# SUMMATIVE ASSESSMENT 1

|  |  |  |  |
| --- | --- | --- | --- |
| **Student Name** |  | **Student ID** |  |
| **Unit Code & Title/s** | NSA 207- Manage VLANs and WANs | **Semester** | 2024-10 |
| **Qualification Title** | Network and Systems Administration | | |

## Instructions

* Before commencing an assessment task, it is recommended that you:
  + Review the relevant learning material for the unit/s; and
  + Read the assessment instructions carefully. If anything is not clear, speak to your Assessor.
* Complete each assessment task described in this document and submit your work in Blackboard for marking.
* All tasks must be completed individually. Plagiarised work will not be accepted.
* Any words, ideas or images that you have taken from another source must be referenced.
* Once the assessment process is complete, upload the items listed below to your Blackboard Student Portfolio:
  + All portfolio evidence;
  + Other assessment documents as required by your teacher.

## Your Portfolio

* The Student Acknowledgment and Feedback Forms in this document show the portfolio evidence required for each Performance Criteria (PC).
* All documents you upload must show your name, student ID, signature, and date.
* If you are making a video or voice recording for your portfolio, please include the following information at the start of the record:
  + Your name and student ID
  + The unit title
  + The Performance Criteria being assessed
  + The date recorded.
* Any digital media such as a photo, video or voice recording, must be accompanied by a Digital Media Evidence Form.

|  |
| --- |
| **Summative Assessment 1**  **Task 1:**  **Learning Outcome/s**  LO1: Configure VLANs across various switches and routers to create segmented network environments.  LO4: Apply security protocols to VLANs and WANs to maintain data integrity and confidentiality.  **Performance Criteria**  PC1.1-Configure VLANs, including port assignments and VLAN IDs  PC1.2-Manage VLAN configurations and security settings  PC1.3-Implement and validate inter-VLAN routing to ensure communication across different  PC4.1-Configure security settings on network devices within VLANs and WANs to enforce data integrity and confidentiality. |

**Assessment Summary:**

The assessment focuses on evaluating the student's ability to configure, manage, and secure VLANs on switches and implement inter-VLAN routing. The assessment covers the following Performance Criteria (PCs): PC 1.1, 1.2, and 1.3. PC 4.1 (security settings on network devices within VLANs) is assessed as part of the tasks related to PC 1.2. The assessment includes both mandatory and optional tasks, with the latter offering opportunities for Merit and Distinction grades. The tasks involve configuring VLANs, subinterfaces, and implementing inter-VLAN routing. The assessment utilizes Packet Tracer for a hands-on, simulated learning experience, and incorporates elements to ensure authenticity.

**Business Case Scenario: SecureNet Solutions Network Upgrade**

You're a network technician at SecureNet Solutions, tasked with upgrading and securing the network infrastructure for a growing client. The client currently has three departments (Sales, Marketing, and IT) operating on a flat network, which is causing security and performance issues. They also rely on a PPPoE connection for their WAN link, which needs to be more resilient and secure. Additionally, the client wants to implement network monitoring and troubleshooting capabilities to proactively identify and address potential issues.

**Your Mission:**

1. **VLAN Segmentation:** Implement VLANs to segment the network into separate broadcast domains for each department (Sales, Marketing, and IT), improving security and performance.
2. **WAN Resilience and Security:** Enhance the PPPoE WAN connection by configuring CHAP authentication and setting up a backup PPPoE link for redundancy.
3. **Network Monitoring and Troubleshooting:** Configure SPAN (Switched Port Analyzer) to monitor network traffic and assist in troubleshooting potential issues.
4. **Switch Security:** Harden the switch configuration by disabling DNS lookup, setting strong passwords, encrypting clear-text passwords, and displaying a warning banner (MOTD).
5. **Advanced Configurations (Optional):** For those seeking to demonstrate advanced skills, there are opportunities to configure inter-VLAN routing, VTP, SSH access, DHCP relay, port security enhancements, and WAN bandwidth management.

**Success Criteria:**

* **Competent:** Successfully complete all mandatory tasks, demonstrating a basic understanding of VLANs, WAN connections, and switch security.
* **Competent with Merit:** Complete all mandatory tasks and at least one optional Merit task, showcasing a deeper understanding and the ability to apply knowledge effectively.
* **Competent with Distinction:** Complete all mandatory tasks and at least one optional Distinction task, exhibiting exceptional skills, critical thinking, and problem-solving abilities.

**Remember:**

* Use the provided Packet Tracer file ("a-LO1 and 4-TASK 1-Packet Tracer") to complete the assessment tasks.
* Replace placeholders (e.g., usernames, passwords) with actual values provided by your instructor.
* Provide clear and concise screenshots as evidence of your configurations and verifications.
* Refer to the additional resources provided for guidance and support in completing the optional Merit and Distinction tasks.

By successfully completing this assessment, you will demonstrate your competency in configuring, managing, and securing VLANs and WAN connections, essential skills for any network technician in today's business environment.

Good luck!

**The IP addressing scheme for the LANs and WAN links is as follows:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Location | Network Address | First Usable Host Address | Last Usable Host Address | Broadcast Address | Interface (Router) | IP Address (Interface) |
| **Sharjah LAN** | **192.168.1.0/24** | **192.168.1.1** | **192.168.1.254** | **192.168.1.255** | **R1 G0/0**  **G0/0.<sales vlanid>**  **G0/0.<Marketing vlanid>**  **G0/0.<IT vlanid>** | **192.168.1.254**  **192.168.10.1/24**  **192.168.11.1/24**  **192.168.12.1/24** |
| **Abu Dhabi LAN** | **192.168.2.0/24** | **192.168.2.1** | **192.168.2.254** | **192.168.2.255** | **R2 G0/0** | **192.168.2.254** |
| **Dubai LAN** | **192.168.3.0/24** | **192.168.3.1** | **192.168.3.254** | **192.168.3.255** | **R3 G0/1** | **192.168.3.254** |
| **WAN-1** | **10.0.12.0/30** | **10.0.12.1** | **10.0.12.2** | **10.0.12.3** | **R1 S0/0/0** | **10.0.12.1** |
|  | **R2 S0/0/0** | **10.0.12.2** |
| **WAN-2** | **10.0.13.0/30** | **10.0.13.1** | **10.0.13.2** | **10.0.13.3** | **R2 S0/0/1** | **10.0.13.1** |
|  | **R3 S0/0/1** | **10.0.13.2** |

**Task 1: Configure and Secure VLANs**

|  |  |
| --- | --- |
| Assessed Task | Screenshot Evidence |
| Rename Switch S1, S2 and S3 and Router R1, R2 and R3 as follows:  Switch: S1-YourName-Last 3 digits of your ID (S1-Saleel-265) Router: R1-YourName-Last 3 digits of your ID (R1-Saleel-265) | After the rename switch and router name should be as follows: use your name and ID  Switch: S1 = S1-Saleel-265 S2= S2-Saleel-265 S3= S3-Saleel-265  Router: R1 = R1-Saleel-265 R2= R2-Saleel-265 R3= R3-Saleel-265 |
| PC 1.1: Access the switch “S1-yourname-id” and create three VLANs.  Use VLAN IDs calculated by adding 100 to the last three digits of your student ID (e.g., if your ID ends in 265, use VLAN IDs 102 (2+100), 106 (6+100), and 105(5+100)).  Name the VLANs "Sales," "Marketing," and "IT" respectively. | Provide screenshots showing the configuration and verification of the VLANs. |
| PC 1.1:  Assign ports 1-3 to the "Sales" VLAN,  Assign ports 4-6 to the "Marketing" VLAN,  Assign ports 7-9 to the "IT" VLAN. | Provide screenshots showing the configuration and verification of the port assignments. |
| PC 1.2 & PC 4.1: Rename the "Sales" VLAN to "Finance". | Provide a screenshot showing the VLAN renaming and verification. |
| PC 1.2 & PC 4.1: Disable DNS lookup on the switch | Provide a screenshot showing the configuration and verification of DNS lookup being disabled. |
| PC 1.2 & PC 4.1: Set the switch name to "S1-[YourName]-[Last 3 digits of your ID]".  For example: S1-Saleel-265 | Provide a screenshot showing the configuration and verification of the switch name. |
| PC 1.2 & PC 4.1: Set an encrypted privileged exec password "class". | Provide a screenshot showing the configuration and verification of the encrypted privileged exec password. |
| PC 1.2 & PC 4.1: Set the console access password to "cisco". | Provide a screenshot showing the configuration and verification of the console access password. |
| PC 1.2 & PC 4.1: Set the Telnet access password to "cisco". | Provide a screenshot showing the configuration and verification of the Telnet access password. |
| PC 1.2 & PC 4.1: Encrypt all clear text passwords. | Provide a screenshot showing the configuration and verification of password encryption. |
| PC 1.2 & PC 4.1: Set the MOTD banner to "Unauthorized Access is Prohibited!". | Provide a screenshot showing the configuration and verification of the MOTD banner. |
| PC 1.3: On R1,  Enable the g0/0 interface  create sub-interfaces on interface G0/0.<vlanid> for all three VLANs created in PC 1.1. -Use dot1q encapsulation  -Set the correct IP address per sub interface: 1st vlan-Sales/Finance:  IP address 192.168.10.1 255.255.255. 0  2nd vlan-Marketing: IP address 192.168.11.1 255.255.255.-0  3rd Vlan-IT: IP address 192.168.12.1 255.255.255.0  For example: for vlan 102, create sub-interface g0/0.102 | Provide screenshots showing the sub-interface configuration and verification for each VLAN. |
| PC1.3: Configure Switch S1-<yourname>-<ID> g0/1 interface to a trunk mode | Provide a screenshot showing the Trunk configuration |
| PC 1.3: Verify connectivity between devices in different VLANs using ping. | Provide a screenshot showing successful ping results between devices PC1, PC2, PC3 in different VLANs. |
| Optional - Merit (PC 1.1): Create an additional VLAN and assign it to unused ports on the switch. | \* **Steps:** Access the switch's configuration.  \* Create a new VLAN with a unique VLAN ID and a descriptive name (e.g., "Guest").  \* Assign any unused ports on the switch to this new VLAN.  \* Verify the VLAN configuration and port assignments using appropriate show commands.  \* \*\*Evidence:\*\* Provide screenshots showing the creation of the new VLAN, the port assignments, and the verification of the configuration. **Help Merit (PC 1.1):**   * **Lab:** [3.2.2.5 Lab-VLANs and Trunking.pdf](https://hctuae-my.sharepoint.com/:b:/g/personal/sap_hct_ac_ae1/ESZegHEHYuhPq5yEPxPNeQMBV-pVspq2sfLt4XUdElc-sQ?e=aYPTfE) * **Video:** [Cconfiguring VLAN and Trunk](https://youtu.be/ykiSQ5ht-js?si=4fzd4FYgl9Sk7Gjc) |
| Optional - Merit (PC 1.2 & PC 4.1): Modify port security on ports 1-10 to allow a maximum of two MAC addresses per port and implement the 'restrict' violation mode. | **Steps:** \* Access the switch's configuration.  \* Enter the interface configuration mode for the range of ports 1-10  \* Modify the port security configuration to allow a maximum of two MAC addresses per port  \* Set the violation mode to 'restrict'  \* Verify the updated port security configuration using appropriate show commands  \*\*Evidence:\*\* Provide screenshots showing the modified port security configuration and verification  **Help Merit (PC 1.2 & PC 4.1):**   * **Lab:** [Configuring the Maximum Number of Secure MAC Addresses on a Port](https://www.cisco.com/en/US/docs/general/Test/dwerblo/broken_guide/port_sec.html" \l "wp1080631) * **Lab:** [Configuring the Port Security Violation Mode on a Port](https://www.cisco.com/en/US/docs/general/Test/dwerblo/broken_guide/port_sec.html#wp1055296) * **Video:** [Switch Security Configuration](https://youtu.be/Mniom9xrd98?si=9akYr4yM9qAjVfsM) |
| Optional - Merit (PC 1.3): Configure and verify a default gateway on each VLAN interface on R1 | \* **Steps:** \* Access the router's configuration  \* Enter the configuration mode for each VLAN subinterface  \* Configure the IP address of the subinterface as the default gateway for the corresponding VLAN  \* Verify the default gateway configuration on devices connected to each VLAN  \*\*Evidence:\*\* Provide screenshots showing the default gateway configuration on each VLAN subinterface and the verification of the default gateway on devices in each VLAN.  **Help Merit (PC 1.3):**   * **Lab:** [5.1.3.7 Lab - Configuring 802.1Q Trunk-Based Inter-VLAN Routing](https://hctuae-my.sharepoint.com/:b:/g/personal/sap_hct_ac_ae1/EadZv3jlEPNLrMfJEuEeO7UBlVLFOleMBnffEAROAsG0Sw?e=PmIMvK) * **Video:** [Inter-VLAN Routing Configuration](https://youtu.be/DtUoMwqnLLI?si=fvV6JA44rTsqptfc) |
| Optional - Distinction (PC 1.1): Configure and verify VTP (VLAN Trunking Protocol) on the switches to automate VLAN creation and propagation across the network. | **Steps:**  \* Add a new switch (S3) to the topology and connect it to S1 using a trunk port  \* Configure one switch as the VTP server and the other as a VTP client  \* Set the VTP domain name and password  \* Create new VLANs on the VTP server and verify that they are propagated to the VTP client  \* Make changes to VLAN configurations on the VTP server and verify that the changes are propagated to the VTP client  \*\*Evidence:\*\* Provide screenshots showing the VTP configuration on both switches, the creation and propagation of VLANs, and the verification of configuration changes  **Help Distinction (PC 1.1):**   * **Lab:** [Configuring VTP - Packet Tracer Lab](https://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/98154-conf-vlan.html#toc-hId-751508965) * **Video:** [VLAN Trunking Protocol (VTP) Configuration](https://youtu.be/rMjhI5uTdaY?si=Gwok6OZ973zatT6X) |
| Optional - Distinction (PC 1.2 and PC 4.1): Configure and verify SSH access to the switch, disabling Telnet for enhanced security. | **Steps:**  \* Generate an RSA key pair on the switch  \* Configure the switch to use SSH version 2  \* Create a local user account with a strong password and assign it to the appropriate privilege level  \* Enable SSH access and disable Telnet access  \* Verify SSH access by connecting to the switch using an SSH client  \*\*Evidence:\*\* Provide screenshots showing the SSH configuration on the switch, the attempt to connect using Telnet (which should fail), and the successful SSH connection using an SSH client.  **Distinction (PC 1.2 and PC 4.1):**   * **Lab:** * **Video:** [SSH Configuration on Cisco Switches](https://youtu.be/F1NU_PPGmHQ?si=lepvVlLkNTl-iShS) |
| Optional - Distinction (PC 1.3 and PC 4.1): Configure and verify VLAN access control lists (VACLs) on the switch to filter traffic between specific VLANs. | * **Steps:**   + Create and configure VACLs to define specific traffic filtering rules between VLANs.   + Apply the VACLs to the appropriate VLAN interfaces or subinterfaces.   + Verify the VACL functionality by attempting to send traffic that should be blocked and confirming that it is indeed dropped, and by sending traffic that should be allowed and confirming that it reaches its destination. * **Evidence:** Provide screenshots showing the VACL configuration, application to interfaces, and verification of traffic filtering.   **Distinction (PC 1.3 and PC 4.1):**   * **[Lab: VLAN Access-List (VACL)](https://networklessons.com/cisco/ccie-routing-switching/vlan-access-list-vacl)** * **Video:** [**VLAN Access Control List.**](https://youtu.be/IoM4GeLnm5w?si=4aXkk31XFJHQsYMk)[**A**rabic: VLAN Access Control List.](https://youtu.be/OzoGu-3OQtw?si=2fmLR3zd_XXP8Dnc) |

## Grading Rubric – Summative Assessment 1

| **Performance Criteria** | **Not Yet Competent** | **Competent** | **Competent with Merit** | **Competent with Distinction** |
| --- | --- | --- | --- | --- |
| **0 – 59%** | **60 – 69%** | **70 – 84%** | **85 – 100%** |
| **LO1: Configure VLANs across various switches and routers to create segmented network environments** | | | | |
| PC 1.1: Configure VLANs, including port assignments and VLAN IDs | Inaccurate or incomplete VLAN configuration, with errors in VLAN IDs, names, or port assignments. | Successfully configures VLANs, including port assignments and VLAN IDs, and provides clear evidence of the configuration through screenshots or other means | VLAN configuration is accurate and well-verified, demonstrating a clear understanding of the process. The student also successfully create an additional VLAN and assign it to unused ports on the switch. | VLAN configuration is exemplary, showcasing efficient use of commands and clear evidence of understanding VLAN concepts. The student also successfully configure and verify VTP (VLAN Trunking Protocol) on the switches to automate VLAN creation and propagation across the network. |
| PC 1.2: Manage VLAN configurations and security settings | Fails to manage VLAN configurations or implement basic security settings, leaving the network vulnerable. | Successfully manages VLAN configurations and implements basic security settings, providing evidence of the configuration and its effectiveness. | Accurately manages VLAN configurations and implements essential security settings, demonstrating a good understanding of security best practices. The student also successfully modify port security on ports to allow a maximum of two MAC addresses per port and implement the 'restrict' violation mode. | Demonstrates mastery in managing VLAN configurations and implementing robust security measures, showcasing a deep understanding of network security principles. The student also successfully configure and verify SSH access to the switch, disabling Telnet for enhanced security. |
| PC 1.3: Implement and validate inter-VLAN routing to ensure communication across different VLANs | Fails to implement inter-VLAN routing, resulting in no communication between VLANs. | Successfully implements and validates inter-VLAN routing, ensuring communication across different VLANs, and provides clear evidence of the configuration and verification. | Implements and verifies inter-VLAN routing correctly, demonstrating a clear understanding of the process and its importance for network communication. The student also successfully configure and verify a default gateway on each VLAN interface on R1. | Implements inter-VLAN routing efficiently, showcasing advanced configuration and troubleshooting skills, and ensuring seamless communication between VLANs. The student can also successfully configure and verify VLAN-based access control lists (VACLs) on the switch to further restrict traffic between specific VLANs. |
| **LO4: Apply security protocols to VLANs and WANs to maintain data integrity and confidentiality** | | | | |
| PC 4.1: Configure security settings on network devices within VLANs and WANs to enforce data integrity and confidentiality. | Fails to configure any security settings on network devices, leaving VLANs and WANs highly vulnerable. | Configures some basic security settings on network devices within VLANs and WANs, demonstrating a basic understanding of security requirements. | Configures and verifies essential security settings on network devices within VLANs and WANs, demonstrating a good understanding of security best practices. Also successfully Modifies port security on ports to allow a maximum of two MAC addresses per port and implement the 'restrict' violation mode. | Configures and verifies essential security settings on network devices within VLANs and WANs, demonstrating a good understanding of security best practices. The student can also successfully complete at least one of the following optional tasks:  \* Configure and verify VLAN access control lists (VACLs) on the switch to filter traffic between specific VLANs.  \* Configure and verify SSH access to the switch, disabling Telnet for enhanced security. |

*Add rows as required.*

## Student Acknowledgment – Summative Assessment 1

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Student Name** | |  | | **ID No.** |  |
| **Unit Title/s** | | Manage VLANs and WANs | | | |
| **LO & PC** | **Portfolio Evidence Requirements** | | | | |
| LO1: PC1.1, PC 1.2, PC 1.3 | Tables within the assessment sheet include screenshots with annotations.  or  Screen recording with oral description of the steps  or  Assessor’s observation record supported by the cisco packet tracer file | | | | |
| LO4: PC 4.1, |
| **Student Acknowledgment** | | | | | |
| I confirm that:   1. The portfolio evidence for this assessment has been submitted in Blackboard Learn; 2. All submitted evidence is my own work and does not contain any material that is subject to copyright or that has been submitted previously for assessment (unless requested by my teacher); 3. I have read and understood the Academic Integrity information in the HCT Student Handbook, including possible disciplinary action for academic dishonesty. | | | | | |
| **Signature:** |  | | **Date:** | |  |

## Assessment Results and Feedback – Summative Assessment 1

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Student Name** | |  | | | | **ID No.** | | |  | |
| **Unit Title** | | Manage VLANs and WANs | | | | | | | | |
| **Assessment Results:**  *Based on the Grading Rubric, choose the most appropriate Grade Classification for* ***each PC*** *and assign a percentage value within the range shown. You will then use these PC Grades to calculate the Summative Assessment Grade. See calculation notes below.* | | | | | | | | | | |
| **LO & PC** | **Grade Classification** | | **Not Yet Competent** | | **Competent** | | | **Competent with Merit** | | **Competent with Distinction** |
| **PC Grade %** | | **0 – 59%** | | **60 – 69%** | | | **70 – 84%** | | **85 – 100%** |
| LO1-PC1.1 |  | | 0 | |  | | |  | |  |
| LO1-PC1.2 | 0 | |  | | |  | |  |
| LO1-PC1.3 | 0 | |  | | |  | |  |
| LO4-PC4.1 | 0 | |  | | |  | |  |
|  |  | |  | | |  | |  |
|  |  | |  | | |  | |  |
|  |  | |  | | |  | |  |
| **Summative Assessment Grade %:** | | | 0 | |  | | |  | |  |
| *Calculation Notes:*   * *If* ***any PC*** *has a grade % in the Not Yet Competent range, the Summative Assessment grade must be in the Not Yet Competent range, regardless of other PC grades.* * *If all PCs have a grade % of 60% or more, the percentage values for all PCs should be averaged to determine the Summative Assessment Grade %. Use whole numbers.* | | | | | | | | | | |
| **Assessor Feedback:**  *Please ensure feedback is provided for all PCs covered by this assessment.* | | | | | | | | | | |
| Student Kholoud, you get not yet competent for all the PCs questions as you didn’t provide your answers.  Make sure to answer the questions based on the requested tasks. | | | | | | | | | | |
| **Student Comments:** | | | | | | | | | | |
|  | | | | | | | | | | |
| **Assessment Feedback Acknowledgement:** | | | | | | | | | | |
| I acknowledge that I have received and understood feedback from my teacher about this assessment.  I also acknowledge that all grades are **interim** until approved by the Internal Verifier. | | | | **Student** Signature: | |  | | | | |
| Date: | |  | | | | |
| I confirm that I have provided feedback about this assessment to this student. | | | | **Assessor** Signature: | | A black text on a white background  Description automatically generated | | | | |
| Date: | | 17th sep 2024 | | | | |
| **Assessor Name:** | | | | | | | | | | |
| Signature:  A black text on a white background  Description automatically generated | | | | | | | Date:  17th sep 2024 | | | |
| **Countersigning Assessor Name (if required):** | | | | | | | | | | |
| Signature: | | | | | | | Date: | | | |