



**INDIVIDUAL ASSIGNMENT**

**CT133-3-2-SRE**

**SWITCHING AND ROUTING ESSENTIALS**

**APU2F2211CS (CYB), APD2F2211CS (CYB)**

**APU2F2211IT (CE), APD2F2211IT (CE)**

**HAND OUT DATE: 12<sup>th</sup> December 2022**

**HAND IN DATE: 4<sup>th</sup> March 2023**

**Weightage: 40%**

**Online Submission Time before = 11: 59 PM**

**Lecturer: Noris Ismail**

**Student Name: KUAN ZHI HUI [Report B]**

**Student ID: TP067195**

## Table of Contents

Introduction.....	3
<b>1.0 IP Address Allocation Table .....</b>	<b>4</b>
1.1 KL .....	4
1.2 Server Farm.....	6
1.3 Brunei – Remote Branch.....	7
WAN IP Addressing Table .....	8
2.0 Entire Network layout for MicroTech Sdn Bhd.....	9
<b>3.0 Propose of LAN and WAN Network .....</b>	<b>10</b>
3.1 VLAN .....	10
KL HQ VLAN .....	11
Server Farm VLAN.....	12
Hanoi VLAN.....	13
3.2 Inter-VLAN Routing.....	14
3.3 Router-on-a-Stick.....	14
3.4 Spanning Tree Protocol.....	16
3.5 EtherChannel.....	17
3.6 OSPF .....	20
The IP Routing Table Route Sources.....	21
3.7 DHCPv4.....	22
<b>4.0 Deployment of Layer 2 Security Mechanisms in Configuration.....</b>	<b>24</b>
4.1 Mitigation VLAN attacks .....	25
4.2 Mitigation STP attacks.....	28
4.3 Mitigation DHCP attacks .....	30
4.4 Mitigation MAC Address Table Flooding Attacks .....	32
SSH configuration.....	35
Conclusion .....	36
References.....	37

## Introduction

In the Part B report, I was assigned to explain and discuss new VLAN designs, LAN and WLAN, DHCPv4, dynamic or static routing, and deploy layer 2 security attacks to design and engineer a new wireless network for MicroTech Sdn Bhd. The purpose of this report is to implement a new network for MicroTech Sdn Bhd. It will be divided into 3 parts to configure different types of network configuration techniques. For the KL headquarters, there will be a router, 4 switches and 7 PCs connected together via spanning tree. For a server farm, there will be a router, a switch, and 3 servers connected together. The Hanoi network in Brunei will be a wireless network connected by a router, a multilayer switch, PCs and so on.

## 1.0 IP Address Allocation Table

IP addresses are essential in network communication and management; communication between devices would be impossible without IP addresses (Kaspersky, n.d.). IP addresses can be used by network administrators to identify devices and monitor network traffic and performance. An IP address is a numerical identifier that uniquely identifies a network device and is used to locate and transmit data over a network. IP addresses are major elements of network security. Access control lists based on IP addresses, for example, can help prevent unauthorized access and protect the network from malicious attacks.

### 1.1 KL

In the KL network, there are 4 switches connected to the switch and all IP addresses will be assigned statically.

Management Department						
VLAN	Device	Interface	Network Address	IP Address	Subnet mask	Default gateway
50	Dis_SW	VLAN 50	192.168.50.0/24	192.168.50.5	255.255.255.0	192.168.50.1
99	Blackhole VLAN					
100	Native VLAN					

Delivery Department						
VLAN	Device	Interface	Network Address	IP Address	Subnet mask	Default gateway
30	Delivery-PC1	Fa0/2	192.168.20.0/24	192.168.20.2	255.255.255.0	192.168.20.1
	Delivery-PC2	Fa0/1		192.168.20.3		
50	Delivery_SW	VLAN 50	192.168.50.0/24	192.168.50.6		192.168.50.1
99	Blackhole VLAN					
100	Native VLAN					

Design Department						
VLAN	Device	Interface	Network Address	IP Address	Subnet mask	Default gateway
20	Design-PC 1	Fa0/1	192.168.30.0/24	192.168.30.2	255.255.255.0	192.168.30.1
	Design-PC 2	Fa0/2		192.168.30.3		
50	Design_SW	VLAN 50	192.168.50.0/24	192.168.30.1		192.168.50.1
99	Blackhole VLAN					
100	Native VLAN					

HR Department						
VLAN	Device	Interface	Network Address	IP Address	Subnet mask	Default gateway
10	HR-PC0	Fa0/1	192.168.10.0/24	192.168.10.2	255.255.255.0	192.168.10.1
	HR-PC1	Fa0/2		192.168.10.3		
	HR-PC2	Fa0/3		192.168.10.4		
50	Delivery_SW	VLAN 50	192.168.50.0/24	192.168.10.5		
99	Blackhole VLAN					
100	Native VLAN					

## 1.2 Server Farm

In Server Farm network, all the IP addresses are assigning statically which are in between 198.51.100.10 to 198.51.100.30.

Server Farm						
VLAN	Device	Interface	Network ID	IP Address	Subnet Mask	Default Gateway
10	DNS-Server 198.51.100.10	Fa0/1	192.51.100.0/24	198.51.100.10	255.255.255.0	198.51.100.1
	FTP-Server: 198.51.100.30	Fa0/2		198.51.100.30		
	WebServer: 198.51.100.20	Fa0/3		198.51.100.20		
99	Blackhole VLAN					
100	Native VLAN					

### 1.3 Brunei – Remote Branch

Brunei						
VLAN	Device	Interface	Network ID	IP Address	Subnet Mask	Default Gateway
100	RB-Admin-PC	G1/0/1	192.51.100.0/24	198.51.100.2	255.255.255.0	198.51.100.1
	RB_WLC	G1/0/23		198.51.100.254		
	LAP-Floor1	G1/0/21		198.51.100.241		
	LAP-Floor2	G1/0/22		198.168.100.242		
	LAP-Floor3	G1/0/20		198.168.100.240		
	RB_SWML	VLAN 100		192.168.100.100		
10	Tablet PC1-User1	Wireless0	192.51.10.0/24	192.168.10.14		192.168.10.1
	Laptop PT Laptop-User1			192.168.10.11		
	PC-PT PC1-User1			192.168.10.15		
	PC-PT PC2 User 2			192.168.10.7		
	PC-PT PC2 User 1			192.168.10.8		
	SMARTPHONE-PT Smartphone 2			192.168.10.6		
	PC-PT PC 3 User 1			192.168.10.10		
	Smartphone 3			192.168.10.3		
	Tablet PC1 – User 3			192.168.10.12		
	Laptop 1 – User 3			192.168.10.9		
99	blackhole					

In the Brunei network, VLAN 10 end devices and wireless devices are connected to the wireless network; therefore, the IP address is dynamically assigned, and the IP address is between 192.168.10.3 and 192.168.10.15. Whereas for VLAN 100, the IP address starts with 192.51.100.1.

## WAN IP Addressing Table

From the network layout design, there will be 5 routers group together connect to the network. The HQ-Router and ServerFarm\_Router is for KL network. The Brunei-Router is for the Brunei network. ISP 1 and 2 is the Internet Server Providers router.

Routers				
Device	Interface	Network ID	IP Address	Subnet Mask
HQ-Router	Se0/1/0	200.100.100.4/30	200.100.100.5	255.255.255.255
	Se0/1/1	200.100.100.8/30	200.100.100.9	
ServerFam_Router	Se0/1/0	200.100.100.16/30	200.100.100.18	
ISP-1	Se0/1/0	200.100.100.0/30	200.100.100.2	
	Se0/1/1	200.100.100.8/30	200.100.100.10	
	Se0/2/0	200.100.100.12/30	200.100.100.13	
ISP-2	Se0/1/0	200.100.100.16/30	200.100.100.17	
	Se0/1/1	200.100.100.12/30	200.100.100.14	
Brunei-Router	Se0/1/0	200.100.100.4/30	200.100.100.6	
	Se0/1/1	200.100.100.0/30	200.100.100.1	





## 3.0 Propose of LAN and WAN Network

### 3.1 VLAN

VLAN (virtual local area network) is a logical custom subnetwork. The benefits of using VLAN for network is to improve the security, avoid network redundancy traffic and enhance bandwidth. From all the benefits it can combine it together, for it can manage the network effectively and it also can affect the whole network. In order to explain each viewpoint from a different perspective, below are the details:

**Security:** By separating different types of network traffic, VLANs can improve network security. VLANs can prevent unauthorized access to sensitive data and reduce the risk of attacks such as network eavesdropping, man-in-the-middle attacks, and network spoofing by segmenting the network into smaller logical segments. Security is also related to network traffic and bandwidth because unauthorized access, attacks, and other security threats can increase network traffic and reduce bandwidth.

**Scalability:** VLANs make network management and scaling easier. VLANs can be used to group devices based on their function or location as businesses grow and new devices are added to the network, making it easier to manage and troubleshoot the network.

**Cost-effectiveness:** VLANs can be a cost-effective solution for managing network traffic, especially in larger networks. VLANs allow for the logical separation of network traffic, eliminating the need to install and manage separate physical networks for different types of devices.

Every VLAN has its own broadcast domain. This means that only VLAN-specific ports share broadcasts, preventing unnecessary traffic from flooding the entire network and thus improving overall network performance by segmenting VLANs based on the group (Antoniou, 2022). In order to group all the networks to manage the network effectively, we can use the 5 types of VLAN to config the different types of network traffic VLAN on the switch to switch by segment the network into smaller logical segments. The 5 types of VLAN used for managing such as voice VLAN for handling voice traffic, Data VLAN for handling the data traffic such as email or web browsers, blackhole VLAN for unused ports, access port VLAN to connect the PC, printer, or smartphone and native VLAN is to handle trunk link on the switch to switch. To give an illustration in the Microtech Network, there is a total of six VLANs that have been set up in the KL headquarter network, each with a specific purpose. These include VLAN 99 for blackhole, VLAN 100 for native, VLAN 20 for the Delivery department,

VLAN 30 for the design department, VLAN 10 for the HR department, and VLAN 50 for the management department. Additionally, VLAN 99 for blackhole and VLAN 10 for Server Farm have been configured and set up in the KL Server Farm network. Lastly, VLAN 10 for R&D, VLAN 99 for blackhole, and VLAN 100 for Mgmt&Native have been configured and set up in the Brunei network.

### KL HQ VLAN

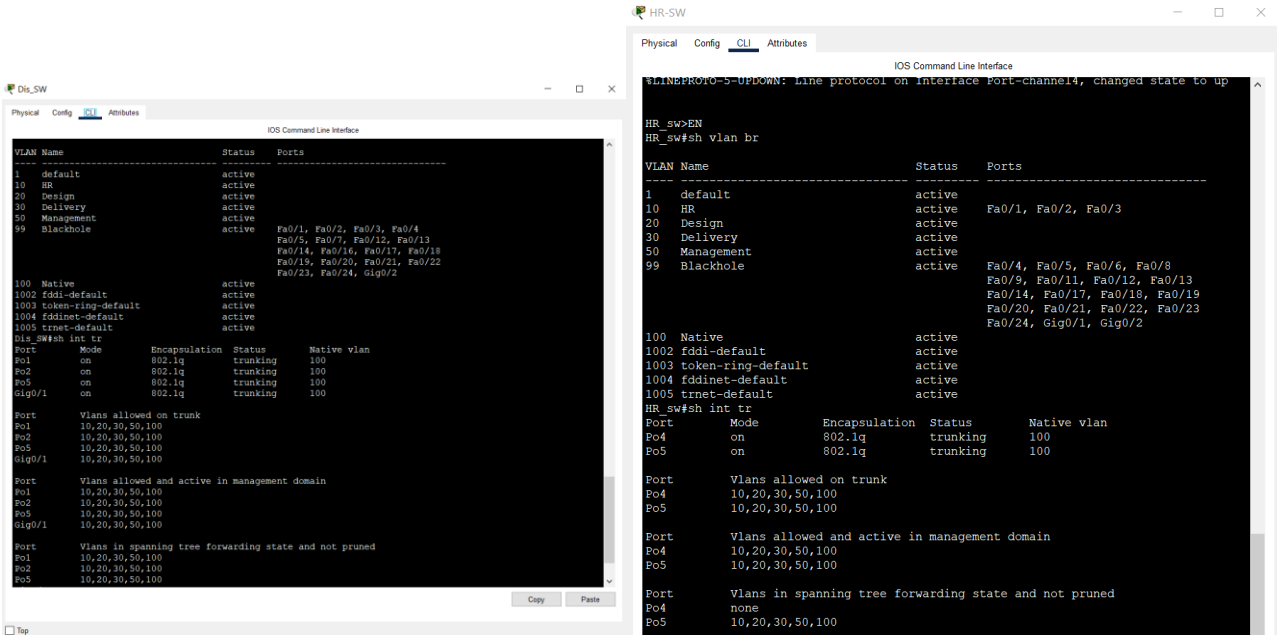


Figure 2: VLANs of Management & HR

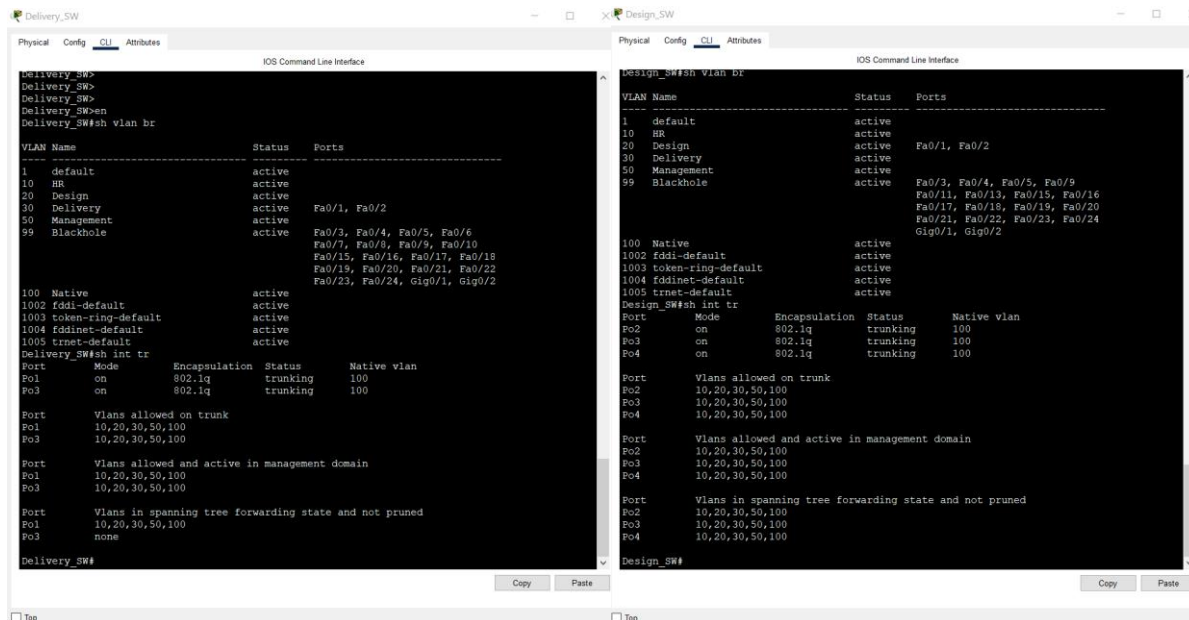


Figure 3: VLANs of Delivery & Design

## Server Farm VLAN

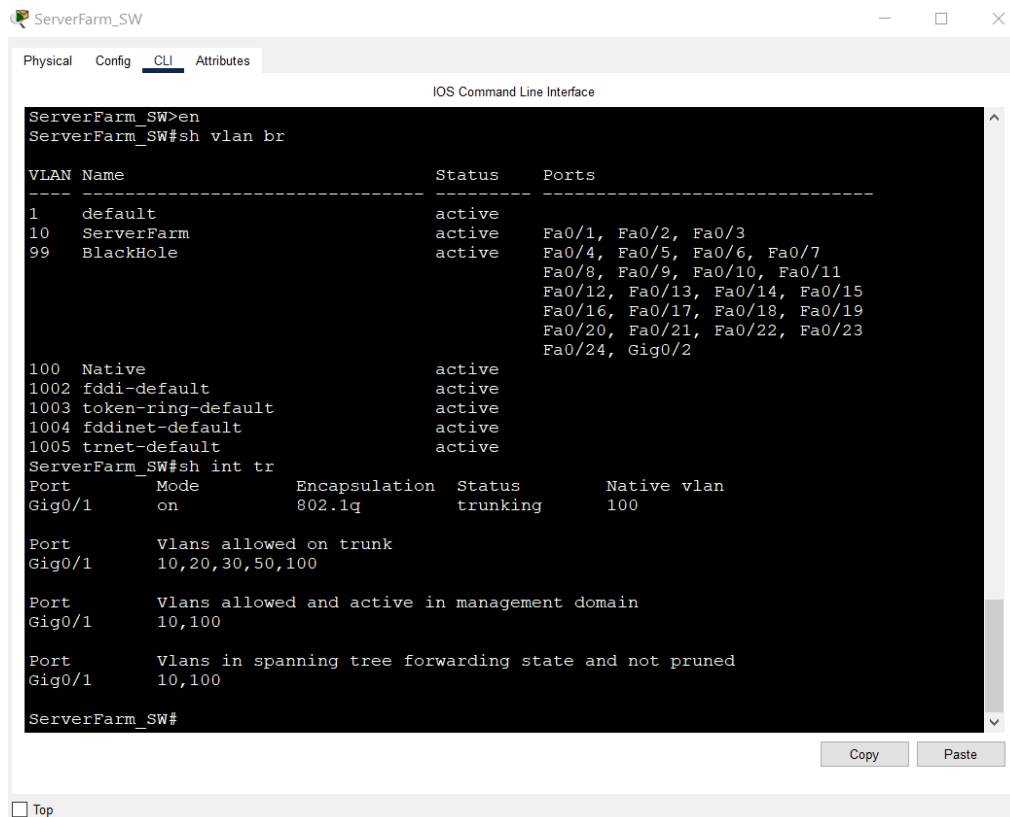


Figure 4: VLANs of Server Farm

## Hanoi VLAN

RB\_SWML

Physical Config CLI Attributes

IOS Command Line Interface

```
1005 trnet-default          active
RB_SWML#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
RB_SWML(config)#int ra g1/0/3-19, g1/1/1-4
RB_SWML(config-if-range)#switchport mode access
RB_SWML(config-if-range)#switchport access vlan 99
RB_SWML(config-if-range)#do sh vlan br

VLAN Name                Status    Ports
-----
1    default                active
10   R&D                     active
99   Blackhole                active    Gig1/0/3, Gig1/0/4, Gig1/0/5, Gig1/0/6
                                           Gig1/0/7, Gig1/0/8, Gig1/0/9, Gig1/0/10
                                           Gig1/0/11, Gig1/0/12, Gig1/0/13, Gig1/0/14
                                           Gig1/0/15, Gig1/0/16, Gig1/0/17, Gig1/0/18
                                           Gig1/0/19, Gig1/1/1, Gig1/1/2, Gig1/1/3
                                           Gig1/1/4
100  Mgmt&Native              active    Gig1/0/1, Gig1/0/2
1002 fddi-default            active
1003 token-ring-default      active
1004 fddinet-default          active
1005 trnet-default            active
RB_SWML(config-if-range)#
```

Figure 5: VLANs of Hanoi

### 3.2 Inter-VLAN Routing

The routing traffic between various VLANs in a network is known as inter-VLAN routing. This allows devices in separate VLANs to communicate, even if they are in different IP subnets (Knobbe, 2021). Inter-VLAN routing provides several benefits, including enhanced network security, improved network performance, and more effective use of network resources. Segmenting traffic by dividing devices into separate VLANs can help contain and isolate security threats. Moreover, inter-VLAN routing can enhance network performance by minimizing the amount of broadcast traffic that devices need to process. This can also aid in optimizing network resources by preventing unnecessary traffic from being sent to devices that don't require it.

### 3.3 Router-on-a-Stick

The router-on-a-stick technique enables a single router to be configured to identify routable VLANs using sub-interfaces. Each sub-interface has its own IP address and VLAN assignment, allowing for logical routing between different subnets. VLAN-tagged traffic is forwarded to the corresponding VLAN sub-interface, and a routing decision is made based on the destination IP network address. This simplifies network configurations, reduces the number of physical interfaces required to support multiple VLANs, and improves network performance, security, and manageability. For example, if an employee in VLAN 10 wants to send a file to another department in VLAN 20 or VLAN 30, the frame is tagged with VLAN 10 and forwarded to the router through a trunk link. The router receives the frame, verifies the destination IP address, and routes the packet to the appropriate VLAN based on the destination IP address. The benefits of this technique include facilitating communication between different VLANs, providing a deeper understanding of VLANs and sub-interfaces, and enhancing network performance and security. However, it has some drawbacks, including the risk of becoming a single point of failure in the network, complicated configuration, and limited realism.

```

ServerFam_Router>en
ServerFam_Router#sh r | s encap
  encapsulation dot1Q 10
  encapsulation dot1Q 30
  encapsulation dot1Q 100 native
ServerFam_Router#sh ip int br

```

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0/0	unassigned	YES	manual	up	up
GigabitEthernet0/0/0.10	198.51.10.1	YES	manual	up	up
GigabitEthernet0/0/0.30	198.51.30.1	YES	manual	up	up
GigabitEthernet0/0/0.100	198.51.100.1	YES	manual	up	up
GigabitEthernet0/0/1	unassigned	YES	unset	administratively down	down
Serial0/1/0	200.100.100.18	YES	manual	up	up
Serial0/1/1	unassigned	YES	unset	administratively down	down
Vlan1	unassigned	YES	unset	administratively down	down

Figure 6: Server Farm Router-on-a-stick

```

00:00:10: %OSPF-5-ADJCHG: Process 10, Nbr 200.100.100.9 on Serial0/1/0 from LOADING to FULL, Loading Done

User Access Verification

Username: Cyberg
Password:

Hanoi_Router>en
Hanoi_Router#sh r | s encap
  encapsulation dot1Q 10
  encapsulation dot1Q 100
Hanoi_Router#sh ip int br

```

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0/0	unassigned	YES	manual	up	up
GigabitEthernet0/0/0.10	192.168.10.1	YES	manual	up	up
GigabitEthernet0/0/0.100	192.168.100.1	YES	manual	up	up
GigabitEthernet0/0/1	unassigned	YES	unset	administratively down	down
Serial0/1/0	200.100.100.6	YES	manual	up	up
Serial0/1/1	200.100.100.1	YES	manual	up	up
Vlan1	unassigned	YES	unset	administratively down	down

Figure 7: Brunei Router Router-on-a-Stick

```

HQ-Router>en
HQ-Router#sh r | s encap
  encapsulation dot1Q 10
  encapsulation dot1Q 20
  encapsulation dot1Q 30
  encapsulation dot1Q 50
  encapsulation dot1Q 100 native
HQ-Router#sh ip int br

```

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0/0	unassigned	YES	manual	up	up
GigabitEthernet0/0/0.10	192.168.10.1	YES	manual	up	up
GigabitEthernet0/0/0.20	192.168.20.1	YES	manual	up	up
GigabitEthernet0/0/0.30	192.168.30.1	YES	manual	up	up
GigabitEthernet0/0/0.50	192.168.50.1	YES	manual	up	up
GigabitEthernet0/0/0.100	192.168.100.1	YES	manual	up	up
GigabitEthernet0/0/1	unassigned	YES	unset	administratively down	down
Serial0/1/0	200.100.100.5	YES	manual	up	up
Serial0/1/1	200.100.100.9	YES	manual	up	up
Vlan1	unassigned	YES	unset	administratively down	down

Figure 8: HQ Router-on-a-Stick

### 3.4 Spanning Tree Protocol

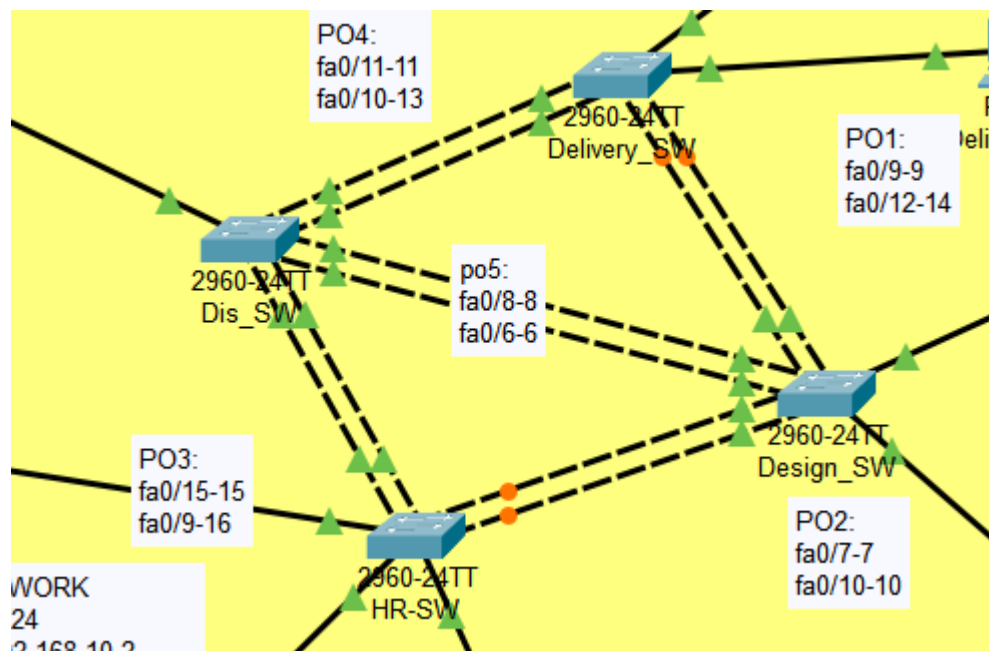


Figure 9: STP network layout

STP the Spanning Tree Protocol a network protocol used to avoid loops in network at a layer 2 network protocol. When there is a loop in a network it can lead to serious consequences such as network redundant, but to avoid this issue we can use STP to alternate or blocked the redundant links at each switch. (Antoniou, 2011). Other than that, if there is a failure of a switch or a cable, STP will detect changes and determine the best path for a network traffic to respond topology changes by ensuring that there is only one active path between network devices.

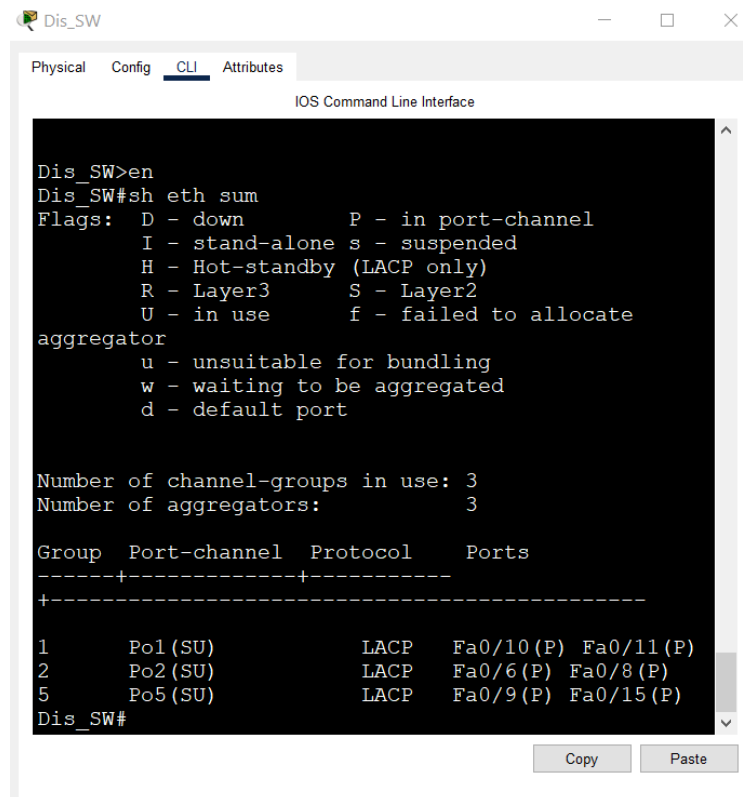
To give an illustration, from the figure above it shows that when the port with amber color it is an alternate port, when the port with green color it is set as a designated ports and the root bridge is at Dis\_SW. The alternate port here is used for blocked state, effectively disabling some redundant port and prevent loop. Whereas the designated ports are selected the most direct route to the root bridge and ensure the data is always forwarded. For the root bridge all the other 3 switches have relation to the switch that have root bridge. When a switch is designated as the root bridge, it means that it has been assigned the lowest bridge ID and MAC address. The bridge ID is calculated by combining the bridge priority with the MAC address, and it is utilized as a means of resolving any ties that may occur when two bridges have the same priority. Therefore, STP is working by electing a root bridge and using port



states to assign the port should be forwarding or blocking the network traffic, and it also help to prevent loops by blocking redundant paths by default.

### 3.5 EtherChannel

A Link Aggregation Protocol (LACP) is an EtherChannel that is viewed as a single logical link, allowing redundant links between devices that are not blocked by STP (section, 2021). In certain situations where there is a requirement for greater bandwidth and redundancy to maintain connectivity between devices, the use of EtherChannel can be advantageous. By merging multiple physical links between switches, EtherChannel can augment the overall speed of communication between switches. However, to prevent switching loops, STP may need to deactivate one of the EtherChannel bundles between two switches. This leads to the complete deactivation of the entire EtherChannel, and all of the ports linked to that EtherChannel. Conversely, when only one EtherChannel link is present, STP views it as a single logical link, enabling all physical EtherChannel links to remain active.



```
Dis_SW>en
Dis_SW#sh eth sum
Flags:  D - down          P - in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby (LACP only)
        R - Layer3       S - Layer2
        U - in use       f - failed to allocate
aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

Number of channel-groups in use: 3
Number of aggregators:          3

Group  Port-channel  Protocol    Ports
-----+-----+-----
+-----+-----+-----
1      Po1 (SU)      LACP       Fa0/10 (P) Fa0/11 (P)
2      Po2 (SU)      LACP       Fa0/6 (P)  Fa0/8 (P)
5      Po5 (SU)      LACP       Fa0/9 (P)  Fa0/15 (P)
Dis_SW#
```

Figure 10: EtherChannel summary for management switch

```

Delivery_SW>en
Delivery_SW#sh eth sum
Flags:  D - down          P - in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby (LACP only)
        R - Layer3       S - Layer2
        U - in use       f - failed to allocate

aggregator
  u - unsuitable for bundling
  w - waiting to be aggregated
  d - default port

Number of channel-groups in use: 2
Number of aggregators:          2

Group  Port-channel  Protocol  Ports
-----+-----+-----
+-----+-----+-----
1      Po1 (SU)      LACP      Fa0/11 (P) Fa0/13 (P)
3      Po3 (SU)      LACP      Fa0/12 (P) Fa0/14 (P)
Delivery_SW#

```

Figure 11: EtherChannel summary for Delivery department

```

Design_SW>en
Design_SW#sh eth sum
Flags:  D - down          P - in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby (LACP only)
        R - Layer3       S - Layer2
        U - in use       f - failed to allocate

aggregator
  u - unsuitable for bundling
  w - waiting to be aggregated
  d - default port

Number of channel-groups in use: 3
Number of aggregators:          3

Group  Port-channel  Protocol  Ports
-----+-----+-----
+-----+-----+-----
2      Po2 (SU)      LACP      Fa0/6 (P)  Fa0/8 (P)
3      Po3 (SU)      LACP      Fa0/12 (P) Fa0/14 (P)
4      Po4 (SU)      LACP      Fa0/7 (P)  Fa0/10 (P)
Design_SW#

```

Figure 12: EtherChannel summary for Design department

```
HR_sw#sh eth sum
Flags:  D - down          P - in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby (LACP only)
        R - Layer3       S - Layer2
        U - in use       f - failed to allocate

aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

Number of channel-groups in use: 2
Number of aggregators:          2

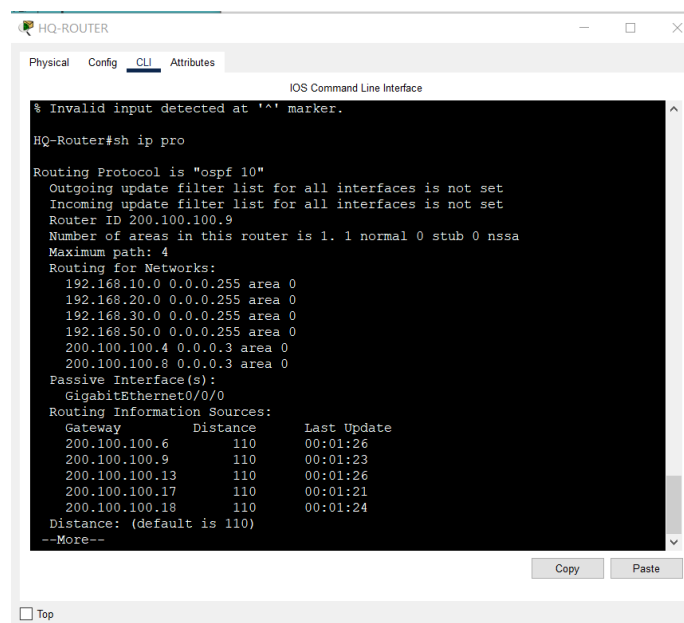
Group  Port-channel  Protocol    Ports
-----+-----+-----
+-----+-----+-----
4      Po4 (SU)          LACP       Fa0/7 (P) Fa0/10 (P)
5      Po5 (SU)          LACP       Fa0/15 (P) Fa0/16 (P)
HR_sw#
```

*Figure 13: EtherChannel summary for HR department*

From figure 17,18,19 & 20, the port-channel status displays the EtherChannel logical interface as a whole. If the port-channel is active, this should display SU (Layer 2 channel in use). Each port within the channel can also be checked for status. The interfaces in the ports category with flags (P) that indicate they are active in the port-channel. One port is visible because it is not physically connected or turned off. If a port is connected but not bundled in a channel, it has an independent flag, or (I) (ccexpert.us, 2023).

### 3.6 OSPF

If the topology changes, the system will automatically find a new best path through dynamic routing protocols to choose the best path. OSPF is widely used in large enterprise networks and the Internet because it can calculate the shortest path between individual routers in a network and has advantages such as fast convergence and scalability. It can handle changes in network topology adaptively, making data transmission in the network more efficient and reliable. OSPF routing protocol stand for **Open Shortest Path First**, which is able to dynamically exchange routing information by finding the path with lowest metric (Aakriti, 2023). The best path is selected by a routing protocol based on the metric, for determine the distance to reach a network and connect to the remote network to find lower values represent preferred routes the Metric is used to identify the assigned value. When performing data transmission, routers need to determine the path of data transmission-based Network ID to identify different networks. OSPF calculates the cost of links based on the cumulative bandwidth between source and destination, with lower-cost links being faster than higher-cost links. The metric used in OSPF for this purpose is called "cost." Since the path is predictability in dynamic routing the routes will depend on topology and routing protocol used. Resources will be usage for CPU, memory, and link bandwidth, for the main purpose of OSPF routing protocol is to dynamically find the best path for forwarding data.



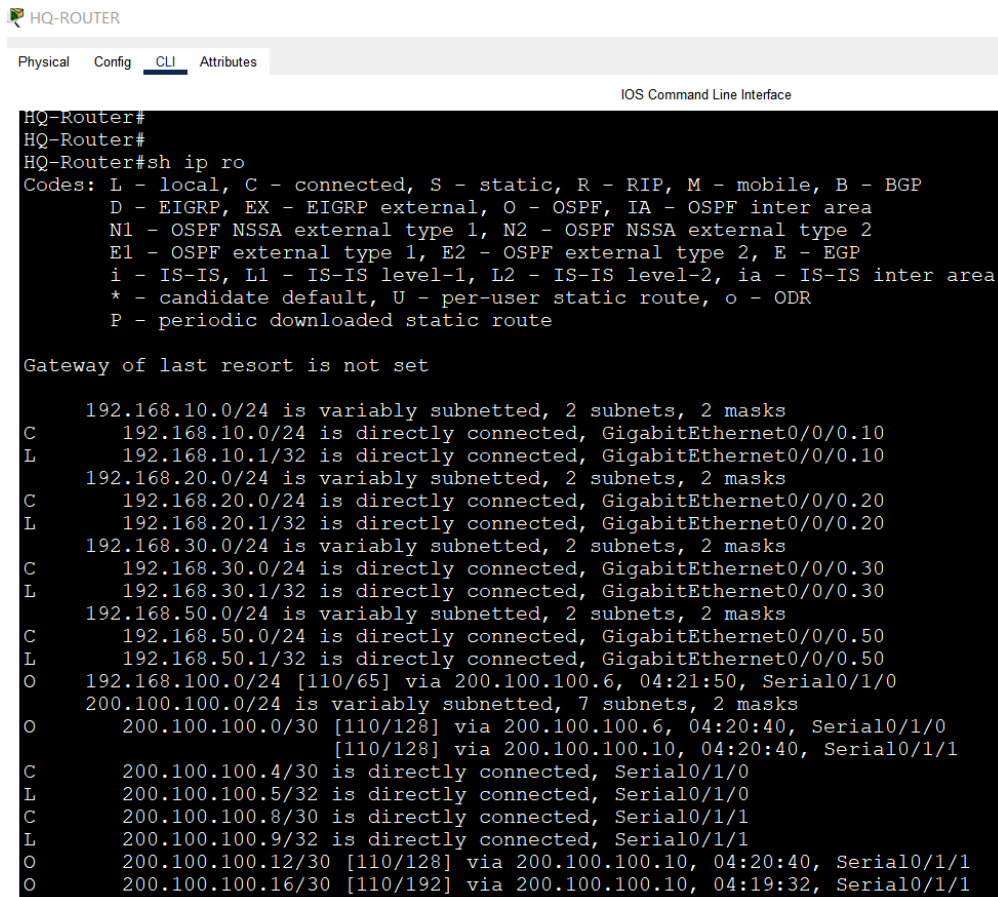
```
Invalid input detected at '^' marker.

HQ-Router#sh ip pro

Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 200.100.100.9
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.10.0 0.0.0.255 area 0
    192.168.20.0 0.0.0.255 area 0
    192.168.30.0 0.0.0.255 area 0
    192.168.50.0 0.0.0.255 area 0
    200.100.100.4 0.0.0.3 area 0
    200.100.100.8 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    200.100.100.6    110          00:01:26
    200.100.100.9    110          00:01:23
    200.100.100.13   110          00:01:26
    200.100.100.17   110          00:01:21
    200.100.100.18   110          00:01:24
  Distance: (default is 110)
  --More--
```

Figure 14: show IP pro

## The IP Routing Table Route Sources



```
HQ-Router#
HQ-Router#
HQ-Router#sh ip ro
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

    192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/0/0.10
L       192.168.10.1/32 is directly connected, GigabitEthernet0/0/0.10
    192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.20.0/24 is directly connected, GigabitEthernet0/0/0.20
L       192.168.20.1/32 is directly connected, GigabitEthernet0/0/0.20
    192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.30.0/24 is directly connected, GigabitEthernet0/0/0.30
L       192.168.30.1/32 is directly connected, GigabitEthernet0/0/0.30
    192.168.50.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.50.0/24 is directly connected, GigabitEthernet0/0/0.50
L       192.168.50.1/32 is directly connected, GigabitEthernet0/0/0.50
O       192.168.100.0/24 [110/65] via 200.100.100.6, 04:21:50, Serial0/1/0
    200.100.100.0/24 is variably subnetted, 7 subnets, 2 masks
O       200.100.100.0/30 [110/128] via 200.100.100.6, 04:20:40, Serial0/1/0
        [110/128] via 200.100.100.10, 04:20:40, Serial0/1/1
C       200.100.100.4/30 is directly connected, Serial0/1/0
L       200.100.100.5/32 is directly connected, Serial0/1/0
C       200.100.100.8/30 is directly connected, Serial0/1/1
L       200.100.100.9/32 is directly connected, Serial0/1/1
O       200.100.100.12/30 [110/128] via 200.100.100.10, 04:20:40, Serial0/1/1
O       200.100.100.16/30 [110/192] via 200.100.100.10, 04:19:32, Serial0/1/1
```

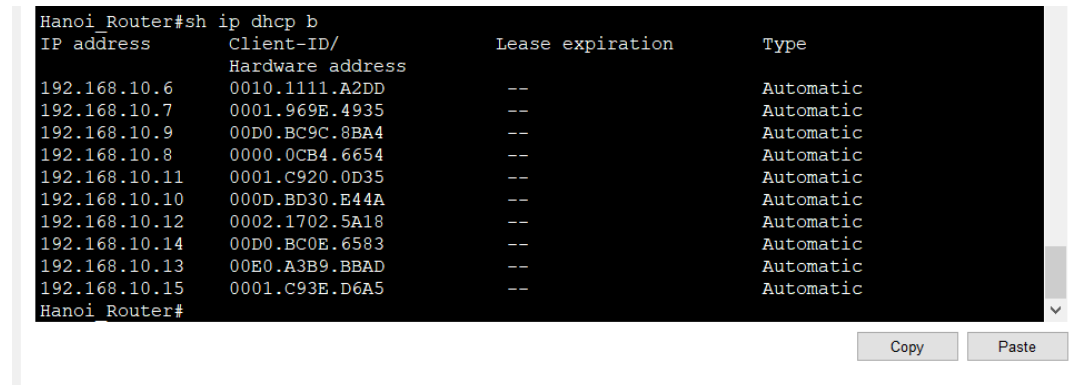
*Figure 15: Routing table of the KL router*

In order to verify the OSPF is configure successfully, one can use command **show ip route**. The L stand for shows the address that has been assigned to a router interface. C stand for indicates a network that is immediately connected. O stand for uses the OSPF routing protocol to recognize a dynamically learned network from another router (ccexpert.us, 2023).

If a route entry is the subnet of a classful address, it is indented (class A, B or C network). The route source, as well as all forwarding information such as the next-hop address, will be included in the child route. This subnet's classful network address will be shown above the route entry, less indented, and without a source code. This is referred to as a parent route.

### 3.7 DHCPv4

The DHCPv4 protocol is managed by a DHCPv4 server, which is responsible for dynamically distributing vital network configuration information to end devices. This information includes IP addresses, subnet masks, DNS server details, and gateway addresses. DHCPv4 is highly beneficial for network devices since it streamlines and automates the process of IP address assignment via the Dynamic Host Configuration Protocol (DHCP), saving a significant amount of time and effort.



```
Hanoi_Router#sh ip dhcp b
IP address      Client-ID/      Lease expiration    Type
                Hardware address
192.168.10.6    0010.1111.A2DD   --                  Automatic
192.168.10.7    0001.969E.4935   --                  Automatic
192.168.10.9    00D0.BC9C.8BA4   --                  Automatic
192.168.10.8    0000.0CB4.6654   --                  Automatic
192.168.10.11   0001.C920.0D35   --                  Automatic
192.168.10.10   000D.BD30.E44A   --                  Automatic
192.168.10.12   0002.1702.5A18   --                  Automatic
192.168.10.14   00D0.BC0E.6583   --                  Automatic
192.168.10.13   00E0.A3B9.BBAD   --                  Automatic
192.168.10.15   0001.C93E.D6A5   --                  Automatic
Hanoi_Router#
```

Copy Paste

*Figure 1: DHCPv4 implementation and the binding list*

Additionally, as seen from figure above in this new network design we do not have set the lease expire the leased so that the client does not have to worry about renewing the leased IP address. One of things need to be considered is most DHCP servers by default will assign an IP address to a client for a specific period of time, usually around 24 hours, but this can be configured to a different value. When a DHCP lease expires, request a new IP address assignment from the DHCP server. If it is unable to renew its lease, it will lose network connectivity until a new IP address is obtained (SoftwareKeep, n.d.).

```

Hanoi_Router#sh ip dhcp pool

Pool RBM-Wireless :
Utilization mark (high/low)      : 100 / 0
Subnet size (first/next)          : 0 / 0
Total addresses                   : 254
Leased addresses                  : 10
Excluded addresses                : 2
Pending event                     : none

1 subnet is currently in the pool
Current index      IP address range      Leased/Excluded/Total
192.168.10.1      192.168.10.1 - 192.168.10.254  10 / 2 / 254

```

*Figure 17: verify the DHCPv4*

In order to keep some IPs from being sent out, we can use the **ip dhcp pool excluded-addresses <ip>** command. Therefore, as can be seen from the figure above there will be 2 excluded IP addresses. The IP addresses will be theoretically available for 252 to allocate the subnet mask configuration, and the IP address range is between 192.168.10.1 to 192.168.10.254.

#### **4.0 Deployment of Layer 2 Security Mechanisms in Configuration**

Deployment of Layer 2 Security Mechanisms in Configuration are designed to protect the Data Link layer from various types of attacks in switches, such as STP attacks, MAC Spoofing, VLAN Hopping and DHCP Spoofing (Pearson IT Certification , n.d.). By applying the Layer 2 security mechanisms in a switch, it can enhance their overall security status and reduce the risk of cyberattacks. Port security, Mac addresses filtering, VLANs, STP and DHCP can be applied in a switch for layer 2 security mechanism. Deploying layer 2 security mechanisms in switch, on the other hand, can have an impact on a router's packet forwarding function by adding additional processing and authentication steps, which can slow down the encapsulation process. Furthermore, these security measures are required to ensure the integrity and confidentiality of data transmitted over a network. As a result, when configuring layer 2 security mechanisms on a switch, it is critical to strike a balance between security and performance.



## 4.1 Mitigation VLAN attacks

In order to mitigate these VLAN attacks, it is recommended to reduce the frequency of DTP Hello Packets, set the Dynamic Trunking Timeout to a lower value and set zero interfaces using DTP.

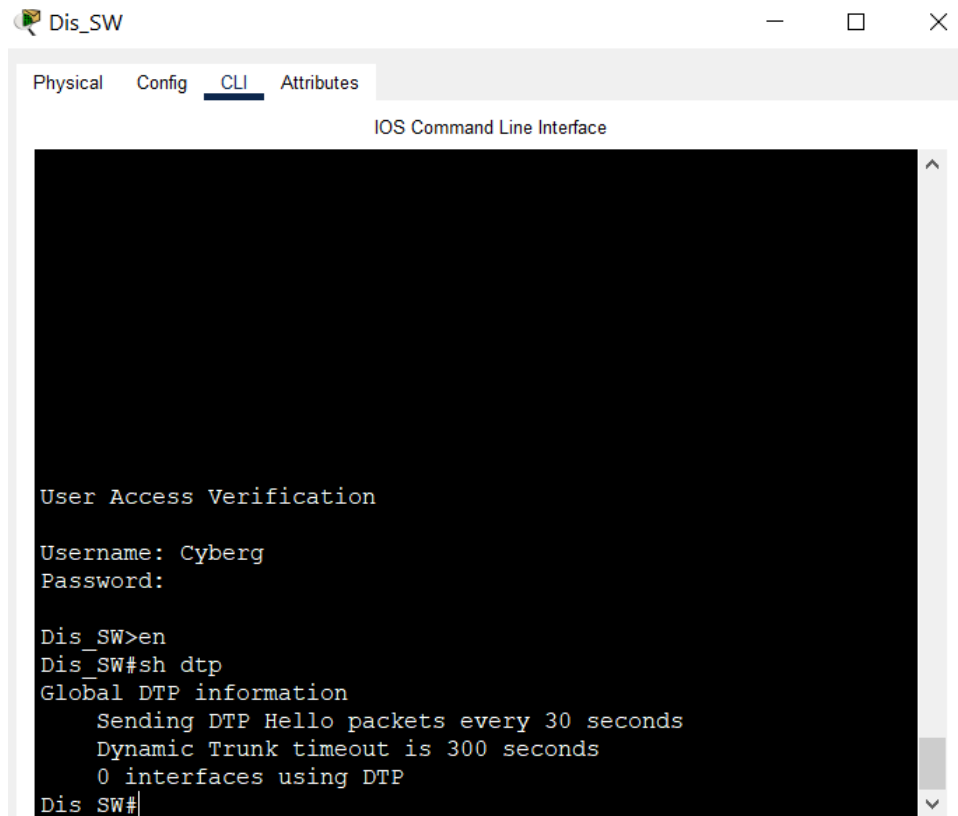


Figure 18: DTP details for management switch

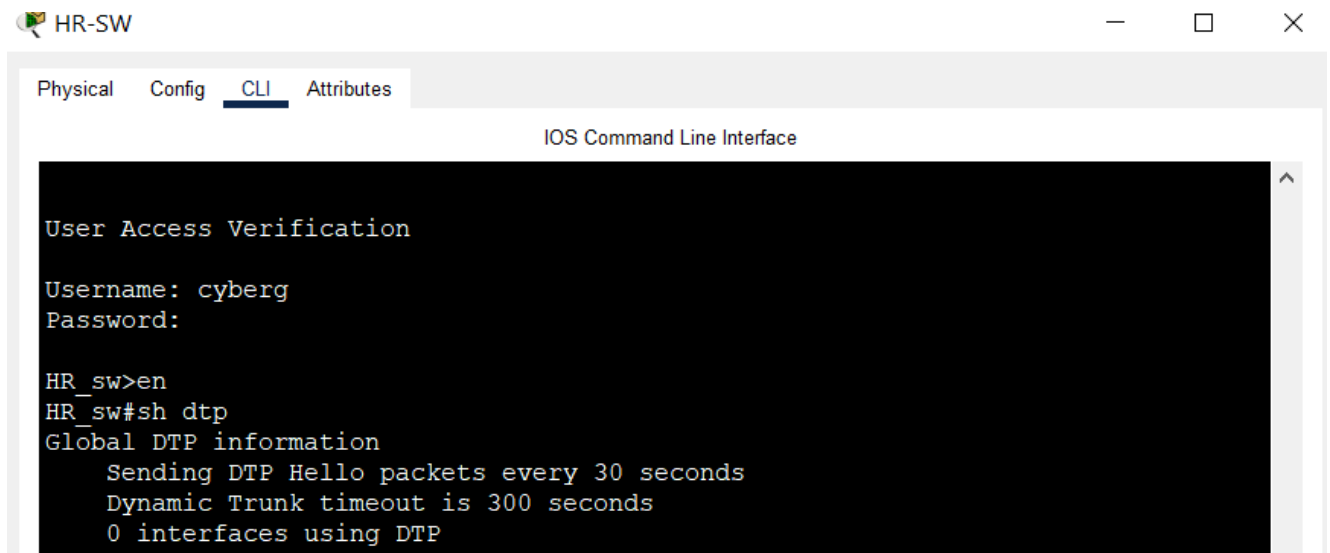
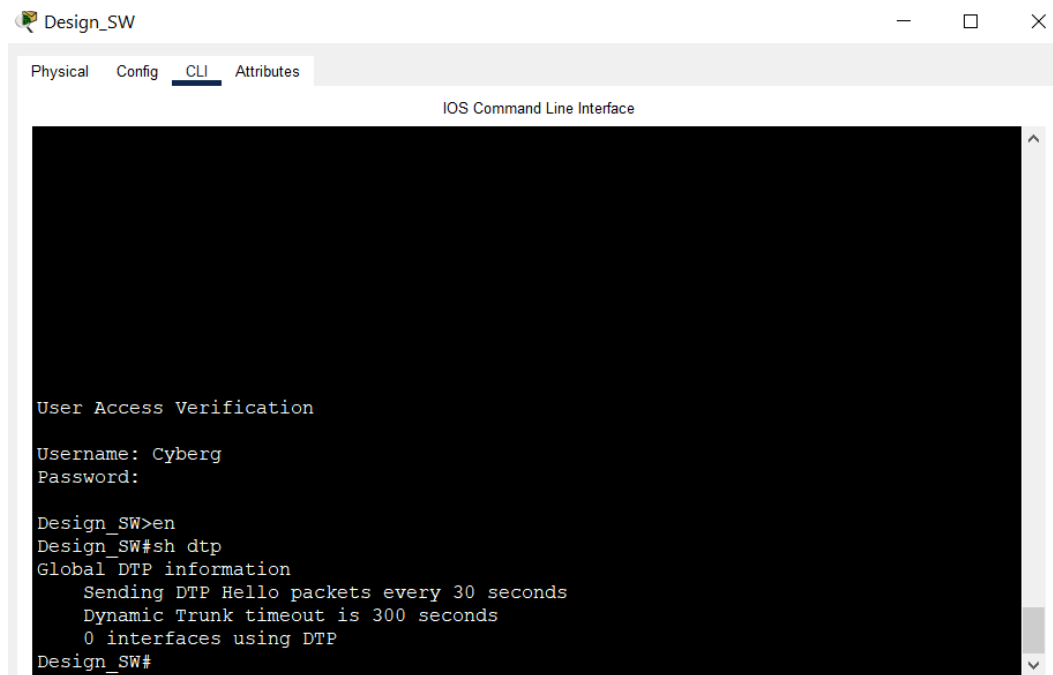
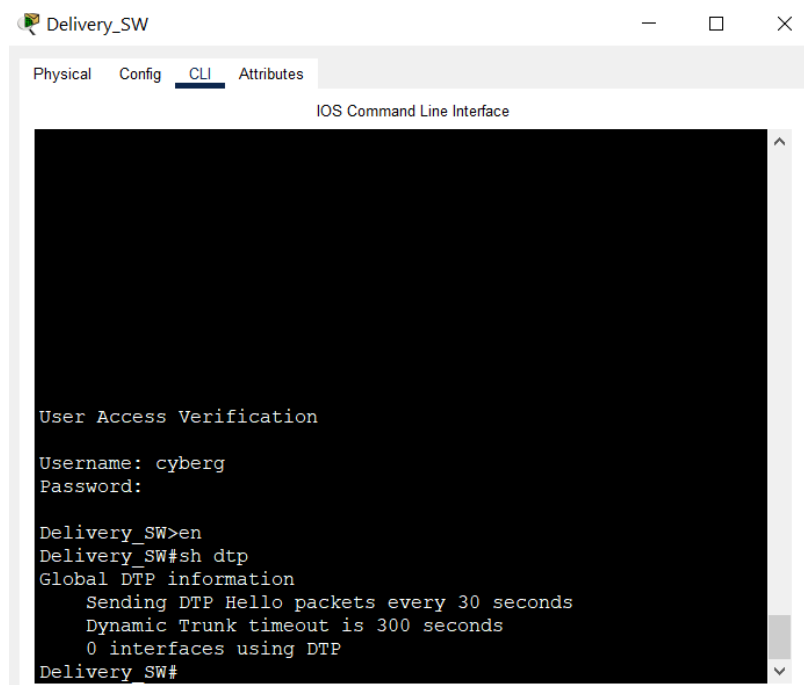


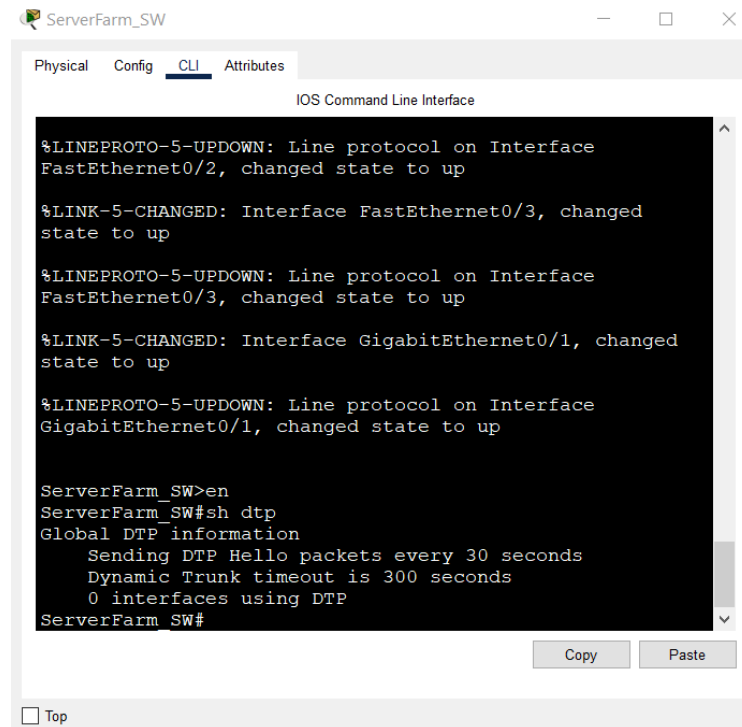
Figure 19: DTP details for HR switch



*Figure 20: DTP details for Design switch*



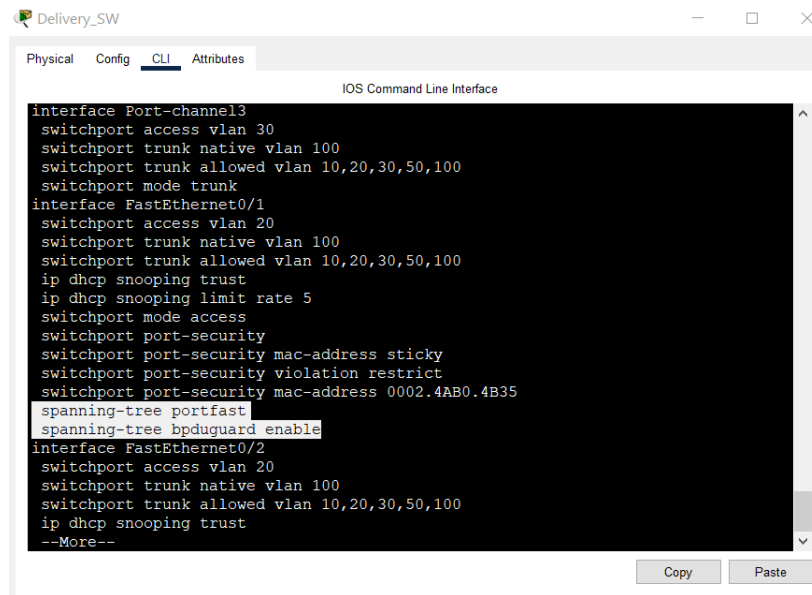
*Figure 21: DTP details for Delivery switch*



*Figure 22: DTP details for Server Farm*

## 4.2 Mitigation STP attacks

In order to mitigate the STP attacks, it is important to configure PortFast and BPDU Guard to enable on access port. It is usually used in conjunction with BPDU protection, so that when the port receives a BPDU, it immediately shuts down. When PortFast is in access mode, the various STP states are bypassed. It basically goes from blocking to forwarding. If the port continues to receive BPDUs, it indicates that a user has connected a switch rather than his PC, which could result in a loop. This is where BPDU GUARD can help. If BPDUs are received on a fast port, the port is immediately disabled and a message of this type is displayed on the console (Soulages, 2023).



The screenshot shows a network switch configuration window titled "Delivery\_SW" with tabs for Physical, Config, CLI, and Attributes. The CLI tab is active, displaying the "IOS Command Line Interface". The configuration includes:

```
interface Port-channel3
 switchport access vlan 30
 switchport trunk native vlan 100
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
interface FastEthernet0/1
 switchport access vlan 20
 switchport trunk native vlan 100
 switchport trunk allowed vlan 10,20,30,50,100
 ip dhcp snooping trust
 ip dhcp snooping limit rate 5
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address 0002.4AB0.4B35
 spanning-tree portfast
 spanning-tree bpduguard enable
interface FastEthernet0/2
 switchport access vlan 20
 switchport trunk native vlan 100
 switchport trunk allowed vlan 10,20,30,50,100
 ip dhcp snooping trust
--More--
```

Buttons for "Copy" and "Paste" are visible at the bottom right of the CLI window.

Figure 23: verify delivery switch STP bpduguard enable and portfast.

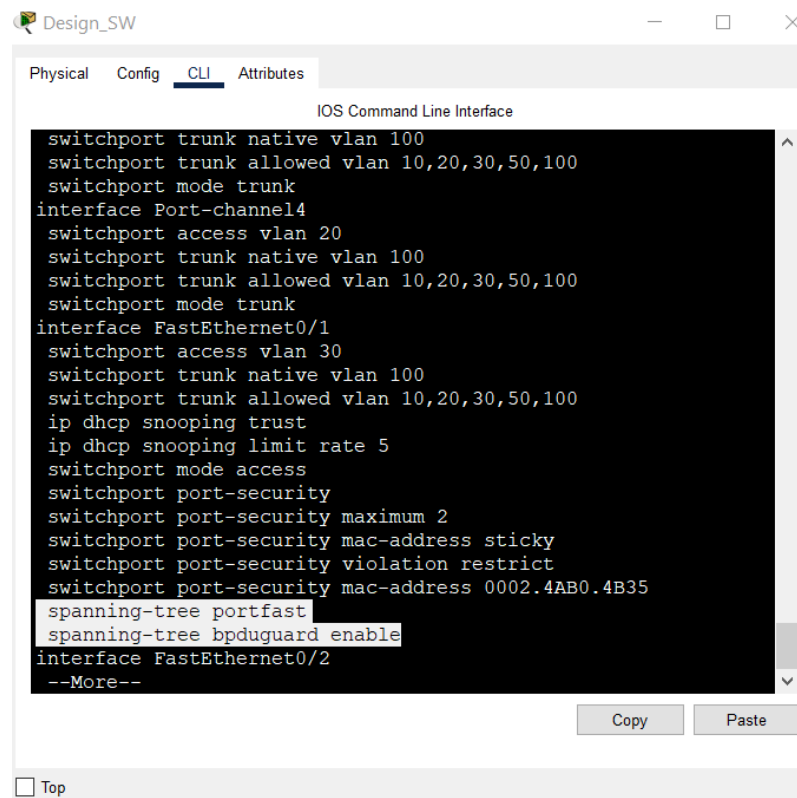


Figure 24: verify design switch STP bduguard enable and portfast

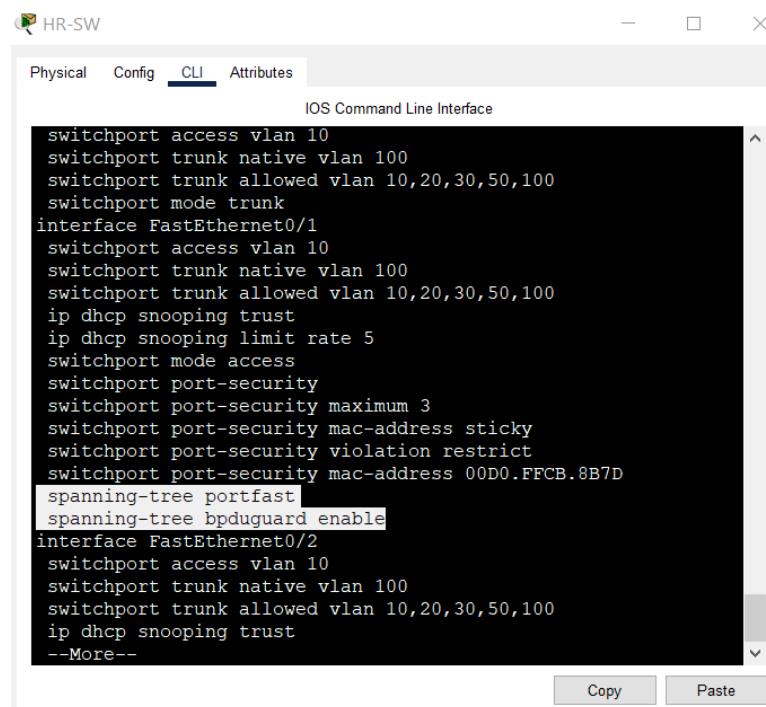


Figure 2: verify HR switch STP bduguard enable and portfast

### 4.3 Mitigation DHCP attacks

```
Delivery_SW(config)#do sh ip dhcp sno
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10,20,30,50,99
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                Trusted      Rate limit (pps)
-----
FastEthernet0/1          yes         5
FastEthernet0/2          yes         5
```

Figure 26: the list of Ip DHCP snooping of delivery switch

```
Design_SW(config)#do sh ip dhcp sno
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10,20,30,50,99
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                Trusted      Rate limit (pps)
-----
FastEthernet0/1          yes         5
FastEthernet0/2          yes         5
```

Figure 27: the list of Ip DHCP snooping of design switch

```
HR_sw(config-if-range)#ip dhcp sno vlan 10,20,30,50,99
HR_sw(config)#do sh ip dhcp sno
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10,20,30,50,99
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                Trusted      Rate limit (pps)
-----
FastEthernet0/3          yes         5
FastEthernet0/1          yes         5
FastEthernet0/2          yes         5
```

Figure 3: the list of Ip DHCP snooping of HR switch

DHCP attacks can be a serious threat to network security as they can allow unauthorized devices to gain access to the network and potentially compromise sensitive data. A DHCP starvation attack is utilized by attackers to flood the DHCP server with requests, depleting all of the available IP addresses. As a result, the server becomes incapable of assigning any more IP addresses, causing a denial-of-service (DoS) attack that prevents new clients from accessing the network (ProSec, n.d.). The presence of an unauthorized DHCP server can result in DHCP clients being assigned incorrect IP addresses and network configuration settings, which may cause communication issues and potential network downtime. To facilitate the acquisition of IP addresses by DHCP clients from legitimate DHCP servers, the activation of DHCP Snooping security mechanism is essential. It permits the classification of ports into trusted and untrusted ones, limiting the transmission of DHCP packets exclusively from authorized ports and ensuring the genuineness of DHCP packets. This feature intercepts all DHCP messages and verifies the source IP address of the server to ensure that only authorized DHCP servers are used. The settings for the DHCP relay Option 82 command are omitted when snooping is controlling Option 82 insertion when DHCP is enabled globally and also on a VLAN, and the switch is functioning as a DHCP relay.

## 4.4 Mitigation MAC Address Table Flooding Attacks

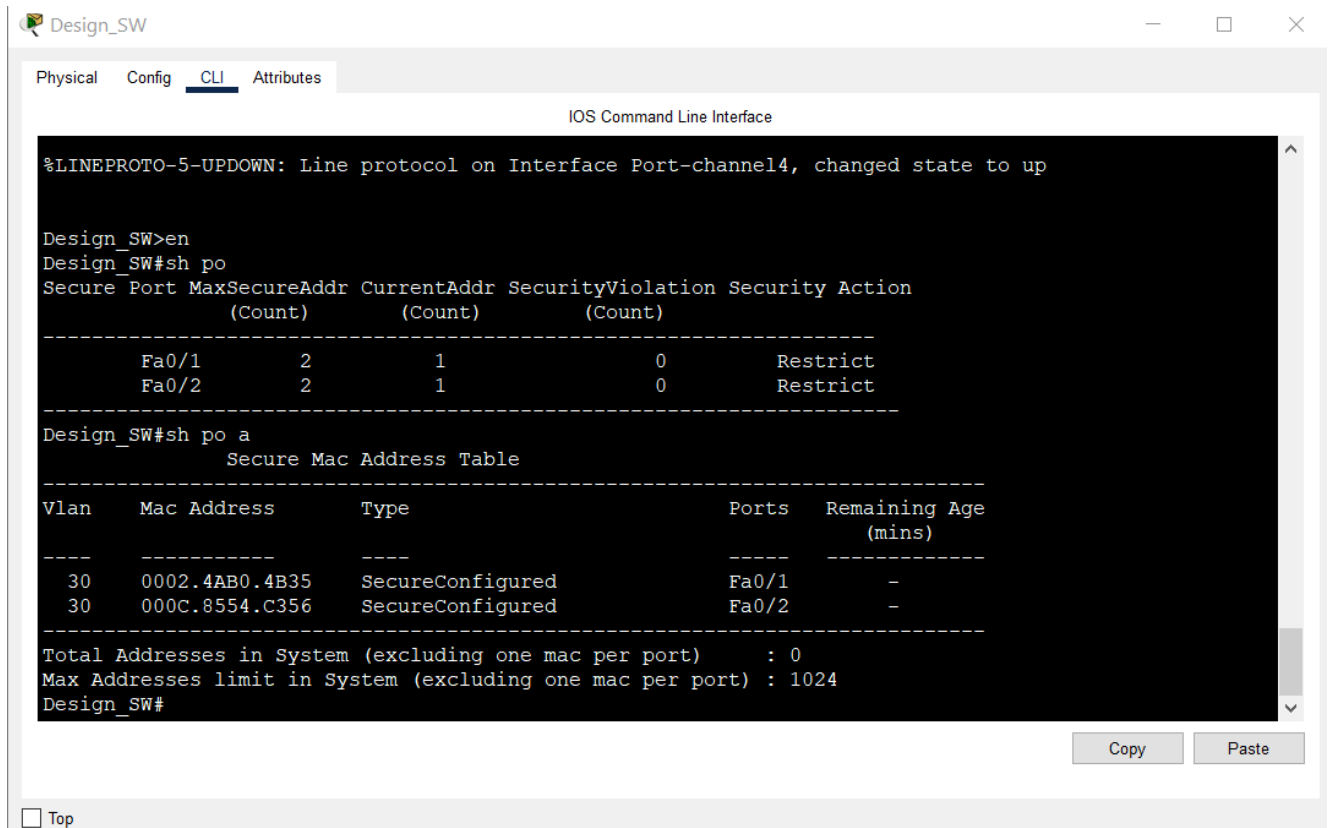


Figure 29: port security for Design switch

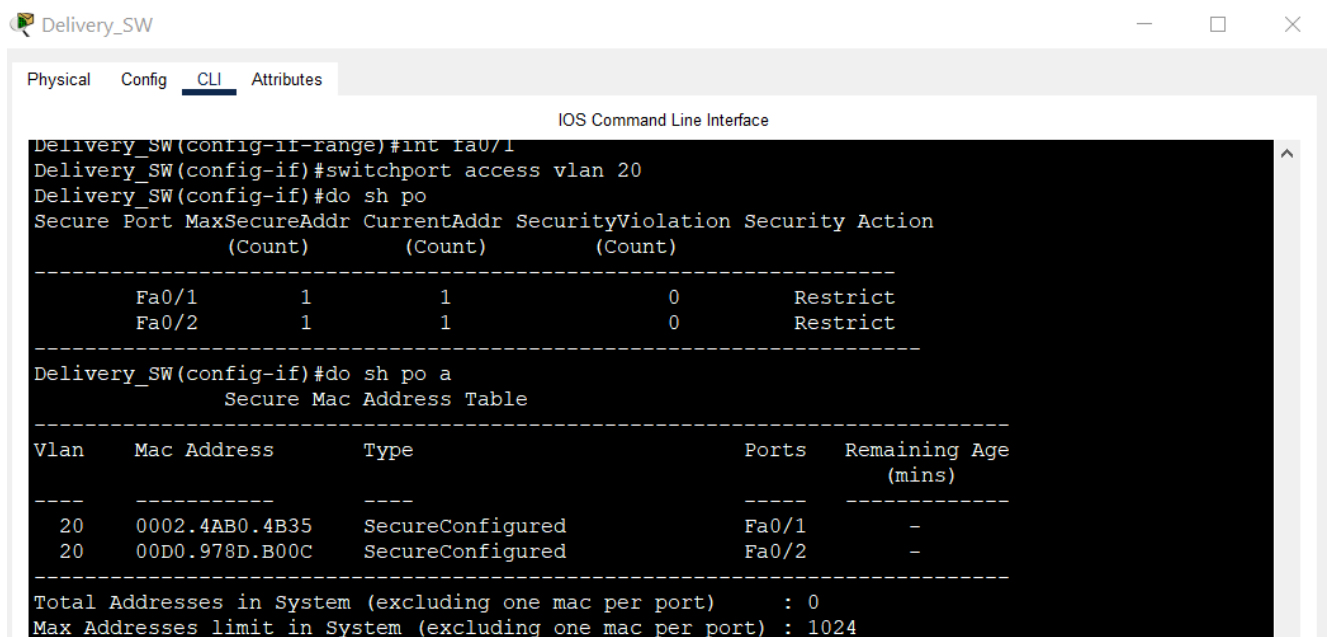


Figure 30: port security for Delivery switch



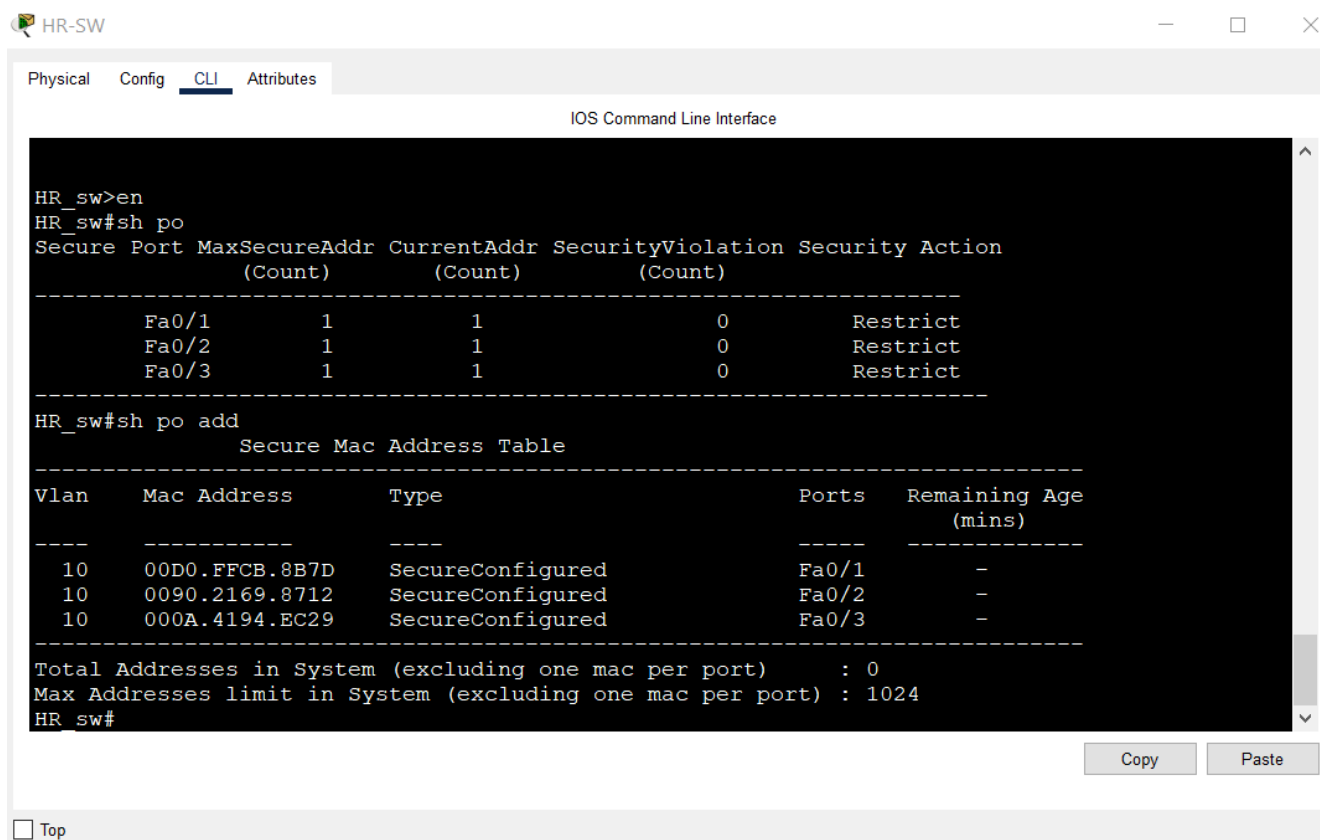


Figure 31: port security for HR switch

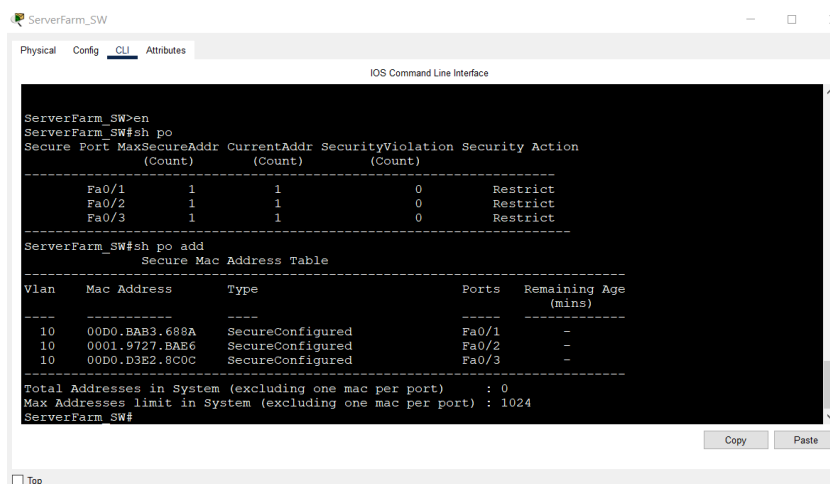


Figure 32: port security for Server Farm switch

```

RB_SWML(Physical) Config CLI Attributes
IOS Command Line Interface
RB_SWML(config-if)#switchport port-security maximum 4
RB_SWML(config-if)#switchport port-security violation restrict
RB_SWML(config-if)#switchport port-security mac-address sticky
RB_SWML(config-if)#switchport port-security mac-address 0030.F203.53C4
RB_SWML(config-if)#switchport access vlan 100
RB_SWML(config-if)#do sh po
% Ambiguous command: "sh po"
RB_SWML(config-if)#do show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
          (Count)          (Count)          (Count)
-----
Gig1/0/1      4              1              0      Restrict
-----
RB_SWML(config-if)#do show port-security address
Secure Mac Address Table
-----
Vlan  Mac Address      Type                Ports  Remaining Age
(mins)
-----
100   0030.F203.53C4    SecureConfigured    Gig1/0/1  -
-----
Total Addresses in System (excluding one mac per port)  : 0
Max Addresses limit in System (excluding one mac per port) : 1024
RB_SWML(config-if)#

```

Copy Paste

Top

*Figure 33: port security for RB multilayer switch*

Port security can be used to limit the number of MAC addresses (NETGEAR, 2016). Enable MAC Address Limit some network switches allow the configuration of maximum MAC address limits per port, VLAN, or per switch to prevent overloading the switch's MAC address table. In general, the "restrict" violation mode is a good choice for mitigating MAC address flooding attacks because it allows the switch to operate normally while still alerting the administrator.

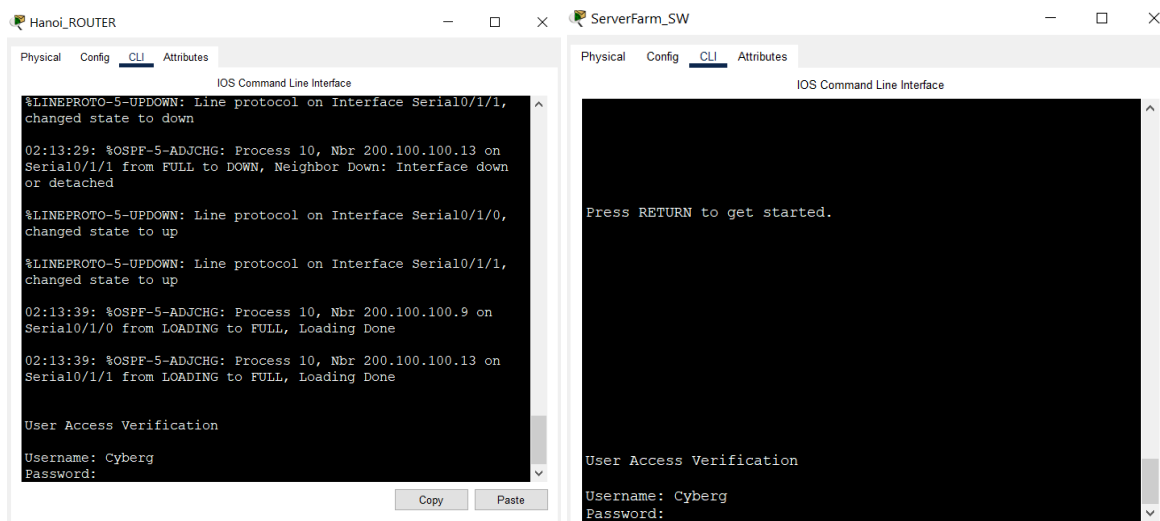
## SSH configuration

Secure Shell Protocol (SSH) is an encrypted network protocol used to securely transmit data over an insecure network based on the cryptography method. It is a remote login protocol that allows users to remotely connect to another network through an encrypted connection in a terminal on routers and switches. SSH provides a high level of security while protecting sensitive data and allows users to perform various tasks and operations on remote network configuration. Through the SSH connection in the terminal, one can execute commands and operations on routers and switches, which is very useful for manage network securely (geeksforgeeks, 2021).

```
Hanoi_Router>en
Hanoi_Router#sh r | s ssh
ip ssh version 2
transport input ssh
transport input ssh
```

*Figure 34: SSH details for Hanoi Router*

The SSHv2 client, with authentication and encryption, enables secure communication over an insecure network.



*Figure 35: Hanoi Router & ServerFarm switch SSH*

All SSH connections on this network are configured with User Access Verification. User Access Verification is required when a user first accesses the terminal, as shown in the figures above. Before being able to edit on the terminal, this SSH configuration it requires to enter a username "**Cyberg**" and password "**01234**". Access to the terminal will be denied if an invalid username or password is entered.

## Conclusion

In conclusion, the entire network layout of the new MicroTech Sdn Bhd network is managed through LAN and WAN configurations. Implemented security measures, including BPDU, port security, VLAN, and DHCP snooping help ensure the security and integrity of the network. However, it is important to note that no security measures are foolproof and require constant monitoring and maintenance to ensure the network remains secure. The use of VLAN helps to segment the network and improve network performance by reducing network congestion and optimizing traffic flow. However, VLAN configuration and management can also be complex and require careful planning and monitoring to ensure they are implemented correctly. When one of the routers goes down, the other routers can't depend on the other routers, which will be a challenge, for I did not configure the HSRP for the new network.

## References

- Aakriti. (2023, January 9). Retrieved from [https://www.nwking.com/what-is-ospf-protocol-in-networking#How\\_OSPF\\_Works](https://www.nwking.com/what-is-ospf-protocol-in-networking#How_OSPF_Works)
- Antoniou, S. (2011, September 28). Retrieved from <https://www.pluralsight.com/blog/software-development/spanning-tree-protocol-tutorial>
- Antoniou, S. (2022, November 18). Retrieved from <https://www.pluralsight.com/blog/tutorials/cisco-ccna-vlan>
- ccexpert.us. (2023, January 16). Retrieved from <https://www.ccexpert.us/root-bridge/troubleshooting-an-etherchannel.html>
- ccexpert.us. (2023, Feb 10). Retrieved from <https://www.ccexpert.us/routing-table/verifying-the-ospf-configuration.html>
- geeksforgeeks. (2021, August 16). Retrieved from <https://www.geeksforgeeks.org/how-to-configure-ssh-on-cisco-routers-and-switches/>
- geeksforgeeks. (2022, Oct 11). Retrieved from <https://www.geeksforgeeks.org/what-is-dhcpv4-operation/>
- Kaspersky. (n.d.). Retrieved from <https://www.kaspersky.com/resource-center/definitions/what-is-an-ip-address>
- Knobbe, D. (2021, November 18). Retrieved from <https://info.pivtglobal.com/resources/inter-vlan-routing-configuration-guide-for-cisco>
- NETGEAR. (2016, November 28). Retrieved from <https://kb.netgear.com/21786/What-is-port-security-and-how-does-it-work-with-my-managed-switch>
- Pearson IT Certification . (n.d.). Retrieved from <https://www.pearsonitcertification.com/articles/article.aspx?p=2491767>
- ProSec. (n.d.). Retrieved from <https://www.prosec-networks.com/en/blog/dhcp-starvation-attack/>
- section. (2021, May 10). Retrieved from <https://www.section.io/engineering-education/etherchannel-technology/>
- SHAH, S. (2022, Feb 11). Retrieved from <https://goteleport.com/blog/comparing-passwordless-ssh-authentication-methods/>
- SoftwareKeep. (n.d.). Retrieved from <https://softwarekeep.com/help-center/what-is-dhcp-lease-time-and-how-does-it-work>
- Soulages, P. D. (2023, January 14). Retrieved from <https://formip.com/en/portfast-and-bpdu-guard-spanning-tree-loop/>
- techhub. (n.d.). Retrieved from [https://techhub.hpe.com/eginfolib/networking/docs/switches/RA/15-18/5998-8151\\_ra\\_2620\\_asg/content/ch11s02.html](https://techhub.hpe.com/eginfolib/networking/docs/switches/RA/15-18/5998-8151_ra_2620_asg/content/ch11s02.html)
- WELEKWE, A. (2023, January 20). Retrieved from <https://www.comparitech.com/net-admin/inter-vlan-routing-configuration/>