ASIA PACIFIC UNIVERSITY
OF TECHNOLOGY & INNOVATION

GROUP ASSIGNMENT

TECHNOLOGY PARK MALAYSIA

CT037-3-2-NWS

Network Security

INTAKE CODE: APU2F2506IT(FT) / APU2F2506IT(ISS)

LECTURER: Noris binti Ismail

DATE ASSIGNED: 1/7/2025

DATE COMPLETED: 17/10/2025

NO	STUDENT NAME	TP NUMBER
1	CHAN MIN HUEY	TP083261
2	GONG YEE CHENG	TP081910
3	KANG HONG QIAN	TP081205
4	WOO MAY ENG	TP082001
5	YAP LI SHAN	TP080968

Table of Contents

1.0 Work Breakdown Structure

NAME PART	CHAN MIN HUEY **TP083261**	KANG HONG QIAN **TP081205**	GONG YEE CHENG **TP081910**	YAP LI SHAN **TP080968**
Introduction	✓			
Topology of Diagram				✓
Q1				
Q2		✓		
Q3				
Q4		✓		
Q5	✓			
Q6		✓		
Q7				✓
Q8	✓			
Q9				✓
Q10				
Q11				✓
Q12			✓	
Q13		✓		
Q14			✓	
Q15			✓	
Q16	✓			
Q17				
Documentation of the configured devices		✓		
Conclusion			✓	

Signature				
Workload %	25%	25%	25%	25%

2.0 Introduction

In today’s world, safeguarding corporate network security is very important. It helps to protect sensitive data, guarantee service accessibility and ensure business continuity. NetSecure Solutions headquartered in Kuala Lumpur and has a branch in Singapore, operates multiple departments and critical services deployed within a DMZ environment. With the growing number of cybersecurity threats, this project aims to design and deploy a network infrastructure that is secure and extensible. The solution proposed will use structured IP addressing schemes and routing mechanisms, VLAN segmentation and VPN connections to secure safe communications between the two office locations. Network security will also be enhanced by Layer 2 and Layer 3 security mechanisms, access controls, encryption protocols, intrusion detection mechanisms, and implementation of bastion host. Wireless networks, DHCP, and IoT deployments will be secured using proper mitigation methods. The project overall shall establish a network that is highly resilient and complies with organizational needs while safeguarding itself against internal and external hacking attempts.

3.0 Topology of Network Diagram

3.1 Overview of Network Topology

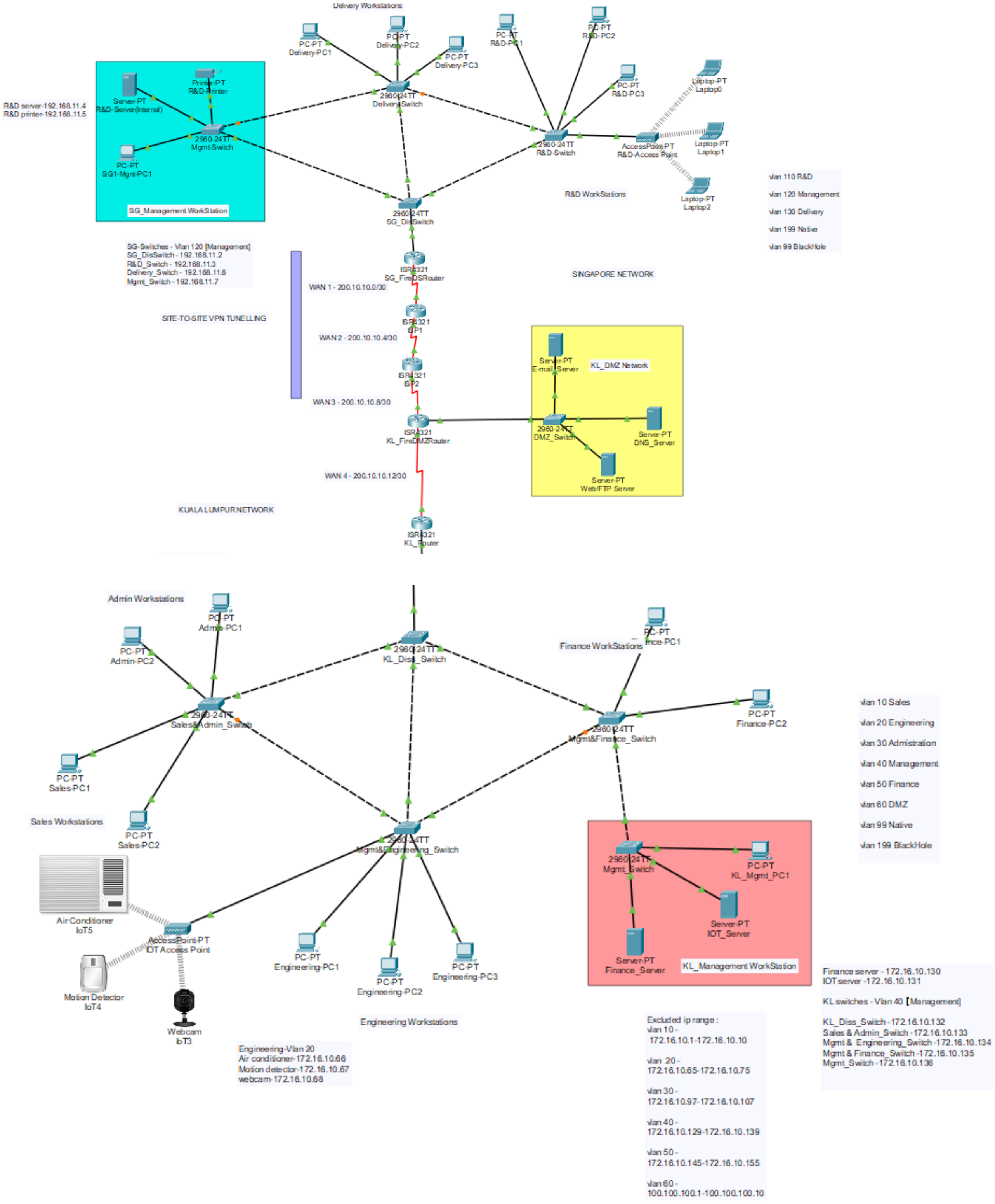


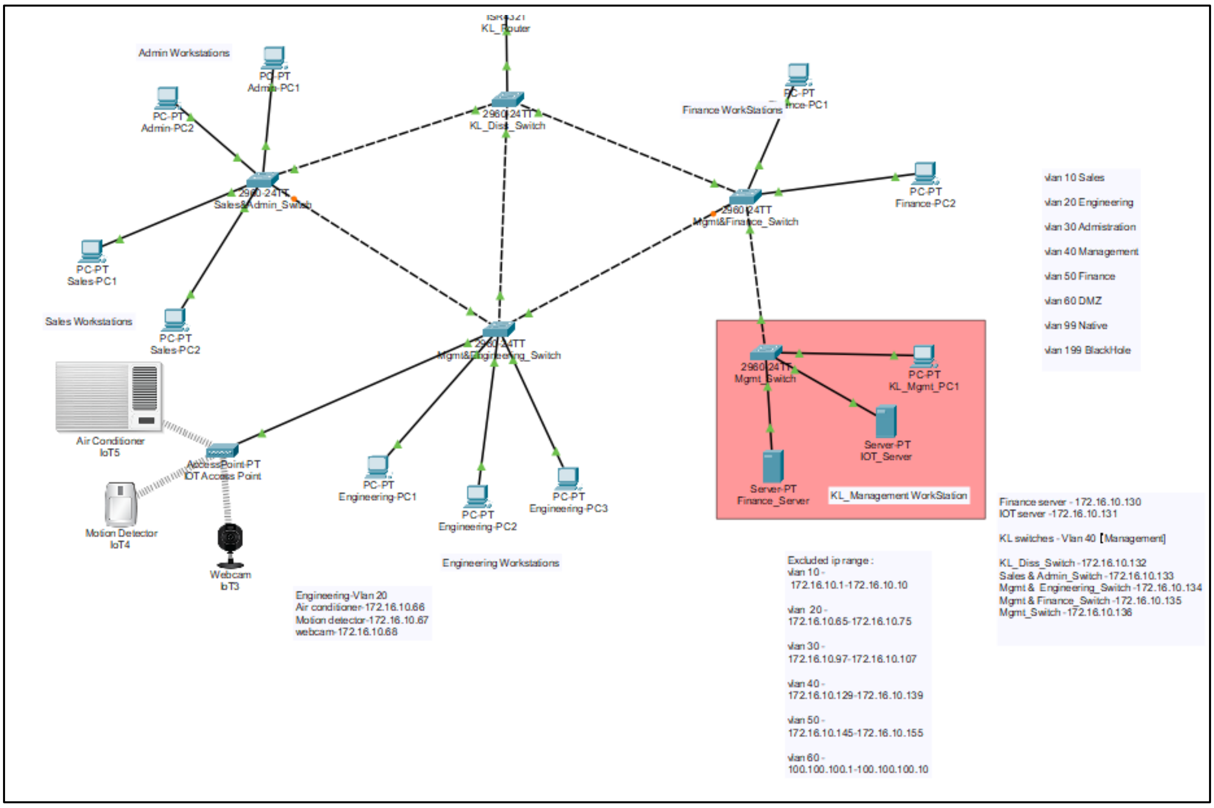
Figure 3.1 NetSecure Headquarters and Branch Network Topology Overview Diagram

This project aims to design and implement a secure and efficient enterprise network architecture for NetSecure Solutions. The company's headquarters is located in Kuala Lumpur, Malaysia (KL HQ), and its Branch is established in Singapore. Both sites are interconnected via a Wide Area Network (WAN), with secure isolation for internal communications and external access achieved through firewalls, a DMZ, and a multi-layer switching network.

This network topology adopts the typical Hierarchical network design model, including the core layer, distribution layer and access layer. Different departments are logically divided through VLAN technology, and a DMZ (Demilitarized Zone) area is set up at the headquarters to host public servers such as Web, Mail, and FTP servers.

This architecture not only meets the communication needs of all departments within the company but also complies with the standards of enterprise-level security management. The entire topology is protected by a firewall at the boundary and accessed through the public network provided by the ISP to achieve data communication between the headquarters and the branches.

3.2 KL HQ Network Topology



vlan 10 Sales
vlan 20 Engineering
vlan 30 Admistration
vlan 40 Management
vlan 50 Finance
vlan 60 DMZ
vlan 99 Native
vlan 199 BlackHole

Engineering-Vlan 20
Air conditioner-172.16.10.66
Motion detector-172.16.10.67
webcam-172.16.10.68

Excluded ip range :
vlan 10 -
172.16.10.1-172.16.10.10

vlan 20 -
172.16.10.65-172.16.10.75

vlan 30 -
172.16.10.97-172.16.10.107

vlan 40 -
172.16.10.129-172.16.10.139

vlan 50 -
172.16.10.145-172.16.10.155

vlan 60 -
100.100.100.1-100.100.100.10

Finance server - 172.16.10.130
IOT server -172.16.10.131

KL switches - Vlan 40 【Management]

KL_Diss_Switch -172.16.10.132
Sales & Admin_Switch -172.16.10.133
Mgmt & Engineering_Switch -172.16.10.134
Mgmt & Finance_Switch -172.16.10.135
Mgmt_Switch -172.16.10.136

Figure 3.2 Topology Diagram of Kuala Lumpur Headquarters

The Kuala Lumpur headquarters network is composed of multiple subnets, covering five main departments, namely Sales, Engineering, Administration, Management and Finance. Additionally, the headquarters also has a DMZ area, which is used to deploy servers for external services.

VLAN planning table:

Department	VLAN	IP Adress	Number of Hosts
Sales	10	172.16.10.0	50
Engineering	20	172.16.10.64	30
Administration	30	172.16.10.96	20
Management	40	172.16.10.128	15
Finance	50	172.16.10.144	15
Native VLAN	99		
Black Hole	199		

In this topology, each department's VLAN is independently assigned an IP address range, and the Layer 3 routing forwarding is handled by the distributed switch. This structure effectively reduces the broadcast domain range, improving network performance and management efficiency.

3.3 DMZ (Demilitarized Zone) structure

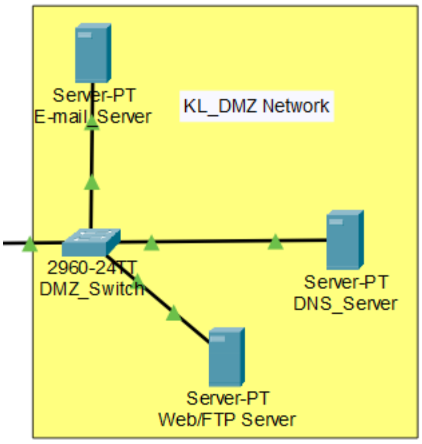


Figure 3.3 DMZ Network Topology Diagram

DMZ (Demilitarized Zone) area as the external service interface and is used to host server resources that need to be accessed from the outside. The DMZ and the internal local area network (LAN) are logically isolated by a firewall, thereby preventing external attacks from directly threatening the internal network security. This is because the firewall applies access control policies between the DMZ and the LAN, so only opening necessary ports such as 80, 443, 25 to ensure the security of the internal system while maintaining the accessibility of external communication.

3.4 SG Network Topology

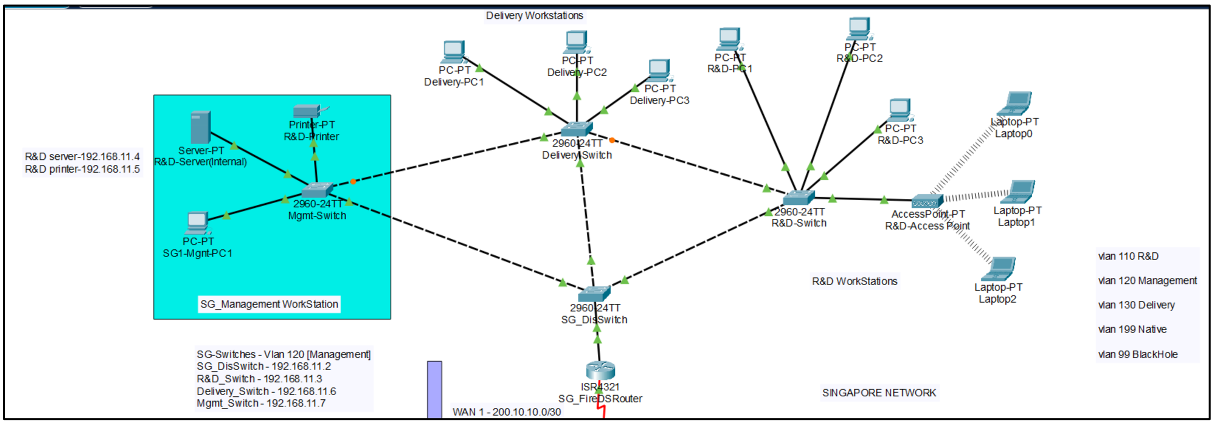


Figure 3.4 Topology Diagram of SG

The Singapore branch mainly consists of three departments, which is Research & Development Department, Management Department and Delivery Department. The network structure of the SG branch is simple and clear. It uses a single core routing device (SG_FireDSRouter) to achieve communication between internal VLANs and external connections.

VLAN planning table:

Department	VLAN	IP Adress	Number of Hosts
Research & Development	110	192.168.10.0	150
Management	120	192.168.11.0	150
Delivery departments	130	192.168.12.0	150
Native VLAN	99	[redacted]	
Black Hole	199		

SG_FireDSRouter functions as a multi-purpose router, is not only responsible for inter-VLAN routing but also serves as a NAT and DHCP service device. It provides default gateways, DNS forwarding, and security exits for each subnet. The terminal devices (PC or IoT devices) of each department are connected to the router through the switch to achieve high-speed local area communication and external access.

4.0 Chapters / sections with screen shots for evidence

4.1 HTTP, HTTPS

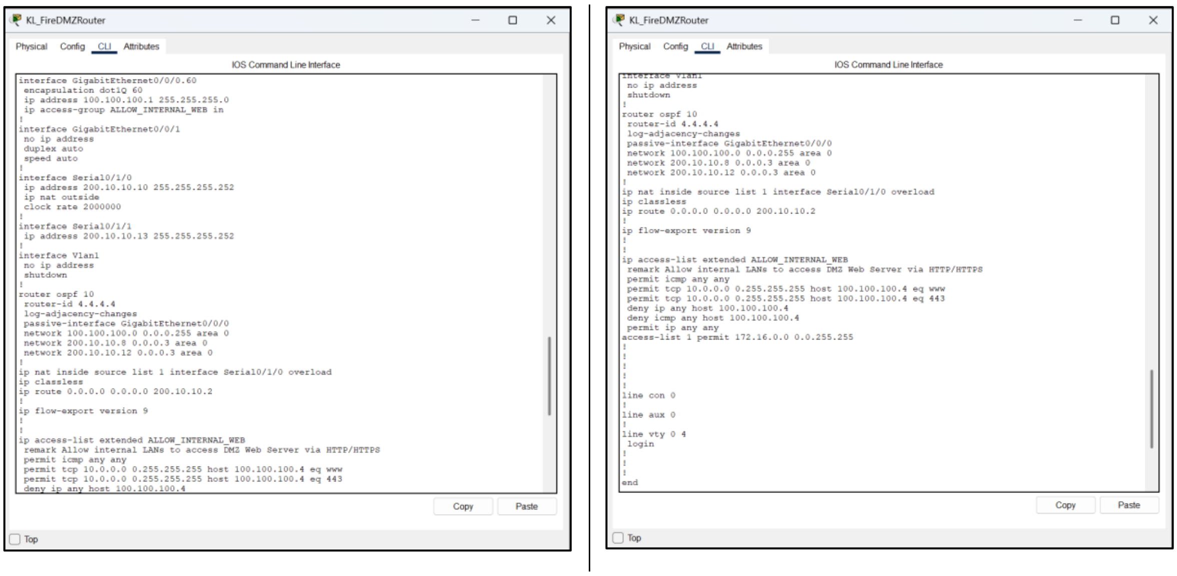
4.1.1 Question

Client workstations (admin, management, sales, engineering, finance, R&D and delivery) must be able to access the web server at the DMZ over HTTP and HTTPS. (Solution and configuration)

4.1.2 Solution

To ensure all clients VLANs (Admin, Sales, Engineering, Finance, R&D, Delivery, Management) within the internal LAN can access the Web Server hosted in the DMZ network using HTTP (port 80) and HTTPS (port 443). The Demilitarized Zone (DMZ) network hosts the organization’s Web Server with IP address 100.100.100.4. An Access Control List (ACL) named ALLOW_INTERNAL_WEB was configured on the KL_FireDMZRouter to permit only the required traffic, and it was applied to the DMZ sub-interface GigabitEthernet0/0/0.60.

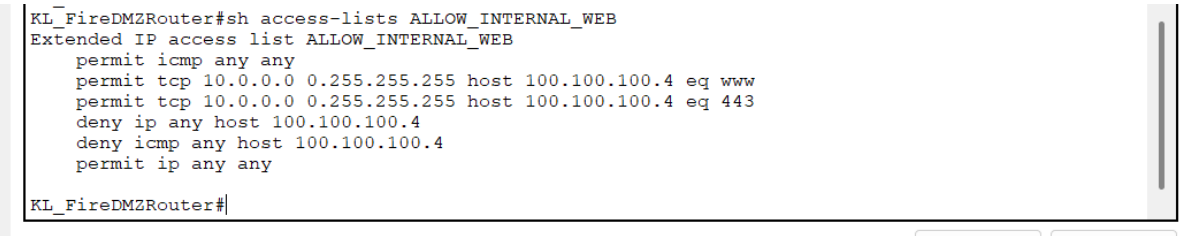
4.1.3 Configuration



```
interface GigabitEthernet0/0/0.60
 encapsulation dot1Q 60
 ip address 100.100.100.1 255.255.255.0
 ip access-group ALLOW_INTERNAL_WEB in
!
interface GigabitEthernet0/0/1
 no ip address
 duplex auto
 speed auto
!
interface Serial0/1/0
 ip address 200.10.10.10 255.255.255.252
 ip nat outside
 clock rate 2000000
!
interface Serial0/1/1
 ip address 200.10.10.13 255.255.255.252
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 10
 router-id 4.4.4.4
 log-adjacency-changes
 passive-interface GigabitEthernet0/0/0
 network 100.100.100.0 0.0.0.255 area 0
 network 200.10.10.8 0.0.0.3 area 0
 network 200.10.10.12 0.0.0.3 area 0
!
ip nat inside source list 1 interface Serial0/1/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 200.10.10.2
!
ip flow-export version 9
!
!
ip access-list extended ALLOW_INTERNAL_WEB
 remark Allow internal LANs to access DMZ Web Server via HTTP/HTTPS
 permit icmp any any
 permit tcp 10.0.0.0 0.255.255.255 host 100.100.100.4 eq www
 permit tcp 10.0.0.0 0.255.255.255 host 100.100.100.4 eq 443
 deny ip any host 100.100.100.4
```

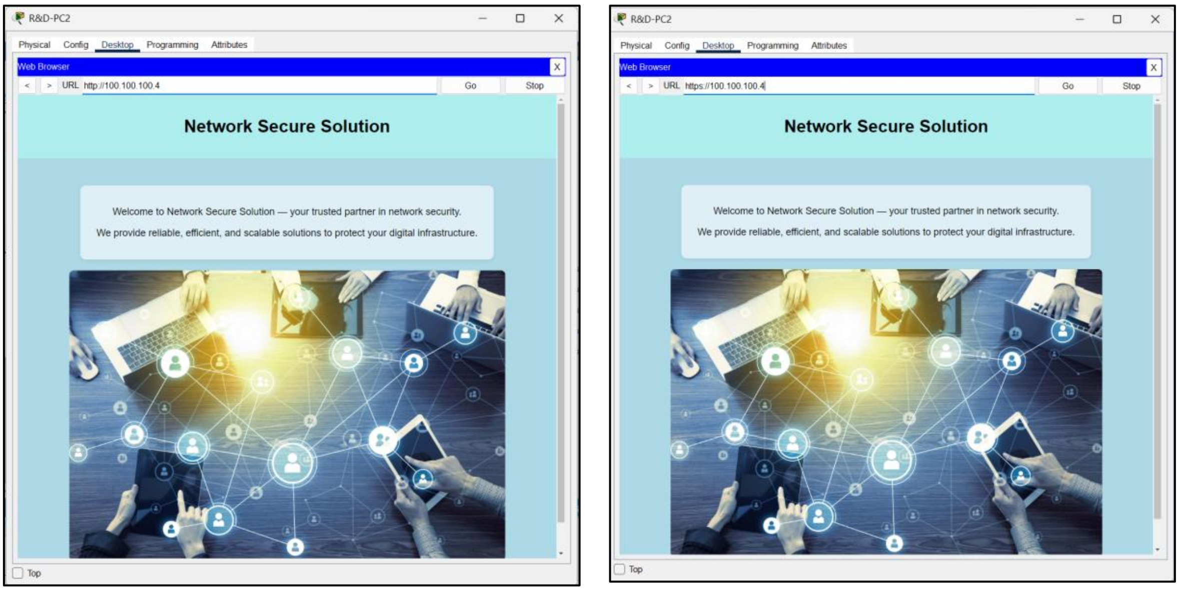
```
interface Vlan1
 no ip address
 shutdown
!
router ospf 10
 router-id 4.4.4.4
 log-adjacency-changes
 passive-interface GigabitEthernet0/0/0
 network 100.100.100.0 0.0.0.255 area 0
 network 200.10.10.8 0.0.0.3 area 0
 network 200.10.10.12 0.0.0.3 area 0
!
ip nat inside source list 1 interface Serial0/1/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 200.10.10.2
!
ip flow-export version 9
!
!
ip access-list extended ALLOW_INTERNAL_WEB
 remark Allow internal LANs to access DMZ Web Server via HTTP/HTTPS
 permit icmp any any
 permit tcp 10.0.0.0 0.255.255.255 host 100.100.100.4 eq www
 permit tcp 10.0.0.0 0.255.255.255 host 100.100.100.4 eq 443
 deny ip any host 100.100.100.4
 deny icmp any host 100.100.100.4
 permit ip any any
access-list 1 permit 172.16.0.0 0.0.255.255
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
!
end
```

Figure 4.1.1 – Configure ACL in KL_FireDMZRouter



```
KL_FireDMZRouter#sh access-lists ALLOW_INTERNAL_WEB
Extended IP access list ALLOW_INTERNAL_WEB
    permit icmp any any
    permit tcp 10.0.0.0 0.255.255.255 host 100.100.100.4 eq www
    permit tcp 10.0.0.0 0.255.255.255 host 100.100.100.4 eq 443
    deny ip any host 100.100.100.4
    deny icmp any host 100.100.100.4
    permit ip any any

KL_FireDMZRouter#
```

Figure 4.1.2 – Verify ACL working



URL http://100.100.100.4

URL https://100.100.100.4

Network Secure Solution

Welcome to Network Secure Solution — your trusted partner in network security.

We provide reliable, efficient, and scalable solutions to protect your digital infrastructure.

Figure 4.1.3 – HTTP & HTTPS

As seen in the Figure 4.1.3, from any external VLAN workstation such as access via HTTP (http://100.100.100.4) is successful, while access via HTTPS (https://100.100.100.4) is also successful.

4.2 FTP

4.2.1 Question

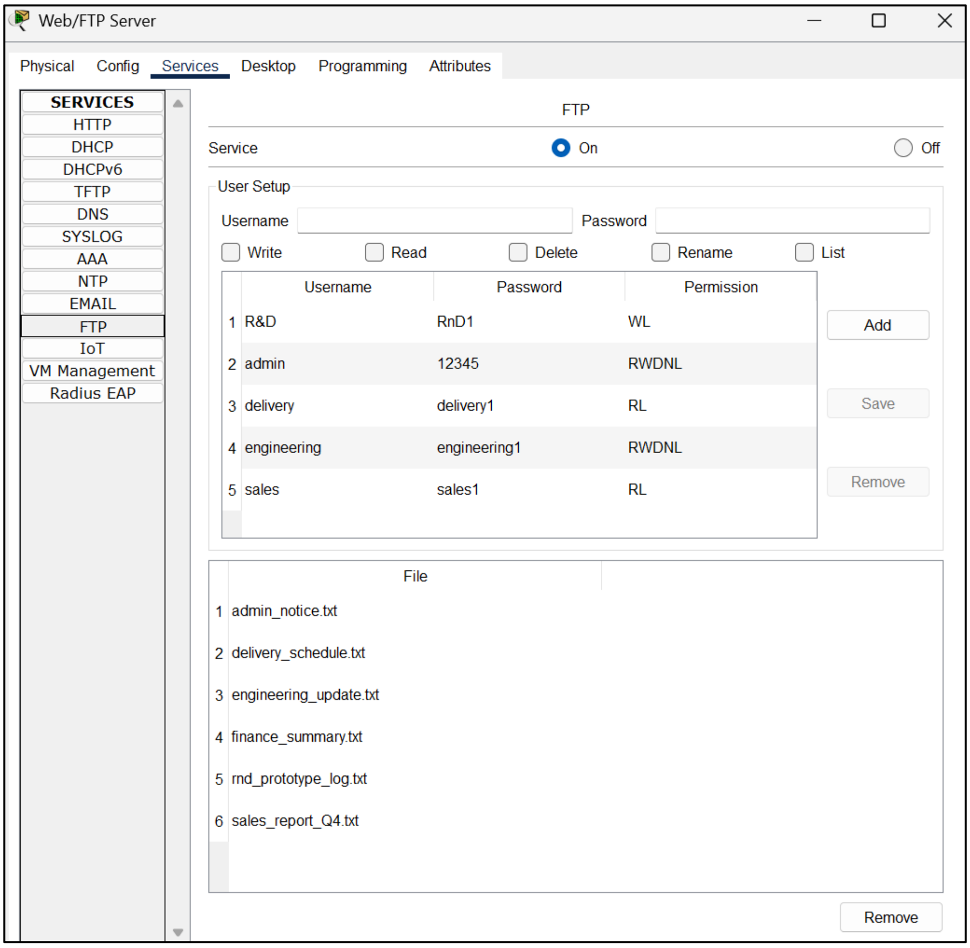
Clients should also be able to put and get files via FTP to the same server. The company requires implementing FTP with user and password is essential for each transaction. (Solution and configuration.)

4.2.2 Solution

The File Transfer Protocol (FTP) functions on the TCP/IP model's application layer to facilitate the transfer of files between servers and clients over TCP ports 20 and 21. On NetSecure Solutions, the FTP service is used to let users from various departments put up files to upload and get files to download from a centralized server.

In order to guarantee secure and proper access, each FTP operation must be authenticated with a correct username and password. This authentication ensures that unapproved individuals cannot read or change files on the server, both protecting data confidentiality as well as integrity. Through the enforcement of user-defined permissions like Read, Write, Delete, Rename, and List, each department can access its own assets safely without compromising the integrity of the network and that of accountability (Stallings, 2017).

4.2.3 Configuration



FTP

Service ● On ○ Off

User Setup

Username Password

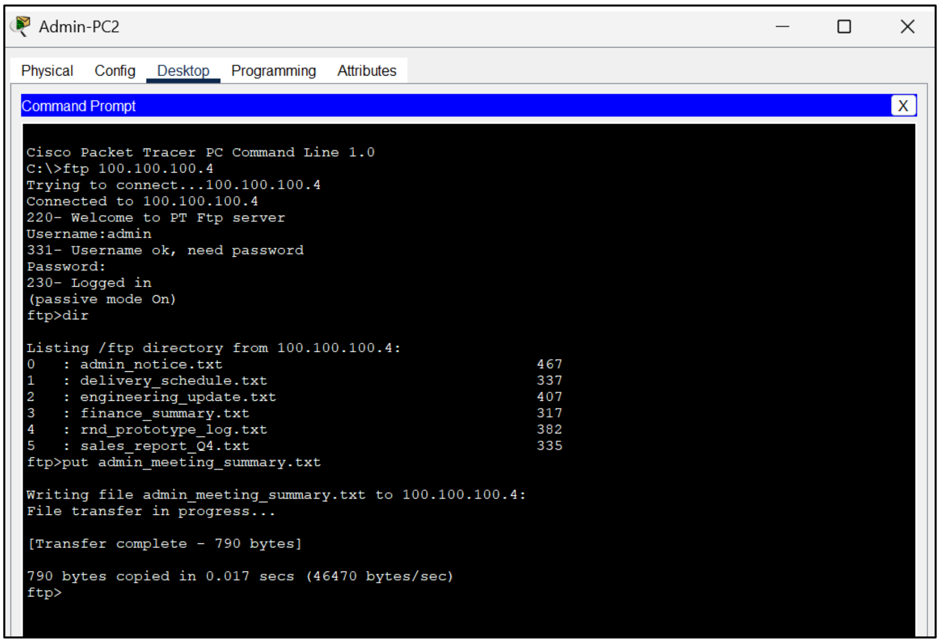
□ Write □ Read □ Delete □ Rename □ List

	Username	Password	Permission
1	R&D	RnD1	WL
2	admin	12345	RWDNL
3	delivery	delivery1	RL
4	engineering	engineering1	RWDNL
5	sales	sales1	RL

	File
1	admin_notice.txt
2	delivery_schedule.txt
3	engineering_update.txt
4	finance_summary.txt
5	rnd_prototype_log.txt
6	sales_report_Q4.txt

Figure 4.2.1 – Web/FTP Server FTP Services

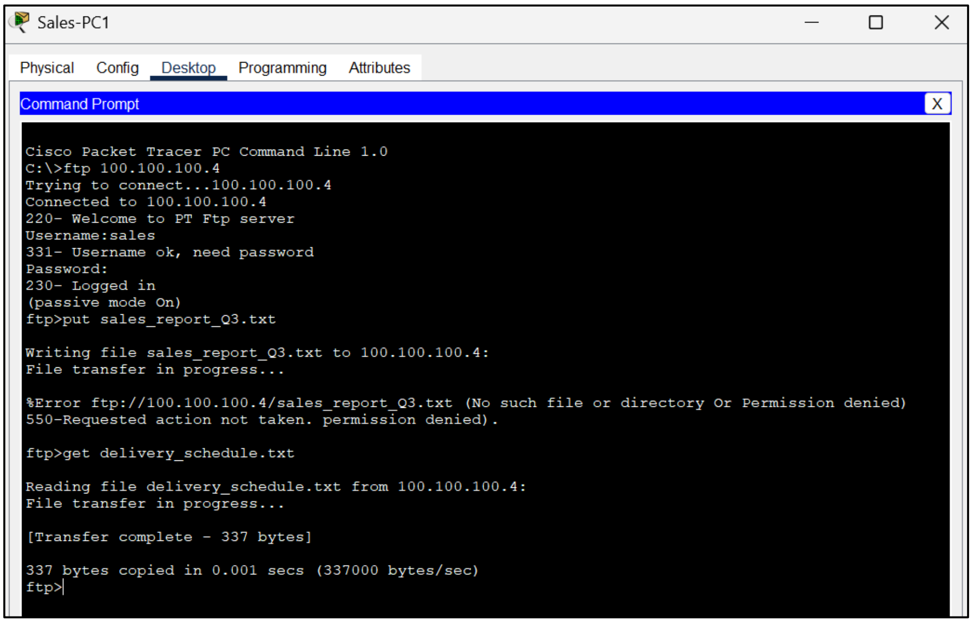
FTP service enabled with department user permissions.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 100.100.100.4
Trying to connect...100.100.100.4
Connected to 100.100.100.4
220- Welcome to PT Ftp server
Username:admin
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>dir

Listing /ftp directory from 100.100.100.4:
0   : admin_notice.txt                                 467
1   : delivery_schedule.txt                            337
2   : engineering_update.txt                           407
3   : finance_summary.txt                              317
4   : rnd_prototype_log.txt                            382
5   : sales_report_Q4.txt                              335
ftp>put admin_meeting_summary.txt

Writing file admin_meeting_summary.txt to 100.100.100.4:
File transfer in progress...

[Transfer complete - 790 bytes]

790 bytes copied in 0.017 secs (46470 bytes/sec)
ftp>
```

Figure 4.2.2 – Admin PC2_List &put (admin)

Admin user successfully authenticates and **puts** (uploads) a file.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 100.100.100.4
Trying to connect...100.100.100.4
Connected to 100.100.100.4
220- Welcome to PT Ftp server
Username:sales
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>put sales_report_Q3.txt

Writing file sales_report_Q3.txt to 100.100.100.4:
File transfer in progress...

%Error ftp://100.100.100.4/sales_report_Q3.txt (No such file or directory Or Permission denied)
550-Requested action not taken. permission denied).

ftp>get delivery_schedule.txt

Reading file delivery_schedule.txt from 100.100.100.4:
File transfer in progress...

[Transfer complete - 337 bytes]

337 bytes copied in 0.001 secs (337000 bytes/sec)
ftp>
```

Figure 4.2.3 – Sales PC1_Put & get(sales)

Sales user **get** succeeds; **put** denied, confirming access control.

4.3 ICMP

4.3.1 Question

All departments in either KL or Singapore networks must be able to access the Internet (to reach both companies location) over ICMP, HTTP and HTTPS with DNS. (Solution and configuration.)

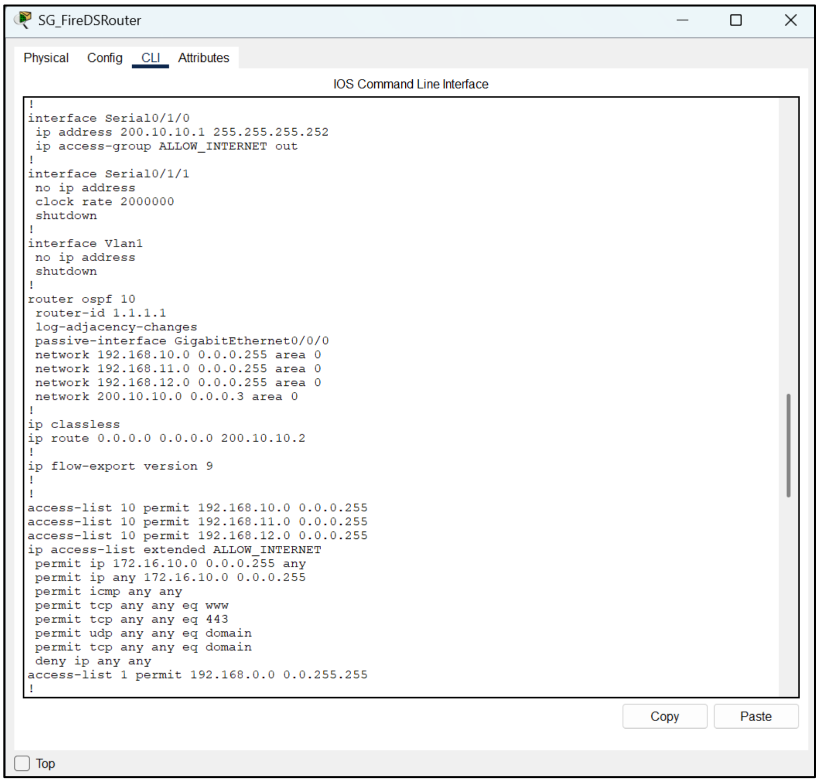
4.3.2 Solution

To ensure that all departments either Kuala Lumpur (KL) network and Singapore (SG) networks are able to access the Internet and communicate between both company sites by using ICMP (ping), HTTP (port 80), HTTPS (port 443), DNS (port 53). This network using static routing and OSPF to enable end-to-end connectivity between the KL and SG network. The Access Control Lists (ACL) is configure on the SG_FireDSRouter to restrict traffic so that the security is maintained.

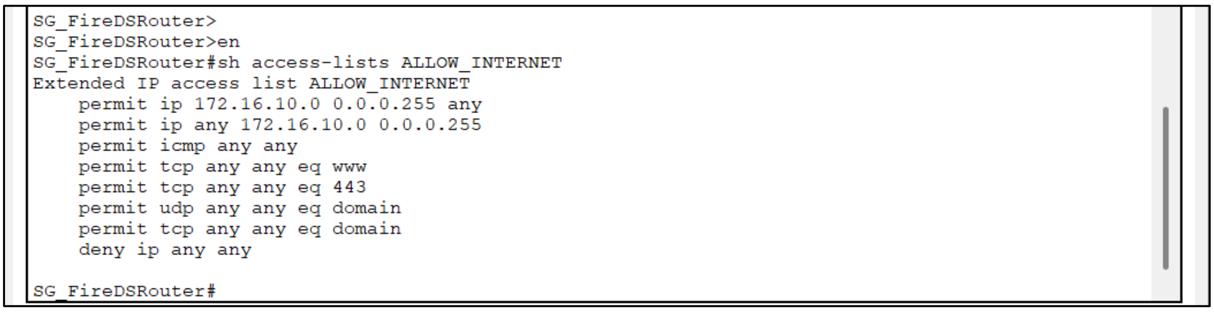
4.3.3 Configuration

(A) SG_FireDSRouter

The ACL named ALLOW_INTERNET controls which protocols and traffic types are allowed to and from the Internet.



```
!
interface Serial0/1/0
 ip address 200.10.10.1 255.255.255.252
 ip access-group ALLOW_INTERNET out
!
interface Serial0/1/1
 no ip address
 clock rate 2000000
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 10
 router-id 1.1.1.1
 log-adjacency-changes
 passive-interface GigabitEthernet0/0/0
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.11.0 0.0.0.255 area 0
 network 192.168.12.0 0.0.0.255 area 0
 network 200.10.10.0 0.0.0.3 area 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 200.10.10.2
!
ip flow-export version 9
!
!
access-list 10 permit 192.168.10.0 0.0.0.255
access-list 10 permit 192.168.11.0 0.0.0.255
access-list 10 permit 192.168.12.0 0.0.0.255
ip access-list extended ALLOW_INTERNET
 permit ip 172.16.10.0 0.0.0.255 any
 permit ip any 172.16.10.0 0.0.0.255
 permit icmp any any
 permit tcp any any eq www
 permit tcp any any eq 443
 permit udp any any eq domain
 permit tcp any any eq domain
 deny ip any any
access-list 1 permit 192.168.0.0 0.0.255.255
!
```



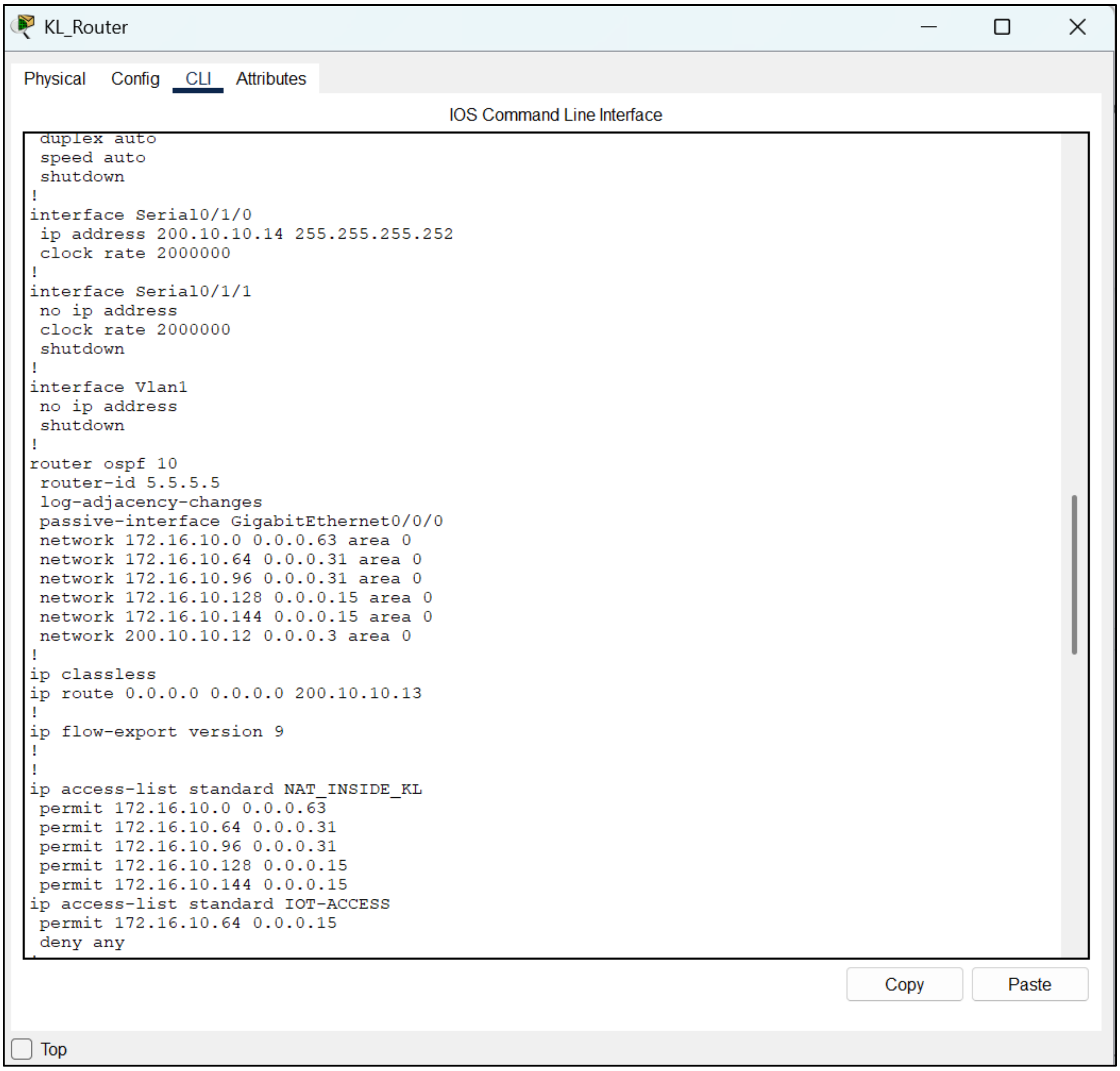
```
SG_FireDSRouter>
SG_FireDSRouter>en
SG_FireDSRouter#sh access-lists ALLOW_INTERNET
Extended IP access list ALLOW_INTERNET
    permit ip 172.16.10.0 0.0.0.255 any
    permit ip any 172.16.10.0 0.0.0.255
    permit icmp any any
    permit tcp any any eq www
    permit tcp any any eq 443
    permit udp any any eq domain
    permit tcp any any eq domain
    deny ip any any

SG_FireDSRouter#
```

Figure 4.3.1

As seen in Figure….., command "permit ip 172.16.10.0 0.0.0.255 any" is allows KL internal network to send packets out. While the "permit ip any 172.16.10.0 0.0.0.255" allows Internet or other sites to reply. Furthermore, command "permit icmp any any" is allows ping. Command "permit tcp any eq www / eq 443" is allows HTTP and HTTPS. The "permit udp/tcp any any eq domain" is allows DNS queries, while the "deny ip any any" is to blocks other unwanted protocols.

(B) KL_Router

KL_Router connects all department VLANs (10-50) to the WAN and advertises them through OSPF.

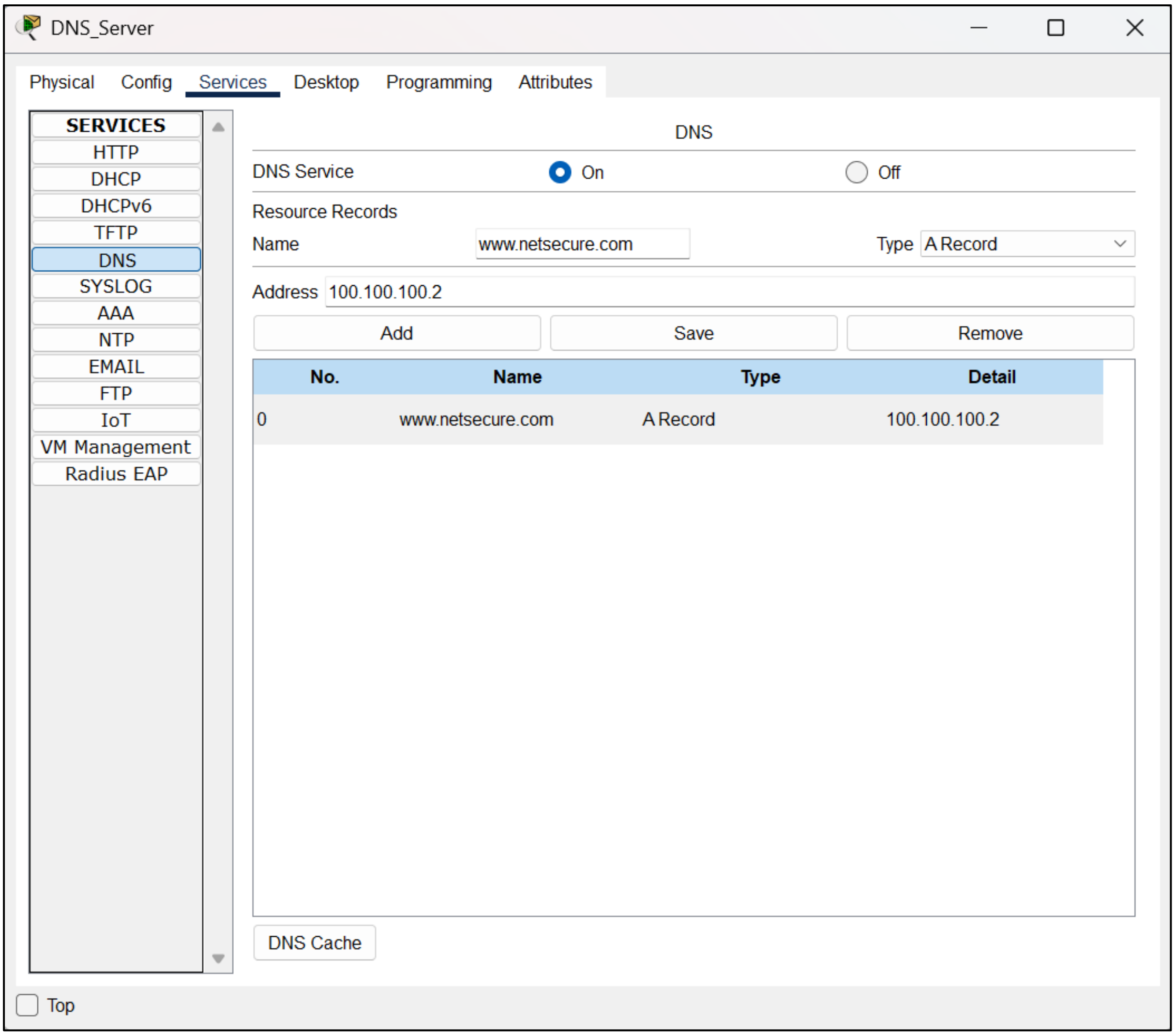


```
 duplex auto
 speed auto
 shutdown
!
interface Serial0/1/0
 ip address 200.10.10.14 255.255.255.252
 clock rate 2000000
!
interface Serial0/1/1
 no ip address
 clock rate 2000000
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 10
 router-id 5.5.5.5
 log-adjacency-changes
 passive-interface GigabitEthernet0/0/0
 network 172.16.10.0 0.0.0.63 area 0
 network 172.16.10.64 0.0.0.31 area 0
 network 172.16.10.96 0.0.0.31 area 0
 network 172.16.10.128 0.0.0.15 area 0
 network 172.16.10.144 0.0.0.15 area 0
 network 200.10.10.12 0.0.0.3 area 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 200.10.10.13
!
ip flow-export version 9
!
!
ip access-list standard NAT_INSIDE_KL
 permit 172.16.10.0 0.0.0.63
 permit 172.16.10.64 0.0.0.31
 permit 172.16.10.96 0.0.0.31
 permit 172.16.10.128 0.0.0.15
 permit 172.16.10.144 0.0.0.15
ip access-list standard IOT-ACCESS
 permit 172.16.10.64 0.0.0.15
 deny any
```

Figure 4.3.2

From the Figure 4.3.2, this advertises KL all internal subnets to OSPF for dynamic routing. The static default route sends all non-local traffic to the WAN via IP 200.10.10.13.

(C) DNS


DNS_Server

DNS

DNS Service ● On ○ Off

Resource Records

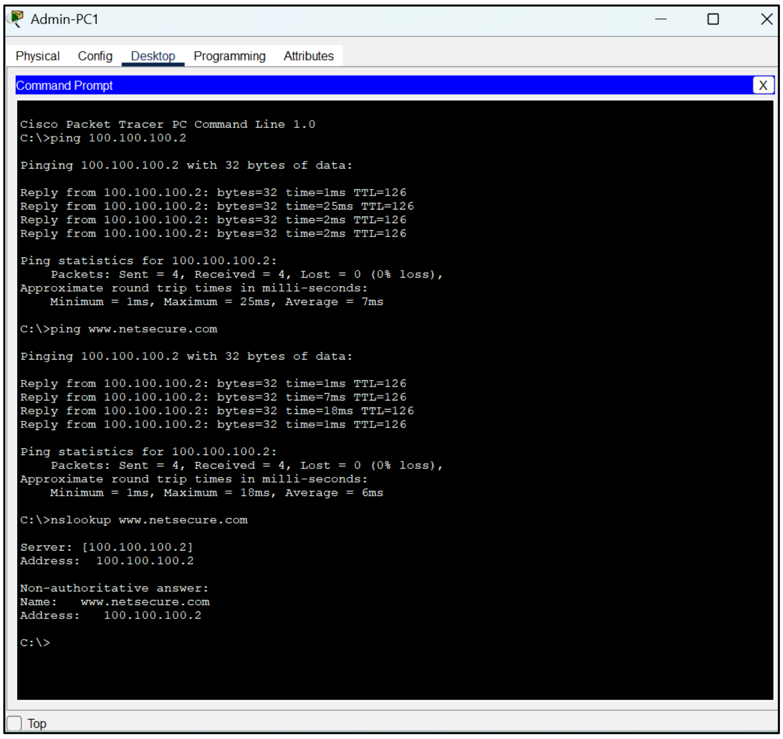
Name www.netsecure.com Type A Record

Address 100.100.100.2

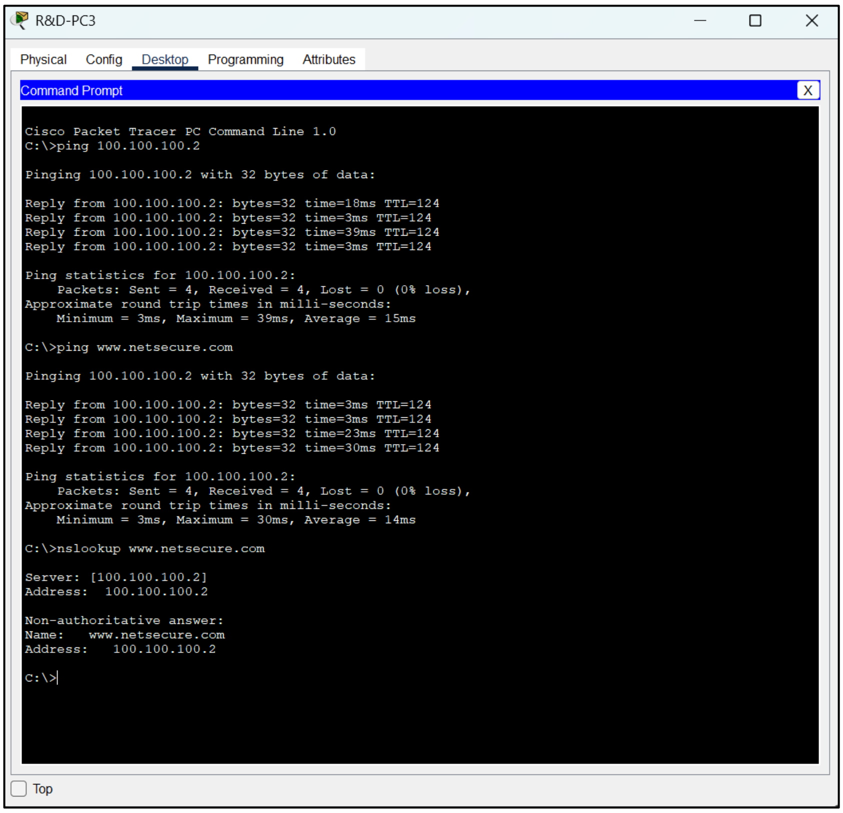
No.	Name	Type	Detail
0	www.netsecure.com	A Record	100.100.100.2

Figure 4.3.3

Added an www.netsecure.com in the DNS_Server



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 100.100.100.2

Pinging 100.100.100.2 with 32 bytes of data:

Reply from 100.100.100.2: bytes=32 time=1ms TTL=126
Reply from 100.100.100.2: bytes=32 time=25ms TTL=126
Reply from 100.100.100.2: bytes=32 time=2ms TTL=126
Reply from 100.100.100.2: bytes=32 time=2ms TTL=126

Ping statistics for 100.100.100.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 25ms, Average = 7ms

C:\>ping www.netsecure.com

Pinging 100.100.100.2 with 32 bytes of data:

Reply from 100.100.100.2: bytes=32 time=1ms TTL=126
Reply from 100.100.100.2: bytes=32 time=7ms TTL=126
Reply from 100.100.100.2: bytes=32 time=18ms TTL=126
Reply from 100.100.100.2: bytes=32 time=1ms TTL=126

Ping statistics for 100.100.100.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 18ms, Average = 6ms

C:\>nslookup www.netsecure.com

Server: [100.100.100.2]
Address:  100.100.100.2

Non-authoritative answer:
Name:   www.netsecure.com
Address:   100.100.100.2

C:\>
```



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 100.100.100.2

Pinging 100.100.100.2 with 32 bytes of data:

Reply from 100.100.100.2: bytes=32 time=18ms TTL=124
Reply from 100.100.100.2: bytes=32 time=3ms TTL=124
Reply from 100.100.100.2: bytes=32 time=39ms TTL=124
Reply from 100.100.100.2: bytes=32 time=3ms TTL=124

Ping statistics for 100.100.100.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 39ms, Average = 15ms

C:\>ping www.netsecure.com

Pinging 100.100.100.2 with 32 bytes of data:

Reply from 100.100.100.2: bytes=32 time=3ms TTL=124
Reply from 100.100.100.2: bytes=32 time=3ms TTL=124
Reply from 100.100.100.2: bytes=32 time=23ms TTL=124
Reply from 100.100.100.2: bytes=32 time=30ms TTL=124

Ping statistics for 100.100.100.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 30ms, Average = 14ms

C:\>nslookup www.netsecure.com

Server: [100.100.100.2]
Address:  100.100.100.2

Non-authoritative answer:
Name:   www.netsecure.com
Address:   100.100.100.2

C:\>
```

Figure 4.3.4

From KL network Admin-PC1 and SG network R&D-PC3 can ping to DNS_Server, means that KL and SG clients are able to access the Internet over ICMP, HTTP and HTTPS with DNS.

4.4 Email

4.4.1 Question

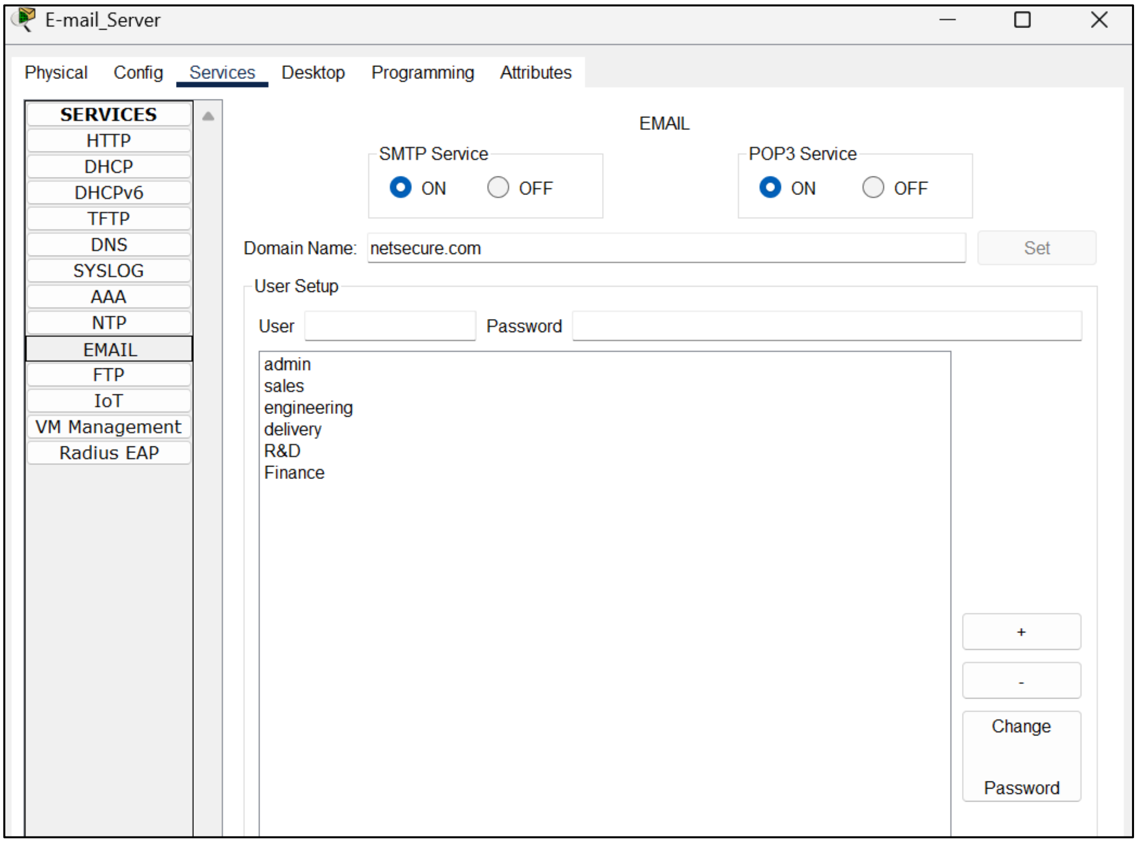
Client workstations must be able to check their e-mail on the e-mail server at the DMZ. The e-mail server should be able to receive e-mail from external hosts over the simple mail transfer protocol (SMTP). The email transaction also needs to be secured. (Solution and configuration.)

4.4.2 Solution

Electronic mail (E-mail) is the foremost communication service that must be protected to prevent data breaches as well as unauthorised access. Under this setup, NetSecure Solutions configures an email server in the Demilitarized Zone (DMZ), a managed barrier between internal networks as well as the external world. The email server receives incoming mail from outside hosts with the assistance of Simple Mail Transfer Protocol (SMTP, port 25) and internal users download mail with the assistance of Post Office Protocol (POP3, port 110) or Internet Message Access Protocol (IMAP, port 143).

Each user must be authenticated with a strong password and username before they can send or retrieve mail, therefore making the access control secure. On real networks, encryption protocols such as SSL/TLS (SMTPS 465, POP3S 995) are also implemented to prevent the interception of authentication information as well as the contents of the email. This makes all the email transactions within NetSecure Solutions private, authenticated, and secure (Stallings, 2017).

4.4.3 Configuration



SMTP Service ● ON ○ OFF

POP3 Service ● ON ○ OFF

Domain Name: netsecure.com

User Setup

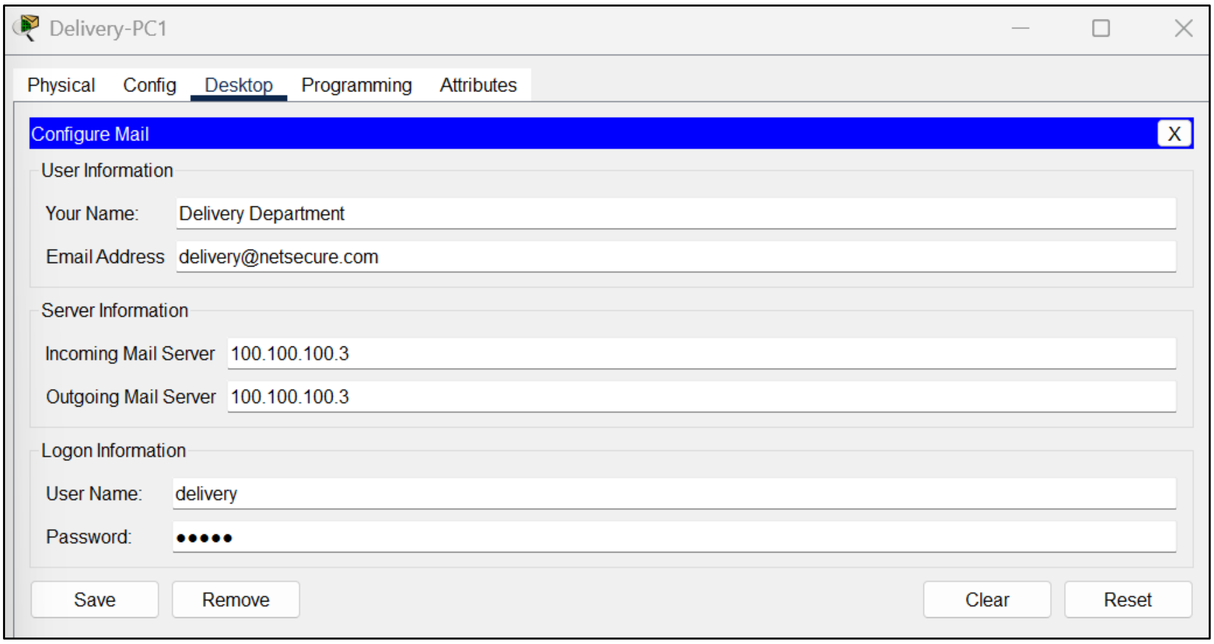
User

Password

admin
sales
engineering
delivery
R&D
Finance

Figure 4.4.1 – Email Server's USERLIST

Email server enabled with SMTP/POP3 services and department user accounts.



User Information

Your Name: Delivery Department

Email Address delivery@netsecure.com

Server Information

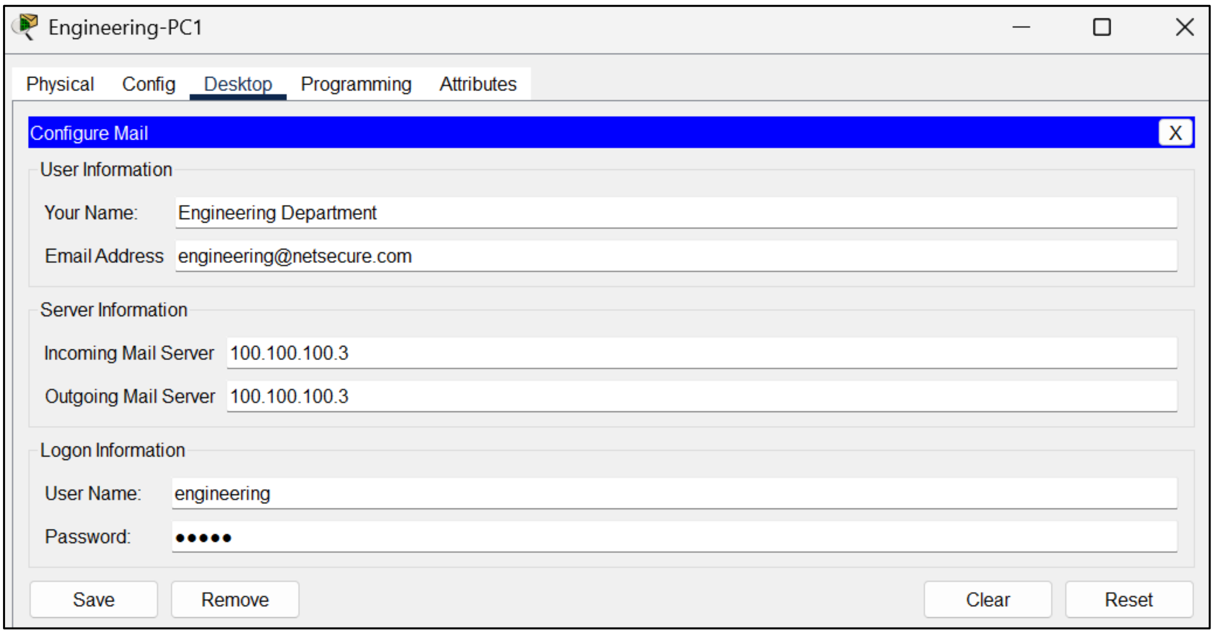
Incoming Mail Server 100.100.100.3

Outgoing Mail Server 100.100.100.3

Logon Information

User Name: delivery

Password: •••••



User Information

Your Name: Engineering Department

Email Address engineering@netsecure.com

Server Information

Incoming Mail Server 100.100.100.3

Outgoing Mail Server 100.100.100.3

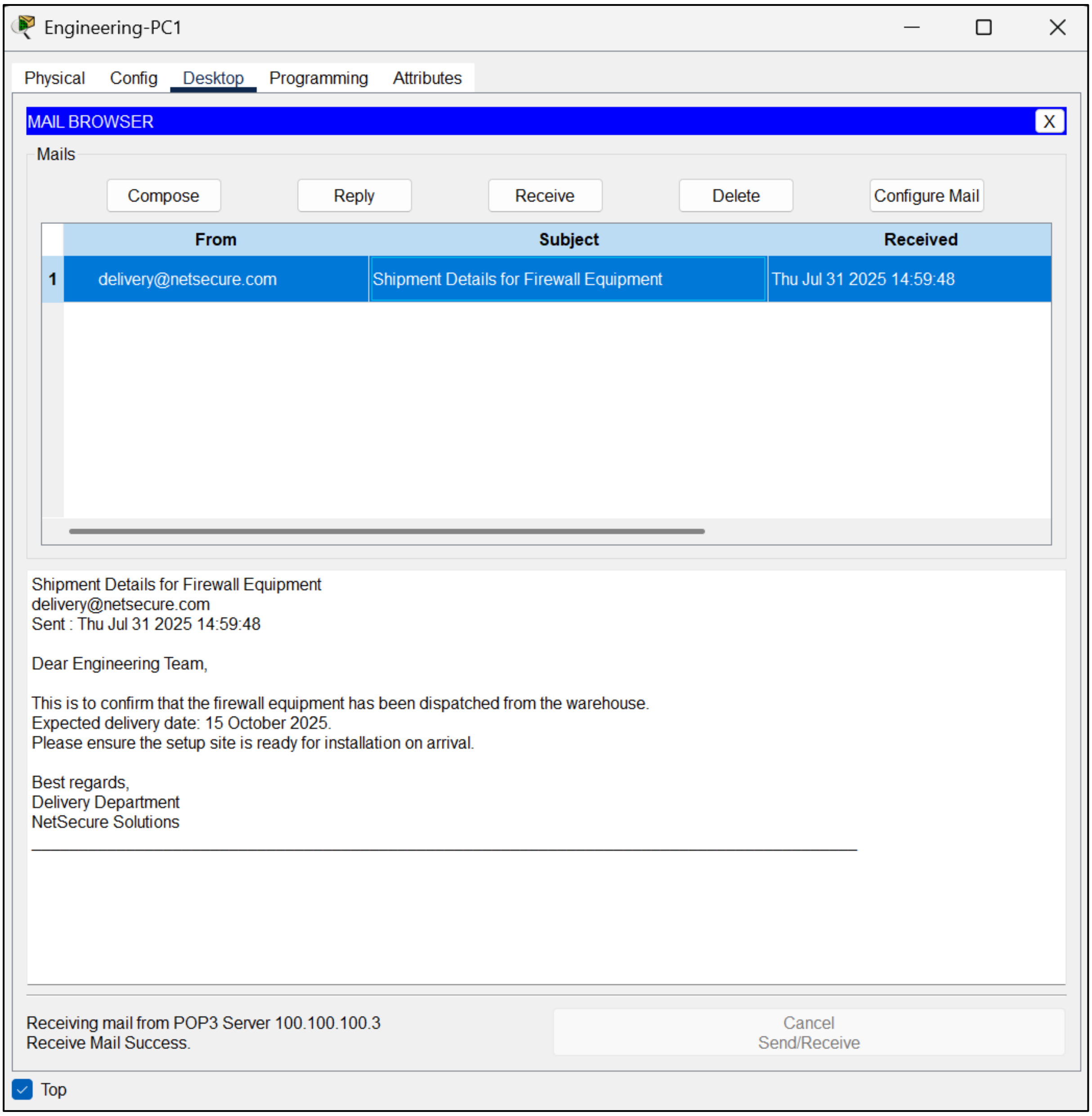
Logon Information

User Name: engineering

Password: •••••

Figure 4.4.2 & 4.4.3 – Delivery_PC1 & Engineering_PC1 User configuration

Client PCs configured with mail settings for the DMZ email server.



	From	Subject	Received
1	delivery@netsecure.com	Shipment Details for Firewall Equipment	Thu Jul 31 2025 14:59:48

Shipment Details for Firewall Equipment
delivery@netsecure.com
Sent : Thu Jul 31 2025 14:59:48

Dear Engineering Team,

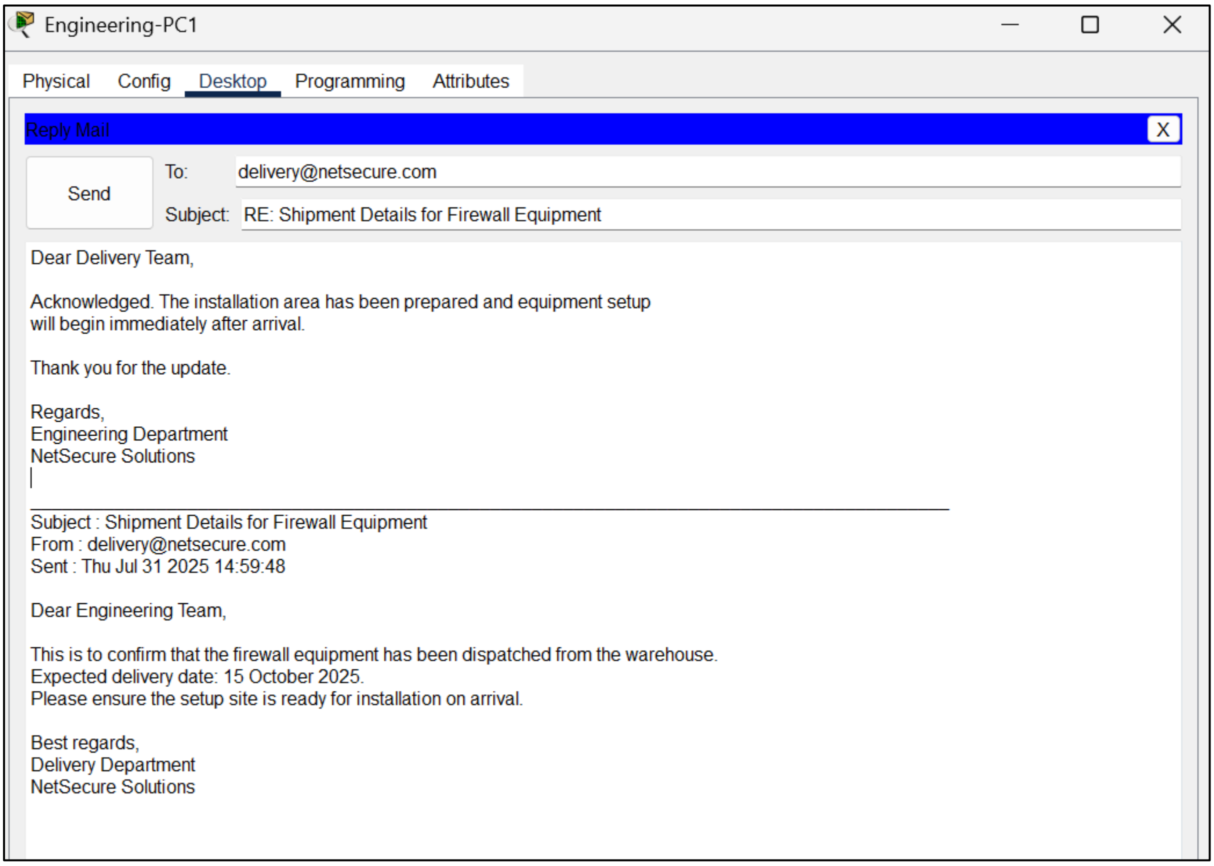
This is to confirm that the firewall equipment has been dispatched from the warehouse.
Expected delivery date: 15 October 2025.
Please ensure the setup site is ready for installation on arrival.

Best regards,
Delivery Department
NetSecure Solutions

Receiving mail from POP3 Server 100.100.100.3
Receive Mail Success.

Figure 4.4.4 – Engineering PC1 Mail Browser Page

Successful email reception on Engineering-PC1 using the Email server.



To: delivery@netsecure.com

Subject: RE: Shipment Details for Firewall Equipment

Dear Delivery Team,

Acknowledged. The installation area has been prepared and equipment setup
will begin immediately after arrival.

Thank you for the update.

Regards,
Engineering Department
NetSecure Solutions

Subject : Shipment Details for Firewall Equipment
From : delivery@netsecure.com
Sent : Thu Jul 31 2025 14:59:48

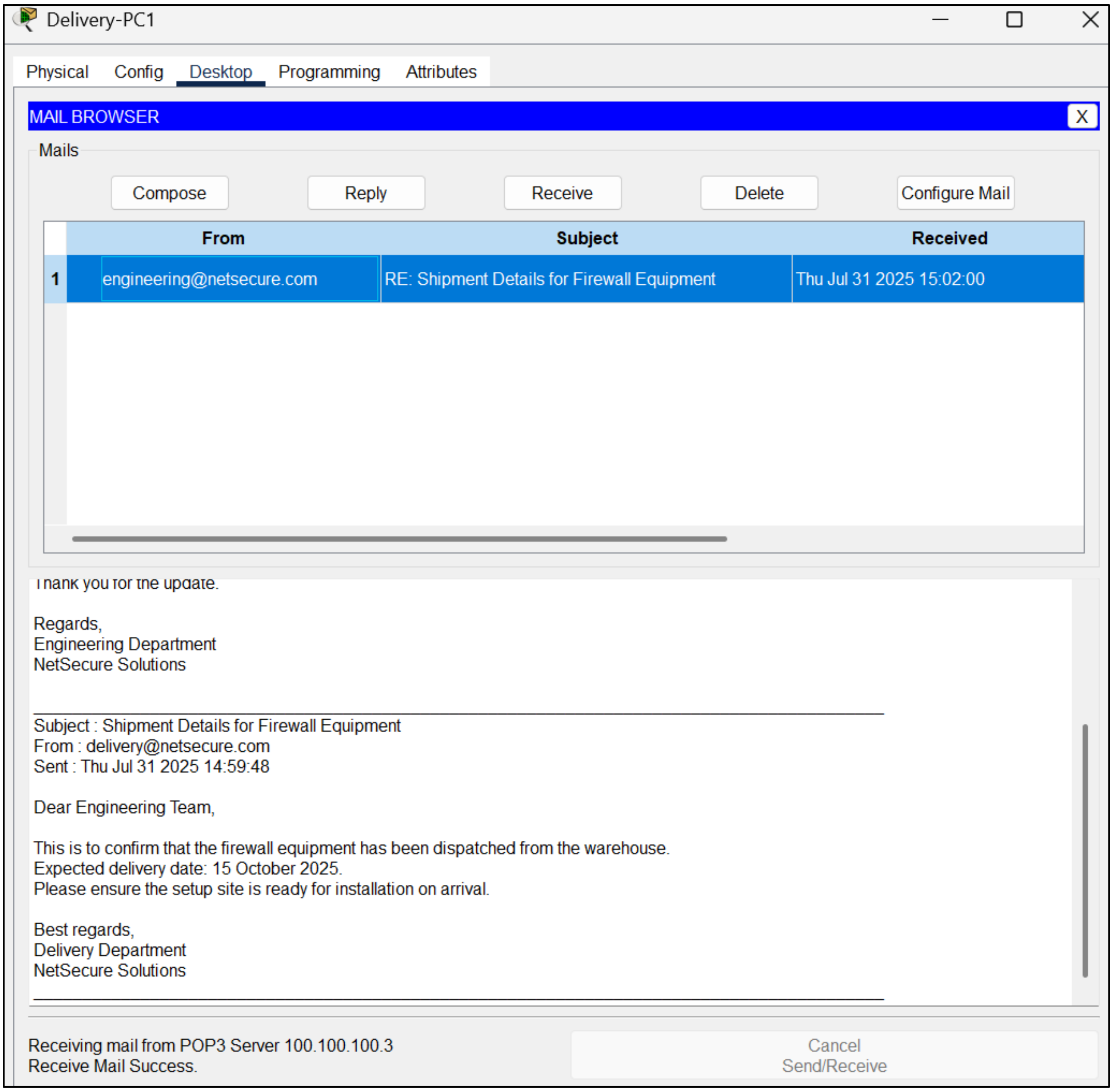
Dear Engineering Team,

This is to confirm that the firewall equipment has been dispatched from the warehouse.
Expected delivery date: 15 October 2025.
Please ensure the setup site is ready for installation on arrival.

Best regards,
Delivery Department
NetSecure Solutions

Figure 4.4.4 – Engineering PC1 Reply Mail Page

Engineering-PC1 composes a reply message for the Delivery Department.



	From	Subject	Received
1	engineering@netsecure.com	RE: Shipment Details for Firewall Equipment	Thu Jul 31 2025 15:02:00

Thank you for the update.

Regards,
Engineering Department
NetSecure Solutions

Subject : Shipment Details for Firewall Equipment
From : delivery@netsecure.com
Sent : Thu Jul 31 2025 14:59:48

Dear Engineering Team,

This is to confirm that the firewall equipment has been dispatched from the warehouse.
Expected delivery date: 15 October 2025.
Please ensure the setup site is ready for installation on arrival.

Best regards,
Delivery Department
NetSecure Solutions

Receiving mail from POP3 Server 100.100.100.3
Receive Mail Success.

Figure 4.4.5 – Delivery PC1 Mail Browser Page

Successful reception of the reply message on Delivery-PC1.

4.5. IoT Server

4.5.1 Question

IoT devices to be deployed in KL network using wireless connection. All the devices need to be connected to the IoT server. Identify **THREE** types of attacks and proposed mitigation techniques against these attacks while ensuring secure communication with the IoT server. (Solution and configuration.)

4.5.2 Solutions

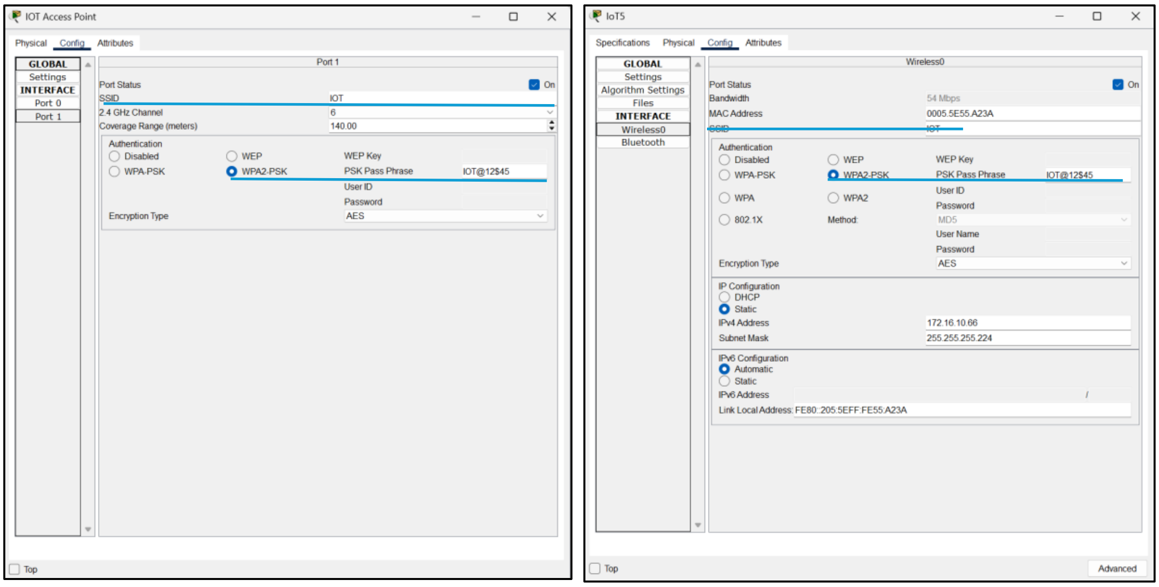
Three types of attacks and proposed mitigation techniques against these attacks while ensuring secure communication with the IoT server are shown below:

The first type of attack is Wi-Fi Eavesdropping. The attackers may interrupt unencrypted wireless communications between IoT devices and access points to obtain sensitive information or credentials. To mitigate this, the IoT access point should enable WPA2-PSK authentication to let only the correct SSID (IOT) and pre-shared key (IOT@12$45) devices connect to the access point. This ensures the communications between IoT devices and IoT server are encrypted and prevents from unauthorized interceptions.

The second type of attacks is Man-in-the-Middle (MitM) Attack. The attackers can secretly forward and alter the communications between IoT devices and servers. To mitigate this, Transport Layer Security (TLS) should be configured in the IoT device and enable certificate pinning. Also, the device software should be programmed to only accept specific and known certificates from legitimate IoT servers. This solution ensures the integrity of communication channel and prevents attackers.

The third type of attacks is device spoofing. The attackers will act itself as legitimate to authorized IoT devices to send malicious or false commands to the IoT server. To mitigate this, IoT device should be assigned a unique X.509 client certificate during manufacturing. Then, the IoT device should be configured with mutual TLS (mTLS) authentication. This ensures the serve only accepts authorized device connections and block unauthorized devices from network.

4.5.3 Configuration



Port 1

Port Status ☑ On
SSID IOT
2.4 GHz Channel 6
Coverage Range (meters) 140.00

Authentication
○ Disabled ○ WEP WEP Key
○ WPA-PSK ● WPA2-PSK PSK Pass Phrase IOT@12$45
User ID
Password
Encryption Type AES

Wireless0

Port Status ☑ On
Bandwidth 54 Mbps
MAC Address 0005.5E55.A23A
SSID IOT

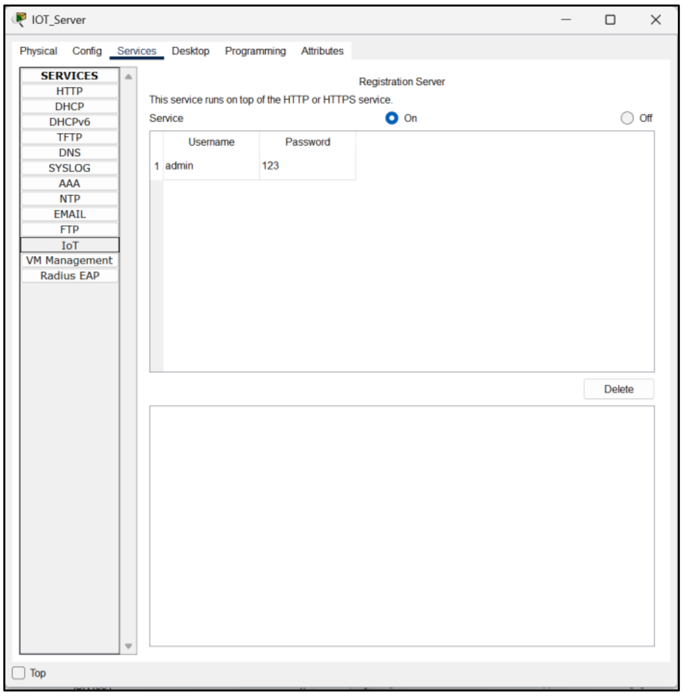
Authentication
○ Disabled ○ WEP WEP Key
○ WPA-PSK ● WPA2-PSK PSK Pass Phrase IOT@12$45
User ID
○ WPA ○ WPA2 Password
○ 802.1X Method: MD5
User Name
Password
Encryption Type AES

IP Configuration
○ DHCP
● Static
IPv4 Address 172.16.10.66
Subnet Mask 255.255.255.224

IPv6 Configuration
● Automatic
○ Static
IPv6 Address /
Link Local Address: FE80::205:5EFF:FE55:A23A

Figure 4.5.3.1: Connecting IoT device wirelessly to the IoT access point with WPA2-PSK

The IoT device is connected wirelessly to the IoT access point with the same SSID and WPA2-PSK Pass Phrase Configured.



Registration Server

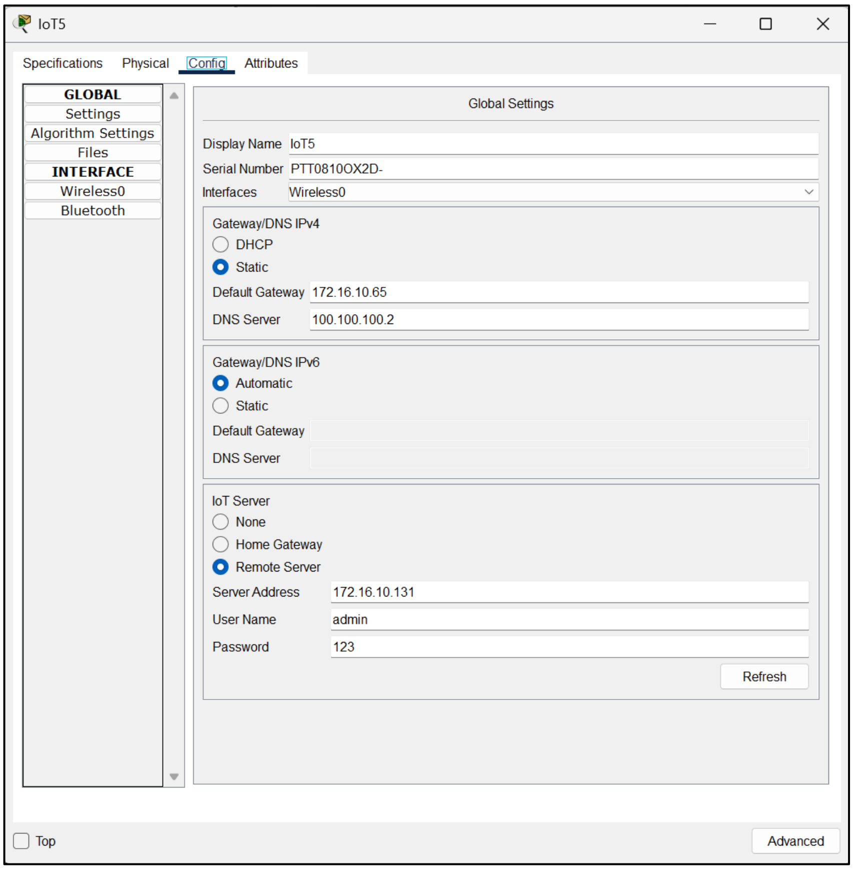
This service runs on top of the HTTP or HTTPS service.

Service ● On ○ Off

	Username	Password
1	admin	123

Figure 4.5.3.2: IoT Server configuration

The IoT services is enabled in the IoT server with user created name admin.



Global Settings

Display Name IoT5

Serial Number PTT0810OX2D-

Interfaces Wireless0

Gateway/DNS IPv4

○ DHCP

● Static

Default Gateway 172.16.10.65

DNS Server 100.100.100.2

Gateway/DNS IPv6

● Automatic

○ Static

Default Gateway

DNS Server

IoT Server

○ None

○ Home Gateway

● Remote Server

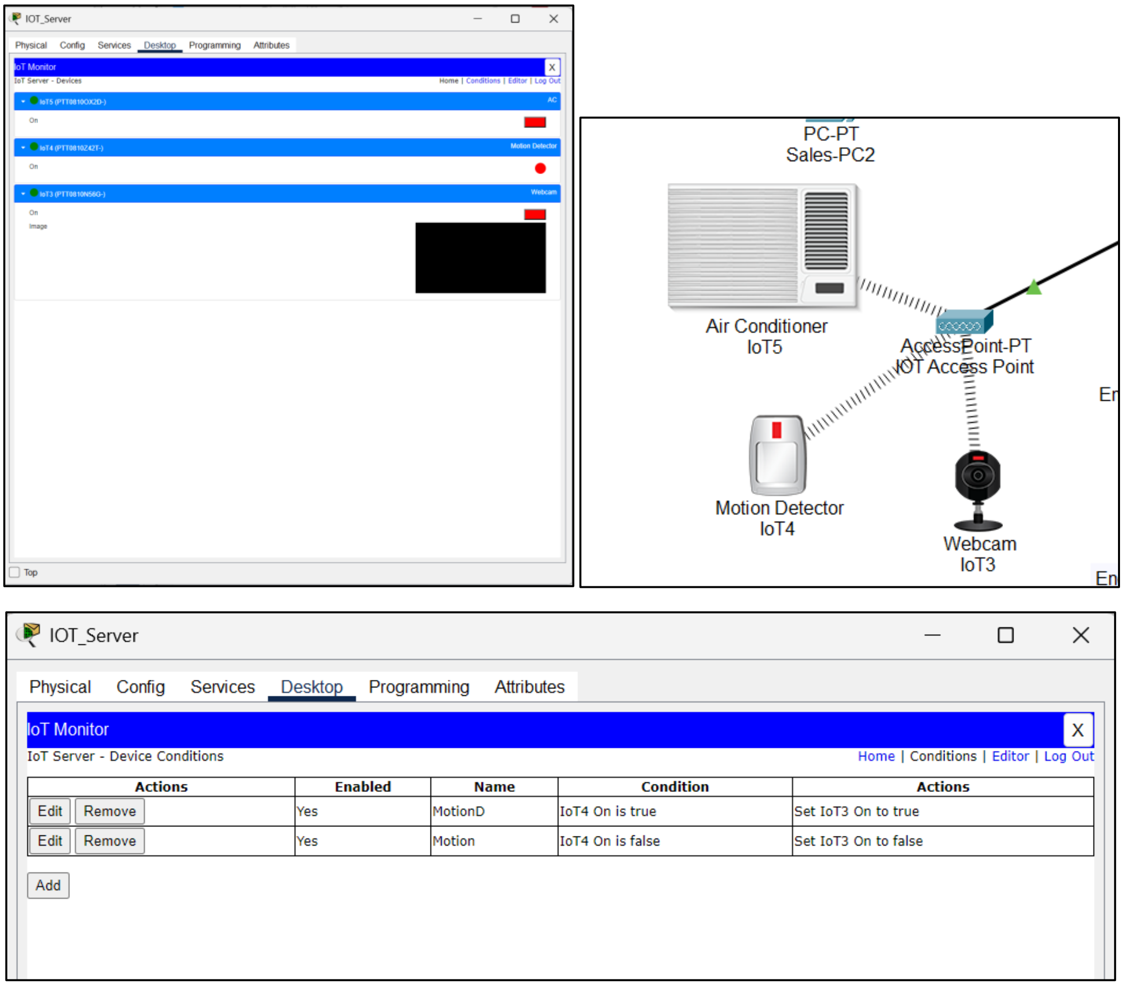
Server Address 172.16.10.131

User Name admin

Password 123

Figure 4.5.3.3: Connecting IoT Device to IoT Server

By entering the same address, username and password that configured in the IoT server, the IoT device is able to connect to the IoT server.



IOT_Server

Physical Config Services Desktop Programming Attributes

IoT Monitor

IoT Server - Devices Home | Conditions | Editor | Log Out

IoT5 (PTT0810OX2D-) AC

On

IoT4 (PTT0810Z42T-) Motion Detector

On

IoT3 (PTT0810N56G-) Webcam

On

Image

IOT_Server

Physical Config Services Desktop Programming Attributes

IoT Monitor

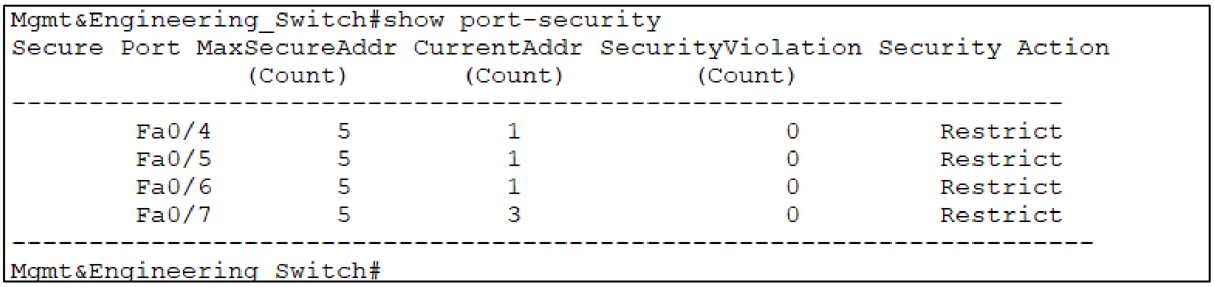
IoT Server - Device Conditions Home | Conditions | Editor | Log Out

Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	MotionD	IoT4 On is true	Set IoT3 On to true
Edit Remove	Yes	Motion	IoT4 On is false	Set IoT3 On to false

Add

Figure 4.5.3.4 : IoT Monitor homepage and IoT conditions

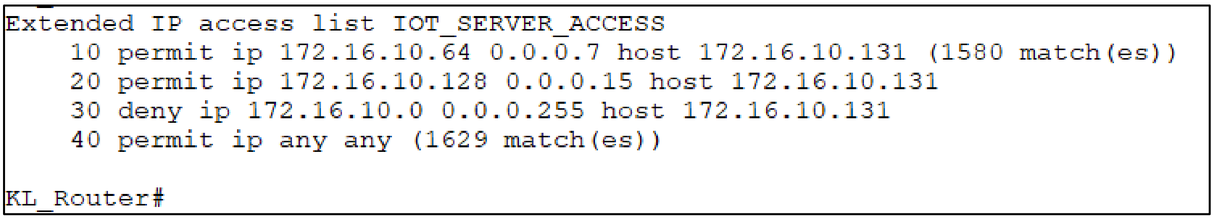
After logging in IoT Monitor with valid credenentials, the homepage shows all 3 IoT devices has successfully connected to the IoT server. An automation condition is then added — when the motion detector senses movement, the webcam will automatically activate to start recording.This setup ensures real-time monitoring and enhances security within the IoT environment.



```
Mgmt&Engineering_Switch#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)          (Count)
--------------------------------------------------------------------
        Fa0/4          5          1                 0         Restrict
        Fa0/5          5          1                 0         Restrict
        Fa0/6          5          1                 0         Restrict
        Fa0/7          5          3                 0         Restrict
----------------------------------------------------------------------
Mgmt&Engineering_Switch#
```

Figure 4.5.3.5(Extra Security features): Port security on Engineering vlan (vlan 20)

A port security is implemented to protect VLAN 20 from MAC flooding.



```
Extended IP access list IOT_SERVER_ACCESS
    10 permit ip 172.16.10.64 0.0.0.7 host 172.16.10.131 (1580 match(es))
    20 permit ip 172.16.10.128 0.0.0.15 host 172.16.10.131
    30 deny ip 172.16.10.0 0.0.0.255 host 172.16.10.131
    40 permit ip any any (1629 match(es))

KL_Router#
```

Figure 4.5.3.6(Extra Security features): Extended ACL to access IoT Server

An extended ACL limits which department, or which devices could access the IoT servers.

4.6 Wireless Security

4.6.1 Question

In addition to wired connections, wireless connections play a vital role in today's network deployments. Configure wireless connection to the topology above. Discuss **THREE** types of attacks on wireless network and proposed mitigation techniques against these attacks. (Solution and configuration.)

4.6.2 Solution

- **Rogue / Evil Twin AP**: Attacker clones the SSID to lure clients and intercept traffic. Mitigation: prefer WPA2/WPA3-Enterprise (802.1X) and enable rogue AP detection / WIDS to locate and remove unauthorized APs (Souppaya & Scarfone, 2012).
- **Deauthentication / Disassociation Attack**: Spoofed management frames disconnect clients to capture handshakes or cause DoS. Mitigation: enable Protected Management Frames (802.11w/PMF) to protect deauth/disassoc frames (Notter, 2018).
- **Eavesdropping / Handshake Capture & Key-Cracking**: Over-the-air packets/handshakes are captured for offline cracking attempts. Mitigation: enforce WPA2-AES or WPA3 only (no WEP/open), use strong non-dictionary PSKs with periodic rotation, and add VPN for sensitive traffic (Souppaya & Scarfone, 2012).

4.6.3 Configuration

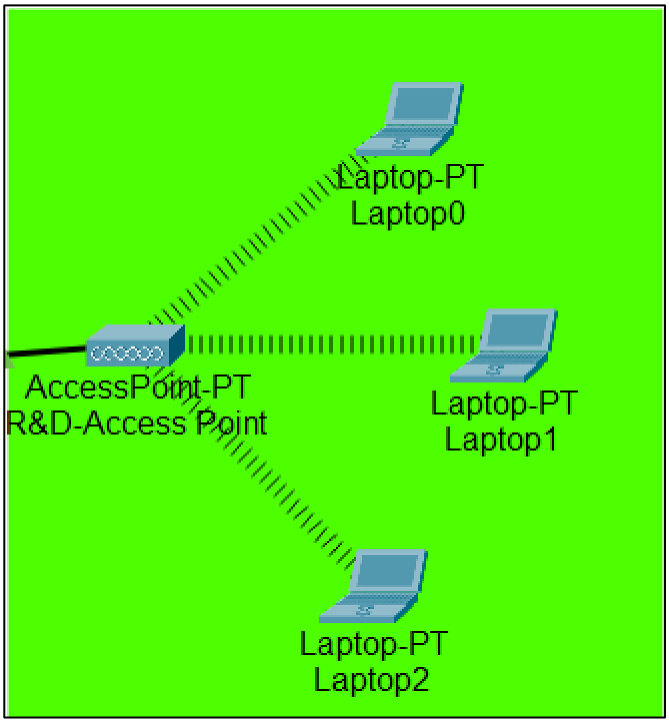
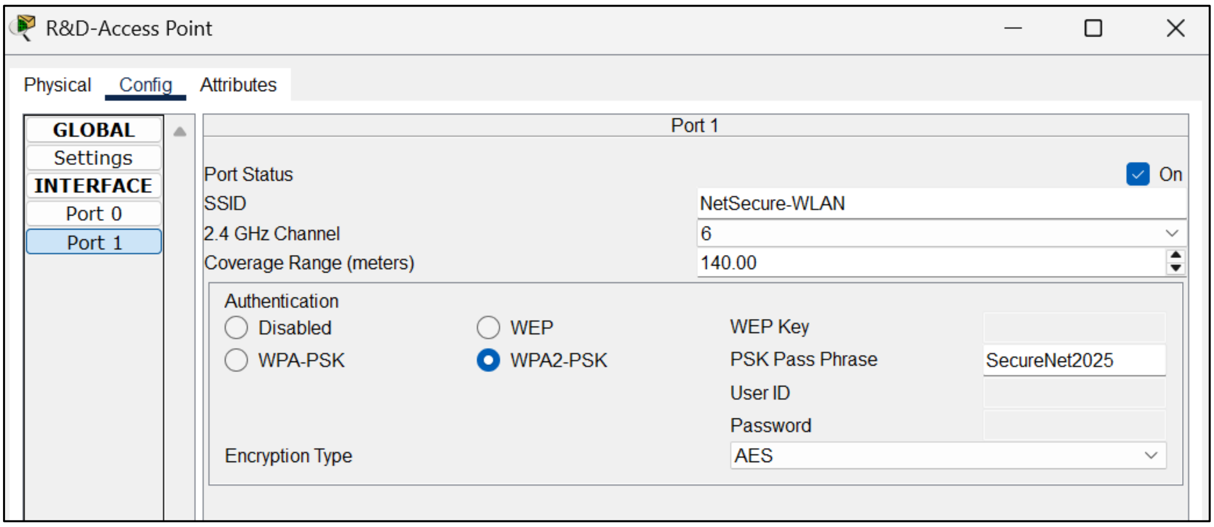


Figure 4.6.1- R&D Workstation



Port 1

Port Status ☑ On

SSID: NetSecure-WLAN

2.4 GHz Channel: 6

Coverage Range (meters): 140.00

Authentication

○ Disabled ○ WEP

○ WPA-PSK ● WPA2-PSK

WEP Key:

PSK Pass Phrase: SecureNet2025

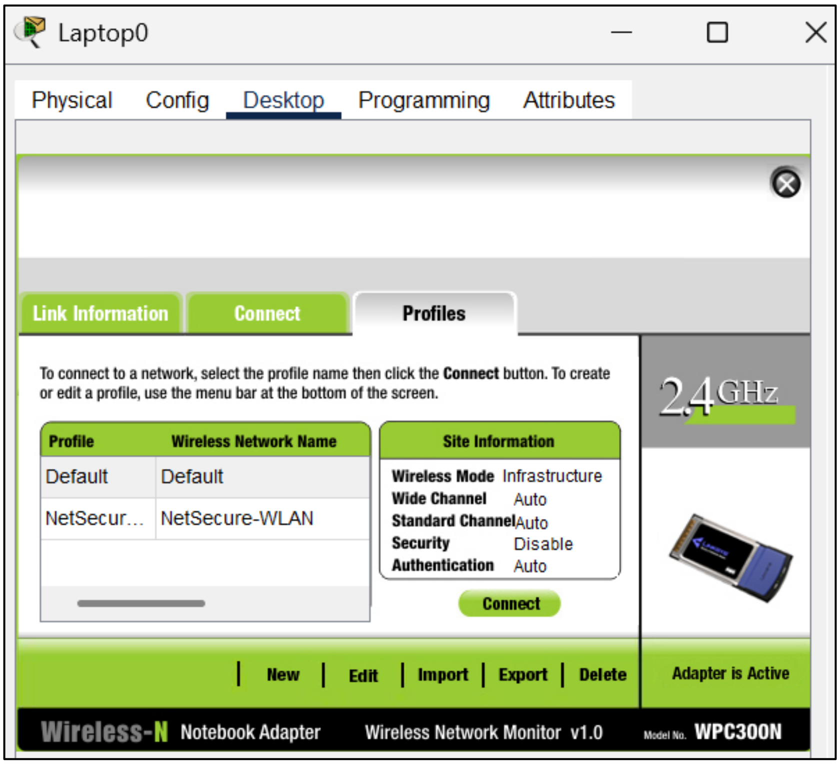
User ID:

Password:

Encryption Type: AES

Figure 4.6.2 - R&D_Access Configuration Page

SSID NetSecure-WLAN on channel 6 with coverage 140 m. Security set to WPA2-PSK (passphrase SecureNet2025) and AES encryption to protect over-the-air traffic.



To connect to a network, select the profile name then click the **Connect** button. To create or edit a profile, use the menu bar at the bottom of the screen.

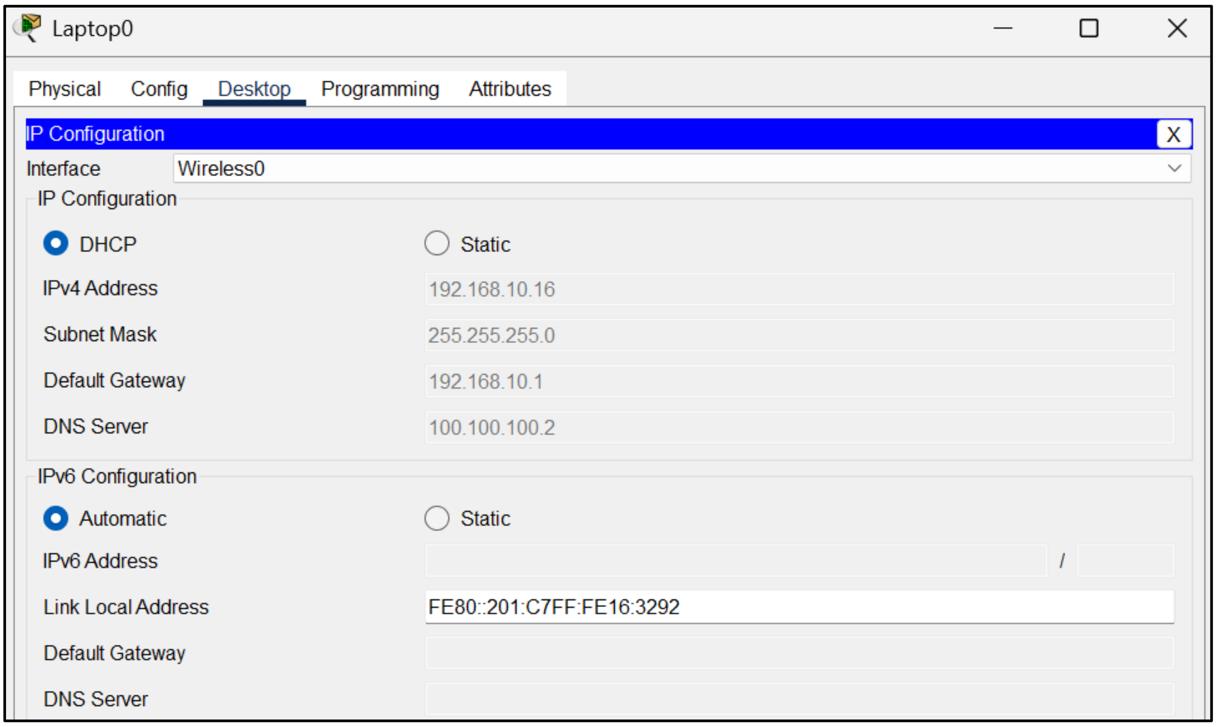
Profile	Wireless Network Name
Default	Default
NetSecur…	NetSecure-WLAN

Site Information

Wireless Mode Infrastructure
Wide Channel Auto
Standard Channel Auto
Security Disable
Authentication Auto

Figure 4.6.3 – Laptop Wireless Page

A profile for NetSecure-WLAN is created in Infrastructure mode. Clicking Connect prompts for the WPA2-PSK key to join the secured SSID.



Interface: Wireless0

IP Configuration

● DHCP ○ Static

IPv4 Address: 192.168.10.16

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.10.1

DNS Server: 100.100.100.2

IPv6 Configuration

● Automatic ○ Static

IPv6 Address: /

Link Local Address: FE80::201:C7FF:FE16:3292

Default Gateway:

DNS Server:

Figure 4.6.4 – Laptop's IP Configuration Page

Successfully connected to the DHCP.

4.7. DHCPv4

4.7.1 Question

Configure DHCPv4 or DHCPv6 in both networks. While DHCP provides considerable advantages in automation and management, it also poses challenges concerning security and reliability that need to be addressed for successful deployment. Discuss the details of DHCP deployment, highlighting the benefits and challenges associated with it. (Solution and configuration.)

4.7.2 Solution

In this task, the team successfully deployed DHCPv4 (Dynamic Host Configuration Protocol) in the two network branches of Singapore and Kuala Lumpur. This protocol is used to automatically assign IP addresses, gateways and DNS servers to clients (PCs), thereby reducing manual configuration errors and improving network management efficiency.

Routers (SG_FireDSRouter and KL_Router) are configured as DHCP servers for their respective branch networks, providing automatic IP allocation for each VLAN through different address pools. Meanwhile, IoT devices and servers were assigned static IP configurations to ensure that the devices maintain a fixed address in the network and enhance connection stability.

This hybrid DHCP deployment design enables the automated management of dynamic devices while also ensuring the reliability of IoT devices and servers.

4.7.2.1 Advantages of DHCP

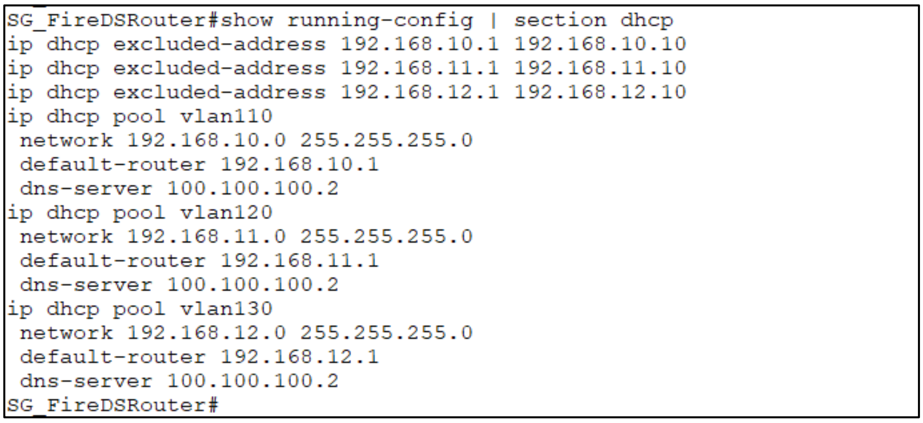
- Automated management: Automatically assigns IP addresses, significantly reducing the time and error rate of manual configuration.
- Centralized control: The router acts as the central DHCP server and can manage IP allocation across multiple VLANs simultaneously.
- Flexible expansion: When adding a new subnet or department, only a new DHCP pool needs to be added, without the need to configure each device one by one.
- Consistency and reliability: All hosts receive unified gateway and DNS parameters to ensure stable connections.

4.7.2.2 Challenges and Security Issues of DHCP Deployment

- Forged DHCP server (DHCP Snooping attack risk) : Malicious devices may act as fake DHCP servers, leading to IP conflicts or traffic hijacking.
- Single point of failure risk: If the DHCP service on the router fails, all dynamic clients will be unable to obtain IP addresses.
- Lease Time issue: An unreasonable lease duration may result in the address pool being filled up or allocation being delayed.
- High maintenance burden for static devices: IoT devices need to be manually configured, increasing the management workload.

Overall, DHCP brings significant benefits in terms of efficiency improvement, but it simultaneously also brings some security issues and challenges for us. To mitigate the impact brought by DHCP, there is a series of mitigation measures such as DHCP snooping, port security and backup static configuration that can reduce these risks.

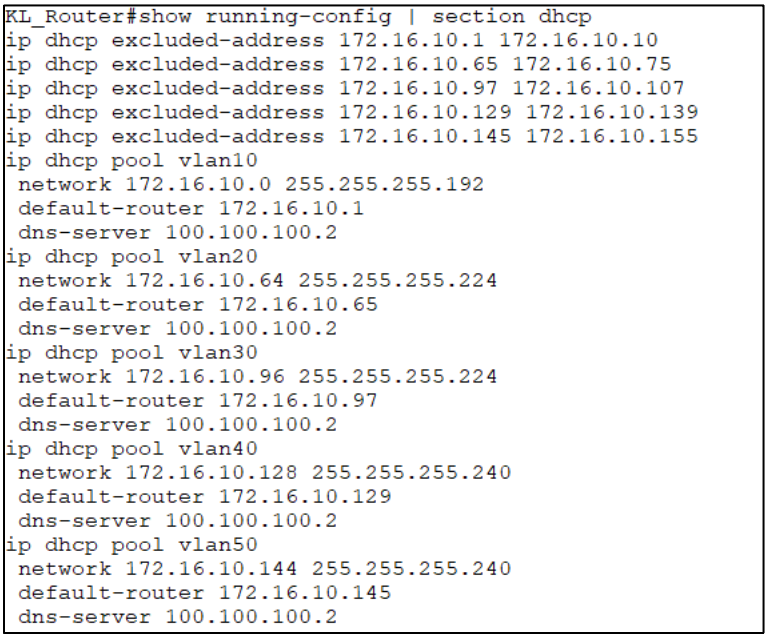
4.7.3 Configuration



```
SG_FireDSRouter#show running-config | section dhcp
ip dhcp excluded-address 192.168.10.1 192.168.10.10
ip dhcp excluded-address 192.168.11.1 192.168.11.10
ip dhcp excluded-address 192.168.12.1 192.168.12.10
ip dhcp pool vlan110
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
 dns-server 100.100.100.2
ip dhcp pool vlan120
 network 192.168.11.0 255.255.255.0
 default-router 192.168.11.1
 dns-server 100.100.100.2
ip dhcp pool vlan130
 network 192.168.12.0 255.255.255.0
 default-router 192.168.12.1
 dns-server 100.100.100.2
SG_FireDSRouter#
```

Figure 4.7.3.1 sg - show running-config | section dhcp

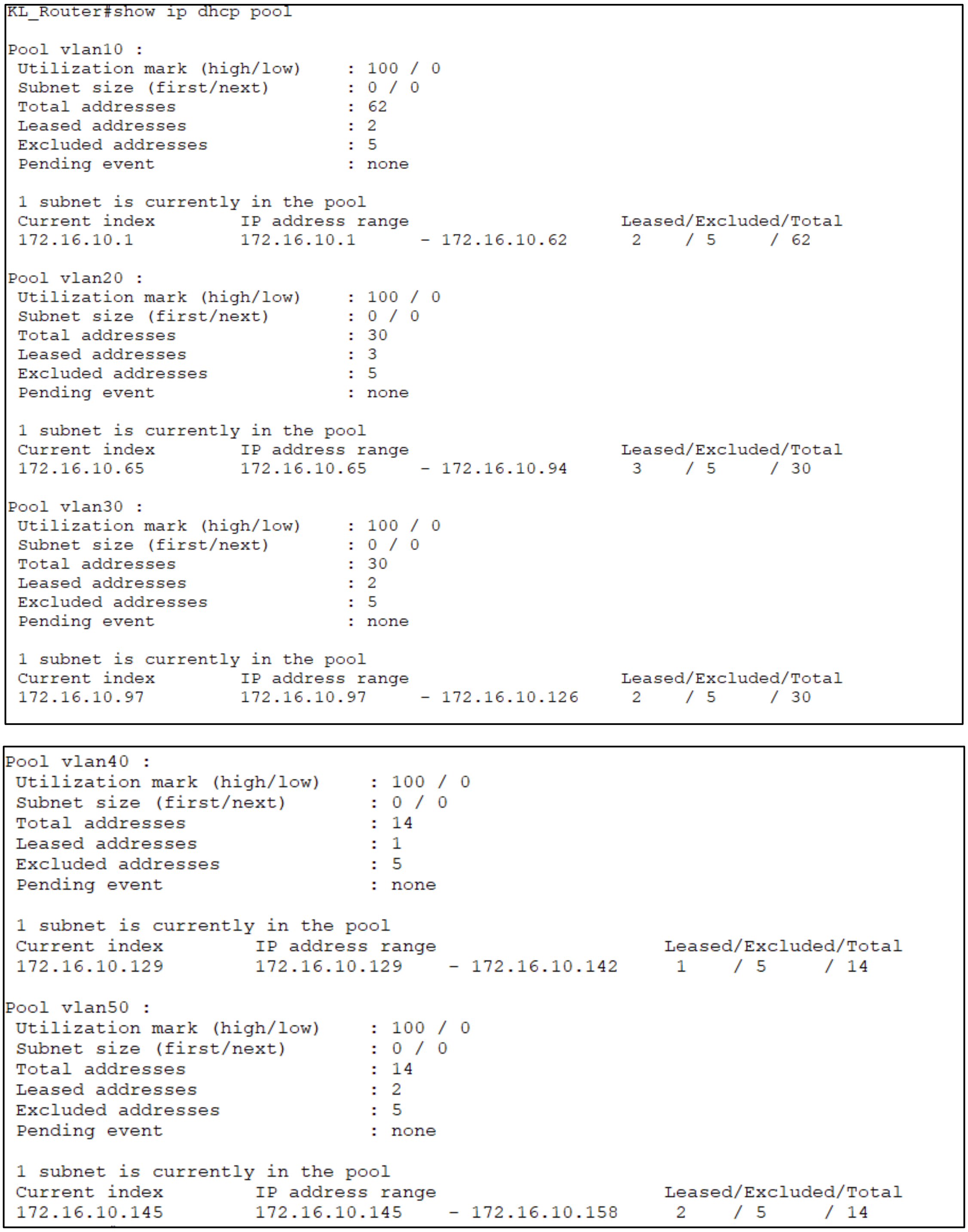
Display the DHCP pool configuration for VLANs 110, 120, and 130 on the 'SG_FireDSRouter' router.



```
KL_Router#show running-config | section dhcp
ip dhcp excluded-address 172.16.10.1 172.16.10.10
ip dhcp excluded-address 172.16.10.65 172.16.10.75
ip dhcp excluded-address 172.16.10.97 172.16.10.107
ip dhcp excluded-address 172.16.10.129 172.16.10.139
ip dhcp excluded-address 172.16.10.145 172.16.10.155
ip dhcp pool vlan10
 network 172.16.10.0 255.255.255.192
 default-router 172.16.10.1
 dns-server 100.100.100.2
ip dhcp pool vlan20
 network 172.16.10.64 255.255.255.224
 default-router 172.16.10.65
 dns-server 100.100.100.2
ip dhcp pool vlan30
 network 172.16.10.96 255.255.255.224
 default-router 172.16.10.97
 dns-server 100.100.100.2
ip dhcp pool vlan40
 network 172.16.10.128 255.255.255.240
 default-router 172.16.10.129
 dns-server 100.100.100.2
ip dhcp pool vlan50
 network 172.16.10.144 255.255.255.240
 default-router 172.16.10.145
 dns-server 100.100.100.2
```

Figure 4.7.3.2 kl - show running-config | section dhcp

Display the DHCP pool configuration for VLANs 110, 120, and 130 on the 'KL_Router' router.

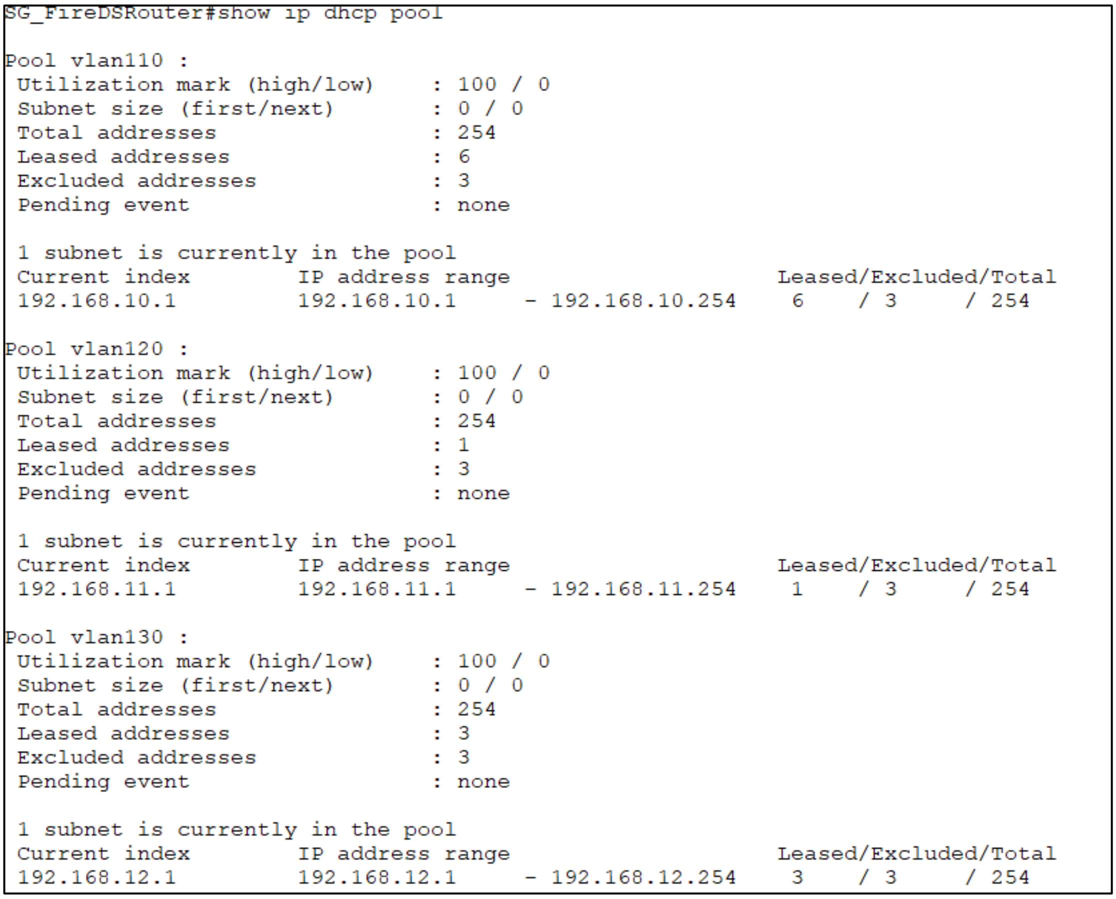


```
KL_Router#show ip dhcp pool

Pool vlan10 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 62
 Leased addresses               : 2
 Excluded addresses             : 5
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 172.16.10.1          172.16.10.1      - 172.16.10.62      2    / 5     / 62

Pool vlan20 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 30
 Leased addresses               : 3
 Excluded addresses             : 5
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 172.16.10.65         172.16.10.65     - 172.16.10.94      3    / 5     / 30

Pool vlan30 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 30
 Leased addresses               : 2
 Excluded addresses             : 5
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 172.16.10.97         172.16.10.97     - 172.16.10.126     2    / 5     / 30
```

```
Pool vlan40 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 14
 Leased addresses               : 1
 Excluded addresses             : 5
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 172.16.10.129        172.16.10.129    - 172.16.10.142     1    / 5     / 14

Pool vlan50 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 14
 Leased addresses               : 2
 Excluded addresses             : 5
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 172.16.10.145        172.16.10.145    - 172.16.10.158     2    / 5     / 14
```

Figure 4.7.3.3 kl - DHCP Address Pool Status

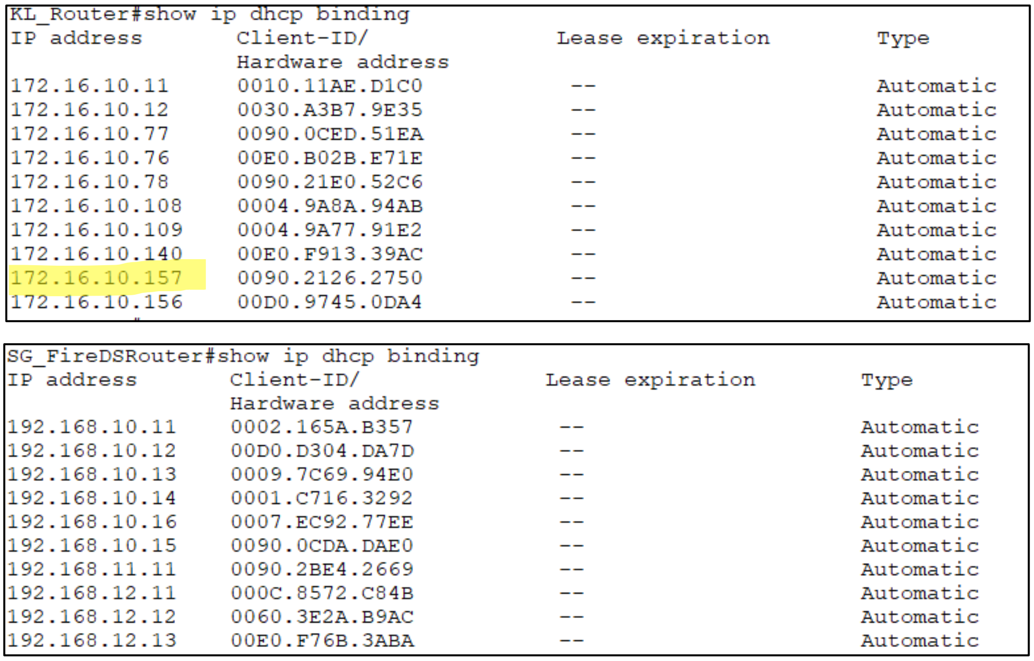
Display the total number of available addresses and the number of addresses leased for each DHCP pool on the 'KL_Router'.



```
SG_FireDSRouter#show ip dhcp pool

Pool vlan110 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 6
 Excluded addresses             : 3
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.10.1         192.168.10.1     - 192.168.10.254    6     / 3     / 254

Pool vlan120 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 1
 Excluded addresses             : 3
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.11.1         192.168.11.1     - 192.168.11.254    1     / 3     / 254

Pool vlan130 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 3
 Excluded addresses             : 3
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.12.1         192.168.12.1     - 192.168.12.254    3     / 3     / 254
```

Figure 4.7.3.4 sg - DHCP Address Pool Status

Display the total number of available addresses and the number of addresses leased for each DHCP pool on the ‘SG_FireDSRoute’.

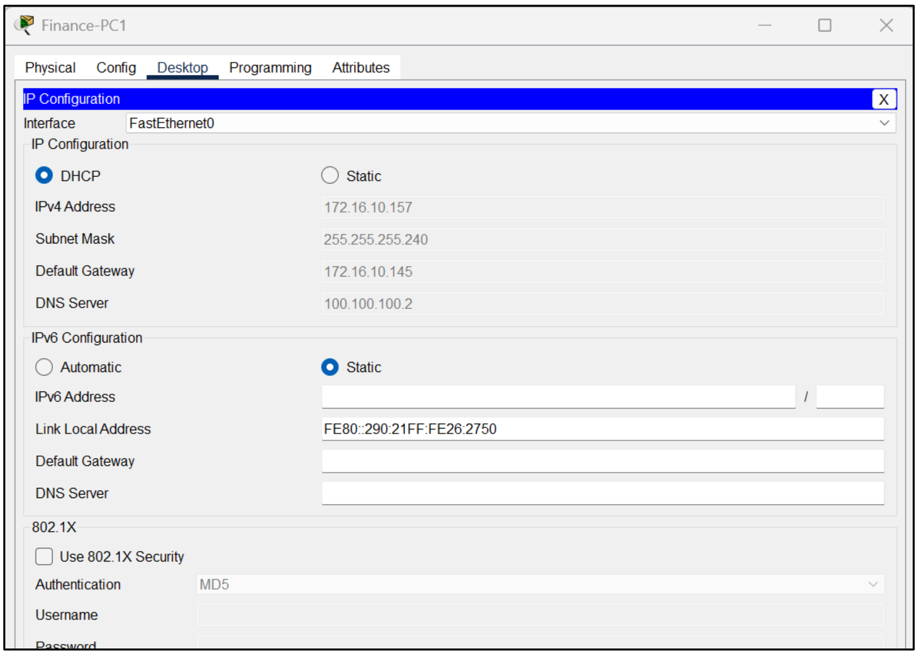


```
KL_Router#show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
172.16.10.11     0010.11AE.D1C0           --                     Automatic
172.16.10.12     0030.A3B7.9E35           --                     Automatic
172.16.10.77     0090.0CED.51EA           --                     Automatic
172.16.10.76     00E0.B02B.E71E           --                     Automatic
172.16.10.78     0090.21E0.52C6           --                     Automatic
172.16.10.108    0004.9A8A.94AB           --                     Automatic
172.16.10.109    0004.9A77.91E2           --                     Automatic
172.16.10.140    00E0.F913.39AC           --                     Automatic
172.16.10.157    0090.2126.2750           --                     Automatic
172.16.10.156    00D0.9745.0DA4           --                     Automatic
```

```
SG_FireDSRouter#show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
192.168.10.11    0002.165A.B357           --                     Automatic
192.168.10.12    00D0.D304.DA7D           --                     Automatic
192.168.10.13    0009.7C69.94E0           --                     Automatic
192.168.10.14    0001.C716.3292           --                     Automatic
192.168.10.16    0007.EC92.77EE           --                     Automatic
192.168.10.15    0090.0CDA.DAE0           --                     Automatic
192.168.11.11    0090.2BE4.2669           --                     Automatic
192.168.12.11    000C.8572.C84B           --                     Automatic
192.168.12.12    0060.3E2A.B9AC           --                     Automatic
192.168.12.13    00E0.F76B.3ABA           --                     Automatic
```

Figure 4.7.3.5 DHCP Address Binding Table

Display the IP address currently assigned to the host. For example, the Ip address assigned to the PC in the Kuala Lumpur Network Finance Department is 172.16.10.157.



Interface: FastEthernet0

IP Configuration

● DHCP ○ Static

IPv4 Address: 172.16.10.157

Subnet Mask: 255.255.255.240

Default Gateway: 172.16.10.145

DNS Server: 100.100.100.2

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::290:21FF:FE26:2750

Default Gateway:

DNS Server:

802.1X

□ Use 802.1X Security

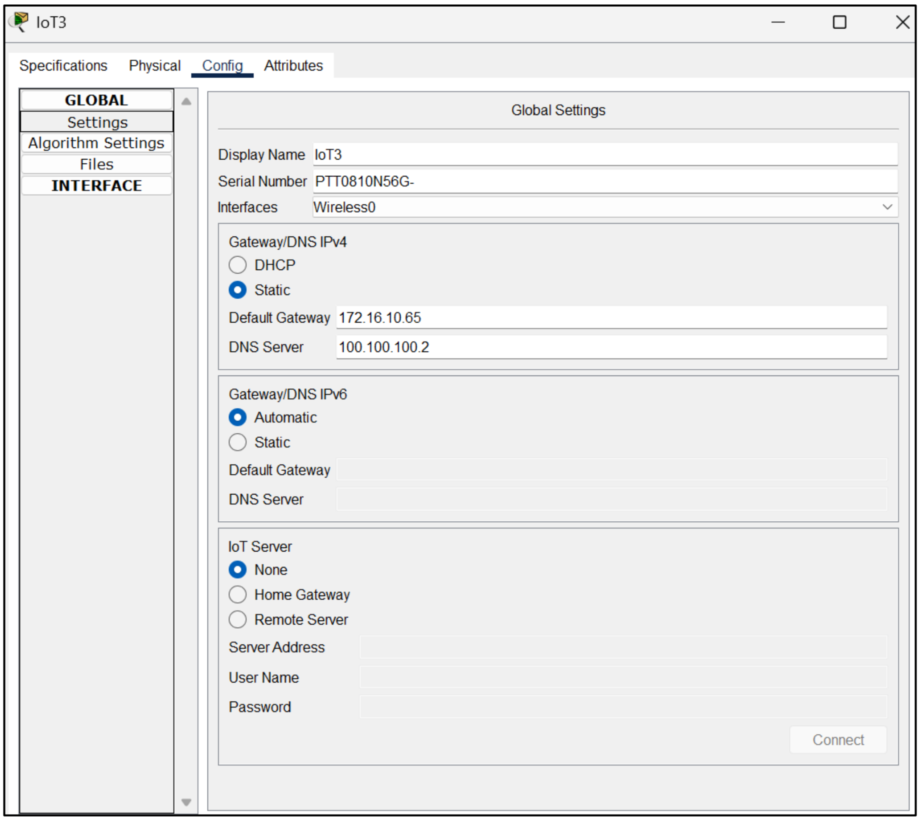
Authentication: MD5

Username:

Password

Figure 4.7.3.6 PC Dynamic Address Verification

After opening the 'Desktop' of a PC within the Finance department of Kuala Lumpur Network and clicking on IP configuration, you can view that the pc has successfully obtained the dynamic address via DHCP.



Global Settings

Display Name IoT3

Serial Number PTT0810N56G-

Interfaces Wireless0

Gateway/DNS IPv4

○ DHCP

● Static

Default Gateway 172.16.10.65

DNS Server 100.100.100.2

Gateway/DNS IPv6

● Automatic

○ Static

Default Gateway

DNS Server

IoT Server

● None

○ Home Gateway

○ Remote Server

Server Address

User Name

Password

Figure 4.7.3.7 Example of Static Addresses for IoT Devices

IoT devices use static IP addresses to ensure stable connections and unique identification. This is because IoT servers often need to actively initiate connections to control or query devices. A fixed IP address can ensure the permanent validity of the communication pathway and provide each device with a reliable network identity identifier, facilitating precise monitoring and management.

4.8 VLAN

4.8.1 Question

VLAN technology is mandatory to be implemented in all sub networks. Management and Native VLAN are required for deployment. Implement secured VLAN is mandatory (static trunk, native vlan, vlan allowed on trunk, blackhole and etc.) (Solution and configuration.)

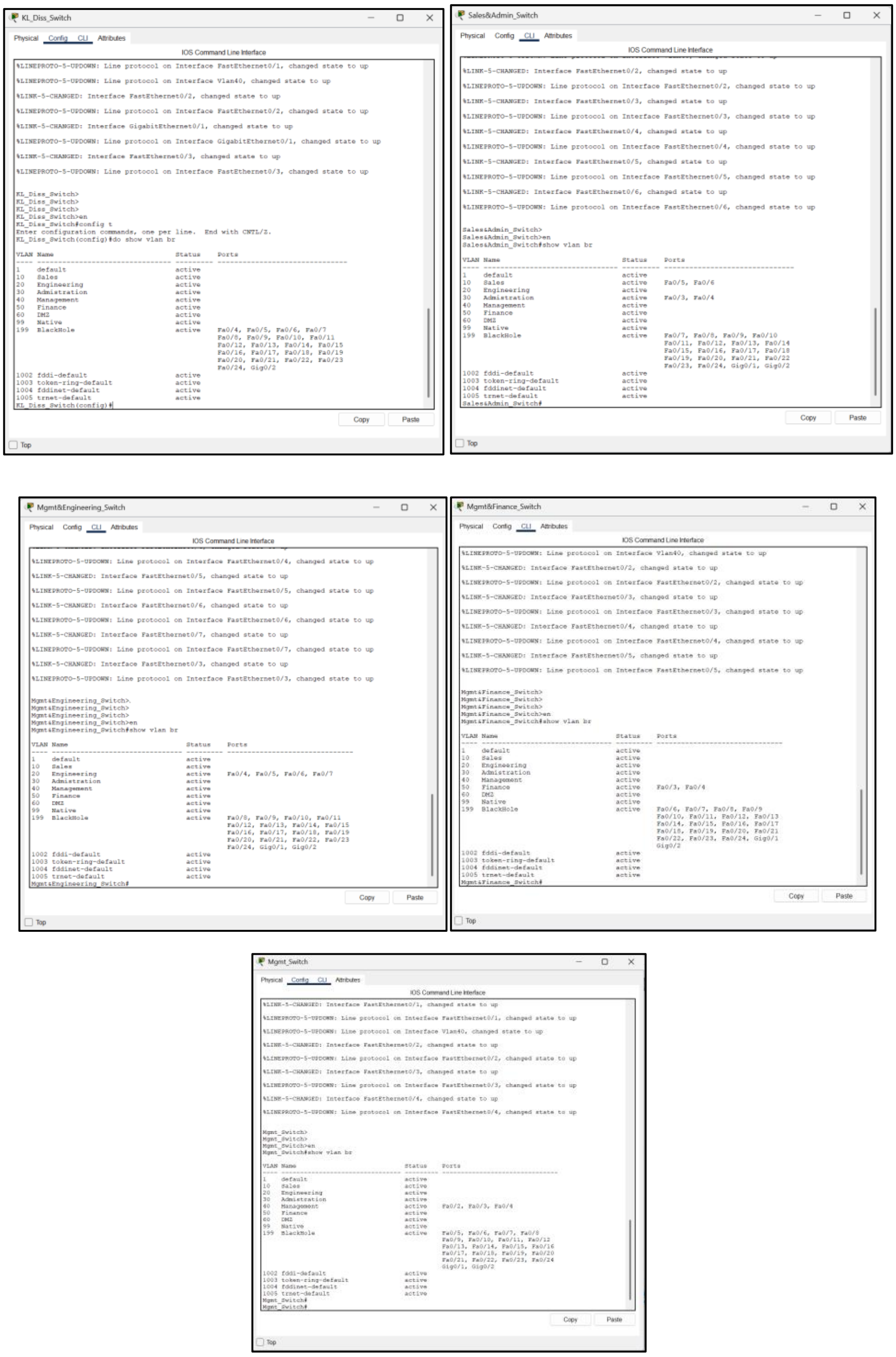
4.8.2 Solution

A Virtual Local Area Network (VLAN) is a logical segmentation of a Layer 2 (Data Link Layer) network that enables devices to be grouped together regardless of their physical location. Unlike traditional LANs that rely on physical topology, VLANs are implemented in switches using IEEE 802.1Q VLAN tagging. (Greeksforgeeks,2025)

To enhance network security, VLAN technology is essential to be deployed across all the subnets in Kuala Lumpur and Singapore branch. All the departments in KL and Singapore branches have its own VLAN. For example, Sales department operates within its own secure broadcast domain VLAN 10 while Engineering department is operating VLAN 20. Other than the departments VLAN, native VLAN and blackhole are configured in both branches to carry untagged traffic and store unused ports. The main goals of implement VLAN are to present logical traffic isolation and prevent attacks like Vlan hopping.

Overall, by implementing VLAN, it helps to improve the security of the company’s network infrastructure. Furthermore, it also helps on reducing the risk of internal data breaches and misconfigurations.

4.8.3 VLAN Configuration in KL



```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan40, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up


KL_Diss_Switch>
KL_Diss_Switch>
KL_Diss_Switch>
KL_Diss_Switch>en
KL_Diss_Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
KL_Diss_Switch(config)#do show vlan br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    
10   Sales                            active    
20   Engineering                      active    
30   Admistration                     active    
40   Management                       active    
50   Finance                          active    
60   DMZ                              active    
99   Native                           active    
199  BlackHole                        active    Fa0/4, Fa0/5, Fa0/6, Fa0/7
                                                Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gig0/2
1002 fddi-default                     active    
1003 token-ring-default               active    
1004 fddinet-default                  active    
1005 trnet-default                    active    
KL_Diss_Switch(config)#
```

```
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up


Sales&Admin_Switch>
Sales&Admin_Switch>en
Sales&Admin_Switch#show vlan br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    
10   Sales                            active    Fa0/5, Fa0/6
20   Engineering                      active    
30   Admistration                     active    Fa0/3, Fa0/4
40   Management                       active    
50   Finance                          active    
60   DMZ                              active    
99   Native                           active    
199  BlackHole                        active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
1002 fddi-default                     active    
1003 token-ring-default               active    
1004 fddinet-default                  active    
1005 trnet-default                    active    
Sales&Admin_Switch#
```

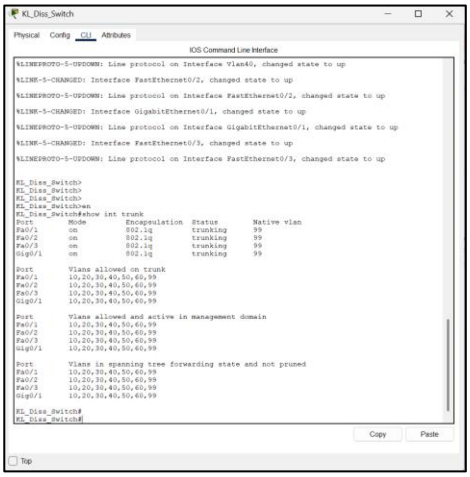
```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up


Mgmt&Engineering_Switch>
Mgmt&Engineering_Switch>
Mgmt&Engineering_Switch>
Mgmt&Engineering_Switch>en
Mgmt&Engineering_Switch#show vlan br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    
10   Sales                            active    
20   Engineering                      active    Fa0/4, Fa0/5, Fa0/6, Fa0/7
30   Admistration                     active    
40   Management                       active    
50   Finance                          active    
60   DMZ                              active    
99   Native                           active    
199  BlackHole                        active    Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gig0/1, Gig0/2
1002 fddi-default                     active    
1003 token-ring-default               active    
1004 fddinet-default                  active    
1005 trnet-default                    active    
Mgmt&Engineering_Switch#
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan40, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up


Mgmt&Finance_Switch>
Mgmt&Finance_Switch>
Mgmt&Finance_Switch>
Mgmt&Finance_Switch>en
Mgmt&Finance_Switch#show vlan br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    
10   Sales                            active    
20   Engineering                      active    
30   Admistration                     active    
40   Management                       active    
50   Finance                          active    Fa0/3, Fa0/4
60   DMZ                              active    
99   Native                           active    
199  BlackHole                        active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                                Gig0/2
1002 fddi-default                     active    
1003 token-ring-default               active    
1004 fddinet-default                  active    
1005 trnet-default                    active    
Mgmt&Finance_Switch#
```

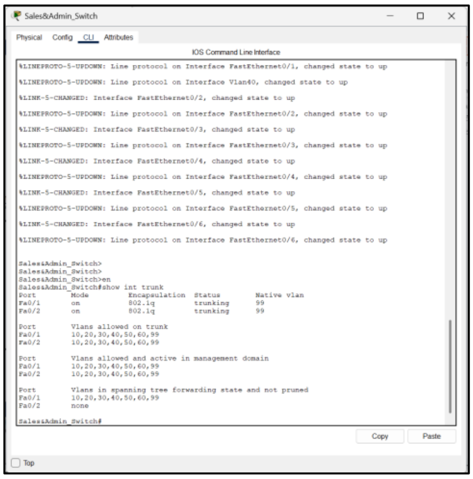
```
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan40, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up


Mgmt_Switch>
Mgmt_Switch>
Mgmt_Switch>en
Mgmt_Switch#show vlan br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    
10   Sales                            active    
20   Engineering                      active    
30   Admistration                     active    
40   Management                       active    Fa0/2, Fa0/3, Fa0/4
50   Finance                          active    
60   DMZ                              active    
99   Native                           active    
199  BlackHole                        active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
1002 fddi-default                     active    
1003 token-ring-default               active    
1004 fddinet-default                  active    
1005 trnet-default                    active    
Mgmt_Switch#
Mgmt_Switch#
```

Figure 4.8.3.1 : VLAN interfaces in KL Switches

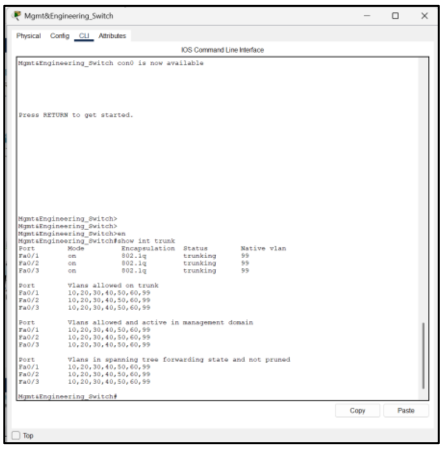
In KL network, there are total of 5 departments, which is Sales (VLAN 10), Engineering(VLAN 20), Adminstration (VLAN 30) , Management (VLAN 40) and Finance (VLAN 50) departments. VLAN 99 is choosen to be Native VLAN to carry untagged traffic across trunk links. The unused ports are shut down and assigned to VLAN 199, which is the BlackHole VLAN.



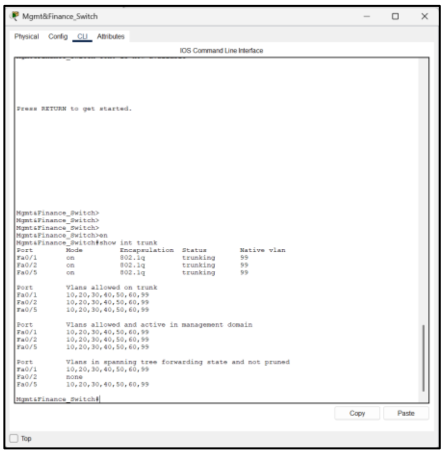
```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan40, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up


KL_Diss_Switch>
KL_Diss_Switch>
KL_Diss_Switch>
KL_Diss_Switch>en
KL_Diss_Switch#show int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      99
Fa0/2       on           802.1q         trunking      99
Fa0/3       on           802.1q         trunking      99
Gig0/1      on           802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       10,20,30,40,50,60,99
Fa0/2       10,20,30,40,50,60,99
Fa0/3       10,20,30,40,50,60,99
Gig0/1      10,20,30,40,50,60,99

Port        Vlans allowed and active in management domain
Fa0/1       10,20,30,40,50,60,99
Fa0/2       10,20,30,40,50,60,99
Fa0/3       10,20,30,40,50,60,99
Gig0/1      10,20,30,40,50,60,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       10,20,30,40,50,60,99
Fa0/2       10,20,30,40,50,60,99
Fa0/3       10,20,30,40,50,60,99
Gig0/1      10,20,30,40,50,60,99

KL_Diss_Switch#
KL_Diss_Switch#
```



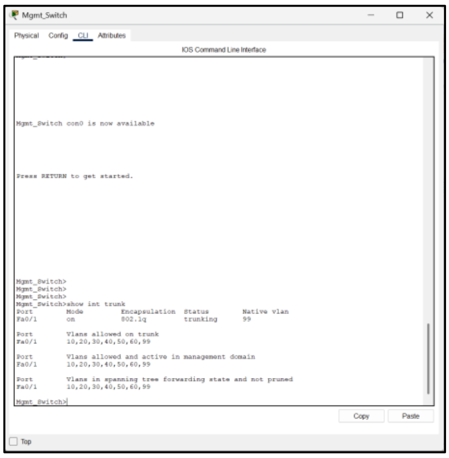
```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan40, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up


Sales&Admin_Switch>
Sales&Admin_Switch>
Sales&Admin_Switch>en
Sales&Admin_Switch#show int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      99
Fa0/2       on           802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       10,20,30,40,50,60,99
Fa0/2       10,20,30,40,50,60,99

Port        Vlans allowed and active in management domain
Fa0/1       10,20,30,40,50,60,99
Fa0/2       10,20,30,40,50,60,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       10,20,30,40,50,60,99
Fa0/2       none

Sales&Admin_Switch#
```



```
Mgmt&Engineering_Switch con0 is now available




Press RETURN to get started.










Mgmt&Engineering_Switch>
Mgmt&Engineering_Switch>
Mgmt&Engineering_Switch>en
Mgmt&Engineering_Switch#show int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      99
Fa0/2       on           802.1q         trunking      99
Fa0/3       on           802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       10,20,30,40,50,60,99
Fa0/2       10,20,30,40,50,60,99
Fa0/3       10,20,30,40,50,60,99

Port        Vlans allowed and active in management domain
Fa0/1       10,20,30,40,50,60,99
Fa0/2       10,20,30,40,50,60,99
Fa0/3       10,20,30,40,50,60,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       10,20,30,40,50,60,99
Fa0/2       10,20,30,40,50,60,99
Fa0/3       10,20,30,40,50,60,99

Mgmt&Engineering_Switch#
```



```
Press RETURN to get started.










Mgmt&Finance_Switch>
Mgmt&Finance_Switch>
Mgmt&Finance_Switch>
Mgmt&Finance_Switch>en
Mgmt&Finance_Switch#show int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      99
Fa0/2       on           802.1q         trunking      99
Fa0/5       on           802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       10,20,30,40,50,60,99
Fa0/2       10,20,30,40,50,60,99
Fa0/5       10,20,30,40,50,60,99

Port        Vlans allowed and active in management domain
Fa0/1       10,20,30,40,50,60,99
Fa0/2       10,20,30,40,50,60,99
Fa0/5       10,20,30,40,50,60,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       10,20,30,40,50,60,99
Fa0/2       none
Fa0/5       10,20,30,40,50,60,99

Mgmt&Finance_Switch#
```

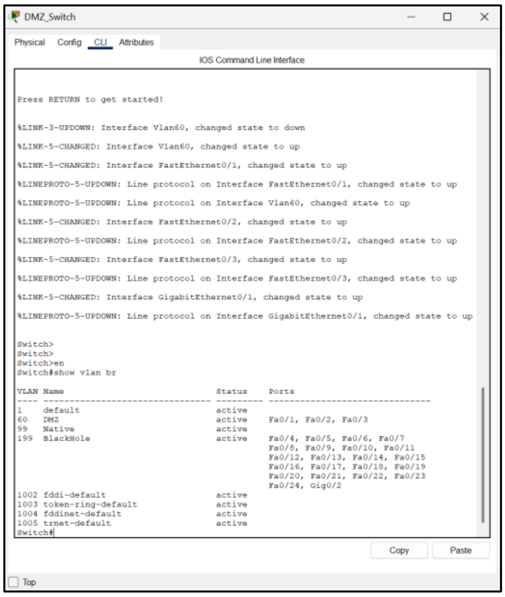


```
Mgmt_Switch con0 is now available




Press RETURN to get started.










Mgmt_Switch>
Mgmt_Switch>
Mgmt_Switch>
Mgmt_Switch>show int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       10,20,30,40,50,60,99

Port        Vlans allowed and active in management domain
Fa0/1       10,20,30,40,50,60,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       10,20,30,40,50,60,99

Mgmt_Switch>
```

Figure 4.8.3.2: VLAN Trunking in KL Switches

The static trunk ports are configured based on different connection situation on the switches. For example, at the management & Engineering switch, fa0/1-3 are configured as static trunk port to prevent VLAN hopping attack.Only authourized VLAN(10,20,30,40,50,60,99) are allowed on trunk to minimuze unnecessary VLAN exposure. The encapsulation 802.1Q is used for VLAN tagging, which is standard and secure for trunk communication.

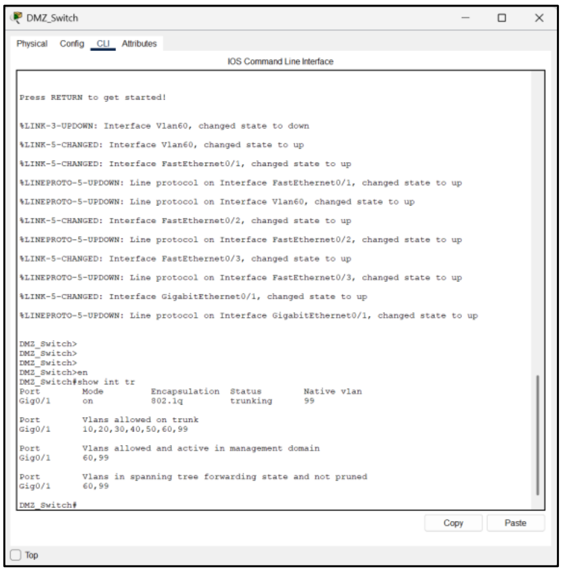
4.8.4 VLAN Configuration in DMZ zone



```
Press RETURN to get started!


%LINK-3-UPDOWN: Interface Vlan60, changed state to down

%LINK-5-CHANGED: Interface Vlan60, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan60, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up


Switch>
Switch>
Switch>en
Switch#show vlan br

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

Figure 4.8.4.1 : VLAN interfaces in DMZ Zone

The DMZ zone is isolated from KL, and it operates its own VLAN, which is VLAN 60. Same as KL network, unused ports are shut down and assigned to VLAN 199 (Blackhole) and the untagged traffic is carried through VLAN 99(Native).

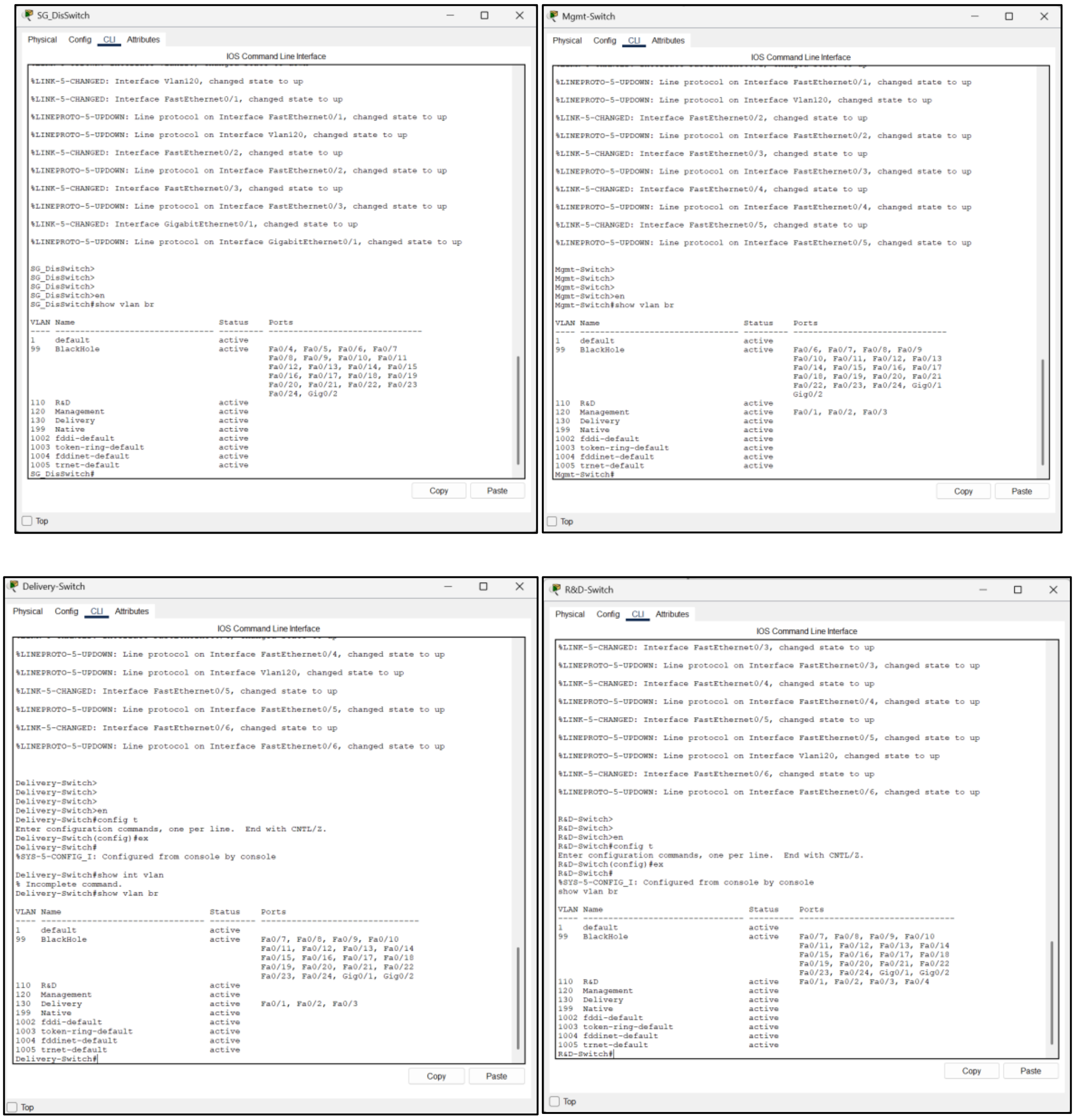


```
Press RETURN to get started!


%LINK-3-UPDOWN: Interface Vlan60, changed state to down

%LINK-5-CHANGED: Interface Vlan60, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan60, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up


DMZ_Switch>
DMZ_Switch>
DMZ_Switch>
DMZ_Switch>en
DMZ_Switch#show int tr
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      on           802.1q         trunking      99

Port        Vlans allowed on trunk
Gig0/1      10,20,30,40,50,60,99

Port        Vlans allowed and active in management domain
Gig0/1      60,99

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      60,99

DMZ_Switch#
```

Figure 4.8.4.2 : VLAN trunking in DMZ Switches

At the DMZ switch, g0/1 are configured as static trunk port to prevent VLAN hopping attack.Only authourized VLAN(60,99) are allowed on trunk to minimuze unnecessary VLAN exposure. The encapsulation 802.1Q is used for VLAN tagging, which is standard and secure for trunk communication.

4.8.5 VLAN Configuration in Singapore



```
%LINK-5-CHANGED: Interface Vlan120, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan120, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up


SG_DisSwitch>
SG_DisSwitch>
SG_DisSwitch>
SG_DisSwitch>en
SG_DisSwitch#show vlan br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    
99   BlackHole                        active    Fa0/4, Fa0/5, Fa0/6, Fa0/7
                                                Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gig0/2
110  R&D                              active    
120  Management                       active    
130  Delivery                         active    
199  Native                           active    
1002 fddi-default                     active    
1003 token-ring-default               active    
1004 fddinet-default                  active    
1005 trnet-default                    active    
SG_DisSwitch#
```

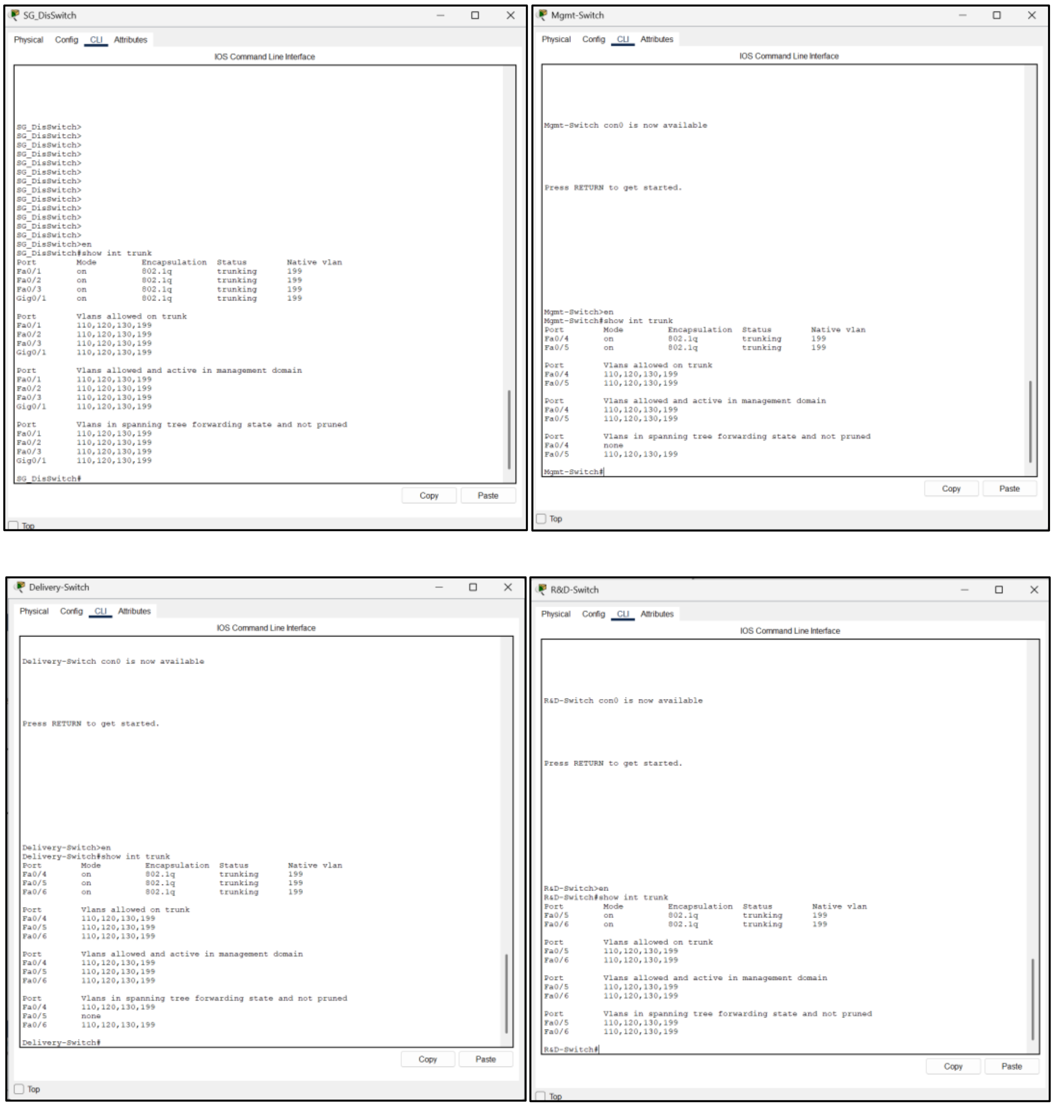
```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan120, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up


Mgmt-Switch>
Mgmt-Switch>
Mgmt-Switch>
Mgmt-Switch>en
Mgmt-Switch#show vlan br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    
99   BlackHole                        active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                                Gig0/2
110  R&D                              active    
120  Management                       active    Fa0/1, Fa0/2, Fa0/3
130  Delivery                         active    
199  Native                           active    
1002 fddi-default                     active    
1003 token-ring-default               active    
1004 fddinet-default                  active    
1005 trnet-default                    active    
Mgmt-Switch#
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan120, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up



Delivery-Switch>
Delivery-Switch>
Delivery-Switch>
Delivery-Switch>en
Delivery-Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Delivery-Switch(config)#ex
Delivery-Switch#
%SYS-5-CONFIG_I: Configured from console by console

Delivery-Switch#show int vlan
% Incomplete command.
Delivery-Switch#show vlan br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    
99   BlackHole                        active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
110  R&D                              active    
120  Management                       active    
130  Delivery                         active    Fa0/1, Fa0/2, Fa0/3
199  Native                           active    
1002 fddi-default                     active    
1003 token-ring-default               active    
1004 fddinet-default                  active    
1005 trnet-default                    active    
Delivery-Switch#
```

```
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan120, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up


R&D-Switch>
R&D-Switch>
R&D-Switch>en
R&D-Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R&D-Switch(config)#ex
R&D-Switch#
%SYS-5-CONFIG_I: Configured from console by console
show vlan br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    
99   BlackHole                        active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
110  R&D                              active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
120  Management                       active    
130  Delivery                         active    
199  Native                           active    
1002 fddi-default                     active    
1003 token-ring-default               active    
1004 fddinet-default                  active    
1005 trnet-default                    active    
R&D-Switch#
```

Figure 4.8.5.1 : VLAN interfaces in Singapore Switches

In KL network, there are total of 3 departments, which is R&D (VLAN 110), Management(VLAN 120) and Delivery (VLAN 130). VLAN 199 is choosen to be Native VLAN to carry untagged traffic across trunk links. The unused ports are shut down and assigned to VLAN 99, which is the BlackHole VLAN.



```
SG_DisSwitch>
SG_DisSwitch>
SG_DisSwitch>
SG_DisSwitch>
SG_DisSwitch>
SG_DisSwitch>
SG_DisSwitch>
SG_DisSwitch>
SG_DisSwitch>
SG_DisSwitch>
SG_DisSwitch>
SG_DisSwitch>
SG_DisSwitch>
SG_DisSwitch>en
SG_DisSwitch#show int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      199
Fa0/2       on           802.1q         trunking      199
Fa0/3       on           802.1q         trunking      199
Gig0/1      on           802.1q         trunking      199

Port        Vlans allowed on trunk
Fa0/1       110,120,130,199
Fa0/2       110,120,130,199
Fa0/3       110,120,130,199
Gig0/1      110,120,130,199

Port        Vlans allowed and active in management domain
Fa0/1       110,120,130,199
Fa0/2       110,120,130,199
Fa0/3       110,120,130,199
Gig0/1      110,120,130,199

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       110,120,130,199
Fa0/2       110,120,130,199
Fa0/3       110,120,130,199
Gig0/1      110,120,130,199

SG_DisSwitch#
```

```
Mgmt-Switch con0 is now available




Press RETURN to get started.










Mgmt-Switch>en
Mgmt-Switch#show int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/4       on           802.1q         trunking      199
Fa0/5       on           802.1q         trunking      199

Port        Vlans allowed on trunk
Fa0/4       110,120,130,199
Fa0/5       110,120,130,199

Port        Vlans allowed and active in management domain
Fa0/4       110,120,130,199
Fa0/5       110,120,130,199

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/4       none
Fa0/5       110,120,130,199

Mgmt-Switch#
```

```
Delivery-Switch con0 is now available




Press RETURN to get started.










Delivery-Switch>en
Delivery-Switch#show int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/4       on           802.1q         trunking      199
Fa0/5       on           802.1q         trunking      199
Fa0/6       on           802.1q         trunking      199

Port        Vlans allowed on trunk
Fa0/4       110,120,130,199
Fa0/5       110,120,130,199
Fa0/6       110,120,130,199

Port        Vlans allowed and active in management domain
Fa0/4       110,120,130,199
Fa0/5       110,120,130,199
Fa0/6       110,120,130,199

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/4       110,120,130,199
Fa0/5       none
Fa0/6       110,120,130,199

Delivery-Switch#
```

```
R&D-Switch con0 is now available




Press RETURN to get started.










R&D-Switch>en
R&D-Switch#show int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/5       on           802.1q         trunking      199
Fa0/6       on           802.1q         trunking      199

Port        Vlans allowed on trunk
Fa0/5       110,120,130,199
Fa0/6       110,120,130,199

Port        Vlans allowed and active in management domain
Fa0/5       110,120,130,199
Fa0/6       110,120,130,199

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/5       110,120,130,199
Fa0/6       110,120,130,199

R&D-Switch#
```

Figure 4.8.5.2 : VLAN Trunking in Singapore Switches

The static trunk ports are configured based on different connection situation on the switches. For example, at the Delivery switch, fa0/4-6 are configured as static trunk port to prevent VLAN hopping attack.Only authourized VLAN(110,120,130,199) are allowed on trunk to minimuze unnecessary VLAN exposure. The encapsulation 802.1Q is used for VLAN tagging, which is standard and secure for trunk communication.

4.9 ACL

4.9.1 Question

Proposed several policies for both networks (KL and Singapore) to reduce the internal/external access to its resources. Examples: No client from admin, sales, engineering, and finance department can access clients in the other departments and any. (Solution and configuration.)

4.9.2 Solution

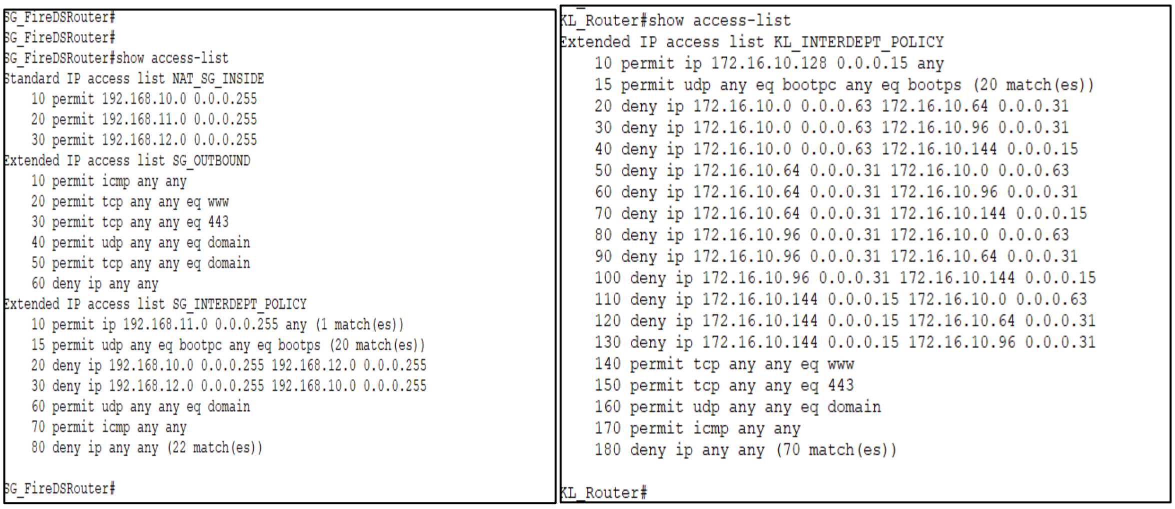
To reduce the potential risks existing in the internal and external access of enterprise network resources, this design employs a combined strategy of Standard Access Control Lists (Standard ACL) and Extended Access Control Lists (Extended ACL) across networks in Kuala Lumpur and Singapore. These two approaches complement each other within the overall architecture, collectively forming a multi-layered network access protection system.

In the overall design, Standard ACL is used to implement basic-level traffic restrictions, such as prohibiting specific IP addresses or subnet segments from accessing management resources or servers. In conclusion, Standard ACL is more attention to the coarse-grained control of unidirectional flow. The Extended ACL undertakes more detailed access layering tasks. By simultaneously matching the source address, destination address, and transport layer port number, it achieves interdepartmental isolation and external access control. Extended ACL covers the inbound directions of each VLAN sub-interface, ensuring that the traffic of each department is reviewed and restricted as soon as it enters the router, preventing unauthorized lateral access.

The overall solution adheres to the Least Privilege Principle, meaning that each department can only access resources related to its own business and avoid unnecessary internal communication. Secondly, Role-Based Access Control enables the Management VLAN (VLAN40 and VLAN120) to have cross-departmental access rights, which can be used for supervision and operation and maintenance. Finally, it is to achieve a balance between security and usability. For example, while strictly restricting internal lateral access, all departments are allowed to securely access external networks (e.g. HTTP, HTTPS, DNS) to ensure business continuity.

Through the combined configuration of Standard and Extended ACL, the two branch networks in Kuala Lumpur and Singapore have achieved the goal of defence-in-depth in the security structure of the enterprise Intranet. Standard ACL provides the first layer of filtering to block unnecessary external host traffic, while the Extended ACL achieves refined internal access control, ensuring that interdepartmental isolation and cross-branch communication are all carried out within the secure boundary.

4.9.3 Configuration

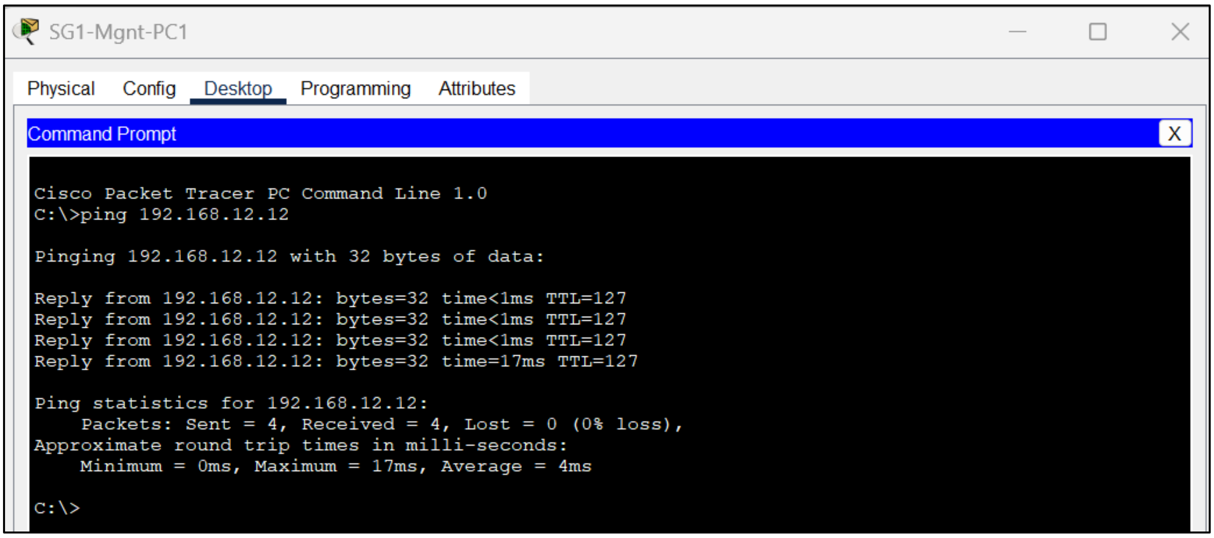


```
SG_FireDSRouter#
SG_FireDSRouter#
SG_FireDSRouter#show access-list
Standard IP access list NAT_SG_INSIDE
   10 permit 192.168.10.0 0.0.0.255
   20 permit 192.168.11.0 0.0.0.255
   30 permit 192.168.12.0 0.0.0.255
Extended IP access list SG_OUTBOUND
   10 permit icmp any any
   20 permit tcp any any eq www
   30 permit tcp any any eq 443
   40 permit udp any any eq domain
   50 permit tcp any any eq domain
   60 deny ip any any
Extended IP access list SG_INTERDEPT_POLICY
   10 permit ip 192.168.11.0 0.0.0.255 any (1 match(es))
   15 permit udp any eq bootpc any eq bootps (20 match(es))
   20 deny ip 192.168.10.0 0.0.0.255 192.168.12.0 0.0.0.255
   30 deny ip 192.168.12.0 0.0.0.255 192.168.10.0 0.0.0.255
   60 permit udp any any eq domain
   70 permit icmp any any
   80 deny ip any any (22 match(es))

SG_FireDSRouter#
```

```
KL_Router#show access-list
Extended IP access list KL_INTERDEPT_POLICY
    10 permit ip 172.16.10.128 0.0.0.15 any
    15 permit udp any eq bootpc any eq bootps (20 match(es))
    20 deny ip 172.16.10.0 0.0.0.63 172.16.10.64 0.0.0.31
    30 deny ip 172.16.10.0 0.0.0.63 172.16.10.96 0.0.0.31
    40 deny ip 172.16.10.0 0.0.0.63 172.16.10.144 0.0.0.15
    50 deny ip 172.16.10.64 0.0.0.31 172.16.10.0 0.0.0.63
    60 deny ip 172.16.10.64 0.0.0.31 172.16.10.96 0.0.0.31
    70 deny ip 172.16.10.64 0.0.0.31 172.16.10.144 0.0.0.15
    80 deny ip 172.16.10.96 0.0.0.31 172.16.10.0 0.0.0.63
    90 deny ip 172.16.10.96 0.0.0.31 172.16.10.64 0.0.0.31
    100 deny ip 172.16.10.96 0.0.0.31 172.16.10.144 0.0.0.15
    110 deny ip 172.16.10.144 0.0.0.15 172.16.10.0 0.0.0.63
    120 deny ip 172.16.10.144 0.0.0.15 172.16.10.64 0.0.0.31
    130 deny ip 172.16.10.144 0.0.0.15 172.16.10.96 0.0.0.31
    140 permit tcp any any eq www
    150 permit tcp any any eq 443
    160 permit udp any any eq domain
    170 permit icmp any any
    180 deny ip any any (70 match(es))

KL_Router#
```

Figure 4.9.3.1 show access-list

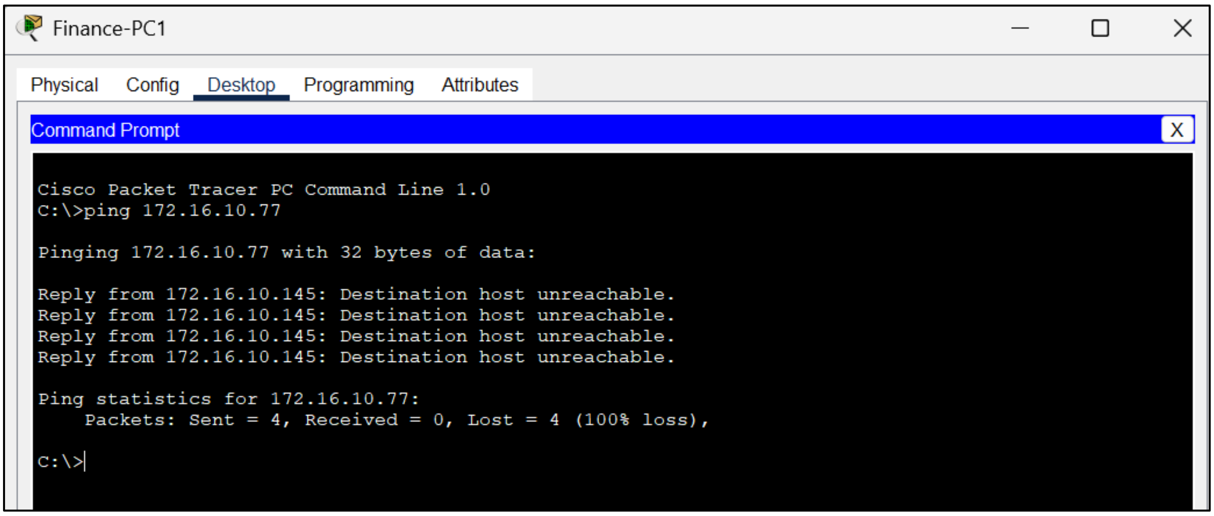
The output shows that SG_INTERDEPT_POLICY and KL_INTERDEPT_POLICY has taken effect. Management (SG: 192.168.11.0/24 and KL: 172.16.10.128) is allowed to access any destination address. Mutual visits between Admin and Engineering are explicitly rejected. Externally, only HTTP/HTTPS/DNS/ICMP is allowed, and all other protocols are rejected by default.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.12.12

Pinging 192.168.12.12 with 32 bytes of data:

Reply from 192.168.12.12: bytes=32 time<1ms TTL=127
Reply from 192.168.12.12: bytes=32 time<1ms TTL=127
Reply from 192.168.12.12: bytes=32 time<1ms TTL=127
Reply from 192.168.12.12: bytes=32 time=17ms TTL=127

Ping statistics for 192.168.12.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 17ms, Average = 4ms

C:\>
```

Figure 4.9.3.2 SG Management ping SG Delivery PC-1

This test is initiated from the client of the Management department (192.168.11.11) and performs an ICMP Ping test on the target of the Delivery department (192.168.12.12). The result means that Management has full network access privileged and can access other departments.

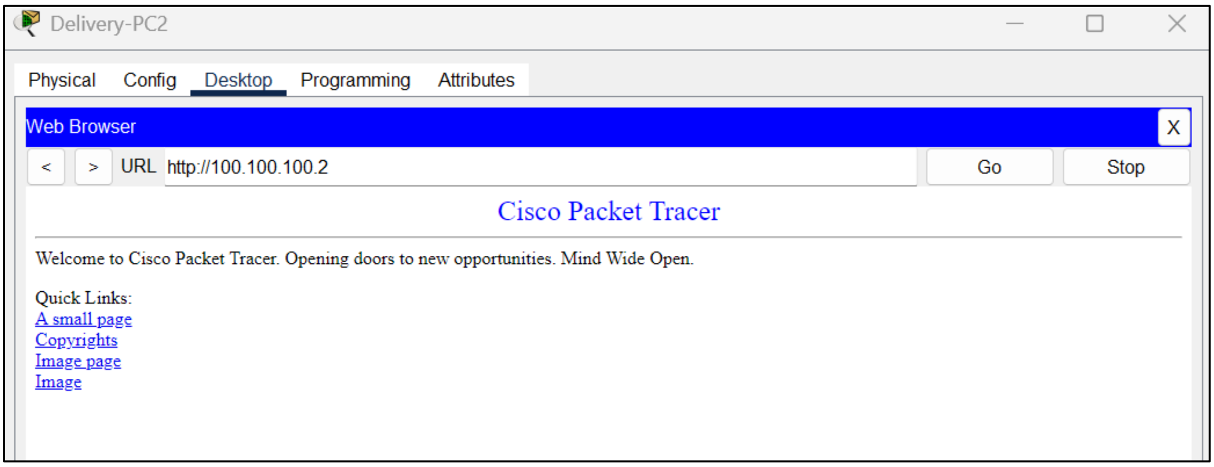


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.16.10.77

Pinging 172.16.10.77 with 32 bytes of data:

Reply from 172.16.10.145: Destination host unreachable.
Reply from 172.16.10.145: Destination host unreachable.
Reply from 172.16.10.145: Destination host unreachable.
Reply from 172.16.10.145: Destination host unreachable.

Ping statistics for 172.16.10.77:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Figure 4.9.3.2 KL Finance ping KL Engineering-PC1

This test is initiated from the client of the Finance department (172.16.10.157) and performs ICMP Ping tests on the target of the Engineering department (172.16.10.76). The outcome indicates that mutual access between Finance and Engineering departments is entirely prohibited, regardless of direction.

Therefore, the Ping Request was rejected by the firewall, verifying that the internal cross-departmental access restriction policy was effective.



http://100.100.100.2

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image

Figure 4.9.3.3 Web Access Testing (Delivery Department PCs)

As illustrated, the Delivery department's client successfully accessed the Web/DNS server located on the KL network (IP: 100.100.100.2). This outcome verifies that external access (HTTP, HTTPS, DNS) remains permitted following the application of extended access control lists, whilst internal cross-departmental communication is restricted. This achieves a balance between network resource isolation and external service accessibility.

4.10 Layer two attacks

4.10.1 Question

Explain any THREE types of layer two attacks. Implement layer two securities as a requirement in the company LAN. (Solution and configuration.)

4.10.2 Solution

1. MAC Address Flooding

MAC Address Flooding is a type of attack where an attacker connects a device and flood fake MAC addresses into the switches whereby it will fill up its memory. Once the table is full, the switch forwards frames to all ports, allowing the attacker to capture traffic.

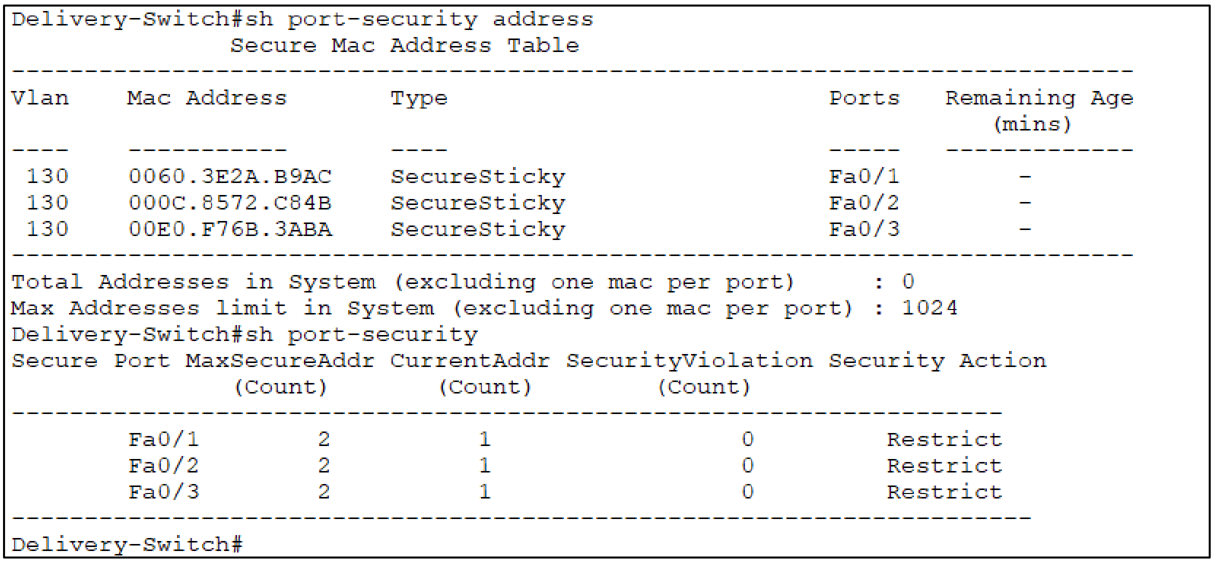
2. DHCP Spoofing Attack

DHCP Spoofing is a type of attack where an attacker creates a fake DHCP server to issue fake IP addresses and default gateways to users, distribute network configurations to be able to read network traffic like Man-in-the-middle attack. (Jannik, 2022).

3. Spanning Tree Protocol (STP) Attack

Spanning Tree Protocol (STP) attack is a type of attack where an attacker sends superior BPDUs to become the root bridge, changing the network topology and causing loops or traffic disruption.

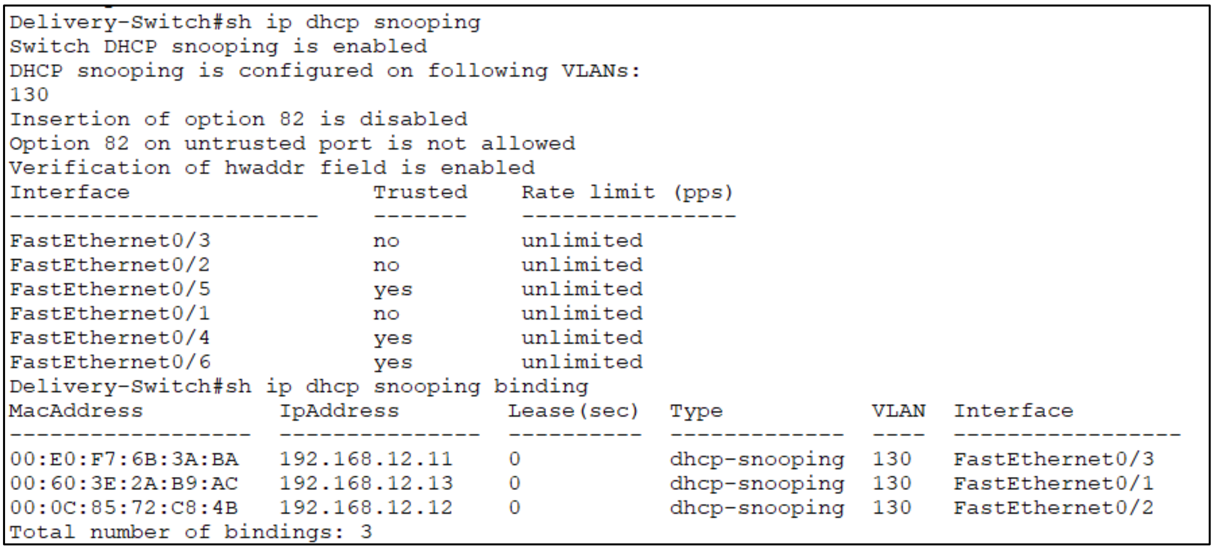
4.10.3 Configuration



```
Delivery-Switch#sh port-security address
               Secure Mac Address Table
-----------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                   (mins)
----    -----------       ----                          -----   -------------
 130    0060.3E2A.B9AC    SecureSticky                  Fa0/1        -
 130    000C.8572.C84B    SecureSticky                  Fa0/2        -
 130    00E0.F76B.3ABA    SecureSticky                  Fa0/3        -
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)      : 0
Max Addresses limit in System (excluding one mac per port) : 1024
Delivery-Switch#sh port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
--------------------------------------------------------------------
        Fa0/1        2           1                 0         Restrict
        Fa0/2        2           1                 0         Restrict
        Fa0/3        2           1                 0         Restrict
----------------------------------------------------------------------
Delivery-Switch#
```

Figure 10.2.1 – show port-security

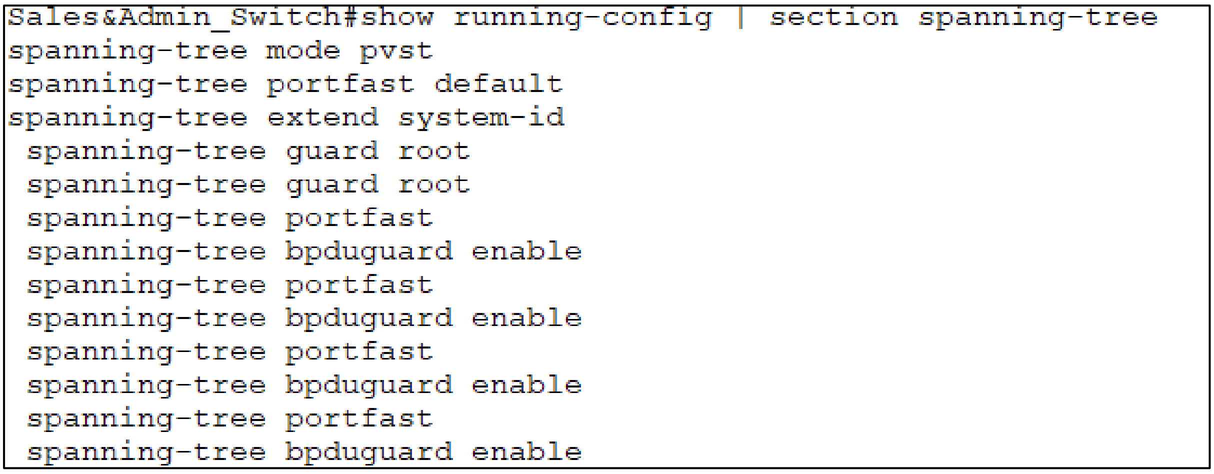
To protect SG branch network from MAC Address Flooding, port security must be configured to ensure that only a certain number of MAC addresses can be learnt on the switchport. As seen in Figure10.1, port security has been configured on all access ports to limit the number of MAC addresses and has been set with the violation level "Shutdown." If a violation occurs, the port will automatically shut down to prevent further attacks.



```
Delivery-Switch#sh ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
130
Insertion of option 82 is disabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                  Trusted    Rate limit (pps)
-----------------------    -------    ----------------
FastEthernet0/3            no         unlimited
FastEthernet0/2            no         unlimited
FastEthernet0/5            yes        unlimited
FastEthernet0/1            no         unlimited
FastEthernet0/4            yes        unlimited
FastEthernet0/6            yes        unlimited
Delivery-Switch#sh ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  -----------------
00:E0:F7:6B:3A:BA   192.168.12.11    0           dhcp-snooping  130   FastEthernet0/3
00:60:3E:2A:B9:AC   192.168.12.13    0           dhcp-snooping  130   FastEthernet0/1
00:0C:85:72:C8:4B   192.168.12.12    0           dhcp-snooping  130   FastEthernet0/2
Total number of bindings: 3
```

Figure 10.2.2 – show ip dhcp snooping

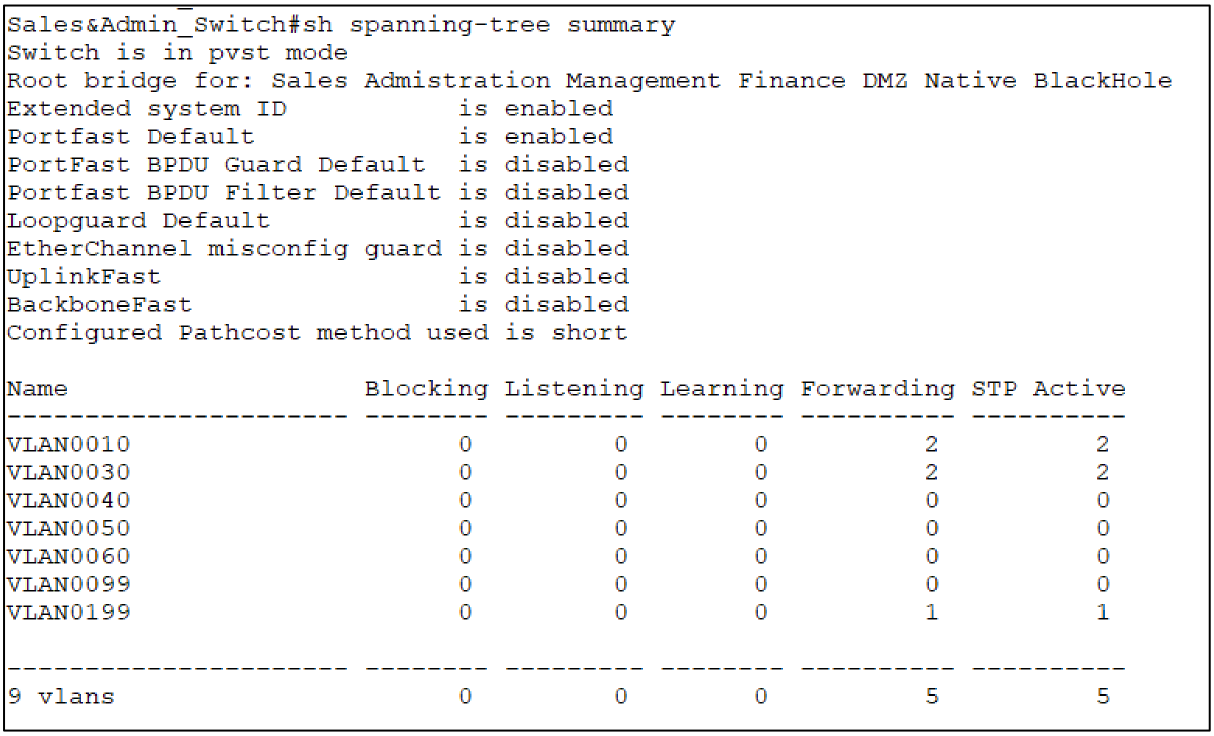
As seen in Figure 10.2.2, by using “show ip dhcp snooping” command indicates uplink interfaces Fa0/4-6 were configured as trusted ports which allowing legitimate DHCP offers from the authorized DHCP server to pass through. All access port like interfaces Fa0/1-3 were set as untrusted, when any fake DHCP replies from and devices will be dropped automatically. Furthermore, “sh ip dhcp binding” command indicates that three legitimate DHCP client bindings with MAC Address, IP Address, VLAN, and Interface. These verifies that only authorized DHCP transactions were recorded, preventing any fake DHCP server from accessing malicious IP information to clients.



```
Sales&Admin_Switch#show running-config | section spanning-tree
spanning-tree mode pvst
spanning-tree portfast default
spanning-tree extend system-id
 spanning-tree guard root
 spanning-tree guard root
 spanning-tree portfast
 spanning-tree bpduguard enable
 spanning-tree portfast
 spanning-tree bpduguard enable
 spanning-tree portfast
 spanning-tree bpduguard enable
 spanning-tree portfast
 spanning-tree bpduguard enable
```

Figure 10.2.3 – BPDUGuard enable

From the Figure 10.3, by using “show running-config | section spanning tree” command shows spanning-tree settings have been issued.



```
Sales&Admin_Switch#sh spanning-tree summary
Switch is in pvst mode
Root bridge for: Sales Admistration Management Finance DMZ Native BlackHole
Extended system ID           is enabled
Portfast Default             is enabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is disabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0010                     0         0        0          2          2
VLAN0030                     0         0        0          2          2
VLAN0040                     0         0        0          0          0
VLAN0050                     0         0        0          0          0
VLAN0060                     0         0        0          0          0
VLAN0099                     0         0        0          0          0
VLAN0199                     0         0        0          1          1

---------------------- -------- --------- -------- ---------- ----------
9 vlans                      0         0        0          5          5
```

Figure 10.2.4 – show spanning-tree summary

As seen in Figure 10.3.2, by using "sh spanning-tree summary" command indicates this switch operating in Per-VLAN Spanning Tree (PVST) mode, and the root bridge for multiple VLANs including Sales, Adminstration, Management, Finance, DMZ, and BlackHole VLANs. The PortFast is enabled and BPDU Guard recommended on access ports to prevent fake root election. Therefore, by combining PortFast and BPDU Guard configuration on access interfaces protect network from STP Attack.

4.11 Bastion Host

4.11.1 Question

Bastion host works as an application proxy. You are required to explain the solution in detail. (Configuration is not required.).

4.11.2 Solution

In the modern enterprise network security architecture, the Bastion Host plays a crucial role in security protection. As a hardened intermediary proxy server, it is designed to provide a controlled, auditable and secure connections between the internal network and external access. When the Bastion Host is deployed in the form of an Application Proxy, it not only isolates the internal system from external threats, but also perform authentication, access control and traffic auditing at the application layer, thereby building a multi-layered defence-in-depth system.

1. Reverse Proxy

Bastion host can act as a Reverse Proxy within the DMZ zone to protect the enterprise's public services such as Web, API or email. All external traffic must first pass through the bastion host for protocol parsing and security checks, such as TLS termination, application layer filtering, malicious request blocking and rate limiting. This action can effectively defend against common Web attacks while concealing the real internal server information and reducing the risk of direct attacks.

2. Jump Server Proxy

Bastion host can act as a secure Jump Server Proxy for administrators to access internal devices. Through centralised authentication mechanisms such as multi-factor authentication (MFA) and role-based access control (RBAC), all remote management operations are routed via the bastion proxy. The system will automatically record command logs and session recording to enable comprehensive operation auditing and traceability. This approach not only prevents the risk of administrator credential leakage but also ensures that all accesses are conducted in a controlled and monitorable environment.

3. Integrate Content Detection and Data Leakage Prevention (DLP) Proxy

Bastion host can also integrate content detection and data leakage prevention (DLP) proxy functions to perform deep content checks and sensitive information identification on uploaded and downloaded data packets. By matching file characteristics, keywords or regular rules, the system can automatically block content containing confidential information during transmission to prevent sensitive data from being leaked to unauthorized channels.

4.12 WAN Conectivity

4.12.1 Question

Connectivity between HQ in KL and branch office in Singapore is a requirement. Other than OSPF, discuss any other routing protocol that can be used for WAN connectivity. What is the best solution? Elaborate on the solution. (Configuration is not required FOR BGP).

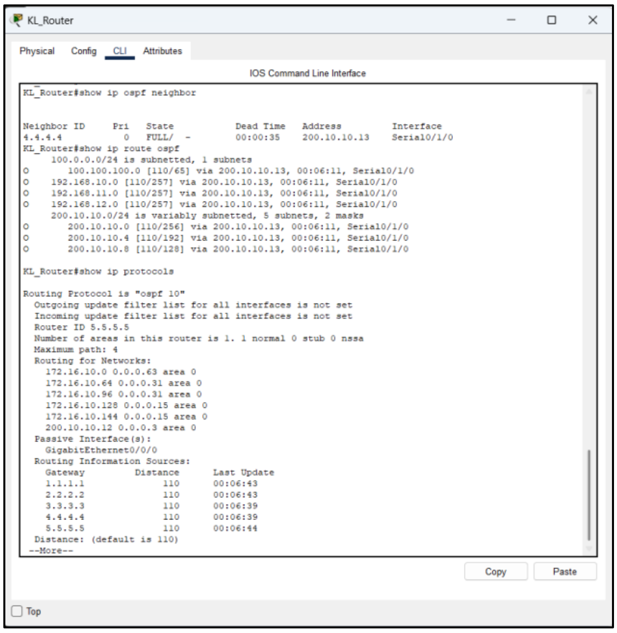
4.12.2 Solution

In this design, **OSPF** (Open Shortest Path First) is implemented as the main internal routing protocol for both sites.
It provides fast convergence, loop-free topology, and dynamic route learning between VLANs and routers within each location.

For WAN connectivity between KL and SG, **BGP** (Border Gateway Protocol) is discussed as an alternative and complementary protocol. **BGP** operates between autonomous systems (AS) and is designed for large-scale WAN or Internet-based routing. It is a highly scalable and suitable for large networks that making it an ideal choice for wide area networks (WANs) and inter-site connectivity. It supports policy-based routing, enabling administrators to control how routes are advertised or selected. BGP is robust and reliable, it will sending updates only when changes occur, thus reducing bandwidth usage. Other than that, it also supports redundancy and loop prevention, to ensuring consistent and secure inter-site communication.

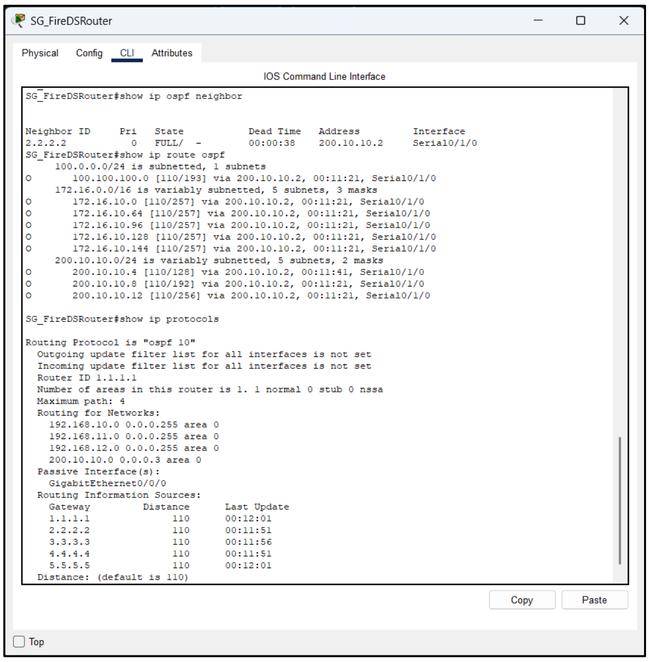
The best solution for WAN connectivity between the KL and the SG network is to use OSPF for internal routing and BGP for external WAN communication. OSPF can provides fast convergence and efficient dynamic routing within each site, BGP can offers scalability, policy control, and stability for inter-site or multi-ISP connections. This hybrid approach ensures that both internal and external networks are operate efficiently and securely, allowing the organization to maintain reliable connectivity while supporting future expansion.

4.12.3 Configuration:



```
KL_Router#show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
4.4.4.4           0   FULL/  -        00:00:35    200.10.10.13    Serial0/1/0
KL_Router#show ip route ospf
     100.0.0.0/24 is subnetted, 1 subnets
O       100.100.100.0 [110/65] via 200.10.10.13, 00:06:11, Serial0/1/0
O    192.168.10.0 [110/257] via 200.10.10.13, 00:06:11, Serial0/1/0
O    192.168.11.0 [110/257] via 200.10.10.13, 00:06:11, Serial0/1/0
O    192.168.12.0 [110/257] via 200.10.10.13, 00:06:11, Serial0/1/0
     200.10.10.0/24 is variably subnetted, 5 subnets, 2 masks
O       200.10.10.0 [110/256] via 200.10.10.13, 00:06:11, Serial0/1/0
O       200.10.10.4 [110/192] via 200.10.10.13, 00:06:11, Serial0/1/0
O       200.10.10.8 [110/128] via 200.10.10.13, 00:06:11, Serial0/1/0

KL_Router#show ip protocols

Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 5.5.5.5
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.10.0 0.0.0.63 area 0
    172.16.10.64 0.0.0.31 area 0
    172.16.10.96 0.0.0.31 area 0
    172.16.10.128 0.0.0.15 area 0
    172.16.10.144 0.0.0.15 area 0
    200.10.10.12 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:06:43
    2.2.2.2              110      00:06:43
    3.3.3.3              110      00:06:39
    4.4.4.4              110      00:06:39
    5.5.5.5              110      00:06:44
  Distance: (default is 110)
 --More--
```

Figure 4.12.3.1 Show ospf configuration of KL_Router



```
SG_FireDSRouter#show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           0   FULL/  -        00:00:38    200.10.10.2     Serial0/1/0
SG_FireDSRouter#show ip route ospf
     100.0.0.0/24 is subnetted, 1 subnets
O       100.100.100.0 [110/193] via 200.10.10.2, 00:11:21, Serial0/1/0
     172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
O       172.16.10.0 [110/257] via 200.10.10.2, 00:11:21, Serial0/1/0
O       172.16.10.64 [110/257] via 200.10.10.2, 00:11:21, Serial0/1/0
O       172.16.10.96 [110/257] via 200.10.10.2, 00:11:21, Serial0/1/0
O       172.16.10.128 [110/257] via 200.10.10.2, 00:11:21, Serial0/1/0
O       172.16.10.144 [110/257] via 200.10.10.2, 00:11:21, Serial0/1/0
     200.10.10.0/24 is variably subnetted, 5 subnets, 2 masks
O       200.10.10.4 [110/128] via 200.10.10.2, 00:11:41, Serial0/1/0
O       200.10.10.8 [110/192] via 200.10.10.2, 00:11:21, Serial0/1/0
O       200.10.10.12 [110/256] via 200.10.10.2, 00:11:21, Serial0/1/0

SG_FireDSRouter#show ip protocols

Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.10.0 0.0.0.255 area 0
    192.168.11.0 0.0.0.255 area 0
    192.168.12.0 0.0.0.255 area 0
    200.10.10.0 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:12:01
    2.2.2.2              110      00:11:51
    3.3.3.3              110      00:11:56
    4.4.4.4              110      00:11:51
    5.5.5.5              110      00:12:01
  Distance: (default is 110)
```

Figure 4.12.3.2 Show ospf configuration of SG_FireDSRouter

Above indicates that OSPF adjacency between KL and SG routers is established and confirms OSPF has learned remote networks dynamically. The "**show ip protocols**" command is to confirms that OSPF is currently the active dynamic routing protocol.

4.13 Crypto System

4.13.1 Question

Data transmitted over the network must be kept disguised and only intended recipient can read it. Hackers are unable to understand the content even they can wiretap the communication. (Solution on the techniques, no configuration is required)

4.13.2 Solution

A cryptosystem is a set of protocols, procedures, and keys that encrypt readable information (plaintext) to make it unreadable (ciphertext), such that the information can be read and understood only by the authorized receivers. The encryption keeps the information secret even though the information is intercepted during attacks. The receiver decodes the information with a similar decryption key to regain the original communication. Without the correct decryption key, any intercepted information remains illegible (Stallings, 2017; algoTRIC, 2024).

Cryptosystems are usually categorized as symmetric and asymmetric systems. Symmetric-key cryptography employs a single secret key to encrypt as well as decrypt, with fast efficient security through the use of Advanced Encryption Standard (AES) and Data Encryption Standard (DES). However, it suffers from the inability to distribute the key securely. Asymmetric-key cryptography involves the use of two mathematically connected keys, a public key to encrypt and a private key to decrypt, typically used in RSA and Diffie-Hellman key exchange. This approach overcomes the distribution of the key difficulty and includes digital authentication (Stallings, 2017).

The most recent developments, as identified in algoTRIC (2024), enhance cryptosystem performance with the integration of symmetric and asymmetric techniques in hybrid schemes of encryption. The systems benefit from the speed of symmetric encryption combined with the sturdy security of the asymmetric key exchange. AlgoTRIC also focuses on enhanced key management and flexible encryption schemes that enhance resistance to existing threats in the cyber world, such as quantum-enabled attacks as well as side-channel attacks (algoTRIC, 2024). In the case of Net Secure Solutions, the use of TLS/SSL in web communication combined with the use of VPN encryption on the Kuala Lumpur-Singapore inter-branch connection will be enough to hide the data that is being passed. Even if hackers wiretap the communication, the encrypted data will be uninterpretable to them (Stallings, 2017; algoTRIC, 2024).

4.14 Intrusion detection systems (IDS).

4.14.1 Question

The company requires implementing intrusion detection systems (IDS). (No Configuration is required.)

4.14.2 Solution

An Intrusion Detection System (IDS) is a critical security solution designed to monitor, detect, and alert administrators about unauthorized or abnormal network activities. Unlike firewalls, which prevent attacks by blocking traffic, an IDS focuses on analysing network packets to identify potential security breaches such as malware infections, denial-of-service (DoS) attempts, or unauthorized access within both internal and external networks.

There are two main types of IDS:

- Network-based IDS (NIDS): Monitors network traffic in real time and can be strategically placed at key points such as between the internal LAN, DMZ, or WAN connection to detect suspicious external activities.
- Host-based IDS (HIDS): Installed directly on servers or endpoints to monitor system processes, log files, and application behaviours for abnormal patterns or unauthorized actions.

For the company, a hybrid IDS approach is recommended. A NIDS should be deployed at the KL_Router and SG_FireDSRouter to detect external threats, while HIDS should be installed on critical servers such as those used by the Finance or Management departments to protect sensitive information. This layered IDS implementation provides comprehensive visibility and detection across the entire network, enabling administrators to respond quickly to potential intrusions and minimize the risk of data breaches or system compromise.

4.15 VPN

4.15.1 Question

Implement VPN between KL and Singapore network. (Solution and configuration.)

4.15.2 Solution

The verification confirms that the Site-to-Site IPsec VPN between KL and SG routers is successfully established.

Phase 1: ISAKMP (Internet Security Association and Key Management Protocol)

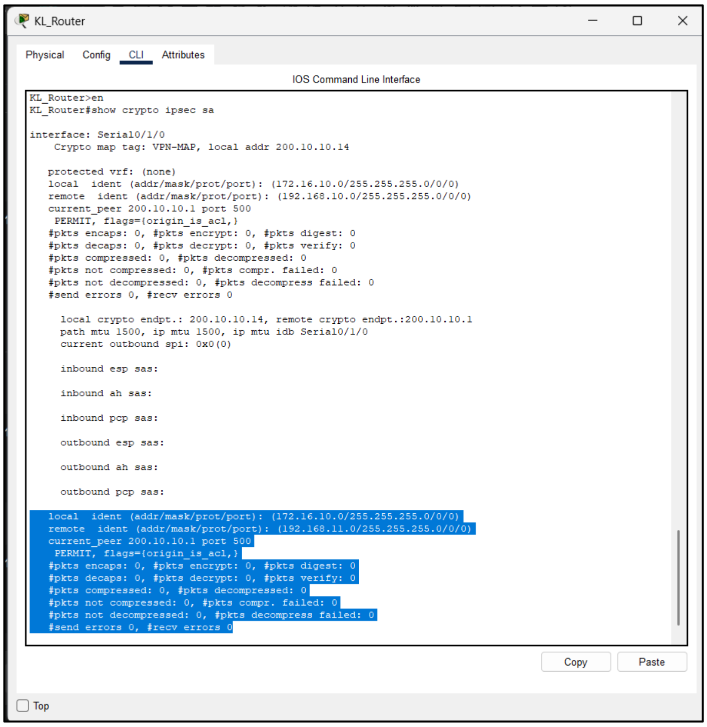
- Defines the encryption, authentication, and Diffie-Hellman key exchange parameters.
- Creates a Security Association (SA) between KL and SG routers to authenticate both sides.
- Both routers share a pre-shared key for authentication.

Phase 2: IPsec Configuration

- Defines the transform set used for data encryption (ESP-3DES) and integrity (ESP-SHA-HMAC).
- A crypto map is created to bind all IPsec parameters and specify the peer.

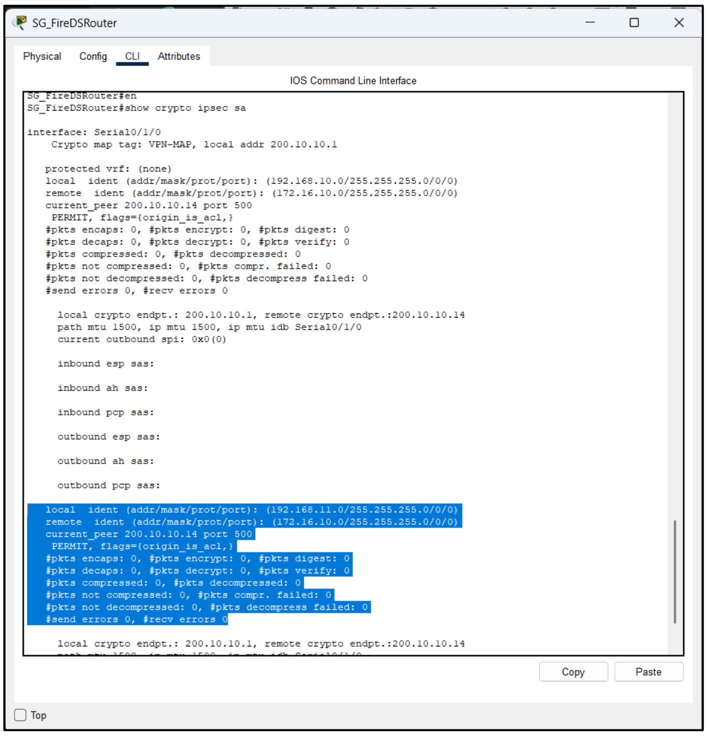
This implementation enhances data confidentiality, integrity, and security for communication between the headquarters and the branch, ensuring safe WAN connectivity even over untrusted public networks.

4.15.3 Configure



```
KL_Router>en
KL_Router#show crypto ipsec sa

interface: Serial0/1/0
    Crypto map tag: VPN-MAP, local addr 200.10.10.14

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (172.16.10.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
   current_peer 200.10.10.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 200.10.10.14, remote crypto endpt.:200.10.10.1
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0
     current outbound spi: 0x0(0)

     inbound esp sas:

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:

     outbound ah sas:

     outbound pcp sas:

   local  ident (addr/mask/prot/port): (172.16.10.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.11.0/255.255.255.0/0/0)
   current_peer 200.10.10.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0
```

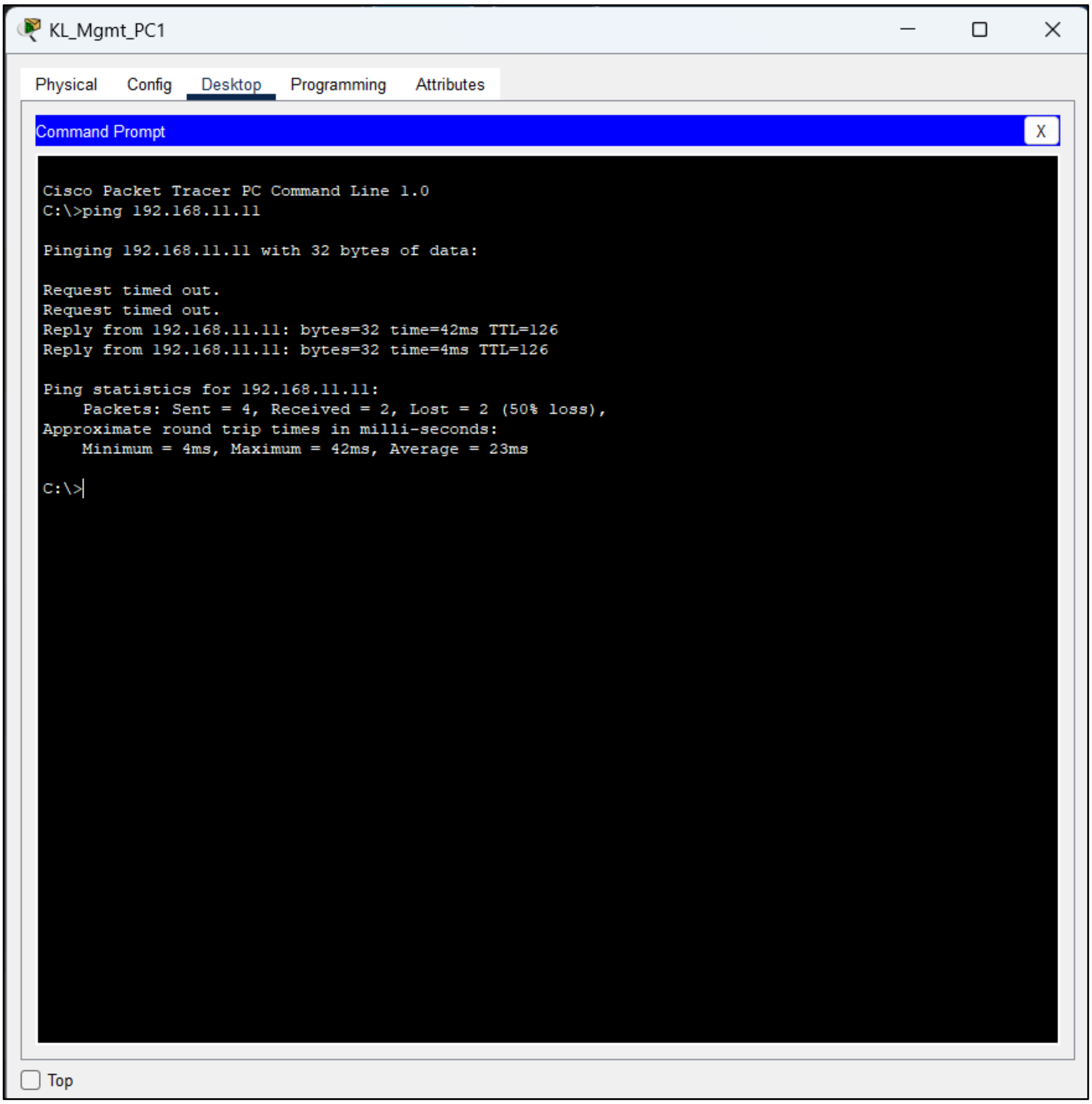
Figure 4.15.3.1 show crypto ipsec sa before pinging(KL_Router)



```
SG_FireDSRouter#en
SG_FireDSRouter#show crypto ipsec sa

interface: Serial0/1/0
    Crypto map tag: VPN-MAP, local addr 200.10.10.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (172.16.10.0/255.255.255.0/0/0)
   current_peer 200.10.10.14 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 200.10.10.1, remote crypto endpt.:200.10.10.14
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0
     current outbound spi: 0x0(0)

     inbound esp sas:

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:

     outbound ah sas:

     outbound pcp sas:

   local  ident (addr/mask/prot/port): (192.168.11.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (172.16.10.0/255.255.255.0/0/0)
   current_peer 200.10.10.14 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 200.10.10.1, remote crypto endpt.:200.10.10.14
```

Figure 4.15.3.2 show crypto ipsec sa before pinging(SG_FireDSRouter)

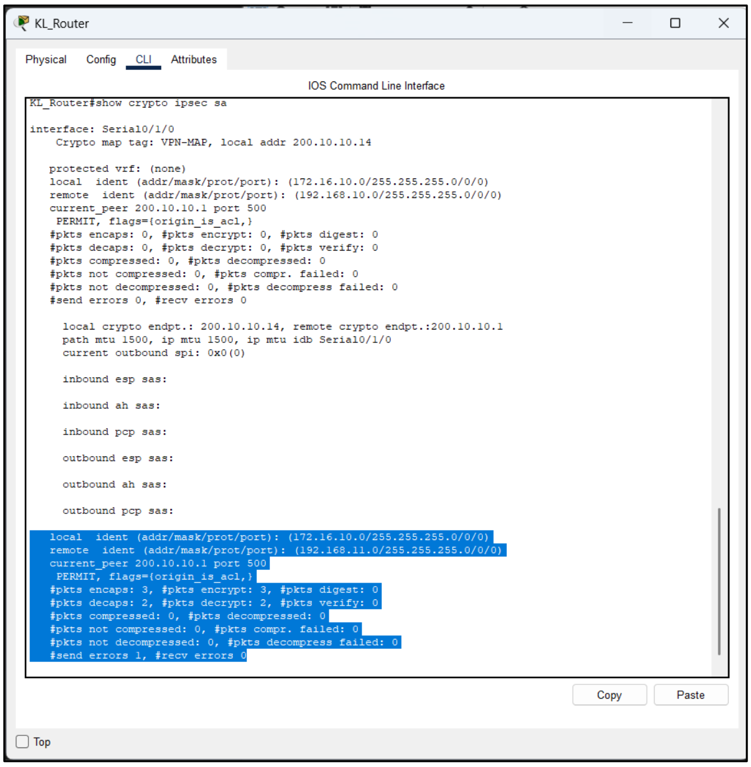
Above indicates that the tunnel at KL_Router and SG_FireDSRouter is configured correctly but not yet active, since no interesting traffic has triggered it. Issue the "**show crypto ipsec sa**" command on KL_Router and SG_FireDSRouter, we can notice that the number of packets encapsulated, encrypted, decapsulated and decrypted are all set to 0.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.11.11

Pinging 192.168.11.11 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 192.168.11.11: bytes=32 time=42ms TTL=126
Reply from 192.168.11.11: bytes=32 time=4ms TTL=126

Ping statistics for 192.168.11.11:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 42ms, Average = 23ms

C:\>
```

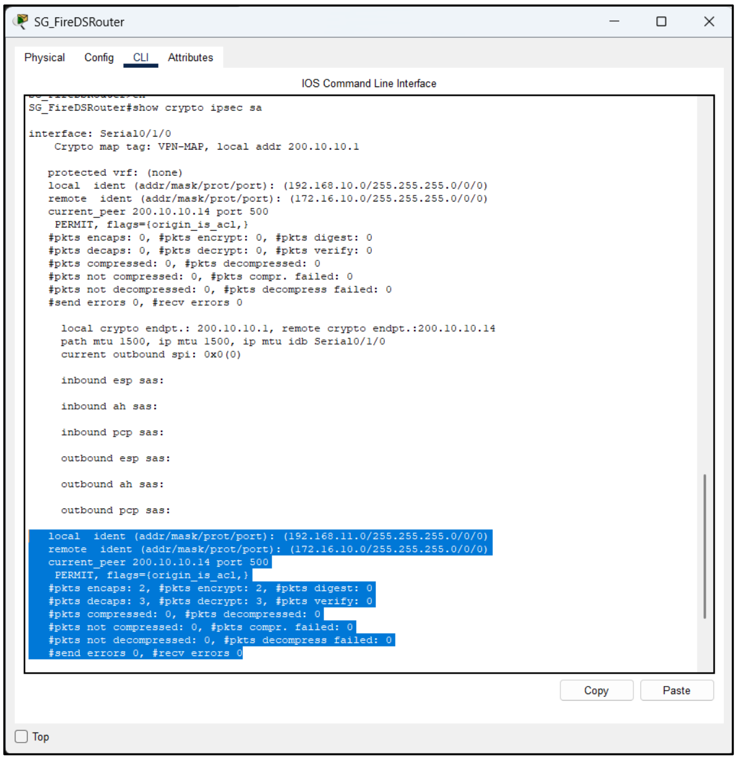
Figure 4.15.3.3 Test ping form KL_Mgmt_PC1 to SG_Mgmt_PC1

Now we try to ping from **KL_Mgmt_PC1** to **SG_Mgmt PC1(192.168.11.11).**



```
KL_Router#show crypto ipsec sa

interface: Serial0/1/0
    Crypto map tag: VPN-MAP, local addr 200.10.10.14

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (172.16.10.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
   current_peer 200.10.10.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 200.10.10.14, remote crypto endpt.:200.10.10.1
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0
     current outbound spi: 0x0(0)

     inbound esp sas:

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:

     outbound ah sas:

     outbound pcp sas:

   local  ident (addr/mask/prot/port): (172.16.10.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.11.0/255.255.255.0/0/0)
   current_peer 200.10.10.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 0
   #pkts decaps: 2, #pkts decrypt: 2, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 1, #recv errors 0
```

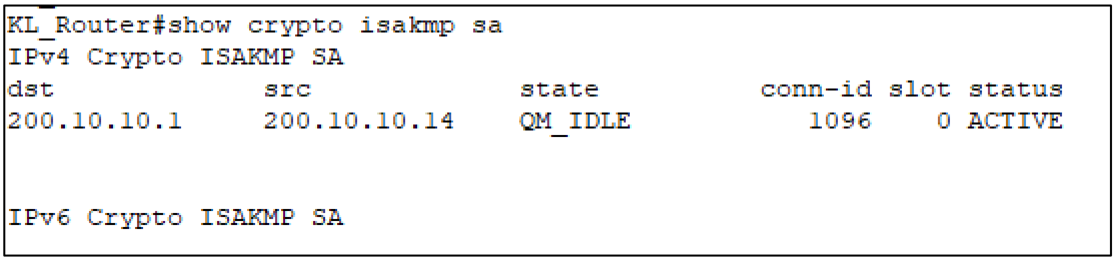
Figure 4.15.3.4 show crypto ipsec sa after pinging(KL_Router)



```
SG_FireDSRouter#show crypto ipsec sa

interface: Serial0/1/0
    Crypto map tag: VPN-MAP, local addr 200.10.10.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (172.16.10.0/255.255.255.0/0/0)
   current_peer 200.10.10.14 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 200.10.10.1, remote crypto endpt.:200.10.10.14
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0
     current outbound spi: 0x0(0)

     inbound esp sas:

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:

     outbound ah sas:

     outbound pcp sas:

   local  ident (addr/mask/prot/port): (192.168.11.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (172.16.10.0/255.255.255.0/0/0)
   current_peer 200.10.10.14 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 2, #pkts encrypt: 2, #pkts digest: 0
   #pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0
```

Figure 4.15.3.5 show crypto ipsec sa after ping(SG_FireDSRouter)

And next step, we can issue **“show crypto isakmp sa”** again to confirms that the VPN tunnel is active and now we can see that the number of packets of **Figure 4.15.3.4** and **Figure 1.15.3.5** is more than 0 indicating that the IPsec VPN tunnel is working.



```
KL_Router#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
200.10.10.1     200.10.10.14    QM_IDLE           1096    0 ACTIVE


IPv6 Crypto ISAKMP SA
```

Figure 4.15.3.6

The “**show crypto isakmp sa**” command is to indicates the ISAKMP Security Association is established, and the VPN tunnel is stable and active.

4.16 SSL

4.16.1 Question

Implement SSL encryption between KL and Singapore. (Solution).

4.16.2 Solution

By implementing SSL between KL and Singapore branches, SSL (or its modern successor, TLS) could secure the communication between them by end-to-end encryption and ensure confidentiality, integrity and authorisation between the data transmissions.

In this solutions, NetSecure Solutions should use a valid digital certificate issued by trusted CA(Certificate Authority) to enable DMZ Web Server HTTPS service. This certificate contains server's public key and verify the server identity to prevent it from Man-in-the-Middle (MitM) attacks. Both clients from KL and Singapore branch could access the website by using SSL encrypted connection, ensure that all the data transmitted remains private and not altered.

Other than that, the routers and firewall on both branches should only permit HTTPS (port 443) traffic while blocking HTTP (port 80) traffic. This is because HTTPS is more secured (with a lock icon beside the https:// if is authorised) than HTTP. To enhance a strong and better community security, the best way should NetSecure Solution do is to use SSL encryption algorithms and regular updating digital certificates.The SSL configuration should disable the weak cyphers and use strong ciphers like AES-256.

In a nutshell, implementing SSL between KL and Singapore branches together with network control measures and certificte management could maintain the confidentiality, intergrity and autheticity between the cross-branch communications.

4.17 Three Solution Security Network

4.17.1 Question

Proposed THREE (3) other solutions to increase the security in both networks. (Solution)

4.17.2 Solution

1. Honeypot (Deception System)

Honeypot work as a baiting trap for hackers. It is a sacrificial computer system designed to act as bait to attract hackers. It simulates a hacker's target and exploits their intrusion attempts to gain information about the cybercriminals and their methods or to distract them from other targets. From this network, place a honeypot in the DMZ or a separate VLAN to simulate a web server, database or IoT device. It will forward honeypot logs to the security team or logging server. To implement this honeypot to identify external and internal attackers. It collects attack techniques for future defence and adds extra layer of deception and protection on this network.

2. Network Access Control (802.1X NAC)

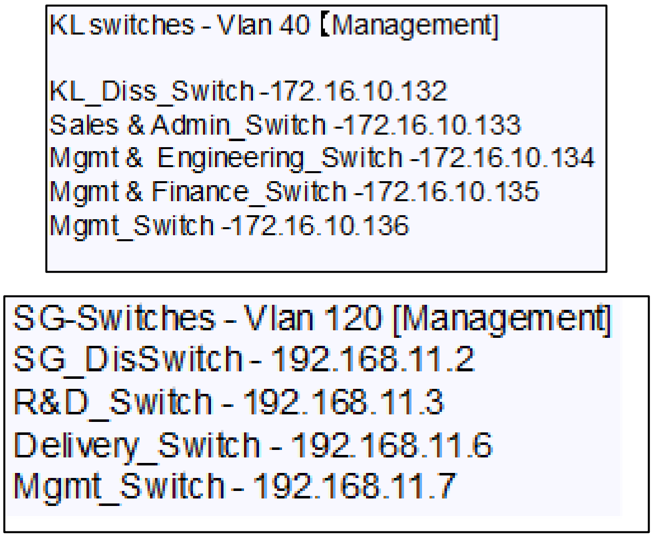
Network Access Control (NAC) using 802.1X requires every device to authenticate like username and password before joining the network. The switch or wireless access point acts as authenticator and only allows access to the correct VLAN after successful authentication. If unauthorized devices plug into LAN ports or connect to wireless networks, Network Access Control can block unknown device to protect internal VLANs.

3. Centralized Logging with SIEM

Centralized logging with a Security Information and Event Management (SIEM) system in networking is collecting log data from network devices such as router, firewalls, switches, and servers to generate security logs. It centralized logging in one place, analyses patterns, and alert administrators in real time when suspicious activity occurs. It faster detection of attacks and easier troubleshooting and auditing.

5.0 Documentation of the configured devices

5.1 Switches IP Address



KL switches - Vlan 40 【Management]

KL_Diss_Switch -172.16.10.132
Sales & Admin_Switch -172.16.10.133
Mgmt & Engineering_Switch -172.16.10.134
Mgmt & Finance_Switch -172.16.10.135
Mgmt_Switch -172.16.10.136

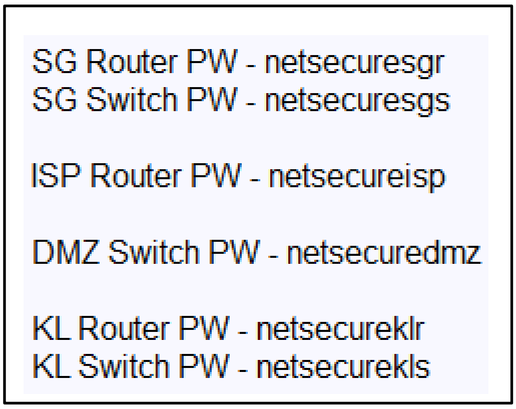
SG-Switches - Vlan 120 [Management]
SG_DisSwitch - 192.168.11.2
R&D_Switch - 192.168.11.3
Delivery_Switch - 192.168.11.6
Mgmt_Switch - 192.168.11.7

Figure 5.1.1 Switches IP in KL and Singapore

Both switches in KL and Singapore branches are configured statically with reserved IP address (excluded range in the router IP DHCP) in Management VLAN, which is VLAN 40 in KL and VLAN 120 in Singapore.

5.2 Enable Password

The enable secret password was configured on all routers and switches to protect privileged EXEC mode access. This encrypted password helps prevent unauthorized configuration changes and provides a secure foundation for subsequent network implementation.



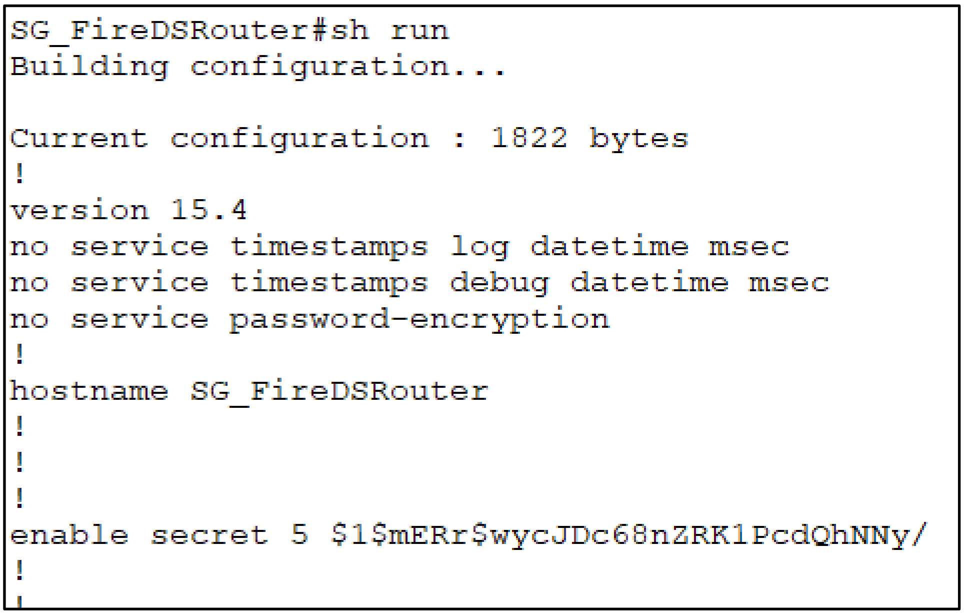
SG Router PW - netsecuresgr
SG Switch PW - netsecuresgs

ISP Router PW - netsecureisp

DMZ Switch PW - netsecuredmz

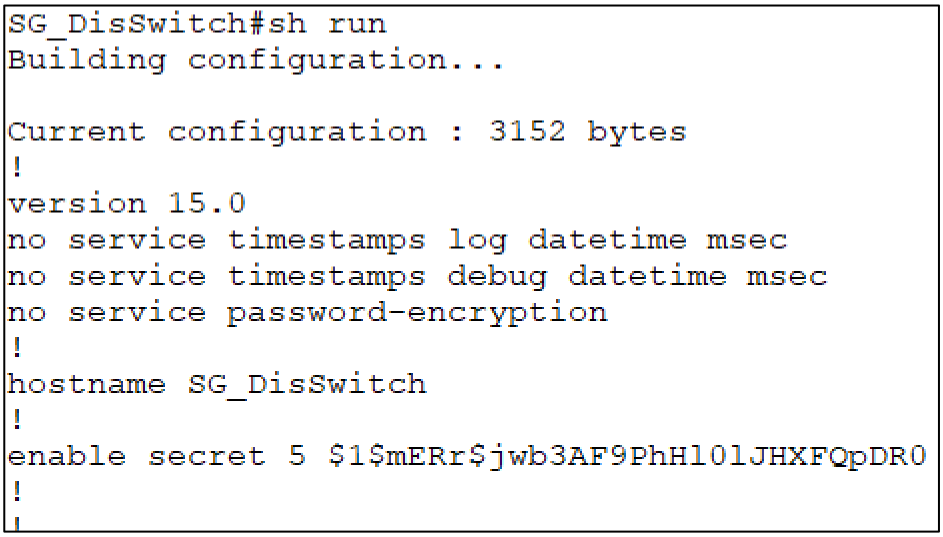
KL Router PW - netsecureklr
KL Switch PW - netsecurekls

Figure 5.2.1 – Password of each Device



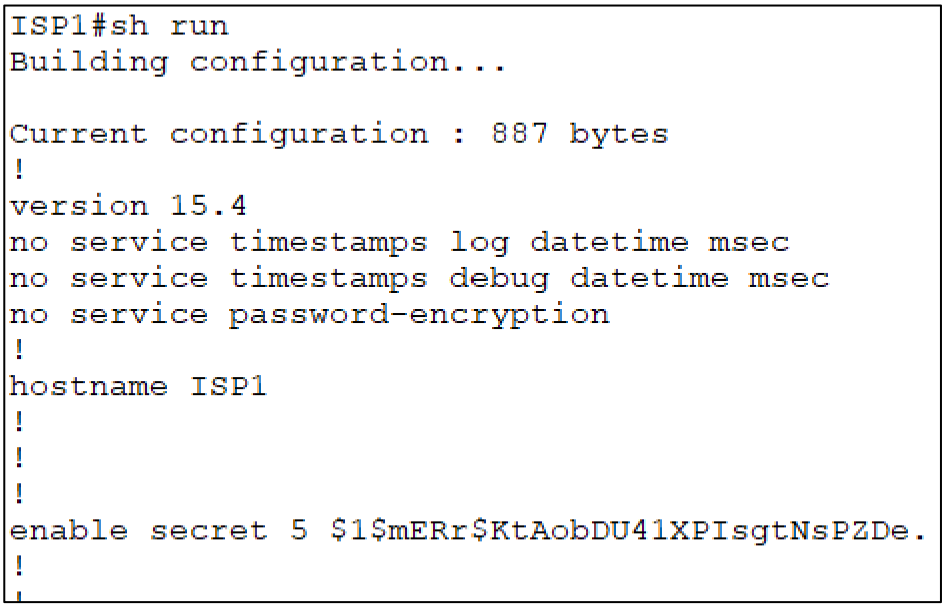
```
SG_FireDSRouter#sh run
Building configuration...

Current configuration : 1822 bytes
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SG_FireDSRouter
!
!
!
enable secret 5 $1$mERr$wycJDc68nZRK1PcdQhNNy/
!
!
```

Figure 5.2.2 - Singapore router



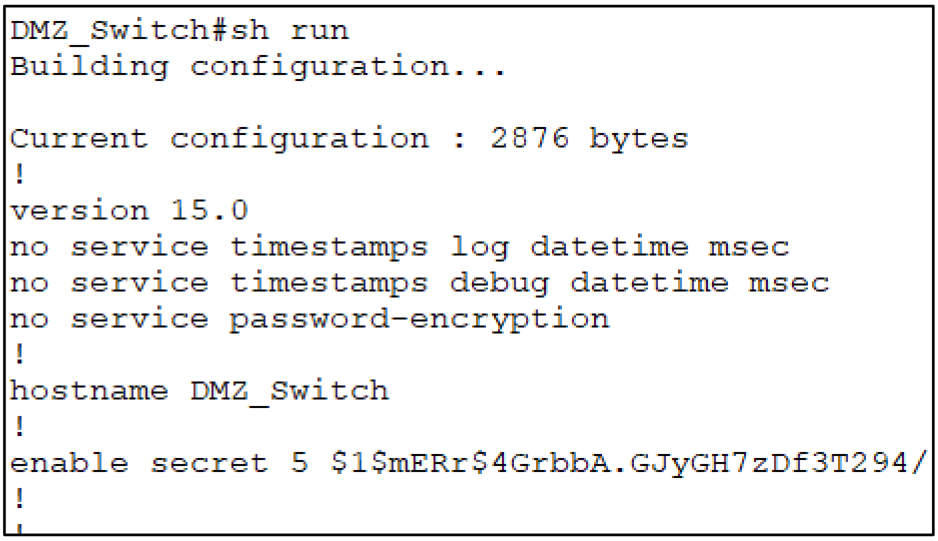
```
SG_DisSwitch#sh run
Building configuration...

Current configuration : 3152 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SG_DisSwitch
!
enable secret 5 $1$mERr$jwb3AF9PhHl0lJHXFQpDR0
!
!
```

Figure 5.2.3 - Singapore switch



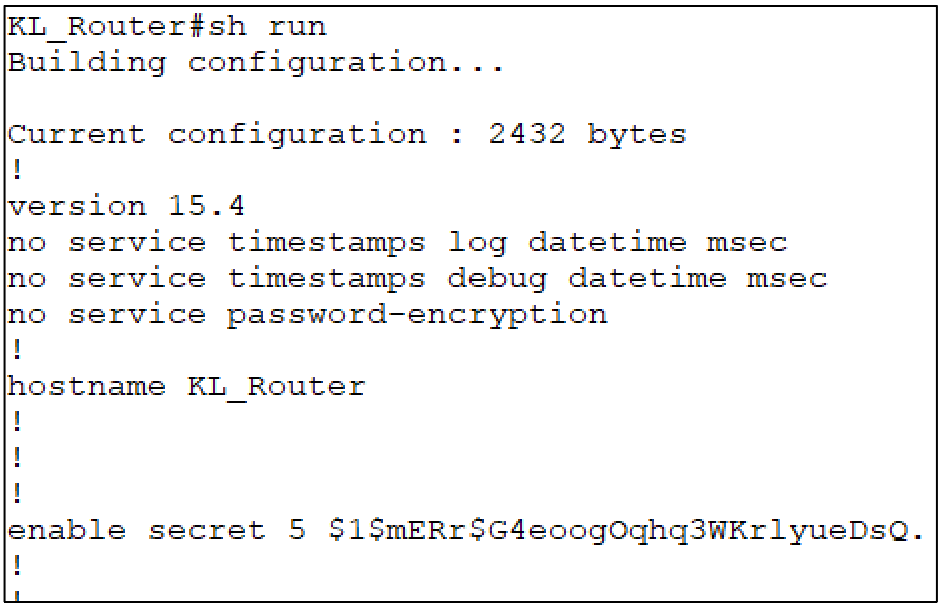
```
ISP1#sh run
Building configuration...

Current configuration : 887 bytes
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname ISP1
!
!
!
enable secret 5 $1$mERr$KtAobDU41XPIsgtNsPZDe.
!
!
```

Figure 5.2.4 - ISP router



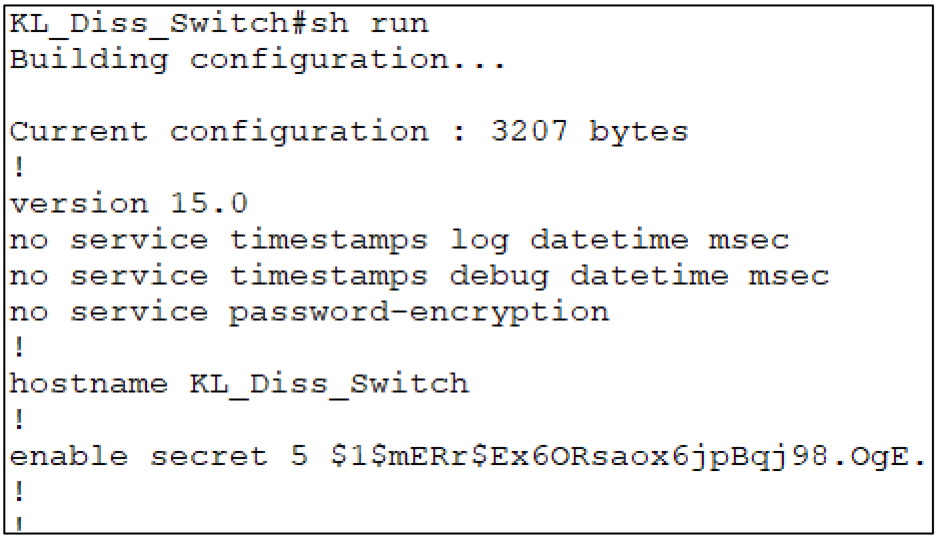
```
DMZ_Switch#sh run
Building configuration...

Current configuration : 2876 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname DMZ_Switch
!
enable secret 5 $1$mERr$4GrbbA.GJyGH7zDf3T294/
!
!
```

Figure 5.2.5- DMZ Switch



```
KL_Router#sh run
Building configuration...

Current configuration : 2432 bytes
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname KL_Router
!
!
!
enable secret 5 $1$mERr$G4eoogOqhq3WKrlyueDsQ.
!
!
```

Figure 5.2.6 - KL Router



```
KL_Diss_Switch#sh run
Building configuration...

Current configuration : 3207 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname KL_Diss_Switch
!
enable secret 5 $1$mERr$Ex6ORsaox6jpBqj98.OgE.
!
!
```

Figure 5.2.7 - KL Switch

6.0 Conclusion

In conclusion, this assignment successfully demonstrated NetSecure Solutions' design and configuration of a secure and scalable enterprise network infrastructure, integrating the Kuala Lumpur headquarters and Singapore branch. Throughout the implementation, we configured various network services and security mechanisms, such as VLAN segmentation, ACLs, DHCP automation, wireless protection, and VPN tunnels, to ensure the confidentiality, integrity, and availability of company resources.

Layer 2 and Layer 3 security features effectively reduce insider threats such as MAC flooding, DHCP spoofing and ACLs also enforce strict cross-office access control based on the principle of least privilege. VPN and SSL encryption secure data transmission between branch offices, ensuring the privacy of sensitive communications even over public networks. Furthermore, IoT and wireless networks are protected by using WPA2, TLS, and certificate-based authentication to reduce the modern threats such as eavesdropping and spoofing etc.

Integration of the intrusion detection system (IDS) and the network access control (NAC) enable a proactive defence model that will enhance the threat detection and tracking. Such controls provide a multi-layered defence architecture that hardens the organisation's resistance to insider and outsider attacks.

7.0 References

GeeksforGeeks. (2018, March 26). *Virtual LAN (VLAN)*. GeeksforGeeks. https://www.geeksforgeeks.org/computer-networks/virtual-lan-vlan/

GeeksforGeeks. (2019, June 10). *Secure Socket Layer (SSL)*. GeeksforGeeks. https://www.geeksforgeeks.org/computer-networks/secure-socket-layer-ssl/

GeeksforGeeks. (2020, September 20). *What is AWS Bastion Host*. GeeksforGeeks. https://www.geeksforgeeks.org/blogs/what-is-aws-bastion-host/

GeeksforGeeks. (2025, October). *IoT Devices Vulnerability and Attack Vectors*. GeeksforGeeks. https://www.geeksforgeeks.org/ethical-hacking/iot-devices-vulnerability-and-attack-vectors/

Intrusion Detection Systems (IDS): Definition, Types, Purpose | Splunk. (2025). Splunk. https://www.splunk.com/en_us/blog/learn/ids-intrusion-detection-systems.html

Jannik. (2022, June 14). DHCP Attack + WPAD. ProSec GmbH. https://www.prosec-networks.com/en/blog/dhcp-attacks-wpad/

Johnson, B. (2022, December 13). *What is a Bastion Host?* Www.strongdm.com. https://www.strongdm.com/what-is/bastion-host

Notter, R. (2018, October 13). *802.11w-2009 – Protected Management Frames (PMF): Overview and lab tests*. dot11 exposed. https://dot11.exposed/2018/10/13/802-11w-2009-protected-management-frames-pmf-overview-and-lab-tests/

Scarfone, K. A., & Mell, P. M. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS). Guide to Intrusion Detection and Prevention Systems (IDPS). https://doi.org/10.6028/nist.sp.800-94

Souppaya, M., & Scarfone, K. (2012, February). *Guidelines for securing wireless local area networks (WLANs) (NIST SP 800-153)*. National Institute of Standards and Technology. https://csrc.nist.gov/pubs/sp/800/153/final

Stallings, W. (2017). *Cryptography and network security: Principles and practice* (7th ed.). Pearson. Retrieved from http://staff.ustc.edu.cn/~mfy/moderncrypto/crypto7ed.pdf

Xcitium Software. (2025). Xcitium Blog. https://www.xcitium.com/blog/network/what-is-iot-network/

Kshetri, N., Rahman, M. M., Rana, M. M., Osama, O. F., & Hutson, J. (2024). AlgOTRIC: Symmetric and Asymmetric Encryption Algorithms for Cryptography – A Comparative Analysis in AI Era. *International Journal of Advanced Computer Science and Applications*, *15*(12). https://thesai.org/Downloads/Volume15No12/Paper_1-algoTRIC_Symmetric_and_Asymmetric_Encryption_Algorithms.pdf