Networking Project

Switching and VLAN Concepts

Semester 1 Year 2

Daniel Egharevba | Networking: Switching and VLAN Concepts | 21/11/2023

Contents

[**VLAN (Virtual Local Area Network)** 2](#_Toc152619556)

[**STEPS (VLANS)** 2](#_Toc152619557)

[**STEPS (TRUNK LINES)** 3](#_Toc152619558)

[**Inter-VLAN Routing with MLS** 3](#_Toc152619559)

[**STEPS (INTER-VLAN ROUTING)** 4](#_Toc152619560)

[**CLOUD** 4](#_Toc152619561)

[**DHCPv4 (Dynamic Host Configuration Protocol)** 4](#_Toc152619562)

[**DHCPv4 Operation** 5](#_Toc152619563)

[**DHCPV4 Server CONFIGURATION** 5](#_Toc152619564)

[**DNS Server** 6](#_Toc152619565)

[**STP (Spanning Tree Protocol)** 6](#_Toc152619566)

[**Switch A** 7](#_Toc152619567)

[**Switch B** 8](#_Toc152619568)

[**Switch C** 8](#_Toc152619569)

[**Switch D** 9](#_Toc152619570)

[**Switch E** 9](#_Toc152619571)

[**Switch F** 10](#_Toc152619572)

[**Central switch (Root Bridge)** 10](#_Toc152619573)

[**Multi-Layer Switch** 11](#_Toc152619574)

[**Network Security** 11](#_Toc152619575)

# **VLAN (Virtual Local Area Network)**

In my network topology, the physical network is being subdivided into smaller subnets to provide more security and network management. The VLANs created were made in accordance with the requirements of the services needed for the Kilkenny University campus. The number of VLANs present in the network is 8 and they have all been configured appropriately to be able to communicate between VLAN-like devices.

For example, in the network topology, if PC A1 wants to ping PC B1 it can as they are part of the same VLAN. The creation of VLANs provides the network with security, efficiency, better performance, simpler management, and smaller broadcast domains.

List of VLANs created in network.

1. Senior management (VLAN 10)
2. Administration staff (VLAN 20)
3. Accounting staff (VLAN 30)
4. Computing services staff (VLAN 40)
5. Academic staff (VLAN 50)
6. Students (VLAN 60)
7. Native (VLAN 100)
8. Unused ports (VLAN 1000)

## **STEPS (VLANS)**

* Enter switch CLI (Command-Line Interface).
* Enter global configuration mode after providing both console and privileged executive mode passwords.
* Create and name VLANs on the switch.
* Assign created VLANs to the correct switch interfaces and set switchports mode correctly.
* Move the switch IP address to the VLAN needed for remote handling and switch management.
* To verify VLANs creation and correct interface assignments, use the commands “*show vlan brief*” and “*show ip interface brief*”.

There are 2 methods to configure trunk lines in a network. DTP (Dynamic Trunking Protocol) and manually configuring the trunk interfaces. In my network topology, I decided to manually configure trunk lines because DTP poses a security threat to the network. DTP is a Cisco proprietary protocol, switches from other manufacturers cannot use it. Also, it permits illegal devices to create trunk links with switches and access several VLANs which pose security problems.

## **STEPS (TRUNK LINES)**

* Enter global configuration mode.
* Enter the interface meant to be configured as trunk.
* Issue the command “*switchport mode trunk*” which forces the port to trunking mode. Remember to issue the command on both ports of the trunk line on both switches involved.
* Modify the trunk configuration on both switches by changing the native vlan from the default vlan 1 to vlan 100 (Native vlan created previously).
* Leave global configuration mode and issue the command “*show interfaces trunk*” to view the trunk lines created.

After successfully following these steps, VLAN-like devices can communicate with each other and send traffic signals over the network. Note that end devices from different VLANs cannot ping each other at the stage yet.

# **Inter-VLAN Routing with MLS**

In the network topology created for the Kilkenny university campus, end devices from different VLANs are meant to be able to communicate and ping each other. Because the network set up needs end users to be able to transfer traffic from one user on a specific VLAN to another user on a different VLAN. For example, if an academic staff, a teacher on VLAN 50, wants to reach out and send traffic to students on VLAN 60 over the network, inter-VLAN routing needs to be implemented for the students to be able to receive the traffic.

There are 3 ways to configure Inter-VLAN routing on a network. There is the Legacy method, the Router-on-a-Stick method, and the multi-layer switch method. In this network, the multi-layer switch method was implemented as it covers a wide range of uses and is easy to implement. It is the fastest and most scalable method of inter-vlan routing.

A multi-layer switch (MLS) might be more expensive than a router, but it has more capabilities over it. MLS can route from one VLAN to another using SVIs, Switched Virtual Interfaces, which are virtual routed interfaces that connect a VLAN on the device to the Layer 3 router engine on the same device. MLS can also convert a layer 2 switchport to a layer 3 interface (i.e., a routed port). With these capabilities, MLSs can provide inter-vlan routing to a network.

## **STEPS (INTER-VLAN ROUTING)**

* Enter the MLS global configuration mode.
* Configure and activate the SVI interfaces for VLANs 10, 20, 30, 40, 50, 60, and 100 on the MLS.
* Configure trunking on MLS and specify the native VLAN.
* Encapsulate the link with the dot1q protocol to enable trunking. Remember to configure trunking on the other side port of the trunk line.
* Enable routing with the command “*ip routing*” in the global configuration mode. This command must be configured to enable inter-VLAN routing on a Layer 3 switch for IPv4.
* Use the command “*show ip route*” to verify routing is enabled.

After following the step above, you should be able to ping from one end device on a VLAN to another device on a different VLAN. For VLANs to be reachable by other layer 3 devices, the layer 3 switchport must become a routed port. The command to convert a layer 2 port to a layer 3 interface is “*no switchport*”. It acts as a toggle on/off command between both port types. To verify routing, use the command “*show ip route*” and to verify connectivity use “*ping*” command.

## **CLOUD**

In the requirement to allow devices on different VLANs to be able to communicate, it was also stated that users should be able to communicate with devices outside the university’s network as well. And to fulfill this requirement, the university campus network topology has a cloud and DNS server that are on different networks. And act as external networks to the university’s separate network. The configured the same you would configure a routed port on a router, change the switchport to a layer 3 interface, give it an ip address with a different subnet mask and enable the interface. There you have it. An external network to the university’s network. Refer to the bottom of the document for the cloud IP address.

# **DHCPv4 (Dynamic Host Configuration Protocol)**

In this network topology, so far to verify VLAN connectivity and inter-vlan routing between end devices, IPv4 addresses where assigned statically (manually entered). As you might guess this does not scale well because it would require that for all devices owned and used by students and university personnel (including phones, laptops, printers, server, etc.), an IP address would need to be assigned manually to it. Which is near-impossible and not manageable in any means. But with the use of a DHCP server, we can automatically lease and assign IPv4 addresses to devices on our network.

A DHCPv4 (Dynamic Host Configuration Protocol) server assigns IPv4 addresses and other network information dynamically (automatically). Given that most network nodes will be desktop clients, DHCPv4 makes it easy to manage IPv4 addresses among them and saves us time. A dedicated DHCPv4 server is scalable and relatively easy to manage. What the DHCPv4 server does is dynamically assign, or lease, an IPv4 address from a pool of addresses for a short, limited period chosen by the server or until the client no longer needs it.

## **DHCPv4 Operation**

DHCPv4 works in a client/server mode. When a client communicates with a DHCPv4 server to request an IPv4 address, the server assigns and leases an IPv4 address to the client.

* With the IPv4 address, the client connects to the network until the IPv4 address lease expires. To extend the lease, the client must contact the server periodically.
* This process makes sure that when the clients power off or leave the network the addresses are not kept by them but instead are returned to the address pool, so that other network devices can use them.

In my network topology, the MLS is configured as the DHCPv4 server that leases IP addresses around the network. Below are steps of how the MLS was configured as a DHCPv4 server.

## **DHCPV4 Server CONFIGURATION**

* Exclude a segment of IPv4 addresses for each VLAN including the address used for the default router. These IPv4 addresses will be put aside to be statically assigned to other network devices present on the network. For example, routers, servers, printers, and other devices that will be on the network. The command used is “*ip dhcp excluded-address low-ip-address [high-ip-address]*” for IPv4 addresses exclusion.
* Create DHCPv4 pool names for each VLANs present in the network. Using the command “*ip dhcp pool pool-name*”, a VLAN pool is created, and the router is set in DHCPv4 configuration mode.
* Then configure the DHCPv4 pool. The address pool and default gateway router will be configured here, as well as the DNS server if present in the network. The domain name and other DHCP lease configurations can be made here.
* Use these commands to verify that the DHCPv4 server is functioning and operational, “*show running-config | section dhcp*” for DHCP commands configured on MLS, “*show ip dhcp binding*” for displaying list of bindings between MAC address and IPv4 addresses on the network and “*show ip dhcp server statistics*” for displaying count information regarding the messages to and from the DHCPv4 server.

## **DNS Server**

In the requirements for the Kilkenny university campus network topology, a DNS (Domain Name System) server was never specified to be configured. The network topology implemented by me includes one, but it is not fully configured as it is not required. But what use does a DNS server provide to a network. It offers another means of pinging between hosts on a network. For example, host 1 can ping host 2 by simply knowing the name of the device used by host 2 on the network. A DNS server essentially translates what a user types into a browser into something the machine can use to find a webpage. The DNS server translates domain names to IP addresses so browsers can load Internet resources. There is nothing special about it that requires the client and the server to be within the same IP subnet. If they are not, the UDP (User Datagram Protocol) segments simply follow normal IP routing rules to get to the server’s IP address, and the replay UDP segment is routed back to the client. UDP refers to a protocol used for communication throughout the internet.

# **STP (Spanning Tree Protocol)**

Now the Kilkenny campus university network has communication all round and every end device can send traffic to another with the use of DHCPv4 IP addresses whether the receiver is on a different VLAN or not. But what happens if there is a physical loop between switches and the traffic sent from a device ends up travelling in that loop without a destination port (egress port)? First, it will lead to switches CAM table inconsistency and high CPU utilization which will make switches unable to forward frames.

Also, what happens if a physical link suddenly fails, and a switch has no access to the central switch to communicate with the whole network? The switch will end up being isolated and all network client devices connected to that switch will not have an IPv4 address and will not be able to communicate with any other device.

To solve these issues, STP (Spanning Tree Protocol) comes in which is basically a loop-prevention network protocol that allows for redundancy while creating a loop-free network topology. In simple terms, it allows the physical loop between switches to exist, but logically traffic does not travel through that loop, because some ports are set to a blocked state where they cannot forward traffic.

STP also compensates for link failure by recalculating and opening the blocked ports in a loop. STP is automatically enabled in layer 2 devices on a network. So not much configuration has to be done. But if a specific switch is to be set as a Root Bridge. Then the following command can do such *“spanning-tree vlan 10,20,30,40,50,60,100 root primary”*, with this command a switch can be configured to be the root bridge for specific VLANs on a network.

In the Kilkenny university campus network topology, a few physical loops between switches were implemented in case of switchport failure or link saturation. And below are tables of the various states and modes each switchport for every switch is set to. The states and modes may differ based on the different ports VLANs pass through.

## **Switch A**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **VLAN ID / Switchports** | **Gi 0/1 (Root)** | **Gi 0/2 (Altn)** | **Fa 0/1 (Desg)** | **Fa 0/2 (Desg)** | **Fa0/3 (Desg)** | **Fa 0/4 (Desg)** |
| **VLAN 10** | **FWD** | **BLK** | **FWD** | **-** | **-** | **-** |
| **VLAN 20** | **FWD** | **BLK** | **-** | **FWD** | **-** | **-** |
| **VLAN 30** | **FWD** | **BLK** | **-** | **-** | **FWD** | **-** |
| **VLAN 40** | **FWD** | **BLK** | **-** | **-** | **-** | **FWD** |
| **VLAN 50** | **FWD** | **BLK** | **-** | **-** | **-** | **-** |
| **VLAN 60** | **FWD** | **BLK** | **-** | **-** | **-** | **-** |
| **VLAN 100** | **FWD** | **BLK** | **-** | **-** | **-** | **-** |

## **Switch B**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **VLAN ID / Switchports** | **Gi 0/1 (Root)** | **Gi 0/2 (Desg)** | **Fa 0/1 (Desg)** | **Fa 0/2 (Desg)** | **Fa 0/3 (Desg)** | **Fa 0/4 (Desg)** | **Fa 0/5 (Desg)** | **Fa 0/24 (Desg)** |
| **VLAN 10** | **FWD** | **FWD** | **FWD** | **-** | **-** | **-** | **-** | **FWD** |
| **VLAN 20** | **FWD** | **FWD** | **-** | **FWD** | **-** | **-** | **-** | **FWD** |
| **VLAN 30** | **FWD** | **FWD** | **-** | **-** | **FWD** | **-** | **-** | **FWD** |
| **VLAN 40** | **FWD** | **FWD** | **-** | **-** | **-** | **FWD** | **-** | **FWD** |
| **VLAN 50** | **FWD** | **FWD** | **-** | **-** | **-** | **-** | **FWD** | **FWD** |
| **VLAN 60** | **FWD** | **FWD** | **-** | **-** | **-** | **-** | **-** | **FWD** |
| **VLAN 100** | **FWD** | **FWD** | **-** | **-** | **-** | **-** | **-** | **FWD** |

## **Switch C**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **VLAN ID / Switchports** | **Gi 0/1 (Root)** | **Gi 0/2 (Altn)** | **Fa 0/1 (Desg)** | **Fa 0/2 (Desg)** | **Fa 0/24 (Altn)** |
| **VLAN 10** | **FWD** | **BLK** | **-** | **-** | **BLK** |
| **VLAN 20** | **FWD** | **BLK** | **-** | **-** | **BLK** |
| **VLAN 30** | **FWD** | **BLK** | **-** | **-** | **BLK** |
| **VLAN 40** | **FWD** | **BLK** | **-** | **-** | **BLK** |
| **VLAN 50** | **FWD** | **BLK** | **FWD** | **-** | **BLK** |
| **VLAN 60** | **FWD** | **BLK** | **-** | **FWD** | **BLK** |
| **VLAN 100** | **FWD** | **BLK** | **-** | **-** | **BLK** |

## **Switch D**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **VLAN ID / Switchports** | **Gi 0/1 (Root)** | **Gi 0/2 (Desg)** | **Fa 0/1 (Desg)** | **Fa 0/2 (Desg)** | **Fa 0/24 (Altn)** |
| **VLAN 10** | **FWD** | **FWD** | **-** | **-** | **BLK** |
| **VLAN 20** | **FWD** | **FWD** | **-** | **-** | **BLK** |
| **VLAN 30** | **FWD** | **FWD** | **-** | **-** | **BLK** |
| **VLAN 40** | **FWD** | **FWD** | **-** | **-** | **BLK** |
| **VLAN 50** | **FWD** | **FWD** | **FWD** | **-** | **BLK** |
| **VLAN 60** | **FWD** | **FWD** | **-** | **FWD** | **BLK** |
| **VLAN 100** | **FWD** | **FWD** | **-** | **-** | **BLK** |

## **Switch E**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **VLAN ID / Switchports** | **Gi 0/1 (Root)** | **Gi 0/2 (Desg)** | **Fa 0/1 (Desg)** | **Fa 0/2 (Desg)** | **Fa 0/3 (Desg)** | **Fa 0/24 (Desg)** |
| **VLAN 10** | **FWD** | **FWD** | **FWD** | **-** | **-** | **FWD** |
| **VLAN 20** | **FWD** | **FWD** | **-** | **-** | **-** | **FWD** |
| **VLAN 30** | **FWD** | **FWD** | **-** | **-** | **-** | **FWD** |
| **VLAN 40** | **FWD** | **FWD** | **-** | **FWD** | **-** | **FWD** |
| **VLAN 50** | **FWD** | **FWD** | **-** | **-** | **FWD** | **FWD** |
| **VLAN 60** | **FWD** | **FWD** | **-** | **-** | **-** | **FWD** |
| **VLAN 100** | **FWD** | **FWD** | **-** | **-** | **-** | **FWD** |

## **Switch F**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **VLAN ID / Switchports** | **Gi 0/1 (Root)** | **Gi 0/2 (Altn)** | **Fa 0/1 (Desg)** | **Fa 0/2 (Desg)** |
| **VLAN 10** | **FWD** | **BLK** | **-** | **-** |
| **VLAN 20** | **FWD** | **BLK** | **-** | **-** |
| **VLAN 30** | **FWD** | **BLK** | **-** | **-** |
| **VLAN 40** | **FWD** | **BLK** | **FWD** | **-** |
| **VLAN 50** | **FWD** | **BLK** | **-** | **-** |
| **VLAN 60** | **FWD** | **BLK** | **-** | **FWD** |
| **VLAN 100** | **FWD** | **BLK** | **-** | **-** |

## **Central switch (Root Bridge)**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **VLAN ID / Switchports** | **Gi 0/1 (Desg)** | **Fa0/1 (Desg)** | **Fa0/2 (Desg)** | **Fa0/3 (Desg)** | **Fa0/4 (Desg)** | **Fa0/5 (Desg)** | **Fa0/6 (Desg)** |
| **VLAN 10** | **FWD** | **FWD** | **FWD** | **FWD** | **FWD** | **FWD** | **FWD** |
| **VLAN 20** | **FWD** | **FWD** | **FWD** | **FWD** | **FWD** | **FWD** | **FWD** |
| **VLAN 30** | **FWD** | **FWD** | **FWD** | **FWD** | **FWD** | **FWD** | **FWD** |
| **VLAN 40** | **FWD** | **FWD** | **FWD** | **FWD** | **FWD** | **FWD** | **FWD** |
| **VLAN 50** | **FWD** | **FWD** | **FWD** | **FWD** | **FWD** | **FWD** | **FWD** |
| **VLAN 60** | **FWD** | **FWD** | **FWD** | **FWD** | **FWD** | **FWD** | **FWD** |
| **VLAN 100** | **FWD** | **FWD** | **FWD** | **FWD** | **FWD** | **FWD** | **FWD** |

## **Multi-Layer Switch**

|  |  |
| --- | --- |
| **VLAN ID / Switchports** | **Gigabit Ethernet 0/1 (Root)** |
| **VLAN 10** | **LSN** |
| **VLAN 20** | **LSN** |
| **VLAN 30** | **LSN** |
| **VLAN 40** | **LSN** |
| **VLAN 50** | **LSN** |
| **VLAN 60** | **LSN** |
| **VLAN 100** | **LSN** |

# **Network Security**

* Password for console line configuration mode set.
* Password for VTY line configuration mode set.
* Password for privileged executive mode set.
* All passwords were encrypted.
* Deactivated any kind of ip domain lookup.
* All unused ports were turned down administratively.
* All unused ports are set to a VLAN to avoid illegal access to the network.
* Set list of allowed VLANs over a trunk line to stop illegal access.
* Manually configuring trunk lines so that illegal access to switches is prevented.

Network IP format = **191.31.vlan-id.x**

VLANs default router = **191.31.vlan-id.254**

Switches IP = **191.31.40.1/7**

DNS default gateway = **181.21.254.254 255.255.0.0**

DNS server IP = **181.21.1.1 255.255.0.0 (External)**

Cloud = **209.165.200.225 255.255.255.252 (External)**

University subnet mask = ***255.255.255.0***

DHCP Excluded pool for VLANs :

* *VLAN 10 = 191.31.10.1 - 10 & .254*
* *VLAN 20 = 191.31.20.1 - 10 & .254*
* *VLAN 30 = 191.31.30.1 - 10 & .254*
* *VLAN 40 = 191.31.40.1 - 10 & .254*
* *VLAN 50 = 191.31.50.1 - 10 & .254*
* *VLAN 60 = 191.31.60.1 - 10 & .254*