**Course Code - Course Name:** - COMP4039 – Network Foundations

**Program:** T433 - Cybersecurity

**Section:** A

**Term:** - Winter 2024

**Group Number:** 06

**Student Names - ID:**

* Prabhjot Singh Sains – 101495218
* Rahul Patel - 101378458
* Jai Deep Rawat - 101503760
* M. Salmaan Mustafa Shah – 10151007

**Lab Report by -** Prabhjot Singh Sains

**Topology**

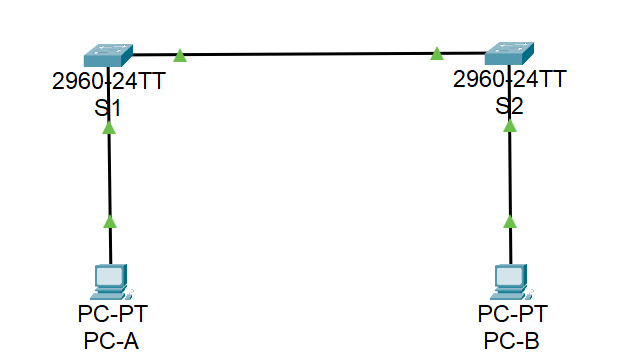


Fig 1. – Topology

**Addressing Table**

|  |  |  |  |
| --- | --- | --- | --- |
| **Device** | **Interface** | **IP Address** | **Subnet Mask** |
| S1 | VLAN 1 | 192.168.1.1 | 255.255.255.0 |
| S2 | VLAN 1 | 192.168.1.2 | 255.255.255.0 |
| PC-A | NIC | 192.168.1.10 | 255.255.255.0 |
| PC-B | NIC | 192.168.1.11 | 255.255.255.0 |

**Objectives**

* **Part 1:** Build and Configure the Network
* **Part 2:** Examine the Switch MAC Address Table

**Background / Scenario**

In this lab, we build a simple network with two hosts and switches. We also configured basic settings including hostname, local passwords, and login banner. Used show commands to display the running configuration, IOS version, and interface status. Used the copy command to save device configurations. We applied IP addressing for this lab to the PCs and switches to enable device communication. Use the ping utility to verify connectivity. In Part 2, we pinged various devices and observed how the two switches built their MAC address tables.

**Instructions**

**Build and Configure the Network**

1. Set Up the Network Topology.
2. Configure PC Hosts: Configure and verify static IP address information on the PCs according to the Addressing Table.

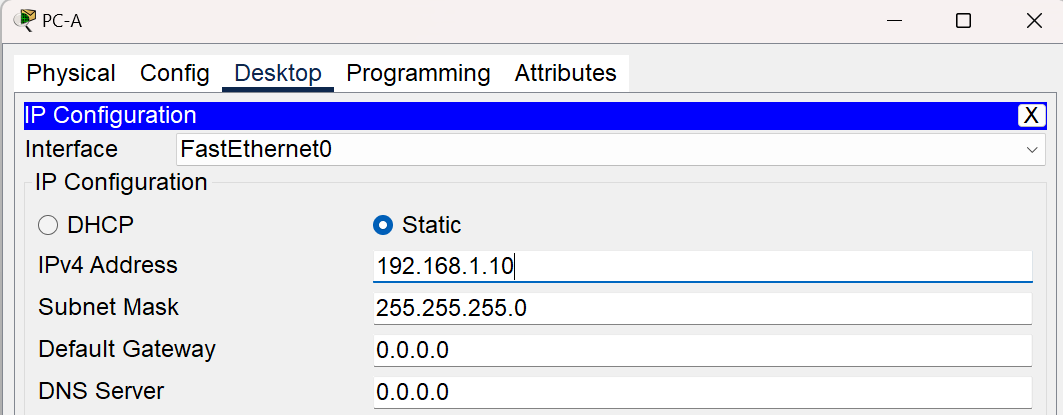


Fig 2. – PC-A

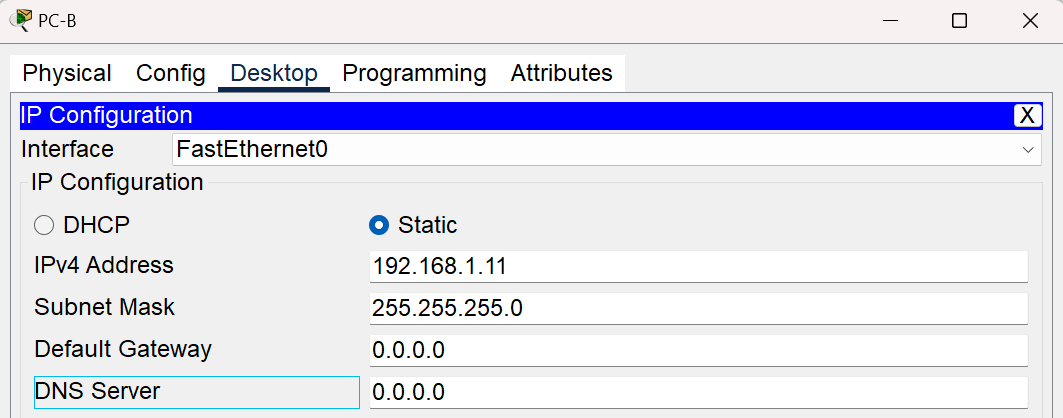


Fig 2. – PC-B

1. Configure and Verify Basic Switch Settings for S1 and S2.
   * Give the switch a name according to the Addressing Table.
   * Prevent unwanted DNS lookups.
   * Enter local passwords. Use class as the privileged EXEC password and Cisco as the password for console access.
   * Configure and enable the SVI on both switches according to the Addressing Table.
   * Enter a login MOTD banner to warn about unauthorized access.
   * Save the configuration.

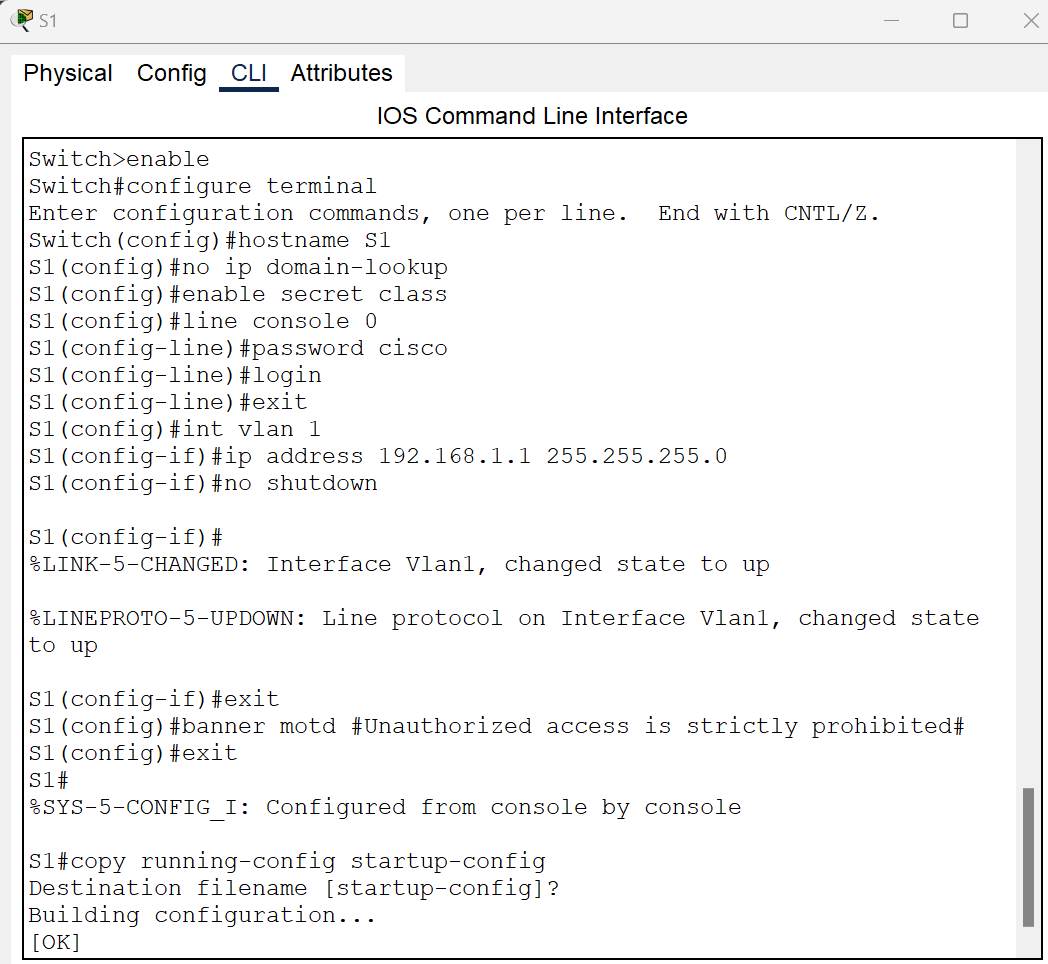


Fig 3. – S1

**Question 1:** Use the show command with appropriate arguments to display the following.

**Answer:**

* Display the current configuration.

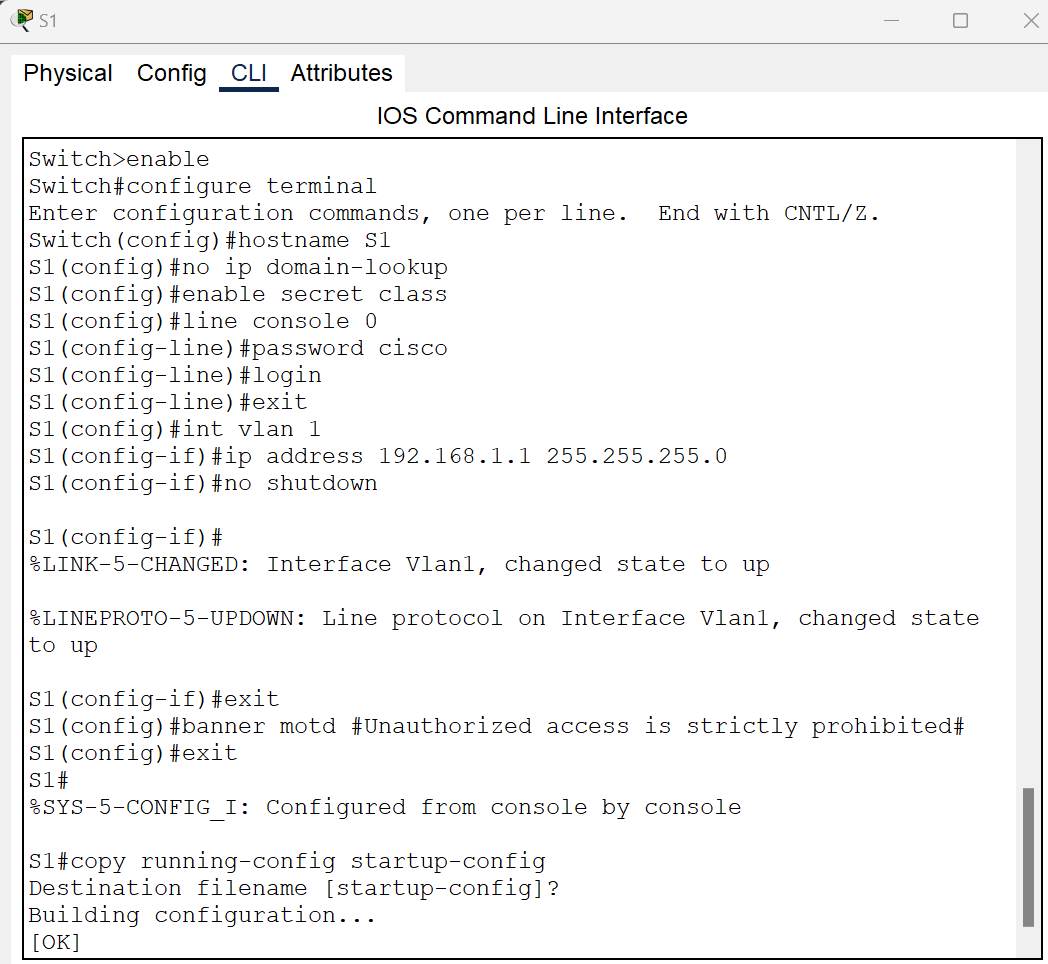


Fig 4. – S1

* Display the IOS version and other useful switch information.

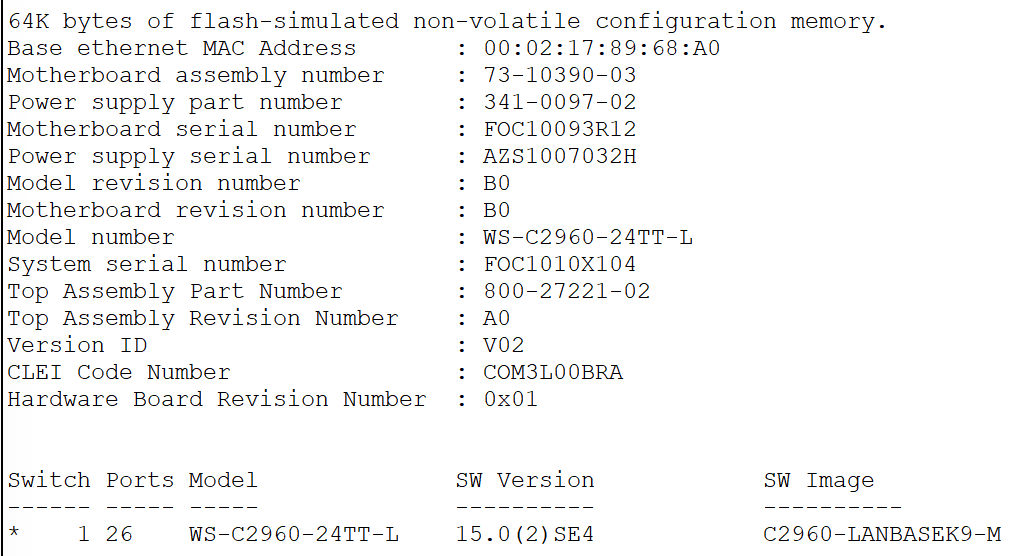


Fig 5. – S1

* Display the status of the connected interfaces on the switch.

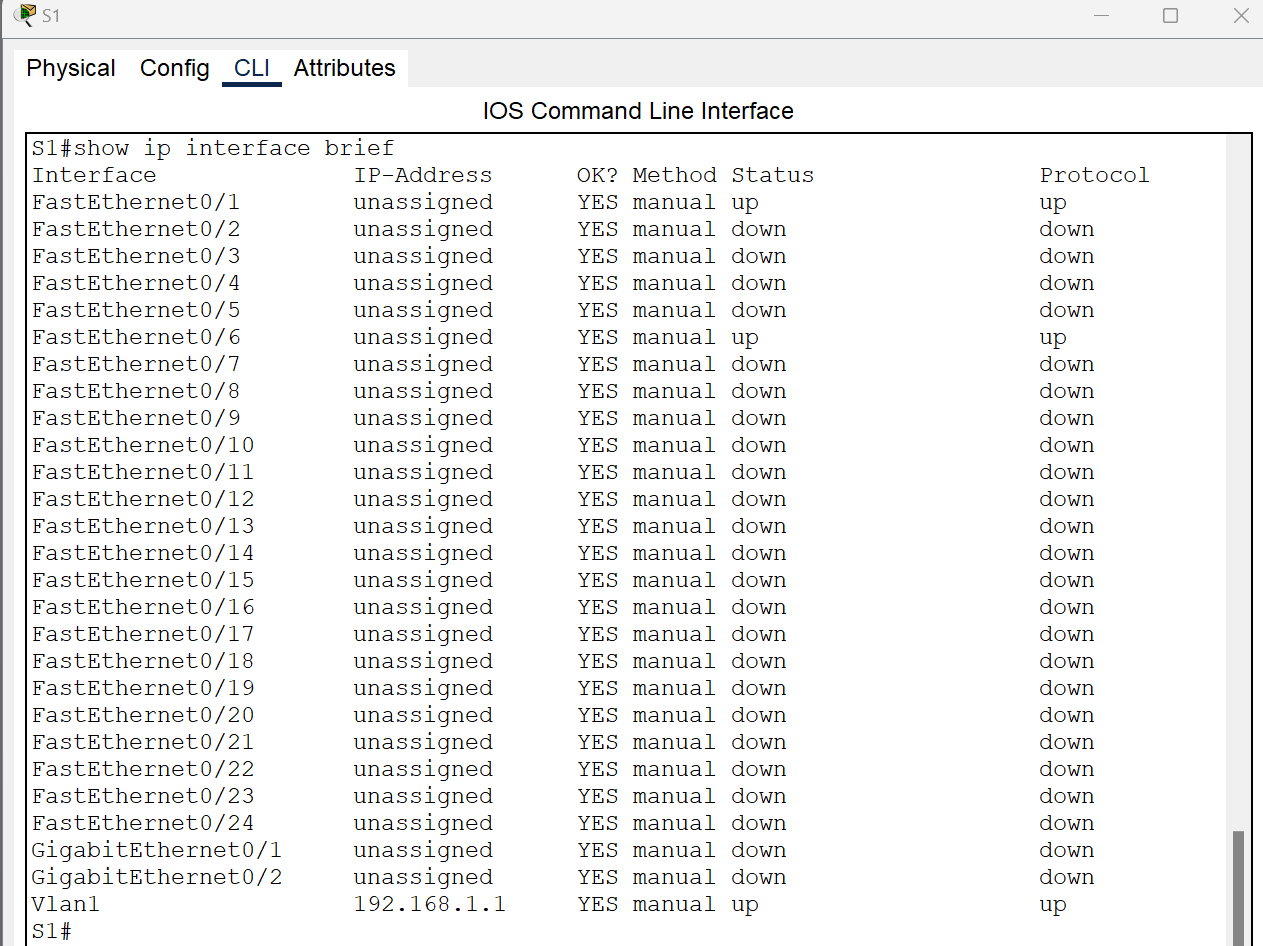


Fig 6. – S1

* Configure switch S2.

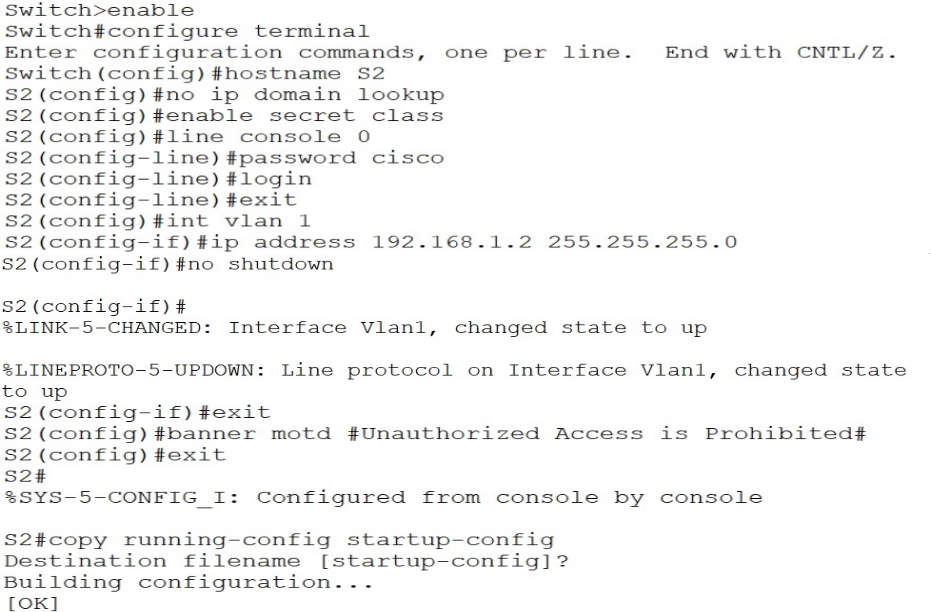


Fig 7. – S2

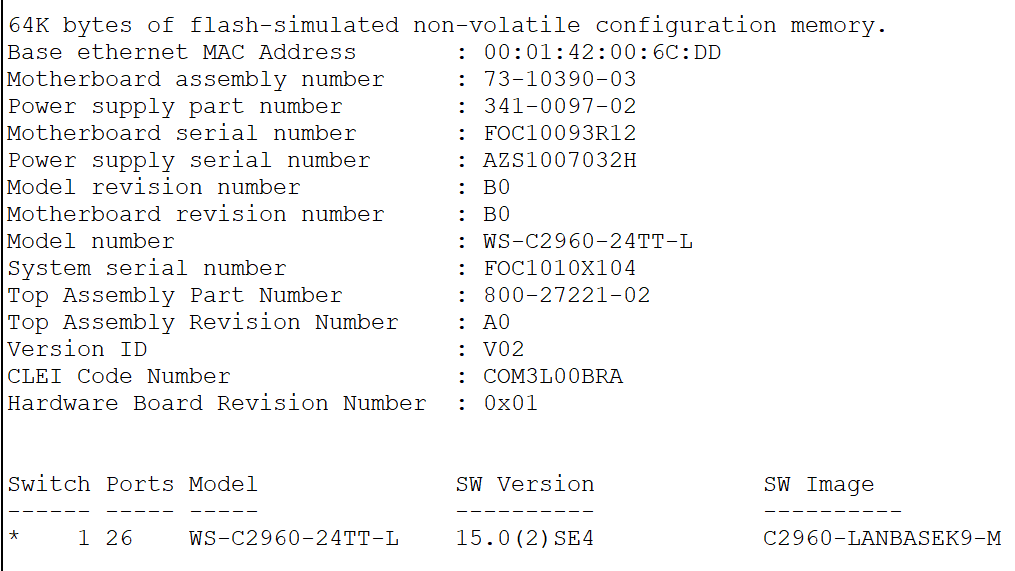


Fig 8. – S2

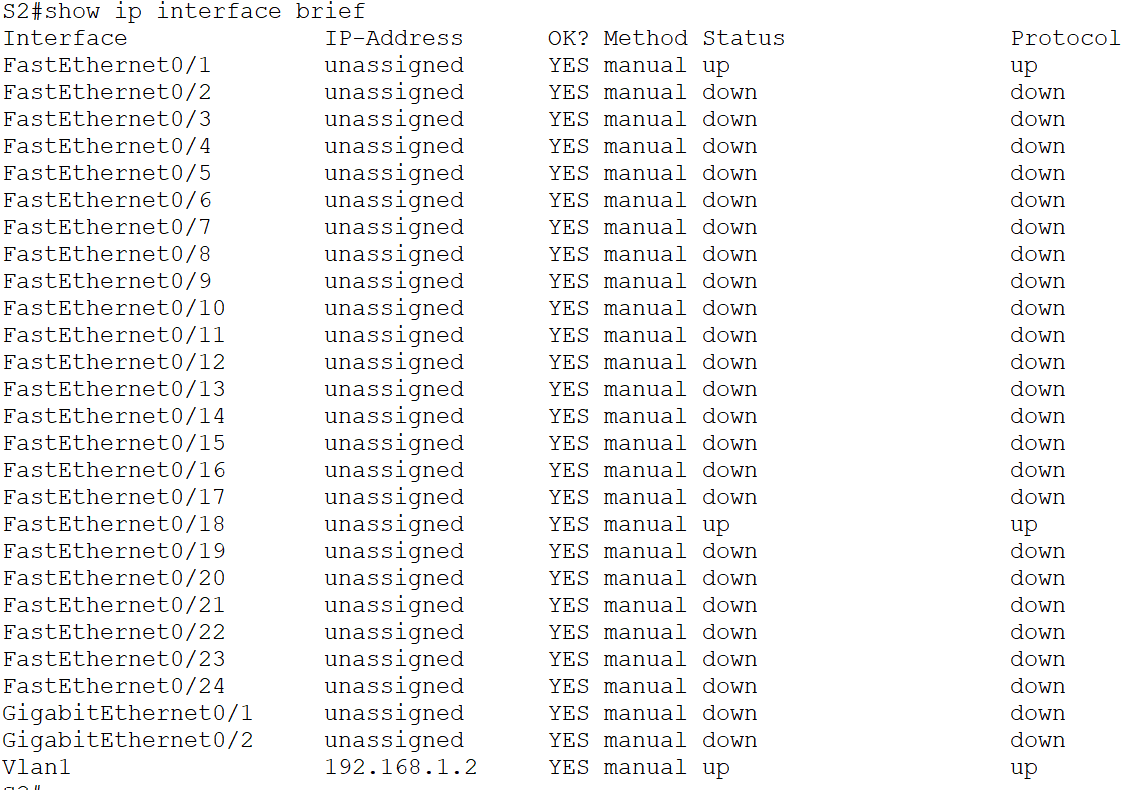


Fig 9. – S2

* Record the interface status for the following interfaces.

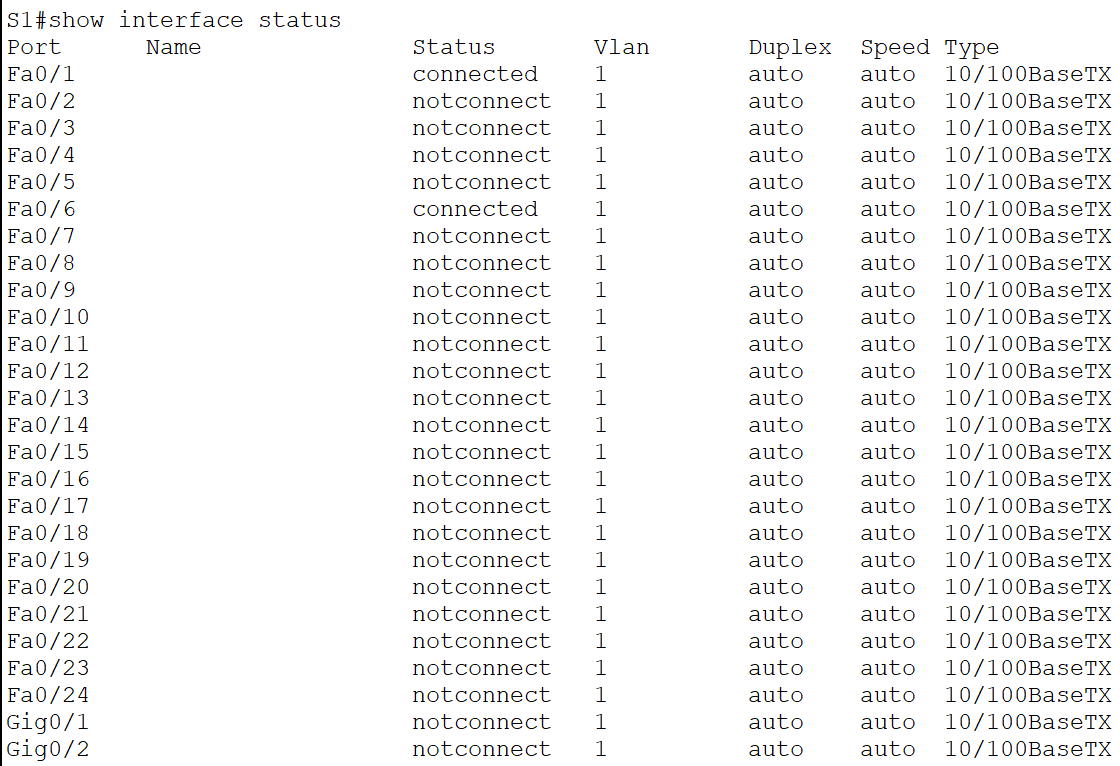


Fig 10. – S1

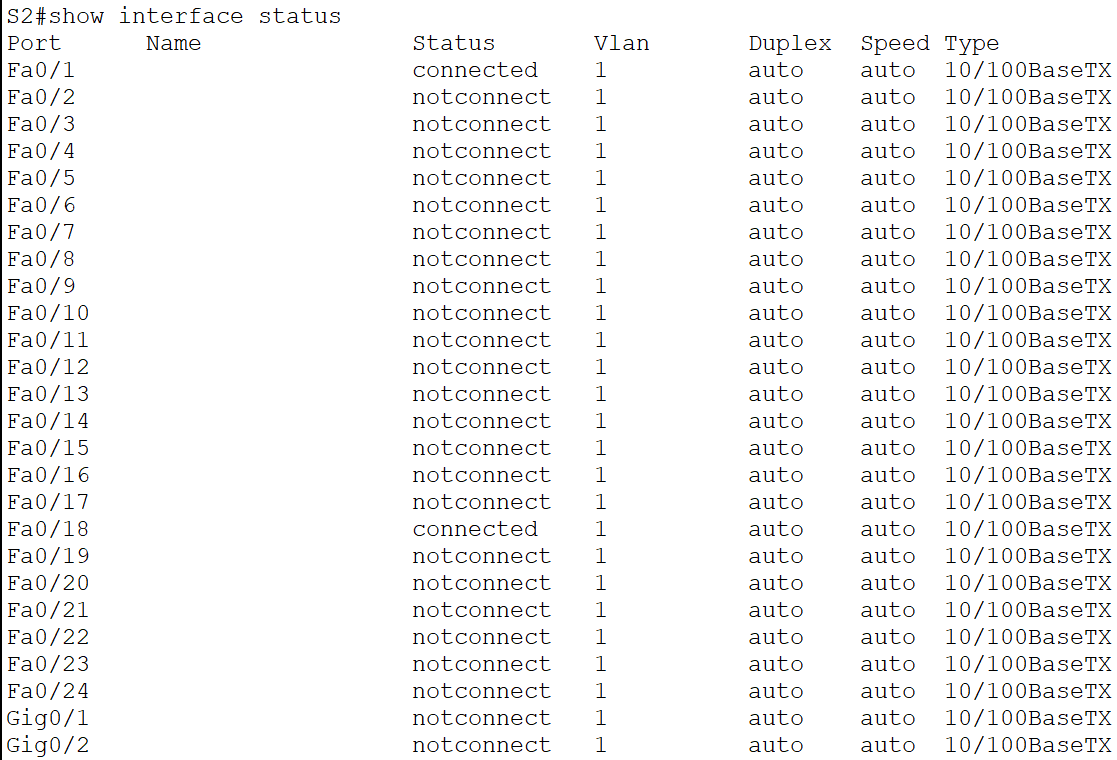


Fig 11. – S2

1. Test network connectivity.

**Question 2:** Show the ping results. From a PC, ping S1 and S2. The pings should be successful.

**Answer:**

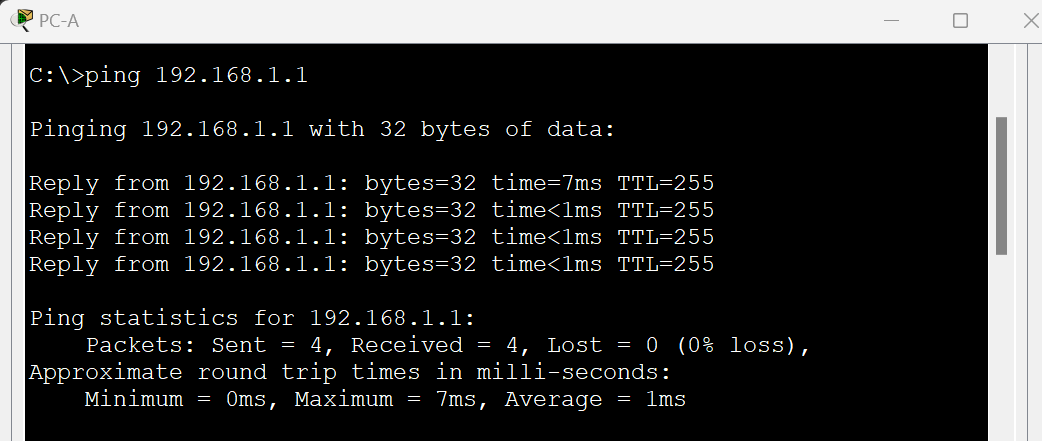


Fig 12. – PC-A

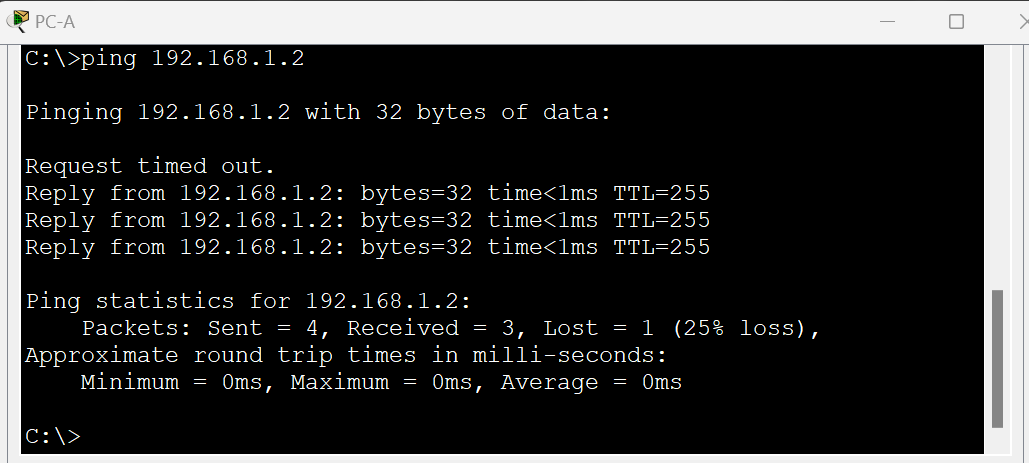


Fig 13. – PC-A

* + From a switch, ping PC-A and PC-B. The pings should be successful.

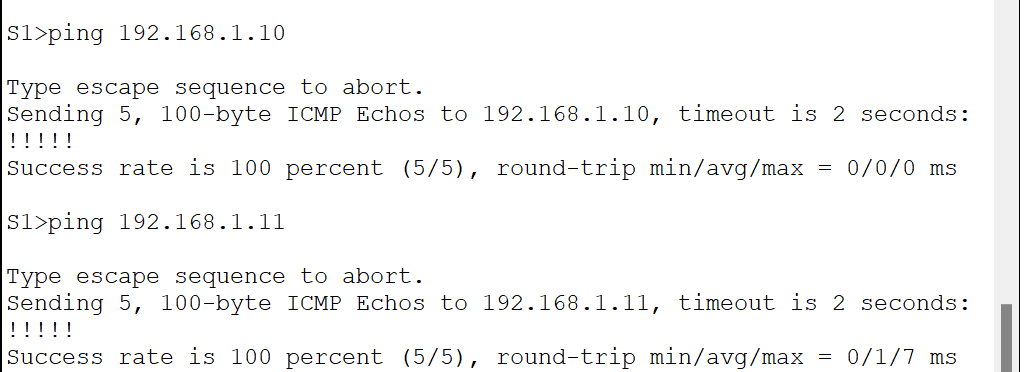


Fig 14. – S1

1. Record network device MAC addresses
   * A switch learns MAC addresses and builds the MAC address table, as network devices initiate communication on the network. In this step, we will examine the switch MAC address table.
   * On PC-A and PC-B, open a command prompt and type ipconfig /all

**Question 3:** What are the Ethernet adapter physical addresses for PC-A and PC-B?

**Answer:**

* **PC-A:** 0002.162E.9552
* **PC-B:** 00D0.586E.8362

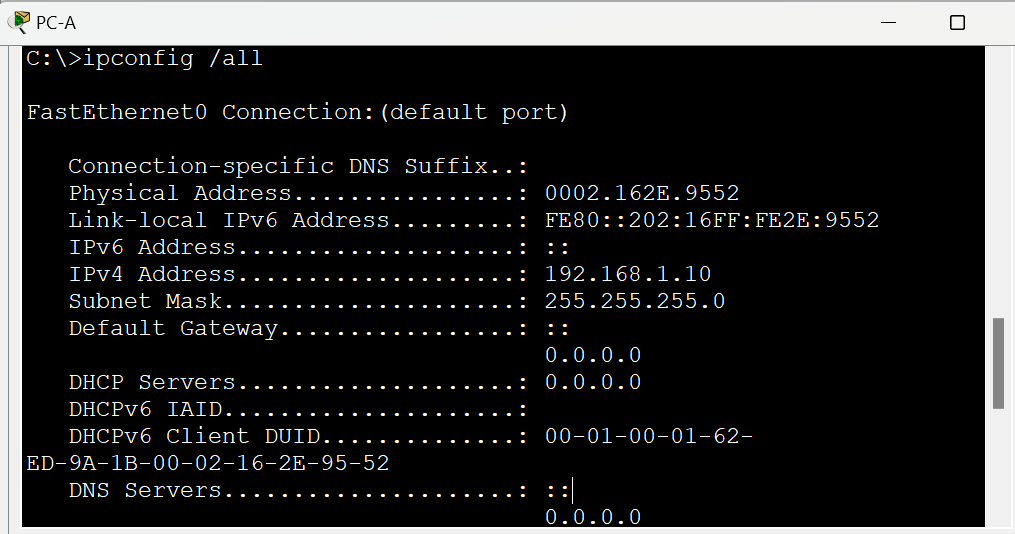


Fig 15. – PC-A

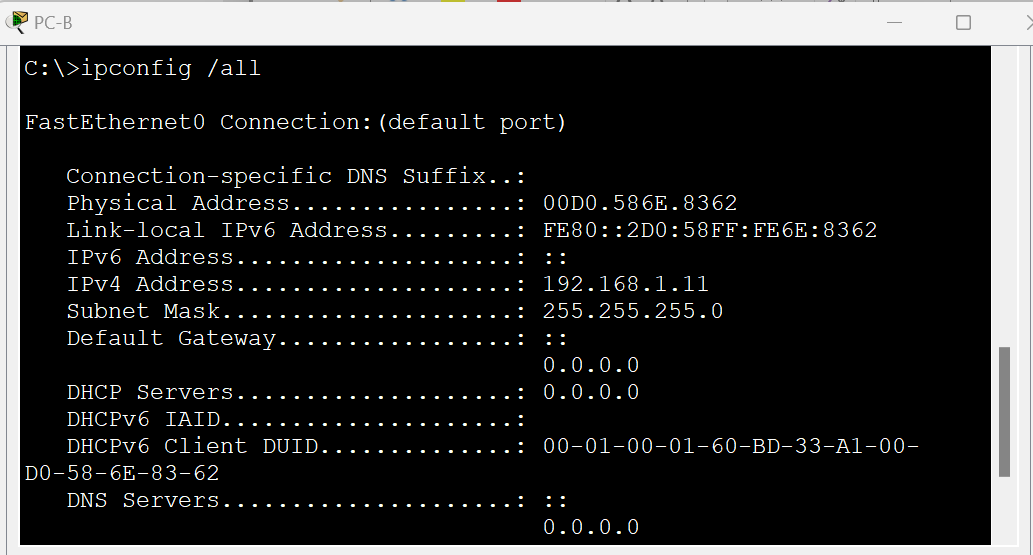


Fig 16. – PC-B

**Question 4:** Type the show interface F0/1 command on each switch and answer the following questions. what are the hardware addresses of interface Fast Ethernet 0/1 for S1 and S2?

**Answer:**

* **S1:** 0002.1626.4c01
* **S2:** 00e0.b011.d101

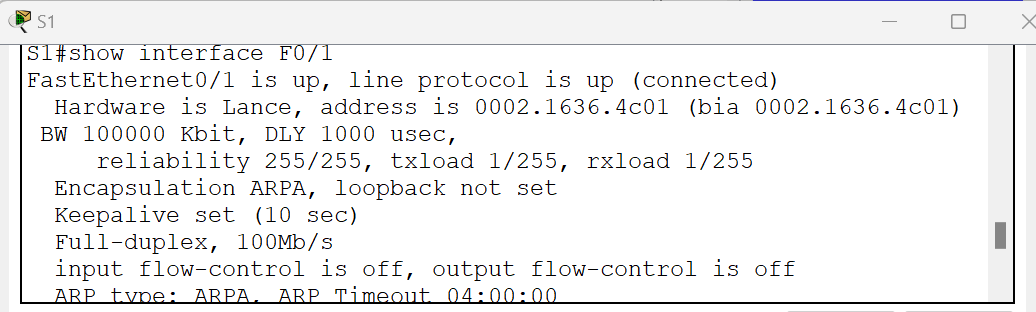


Fig 17. – S1

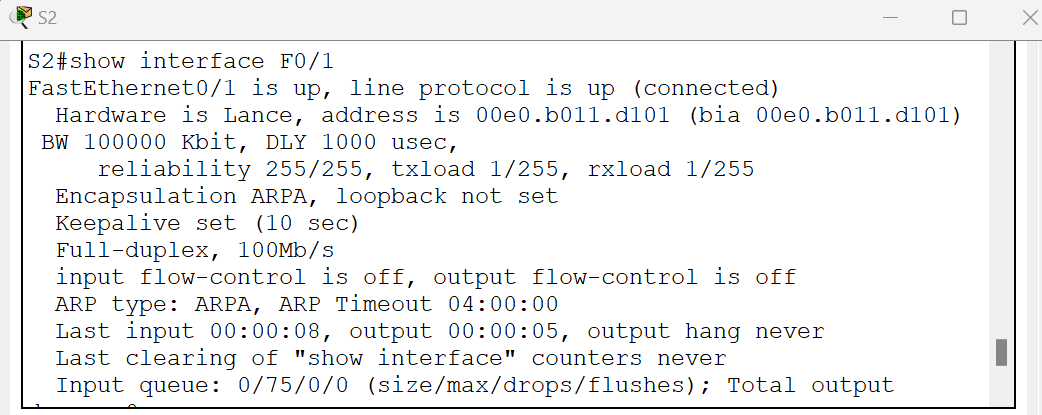


Fig 18. – S2

1. Display the switch MAC address table.

* Console into switch S2 and view the MAC address table, both before and after running network communication tests with ping. In privileged EXEC mode, type the show mac address-table command and press Enter. Even though there has been no network communication initiated across the network (i.e., no use of ping), the switch may have learned MAC addresses from its connection to the PC and the other switch.

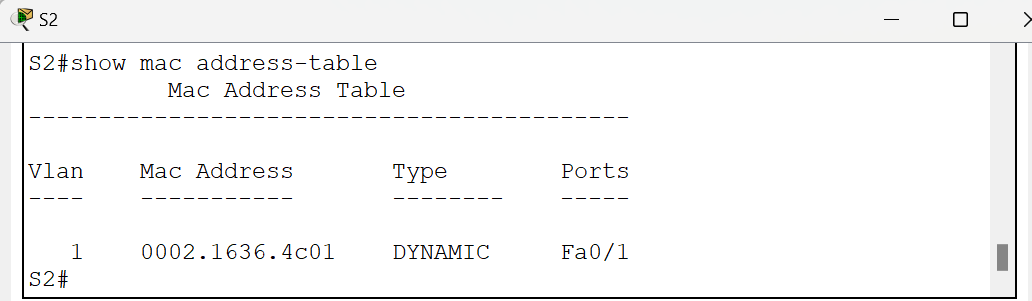


Fig 19. – S2 MAC Address table Before running network communication tests with ping

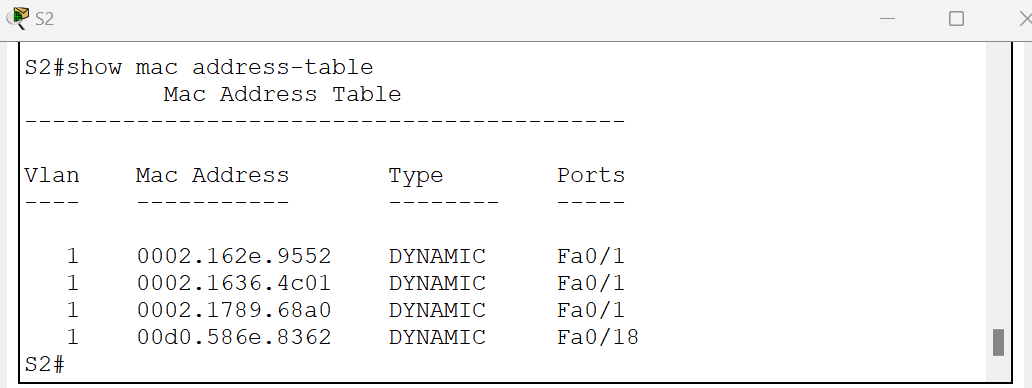


Fig 20. – S2 MAC Address table After running network communication tests with ping

**Question 5:** Are there any MAC addresses recorded in the MAC address table?

**Answer:** Yes (See the Fig 19 and Fig 20)

**Question 6:** What MAC addresses are recorded in the table? To which switch ports are they mapped and to which devices do they belong? Ignore MAC addresses that are mapped to the CPU.

If you had not previously recorded the MAC addresses of network devices in Step 1, how could we tell which devices the MAC addresses belong to, using only the output from the show mac address-table command? Does it work in all scenarios?

**Answer:**

See Figures 19 and 20 for the MAC Address table before and after running network communication tests with ping.

* 0002.1636.4c01 is the MAC Address for S2 (from figures 19 and 20) and for port Fa0/1
* 0002.162e.9552 is the MAC Address for PC-A (from Figure 20) and for port Fa0/1
* 00d0.586e.8362 is the MAC Address for PC-B (from Figure 20) and for port Fa0/18

**Step 3:** Clear the S2 MAC address table and display the MAC address table again.

* In privileged EXEC mode, type the clear Mac address-table dynamic command and press Enter.
* Quickly type the show mac address-table command again.

**Question 7**: Does the MAC address table have any addresses in it for VLAN 1? Are there other MAC addresses listed?

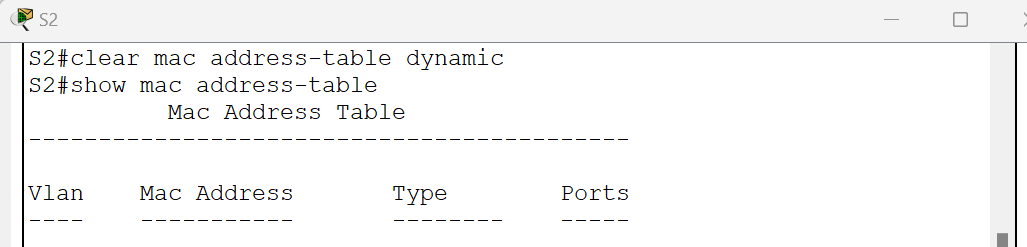


Fig 21. Clear Mac address-table dynamic command

Wait 10 seconds, type the show mac address-table command, and press Enter. Are there new addresses in the MAC address table?

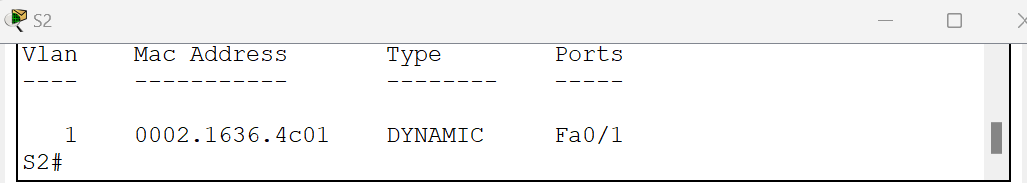


Fig 21. Mac address-table dynamic after waiting 10 seconds

**Step 4:** From PC-B, ping the devices on the network and observe the switch MAC address table.

**Question 8:** From PC-B, open a command prompt and type ARP, Not including multicast or broadcast addresses, how many devices' IP-to-MAC address pairs have been learned by ARP?

**Answer:** Three devices' IP-to-MAC address pairs have been learned by ARP.

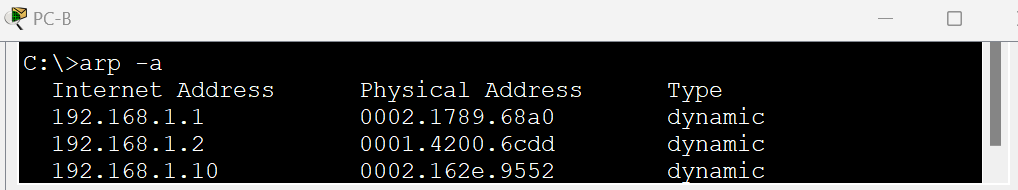


Fig 22

**Question 9:** From the PC-B command prompt, ping PC-A, S1, and S2. Did all devices have successful replies? If not, check your cabling and IP configurations.

**Answer:** Yes, ping PC-A, S1, and S2 was successful.

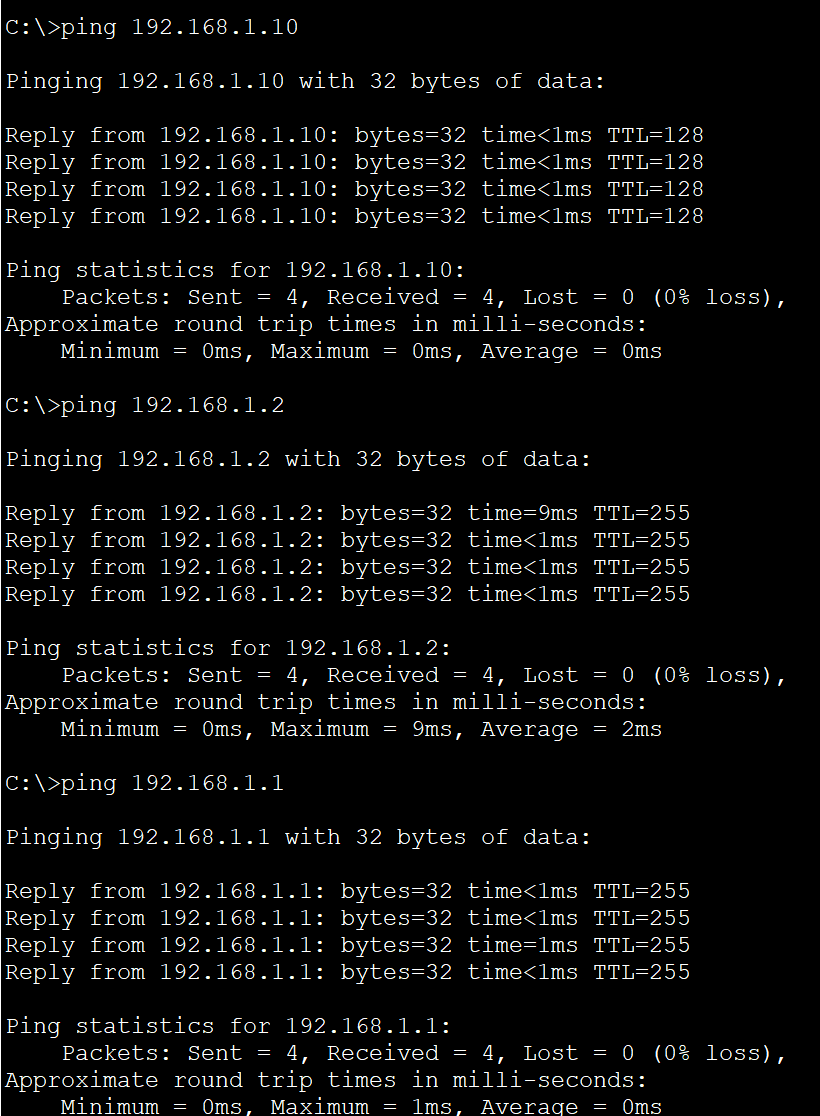


Fig 23

**Question 10:** From a console connection to S2, enter the show mac address-table command. Has the switch added additional MAC addresses to the MAC address table? If so, which addresses and devices?

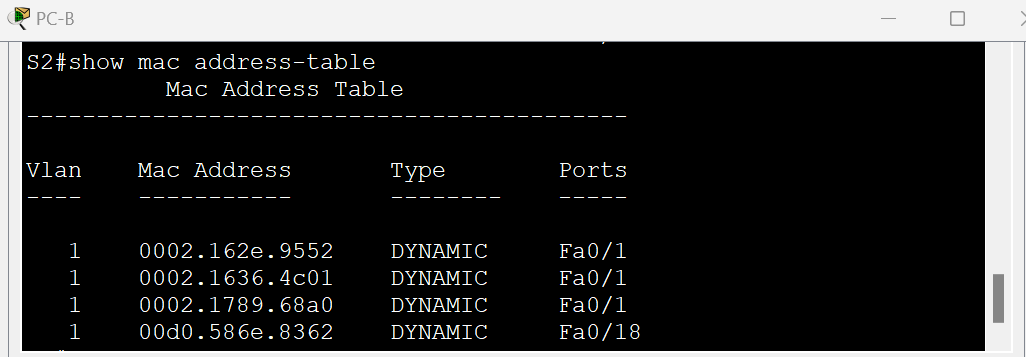


Fig 24

The switch added the following additional MAC addresses to the MAC address table:

* 0002.162.e.9552 is the MAC Address for PC-A for port F0/1
* 0002.1789.68a0 is the MAC Address for S1for port F0/1

**Question 11:** From PC-B, open a command prompt and retype ARP -a. Does the PC-B ARP cache have additional entries for all network devices that were sent pings?

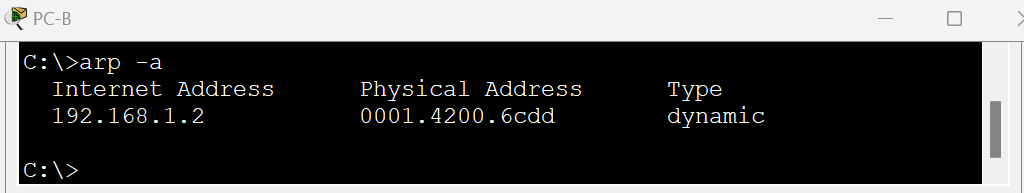


Fig 25

**Reflection Question**:

1. Why some Fast Ethernet ports on the switches are up and others are down?

* Configuration
* Link Speed/Duplex Mismatch
* Physical Connection

1. What could prevent a ping from being sent between the PCs?
   * Incorrect IP Addresses
   * Firewall Settings
   * Network Address Translation
   * Physical Connectivity Issues
   * Network Configuration Issues
   * Everything was right, forgot to run the no shutdown command and turned off the switch (occurred with us)
2. On Ethernet networks, data is delivered to devices by their MAC addresses. For this to happen, switches and PCs dynamically build ARP caches and MAC address tables. With only a few computers on the network, this process seems fairly easy. What might be some of the challenges on larger networks?
   * Increased Traffic and Complexity
   * Scalability
   * Security Concerns
   * ARP Cache Exhaustion
   * Broadcast Domain Size