**CSCI 7000-011 Introduction to Enterprise Networks**

# Lab 1

## Learning about Switches

**Spring 2020**

## OBJECTIVES

1. **Learn how to perform basic switch configuration & troubleshooting including.**
    a. **Review basics for switch password assignment and IOS navigation**
    b. **How to activate/deactivate a Port**
    c. **How to change the Speed and Duplex Mode on a Switch port**
    d. **How to verify the MAC addresses of computers connected to a specific port**
2. **Learn how to secure a Switch port so that only a specific user/device can connect to it.**
3. **Learn how to Create VLANs within a single Switch**
4. **Learn how to create VLANs across multiple Switches**
5. **Learn how to achieve Inter-VLAN communication using Trunking Protocols such as 801q and ISL**
6. **Configure VLAN Trunking Protocol (VTP) to manage multiple switches from a single one**
7. **Review the usage of Spanning Tree Protocol and how switching environment behaves in the event of a network failure**
8. **Learn how Rapid Spanning Tree Protocol (RSTP) or IEEE 802.1W is essential for faster convergence**
9. **Learn to increase efficiency of a redundant network (PVST)**
10. **Learn about optional STP features like “Portfast” and “Etherchannel”**
11. **Sniff packets from your network.**

**1. Port Configuration:**

This is in continuation to the lab 0. The sniffer station will be PC-A and the other PC will be PC-B

a) Ping from PC-A to PC-B

b) Check the status of ports on switch using 'show interface status' or 'show ip interface brief'

c) Configure Port that connects PC-A to Switch. Set it up to 10Mbps and Half Duplex

d) Verify that PC-B adjusts to Switch port configuration

e) Verify that PC-A still reaches PC-B

**2. Port Security:**

a) Configure the switch port that connects to PC-A, so it does not permit any other computer to use it.

b) Swap cables that connect to PC-B and PC-A to verify if your security policy works. (report the messages you get on the IOS console as well as the port status after the security policy

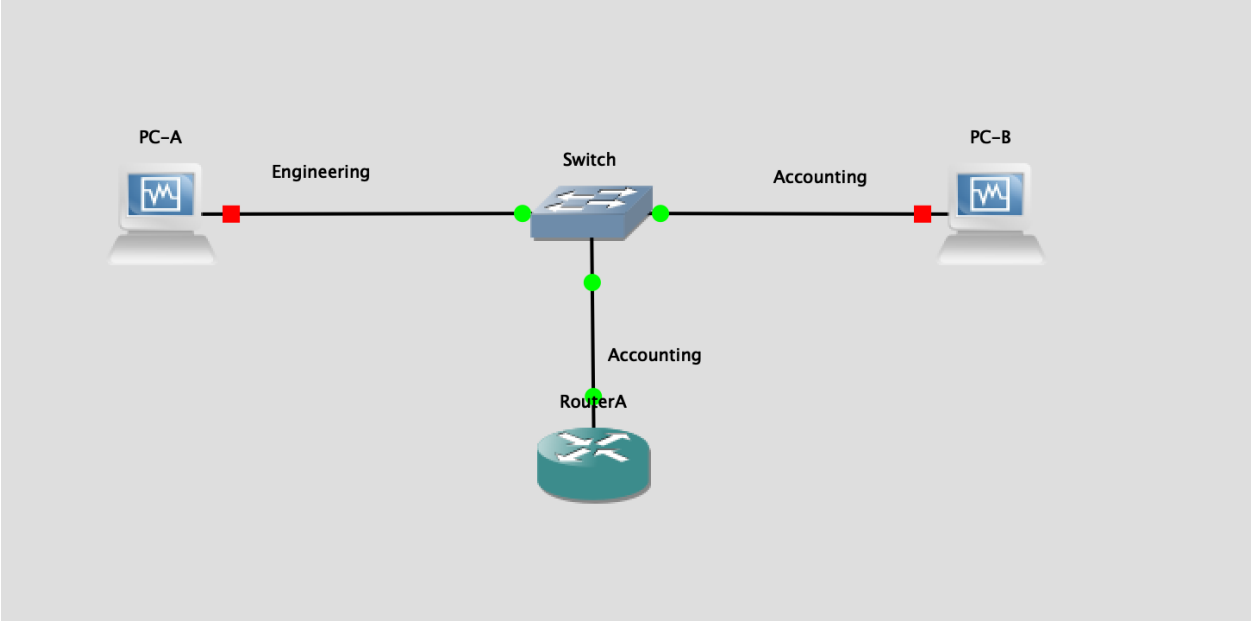
is applied)

c) Verify network reachability. Report your results.

d) Restore network connectivity without reconnecting equipment. (**Adjust security policy only)**

**3. Single Switch VLAN configuration:**

a) Connect another router to the switch as shown in the figure



b) Assign IP address to the router in the same subnet as that of the PCs, verify reachability(ping).

c) Create 2 different VLANs (Engineering and Accounting). Use appropriate commands on your switch to verify their existence **(Copy a screenshot on your Report)**

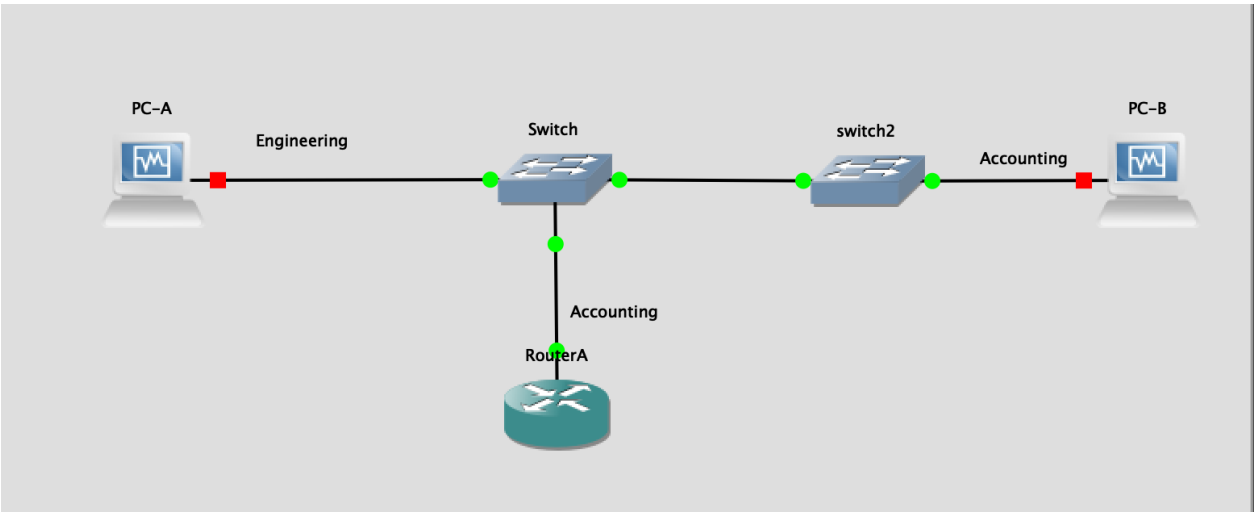
d) Assign PC-A to Engineering, PC-B and Router to Accounting. **Do not Change IP addressing**. Verify IP reachability from/to all endpoints.

e) Do you need to worry about same IP addressing on Different VLANs? Why or Why not?

f) Enable telnet on the switch. Give IP addressing so that you should be able to telnet to the switch from PC-A.

**4. Multiple Switch VLAN configuration:**

1. Add a second switch to your network environment.

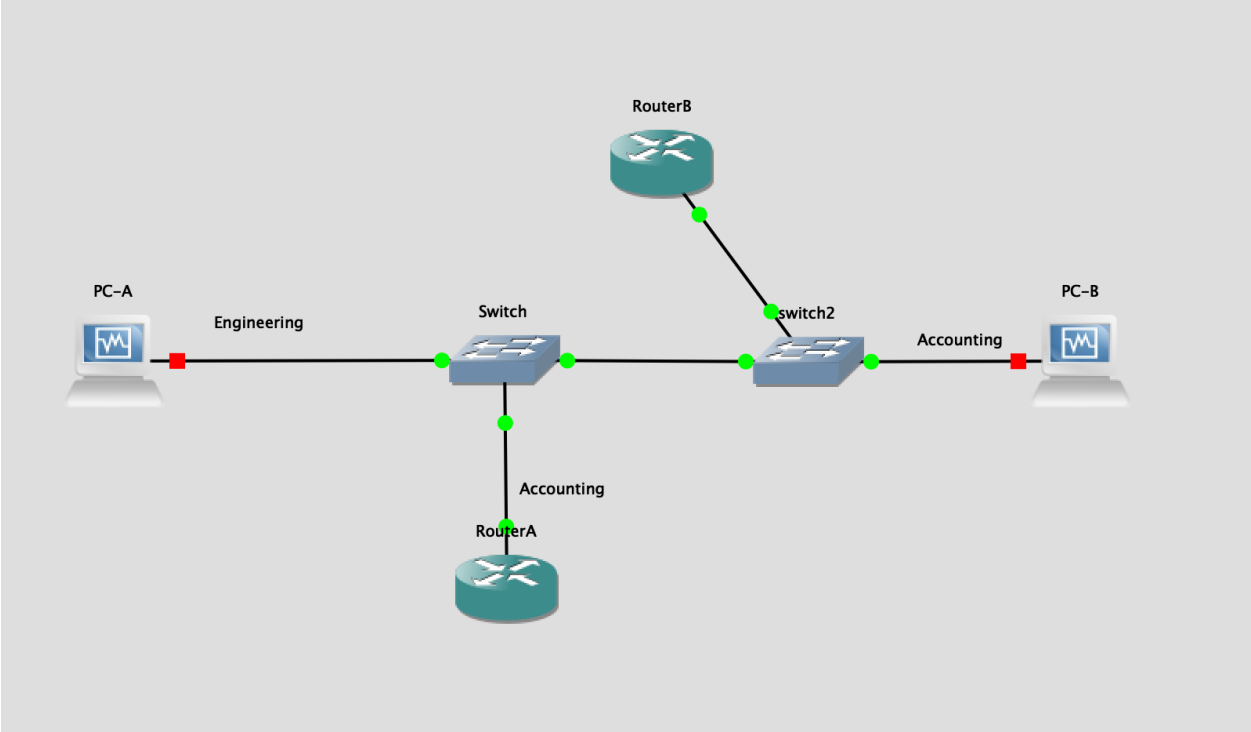



2. Use appropriate commands to restore network reachability.

3. Which trunking encapsulation was supported by both Switches?

**5. Inter-- VLAN Communication (Router on a Stick configuration):**

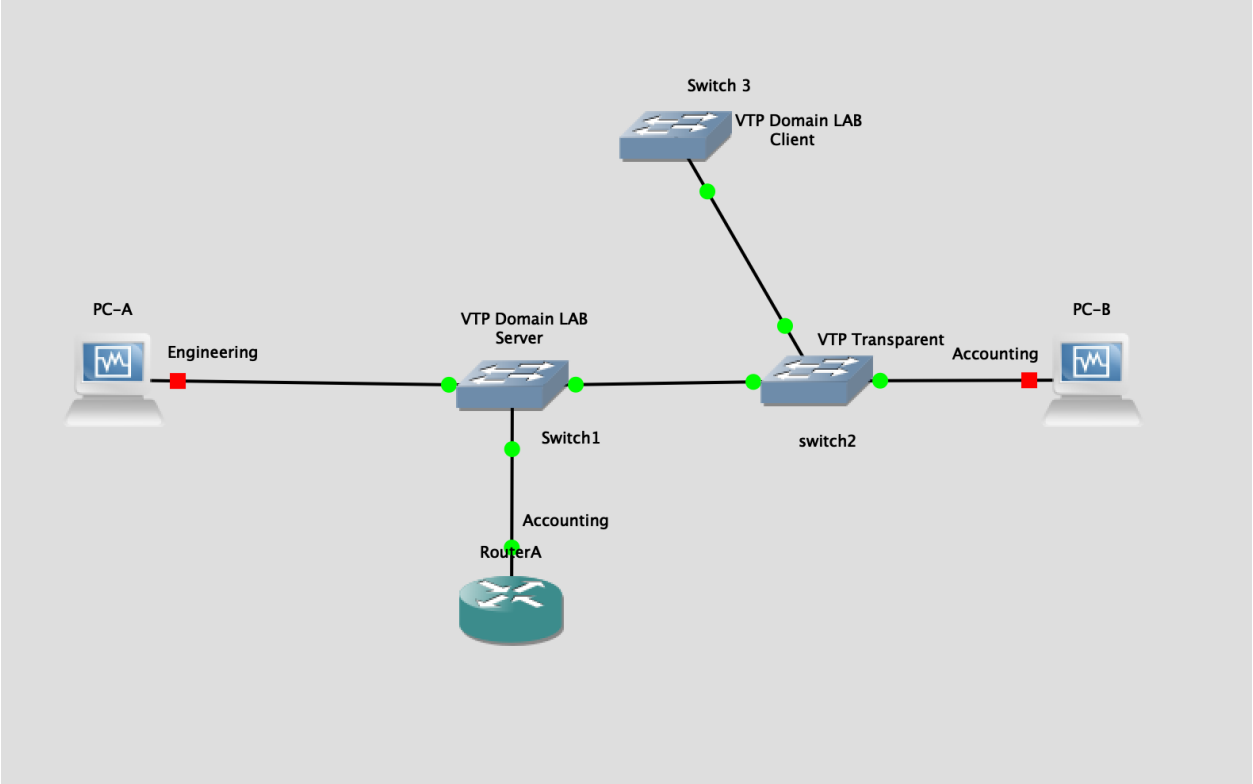
a) Add a Router to your network environment in order to permit Inter-VLAN communication.




b) Achieve Inter-VLAN communications – you should be able to ping between both the PC's and router. Include in your report configuration lines form all 3 devices – (only important sections plus copy of pings from PC A to the rest)

## 6. Configuring VLAN Trunking Protocol (VTP):

a) Remove ONLY the Router and add a third Switch instead.




b) Create a VTP domain that is only relevant to Switch 1 and Switch 3. Report IOS commands used or partial switch configuration used.

c) Confirm that the VLANs available at Switch 1 (Engineering and Accounting) are propagated via VTP to Switch 3 only

d) Move Router A from Switch 1 to an Engineering port on Switch 3 and verify reachability between the PC's and router. Modify RouterA's IP address if necessary.

e) Change the name of Engineering VLAN to HumanRes ONLY on Switch 1. Verify that Switch 3 adjusts to the new changes automatically as result of VTP. Report from Switch IOS VLAN name propagation

## 7. Spanning Tree Protocol

Keep “debug spanning-tree bpdu” and “debug spanning-tree switch” ON on switch 1. Explain the messages generated from these commands when the topology changes.

a) Use appropriate IOS command to verify on which ports do MAC addresses from PC1 and PC2 are being registered (on all switches) Explain your findings.

b) Add a link between Switch 1 and Switch 3

c) Use appropriate commands to obtain the following information from each switch

i. Bridge ID

ii. Root Bridge

iii. Root Ports

iv. Designated Ports

e) Use appropriate commands to replace the root bridge for another of your preference.

f) Shut down one of the ports that connects your Root Bridge to another Switch, document how long does it take STP to re-converge (Report)?

Stop the DEBUG once done

**Rapid Spanning Tree Protocol (RSTP)**

Keep “debug spanning-tree bpdu” and “debug spanning-tree switch” ON on switch 1.
Explain the messages generated from these commands when the topology changes.
STP has disadvantage that it has low convergence which is important at layer 2 LAN. IEEE with document 802.1W introduced an evolution of spanning tree protocol: Rapid Spanning Tree Protocol (RSTP), which reduces the convergence time after a topology change occurs in the network. STP takes 30 to 50 seconds from transit from blocking state to forwarding state. RSTP usually responds less than 10 seconds of a physical link failure.

a) Enable RSTP on all the switches

b) Make Switch 3 the root bridge for HumanRes VLAN. Report the command that was used for this.

c) Shut down one of the ports that connects your Root Bridge to another Switch, document
how long does it take STP to re-converge (Report) Stop the debug commands?

References: http://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/24062146.html

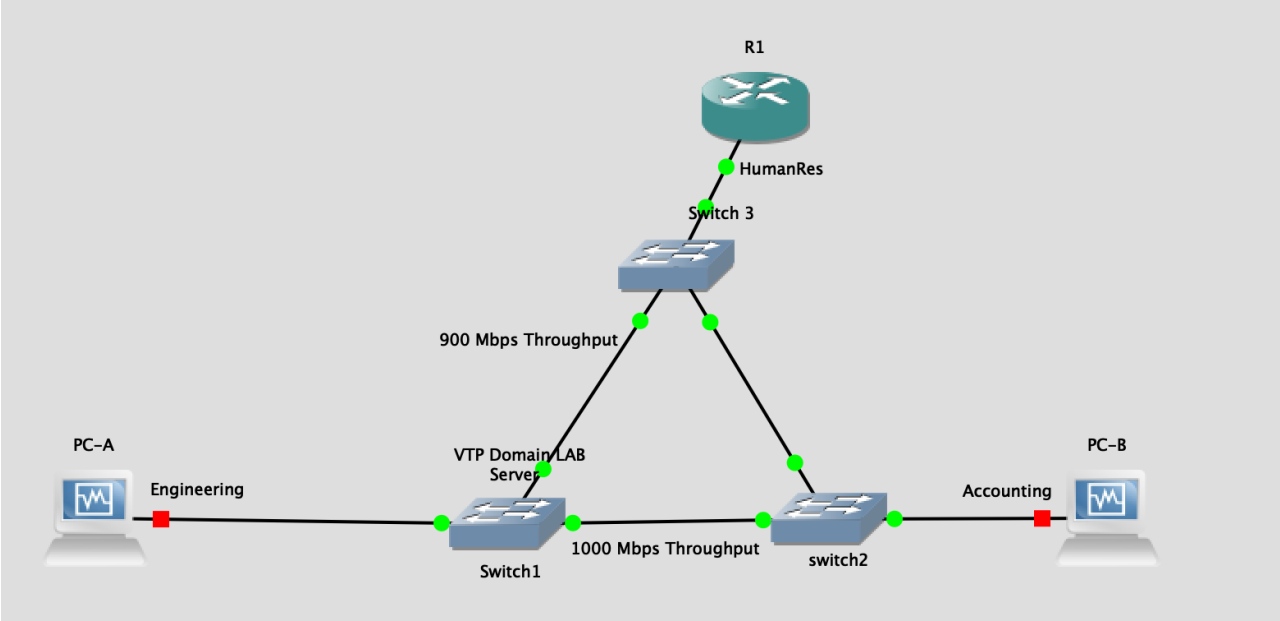
**9.Portfast:**

What are the advantages of portfast?

Enable portfast on one of the ports on which your computer is connected

Verify the change in response time. Give a snapshot of the debug command used and explain what you see in it.

**10.Etherchannel:**




a) You are facing congestion problems on your uplinks to the root bridge, use EtherChannel to increase network capacity as mentioned in the diagram for total throughput per uplink.

b) Verify that STP maintains its tree, regardless of bundled ports.

c) Document what happens if you lose one of your EtherChannel ports (i.e. unplug a cable).

Do you notice any STP changes? Why or why not? Keep debug commands on for spanning tree. Explain the messages you get from them.

d) Explain the difference between speed and bandwidth. Which of these features was useful to you for this objective?

**11.Configuring SPAN (Packet sniffing from your network):**

a) What does SPAN do? Why is this capability provided?

b) Configure SPAN on one of your switch ports

c) Capture a ping sent from one PC to another in the network (Run wireshark on a SPAN port). Include a screenshot in your report and explain.

**Report Questions:**

1) How would you secure a switch to prevent others from accessing the network? (Hint: think layers)

2) What is the length of the MAC address? How is it divided?

3) Are sticky ports secure? Why or why not? Is it recommended?

4) Why are switches faster than routers?

5) How many MAC addresses does your computer have? How do you find out?

6) What problem is portfast meant to solve in a network?

7) Can you change your MAC address? If so, How?

9) Name/explain other applications of SPAN (Why do we need port replication/monitoring services for?)

10) What are the advantages of using VLANs?

11) Tell me any disadvantages of using VLANs

12) Can you do trunking with a PC? Is this a popular practice?

13) Can you telnet into a switch? Can any PC on any VLAN telnet into a switch (assume all PC's are connected to the same switch)?

14) Why do we need a Native VLAN for?

15) Give any important details regarding native VLANs in 802.1Q trunking.

16) Find and explain other trunking services used in industry.

17) What is a multilayer switch?

18) Explain how is RSTP better than STP?

19) What is the advantage of having Per VLAN STP? Explain VTP VLAN pruning.

19) Why do we need a Native VLAN for?

20) Give any important details regarding native VLANs in 802.1Q trunking.

21) Find and explain other trunking services used in industry.

22) What is a multilayer switch? What internal processing has to happen inside the switch (to the packet) in order to be able to do forward data based on layer 3 information?

23) Explain how is RSTP better than STP