ASIA PACIFIC UNIVERSITY OF TECHNOLOGY & INNOVATION

**CT133-3-2-SRE**

**Switching and Routing Essentials**

**Individual Assignment**

**This assignment contributes 40% of the final marks**

**Intake : APU2F2302CS(CYB), APD2F2302CS(CYB), APU2F2302IT(CE), APD2F2302IT(CE)**

**Lecturer : Qistina Najwa binti Mohamad Farid**

**Email :** [**qistina.najwa@ apu.edu.my**](mailto:qistina.najwa@%20apu.edu.my)

**LEARNING OUTCOMES:**

* CLO3: Propose WLAN concepts and configuration using WLC and Layer 2 security best practices (A3, PLO9) – Configuration and Report
* CLO4: Demonstrate the strategies to implement switch security to mitigate LAN attacks using appropriate tools (A3, PLO6) – Configuration and Report

***Note:***

***PLO9 – Personal Skills:***

Personal skills are life skills that learners are expected to use daily. They are normally portrayed through enthusiasm for independent learning, intellectual and self-development; by demonstrating confidence, self-control; social skills and proper etiquette; and commitment to professionalism in the workplace. It also includes capability to plan for career development or further education. Aspects of character such as honesty, punctuality, time management, keeping to and maintaining deadlines that are important in a work environment are also important personal skills.

***PLO6 – Digital Skills:***

Digital skills generally refer to the ability to use information/digital technologies to support work and studies. The skills include sourcing and storing information, processing data, using applications for problem solving and communication, as well as ethics in applying digital skills.

**Instructions:**

This individual assignment carries **40%** of your total module assessment marks. The total word count of the report 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 student. 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.

SCENARIO

**Aspiro Sdn. Bhd.** is a networking company that has planned to upgrade their IT services in their existing locations i.e., in KL (HQ) and Brunei (Remote Branch). The network administrator in Brunei has planned to replace the current configuration with new VLAN design to make the network more efficient and to enhance the security of the network especially in HQ branch located in KL. Apart from that, the KL Server Farm will be managed remotely by the Management department in HQ. For the Brunei network, the network administrator has planned to deploy WLC WLAN to ease the configuration of Wireless network and its access.

The company may be characterised by its departments. The names and locations of these departments are as follows:

* Management – (KL Site)
* Human Resource (HR) - (KL Site)
* Design - (KL Site)
* Delivery - (KL Site)
* R&D - (Brunei Site)
* WLC Management - (Brunei Site)
* Server Farm - (KL Server Farm)

As a newly appointed network executive, you have been asked to work on the design and prototype of the new network. You need to create the logical topology as stated in figure 1 below and configure all devices using Cisco Packet Tracer as the simulator to evaluate the design.

Chart

Description automatically generated

Figure 1: Logical Topology for **Aspiro Sdn. Bhd.**

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

1. Implement DHCPv4 to operate across multiple LANs.
2. Configure a WLC WLAN to use a VLAN interface, a DHCP server, and WPA2 authentication. – Brunei network – VLAN 10 – 192.168.10.0, Management VLAN – 192.168.100.0/24 etc. Optional – Radius server.
3. Configure IPv4 static/dynamic routes.
4. Implement port security to mitigate L2 attacks.

Each student is required to provide an individual report to justify the network topology and IP addressing used in network plan. A written report should be completed based on the network design and configurations implemented in Cisco Packet Tracer. Below are the proposed guidelines for the report:

**Guidelines for the Report [2 sections]:**

Document the results of your work in a **professional and systematic** manner, in the form of a **computerized report**. Your completed documentation should meet the following requirements:

**Section A: [Report]**

1. Table of contents for every detailed chapter/section.
2. Introduction
3. Proposed WLAN Architecture. Explanation and screenshots on configuration. [T&P]
4. Types of security attacks on Layer 2 and security deployment to mitigate the attacks. [Maximum – Three (3) L2 attacks and Three (3) mitigation techniques] – [T]
5. Conclusion
6. References

**Section B: [Report and Packet Tracer] and video submission.**

1. Table of contents for every detailed chapter/section.
2. Introduction
3. Entire Network Layout – packet tracer
4. LAN and WAN configuration. Explanation and screenshots on configuration. [T&P]
5. Layer 2 Security Mechanisms Deployment in configuration. Explanation and Screenshots. [T&P]
6. Conclusion
7. Appendices (network configurations and screen shots)
8. References

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 – APA style. <https://library.apiit.edu.my/apa-referencing/>
* Your report must be typed using Microsoft Word with Times New Roman font and size 12. **Expected length is 2,500 words (excluding diagrams, appendixes, and references) for each report**. You need use to include a word count at the end of the report and it should be in 1.5 spaces.
* Every report must have a front cover with 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:**

Students are required to hand in their assignment (softcopy only) on time to the Online Submission System (Moodle – Turnitin Assignment). In addition, demo / presentation of the network design will be scheduled for all students before submission date.

**LINK to check your Similarity report: Self Enrolment:**

<https://apiit.atlassian.net/servicedesk/customer/portal/4/article/1117945857?src=668985563>

**Submission of both reports and video Week 12 [22nd May 2023 – 11:59 pm].**

**Video submission Week 12 [in Moodle – Walk through the .pkt files] – 3-5 min. duration.**

**Note: DO NOT duplicate the content in section A and B.**

The submission includes:

* 2 Reports in Ms. Word (assessed in Criteria A and Criteria B)
* Softcopy of network design (Cisco Packet Tracer diagram) – Criteria B
* Video submission.

**Assessment Criteria: Marking Scheme (Overall 100%)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Criteria A: CLO3: Propose WLAN concepts and configuration using WLC and Layer 2 security best practices (A3, PLO9) – Personal Skills [100 Marks] | | | | | | |
| **Marking Criteria** | **1**  **(Fail)** | **2**  **(Marginal Fail)** | **3**  **(Pass)** | **4**  **(Credit)** | **5**  **(Distinction)** | **Weightage** |
| **Proposed WLAN Architecture**  **(30%)** | Poor proposal on WLAN architecture were provided  (Not feasible). | Inadequate justification on the WLAN architecture and its security mechanisms | The justification on the proposed WLAN architecture and its security mechanisms are clearly written | The justification on the proposed WLAN architecture and its security mechanisms are comprehensive, with sufficient rationalizations. | The justification on the proposed WLAN architecture and its security mechanisms has good rationalizations and critical discussion | **6** |
| **Security attacks and security mechanisms to be deployed**  **(20%)** | Poor justifications on the security attacks and security mechanisms deployment on Layer 2 were provided  (Not feasible). | Inadequate justification on the security attacks and security mechanisms deployment on Layer 2 | The justification on the security attacks and security mechanisms deployment on Layer 2 are clearly written | The justification on the security attacks and security mechanisms deployment on Layer 2 are comprehensive, with sufficient rationalizations. | The on the security attacks and security mechanisms deployment on Layer 2 has good rationalizations and critical discussion | **4** |
| **Research & Investigation**  **(20%)** | Poor research and investigation of the problem. Poor evaluation of the requirement | Inadequate research and investigation of the problem. Poor evaluation of the requirement. | Well research and investigation are done. Good evaluation of the requirements with proper reasoning with proper project planning and management. | Very well analysis and investigation of the problem. Outstanding evaluation of the requirements with proper reasoning. Outstanding project planning and management with the screenshots of used tools. | Poor research and investigation of the problem. Poor evaluation of the requirement. | **4** |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Marking Criteria** | **1**  **(Fail)** | **2**  **(Marginal Fail)** | **3**  **(Pass)** | **4**  **(Credit)** | **5**  **(Distinction)** | **Weightage** |
| **Referencing**  **(20%)** | 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 and lack of originality. | Enough references and citation in the report. No issue in the referencing format  Able to fully utilize the referencing features in Microsoft Word. Lack of originality. | 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. | **4** |
| **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 formatting standard | 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 formatting standard | 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 standard, with minor issues. | 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** |
| **Total Marks (Criteria 1)** | | | | | | **/100** |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Criteria B: CLO4: Demonstrate the strategies to implement switch security to mitigate LAN attacks using appropriate tools (A3, PLO6) – Digital Skills [60 Marks] | | | | | | |
| **Marking**  **Criteria** | **1**  **(Fail)** | **2**  **(Marginal Fail)** | **3**  **(Pass)** | **4**  **(Credit)** | **5**  **(Distinction)** | **Weightage** |
| **Network Design**  **(20%)** | Network design is not clear. Minor issues in network design (not feasible). | Feasible network design, meeting the minimum requirement of a network. | Good network design showing complete setting of the network | Good quality / complexity of network design. | Excellent quality / complexity of network design.  Good justification for the diagrams with citation (if needed) | **4** |
| **LAN and WAN Configuration Techniques**  **(20%)** | LAN and WAN Configuration not clear.  No configuration found. | Incomplete LAN and WAN configuration.  Major issues in configuration (some parts are unable to ping). | Feasible LAN and WAN configuration with minimum requirement for the selected technique.  Minimal issues in configuration – not fully working according to the network design. | Feasible LAN and WAN configuration to demonstrate the selected technique  Successful LAN and WAN configuration (able to ping to all devices). | Good quality / complexity of LAN and WAN configuration. Extra effort shown to create a good design.  Successful LAN and WAN configuration (able to ping to all devices). | **4** |
| **Layer 2 Security Mechanisms Deployment in configuration**  **(20%)** | Layer 2 security mechanisms implemented is not clear.  None or only one mechanism deployed. (Not feasible). | Feasible layer 2 security mechanisms implemented, meeting the minimum requirement of a network. | Good layer 2 security mechanisms implemented, showing complete coverage on the security setting of the network  Satisfactory number of relevant mechanisms provided in the network plan | Good quality / complexity of layer 2 security mechanisms implemented.  Good number of relevant mechanisms provided in the network plan | Excellent quality / complexity of layer 2 security mechanisms implemented.  Very good choice of relevant mechanisms good justification for the diagrams with citation (if needed) | **4** |
| **Timeline**  **(10%)** | Not showing any progress. | Hardly able to show the progress on time.  Incomplete work as working far behind the expected timeline. | Putting effort in providing the progress on time but showing incomplete work. Need major modifications to the work done | Complete work showed. However, work need some changes and modifications for improvement. | Very good quality of work showed. Well prepared, and not doing last minute work | **2** |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Demonstration** | | | | | | |
| **Marking**  **Criteria** | **1**  **(Fail)** | **2**  **(Marginal Fail)** | **3**  **(Pass)** | **4**  **(Credit)** | **5**  **(Distinction)** | **Marks Awarded** |
| **Utilization of tools for network design**  **(20%)** | Hardly able to use packet tracer simulation tool in providing network design. | Least use of 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** |
| **[Video Submission- content]**  **(10%)** | Not submitting for project demonstration.  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. | **2** |
| **Total Marks (Criteria 2)** | | | | | | **/100** |

**Final Marks Calculation**

|  |  |  |  |
| --- | --- | --- | --- |
| **A** | **B** | **C** |  |
| **Criteria 1 (16%)** | **Criteria 2 (24%)** | **Grand Total (40%)** | **Final Assignment Marks (100%)** |
| **X / 100** | **X / 100** | **A + B** | **(C)/40 \* 100** |

**Appendices:**

**HQ Network – KL:**

Chart, radar chart

Description automatically generated

Figure 2: KL Network

**Networks:**

1. **HR – 172.16.10.0/24**
2. **Design – 172.16.30.0/24**
3. **Delivery – 172.16.20.0/24**
4. **Management – 172.16.50.0/24**
5. **BlackHole [Unused Ports]**
6. **Native**

Diagram

Description automatically generated

Figure 3: Server Farm Network

**Networks:**

1. **ServerFarm – 198.51.100.0/24**
2. **BlackHole [Unused Ports]**
3. **Native**

**Remote Branch Network – Hanoi:**

Diagram

Description automatically generated

Figure 4: Brunei Network

**Networks:**

1. **RBMgmt – 192.168.100.0/24**
2. **R&D-Wireless – 192.168.10.0/24**
3. **BlackHole [Unused Ports]**

**WAN Connections:**

Diagram

Description automatically generated

Figure 5: WAN Network

A picture containing chart

Description automatically generated

Figure 6: ISPs Network

**WAN Connections:**

1. **WAN 1 – 200.100.100.0/30**
2. **WAN 2 – 200.100.100.4/30**
3. **WAN 3 – 200.100.100.8/30**
4. **WAN 4 – 200.100.100.12/30**
5. **WAN 5 – 200.100.100.16/30**
6. **WAN 6 – 200.100.100.20/30 [Extra WAN required for HSRP Configuration]**

Diagram

Description automatically generated

Figure 7: ISPs Network - Enlarge