Networking and Internet Services
Virtual LANs (VLAN)

Presented by
Omid panahi

Champlain
COLLEGE SAINT-LAMBERT

Goals of this section

- Understand VLAN
- Difference Between subnetting and VLANs
- Configure VLAN and simulate

Virtual LANs

- Today’s LANs are complex places. It’s rare to see any serious network that doesn’t have remote incoming connections, public Web or e-mail servers, wireless networks, as well as the basic string of connected switches. Leaving all of these different features on a single broadcast domain creates a tremendous amount of broadcast traffic and creates a security nightmare

How to solve the complexity

- Separate networks with multiple switches and router(subnetting)
- Program switches to act as Virtual Local Area Network.
- To create a VLAN, you take a single physical broadcast domain made up of one or more switches and chop it up into multiple broadcast domains. This is most simply done by assigning each port to a specific VLAN

Configuring a switch

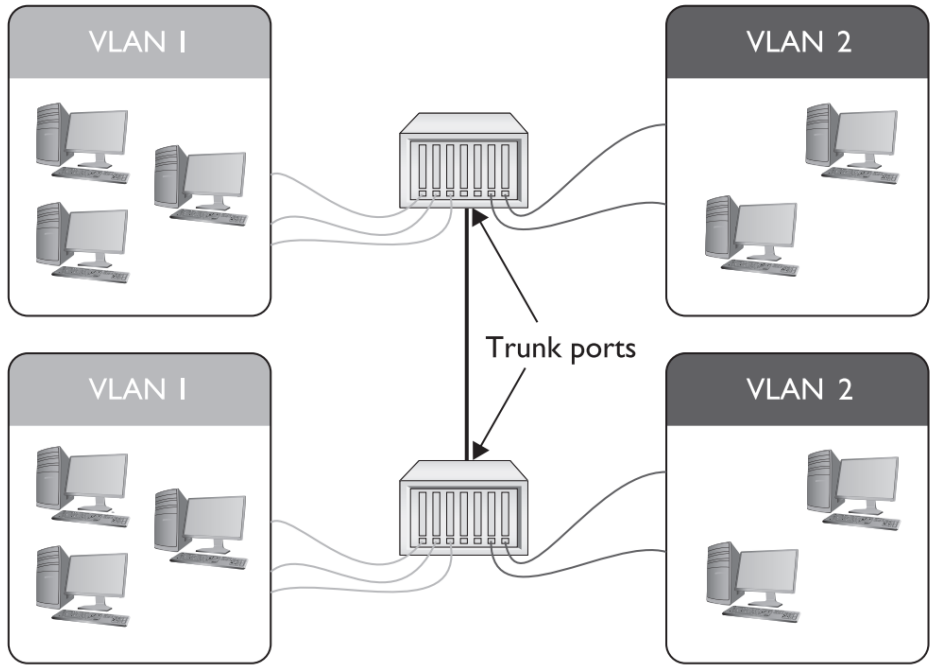
- When setting up a VLAN switch, one or more **VLANs** are created.
- Ports are assigned to those VLANs.
- Any host connected to a VLAN port becomes part of that VLAN's **broadcast domain**.
- A single switch with two VLANs represents the **simplest VLAN configuration**.
- Larger networks often have multiple switches while maintaining the same VLANs (e.g., VLAN1 and VLAN2).

Trunking

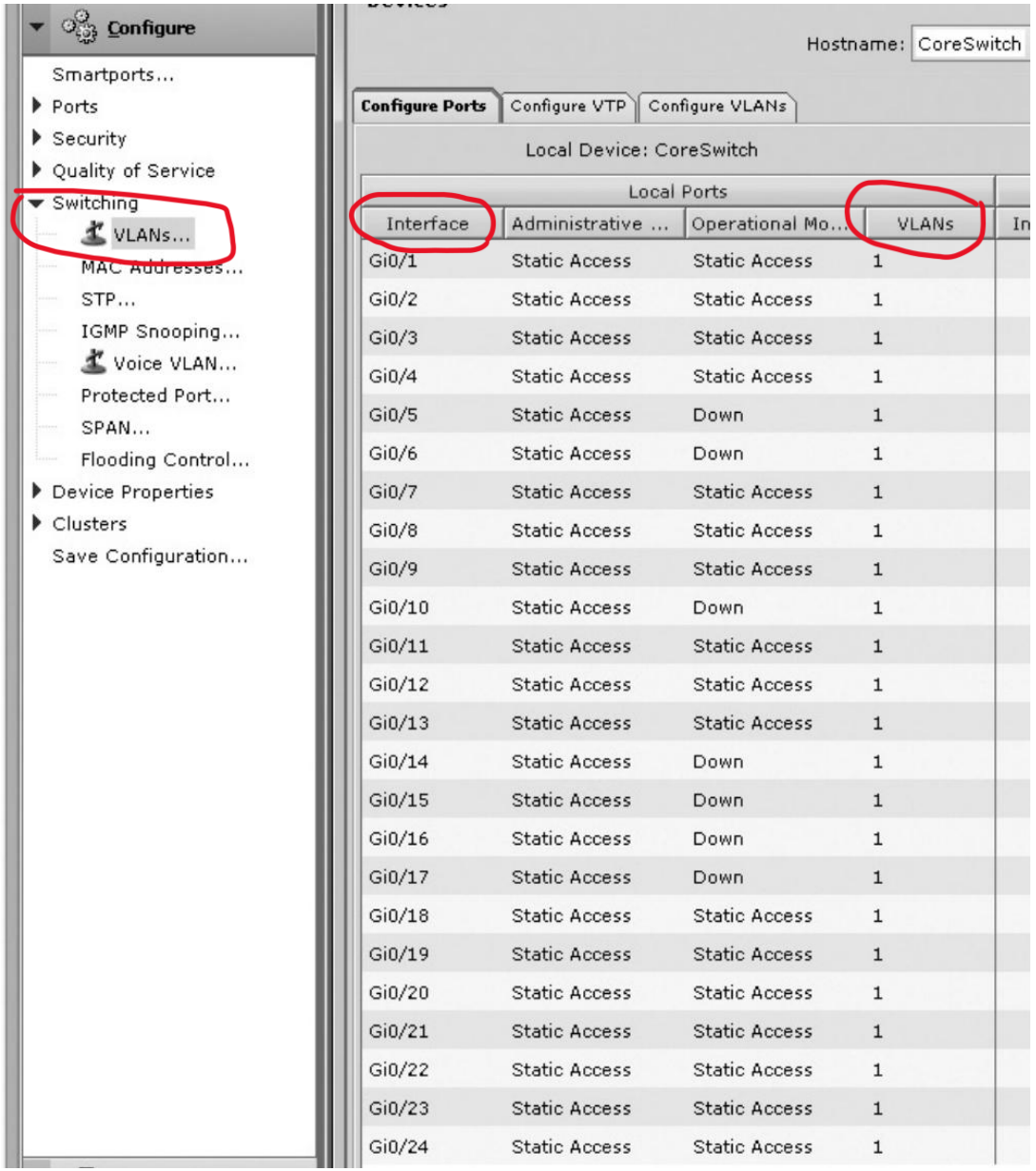
- **Trunking** is the process of transferring VLAN traffic between two or more switches.
- Imagine two switches, each configured with a VLAN1 and a VLAN2, as shown in Figure

✓ You want all of the computers connected to VLAN1 on one switch to talk to all of the computers connected to VLAN1 on the other switch.

✓ A trunk port is a port on a switch configured to carry all traffic, regardless of VLAN number, between all switches in a LAN



Defining VLANs in Cisco Network Assistant



Busy Network with many VLANs

- When you have a busy network with multiple switches and multiple VLANs, how does a frame from a workstation?
- What if the workstations are several switches apart?

Solution is **Tagging**

Tagging

Purpose of Tagging

Tagging allows frames from one VLAN (e.g., VLAN 100) to travel across multiple switches while maintaining VLAN separation and identity.

- **Access Ports**:
  Workstations connect to **access ports**, which belong to a specific VLAN.
  - When a frame enters through an access port, the **switch tags it** with that VLAN's ID.
  - If the destination is on the same switch, the **tag is removed** before delivery
- **Trunk Ports:**
  - Used to **connect switches** and carry traffic for multiple VLANs.
  - If the VLAN tag matches the **native VLAN**, the tag is **removed** before sending.
  - If it differs, the frame **keeps the tag** as it moves across trunk links.

Tagging…

- **Native VLAN and Security:**

Native VLANs exist to provide compatibility with older or simpler non-VLAN tagging switches, but there is a catch.

The native VLAN opens your network to a nasty vulnerability called a double-tagging attack that lets the attacker access VLANs they should not be able to access.

For this reason, in modern networks ,the native VLAN is set to an unused VLAN and the trunk port is configured to tag its native VLAN traffic as well.

VLAN Trunking Protocol

- A busy network with many VLAN switches can require periods of intensive work to update
- Cisco uses a proprietary protocol called VLAN Trunking Protocol (VTP) to automate the updating of multiple VLAN switches. With VTP, you put each switch into one of three states:

1. server
2. client
3. transparent

VLAN Trunking Protocol …

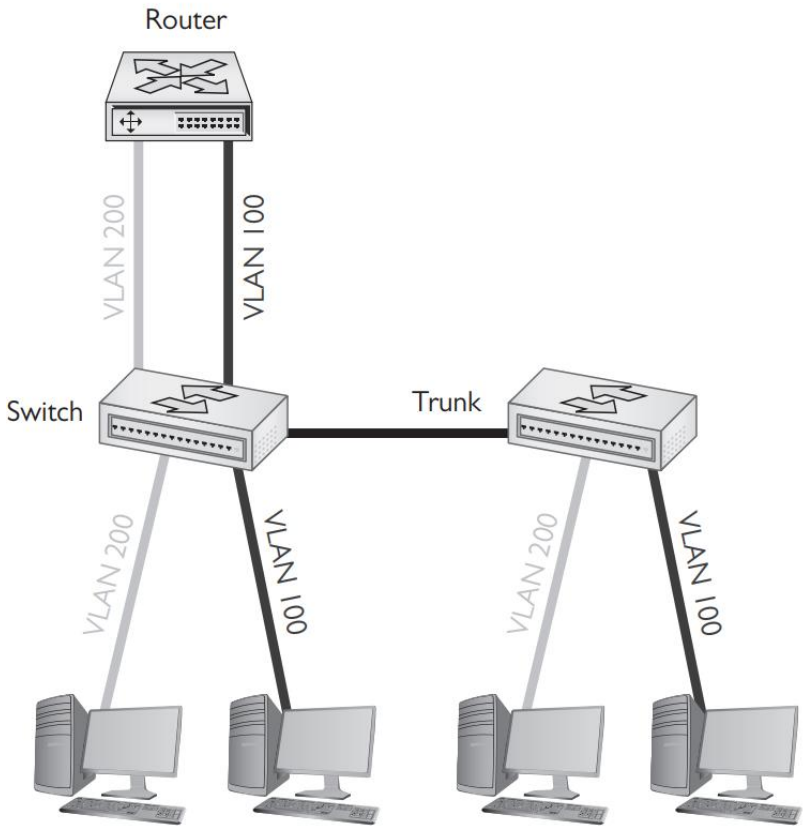
- Server: When you make changes to the VLAN configuration of the **server** switch, all the connected client switches update their configurations within minutes
- Transparent: When you set a VLAN switch to transparent, you tell it not to update but to hold onto its manual settings
- Client: Clients can update servers the same way servers update clients. The difference is that VLAN info can only be changed on servers.

InterVLAN Routing

- Once you've configured a switch to support multiple VLANs, each VLAN is its own broadcast domain, just as if the two VLANs were on two completely separate switches and networks.
- There is no way for data to get from one VLAN to another unless you use a router or a multilayer switch.
- The process of making a router work between two VLANs is called interVLAN routing

One Router connecting multiple VLANs

One router connecting multiple VLANs



DHCP and VLANs

- **DHCP functionality**
  - **DHCP** automates and manages IP address assignments efficiently.
  - Its default operation is limited to **a single subnet**.
  - **DHCP requests cannot cross routers** by default.

- In networks with **multiple VLANs connected by routers**, an additional method is needed to deliver IP addresses and TCP/IP information to hosts.
- How?

DHCP relay

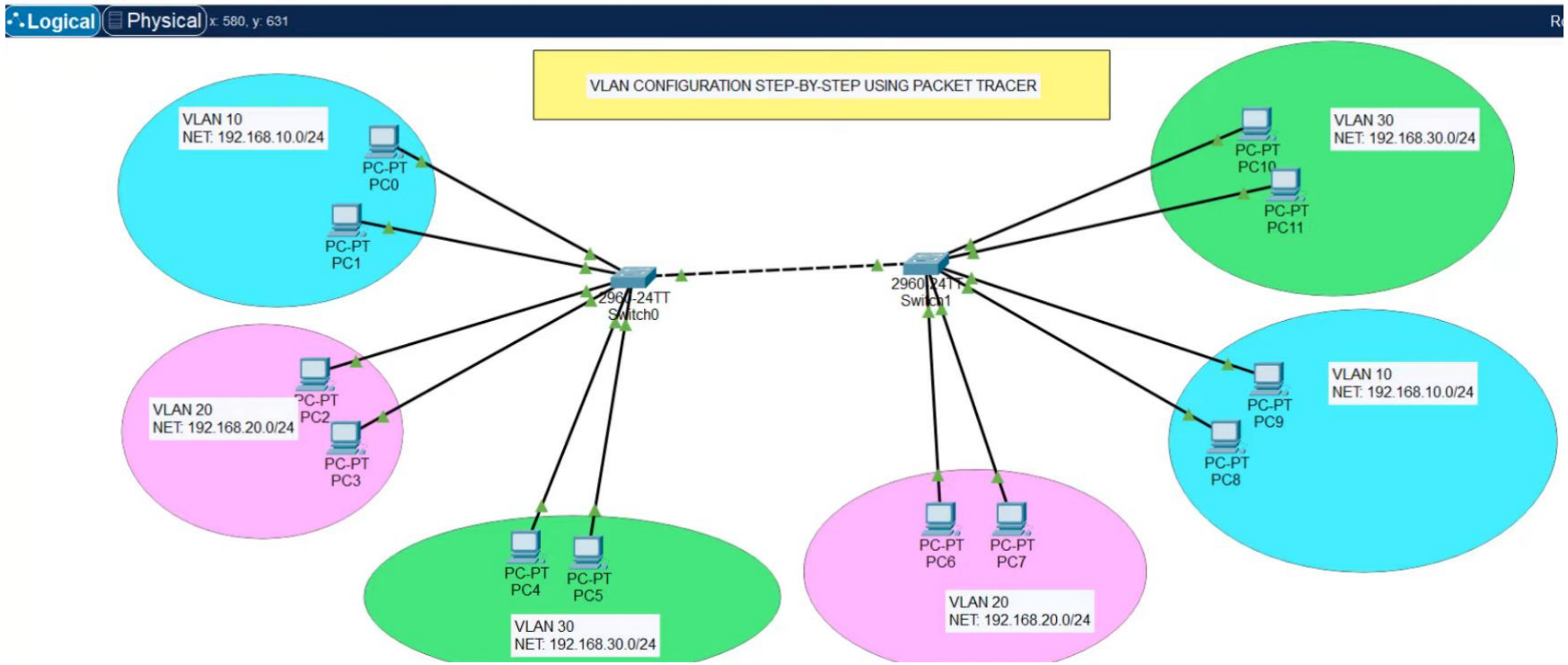
- When DHCP relay is *enabled* and configured within a router, the router will pass DHCP requests and responses across the router interfaces

- So now we can use a single DHCP server to serve addresses to multiple networks or subnetworks

Summary:

- **DHCP relay** allows routers to forward DHCP requests and responses between networks.
- Relay enables **one DHCP server** to provide addresses to **multiple subnets or VLANs**.
- **Cisco** uses the ***ip helper*** command to implement DHCP relay functionality

Complete the VLAN lab



Complete the VLAN lab

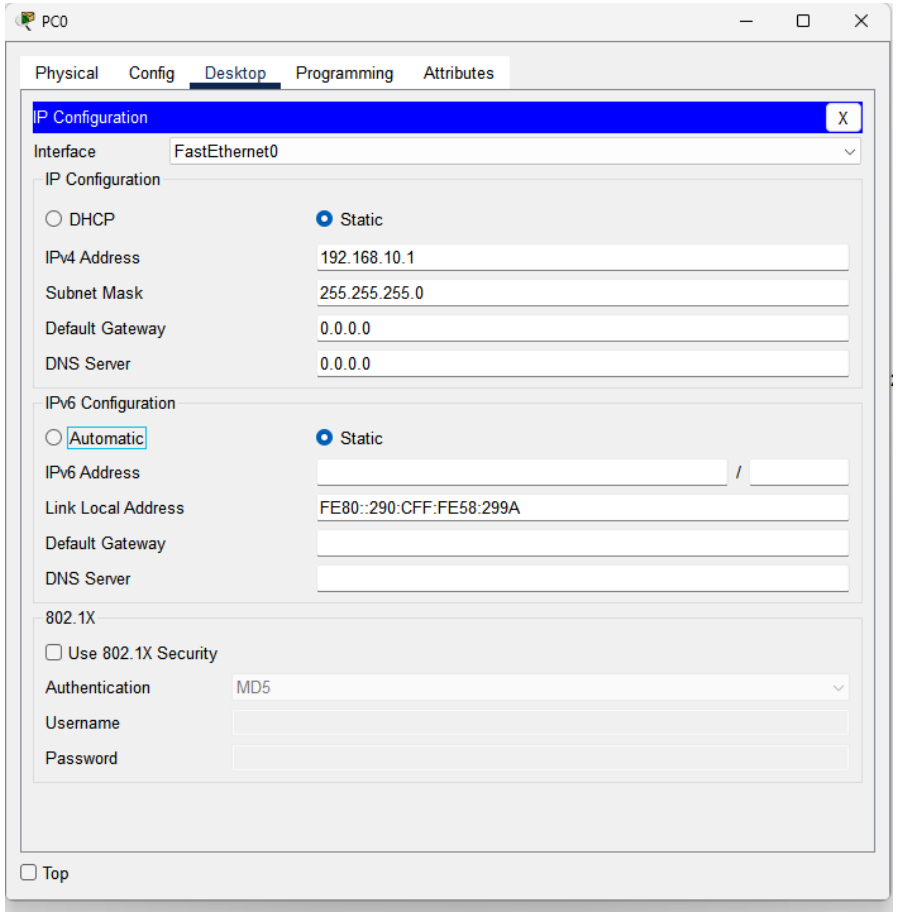
########## VLANs CONFIG STEPS ##########

1. Draw the necessary topology, decorate and give comments on VLANs + Network.
2. Assign host devices IP addresses.
3. Create VLANs on the switches and name them accordingly.
4. Identify switch ports of interest and assign them VLAN numbers that were created.
5. Identify and configure trunk ports between switches (just in case).
6. Test communication between VLANs.

NOTE: Devices in the same VLAN will communicate while devices in different VLANs will not communicate by default.

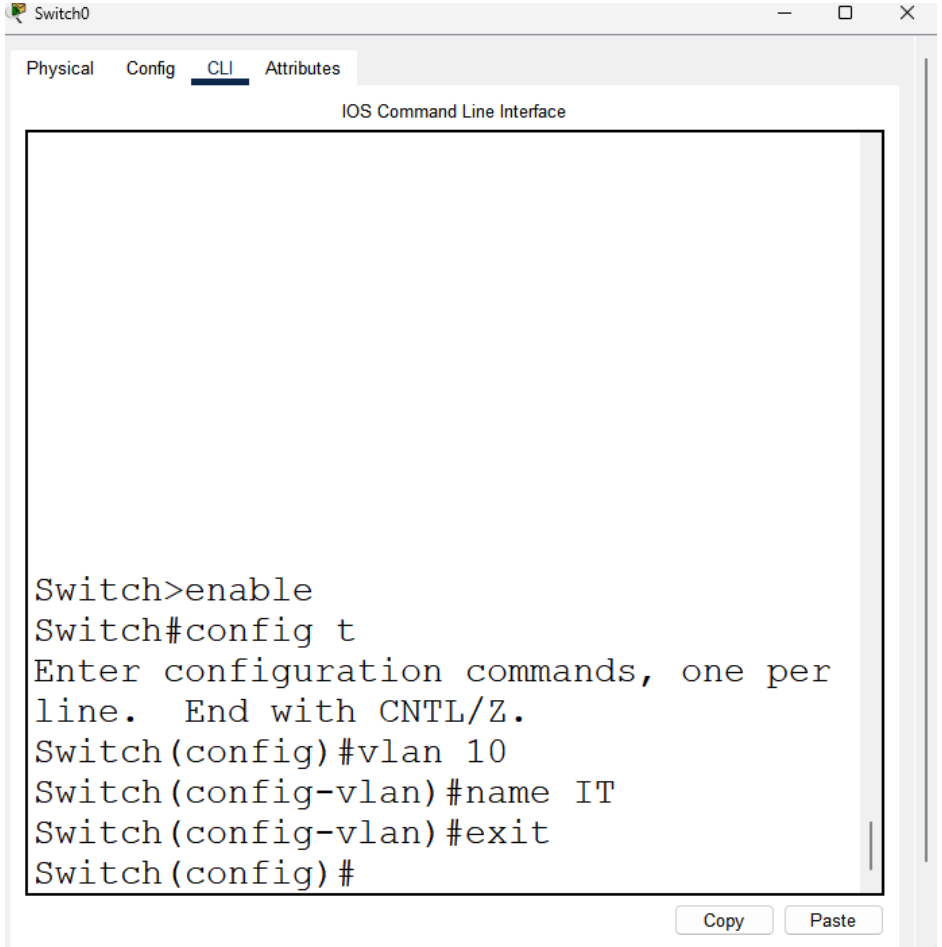
Complete the VLAN lab

- First configure all pcs based on subnet that they have for example for PC0



Complete the VLAN lab

- Configure Switch:
  - Check the switch command in reference sheet.(or look at image)
  - 1st : we need to create VLANs
  - 2nd : we give each VLAN a name
  - Repeat this steps for other VLANs regarding a related Switch (Switch 0 and switch 1)



Complete the VLAN lab

- Display all the VLANs with the following command
- You see VLAN name and id

```
Switch(config)#do show vlan
```

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
10   IT                               active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Complete the VLAN lab

- Get access to ports and assign vlan

```
Switch(config)#interface range fastEthernet0/2-3

Switch(config-if-range)#switchport mode access

Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#ex
```

- Repeat for other vlan and then execute

```
Switch(config)#do show vlan
```

- You should see all the interfaces with VLAN name and ports and status.

Complete the VLAN lab

- Configure Trunk port for both switches(be sure to select the correct interface. Check connection between switches

```
Switch(config)#interface fa0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
```

- Override the configuration

```
Switch(config)#do write
Building configuration...
[OK]
```

- Repeat the same steps for another switch

Complete the VLAN lab

- Test:
  - Devices with different VLANs cannot communicate over switches

```
C:\>ping 192.168.20.3

Pinging 192.168.20.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.20.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Champlain

COLLEGE SAINT-LAMBERT