Lab 02 – 802.1Q, VTP, VLANs, and STP

For this lab, you will:

1. Create a network topology within Cisco Packet Tracer using the following information:

   - ✓ PC1's FastEthernet connection is connected to Switch1
   - ✓ PC2's FastEthernet connection is connected to Switch2
   - ✓ PC3's FastEthernet connection is connected to Switch3
   - ✓ PC4's FastEthernet connection is connected to Switch4
   - ✓ PC5's FastEthernet connection is connected to Switch1
   - ✓ PC6's FastEthernet connection is connected to Switch2
   - ✓ Switch1 is connected to Switch2 via two physical interfaces
   - ✓ Switch1 is connected to Switch3 via two physical interfaces
   - ✓ Switch1 is connected to Switch4 via two physical interfaces
   - ✓ Switch2 is connected to Switch4 via two physical interfaces
   - ✓ Switch2 is connected to Switch3 via two physical interfaces
   - ✓ Switch3 is connected to Switch4 via two physical interfaces
   - ✓ PC1's IP Address is 172.31.13.101/24
   - ✓ PC2's IP Address is 172.31.24.102/24
   - ✓ PC3's IP Address is 172.31.13.103/24
   - ✓ PC4's IP Address is 172.31.24.104/24
   - ✓ PC5's IP Address is 172.31.56.105/24
   - ✓ PC6's IP Address is 172.31.56.106/24
   - ✓ Switch1's administrative vlan interface IP Address is 172.31.99.11/24
   - ✓ Switch2's administrative vlan interface IP Address is 172.31.99.12/24
   - ✓ Switch3's administrative vlan interface IP Address is 172.31.99.13/24
   - ✓ Switch4's administrative vlan interface IP Address is 172.31.99.14/24

   - ✓ Remember to use straight-through cables when making the PC to Switch connections.
   - ✓ Remember to use cross-over cables when making the Switch to Switch connections.

   Please NOTE: For your subnet mask, /24 = 255.255.255.0

   You should specify all of your IP Addresses and subnet masks (in bit notation) within individual text boxes on your topology diagram for each interface or device that has one assigned. Make sure the interfaces are visible in your topology diagram as well.

   Please know that you should use a Cisco 3560 switch for Switch1 and Switch3 and a Cisco 2960 switch for Switch2 and Switch4.

2. Using the network topology from above, complete the following:

   a) On each PC, configure:

- ✓ IP Address
- ✓ Subnet Mask

b) On Switch1, configure:

- ✓ hostname
- ✓ an encrypted privileged mode password of 'cisco'
- ✓ the IP Address and Subnet Mask of the Administrative vlan interface of “int vlan 1”
- ✓ enable this interface
- ✓ enable 'logging synchronous' on the console line *(This enables the console line to synchronous the device with the terminal emulation program.)*
- ✓ password of 'cisco' on the console line
- ✓ enable a login prompt to appear when consoling into the router from the PC
- ✓ enable 'logging synchronous' on the first sixteen virtual terminal lines
- ✓ password of 'cisco' on the first sixteen virtual terminal lines
- ✓ enable a login prompt to appear when using the first sixteen virtual terminal lines (ie: when you telnet into the router from the PC you should receive a login prompt)
- ✓ setup this switch as a VTP Server using the domain name of ‘INETLAB’ and password of ‘cisco’
- ✓ create VLAN 13 and name it ‘PC1+PC3’
- ✓ create VLAN 24 and name it ‘PC2+PC4’
- ✓ create VLAN 56 and name it ‘PC5+PC6’
- ✓ setup the interface of the switch that PC1 is connected to as an Access port.
- ✓ assign this interface to VLAN 13
- ✓ setup the interface of the switch that PC5 is connected to as an Access port.
- ✓ assign this interface to VLAN 56
- ✓ setup all switch to switch connections to use IEEE 802.1Q encapsulation
- ✓ make sure this switch is the STP root bridge
- ✓ save your current configuration file named running-config (stored in RAM) to the configuration file named startup-config (stored in NVRAM)
- ✓ display your vlans
- ✓ display your interfaces in use in an abbreviated format (ie: show ip int brief)
- ✓ display the status of your STP

c) On Switch3, configure:

- ✓ hostname
- ✓ an encrypted privileged mode password of 'cisco'
- ✓ the IP Address and Subnet Mask of the Administrative vlan interface of “int vlan 1”
- ✓ enable this interface
- ✓ enable 'logging synchronous' on the console line
- ✓ password of 'cisco' on the console line
- ✓ enable a login prompt to appear when consoling into the router from the PC
- ✓ enable 'logging synchronous' on the first five virtual terminal lines
- ✓ password of 'cisco' on the first five virtual terminal lines

- ✓ enable a login prompt to appear when using the first five virtual terminal lines (ie: when you telnet into the router from the PC you should receive a login prompt)
- ✓ setup this switch as a VTP Server using the domain name of 'INETLAB' and password of 'cisco'
- ✓
- ✓ create VLAN 13 and name it 'PC1+PC3'
- ✓ create VLAN 24 and name it 'PC2+PC4'
- ✓ create VLAN 56 and name it 'PC5+PC6'
- ✓ setup the interface of the switch that PC3 is connected to as an Access port.
- ✓ assign this interface to VLAN 13
- ✓ setup all switch to switch connections to use IEEE 802.1Q encapsulation
- ✓ make sure this switch is the STP root bridge if Switch1 fails and can no longer be the STP root bridge
- ✓ save your current configuration file to nvram (ie: the filename should be 'startup-config)
- ✓ display your vlans
- ✓ display your interfaces in use in an abbreviated format (ie: show ip int brief)
- ✓ display the status of your STP

d) On Switch2, configure:

- ✓ hostname
- ✓ an encrypted privileged mode password of 'cisco'
- ✓ the IP Address and Subnet Mask of the Administrative vlan interface of "int vlan 1"
- ✓ enable this interface
- ✓ enable 'logging synchronous' on the console line
- ✓ password of 'cisco' on the console line
- ✓ enable a login prompt to appear when consoling into the router from the PC
- ✓ enable 'logging synchronous' on the first five virtual terminal lines
- ✓ password of 'cisco' on the first five virtual terminal lines
- ✓ enable a login prompt to appear when using the first five virtual terminal lines (ie: when you telnet into the router from the PC you should receive a login prompt)
- ✓ setup this switch as a VTP Client using the domain name of 'INETLAB' and password of 'cisco'
- ✓ setup the interface of the switch that PC2 is connected to as an Access port.
- ✓ assign this interface to VLAN 24
- ✓ setup the interface of the switch that PC6 is connected to as an Access port.
- ✓ assign this interface to VLAN 56
- ✓ setup all switch to switch connections to use IEEE 802.1Q encapsulation
- ✓ save your current configuration file to nvram (ie: the filename should be 'startup-config)
- ✓ display your vlans
- ✓ display your interfaces in use in an abbreviated format (ie: show ip int brief)
- ✓ display the status of your STP

e) On Switch4, configure:
- ✓ hostname
- ✓ an encrypted privileged mode password of 'cisco'
- ✓ the IP Address and Subnet Mask of the Administrative vlan interface of “int vlan 1”
- ✓ enable this interface
- ✓ enable 'logging synchronous' on the console line
- ✓ password of 'cisco' on the console line
- ✓ enable a login prompt to appear when consoling into the router from the PC
- ✓ enable 'logging synchronous' on the first five virtual terminal lines
- ✓ password of 'cisco' on the first five virtual terminal lines
- ✓ enable a login prompt to appear when using the first five virtual terminal lines (ie: when you telnet into the router from the PC you should receive a login prompt)
- ✓ setup this switch as a VTP Client using the domain name of ‘INETLAB’ and password of ‘cisco’
- ✓ setup the interface of the switch that PC4 is connected to as an Access port.
- ✓ assign this interface to VLAN 24
- ✓ setup all switch to switch connections to use IEEE 802.1Q encapsulation
- ✓ save your current configuration file to nvram (ie: the filename should be 'startup-config)
- ✓ display the status of your VTP configuration
- ✓ display your vlans
- ✓ display your interfaces in use in an abbreviated format (ie: show ip int brief)
- ✓ display the status of your STP

f) Verify each PC is able reach the other PCs within the same VLAN using the Windows CLI commands you learned in class. Provide screenshot captures of the output within your lab report for the verification.

g) Verify each Switch is able to reach the other Switches within in the topology using the Cisco IOS CLI commands you learned in class. Provide screenshot captures of the output within your lab report for the verification.

h) Display the status of STP and highlight the portion of the screenshot displaying the switch that is the root bridge. Provide a screenshot capture of the output.

Please NOTE: When you provide a screenshot capture, please do not capture the entire screen. Minimize this to a specific window or output you are focusing on.

Please NOTE: Download and install Cisco Packet Tracer. This software is supported on Windows, macOS, or Linux. The switch models you will be using in Cisco Packet Tracer are the 3560 and the 2960 Switches for this lab. Please know the way you implement IEEE 802.1Q may differ from switch to switch.

Make sure you save your packet tracer file frequently (and make a backup copy) so you do not lose your work in case the application crashes. It is always nice to revert back to a previous backup in case the file is corrupt.

3. Create a lab report document and include the following information:

    a) **Description:** Brief Description of what topic or technology you are concentrating on within this lab. Keep this short and to the point.

    b) **Topology/Diagram:** Take the original topology you created within Cisco Packet Tracer and take a screenshot of the topology. Paste this into your Document. Please do not submit a screen capture of your entire screen or window. This should ONLY be of the topology. Make sure you include IP Addresses in your topology with the interfaces showing.

    c) **Syntax:** Table of Command Syntax and the associated description (ie: If you issued a cli command within the Cisco IOS or within the Windows CMD prompt, list it here and write a description as to what it does in your own words) – please make sure this is written in a nice, easy-to-read table format. (CLI Command on the left, description on the right, and (optionally) add another column for what mode of Cisco IOS you are in when issuing the CLI command.)

    d) **Verification:** This is screenshot based. You will be asked to provide screenshots to verify that you have completed the assignment correctly. Please only include the screenshots I ask of you. Nothing more. These are listed above within the specifications.

    e) **Conclusion:** Wrap up your lab report with a short conclusion. If something did not work, state it. If everything did work successfully, state that as well.

    Please NOTE: Your submission should not include one screenshot per page. Please maximize the space on each page. The lab report should (most likely) be less than four or five pages – It could even be two to three pages in length depending upon the screenshots I ask you to submit for verification. Please make sure the screenshots are legible though!

4. Submit your lab report as a .pdf file and your .pkt to the appropriate assignment within iLearn.

(Please do not zip these files nor should you submit multiple .pngs, .gifs, .jpgs, etc…)

Good Luck with your lab!