A logo of a globe with yellow rings around it

Description automatically generated

**GROUP ASSIGNMENT**

**CT133-3-2-SRE  
APD2F2406CS(CYB),**

**SWITCHING AND ROUTING ESSENTIALS**

**LECTURER NAME: JOSHUA SAMUAL**

**HAND OUT DATE: August 2024**

**HAND IN DATE: 11th October 2024**

**WEIGHTAGE: 50%**

|  |  |
| --- | --- |
| STUDENT NAME: | TP NUMBER: |
| Abdulrazaq Muhammad Mukhtar | TP073072 |
| Mohamed Habiib Abshir | TP074880 |
| Abdullah Saleh Ahmed Qanaan | TP075316 |
| Adriel Benyamin Hartadji Djie | TP073936 |
| Jason Maalik | TP067865 |
| JM Nazmus Saquib | TP074864 |
| Khaled Abdullah Rabea | TP075479 |

Table of Contents

[1.0 Introduction: 4](#_Toc179745367)

[2.0 Network Diagram Overview: 5](#_Toc179745368)

[2.1 KL Network Diagram: 5](#_Toc179745369)

[2.2 Server Farm: 6](#_Toc179745370)

[2.3 Krung Thep Network: 7](#_Toc179745371)

[3.0 IPv4 Addressing Table: 8](#_Toc179745372)

[3.1 Private IP KL Network: 8](#_Toc179745373)

[3.2 PRIVATE IP FOR KRUNG THEP NETWORK 8](#_Toc179745374)

[3.3 PRIVATE IP FOR KL SERVER FARM 8](#_Toc179745375)

[3.4 WAN Public IP address 9](#_Toc179745376)

[4.0 LAN and WAN Configuration: 10](#_Toc179745377)

[4.1 KL Network: 10](#_Toc179745378)

[4.1.1 VLAN and Trunking KL Switch: 10](#_Toc179745379)

[4.1.2 VLAN and Trunking Design Switch: 12](#_Toc179745380)

[4.1.3 VLAN and Trunking Delivery Switch: 13](#_Toc179745381)

[4.1.4 VLAN and Trunking HR Switch: 13](#_Toc179745382)

[4.2 Inter-VLAN Routing KL: 14](#_Toc179745383)

[4.3 OSPF KL: 16](#_Toc179745384)

[4.4 Spanning Tree Protocol KL: 17](#_Toc179745385)

[4.5 Krung Thep Networks: 24](#_Toc179745386)

[4.6 VLAN and Trunking Krung Switch: 24](#_Toc179745387)

[4.6.1 Inter-VLAN Routing Krung 25](#_Toc179745388)

[4.7 DHCP Krung: 26](#_Toc179745389)

[4.8 OSPF Krung: 27](#_Toc179745390)

[5.0 Proposed WLAN Architecture: 27](#_Toc179745391)

[5.1 PRE-SETUP THE WLC 28](#_Toc179745392)

[5.2 CREATE VIRTUAL INTERFACE IN THE WLC 32](#_Toc179745393)

[5.3 CREATE WLAN 33](#_Toc179745394)

[5.4 AP Group Configuration 34](#_Toc179745395)

[6.0 EtherChannel Implementation: 35](#_Toc179745396)

[6.1 Configuration 35](#_Toc179745397)

[6.2 Justification 36](#_Toc179745398)

[KL\_Switch 37](#_Toc179745399)

[HR\_SW 39](#_Toc179745400)

[Design\_SW 43](#_Toc179745401)

[Delivery\_SW 47](#_Toc179745402)

[7.0 HSRP Implementation: 49](#_Toc179745403)

[8.0 Server Farm Services Configuration: 51](#_Toc179745404)

[8.1 DNS Service 51](#_Toc179745405)

[8.2 Web Server 55](#_Toc179745406)

[8.3 FTP Server 58](#_Toc179745407)

[8.4 Testing 60](#_Toc179745408)

[9.0 Tracer/Ping Commands: 60](#_Toc179745409)

[9.1 Tracert HRSP: 60](#_Toc179745410)

[9.2 Ping Commands: 61](#_Toc179745411)

[9.2.1 KL Network: 61](#_Toc179745412)

[9.2.2 Krung Thep Network 63](#_Toc179745413)

[9.3 Inter-Connected Router: 64](#_Toc179745414)

[9.4 KL Server Farm Ping commands 66](#_Toc179745415)

[10.0 Layer 2 Security: 67](#_Toc179745416)

[10.1 Types of Attacks on Layer 2: 67](#_Toc179745417)

[10.1.1 MAC Address Table attack 67](#_Toc179745418)

[10.1.2 VLAN Hopping Attack 67](#_Toc179745419)

[10.1.3 DHCP Starvation Attack 67](#_Toc179745420)

[10.1.4 ARP Spoofing and ARP Poisoning 68](#_Toc179745421)

[10.2 Layer 2 Security Deployment 68](#_Toc179745422)

[10.2.1 Mitigation Technique of MAC Address Flooding Attack 68](#_Toc179745423)

[Port security for Krung Thep switch branch: 68](#_Toc179745424)

[10.2.2 Mitigation Technique of VLAN Hopping Attack 70](#_Toc179745425)

[10.2.3 Mitigation Technique for STP Attacks: 70](#_Toc179745426)

[10.2.4 Mitigation Technique for DHCP Snooping: 71](#_Toc179745427)

[11.0 Recommendations: 72](#_Toc179745428)

[11.1 Access Control List (ACL): 72](#_Toc179745429)

[11.2 Virtual Private Network (VPN): 73](#_Toc179745430)

[11.3 Honeypot 74](#_Toc179745431)

[12.0 Conclusion: 75](#_Toc179745432)

[13.0 References: 75](#_Toc179745433)

# Introduction:

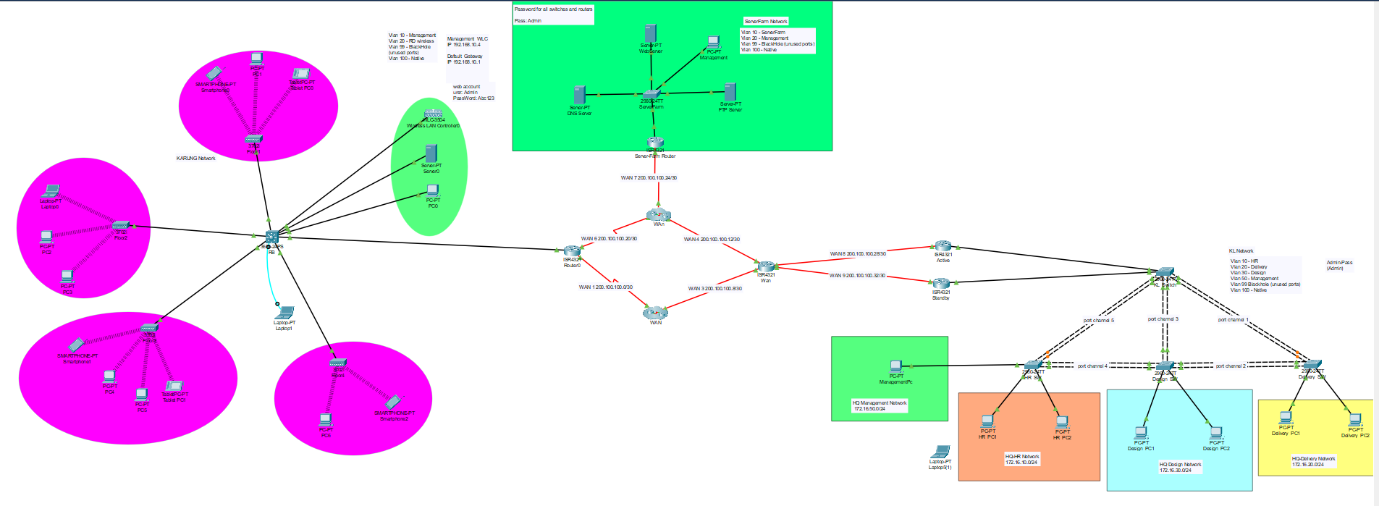


This project focuses on upgrading the network for Microtech Sdn. Bhd., A company seeking to enhance its IT infrastructure at two key locations: its headquarters in Kuala Lumpur (KL) and a remote branch in Krung Thep Vietnam. The objective of the upgrade is to implement a more efficient and secure network by redesigning VLANs at the KL headquarters and deploying Wireless LAN Controller (WLC) technology in Krung Thep. This upgrade aims to improve network management, security, and wireless access.

Microtech’s network is structured across several departments located at both sites, with specific departments including Management, Human Resources, Design, and Delivery based in KL, while Research and Development (R&D) and WLC Management are based in Krung Thep. Additionally, the server farm is housed in KL’s server facility.

As part of this project, the appointed network executive is tasked with designing the logical topology of the network based on the requirements and implementing it in Cisco Packet Tracer. This will involve configuring VLANs, wireless access, and various routing and switching protocols to ensure the network operates efficiently and securely across both locations. The design prototype is crucial for evaluating the effectiveness of the proposed network changes.

# 2.0 Network Diagram Overview:



2.1 KL Network Diagram:  
  
A computer network diagram with many different colored squares

Description automatically generated with medium confidence

2.2 Server Farm:  
  
A computer network diagram with text

Description automatically generated

## 2.3 Krung Thep Network:

A diagram of a computer network

Description automatically generated

# 3.0 IPv4 Addressing Table:

## 3.1 Private IP KL Network:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| KL Network | VLAN | Network ID | Range Of Available IP addresses | | Broadcast IP | Prefix |
|  |  |  | First IP address | Last IP address |  |  |
| HR | VLAN 10 | 172.16.10.0 | 172.16.10.1 | 172.16.10.254 | 172.16.10.255 | /24 |
| Design | VLAN 20 | 172.16.20.0 | 172.16.20.1 | 172.16.20.254 | 172.16.20.255 | /24 |
| Delivery | VLAN 30 | 172.16.30.0 | 172.16.30.1 | 172.16.30.254 | 172.16.30.255 | /24 |
| Management | VLAN 50 | 172.16.50.0 | 172.16.50.1 | 172.16.50.254 | 172.16.50.255 | /24 |

## 3.2 PRIVATE IP FOR KRUNG THEP NETWORK

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| KL Network | VLAN | Network ID | Range Of Available IP addresses | | Broadcast IP | Prefix |
|  |  |  | First IP address | Last IP address |  |  |
| RBMgmt | VLAN 100 | 192.168.100.0 | 192.168.100.1 | 192.168.100.254 | 192.168.100.255 | /24 |
| R&D-Wireless | VLAN 10 | 192.168.10.0 | 192.168.10.1 | 192.168.10.254 | 192.168.10.255 | /24 |
| BlackHole (Unused Ports) | VLAN 99 | (Unused Ports) | (Unused Ports) | (Unused Ports) | (Unused Ports) |  |

## 3.3 PRIVATE IP FOR KL SERVER FARM

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| KL Server Farm Network | VLAN | Network ID | Range Of Available IP addresses | Broadcast IP | Prefix |
|  |  |  | Range Of IP’s |  |  |
| Server Farm | VLAN 10 | 192.168.10.0 | 192.168.10.1 - 192.168.10.254 | 192.168.10.255 | /24 |
| Management | VLAN 20 | 192.168.100.0 | 192.168.100.1 - 192.168.100.254 | 192.168.100.255 | /24 |
| Black Hole | VLAN 99 | N/A | N/A | |  | | --- | |  |   N/A | /24 |
| Native | VLAN 100 | N/A | N/A | N/A | /24 |

## 3.4 WAN Public IP address

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Network** | **Network ID** | **Usable Range** | **Broadcast ID** | **Hosts** | **Prefix Length** | **Subnet Masks** |
| WAN 1 | 200.10.1.0 | 1–2 | 200.10.1.3 | 2 | /30 | 255.255.255.252 |
| WAN 2 | 200.10.1.4 | 5-6 | 200.10.1.7 | 2 | /30 | 255.255.255.252 |
| WAN 3 | 200.10.1.8 | 9-10 | 200.10.1.11 | 2 | /30 | 255.255.255.252 |
| WAN 4 | 200.10.1.12 | 13-14 | 200.10.1.15 | 2 | /30 | 255.255.255.252 |
| WAN 5 | 200.10.1.16 | 17-18 | 200.10.1.19 | 2 | /30 | 255.255.255.252 |
| WAN 6 | 200.10.1.20 | 21-22 | 200.10.1.23 | 2 | /30 | 255.255.255.252 |
| WAN 7 | 200.10.1.24 | 25-26 | 200.10.1.27 | 2 | /30 | 255.255.255.252 |
| WAN 8 | 200.10.1.28 | 29-30 | 200.10.1.31 | 2 | /30 | 255.255.255.252 |
| WAN 9 | 200.10.1.32 | 33-34 | 200.10.1.35 | 2 | /30 | 255.255.255.252 |

# 4.0 LAN and WAN Configuration:

## 4.1 KL Network:

The KL network uses the private network address 172.16.10.0, which is shared by all devices within the network. These devices are physically connected to the same network infrastructure. VLANs have been assigned in the KL network as follows: each department has a unique VLAN ID, with VLAN 10 assigned to the HR department, VLAN 20 to the delivery department, VLAN 30 to the design department, and VLAN 50 to the management department.

### 4.1.1 VLAN and Trunking KL Switch:

In the HQ Network, there are 6 VLANs which have been configured. These are VLAN 10-HR for HR departments, VLAN 20-Design for design departments, VLAN 30-Delivery department, VLAN 40-Management department, VLAN 99-Native for Native VLAN, and VLAN 100-Black Hole for unused ports. The command that have been used to verify VLAN and trunking configuration is “show vlan brief” to show the VLAN that has been configured, and “show interfaces trunk” to show the port that enable trunking and VLAN that allowed on trunk.

**A screenshot of a computer

Description automatically generated**A screenshot of a computer

Description automatically generated

### 4.1.2 VLAN and Trunking Design Switch:

A screenshot of a computer

Description automatically generated

A white sheet with black text

Description automatically generated

### 4.1.3 VLAN and Trunking Delivery Switch:

A screenshot of a computer screen

Description automatically generated

A white text with black text

Description automatically generated

### 4.1.4 VLAN and Trunking HR Switch:

A screenshot of a computer screen

Description automatically generated

A screenshot of a computer program

Description automatically generated

## 4.2 Inter-VLAN Routing KL:

In each network, the commands “show ip route” and “show ip interface brief” can be used on the router to verify the configuration of inter-VLAN routing. The “show ip route” command displays the router’s connection to the VLAN networks, while “show ip interface brief” confirms that subinterfaces have been configured on the router to connect with the VLAN networks.

**KL Active Router:**

A screenshot of a computer program

Description automatically generated

A screenshot of a computer program

Description automatically generated

**KL Standby Router:**

A screenshot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

## 4.3 OSPF KL:

KL Standby Router:

A screen shot of a computer

Description automatically generated

KL Active Router:

A computer screen shot of numbers

Description automatically generated

## 4.4 Spanning Tree Protocol KL:

Spanning Tree Protocol (STP) is a Layer 2 protocol that is used to prevent network loops in Ethernet networks with redundant paths. It ensures that there is only one active path between any two devices, preventing issues like broadcast storms, duplicate frames, and MAC address table instability, which can occur in networks with multiple connections between switches.

STP works by selecting a root bridge and calculating the shortest path to this bridge for all other switches. It blocks any redundant paths that could cause loops, ensuring that only the optimal paths remain active. If the main path fails, STP reactivates the blocked paths to maintain network connectivity.

The importance of STP lies in its ability to maintain a loop-free network while still providing redundancy. Without STP, networks with multiple connections between switches would experience significant disruptions due to looping traffic, making the protocol essential for stable and reliable network performance.

KL\_SW:

A screen shot of a computer

Description automatically generated

VLAN 20:

A computer screen shot of a computer program

Description automatically generated

VLAN 30:

A white screen with black text

Description automatically generated

VLAN 50:

A white screen with black text

Description automatically generated

HR\_SW:

VLAN 10:

A screenshot of a computer program

Description automatically generated

VLAN 20:

A computer screen shot of a computer program

Description automatically generated

VLAN 30:

A computer screen shot of a computer

Description automatically generated

VLAN 50:

A computer screen shot of a computer

Description automatically generated

Design\_SW:

VLAN 10:

A computer screen shot of a computer program

Description automatically generated

VLAN 20:

A white screen with black text

Description automatically generated

VLAN 30:

A screenshot of a computer program

Description automatically generated

VLAN 50:

A screenshot of a computer program

Description automatically generated

Delivery\_SW:

VLAN 10:

A computer code with numbers and letters

Description automatically generated with medium confidence

VLAN 20:

A white paper with black text

Description automatically generated

VLAN 30:

A computer screen shot of a computer

Description automatically generated

VLAN 50:

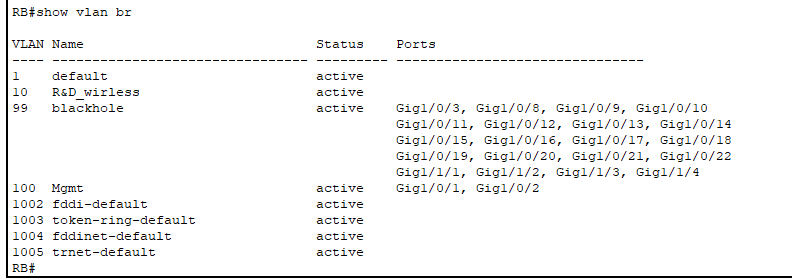
A computer screen shot of a computer code

Description automatically generated

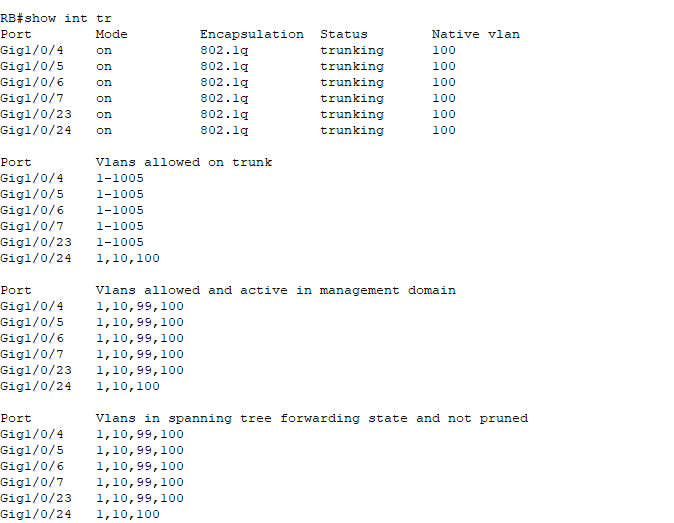
## 4.5 Krung Thep Networks:

A 192. 168. 100. 0 private IP address is part of the KT network. The KT network devices use Wireless LAN (WLAN) controllers to connect to this network. This indicates that the KT devices serve a wireless network sharing. The KT network is connected logically and has been divided up into 3 Virtual Local Area Networks (VLAN). Setting up VLANs The R&D-Ireless department is assigned under VLAN ID 10, and RB management is assigned under VLAN ID 100 throughout the VLAN configuration. The Unused Ports will be assigned to VLAN 99, also known as BlackHole.

## 4.6 VLAN and Trunking Krung Switch:

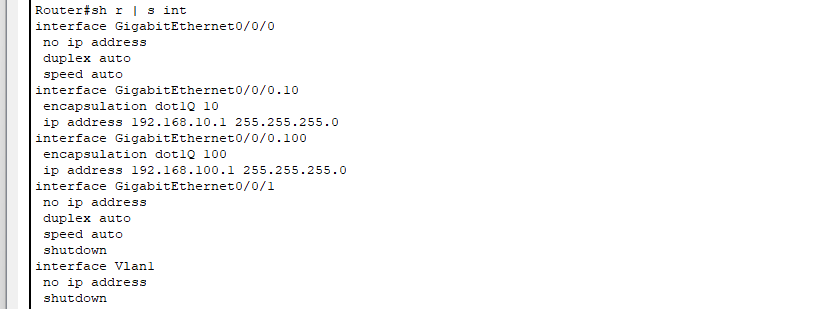


According to the setup, VLAN 10 has several Gigabit Ethernet ports allocated to it and is used only for R&D wireless devices. The fact that VLAN 100 is designated for management indicates how important network administration is to this field. Improved network security and traffic control are made possible by this organized method.



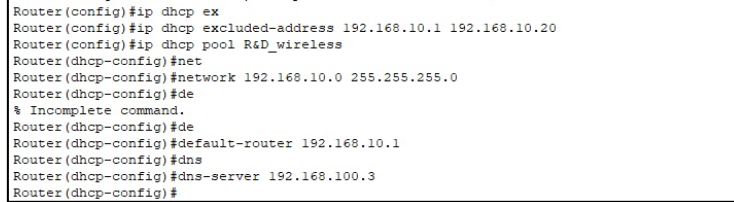
This output gives a thorough overview of the network device's trunk interfaces, displaying how they are configured for VLAN administration and use. With VLAN 100 being the original VLAN, each trunk port actively supports numerous VLANs, allowing for efficient network traffic management.

### 4.6.1 Inter-VLAN Routing Krung



This output shows the router's setup for multiple interfaces, with two subinterfaces that help with VLAN 10 and 100 routing and have assigned IP addresses highlighted. There are also other interfaces, some of which are shut down and do not have IP addresses, therefore they are not in use at this moment.

## 4.7 DHCP Krung:



The figure above illustrates DHCP configuration on a Cisco ISR4321 router setting up dynamic IP assignment for the end-devices in the 192.168.10.0/24 network. The IP addresses from 192.168.10.1 to 192.168.10.20 are excluded, reserved for static IP devices. The pool name for DHCP is R&D\_wireless is created to assign IP addresses dynamically. The default gateway for the DHCP is 192.168.10.1, and the DNS server is configured as 192.168.100.3. This make sure end devices automatically receive the necessary IP configuration to connect to the network.

A white background with black text

Description automatically generated

The (“do sh r | s dhcp”) command to see if the DHCP is running and configured correctly. Now the DHCP is set up and ready to use.

## 4.8 OSPF Krung:

Krung Thep Switch:

A white background with black text

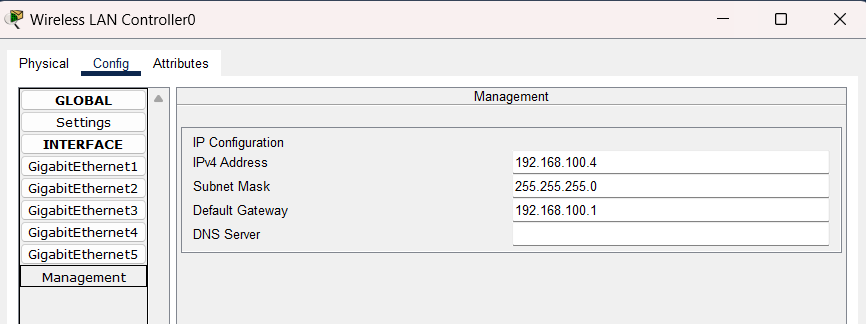
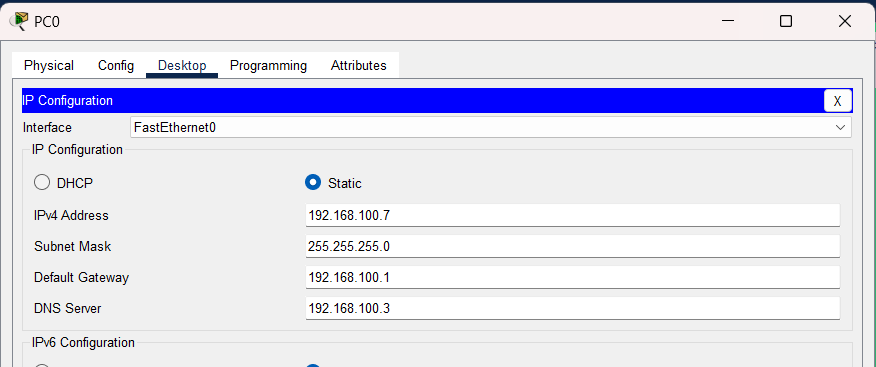
Description automatically generated

A computer screen with numbers and letters

Description automatically generated

The command (“sh ip ospf int br”) shows the interfaces participating in OSPF (GigabitEthernet and Serial interfaces)

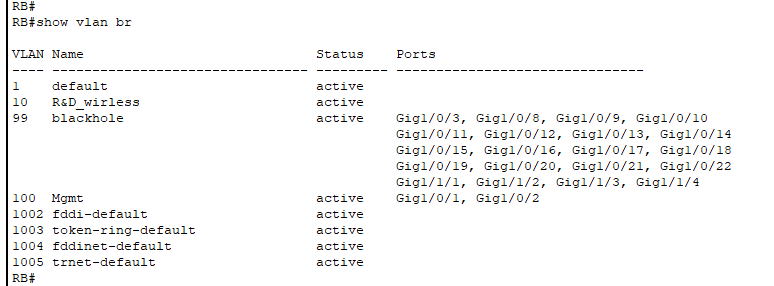
# 5.0 Proposed WLAN Architecture:



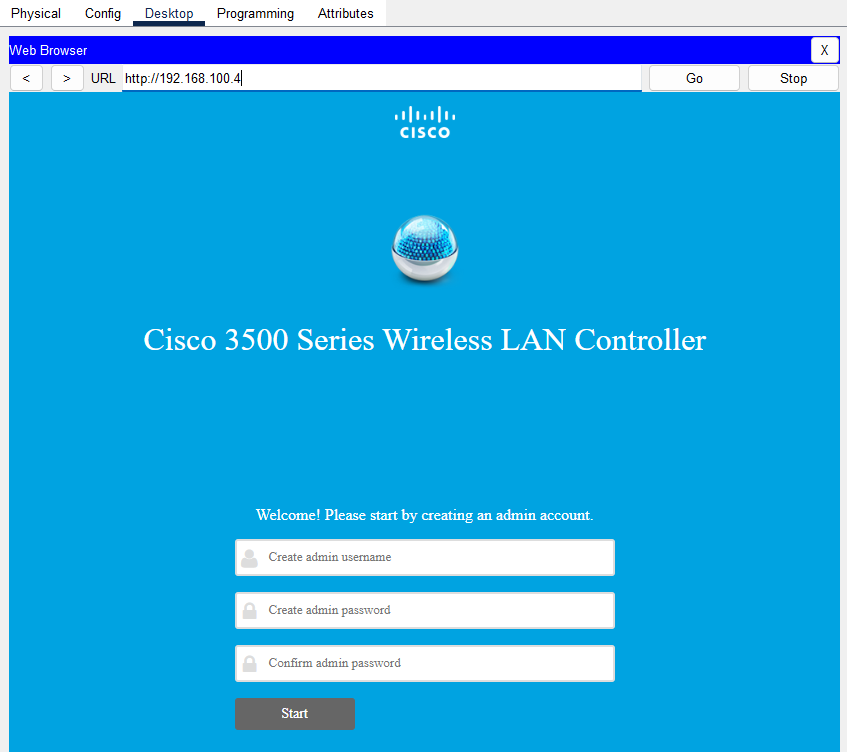
A network device called a Wireless LAN Controller (WLC) controls the wireless access points inside a network, facilitating wireless device connections. All wireless network components may be centrally controlled thanks to the WLC, which enhances overall network administration. It provides a comprehensive picture of all connected devices and their activity, making network monitoring easy. All wireless access points' setups, security settings, and troubleshooting may be handled effectively with the aid of this unified administration system. The WLC makes sure that the wireless network runs smoothly and securely by optimizing these operations, giving all wireless devices a dependable connection.

## 5.1 PRE-SETUP THE WLC

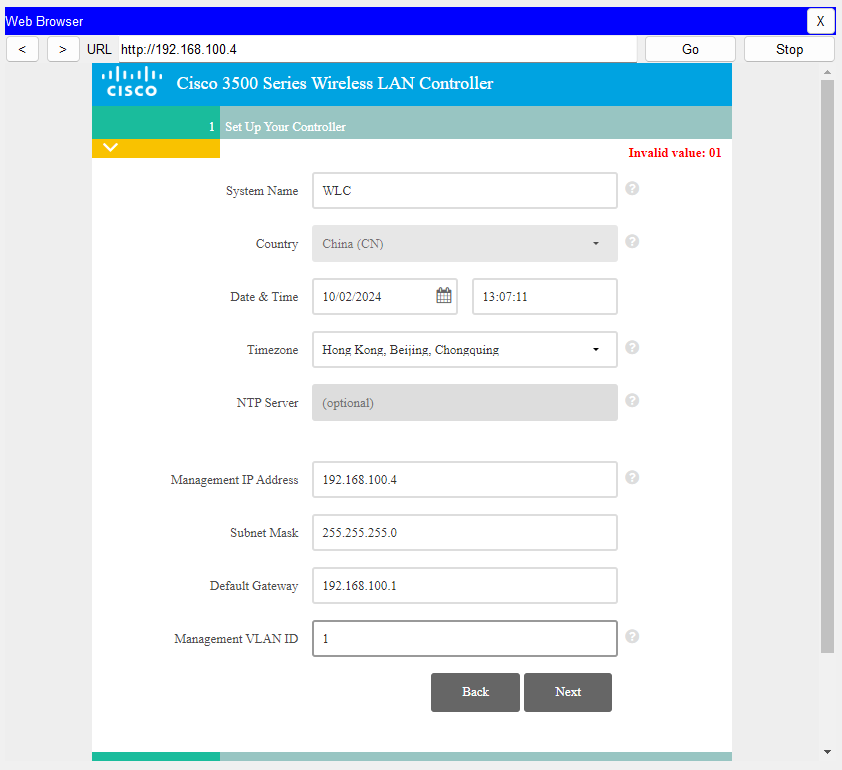
We must do a few preliminary actions before configuring the Wireless LAN Controller (WLC). In these stages, VLANs are configured and IP addresses are assigned to each VLAN. We first set up the VLANs and give each one a unique IP address.



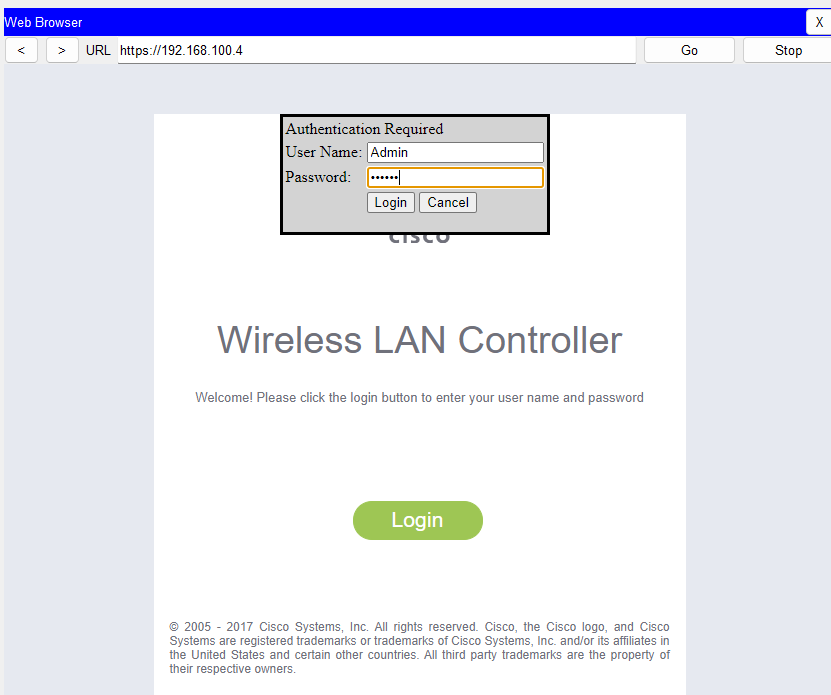
Since the administration VLAN (VLAN100) is only used for administration, all management hardware, including PCs, servers and WLC will be on it. We can improve network administration and centralize control by making sure these devices are on the administration VLAN.



The first configuration screen of the Cisco 3500 Series Wireless LAN Controller is seen in this image. To operate the WLC, users are now required to create an administrative account. Your username and password can be entered in certain places on the screen. In this case, the username "admin" is entered. A password must have a least of six characters and be made up of a mix of capital and lowercase letters, numerals, and special characters. It must also match the standards listed in the password field. The user inputs their username and password, then clicks "Start" to initiate the first setting. This is a crucial step to safeguard access to the WLC and ensure that only authorized personnel may modify the wireless network settings.

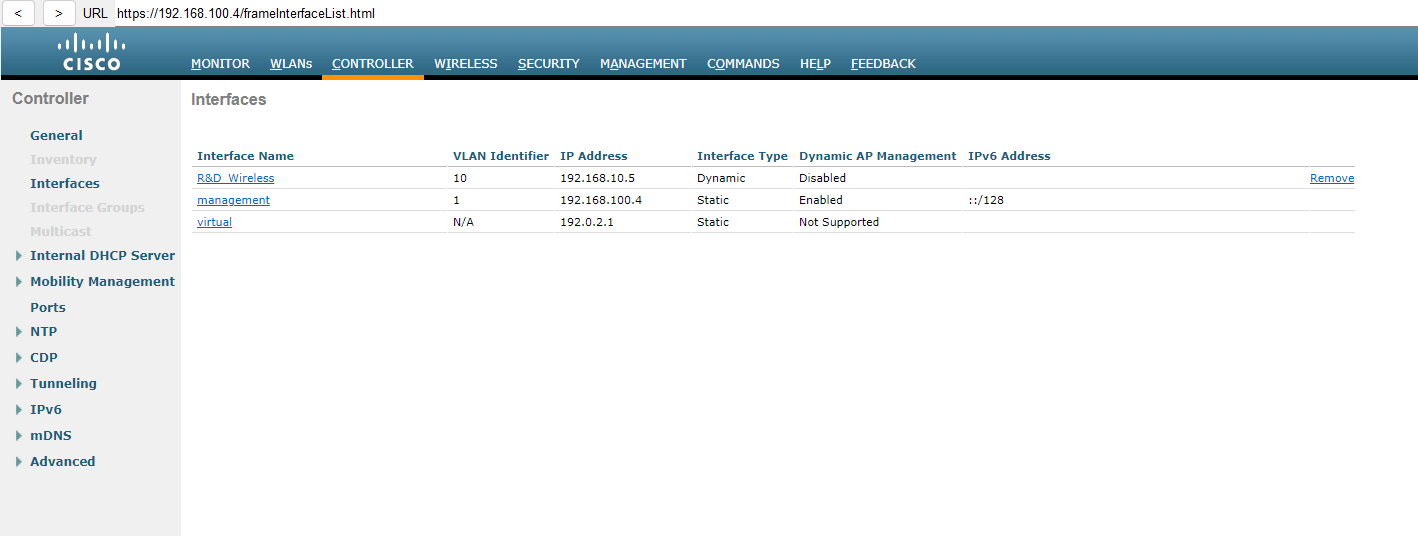


This snapshot shows a summary of the network settings for the Wireless LAN Controller and the setup information for the admin account. This displays the username "admin" that was generated in the initial setup. "Management" is selected as the system name. The date and time are displayed. The management IP address configuration is "192.168.100.4"; the subnet mask is "255.255.255.0"; and the management gateway is "192.168.100.1". For management, the VLAN ID is 0. Moreover, the Wireless Network Settings provide information on the Employee Network. The network name "Management," security type "WPA2 Personal," and matching VLAN ID are all included in this data. This comprehensive check ensures that the user has correctly configured the required network settings and administrative data.



The router's configuration for multiple interfaces is displayed in this output, with two subinterfaces that support VLAN 10 and 100 routing highlighted and allocated IP addresses. There are other interfaces, some of which are not in use at the present since they are closed and do not have IP addresses.

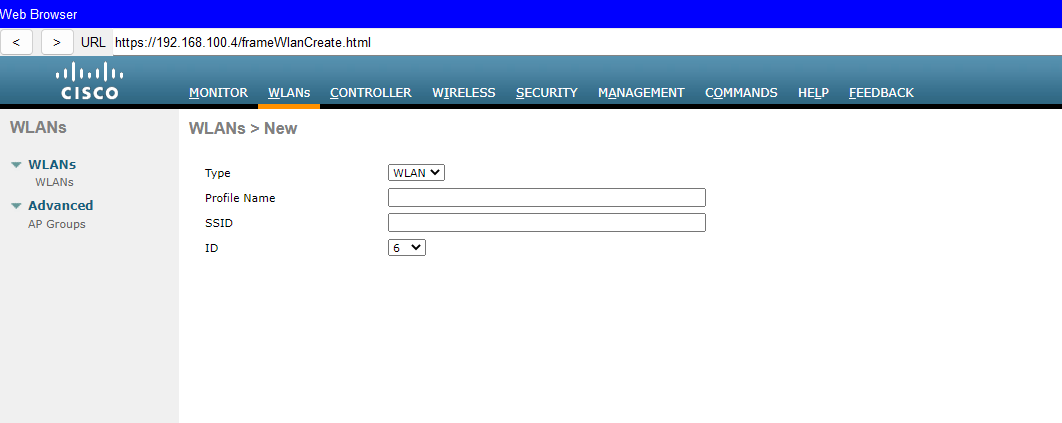
## 5.2 CREATE VIRTUAL INTERFACE IN THE WLC



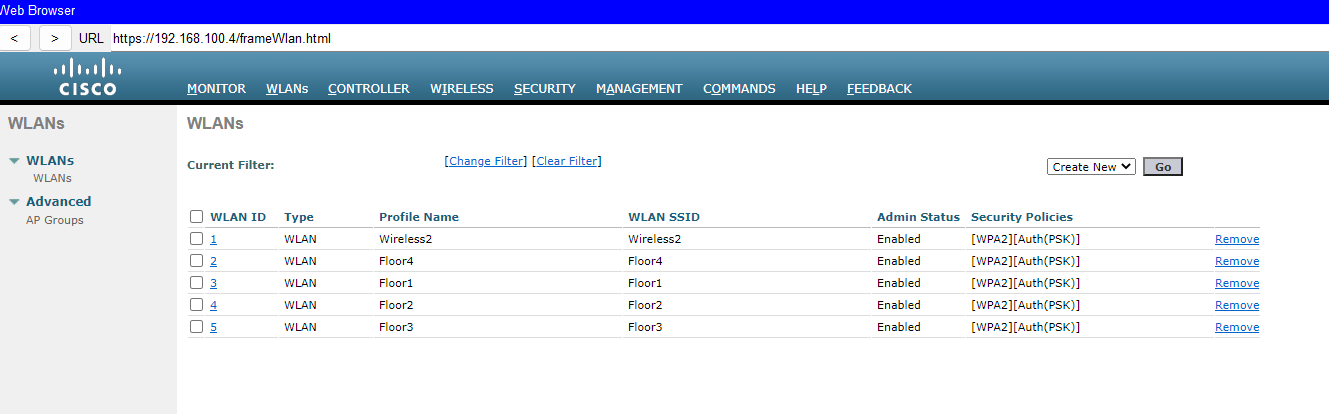
This image displays the "Interfaces" configuration panel for the Cisco Wireless LAN Controller (WLC) as seen in Cisco Packet Tracer. This page allows you to control and configure the many interfaces of the WLC. This sample shows the "virtual" and "management" interfaces. The "management" interface is usually used to establish connections with other network devices and get administrative access to the WLC. The IP address designated to be used for managing the WLC is "192.168.100.4". Due to its "untagged" status, this interface is not a member of any particular VLAN and can establish a connection with any untagged VLAN. Other variables, such the IP address, are set manually and do not change dynamically because of the "Static" interface type. Additionally, the WLC may dynamically manage access points using this interface since Dynamic AP Management is enabled. The IPv6 address of this interface is "::/128", which is a loopback address commonly used for internal or testing purposes.

To access the GUI, type the IP address of the WLC, for instance, 192.168.100.4, into a web browser. From there, select the "Interfaces" tab in the "CONTROLLER" section to begin creating a new virtual interface. From there, you may choose "New" to start creating a new interface by entering the required data, such as the interface name, IP address, and VLAN identification. After modifying any additional settings that were necessary, you would save the configuration in order to put the changes into effect. This interface page is crucial for managing the various interfaces within the WLC in order to offer proper network management and communication between the WLC and other network components.

## 5.3 CREATE WLAN

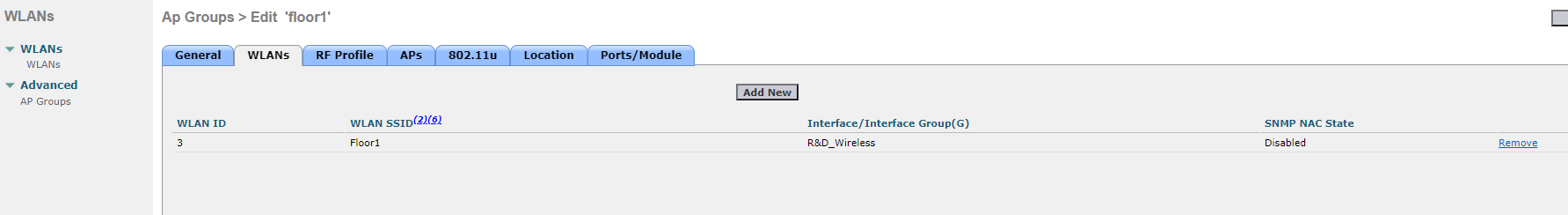


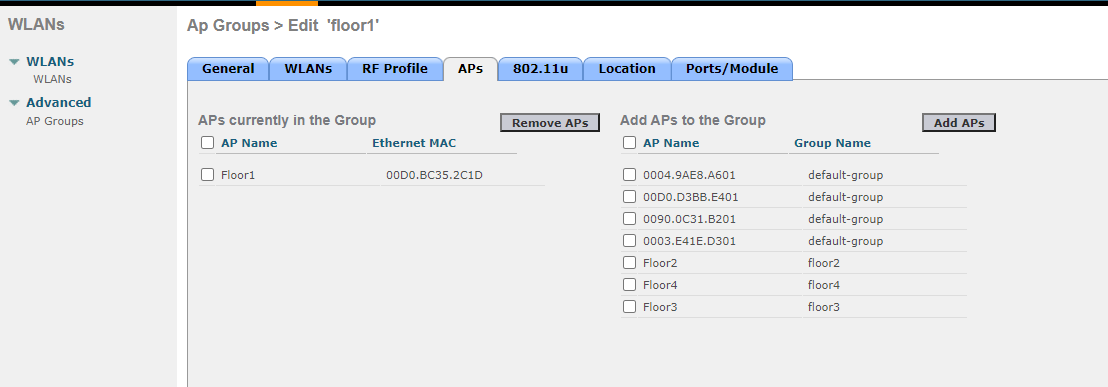
The Cisco Wireless LAN Controller (WLC) interface's "Create WLAN" page, which is used to configure a new Wireless Local Area Network (WLAN), is seen in the above image. This page allows the user to modify some crucial WLAN settings. It is possible to choose the WLAN type using the "Type" dropdown menu. "WLAN" in this instance denotes the creation of a brand-new wireless network. The user enters the name of their WLAN profile in the "Profile Name" field, which serves as the setup's identity. The "SSID" column has to contain the network name that consumers would see while searching for accessible wireless networks. Clients will be informed about this name. The "ID" parameter may be used to provide the WLAN a special identify that will help it stand out from other WLANs in the WLC. To finish setting up the new WLAN, the user must fill out these sections and click the "Apply" button to save the changes. The "Back" button allows the user to return to the previous page without saving changes.

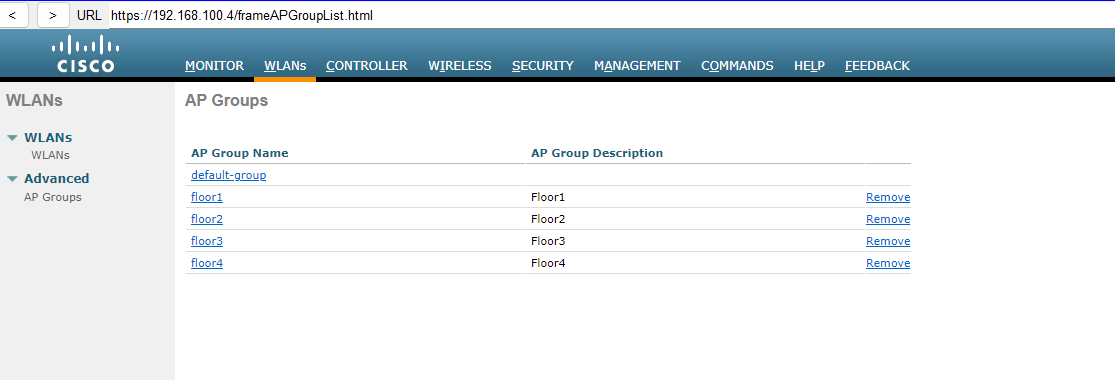


The above image shows the "Create WLAN" page of the Cisco Wireless LAN Controller (WLC) interface, which is used to configure a new Wireless Local Area Network (WLAN). The user may adjust certain important WLAN settings on this page. The "Type" dropdown menu may be used to select the kind of WLAN. In this case, "WLAN" refers to the establishment of a new wireless network. The setup's identification is determined by the user entering the name of their WLAN profile in the "Profile Name" box. The network name that users would see while looking for available wireless networks must be entered in the "SSID" field. Customers will be made aware of this name. To give the WLAN a unique identity that will make it stand out from other WLANs in the WLC, use the "ID" option. The user has to complete these areas and click "Apply" to save the changes in order to complete the WLAN setup. Without preserving changes, the user may go back to the previous page by using the "Back" button.

## 5.4 AP Group Configuration







We've established floor1, floor2, floor3, and floor 4 groups. These groupings most likely match various zones or levels in your building. In order to ensure optimal performance and minimise interference between access points, you may arrange the access points in this way and manage the wireless settings, including SSIDs (Service Set Identifiers) and frequency channels, more efficiently for each group.

# 6.0 EtherChannel Implementation:

## 6.1 Configuration

KL\_SW

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Port Channel | | Devices | Port Connections | Type |
| 5 | | To HR | F0/3 to F0/1 | PAgP |
|  |  | F0/4 to F0/2 | |
| 4 | | To Design | F0/5 to F0/1 |
|  |  | F0/6 to F0/2 | |
| 2 | | To Delivery | F0/7 to F0/1 |
|  |  | F0/8 to F0/2 | |

HR\_SW

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Port Channel | | Devices | Port Connections | Type |
| 5 | | To KL | F0/1 to F0/3 | PAgP |
|  |  | F0/2 to F0/4 | |
| 4 | | To Design | F0/3 to F0/3 |
|  |  | F0/4to F0/4 | |

Design\_SW

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Port Channel | | Devices | Port Connections | Type |
| 3 | | To KL | F0/2 to F0/6 | PAgP |
|  |  | F0/1 to F0/5 | |
| 4 | | To HR | F0/3 to F0/3 |
|  |  | F0/4 to F0/4 | |
| 2 | | To Delivery | F0/5 to F0/3 |
|  |  | F0/6 to F0/4 | |

Delivery\_SW

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Port Channel | | Devices | Port Connections | Type |
| 1 | | To KL | F0/1 to F0/7 | PAgP |
|  |  | F0/2 to F0/8 | |
| 2 | | To Design | F0/3 to F0/5 |
|  |  | F0/4 to F0/6 | |

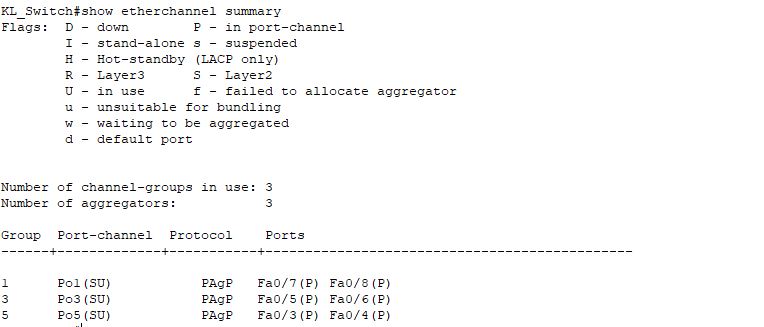
## 6.2 Justification

To verify that etherchannel has been established the command “show etherchannel summary” is used for etherchannel justification. This command displays each groups physical ports connected protocol and logical interface status code along with a list of port-channel groups.

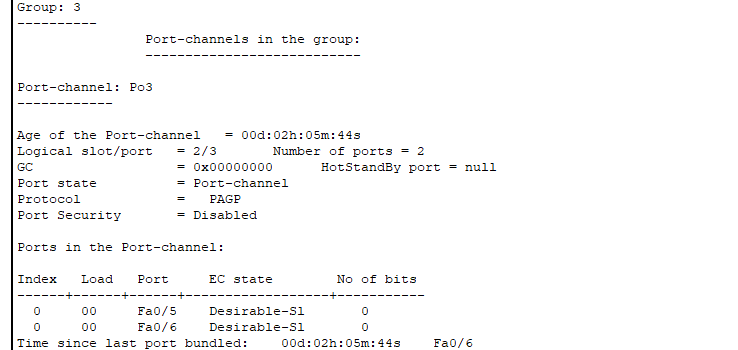
To confirm that etherchannel is implemented on interfaces use the command “show interfaces etherchannel”. The information displayed by this command is extremely comprehensive and includes details about each port-channel and etherchannel-configured interface. The command shows interfaces etherchannel: displays the data listed below.

|  |  |
| --- | --- |
| Interface port | Interface port channel |
| * Port Channel * Port index * Port State * Port number * Channel group * Flags status * PAgP port * Operation key * Admin key * Partner port’s information * Local port’s information * Age of the port in current state * State | * Port security * Protocol * Hot standby port * EC state * Logical slot * Load * Index * Number of bits * Age of port channel * Time since the last port bundled |

### KL\_Switch

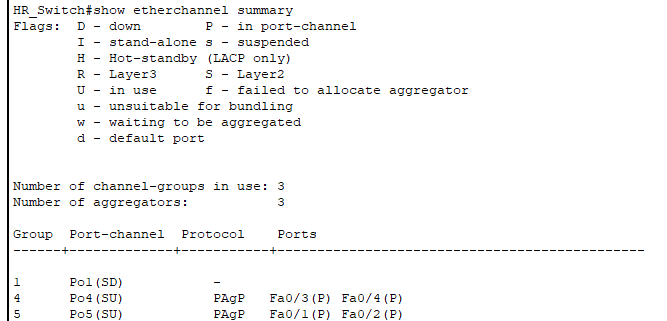


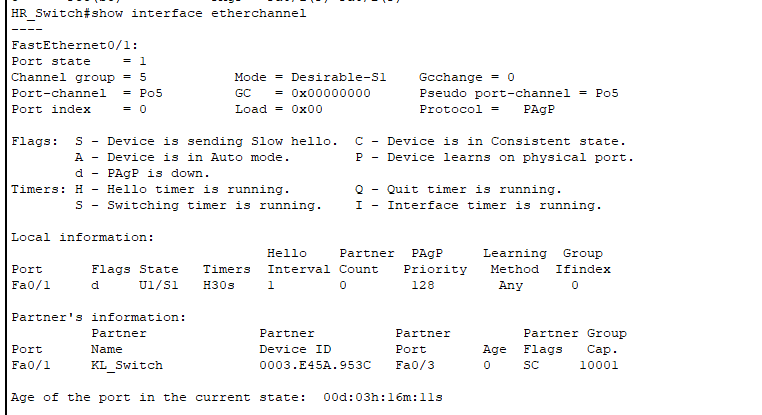


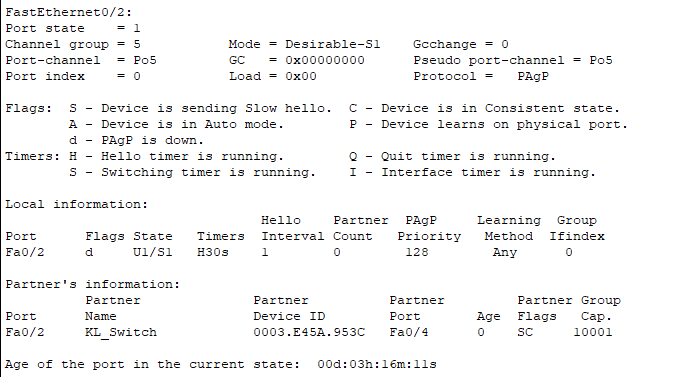


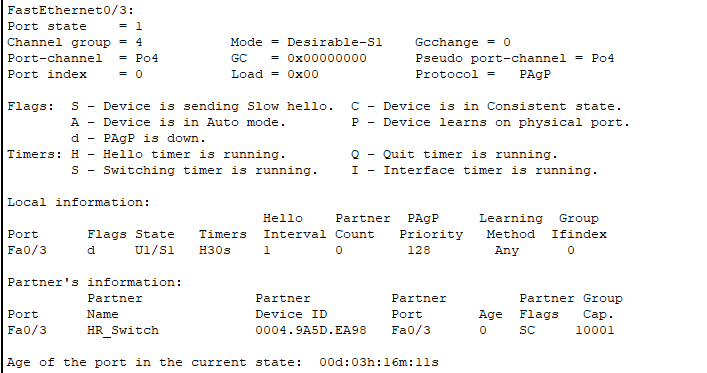


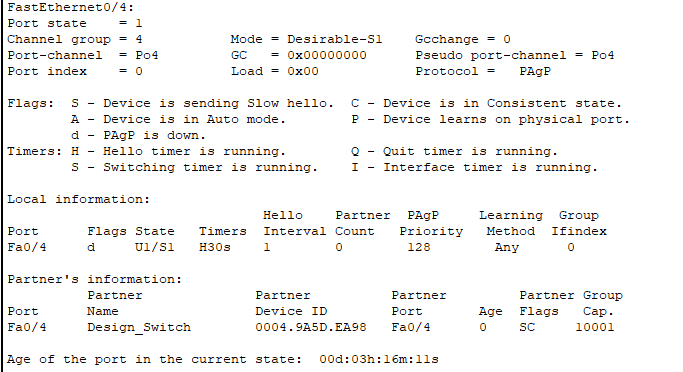
### HR\_SW

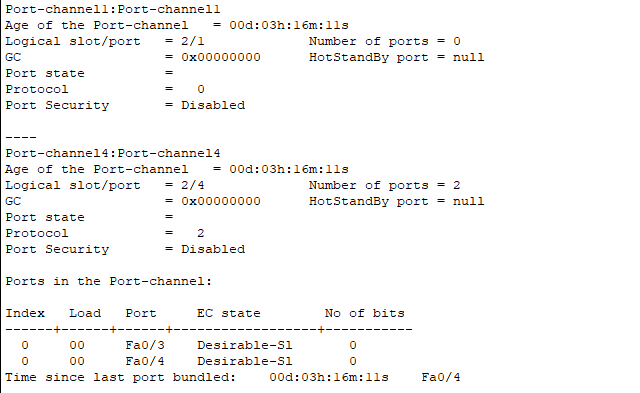


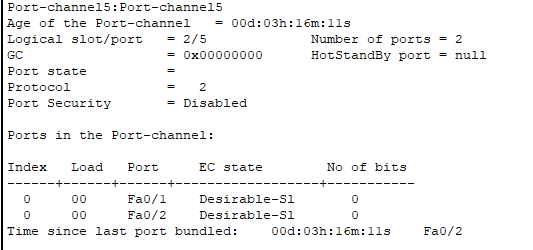




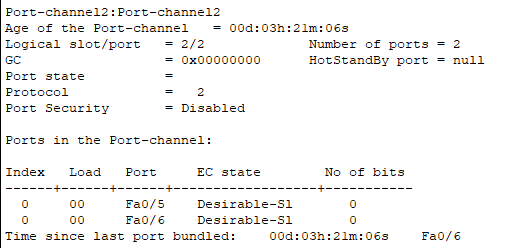
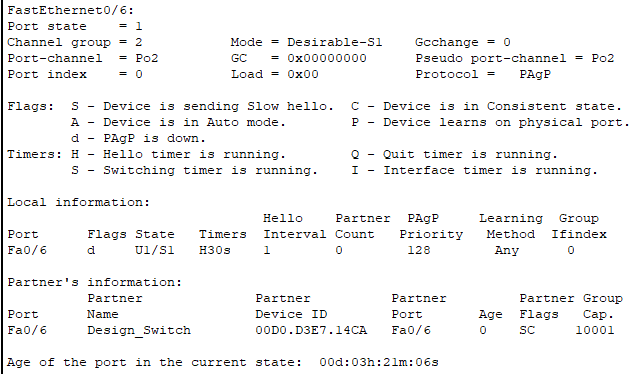
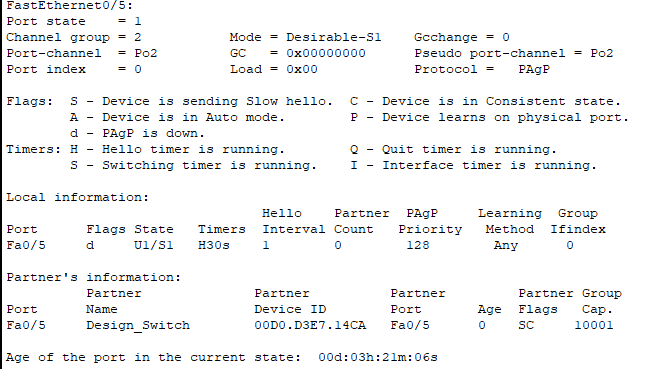
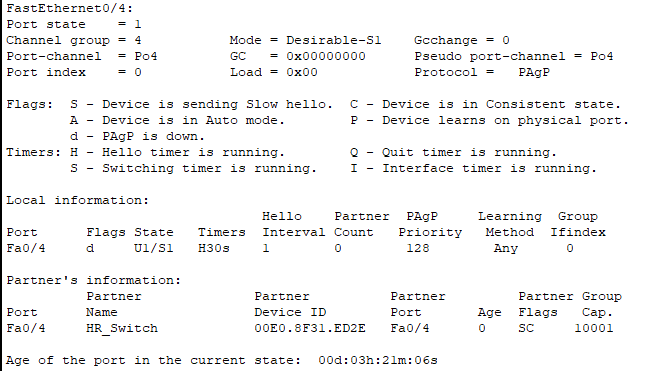
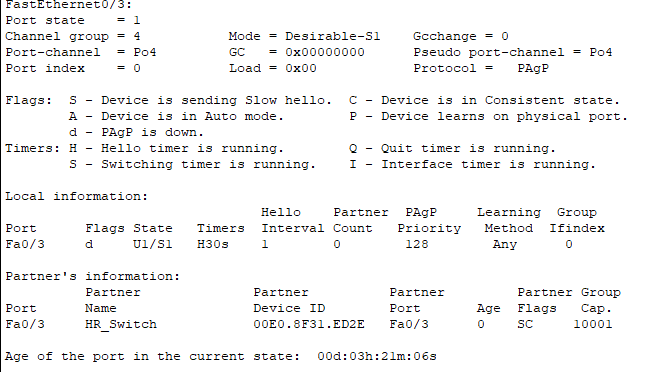
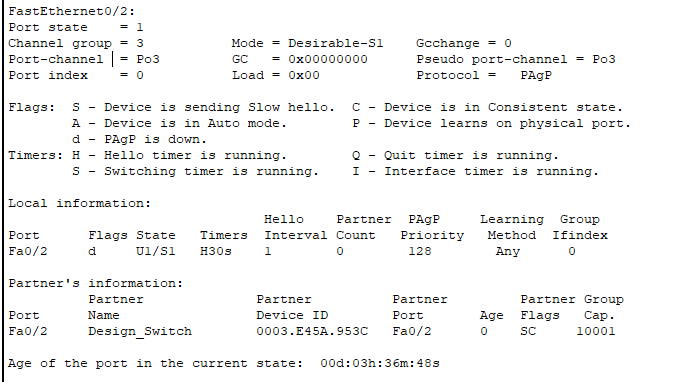
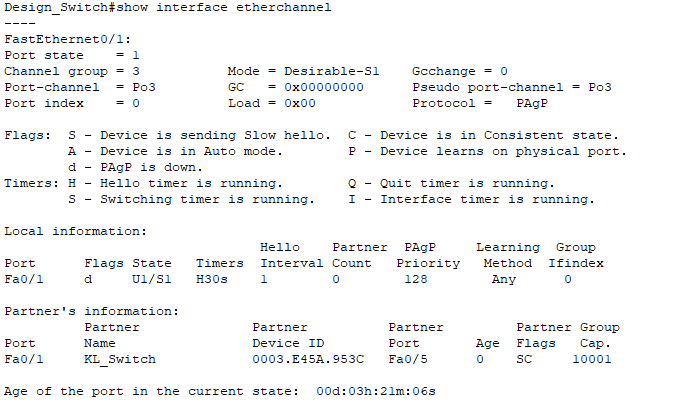
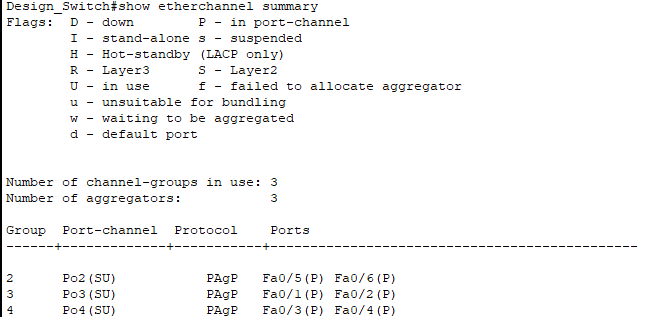


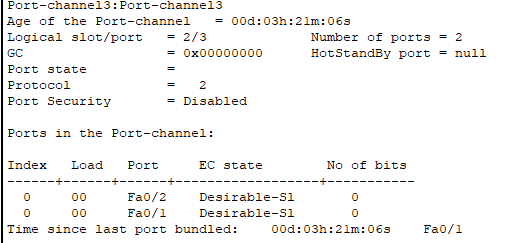


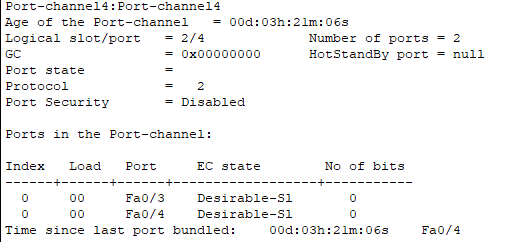




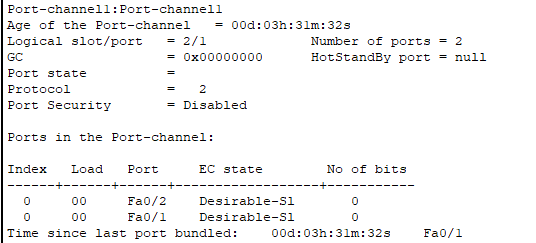
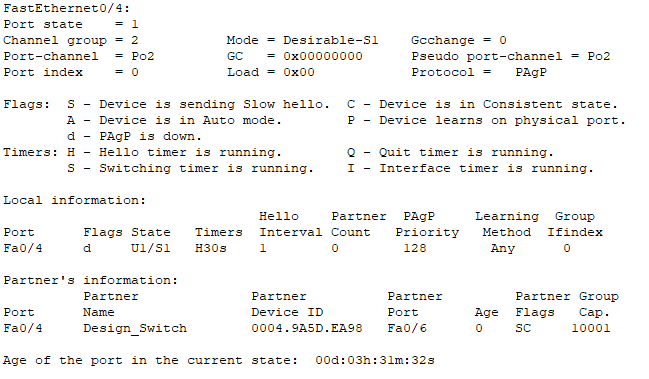
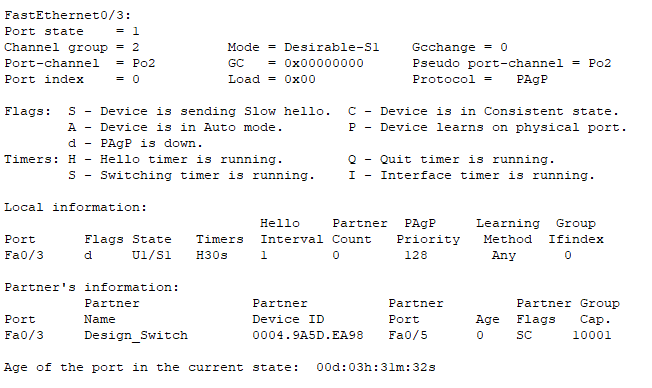
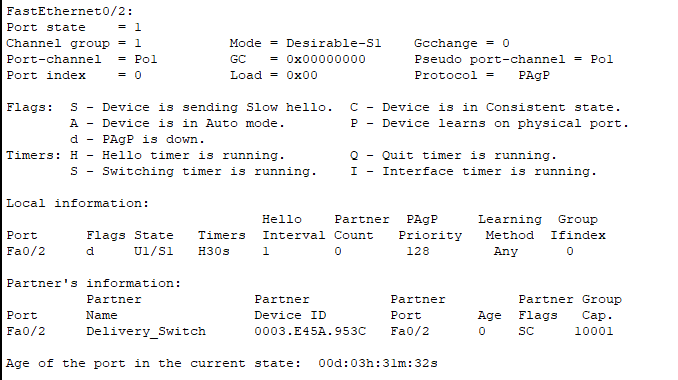
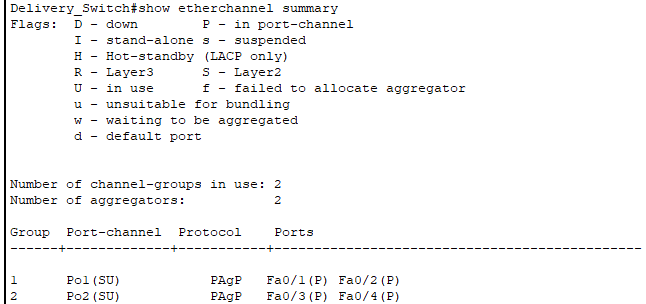
### Design\_SW

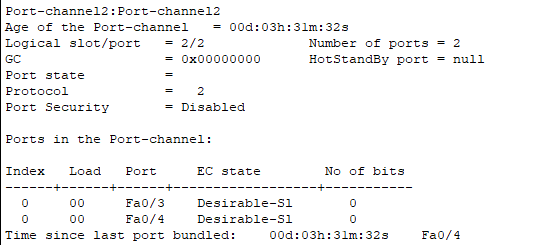






### Delivery\_SW





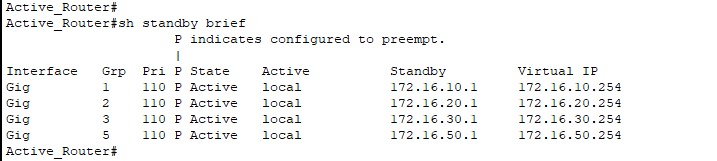
# 7.0 HSRP Implementation:

HSRP improves network availability by ensuring that all IP hosts on a network with an IP default gateway have a redundant first-hop routing path. HSRP is used in a network of routers to pick an active and standby device. The Active device handles packet forwarding, whereas the Standby device takes over when the Active device fails.

In this figure we can see the command (sh standby) which is used to check the information of router. It also shows the status of the router.



**KL\_ROUTER(Standby):**



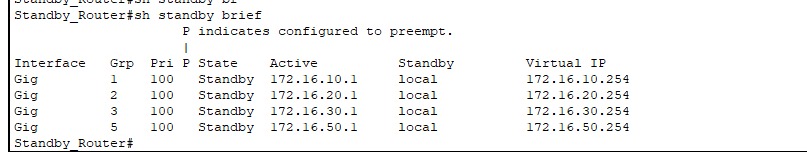
In this figure we can see the (sh standby brief) command shows the summary of Active router.

State : Active

Active : Local router

Pri : Priority is 110

**KL ROUTER (Standby):**



# 8.0 Server Farm Services Configuration:

## **8.1 DNS Service**





A white background with black text

Description automatically generated

A white background with black text

Description automatically generated

A black text on a white background

Description automatically generated

****

**A close-up of a computer screen

Description automatically generated**

****

****

****

****

****

**A close up of a text

Description automatically generated with medium confidence**

**A black text on a white background

Description automatically generated**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

The KL server Farn is an essential component of the network topology designed to server the various other branches of the organization. The configuration of server services such as the Domain Name System (DNS) , Web server and File Transfer Protocol (FTP) ensures efficient communication and data access across the branches.

To configure the DNS server, the IP address of 198.51.100.30 was set up on the server farm subnet, then DNS records were created. The DNS service was then tested using “nslookup” commands from client devices across the network to ensure the name was readable.

## **8.2 Web Server**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

## **8.3 FTP Server**

A screenshot of a computer

Description automatically generated

The web server was configured by assigning 198.51.100.20, then the Web content including the HTML files as shown above “index.html” was uploaded to the server, enabling it to host a basic website. To test the configuration, client devices within the network the network accessed the web server using its domain name resolved by the DNS server mentioned previously ensuring accessibility internally.

**A screenshot of a computer

Description automatically generated**

Firstly, the assigning the IP address of 198.51.100.10 within the server. FTP services were then enabled through the server settings, and users were provided with appropriate credentials for access. Connectivity and functionality were verified by transferring packets between the FTP server and client systems.

## **8.4 Testing**

A screenshot of a computer

Description automatically generated

The configuration of DNS, FRP and web services within the KL server Farm was successfully completed, the DNS server was able to resolve internal hostnames, the FTP server allowed for packet transfers between client devices, and lastly the web server hosted an internal web content accessible to all outside branches.

# 9.0 Tracer/Ping Commands:

## 9.1 Tracert HRSP:

A screenshot of a computer program

Description automatically generated

A screenshot of a computer screen

Description automatically generated

## 9.2 Ping Commands:

### 9.2.1 KL Network:

From Design\_PC1 to Active Router, HR\_PC and Management\_PC

A screenshot of a computer program

Description automatically generated

From Design\_PC1 to Design\_PC

A screen shot of a computer

Description automatically generated

From Design\_PC1 to Delivery\_PC

A screen shot of a computer program

Description automatically generated

### 9.2.2 Krung Thep Network

A computer screen shot of a computer program

Description automatically generated

Pinging from PC1 VLAN10 in floor 1 to the PC0 VLAN100 in the RBmanagement

A computer screen shot of a program

Description automatically generated

Pinging from Smartphone VLAN10 in floor 4 to the Laptop0 VLAN10 in floor 2

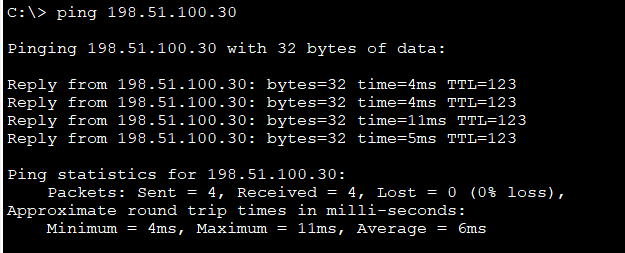
A computer screen shot of a computer program

Description automatically generated

Pinging from PC0 VLAN100 in RBmanagement to the Tablet VLAN10 in floor 3

## 9.3 Inter-Connected Router:

From Design\_pc1 to DNS server:



From Design\_pc1 to FTP server:

A screen shot of a computer program

Description automatically generated

From Design\_pc1 to Web server:

A screenshot of a computer program

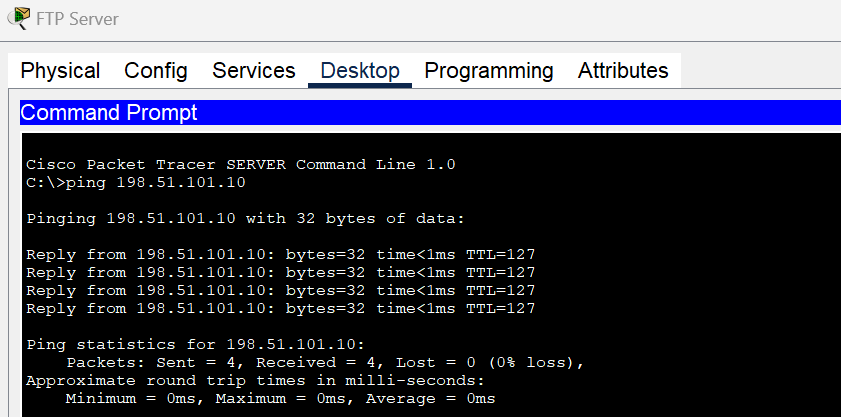
Description automatically generated

## 9.4 KL Server Farm Ping commands

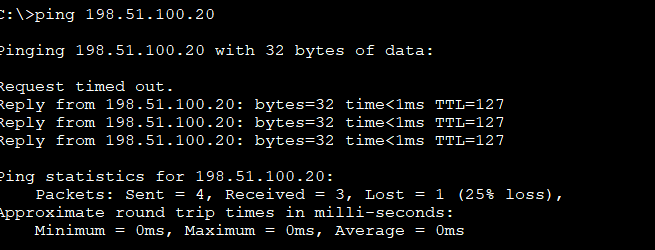
A computer screen with white text

Description automatically generated

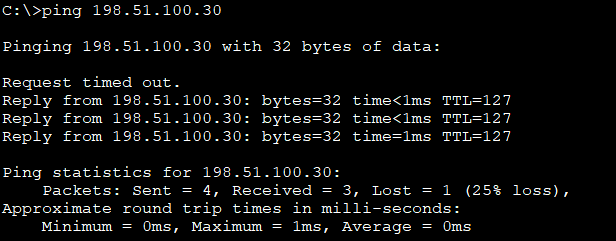
PC Management to FTP Server.



FTP Server to PC management.



PC to Webserver Server.



PC to DNS Server.

A screenshot of a computer code

Description automatically generated

Management PC to KL Server Farm Router.

# 10.0 Layer 2 Security:

## 10.1 Types of Attacks on Layer 2:

### 10.1.1 MAC Address Table attack

Mac address table attack is launched by flooding a switch’s MAC address table with fake MAC address until its full. With the switch’s MAC address table is full the switch enters a fail-open mode, broadcasting all incoming traffic to all ports. This makes the attacker able to capture network traffic intended for other hosts.

### 10.1.2 VLAN Hopping Attack

VLAN Hopping attack exploits VLAN configs to send traffic to different VLANs without proper routing. By manipulating trunking protocols or using double tagging. VLAN hopping attacker can access and intercept traffic from VLANs that the attacker doesn’t have access to.

### 10.1.3 DHCP Starvation Attack

DHCP starvation attack works by the attacker sending huge amount of DHCP request messages with spoofed MAC address to exhaust the DHCP’s server pool of IP addresses. Making real users unable to obtain Ip addresses, leading to a DOS (denial of service) situation.

### 10.1.4 ARP Spoofing and ARP Poisoning

This attack works by sending falsified ARP messages over the local network, using their MAC address with the IP address of another host (ex. Default gateway). This fools other network devices to send traffic to the attacker rather than the legitimate host, making the attacker able to intercept or manipulate the data.

## 10.2 Layer 2 Security Deployment

### 10.2.1 Mitigation Technique of MAC Address Flooding Attack

#### 10.2.1.1 PORT SECURITY Implementation:

One of the crucial components of networking is port security. It is a method used to make sure that a network can only be accessed by authorized devices. There are several methods for implementing port security, such as using firewalls, virtual local area networks (VLANs), and access control lists (ACLs) (Aakriti, 2024). By implementing port security, organizations can protect their own networks from unauthorized access and potential threats.

### Port security for Krung Thep switch branch:

A screen shot of a computer

Description automatically generated

1. The first command (“int range g1/0/4-7,g1/0/23-24”) selects multiple interfaces (GigabitEthernet 1/0/4 to 1/0/7 and GigabitEthernet 1/0/23 to 1/0/24) to start configure these interfaces.
2. **(“switchport mode trunk”)**: Trunk mode is applied to the chosen interfaces. Traffic for several VLANs is transported via trunk ports between switches or between a switch and a router.
3. **(“switchport port-security”):** This enables port security on the selected interfaces.
4. **(“switchport port-security mac-address sticky”):** Using sticky learning, dynamically learned MAC addresses can be automatically added as "sticky" addresses to the port security configuration. This implies that these MAC addresses are going to be stored and treated as static entries.
5. **(“switchport port-security maximum 10”):** This limits the number of MAC addresses that the interface can manually configure or learn to 10. If more than 10 devices try to connect, the switch will act according to the violation mode.
6. **(“switchport port-security violation restrict”):** This set the action to be taken if a security violation occur. When the "restrict" option is selected, the port will continue to function normally but will drop packets from MAC addresses that violate it and log the violation.

A screen shot of a computer

Description automatically generated

This command is important in Cisco switch/router configurations Because it duplicates the running configuration to the startup configuration.

A screen shot of a computer

Description automatically generated

Now after the port security is implemented the command (“sh port-security”), provides a summary of port security information on the switch ports that have been secured.

A screenshot of a computer

Description automatically generated

To display all the mac-addresses for each port must use (“port-security address”) command, which shows the learned mac addresses on the secure ports

### 10.2.2 Mitigation Technique of VLAN Hopping Attack

#### 10.2.2.1 SECURE UNUSED SWITCH PORTS for Krung Thep switch

A screen shot of a computer

Description automatically generated

The configuration displayed in the image shows that ports Gi1/0/8 to Gi1/0/22 and Gi1/1 to Gi1/1/4 have been put in VLAN 99 (BlackHole) left unconnected. This setup provide unauthorized devices from accessing these ports, reducing the chance of security breaches. By assigning these inactive ports to a non-routable VLAN and disabling them, the network security is enhanced, minimizing the risk posed by unused but potentially accessible switchports.

### 10.2.3 Mitigation Technique for STP Attacks:

This is done by implementing BPDU guards on all access ports

A screenshot of a computer code

Description automatically generated

To configure a BPDU Guard on a switch, you need to follow a few steps. First, enter the command spanning-tree portfast bpduguard default to enable BPDU Guard on the switch. Next, use the command interface range f0/3-5 to select the interfaces that connect to the access ports. Finally, activate BPDU Guard on the selected interfaces by entering the command spanning-tree bpduguard enable. Once these steps are completed, BPDU Guard will be successfully implemented on the switch.

A screenshot of a computer program

Description automatically generated

As you can see after running the command show running-config the BPDU guards are enabled on the ports.

### 10.2.4 Mitigation Technique for DHCP Snooping:

Implement DHCP snooping

A white text with black text

Description automatically generated

To configure a DHCP snooping on a switch, these steps need to be followed. First, use the command ip dhcp snooping to enable DHCP snooping on the switch. Then, enter ip dhcp snooping vlan 10,99 to enable DHCP snooping on the selected VLANs. To disable the insertion of DHCP option information, use the command no ip dhcp snooping information option. Next, select the interfaces by entering int g1/0/1, and configure it as a trusted port by using ip dhcp snooping trust; this port is typically connected to the DHCP server. After that, select a range of interfaces using the command int range g1/0/2-8, and finally, set the limit for incoming DHCP packets on the selected ports by using ip dhcp snooping limit rate 20.

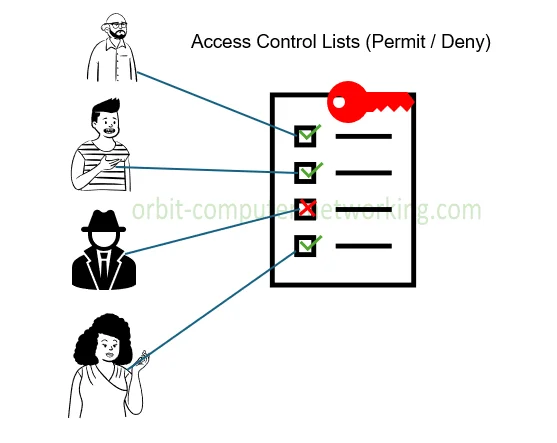
A screenshot of a computer

Description automatically generated

The command “show ip dhcp snooping” can utilized to verify the configuration of DHCP snooping.

# 11.0 Recommendations:

## 11.1 Access Control List (ACL):



A list of rules called an access control list (ACL) determines which users or systems are allowed or prohibited access to a specific object or system resource. Additionally, access control lists can be installed in switches or routers to serve as filters and control which traffic is allowed to access the network and which is not (Lutkevich, 2022).

**There are two basic kinds of ACLs:**

1. Filesystem ACLs: These function as filters to control who has access to certain files or directories. The operating system receives instructions from a filesystem ACL regarding which users are permitted to access to the system and what privileges they are granted once they are inside.
2. Networking ACLs: ACLs for networking control network access. ACLs accomplish this by giving switches and routers instructions on the types of traffic that are permitted to interface with the network. ACLs also specify what can be done inside by each user or device.

**How Does An ACL Work?**

The operating system of the computer can determine which users have what access privileges because of a table you have with a filesystem ACL. Users who are permitted to access particular items, like files or directories on the system, are determined by the table. Each and every item on the computer has a security attribute that connects it to the corresponding access control list. Each user with the necessary permissions to access the system has their information on the list. An ACL controls access to certain files or objects on computer based on user permissions. Such as, regular users can be restricted from accessing files that only administrators can open. in networking, both network ACL and security groups define who can access resources. A security group might list specific users or categories, such as administrator, guest, and normal users, that are allowed access.

## 11.2 Virtual Private Network (VPN):



"Virtual Private Network" (VPN) refers to the ability to create a secure network connection when using public networks. VPNs mask online identity and encrypt internet traffic. This increases the difficulty level for third parties to monitor users online activity and steal data. Real-time encryption is employed.

**How does a VPN work?**

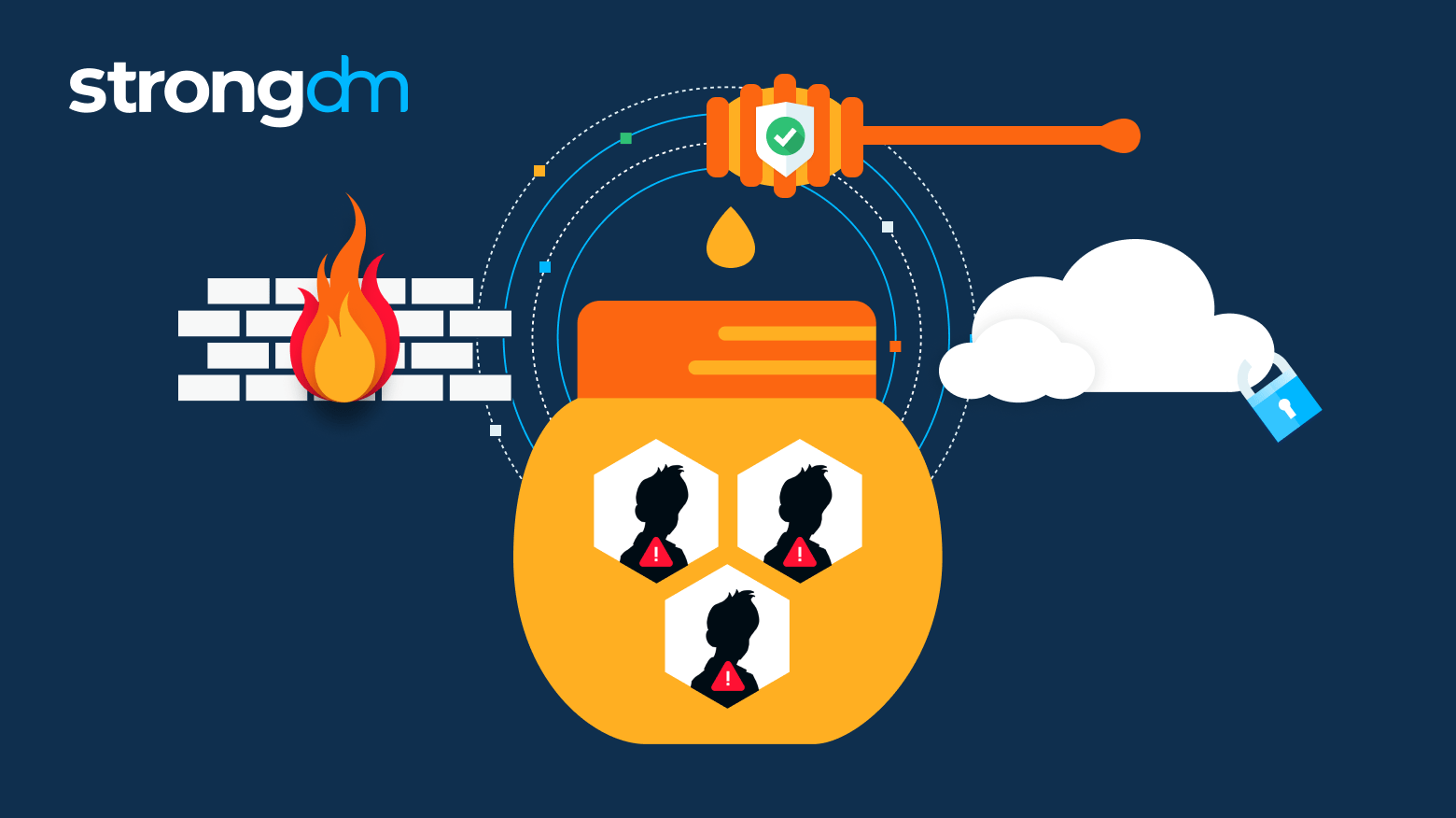
Through the use of a specially configured remote server operated by a VPN host, a VPN masks your IP address on the network. This implies that when using a VPN to surf the internet, the VPN server becomes the source of your data. Thus, neither your Internet Service Provider (ISP) nor any other third party will be able to see the websites you visit or the information you send and receive online. A VPN works like a filter that turns all your data into "gibberish". The users data would be useless even if it were to fall into the wrong hands (*What Is VPN? How It Works, Types of VPN*, 2023).

VPN provides:

**Secure encryption**: An encryption key is required in order to read the data. In the case of a brute force attack, a computer would need millions of years to decode the code in the absence of one. Even on public networks, your online activity remains anonymous with the use of a VPN.

**Hide your location**: VPN servers function as virtual proxies over the internet. user exact location cannot be discovered because the demographic location data originates from a server located in a different nation. most VPN services do not store logs of your activities. And many more benefits.

## 11.3 Honeypot



A honeypot is a cybersecurity tool that draws hackers away from real targets by creating a fake attack target. They also get information about the identities, strategies, and objectives of attackers.   
  
A honeypot can be designed to resemble any kind of digital asset, such as servers, software programs, or even the network itself. It is purposefully made to appear like a respectable target, mirroring the model in terms of structure, elements, and content. By doing this, the adversary will be led to believe that they have gained access to the real system and will be encouraged to spend more time in this controlled environment.

**How Does a Honeypot Work?**

The fundamental idea behind honeypot is that it should be designed to look like the network target a company is attempting to protect. It is possible to create a honeypot trap that imitates a payment gateway, which is a common target for hackers due to the plenty of personal data and transaction details it contains, including bank account and credit card details that have been encrypted. In order to attract individuals interested in obtaining trade secrets, intellectual property (IP), or other sensitive information, a honeypot or honeynet may also mimic a database (Vaideeswaran, 2022).

12.0 Conclusion:  
  
In conclusion, the network upgrade for the company Microtech Sdn. Bhd. has been successfully designed and configured to meet the company's operational needs across its KL headquarters and Krung Thep branch. The implementation of VLANs, inter-VLAN routing, and Spanning Tree Protocol (STP) were all successful and has enhanced network segmentation, efficiency, and loop prevention. Additionally, the deployment of Wireless LAN Controller (WLC) technology at the remote branch has streamlined wireless access management. Through the use of Cisco Packet Tracer, the network's logical topology and configurations were validated, ensuring a robust and secure network infrastructure capable of supporting the company's growing demands.

# 13.0 References:

Aakriti. (2024, June 17). *Port security in Networking: All you need to know*. Network Kings. <https://www.nwkings.com/port-security-in-networking>

Lutkevich, B. (2022, February 3). *access control list (ACL)*. Networking. <https://www.techtarget.com/searchnetworking/definition/access-control-list-ACL>

*What is a Network Access Control List (ACL)? | Fortinet*. (n.d.-b). Fortinet. <https://www.fortinet.com/resources/cyberglossary/network-access-control-list#:~:text=Network%20Access%20Control%20List%20Meaning,are%20allowed%20in%20the%20doors>.

*What is VPN? How It Works, Types of VPN*. (2023, May 5). /. <https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn>

Vaideeswaran, N. (2022, March 9). *Honeypots in Cybersecurity Explained*. Crowdstrike. <https://www.crowdstrike.com/en-us/cybersecurity-101/exposure-management/honeypots/>

Meena. (2024). *How to Configure EtherChannel Easily? - A Demonstration*. Retrieved from luminisindia: <https://luminisindia.com/it-networking-blog/155-how-to-configure-etherchannel-or-port-channel-easily-a-demonstration>

N-able. (2019, Aug 5). *Understanding VLAN Trunking*. Retrieved from n-able: <https://www.n-able.com/blog/vlan-trunking>

*Cisco Wireless Controller Configuration Guide, Release 8.5 - Initial Setup [Cisco Wireless LAN Controller Software]*. (2024, April 30). Cisco. <https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/initial_setup.html>

*WLANs Tab*. (2015, September 21). Cisco. <https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-1/olh/wlc-olh-81/wlansc.html>

Gillis, A. S. (2023). *DHCP (Dynamic Host Configuration Protocol)*. Retrieved from techtarget: <https://www.techtarget.com/searchnetworking/definition/DHCP>

KHAN, I. (2023, Oct 23). *HSRP Configuration: Explained*. Retrieved from nwkings: <https://www.nwkings.com/hsrp-configuration>

GAVIN, B. (2023). *How to Use the Ping Command to Test Your Network*. Retrieved from How to Geek: <https://www.howtogeek.com/355664/how-to-use-ping-to-test-your-network/>