PROJECT REPORT

COMPUTER NETWORKS (19EAC384)

“Secure, Reliable, and Scalable Network System for Telecommunication Network”

Team Members

Student Name	Roll No
K Majidh	AM.EN.U4EAC21035
Lade Ritish Rishi	AM.EN.U4EAC21043
Kancherla Yeswanth Chowdary	AM.EN.U4EAC21039
Dessetti Dinesh	AM.EN.U4EAC21024
Kalyan Preetham Adivi	AM.EN.U4EAC21007

Abstract

This project focuses on designing and implementing a secure, reliable, and scalable network system for Cairo Telco, a fast-growing telecommunication company in Cairo, Egypt.

The project is designed to ensure high performance and security, using cisco hardware like firewalls, switches, and access points. The network in this project uses Microsoft Azure for cloud services and Windows Server 2022 for managing things like user accounts and IP addresses.

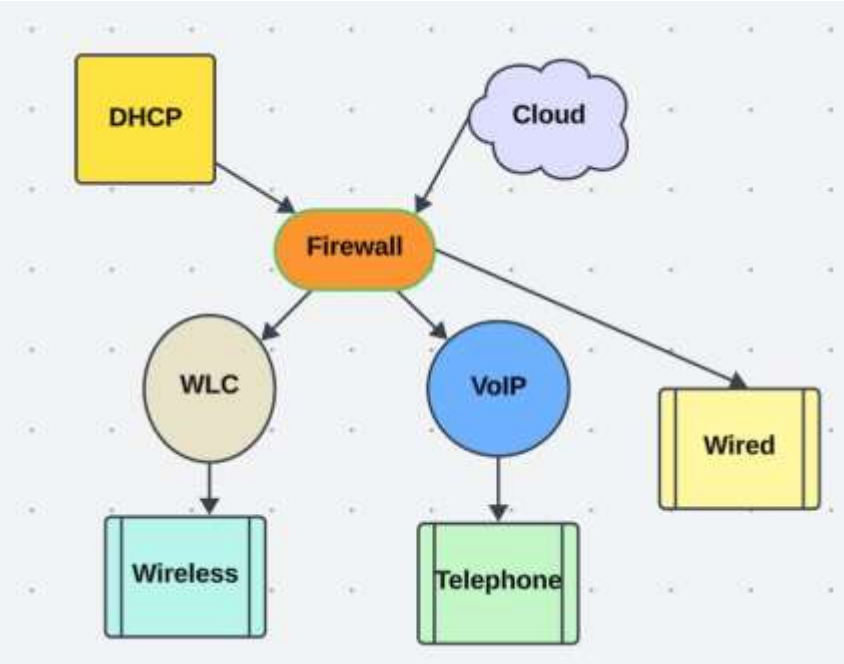
To keep things organised and secure, the network is divided into different segments for regular users, wireless users, and VoIP(Voice over internet protocol). Now here a firewall controls the traffic between these segments. Utilized OSPF, a technique that facilitates seamless communication across various network components, for routing.

Finally, evaluated the network after everything was set up to make sure everything functions as it should and Cairo Telco can run securely and effectively.

Introduction

The telecommunications industry is rapidly evolving, necessitating robust, scalable, and secure network infrastructures. Cairo Telco, a prominent telecommunications company in Egypt, aims to enhance its IT infrastructure to support its growth and service delivery. The company occupies the fourth and fifth floors of Pharaoh's Mega Plaza in Cairo, hosting various departments including HR, Finance, IT Network & Support, Software Engineering, and Cloud Engineering. To meet the company's security, performance, and scalability requirements, a comprehensive network design and implementation strategy is essential. This project focuses on designing and implementing a secure, reliable, and scalable network system for Cairo Telco, ensuring high performance, redundancy, and availability while safeguarding the confidentiality, integrity, and availability of data and communication.

Block diagram



Requirements

Design Tool: Used Cisco Packet Tracer to design and implement the network solution.

ISPs: The network is connected to a Seacom ISP Router.

Wireless Access Points (WAP): Each department had WAP providing both employee and guest WIFI managed by a Wireless LAN Controller (WLC).

VoIP: Each department has IP phones.

VLANs: The LAN, WLAN, and VoIP VLANs are 50, 60, and 101 respectively for the entire network.

EtherChannel: Used standard Link Aggregation Control Protocol (LACP) for link aggregation.

STP Port Fast and BPDUguard: Configured these protocols to enable faster port transitions from blocking to forwarding.

Subnetting: Allocated the correct number of IP addresses to each department based on provided networks.

Inter-VLAN Routing: Devices in all departments can communicate using a multilayer switch for inter-VLAN routing.

Core Switch: The multilayer switches performs both routing and switching functionalities.

DHCP Server: All devices (except IP phones) get IP addresses dynamically from the AD servers.

Static Addressing: Devices in the server room should have static IP addresses.

Routing Protocol: Used OSPF(Open Shortest Path First) to advertise routes on the routers and multilayer switches.

Final Testing: Tested communication to ensure everything is working as expected.

Implementation Steps

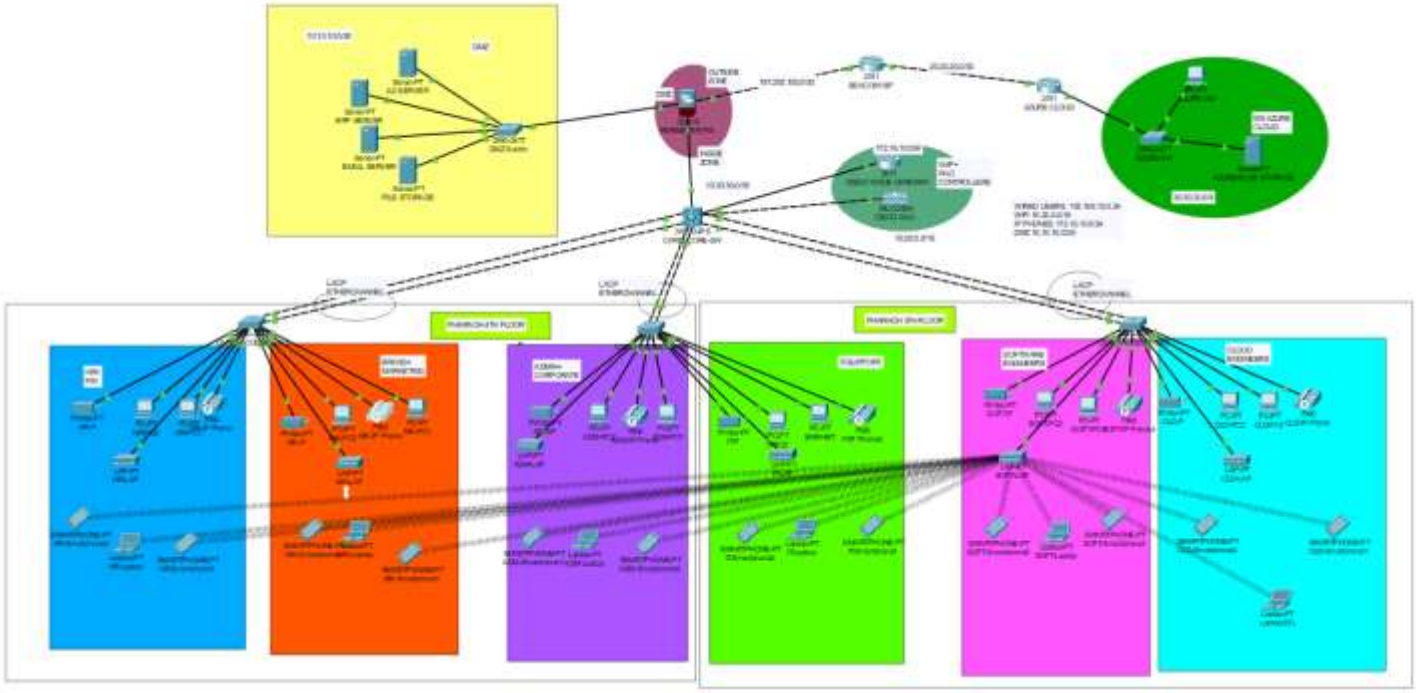
1. Network Design.
2. Basic settings to all devices.
3. VLANs (for WIRED, WIRELESS & VOICE) assignment plus all access and trunk ports on 12 and 13 switches.
4. EtherChannel, STP Portfast and BPDUguard configs.
5. Subnetting and IP addressing
6. Inter-VLAN routing on the 13 switches plus ip dhcp helper addresses.
7. Static IP address to DMZ/server devices.
8. DHCP server device configurations.
9. OSPF on the firewall, routers and switch.
10. Firewall interface security zones and levels
11. Firewall inspection policy configuration
12. Standard ACL for SSH
13. Wireless network configurations
14. Telephony service configuration
15. Verifying and testing configurations.

IP Addressing

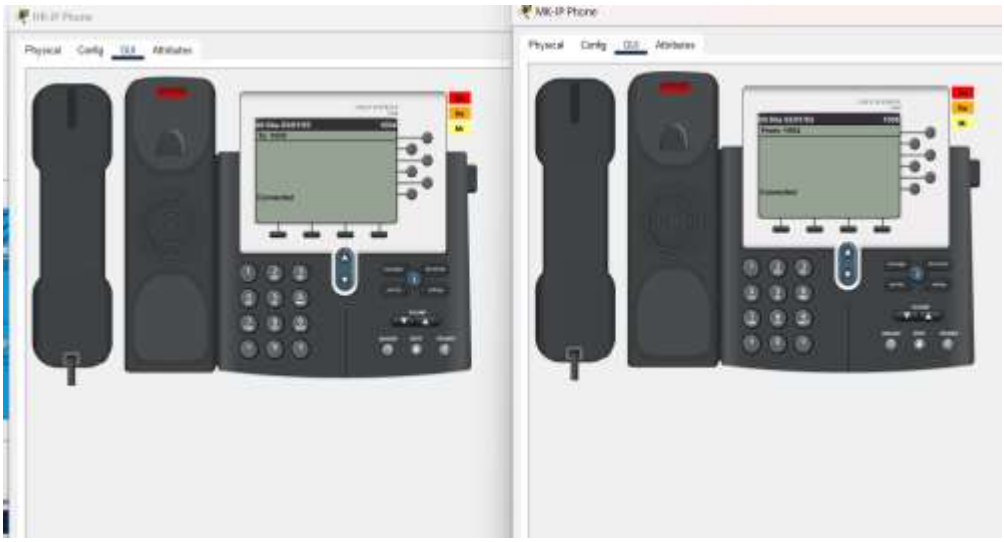
Category	Network & Subnet Mask	Valid Host Addresses	Default Gateway	Broadcast Address
WLAN	10.20.0.0/16	10.20.0.1 to 10.20.255.254	10.20.0.1	10.20.255.254
LAN	192.168.10.0/24	192.168.10.1 to 192.168.10.254	192.168.10.1	192.168.10.255
VoIP	172.16.10.0/24	172.16.10.1 to 172.16.10.254	172.16.10.1	172.16.10.255
DMZ	10.10.10.0/28	10.10.10.1 to 10.10.10.14	10.10.10.1	10.10.10.15

Simulation

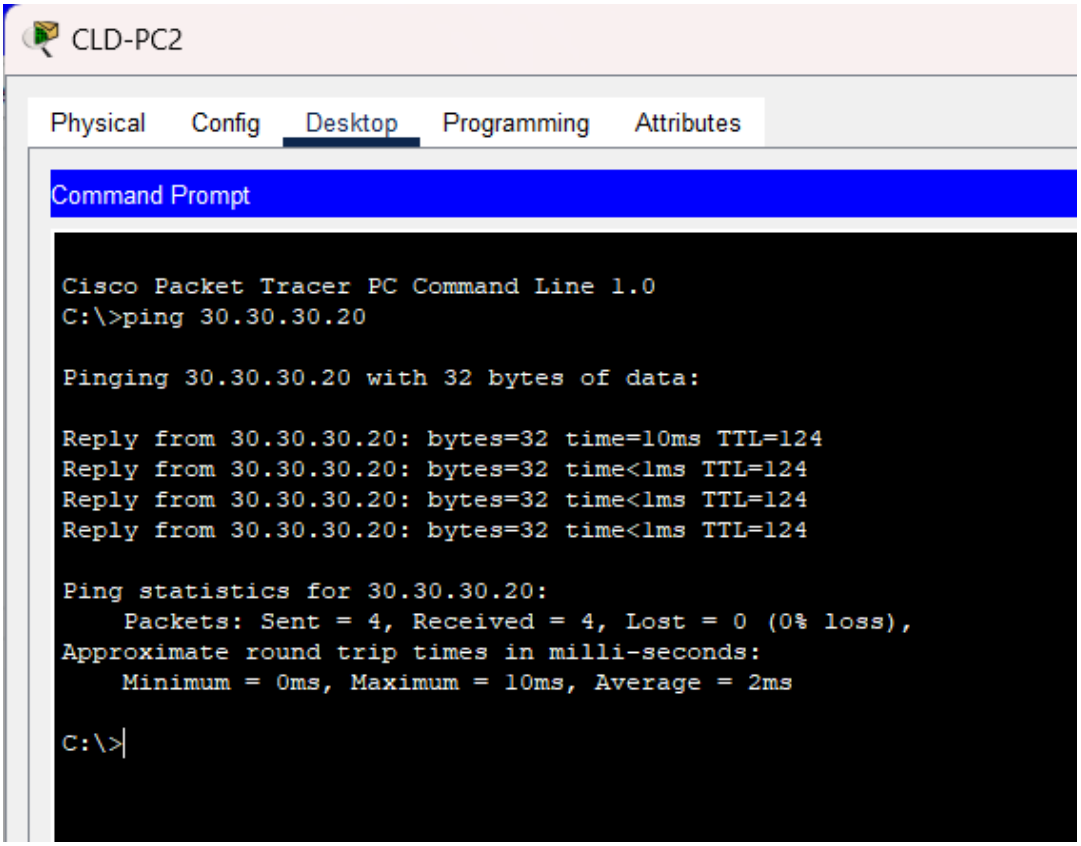
1.Circuit



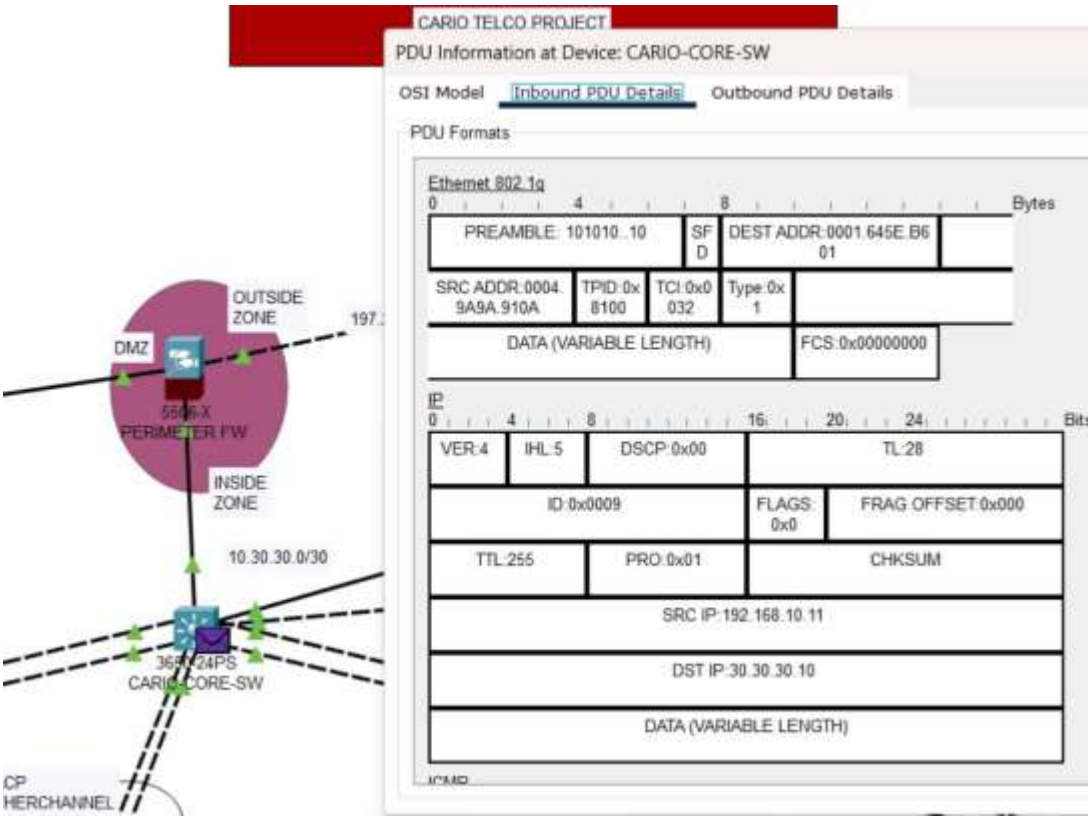
2.Telephony Service Testing

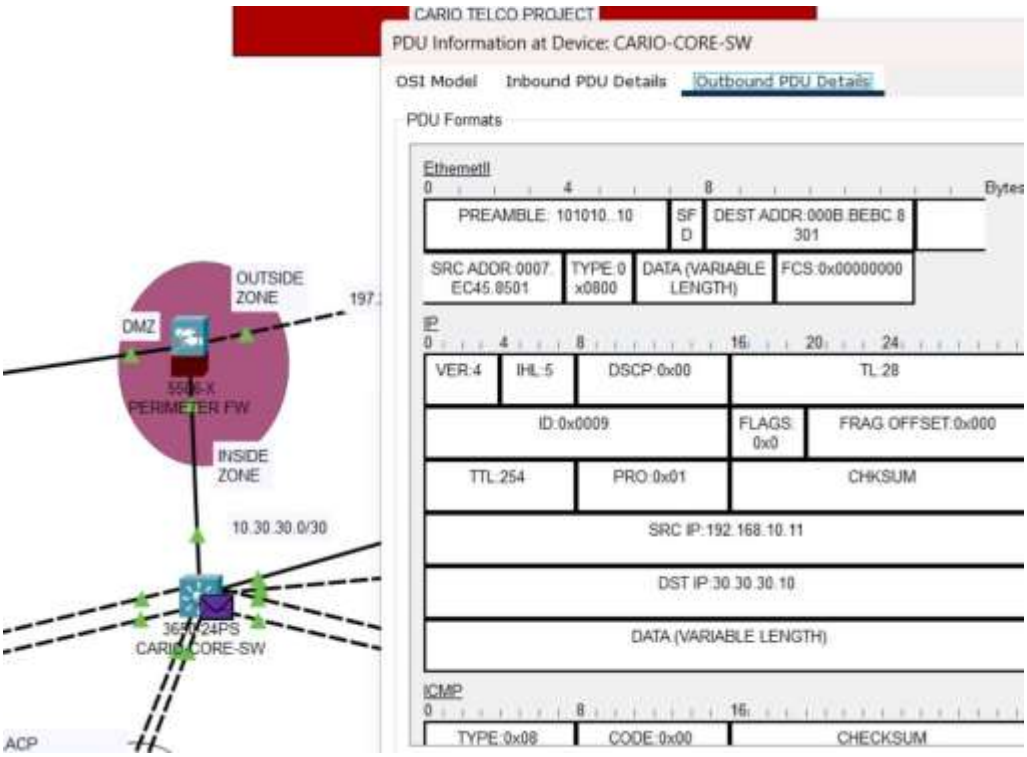


3.Testing Connections to the cloud



From Pc to Cloud Virtual Machine

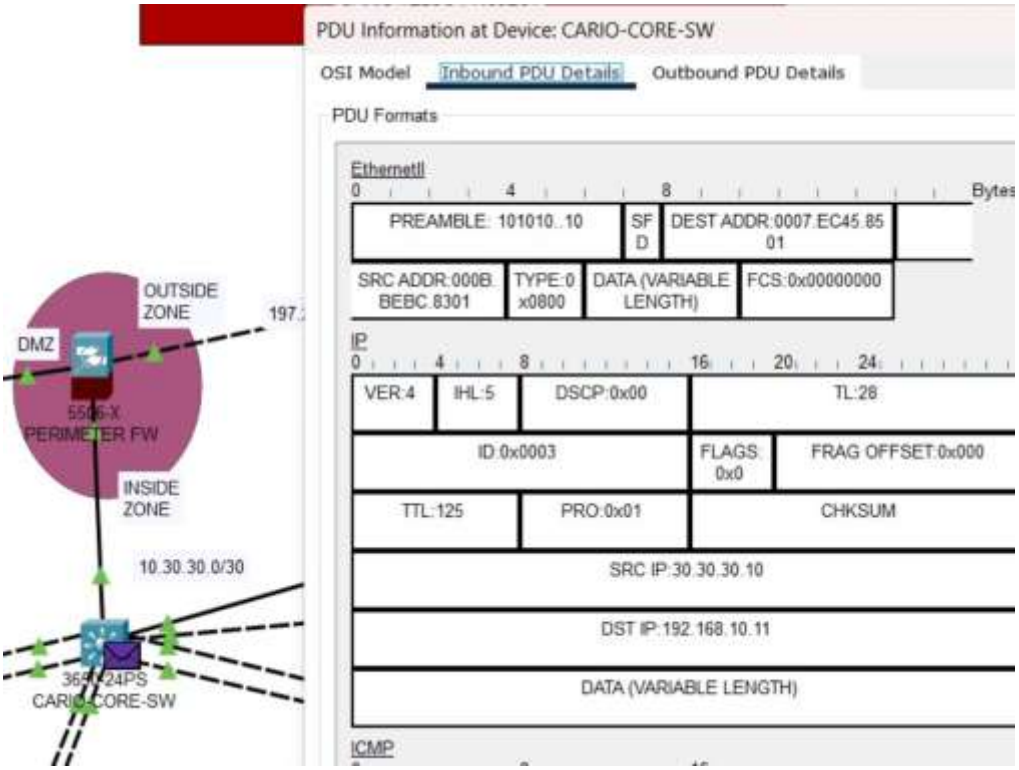


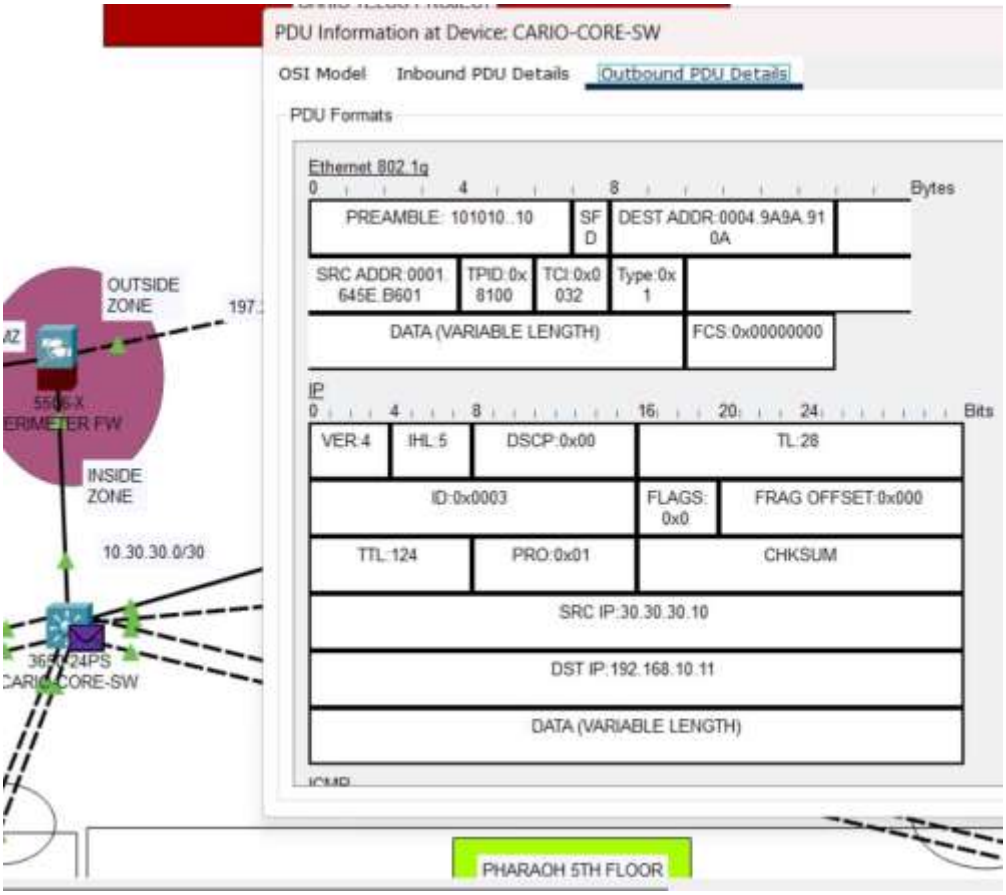


These shows the structure and details of network packets as they are transmitted through the network. The Ethernet frame encapsulates the IP packet. The details of each field within these headers are shown, explaining how devices on the network can interpret and route the data appropriately.

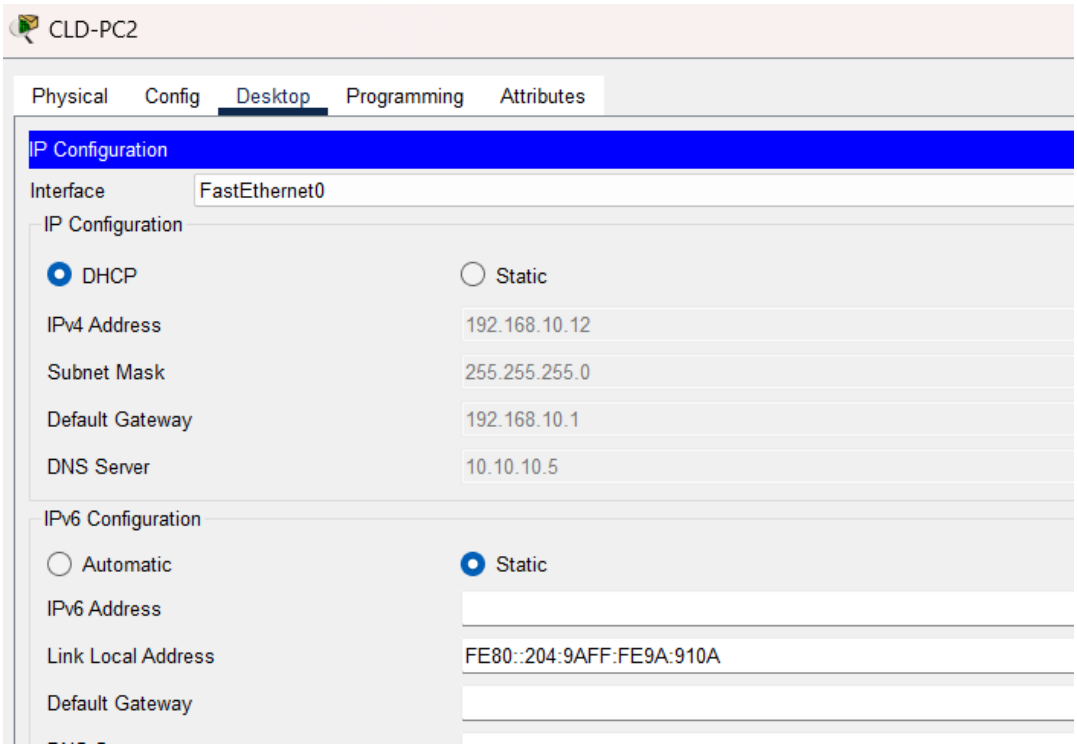
Protocol Used: ICMP(Internet Control Message Protocol), used for things like ping.

From Cloud VM to PC

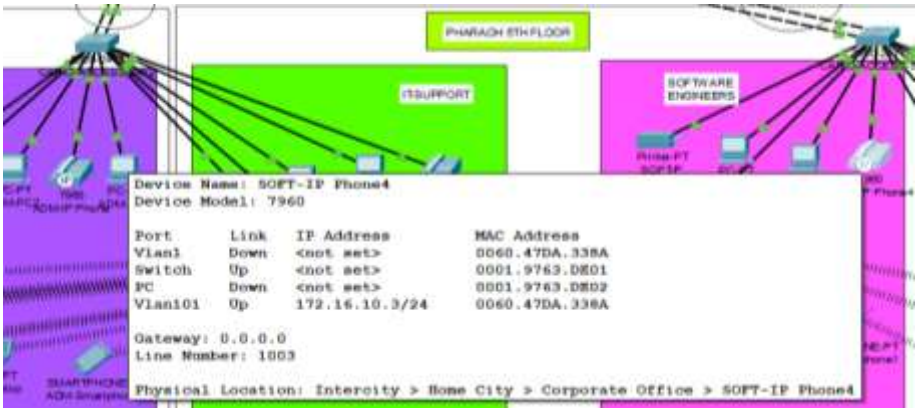




4.DHCP Check



Configuration done through CLI commands and DHCP



Results and Discussion

VLAN Configuration

- VLAN IDs: LAN (VLAN 50), WLAN (VLAN 60), and VoIP (VLAN 101). This ensures efficient traffic management and security by having different types of network traffic.

IP Addressing

- Subnetting: Subnetting was performed based on the provided IP ranges to allocate appropriate IP addresses to each department.

Inter-VLAN Routing

- Multilayer Switches: Configured for inter-VLAN routing, enabled communication across different departments while maintaining network segmentation.

DHCP Server

- Dynamic IP Allocation: Configured to dynamically allocate IP addresses to all devices, except those in the server room which were assigned static IPs.

Routing Protocol

- OSPF (Open Shortest Path First): Chosen for efficient route advertisement and management.

Security

- Cisco ASA Firewall: Configured to define security levels, zones, and policies, controlling access to network resources and protecting against external threats.
- Standard ACL for SSH: Set up to allow only the Senior Network Security Engineer to perform remote administrative tasks using SSH, enhancing security by restricting SSH access to authorized personnel.

Conclusion

The design and implementation of a secure network for Cairo Telco successfully addressed the company's requirements for performance, redundancy, scalability, and availability. The network's hierarchical design, combined with robust security measures, ensures the Confidentiality, Integrity, and Availability of the company's data and communications. Future enhancements and upgrades will further strengthen the network, supporting Cairo Telco's continued growth and technological advancement.