.255.240

Between the Firewall, ISP Router and Layer 3 switch

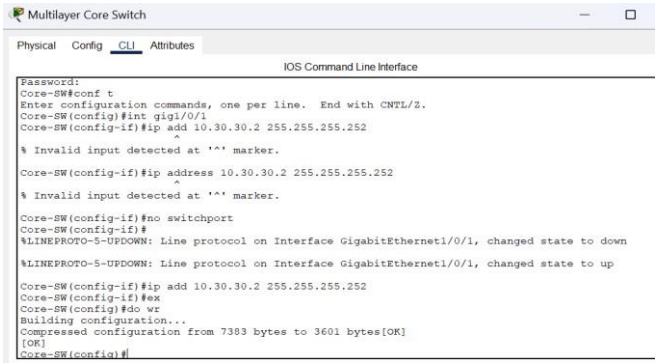
Firewall-ISP	197.200.100.0/30
Firewall-MLSW1	10.30.30.0/30
ISP-Cloud	20.20.20.0/30
Cloud	30.30.30.0/8

IP Addressing configuration

On Firewall



On Multilayer Switch



On ISP Router

SEACOM-ISP

IOS Command Line Interface

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int gig0/0
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

Router(config-if)#ip add 197.200.100.1 255.255.255.252
Router(config-if)#ex
Router(config)#int gig0/1
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

Router(config-if)#ip add 20.20.20.1 255.255.255.252
Router(config-if)#ex
Router(config)#
```

On Azure Cloud Router

Azure Cloud

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int gig0/0
Router(config-if)#no shut
Router(config-if)#ip add 20.20.20.2 255.255.255.252
Router(config-if)#ex
Router(config)#int gig0/1
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

Router(config-if)#ip add 30.30.30.1 255.0.0.0
Router(config-if)#ex
Router(config)#do wr
Building configuration...
[OK]
Router(config)#
```

Configuring Inter VLAN Routing on the Switches (SVI) and DHCP helper

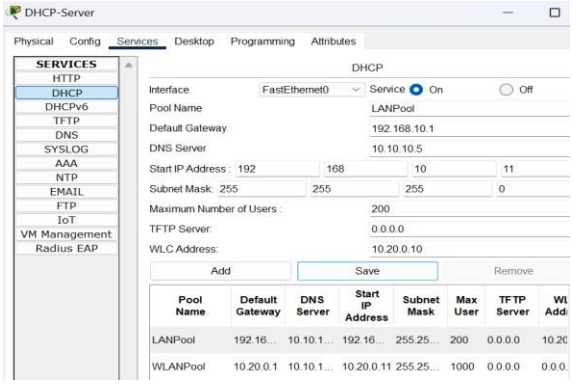
Multilayer Core Switch

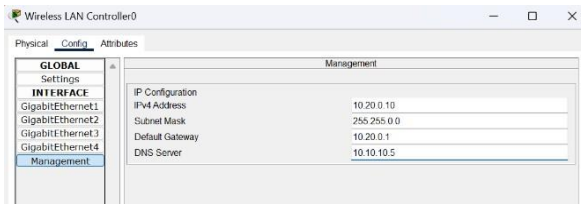
Physical Config CLI Attributes

IOS Command Line Interface

```
Password:
Core-SW#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Core-SW(config)#int gig1/0/1
Core-SW(config-if)#ip add 10.30.30.2 255.255.255.252
Core-SW(config-if)#ex
Core-SW(config)#-----
                ^
% Invalid input detected at '^' marker.

Core-SW(config)#int vlan 50
Core-SW(config-if)#no shut
Core-SW(config-if)#ip add 192.168.10.1 255.255.255.0
Core-SW(config-if)#ex
Core-SW(config)#int vlan 60
Core-SW(config-if)#no shut
Core-SW(config-if)#ip add 10.20.0.1 255.255.0.0
Core-SW(config-if)#ex
Core-SW(config)#do wr
Building configuration...
Compressed configuration from 7383 bytes to 3601 bytes[OK]
[OK]
Core-SW(config)#int vlan 50
Core-SW(config-if)#ip helper-address 10.10.10.5
Core-SW(config-if)#ex
Core-SW(config)#int vlan 60
Core-SW(config-if)#ip helper-address 10.10.10.5
Core-SW(config-if)#ex
Core-SW(config)#do wr
Building configuration...
Compressed configuration from 7383 bytes to 3601 bytes[OK]
[OK]
```

DHCP pool server configuration for LAN & WLAN





OSPF on Switch, Firewall and ISP & Cloud Router

Multilayer Core Switch

```
%SYS-5-CONFIG_I: Configured from console by console

Core-SW#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Core-SW(config)#ip routing
Core-SW(config)#router ospf 30
Core-SW(config-router)#router-id 1.1.1.1
Core-SW(config-router)#network 192.168.10.0 0.0.0.255 area 0
Core-SW(config-router)#network 10.20.0.0 0.0.255.255 area 0
Core-SW(config-router)#network 10.30.30.0 0.0.0.3 area 0
Core-SW(config-router)#ex
Core-SW(config)#do wr
Building configuration...
Compressed configuration from 7383 bytes to 3601 bytes[OK]
[OK]
Core-SW(config)#
```

ASA-Firewall

```
Firewall#conf t
Firewall(config)#router ospf 30
Firewall(config-router)#router-id 1.1.2.2
Firewall(config-router)#network 10.30.30.0 255.255.255.252 area 0
Firewall(config-router)#network 10.10.10.0 255.255.255.240 area 0
Firewall(config-router)#network 197.200.100.0 255.255.255.252 area 0
Firewall(config-router)#ex
Firewall(config)#do wr
Firewall(config)#ex
Firewall#do wr
         ^
% Invalid input detected at '^' marker.

Firewall#wr mem
Building configuration...
Cryptochecksum: 06351d0c 1a044452 70b57cdb 2aec55de

1454  bytes copied in 1.316 secs (1104 bytes/sec)
[OK]
Firewall#
```

ISP1

```
changed state to up


Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 30
Router(config-router)#router-id 1.1.3.3
Router(config-router)#network 197.200.100.0 0.0.0.3 area 0
Router(config-router)#
00:07:15: %OSPF-5-ADJCHG: Process 30, Nbr 1.1.2.2 on GigabitEthernet0/0
from LOADING to FULL, Loading Done

Router(config-router)#network 20.20.20.0 0.0.0.3 area 0
Router(config-router)#ex
Router(config)#do wr
Building configuration...
[OK]
Router(config)#
```

Azure Cloud

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 30
Router(config-router)#router-id 1.1.4.4
Router(config-router)#network 20.20.20.0 0.0.0.3 area 0
Router(config-router)#network 30.30.30.0 0.
00:10:59: %OSPF-5-ADJCHG: Process 30, Nbr 1.1.3.3 on GigabitEthernet0/0 from LOADING to FULL,
Loading Done
                                          ^
% Invalid input detected at '^' marker.

Router(config-router)#network 30.30.30.0 0.255.255.255.255 area 0
                                         ^
% Invalid input detected at '^' marker.

Router(config-router)#network 30.30.30.0 0.255.255.255 area 0
Router(config-router)#ex
Router(config)#do wr
```

Configuring Firewall Object Network + NAT

ASA-Firewall

Physical Config CLI Attributes

IOS Command Line Interface

```
Firewall>en
Password:
Firewall#conf t
Firewall(config)#object network INSIDE-TO-OUT
Firewall(config-network-object)#SUBNET 192.168.10.0 255.255.255.0
Firewall(config-network-object)#NAT (INSIDE,OUTSIDE) dynamic interface
Firewall(config-network-object)#ex
Firewall#conf t
Firewall(config)#object network INSIDE-TO-OUT2
Firewall(config-network-object)#subnet 10.20.0.0 255.255.0.0
Firewall(config-network-object)#nat (INSIDE,OUTSIDE) dynamic interface
Firewall(config-network-object)#ex
Firewall#conf t
Firewall(config)#object network INSIDE-TO-OUT3
Firewall(config-network-object)#subnet 10.10.10.0 255.255.255.240
Firewall(config-network-object)#nat (INSIDE,OUTSIDE) dynamic interface
Firewall(config-network-object)#ex
Firewall#conf t
Firewall(config)#route OUTSIDE 0.0.0.0 0.0.0.0 197.200.100.1
Firewall(config)#wr mem
Building configuration...
Cryptochecksum: 06351d0c 1a044452 70b57cdb 2aec55de

1799  bytes copied in 2.696 secs (667 bytes/sec)
[OK]
Firewall(config)#
```

Firewall inspection policy configuration

ASA-Firewall

Physical Config CLI Attributes

IOS Command Line Interface

```
% Invalid input detected at '^' marker.

Firewall(config)#access-list INSIDE-DMZ extended permit icmp any any
Firewall(config)#
Firewall(config)#access-list INSIDE-DMZ extended permit udp any any eq 53
Firewall(config)#access-list INSIDE-DMZ extended permit tcp any any eq 53
Firewall(config)#
Firewall(config)#access-list INSIDE-DMZ extended permit udp any any eq 67
Firewall(config)#access-list INSIDE-DMZ extended permit udp any any eq 68
Firewall(config)#
Firewall(config)#access-list INSIDE-DMZ extended permit tcp any any eq 80
Firewall(config)#
Firewall#
Firewall#
%SYS-5-CONFIG_I: Configured from console by console

Firewall#conf t
Firewall(config)#access-list INSIDE-DMZ extended permit tcp any any eq 443
Firewall(config)#access-list INSIDE-DMZ extended permit tcp any any eq 80
WARNING: <INSIDE-DMZ> found duplicate element
Firewall(config)#access-list INSIDE-DMZ extended permit tcp any any eq 8080
Firewall(config)#access-list INSIDE-DMZ extended permit tcp any any eq 8443
Firewall(config)#
Firewall(config)#access-group INSIDE-DMZ in interface DMZ
Firewall(config)#wr mem
Building configuration...
Cryptochecksum: 06351d0c 1a044452 70b57cdb 2aec55de

2360  bytes copied in 1.427 secs (1653 bytes/sec)
[OK]
Firewall(config)#show start
```

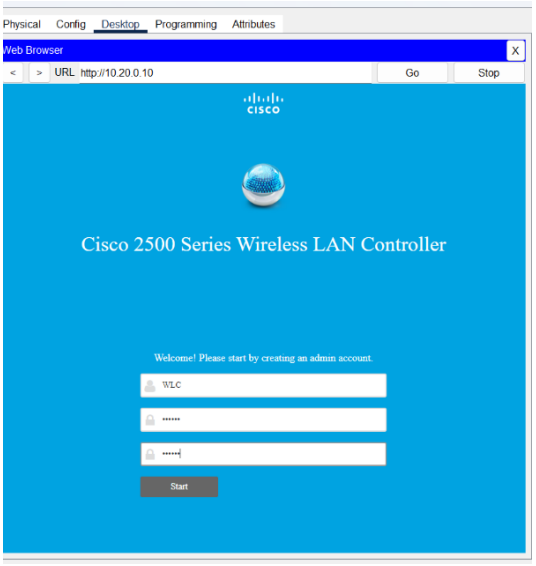
ASA-Firewall

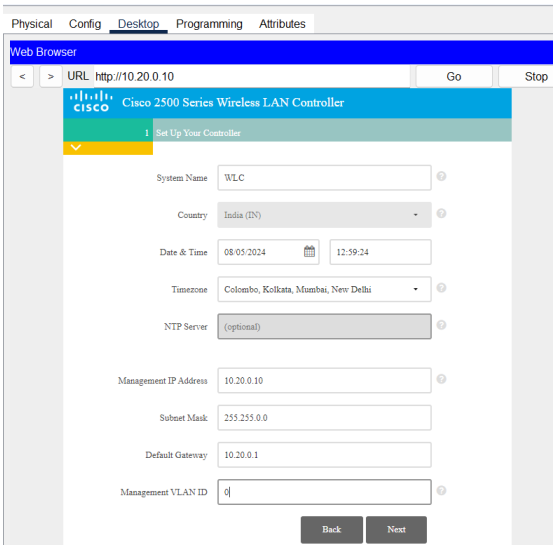
Physical Config CLI Attributes

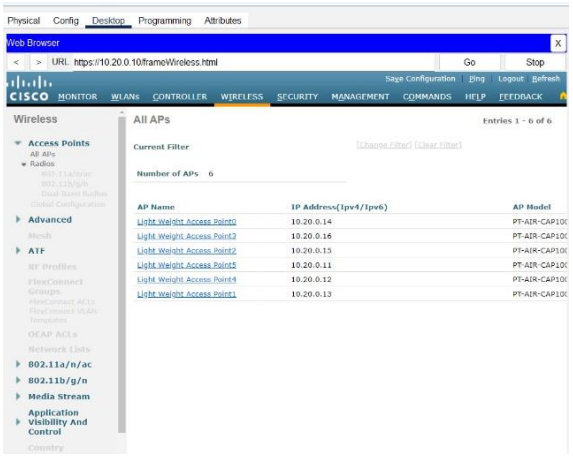
IOS Command Line Interface

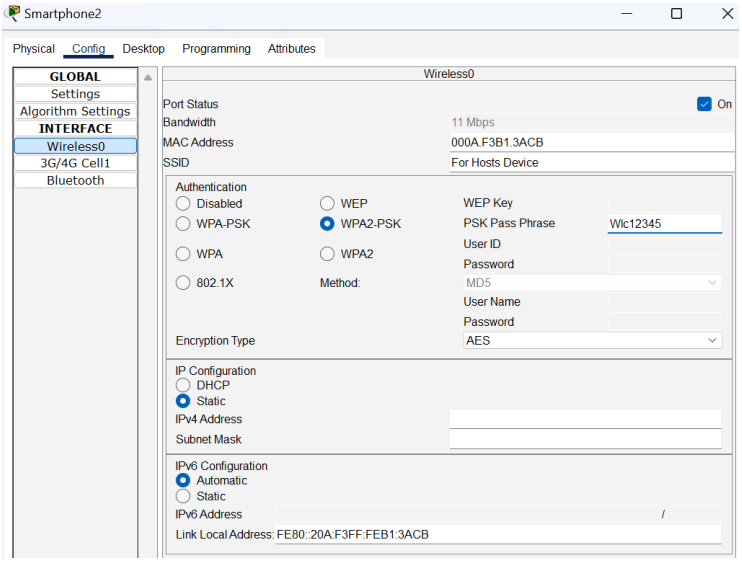
```
Firewall>en
Password:
Firewall#conf t
Firewall(config)#access-list INSIDE-TO-OUTSIDE permit icmp any any
Firewall(config)#access-list INSIDE-TO-OUTSIDE permit tcp any any 80
                                                                   ^
% Invalid input detected at '^' marker.

Firewall(config)#access-list INSIDE-TO-OUTSIDE permit tcp any any eq 80
Firewall(config)#access-list INSIDE-TO-OUTSIDE permit tcp any any eq 8080
Firewall(config)#access-list INSIDE-TO-OUTSIDE permit tcp any any eq 443
Firewall(config)#access-list INSIDE-TO-OUTSIDE permit tcp any any eq 8443
Firewall(config)#ex
Firewall#wr mem
Building configuration...
Cryptochecksum: 06351d0c 1a044452 70b57cdb 2aec55de

2676  bytes copied in 1.711 secs (1563 bytes/sec)
[OK]
Firewall#access-group INSIDE-TO-OUTSIDE in interface OUTSIDE
          ^
% Invalid input detected at '^' marker.

Firewall#conf t
Firewall(config)#access-group INSIDE-TO-OUTSIDE in interface OUTSIDE
Firewall(config)#ex
Firewall#wr mem
Building configuration...
Cryptochecksum: 06351d0c 1a044452 70b57cdb 2aec55de

2727  bytes copied in 1.549 secs (1760 bytes/sec)
[OK]
Firewall#
```

Configuring WLAN network Wireless LAN Controller

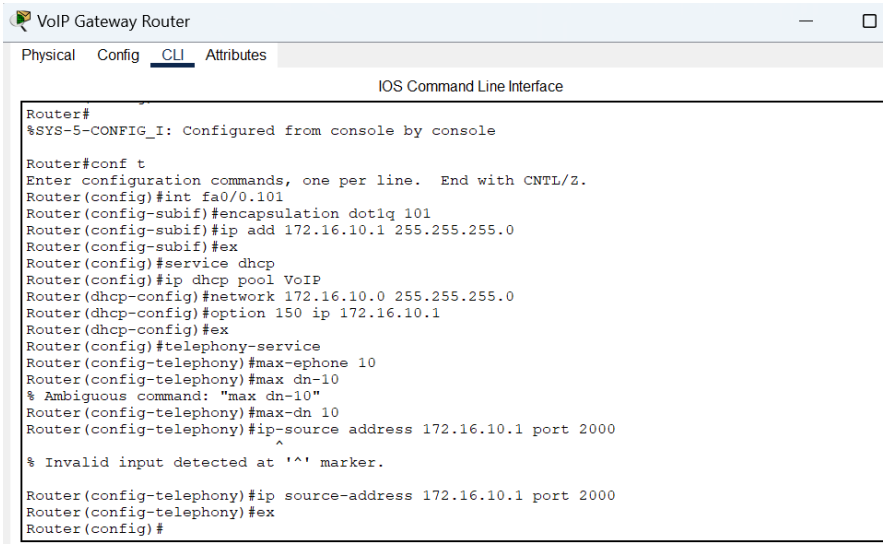




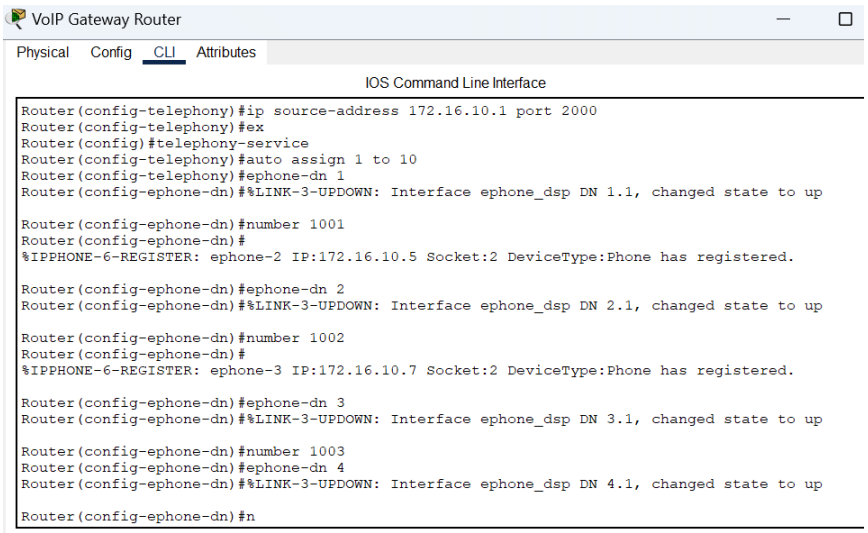


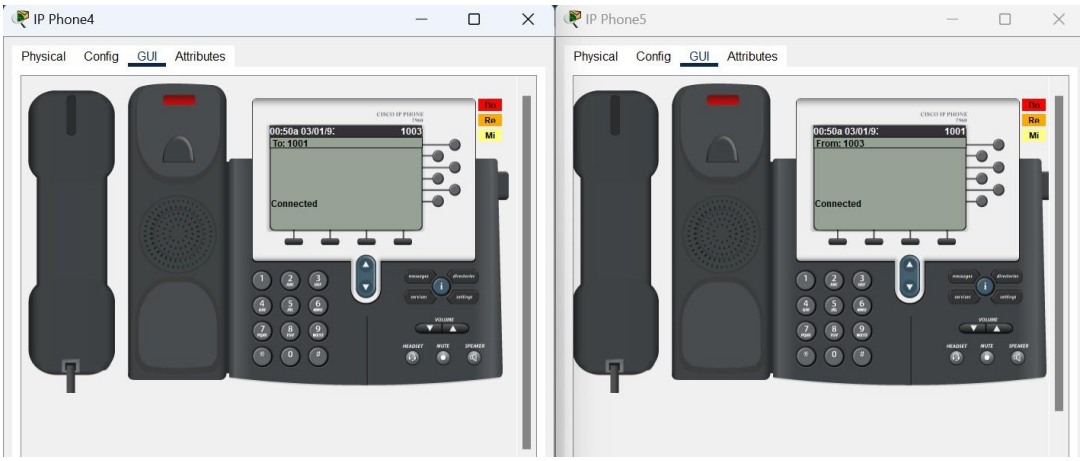


Configuring Telephony service configuration in VoIP router



Dial number is assigned from 1001-1009 to the IP phones shown below.





Snapshot showing above demonstrate that IP phones are working fine and connected when called from dial number 1003 to 1001.

Results

- ### Functionality
    - All configurations were tested and validated to ensure proper functionality. The IP phones successfully connected and communicated as expected.
    - The network devices were correctly configured with the necessary basic settings, VLANs, inter-VLAN routing, DHCP, and security measures.
- ### Performance and Redundancy
    - The hierarchical design and EtherChannel implementation provided high performance and redundancy, ensuring reliable network operations.
- ### Security
    - The network was secured through VLAN segmentation, ACLs, and the Cisco ASA Firewall, protecting against unauthorized access and potential threats.

Analysis

The project successfully achieved its objectives of designing and implementing a secure, high-performance, scalable, and redundant telecommunication network. The following points highlight the strengths and areas for potential improvement:

Strengths

- **Robust Design:** The hierarchical network design with redundancy at every layer ensures high availability and performance.
- **Effective Use of VLANs:** Segmentation of traffic into data, voice, and wireless VLANs enhances traffic management and security.
- **Comprehensive Security Measures:** The combination of ACLs, firewall configurations, and secure remote access ensures a secure network environment.
- **Efficient IP Addressing:** Proper subnetting and IP addressing schemes were implemented, allowing efficient use of IP addresses.