

# Secure Company Network System Design

Name: Jainil Patel

Project end date: September 1, 2024

**NOTE:** All connection is done for example and to look clean, of course I don't suggest keeping switching on all department, it should be in data center and physically protected from threat actors (according to CompTIA security+). All the passwords are kept making things easy, like login again and again, but in Real life never use this easy and common password, even you have to login many times. I suggest keeping at least 16 characters passwords.

## Content

- Content ..... 1**
- Introduction.....2**
  - Objective..... 2
  - Scope ..... 2
  - Tool Used ..... 2
- Network Design .....3**
  - Topology..... 3
  - Components ..... 3
  - VLANs ..... 4
  - IP address scheme..... 4
- Security Measures .....6**
  - Firewall ..... 6
  - Access Control lists (ACLs)..... 6
  - Virtual Local Area Network (VLAN) ..... 7
  - Encryption..... 8
- Implementation .....8**
- Testing and Validation .....8**

Ping Test (Between network zones).....	8
SSH test (to test ACL) .....	10
<b>Problems and troubleshooting.....</b>	<b>11</b>
<b>Conclusion .....</b>	<b>12</b>
Summary of Key point .....	12
Future Work.....	12
Final Thoughts .....	12
<b>Appendices .....</b>	<b>12</b>

## Introduction

This project is about securing a company network which provide innovative cloud services to clients worldwide (More details are in ‘Network Design Requirements’ file).

### Objective

The primary objective of this project is to design and implement a secure network for a company using Cisco Packet Tracer. The project aims to demonstrate the ability to create a robust and secure network infrastructure that can protect sensitive data and implement proper DMZ and non-DMZ zones and ensure reliable communication within the organization.

### Scope

This project covers the design, configuration, and testing of a secure network for a hypothetical company. The network includes various security measures such as firewalls, Access control lists (ACLs), Virtual Local Area Network (VLAN), encryption techniques, and De-Militaries Zone (DMZ) to protect against potential threats. This functionality will be check in testing stage to confirm security.

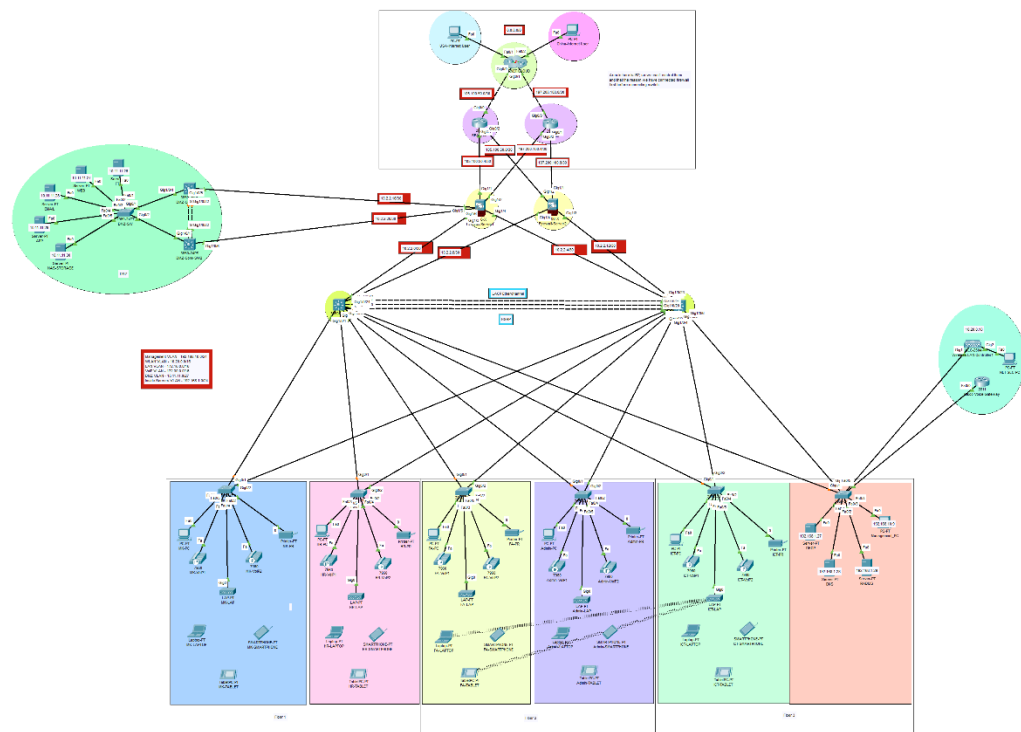
### Tool Used

For this project, it is developed only using Cisco Packet Tracer, a powerful tool for network simulation that allows for the creation and testing of complex network topologies (I have considered tools as a software which I have used not any protocols or anything else).

# Network Design

## Topology

This network topology for the company secure network is designed to ensure both efficiency and security and provide redundancy. The topology is using hierarchical method for its effectiveness and can be more scalable. And as we cannot configure ISP because of policy, I have outlined an area (on-top of topology) which we can not control, the only thing we can configure on device in that area is IP and OSPF. And for that reason, the first important thing to put is firewall to control who can come in and go out.



## Components

The following components are used in the network design:

- Routers: Cisco 2911 (Internet, SEACOM, SafariCOM) and Cisco 8211 IOS15 (VoIP Gateway).
- Firewalls: Cisco ASA 5506-X (Firewall 1 and Firewall 2).
- Switches: Cisco 3650-24PS (Core switches 1 and 2, and DMZ core switches 1 and 2) and Cisco Catalyst 2960 Series (For all access layer switches).

- Servers: Cisco Server-PT (For all Server like HTTP, DNS, and all).
- Workstations: PCs, laptops, tablets, smartphones, printers, and IP phones.
- Wireless Access Points: LAP-PT (For all wireless access devices on access layer).
- Wireless Access Controller: Cisco 2500 Series Wireless Controller (model number – 2504).

## VLANs

The VLAN ID are being already in requirement file. VLAN increase security and manageability. Since their were no Native VLAN and Internal Server VLAN but I add it for more security of Internal VLAN and to manage native VLAN more easily.

Category	VLAN ID	
Management	10	
WLAN	50	
LAN	20	
VOIP	70	
DMZ	11	
Inside Servers	90	
Native	100	
Blackhole	999	I added this VLAN to increase security and have more control over who can access the vlan using DAC,MAC, or RBAC.

## IP address scheme

The IP addressing is needs are already mentioned on requirement file for this project.

Category	Network & Subnet Mask	Valid Host Addresses	Default Gateway	Broadcast Address
Management	192.168.10.0/24	192.168.10.1 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	10.20.255.255

LAN	172.16.0.0/16	172.16.0.1 to 172.16.255.254	172.16.0.1	172.16.255.255	
VOIP	172.30.0.0/16	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	192.168.1.0/27	192.168.1.1 to 192.168.1.30	192.168.1.1	192.168.1.31	I added this VLAN to increase security and have more control over who can access the vlan using DAC,MAC, or RBAC.

And there is no specific IP address for IP address in internet (which make sense) and according to requirement file. SEACOM and SafariCOM IP address are mentioned I have designed this IP address scheme.

Connection between	Network Address
CLOUD Area	8.0.0.0/8
SEACOM - Internet	105.100.50.0/30
SafariCOM - Internet	205.200.100.0/30
SEACOM - FWL1	105.100.50.4/30
SEACOM - FWL2	105.100.50.8/30
SafariCOM-FWL1	205.200.100.4/30
SafariCOM-FWL2	205.200.100.8/30
FWL1 - MLSW1	10.2.2.0/30

FWL1 - MLSW2	10.2.2.4/30
FWL2 - MLSW1	10.2.2.8/30
FWL2 - MLSW2	10.2.2.12/30
FWL1 - DMZSW1	10.2.2.16/30
FWL1 - DMZSW2	10.2.2.20/30

## Security Measures

To ensure the security of the company's network, several measures have been implemented. These measures are designed to protect sensitive data, prevent unauthorized access, and maintain the integrity and availability of network resources. It is one of the most important parts of any company's network design.

### Firewall

Firewall are configured to control incoming and outgoing traffic as follows:

- 1) Outside area (Security level 0) traffic is NOT permitted in Inside area (Security level 100).
- 2) DMZ area (Security level 50) traffic is NOT permitted in Inside area (Security level 100).
- 3) DMZ area (Security level 50) traffic is allowed to go outside area (Security level 0).
- 4) Inside area (Security level 100) traffic is allowed to go outside area (Security level 0).
- 5) Outside area (Security level 0) traffic is NOT allowed in DMZ area (Security level 50).

### Access Control lists (ACLs)

ACLs are used to restrict access to sensitive information parts of the network. ACLs are configured on firewall and switches.

Firewalls:

Firewalls are configured with extended type ACL named RES. It allows any traffic from any IP address and send to any IP address sender requesting for. But it filters the packet by their type, only ICMP and TCP packets are allowed and for TCP only port 80

(HTTP) and 53 (DNS) are allowed. Also, UDP packets are allowed only for port 53 as DNS is UDP and TCP.

And this ACL is assigned on the port which is connected to DMZ area and Outside area. And Inside area port did not require the ACL because of security level set during the security measures on firewall.

FTP can be open to a specific IP because it is not good to allow IP to access data in FTP server.

Switches:

In switches only one access list is configured for SSH on VTY lines on switch to access the switches using remote connection which in network (not outside the network, because VPN is not setup). This ACL only allow management VLAN IPs to control the switches using SSH.

### Virtual Local Area Network (VLAN)

VLAN is best way to separate devices connected in network in same switch with out actually separating them from same switch. VLAN are implemented to segment the network into different logical groups, enhancing security and manageability.

In this topology there are 8 VLAN in total:

- 1) Management: This VLAN is assigned only on Internal Server switch to port which is connected to management PC.
- 2) WLAN: This VLAN is assigned to all the wireless access point devices on each floor.
- 3) LAN: This VLAN is assigned to all the PCs and Printer on all the floors.
- 4) VoIP: This VLAN is assigned to all the IP phone, which is two on each floor.
- 5) DMZ: This VLAN is assigned to all the server in DMZ area of the network.
- 6) Internal-Server: This VLAN is assigned to all servers which are in Inside area of the network, which is DNS, Radius, and DHCP.
- 7) Native: This VLAN is assigned to each port which are connected to either Switch-to-switch or switch-to-firewall. And switch-to-router for only one case here, in VoIP gateway router.
- 8) Blackhole VLAN: This VLAN is assigned to all the port which are not connected to any device and, they all ports are shutdown for more security.

## Encryption

For encryption default encryption method is used which is “service password-encryption”, I do not recommend using the default one always uses type 9 encryption which much more secure to crack. But this project is on securing the network not for encryption methods, for that reason this method is used to make things easy.

## Implementation

The implementation phase involves configuring the network devices and applying the security measures as planned. This section only contain plan on what to do. But configuration command is on the excel file with name ‘Plan’ in same directory or repository.

Thing which are implemented on this network topology are:

- SSH with ACL which permit only management VLAN device.
- EtherChannel on core layer switches on both areas, inside as well as DMZ.
- HSRP and Inter-VLAN routing on L3 switches and setting up DHCP helper address.
- DHCP configuration.
- OSPF on firewall and all L3 switches and routers.
- Firewall security zones, inspection policy.
- Wireless network configuration with WLC and LAP.
- VoIP configuration.

## Testing and Validation

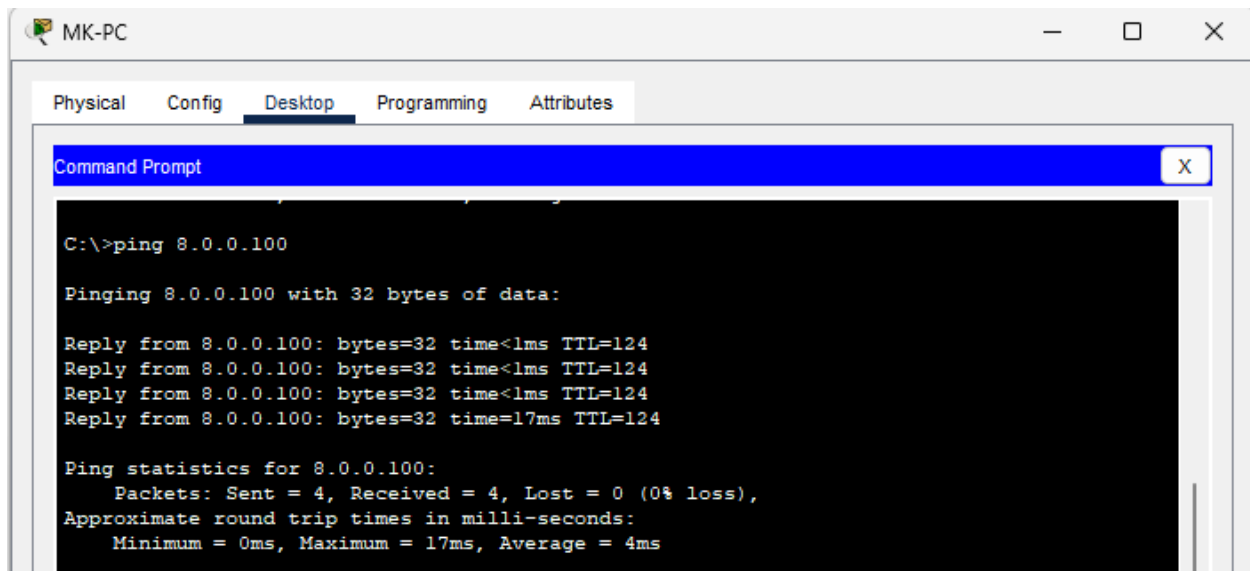
To test network configuration testing is important part of the process. Here are some tests results of the scope from this project:

### Ping Test (Between network zones)

Inside to Outside. Here is the test from the only one VLAN but according to the regular testing process all the VLAN were successful to ping the outside zone.



Ping from MK-PC to USA-Internet user:



The screenshot shows a window titled 'MK-PC' with tabs for 'Physical', 'Config', 'Desktop', 'Programming', and 'Attributes'. The 'Desktop' tab is active, displaying a 'Command Prompt' window. The command prompt shows the execution of the command 'C:\>ping 8.0.0.100'. The output indicates that four packets were sent and received with 0% loss. The round trip times are: Minimum = 0ms, Maximum = 17ms, and Average = 4ms.

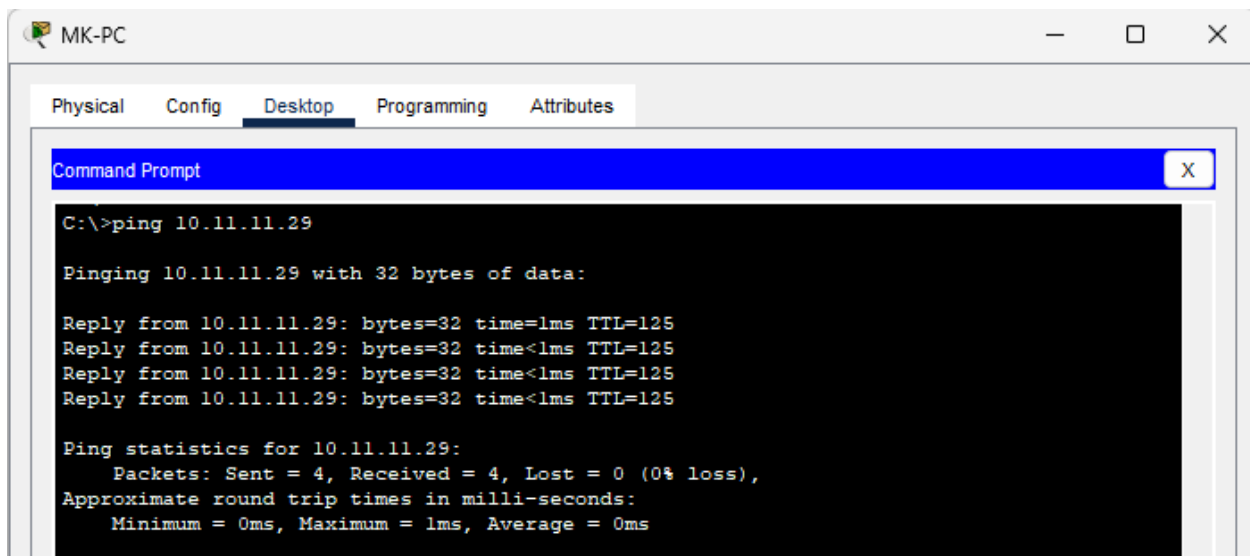
```
C:\>ping 8.0.0.100

Pinging 8.0.0.100 with 32 bytes of data:

Reply from 8.0.0.100: bytes=32 time<1ms TTL=124
Reply from 8.0.0.100: bytes=32 time<1ms TTL=124
Reply from 8.0.0.100: bytes=32 time<1ms TTL=124
Reply from 8.0.0.100: bytes=32 time=17ms TTL=124

Ping statistics for 8.0.0.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 17ms, Average = 4ms
```

Ping for MK-PC to APP server (DMZ Zone):



The screenshot shows a window titled 'MK-PC' with tabs for 'Physical', 'Config', 'Desktop', 'Programming', and 'Attributes'. The 'Desktop' tab is active, displaying a 'Command Prompt' window. The command prompt shows the execution of the command 'C:\>ping 10.11.11.29'. The output indicates that four packets were sent and received with 0% loss. The round trip times are: Minimum = 0ms, Maximum = 1ms, and Average = 0ms.

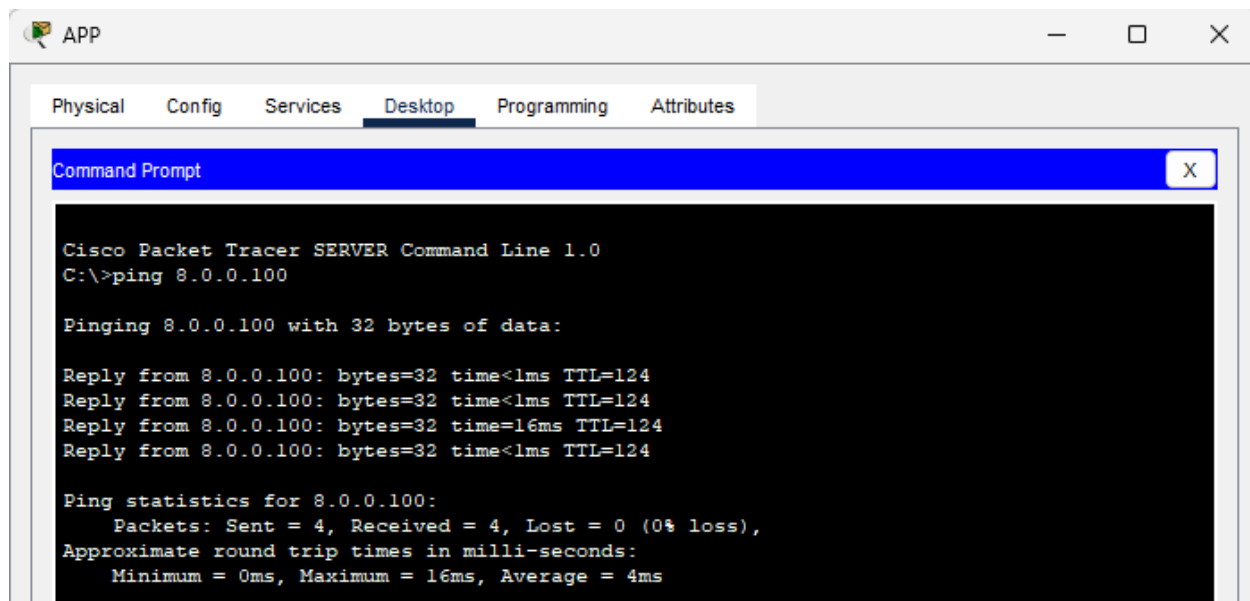
```
C:\>ping 10.11.11.29

Pinging 10.11.11.29 with 32 bytes of data:

Reply from 10.11.11.29: bytes=32 time=1ms TTL=125
Reply from 10.11.11.29: bytes=32 time<1ms TTL=125
Reply from 10.11.11.29: bytes=32 time<1ms TTL=125
Reply from 10.11.11.29: bytes=32 time<1ms TTL=125

Ping statistics for 10.11.11.29:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

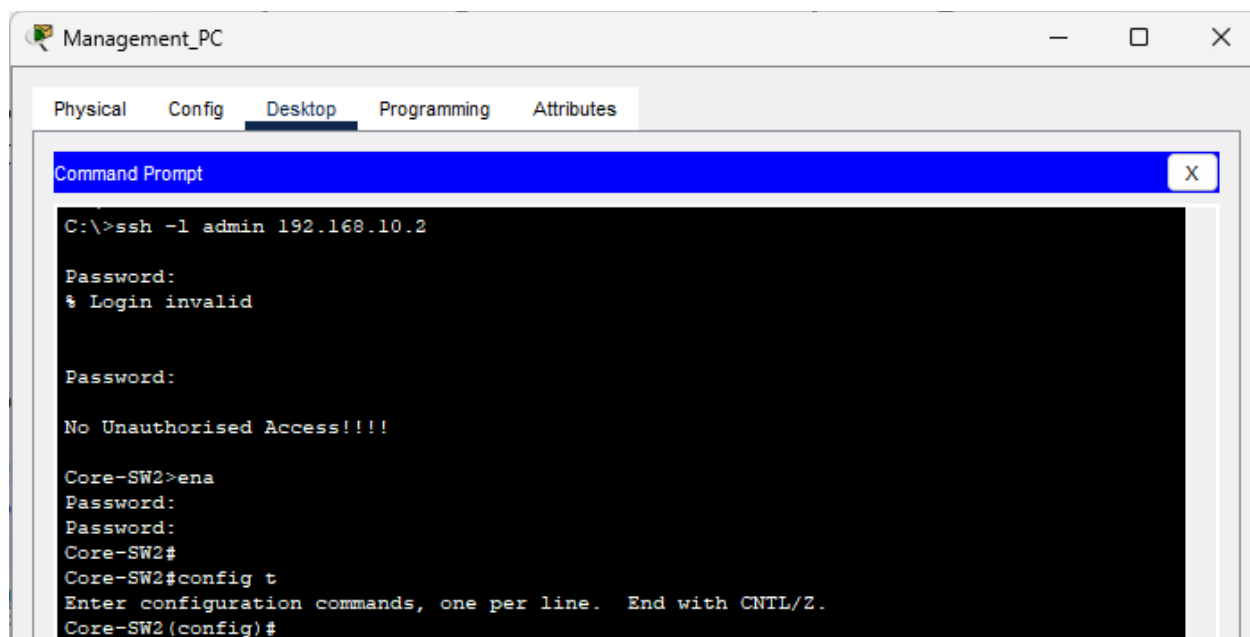
Ping from APP server to USA-Internet User:



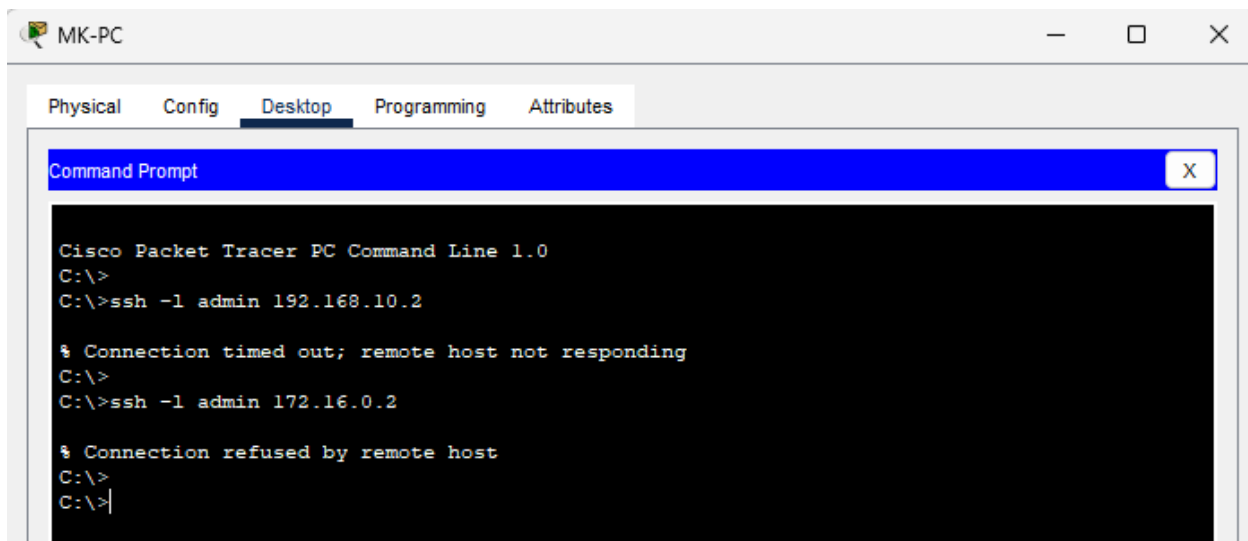
### SSH test (to test ACL)

To test SSH is important for privacy and security of the server, making sure no one is allowed to SSH in server. VLAN 10 users are only VLAN that are allowed to SSH the switches.

SSH to Core-SW2 from Management\_PC, part of VLAN 10



SSH to Core-SW2 from MK\_PC, NOT part of VLAN 10



## Problems and troubleshooting

The problem was easy to identify but I was my mistake that I have configured it wrong by mistake but there was no loss in that problems.

- 1) Not able to connect to SafariCOM and firewalls. SafariCOM router was configured with right IP addresses but it was not assigned to right port.

Solution: swapped G0/1 and G0/2 in configuration.

When Identified: It was identified during ping testing from device-to-device.

- 2) Not able to see the access point list in WLC. It was assigned with right IP address but on switch it was not assigned to WLAN VLAN.

Solution: Configure the port which is connected to WLC, and assign the VLAN to WLAN (which is VLAN 50 in this project).

When Identified: It was identified as soon as it was setup (after incisal sign-in, creating account).

# Conclusion

The Company Secure Network project successfully demonstrated the design, implementation, and validation of a robust and secure network infrastructure. By leveraging Cisco Packet Tracer, we were able to create a network that meets the company's requirements for security, efficiency, and reliability.

## Summary of Key point

- 1) Network design: A proper network is designed and developed, incorporating routers, switches, firewalls, and servers to ensure seamless communication and data protection.
- 2) Security measures are taken for safeguard the network.
- 3) Testing and Validation have taken place to ensure that network is secure.

## Future Work

While the current network design and implementation provide a solid foundation, there are opportunities for further enhancement. It could include:

- 1) Advanced Security Protocols: Implementing more advanced security protocols to further enhance network protection.
- 2) Scalability: Expanding the network to accommodate future growth and additional users.

## Final Thoughts

This project not only highlights the technical skills required to design and implement a secure network but also demonstrates the importance of thorough planning, attention to detail, and proactive security measures. The knowledge and experience gained from this project will be invaluable in future networking endeavors.

# Appendices

Company requirement file is in this folder or GitHub repository named "Network Design Requirement", and it is in word format.

Network Design and implementation are in the packet tracer file named “Network Design”, located in this folder or GitHub repository.

Script or command file in on of the sheets in excel file named “Plan”, located in this folder or GitHub repository.