CSCI 5010 – Fundamentals of Data Communications

Lab 2 – Introduction to Cisco IOS and Switching Spanning Tree Protocol (STP)

University of Colorado Boulder

Department of Computer Science

Network Engineering

Professor Levi Perigo, Ph.D.

# Summary

This lab will provide an introduction to Cisco IOS, and how to use the Command Line Interface (CLI). For Cisco devices, the CLI is the primary way to configure and troubleshoot. It is important that you understand the basic CLI commands to navigate a Cisco device. Several videos have been linked for additional assistance and clarification, but you are also encouraged to search for other videos that may be of assistance to you.

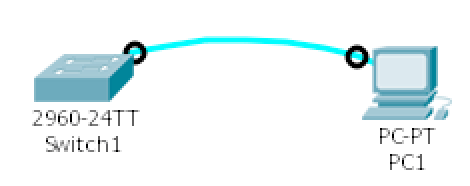
The foundational layer to any network revolves around switching. This lab is intended to be an overview of Cisco IOS, and switching technology - STP.

The questions in the lab are intentionally vague. The purpose of this is for you not only to research, investigate, and learn the technologies, but also become proficient at interpreting both non-technical and technical questions. Being able to research and discover answers on your own will be critical as you progress in your career.

* Learn how to perform basic switch configuration & troubleshooting including:
  + Switch password assignment and IOS navigation
  + How to activate/deactivate a port
  + How to change the speed and duplex of a port
  + How to verify the MAC addresses of computers connected to a specific port
* Review the usage of Spanning Tree Protocol (STP) including how switching environments behave regarding:
  + network failure
  + network loops

# Part 1

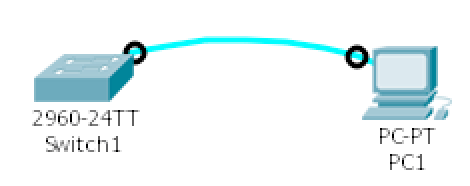
# Objective 1: Connect PC to Cisco Switch in Cisco Packet Tracer This objective will provide instructions for how to connect a PC to a Cisco device for configuration purposes.



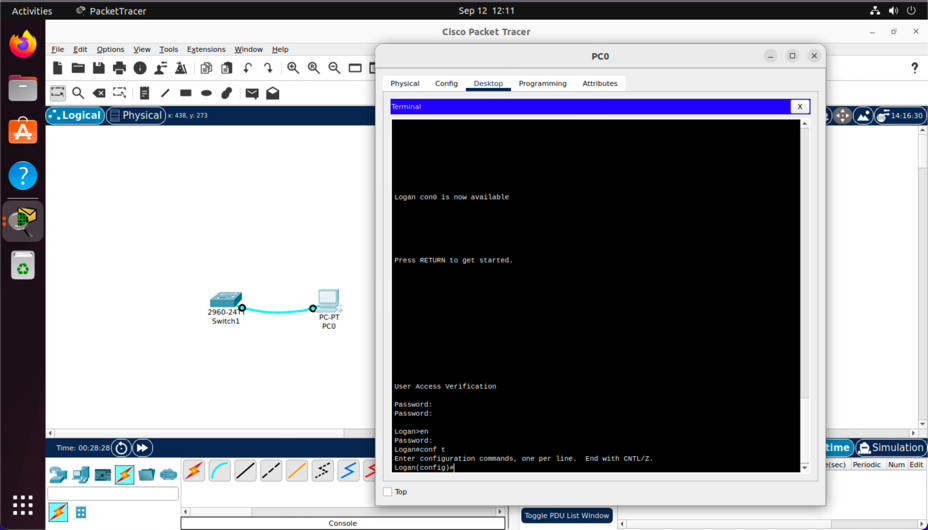
1. Use a Cisco console cable to connect PC1 to the switch “Switch1”

# Objective 2: Cisco IOS User Levels & Command Line Interface (CLI)

This objective will provide an introduction to Cisco IOS network device user levels. Cisco user levels are important to understand how to navigate the prompts of a Cisco device and determine how to configure and troubleshoot the device.



1. Follow the Cisco documentation [Using the CLI](http://www.cisco.com/c/en/us/td/docs/ios/12_2/configfun/configuration/guide/ffun_c/fcf001.html).
2. Configure the hostname on the switch to be “your name.”
3. Create an enable password of “cisco”
4. Create a console password of “lab”.
5. Logout from the switch and console again using the PC (PC>>Desktop>>Terminal).
   1. Make sure to remember which password is for which level
   2. Verify the spelling and case sensitivity. Paste the screenshot of successful login. **[10 points]**



1. Paste the switch’s running configuration **[5 points]**

Logan#show running-config

Building configuration...

Current configuration : 1124 bytes

!

version 15.0

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname Logan

!

enable password cisco

!

!

!

!

!

!

spanning-tree mode pvst

spanning-tree extend system-id

!

interface FastEthernet0/1

!

interface FastEthernet0/2

!

interface FastEthernet0/3

!

interface FastEthernet0/4

!

interface FastEthernet0/5

!

interface FastEthernet0/6

!

interface FastEthernet0/7

!

interface FastEthernet0/8

!

interface FastEthernet0/9

!

interface FastEthernet0/10

!

interface FastEthernet0/11

!

interface FastEthernet0/12

!

interface FastEthernet0/13

!

interface FastEthernet0/14

!

interface FastEthernet0/15

!

interface FastEthernet0/16

!

interface FastEthernet0/17

!

interface FastEthernet0/18

!

interface FastEthernet0/19

!

interface FastEthernet0/20

!

interface FastEthernet0/21

!

interface FastEthernet0/22

!

interface FastEthernet0/23

!

interface FastEthernet0/24

!

interface GigabitEthernet0/1

!

interface GigabitEthernet0/2

!

interface Vlan1

no ip address

shutdown

!

!

!

!

line con 0

password lab

login

!

line vty 0 4

login

line vty 5 15

login

!

!

!

!

end

* 1. Do you see the settings you configured?
     1. Hostname
        1. “hostname Logan”
     2. Enable password
        1. “enable password cisco”
     3. Console password

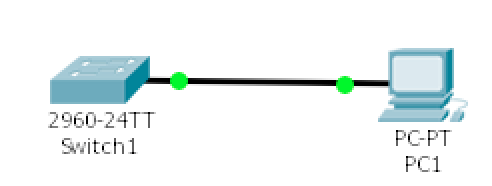
line con 0

password lab

login

# Objective 3: Creating Remote Access to Cisco Networking Device (Telnet)

This objective will allow you to connect remotely to the Cisco device via the network, without using a console cable in Cisco Packet Tracer. Use this “[Enable Telnet](https://www.youtube.com/watch?v=cb7jCMNJLkQ)” video for assistance.

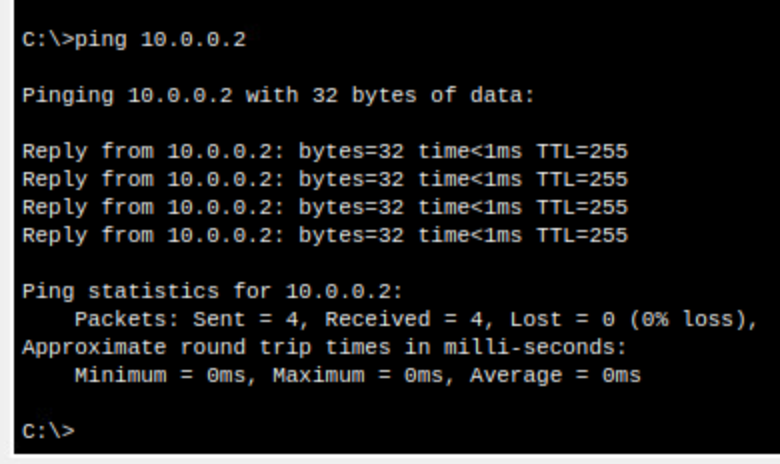


1. Configure and connect the PC and switch according to the diagram. Which cable did you use this time? **[2 points]**

I used a copper straight through cable

* 1. Make sure the PC has an IP address (10.0.0.1) and subnet mask (255.255.255.0) in the same subnet as the switch (VLAN 1 IP - 10.0.0.2/255.255.255.0)

1. Verify the PC can ping the IP address of the switch. Paste the screenshot of the command output. **[5 points]**



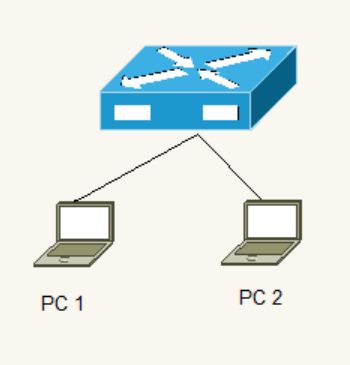
1. Configure Telnet on the switch
   1. Use all the vty lines
   2. Create a password of “telnet” as “cisco”
2. Use Terminal (PC>>Desktop>>Command Prompt) of the PC to Telnet to the switch. Paste the screenshot of telnet output. **[10 points]**

A screen shot of a computer

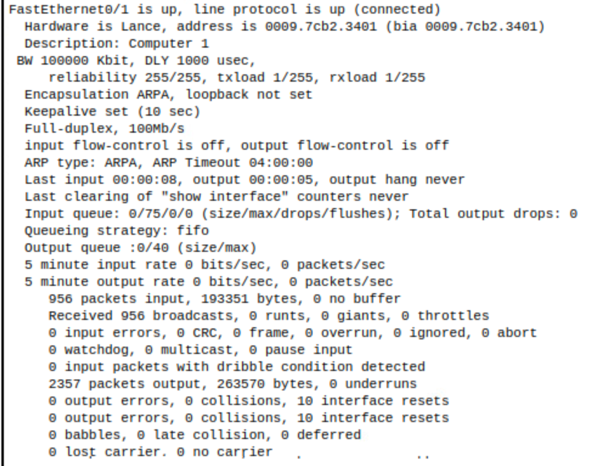
Description automatically generated

# Part 2

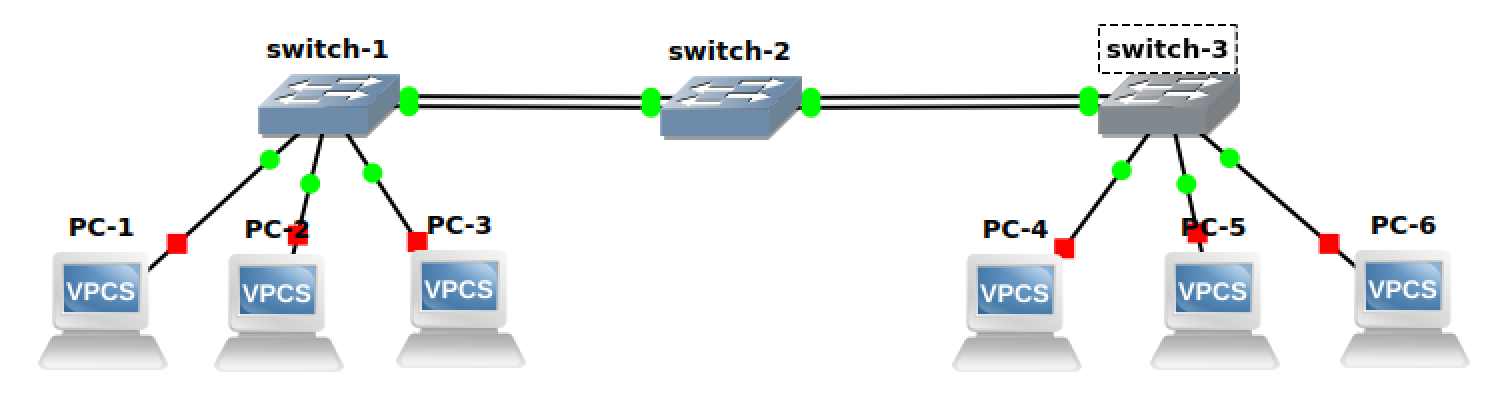
# Objective 1: Cisco IOS Switch Port Configuration This objective will allow you to configure port settings on the industry standard Cisco switches.



1. Connect PC1 and PC2 to a switch
2. Configure a description on the switchports connected to each PC
   1. The port connected to PC 1 should have a “description Computer 1”
   2. The port connected to PC 2 should have a “description Computer 2”
3. Configure the necessary steps to ping from PC1 to PC2 (*hint: you will have to configure settings on the switch (use the default VLAN), but you will also have to configure both PCs*)
   1. List the steps you had to perform to get the PCs to ping each other [**20 points**]
4. First I entered the switch to configure the ports that were connected by the 2 computers
5. I configured both ports individually, making their switchport mode access and doing a no shutdown to enable those ports
6. I then created a VLAN 1 with IP: 10.0.0.1 and subnet: 255.255.255.0 and enabled it
7. I then went to each PC desktop and clicked the IP configuration option and configured PC1 with 10.0.0.2 \ 255.255.255.0 and PC2 with 10.0.0.3 \ 255.255.255.0
8. I then went onto the command prompt of PC1 and entered: ping 10.0.0.3 and it worked!
9. Check the status of the switch port connected to PC1
   1. Provide a screenshot of the status of the port [**2 points**]



* + 1. Indicate that the port is up [**2 points**]
       1. As you can see on the first line in the screenshot, FastEthernet0/1 is up
    2. Indicate the speed and duplex of the port [**2 points**]
       1. As you can see on line 8, the port is Full-duplex, 100Mb/s
    3. Make sure it has the proper description (above)
       1. As you can see on line 3: Description: Computer 1

1. Configure the switch port that connects to PC1
   1. Hard set the port to 10Mbps and Half Duplex
   2. Can PC1 still reach PC2? Why or why not? [**2 points**]
      1. PC1 can still reach PC2 because the speed at which it reaches PC2 is just reduced and half-duplex means data can only go in direction. When I issue a ping to PC2 from PC1, it is a one way send and receive, so it does not matter if it is half or full duplex
2. Now create a following topology in Cisco Packet Tracer
   1. Provide the screenshot of the created topology in Cisco Packet Tracer. Assign IPs to all the hosts. **[5 points]**

A diagram of a computer network

Description automatically generated

* 1. Ping PC-6 from PC-1. What command would you use to look at the mac-table on switch-2? Paste the screenshot showing its output. **[5 points]**

**show mac-address-table**

A computer screen shot of a computer

Description automatically generated

* 1. Interpret the mac-table of switch-3 and briefly explain it. **[5 points]**
     1. What is happening is there only Mac Address listed on switch-3. This MAC is from PC1 when I pinged PC6. So it has PC1s MAC and the associated port is switch-2 because from what switch-3 know, it came from that device.

1. Now disconnect PC-6 from switch-3 and connect it to switch-1. Did you notice any change in the mac-table of switch-2? Yes or No? Why so? Paste the screenshot of the output. **[10 points]**

A computer code with numbers and lines

Description automatically generated with medium confidence

I did notice a change in the mac-table of switch02. It changed because PC6 is no longer connected to switch-3 and the mac-table has lost the mac-address and source. The source is now different given that it is connected to switch 1 and that is why the table is different.

* 1. Now ping PC-6 from PC-4. Check the mac-table once again on switch-2. Did you notice any change in the mac-table of switch-2? Yes or No? Why so? Paste the screenshot of the output. **[10 points]**

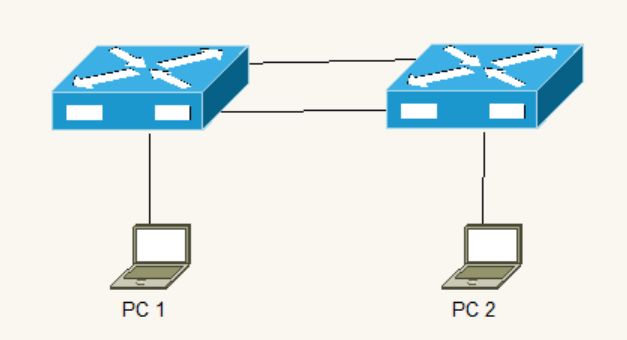
A close-up of a computer address

Description automatically generated

I did notice a change in the mac-table of switch-2 because the MAC address of PC-6 and PC-4 are there with the associated ports of the connected switches the pings came from (Switch 1 and 3).

# Objective 2: Spanning Tree Protocol (STP)

This objective will indicate how STP prevents loops and provides redundancy.



1. Connect PC1 to Switch1 and PC2 to Switch 2
   1. Verify PCs can Ping each other
2. Interconnect the switches
   1. Verify PCs can Ping each other
3. Use the appropriate IOS command to verify which ports on the switch map to the MAC addresses from PC1 and PC2
   1. Explain your findings [**2 points**]

I notice that there is a MAC address for the port connecting to the computer from switch 1 and there is another port from switch 2 that has the MAC address of the other PC.

1. Add an additional link between Switch1 and Switch2
   1. Explain what should happen in this case [**5 points**]

For example, if I were to ping PC2 from PC1, switch 1 would flood the signal out the two links and once received by the other switch, those links would be flooded. This would create an infinite loop of flooding and eventually crash the switches.

* 1. Verify the switches resolved the problem above, indicate how you can determine this in the Cisco switch (*hint: Spanning-tree blocked*) [**5 points**]

“show spanning-tree summary”. I noticed that switch 1 blocked one of the ports that was connected to switch 2. When this happens, it does not allow for infinite looping of signals AKA STP.

1. Issue a continuous ping from PC1 to PC2
   1. Unplug one of the cables interconnecting the switches
   2. Did the pings fail? If so, for how long? If they didn’t fail, why not? [**5 points**]

The ping did fail, for about 30 seconds. The reason why it failed is because I disconnected the connection that was active and sending pings on that wire. Because the secondary wire was blocked by switch 1 due to STP, it had to turn on that port to continue the connection.

Report Questions

1. What is the length of the MAC address? How is it divided? [**2 points**]

The length of the MAC address is 48 bits in hexadecimal. The first 24 bits is dedicated to the vendor, identifying what company it is from, and the last 24 bits is completely unique to the device itself, making every MAC address different.

1. Why are switches faster than routers? [**2 points**]

Switches are faster than routers because they operate lower on the OSI model and deal with hardware addresses sent through frames. On the other hand, routers have to deal with packets which can include more information higher on the OSI model and don’t have to deal with looking through the packet header for information.

1. Explain how ARP works. [**5 points**]

ARP or address resolution protocol “provides a map of IP addresses to MAC addresses” (Data Com – OSI Model, slide 37). When a computer needs a MAC address of an IP on a network, it will send a broadcast that asks what the MAC address of this IP is. It will send it to every device on the network, hence a broadcast. Every device on that network will check if they have the IP address and if they do, will send their MAC address back to the device that requested it.

# Total Score = \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/121