ASIA PACIFIC UNIVERSITY OF TECHNOLOGY & INNOVATION
CT037-3-2-NWS
Network Security
Group Assignment

This assignment contributes 50% of the final marks

Intake : APU2F2409IT(DT), APU2F2409IT(CE), APU2F2409CS, APD2F2409IT(ISS), APD2F2409IT(IOT), APD2F2409IT(FT), APD2F2409IT(DT), APD2F2409IT(CE), APD2F2409CS, APU2F2409IT(FT), APU2F2409IT(ISS), APU2F2409IT(OT)

Lecturer : Nor Azlina Abd Rahman
Email : nor_azlina@apu.edu.my

LEARNING OUTCOMES:

- CLO2: Propose a network that demonstrates a working IP configuration for an organisation. (A5, PLO4)
- CLO3: Build a secure network by integrating layer 2 security, layer 3 security, Virtual Private Network or firewall technologies using appropriate simulation tool. (P3, PLO3)

In-course Assignment Information Assignment

This assignment consists of **TWO (2)** sections: Section A and Section B. Section A is group that contributes 20% of total 50% while Section B is the remaining 30%.

Instructions:

This group assignment carries **50%** of your total module assessment marks [Group Assignment], with 60% of the total contributed by an individual component and 40% by group components. A group consist of maximum **5** students. (Minimum 2 students). The total word count for both reports should **not exceed 5000 words**. No marks will be awarded for the entire assignment if any part of it is found to be copied directly from printed materials or from another group. All submissions should be made on or before the due date. Any late submissions after the deadline will not be entertained. **Zero (0)** mark will be awarded for late submission, unless extenuating circumstances are upheld.

Section A: GROUP COMPONENT (40%)

Scenario:

Starcom Asia Sdn Bhd is a network cable manufacturing company based in Penang. The headquarter office in Penang consists of 3 departments: Sales, Engineering and Finance. It has a branch company in Krung Thep, Thailand located 250km away from Penang and hosts 100 employees in each department. Only R&D and Delivery departments are located there. Figure 1 illustrates the network architecture and topology of the Penang HQ and its branch in Krung Thep for Starcom Asia Sdn Bhd.

The Penang HQ has simple network architecture. Clients' workstations are connected to an access switch, distributed switch and the router's internal interface as shown in figure 1. The firewall's external interface connects directly to the internet service provider (ISP) router. The ISP completely manages this router and the Starcom Asia Sdn. Bhd. has no control over it. A third interface on the firewall hosts a demilitarised zone (DMZ) hosting several servers. These servers include web, email, and FTP applications.

a) In a group, design and configure basic network requirements based on network diagram given using packet tracer. The design must follow the basic requirements as below:
   - Use any private IP address range for the LAN in Penang and Krung Thep network.
   - Use any public IP address range for the DMZ area and WAN connections including the router in the ISP cluster.

Guidelines for the Group Report:

Note: Phase 1 – Presentation, Group Report and Packet Tracer – Group Assessment – 21th April 2025 – 25th April 2025] – Group Report submission in Moodle [Only the group leader to submit – 27th April 2025]. The total word count of the main body of the document (excluding title & contents pages) is to be in the region of 1000 - 2000 words.

1. Table of contents for every detailed chapter/section.
2. Detailed Work Breakdown Structure. Contribution of each member.
3. Introduction
4. Topology of the network diagram – LAN and WAN topology used. – screen shots and explanations.
5. IP addressing table – VLSM and explanations.
6. Conclusion
7. References

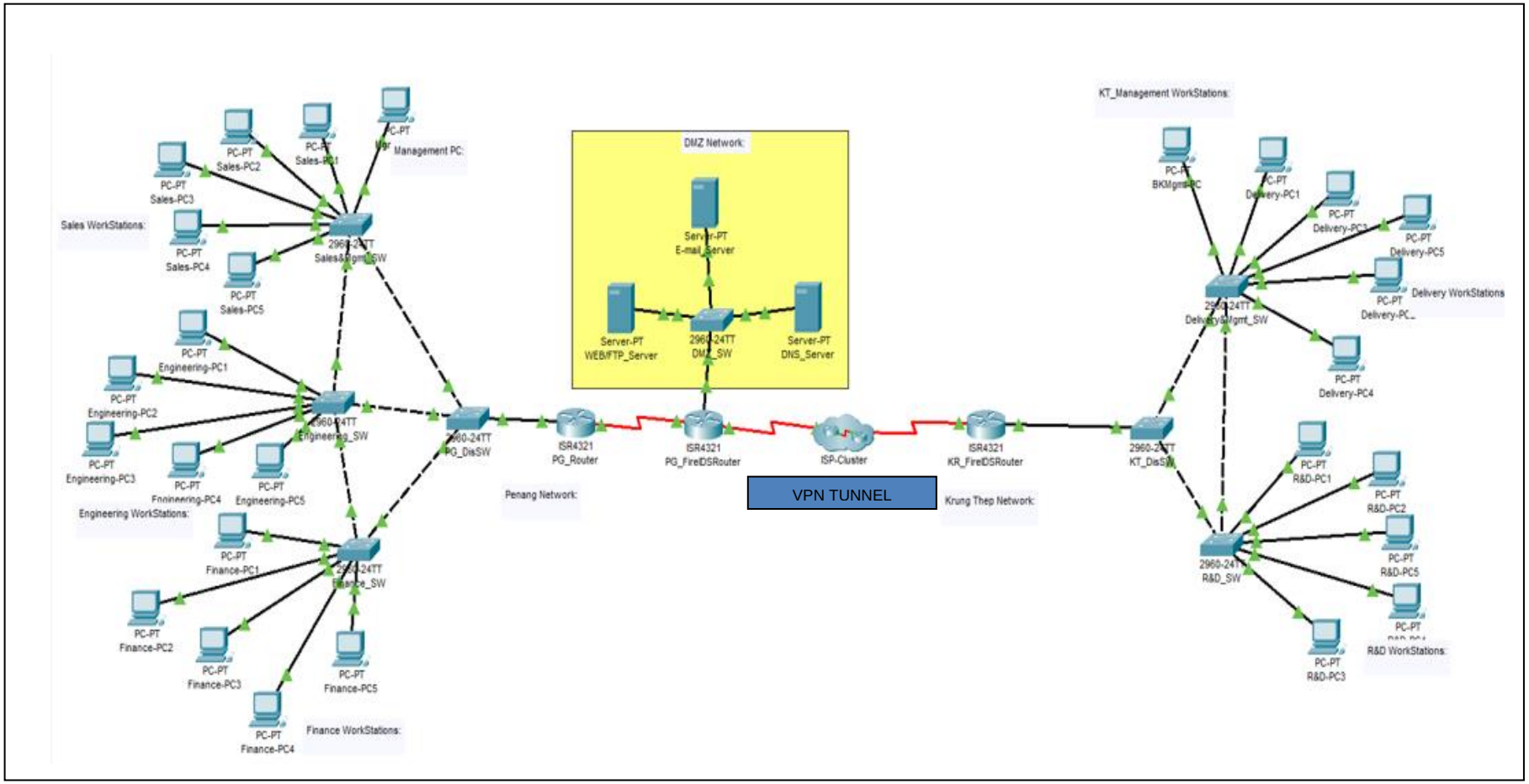


Figure 1: Starcom Asia Sdn Bhd Network Layout

Page **4** of **9**

Section B: INDIVIDUAL COMPONENT (60%)

a) The goal is to protect the internal and DMZ hosts from external threats. As a network security specialist, each of you are required to provide a security solution for Penang HQ and Krung Thep Branch office.

There are some requirements in the above scenario that must be considered in this security design.

1. Client workstations (sales, engineering, finance, R&D and delivery) must be able to access the web server at the DMZ over **HTTP and HTTPS.** The web server should be reachable from the external clients over HTTP and HTTPS only. (Solution and configuration)

2. 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)

3. Engineering, finance and sales workstations must be able to access the Internet (to reach the branch company) over ICMP, HTTP and HTTPS with **DNS.** No other protocol access is allowed to the Internet. (Solution and configuration)

4. 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). Propose one protocol to ensure that the email transactions are secured between sender and receiver. (Solution and configuration)

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)

6. Proposed several policies for both networks (Penang and Krung Thep) to reduce the internal/external access to its resources. Suggest appropriate **ACL** to be deployed for the three main networks. Examples: No client from sales, engineering and finance department can access clients in the other departments and any. (Solution and configuration)

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

8. **Bastion host** works as an application proxy. You are required to explain the solution in detail. (Solution)

9. Connectivity between HQ in Penang and branch office in Krung Thep 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. (Solution and configuration)

10. 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)

11. The company requires implementing **intrusion detection systems (IDS).** (Solution)

12. Implement **VPN** between Penang and Krung Thep network. (Solution and configuration)

Page **5** of **9**

13. Implement **SSL** encryption between Penang and Krung Thep. (Solution)

14. Proposed other **TWO (2)** security mechanisms that can be deployed to strengthen the internal and DMZ hosts from external threats. (Solution)

Note: The "solution" in the parenthesis means that, you have to recommend, what should be done in order to fulfil the company's requirement. In this case, you do not have to configure any of the device(s) in the topology. The "configuration" in the parenthesis means that, in addition to the solution that you provide, you must implement it by configuring the appropriate device with commands and setups.

Guidelines for the Individual Report:
Document the results of your work in a **professional and systematic** manner, in the form of a **computerized report**. **One (1**) softcopy of your documentation is to be submitted.

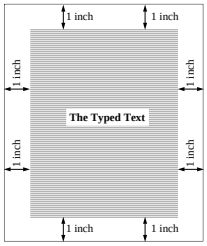
Your completed documentation should meet the following requirements:

1. Table of contents for every detailed chapter/section.
2. Introduction
3. Topology of the network diagram – screen shots and explanations
4. Chapters / sections with screen shots for evidence
5. Documentation of the configured device(s) – Passwords etc.
6. Conclusion
7. Appendices [Optional]
8. Bibliography or References

In your document the report is to be written in a professional manner, paying due regard to the following aspects:

- The report is to be written in the 3rd person.
- The report should have a consistent layout and be divided into enumerated sections, sub-sections, sub-sub sections etc.
- The report should be fully referenced using the University standard.
  - ✓ Expected Turnitin overall similarity is below 20% (excluding cover page and table of content).
  - ✓ Note: Link to self-check the similarity: https://apiit.atlassian.net/servicedesk/customer/portal/4/article/1117945857?src=668985563
- Your report must be typed using Microsoft Word with Times New Roman font and size 12. Expected length is 5,000 words (excluding diagrams, appendixes, and references). You need use to include a word count at the end of the report and it should be in 1.5 spaces.
- Submission of reports that are unprofessional in its outlook (dirty, disorganised, inconsistent look, varying coloured paper and size) will not fare well when marks are allocated.
- Ensure that the report is printed on standard A4 (210 X 297 mm) sized paper.
- The report should have a one (1") margin all around the page as illustrated below:

Page **6** of **9**



- Every report must have a front cover. A transparent plastic sheet can be placed in front of the report to protect the front cover. The front cover should have the following details:
  - Name
  - Intake code.
  - Subject.
  - Project Title.
  - Date Assigned (the date the report was handed out).
  - Date Completed (the date the report is due to be handed in).

Submission requirements

An online submission through Moodle is required for this module for both individual and group sections. The total word count of the main body of the document (excluding title & contents pages) is to be in the region of 3000 words. **Submission of the individual report and walk-through video - 18th May 2025]**

Demonstration on the results of your work in a **professional and systematic** manner, in the form of a **video recording**. **One (1**) softcopy of your video file is to be submitted individually in another Moodle link that will be provided.

- The recording should include 1 minute of introducing the name and programme followed by 10 -15 minutes of showing the configuration and skills that has been gathered or used in the configuration.
- Students need to demo their configuration skills in packet tracer only. DO NOT need to include the report.
- Please dress formally for the presentation and do turn on the webcam throughout the demo and make yourself available during the demo.
- Make sure the audio also being recorded during the demo.

Page **7** of **9**

Assessment Criteria:

PLO3- Practical skills: Marking Scheme Rubrics: Individual Part – 60%

Marking Criteria	1 (Fail)	2 (Marginal Fail)	3 (Pass)	4 (Credit)	5 (Distinction)	Weightage
Protocol Implementation (20%)	Limited ability to implement and configure network protocols.	Basic ability to implement and configure network protocols for simple scenarios.	Acceptable ability to implement and configure network protocols for most scenarios.	Good ability to implement and configure network protocols for most scenarios.	Excellent ability to implement and configure network protocols for complex scenarios.	**4**
Security Measures (20%)	Limited understanding of security measures and unable to implement them effectively.	Basic understanding of security measures and can implement them effectively for simple scenarios.	Acceptable understanding of security measures and can implement them effectively for most scenarios.	Good understanding of security measures and can implement them effectively for most scenarios.	Excellent understanding of security measures and can implement them effectively for complex scenarios.	**4**
Utilization of tools for network design (20%)	Hardly able to use packet tracer simulation tool in providing network design.	Basic ability to use packet tracer simulation tool providing network design.	Satisfactory use of packet tracer simulation tool providing network design.	Good use of packet tracer simulation tool providing network design.	Excellent use of packet tracer simulation tool providing network design.	**4**
Referencing (15%)	No in-text citation and very minimal references. Major issues in the referencing format. Referencing was done manually, without using Microsoft Word features	Minimal in-text citation and references used. Minor issues in the referencing format. Not able to fully utilize the referencing features in Microsoft Word	Enough references and citation in the report. No issue in the referencing format Able to fully utilize the referencing features in Microsoft Word	Recent source of references used, with proper reference list. Limited in-text citation in the report Good utilization of the referencing features in Microsoft Word	Very good quality of references used, with proper citation and reference list for all facts and diagrams used Proficient in using the referencing features in Microsoft Word, without error	**3**
Documentation (10%)	No table of content and page numbering, font size and type are not standardized. Not able to show personal skills in utilizing features in Microsoft Word to produce good	Table of content exist but without page numbers, report structure not standardized (including alignment and spacing). Able to show some personal skills in utilizing features in Microsoft Word but has major issues in	Table of content included with proper page numbering, standardized report structure & headings. Able to show sufficient personal skills in utilizing features in Microsoft Word to produce good formatting	Good structure and flow of documentation with appropriate header & footer. Good personal skills in utilizing features in Microsoft Word to produce good formatting standard without any issue.	Very good structure and flow of documentation, with very good appearance. Very good and proficient personal skills in utilizing features in Microsoft Word to produce outstanding formatting standard.	**2**

Page **8** of **9**

	formatting standard.	formatting standard.	standard, with minor issues.			
Presentation Skills (15%)	Poor understanding on the configuration.	Able to show minimal understanding on the configuration done.	Show good understanding in configuration but can be improved in technical and IP addressing scheme knowledge. Not very good in explaining technical configuration and average verification commands.	Very good understanding in configuration and IP addressing scheme deployed. Able to explain technical configuration and good verification commands.	Outstanding configuration skills demonstrated, exceeding the expectation. Able to explain technical configuration and excellent verification commands.	**3**
Total Marks (Criteria 1):						**/100**

Page **9** of **9**

PLO4 - Interpersonal skills. Marking Scheme Rubrics: Group Part – 40%

Marking Criteria	1 (Fail)	2 (Marginal Fail)	3 (Pass)	4 (Credit)	5 (Distinction)	Weightage
Leadership (15%)	Poor leadership and teamwork	Acceptable leadership and teamwork	Moderate leadership and teamwork	Good leadership and teamwork	Outstanding leadership and teamwork	**3**
Task distributed equally and appropriate security technologies chosen (15%)	Imbalance distribution of tasks among the team members. No discussion on technologies chosen	Imbalance distribution of tasks among the team members. Inaccurate technologies chosen with very brief explanation provided	Fair distribution of tasks among the team members. Acceptable technologies chosen with brief explanation provided	Fair distribution of tasks among the team members. Acceptable technologies chosen and detail explanation provided.	Balance distribution of tasks among the team members. Accurate technologies chosen. Detail explanation provided	**3**
Design follows the requirements and good integration (25%)	All submission requirements were not adhered or poor writing or poor quality of contents. No integration of the tasks given.	Network design follows the requirements but with some missing parts. Partially integrated and not all the configurations are working after integration.	Network design and configurations follow the requirements but with some missing parts. Fully integrated but not all the configurations are working after integration.	Network design and configurations follow exactly the requirements. No missing part. Fully integrated and configuration is working well.	Outstanding configuration. All requirements fulfil with extra configuration implemented. Fully integrated and configuration is working well.	**5**
IP configurations. (20%)	Poor addressing table provided but configuration done with major issue.	Acceptable addressing table provided with basic configuration.	Moderate addressing table provided with good configuration done,	Good addressing table provided with good configuration done.	Outstanding addressing table provided with outstanding configuration done.	**4**
WAN Configuration Techniques (25%)	WAN Configuration not clear. No configuration found.	Incomplete WAN configuration. Major issues in configuration (some parts are unable to ping).	Feasible WAN configuration with minimum requirement for the selected technique. Minimal issues in configuration – not fully working according to the network design.	Feasible WAN configuration to demonstrate the selected technique Successful LAN and WAN configuration (able to ping to all devices).	Good quality / WAN configuration. Extra effort shown to create a good design. Successful LAN and WAN configuration (able to ping to all devices).	**5**
Total Marks (Criteria 2):						**/100**