INDIVIDUAL ASSIGNMENT

CT133-3-2-SRE

SWITCHING AND ROUTING ESSENTIALS

APU2F2111CS (CYB), APD2F2111CS (CYB)

HAND OUT DATE: 29th November 2021

HAND IN DATE: 27th February 2022

Weightage: 40%

Online Submission Time before = 12: 59 PM

Student Name: Lee Jun Lam [Section B]

Student ID: TP055697

INSTRUCTIONS TO CANDIDATES:

1. Assignment is to be submitted through online submission (Moodle).
2. Students are advised to underpin their answers with the use of references (cited using the Harvard Name System of Referencing).
3. Late submission will be awarded zero (0) unless Extenuating Circumstances (EC) are upheld.
4. Cases of plagiarism will be penalized.
5. You must obtain 50% overall to pass this module.

Table of Contents

Section B: Report and Packet Tracer

1.0 Introduction

1.1. Company's Background

A fiber optic firm named Fiberoptic Systems Inc. has declared a planning to expand its services and locations in numerous locations (Remote Office Branch) and online (Remote Branch).

1.2. Objectives

A representative from the firm, Fiberoptic Systems Inc has request the network executive to work on the new network's design and prototype in accordance with the network logical topology specified in the Cisco Packet Tracer's network request. The client's requests, such as various VLANs for each department in each branch, security methods such as implement port security to mitigate LAN attacks and MAC address table attacks, and a wireless network topology by implementing DHCPv4 to operate across multiple LANs for Cyberjaya Remote Branch, must be included in the prototype network. End devices, such as desktops and laptops from the HQ branch and the Cyberjaya Remote Branch, must be able to connect with one another and with the server farm. Any further detail about any additional features or security mechanisms will be updates and further stated in the report.

1.3. Assumptions

The initial design of Fiberoptic Systems Inc does not implement multiples VLANs. Thus, this prototype design will implement multiples VLANs due to the client's request. Additional configuration such as Inter VLAN Routing (Router on the stick), Open shortest path first (OSPF), Layer 2 Redundancy (Spanning-tree protocol), Link-aggregation technology will be implemented to fulfill LAN and WAN Configuration in order to expand its services and locations in numerous locations.

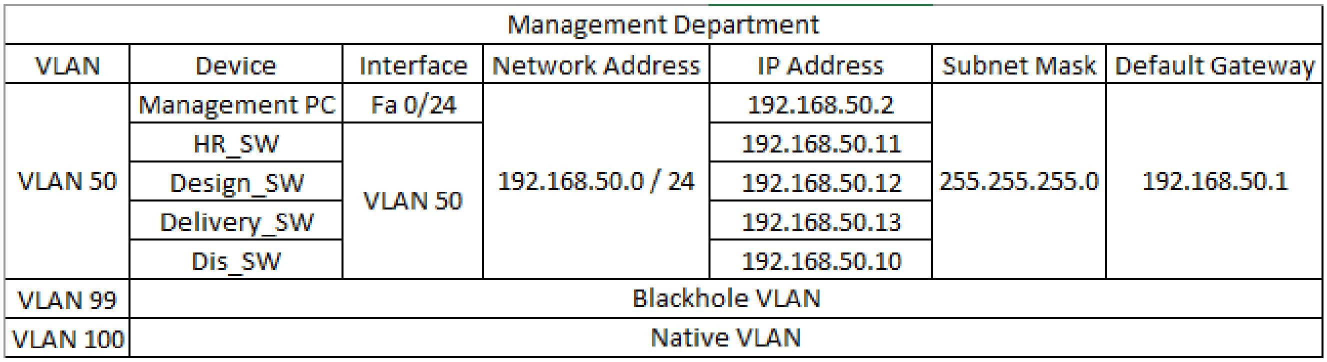
2.0 IP Addressing Table

An IP address, which is a unique address, is used to identify devices on the Internet or in local area networks. The Internet Protocol (IP) is a collection of rules that control data transmission across the Internet and local area networks. In other words, an IP address is a unique identification that enables data to be sent between devices on a network. The IP address holds information about the device's location, which allows it to interact. Different computers, routers, and webpages all need to be distinguished on the Internet. IP addresses are a crucial part of how the Internet functions and give a means to do this. There are two types of IP addresses used by Fiberoptic System Inc.: static IP addresses and dynamic IP addresses (Cyberjaya remote branch only).

Dynamic IP addresses are those that change on a regular basis. ISPs buy a large pool of IP addresses and automatically assign them to their customers. They re-assign them on a regular basis, and the older IP addresses are returned to the pool for use by other customers. Because IP addresses are often shifted, the purpose of this strategy is to save money for the ISP by avoiding the need for additional operations to re-establish a customer's IP address whenever they move residence. There are also security benefits; changing IP addresses makes it more difficult for hackers to get access to the company's network interface. In contrast to dynamic IP addresses, static IP addresses are fixed once an IP address is assigned by the network. For businesses that wish to run their own server, static IP addresses are essential. This is because a static IP address ensures that the websites and email addresses linked with it have a consistent IP address, which is required if other devices are to consistently locate them on the internet. (Kaspersky, n.d.).

2.1 Headquarter (HQ) IP addressing Table

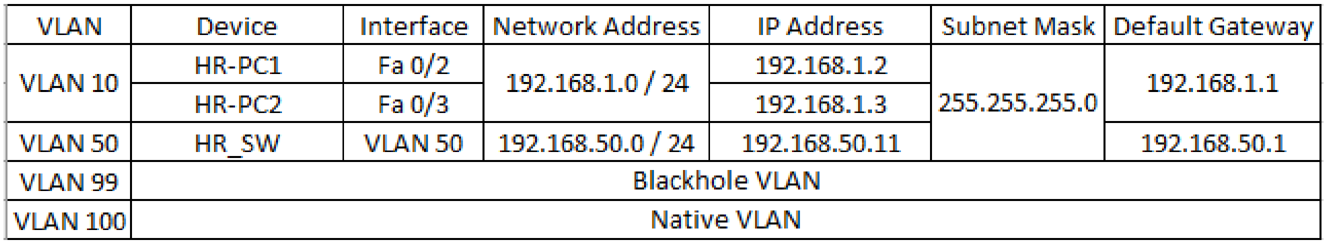
The headquarter (HQ) network is located in KL and it is split into 4 departments which are the Management Department, Human Resources (HR) Department, Design Department and Delivery Department. The IP Addressing Table will be divided according to the respective department.



Management Department						
VLAN	Device	Interface	Network Address	IP Address	Subnet Mask	Default Gateway
VLAN 50	Management PC	Fa 0/24	192.168.50.0 / 24	192.168.50.2	255.255.255.0	192.168.50.1
	HR_SW	VLAN 50		192.168.50.11		
	Design_SW			192.168.50.12		
	Delivery_SW			192.168.50.13		
	Dis_SW			192.168.50.10		
VLAN 99	Blackhole VLAN					
VLAN 100	Native VLAN					

Figure 1: IP addressing table for Management Department

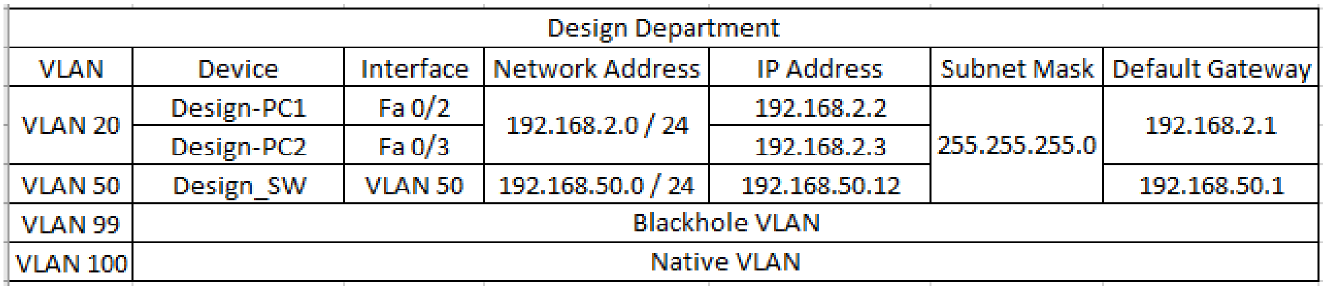
Management Department has been assigned to VLAN 50 and each host devices such as end device (PC) and switches has been configured with static IP Address respectively alongside with the same default gateway due to same VLAN. Any unused port will be administrative shutdown and assigned to VLAN 99 (Blackhole VLAN) for security enhancement purpose and the trunk ports has been configured to VLAN 100 (Native VLAN).



VLAN	Device	Interface	Network Address	IP Address	Subnet Mask	Default Gateway
VLAN 10	HR-PC1	Fa 0/2	192.168.1.0 / 24	192.168.1.2	255.255.255.0	192.168.1.1
	HR-PC2	Fa 0/3		192.168.1.3		
VLAN 50	HR_SW	VLAN 50	192.168.50.0 / 24	192.168.50.11		192.168.50.1
VLAN 99	Blackhole VLAN					
VLAN 100	Native VLAN					

Figure 2: IP addressing table for Human Resource (HR) Department

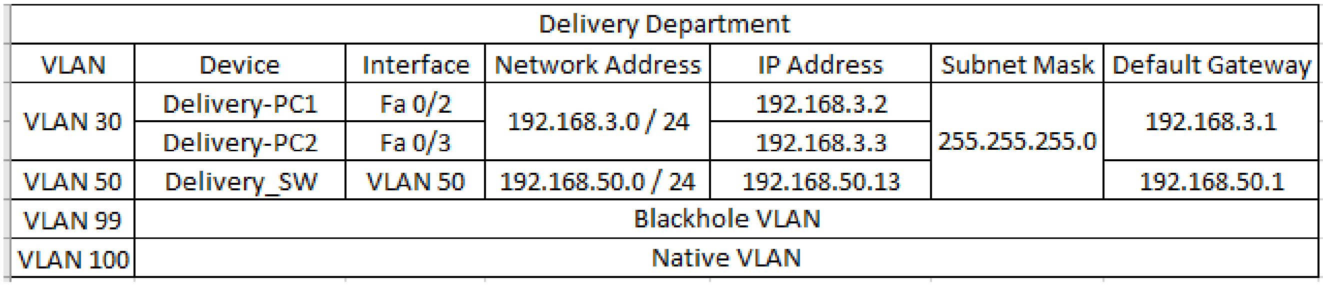
Huma Resource Department has been assigned to VLAN 10 while HR_SW has been assigned to VLAN 50 due to the switch is part of management VLAN. Each host devices such as end device (PC) and has been configured with static IP Address respectively alongside with the same default gateway due to same VLAN. Any unused port will be administrative shutdown and assigned to VLAN 99 (Blackhole VLAN) for security enhancement purpose and the trunk ports has been configured to VLAN 100 (Native VLAN).



Design Department						
VLAN	Device	Interface	Network Address	IP Address	Subnet Mask	Default Gateway
VLAN 20	Design-PC1	Fa 0/2	192.168.2.0 / 24	192.168.2.2	255.255.255.0	192.168.2.1
	Design-PC2	Fa 0/3		192.168.2.3		
VLAN 50	Design_SW	VLAN 50	192.168.50.0 / 24	192.168.50.12		192.168.50.1
VLAN 99	Blackhole VLAN					
VLAN 100	Native VLAN					

Figure 3: IP addressing table for Design Department

Design Department has been assigned to VLAN 20 while Design_SW has been assigned to VLAN 50 due to the switch is part of management VLAN. Each host devices such as end device (PC) and has been configured with static IP Address respectively alongside with the same default gateway due to same VLAN. Any unused port will be administrative shutdown and assigned to VLAN 99 (Blackhole VLAN) for security enhancement purpose and the trunk ports has been configured to VLAN 100 (Native VLAN).



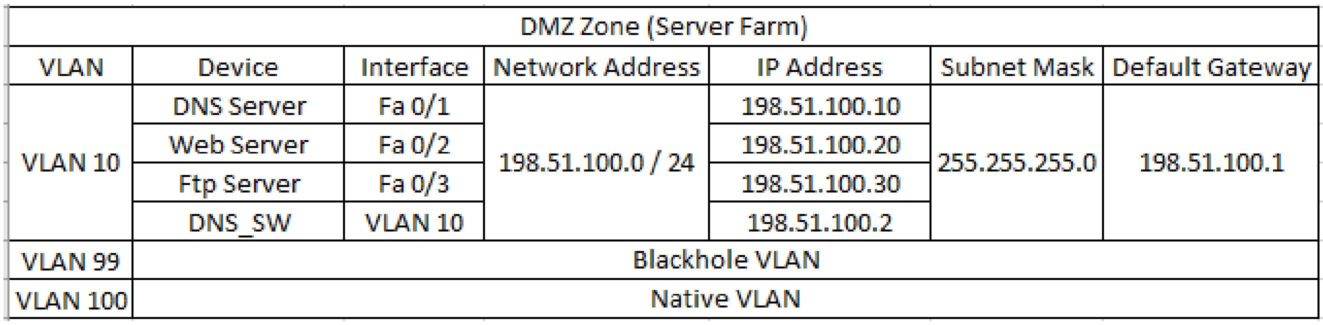
Delivery Department						
VLAN	Device	Interface	Network Address	IP Address	Subnet Mask	Default Gateway
VLAN 30	Delivery-PC1	Fa 0/2	192.168.3.0 / 24	192.168.3.2	255.255.255.0	192.168.3.1
	Delivery-PC2	Fa 0/3		192.168.3.3		
VLAN 50	Delivery_SW	VLAN 50	192.168.50.0 / 24	192.168.50.13		192.168.50.1
VLAN 99	Blackhole VLAN					
VLAN 100	Native VLAN					

Figure 4: IP addressing table for Delivery Department

Delivery Department has been assigned to VLAN 30 while Delivery_SW has been assigned to VLAN 50 due to the switch is part of management VLAN. Each host devices such as end device (PC) and has been configured with static IP Address respectively alongside with the same default gateway due to same VLAN. Any unused port will be administrative shutdown and assigned to VLAN 99 (Blackhole VLAN) for security enhancement purpose and the trunk ports has been configured to VLAN 100 (Native VLAN).

2.2 DMZ Zone IP Addressing Table

The DMZ zone is located in KL and it only contains 1 department: Server Farm.



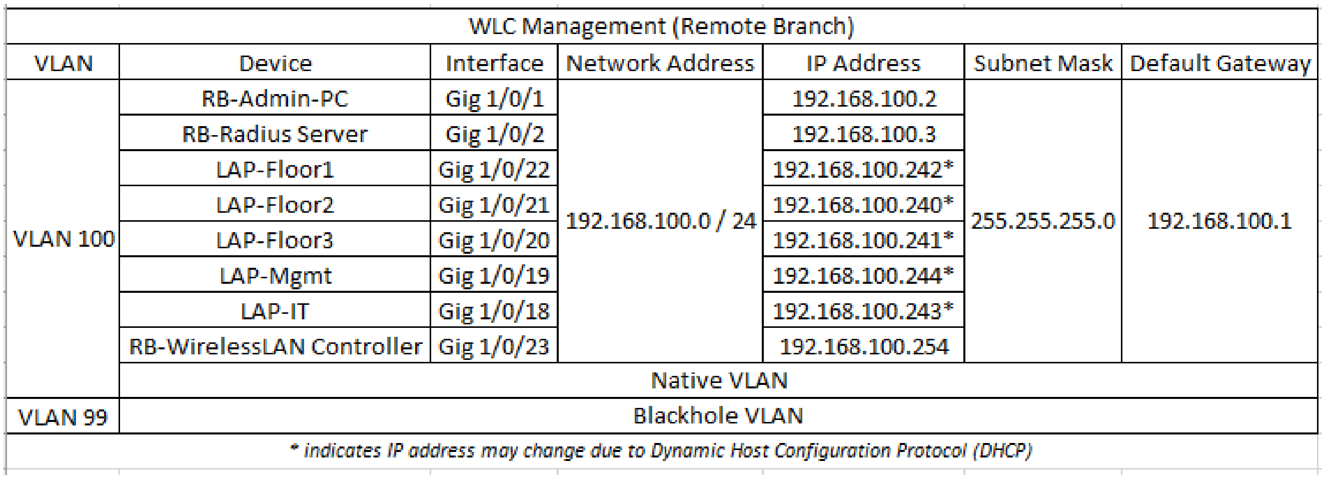
DMZ Zone (Server Farm)						
VLAN	Device	Interface	Network Address	IP Address	Subnet Mask	Default Gateway
VLAN 10	DNS Server	Fa 0/1	198.51.100.0 / 24	198.51.100.10	255.255.255.0	198.51.100.1
	Web Server	Fa 0/2		198.51.100.20		
	Ftp Server	Fa 0/3		198.51.100.30		
	DNS_SW	VLAN 10		198.51.100.2		
VLAN 99	Blackhole VLAN					
VLAN 100	Native VLAN					

Figure 5: IP addressing table for Server Farm in DMZ Zone

The DMZ Zone is the house of server farm for Fiber Optic Inc servers. The servers have been assigned to VLAN 10. Each host devices such as the server devices and the server farm switch and has been configured with static IP Address respectively alongside with the same default gateway due to same VLAN. Any unused port will be administrative shutdown and assigned to VLAN 99 (Blackhole VLAN) for security enhancement purpose and the trunk ports has been configured to VLAN 100 (Native VLAN).

2.3 Remote Branch IP Addressing Table

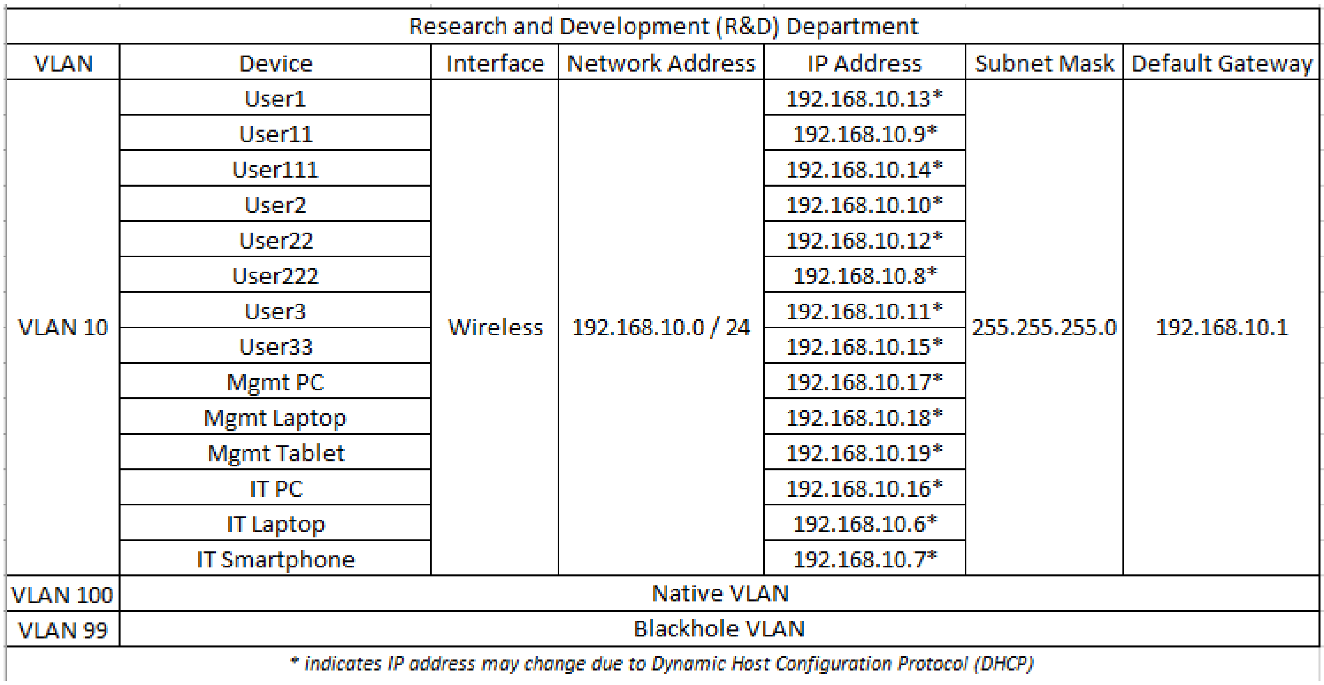
The Remote Branch of Fiber Optic Inc. is located in Cyberjaya. It consists of two departments: WLC Management Department, Research and Development (R&D) Department.



WLC Management (Remote Branch)						
VLAN	Device	Interface	Network Address	IP Address	Subnet Mask	Default Gateway
VLAN 100	RB-Admin-PC	Gig 1/0/1	192.168.100.0 / 24	192.168.100.2	255.255.255.0	192.168.100.1
	RB-Radius Server	Gig 1/0/2		192.168.100.3		
	LAP-Floor1	Gig 1/0/22		192.168.100.242*		
	LAP-Floor2	Gig 1/0/21		192.168.100.240*		
	LAP-Floor3	Gig 1/0/20		192.168.100.241*		
	LAP-Mgmt	Gig 1/0/19		192.168.100.244*		
	LAP-IT	Gig 1/0/18		192.168.100.243*		
	RB-WirelessLAN Controller	Gig 1/0/23		192.168.100.254		
	Native VLAN					
VLAN 99	Blackhole VLAN					
** indicates IP address may change due to Dynamic Host Configuration Protocol (DHCP)*						

Figure 6: IP addressing table for WLC Management

The WLC Management Department is assigned to VLAN 100. The Light weighted Access Points (LAP) are controlled by the Wireless LAN Controller which is labelled as RB-WirelessLAN Controller. Any unused port in the Multi-Layer Switch has been administrative shut down and assigned to the Blackhole VLAN (VLAN 99).



Research and Development (R&D) Department						
VLAN	Device	Interface	Network Address	IP Address	Subnet Mask	Default Gateway
VLAN 10	User1	Wireless	192.168.10.0 / 24	192.168.10.13*	255.255.255.0	192.168.10.1
	User11			192.168.10.9*		
	User111			192.168.10.14*		
	User2			192.168.10.10*		
	User22			192.168.10.12*		
	User222			192.168.10.8*		
	User3			192.168.10.11*		
	User33			192.168.10.15*		
	Mgmt PC			192.168.10.17*		
	Mgmt Laptop			192.168.10.18*		
	Mgmt Tablet			192.168.10.19*		
	IT PC			192.168.10.16*		
	IT Laptop			192.168.10.6*		
	IT Smartphone			192.168.10.7*		
VLAN 100	Native VLAN					
VLAN 99	Blackhole VLAN					

** indicates IP address may change due to Dynamic Host Configuration Protocol (DHCP)*

Figure 7: IP addressing table for Research and Development (R&D) Department

The Research and Development (R&D) Department is assigned to VLAN 10. The IP Addresses of the end devices are Dynamic IP Address. Certain devices receive IP Address once pre-shared key is successfully verify by the access point while certain end devices receive IP Address once profile is created in WPA2 Enterprise match with the username and password created in the Radius Server.

3.0 Network Topology Diagram (Entire Network Layout – packet tracer)

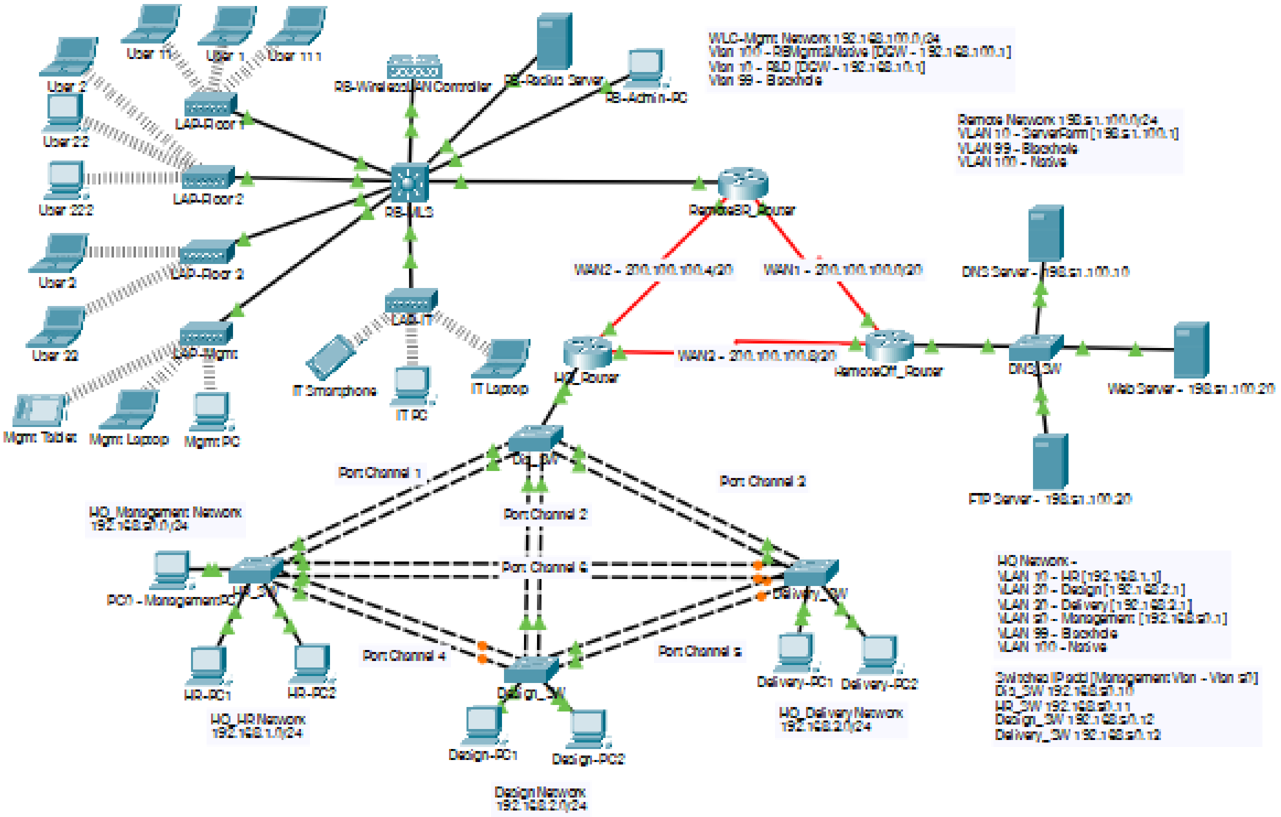


Figure 8: Prototype of Network Topology Diagram for Fiberoptic Systems Inc.'s new Network

4.0 LAN and WAN Configuration

4.1 Dynamic Host Configuration Protocol (DHCPv4)

IPv4 addresses and other network configuration information are assigned dynamically using the Dynamic Host Configuration Protocol v4 (DHCPv4). The DHCPv4 server dynamically allocates, or leases, an IPv4 address from a pool of addresses for a predetermined amount of time, or until the client no longer requires it. The DHCP server returns the address to the pool after a lease ends, so it may be reassigned as needed (CCNA2, n.d.).

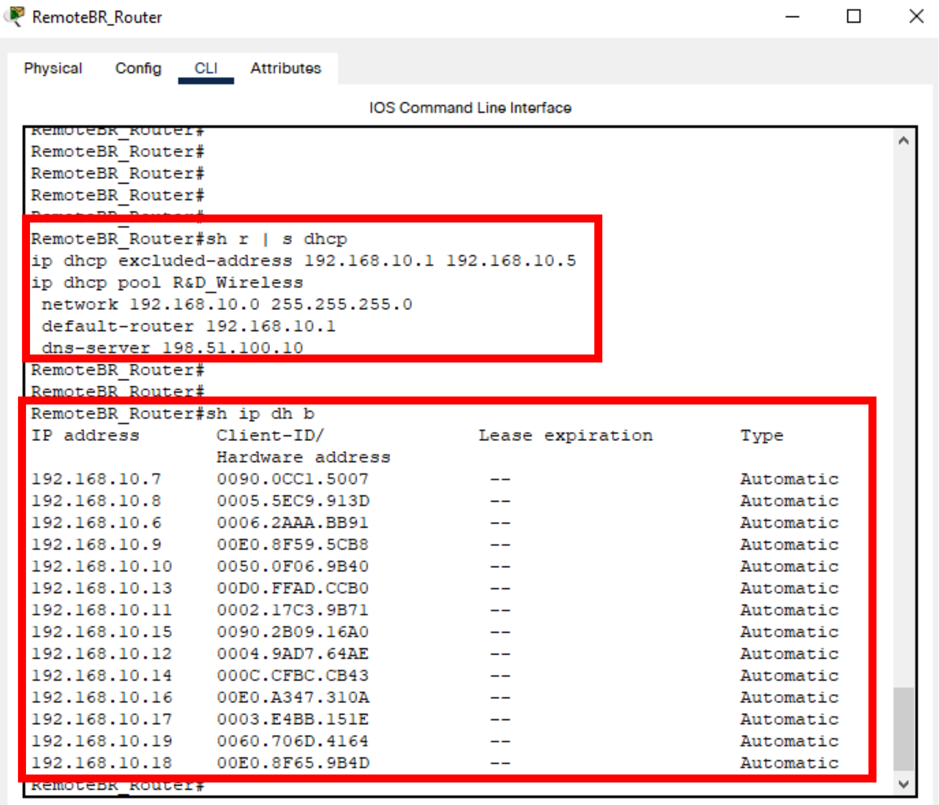
How DHCP is allocated?

Step 1: To find accessible DHCPv4 servers, the client sends out a broadcast DHCPDISCOVER message with its own MAC address. Because the client does not have proper IPv4 information at bootup, it communicates with the server via Layer 2 and Layer 3 broadcast addresses. The DHCPDISCOVER message is used to locate DHCPv4 servers on a network.

Step 2: When a DHCPDISCOVER message is received, the DHCPv4 server reserves an available IPv4 address to lease to the client. The server additionally creates an ARP entry with the requesting client's MAC address and the client's leased IPv4 address. The DHCPv4 server delivers the requesting client the bound DHCPOFFER message.

Step 3: The client responds with a DHCPREQUEST message after receiving the DHCPOFFER from the server. This mail is sent out for both new leases and lease renewals. When used for lease origination, the DHCPREQUEST acts as a binding acceptance notification to the selected server for the parameters it has supplied, as well as an implicit refuse to any other servers who may have made a binding offer to the client.

Step 4: The server will check the lease information using an ICMP ping to that address to confirm it is not already in use, generate a new ARP entry for the client lease, and react with a DHCPACK message after receiving the DHCPREQUEST message. Except for a change in the message type field, the DHCPACK message is identical to the DHCPOFFER. The client logs the configuration information and may do an ARP search for the allocated address when it gets the DHCPACK message. If the client receives no response to the ARP, it assumes the IPv4 address is genuine and begins using it as its own.



```
RemoteBR_Router#
RemoteBR_Router#
RemoteBR_Router#
RemoteBR_Router#
RemoteBR_Router#
RemoteBR_Router#sh r | s dhcp
ip dhcp excluded-address 192.168.10.1 192.168.10.5
ip dhcp pool R&D_Wireless
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
 dns-server 198.51.100.10
RemoteBR_Router#
RemoteBR_Router#
RemoteBR_Router#sh ip dh b
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
192.168.10.7     0090.0CC1.5007           --                     Automatic
192.168.10.8     0005.5EC9.913D           --                     Automatic
192.168.10.6     0006.2AAA.BB91           --                     Automatic
192.168.10.9     00E0.8F59.5CB8           --                     Automatic
192.168.10.10    0050.0F06.9B40           --                     Automatic
192.168.10.13    00D0.FFAD.CCB0           --                     Automatic
192.168.10.11    0002.17C3.9B71           --                     Automatic
192.168.10.15    0090.2B09.16A0           --                     Automatic
192.168.10.12    0004.9AD7.64AE           --                     Automatic
192.168.10.14    000C.CFBC.CB43           --                     Automatic
192.168.10.16    00E0.A347.310A           --                     Automatic
192.168.10.17    0003.E4BB.151E           --                     Automatic
192.168.10.19    0060.706D.4164           --                     Automatic
192.168.10.18    00E0.8F65.9B4D           --                     Automatic
RemoteBR_Router#
```

Figure 9: Configuration of DHCPv4 on RemoteBR_Router

RemoteBR_Router is implemented DHCPv4 and the services can be provided either by a dedicated server or a router. The reason why DHCPv4 is implemented is to assume the number of employees will increased in the future, thus using DHCP is an ideal option. At the same time, errors of manual configuration can be reduced as manual configuration might accidentally configured the same IP Address or invalid IP Address for the network.

4.2 VLAN and Trunking

In essence, a VLAN is a group of devices or network nodes that interact with one another as if they were part of a single LAN segment, even when they are really part of one or more LAN segments. A bridge, router, or switch separates a segment from the rest of the LAN, and it's usually utilized for a certain department which is suitable for Fiberoptic Systems Inc. as HQ Network consist of multiple departments. This implies that when a workstation broadcasts packets, they are received by all other workstations on the same VLAN only.

By operating as LAN segments, VLANs lower the frequency of collisions and the amount of network resources lost. Data packets transmitted from a segment's workstation are transported through a bridge or switch, which does not forward collisions but sends out broadcasts to all network devices. As a result, segments are referred to as "collision domains" since they include collisions inside their boundaries. VLANs, on the other hand, also offer more features than a LAN segment since they allow for additional data protection and logical partitioning especially in Layer 2 Security mitigation. Increased performance, more flexibility in network setup and workgroup formation, and decreased administrative labor are the benefits of VLAN adoption exactly needed for Fiberoptic System Inc. business operation (N-able, 2019).

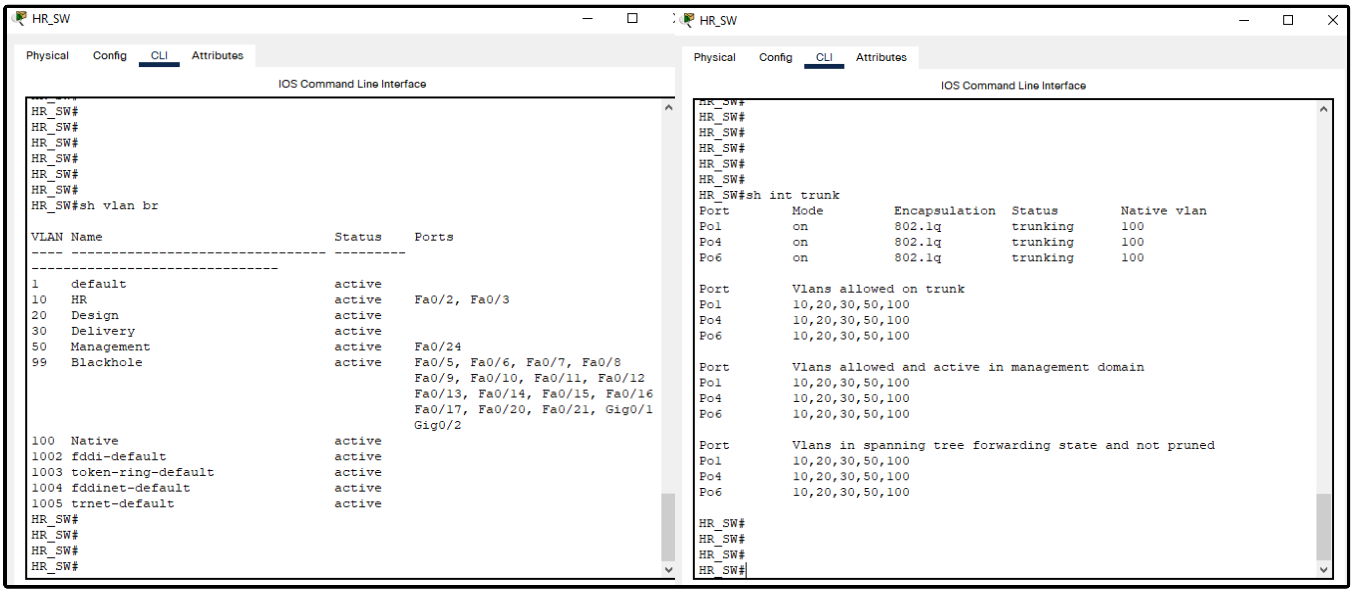
Four categories VLANs are divided into based on the sort of network they carry:

1. Default VLAN - When the switch is turned on, all of the switch's ports join the default VLAN (typically VLAN 1), putting them all in the same broadcast domain. Every network device connected to any switch port can interact with devices connected to other switch ports while using default VLAN. One of the unique properties of the Default VLAN is that it cannot be renamed or erased.
2. Data VLAN - A VLAN separates the whole network into two groups. There are two types of users, as well as two types of devices. Only user-generated data is sent over the data VLAN, also known as a user VLAN. This VLAN is just for the transfer of data. It isn't used to transport speech or regulate traffic.
3. Management VLAN — To acquire access to a switch's administration capabilities, a management VLAN is used (traffic like system logging, monitoring). VLAN 1 is the administration VLAN by default (VLAN 1 would be a bad choice for the management VLAN). If the admin has not created a unique VLAN to act as the management VLAN, any of the switch VLANs might be defined as the management VLAN. Even when user traffic is heavy, this VLAN guarantees that bandwidth for administration is accessible.

4. Native VLAN - This VLAN is used to distinguish traffic coming from both ends of a trunk link. A native VLAN is allocated to only one 802.1Q trunk port. Untagged traffic (traffic that does not originate from a VLAN) is routed to the native VLAN through the 802.1Q trunk port. The original VLAN should be set as an unused VLAN, if possible.

4.2.1 VLAN and Trunking in HQ Network

HQ Network is located in KL and the network consists of 4 switches (Dis_SW, HR_SW, Design_SW and Delivery_SW) and 7 end devices. The HQ Network consists of 4 departments: Management Department, Human Resource Department, Design Department and Delivery Department. Each department has been differentiated with different VLANs.



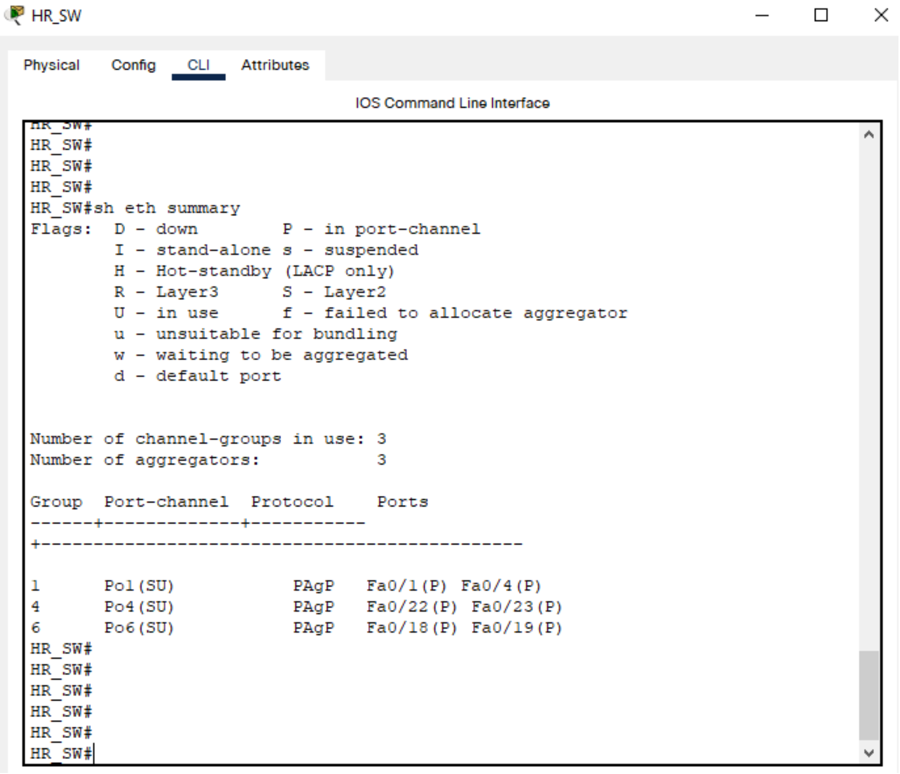
```
HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#sh vlan br

VLAN Name                             Status    Ports
---- -------------------------------- ---------
-------------------------------
1    default                          active
10   HR                               active    Fa0/2, Fa0/3
20   Design                           active
30   Delivery                         active
50   Management                       active    Fa0/24
99   Blackhole                        active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/20, Fa0/21, Gig0/1
                                                Gig0/2
100  Native                           active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
HR_SW#
HR_SW#
HR_SW#
HR_SW#
```

```
HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#sh int trunk
Port        Mode         Encapsulation  Status        Native vlan
Po1         on           802.1q         trunking      100
Po4         on           802.1q         trunking      100
Po6         on           802.1q         trunking      100

Port        Vlans allowed on trunk
Po1         10,20,30,50,100
Po4         10,20,30,50,100
Po6         10,20,30,50,100

Port        Vlans allowed and active in management domain
Po1         10,20,30,50,100
Po4         10,20,30,50,100
Po6         10,20,30,50,100

Port        Vlans in spanning tree forwarding state and not pruned
Po1         10,20,30,50,100
Po4         10,20,30,50,100
Po6         10,20,30,50,100

HR_SW#
HR_SW#
HR_SW#
HR_SW#
```

Figure 10: Example of VLANs and Trunk Interface for HR_SW

The first switch console, as shown in the diagram, displayed the allocation of switch ports to various VLANs. The ports that are visible have been set to access mode by an administrator. The Human Resource Department's workstations are linked to the interfaces fa0/2 and fa0/3, while the Management Department's workstations are connected to Gig0/2. To prevent VLAN attacks, all unused ports are assigned to the blackhole VLAN (VLAN 99) and administratively shut off.

The second switch console, on the other hand, reflected the allocation of ports to trunking modes. The Trunk Link is a connection between two trunk ports that allows traffic from several VLANs to pass through. Traffic from each department's VLAN can pass through HR SW, and any switch that fails can continue send traffic to HR SW as long as the VLAN is active. The logical port is displayed in replacement of the real physical port since EtherChannel is set in HQ Network.



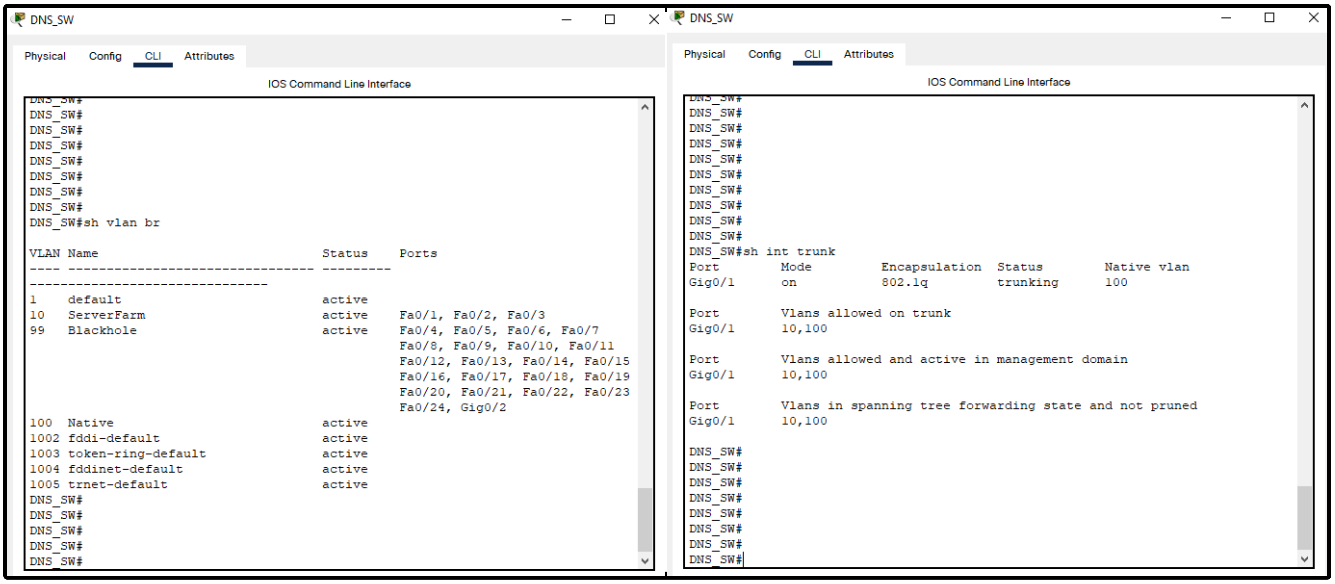
```
HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#sh eth summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        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)           PAgP   Fa0/1(P) Fa0/4(P)
4      Po4(SU)           PAgP   Fa0/22(P) Fa0/23(P)
6      Po6(SU)           PAgP   Fa0/18(P) Fa0/19(P)
HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#
```

Figure 11: Example of physical switchport used in port channel group

The figure above shown the ports that used to configure as trunk links through PAgP protocol concept. The similar concept is also applied for Dis_SW, Design_SW and Delivery_SW.

4.2.2 VLAN and Trunking in DMZ Zone

The DMZ Zone only utilized one switch: DNS_SW



```
DNS_SW#
DNS_SW#
DNS_SW#
DNS_SW#
DNS_SW#
DNS_SW#
DNS_SW#
DNS_SW#
DNS_SW#sh vlan br

VLAN Name                             Status    Ports
---- -------------------------------- ---------
-------------------------------
1    default                          active
10   ServerFarm                       active    Fa0/1, Fa0/2, Fa0/3
99   Blackhole                        active    Fa0/4, Fa0/5, Fa0/6, Fa0/7
                                                Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gig0/2
100  Native                           active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
DNS_SW#
DNS_SW#
DNS_SW#
DNS_SW#
DNS_SW#
```

```
DNS_SW#
DNS_SW#
DNS_SW#
DNS_SW#
DNS_SW#
DNS_SW#
DNS_SW#
DNS_SW#
DNS_SW#
DNS_SW#
DNS_SW#sh int trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      on           802.1q         trunking      100

Port        Vlans allowed on trunk
Gig0/1      10,100

Port        Vlans allowed and active in management domain
Gig0/1      10,100

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      10,100

DNS_SW#
DNS_SW#
DNS_SW#
DNS_SW#
DNS_SW#
DNS_SW#
DNS_SW#
DNS_SW#
```

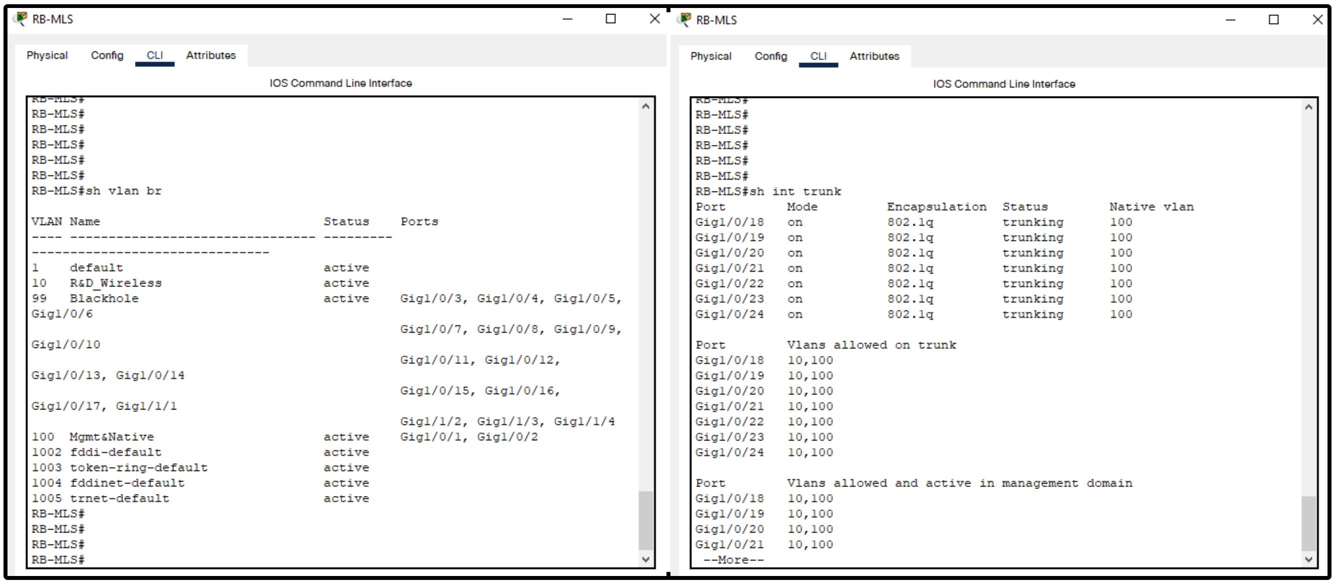
Figure 12: Example of VLANs and Trunk Interface for DNS_SW

The first switch console, as shown in the diagram, displayed the allocation of switch ports to various VLANs. The ports that are visible have been set to access mode by an administrator. The Servers workstations are linked to the interfaces fa0/1, fa0/2 and fa0/3. To prevent VLAN attacks, all unused ports are assigned to the blackhole VLAN (VLAN 99) and administratively shut off.

The second switch console, on the other hand, reflected the allocation of ports to trunking modes. The Trunk Link is a connection between two trunk ports that allows traffic from several VLANs (VLAN 10 and 100) to pass through.

4.2.3 VLAN and Trunking in Remote Branch

The Remote Branch is located in Cyberjaya and utilize multi-layer switch: RB_MLS.



```
RB-MLS#
RB-MLS#
RB-MLS#
RB-MLS#
RB-MLS#
RB-MLS#
RB-MLS#sh vlan br

VLAN Name                             Status    Ports
---- -------------------------------- ---------
-------------------------------
1    default                          active
10   R&D_Wireless                     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, Gig1/1/1
                                                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-MLS#
RB-MLS#
RB-MLS#
RB-MLS#
```

```
RB-MLS#
RB-MLS#
RB-MLS#
RB-MLS#
RB-MLS#
RB-MLS#
RB-MLS#sh int trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig1/0/18   on           802.1q         trunking      100
Gig1/0/19   on           802.1q         trunking      100
Gig1/0/20   on           802.1q         trunking      100
Gig1/0/21   on           802.1q         trunking      100
Gig1/0/22   on           802.1q         trunking      100
Gig1/0/23   on           802.1q         trunking      100
Gig1/0/24   on           802.1q         trunking      100

Port        Vlans allowed on trunk
Gig1/0/18   10,100
Gig1/0/19   10,100
Gig1/0/20   10,100
Gig1/0/21   10,100
Gig1/0/22   10,100
Gig1/0/23   10,100
Gig1/0/24   10,100

Port        Vlans allowed and active in management domain
Gig1/0/18   10,100
Gig1/0/19   10,100
Gig1/0/20   10,100
Gig1/0/21   10,100
 --More--
```

Figure 13: Example of VLANs and Trunk Interface for RB_MLS

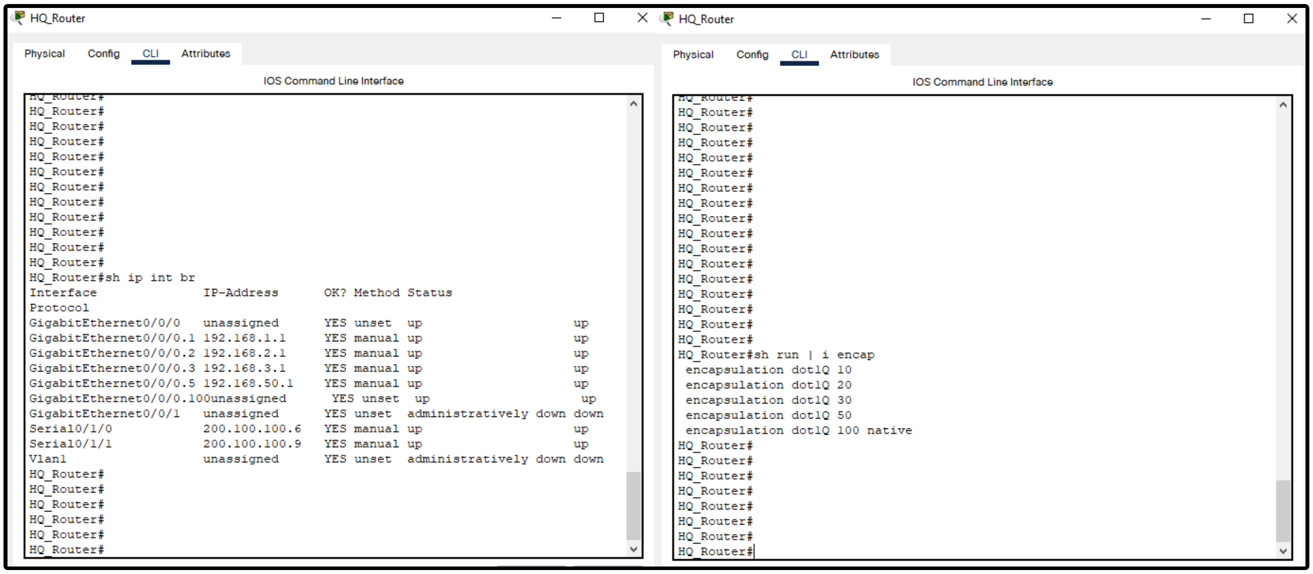
The first switch console, as shown in the Figure 13, displayed the allocation of switch ports to various VLANs. The ports that are visible have been set to access mode by an administrator. To prevent VLAN attacks, all unused ports are assigned to the blackhole VLAN (VLAN 99) and administratively shut off.

The second switch console, on the other hand, reflected the allocation of ports to trunking modes. The Trunk Link is a connection between two trunk ports that allows traffic from several VLANs (VLAN 10 and 100) to pass through.

4.3 Inter VLAN Routing (Router on the Stick)

A "router-on-a-stick" is a router setup that allows network administrator to transport traffic between numerous VLANs using a single physical interface by connecting two or more Virtual LANs through a single Ethernet network interface port, allowing them to be linked. Multiple virtual LANs can coexist on the same physical LAN thanks to Inter VLAN routing. The router interface is linked to a trunk switch port and configured as a trunk link. On the trunk interface, the router accepts tagged traffic and routes it internally using sub interfaces. On a single physical interface, trunk lines can accept numerous VLANs. Encapsulation methods that encapsulate or tag the frames enable switches to detect the VLAN utilized for a certain packet. Inter VLAN Routing is necessary for every single LAN in Fiberoptic Systems Inc. as multiple VLANs is utilized in each LAN (CertificationKits, n.d.).

4.3.1 Example of Inter VLAN Routing (HQ Network)



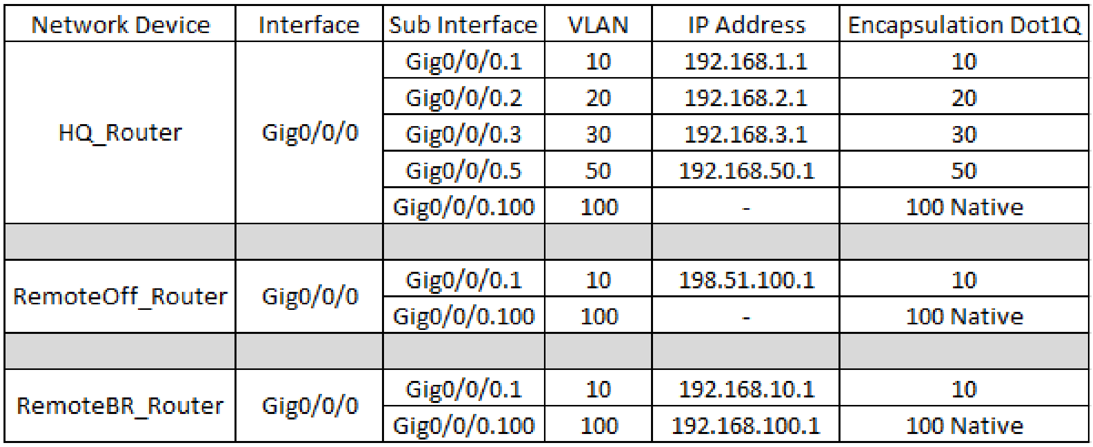
```
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#sh ip int br
Interface              IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0/0   unassigned      YES unset  up                    up
GigabitEthernet0/0/0.1 192.168.1.1     YES manual up                    up
GigabitEthernet0/0/0.2 192.168.2.1     YES manual up                    up
GigabitEthernet0/0/0.3 192.168.3.1     YES manual up                    up
GigabitEthernet0/0/0.5 192.168.50.1    YES manual up                    up
GigabitEthernet0/0/0.100unassigned      YES unset  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            200.100.100.9   YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
```

```
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#sh run | i encap
 encapsulation dot1Q 10
 encapsulation dot1Q 20
 encapsulation dot1Q 30
 encapsulation dot1Q 50
 encapsulation dot1Q 100 native
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
```

Figure 14: Example of configuring Inter VLAN Routing on HQ_Router

As an example, any user from one department wishes to communicate with another user from different department (VLAN 10 HR Department to VLAN 20 Design Department), the traffic from VLAN 10 arrives to sub interface of the router and the router determine the exit traffic and the traffic is retagged with VLAN 20 802.1Q-tag as the router interface is configured using the command “encapsulation dot1q 20”.

4.3.2 Inter VLAN Routing Table (For Each LAN)



Network Device	Interface	Sub Interface	VLAN	IP Address	Encapsulation Dot1Q
HQ_Router	Gig0/0/0	Gig0/0/0.1	10	192.168.1.1	10
		Gig0/0/0.2	20	192.168.2.1	20
		Gig0/0/0.3	30	192.168.3.1	30
		Gig0/0/0.5	50	192.168.50.1	50
		Gig0/0/0.100	100	-	100 Native
RemoteOff_Router	Gig0/0/0	Gig0/0/0.1	10	198.51.100.1	10
		Gig0/0/0.100	100	-	100 Native
RemoteBR_Router	Gig0/0/0	Gig0/0/0.1	10	192.168.10.1	10
		Gig0/0/0.100	100	192.168.100.1	100 Native

Figure 15: Inter VLAN Routing Table (For Each LAN)

4.4 Layer 2 Redundancy (Spanning-Tree Protocol)

When utilizing numerous switches, it is important to make sure they're all linked. This is secure with any type of switch as long as there is only one connection between the two switches and no bridge on either of the firewalls. Redundancy is an important component of hierarchical design for minimizing network service interruptions for users. In redundant networks, physical channels must be created and the logical redundancy must also be addressed. However, the drawbacks of creating redundant connections in a switched Ethernet network can cause both physical and logical Layer 2 loops. Layer 2 loops must be avoided when employing bridging or when several linkages exist between the switches. A controlled switch would be required, capable of detecting and blocking ports that might otherwise cause switch loops using Spanning Tree Protocol (STP). When employing STP, if an active connection fails (for example, due to a switch failure), a backup link can be instantly established in its stead (NetgateDocs, n.d.).

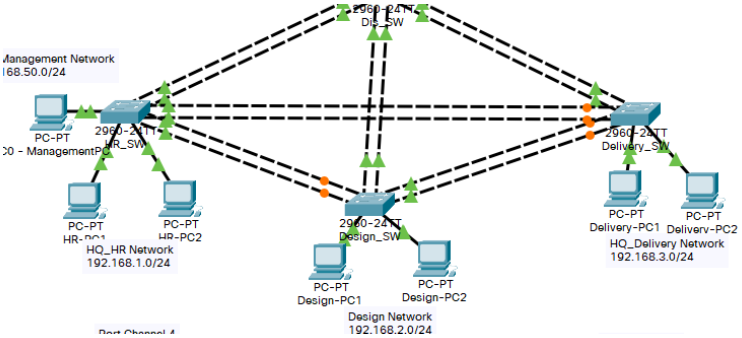
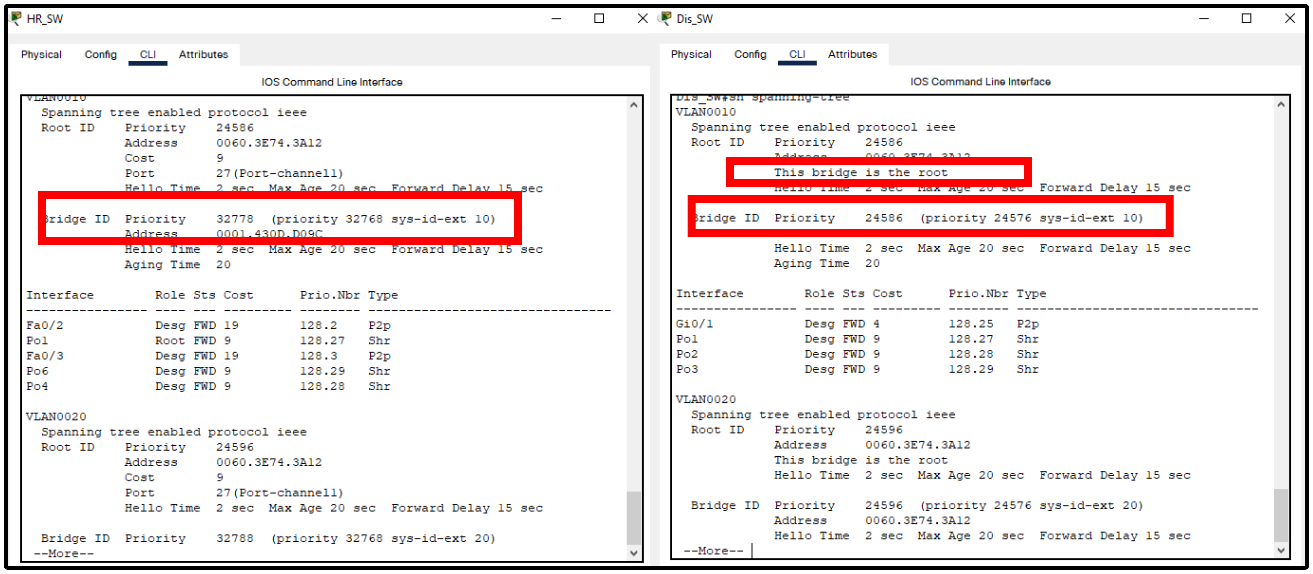


Figure 16: Implementation of Layer 2 Redundancy (Spanning-Tree Protocol)

Thanks to the implementation of Layer 2 Redundancy (Spanning-Tree Protocol), if one of the links between HR_SW and Dis_SW malfunction, the backup link is on standby due to Spanning-Tree Protocol. When using a spanning tree, redundant data pathways are forced into a standby (blocked) state. The spanning-tree method recalculates the spanning-tree topology and activates the standby path whenever a network segment in the spanning tree breaks and a redundant path exists. At regular intervals, switches send and receive spanning-tree frames, also known as bridge protocol data units (BPDUs). These frames are not sent by the switches; instead, they are used to provide a loop-free routing. The transmitting switch and its ports are described in BPDUs, which include switch and MAC addresses, switch priority, port priority, and path cost. The root switch and root port for the switched network, as well as the root port and designated port for each switched segment, are chosen using this information.



```
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    24586
             Address     0060.3E74.3A12
             Cost        9
             Port        27(Port-channel1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     0001.430D.D09C
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Desg FWD 19        128.2    P2p
Po1              Root FWD 9         128.27   Shr
Fa0/3            Desg FWD 19        128.3    P2p
Po6              Desg FWD 9         128.29   Shr
Po4              Desg FWD 9         128.28   Shr

VLAN0020
  Spanning tree enabled protocol ieee
  Root ID    Priority    24596
             Address     0060.3E74.3A12
             Cost        9
             Port        27(Port-channel1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32788  (priority 32768 sys-id-ext 20)
 --More--
```

```
Dis_SW#sh spanning-tree
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    24586
             Address     0060.3E74.3A12
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24586  (priority 24576 sys-id-ext 10)

             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi0/1            Desg FWD 4         128.25   P2p
Po1              Desg FWD 9         128.27   Shr
Po2              Desg FWD 9         128.28   Shr
Po3              Desg FWD 9         128.29   Shr

VLAN0020
  Spanning tree enabled protocol ieee
  Root ID    Priority    24596
             Address     0060.3E74.3A12
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24596  (priority 24576 sys-id-ext 20)
             Address     0060.3E74.3A12
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
 --More--
```

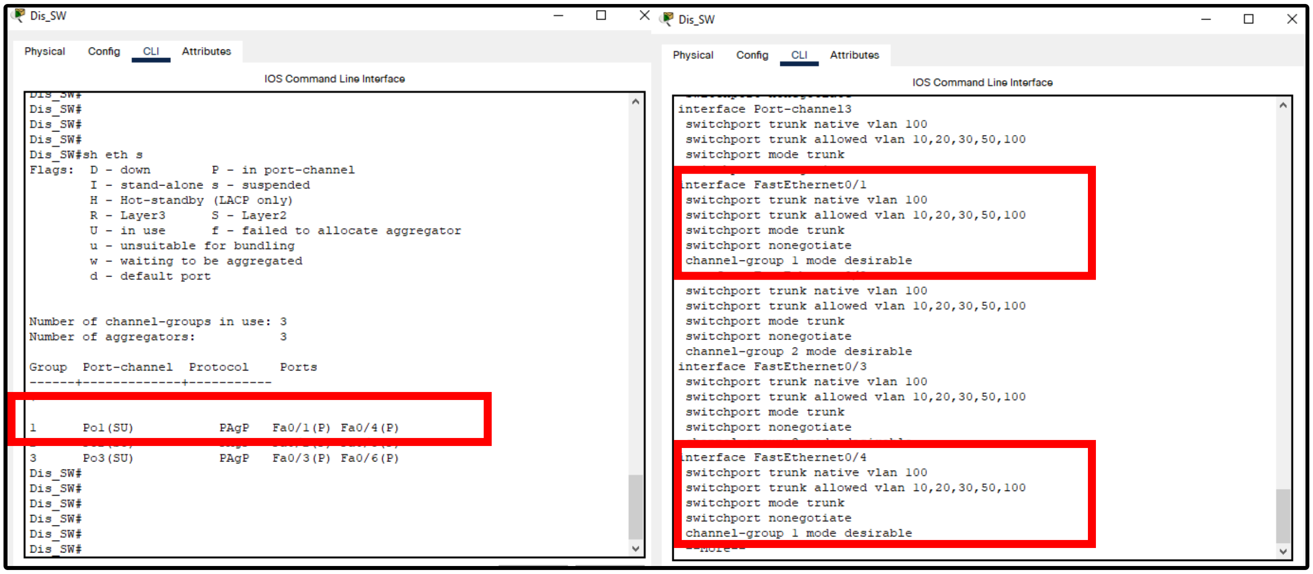
Figure 17: Configuring of STP in the Prototype Network

Based on the figure above, Dis_SW has lowest Bridge ID Priority than HR_SW (and also compare to other switches in the HQ Network), thus Dis_SW is the root bridge and root bridge does not have any block state, which allows data to send through Dis_SW easily.

4.5 Link Aggregation Technology: EtherChannel

EtherChannel is a port link aggregation technique that combines several multiple port links into a single logical link. It's utilized to provide high-speed connections as well as redundancy. To make a single logical link, a maximum of 8 links can be aggregated. All ports in an EtherChannel should have: Identical duplex, the same rate, same VLAN setup (i.e., native VLAN and allowed VLAN should be same) and the modes of the switch ports should be the same (access or trunk mode) (CCNA, n.d.).

EtherChannel has 2 types, PAgP for port aggregation protocol and LACP stands for link aggregation control protocol, respectively. EtherChannel is vital for enhancing capacity by aggregating or combining traffic across all active lines, giving the appearance of a single logical wire, redundancy by providing extra accessible links in the event that one or more links go down, and load balancing by balancing traffic loads across the networks and improving bandwidth efficiency.

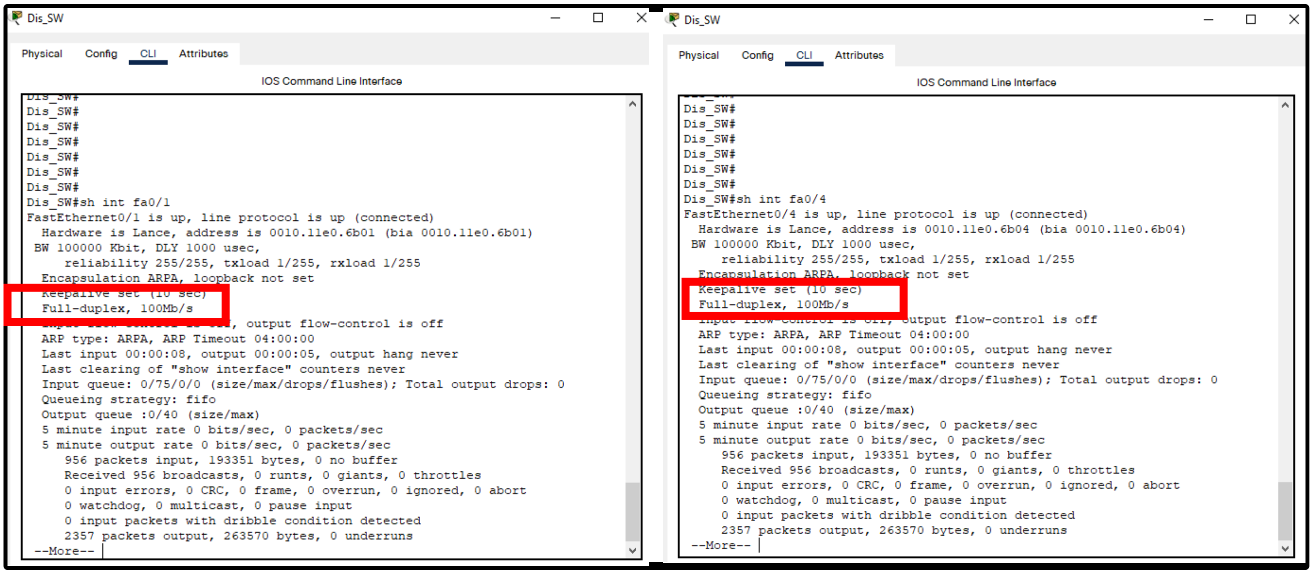


```
Dis_SW#
Dis_SW#
Dis_SW#
Dis_SW#sh eth s
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - 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)           PAgP   Fa0/1(P)  Fa0/4(P)
3      Po3(SU)           PAgP   Fa0/3(P)  Fa0/6(P)
Dis_SW#
Dis_SW#
Dis_SW#
Dis_SW#
Dis_SW#
Dis_SW#
```

```
interface Port-channel3
 switchport trunk native vlan 100
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
interface FastEthernet0/1
 switchport trunk native vlan 100
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode desirable
 switchport trunk native vlan 100
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode desirable
interface FastEthernet0/3
 switchport trunk native vlan 100
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
 switchport nonegotiate
interface FastEthernet0/4
 switchport trunk native vlan 100
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode desirable
```

Figure 18: Configuring of EtherChannel (PAgP on Port Channel 1)

Based on the figure above, the Port Channel 1 utilise PAgP protocol due to conditional fulfill (Dis_SW fa0/1 and fa0/4 has been configured to both desirable mode. At the same time, same Native VLAN is applied and allowed VLAN are identical).

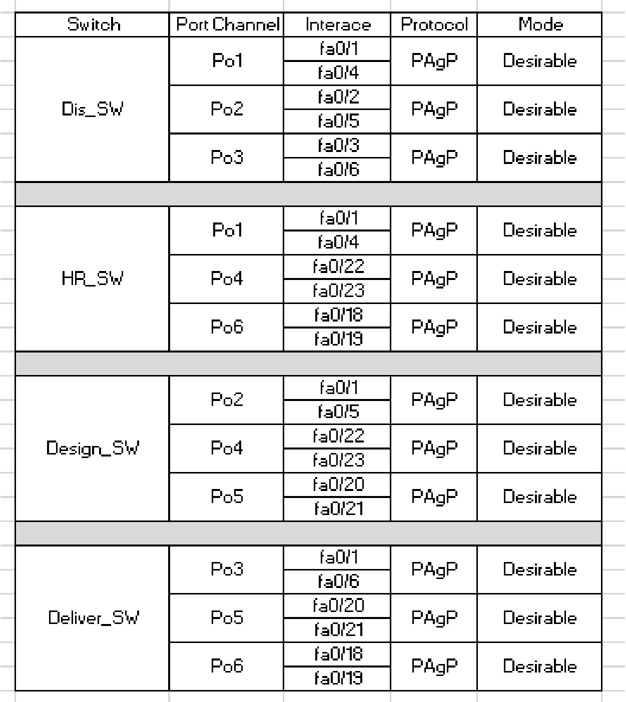


```
Dis_SW#
Dis_SW#
Dis_SW#
Dis_SW#
Dis_SW#
Dis_SW#
Dis_SW#
Dis_SW#sh int fa0/1
FastEthernet0/1 is up, line protocol is up (connected)
  Hardware is Lance, address is 0010.11e0.6b01 (bia 0010.11e0.6b01)
 BW 100000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     956 packets input, 193351 bytes, 0 no buffer
     Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     2357 packets output, 263570 bytes, 0 underruns
 --More--
```

```
Dis_SW#
Dis_SW#
Dis_SW#
Dis_SW#
Dis_SW#
Dis_SW#
Dis_SW#
Dis_SW#sh int fa0/4
FastEthernet0/4 is up, line protocol is up (connected)
  Hardware is Lance, address is 0010.11e0.6b04 (bia 0010.11e0.6b04)
 BW 100000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     956 packets input, 193351 bytes, 0 no buffer
     Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     2357 packets output, 263570 bytes, 0 underruns
 --More--
```

Figure 19: Duplex Settings and Port speed in Dis_SW

Condition fulfill (Same duplex and same port speed). As there are two cables connect from Dis_SW to HR_SW, the port speed is increased from 100Mb/s to 200Mb/s. At the same time, if one of the cable malfunction, the backup cable can used as usaully. Last but not least, lost balancing can be applied between links in an EtherChannel link. These 3 advantages fulfills the main goals of EtherChannel implementation as long as the 4 condition is fulfill.



Switch	Port Channel	Interace	Protocol	Mode
Dis_SW	Po1	fa0/1 fa0/4	PAgP	Desirable
	Po2	fa0/2 fa0/5	PAgP	Desirable
	Po3	fa0/3 fa0/6	PAgP	Desirable
HR_SW	Po1	fa0/1 fa0/4	PAgP	Desirable
	Po4	fa0/22 fa0/23	PAgP	Desirable
	Po6	fa0/18 fa0/19	PAgP	Desirable
Design_SW	Po2	fa0/1 fa0/5	PAgP	Desirable
	Po4	fa0/22 fa0/23	PAgP	Desirable
	Po5	fa0/20 fa0/21	PAgP	Desirable
Deliver_SW	Po3	fa0/1 fa0/6	PAgP	Desirable
	Po5	fa0/20 fa0/21	PAgP	Desirable
	Po6	fa0/18 fa0/19	PAgP	Desirable

Figure 20: EtherChannel Table

4.6 Routing Protocol - Open Shortest Path First (OSPF)

OSPF (Open Shortest Path First) is a link-state routing protocol for IP networks based on the Shortest Path First (SPF) algorithm. The link-state database, which reflects the area's topology, is shared by routers or systems in the same area in an OSPF network. By integrating the link-state advertisements (LSAs) it receives from other routers or systems in the area with the LSAs it generates, each router or system in the region develops its own link-state database. An LSA is a packet containing information about neighbors as well as route costs. In OSPF, an autonomous system (AS) is a group of IP networks that are all managed by the same operator, have the same routing strategy, and use the same routing protocol. The AS's routers and connections are organized into logical groups called regions. Areas are defined by numbers that are unique to each AS, and each AS must specify at least one area. When an AS is divided into many areas, each area is connected by a router known as an area border router (ABR). An ABR, by definition, has several OSPF interfaces connected to multiple OSPF areas, allowing it to function in multiple areas. For each related region, the ABR stores a copy of the link-state database. The autonomous system topology database is duplicated on all routers in a given area (IBM, n.d.)

The following are some of the primary benefits of OSPF:

1. OSPF, rather than distance-vector routing systems like the Routing Information Protocol, is better suited to serve large, diversified internetworks (RIP). Fiberoptic System Inc. will be able to expand in the near future.
2. If the network topology changes, OSPF can swiftly recalculate the routes.
3. Split an Autonomous System (AS) into areas and keep area topologies separate from OSPF to decrease OSPF routing traffic and the size of each area's link-state database.
4. OSPF provides equal-cost multipath routing. Duplicate routes with different next hops can be added to the TCP stack.

Routers or systems in an OSPF network send out Hello packets after checking that their interfaces are operational through their OSPF interfaces to discover neighbors, using the Hello protocol. Neighbors are routers or systems that have shared network interfaces. Then, to build adjacencies, nearby routers or systems share their link-state databases (IBM, n.d.): ~

STAGE OF EXSTART

The link-state database interchange begins with this phase. The master and subordinate roles are negotiated between the two systems.

STAGE OF EXCHANGE

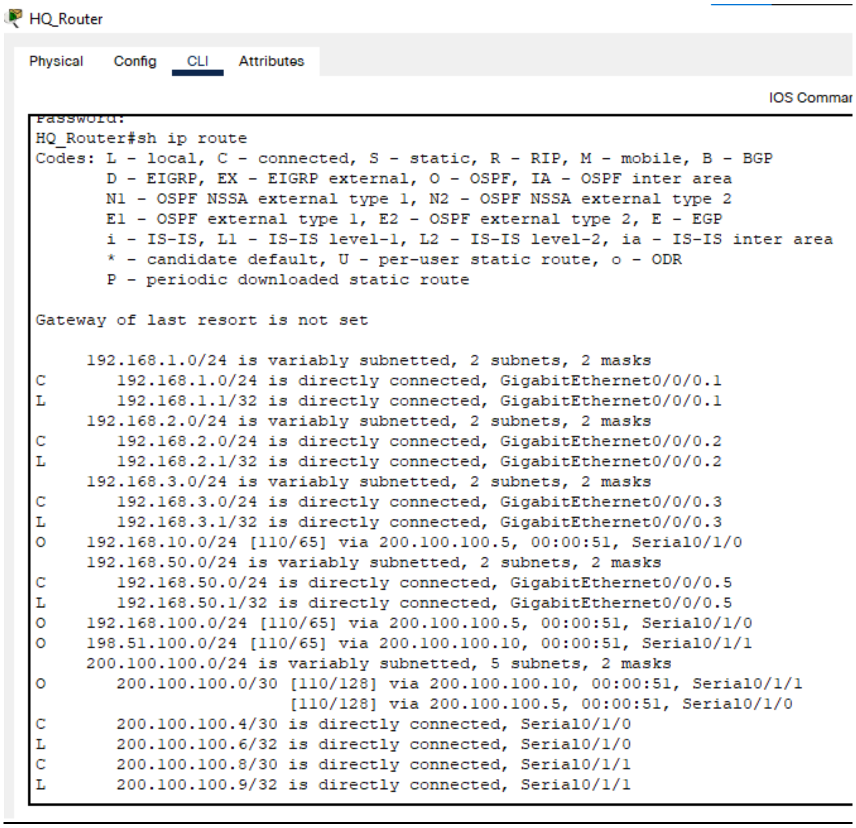
The two systems exchange Database Description packets to determine which LSAs each system's link-state database does not include. The retransmission list is where each system keeps the LSAs that aren't in its link-state database.

STAGE OF LOADING

Each system sends Link State Request packets to its neighbour (in this case, the other system) asking for all of the LSAs that were saved in the retransmission list during the EXCHANGE phase to be sent to it. The LSAs in Link State Update packets are returned by the neighbour in response to the request.

FULL PHASE

Adjacency is created between the two systems once they have finished exchanging LSAs and synced their link-state databases.



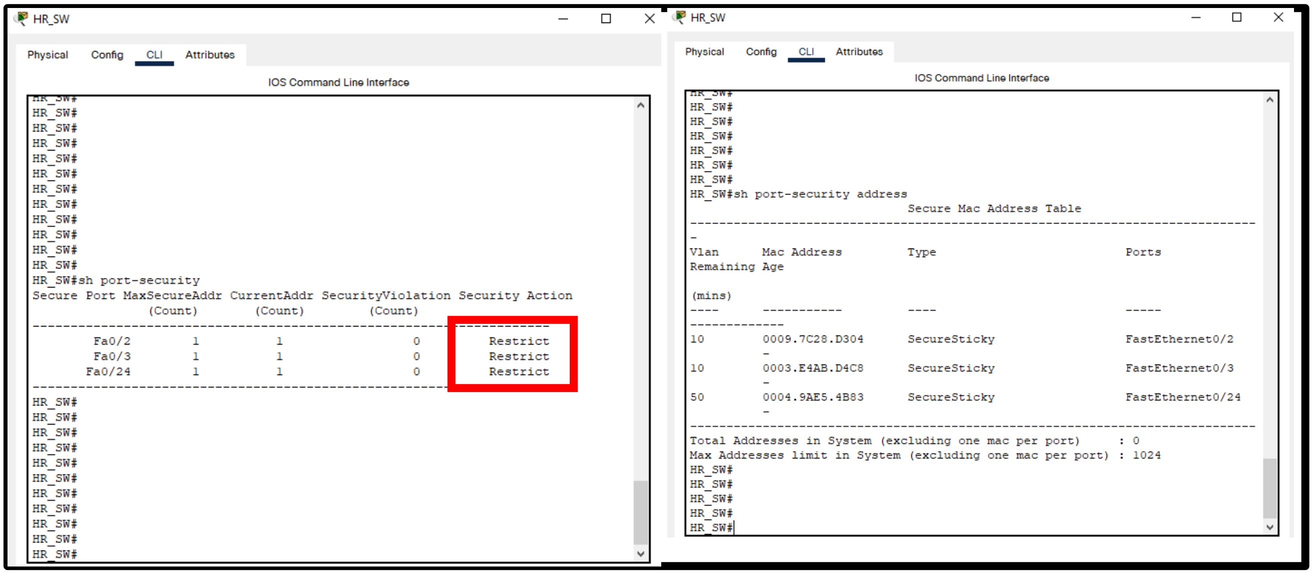
```
Password:
HQ_Router#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external 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

     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0/0.1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0/0.1
     192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, GigabitEthernet0/0/0.2
L       192.168.2.1/32 is directly connected, GigabitEthernet0/0/0.2
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, GigabitEthernet0/0/0.3
L       192.168.3.1/32 is directly connected, GigabitEthernet0/0/0.3
O    192.168.10.0/24 [110/65] via 200.100.100.5, 00:00:51, Serial0/1/0
     192.168.50.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.50.0/24 is directly connected, GigabitEthernet0/0/0.5
L       192.168.50.1/32 is directly connected, GigabitEthernet0/0/0.5
O    192.168.100.0/24 [110/65] via 200.100.100.5, 00:00:51, Serial0/1/0
O    198.51.100.0/24 [110/65] via 200.100.100.10, 00:00:51, Serial0/1/1
     200.100.100.0/24 is variably subnetted, 5 subnets, 2 masks
O       200.100.100.0/30 [110/128] via 200.100.100.10, 00:00:51, Serial0/1/1
                         [110/128] via 200.100.100.5, 00:00:51, Serial0/1/0
C       200.100.100.4/30 is directly connected, Serial0/1/0
L       200.100.100.6/32 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
```

Figure 21: Routing Table in HQ_Network

Based on the figure shown above, Fiberoptic Systems Inc. is utilizing OSPF to build routing table. OSPF calculate and elects the best path using the lowest cumulative cost of bandwidth from source to destination. Path with highest or lowest bandwidth will likely to be chosen as the path. C represent network (WAN) direct connected to the path while L represent the address assign to the network (Serial interface from the router). Meanwhile, O represent the routes that learn through OSPF protocol (the passive interface is learn by the router).

5.0 Layer 2 Security Mechanisms Deployment

5.1 MAC Address Table Attack Mitigation (Port Security)



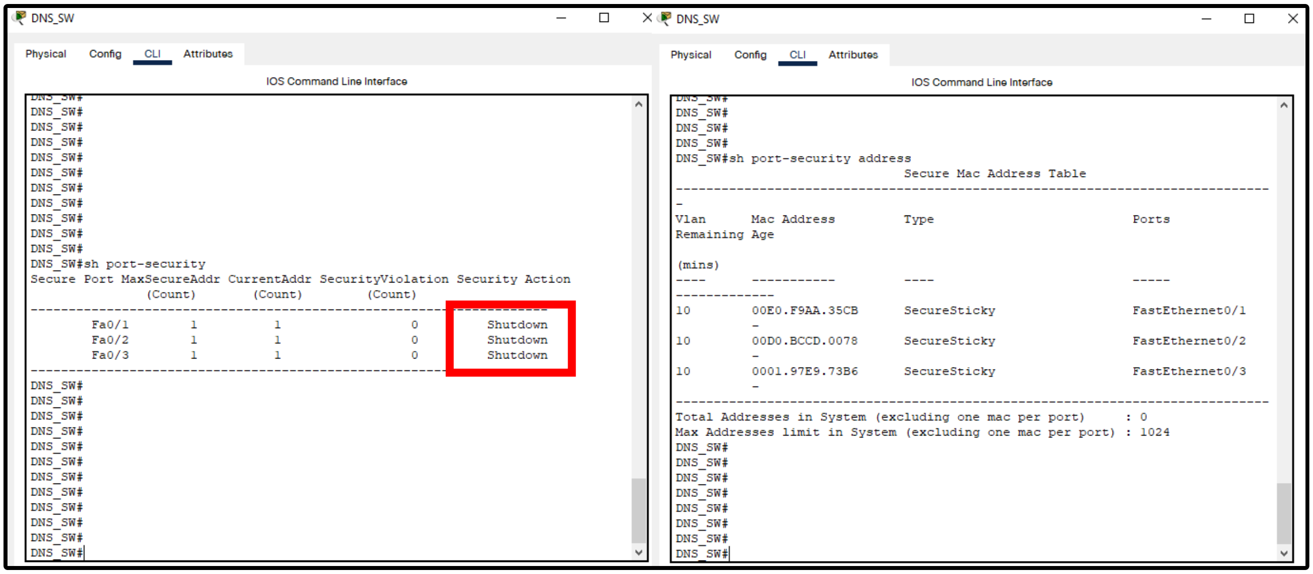
```
HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#sh port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)          (Count)
--------------------------------------------------------------------
        Fa0/2        1          1                 0         Restrict
        Fa0/3        1          1                 0         Restrict
       Fa0/24        1          1                 0         Restrict
--------------------------------------------------------------------
HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#
```

```
HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#sh port-security address
                              Secure Mac Address Table
-----------------------------------------------------------------------------
-
Vlan      Mac Address         Type                          Ports
Remaining Age

(mins)
----      -----------         ----                          -----
-------------
10        0009.7C28.D304      SecureSticky                  FastEthernet0/2
          -
10        0003.E4AB.D4C8      SecureSticky                  FastEthernet0/3
          -
50        0004.9AE5.4B83      SecureSticky                  FastEthernet0/24
          -
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#
```

Figure 22: Port Security (RESTRICT) configured on HR_SW access ports

The number of valid MAC addresses that can be used on a port on a switch is limited by switch port security. When a MAC address (or a combination of MAC addresses) is used to enable switch port security, packets are only forwarded to devices with those MAC addresses. Each port only enables traffic from a single MAC Address, as seen in the Figure 22. The port can be configured to limit the amount of acceptable MAC Addresses and to manually specify approved MAC Addresses by the network administrator. The port security applied in HR SW is set to "Sticky" in this circumstance (Dynamic learn MAC Address and store in the database, it will not be discarded even after reboot the system). The ageing timer, on the other hand, is not specified because it is anticipated that each port would only have one PC attached to it.

If there is any security violation occurs, unknown source addresses are discarded when the number of secure MAC addresses approaches the maximum value permitted on the port. The network administrator will be alerted if a security breach occurs due to the security action is set to “Restrict”.



```
DNS_SW#
DNS_SW#
DNS_SW#
DNS_SW#
DNS_SW#
DNS_SW#
DNS_SW#
DNS_SW#
DNS_SW#
DNS_SW#
DNS_SW#sh port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)          (Count)
--------------------------------------------------------------------
        Fa0/1        1           1                 0         Shutdown
        Fa0/2        1           1                 0         Shutdown
        Fa0/3        1           1                 0         Shutdown
----------------------------------------------------------------------
DNS_SW#
DNS_SW#
DNS_SW#
DNS_SW#
DNS_SW#
DNS_SW#
DNS_SW#
DNS_SW#
DNS_SW#
DNS_SW#
DNS_SW#
DNS_SW#
```

```
DNS_SW#
DNS_SW#
DNS_SW#
DNS_SW#sh port-security address
                              Secure Mac Address Table
-------------------------------------------------------------------------------
-
Vlan      Mac Address         Type                          Ports
Remaining Age

(mins)
----      -----------         ----                          -----
-------------
10        00E0.F9AA.35CB      SecureSticky                  FastEthernet0/1
          -
10        00D0.BCCD.0078      SecureSticky                  FastEthernet0/2
          -
10        0001.97E9.73B6      SecureSticky                  FastEthernet0/3
          -
-------------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)      : 0
Max Addresses limit in System (excluding one mac per port) : 1024
DNS_SW#
DNS_SW#
DNS_SW#
DNS_SW#
DNS_SW#
DNS_SW#
DNS_SW#
DNS_SW#
```

Figure 23: Port Security (SHUTDOWN) configured on DNS_SW access ports

DNS_SW follows the same port security approach. Each port only enables traffic from a single MAC Address, as seen in the diagram. The port can be configured to limit the amount of acceptable MAC Addresses and to manually specify approved MAC Addresses by the network administrator. The port security applied in DNS SW is set to "Sticky" in this circumstance (Dynamic learn MAC Address and store in the database, it will not be discarded even after reboot the system). The ageing timer, on the other hand, is not specified because it is anticipated that each port would only have one PC attached to it.

However, unlike HR_SW, the interface becomes error-disabled and shuts down instantly if a port security violation occurs, and the port LED goes off. A syslog message will record the suspicion packet. When a secure port is deactivated due to an error, network administrators have to use no shut down configuration commands to manually reactivate it.

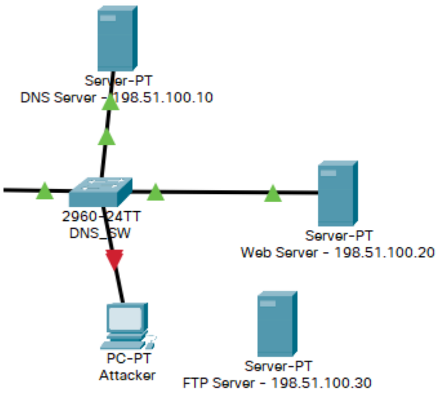
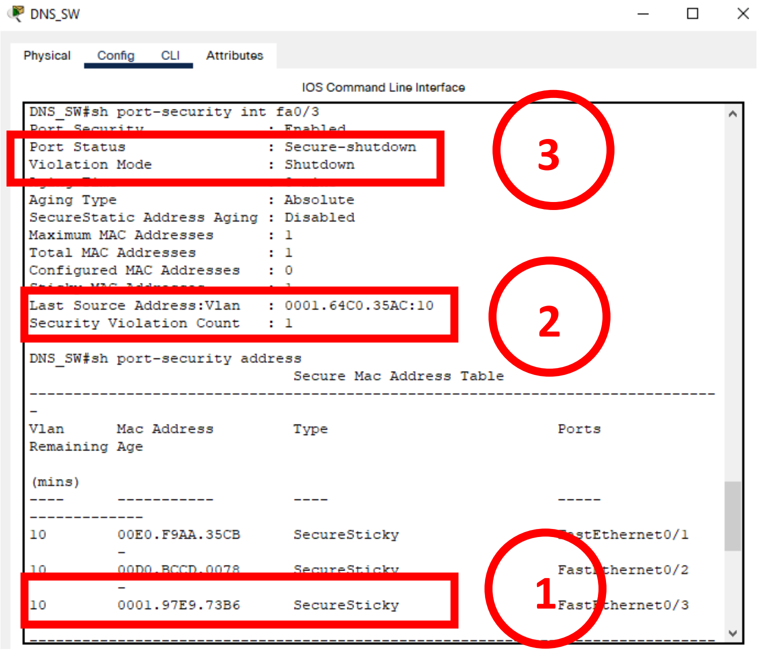

Server-PT
DNS Server - 198.51.100.10
2960-24TT
DNS_SW
Server-PT
Web Server - 198.51.100.20
PC-PT
Attacker
Server-PT
FTP Server - 198.51.100.30

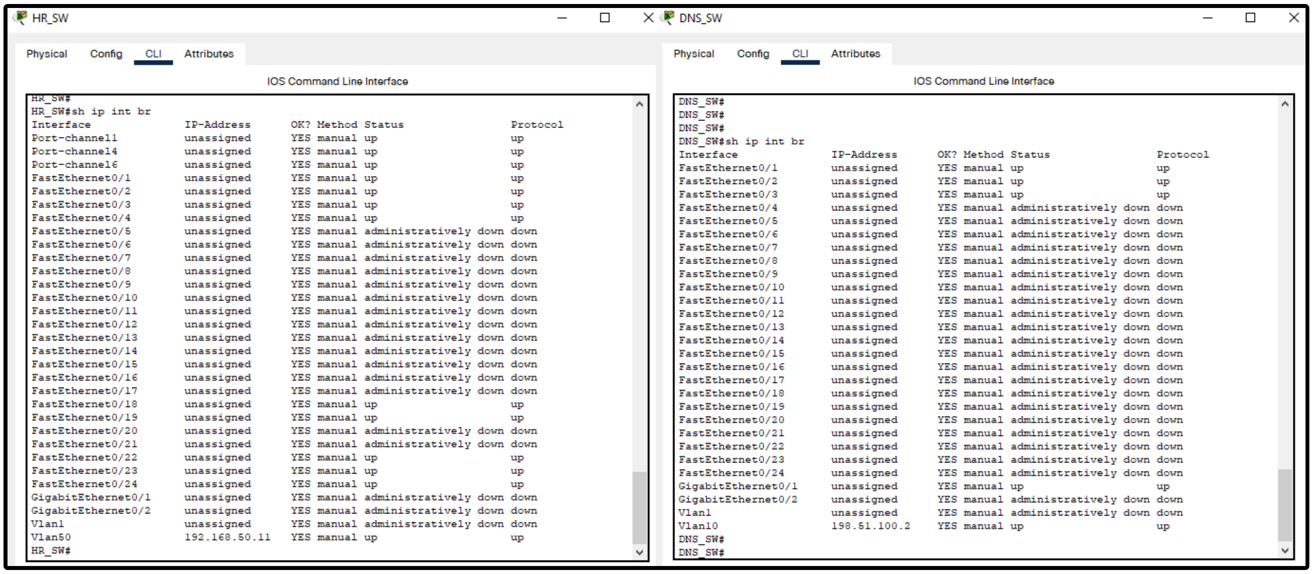
Figure 24: Example of port security violation (Attacker PC connect to fa0/3 interface in DNS_SW)



```
DNS_SW#sh port-security int fa0/3
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0001.64C0.35AC:10
Security Violation Count   : 1

DNS_SW#sh port-security address
                              Secure Mac Address Table
------------------------------------------------------------------------------
-
Vlan      Mac Address         Type                          Ports
Remaining Age

(mins)
----      -----------         ----                          -----
-------------
10        00E0.F9AA.35CB      SecureSticky                  FastEthernet0/1
          -
10        00D0.BCCD.0078      SecureSticky                  FastEthernet0/2
          -
10        0001.97E9.73B6      SecureSticky                  FastEthernet0/3
------------------------------------------------------------------------------
```

Figure 25: Security violation count: 1 due to unmatched Mac Address

Based on both figures above, if the attacker pc connected to interface fa0/3 in DNS_SW (server farm switch that already configure with port-security), it will be consider as security violation as the interface has been configured that only accepted one mac address (FTP Server MAC Address: **0001.97E9.73B6**) (1). The attacker pc mac address does not match will the FTP Server MAC Address, thus the last source access/vlan (attacker pc mac address) will be record in the syslog message (2) and the interface will be shutdown due to the violation mode is shutdown (3). The only way to reactive the interface is to manually configure the interface to no shutdown.



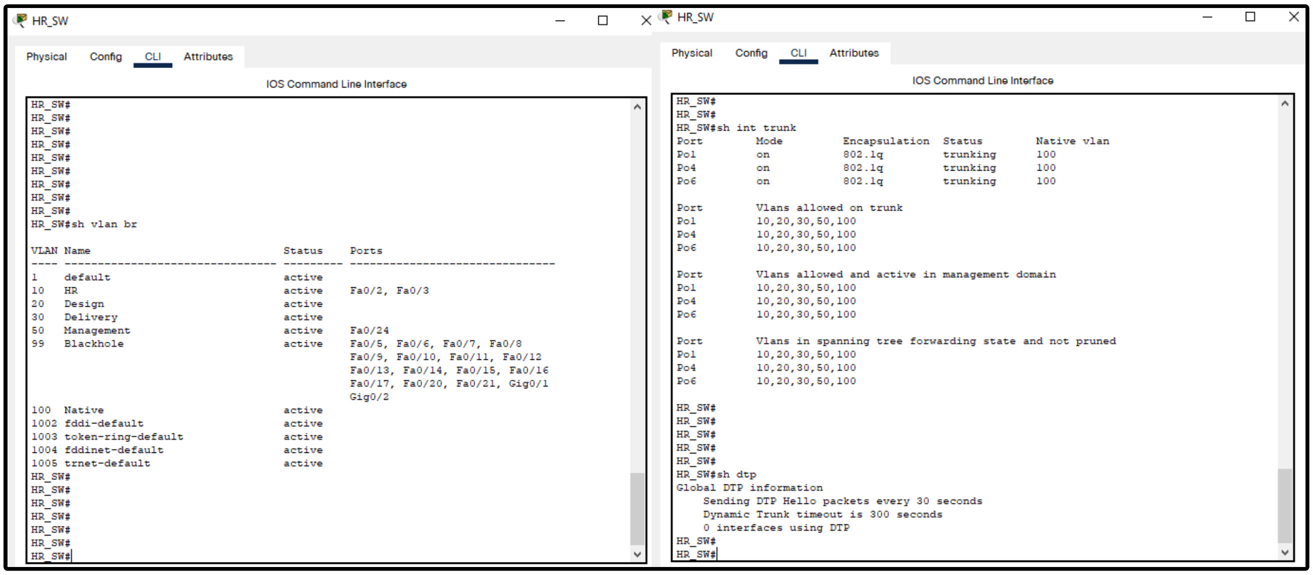
```
HR_SW#
HR_SW#sh ip int br
Interface              IP-Address      OK? Method Status                Protocol
Port-channel1          unassigned      YES manual up                    up
Port-channel4          unassigned      YES manual up                    up
Port-channel6          unassigned      YES manual up                    up
FastEthernet0/1        unassigned      YES manual up                    up
FastEthernet0/2        unassigned      YES manual up                    up
FastEthernet0/3        unassigned      YES manual up                    up
FastEthernet0/4        unassigned      YES manual up                    up
FastEthernet0/5        unassigned      YES manual administratively down down
FastEthernet0/6        unassigned      YES manual administratively down down
FastEthernet0/7        unassigned      YES manual administratively down down
FastEthernet0/8        unassigned      YES manual administratively down down
FastEthernet0/9        unassigned      YES manual administratively down down
FastEthernet0/10       unassigned      YES manual administratively down down
FastEthernet0/11       unassigned      YES manual administratively down down
FastEthernet0/12       unassigned      YES manual administratively down down
FastEthernet0/13       unassigned      YES manual administratively down down
FastEthernet0/14       unassigned      YES manual administratively down down
FastEthernet0/15       unassigned      YES manual administratively down down
FastEthernet0/16       unassigned      YES manual administratively down down
FastEthernet0/17       unassigned      YES manual administratively down down
FastEthernet0/18       unassigned      YES manual up                    up
FastEthernet0/19       unassigned      YES manual up                    up
FastEthernet0/20       unassigned      YES manual administratively down down
FastEthernet0/21       unassigned      YES manual administratively down down
FastEthernet0/22       unassigned      YES manual up                    up
FastEthernet0/23       unassigned      YES manual up                    up
FastEthernet0/24       unassigned      YES manual up                    up
GigabitEthernet0/1     unassigned      YES manual administratively down down
GigabitEthernet0/2     unassigned      YES manual administratively down down
Vlan1                  unassigned      YES manual administratively down down
Vlan50                 192.168.50.11   YES manual up                    up
HR_SW#
```

```
DNS_SW#
DNS_SW#
DNS_SW#
DNS_SW#sh ip int br
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/1        unassigned      YES manual up                    up
FastEthernet0/2        unassigned      YES manual up                    up
FastEthernet0/3        unassigned      YES manual up                    up
FastEthernet0/4        unassigned      YES manual administratively down down
FastEthernet0/5        unassigned      YES manual administratively down down
FastEthernet0/6        unassigned      YES manual administratively down down
FastEthernet0/7        unassigned      YES manual administratively down down
FastEthernet0/8        unassigned      YES manual administratively down down
FastEthernet0/9        unassigned      YES manual administratively down down
FastEthernet0/10       unassigned      YES manual administratively down down
FastEthernet0/11       unassigned      YES manual administratively down down
FastEthernet0/12       unassigned      YES manual administratively down down
FastEthernet0/13       unassigned      YES manual administratively down down
FastEthernet0/14       unassigned      YES manual administratively down down
FastEthernet0/15       unassigned      YES manual administratively down down
FastEthernet0/16       unassigned      YES manual administratively down down
FastEthernet0/17       unassigned      YES manual administratively down down
FastEthernet0/18       unassigned      YES manual administratively down down
FastEthernet0/19       unassigned      YES manual administratively down down
FastEthernet0/20       unassigned      YES manual administratively down down
FastEthernet0/21       unassigned      YES manual administratively down down
FastEthernet0/22       unassigned      YES manual administratively down down
FastEthernet0/23       unassigned      YES manual administratively down down
FastEthernet0/24       unassigned      YES manual administratively down down
GigabitEthernet0/1     unassigned      YES manual up                    up
GigabitEthernet0/2     unassigned      YES manual administratively down down
Vlan1                  unassigned      YES manual administratively down down
Vlan10                 198.51.100.2    YES manual up                    up
DNS_SW#
DNS_SW#
```

Figure 26: Unused port has been shut down

In addition to reinforce the security enhancement for port security, any unused port has been administratively shut down.

5.2 VLAN Attack Mitigation (Create New VLAN for Native VLAN, Disable Trunking Port and DTP)

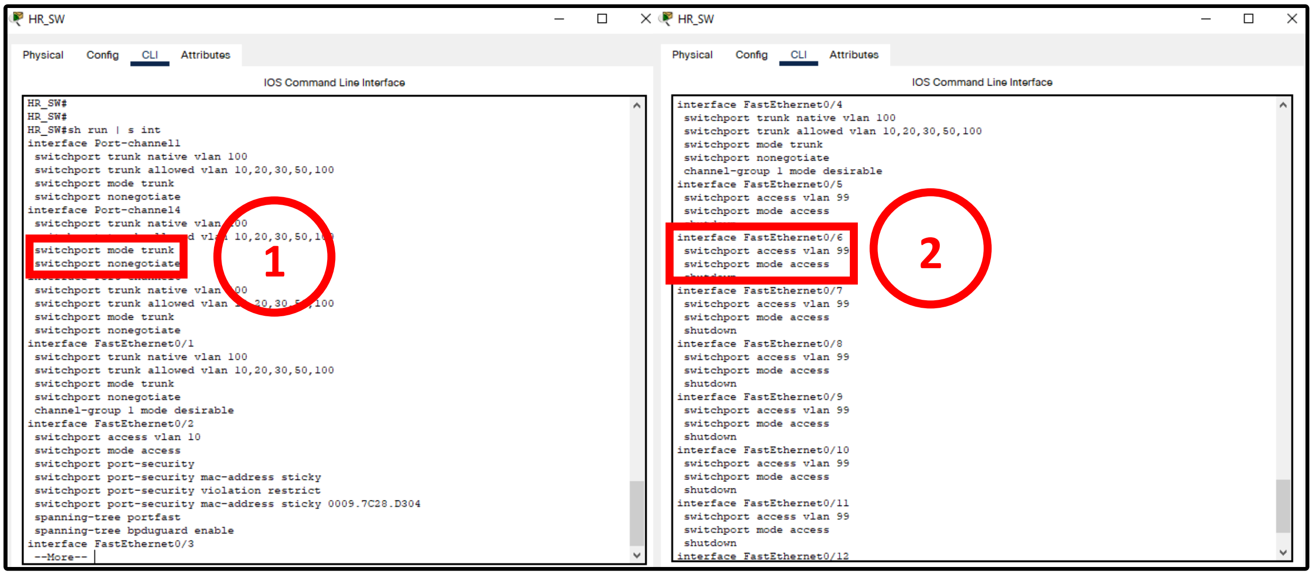


```
HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#sh vlan br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
10   HR                               active    Fa0/2, Fa0/3
20   Design                           active
30   Delivery                         active
50   Management                       active    Fa0/24
99   Blackhole                        active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/20, Fa0/21, Gig0/1
                                                Gig0/2
100  Native                           active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#
```

```
HR_SW#
HR_SW#
HR_SW#sh int trunk
Port        Mode         Encapsulation  Status        Native vlan
Po1         on           802.1q         trunking      100
Po4         on           802.1q         trunking      100
Po6         on           802.1q         trunking      100

Port        Vlans allowed on trunk
Po1         10,20,30,50,100
Po4         10,20,30,50,100
Po6         10,20,30,50,100

Port        Vlans allowed and active in management domain
Po1         10,20,30,50,100
Po4         10,20,30,50,100
Po6         10,20,30,50,100

Port        Vlans in spanning tree forwarding state and not pruned
Po1         10,20,30,50,100
Po4         10,20,30,50,100
Po6         10,20,30,50,100

HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#sh dtp
Global DTP information
    Sending DTP Hello packets every 30 seconds
    Dynamic Trunk timeout is 300 seconds
    0 interfaces using DTP
HR_SW#
HR_SW#
```

Figure 27: Native VLAN has been changed to VLAN 100, no interface used default VLAN 1

VLAN 1 is assigned to all switch ports by default. VLAN 1 is used to carry control plane communication and may also be used to carry user traffic. It is suggested that user traffic be routed over VLANs other than VLAN 1, largely to avoid the supervisor's Network Management Processor (NMP) processing superfluous user broadcast and multicast traffic. Based on the figure above, it is strongly recommended that Native VLAN should be configured in one VLAN (VLAN that no access port) and any unused port should assign to blackhole (VLAN) to prevent threat actors from accessing any VLAN (particularly Native VLAN) and carry out VLAN Double Tagging Attack. Use show dtp command to review how many ports are connected to DTP (ensure it is 0).



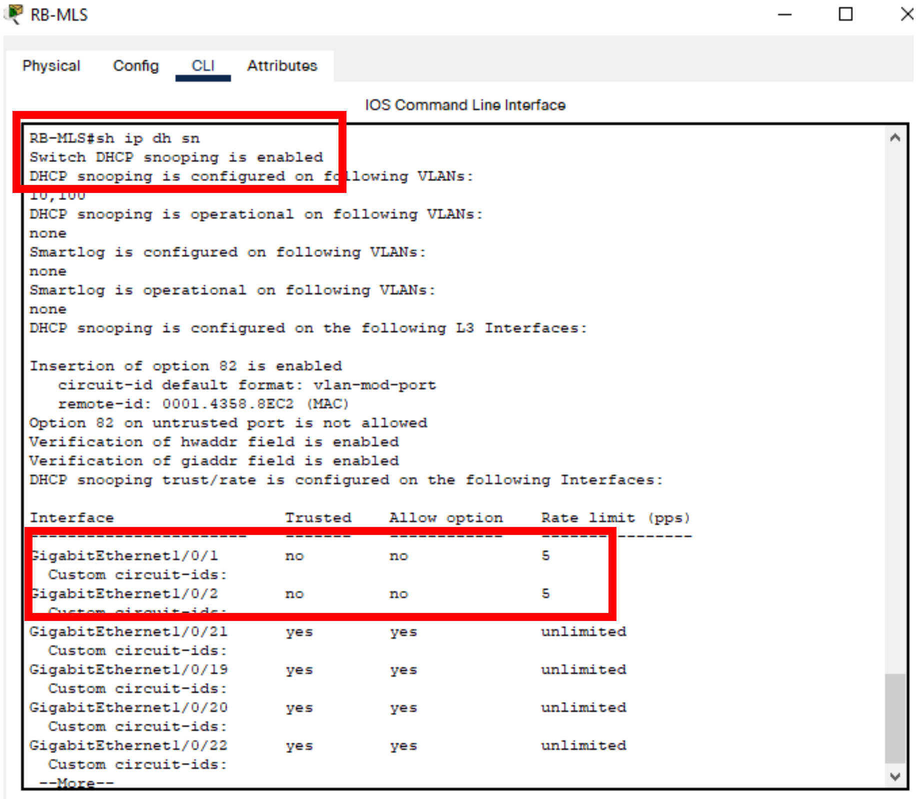
```
HR_SW#
HR_SW#
HR_SW#sh run | s int
interface Port-channel1
 switchport trunk native vlan 100
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
 switchport nonegotiate
interface Port-channel4
 switchport trunk native vlan 100
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
 switchport nonegotiate
interface Port-channel[illegible]
 switchport trunk native vlan 100
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
 switchport nonegotiate
interface FastEthernet0/1
 switchport trunk native vlan 100
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode desirable
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 0009.7C28.D304
 spanning-tree portfast
 spanning-tree bpduguard enable
interface FastEthernet0/3
 --More--
```

```
interface FastEthernet0/4
 switchport trunk native vlan 100
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode desirable
interface FastEthernet0/5
 switchport access vlan 99
 switchport mode access
 shutdown
interface FastEthernet0/6
 switchport access vlan 99
 switchport mode access
 shutdown
interface FastEthernet0/7
 switchport access vlan 99
 switchport mode access
 shutdown
interface FastEthernet0/8
 switchport access vlan 99
 switchport mode access
 shutdown
interface FastEthernet0/9
 switchport access vlan 99
 switchport mode access
 shutdown
interface FastEthernet0/10
 switchport access vlan 99
 switchport mode access
 shutdown
interface FastEthernet0/11
 switchport access vlan 99
 switchport mode access
 shutdown
interface FastEthernet0/12
```

Figure 28: Switchport nonegotiate on trunk port, Switchport mode access for non-trunk port

In addition to reinforce the security enhancement, it is necessary to implement “switchport nonegotiate” command when configure trunk port (1). Any port that is not trunk port should be assign as access port and if the access port is unused, consider implement “shutdown” command (2) to avoid Switch Spoofing Attack.

5.3 DHCP Attack Mitigation (DHCP Snooping and DHCP Rate Limit)

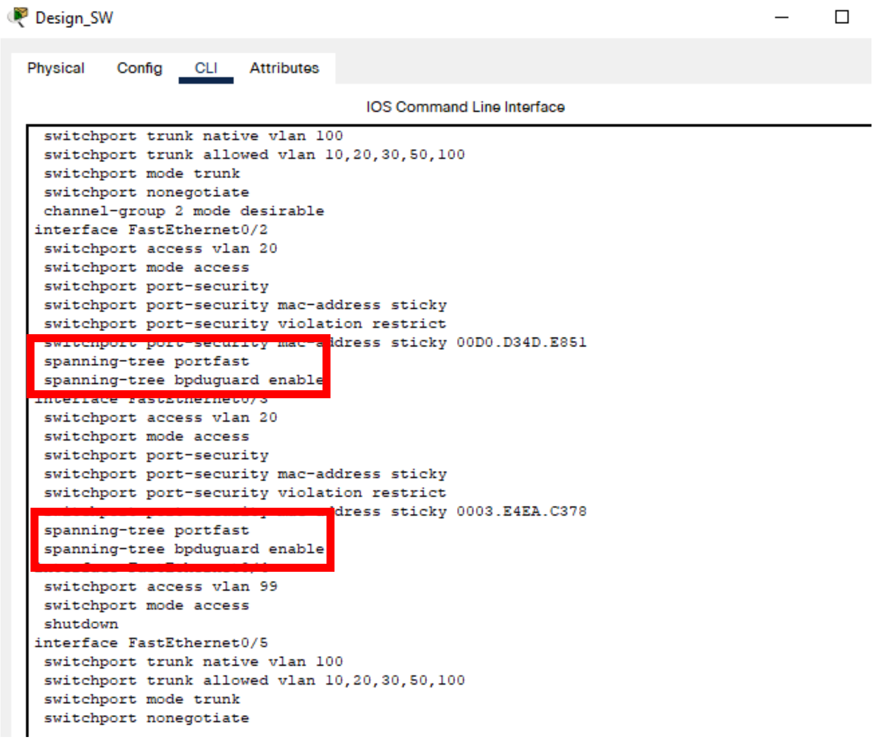


```
RB-MLS#sh ip dh sn
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10,100
DHCP snooping is operational on following VLANs:
none
Smartlog is configured on following VLANs:
none
Smartlog is operational on following VLANs:
none
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
   circuit-id default format: vlan-mod-port
   remote-id: 0001.4358.8EC2 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                  Trusted    Allow option    Rate limit (pps)
-----------------------    -------    ------------    ----------------
GigabitEthernet1/0/1       no         no              5
  Custom circuit-ids:
GigabitEthernet1/0/2       no         no              5
  Custom circuit-ids:
GigabitEthernet1/0/21      yes        yes             unlimited
  Custom circuit-ids:
GigabitEthernet1/0/19      yes        yes             unlimited
  Custom circuit-ids:
GigabitEthernet1/0/20      yes        yes             unlimited
  Custom circuit-ids:
GigabitEthernet1/0/22      yes        yes             unlimited
  Custom circuit-ids:
 --More--
```

Figure 29: DHCP Snooping enable in Remote Branch Multi-Layer Switch (RB_MLS) and the rate is set to 5PPS

According to the figure above, DHCP Snooping has been enable in Remote Branch Multi-Layer Switch on VLAN 10 and 100 and the untrusted interface (access port that are used) are rate limited to 5 PPS. DHCP came from 2 ways, DHCP Starvation Attacks (leads to DDoS) or DHCP Spoofing (leads to Middle in Man Attack). Despite that port security assist in mitigate DHCP Starvation Attacks, there is an occasion where a malicious software is used to depleted the available DHCP IP Address causing address pool exhausted. Meanwhile, DHCP Spoofing Attack represent a threat actor successfully bypassing port security and uses a rogue DHCP Server device as address pool. Thus, DHCP Snooping is enable to limit the rate of DHCP traffic thus attacker unable to send DHCPOFFER messages to client as rogue server.

5.4 STP Attack Mitigation (PortFast and BPDU Guard)

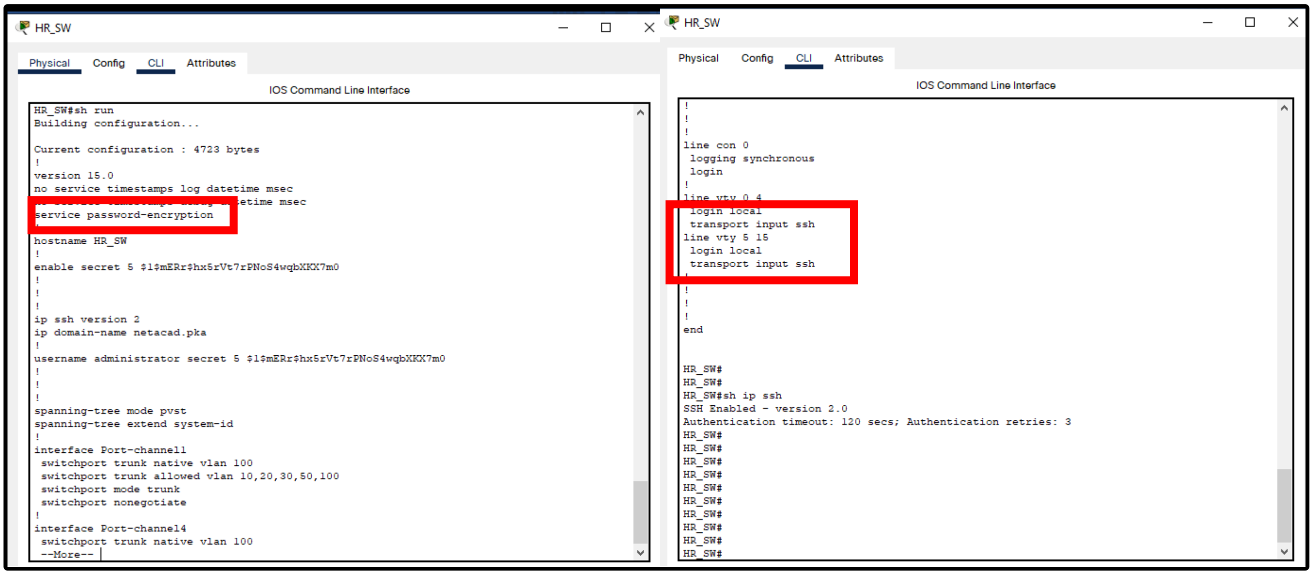


```
 switchport trunk native vlan 100
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode desirable
interface FastEthernet0/2
 switchport access vlan 20
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 00D0.D34D.E851
 spanning-tree portfast
 spanning-tree bpduguard enable
interface FastEthernet0/3
 switchport access vlan 20
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 0003.E4EA.C378
 spanning-tree portfast
 spanning-tree bpduguard enable
interface FastEthernet0/4
 switchport access vlan 99
 switchport mode access
 shutdown
interface FastEthernet0/5
 switchport trunk native vlan 100
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
 switchport nonegotiate
```

Figure 30: Configuration of PortFast and BPDU Guard

Based on the figure shown above, PortFast and BPDU Guard is enable in Design_SW interface fa0/2 and interface fa0/3 (both interfaces are access port). PortFast immediately switches an interface configured as an access or trunk port from blocking to forwarding, skipping the listening and learning processes. With BPDU protection enabled, an attacker will be unable to force root bridge election since the BPDU message will be refused on the port to which they are connected. Thus, Spanning Tree Protocol Attack is mitigated.

6.0 Secure Remote Access (SSH and ACL)

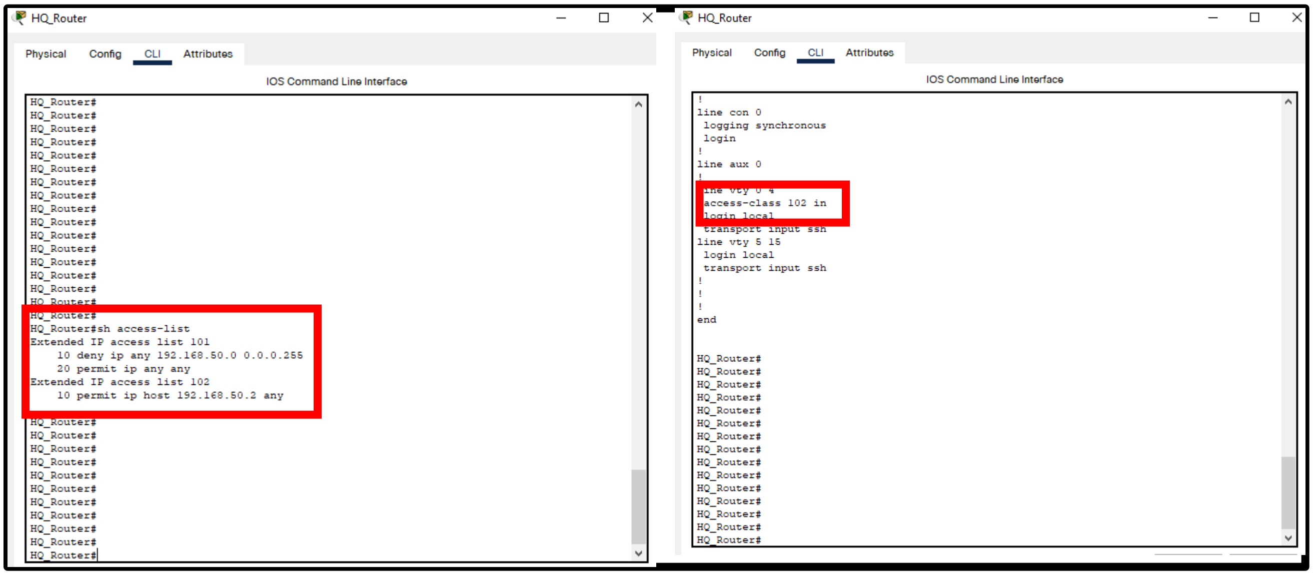


```
HR_SW#sh run
Building configuration...

Current configuration : 4723 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname HR_SW
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
!
!
ip ssh version 2
ip domain-name netacad.pka
!
username administrator secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface Port-channel1
 switchport trunk native vlan 100
 switchport trunk allowed vlan 10,20,30,50,100
 switchport mode trunk
 switchport nonegotiate
!
interface Port-channel4
 switchport trunk native vlan 100
 --More--
```

```
!
!
!
line con 0
 logging synchronous
 login
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
!
!
!
end


HR_SW#
HR_SW#
HR_SW#sh ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#
HR_SW#
```

Figure 31: SSH Configuration

Based on the figure shown above, the HR_SW telnet protocol has been disabled and replace with SSH as line vty 0-15 shows "transport input shh" which delivers the meaning of only SSH connection is accepted. At the same time, the password or secret is encrypted with the command "service password encryption". Thus, the encrypted SSH login password is store locally and the credential is received by the switch in encrypted form.



```
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#sh access-list
Extended IP access list 101
    10 deny ip any 192.168.50.0 0.0.0.255
    20 permit ip any any
Extended IP access list 102
    10 permit ip host 192.168.50.2 any

HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
```

```
!
line con 0
 logging synchronous
 login
!
line aux 0
!
line vty 0 4
 access-class 102 in
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
!
!
end


HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
HQ_Router#
```

Figure 32: ACL Configuration

Based on the figure shown above, HQ Router contains ACL 10 to permits the host with IP Address of 192.168.50.2 which is the IP Address for Management PC in HQ Network. The command "access-class

102 in" means that only inbound management from the Management-PC is allowed to access the teletype line. Any device that has no connection with the management VLAN in HQ Network will be denied access by ACL as it filtering out non-management traffic or non-SSH traffic.

7.0 Conclusion for Section B

The network executive's prototype network design for Fiberoptic Systems Inc. has been taken into consideration. VLAN and Inter-VLAN Routing are network configurations that allow separated employees from each department to connect to their own network and interact through a router. All routers in the prototype network are configured with the dynamic routing protocol OSPF, which facilitates communication across all three LANS (headquarter, DMZ Zone and the remote branch). Static IP addresses are used for host devices at the headquarters and in the DMZ Zone, whereas hosts in the distant branch use DHCP to simplify their network configuration.

At the same, various Layer 2 Security Mechanisms Deployment is configured in order to mitigate any possible Layer 2 Security Attacks (MAC Address Table Attack, VLAN Attack, DHCP Attack, STP Attack). SSH and ACL is configured for further security enhancement purpose.

References

CCNA. (n.d.). *What is EtherChannel and Why Do We Need It?* Retrieved February 26, 2022, from CCNA: https://study-ccna.com/what-is-etherchannel/

CCNA2. (n.d.). *DHCPv4 Concepts*. Retrieved February 25, 2022, from CCNA: https://ccna-200-301.online/dhcpv4-concepts/

CertificationKits. (n.d.). *InterVLAN Routing, Router on a Stick & Configuration*. Retrieved February 26, 2022, from CertificationKits: https://www.certificationkits.com/cisco-certification/ccna-articles/cisco-ccna-vlans-virtual-lans/intervlan-routing-router-on-a-stick-a-configuration/

IBM. (n.d.). *Open Shortest Path First*. Retrieved February 26, 2022, from IBM: https://www.ibm.com/docs/en/i/7.2?topic=routing-open-shortest-path-first

Kaspersky. (n.d.). *What is an IP Address – Definition and Explanation*. Retrieved February 23, 2022, from https://www.kaspersky.com/resource-center/definitions/what-is-an-ip-address

N-able. (2019, July 8). *How VLAN Works*. Retrieved February 24, 2022, from N-able: https://www.n-able.com/blog/what-are-vlans

NetgateDocs. (n.d.). *Layer 2 Redundancy*. Retrieved February 26, 2022, from NetgateDocs: https://docs.netgate.com/pfsense/en/latest/highavailability/layer-2-redundancy.html