Scenario

MEMBERS:

Lava, Maria Kassandra Ileana
Parreno, Emmanuel P.

SCENARIO:

StarCollabs2025 needs to establish a network that will connect their new talents. Funded by Star Magic, they are launching a collaboration between BINI (a Filipino girl group) and Twice (a Korean girl group). The headquarters of the two girl groups will be situated at the same location at Malvar, Batangas. StarCollabs requires you to create an efficient, secure, and scalable network for the headquarters.

Requirements:

1. Two VLANs per group:
    a. Talents VLAN
    b. Managers VLAN
2. A Management VLAN
3. Good Fault tolerance (Layer 2 and 3 redundancy)
4. One wired device and wireless device for each idol and manager
5. Connection to an ISP/internet
6. Admins should be able to SSH into switches
7. Secure intermediary devices
8. Hierarchical network (core, distribution, and access layers)
9. Efficient allocation of IP
10. Centralized AP control

Table of Content

Approach:

The hired network architects' first step was to create the network topology. The network topology was made with Layer 2 and Layer 3 redundancy in mind, as well as efficiency.

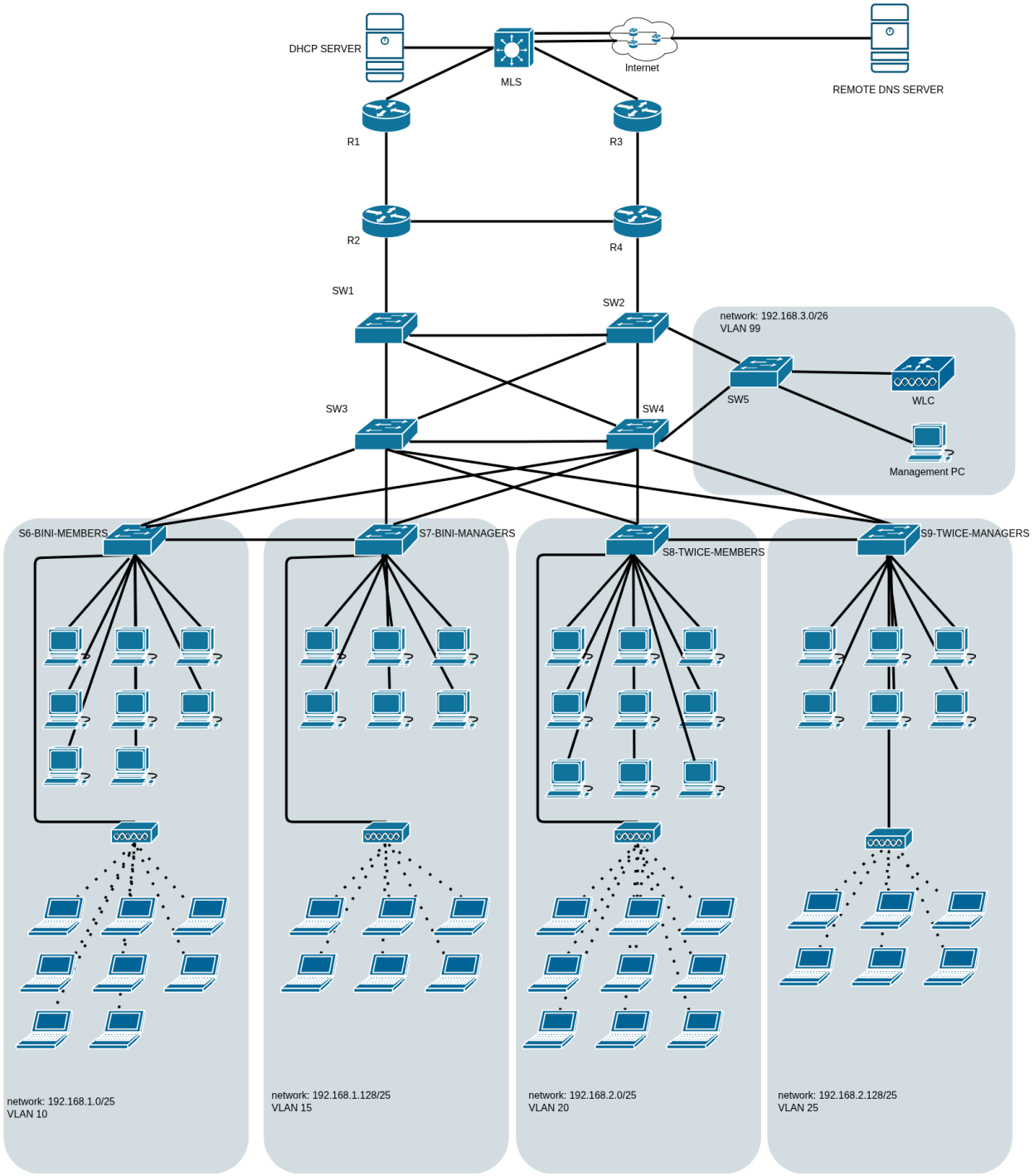

FIGURE 1. NETWORK TOPOLOGY DRAFT

After creating the visual representation of the network topology, the network was then transferred into cisco packet tracer.

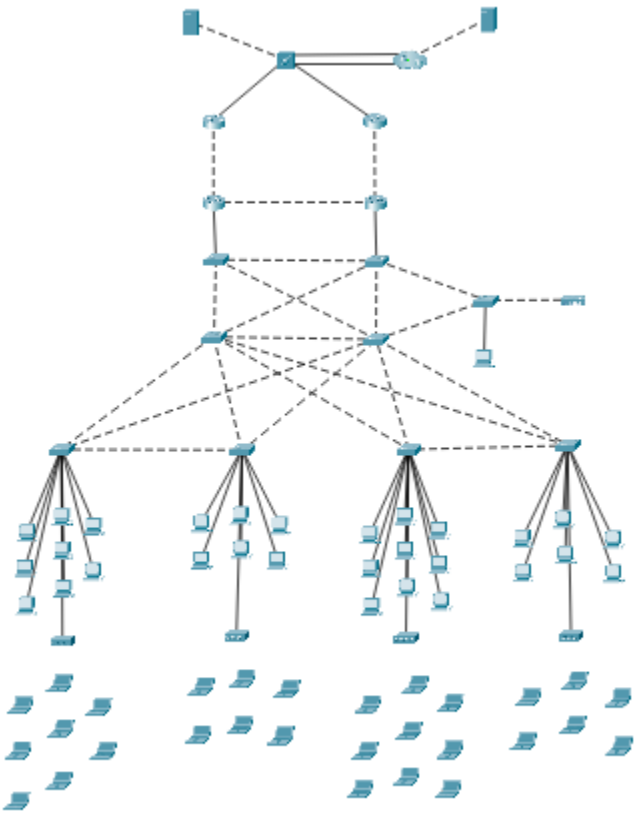

FIGURE 2. Network topology in cisco packet tracer

Then, the network was labeled with their respected network areas and host names. The network related labels were obtained through the use of VLSM

Name	Hosts Needed	Hosts Available	Unused Hosts	Network Address	Slash	Mask	Usable Range	Broadcast	Wildcard
BINI-Members-subnet	100	126	26	192.168.1.0	/25	255.255.255.128	192.168.1.1 - 192.168.1.126	192.168.1.127	0.0.0.127
BINI-Managers-subnet	100	126	26	192.168.1.128	/25	255.255.255.128	192.168.1.129 - 192.168.1.254	192.168.1.255	0.0.0.127
TWICE-Members-subnet	100	126	26	192.168.2.0	/25	255.255.255.128	192.168.2.1 - 192.168.2.126	192.168.2.127	0.0.0.127
TWICE-Managers-subnet	100	126	26	192.168.2.128	/25	255.255.255.128	192.168.2.129 - 192.168.2.254	192.168.2.255	0.0.0.127
Management	50	62	12	192.168.3.0	/26	255.255.255.192	192.168.3.1 - 192.168.3.62	192.168.3.63	0.0.0.63
link R1 to MLS	5	6	1	192.168.3.64	/29	255.255.255.248	192.168.3.65 - 192.168.3.70	192.168.3.71	0.0.0.7
link R1 to R2	5	6	1	192.168.3.72	/29	255.255.255.248	192.168.3.73 - 192.168.3.78	192.168.3.79	0.0.0.7
link R2 to R4	5	6	1	192.168.3.80	/29	255.255.255.248	192.168.3.81 - 192.168.3.86	192.168.3.87	0.0.0.7
link R3 to MLS	5	6	1	192.168.3.88	/29	255.255.255.248	192.168.3.89 - 192.168.3.94	192.168.3.95	0.0.0.7
link R3 to R4	5	6	1	192.168.3.96	/29	255.255.255.248	192.168.3.97 - 192.168.3.102	192.168.3.103	0.0.0.7
link R5 to MLS	5	6	1	192.168.3.104	/29	255.255.255.248	192.168.3.105 - 192.168.3.110	192.168.3.111	0.0.0.7
link R5 to R6	5	6	1	192.168.3.112	/29	255.255.255.248	192.168.3.113 - 192.168.3.118	192.168.3.119	0.0.0.7
link R5 to R7	5	6	1	192.168.3.120	/29	255.255.255.248	192.168.3.121 - 192.168.3.126	192.168.3.127	0.0.0.7
link R6 to R7	5	6	1	192.168.3.128	/29	255.255.255.248	192.168.3.129 - 192.168.3.134	192.168.3.135	0.0.0.7
link R6 to dns server	5	6	1	192.168.3.136	/29	255.255.255.248	192.168.3.137 - 192.168.3.142	192.168.3.143	0.0.0.7
link R7 to MLS	5	6	1	192.168.3.144	/29	255.255.255.248	192.168.3.145 - 192.168.3.150	192.168.3.151	0.0.0.7
link MLS to DHCP Server	5	6	1	192.168.3.152	/29	255.255.255.248	192.168.3.153 - 192.168.3.158	192.168.3.159	0.0.0.7
link R1 to R3	5	6	1	192.168.3.160	/29	255.255.255.248	192.168.3.161 - 192.168.3.166	192.168.3.167	0.0.0.7

Figure 3. VLSM table

If examined, it can be seen that the links which usually only require two hosts (thus the prefix /30) requires 6. This was made by design. The network architects took into consideration the future expansion of the network, which might require more addresses.

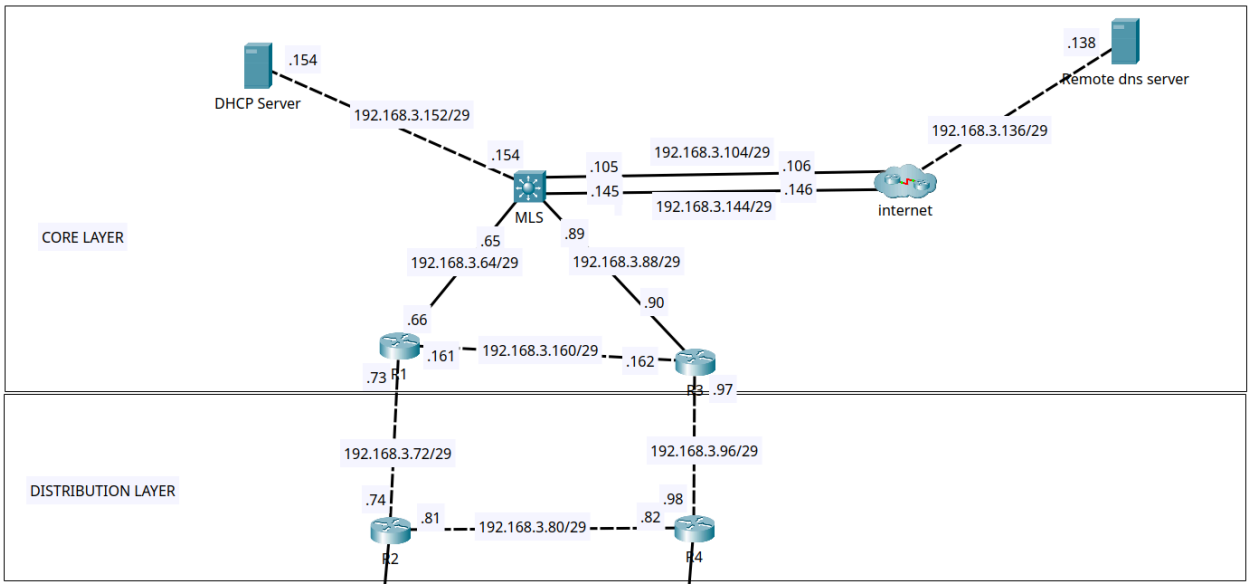

FIGURE 4.1. Labeled topology: core and distribution layers

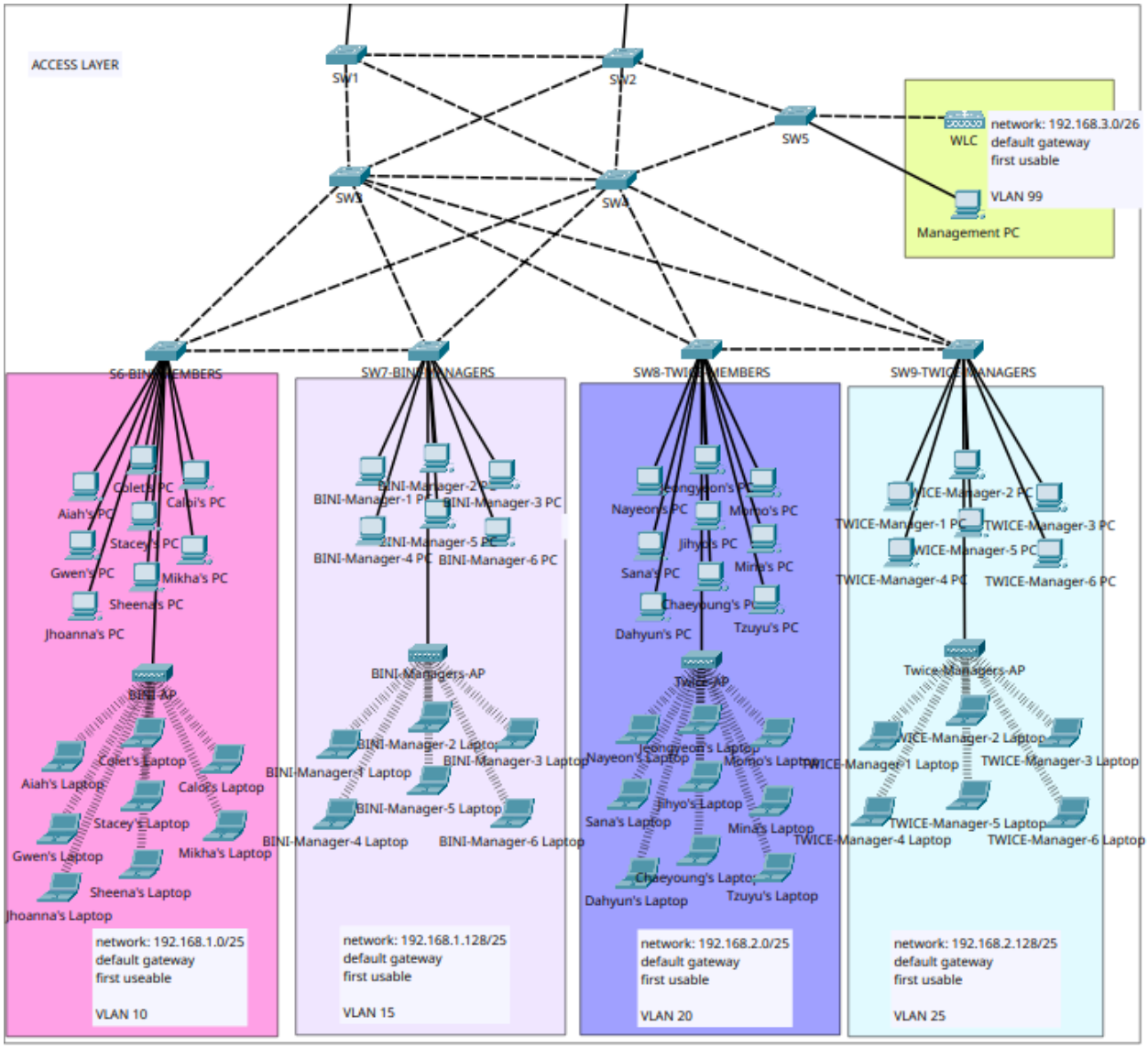

Figure 4. Labeled topology: access layer

As per the requirements, the topology follows a hierarchical structure: core layer, distribution layer, and access layer. Such a structure is more efficient and easier to maintain and diagnose.

Device name	Port	Connected to	IP address	Subnet Mask	Default gateway
MLS	fa0/1	DHCP Server port fa0	192.168.3.153	255.255.255.248	
	fa0/2	R5 port g0/0	192.168.3.105	255.255.255.248	
	fa0/3	R7 port g0/0	192.168.3.145	255.255.255.248	
	g0/1	R1 port g0/0	192.168.3.65	255.255.255.248	
	g0/2	R3 port g0/2	192.168.3.89	255.255.255.248	
DHCP Server	fa0	MLS port fa0/1	192.168.3.154	255.255.255.248	192.168.3.153
R1	g0/0	MLS port g0/1	192.168.3.66	255.255.255.248	
	g0/2	R2 port g0/2	192.168.3.73	255.255.255.248	
	g0/1	R3 port g0/0	192.168.3.161	255.255.255.248	
R2	g0/2	R1 port g0/2	192.168.3.74	255.255.255.	

				248	
	g0/0	R4 port g0/0	192.168.3.81	255.255.255.248	
R2 subinterfaces	g0/1.10	SW1 port g0/1	192.168.1.2	255.255.255.128	
	g0/1.15	SW1 port g0/1	192.168.1.130	255.255.255.128	
	g0/1.20		192.168.2.2	255.255.255.128	
	g0/1.25		192.168.2.130	255.255.255.128	
	g0/1.99		192.168.3.2	255.255.255.192	
R3	g0/2	MLS port g0/2	192.168.3.90	255.255.255.248	
	g0/1	R4 port g0/1	192.168.3.97	255.255.255.248	
	g0/0	R1 port g0/1	192.168.3.162	255.255.255.248	
R4	g0/1	R3 port g0/1	192.168.3.98	255.255.255.248	

	g0/0	R2 port g0/0	192.168.3.82	255.255.255.248	
R4 subinterfaces	g0/2.10	SW2 port g0/2	192.168.1.3	255.255.255.128	
	g0/2.15	SW2 port g0/2	192.168.1.131	255.255.255.128	
	g0/2.20	SW2 port g0/2	192.168.2.3	255.255.255.128	
	g0/2.25	SW2 port g0/2	192.168.2.131	255.255.255.128	
	g0/2.99	SW2 port g0/2	192.168.3.3	255.255.255.192	
R5	g0/0	MLS port fa0/2	192.168.3.106	255.255.255.248	
	g0/1	R6 port g0/1	192.168.3.113	255.255.255.248	
	g0/2	R7 port g0/2	192.168.3.121	255.255.255.248	

R6	g0/1	R5 port g0/1	192.168.3.114	255.255.255.248	
	g0/2	R7 g0/1	192.168.3.129	255.255.255.248	
	g0/0	DNS Server port f0	192.168.3.137	255.255.255.248	
R7	g0/1	R6 port g0/2	192.168.3.130	255.255.255.248	
	g0/2	R5 port g0/2	192.168.3.122	255.255.255.248	
	g0/0	MLS port fa0/3	192.168.3.146	255.255.255.248	
Remote DNS Server	fa0	R6 port g0/0	192.168.3.138	255.255.255.248	192.168.3.137
All end devices under VLAN10, VLAN15,VLAN20,VLAN25, VLAN99, and all LAP PTs			Dynamically obtained	Dynamically obtained	Dynamically obtained

SW1	VLAN99		192.168.3.6	255.255.255.192	192.168.3.1
SW2	VLAN99		192.168.3.7	255.255.255.192	192.168.3.1
SW3	VLAN99		192.168.3.8	255.255.255.192	192.168.3.1
SW4	VLAN99		192.168.3.9	255.255.255.192	192.168.3.1
SW5	VLAN99		192.168.3.10	255.255.255.192	192.168.3.1
S6-BINI-MEMBERS	VLAN99		192.168.3.11	255.255.255.192	192.168.3.1
SW7-BINI-MANAGERS	VLAN99		192.168.3.12	255.255.255.192	192.168.3.1
SW8-TWICE-MEMBERS	VLAN99		192.168.3.13	255.255.255.192	192.168.3.1
SW9-TWICE-MANAGERS	VLAN99		192.168.3.14	255.255.255.192	192.168.3.1

TABLE 1. Addressing table

The addressing table was based on the VLSM table (figure 3). The address of the subinterfaces are the default gateway of the

VLAN and Inter-VLAN Routing

The requirements specified five VLANs: VLAN for members of BINI, members of TWICE, managers of BINI, managers of TWICE, and Management VLAN. The table Below shows the VLANs created in the switches

VLAN ID	Name
10	BINI-members
15	BINI-managers
20	Twice-members
25	Twice-managers
99	Management

TABLE 2. VLANS

The VLANs were created on all switches with the following commands:

```
SW4>enable
SW4#configure terminal
SW4(config)#vlan 10
SW4(config-vlan)#name BINI-members
SW4(config-vlan)#vlan 15
SW4(config-vlan)#name BINI-managers
SW4(config-vlan)#vlan 20
SW4(config-vlan)#name Twice-members
SW4(config-vlan)#vlan 25
SW4(config-vlan)#name Twice-managers
SW4(config-vlan)#vlan 99
SW4(config-vlan)#name Management
```

FIGURE 5. VLAN creation sample configuration

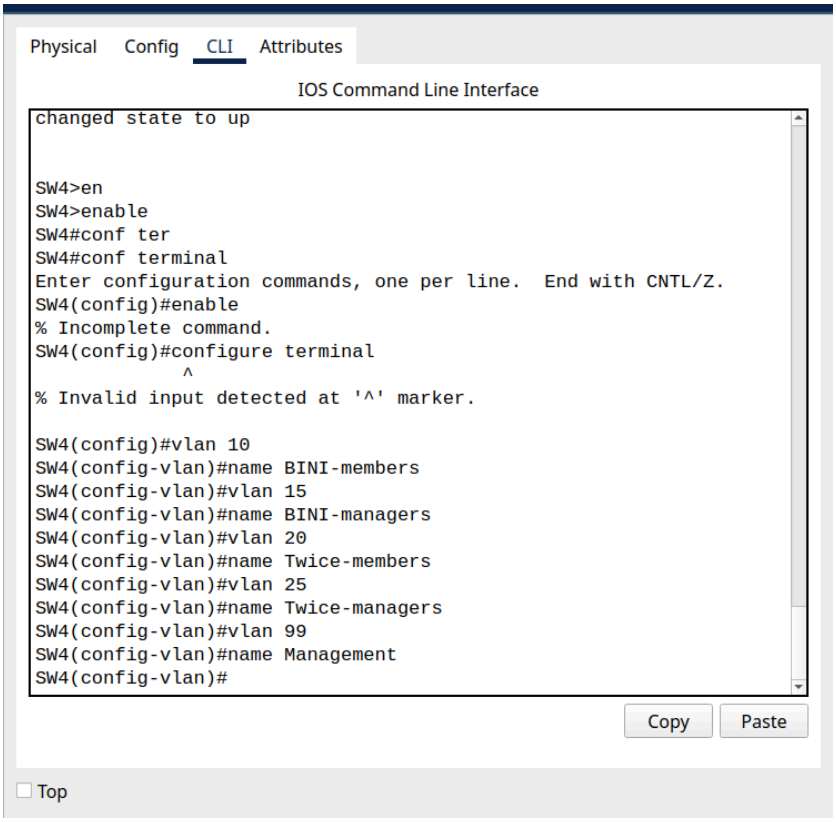

FIGURE 6. VLAN creation on packet tracer

After the VLANs are created on the switches, ports are assigned to their respective VLANs with the interface configuration command ‘switchport mode access’ and ‘switchport access vlan ID’. The following table shows the ports of the switches, their VLANs and respective modes.

Device	Port	Mode	VLAN ID
S6-BINI-MEMBERS	fastEthernet 0/1-8	access	10
S7-BINI-MANAGERS	fastEthernet 0/1-6	access	15
SW8-TWICE-MEMBERS	fastEthernet 0/1-9	access	20
SW9-TWICE-MANAGERS	fastEthernet 0/1-6	access	25

SW5	fastEthernet 0/1	access	99

TABLE 3. Access ports

```
S6-BINI-MEMBERS(config)#interface range fastEthernet 0/1-8
S6-BINI-MEMBERS(config-if-range)#switchport mode access
S6-BINI-MEMBERS(config-if-range)#switchport access
S6-BINI-MEMBERS(config-if-range)#switchport access vlan 10
```

FIGURE 7. Port assignment sample configuration

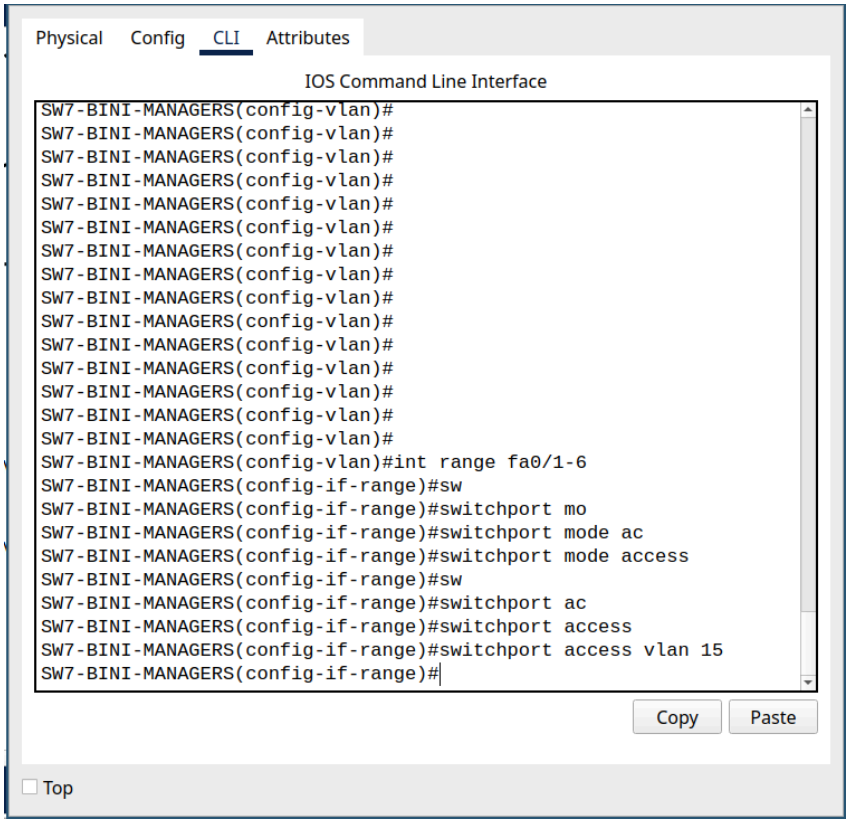

FIGURE 9. Port assignment sample configuration

Vlan trunks can be seen as conduits where different VLANs flow through. They are necessary for a network that requires VLANs. VLAN trunks must be configured on all router to switch, switch to switch, switch to LAP PT, and switch to WLC connections. The following commands were entered on all of the switches

```
Hostname (config)#  interface interface-identifier
Hostname (config-if-range)#  switchport mode access
Hostname (config-if-range)#   switchport mode trunk
Hostname (config-if-range)#   switchport nonegotiate
Hostname (config-if-range)#   switchport trunk allowed vlan 10,15,20,25,99
Hostname (config-if-range)#  switchport trunk native vlan 99
```

FIGURE 10. VLAN trunks configuration

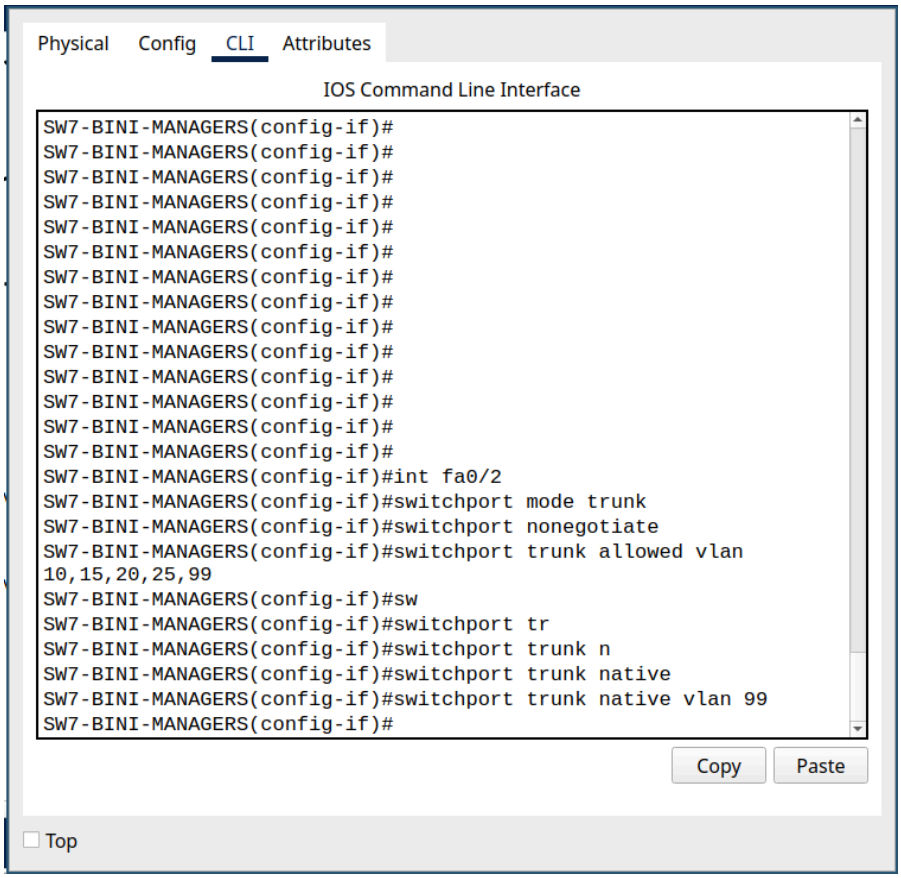

FIGURE 11. Trunking sample configuration

*NOTE: the **'switchport trunk native vlan 99'** command should not be entered on links going to default gateway. For some reason, in packet tracer, the network on the same VLAN (let's say VLAN 99 and its network address), will not be able to form an HSRP connection and also won't go through the intended default gateway.*

All the trunks were configured in manual mode (with DTP disabled). This is to ensure the security of the network (to only allow necessary VLANs).

After the VLAN trunks are configured and the access ports are done, inter-vlan is then configured. Refer to the addressing table above (table 1) for reference. The interfaces that will be configured are the subinterfaces of R2 port g0/1 and R4 port g0/2. ***Take note that in this topology, the inter-VLAN won't work without configuring the HSRP*** (as virtual interfaces will act as the default gateway for all VLANs).

```
R2(config-if)#int g0/1.99
R2(config-subif)#encapsulation dot1Q
R2(config-subif)#encapsulation dot1Q
R2(config-subif)#encapsulation dot1Q 99
R2(config-subif)#ip address 192.168.3.2 255.255.255.192
R2(config-subif)#int g0/1
R2(config-if)#no shutdown
```

FIGURE 12. Subinterface configuration

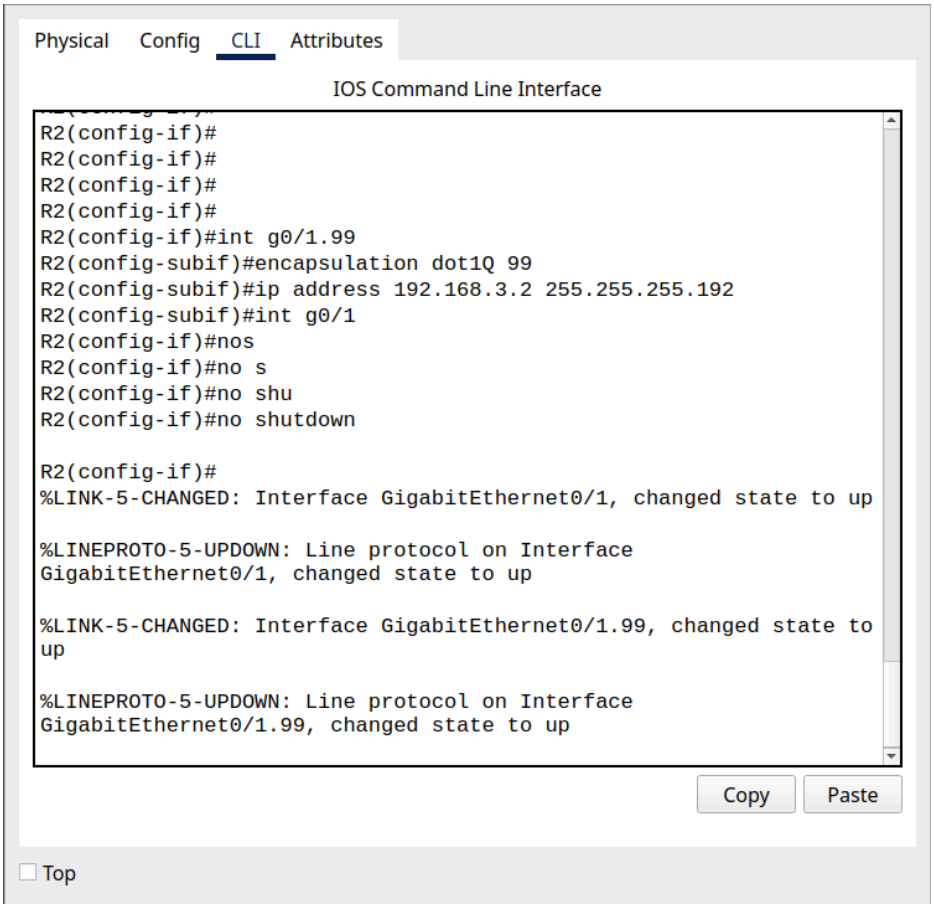

FIGURE 13. Subinterface sample configuration

Layer 3 Redundancy (HSRP)

The following table shows the configuration for HSRP (Layer 3 redundancy). The subinterfaces which are usually used as default gateways were configured with virtual interfaces that will act as default gateways. In this manner, the sub networks under the network are able to take advantage of HSRP.

Virtual Interfaces (HSRP)

Port	Commands	IP address (default gateways per VLAN)
R2 g0/1.10 Default gateway of VLAN 10	standby version 2 standby 10 ip 192.168.1.1 standby 10 priority 150 standby 10 preempt	192.168.1.1
R4 g0/2.10	standby version 2 standby 10 ip 192.168.1.1	192.168.1.1
R2 g0/1.15	standby version 2 standby 15 ip 192.168.1.129 standby 15 priority 150 standby 15 preempt	192.168.1.129
R4 g0/2.15	standby version 2 standby 15 ip 192.168.1.129	192.168.1.129
R2 g0/1.20	standby version 2 standby 20 ip 192.168.2.1	192.168.2.1
R4 g0/2.20	standby version 2 standby 20 ip 192.168.2.1 standby 20 priority 150 standby 20 preempt	192.168.2.1

R2 g0/1.25	standby version 2 standby 25 ip 192.168.2.129	192.168.2.129
R4 g0/2.25	standby version 2 standby 25 ip 192.168.2.129 standby 25 priority 150 standby 25 preempt	192.168.2.129
R2 g0/1.99	standby version 2 standby 99 ip 192.168.3.11	192.168.3.11
R4 g0/2.99	standby version 2 standby 99 ip 192.168.3.1 standby 99 priority 150 standby 99 preempt	192.168.3.11

TABLE 4. HSRP Table

NOTE: the HSRP group number is the same as the VLAN number they will be acting as the default gateway of

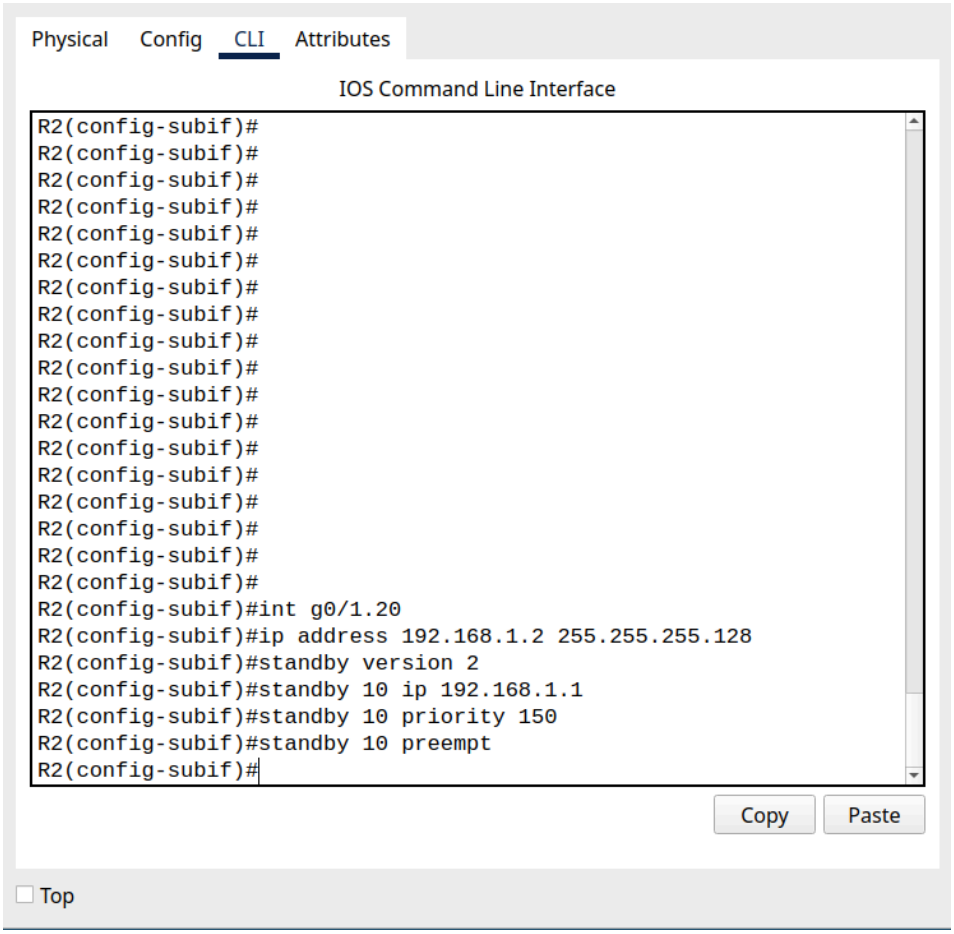

FIGURE 14. HSRP sample configuration

After the HSRP is configured, inter-VLAN should work as expected, but messages still won't be able to go to remote networks. This is because the routers do not know where to forward the messages, they don't have the routing to go to other networks.

Static Routing

Static routing will enable the messages from the local network to go to remote networks. This is needed to communicate with the devices outside the network.

The following Commands were entered for the static routing.

Device	Command	Description
R4		
	ip route 192.168.3.152 255.255.255.248 192.168.3.97	Route to DHCP server through R3 (optional)
	ip route 192.168.3.152 255.255.255.248 192.168.3.81	Route to DHCP server through R2 (optional)
	ip route 0.0.0.0 0.0.0.0 192.168.3.97	Default route for unknown networks through R3
	ip route 0.0.0.0 0.0.0.0 192.168.3.81	Default route for unknown networks through R2
R2		
	ip route 192.168.3.152 255.255.255.248 192.168.3.73	Route to DHCP server through R1 (optional)
	ip route 192.168.3.152 255.255.255.248 192.168.3.82	Route to DHCP server through R4 (optional)

	ip route 0.0.0.0 0.0.0.0 192.168.3.82	Default route for unknown networks through R4
	ip route 0.0.0.0 0.0.0.0 192.168.3.73	Default route for unknown networks through R4
R1		
	ip route 192.168.3.152 255.255.255.248 192.168.3.65	Route to DHCP server through MLS
	ip route 192.168.1.0 255.255.255.128 192.168.3.74	Route to VLAN 10 network through R2
	ip route 192.168.1.128 255.255.255.128 192.168.3.74	Route to VLAN 15 network through R2
	ip route 192.168.2.0 255.255.255.128 192.168.3.74	Route to VLAN 20 network through R2
	ip route 192.168.2.128 255.255.255.128 192.168.3.74	Route to VLAN 25 network through R2
	ip route 192.168.3.0 255.255.255.128 192.168.3.74	Route to VLAN 99 network through R2
	ip route 192.168.1.0 255.255.255.128 192.168.3.162	Route to VLAN 10 network through R3
	ip route 192.168.1.128	Route to VLAN 15 network

	255.255.255.128 192.168.3.162	through R3
	ip route 192.168.2.128 255.255.255.128 192.168.3.162	Route to VLAN 25 network through R3
	ip route 192.168.2.0 255.255.255.128 192.168.3.162	Route to VLAN 20 network through R3
	ip route 192.168.3.0 255.255.255.128 192.168.3.162	Route to VLAN 99 network through R3
	ip route 0.0.0.0 0.0.0.0 192.168.3.162	Default route via R3
	ip route 0.0.0.0 0.0.0.0 192.168.3.65	Default route via MLS
R3		
	ip route 192.168.3.152 255.255.255.248 192.168.3.89	Route to DHCP server through MLS
	ip route 192.168.3.152 255.255.255.248 192.168.3.161	Route to DHCP server through R1
	ip route 192.168.1.0 255.255.255.128 192.168.3.98	Route to VLAN 10 network through R4

	ip route 192.168.1.128 255.255.255.128 192.168.3.98	Route to VLAN 15 network through R4
	ip route 192.168.2.0 255.255.255.128 192.168.3.98	Route to VLAN 20 network through R4
	ip route 192.168.3.0 255.255.255.128 192.168.3.98	Route to VLAN 99 network through R4
	ip route 192.168.2.128 255.255.255.128 192.168.3.98	Route to VLAN 25 network through R4
	ip route 192.168.1.0 255.255.255.128 192.168.3.161	Route to VLAN 10 network through R1
	ip route 192.168.1.128 255.255.255.128 192.168.3.161	Route to VLAN 15 network through R1
	ip route 192.168.2.0 255.255.255.128 192.168.3.161	Route to VLAN 20 network through R1
	ip route 192.168.2.128 255.255.255.128 192.168.3.161	Route to VLAN 25 network through R1
	ip route 192.168.3.0 255.255.255.128 192.168.3.161	Route to VLAN 99 network through R1
	ip route 0.0.0.0 0.0.0.0	Default route through MLS

	192.168.3.89	
	ip route 0.0.0.0 0.0.0.0 192.168.3.161	Default route through R1
MLS		
	ip route 192.168.1.0 255.255.255.128 192.168.3.90	Route to VLAN 10 through R3
	ip route 192.168.1.0 255.255.255.128 192.168.3.66	Route to VLAN 10 through R1
	ip route 192.168.2.128 255.255.255.128 192.168.3.90	Route to VLAN 15 through R3
	ip route 192.168.2.128 255.255.255.128 192.168.3.90	Route to VLAN 25 through R3
	ip route 192.168.2.0 255.255.255.128 192.168.3.90	Route to VLAN 20 through R3
	ip route 192.168.1.128 255.255.255.128 192.168.3.66	Route to VLAN 15 through R1
	ip route 192.168.2.0 255.255.255.128 192.168.3.66	Route to VLAN 20 through R1

	ip route 192.168.2.128 255.255.255.128 192.168.3.66	Route to VLAN 25 through R1
	ip route 192.168.3.0 255.255.255.192 192.168.3.66	Route to VLAN 99 through R1
	ip route 192.168.3.0 255.255.255.192 192.168.3.90	Route to VLAN 99 through R3
	ip route 0.0.0.0 0.0.0.0 192.168.3.106	Default route through R5
	ip route 0.0.0.0 0.0.0.0 192.168.3.146	Default route through R7
R6		
	ip route 0.0.0.0 0.0.0.0 192.168.3.113	Default route through R5
	ip route 0.0.0.0 0.0.0.0 192.168.3.130	Default route through R7
R5		
	ip route 0.0.0.0 0.0.0.0 192.168.3.105	Default route through MLS
	ip route 0.0.0.0 0.0.0.0 192.168.3.122	Default route through R7

	ip route 192.168.3.136 255.255.255.248 192.168.3.122	Route to DNS server through R7
	ip route 192.168.3.136 255.255.255.248 192.168.3.114	Route to DNS server through R6
R7		
	ip route 0.0.0.0 0.0.0.0 192.168.3.121	Default route through R5
	ip route 0.0.0.0 0.0.0.0 192.168.3.145	Default route through MLS
	ip route 192.168.3.136 255.255.255.248 192.168.3.129	Route to DNS server through R6
	ip route 192.168.3.136 255.255.255.248 192.168.3.121	Route to DNS server through R5

TABLE 5. Static routing table

The static routing shown in the table is the more cumbersome way of static IP routing. A shortcut would be supernetting, a technique of summarizing multiple continuous subnets into one ip route command. For example, the network has 192.168.1.0/25 and 192.168.1.128/25 subnets, those can be supernetted into 192.168.1.0/24. Likewise, the addresses 192.168.2.0/25 and 192.168.2.128/25 can be summarized to 192.168.2.0/24. Then the addresses 192.168.1.0/24 and 192.168.2.0/24 can be summarized to 192.168.1.0/23. Thus, the command 'ip route 192.168.1.0 255.255.254.0 next-hop' could summarize some of the ip routes in the table.

DHCP Server

After static routing, the messages in the VLANs can now reach the DHCP server and DNS server over the ‘internet’ cluster. For the end devices to receive DHCP addressing, pools should be created. The following table and figures show the configurations of the pools in the network.

Pool name	**Default gateway**	**Mask**	**Start IP address**	**WLC address**	**Maximum number of hosts**
BINI-members-pool	192.168.1.1	255.255.255.128	10		90
BINI-managers-pool	192.168.1.129	255.255.255.128	139		90
Twice-members-pool	192.168.2.1	255.255.255.128	10		90
Twice-managers-pool	192.168.2.129	255.255.255.128	139		90
Management-pool	192.168.3.1	255.255.255.192	10	192.168.3.5	

TABLE 6. DHCP Pool Table

NOTE: the dns server address is 192.168.3.154 (applies to every pool except the Management pool)

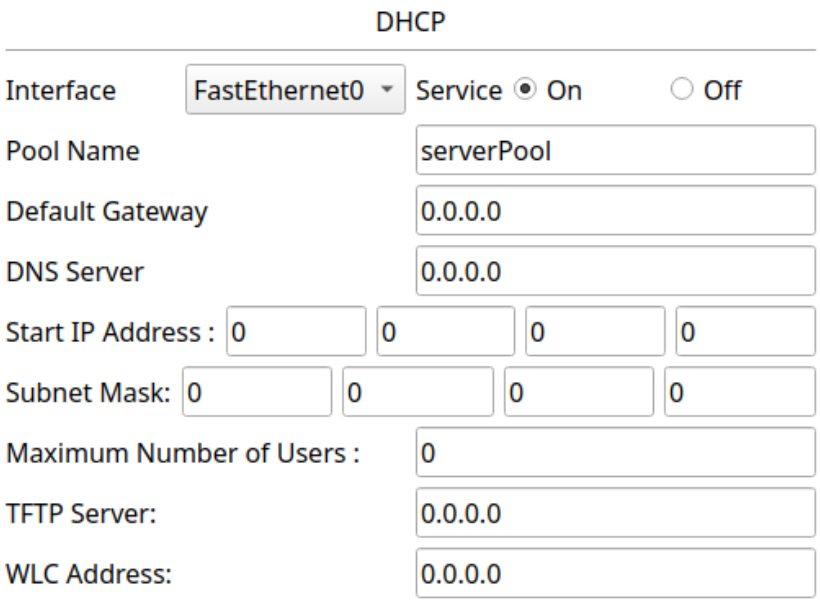

FIGURE 15. ServerPool

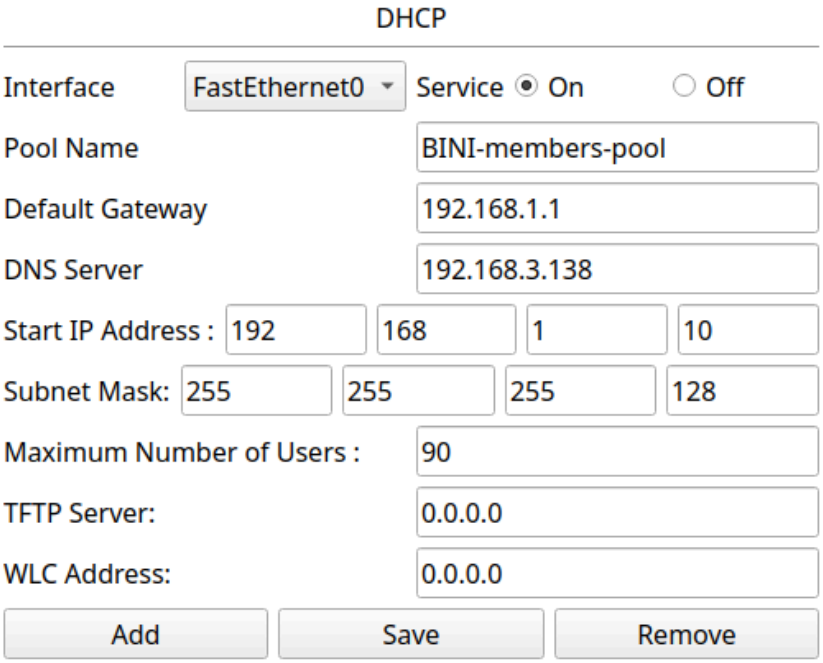

FIGURE 16. BINI-members-pool

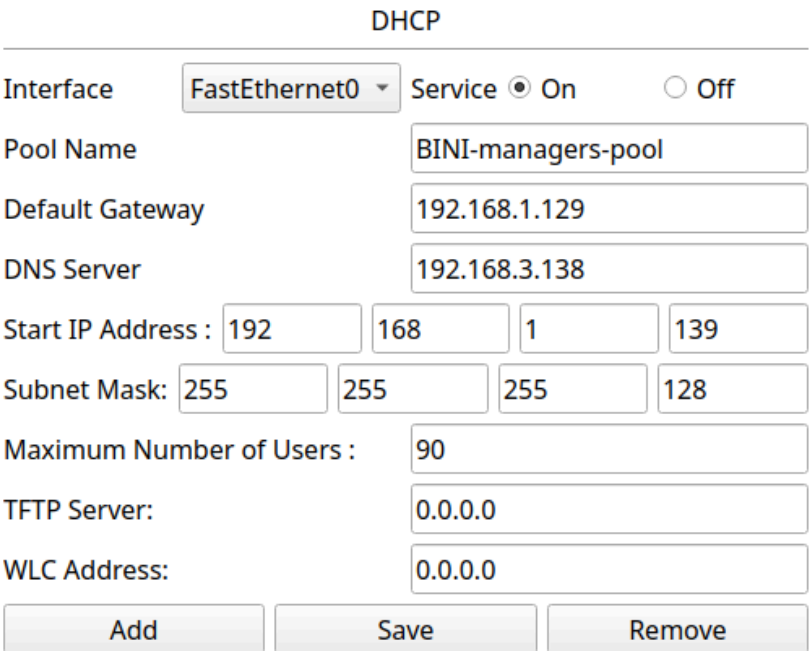

FIGURE 17. BINI-managers-pool

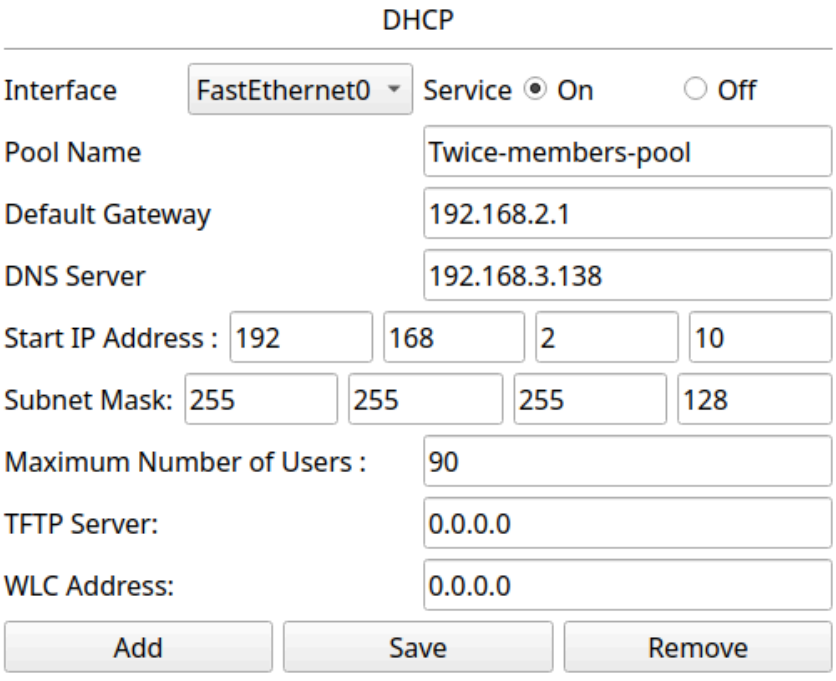

FIGURE 18. TWICE-members-pool

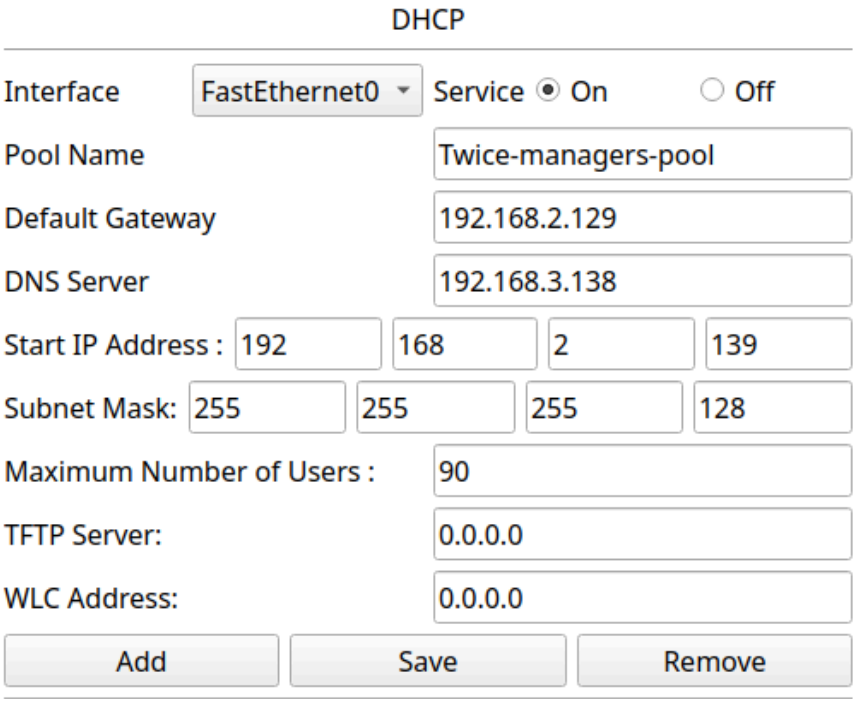

FIGURE 19. TWICE-managers-pool

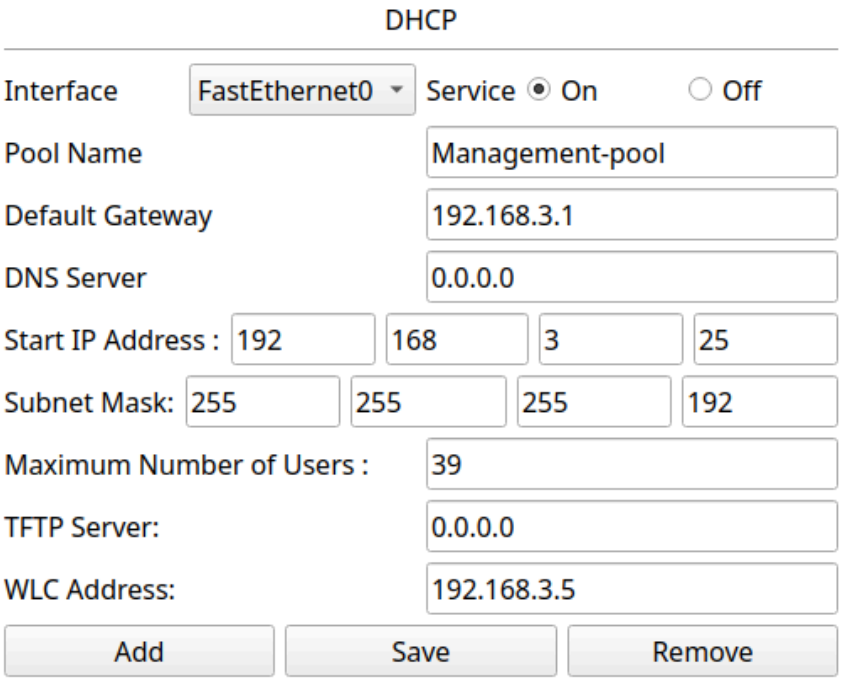

FIGURE 20. Management-pool

Layer 2 Redundancy (STP)

The root bridges will be SW 2 for all VLANs. The choice of what switch to be made as the root bridge was made based on the path cost to the default gateways. The network architects made the decision to use SW2 as the root bridge because it has the shortest path cost to the default gateways (SW1 also has the shortest path cost, but we chose SW2 regardless).

```
SW2(config)#spanning-tree vlan 20 root pri
SW2(config)#spanning-tree vlan 20 root primary
SW2(config)#spanning-tree vlan 20 root primary
SW2(config)#spanning-tree vlan 25 root primary
SW2(config)#spanning-tree vlan 99 root primary
```

FIGURE 21. Sample root bridge configuration (SW2)

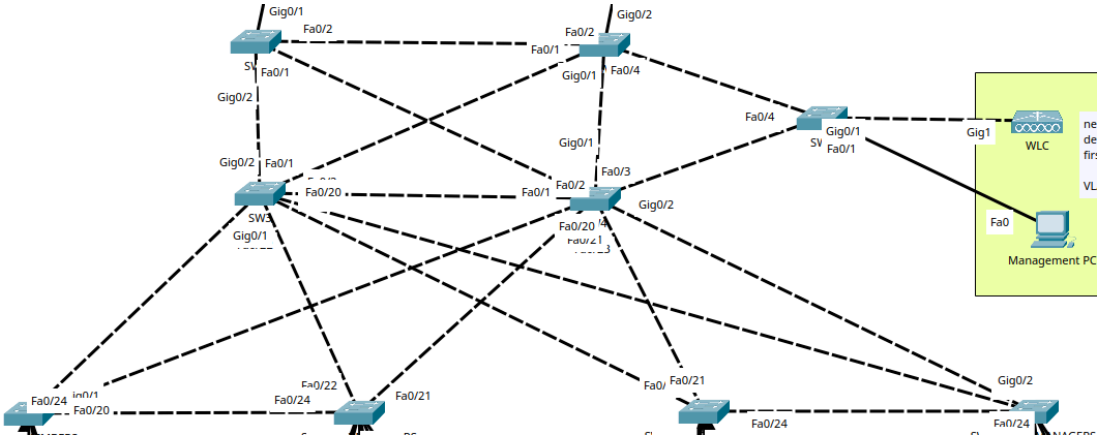

FIGURE 22. STP Configuration

NOTE: More testing of the STP configuration at the testing and troubleshooting section

Wireless Networking

All the wireless APs in the network were configured through the WLC. This was accessed using the Management PC (which resides in the same network area of the WLC). There were four things that were configured in the WLC:

1. WLC itself
2. Interfaces
3. WLAN
4. AP groups

The WLC can be accessed through the browser of Management PC (https://192.168.3.5). The username is ‘admin’ and the password is ‘Admin123’.

The image below shows the interfaces that were made in the WLC. These interfaces are only virtual and hold data of the interfaces of the WLANs that will be broadcasted by the APs later on.

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	IPv6 Address
BINI-Managers-INT	15	192.168.1.134	Dynamic	Disabled	
BINI-Members-INT	10	192.168.1.6	Dynamic	Disabled	
TWICE-Managers-INT	25	192.168.2.134	Dynamic	Disabled	
TWICE-Members-INT	20	192.168.2.6	Dynamic	Disabled	
management	untagged	192.168.3.5	Static	Enabled	::/128
virtual	N/A	192.0.2.1	Static	Not Supported	

FIGURE 24. STP Configuration

SSID / Profile name	Interface	Password
BINI-Members-WLAN	BINI-Members-INT	binibini
BINI-Managers-WLAN	BINI-Managers-INT	binimanager
TWICE-Members-WLAN	TWICE-Members-INT	twicetwice

TWICE-Managers-WLAN	TWICE-Managers-INT	twicemanager

TABLE 6. WLANs Table

The WLANs are the ones that will be broadcasted by the LAP PTs in the topology. The following were the WLANs made inside the WLC:

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	test	test	Enabled	[WPA2][Auth(PSK)]
2	WLAN	BINI-Members-WLAN	BINI-Members-WLAN	Enabled	[WPA2][Auth(PSK)]
3	WLAN	BINI-Managers-WLAN	BINI-Managers-WLAN	Enabled	[WPA2][Auth(PSK)]
4	WLAN	TWICE-Members-WLAN	TWICE-Members-WLAN	Enabled	[WPA2][Auth(PSK)]
5	WLAN	TWICE-Managers-WLAN	TWICE-Managers-WLAN	Enabled	[WPA2][Auth(PSK)]

FIGURE 25. WLAN in WLC.

The WLANs were secured with WPA2 with different passwords for each WLAN.

AP groups are basically groups of APs in the network that will broadcast the same WLAN and configured with the same interface. The following table shows the AP groupname, the APs under them and the WLANs they broadcast.

AP group	**WLANs**	**APs**
BINI-Members-group	BINI-Members-WLAN	BINI-AP
BINI-Managers-group	BINI-Managers-WLAN	BINI-Managers-AP
TWICE-Members-group	TWICE-Members-WLAN	TWICE-AP
TWICE-Managers-group	TWICE-Managers-WLAN	TWICE-Managers-AP

TABLE 7. AP group table

AP Group Name	AP Group Description	
BINI-Members-group	AP group for bini members	Remove
Bini-Managers-group	AP group for bini managers	Remove
TWICE-Managers-group	AP group for twice managers	Remove
TWICE-Members-group	AP group for twice members	Remove
default-group		

FIGURE 26. AP groups in WLC

Port Security

The following commands were used to configure the port security of the switches:

```
hostname(config-if)#switchport port-security
hostname(config-if)#switchport port-security mac-address sticky
hostname(config-if)#switchport port-security maximum 1
hostname(config-if)#switchport port-security violation restrict
```

FIGURE 27. Commands to configure port-security

```
SW5(config-if)#sw
SW5(config-if)#switchport po
SW5(config-if)#switchport port-security
SW5(config-if)#sw
SW5(config-if)#switchport po
SW5(config-if)#switchport port-security max
SW5(config-if)#switchport port-security maximum 1
SW5(config-if)#sw
SW5(config-if)#switchport po
SW5(config-if)#switchport port-security mac
SW5(config-if)#switchport port-security mac-address
SW5(config-if)#switchport port-security mac-address sticky
SW5(config-if)#sw
SW5(config-if)#switchport
SW5(config-if)#switchport po
SW5(config-if)#switchport port-security vi
SW5(config-if)#switchport port-security violation
SW5(config-if)#switchport port-security violation
SW5(config-if)#switchport port-security violation ?
  protect   Security violation protect mode
  restrict  Security violation restrict mode
  shutdown  Security violation shutdown mode
SW5(config-if)#switchport port-security violation restr
SW5(config-if)#switchport port-security violation restrict
SW5(config-if)#
```

FIGURE 28. Port-security sample configuration

These commands were entered to all the access ports to ensure that only one MAC address will be using each access port. The violation was to set ‘restrict’ so that the switchport will not shutdown in case a switch port is compromised, but will still drop the packet and log the event.

Other Security Measures

BPDU GUARD and PORTFAST

```
S1(config)# interface range f0/5-6
S1(config-if)# spanning-tree portfast
S1(config)# interface f0/8
```

```
S1(config-if)# spanning-tree bpduguard enable
```

FIGURE 29. BPDU Guard and PORTFAST configuration

```
SW7-BINI-MANAGERS(config-if-range)#spa
SW7-BINI-MANAGERS(config-if-range)#spanning-tree
SW7-BINI-MANAGERS(config-if-range)#spanning-tree
SW7-BINI-MANAGERS(config-if-range)#spanning-tree ?
  bpduguard  Don't accept BPDUs on this interface
  cost       Change an interface's spanning tree port path cost
  guard      Change an interface's spanning tree guard mode
  link-type  Specify a link type for spanning tree protocol use
  portfast   Enable an interface to move directly to forwarding on link up
  vlan       VLAN Switch Spanning Tree
SW7-BINI-MANAGERS(config-if-range)#spanning-tree portf
SW7-BINI-MANAGERS(config-if-range)#spanning-tree portfast
SW7-BINI-MANAGERS(config-if-range)#spanning-tree portfast ?
  disable  Disable portfast for this interface
  trunk    Enable portfast on the interface even in trunk mode
  <cr>
SW7-BINI-MANAGERS(config-if-range)#spanning-tree portfast
```

FIGURE 30. Portfast sample configuration

```
SW1(config-if-range)#
SW1(config-if-range)#span
SW1(config-if-range)#spanning-tree bpd
SW1(config-if-range)#spanning-tree bpduguard
SW1(config-if-range)#spanning-tree bpduguard ?
  disable  Disable BPDU guard for this interface
  enable   Enable BPDU guard for this interface
SW1(config-if-range)#spanning-tree bpduguard en
SW1(config-if-range)#spanning-tree bpduguard enable
```

FIGURE 31. BPDU guard sample configuration

The BPDU guard will prevent a force root bridge reelection and other switches from joining the STP protocol. If ever a port enabled with BPDU guard receives a BPDU it will be set to a err-disabled state where it will be disabled. Manual interference is required to get the port enabled again. On the other hand, portfast is not really a security measure, but something that will help the network run more smoothly.

Disabling Unused Ports

```
down
FastEthernet0/24       unassigned      YES manual down
down
GigabitEthernet0/1     unassigned      YES manual up
up
GigabitEthernet0/2     unassigned      YES manual down
down
Vlan1                  unassigned      YES manual administratively
down down
SW5(config)#int r fa0/2,fa0/5-24,g0/2
SW5(config-if-range)#shu
SW5(config-if-range)#shutdown
```

FIGURE 32. Disabling unused ports sample configuration

Unused switch ports are also disabled. This was done to prevent the access of rogue agents/devices into the network.

Remote Access (SSH)

SSH was also enabled in all the **switches and routers 1 to 4.**

Domain name	cisco.com
Default gateway, address	Refer to the addressing table
username	admin
password	adminpass
Privilege exec password	class
Console password	cisco

TABLE 8. SSH configuration details

```
hostname(config)#ip domain-name cisco.com
hostname(config)#username admin password adminpass
hostname(config)#crypto key generate rsa general-keys modulus 1024
hostname(config)#ip ssh version 2
hostname(config)#line vty 0 15
hostname(config-line)#transport input ssh
hostname(config-line)#login local
hostname(config-line)#line con 0
hostname(config-line)#password cisco
```

FIGURE 33. SSH configuration

```
The name for the keys will be: SW9-TWICE-MANAGERS.cisco.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 0:27:42.410: %SSH-5-ENABLED: SSH 1.99 has been enabled
SW9-TWICE-MANAGERS(config)#
SW9-TWICE-MANAGERS(config)#ip ssh version 2
SW9-TWICE-MANAGERS(config)#
SW9-TWICE-MANAGERS(config)#enable secret class
SW9-TWICE-MANAGERS(config)#
SW9-TWICE-MANAGERS(config)#line vty 0 15
SW9-TWICE-MANAGERS(config-line)#
SW9-TWICE-MANAGERS(config-line)#transport input ssh
SW9-TWICE-MANAGERS(config-line)#
SW9-TWICE-MANAGERS(config-line)#login local
SW9-TWICE-MANAGERS(config-line)#
SW9-TWICE-MANAGERS(config-line)#line con 0
SW9-TWICE-MANAGERS(config-line)#
SW9-TWICE-MANAGERS(config-line)#password cisco
SW9-TWICE-MANAGERS(config-line)#
SW9-TWICE-MANAGERS(config-line)#login
SW9-TWICE-MANAGERS(config-line)#
SW9-TWICE-MANAGERS(config-line)#exit
SW9-TWICE-MANAGERS(config)#
SW9-TWICE-MANAGERS(config)#ip default-gateway 192.168.3.1
SW9-TWICE-MANAGERS(config)#
SW9-TWICE-MANAGERS(config)#int vlan 99
SW9-TWICE-MANAGERS(config-if)#
SW9-TWICE-MANAGERS(config-if)#ip address 192.168.3.6 255.255.255.192
%LINK-5-CHANGED: Interface Vlan99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

SW9-TWICE-MANAGERS(config-if)#ip address 192.168.3.14 255.255.255.192
SW9-TWICE-MANAGERS(config-if)#do wr
Building configuration...
[OK]
SW9-TWICE-MANAGERS(config-if)#
SW9-TWICE-MANAGERS(config-if)#
```

FIGURE 34. SSH sample configuration

DNS Server

For demonstration purposes, this topology includes a DNS server. The address http://cisco or https://192.168.3.148 holds the website below

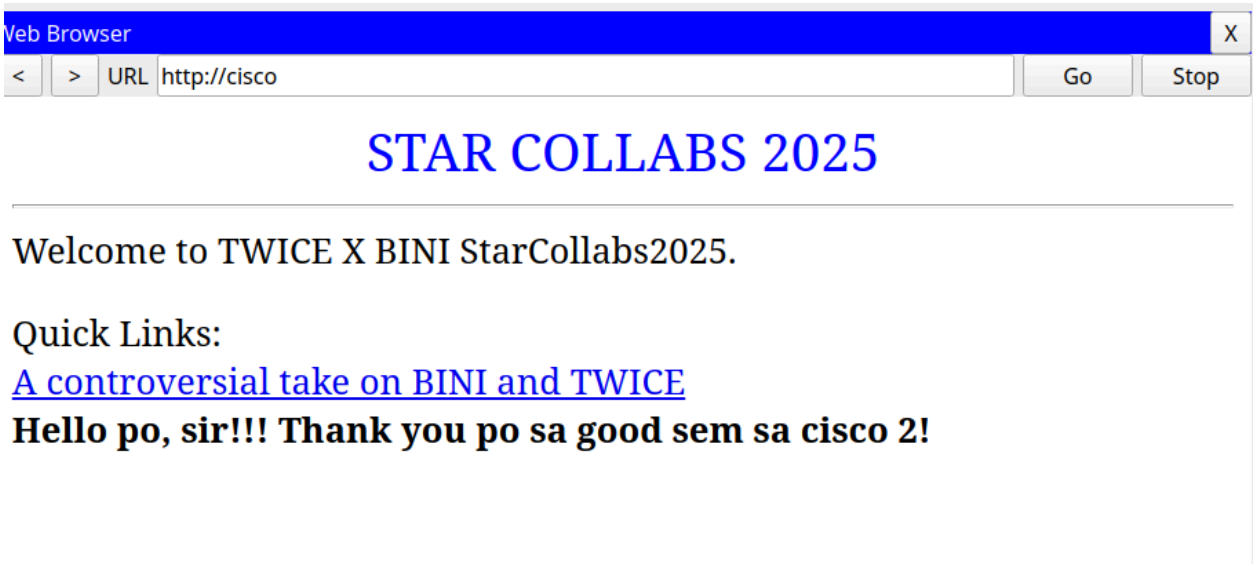

FIGURE 35. Website from the DNS server (through browser)

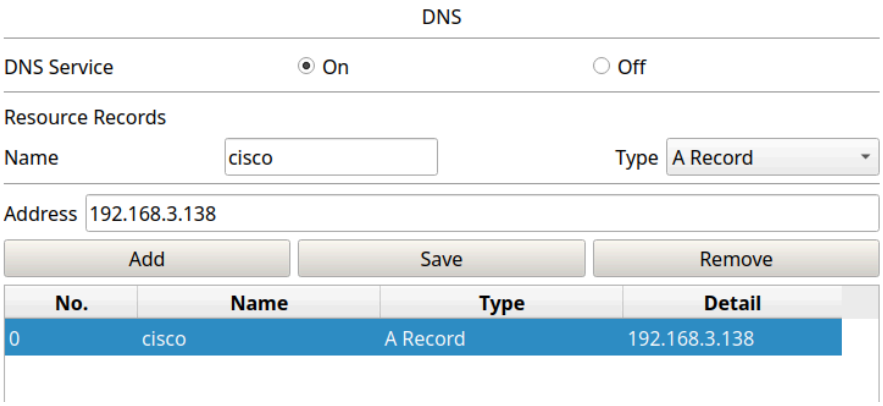

FIGURE 36. DNS Server Configuration

Testing, Troubleshooting, and Verification

Static Routing

```
C:\>tracert 192.168.3.138

Tracing route to 192.168.3.138 over a maximum of 30 hops:

  1    31 ms     6 ms      5 ms      192.168.2.3
  2    30 ms     10 ms     45 ms     192.168.3.97
  3    6 ms      *         42 ms     192.168.3.73
  4    42 ms     *         3 ms      192.168.3.97
  5    15 ms     16 ms     32 ms     192.168.3.73
  6    16 ms     13 ms     18 ms     192.168.3.106

Trace complete.
```

FIGURE 37. Tracert from Jeongyeon's Laptop to DNS Server

The tracert command shows the routing hops a message has to go through. In figure 37, the first hop was the address 192.168.2.3, port g0/2.20 of R4. Port g0/2.20 of R4 is also the current active router of the enabled HSRP (see figure 38), which serves as the default gateway of VLAN 20. The next hop, based on the static routing, should either be R2 or R1. The second hop was 192.168.3.97 which is port g0/1 of R3. It can be seen that the hops 3 to 5 goes back and forth, this is because the Layer 3 static routing is redundant and is prone to such scenarios. Although inefficient, the ping command shows that it reaches its destination (see figure 39).

```
GigabitEthernet0/2.20 - Group 20 (version 2)
  State is Active
    7 state changes, last state change 00:00:18
  Virtual IP address is 192.168.2.1
```

FIGURE 38. ‘show standby’ command in R4

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.138

Pinging 192.168.3.138 with 32 bytes of data:

Reply from 192.168.3.138: bytes=32 time=10ms TTL=123
Reply from 192.168.3.138: bytes=32 time=10ms TTL=119
Reply from 192.168.3.138: bytes=32 time=10ms TTL=123
Reply from 192.168.3.138: bytes=32 time=10ms TTL=119

Ping statistics for 192.168.3.138:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 10ms, Average = 10ms
```

FIGURE 39. Ping from Jeongyeon's Laptop (VLAN 20 device) to DNS Server

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.138

Pinging 192.168.3.138 with 32 bytes of data:

Reply from 192.168.3.138: bytes=32 time=20ms TTL=123
Request timed out.
Reply from 192.168.3.138: bytes=32 time=7ms TTL=123
Reply from 192.168.3.138: bytes=32 time=10ms TTL=119

Ping statistics for 192.168.3.138:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 20ms, Average = 12ms
```

FIGURE 40. Ping from Colet's PC (VLAN 10) to DNS Server

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.138

Pinging 192.168.3.138 with 32 bytes of data:

Request timed out.
Reply from 192.168.3.138: bytes=32 time<1ms TTL=121
Reply from 192.168.3.138: bytes=32 time=10ms TTL=121
Reply from 192.168.3.138: bytes=32 time=10ms TTL=121

Ping statistics for 192.168.3.138:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 6ms
```

FIGURE 31. Ping form BINI-Manager-2 PC (VLAN 15) to DNS Server

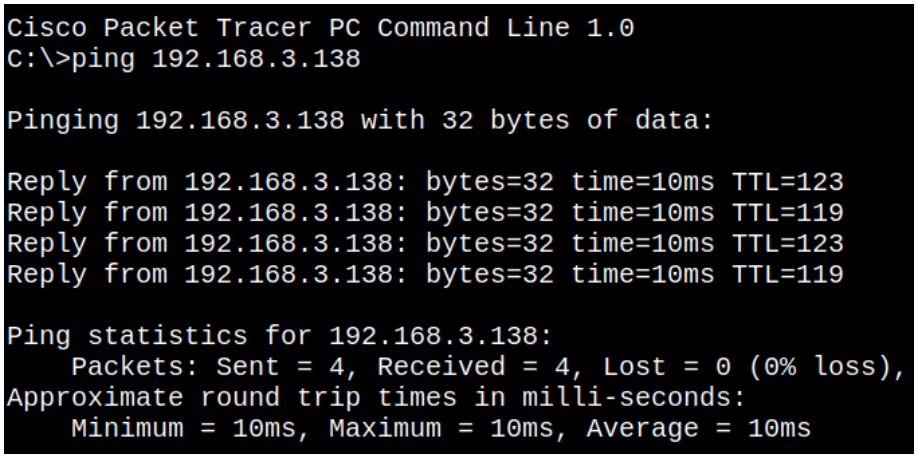

FIGURE 32. Ping from TWICE-Manager-2 PC (VLAN 25) to DNS Server

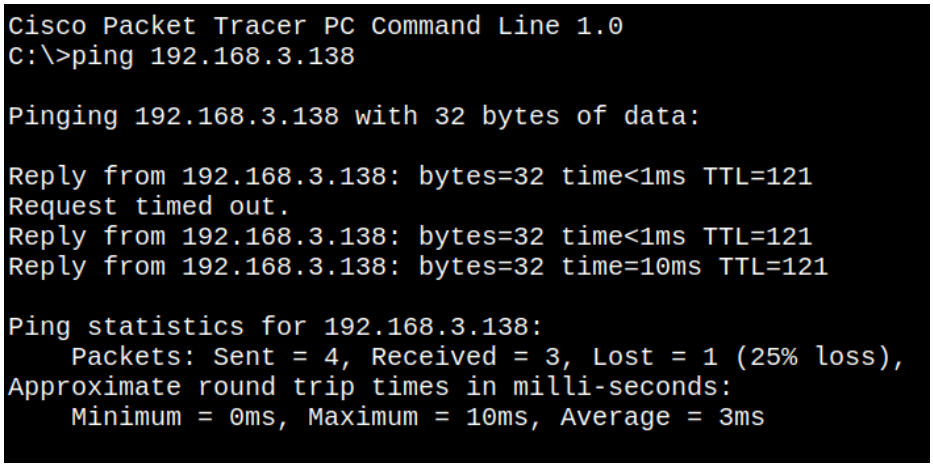

FIGURE 33. Pint from Management PC (VLAN 99) to DNS Server

Static Routing Diagnostic

All routes are operational and working as expected.

DHCPv4 on wired and wireless devices

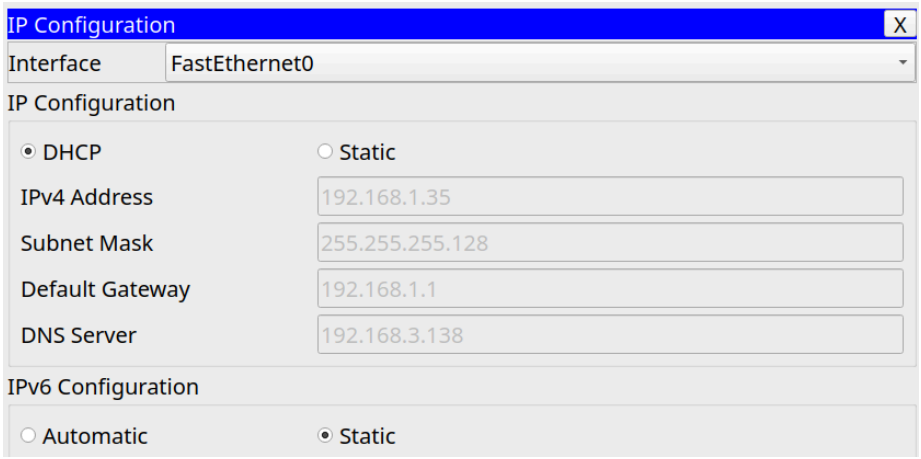

FIGURE 34. Dynamic addressing on a wired device in VLAN 10

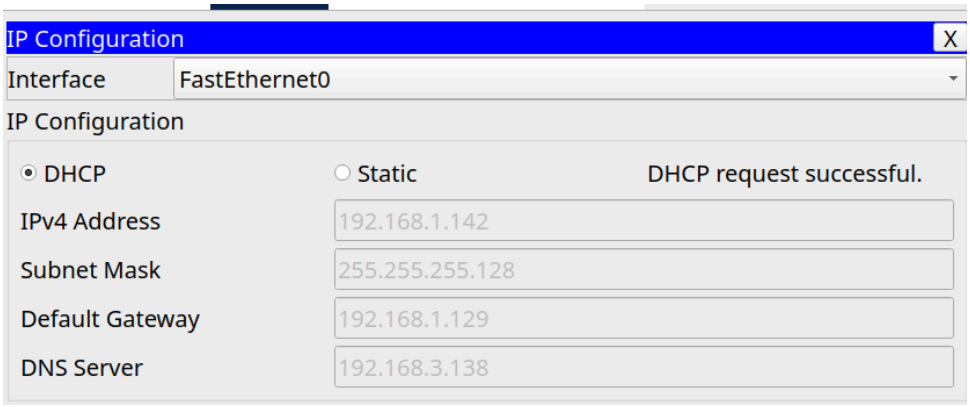

FIGURE 35. Dynamic addressing on a wired device in VLAN 15

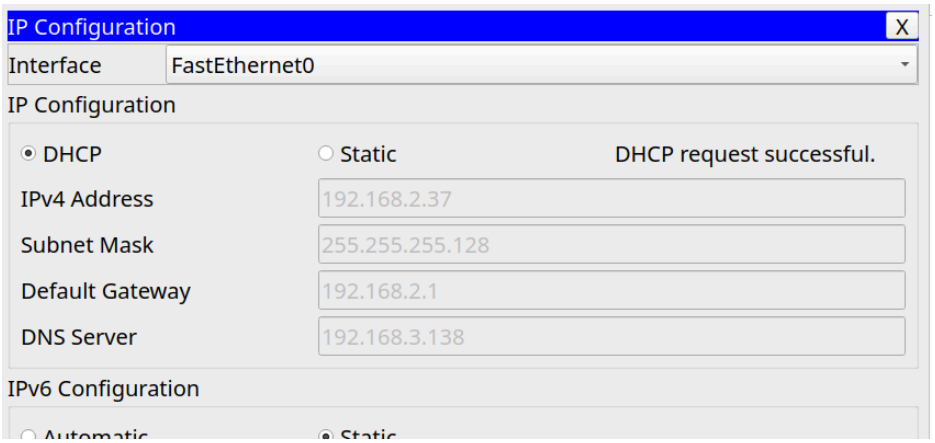

FIGURE 36. Dynamic addressing on a wired device in VLAN 20

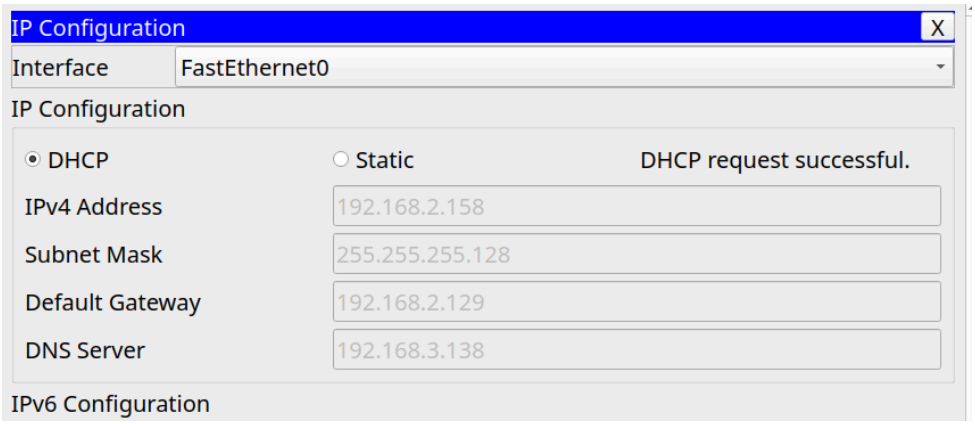

FIGURE 37. Dynamic addressing on a wired device in VLAN 25

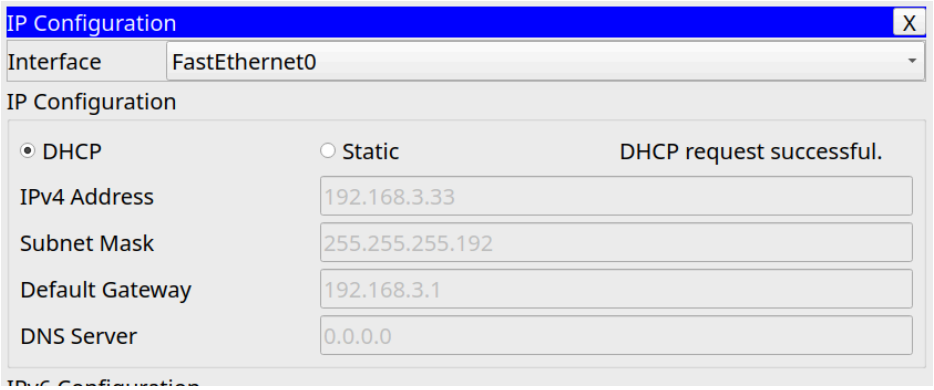

FIGURE 38. Dynamic addressing on a wired device in VLAN 99

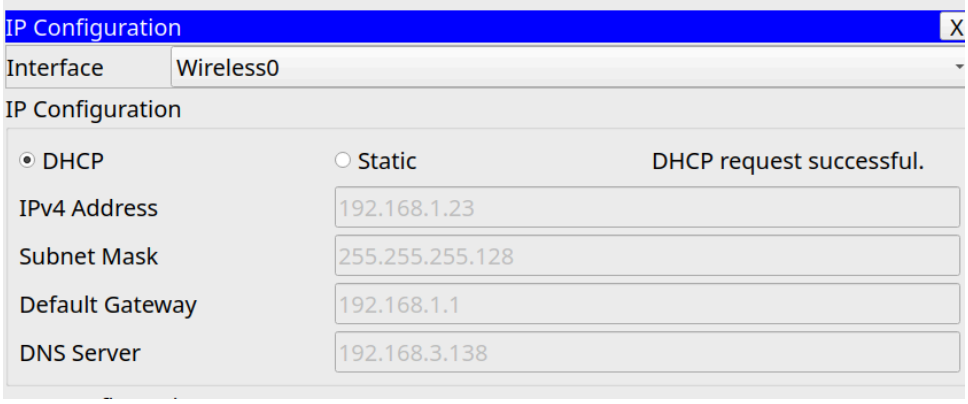

FIGURE 39. Dynamic addressing on a wireless device in VLAN 10

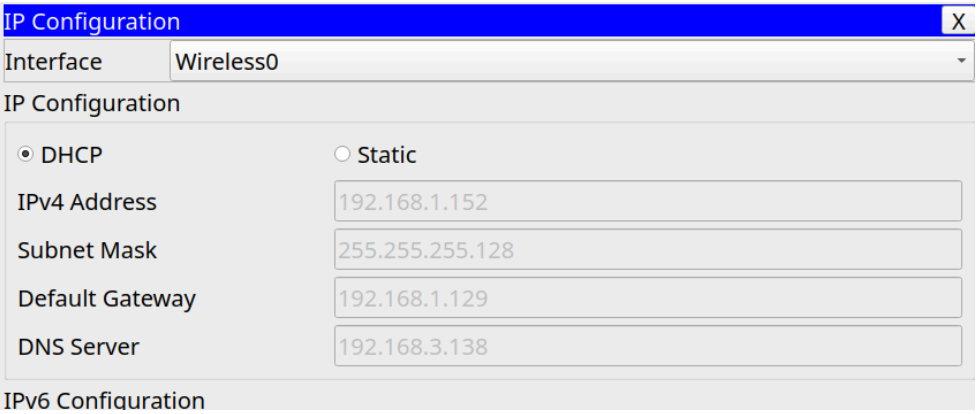

FIGURE 40. Dynamic addressing on a wireless device in VLAN 15

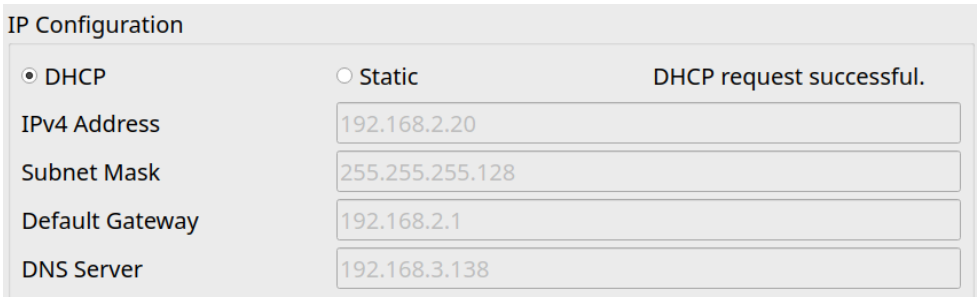

FIGURE 41. Dynamic addressing on a wireless device in VLAN 20

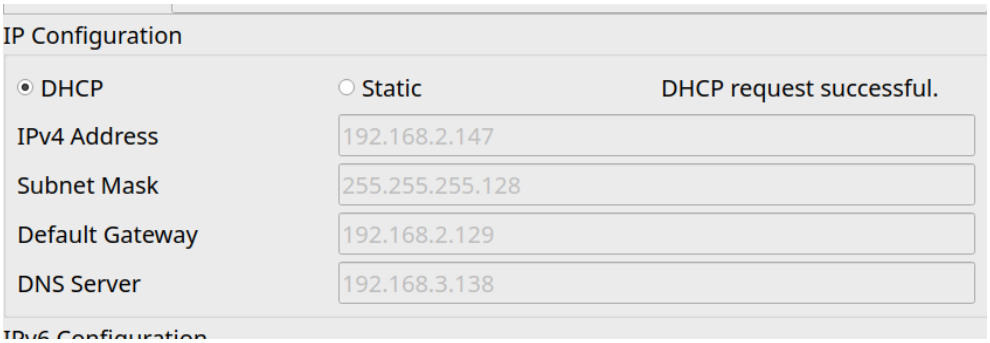

FIGURE 42. Dynamic addressing on a wireless device in VLAN 25

Layer 2 Loop Prevention

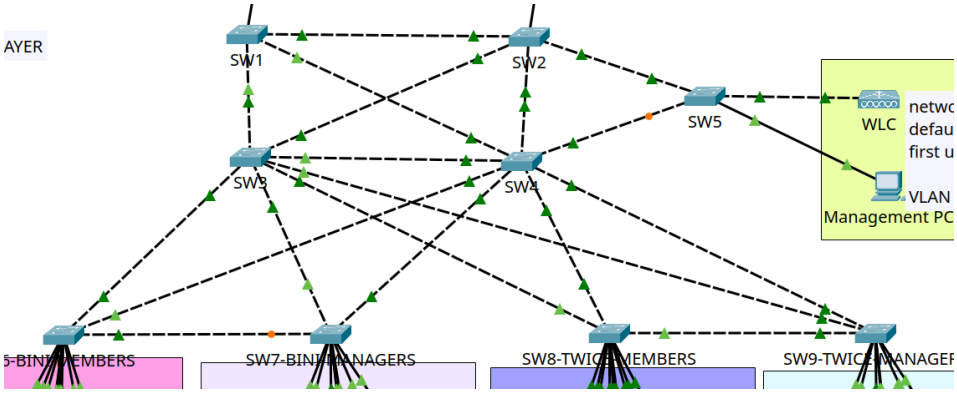

FIGURE 43. Switches with redundant links

Figure 43 shows the redundant links between the switches. Redundancy was added to eliminate single points of failure and improve the fault tolerance of the network. STP is a layer 2 protocol that prevents layer 2 broadcast storms. Without STP the redundant links may cause mac address table instability, making the network unusable.

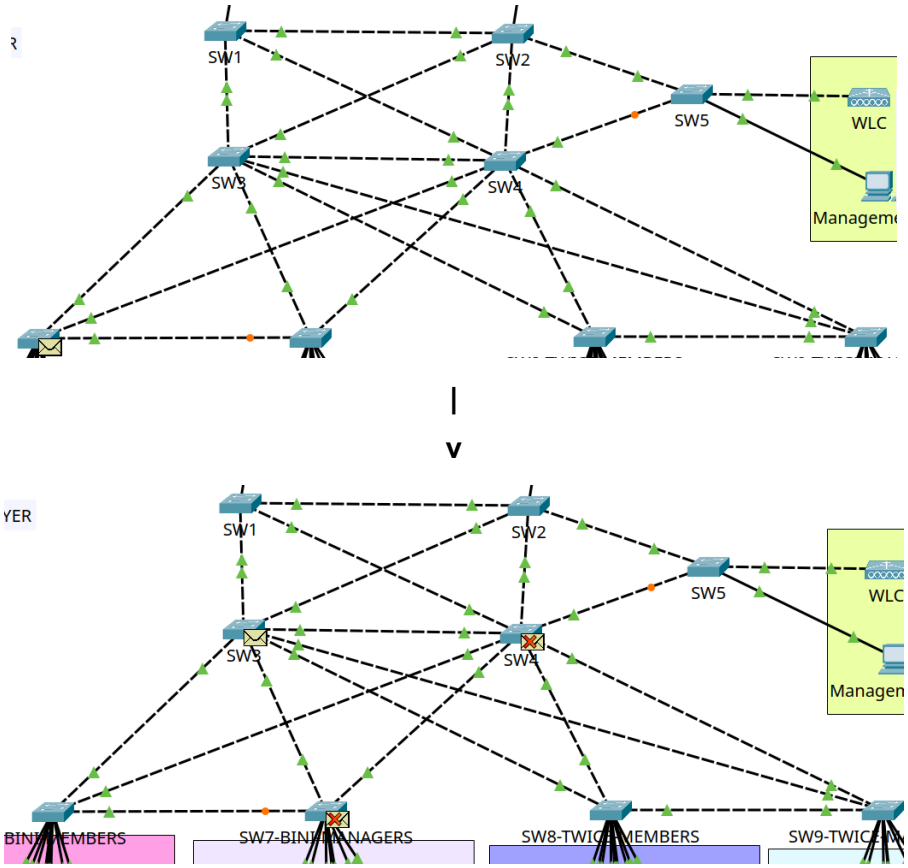

FIGURE 44. STP at work

Figure 44 shows how STP blocks switch ports to prevent layer 2 loops. Blocking ports are assigned based on the spanning tree algorithm developed by Radia Perlman

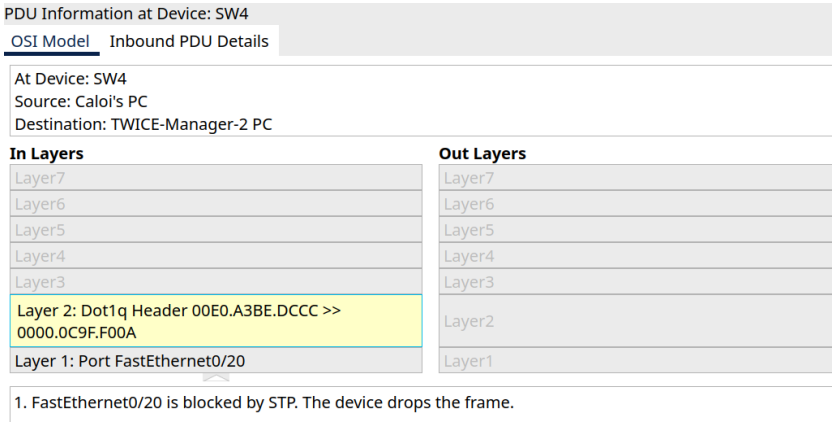

FIGURE 45. PDU information showing why the frame was dropped

As mentioned earlier, STP also allows multiple paths to be present. When a port or a switch becomes unavailable, the blocking ports will switch. Thus still allowing the network to operate.

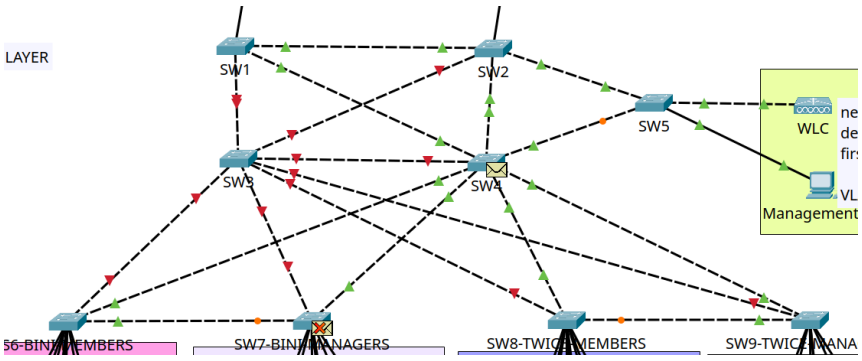

FIGURE 46. STP at work, enabling blocking ports

Layer 3 Redundancy

HSRP is a successor of FHRP, first hop redundancy protocol. It enables a virtual router makes two routers seem as one, therefore have two default gateways (one as backup and another as active). HSRP was tested in the network by shutting down one router or port and seeing if pinging outside the network still works.

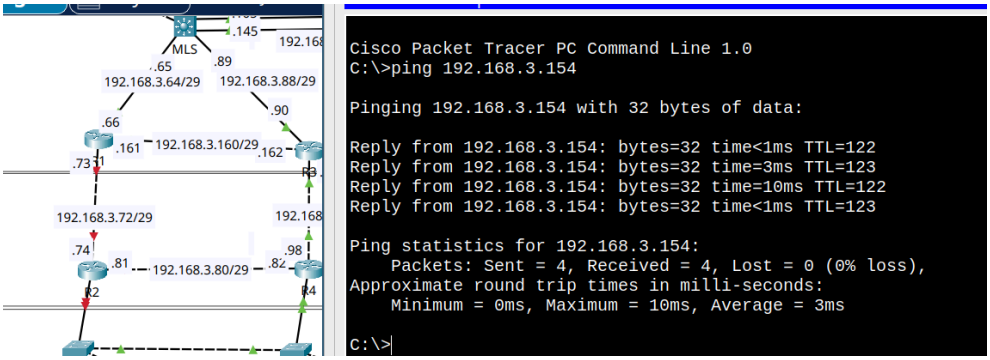

FIGURE 47. HSRP at work, R2 shutdown, pinging from a PC at VLAN 15 to DHCP server

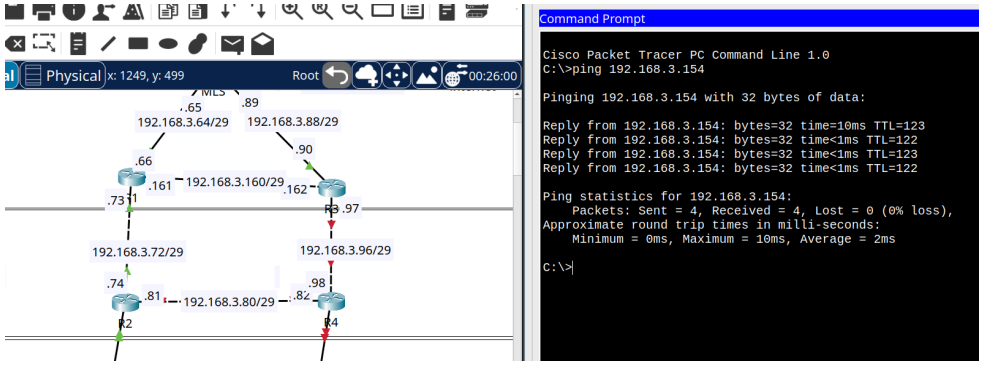

FIGURE 48. HSRP at work, R4 shutdown, pinging from a PC at VLAN 20 to DHCP server

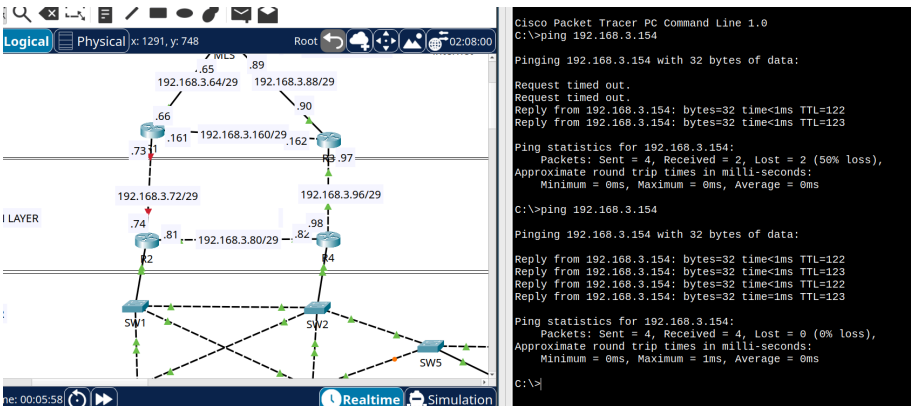

FIGURE 49. HSRP at work, R2 port g0/2 shutdown, pinging from a PC at VLAN 25 to DHCP server

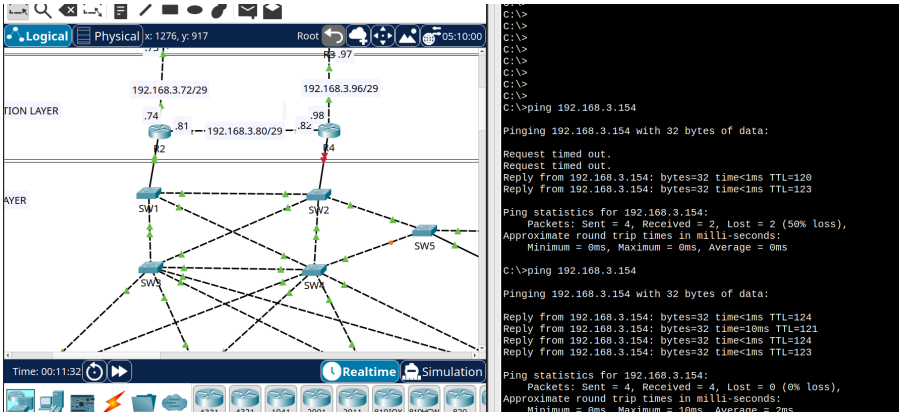

FIGURE 50. HSRP at work, R4 port g0/2 shutdown, pinging from a PC at VLAN 25 to DHCP server

Figures 47 to 49 shows the functionality of the HSRP, even though 1 default gateway is not available, the other can act as a replacement. This shows that the HSRP was configured correctly.

Security Measures

Port security

Since the mac address was limited to one, the PCs cannot be exchanged with other PCs. This eliminates the threat of threat actors connecting to the network through end users

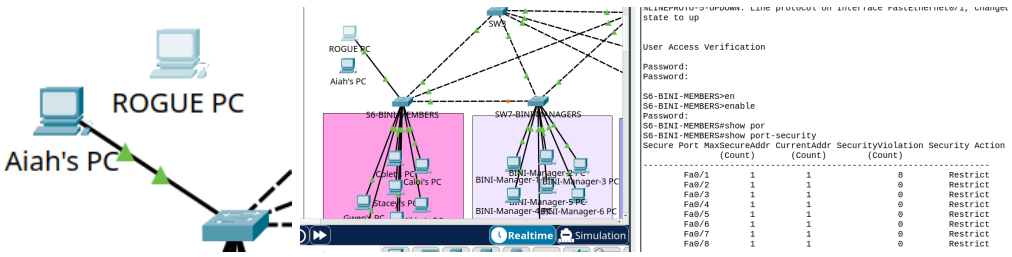

FIGURE 51. Port security

Figure 51 shows that when the rogue PC connected to the switch using Fa0/1 (Aiah's PC's slot), it was restricted. The rogue PC tried to get an address from the DHCP server, but it failed. Instead the switch logged the violations. This stopped the ROGUE PC from infiltrating the network.

Disabled unused ports

Whenever a ROGUE PC tries to connect to a switch's unused port, it will not be able to get a connection since it is disabled.

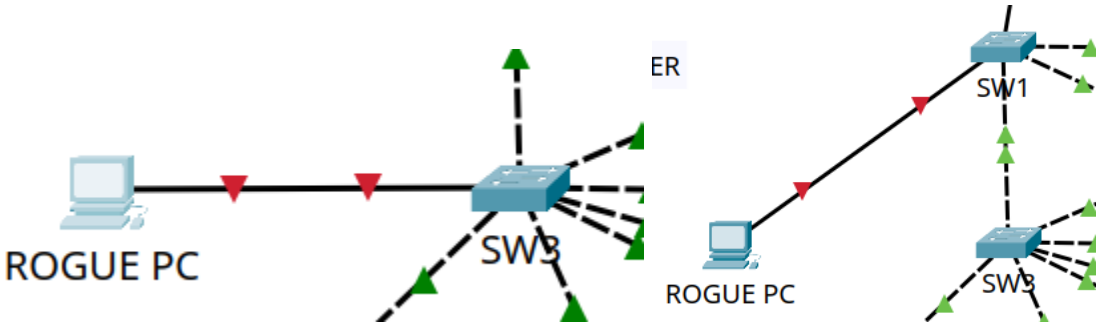

FIGURE 52. A rogue PC trying to use an unused port.

BPDU Guard

BPDU guards were set up on all unused ports of switches. It blocks BPDUs from rogue switches that could be a potential threat (sniffing)

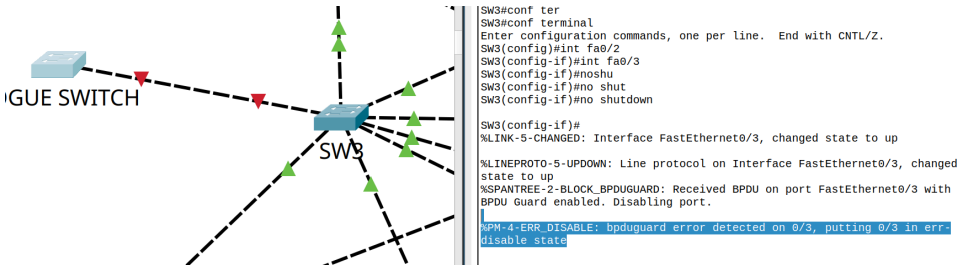

FIGURE 53. The BPDU guard in action.

SSH for all switches and R1 to R4

All the ssh-enabled devices were accessed remotely through the command line. Some screenshots were provided below for documentation purposes.

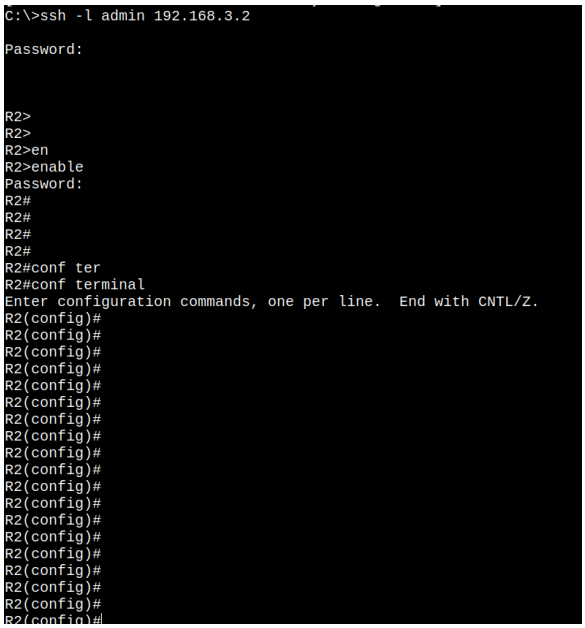

Figure 54. SSH from Management pc to R2

Inter-VLAN communication

The inter-VLAN communication was tested by sending PDUs from one VLAN to another.

Fire	Last Status	Source	Destination	Type	Color
	Successful	Aiah's PC	BINI-Manager-2 PC	ICMP	
	Successful	BINI-Manager-1 PC	Caloi's PC	ICMP	
	Successful	Nayeon's PC	BINI-Manager-3 PC	ICMP	
	Successful	TWICE-Manager-1 PC	Momo's PC	ICMP	
	Successful	TWICE-Manager-1 PC	BINI-Manager-3 PC	ICMP	
	Successful	Nayeon's PC	Caloi's PC	ICMP	

FIGURE 55. Simple PDUs tests in packet tracer.

Challenges faced:

One of the challenges faced by the network architects while implementing the network was the configuration of HSRP on the default gateway of VLAN 99. After putting in all the right commands, standby commands and ip addressing, the HSRP-enabled ports were not able to communicate with each other. Both the HSRP enabled ports were setting themselves as ACTIVE. The HSRP-enabled ports of other VLANs' default gateway were working, although the configurations were the same. After a few hours of diagnosing, the network architects decided to remove the native VLAN on the links that connect switches and routers since that was the only thing different from other VLANs (VLAN 99 is the native VLAN). Surprisingly, after this the HSRP on the default gateway of VLAN 99 worked. The PCs and access points that required the default gateway to work were able to get addressed.