**Switching and VLAN Concepts Projects Report**

Brief: You have been tasked with designing a Local Area Network (LAN), for the Kilkenny campus of the South East Technological University (SETU). As Kilkenny will be the headquarters of the new university the design of this LAN is paramount. After liaising with the Estates department of the new university to define the scope of the network project you will now create a prototype to present to Estates. This prototype will be accompanied by an explanation of each network feature and will be used to confirm the requirements of the new network.

# Introduction

This is my report on making a LAN for the Kilkenny SETU Campus prototype. In this report I will show all the requirements and my explanation on how I implemented them into the prototype and how they work in the LAN and why they are needed.

Table of Contents

[Introduction 1](#_Toc728354183)

[Requirement 1: 2](#_Toc1207136051)

[Requirement 2: 2](#_Toc654319358)

[Requirement 3 2](#_Toc568042211)

[Requirement 4: 2](#_Toc2057012302)

[Requirement 5: 2](#_Toc2077073532)

Requirement 1: The LAN should separate users of different types. VLANs will be used to separate user types and will improve network performance and security, whilst simplifying network management. User types include:

* Senior Management
* Administrative staff
* Accounting Staff
* Computing services staff
* Academic staff
* Students

I started off by making 6 switches with a range of 1 to 3 pcs on each switch and all 6 switches have been named which are Administration, Student Services, Departments, Classroom, Library and Labs

The pcs connected to the switches have been given one of the vlans made which are Vlan 10 Senior Management, Vlan 20 Administrative Staff, Vlan 30 Accounting Staff, Vlan 40 Computing Services Staff, Vlan 50 Academic Staff and Vlan 60 Students.

I did this by doing Vlan 10 then name SeniorManagement and then repeating this for the rest of the Vlans and then went on the interface connected to the pc and used switchport mode access and then giving it access to vlan 10 and repeating this for all the pcs and for the switches connecting to each other I did switchport mode trunk switchport trunk allowed vlan 10,20,30,40,50,60 to allow access to the switches to all the Vlans.

We implement Vlans on the PCs to tailor specific network assignments based on the user's role and requirements. An example would student pc being configured with minimal permissions while academic staff pcs are granted higher levels of access. This makes it an easier way to set up the configuration on Mutiple Pcs.

The reason we also used the command Switchport trunk allowed vlan 10,20,30,40,50,60 is to allow all the switches connected to each other have access to all the vlans as they would need access to all the Vlans and we also make all the connections between the switches a trunk line to make them communicate faster.

Requirement 2: End users from each VLAN should be able to communicate with each other and should be able to communicate with devices outside of the university’s network.

To do this part I first started by assigning a VLAN to each pc depending on what role they are and what they would need to do, this is done by using the commands, Int f0/x (x represents pc connection to switch) and then switchport mode access and then switchport access vlan x (x representing vlan id). Switchport mode access allows you to assign a vlan to the port.

Then I configured the trunk links between all the switches and turned them on to make the connection between the switches faster which was done by using the commands, Int f0/x (x represents switch connection to other switch) and then type switchport mode trunk to make it a trunk connection.

On the MLS I went on vlan interface 10 to 60 and assigned a Ip address and subnet mask to them and put no shutdown, so it doesn’t shutdown as its needed always online

At the end on the MLS, I put ip routing which enables the routing functionality on the MLS and allows it to route packets between VLANs.

Then for communication with a device outside the university network I set up a server and connected it with a wire to the MLS and then I went on the MLS and put the command int f0/7 which connects from MLS to the Server then I put no switchport access as it’s a static ip address and not connected to a vlan then I went on the server and set a static ip address, subnet mask and a default gateway to it.

This is all I used to be able to communicate with all the Pcs in my network and with a server outside my network

Requirement 3: As VLANs create logical networks using layer 2 devices, an IPv4 address allocation must be configured for each VLAN. Each VLAN should have a /24 IPv4 address range and addresses should be assigned dynamically using a DHCP server.

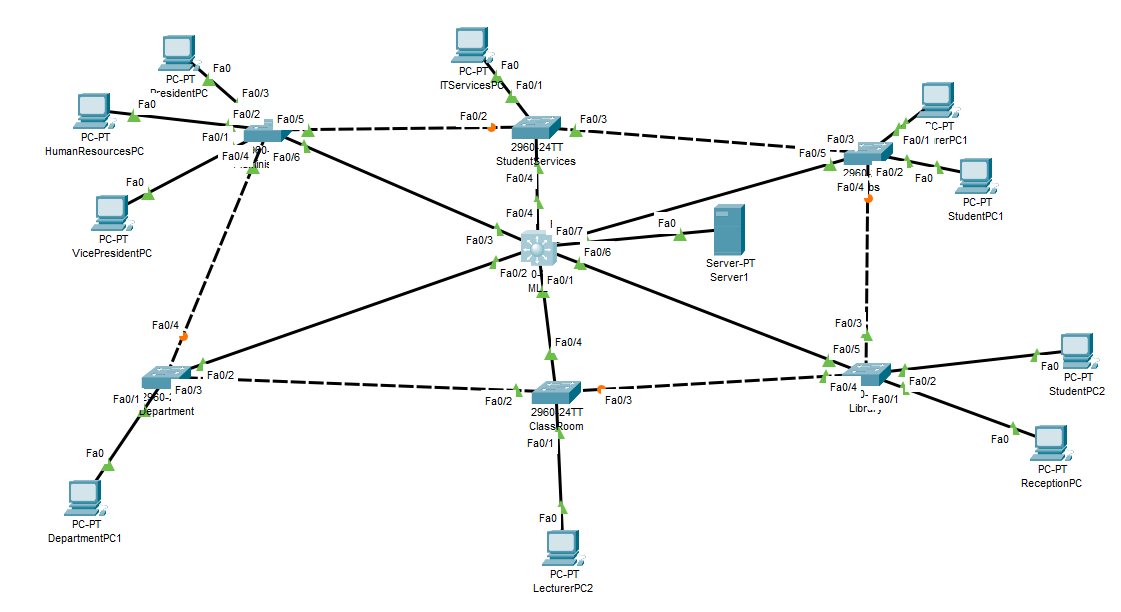
I go on the MLS and firstly exclude ip addresses that could already be in use and then exclude them, then configure the vlans by entering the command Int vlan x (x representing vlan id) and set it an ip address and no shutdown and this is repeated for each vlan

Then I make ip dhcp pools for each vlan by putting the commands Ip dhcp pool Vlan10 and giving it a network ip and default router ip and repeat this for each vlan.

I then go on each pc and set it from static ipv4 address to dhcp ipv4 address so it can request and be given an ipv4 address with network and default router ip which then allows for all the pcs on all the switches to communicate with each other.

Then I tested if all the pcs could communicate by making them ping each other and seeing If the ping worked and if it did.

Requirement 4: Redundancy must be implemented for network pathways of the university’s network. The network redundancy should minimize the occurrence of shutdowns and DoS.



For the redundancy I added connections from my MLS to all the switches so instead when one of them go down the other one will be able to still communicate with all the switches and this is also the same if a connection between switches goes down, they all will be still able to communicate with each other.

The STP is automatically on as you can see by the orange dots between some of the connections this happens, so it doesn’t start a loop, so it just blocks unneeded connections between switches and MLS.

they will only become unblocked if STP notices something wrong with a connection, so it opens the next closest connection to the switch with a missing connection to allow continuous communication within the network so it doesn’t shut down which would be bad for a network in a college campus that needs to be always working.

Requirement 5: Network devices should be hardened to ensure availability of services and resources, to limit the attack surface and improve the security posture of the network.

To prevent unwanted entry, I first started by adding password to the enable command and password to enter the switch CLI then I did service password-encryption command to encrypt all the passwords, so they won't be shown when doing a show run command. For this prototype I put all the passwords as labuser but in the real network the passwords would be more complex to deter unwanted access, then used the commands line vty 0 15 and then put a password which was labuser and put login, so it's required when logging into the network remotely.

Then I added a banner on all the switches and MLS which was done by using the command banner motd and then entered what I wanted to be seen when people tried to access the devices without proper authorization which I put “No unauthorized access allowed”.