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.

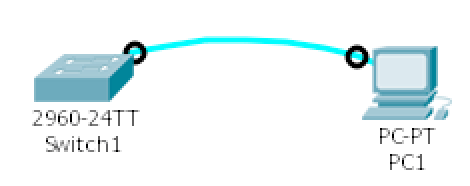
The foundational layer to any network revolves around switching. This lab is intended to be an overview of Cisco IOS, and switching technology - STP.

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

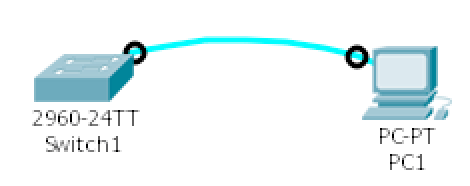
# Objective 1: Connect PC to Cisco Switch in Cisco Packet Tracer This objective will provide instructions for how to connect a PC to a Cisco device for configuration purposes.



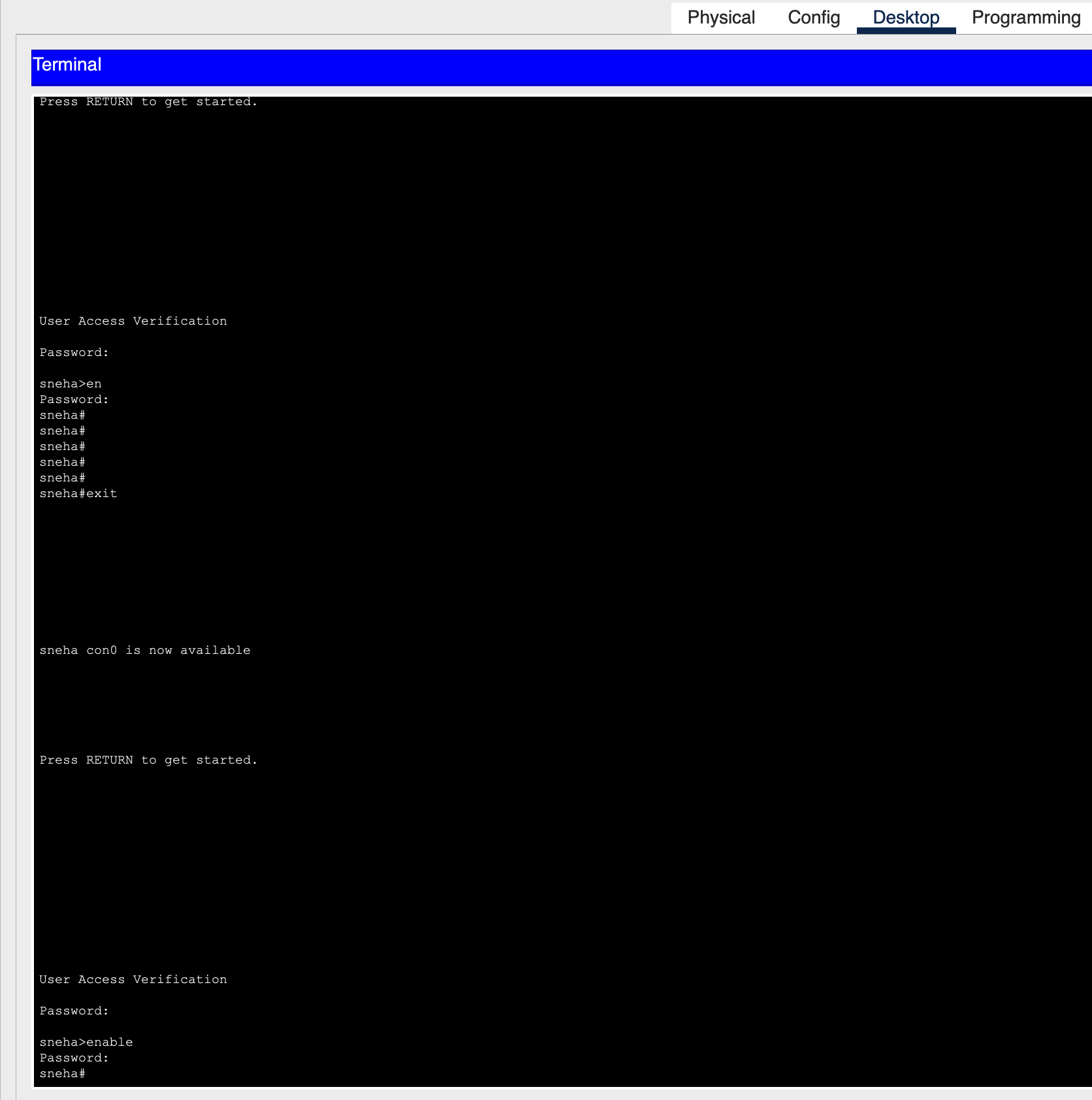
1. Use a Cisco console cable to connect PC1 to the switch “Switch1”

# 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.



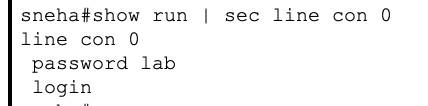
1. Follow the Cisco documentation [Using the CLI](http://www.cisco.com/c/en/us/td/docs/ios/12_2/configfun/configuration/guide/ffun_c/fcf001.html).
2. Configure the hostname on the switch to be “your name.”
3. Create an enable password of “cisco”
4. Create a console password of “lab”.
5. Logout from the 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]**
   1. Do you see the settings you configured?
      1. Hostname

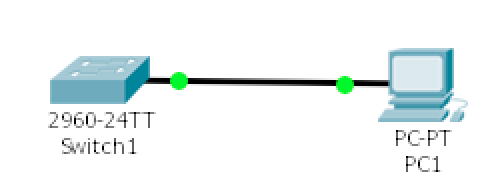


* + 1. Enable password
    2. Console password



# 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.

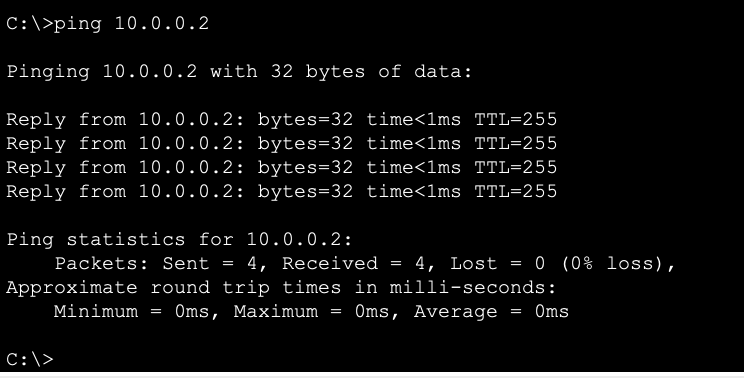


1. Configure and connect the PC and switch according to the diagram. Which cable did you use this time? **[2 points]**

I used a Copper straight-through cable since it is used to connect different types of devices.

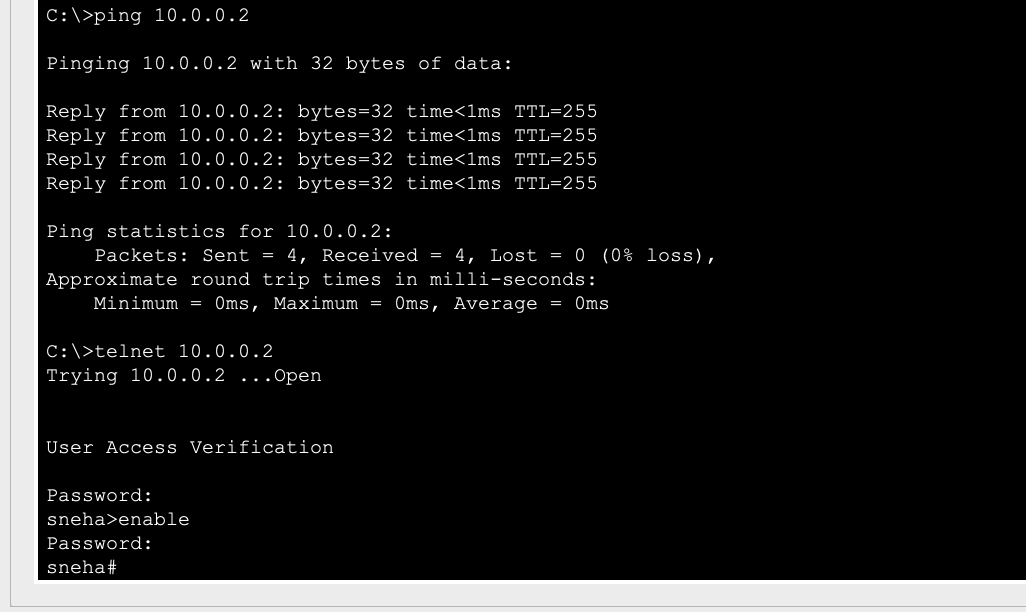
* 1. Make sure the PC has an IP address (10.0.0.1) and subnet mask (255.255.255.0) in the same subnet as the switch (VLAN 1 IP - 10.0.0.2/255.255.255.0)

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



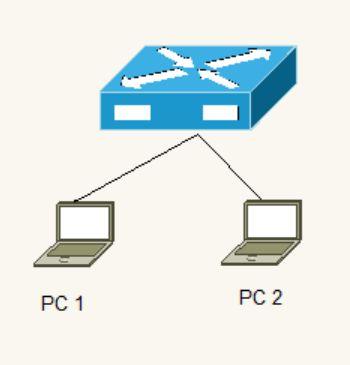
1. Configure Telnet on the switch
   1. Use all the vty lines
   2. Create a password of “telnet” as “cisco”
2. Use Terminal (PC>>Desktop>>Command Prompt) of the PC to Telnet to the switch. Paste the screenshot of telnet output. **[10 points]**

[Screenshot on the next page]



# Part 2

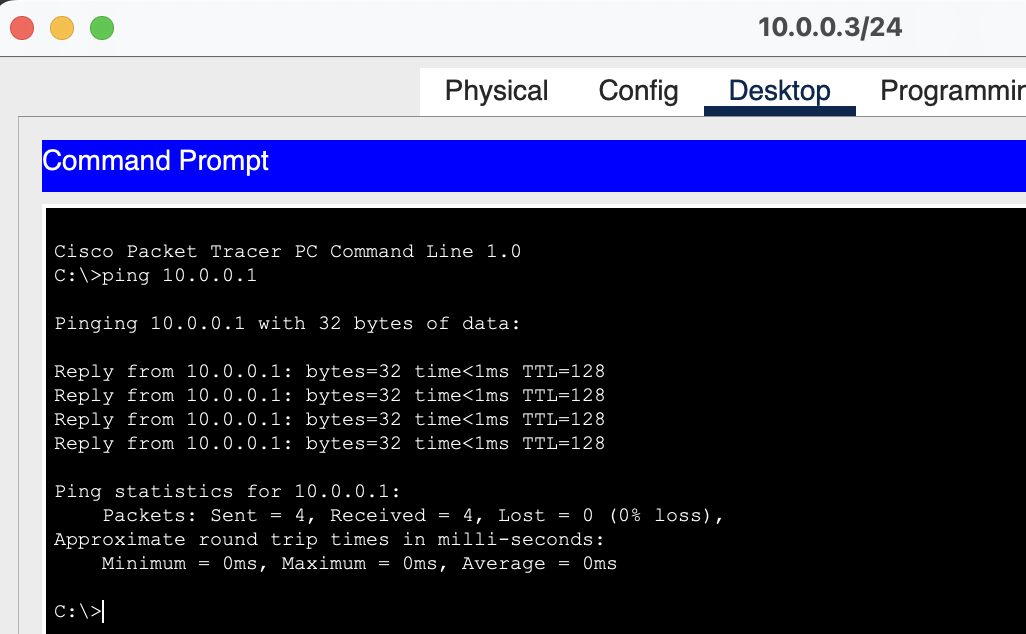
# Objective 1: Cisco IOS Switch Port Configuration This objective will allow you to configure port settings on the industry standard Cisco switches.



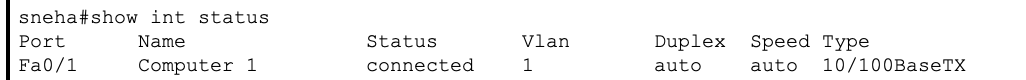
1. Connect PC1 and PC2 to a switch
2. Configure a description on the switchports connected to each PC
   1. The port connected to PC 1 should have a “description Computer 1”
   2. The port connected to PC 2 should have a “description Computer 2”
3. Configure the necessary steps to ping from PC1 to PC2 (*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**]

For both the PCs to be able to ping each other via an L2 switch, they both need to be in the same broadcast domain (*same VLAN and the same subnet*). I first set the IP address for both the PCs such that PC 1 has 10.0.0.1/24 and PC 2 has 10.0.0.3/24 (*Config > Interface > FastEthernet0*).

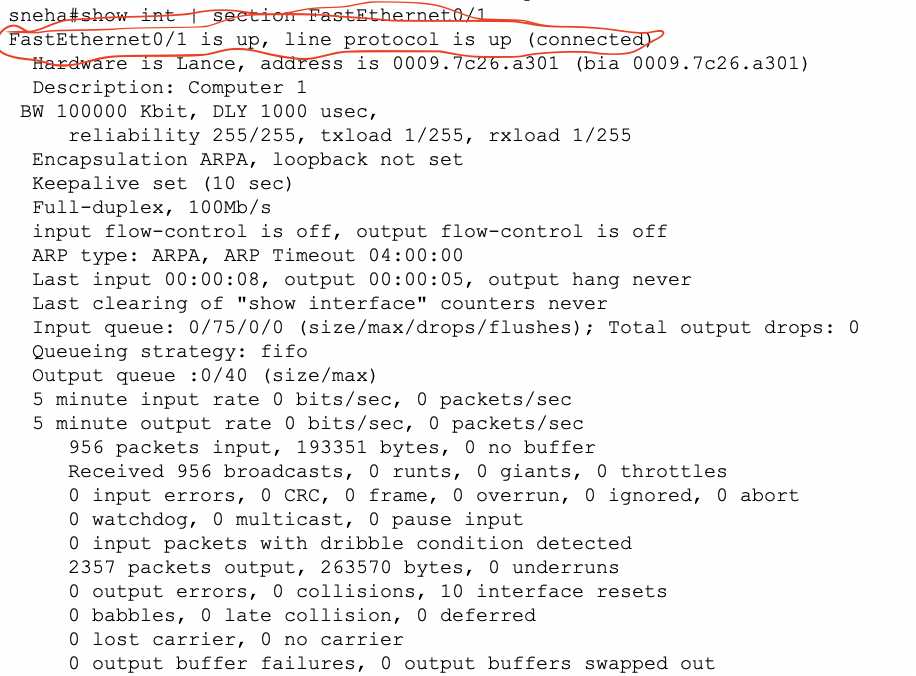
Next, since the switch was already configured with default VLAN as 1, I did not have to make any changes on the switch. Essentially, all ports by default, would be on VLAN 1. To confirm this, I ran the “*show vlan brief*” command on the switch which proved that both Fa0/1 and Fa0/2 were on VLAN1 and voila! The ping went through.



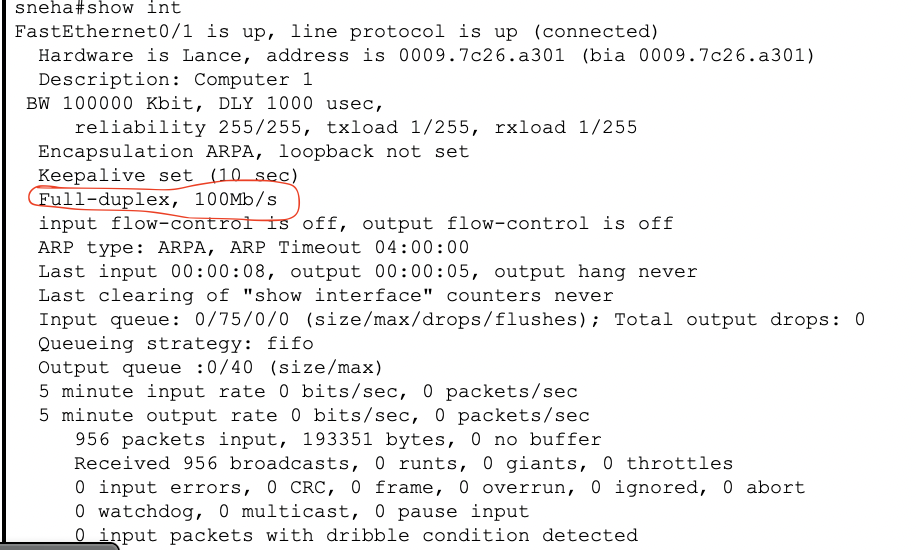
1. Check the status of the switch port connected to PC1
   1. Provide a screenshot of the status of the port [**2 points**]



* + 1. Indicate that the port is up [**2 points**]



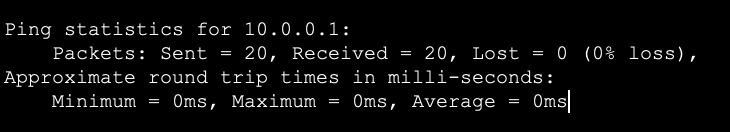
* + 1. Indicate the speed and duplex of the port [**2 points**]



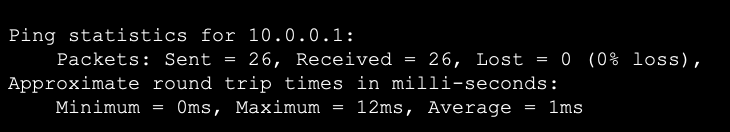
* + 1. Make sure it has the proper description (above)

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**]

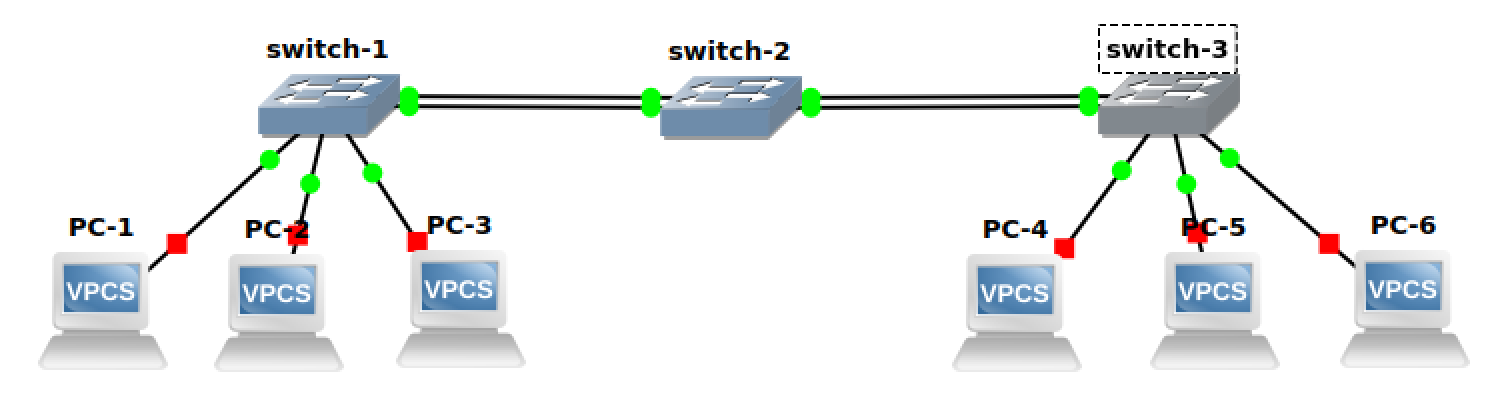
My observations suggest that the two machines can successfully ping each other. However, when the speed and duplex settings are matched (both set to 100 Mbps and full-duplex), the average round-trip time remains consistently at 0 ms.

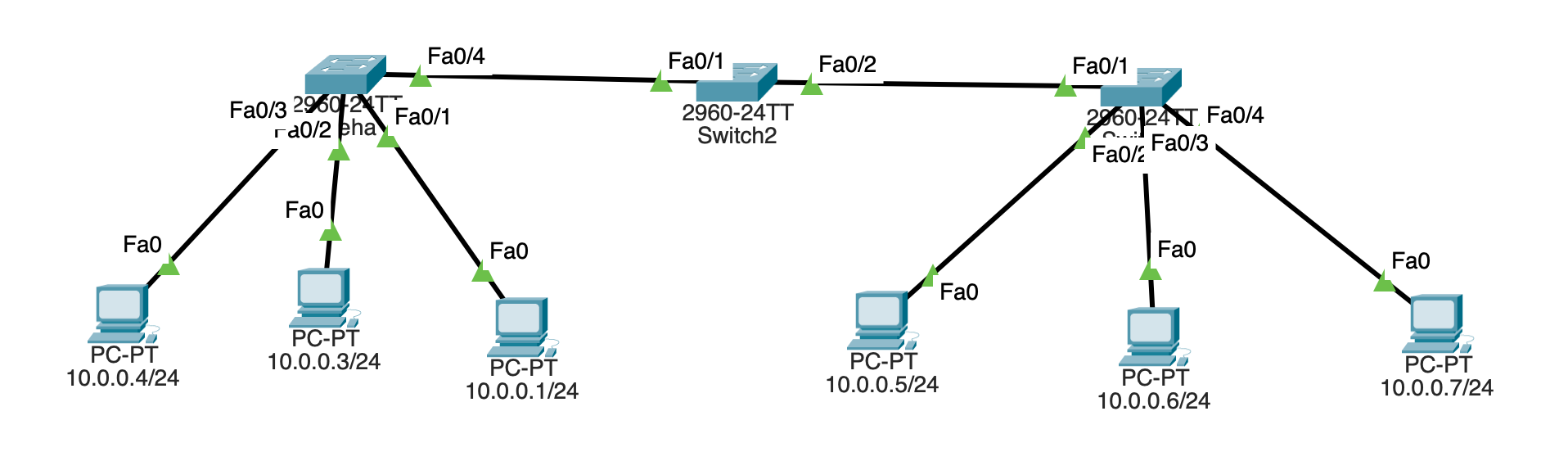


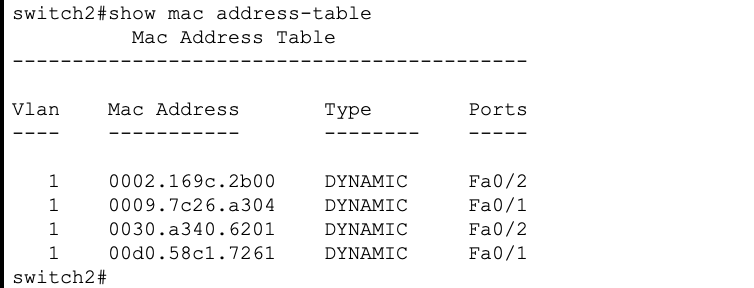
In contrast, when there's a speed and duplex mismatch (e.g., 10 Mbps half-duplex and 100 Mbps full-duplex), the round-trip time is predominantly 0 or 1 ms, though occasional spikes to 12 ms occur.



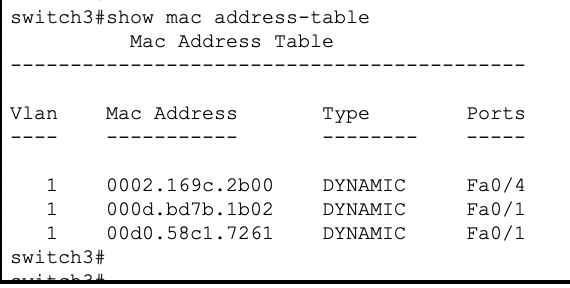
In Half-Duplex mode, only one device can talk at once. If one PC tries to send data while the other is already transmitting, they treat it as a collision, pause, and then retry later. In our test setup, where we're just pinging, these issues may not be obvious. However, in a real production network, one may encounter delays and data loss due to this mismatch. In this example, PC2 is set to a faster speed (100 Mbps) and keeps sending data even when it's busy, while PC1, at a slower speed (10 Mbps), may discard data when overwhelmed.

1. 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]**

****

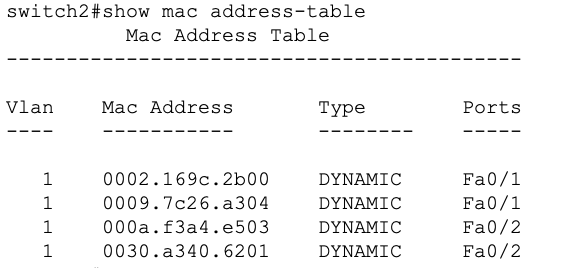
* 1. Ping PC-6 from PC-1. What command would you use to look at the mac-table on switch-2? Paste the screenshot showing its output. **[5 points]**
  2. Interpret the mac-table of switch-3 and briefly explain it. **[5 points]**

This is how the mac address table looks like for switch 3.

****

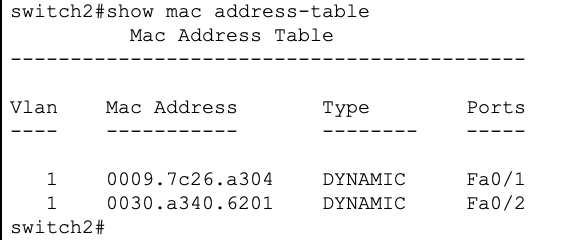
When the PCs are linked to the switch, the switch remains unaware of the MAC addresses associated with any of the devices connected to it. Upon triggering a "ping" command from PC-6 to PC-1, the switch lacks knowledge of both the source and destination MAC addresses. Since this operation works on layer 2 of the OSI model, and the IP addresses fall within the same network (/24), communication is solely dependent on MAC addresses. Initially, the switch only possesses information about the MAC address of the device that initially transmitted a frame to it. As PC6 transmits a frame to the switch, the switch records the source MAC address of that frame, along with the port through which it arrived, in its MAC address table. Consequently, you will observe "Fa0/4" (the interface to which PC6 is connected) in the MAC address table. Subsequently, the switch sends an ARP request by flooding it across all of its connected ports. PC4 and PC5, lacking the relevant IP address for the data frame, reject these packets. The frame then proceeds through Fa0/1, which connects to switch2. Upon receiving a response from switch2, the switch stores the MAC address of Switch2 and the incoming interface in its MAC address table. It's worth noting that the MAC address table initially contained an entry for Fa0/1, which belongs to the source mac address which was broadcasted. ARP request is always a broadcast, whereas ARP response is unicast.

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]**

****

Yes, I do see a change in the mac table. When PC-6 was disconnected from switch3, it caused the Fa0/4 interface to become inactive. When Fa0/4 interface goes offline, switch3 promptly removes the corresponding MAC address table entry associated with that interface. Meanwhile, switch2 maintained four entries: two on Fa0/2 and two on Fa0/1. These entries were established during the ARP (Address Resolution Protocol) process.

To recap, switch2 acquires knowledge of the MAC addresses for both PC-6 and PC-1 when ARP exchanges occur. Specifically, when PC-6 initiates an ARP request, switch3 broadcasts it, switch2 captures the data frame, learns PC-6's MAC address, notes the incoming interface, and records this information in its MAC address table. However, when PC-6 is disconnected and switch3's interface goes offline, the associated MAC entry is deleted. Consequently, switch2's corresponding MAC entry interface also deactivates, resulting in the removal of the communication path.



* 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]**

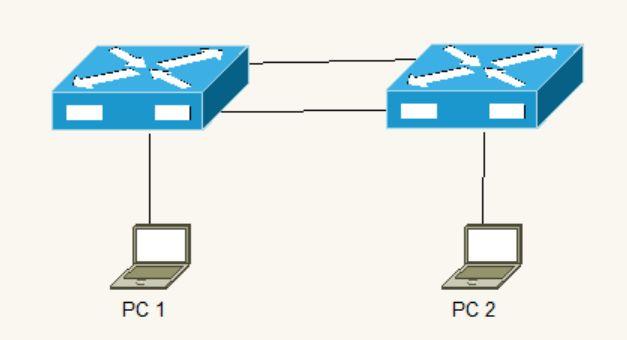
Yes, I see a difference. Now I see 4 entries again on Switch2. 2 of Fa0/1 and 2 of Fa0/2. The physical mac address of Fa0/1 and Fa0/2 and the mac addresses of PC-4 and PC-6.

When ping is initiated from PC-6 which is now connected to switch1 to PC-4 which is connected to switch 3, the following happens:

1. ping initiates from PC-6 to PC-4. PC-6 does not know the mac address of PC-4. Since it is on the same network, it sends an ARP request with MAC address as ff:ff:ff:ff:ff:ff and IP address as 10.0.0.7.
2. switch1, not knowing the path to PC-4, floods to all interfaces connected to it.
3. switch2, on getting the ARP request, checks its mac table to check if the associated IP address is mapped to the mac address. Since there is no entry, it floods its interfaces as well. Meanwhile, switch2 also learns the source mac address (PC-6’s) and the incoming interface (Fa0/1) and stores it in its mac table. Hence we see this entry
4. On receiving the ARP request at switch3, switch3 checks its ARP table to check if it’s aware of the IP address. Since it is not, it floods to its interfaces as well, noting down the incoming interface (Fa0/1) in its mac table.
5. PC-4 on receiving the ARP request, responds to the request by adding its mac address and IP address and sends it to Switch3. Switch3 then learns the mac address of PC-4, stores it in its mac table and sends the response to switch2.
6. switch2, learning this, stores PC-4’s mac address and the incoming interface (Fa0/2) and stores it in its mac table, forwarding the response to Switch1 on fa0/1. Hence we see this entry:
7. Switch1, since now it has learnt the mac address of PC-6, it does not flood its interfaces, instead, send the data frame to PC-4 directly through fa0/5 by checking its own mac table.

# 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

No. The PCs cannot ping each other since they are on different switches and the switches aren’t connected.

1. Interconnect the switches
   1. Verify PCs can Ping each other

Yes. The PCs can now ping.

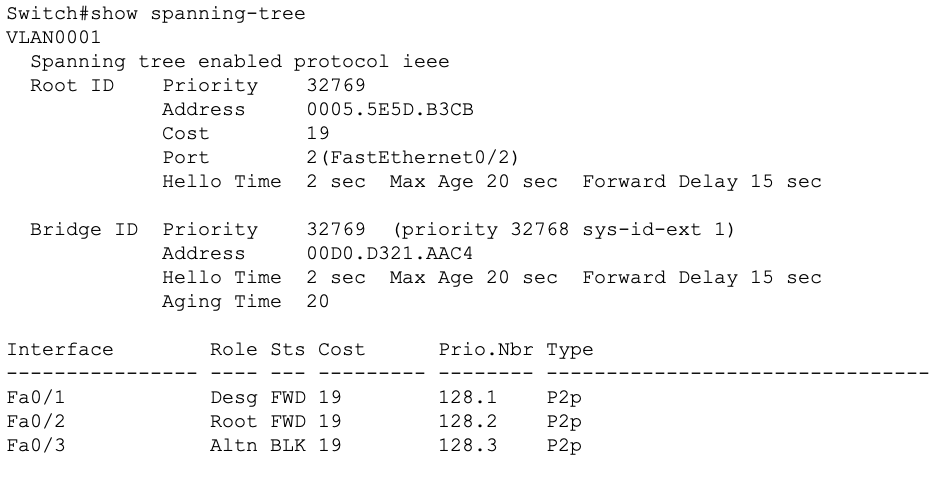
1. Use the appropriate IOS command to verify which ports on the switch map to the MAC addresses from PC1 and PC2
   1. Explain your findings [**2 points**]

The PCs cannot ping each other when they are independently connected to the switches and the switches aren’t connected to each other since the communication is not established. They were able to ping each other once the switches were connected. Using show mac address-table command, we can see the mac addresses connected to each of these switches.

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

Assuming we do not have STP in place, the switches would treat both the links as an active link and may forward the traffic simultaneously through both the links. Without STP to prevent loops for broadcast traffic, such as ARP requests, it can circulate endlessly between the switches. This creates a network loop, leading to a broadcast storm. Broadcast storm would lead to consuming the links’ bandwidth affecting the performance or lead to network downtime or packet losses.

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

The switches prevent this issue through spanning tree protocol (STP). The command to check this is “*show spanning-tree*”.

**Root Bridge**: the root bridge is the central switch in the spanning tree topology. The switch with the lowest Bridge ID becomes the root bridge. In this case, Fa0/2 is the root bridge.

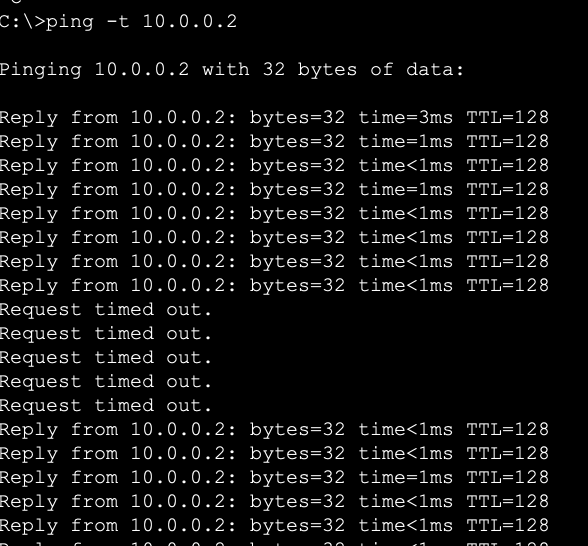
**Designated Ports**: Designated ports are the ports that are in forwarding state and are part of the active path to the root bridge. In this case, Fa0/1 is the designated port.

**Blocked Ports**: Blocked ports are in the blocking state and are not forwarding traffic. These ports are the ones that are preventing network loops. In this case, Fa0/3 is the blocked port. This link is not active.

This output confirms that spanning tree has correctly resolved the problem by blocking one of the links to prevent network loops.

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 pings failed for about 5 seconds or so. It might have taken time to detect the link state, switching the root bridge and making the other link active However, after 10 seconds the pings resumed.



Report Questions

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

MAC addresses are 48 bits long. The first 24 bits (3 bytes) of the MAC address represent the OUI, which is assigned by IEEE to manufacturers or organizations. The remaining 24 bits (3 bytes) of the MAC address is assigned by the manufacturer or organization and is meant to be unique to each network interface they produce.

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

Switches are faster than routers because switches operate at Layer 2 and make forwarding decisions based on MAC addresses, which are hardware addresses, while routers operate at Layer 3 and use IP addresses for routing, which involves more complex routing decisions. Further, switches perform hardware-based forwarding within a local network segment, allowing them to pass data at wire speed without the need for complex routing calculations. Routers, on the other hand, involve software-based processing and routing logic, which can introduce some latency.

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

**1.** When a device wants to communicate with another device on the same network, it knows the target device's IP address but requires the target's MAC address to send data at the data link layer (Layer 2 of OSI model).

**2.** The source machine checks its ARP table. If the mapping is not found in the ARP cache, the device initiates an ARP request.

**3.** The ARP request is sent as a broadcast frame to all devices on the local network known as flooding. The request includes: Sender's MAC and IP address, Target IP address and Target MAC address is populated as ff:ff:ff:ff:ff:ff

4. All devices on the network receive the ARP request. The device with the matching IP address in the request responds with an ARP response.

5. The device with the matching IP address generates an ARP reply. The ARP reply includes: Sender's MAC and IP address and Target MAC address.

6. The requesting device updates its ARP table with the newly discovered mapping.

7. With the MAC address resolved, the requesting device can encapsulate data frames with the destination MAC address and transmit data over the local network without broadcasting. ARP ensures devices on the same local network can communicate by resolving IP addresses to MAC addresses, enabling the proper forwarding of data frames at the data link layer.

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