Network Security Assignment Report

ICT2217 Network Security

AY 2023-2024 Trimester 1

Lab P1&2 - Team Sum (Rack 14)

Prepared By:

Nicholas Sng Ray Shiang (2203197)
Khoo Xiaozhen Natalene (2202639)
Muhammad Fiqri Adam (2202878)
Koh Yong En Xande (2203203)
Karen Goh(2203430)
Khairul Nizam (2201088)
Chiu Zheng Hao Jonathan (2203187)

Table Of Contents

1. Introduction

The report outlines the procedures, rationale and network architecture required to implement a secured enterprise LAN as part of a requirement of design, installation, configuration, testing and commissioning of a secure IT infrastructure that is suitable for the National Gallery Singapore.

To achieve an efficient and high-availability design with minimum wastage of private and public IP addresses, the following concepts is being implemented in this topology:

- JumpHost
- Using firewall for Network Address Translation (NAT)
- Port-Channelling
- Inter-VLAN links by creating trunk links.
- Variable Length Subnet Mask (VLSM)
- Switch Virtual Interface (SVI)
- Terminal Access Controller Access-Control System (TACAS)
- Port Security
- System Logging Protocol (Syslog)
- SNMP
- Access Control Lists
- Network Time Protocol (NTP)
- DHCP
- SSH Key Authentication
- Dynamic Host Configuration Protocol (DHCP) Snooping
- SNORT

2. Setting up the Network Topology

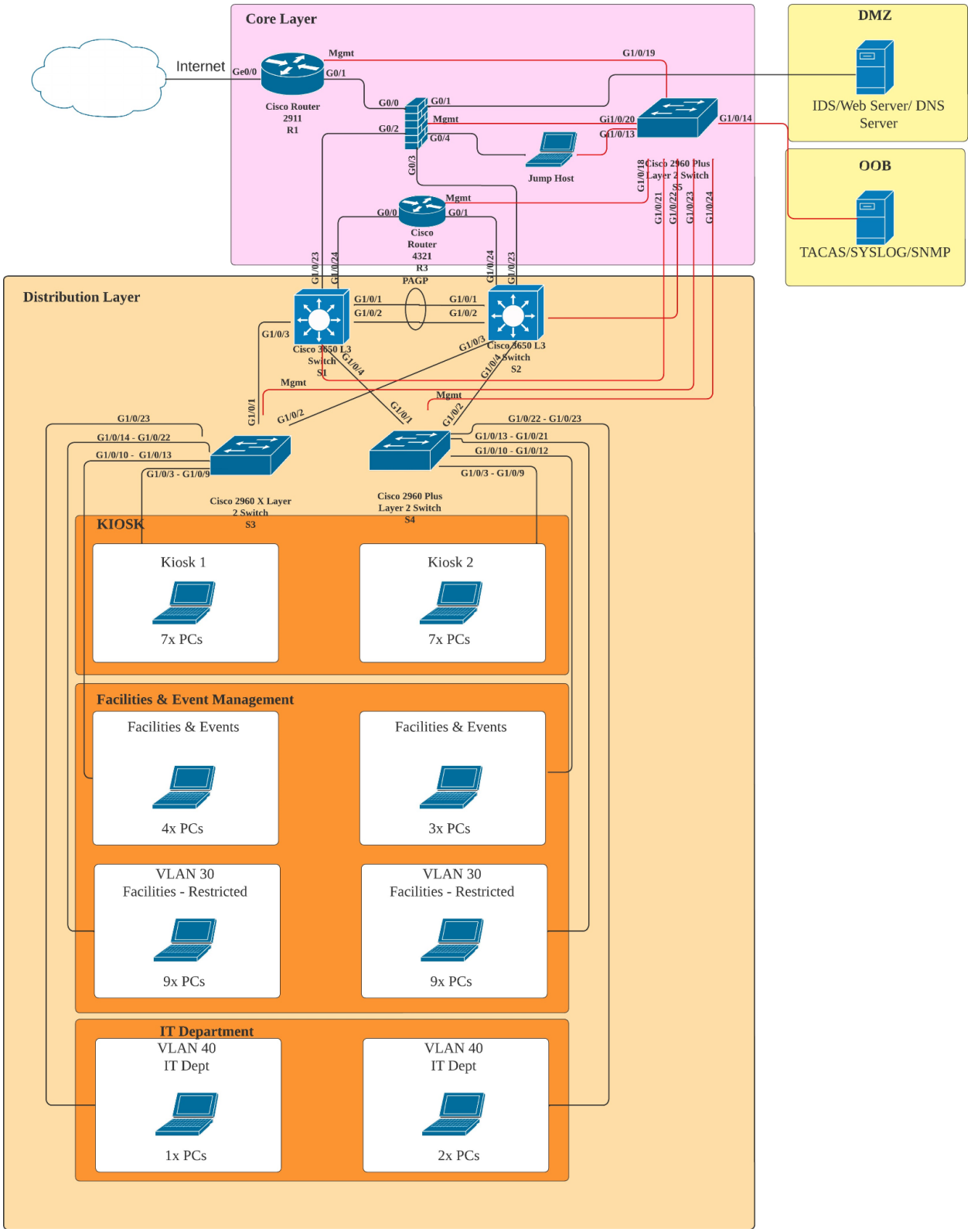
With a constraint budget, we are only limited to the following:

- 1 x ASA firewall
- 3 x routers
- 2 x 24-port layer-3 switch
- 3 x 24 port layer-2 switches
- 25 cables

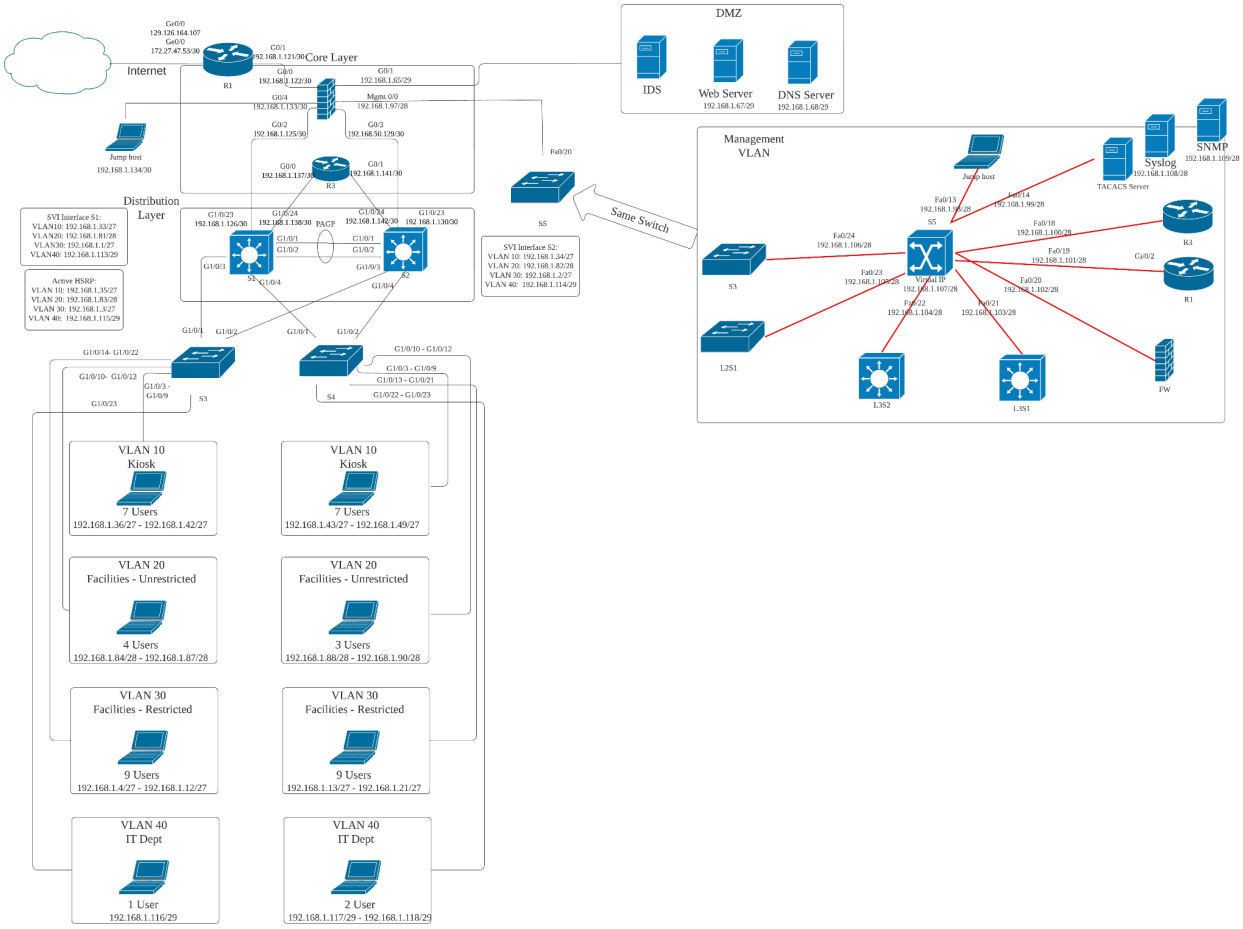
Our enterprise subnet is calculated based on the following requirements:

- 2 visitor kiosks: 7 PCs each with no access to the internet (total 14 PCs)
- Facilities & Event Management Department: 1 Director, 4 Managers and 20 associate staff
- IT Department: 1 Network Manager and 2 Network Engineers

2.1 Physical Topology



2.2 Logical Topology



2.3 Addressing Table - 15-11-23

Device	Interface	IP Address	Subnet Mask	Default Gateway	DNS Server	Comment
R1	G0/0	172.27.47.53	255.255.255.252	NA	NA	R1 - ISP
	G0/1	192.168.1.121	255.255.255.252	NA	NA	R1 - FW
R3	G0/0	192.168.1.137	255.255.255.252	NA	NA	R3 - MLS1
	G0/1	192.168.1.141	255.255.255.252	NA	NA	R3 - MLS2
Firewall	G0/0	192.168.1.122	255.255.255.252	NA	NA	FW - R1
	G0/1	192.168.1.65	255.255.255.248	NA	NA	FW - DMZ
	G0/2	192.168.1.125	255.255.255.252	NA	NA	FW - MLS1
	G0/3	192.168.1.129	255.255.255.252	NA	NA	FW - MLS2
	G0/5	192.168.1.133	255.255.255.252	NA	NA	FW - Jumphost
	Management port	192.168.1.97	255.255.255.240	NA	NA	FW - S5
MLS1	G1/0/1 - G1/0/2	ETHERCHANNEL				
	G1/0/3 - G1/0/4	TRUNKING				
	G1/0/23	192.168.1.126	255.255.255.252	NA	NA	MLS1 - FW
	G1/0/24	192.168.1.138	255.255.255.252	NA	NA	MLS1 - R3
MLS2	G1/0/1 - G1/0/2	ETHERCHANNEL				

	i1/0/3 - G1/0/4	TRUNKING				
	G1/0/23	192.168.1.130	255.255.255.252	NA	NA	MLS2 - FW
	G1/0/24	192.168.1.142	255.255.255.252	NA	NA	MLS2 - R3
L2S1	G1/01 - G1/0/2	TRUNKING				
	G1/0/3 - G1/0/9	192.168.1.36 - 192.168.1.42	255.255.255.224	192.168.1.35		Kiosk
	G1/0/10 - G1/0/13	192.168.1.84 - 192.168.1.87	255.255.255.240	192.168.1.83		Facilities - Unrestricted
	G1/0/14 - G1/0/22	192.168.1.4 - 192.168.1.12	255.255.255.224	192.168.1.3		Facilities - Restricted
	G1/0/23	192.168.1.116	255.255.255.248	192.168.1.115		IT Dept
L2S2	Gi1/0/1 - Gi1/0/2	TRUNKING				
	G1/0/3 - G1/0/9	192.168.1.43 - 192.168.1.49	255.255.255.224	192.168.1.35		Kiosk
	G1/0/10 - G1/0/12	192.168.1.88 - 192.168.1.90	255.255.255.240	192.168.1.83		Facil
	G1/0/13 - G1/0/21	192.168.1.13 - 192.168.1.21	255.255.255.224	192.168.1.3		IT department
	G1/0/22 - G1/0/23	192.168.1.117 - 192.168.1.118	255.255.255.248	192.168.1.115		
L2S3 (Management Switch)	G1/0/13	192.168.1.98	255.255.255.240	192.168.1.97		Jumphost
	G1/0/14 (Computer)	192.168.1.99	255.255.255.240	192.168.1.97		
	G1/0/14	192.168.1.108	255.255.255.240	192.168.1.97		Syslog

	(VM)					
	G1/0/14 (VM)	192.168.1.109	255.255.255.240	192.168.1.97		SNMP
	G1/0/18	192.168.1.100	255.255.255.240	192.168.1.97		R3
	G1/0/19	192.168.1.101	255.255.255.240	192.168.1.97		R1
	G1/0/20	192.168.1.102	255.255.255.240	192.168.1.97		FW
	G1/0/21	192.168.1.103	255.255.255.240	192.168.1.97		L3S1
	G1/0/22	192.168.1.104	255.255.255.240	192.168.1.97		L3S2
	G1/0/23	192.168.1.105	255.255.255.240	192.168.1.97		L2S1
	G1/0/24	192.168.1.106	255.255.255.240	192.168.1.97		L2S2
	VIP	192.168.1.107	255.255.255.240	192.168.1.97		Virtual IP of L2S3
DMZ	Computer	192.168.1.66	255.255.255.248	192.168.1.65		
	VM	192.168.1.67	255.255.255.248			Web Server
	VM	192.168.1.68	255.255.255.248			DNS Server
	VM	192.168.1.69	255.255.255.248			SIEM
JumpHost	Computer	192.168.1.134	255.255.255.252	192.168.1.135		Jumphost

2.4 Publicly accessible addresses

IP address of ISP serving rack 14: 172.27.47.106/30
Public Address: 129.126.164.104/29
https://teamsum.sitict.net/
interface of edge router/firewall connecting to ISP: 172.27.47.53/30
Web Server: 129.126.164.105/29

2.5 VLSM Table

Subnet Name	Needed Size	Allocated Size	Address	Mask	Dec Mask	Assignable Range	Broadcast
Facilities - Restricted	30	30	192.168.1.0	/27	255.255.255.224	192.168.1.1 - 192.168.1.30	192.168.1.31
Visitor Kiosk	30	30	192.168.1.32	/27	255.255.255.224	192.168.1.33 - 192.168.1.62	192.168.1.6 32
DMZ	14	14	192.168.1.64	/28	255.255.255.240	192.168.1.65 - 192.168.1.78	192.168.1.79
Facilities - Unrestricted	14	14	192.168.1.80	/28	255.255.255.240	192.168.1.81 - 192.168.1.94	192.168.1.95
Management	14	14	192.168.1.96	/28	255.255.255.240	192.168.1.97 - 192.168.1.110	192.168.1.111
IT Dept	6	6	192.168.1.112	/29	255.255.255.248	192.168.1.113 - 192.168.1.118	192.168.1.119

WAN Connection - R1 - FW	2	2	192.168.1.120	/30	255.255.255.252	192.168.1.121 - 192.168.1.122	192.168.1.123
WAN Connection - FW - MLS1	2	2	192.168.1.124	/30	255.255.255.252	192.168.1.125 - 192.168.1.126	192.168.1.127
WAN Connection - FW - MLS2	2	2	192.168.1.128	/30	255.255.255.252	192.168.1.129 - 192.168.1.130	192.168.1.131
WAN Connection - FW - Jumphost	2	2	192.168.1.132	/30	255.255.255.252	192.168.1.133 - 192.168.1.134	192.168.1.135
WAN Connection - R3 - MLS1	2	2	192.168.1.136	/30	255.255.255.252	192.168.1.137 - 192.168.1.138	192.168.1.139
WAN Connection - R3 - MLS2	2	2	192.168.1.140	/30	255.255.255.252	192.168.1.141 - 192.168.1.142	192.168.1.143
WAN Connection - MLS2 - Syslog	2	2	192.168.1.144	/30	255.255.255.252	192.168.1.145 - 192.168.1.146	192.168.1.145

2.6 DMZ

Device Name	Interface	Address	Subnet Mask	Connecting Device	
				Device Name	Interface
Web server	E01			IDS-Proxy	Br0
IDS	Br0	-	-	Web server	E01
	Br0	-	-	ASA	G1/0/3
Jumphost	E05			ASA	G1/0/4

3.0 High Availability Implementation

3.1 Multiple Network Connections

High availability is maintained with multiple network connections or paths so that in the case of a device failure, the entire architecture would not be affected and continue to work. It ensures redundancy, fault tolerance, load balancing, reduced latency, flexibility, and scalability.

3.2 Port-Channelling

Port-Channelling is a method of bundling ethernet links with LACP to make them work as a logical link and prevents link failure by providing redundancy, increased bandwidth, load balancing, and simplified management. With Port-Channelling being implemented in multiple Ethernet links, the logical link is still able to survive even if 1 ethernet cable is lost.

4.0 Security

4.1 TACACS

```
aaa new-model
aaa group server tacacs+ TACACS-SVR
 server-private 192.168.1.99 key j0Nc33naAa
ip tacacs source-interface Fddi0
aaa authentication login default group TACACS-SVR local
aaa authorization exec default group TACACS-SVR local
aaa accounting exec default start-stop group TACACS-SVR
username teamsum secret 5 $1$J3fE$JOLu.6Kt4QVZ.A1Alf26l.
aaa authorization exec default group TACACS-SVR local
aaa accounting exec default start-stop group TACACS-SVR
aaa accounting system default start-stop group TACACS-SVR
```

To handle AAA (Authentication, Authorization, Accounting), we will use Terminal Access Controller Access-Control System (TACACS) as our AAA server. We can authorize the users, assign appropriate privilege levels to the users, and account for the user's action when logged in. Our TACACS server will be hosted on Ubuntu.

4.2.1 Authentication:

To link the AAA server with the network device, a key is created. After the network device is configured to use TACACS, to enable access, users can be added into config files with the appropriate password, and placed into appropriate user groups. The key will also be added into the config. The users would be able to login into the network device using SSH with the credentials set on the server upon restarting the service.

4.2.2 Authorization:

Previously, in authentication, users were placed into user groups. Different privilege levels are assigned to each group which are for the user's login.

4.2.3 Accounting:

For accounting, TACACS server does the logging.

4.2 Port-Security

```
interface GigabitEthernet1/0/1
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
```

Port-security is a method where it allows the administrators to control and restrict access to a network switch port based on the MAC address of connected devices. It helps prevent unauthorized access to the network by limiting the number of devices or specific MAC addresses allowed on a particular switch port. This was implemented into the network so as to prevent common attacks such as MAC address spoofing.

4.3 System Logging Protocol (Syslog)

```
logging 192.168.1.99
logging trap debugging
```

Syslog protocol sends event data logs to a central location for collection and storage from network devices like routers, switches and firewalls. These devices are logged so that in case of any attacks we can keep track and investigate. It provides a history of events for audit purposes, and trend analysis and reporting.

4.4 Simple Network Management Protocol (SNMP)

```
snmp-server community public RO
snmp-server host 192.168.1.99 version 2c public
```

SNMP monitors, manages, and configures network devices. By monitoring network devices, we can identify potential security issues like overloaded devices and suspicious traffic patterns. When unusual activity is detected, we will be alerted. It then allows us to remotely configure the network devices. We hosted SNMP on Ubuntu.

4.5 Access Control Lists (ACL)

```
access-list 101 permit ip any any
interface GigabitEthernet1/0/1
ip access-group 101 in
```

ACL controls and limits access to network resources by setting a list of rules, specifying the permit or denying access of network resources. We have installed our ACL on routers and switches, filtering the network traffic. This helps in preventing unauthorized access, mitigating potential attacks like ICMP floods and limiting exposure to threats.

4.6 Network Time Protocol (NTP)

```
ntp server 192.168.1.121
ntp authenticate
ntp trusted-key 1
ntp authentication-key 1 md5 09564F071C0E1F1D
```

Network Time Protocol synchronizes the clock across the network devices in a network. This maintains the consistency of the log's timestamp in different systems and makes it more efficient to troubleshoot when an attack occurs.

4.7 Command privilege

```
privilege exec level 15 show running-config
```

Command privilege manages access to network resources and commands based on the user's role and responsibilities. We configured and allowed only the highest privilege level to use the enable command, to prevent non-admins from having privilege access to change any configurations.

4.8 Dynamic Host Configuration Protocol (DHCP) Snooping

```
ip dhcp snooping vlan 10
ip dhcp snooping trust
interface GigabitEthernet1/0/1
ip dhcp snooping trust
```

To prevent rogue DHCP servers from functioning inside the private network, snooping is used to protect from untrusted hosts that take over DHCP servers. It will be allowed if the DHCP traffic is from a trusted port, but drops if it comes from an untrusted port. With DHCP spoofing being implemented, it prevents attacks like DHCP spoofing attacks, starvation attacks etc.

4.9 SSH Key Authentication

```
crypto key generate rsa
ip ssh version 2
```

The traffic between the client and server is encrypted by the SSH network protocol to prevent eavesdropping on the traffic, like packet sniffing. It provides strong authentication as a private and public key pair is used. This can prevent brute forcing.

5.0 Additional Security / Features

5.1 Snort

Snort can detect intrusion and prevent attacks. Network traffic is analyzed in real time and Snort looks for known patterns or anomalies that could indicate security threats which will take the actions to block that traffic or alert administrators.
Snort also has integration capabilities. Snort can be integrated with other security tools and systems, allowing for comprehensive security architectures that can share alerts and data for overall protection.

5.2 Static NAT Translation on Firewall

NAT translation is used on Cisco ASA firewall. As it uses specific interface names and objects, ASA firewall is more complex syntax for NAT translations.

5.3 Defenses- DHCP spoofing

```
ip dhcp relay information trust-all
ip dhcp snooping vlan 10,20,30,40
no ip dhcp snooping information option
ip dhcp snooping limit rate 5
```

5.2.1 Reason for implementation

1. Intrusion Prevention: DHCP snooping acts as a guard to prevent DHCP spoofing, ensuring only legitimate DHCP responses are relayed.
2. Network integrity: Maintains the network's IP address allocation integrity, protecting against unauthorized access and various attacks.

5.2.2 DHCP configuration

1. VLAN Deployment: Implemented on VLANS 10,20,30 and 40, distinguishing trusted and untrusted interfaces.
2. Traffic control: Rate limiting on untrusted interfaces to prevent DHCP flooding and maintaining network stability.

5.2.3 Procedure

1. Attacker deploys a rogue DHCP server, sending out malicious DHCP messages.
2. DHCP Snooping validates DHCP traffic, distinguishing between authorized and illegitimate DHCP messages.
3. If DHCP Snooping detects an unauthorized DHCP message, it blocks the message from reaching the client.
4. DHCP Snooping logs the event for administrator review, confirming the intervention and details of the blocked attempt.

5.2.4 Limitations

1. Resource overhead: Introduces additional processing which could impact performance on resource-constrained devices.
2. Configuration Complexity: Requires meticulous setup and regular updates to adapt to evolving network demands and threats.

5.4 Defenses- Dynamic ARP Inspection

ip arp inspection trust

5.3.1 Reason for implementation

1. Security Enhancement: Prevents ARP poisoning/spoofing by ensuring only valid ARP messages are relayed.
2. Network Integrity: Maintain accurate IP-MAC address mappings, and prevent main-in-the-middle attacks.

5.3.2 Configuration

1. VLAN Deployment: DAI is enabled on VLANs 10, 20, 30 and 40, segregating traffic based on trust levels.
2. Traffic Management: Traffic is rate-limited on untrusted interfaces to avert ARP flood attacks, with the ip dhcp snooping limit rate 5 command setting a cap of 5 packets per second on certain interfaces, indirectly applying to ARP traffic through DHCP snooping validation.

5.3.3 Procedure:

1. An attacker attempts to compromise network integrity by sending spoofed ARP messages.
2. DAI examines incoming ARP replies on untrusted interfaces, referencing the DHCP snooping database for validation.
3. If DAI identifies a spoofed ARP reply, it blocks the response and may trigger an alert based on the configuration.
4. Administrators can review the DAI logs to verify the detection and response to the ARP spoofing attempt.

5.3.4 Limitations:

1. Resource Consumption: May introduce additional processing load that could affect network device performance.

6.0 Conclusion

In summary, we have designed a network topology that best suits the requirement of deploying in the National Gallery Singapore. With the security features implemented, we believe that it will give appropriate privilege and access to the relevant users and protect the organization’s infrastructure from online attacks.