**CSC 335 Data Communications and Networking**

**Practice Your Knowledge on VLAN**

Name: \_\_\_\_Tyler Prehl\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_6/21/21\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**1. Description**

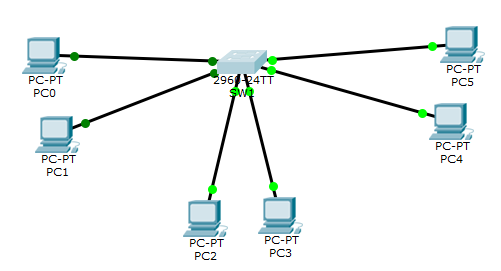
Switching has become the standard for most company internal network infrastructure as each port maintains its own collision domain, and with the advent of VLANs further allow the engineer to segment the network into multiple, smaller broadcast domains. As a Cisco engineer, as well as in the Cisco CCNA exam, you will need to know how to configure VLANs on Cisco switches as well as verify the option.

**Please answer all questions in red and attach required screenshots to this lab report and then submit it to D2L.**

**2. Lab Procedures**

**2.1 Topology**

Step 1: Creating the topology as following figure, where six PCs connected to the same switch



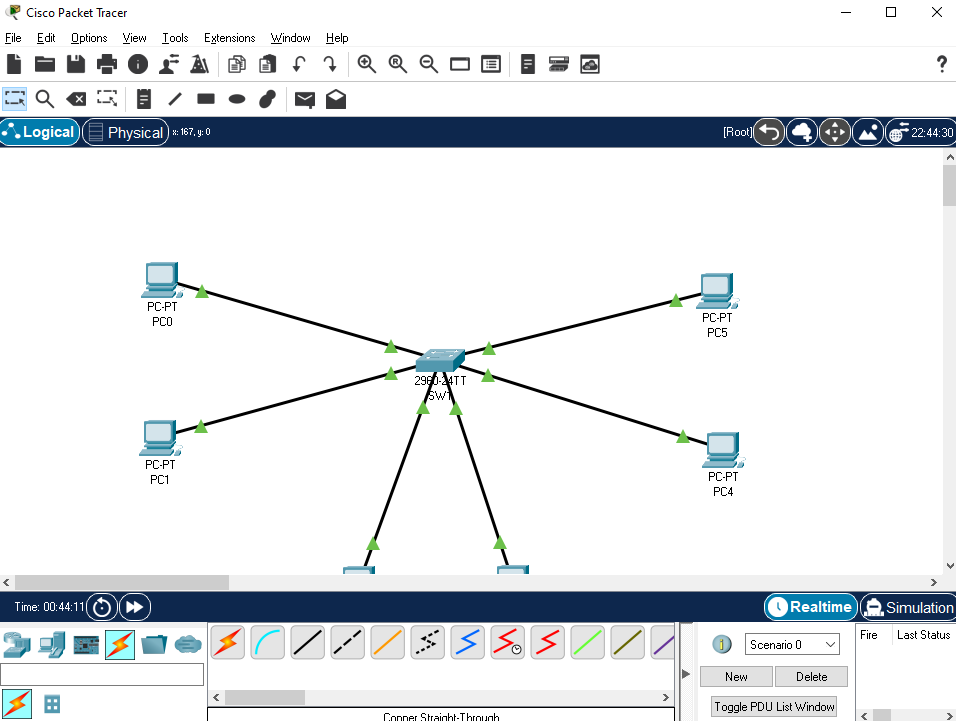
* PC0 interface FastEthernet 0 connect to swtich interface Fa0/1,
* PC1 interface FastEthernet 0 connect to swtich interface Fa0/2
* PC2 interface FastEthernet 0 connect to swtich interface Fa0/3
* PC3 interface FastEthernet 0 connect to swtich interface Fa0/4
* PC4 interface FastEthernet 0 connect to swtich interface Fa0/5,
* PC5 interface FastEthernet 0 connect to swtich interface Fa0/6

**2.2 General Settings**

Step 2: Configure the hostname and display name on Switch0 to be SW1.

C:\Users\75LCUI\AppData\Local\Temp\1493406128(1).png

**Show your topology with screenshot.**

****

Step 3: Configure no ip domain-lookup on SW1

Under the configure terminal mode, enter “no ip domain-lookup” command

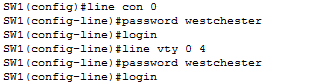
**What is the purpose for no ip domain-lookup command on switch?**

The purpose of the no ip domain-lookup command is so that if anything is an unfamiliar command, the device will not try to recognize it as a hostname but will return back to the user that it is an unknown command or hostname. In other words – it makes recognizing typos in the user’s commands easier.

Step 4: Configure the enable secret password as cisco on SW1

C:\Users\75LCUI\AppData\Local\Temp\1493406770(1).png

Step 5: Configure the console and vty password as westchester on SW1



**What is the meaning for line vty 0 4?**

Line vty 0 4 enters the vty configuration model for the first five vty lines (0-4).

Step 6: Configure the exec-timeout command to the console and virtual terminal lines

C:\Users\75LCUI\AppData\Local\Temp\1493407102(1).png

**What is the purpose for command exec-timeout 0 0?**

The purpose of the exec-timout 0 0 command is to disable the timeout feature – after one successful login with the password to either the console or vty line, the CLI will not lock the user out.

**2.3 Creating VLANs and assign add interfaces to each VLAN**

Step 7: Create the VLANs as shown in figure 1

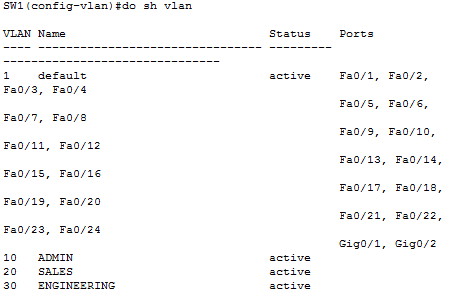
C:\Users\75LCUI\AppData\Local\Temp\1493407699(1).png

Configure vlan 20 (name SALES) and vlan 30 (name ENGINEERING) by using similar command.

**What is VLAN? Why we need VLAN?**

A VLAN is a “logical” network that essentially creates a private network over shared network infrastructure. We need VLAN to create secure networks where companies can separate users into logical groups of workers despite differing physical locations, to help alleviate traffic congestion without adding more bandwidth, to separate categories of traffic, and to make sure broadcast and multi-cast traffic only goes to members of the VLAN.

Step 8: verity vlan configuration by “do sh vlan” command

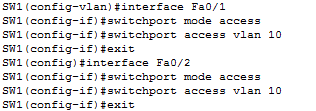


Step 9: Now, add interfaces to each of these VLANs with the switchport command as follows:

* interface Fa0/1, Fa0/2 belongs to VLAN 10, ADMIN
* interface Fa0/3, Fa0/4 belongs to VLAN 20, SALES
* interface Fa0/5, Fa0/6 belongs to VLAN 30, ENGINEERING

There are two ways to add interfaces: (1) add individual interfaces one by one, (2) add a range of interfaces. Let us start from the first method.

Step 9.1 add Fa0/1 and Fa0/2 to VLAN 10 individually



Step 9.2 add ports Fa0/3 – Fa0/4 to VLAN 20 as a group

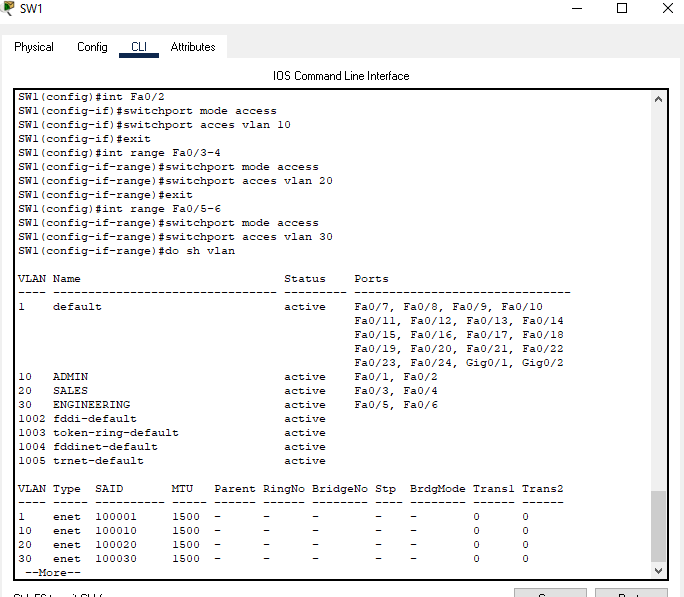
C:\Users\75LCUI\AppData\Local\Temp\1493650837(1).png

Configure interface fa0/5 and interface fa0/6 by using similar command.

Step 10: Verify your VLAN configuration using relevant show commands in Cisco IOS.

Show vlan configuration by using command “do sh vlan” under enable mode.

**Show your VLAN configuration screenshot.**

****

**2.4 Verify VLANs**

Step 11: assign IP address to hosts

You can click the PC, then select Desktop tab, choose IP configuration and enter the IP address

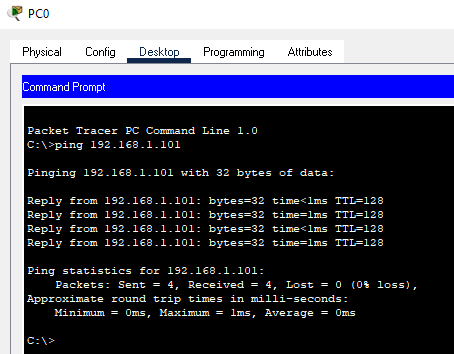
* PC0: 192.168.1.100 255.255.255.0
* PC1: 192.168.1.101 255.255.255.0
* PC2: 192.168.2.100 255.255.255.0
* PC3: 192.168.2.101 255.255.255.0
* PC4: 192.168.3.100 255.255.255.0
* PC5: 192.168.3.101 255.255.255.0

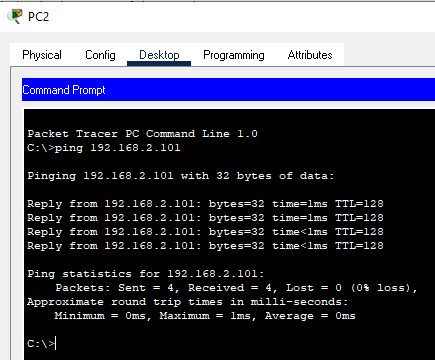
Step 12: ping within VLAN

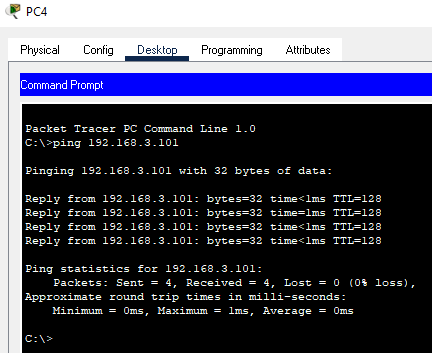
For example, you can click PC0, select Desktop tab, choose command prompt, then ping PC1 by typing command “ping 192.168.1.101” (PC0 and PC1 are in the same VLAN). You can also ping PC3 from PC2 (vice versa), and ping PC5 from PC4 (vice versa) by using proper IP address.

**Can you successfully ping devices in the same VLAN? Show the screenshot from ping, and explain WHY.**

Yes, you can ping devices in the same VLAN because they are connected over the same LAN and since they are both a part of the same VLAN, have permission to access to the other devices on the VLAN (the destination host is within the source’s local subnet).





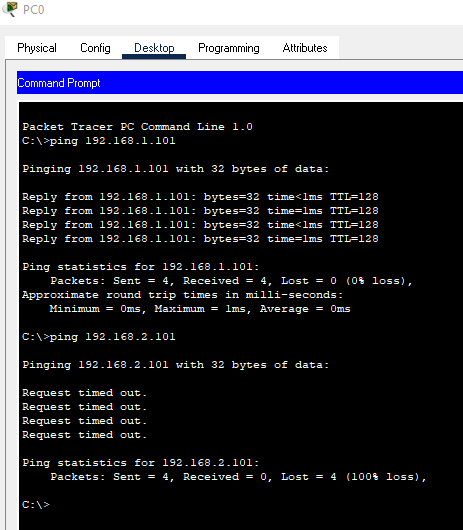


Step 13: ping devices in other VLAN

For example, you can click PC0, select Desktop tab, choose command prompt, then ping PC2, PC3, PC4, or PC5, such as “ping 192.168.1.105”

**Can you successfully ping devices in other VLANs? Show the screenshot from ping, and explain WHY.**

No, you cannot successfully ping devices in other VLANs because the destinations are outside the source’s local subnet. The solution to this problem is enabling a default gateway with a layer 3 switch or a router.

****

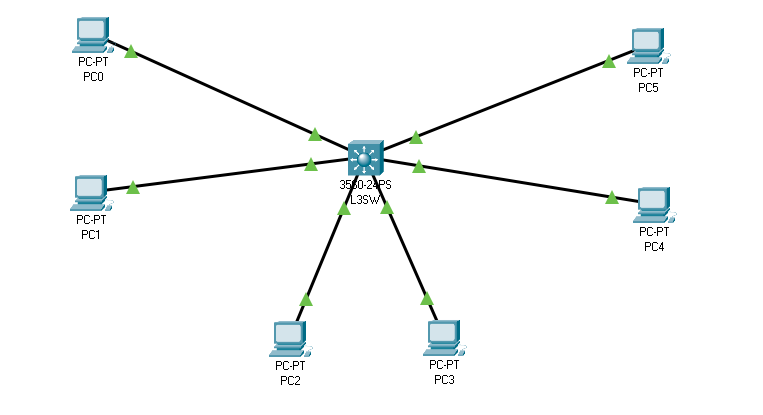


**2.5 OPTIONAL: Configure Inter VLAN Routing (2 points towards final grade)**

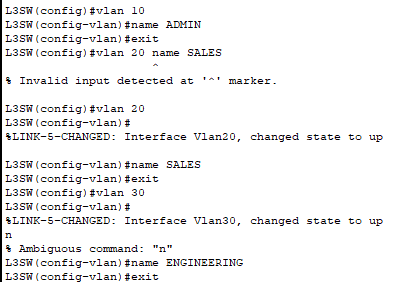
**Configure inter VLAN routing through Layer 3 switch. Show all the configuration steps as I did previously. Eventually, show that PC0 can successfully ping PC5.**

See the following pages for my steps and screenshots

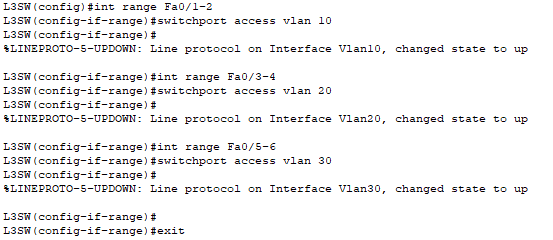
To configure inter VLAN routing through a layer 3 switch, the first step to take is to replace the 2960 switch with a 3560 24PS Layer 3 switch. Here is the topology, where L3SW is the Layer 3 Switch:



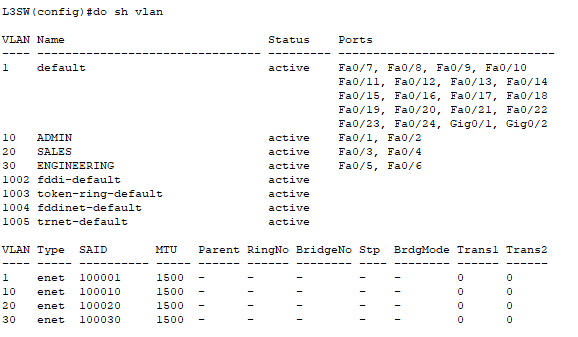
The next step is to recreate the VLANs:



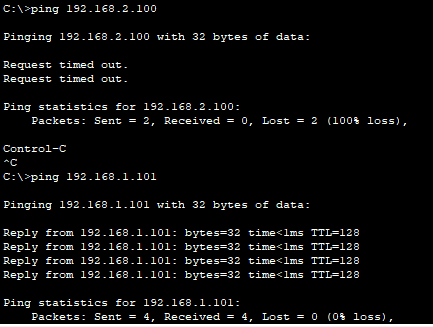
After creating the VLANs, you once again add the interfaces to the VLANs:



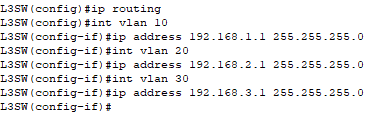
You can confirm successful completion of the above steps with the “do sh vlan” command:



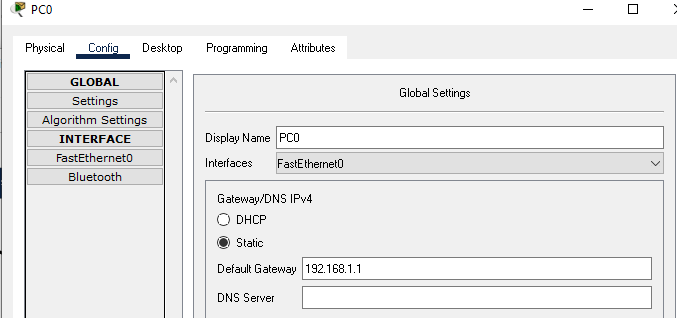
At this point, you can successfully ping intra-VLANs, but not inter-VLANs:



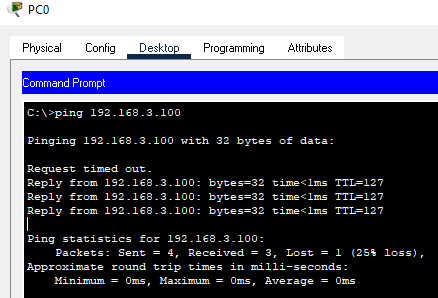
To enable inter-VLAN communication, you must activate ip routing on the Layer 3 switch with the command “ip routing”. Then create default gateways for the vlans:



After this step, go to each PC and give it the correct default gateway according to its VLAN (PCs 0 and 1 will have default gateway 192.168.1.1, and PCs 3 and 4 will have default gateway 192.168.2.1, etc).



Inter-VLAN routing should now be successfully configured, which can be tested by pinging PC5 (of VLAN 30) from PC0 (of VLAN1):



Success! :D