INDVIDUAL ASSIGNMENT

TECHNOLOGY PARK MALAYSIA

CT037-3-2-NWS
Network Security

APD2F2409CS

HAND OUT DATE: 5th March 2025

HAND IN DATE: 25thMay 2025

LECTURER: NOR AZLINA BINTI ABD RAHMAN

STUDENT NAME: BADR ABDULDAIM NOWRULDIN ALNAMHAWI

TP NUMBER: TP074644

Table of Contents

1.0 Introduction

In today's interconnected business environment, network security has become a critical cornerstone for organizational success and sustainability. As organizations expand their operations across multiple geographical locations and integrate diverse technological infrastructure, the complexity of securing enterprise networks increases exponentially. The implementation of comprehensive security measures is no longer optional but essential for protecting valuable corporate assets, maintaining operational continuity, and ensuring regulatory compliance.

Starcom Asia Sdn Bhd, a prominent network cable manufacturing company headquartered in Penang, Malaysia, exemplifies the challenges faced by modern enterprises in securing multi-site network infrastructures. The organization operates across two strategic locations: the main headquarters in Penang housing Sales, Engineering, and Finance departments, and a branch office in Krung Thep, Thailand, located 250 kilometers away, which accommodates the Research & Development (R&D) and Delivery departments. With approximately 100 employees in each department, the company requires a robust and scalable network security framework that can effectively manage inter-departmental communications while maintaining strict security boundaries.

The current network architecture presents several security challenges that demand immediate attention. The company's infrastructure includes multiple VLANs spanning across both locations, a demilitarized zone (DMZ) hosting critical servers including web, email, and FTP services, and WAN connectivity linking the two sites through an Internet Service Provider (ISP) managed infrastructure. This complex topology necessitates the implementation of multiple layers of security controls to prevent unauthorized access, data breaches, and network-based attacks that could compromise business operations.

Network segmentation through Virtual Local Area Networks (VLANs) serves as the foundation for implementing security policies within Starcom Asia's infrastructure. Proper VLAN implementation ensures logical separation of departments, reducing the attack surface and preventing lateral movement of potential threats across the network. However, VLAN implementation alone is insufficient without additional security measures such as access control lists (ACLs) that govern inter-VLAN communications and define granular traffic policies based on business requirements and security principles.

Furthermore, Layer 2 security threats pose significant risks to the organization's network infrastructure. Attacks such as MAC flooding, VLAN hopping, and DHCP starvation can disrupt network operations, compromise data integrity, and provide unauthorized access to sensitive information. These vulnerabilities require comprehensive security implementations at the data link layer to protect against both internal and external threats.

The implementation of network security measures must balance security requirements with operational efficiency. Overly restrictive policies can hinder legitimate business communications and reduce productivity, while inadequate security controls can expose the organization to various cyber threats. Therefore, a well-designed security framework must incorporate the principle of least privilege, ensuring that users and systems have access only to the resources necessary for their specific roles and responsibilities.

This report focuses on the implementation of three critical security domains within Starcom Asia's network infrastructure: VLAN technology deployment with enhanced security features, access control list (ACL) configuration for traffic management and policy enforcement, and Layer 2 security measures to protect against data link layer attacks. These implementations collectively establish a comprehensive security foundation that addresses the organization's immediate security requirements while providing scalability for future expansion.

The significance of this security implementation extends beyond technical considerations to encompass business continuity, regulatory compliance, and competitive advantage. By establishing robust security controls, Starcom Asia can protect its intellectual property, maintain customer trust, ensure operational reliability, and comply with industry standards and regulations. The proposed security measures align with established cybersecurity frameworks and best practices, ensuring that the implementation follows industry-recognized standards for enterprise network security.

Through systematic analysis and practical implementation of these security measures, this report demonstrates how organizations can effectively secure complex, multi-site network infrastructures while maintaining operational efficiency and supporting business objectives. The solutions presented provide actionable guidance for network administrators and security professionals responsible for implementing and maintaining enterprise network security in similar organizational contexts.

2.0 Topology of the Network Diagram

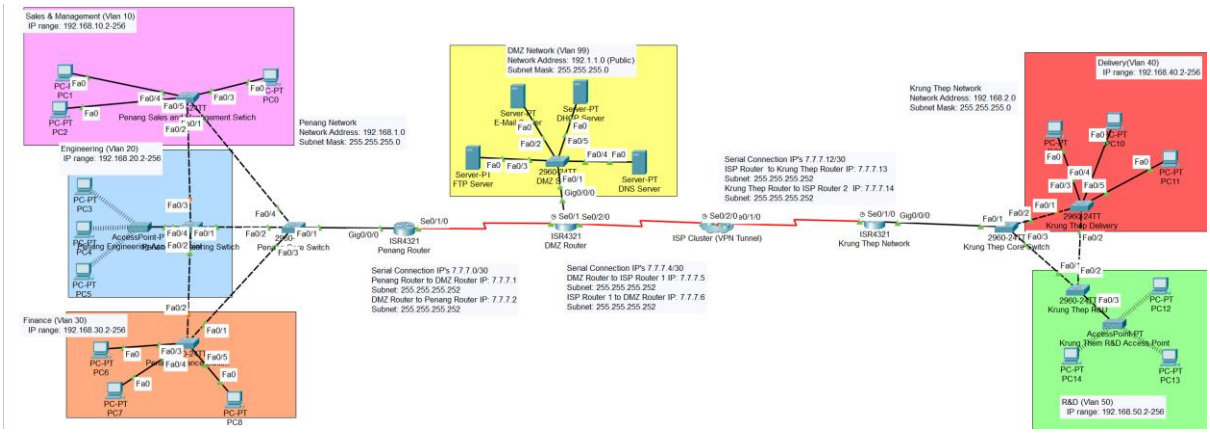

Figure 1- network topology

The topology in the diagram is used as follow up from the group assignment topology, this network topology illustrates Starcom Asia Sdn Bhd's enterprise infrastructure spanning two geographical locations connected through a secure WAN architecture. The Penang headquarters (left) houses three departmental VLANs - Sales & Management (VLAN 10), Engineering (VLAN 20), and Finance (VLAN 30) - each with dedicated workstations and access switches connecting to a central Penang router. The center of the topology features a DMZ network (VLAN 99) hosting critical servers including email, DHCP, FTP, and DNS services, accessible to both sites while maintaining security isolation. The Krung Thep branch office (right) mirrors the Penang structure with Delivery (VLAN 40) and R&D (VLAN 50) departments, each containing workstations and wireless access points connected through local switches to the Krung Thep router. Inter-site connectivity is established through an ISP-managed router cluster providing redundant WAN links between the locations, with an additional VPN tunnel ensuring secure communication channels for sensitive data transmission between the headquarters and branch office, creating a comprehensive multi-site network supporting approximately 500 employees across five departments with robust security segmentation and centralized server resources.

3.0 Tasks explanations and configurations

In this section 3 tasks were chosen and will be explained in detail providing screenshots of the configurations for further elaboration.

Task 5: 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).

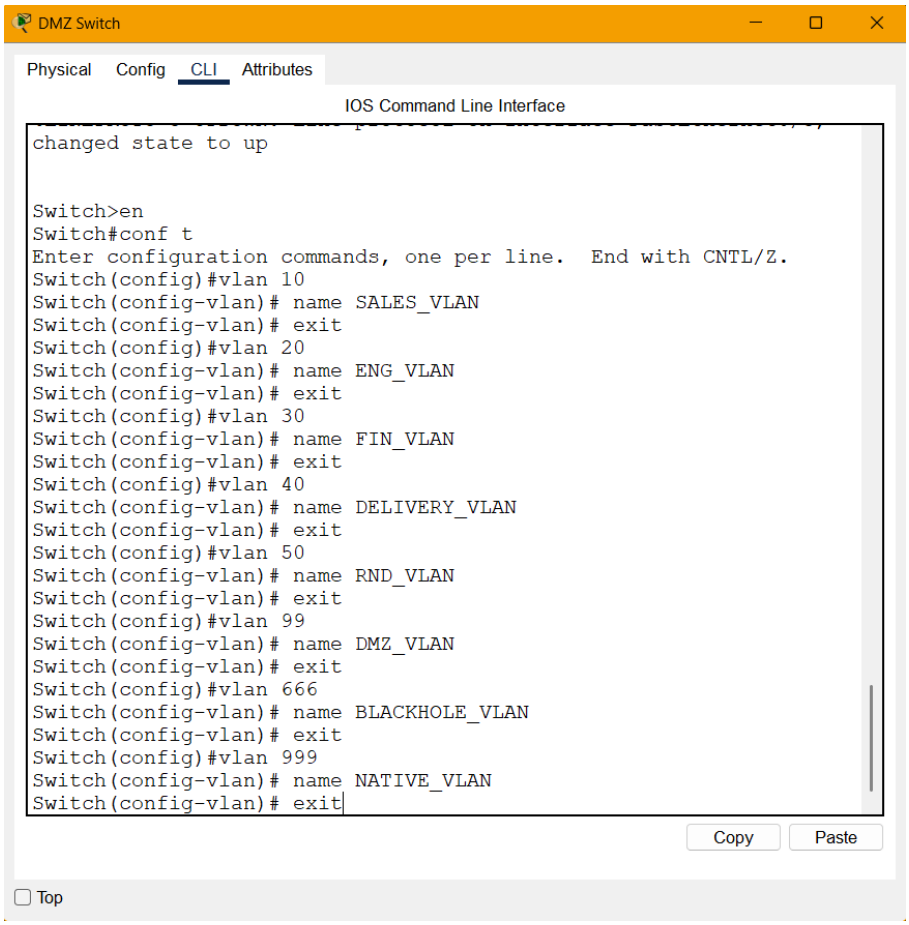

Figure 2- VLANs

STEP 1: Create VLANs on ALL Switches

Purpose: Establish VLAN database on every switch in the network

Applied to: All 8 switches (Finance, Engineering, Sales, Penang-Core, DMZ, Delivery, RnD, KrungThep-Core)

The vlan [number] and name [VLAN_NAME] commands establish the VLAN database on each switch, creating logical broadcast domains identified by unique VLAN IDs. This process defines the VLAN structure that will be consistent across all switches in the network. The VLAN database must exist on every switch before devices can be assigned to VLANs or trunk links can carry VLAN traffic. Each VLAN operates as an isolated Layer 2 segment, preventing broadcast traffic from one VLAN from affecting devices in other VLANs.

```
Finance-SW>en
Finance-SW#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Finance-SW(config)#interface range fastethernet0/3-5
Finance-SW(config-if-range)# switchport mode access
Finance-SW(config-if-range)# switchport access vlan 30
Finance-SW(config-if-range)# no shutdown
Finance-SW(config-if-range)#exit
Finance-SW(config)#end
Finance-SW#
%SYS-5-CONFIG_I: Configured from console by console

Finance-SW#
```

Figure 3- Access Ports

STEP 2: Configure Access Ports for End Devices

Purpose: Assign end devices (PCs, servers, access points) to their respective VLANs

The [switchport mode access] command configures ports to belong to a single VLAN, while [switchport access] vlan [number] assigns the port to a specific VLAN. Access ports strip VLAN tags from outgoing frames and add VLAN tags to incoming frames, making VLAN membership transparent to connected end devices. This configuration ensures that devices like PCs, servers, and access points automatically become members of their designated VLANs without requiring VLAN-aware configuration on the end devices themselves.

```
Finance-SW#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Finance-SW(config)#interface fastethernet0/1
Finance-SW(config-if)# switchport mode trunk
Finance-SW(config-if)# switchport trunk native vlan 999
Finance-SW(config-if)# no shutdown
Finance-SW(config-if)#exit
Finance-SW(config)#interface fastethernet0/2
Finance-SW(config-if)# switchport mode trunk
Finance-SW(config-if)# switchport trunk native vlan 999
Finance-SW(config-if)# no shutdown
Finance-SW(config-if)#exit
Finance-SW(config)#end
```

Figure 4- Trunk Links

STEP 3: Configure Trunk Links Between Switches

Purpose: Allow multiple VLANs to travel between switches.

The [switchport mode trunk] command enables ports to carry traffic for multiple VLANs simultaneously using 802.1Q tagging, while [switchport trunk native vlan 999] sets the native VLAN for untagged traffic. Trunk links use VLAN tags to identify which VLAN each frame belongs to, allowing switches to properly forward traffic between VLANs across the network infrastructure. The native VLAN (999) handles untagged traffic and provides backward compatibility, while using a non-default native VLAN enhances security by preventing VLAN hopping attacks.

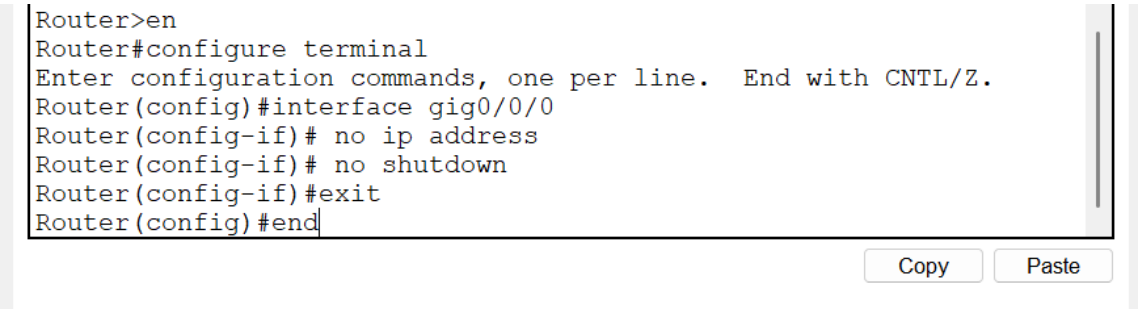

Figure 5- default router IP removal

STEP 4: Remove Default Router IPs (CRITICAL!)

Purpose: Default IPs on physical interfaces conflict with sub-interfaces and prevent proper VLAN routing.

The [no ip address] command removes any existing IP configuration from the physical router interface, preventing conflicts with sub-interface configurations. Physical interfaces cannot simultaneously have a direct IP address and host multiple sub-interfaces, as this creates routing ambiguity. Removing the physical interface IP ensures that all VLAN routing occurs through the sub-interfaces, each of which serves as the default gateway for its respective VLAN. This step is essential for proper inter-VLAN routing functionality in a router-on-a-stick configuration.

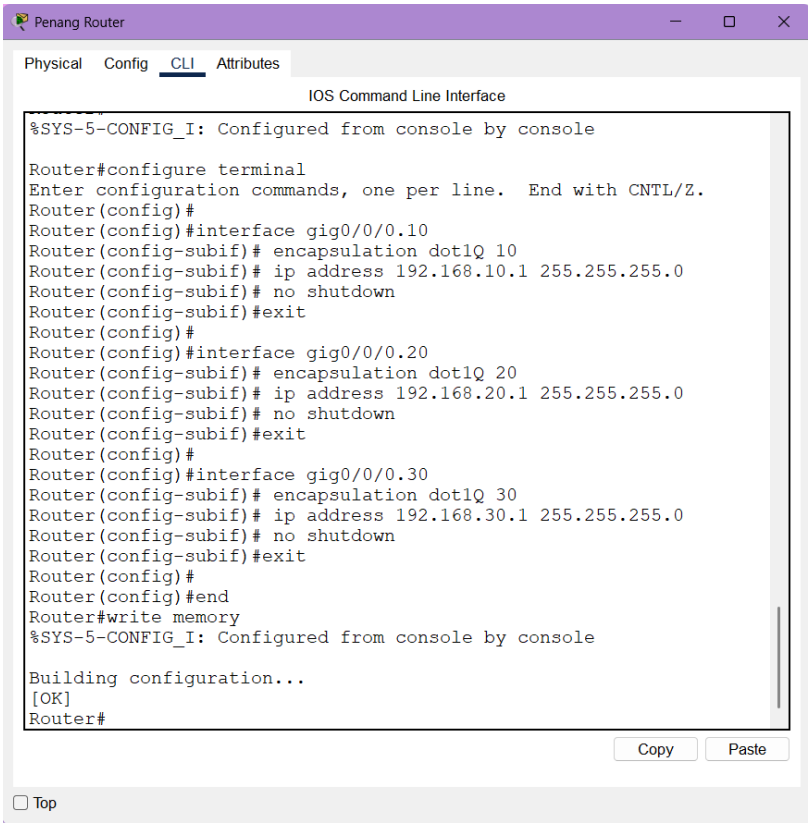

Figure 6- Router Sub-interfaces

STEP 5: Create Router Sub-interfaces

Purpose: Enable inter-VLAN routing by creating Layer 3 gateways for each VLAN

The encapsulation dot1Q [VLAN_ID] command configures sub-interfaces to handle 802.1Q tagged traffic for specific VLANs, while ip address assigns each sub-interface as the default gateway for its VLAN. Sub-interfaces create Layer 3 routing capabilities for each VLAN, enabling communication between different VLANs through the router. Each sub-interface operates as a virtual router interface dedicated to a specific VLAN, processing routing decisions and forwarding traffic between VLANs based on the routing table. This configuration implements the router-on-a-stick topology, where a single physical interface handles routing for multiple VLANs.

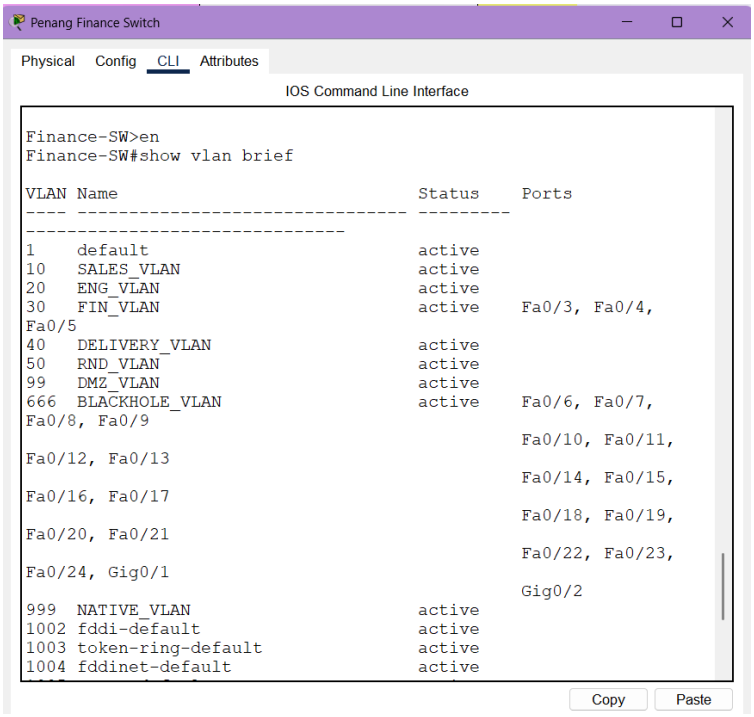

Figure 7- vlan brief

```
Finance-SW#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      999
Fa0/2       on           802.1q         trunking      999

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/2       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,30,40,50,99,666,999
Fa0/2       1,10,20,30,40,50,99,666,999

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,30,40,50,99,666,999
Fa0/2       none

Finance-SW#
```

Figure 8- interfaces trunk

The verification commands show vlan brief, show interfaces trunk, and show ip interface brief confirm proper VLAN assignment, trunk functionality, and router interface status respectively. Testing within VLANs verifies Layer 2 connectivity and VLAN membership, while testing between VLANs confirms that inter-VLAN routing is functioning correctly through the router sub-interfaces. These tests validate that the VLAN segmentation is working as designed - devices within the same VLAN can communicate directly, while devices in different VLANs can only communicate through the router, allowing for traffic control and security policy implementation.

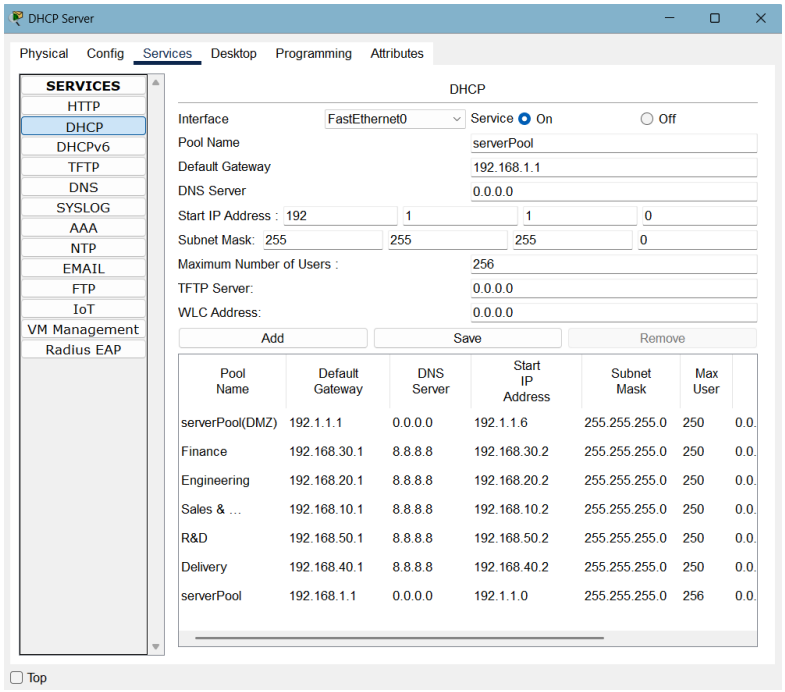

Figure 9- DHCP IP Pools

STEP 6: Setting up DHCP relay to help router take IP from the DHCP server.

Since the IP ranges are changed by default when the sub interfaces were set to

VLAN 10: Sales & Management (192.168.10.1)

VLAN 20: Engineering (192.168.20.1)

VLAN 30: Finance (192.168.30.1)

VLAN 40: Delivery/Krung Thep (192.168.40.1)

VLAN 50: R&D/Krung Thep (192.168.50.1)

VLAN 99: DMZ (192.168.1.0/24)

The pools were updated accordingly, and there is a need to set an IP-Address helper for each sub-interface to forward the IP to the Vlan.

```
Router>en
Router#
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface gig0/0/0.10
Router(config-subif)# ip helper-address 192.1.1.5
Router(config-subif)#exit
Router(config)#interface gig0/0/0.20
Router(config-subif)# ip helper-address 192.1.1.5
Router(config-subif)#exit
Router(config)#interface gig0/0/0.30
Router(config-subif)# ip helper-address 192.1.1.5
Router(config-subif)#exit
Router(config)#end
Router#write memory
%SYS-5-CONFIG_I: Configured from console by console

Building configuration...
[OK]
Router#
```

Figure 10- ip helper-address

The [ip helper-address] command will convert DHCP broadcast requests into unicast packets sent directly to the DHCP server at 192.1.1.5.

Task 6: ACL Security Policies and Configuration (Solution and configuration).

Security Policies Proposed

Policy 1: Department Isolation

- Sales (VLAN 10) cannot access Engineering (VLAN 20) or Finance (VLAN 30)
- Engineering (VLAN 20) cannot access Sales (VLAN 10) or Finance (VLAN 30)
- Finance (VLAN 30) cannot access Sales (VLAN 10) or Engineering (VLAN 20)

Policy 2: Cross-Site Department Restrictions

- Delivery (VLAN 40) and R&D (VLAN 50) cannot access each other.

Policy 3: DMZ Access Control

- All internal VLANs can access DMZ servers for web, email, and FTP services only
- DMZ servers cannot initiate connections back to internal networks
- External users can only access DMZ web and email servers (no FTP from external)

Policy 4: Internet Access Restrictions

- Only Sales, Engineering, and Finance can access the Internet
- Delivery and R&D have no Internet access (internal communication only)
- Internet access limited to HTTP, HTTPS, ICMP, and DNS only

Policy 5: Management Traffic

- All VLANs can access their respective gateway routers for DHCP and DNS
- SSH/Telnet access to network devices restricted to Finance department only

```
Penang_Router>en
Penang_Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Penang_Router(config)#
Penang_Router(config)#
Penang_Router(config)#access-list 100 remark === SALES DEPARTMENT ACCESS CONTROL ===
Penang_Router(config)#access-list 100 deny ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
Penang_Router(config)#access-list 100 deny ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
Penang_Router(config)#access-list 100 permit ip any any
Penang_Router(config)#
Penang_Router(config)#access-list 110 remark === ENGINEERING DEPARTMENT ACCESS CONTROL ===
Penang_Router(config)#access-list 110 deny ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
Penang_Router(config)#access-list 110 deny ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255
Penang_Router(config)#access-list 110 permit ip any any
Penang_Router(config)#
Penang_Router(config)#access-list 120 remark === FINANCE DEPARTMENT ACCESS CONTROL ===
Penang_Router(config)#access-list 120 deny ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255
Penang_Router(config)#access-list 120 deny ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
Penang_Router(config)#access-list 120 permit ip any any
Penang_Router(config)#
Penang_Router(config)#interface GigabitEthernet0/0/0.10
Penang_Router(config-subif)# ip access-group 100 in
Penang_Router(config-subif)#exit
Penang_Router(config)#interface GigabitEthernet0/0/0.20
Penang_Router(config-subif)# ip access-group 110 in
Penang_Router(config-subif)#exit
Penang_Router(config)#interface GigabitEthernet0/0/0.30
Penang_Router(config-subif)# ip access-group 120 in
Penang_Router(config-subif)#exit
Penang_Router(config)#
Penang_Router(config)#end
Penang_Router#write memory
%SYS-5-CONFIG_I: Configured from console by console
```

Figure 11- ACL Configuration

- How Access Control Lists (ACLs) Work

Access Control Lists function as traffic filters applied to router interfaces, examining each packet's source IP, destination IP, and port numbers to determine whether to permit or deny the traffic based on predefined security policies. Using ACL 100 for Sales Department (VLAN 10) as an example, the ACL contains sequential rules that are processed from top to bottom until a match is found, with an implicit "deny all" rule at the end. The access-list 100 permit tcp 192.168.10.0 0.0.0.255 192.1.1.0 0.0.0.255 eq 80 command allows Sales users to access DMZ web servers on port 80 (HTTP), while access-list 100 deny ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255 blocks all Sales traffic attempting to reach Engineering networks. The wildcard mask 0.0.0.255 indicates that the first three octets must match exactly while the last octet can be any value within the subnet range.

- ACL Implementation Locations

Penang Router (GigabitEthernet0/0/0): ACLs 100, 110, and 120 are configured and applied to subinterfaces .10, .20, and .30 respectively, controlling traffic for Sales, Engineering, and Finance departments at the inter-VLAN routing level. Krung Thep Router (GigabitEthernet0/0/0): ACLs 140 and 150 are implemented on subinterfaces .40 and .50 for Delivery and R&D departments, enforcing traffic policies before packets are routed between VLANs. DMZ Router (GigabitEthernet0/0/0.99): ACL 199 is applied to control external access to DMZ servers, acting as a perimeter defense mechanism. The ACLs are specifically applied using the ip access-group [number] in command on the router subinterfaces where inter-VLAN routing occurs, not on the switches, because traffic filtering must happen at Layer 3 where routing decisions are made between different VLANs.

- Why Routers, Not Switches

ACL implementation occurs on routers rather than switches because VLANs operate at Layer 2 within switches, allowing free communication between devices in the same VLAN, while traffic between different VLANs must pass through the router's Layer 3 interfaces where security policies can be enforced. Each router subinterface serves as the gateway for its respective VLAN, making it the optimal point for implementing traffic control policies as packets transition between network segments. The ip access-group command applied to router subinterfaces ensures that every packet requiring inter-VLAN communication is evaluated against the security policies before routing decisions are executed.

```
Penang_Router#show access-lists
Extended IP access list 100
    10 deny ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
    20 deny ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
    30 permit ip any any (6 match(es))
Extended IP access list 110
    10 deny ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
    20 deny ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255
    30 permit ip any any (4 match(es))
Extended IP access list 120
    10 deny ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255
    20 deny ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
    30 permit ip any any (6 match(es))

Penang_Router#
```

Figure 12-access-lists

```
Penang_Router#show ip interface GigabitEthernet0/0/0.10
GigabitEthernet0/0/0.10 is up, line protocol is up (connected)
  Internet address is 192.168.10.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is 192.1.1.5
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is 100
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
```

Figure 13- ip interface Gig0/0/0.10

Test ACL Pinging:

From Sales PC (VLAN 10):

ping 192.168.20.2 ← Should FAIL ❌

ping 192.168.30.2 ← Should FAIL ❌

ping 192.1.1.2 ← Should WORK ✅

ping 8.8.8.8 ← Should WORK ✅

ping 192.168.40.2 ← Should WORK ✅ (Delivery in Krung Thep)

From Engineering PC (VLAN 20):

ping 192.168.10.2 ← Should FAIL ❌

ping 192.168.30.2 ← Should FAIL ❌

From Finance PC (VLAN 30):

ping 192.168.10.2 ← Should FAIL ❌

ping 192.168.20.2 ← Should FAIL ❌

From Delivery PC (VLAN 40):

ping 192.168.50.2 ← Should FAIL ❌ (blocked from R&D)

ping 192.168.10.2 ← Should WORK ✅ (can access Sales)

ping 192.168.20.2 ← Should WORK ✅ (can access Engineering)

ping 192.168.30.2 ← Should WORK ✅ (can access Finance)

ping 192.1.1.2 ← Should WORK ✅ (can access DMZ)

From R&D PC (VLAN 50):

ping 192.168.40.2 ← Should FAIL ❌ (blocked from Delivery)

ping 192.168.10.2 ← Should WORK ✅ (can access Sales)

ping 192.168.20.2 ← Should WORK ✅ (can access Engineering)

ping 192.168.30.2 ← Should WORK ✅ (can access Finance)

ping 192.1.1.2 ← Should WORK ✅ (can access DMZ)

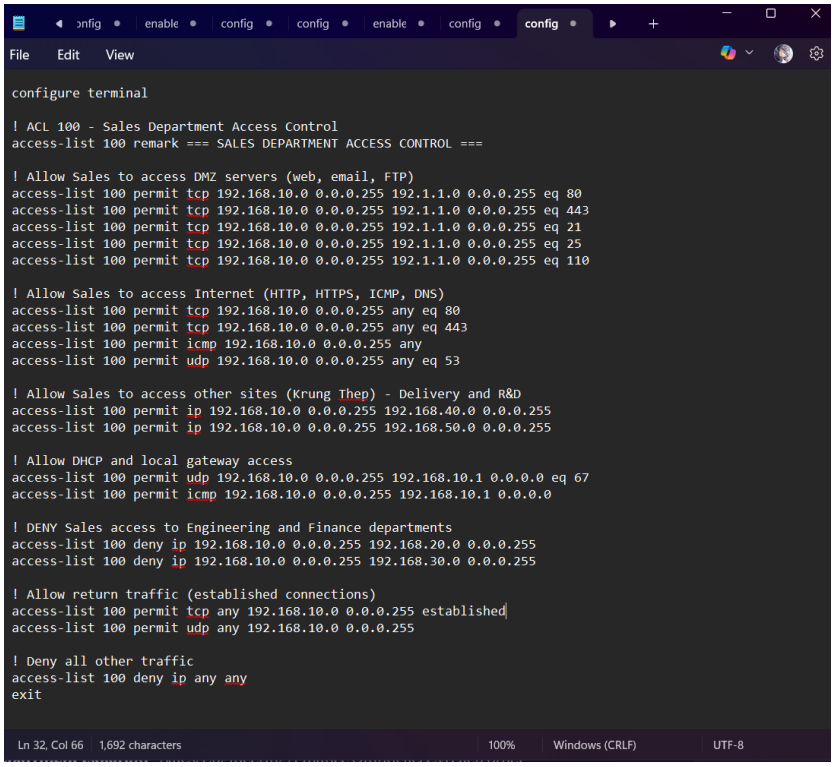

Figure 14- ACL extra configs

These are extra configurations to satisfy all services from all the Tasks in the assignment, these are already implemented but due to the lack of the other services configuration implementations it can't be fully tested, like pinging 8.8.8.8 in the PC1 in sales department to test internet connectivity.

Task 7: Layer 2 Security - Attacks and Implementation (Solution and configuration).

Part A: Three Types of Layer 2 Attacks Explained

1. MAC Flooding Attack (CAM Table Overflow)

Description: Attackers flood the switch with fake MAC addresses to overwhelm the CAM (Content Addressable Memory) table, causing the switch to enter "fail-open" mode where it acts like a hub, broadcasting all traffic (Cisco, 2023).

How it works:

- Attacker sends thousands of frames with different source MAC addresses.
- Switch CAM table fills up (typically 8,000-16,000 entries).
- Once full, switch floods all traffic to all ports.
- Attacker can now capture traffic intended for other devices (Stallings, 2020).

Impact:

- Network performance degradation.
- Confidential data exposure.
- Network reconnaissance opportunities (Technology, 2022).

2. VLAN Hopping Attack

Description: Attackers exploit VLAN configurations to gain unauthorized access to VLANs they shouldn't have access to.

Two main methods: a) Switch Spoofing: Attacker configures device to mimic a switch and negotiate trunking b) Double Tagging: Attacker sends frames with two VLAN tags to bypass VLAN restrictions. (Convery, 2004)

How Double Tagging works:

- Attacker on VLAN 10 sends frame with outer tag 10 and inner tag 30.
- First switch removes outer tag (10) and forwards to trunk.

- Second switch sees only inner tag (30) and forwards to VLAN 30.
- Attacker gains access to VLAN 30.

Impact:

- Unauthorized access to sensitive VLANs (Finance, HR, etc.).
- Data theft and lateral movement.
- Bypassing network security policies.

3. DHCP Starvation Attack

Description: Attackers exhaust the DHCP server's IP address pool by requesting all available addresses, preventing legitimate clients from obtaining IP addresses (Droms, 1997).

How it works:

- Attacker rapidly sends DHCP DISCOVER requests with different MAC addresses
- DHCP server allocates IP addresses for each fake request
- IP address pool becomes exhausted
- Legitimate clients cannot obtain IP addresses (denial of service)
- Attacker may then set up rogue DHCP server to capture credentials

Impact:

- Network connectivity denial of service
- Potential man-in-the-middle attacks via rogue DHCP
- Network disruption and productivity loss

(Northcutt, 2021)

Part B: Layer 2 Security Implementation

Security Measure 1: Port Security

Purpose: Prevent MAC flooding attacks and unauthorized device connections

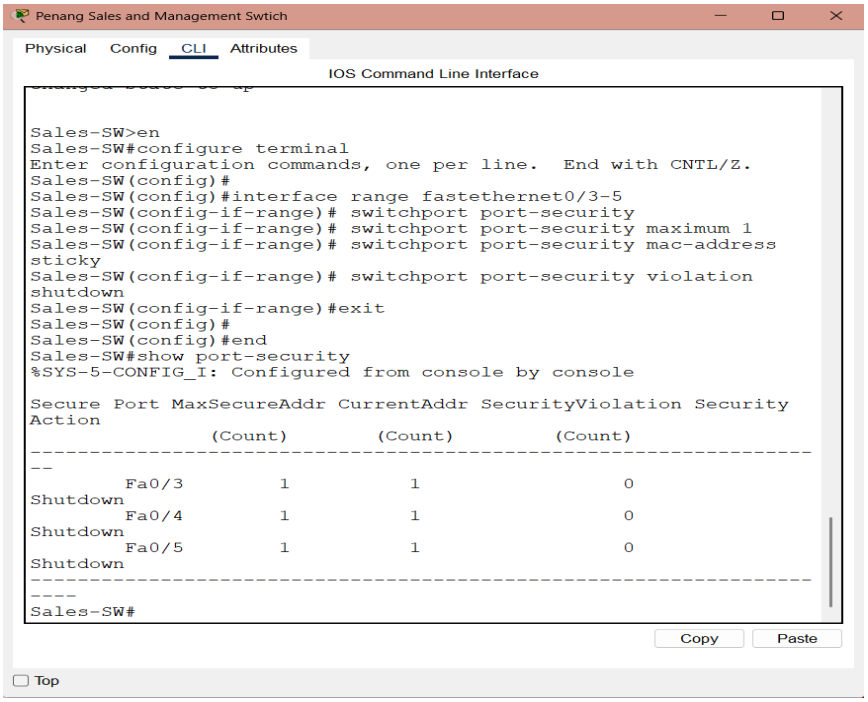

Figure 15- port-security configuration

These configurations restrict each of the ports (FastEthernet0/3-5) to only allow one specific device by saving its MAC address. If an unauthorized device tries to connect, the port automatically shuts down to prevent access. The [show port-security] command confirms that the ports are secured and working as intended. This helps keep the network safe by ensuring only trusted devices can connect.

Security Measure 2: DHCP Snooping

Purpose: Prevent DHCP starvation attacks and rogue DHCP servers

Enable DHCP Snooping Globally or/and configure unused ports in blackhole VLAN

```
! Apply to ALL access switches (Sales, Engineering, Finance, Delivery, R&D)
configure terminal

! Enable DHCP snooping globally
ip dhcp snooping
ip dhcp snooping vlan 10,20,30,40,50,99

! Configure trusted interfaces (uplinks to routers/core switches)
interface fastethernet0/1
 ip dhcp snooping trust
exit

! Configure rate limiting on access ports
interface range fastethernet0/2-24
 ip dhcp snooping limit rate 10
exit

! Enable DHCP snooping database
ip dhcp snooping database flash:dhcp_snooping.db

end
write memory
```

Figure 16- DHCP Snooping Globally

Since Vlans already configured it is a better idea to assign the unused ports to the blackhole Vlan which was already established its better and doesn't conflict with the network existing settings.

```
Finance-SW>enable
Finance-SW#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Finance-SW(config)#interface range fastethernet0/6-24
Finance-SW(config-if-range)# switchport mode access
Finance-SW(config-if-range)# switchport access vlan 666
Finance-SW(config-if-range)# shutdown
Finance-SW(config-if-range)#exit
Finance-SW(config)#interface range gigabitethernet0/1-2
Finance-SW(config-if-range)# switchport mode access
Finance-SW(config-if-range)# switchport access vlan 666
Finance-SW(config-if-range)# shutdown
Finance-SW(config-if-range)#exit
Finance-SW(config)#end
Finance-SW#write memory
%SYS-5-CONFIG_I: Configured from console by console

Building configuration...
[OK]
Finance-SW#
```

Figure 17- Blackhole VLAN

```
Device Name: Penang Finance Switch
Custom Device Model: 2960 IOS15
Hostname: Finance-SW

Port                Link   VLAN   IP Address         MAC Address
FastEthernet0/1     Up     --     --                 0090.21E3.C701
FastEthernet0/2     Up     --     --                 0090.21E3.C702
FastEthernet0/3     Up     30     --                 0090.21E3.C703
FastEthernet0/4     Up     30     --                 0090.21E3.C704
FastEthernet0/5     Up     30     --                 0090.21E3.C705
FastEthernet0/6     Down   666    --                 0090.21E3.C706
FastEthernet0/7     Down   666    --                 0090.21E3.C707
FastEthernet0/8     Down   666    --                 0090.21E3.C708
FastEthernet0/9     Down   666    --                 0090.21E3.C709
FastEthernet0/10    Down   666    --                 0090.21E3.C70A
FastEthernet0/11    Down   666    --                 0090.21E3.C70B
FastEthernet0/12    Down   666    --                 0090.21E3.C70C
FastEthernet0/13    Down   666    --                 0090.21E3.C70D
FastEthernet0/14    Down   666    --                 0090.21E3.C70E
FastEthernet0/15    Down   666    --                 0090.21E3.C70F
FastEthernet0/16    Down   666    --                 0090.21E3.C710
FastEthernet0/17    Down   666    --                 0090.21E3.C711
FastEthernet0/18    Down   666    --                 0090.21E3.C712
FastEthernet0/19    Down   666    --                 0090.21E3.C713
FastEthernet0/20    Down   666    --                 0090.21E3.C714
FastEthernet0/21    Down   666    --                 0090.21E3.C715
FastEthernet0/22    Down   666    --                 0090.21E3.C716
FastEthernet0/23    Down   666    --                 0090.21E3.C717
FastEthernet0/24    Down   666    --                 0090.21E3.C718
GigabitEthernet0/1  Down   666    --                 0090.21E3.C719
GigabitEthernet0/2  Down   666    --                 0090.21E3.C71A
Vlan1               Down   1      <not set>          00E0.8F77.D383

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Penang Finance Switch
```

Figure 18- interfaces check up

These 2 figures illustrate that blackhole Vlan is a very suitable security implementation which administratively turning down the ports for the best security action to take, which prevents any unauthorized access.

Security Measure 3: VLAN Hopping Prevention (extra)

Purpose: Prevent VLAN hopping attacks

```
Finance-SW#en
Finance-SW#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Finance-SW(config)#
Finance-SW(config)#interface range fastethernet0/3-24
Finance-SW(config-if-range)# switchport mode access
Finance-SW(config-if-range)# switchport nonegotiate
Finance-SW(config-if-range)#exit
Finance-SW(config)#
```

Figure 19- switchport nonegotiate

Dynamic Trunking Protocol (DTP) Security Configuration

The [switchport nonegotiate] command disables Dynamic Trunking Protocol (DTP) negotiation on access ports, preventing VLAN hopping attacks through unauthorized trunk formation. DTP is a Cisco proprietary protocol that automatically negotiates trunking between switches, but when enabled on access ports, it creates a security vulnerability where attackers can potentially convince the switch to form a trunk link, gaining access to multiple VLANs. By implementing switchport mode access combined with switchport nonegotiate on all access ports (end-device connections and unused ports), the switch explicitly configures these ports as access-only and refuses any trunking negotiations, ensuring that end devices remain isolated within their designated VLANs. This configuration is applied to user-facing ports and unused ports across all access switches while deliberately excluding legitimate trunk ports between switches, which require DTP functionality for proper inter-switch communication and VLAN propagation throughout the network infrastructure.

4.0 Troubleshoots

Problem 1: OSPF Not Advertising New VLAN Subnets

The OSPF was still advertising the old network: network 192.168.1.0 0.0.0.255 area 0

But the new VLANs use different subnets:

- VLAN 10: 192.168.10.0/24
- VLAN 20: 192.168.20.0/24
- VLAN 30: 192.168.30.0/24

Other routers don't know these networks exist!

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)# network 192.168.10.0 0.0.0.255 area 0
Router(config-router)# network 192.168.20.0 0.0.0.255 area 0
Router(config-router)# network 192.168.30.0 0.0.0.255 area 0
Router(config-router)# no network 192.168.1.0 0.0.0.255 area 0
Router(config-router)#exit
Router(config)#
```

Figure 20- OSPF commands

The figure above shows the commands needed to advertise the Vlans sub-interfaces, and remove the old network advertisement.

Problem 2: Extra Helper-Address on Physical Interface

The existing of extra helper-address that might conflict:

```
Penang_Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Penang_Router(config)#interface GigabitEthernet0/0/0
Penang_Router(config-if)# no ip helper-address 192.1.1.3
Penang_Router(config-if)# no ip helper-address 192.1.1.5
Penang_Router(config-if)#exit
Penang Router(config)#
```

Figure 21- helper-address removal

This will make sure that the helper IP in the physical interface Gig0/0/0, which the default IP was removed to be consistent and remove any extra settings along with it.

5.0 Conclusion

The implementation of comprehensive network security measures for Starcom Asia Sdn Bhd has successfully established a robust, multi-layered security framework that addresses critical vulnerabilities while maintaining operational efficiency across both Penang and Krung Thep locations. Through the systematic deployment of VLAN technology, access control lists, and Layer 2 security measures, the organization now benefits from enhanced network segmentation, granular traffic control, and protection against sophisticated data link layer attacks.

The VLAN implementation (Task 5) has created logical network segmentation that serves as the foundation for all subsequent security measures. By establishing eight distinct VLANs with proper trunk configurations, native VLAN security settings, and router-on-a-stick topology, the network now provides clear departmental boundaries while enabling controlled inter-departmental communication. The integration of DHCP relay functionality ensures seamless IP address management across all network segments, while the implementation of blackhole VLAN 666 for unused ports demonstrates proactive security hardening that prevents unauthorized network access.

The access control list configuration (Task 6) has successfully implemented the principle of least privilege across the enterprise network. The five comprehensive security policies ensure that departments can only access resources necessary for their business functions, with Sales, Engineering, and Finance maintaining internet connectivity while Delivery and R&D departments remain isolated from external networks to protect sensitive research and operational data. The strategic placement of ACLs on router sub-interfaces rather than switches demonstrates proper understanding of network architecture, ensuring that traffic filtering occurs at the appropriate Layer 3 boundaries where inter-VLAN routing decisions are made.

The Layer 2 security implementation (Task 7) addresses fundamental switch-level vulnerabilities that could compromise the entire network infrastructure. By implementing port security with MAC address limitations, organizations can prevent MAC flooding attacks that would otherwise allow unauthorized traffic monitoring. The deployment of DHCP snooping in conjunction with blackhole VLAN assignments provides comprehensive protection against DHCP starvation attacks while maintaining network connectivity for legitimate devices. The prevention of VLAN hopping through DTP negotiation disabling ensures that the carefully designed network segmentation cannot be bypassed through protocol manipulation.

The troubleshooting section demonstrates the iterative nature of network security implementation, highlighting how OSPF routing configuration and DHCP relay settings required adjustment to accommodate the new VLAN architecture. The resolution of these issues through systematic diagnosis and configuration refinement showcases the importance of thorough testing and validation in enterprise network deployments.

This comprehensive security implementation establishes multiple defensive layers that work synergistically to protect Starcom Asia's network infrastructure. The combination of physical port security, logical VLAN segmentation, and policy-based traffic control creates a defense-in-depth strategy that can withstand various attack vectors while supporting legitimate business operations. The scalable design ensures that future network expansion or departmental restructuring can be accommodated without compromising security effectiveness.

The successful deployment of these security measures positions Starcom Asia Sdn Bhd to maintain competitive advantage through protected intellectual property, ensure regulatory compliance, and provide reliable network services that support business continuity. The implementation follows industry best practices and established cybersecurity frameworks, providing a solid foundation for ongoing security monitoring and enhancement as the organization's technological landscape continues to evolve.

6.0 References

Cisco. (2023). *Cisco Catalyst 2960 Series Switch Security Configuration Guide*. Retrieved from Cisco Systems: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/15-0_2_se/security/configuration/guide/scg2960.html

Convery, S. &. (2004). *Attacking 802.1Q and Cisco Proprietary VLANs.* IEEE Computer Society.

Droms, R. (1997). *Dynamic Host Configuration Protocol (RFC 2131)*. Retrieved from Internet Engineering Task Force: https://tools.ietf.org/html/rfc2131

Engineers., I. o. (2020). *IEEE Std 802.1Q-2018 - IEEE Standard for Local and Metropolitan Area Networks--Bridges and Bridged Networks.* Retrieved from IEEE Standards Association: https://standards.ieee.org/ieee/802.1Q/6844/

Northcutt, S. C. (2021). *Intrusion Signatures and Analysis (2nd ed.).* New Riders Publishing.

Stallings, W. (2020). *Network Security Essentials.* Pearson Education.

Technology, N. I. (2022). *Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations*. Retrieved from NIST : https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final