Computer Network Group Project Report (P2-1)

Prepared by

ADIL AMR BIN QAMARUZZAMAN
****

MUHD WAFIYUDDIN BIN ABDUL RAHMAN
****

NURUL AIDA BINTE ZAKARIA
****

MUHAMMAD NAFIS BIN MOHAMED IDRIS
****

MUHAMMAD SAAD BIN HADI
****

Table of Contents

I. Introduction

As part of the SkillsFuture Singapore initiative to promote lifelong learning, and in alignment with the UN 2030 Agenda for Sustainable Development, a company is establishing an IT learning hub to equip the public with future-ready IT skills. To support this initiative, the company requires a reliable enterprise Local Area Network (LAN) with Internet access to facilitate learning, administrative operations, and online course promotion.

Network Requirements

The network must support multiple departments, computer labs, and essential IT services. The infrastructure requirements are detailed in the tables below:

1. Computer Labs

Lab Type	Number of Labs	Computer per Lab	Total Computers
Large Computer Lab	1	28	28
Small Computer Lab	3	12	36
Total	4	-	64

Table 1: Computer Labs

2. Staff Workstations

Office	Role	Number of Computers
Management Office	Learning Hub Manager	1
	HR Executive	1
	Admin Executive	1
	Network Engineer	1
Instructor Office	Instructors	6
Sales Office	Sales Manager	1
	Sales Executive	4
Finance Office	Finance Manager	1
	Finance Executive	1
Total Workstations	-	17

Table 2: Staff Workstations

3. IT Services and Network Infrastructure

Service	Function
Web Server	Hosts a website for course promotion and information.
Authoritative DNS Server	Enables public access to the IT learning hub's website via domain name.
Catching DNS Server	Improves internal network performance by resolving domain names locally.

Table 3: IT Services and Network Infrastructure

IP Addressing and Internet Access

- The 192.168.1.0/24 IP address block is allocated for internal network use.
- The IT learning hub will utilise two Internet Service Providers (ISPs) to ensure redundancy and reliability.

II. Configuration

Topology

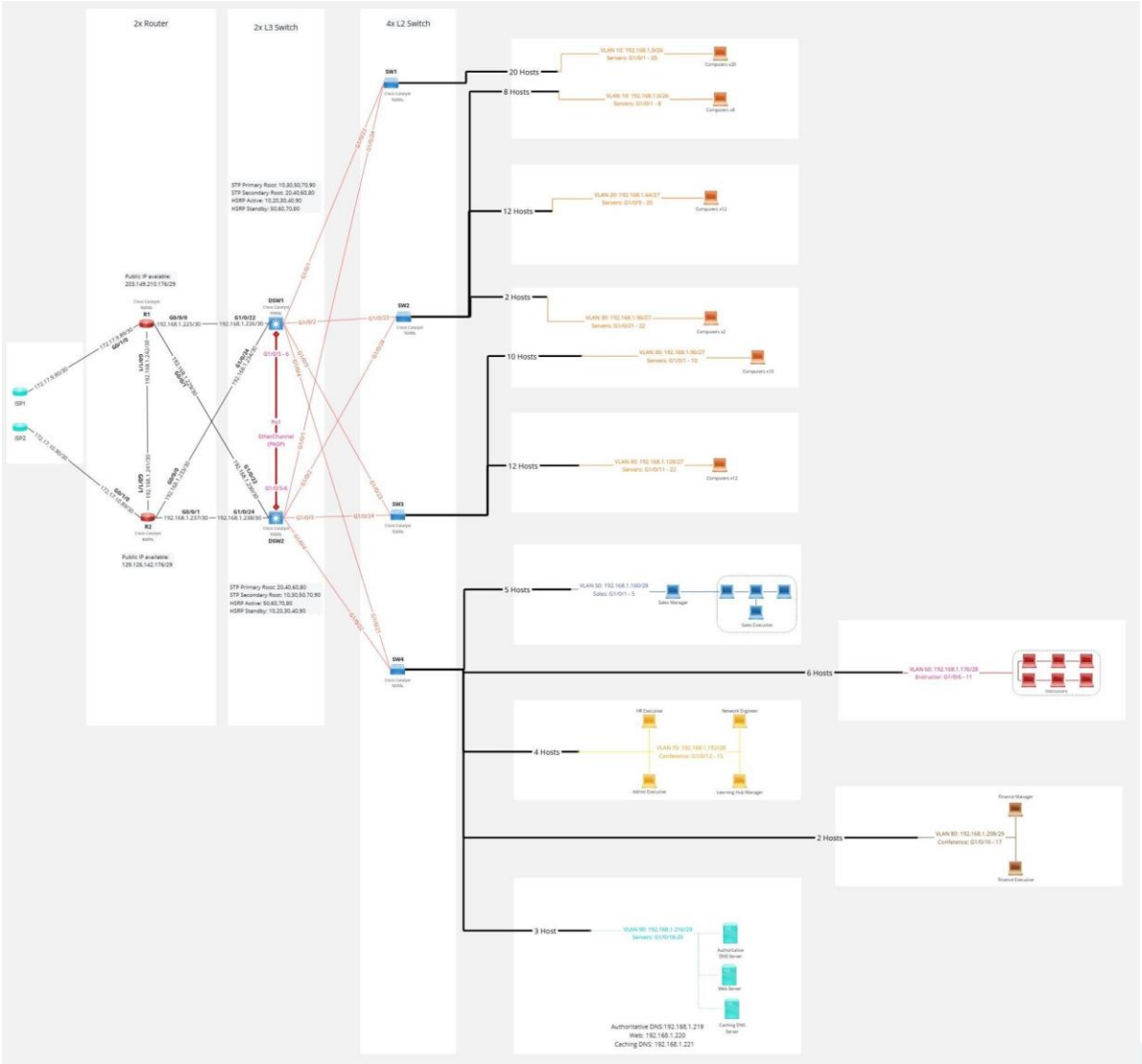

Figure 1: Topology

Click here for website topology

The 3-tier network architecture consists of the core, distribution and access layers, which create a network with high performance, redundancy, scalability, and flexibility.

In Figure 1, the design for each tier has its specific role. The access layer switches connect directly to the end devices and separate the hosts into smaller subnets and VLANs. Hence reducing the collision domain. In addition, the distribution switches layer acts as the network backbone and helps with VLAN routing. Furthermore, it helps with load balancing between inter-vlan

connections. Lastly is the core layer which helps to connect end-user devices to the internet and also enables the load balancing of the traffic.

Addressing Table

Device	Interface	IP Address	Subnet Mask	HSRP	Connecting Device	
					Device	Interface
SW1	G1/0/1 - G1/0/20	NA	NA	NA	Large Computer Lab (20 hosts)	NA
	G1/0/23	NA	NA	NA	DSW1	G1/0/1
	G1/0/24	NA	NA	NA	DSW2	G1/0/1
SW2	G1/0/1 - G1/0/8	NA	NA	NA	Large Computer Lab (8 hosts)	NA
	G1/0/9 - G1/0/20	NA	NA	NA	Small Computer Lab 1 (12 hosts)	NA
	G1/0/21 - G1/0/22	NA	NA	NA	Small Computer Lab 2 (2 hosts)	NA
	G1/0/23	NA	NA	NA	DSW1	G1/0/2
	G1/0/24	NA	NA	NA	DSW2	G1/0/2
SW3	G1/0/1 - G1/0/10	NA	NA	NA	Small Computer Lab 2 (10 hosts)	NA
	G1/0/11 - G1/0/22	NA	NA	NA	Small Computer Lab 3 (12 Hosts)	NA
	G1/0/23	NA	NA	NA	DSW1	G1/0/3
	G1/0/24	NA	NA	NA	DSW2	G1/0/3
SW4	G1/0/1 - G1/0/5	NA	NA	NA	Sales Office (1 Manager, 4 Executive)	NA
	G1/0/6 - G1/0/11	NA	NA	NA	Instructor Office(6 Instructors)	NA

	G1/0/12 - G1/0/15	NA	NA	NA	Management Office (HR executive,Network Engineer, Admin Executive, Learning Hub Manager)	NA
	G1/0/16 - G1/0/17	NA	NA	NA	Finance Office (Finance Manager,Finance Executive)	NA
	G1/0/18- G1/0/20	NA	NA	NA	Data Center (Web, Caching DNS & Authoritative DNS Server)	NA
	G1/0/21	NA	NA	NA	DSW1	G1/0/4
	G1/0/22	NA	NA	NA	DSW2	G1/0/4
DSW1	G1/0/1	NA	NA	NA	SW1	G1/0/23
	G1/0/2	NA	NA	NA	SW2	G1/0/23
	G1/0/3	NA	NA	NA	SW3	G1/0/23
	G1/0/4	NA	NA	NA	SW4	G1/0/23
	G1/0/5 - G1/0/6 (PAGP)	Trunk	Trunk	NA	DSW2	G1/0/5 - G1/0/6
	G1/0/22	192.168.1.226	255.255.255.252 (/30)	NA	R1	G0/0/0
	G1/0/24	192..168.1.234	255.255.255.252 (/30)	NA	R2	G0/0/0
	VLAN 10	192.168.1.1	255.255.255.192 (/26)	192.168.1.62	NA	NA
	VLAN 20	192.168.1.65	255.255.255.224 (/27)	192.168.1.94	NA	NA
	VLAN 30	192.168.1.97	255.255.255.224 (/27)	192.168.1.126	NA	NA
	VLAN 40	192.168.1.129	255.255.255.	192.168.1.158	NA	NA

			224 (/27)			
	VLAN 50	192.168.1.161	255.255.255.240 (/28)	192.168.1.174	NA	NA
	VLAN 60	192.168.1.177	255.255.255.240 (/28)	192.168.1.190	NA	NA
	VLAN 70	192.168.1.193	255.255.255.240 (/28)	192.168.1.206	NA	NA
	VLAN 80	192.168.1.209	255.255.255.248 (/29)	192.168.1.214	NA	NA
	VLAN 90	192.168.1.217	255.255.255.248 (/29)	192.168.1.222	NA	NA
DSW2	G1/0/1	NA	NA	NA	SW1	G1/0/24
	G1/0/2	NA	NA	NA	SW2	G1/0/24
	G1/0/3	NA	NA	NA	SW3	G1/0/24
	G1/0/4	NA	NA	NA	SW4	G1/0/24
	G1/0/5 - G1/0/6 (PAGP)	Trunk	Trunk	NA	DSW1	G1/0/5 - G1/0/6
	G1/0/22	192.168.1.230	255.255.255.252 (/30)	NA	R1	G0/0/1
	G1/0/24	192.168.1.238	255.255.255.252 (/30)	NA	R2	G0/0/1
	VLAN 10	192.168.1.2	255.255.255.192 (/26)	192.168.1.62	NA	NA
	VLAN 20	192.168.1.66	255.255.255.224 (/27)	192.168.1.94	NA	NA
	VLAN 30	192.168.1.98	255.255.255.224 (/27)	192.168.1.126	NA	NA
	VLAN 40	192.168.1.130	255.255.255.224 (/27)	192.168.1.158	NA	NA
	VLAN 50	192.168.1.162	255.255.255.240 (/28)	192.168.1.174	NA	NA
	VLAN 60	192.168.1.178	255.255.255.240 (/28)	192.168.1.90	NA	NA
	VLAN 70	192.168.1.194	255.255.255.240 (/28)	192.168.1.206	NA	NA
	VLAN 80	192.168.1.210	255.255.255.	192.168.1.214	NA	NA

			248 (/29)			
	VLAN 90	192.168.1.218	255.255.255.248 (/29)	192.168.1.222	NA	NA
R1	G0/1/0	172.17.9.89	255.255.255.252 (/30)	NA	ISP	NA
	G0/0/0	192.168.1.225	255.255.255.252 (/30)	NA	DSW1	G1/0/22
	G0/0/1	192.168.1.229	255.255.255.252 (/30)	NA	DSW2	G1/0/22
	G0/1/1	192.168.1.242	255.255.255.252 (/30)	NA	R2	G0/1/1
R2	G0/1/0	172.17.10.90	255.255.255.252 (/30)	NA	ISP	NA
	G0/0/0	192.168.1.233	255.255.255.252 (/30)	NA	DSW1	G1/0/22
	G0/0/1	192.168.1.237	255.255.255.252 (/30)	NA	DSW2	G1/0/22
	G0/1/1	192.168.1.241	255.255.255.252 (/30)	NA	R1	G0/1/1

Table 4: Addressing Table

Core-Distribution Layer

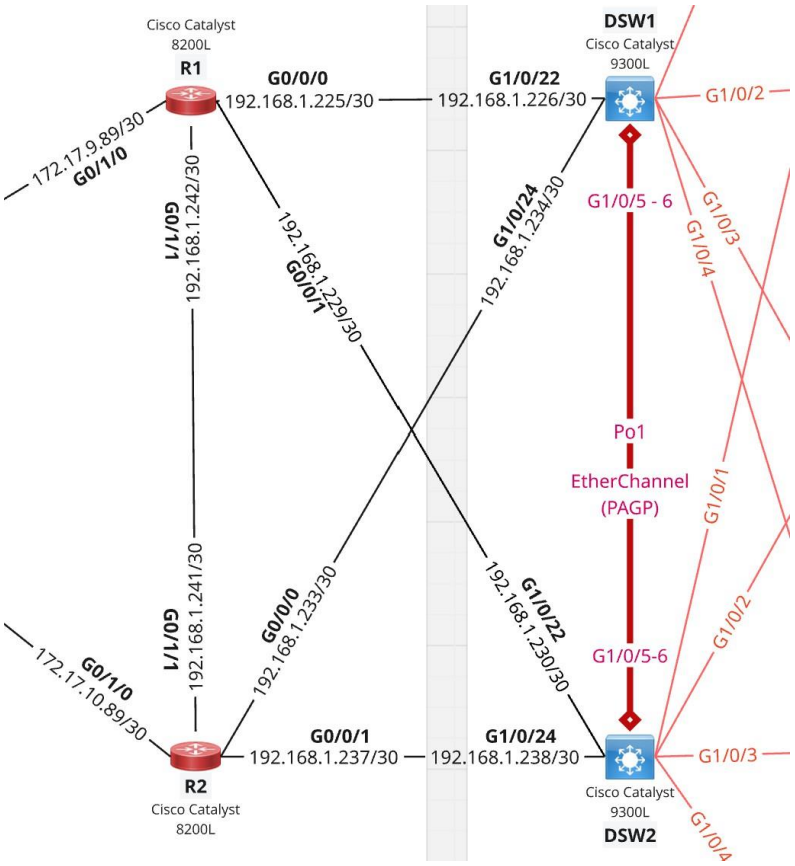

Figure 2: Core-Distribution Layer

In Figure 2, the core distribution layer is designed to handle traffic going in and out of the network such as to the internet and ISP. Based on the requirements, the end user must be able to connect to the internet and internet users must be able to connect to the web server to view the web page. As such, it is configured in such a way that R1 and R2 can receive the packets and forward the packets to the designated area which is to the DSW1 and DSW2. OSPF has been configured in the routers to ensure the best path to send the data packets.

HSRP has been configured on the DSW1 and DSW2 as the active routers for the 9 different VLANs. It helps with load balancing and applying redundancy logic. Each DSW layer 3 switch is connected to R1 and R2, ensuring a fail-safe connection if any of the routers or wires is faulty.

Distribution-Access Layer

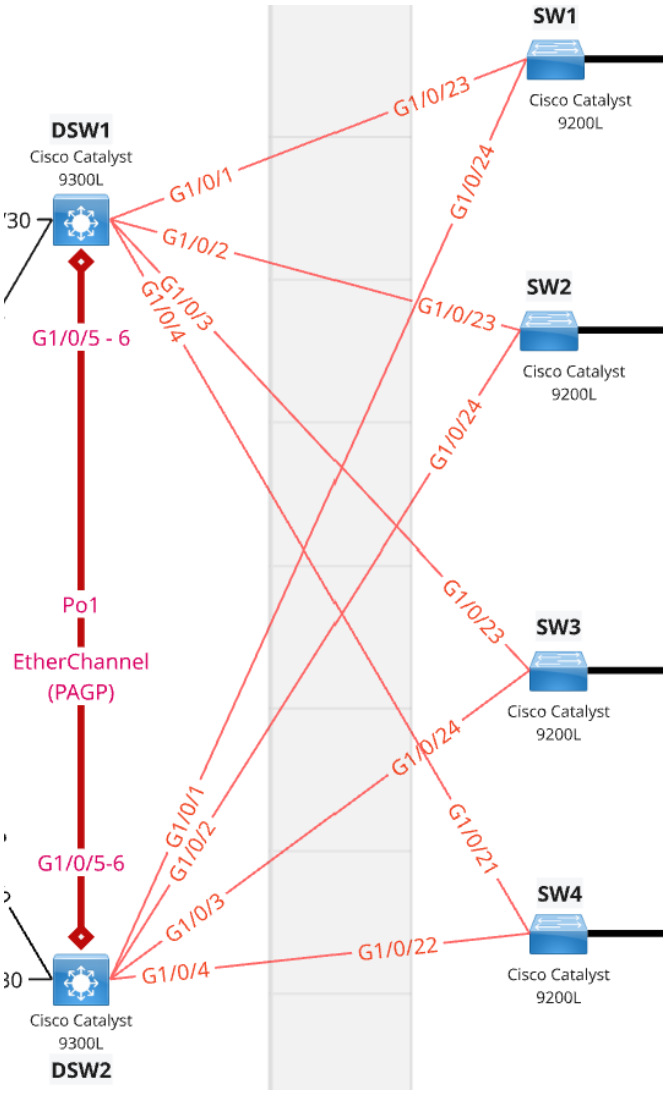

Figure 3: Distribution Access Layer

As shown in Figure 3, the DSW switches are connected to the layer 2 switches ranging from SW1 to SW4. This ensures that each switch is sufficient to support the required host. In the Layer 3 switches, it allows Inter-VLAN routing using Switched Virtual Interfaces (SVI). Additionally, the DSW switches act as the default gateway with HSRP configured to each of the subnets/VLANs interfaces.

Spanning-Tree Protocol is also configured in the distributed switches which ensures load balancing and redundancy. OSPF is also configured to provide the best path to send data across the network.

Finally, the access layer 2 switches. These switches have been configured with VLANs to logically separate the departments and labs into smaller broadcast domains.

Virtual Local Area Network (VLAN)

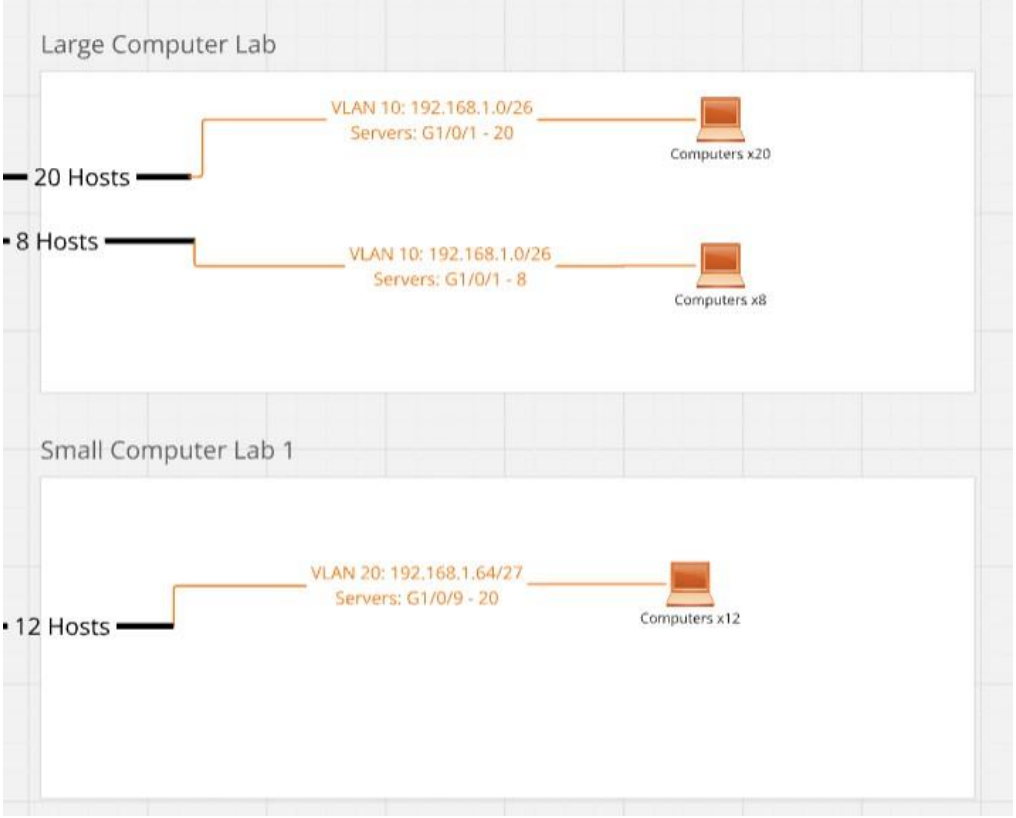

Figure 4: Large computer Lab & Small computer Lab 1 VLANs

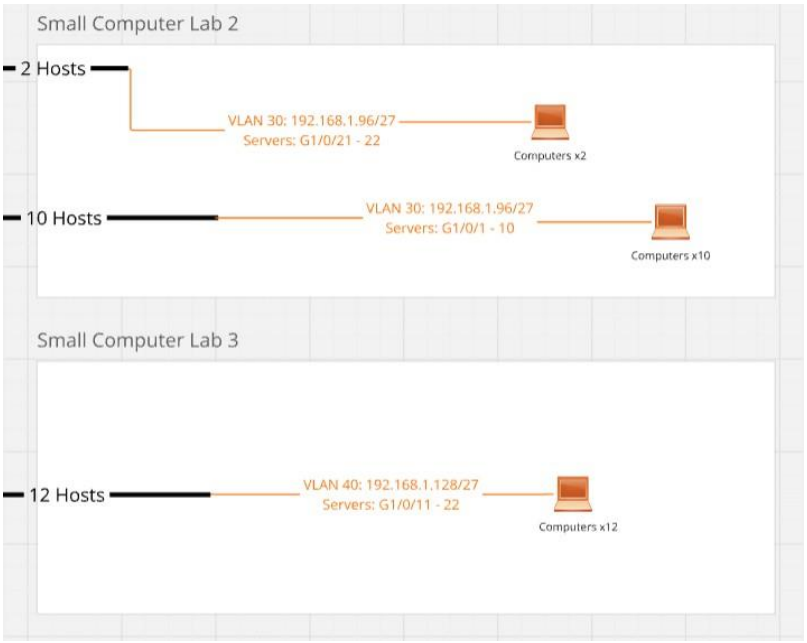

Figure 5: Small computer Lab 2 & 3 VLANs

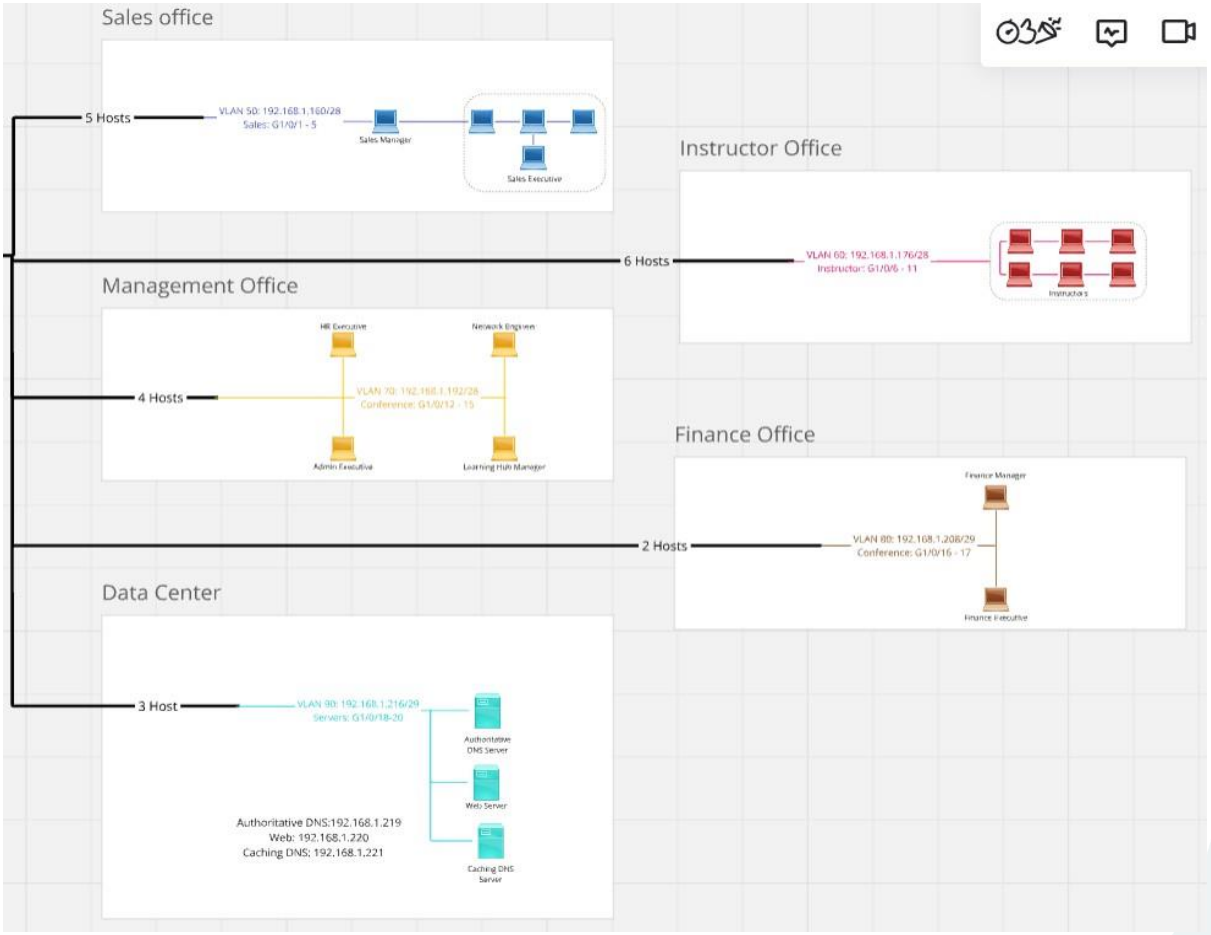

Figure 6: Different Departments VLAN

VLAN 10	VLAN 20	VLAN 30	VLAN 40	VLAN 50
Large Computer Lab	Small Computer Lab 1	Small Computer Lab 2	Small Computer Lab 3	Sales Office
VLAN 60	**VLAN 70**	**VLAN 80**	**VLAN 90**	
Instructor Office	Management Office	Finance Office	Internal Data Center	

Table 5: VLAN Configuration

Device	VLAN PORT MAPPING
S1	10:G0/1-20
S2	10:G0/1-8 , 20:G0/9-20 , 30:G0/21-22
S3	30:G0/1-10 , 40:G0/11-22
S4	50:G0/1-5 , 60:G0/6-11 , 70:G0/12-15 , 80:G0/16-17 , 90:G0/18-20

Table 6: VLAN-Switchport Association

In this topology, the VLANs have been divided by different departments and Labs as shown in Figure 4-6 and Tables 5 & 6. Orange PC colour indicates Lab computers while the other colours indicate department computers. Each computer in the labs and departments have a dedicated switch port for connection.

The reason behind assigning different VLANs to different departments/labs is that it helps to reduce the number of hosts in a network, which eases subnetting and VLSM. This will also help to ease any configuration issues, troubleshooting and maintenance work. It also makes the collision domain smaller, hence reducing the chances of packets not being sent to their destination.

Subnetting (VLSM)

VLAN	Subnet ID	CIDR	Subnet Mask	Hosts	Usable Host IP Range
10	192.168.1.0	/26	255.255.255.192	28	192.168.1.1 - 192.168.1.62
20	192.168.1.64	/27	255.255.255.224	12	192.168.1.65 - 192.168.1.94
30	192.168.1.96	/27	255.255.255.224	12	192.168.1.97 - 192.168.1.126
40	192.168.1.128	/27	255.255.255.224	12	192.168.1.129 - 192.168.1.158
50	192.168.1.160	/28	255.255.255.240	5	192.168.1.161 - 192.168.1.174
60	192.168.1.176	/28	255.255.255.240	6	192.168.1.177 - 192.168.1.190
70	192.168.1.192	/28	255.255.255.240	4	192.168.1.193 - 192.168.1.206
80	192.168.1.208	/29	255.255.255.248	2	192.168.1.209 - 192.168.1.214
90	192.168.1.216	/29	255.255.255.248	1	192.168.1.217 - 192.168.1.222

Table 7: VLSM Subnetting Table

By the given allocated IP address of 192.168.1.0/24 to fit into the topology, the team has created a VLSM table for each configuration and subnetting. Based on calculations, 192.168.1.0/24 can support a total of 254 usable hosts – which is able to support the number of hosts in the topology. As shown in Table 7, Each VLAN has their dedicated subnet which supports the usable host within that VLAN. Large Computer Lab requires the most number of hosts (28). Therefore, the team assigned /26 to support the usable host and have extra IPs for future expansion or configuration. This logic applies to other VLANs.

The team also put into consideration adding extra IPs for each VLAN. Those IPs are used for Network, Broadcast, HSRP Virtual IP and default gateway which is used for the Distributed DSW switches. All of the IPs assigned are being calculated with great accuracy to prevent overlapping of IPs.

Hot Standby Router Protocol (HSRP)

In this network, the Hot Standby Router Protocol (HSRP) is implemented across multiple VLANs to enhance redundancy and ensure continuous routing availability. This allows DSW1 and DSW2 to act as default gateways for devices within their respective subnets. The use of HSRP guarantees that if the active router fails, the standby router will immediately take over, minimising network downtime.

HSRP Configuration Overview:

Each VLAN is configured with Virtual IPs (VIPs), which ensures that devices always have a consistent gateway, even if the active router for the VLAN changes. The VIPs provide seamless failover between DSW1 and DSW2, ensuring continuous access for network devices in case of router failure.

Subnet ID	Switch D1	Switch D2	HSRP Virtual IP
192.168.1.0/26	192.168.1.1	192.168.1.2	192.168.1.3
192.168.1.64/27	192.168.1.65	192.168.1.66	192.168.1.67
192.168.1.96/27	192.168.1.97	192.168.1.98	192.168.1.99
192.168.1.128/27	192.168.1.129	192.168.1.130	192.168.1.131
192.168.1.160/28	192.168.1.161	192.168.1.162	192.168.1.163
192.168.1.176/28	192.168.1.177	192.168.1.178	192.168.1.179
192.168.1.192/28	192.168.1.193	192.168.1.194	192.168.1.195
192.168.1.208/29	192.168.1.209	192.168.1.210	192.168.1.211
192.168.1.216/29	192.168.1.217	192.168.1.218	192.168.1.219

Table 8: HSRP Configuration

DSW1 Configuration:

- Active Routers:
  - VLANs 10, 20, and 90 are active on DSW1.
- Standby Routers:
  - VLANs 30, 40, 50, 60, 70, and 80 are standby on DSW1.

DSW2 Configuration:

- Active Routers:
  - VLANs 30, 40, 50, 60, 70, and 80 are active on DSW2.
- Standby Routers:
  - VLANs 10, 20, and 90 are standby on DSW2

This configuration enables automatic failover, where if the active router for any VLAN fails, the standby router immediately assumes the active role using the pre-configured Virtual IP, ensuring continuous network operation.

Redundancy and Fault Tolerance:

HSRP's failover process is quick and transparent to devices, ensuring they

continue to communicate without noticeable downtime. This mechanism is crucial for maintaining the reliability and stability of the network, especially in environments where network availability is critical.

By implementing HSRP across multiple VLANs, the team has ensured that the network is resilient and fault-tolerant. DSW1 and DSW2 serve as backup gateways for each other, with clear roles for active and standby routers. This setup maximises uptime and minimises potential disruptions.

EtherChannel (PAGP)

In the diagram in figure 1, PAGP (Port Aggregation Protocol) is used to configure an EtherChannel between two Cisco Catalyst 9300L Layer 3 switches, DSW1 and its connected counterpart. EtherChannel is a technology that allows multiple physical network links to be combined into a single logical link. This aggregation increases the bandwidth between devices and provides redundancy in case one of the physical links fails. The use of PAGP simplifies the process of creating an EtherChannel by enabling dynamic negotiation between the switches. PAGP automatically determines whether the physical interfaces can be bundled together to create a single logical interface.

In this case, GigabitEthernet1/0/5 and GigabitEthernet1/0/6 on DSW1 are combined into an EtherChannel, which is represented as Po2 (Port-channel 2). The other Cisco Catalyst 9300L switch has corresponding interfaces, GigabitEthernet1/0/5-6, that are also bundled into the EtherChannel. PAGP ensures that both switches automatically recognize and agree to the EtherChannel configuration, without requiring manual intervention. By automatically managing the negotiation and configuration process, PAGP makes it easier for network administrators to set up link aggregation while reducing the chances of misconfiguration.

Using EtherChannel with PAGP provides several benefits, such as improved bandwidth and reliability. With multiple links in place, the aggregate bandwidth is effectively the sum of the individual physical links. This ensures that higher data throughput is possible between switches. Furthermore, EtherChannel increases fault tolerance. If one of the physical links in the EtherChannel goes down, the traffic is automatically redirected through the remaining active links. This process happens seamlessly, with minimal disruption to the network, ensuring continuous service availability.

Another significant advantage of using EtherChannel in Layer 3 switches is load balancing. The traffic between the two switches is distributed across all the physical links in the EtherChannel, which can help optimize the use of network resources. The distribution of traffic improves the overall network performance by preventing congestion on any single link. With EtherChannel, the network becomes more resilient to bottlenecks and ensures a smoother flow of data, especially in high-demand environments.

Overall, the configuration of EtherChannel using PAGP between two Layer 3 switches, as shown in the diagram, enhances the overall efficiency, scalability, and reliability of the network. It allows for higher throughput, fault tolerance, and load balancing, which are critical for ensuring a robust and high-performance network infrastructure. By using PAGP to dynamically configure the EtherChannel, network administrators can streamline the setup process while maintaining the flexibility to adapt to network changes.

Static Routing

Device	Destination	Next Hop	
		Device	IP Address
R1	0.0.0.0	ISP1	172.17.9.90 (Priority of 2)
	0.0.0.0	R2	192.168.1.241
R2	0.0.0.0	R1	192.168.1.242 (Priority of 2
	0.0.0.0	ISP2	172.17.10.90
DSW1	0.0.0.0	R1	192.168.1.225 (Priority of 250)
	0.0.0.0	R2	192.168.1.233
DSW2	0.0.0.0	R1	192.168.1.229 (Priority of 250)
	0.0.0.0	R2	192.168.1.237

Table 9: Static Routing Configuration

Static routing is used to manually configure network paths, providing a fixed route for traffic between devices and networks. Unlike dynamic routing, where routes are automatically learned and adjusted, static routing requires the network administrator to define each route. This method is particularly useful in

smaller or simpler networks, or when precise control over the routing path is necessary.

In this network, static routing directs traffic between internal devices and external networks. For example, R1 routes traffic to ISP1 via 172.17.9.90, and R2 routes to ISP2 via 172.17.10.90. DSW1 and DSW2 use predefined routes to direct traffic to R1 and R2 based on the destination IP. The advantage of static routing is that it offers complete control over network traffic, improving performance and security by ensuring traffic follows specific paths. However, it requires manual updates if there are network changes, making it less flexible in larger, dynamic environments. Overall, static routing provides a simple, reliable, and efficient way to manage traffic in controlled network setups.

Normally, a static route has an administrative distance (AD) of 1, making it a high-priority route. However, in this case, the AD is set to 250, which makes it a low-priority backup route. This means that if another route, such as one learned through OSPF or a directly connected route with a lower AD, is available, the router will prefer that route instead. The static route with an AD of 250 will only be used if no better (lower AD) routes exist, ensuring it acts as a failover option rather than a primary path.

NAT Pool Overload

NAT Pool Overload is implemented in the network to effectively manage the translation of private IP addresses to public ones. On R1, internal IPs in the 192.168.1.0/24 range are translated to a pool of public addresses ranging from 203.149.210.177/29 to 203.149.210.182/29, while R2 handles the translation of the same internal IP range to public IPs between 129.126.142.177/29 and 129.126.142.182/29.

The decision to use NAT Overload, also known as PAT (Port Address Translation), was driven by the need to maximise the use of a limited number of public IP addresses. With overload, multiple devices within the internal network can share a single or a few public IPs, thus addressing the issue of IPv4 address scarcity. This method is ideal for situations where many internal devices need internet access but there aren’t enough available public IPs to assign a unique one to each device.

Using NAT Pool Overload ensures efficient address utilisation and reduces the need for multiple public IPs. It also provides scalability, enabling the network to accommodate more devices without requiring additional public addresses. This

approach strikes a balance between conserving public IP space, ensuring smooth communication, and maintaining network security.

Dynamic Host Configuration Protocol (DHCP)

Subnet ID	R1 & R2 DHCP Address Pool	R1 & R2 Excluded DHCP Address Pool
192.168.1.0/26	192.168.1.1 - 192.168.1.62	192.168.1.0 - 192.168.1.2, 192.168.1.62
192.168.1.64/27	192.168.1.65 - 192.168.1.94	192.168.1.62 - 192.168.1.66, 192.168.1.94
192.168.1.96/27	192.168.1.97 - 192.168.1.126	192.168.1.94 - 192.168.1.98, 192.168.1.126
192.168.1.128/27	192.168.1.129 - 192.168.1.158	192.168.1.126 - 192.168.1.130, 192.168.1.158
192.168.1.160/28	192.168.1.161 - 192.168.1.174	192.168.1.158 - 192.168.1.162, 192.168.1.174
192.168.1.176/28	192.168.1.177 - 192.168.1.190	192.168.1.174 - 192.168.1.178, 192.168.1.190
192.168.1.192/28	192.168.1.193 - 192.168.1.206	192.168.1.190 - 192.168.1.194, 192.168.1.206
192.168.1.208/29	192.168.1.209 - 192.168.1.214	192.168.1.206 - 192.168.1.210, 192.168.1.214
192.168.1.216/29	192.168.1.217 - 192.168.1.222	192.168.1.214 - 192.168.1.218, 192.168.1.222 - 192.168.1.223

Table 10: DHCP Address Pool

The DHCP (Dynamic Host Configuration Protocol) is used to dynamically assign IP addresses to devices on a network, thus eliminating the need for manual configuration. In addition to assigning IP addresses, DHCP servers can also provide additional configuration parameters, such as the default gateway, DNS server, and other network settings. By using a DHCP addressing pool, devices can automatically obtain all necessary configurations upon connecting to the network.

To provide better network management and prevent conflicts, certain IP addresses within the DHCP pool are excluded. These exclusions are typically reserved for specific purposes, such as network addresses, broadcast

addresses, or other devices that require static IP assignments, such as routers or servers.

For example, in the network described, VLAN 10's DHCP pool spans from 192.168.1.1 to 192.168.1.62, excluding the address 192.168.1.0 (the network address), ensuring no devices are assigned this address. By doing so, network administrators can automate IP address assignments while maintaining control over critical network addresses.

Regarding the Topology, the team used both routers to set up the DHCP and DSW switches for the IP helper address that is to be assigned to the respective hosts in their specific VLANs. In addition, the team also configured the DNS server in the router, so that each host will be automatically assigned to the DNS. The DNS server is configured to use the authoritative server's IP address, and the DHCP lease time is set to 7 hours, meaning the lease must be renewed after this period.

In the distributed switch, the team set the IP helper-address point to the IP address of the router at each interface.

Open Shortest Path First V2 (OSPF)

DSW2 OSPF Configuration:

```
router ospf 1
 router-id 4.4.4.4
 passive-interface default
 no passive-interface GigabitEthernet1/0/22
 no passive-interface GigabitEthernet1/0/24
 network 192.168.1.0 0.0.0.255 area 0
!
```

DSW1 OSPF Configuration:

```
router ospf 1
 router-id 3.3.3.3
 passive-interface default
 no passive-interface GigabitEthernet1/0/22
 no passive-interface GigabitEthernet1/0/24
 network 192.168.1.0 0.0.0.255 area 0
!
```

R2 OSPF Configuration:

```
router ospf 1
 router-id 1.1.1.1
 passive-interface default
 no passive-interface GigabitEthernet0/0/0
 no passive-interface GigabitEthernet0/0/1
 no passive-interface GigabitEthernet0/1/1
 network 192.168.1.232 0.0.0.3 area 0
 network 192.168.1.236 0.0.0.3 area 0
 network 192.168.1.240 0.0.0.3 area 0
 default-information originate always
!
```

R1 OSPF Configuration:

```
router ospf 1
 router-id 2.2.2.2
 passive-interface default
 no passive-interface GigabitEthernet0/0/0
 no passive-interface GigabitEthernet0/0/1
 no passive-interface GigabitEthernet0/1/1
 network 192.168.1.224 0.0.0.3 area 0
 network 192.168.1.228 0.0.0.3 area 0
 network 192.168.1.240 0.0.0.3 area 0
 default-information originate always
!
```

The OSPFv2 configuration in this network is designed to ensure efficient routing, minimize unnecessary traffic, and improve security. OSPF (Open Shortest Path First) is a link-state routing protocol that dynamically learns and advertises network routes based on topology changes. The setup follows a structured approach, with all routers and switches operating in Area 0, the backbone area, which is essential for OSPF to function effectively in a multi-area environment.

Each router is assigned a unique router ID (1.1.1.1 for R2, 2.2.2.2 for R1, 3.3.3.3 for DSW1, and 4.4.4.4 for DSW2). The passive-interface default command is applied across all devices to prevent OSPF from sending Hello packets on unnecessary interfaces, reducing overhead and increasing security. However, specific interfaces are exempted from using no passive-interface to allow OSPF neighbour relationships to form where routing is required.

The network statements define which IP subnets participate in OSPF. R1 and R2 use more specific network statements with /30 subnets (0.0.0.3 wildcard mask), likely indicating point-to-point connections between routers. This precise configuration ensures OSPF only advertises the necessary links,

avoiding unnecessary complexity. Meanwhile, DSW1 and DSW2 use a broader network statement (192.168.1.0 0.0.0.255), allowing them to automatically include all VLANs and subnets within the 192.168.1.0/24 range without needing individual entries.

Another key part of this configuration is the 'default-information-originate always' command on R1 and R2, which ensures that a default route is advertised throughout the OSPF network. This allows all routers to have a path to external networks, which is useful in cases where these routers act as gateways to the internet or other remote destinations.

Overall, this OSPFv2 setup is designed with efficiency, security, and scalability in mind. The use of passive interfaces keeps routing updates controlled, while precise network advertisements ensure optimal performance. By structuring everything within Area 0, the network maintains a simple and reliable topology, preventing routing loops and ensuring seamless communication between all devices.

Domain Name System (DNS)

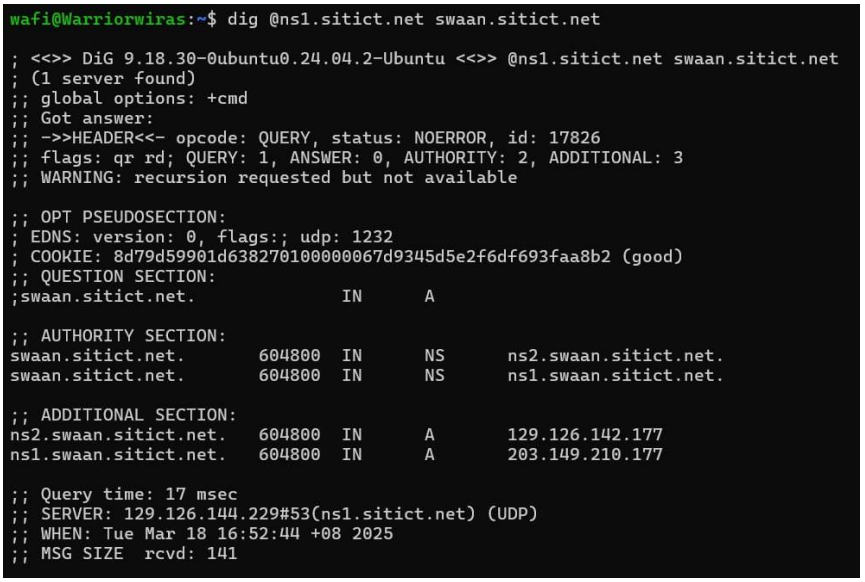

Figure 7: Domain Name System (DNS)

DNS plays a crucial role in converting easily memorable domain names (e.g., swaan.sitict.net) into machine-readable IP addresses. This conversion is essential because it allows users to access resources and services by typing in human-friendly domain names rather than having to remember numeric IP addresses. The primary goal of configuring DNS in the network is to ensure

smooth access to the IT learning hub's services and improve internal and external network communication by simplifying address management.

To achieve efficient domain resolution, the network configuration includes both an authoritative DNS server and a caching DNS server. The authoritative DNS server is responsible for storing and providing accurate DNS records for external users. For internal users, a caching DNS server is implemented to store DNS query results locally, reducing the time taken for future queries and minimising the load on the authoritative servers. By caching frequently accessed domain names, it improves overall network performance, ensuring users experience faster access to services without repeated lookups to the authoritative server.

The dig command result shown in Figure 7 queries the A record for swaan.sitict.net using ns1.sitict.net as the DNS server. The results indicate:

Query Type: The command is querying for an A (Address) record, which provides the IP address associated with the domain name swaan.sitict.net.
Authority Section: The response shows that ns1.sitict.net and ns2.sitict.net are the authoritative nameservers for swaan.sitict.net, meaning these servers are the official source for resolving queries related to this domain.
Additional Section: The query also provides the IP addresses for the nameservers ns1.sitict.net and ns2.sitict.net, confirming their role in handling DNS requests for the domain.
Result: The A record shows that swaan.sitict.net resolves to its corresponding IP address, making it accessible for both internal and external users who wish to visit the website using its domain name.

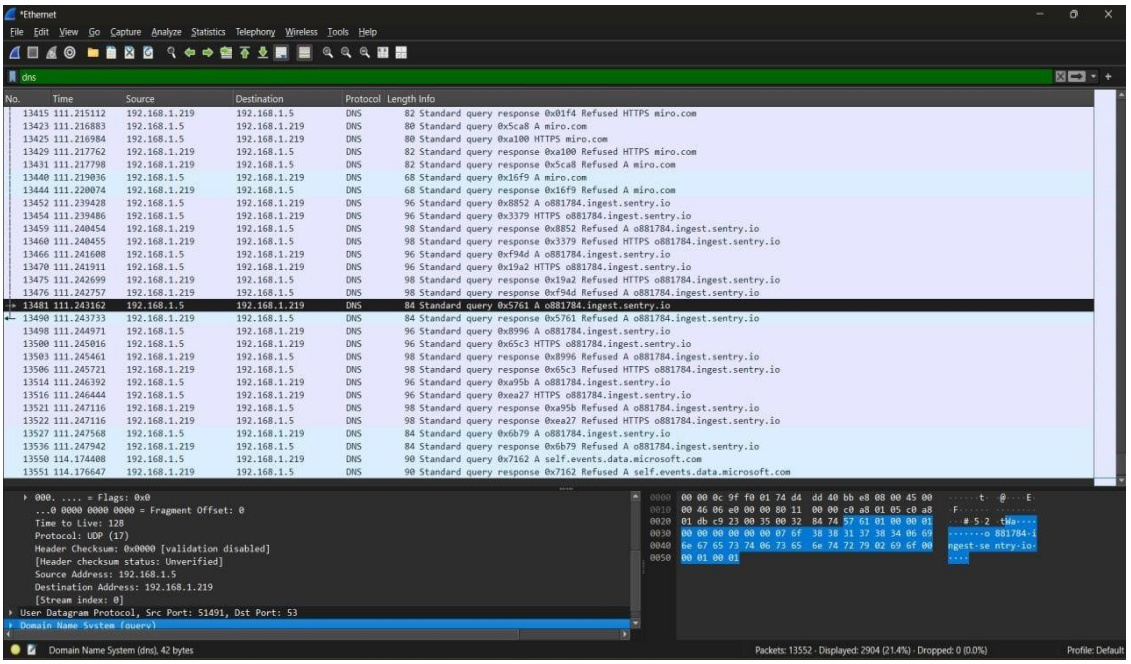

Figure 8: Wireshark (DNS)

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Physical Address. . . . . . . . . : 74-D4-DD-40-BB-E8
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::d68d:d938:f84:6550%4(Preferred)

   IPv4 Address. . . . . . . . . . . : 192.168.1.5(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.192
   Lease Obtained. . . . . . . . . . : Wednesday, 19 March 2025 11:40:17 am
   Lease Expires . . . . . . . . . . : Wednesday, 26 March 2025 3:41:37 pm
   Default Gateway . . . . . . . . . : 192.168.1.62
   DHCP Server . . . . . . . . . . . : 192.168.1.237
   DHCPv6 IAID . . . . . . . . . . . : 74765533
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2E-36-62-D5-74-D4-DD-40-B
B-E8
   DNS Servers . . . . . . . . . . . : 192.168.1.219
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Figure 9: Host Ip address

Upon connecting a laptop it is dynamically assigned an IP address, in this case–192.168.1.5–as shown in Figure 9. Since the host is connected within the internal network, the internal IP address of the web server is required to access the website. In Figure 8 we can see when we search our website domain, www.swaan.sitict.net, the host goes to the internal ip address, 192.168.1.219 which belongs to the authoritative server ip address since we are searching using the domain. Then we can see the server reply host in the next packet line.

Web Server

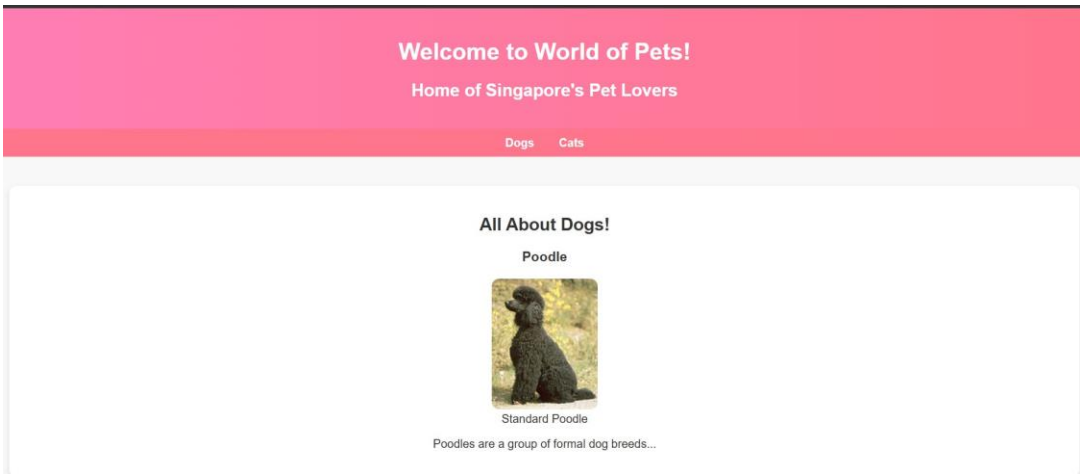

Figure 10: Web Server

Authoritative DNS is used to bind a web server to a static public IP address so that it can be accessed from the internet. With this setup, external users can resolve the server's domain name and access the server-hosted website. In order to convert human-readable domain names—such as www.swaan.sitict.com—into machine-readable IP addresses, the DNS is essential. The authoritative DNS provides internet users a dependable way to find the server. The server is set up using Xampp to host our website.

The internal network's VLAN 90 contains the web server itself, which aids in traffic segmentation and guarantees improved security and performance. 192.168.1.220/29 is the server's static private IP address, which keeps it isolated from other VLANs and external networks while enabling communication with other networked devices. While the web server is still reachable from the outside via the public IP, the private IP address makes sure it stays inside the boundaries of the internal network, increasing its security.

The static public IP is mapped to the web server's private IP using network address translation (NAT) and is appropriately routed in order to allow internet access to the web server. This enables proper routing of external traffic to the server within the internal network. In order for users to easily access the website hosted on the server, the setup also entails making sure that DNS records are propagated correctly throughout the internet.

This configuration, which combines efficient use of DNS, IP addressing, routing, and security measures, is essential for guaranteeing dependable and secure access to the web server. While the use of VLANs and static private IPs

improves network management and security, properly configuring authoritative DNS guarantees that the server is easily accessible. The web server can manage traffic effectively and safely with this configuration, giving users who visit the hosted website a seamless experience.

III. Reflection on GenAI

Throughout this project, we explored the use of Generative AI (GenAI) tools such as ChatGPT to assist with various aspects of our work, including troubleshooting network configurations. These tools helped us tackle complex issues efficiently and enhanced the clarity of our writing.

We used ChatGPT primarily for:

1. **Network Configuration Troubleshooting:**
   When we faced challenges, such as configuring IP routing priority or dealing with DNS cache issues, we turned to ChatGPT for guidance. The tool provided practical solutions and detailed explanations, which helped us solve problems more effectively. For instance, we used it to address DNS conflicts, where it explained how to clear cache and refresh records.

2. **Improving Report Clarity:**
   Writing the technical sections of the report required precision. ChatGPT helped us refine our explanations, ensuring that they were clear, concise, and easy to understand. It also assisted in rephrasing sections to improve readability without changing the technical meaning.

3. **Example Queries and Responses:**
   One example of how we benefited from using ChatGPT is when we asked for advice on how to fix DNS conflicts. Here's a sample query and response:

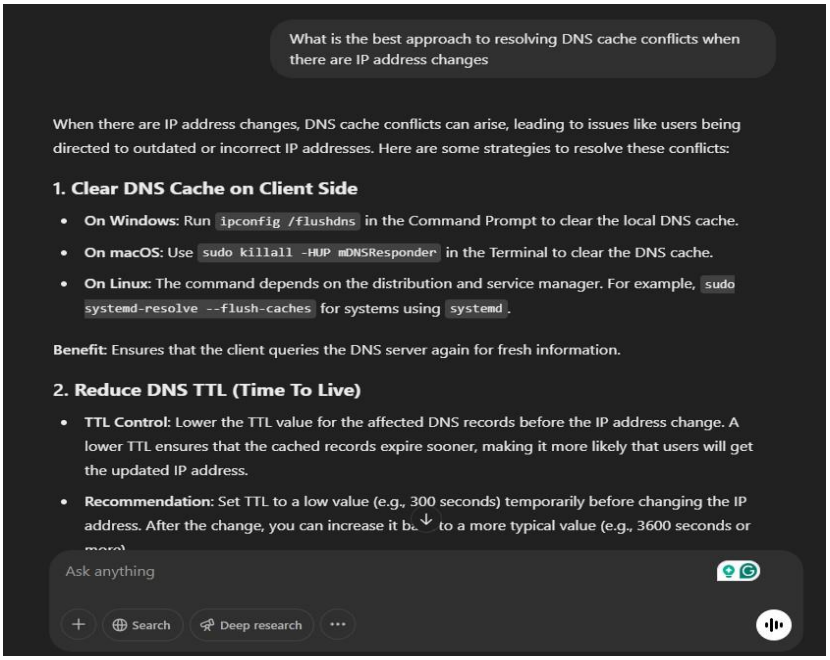

Figure 11: GenAI

This explanation was particularly useful, providing us with a clear and actionable solution to include in our report about DNS troubleshooting.

Benefits of Using GenAI Tools:
Incorporating ChatGPT into our workflow helped streamline the process and enhanced our overall productivity:

- **Time Efficiency**: We were able to get immediate answers, which allowed us to focus more on implementation rather than searching for solutions.
- **Improved Accuracy**: The AI tool assisted in ensuring that our configurations were correct and aligned with best practices.
- **Enhanced Report Quality**: With its assistance, we were able to present our ideas in a more structured and readable manner, improving the quality of the report and its structure.

Disadvantages of Using GenAI Tools:
Sometimes using ChatGPT does not give us the answers we expect, which may make things more difficult and complex.

- **Lack of Contextual Understanding**: Though GenAI tools provide quick answers and assist with ensuring configurations align with best practices, they might still lack a deep understanding of the specific network environment. This can sometimes lead to suggestions that are not fully tailored to the unique needs of the network, requiring manual adjustments.

- **Inconsistent configuration:** Based on our experiences, using GenAI tools sometimes provides inconsistent network configurations between switches. For example, DSW1 switch genAI gives a set of configurations, but in DSW2, another set of configurations. So, it will make the network not be able to get connectivity.
- **Over exaggeration:** ChatGPT may give over complicated answers when we require a short and precise answer. For example, when asked to explain a command simply, ChatGPT may give a long paragraph with redundant and excessive information that may make us more confused.

Using Generative AI tools like ChatGPT was incredibly beneficial throughout the project. It not only helped us solve technical challenges but also elevated the clarity and professionalism of our report. Based on our experience, we would recommend using such tools in future projects, especially when looking for efficient ways to improve the accuracy and quality of both technical work and documentation.

IV. Complications Faced

1a) Issue: Missing IP Routing Priority Between R1 and R2

During the network setup, we encountered an issue where R1 and R2 were both capable of routing traffic, but there was no clear routing priority set between the two. While OSPF was configured properly, this lack of prioritization led to inconsistent routing decisions, as both routers were vying to handle traffic, resulting in suboptimal routing and occasional delays.

1b) Solution: Configuring Routing Priority with R2 as Priority

To resolve the issue, we set R2 as the priority router for outbound traffic by configuring a lower OSPF cost on its connection to ISP2. This ensured that R2 would handle most of the routing duties under normal conditions. On the other hand, R1 was configured as the backup router, with a higher OSPF cost on its link to ISP1, so it would only be used if R2 was unavailable.

1b) Solution: Routing Configuration for ISP1 and ISP2

We also implemented static routes on both routers to make sure R2 would handle all traffic through ISP2, and R1 would step in to handle the traffic if R2 failed. This setup provided redundancy, allowing R1 to take over the routing in case of issues with R2, while still preventing unnecessary competition between the two routers.

1c) Outcome and Benefits

By assigning R2 as the priority router and R1 as the backup, we ensured that traffic was routed efficiently with minimal disruption. The failover mechanism works seamlessly, with R2 handling all traffic under normal circumstances and R1 taking over only when needed. This configuration improved network reliability, performance, and overall traffic management.

List of Figures

List of Tables