A logo of a globe with yellow rings around it

Description automatically generated

GROUP ASSIGNMENT

SECTION A

TECHNOLOGY PARK MALAYSIA

CT037-3-2-NWS

NETWORK SECURITY

APD2F2409IT(CE)

HAND OUT DATE: 5 MARCH 2025

HAND IN DATE: 27 APRIL 2025

WEIGTAGE: 40%

Group 7

|  |  |  |
| --- | --- | --- |
| No | Name | TP Number |
| 1 | LOW KAI WEN | TP064296 |
| 2 | JEYAKUMAR ANITHA HEMANTH | TP066300 |
| 3 | MUHAMMAD IZZUDDIN SYAHMI BIN ZAKARIA | TP067415 |
| 4 | LEE XUAN YUAN | TP070224 |
| 5 | Dickson Kho Jang Wee | TP063882 |

Table of Contents

[1.0 Introduction 3](#_Toc196689792)

[1.1 Overview of Starcom Asia Sdn Bhd Network 3](#_Toc196689793)

[1.2 Purpose of the Report 3](#_Toc196689794)

[2.0 Work Breakdown Structure 3](#_Toc196689795)

[3.0 Network Topology Design 5](#_Toc196689796)

[3.1 Lan and Wan Topology Overview 5](#_Toc196689797)

[3.1.1 Headquarters(Penag HQ) – Main Office 5](#_Toc196689798)

[3.1.2 DMZ 6](#_Toc196689799)

[3.1.3 Branch Office(Krung Thep, Thailand) 6](#_Toc196689800)

[4.0 IP Addressing Scheme 7](#_Toc196689801)

[4.1 VLAN and Subnet Allocation (VLSM) 7](#_Toc196689802)

[4.1.1 HQ(Penang) 7](#_Toc196689803)

[4.1.2 DMZ 7](#_Toc196689804)

[4.1.3 Branch (Krung Thep, Thailand) 7](#_Toc196689805)

[4.2 Addressing Table 8](#_Toc196689806)

[4.2.1 HQ 8](#_Toc196689807)

[4.2.2DMZ 8](#_Toc196689808)

[4.2.4 Branch 9](#_Toc196689809)

[5.0 Basic Network Configuration 10](#_Toc196689810)

[5.1 HQ 10](#_Toc196689811)

[5.1.1 Vlan 10](#_Toc196689812)

[5.1.2 STP 12](#_Toc196689813)

[5.2 Branch 15](#_Toc196689814)

[5.2.1 Vlan 15](#_Toc196689815)

[5.4 OSPF 17](#_Toc196689816)

[5.5 Verification 22](#_Toc196689817)

[6.0 Conclusion 23](#_Toc196689818)

[7.0 References 24](#_Toc196689819)

# Introduction

A well-structured and secure network infrastructure is the backbone of any modern organization. For Starcom Asia Sdn Bhd, a network cable manufacturing company with headquarters in Penang and a branch office in Krung Thep, Thailand, an efficient and reliable network is crucial for seamless operations and communication. This report focuses on designing a functional network topology for the company, ensuring smooth connectivity between its departments and locations.

## 1.1 Overview of Starcom Asia Sdn Bhd Network

Starcom Asia Sdn Bhd has two main locations: Penang HQ, hosting the Sales, Engineering, and Finance departments, and a branch in Krung Thep with R&D and Delivery teams. The HQ network uses a hierarchical design with access and distribution switches, a firewall, and a DMZ containing web, email, and FTP servers for secure service hosting. A WAN connection links both sites, supporting secure inter-office communication. The network emphasizes segmentation, security, and performance through a well-planned topology and IP addressing strategy.

## 1.2 Purpose of the Report

This report presents a network design for Starcom Asia Sdn Bhd that meets its operational requirements. It covers LAN and WAN topologies, IP addressing using VLSM, and implementation of essential services. The report also reflects the team’s collaborative effort in planning and deploying a secure, scalable, and well-structured network.

# 2.0 Work Breakdown Structure

|  |  |  |
| --- | --- | --- |
| Task / Area | Documentation | Configuration |
| LOW KAI WEN | DHCP, STP, TOPOLOGY, VLSM | DHCP, STP, TOPOLOGY |
| JEYAKUMAR ANITHA HEMANTH | DMZ | DMZ |
| MUHAMMAD IZZUDDIN SYAHMI BIN ZAKARIA | BRANCH VLAN | BRANCH VLAN |
| LEE XUAN YUAN | HQ VLAN, CONCLUSION | HQ VLAN |
| Dickson Kho Jang Wee | OSPF, INTRODUNCTION | OSPF |

# 3.0 Network Topology Design

A computer screen shot of a computer network

AI-generated content may be incorrect.

Figure 3.1 Overview Topology Design

An effective network topology supports secure communication and future scalability. The proposed design links Starcom Asia's Penang HQ and Krung Thep branch with optimized data flow and structured segmentation. It includes three main parts: the Headquarters Network, the Demilitarized Zone (DMZ), and the Branch Office Network.

## 3.1 Lan and Wan Topology Overview

### 3.1.1 Headquarters(Penag HQ) – Main Office

The Penang HQ supports the Sales, Engineering, and Finance departments through a hierarchical network model. Each department connects to Layer 2 access switches, which aggregate to a central distribution switch. A core router manages internal routing and connects the LAN to external networks via a firewall. This router also establishes a secure VPN tunnel for inter-office communication with the Krung Thep branch.

### 3.1.2 DMZ

A DMZ is deployed at HQ to isolate public-facing services. The firewall separates internal resources from external access, hosting DNS, web, FTP, and email servers. This design allows secure internal access while limiting exposure to external threats.

### 3.1.3 Branch Office(Krung Thep, Thailand)

The Krung Thep branch includes R&D and Delivery departments, connected through a Layer 2 switch linked to the Branch Router. This router handles local traffic and establishes a VPN tunnel to HQ, ensuring secure, encrypted data exchange over the WAN.

# 4.0 IP Addressing Scheme

## 4.1 VLAN and Subnet Allocation (VLSM)

### 4.1.1 HQ(Penang)

|  |  |  |  |
| --- | --- | --- | --- |
| VLAN Name | VLAN | Subnet | IP-Range |
| Sales | VLAN10 | 192.168.11.0/24 | 192.168.11.1-192.168.11.254 |
| Engineering | VLAN20 | 192.168.12.0/24 | 192.168.12.1-192.168.12.254 |
| Finance | VLAN30 | 192.168.13.0/24 | 192.168.13.1-192.168.13.254 |
| Native | VLAN100 | N/A | N/A |
| Blackhole | VLAN99 | N/A | N/A |

### 4.1.2 DMZ

|  |  |  |  |
| --- | --- | --- | --- |
| VLAN Name | VLAN | Subnet | IP-Range |
| Server | VLAN10 | 192.168.21.0/24 | 192.168.21.1-192.168.21.254 |
| Blackhole | VLAN99 | N/A | N/A |
| Native | VLAN100 | N/A | N/A |

### 4.1.3 Branch (Krung Thep, Thailand)

|  |  |  |  |
| --- | --- | --- | --- |
| VLAN Name | VLAN | Subnet | IP-Range |
| Delivery | VLAN10 | 192.168.31.0/24 | 192.168.31.1-192.168.31.254 |
| R&D | VLAN20 | 192.168.32.024 | 192.168.32.1-192.168.32.254 |
| Blackhole | VLAN99 | N/A | N/A |
| Native | VLAN100 | N/A | N/A |

## 4.2 Addressing Table

### 4.2.1 HQ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device | Interface | IP Address | Subnet Mask | Default Gateway |
| HQ\_Router | S0/2/0 | 192.168.101.1 | 255.255.255.252 | N/A |
|  | G0/0.1 | 192.168.11.1 | 255.255.255.0 | N/A |
|  | G0/0.2 | 192.168.12.1 | 255.255.255.0 | N/A |
|  | G0/0.3 | 192.168.13.1 | 255.255.255.0 | N/A |
| Sales-PC1 | NIC | 192.168.11.3 | 255.255.255.0 | 192.168.11.1 |
| Sales-PC2 | NIC | 192.168.11.4 | 255.255.255.0 | 192.168.11.1 |
| Sales-PC3 | NIC | 192.168.11.5 | 255.255.255.0 | 192.168.11.1 |
| Engineering-PC1 | NIC | 192.168.12.3 | 255.255.255.0 | 192.168.12.1 |
| Engineering-PC2 | NIC | 192.168.12.4 | 255.255.255.0 | 192.168.12.1 |
| Engineering-PC3 | NIC | 192.168.12.5 | 255.255.255.0 | 192.168.12.1 |
| Finance-PC1 | NIC | 192.168.13.3 | 255.255.255.0 | 192.168.13.1 |
| Finance-PC2 | NIC | 192.168.13.4 | 255.255.255.0 | 192.168.13.1 |
| Finance-PC3 | NIC | 192.168.13.5 | 255.255.255.0 | 192.168.13.1 |

### 4.2.2DMZ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device | Interface | IP Address | Subnet Mask | Default Gateway |
| HQ\_DMZRouter | G0/0.1 | 192.168.21.1 | 255.255.255.0 | N/A |
|  | S0/2/0 | 192.168.101.2 | 255.255.255.252 | N/A |
|  | S0/3/1 | 200.200.201.1 | 255.255.255.252 | N/A |
| DNS\_Server | NIC | 192.168.21.3 | 255.255.255.0 | 192.168.21.1 |
| E-mail\_Server | NIC | 192.168.21.4 | 255.255.255.0 | 192.168.21.1 |
| WEBFTP\_Server | NIC | 192.168.21.5 | 255.255.255.0 | 192.168.21.1 |

### 4.2.4 Branch

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device | Interface | IP Address | Subnet Mask | Default Gateway |
| Branch\_Router | G0/0.1 | 192.168.31.1 | 255.255.255.0 | N/A |
|  | G0/0.2 | 192.168.32.1 | 255.255.255.0 | N/A |
|  | S0/2/0 | 200.200.201.10 | 255.255.255.252 | N/A |
| Delivery\_PC1 | NIC | 192.168.31.3 | 255.255.255.0 | N/A |
| Delivery\_PC2 | NIC | 192.168.31.4 | 255.255.255.0 | N/A |
| Delivery\_PC3 | NIC | 192.168.31.5 | 255.255.255.0 | N/A |
| R&D\_PC1 | NIC | 192.168.32.3 | 255.255.255.0 | 192.168.32.1 |
| R&D\_PC2 | NIC | 192.168.32.4 | 255.255.255.0 | 192.168.32.1 |
| R&D\_PC3 | NIC | 192.168.32.5 | 255.255.255.0 | 192.168.32.1 |

4.2.5 ISP Cluster

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device | Interface | IP Address | Subnet Mask | Default Gateway |
| ISP\_Malaysia | Se0/2/0 | 200.200.201.2 | 255.255.255.252 | N/A |
|  | Se0/2/1 | 200.200.201.5 | 255.255.255.252 | N/A |
| ISP\_Thailand | Se0/2/0 | 200.200.201.6 | 255.255.255.252 | N/A |
|  | Se0/2/1 | 200.200.201.9 | 255.255.255.252 | N/A |

# 5.0 Basic Network Configuration

This section outlines the core configurations deployed across Starcom Asia’s network infrastructure, including VLAN setups, STP roles, DMZ services, routing protocol (OSPF), and final connectivity verification.

## 5.1 HQ

### 5.1.1 Vlan

A screenshot of a computer

AI-generated content may be incorrect.

Figure 5.1.1.1 HQ\_DIS\_SW VLAN

The HQ Distribution Switch (HQ\_DIS\_SW) is configured with VLANs for each department:

* VLAN 10 – Sales
* VLAN 20 – Engineering
* VLAN 30 – Finance
* VLAN 99 – Blackhole (for unused/suspicious ports)
* VLAN 100 – Native VLAN for trunk ports

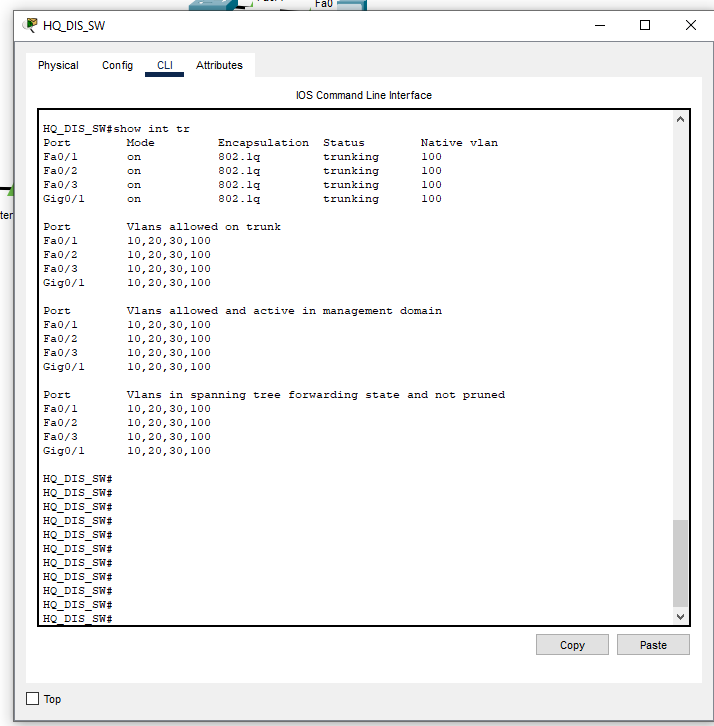


Figure 5.1.1.2 HQ\_DIS\_SW TRUNK

The HQ\_DIS\_SW distribution switch uses four trunk ports (Fa0/1–3, Gi0/1) for inter-switch connectivity, all using 802.1Q encapsulation with Native VLAN 100 to replace the insecure default VLAN 1. These trunks are restricted to VLANs 10 (Sales), 20 (Engineering), 30 (Finance), and 100, ensuring proper segmentation. Consistent settings across all trunks allow uniform traffic flow and prevent VLAN pruning. Assigning Native VLAN to 100 also helps mitigate VLAN hopping attacks, reflecting a secure and standardized trunk configuration throughout the network. (Rose, Nightingale, Garfinkel, & Chandramouli, 2016)

### 5.1.2 STP

A screenshot of a computer

AI-generated content may be incorrect.

A computer screen shot of a number

AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.

A white screen with black text

AI-generated content may be incorrect.

Figure 5.1.2.1 HQ\_DIS\_SW STP

In this topology, the HQ Distribution Switch (HQ\_DS\_SW) acts as the Root Bridge for VLANs 10, 20, and 30, selected due to its lowest Bridge ID. As a result, access switches—Sales\_SW, Engineering\_SW, and Finance\_SW—set their uplinks to HQ\_DS\_SW as Root Ports, enabling the shortest path to the root and remaining in a forwarding state. This setup ensures a loop-free Layer 2 topology and stable inter-VLAN communication.A white text on a white background

AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect. A white text with black text

AI-generated content may be incorrect.

To ensure Engineering\_SW does not become a Root Bridge, its STP priority was increased. This forces all switches to recognize HQ\_DS\_SW as the root. As a result, Engineering\_SW’s uplink becomes the Root Port, while other redundant links are assigned as Alternate Ports and placed in a blocking state. This configuration prevents loops and keeps the STP topology stable and predictable.

## 5.2 Branch

### 5.2.1 Vlan

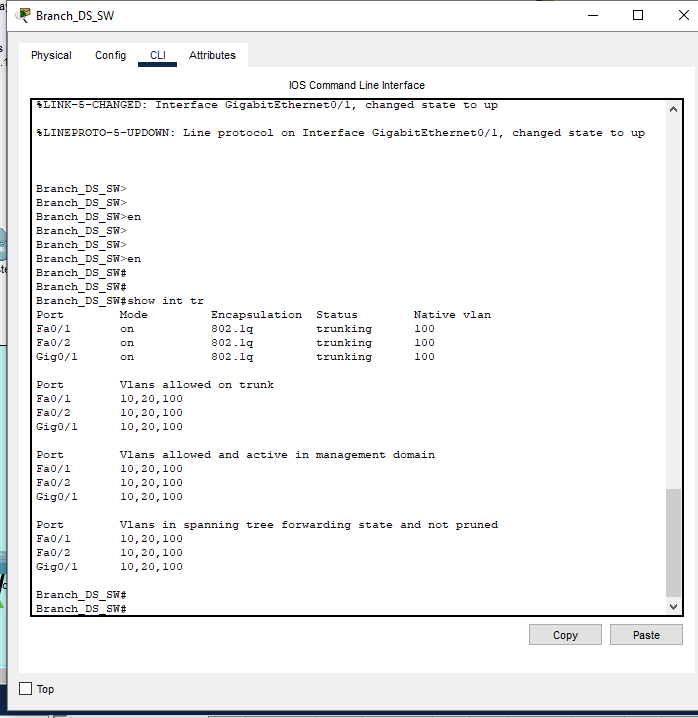
A screenshot of a computer

AI-generated content may be incorrect.

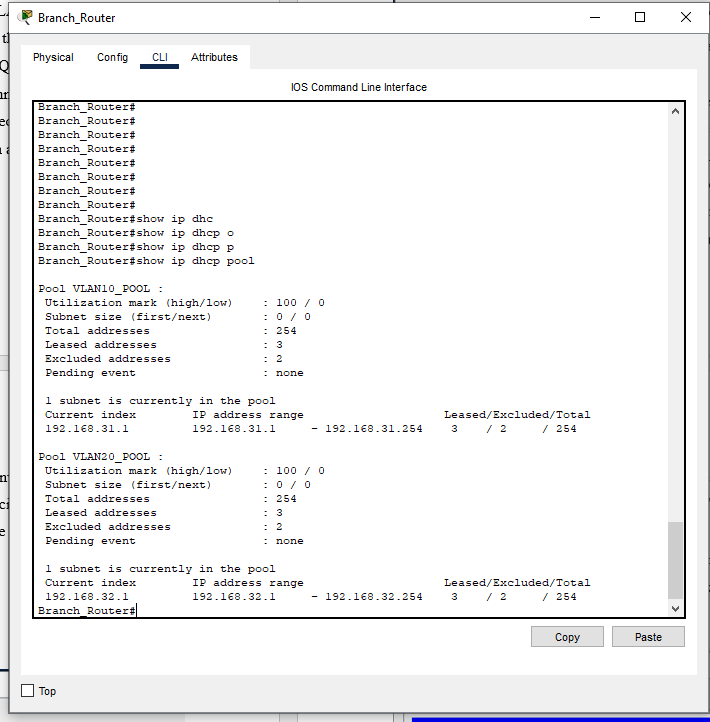
The Branch\_DS\_SW uses:

* VLAN 10 – Delivery
* VLAN 20 – R&D
* VLAN 99 – Blackhole (Fa0/3–24, Gi0/2)
* VLAN 100 – Native VLAN on trunks

(Stalings, 2022)



The Branch\_DS\_SW uses interfaces Fa0/1, Fa0/2, and Gig0/1 as trunk ports, as evidenced by the 'Mode' being 'on', 'Encapsulation' set to '802.1q', and 'Status' showing 'trunking'. All of these ports use VLAN 100 as the native VLAN, and are configured to allow VLANs 10, 20 and 100. The configuration is active in management domain. spanning tree is forwarding and it is not in a pruned state.5.2.2 DHCP



The Branch\_Router is configured with two DHCP pools to support distinct network segments. 'VLAN10\_POOL' provides IP addresses in the 192.168.31.0/24 network, allocating addresses from 192.168.31.1 to 192.168.31.254, with 3 currently leased and 2 excluded. Similarly, 'VLAN20\_POOL' manages the 192.168.32.0/24 network, assigning addresses from 192.168.32.1 to 192.168.32.254, also with 3 leased and 2 excluded. These pools must also include default gateway and DNS configurations, which are not captured in this output but are critical for proper client connectivity, in addition to Ip helpers.

## 5.3 DMZ

A screenshot of a computer

AI-generated content may be incorrect.

## 5.4 OSPF

OSPF was selected as the routing protocol for Starcom Asia’s WAN due to its scalability, fast convergence, and support for VLSM—critical for a multi-department network. As a link-state protocol, OSPF efficiently manages routes between Penang HQ and Krung Thep Branch while minimizing bandwidth usage. Its hierarchical area design aligns with our distributed network topology, unlike distance-vector protocols like RIP that lack these features (Cisco, 2005) (Cisco, Cisco, 2018)

A screenshot of a computer

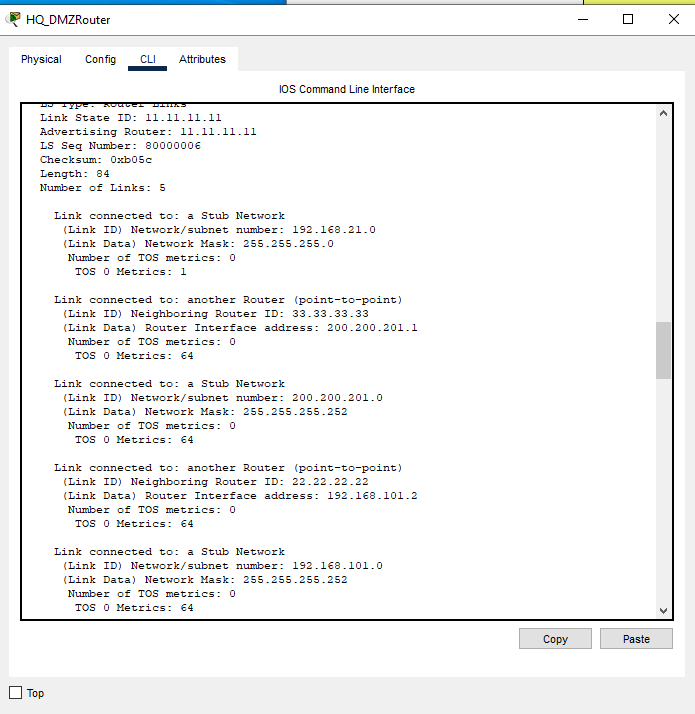
AI-generated content may be incorrect.

The screenshot from HQ\_Router shows the OSPF routing protocol is functioning correctly, as demonstrated by the successful execution of the show ip ospf database command. The output reveals OSPF Router ID 22.22.22.22 participating in OSPF Process ID 1, and it has established OSPF neighbor relationships in Area 0 with multiple routers. The database lists five Link-State Advertisements (LSAs), each representing a unique router: 22.22.22.22, 55.55.55.55, 44.44.44.44, 33.33.33.33, and 11.11.11.11. These entries confirm that OSPF has discovered and synchronized LSAs from all routers in the area, showing their Link IDs, advertising routers, sequence numbers, and link counts, which help determine the OSPF topology. The log message at the top (OSPF-5-ADJCHG) also confirms a neighbor adjacency was formed with router 11.11.11.11, transitioning from LOADING to FULL state, indicating successful OSPF convergence and full route exchange.

A screenshot of a computer

AI-generated content may be incorrect.

The HQ\_Router, identified by OSPF Router ID 22.22.22.22, has successfully formed OSPF adjacencies and is advertising five networks in its OSPF database. These include three stub networks—192.168.11.0/24, 192.168.12.0/24, and 192.168.13.0/24—which are likely local area networks directly connected to the router. Additionally, the router has established a point-to-point OSPF connection with a neighboring router (11.11.11.11) via the interface 192.168.101.1. This link belongs to the subnet 192.168.101.0/30, which is also advertised as a stub network. The cost metric for the LAN interfaces is 1, while the metric for the WAN link is 64. This confirms that the router is actively participating in OSPF routing and correctly advertising its connected networks. (Cisco, Cisco Support, 2014)



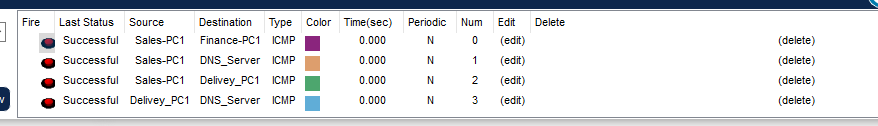
The HQ\_DMZRouter, identified by OSPF Router ID 11.11.11.11, has successfully formed OSPF adjacencies and is advertising five networks in its OSPF database. These include 3 stub networks—192.168.21.0/24, 192.168.101.0—which are likely local area networks directly connected to the router and the 200.200.201.0/30— which is likely Public network address that connect to ISP router. Additionally, the router has established a point-to-point OSPF connection with a neighboring router (22.22.22.2) via the interface 192.168.101.2. This link belongs to the subnet 192.168.101.0/30, which is also advertised as a stub network. The cost metric for the LAN interfaces is 1, while the metric for the WAN link is 64. This confirms that the router is actively participating in OSPF routing and correctly advertising its connected networks.

A screenshot of a computer

AI-generated content may be incorrect.

The Branch\_Router, identified by OSPF Router ID 55.55.55.55, has successfully formed OSPF adjacencies and is advertising five networks in its OSPF database. These include 3 stub networks—192.168.31.0/24,192.168.32.0/24—which are likely local area networks directly connected to the router and the 200.200.201.8/30— which is likely Public network address that connect to ISP router. Additionally, the router has established a point-to-point OSPF connection with a neighboring router (44.44.44.44) via the interface 200.200.201.10. This link belongs to the subnet 200.200.201.8/30, which is also advertised as a stub network. The cost metric for the LAN interfaces is 1, while the metric for the WAN link is 64. This confirms that the router is actively participating in OSPF routing and correctly advertising its connected networks.

## 5.5 Verification



Ping tests from Sales-PC1 to Finance-PC1, DNS\_Server, and Delivery\_PC1 confirm:

* Inter-VLAN routing is operational
* OSPF route propagation is working
* VPN tunnel between HQ and branch is successful

Low latency and successful replies confirm optimized performance and correct ACL/security zone configurations.

# 6.0 Conclusion

In conclusion, the network design for Starcom Asia Sdn Bhd successfully meets the company's needs for secure, scalable, and efficient communication between the Penang headquarters and the Krung Thep branch. The use of VLANs, a hierarchical topology, and proper subnetting with VLSM ensures effective traffic segmentation and IP address management. The implementation of DHCP, DNS, FTP, email, and web services in the DMZ confirms that critical services are available and securely accessible. OSPF has been effectively deployed as the routing protocol, providing fast convergence and reliable WAN connectivity. Spanning Tree Protocol (STP) and VLAN security configurations such as blackhole VLANs, native VLAN reassignment, and trunk port restrictions further enhance the network’s resilience and protection against Layer 2 threats. Connectivity tests validate that inter-VLAN routing and inter-branch communication over VPN are functioning correctly. Overall, this project demonstrates a secure and optimized enterprise network setup based on industry best practices.

# 7.0 References

*Cisco*. (10 August, 2005). Retrieved from Designing Large-Scale Stub Networks with ODR: https://www.cisco.com/c/en/us/support/docs/ip/on-demand-routing-odr/13710-39.html

Cisco. (October, 2014). *Cisco Support*. Retrieved from Chapter: OSPF Commands: ip ospf fast-reroute per-prefix through R: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute\_ospf/command/iro-cr-book/ospf-i1.html

Cisco. (11 September, 2018). *Cisco*. Retrieved from Redistributing Between Classful and Classless Protocols: EIGRP or OSPF into RIP or IGRP: https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/13721-52.html

Rose, S., Nightingale, S., Garfinkel, S., & Chandramouli, R. (September, 2016). *Computer Security Resource Center*. Retrieved from NIST SP 800-177: https://doi.org/10.6028/NIST.SP.800-177

Stalings, W. (2022). *Network Security Essentials: Application And Standards .* New York: Peasson Education Inc.