# LAB 1:Packet Tracer - Who Hears the Broadcast?

## Objectives

**Part 1: Observe Broadcast Traffic in a VLAN Implementation**

**Part 2: Complete Review Questions**

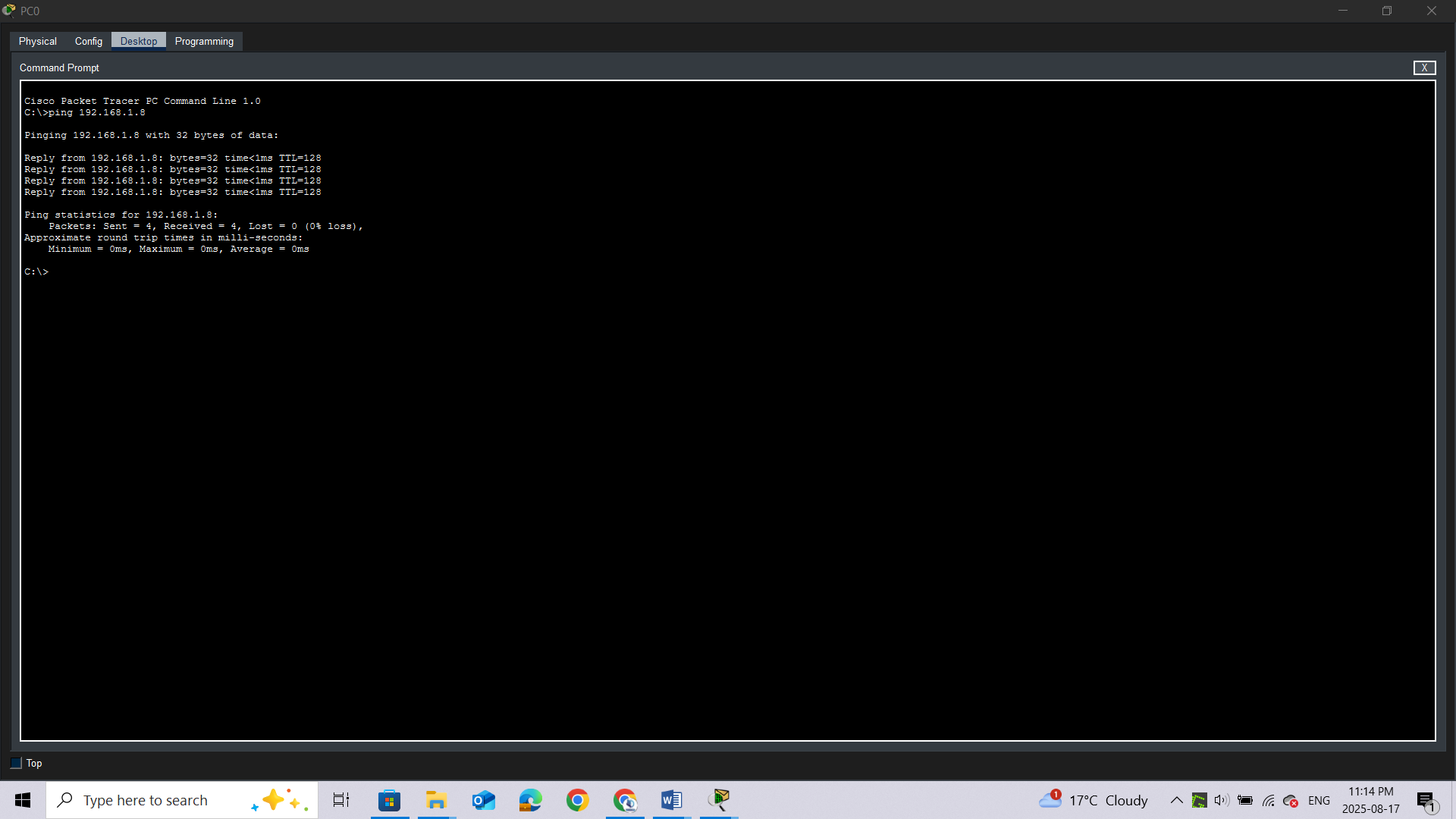
## Scenario

In this activity, a 24-port Catalyst 2960 switch is fully populated. All ports are in use. You will observe broadcast traffic in a VLAN implementation and answer some reflection questions.

## Instructions

### Step 1: Use ping to generate traffic.

1. Click **PC0**and click the **Desktop** tab> **Command Prompt**.
2. Enter the **ping 192.168.1.8** command. The ping should succeed.



Unlike a LAN, a VLAN is a broadcast domain created by switches. Using Packet Tracer **Simulation** mode, ping the end devices within their own VLAN. Based on your observation, answer the questions in Step 2.

### Step 2: Generate and examine broadcast traffic in a VLAN implementation.

1. Switch to **Simulation** mode.

b.     Click **Edit Filters** in the Simulation Panel. Uncheck the **Show All/None** checkbox. Check the **ICMP** checkbox.

c.     Click the **Add Complex PDU** tool, this is the open envelope icon on the right toolbar.

d.     Float the mouse cursor over the topology and the pointer changes to an envelope with a plus (+) sign.

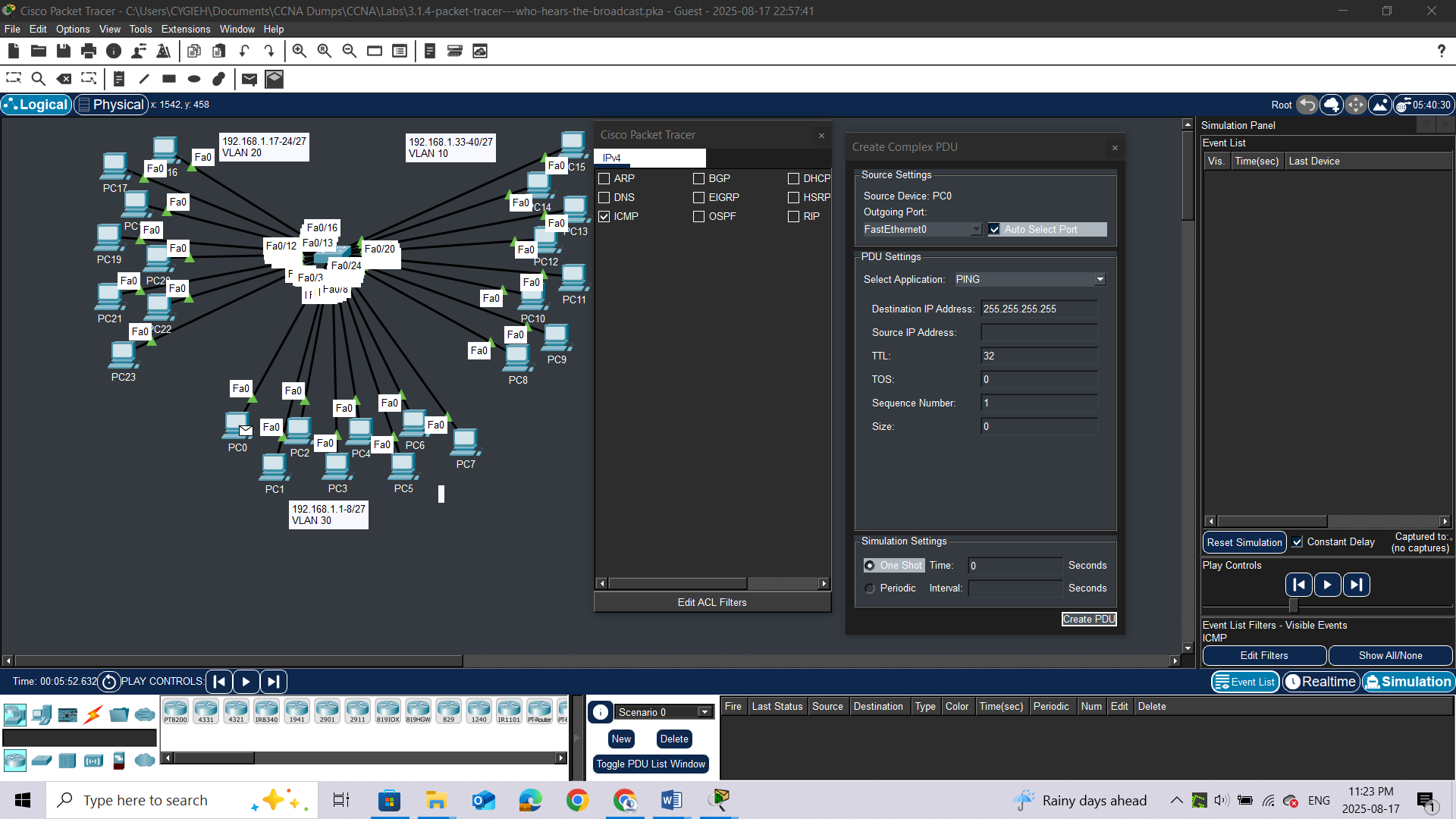
e.     Click **PC0** to serve as the source for this test message and the **Create Complex PDU**dialog window opens. Enter the following values:

o    Destination IP Address: 255.255.255.255 (broadcast address)

o    Sequence Number: 1

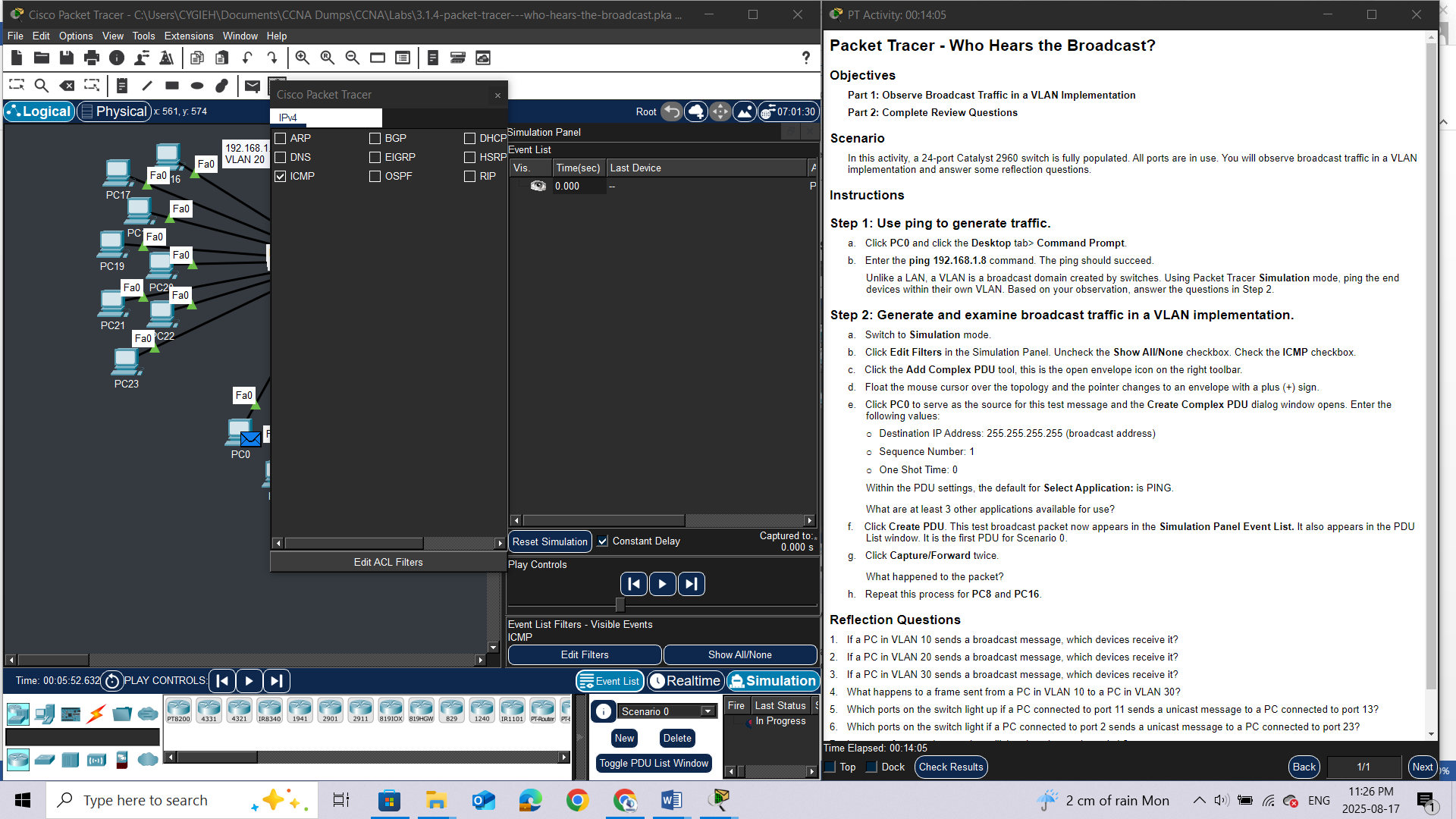
o    One Shot Time: 0

Within the PDU settings, the default for **Select Application:** is PING.

**stion:**

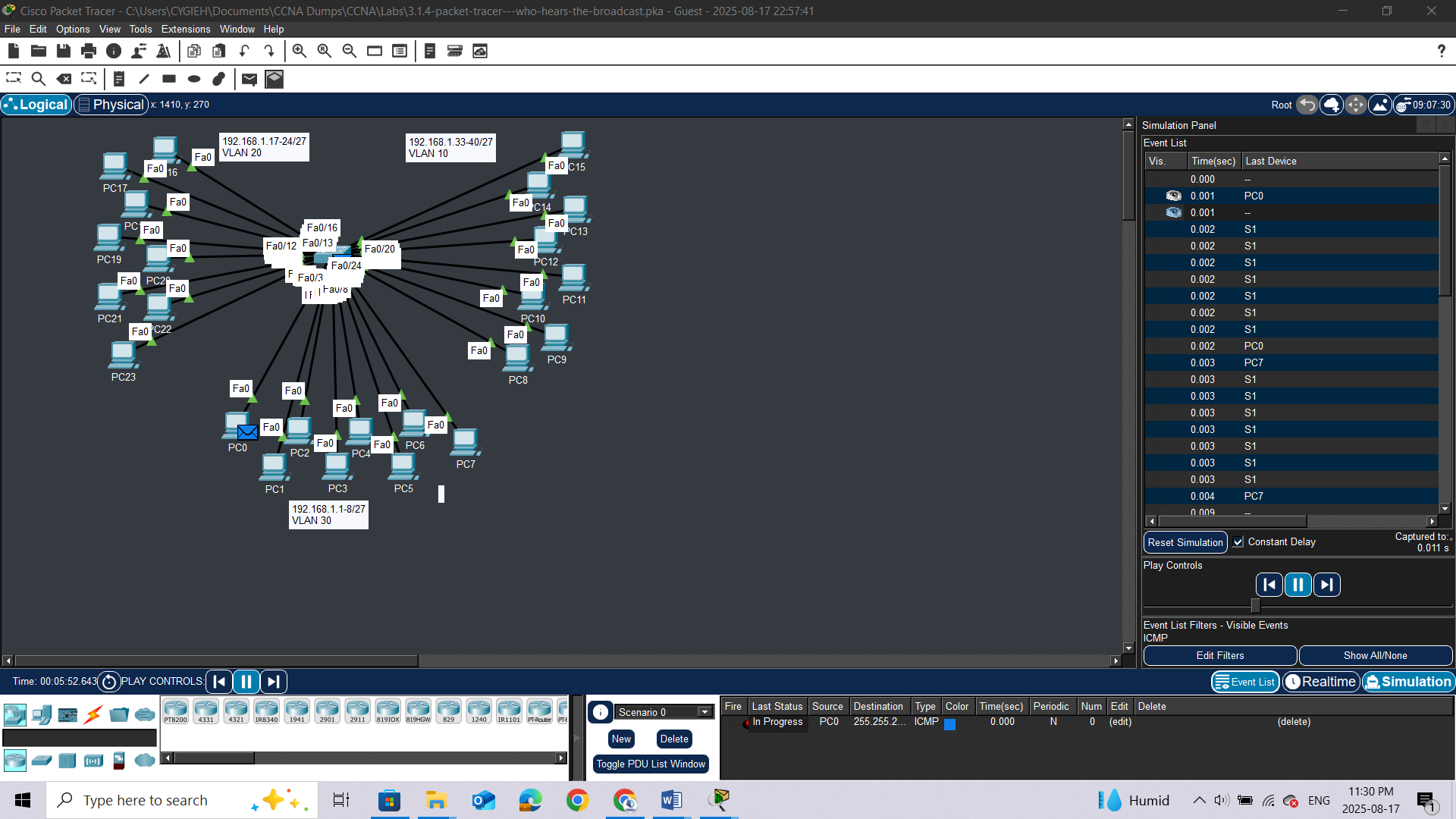
What are at least 3 other applications available for use? ***DNS, FTP, HTTP, IMAP, NETBIOS, HTTPS***

f.      Click **Create PDU**. This test broadcast packet now appears in the **Simulation Panel Event List.**It also appears in the PDU List window. It is the first PDU for Scenario 0.

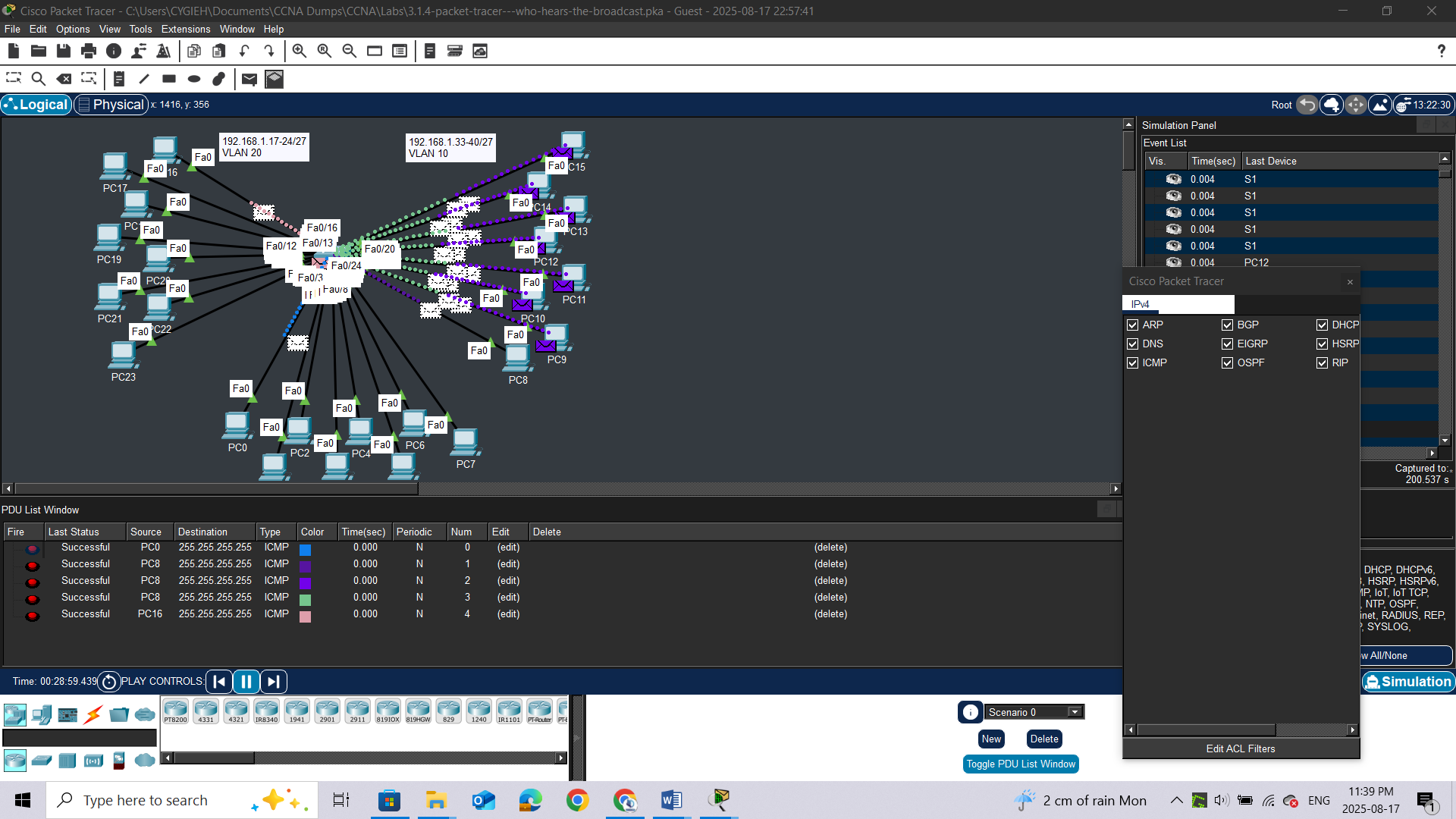


g.     Click**Capture/Forward** twice.**Question:**

What happened to the packet?



h.     Repeat this process for **PC8**and **PC16**.



## Reflection Questions

1.     If a PC in VLAN 10 sends a broadcast message, which devices receive it?

2.     If a PC in VLAN 20 sends a broadcast message, which devices receive it?

3.     If a PC in VLAN 30 sends a broadcast message, which devices receive it?

4.     What happens to a frame sent from a PC in VLAN 10 to a PC in VLAN 30?

5.     Which ports on the switch light up if a PC connected to port 11 sends a unicast message to a PC connected to port 13?

6.     Which ports on the switch light if a PC connected to port 2 sends a unicast message to a PC connected to port 23?

7.     In terms of ports, what are the collision domains on the switch?

8.     In terms of ports, what are the broadcast domains on the switch?

# LAB 2: Packet Tracer - Investigate a VLAN Implementation

## Addressing Table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device** | **Interface** | **IP Address** | **Subnet Mask** | **Default Gateway** |
| S1 | VLAN 99 | 172.17.99.31 | 255.255.255.0 | N/A |
| S2 | VLAN 99 | 172.17.99.32 | 255.255.255.0 | N/A |
| S3 | VLAN 99 | 172.17.99.33 | 255.255.255.0 | N/A |
| PC1 | NIC | 172.17.10.21 | 255.255.255.0 | 172.17.10.1 |
| PC2 | NIC | 172.17.20.22 | 255.255.255.0 | 172.17.20.1 |
| PC3 | NIC | 172.17.30.23 | 255.255.255.0 | 172.17.30.1 |
| PC4 | NIC | 172.17.10.24 | 255.255.255.0 | 172.17.10.1 |
| PC5 | NIC | 172.17.20.25 | 255.255.255.0 | 172.17.20.1 |
| PC6 | NIC | 172.17.30.26 | 255.255.255.0 | 172.17.30.1 |
| PC7 | NIC | 172.17.10.27 | 255.255.255.0 | 172.17.10.1 |
| PC8 | NIC | 172.17.20.28 | 255.255.255.0 | 172.17.20.1 |
| PC9 | NIC | 172.17.30.29 | 255.255.255.0 | 172.17.30.1 |

## Objectives

**Part 1: Observe Broadcast Traffic in a VLAN Implementation**

**Part 2: Observe Broadcast Traffic without VLANs**

## Background

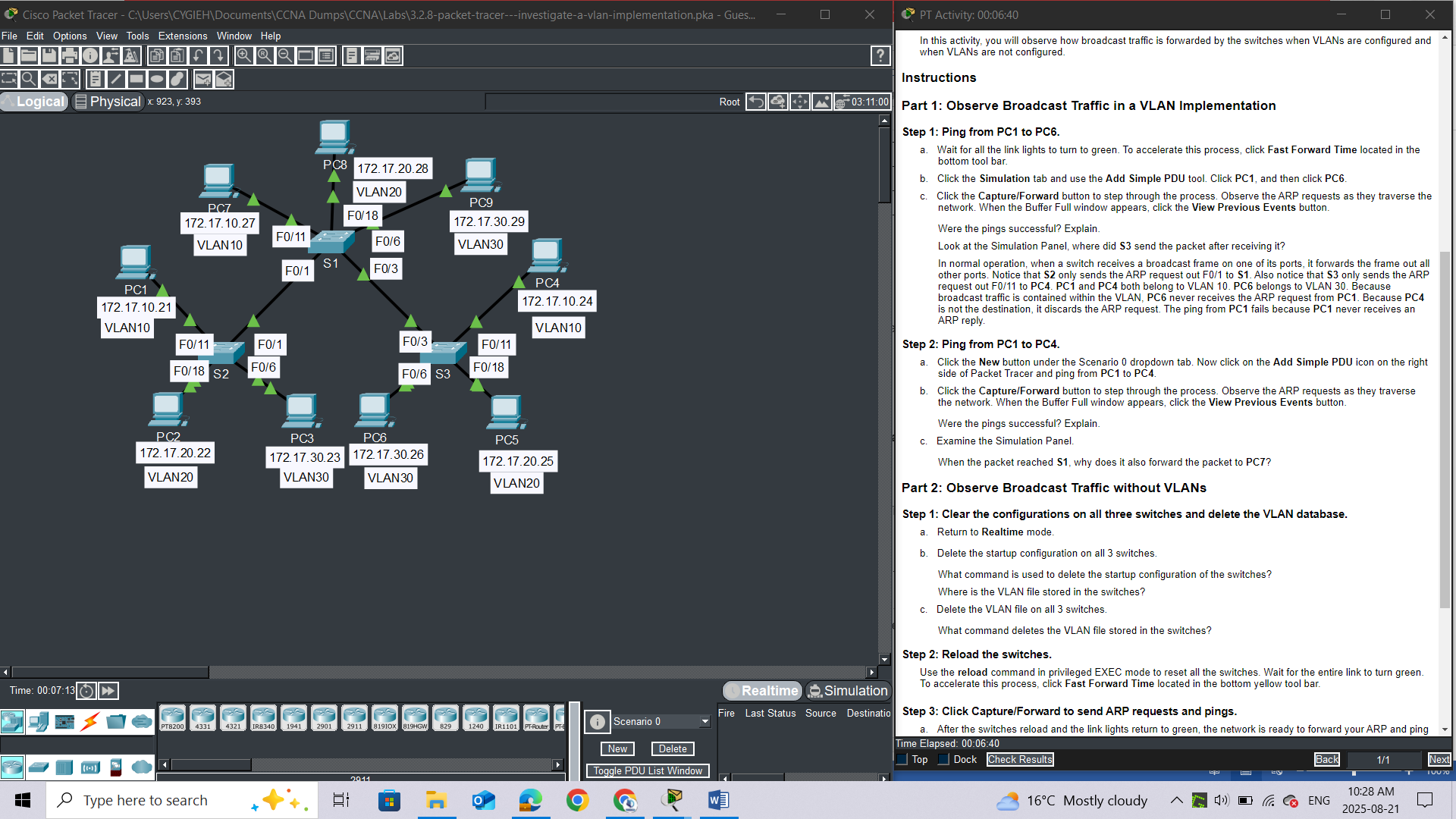
In this activity, you will observe how broadcast traffic is forwarded by the switches when VLANs are configured and when VLANs are not configured.

## Instructions

### Part 1: Observe Broadcast Traffic in a VLAN Implementation

#### Step 1: Ping from PC1 to PC6.

1. Wait for all the link lights to turn to green. To accelerate this process, click **Fast Forward Time** located in the bottom tool bar.

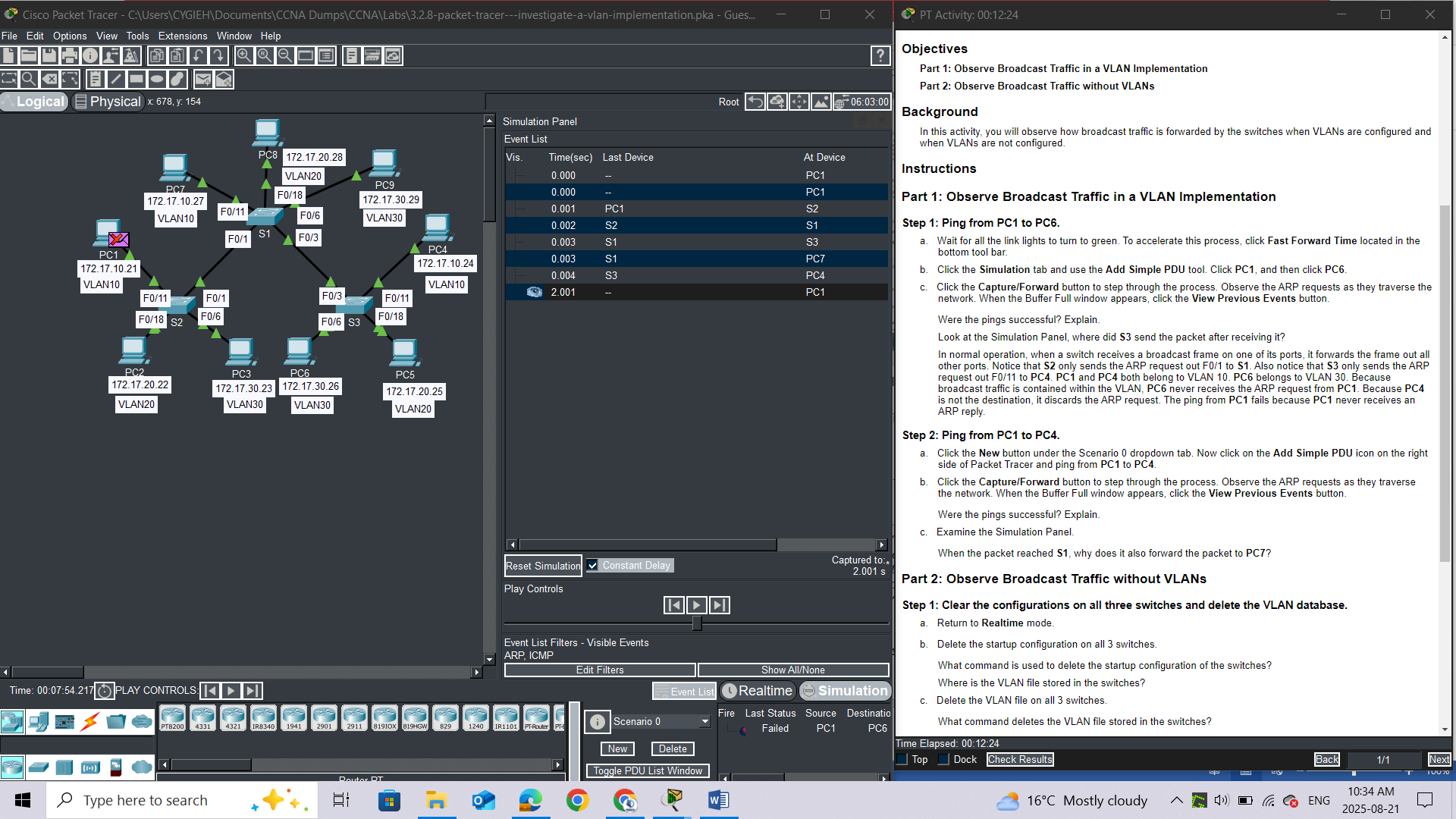


1. Click the **Simulation** tab and use the **Add Simple PDU** tool. Click **PC1**, and then click **PC6**.

c.     Click the **Capture/Forward** button to step through the process. Observe the ARP requests as they traverse the network. When the Buffer Full window appears, click the **View Previous Events** button.**Questions:**

Were the pings successful? Explain.

Look at the Simulation Panel, where did **S3** send the packet after receiving it?



**ANSWER**

*In normal operation, when a switch receives a broadcast frame on one of its ports, it forwards the frame out all other ports. Notice that****S2****only sends the ARP request out F0/1 to****S1****. Also notice that****S3****only sends the ARP request out F0/11 to****PC4****.****PC1****and****PC4****both belong to VLAN 10.****PC6****belongs to VLAN 30. Because broadcast traffic is contained within the VLAN,****PC6****never receives the ARP request from****PC1****. Because****PC4****is not the destination, it discards the ARP request. The ping from****PC1****fails because****PC1****never receives an ARP reply.*

#### Step 2: Ping from PC1 to PC4.

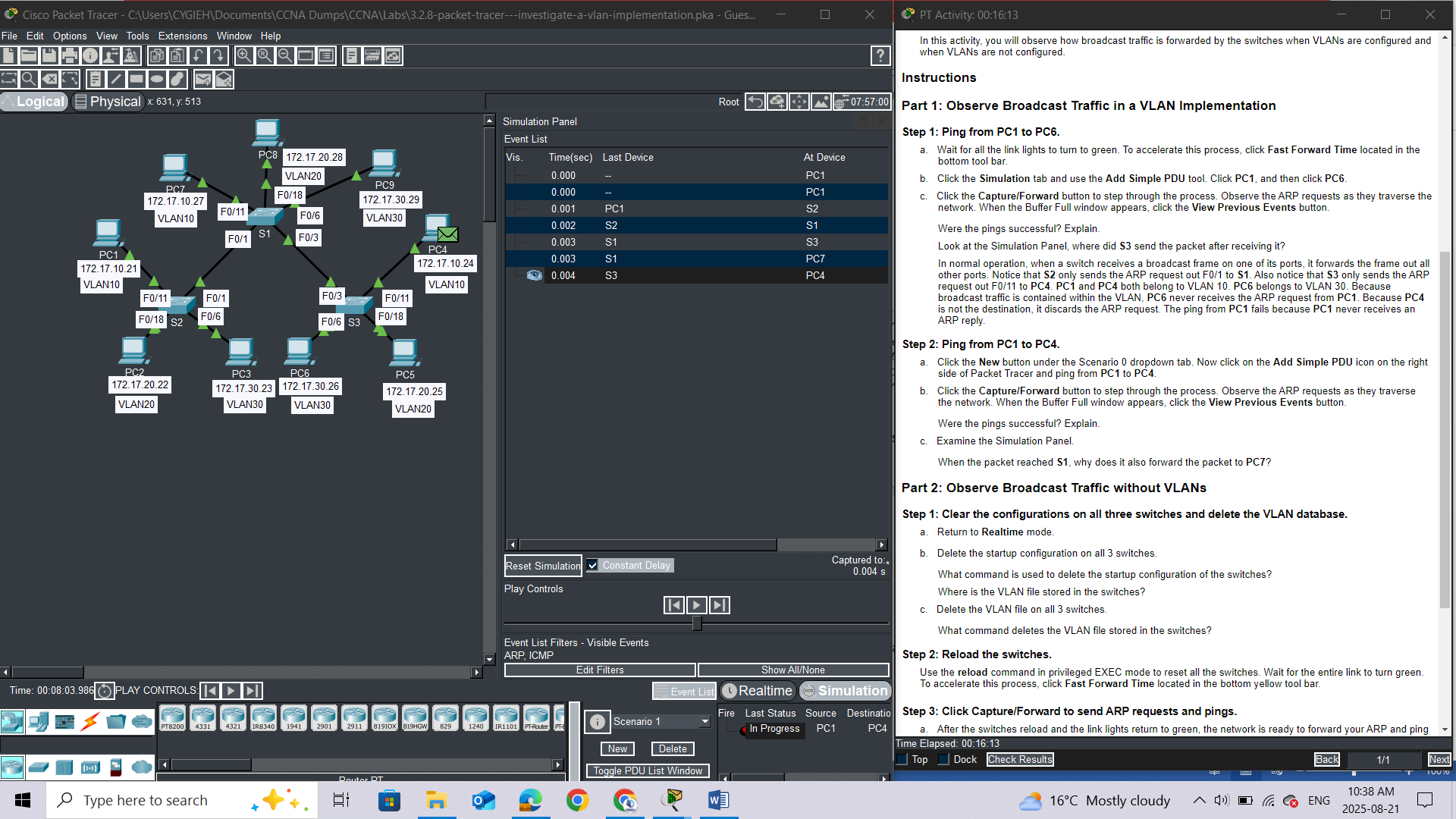
a.     Click the **New** button under the Scenario 0 dropdown tab. Now click on the **Add Simple PDU** icon on the right side of Packet Tracer and ping from **PC1** to **PC4**.

b.     Click the **Capture/Forward** button to step through the process. Observe the ARP requests as they traverse the network. When the Buffer Full window appears, click the **View Previous Events** button.

Were the pings successful? Explain. ***Yes, The ping was successful because both PC1 and PC4 are in VLAN 10***

c.     Examine the Simulation Panel.

When the packet reached **S1**, why does it also forward the packet to **PC7**? ***Because PC7 is in VLAN10 too***



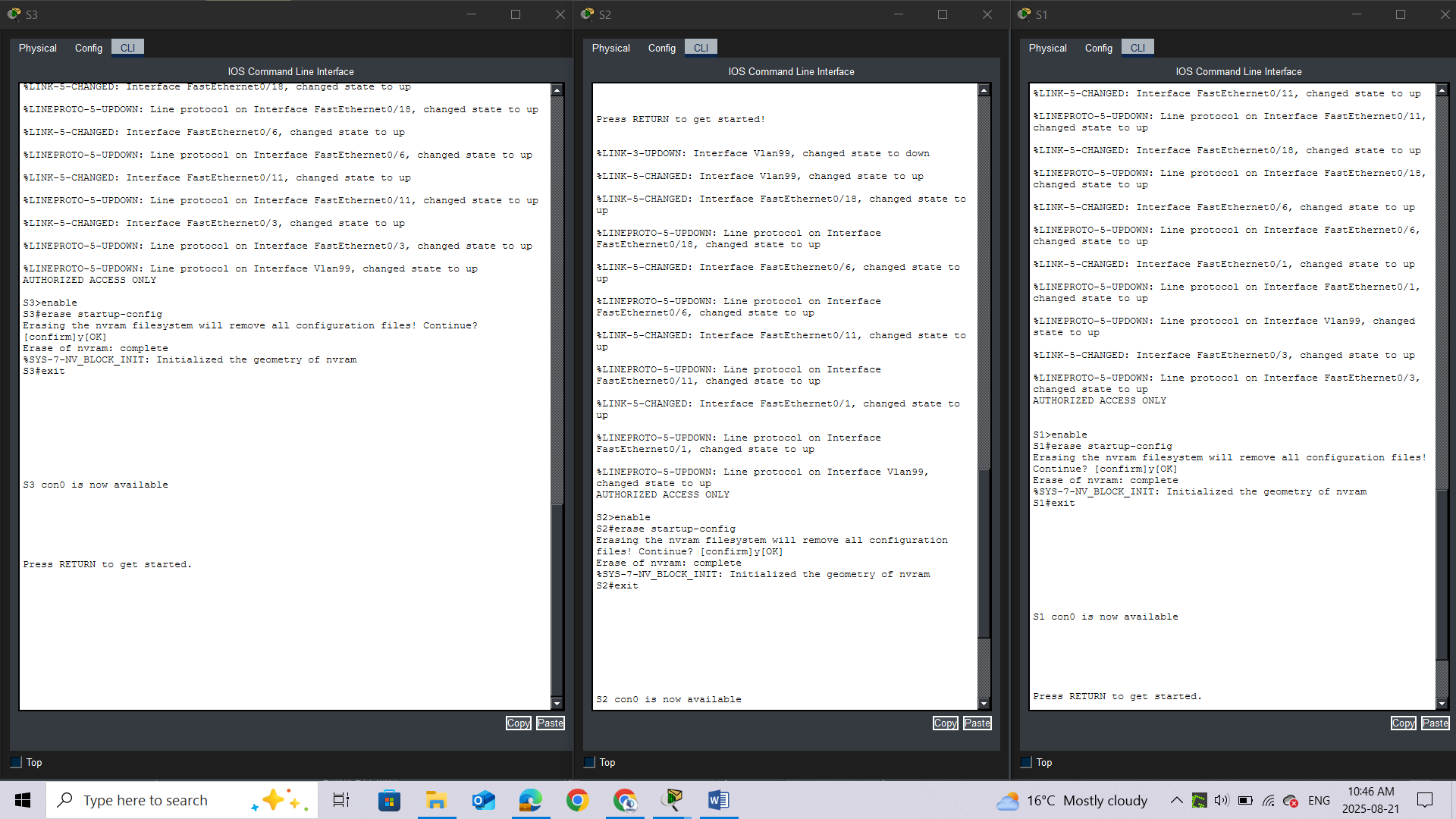
### Part 2: Observe Broadcast Traffic without VLANs

#### Step 1: Clear the configurations on all three switches and delete the VLAN database.

a.     Return to **Realtime** mode.

*Open configuration window*

1. Delete the startup configuration on all 3 switches.

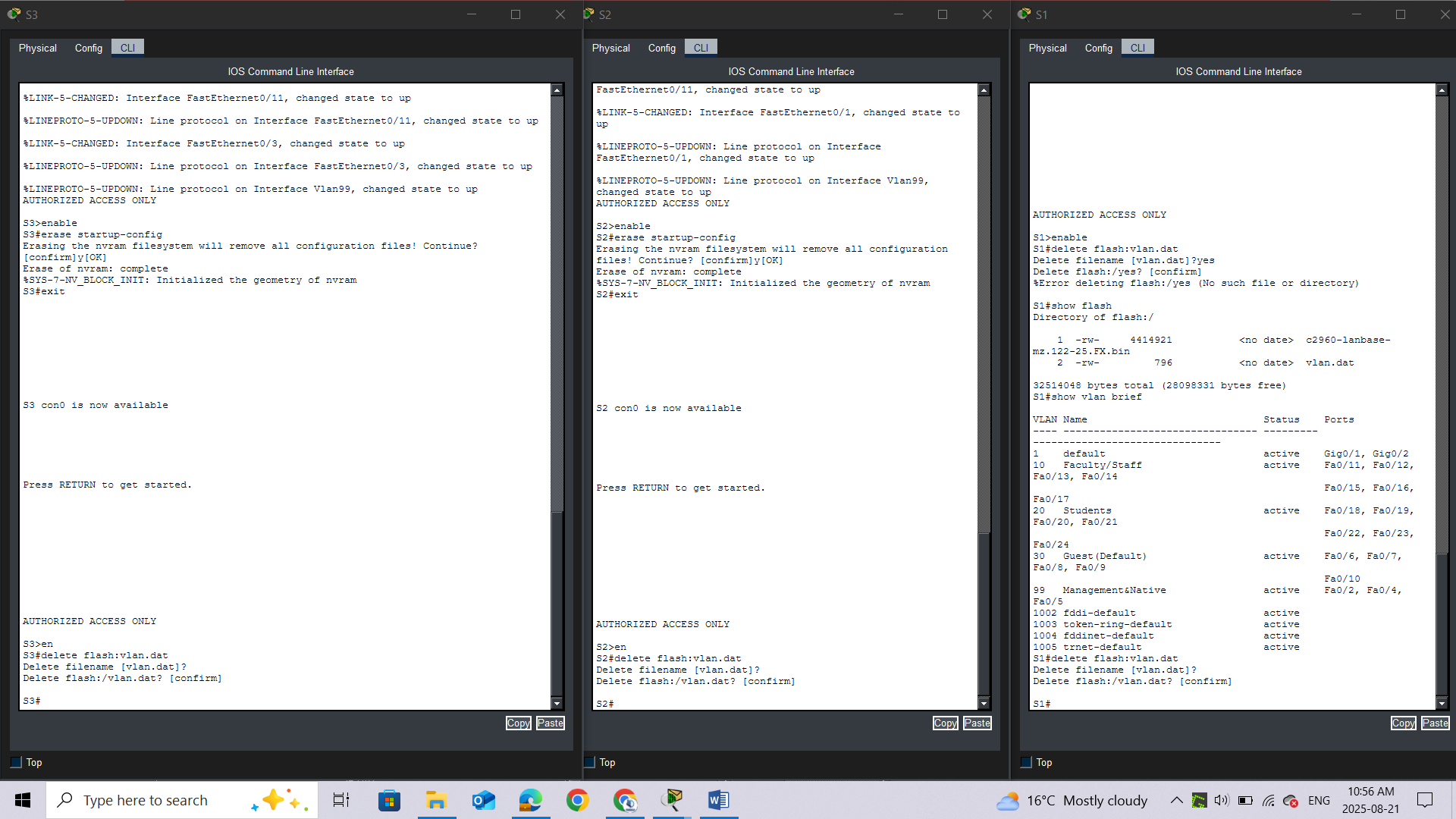


**Questions:**

What command is used to delete the startup configuration of the switches? ***erase startup-config***

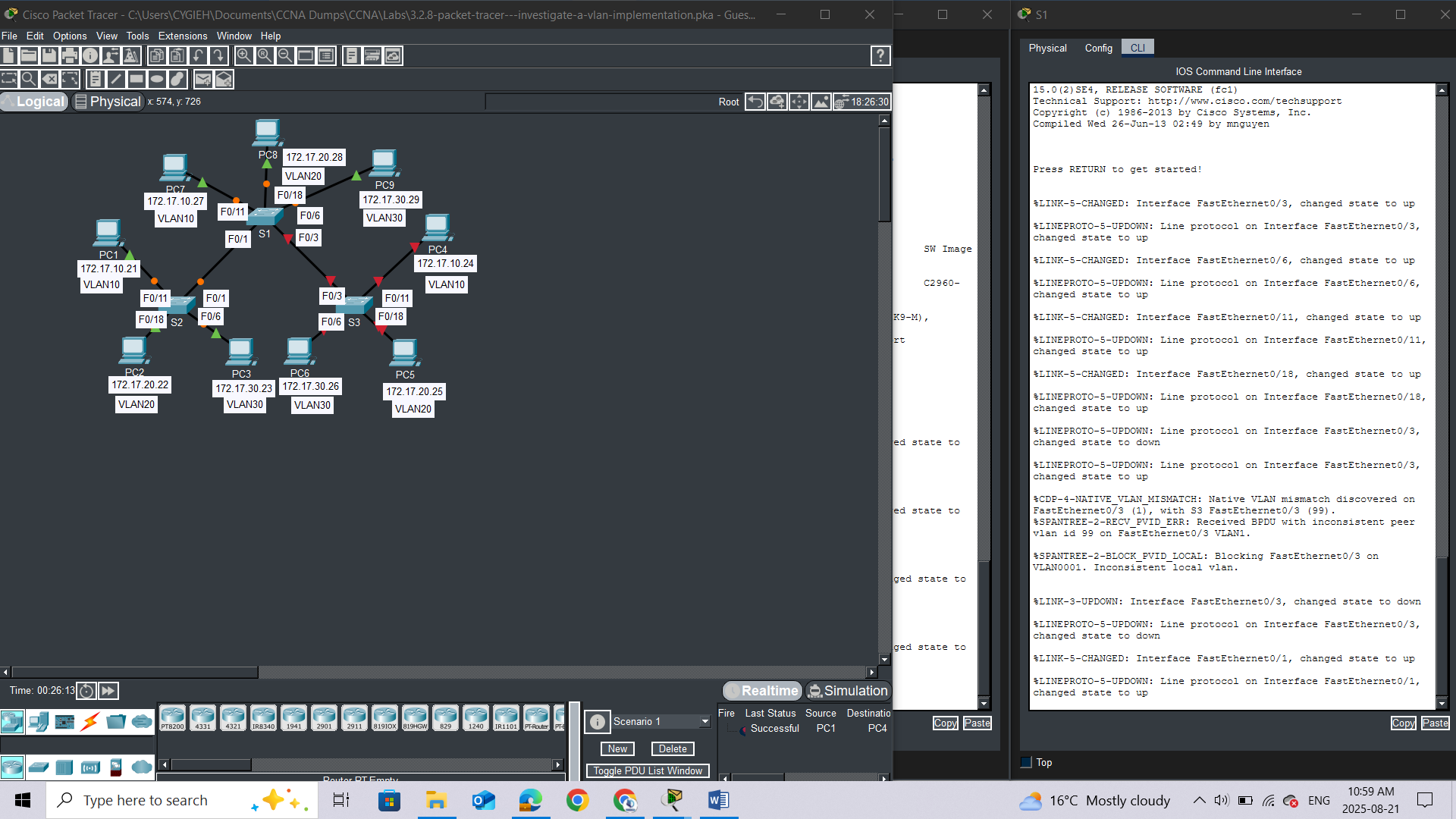
Where is the VLAN file stored in the switches? in [***vlan.dat***](https://www.google.com/search?rlz=1C1GCCU_enKE1161KE1161&cs=0&sca_esv=53bbb5633a515c6e&sxsrf=AE3TifO-j36IiuBvvxYySCaPkFHj58T0Hg%3A1755762510195&q=vlan.dat&sa=X&ved=2ahUKEwi-0-mFtZuPAxWJUaQEHeuxPBEQxccNegQIAhAB&mstk=AUtExfAe7y97b5KaOVbpXiiFL67wpjZc_cQ5xF6gmRYfw2lTtSZBlZekWrzDWZ6B763gxWdR78JFJmYBwDPWxJR-sKcqz1LBofPEkkm9TP1OAYjpzX9nGlMgHth88RiW5Ken-wfbcobGXoOkF_tHE7cqhmz_Zi6VlDXn9aF8LBZd79zoBaNkdjVpxAiocPp-6BXXBVm4izsoFwqSua2S3QqMGx5LuXAKrvy8LIXwNnRDZ6fRgXr_aPhsmPstwAsW6t6Tv0vhO_dAhHo7gk485NMmj1KA&csui=3)***, which resides in the switch's***[***flash memory***](https://www.google.com/search?rlz=1C1GCCU_enKE1161KE1161&cs=0&sca_esv=53bbb5633a515c6e&sxsrf=AE3TifO-j36IiuBvvxYySCaPkFHj58T0Hg%3A1755762510195&q=flash+memory&sa=X&ved=2ahUKEwi-0-mFtZuPAxWJUaQEHeuxPBEQxccNegQIAhAC&mstk=AUtExfAe7y97b5KaOVbpXiiFL67wpjZc_cQ5xF6gmRYfw2lTtSZBlZekWrzDWZ6B763gxWdR78JFJmYBwDPWxJR-sKcqz1LBofPEkkm9TP1OAYjpzX9nGlMgHth88RiW5Ken-wfbcobGXoOkF_tHE7cqhmz_Zi6VlDXn9aF8LBZd79zoBaNkdjVpxAiocPp-6BXXBVm4izsoFwqSua2S3QqMGx5LuXAKrvy8LIXwNnRDZ6fRgXr_aPhsmPstwAsW6t6Tv0vhO_dAhHo7gk485NMmj1KA&csui=3)***.***

1. Delete the VLAN file on all 3 switches.

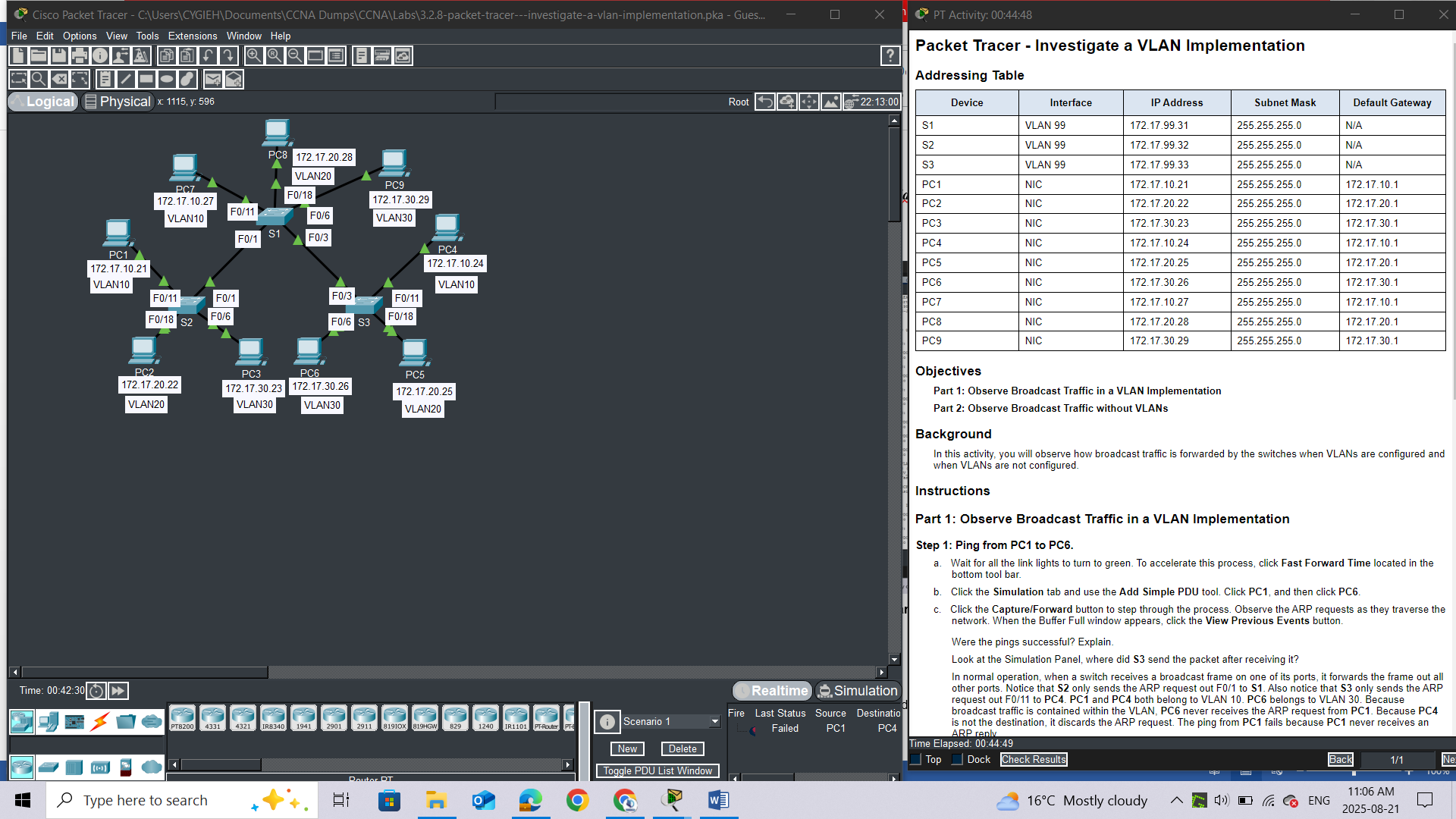
What command deletes the VLAN file stored in the switches? ***delete flash:vlan.dat***

### Step 2: Reload the switches.

Use the **reload** command in privileged EXEC mode to reset all the switches.



Wait for the entire link to turn green. To accelerate this process, click **Fast Forward Time** located in the bottom yellow tool bar.



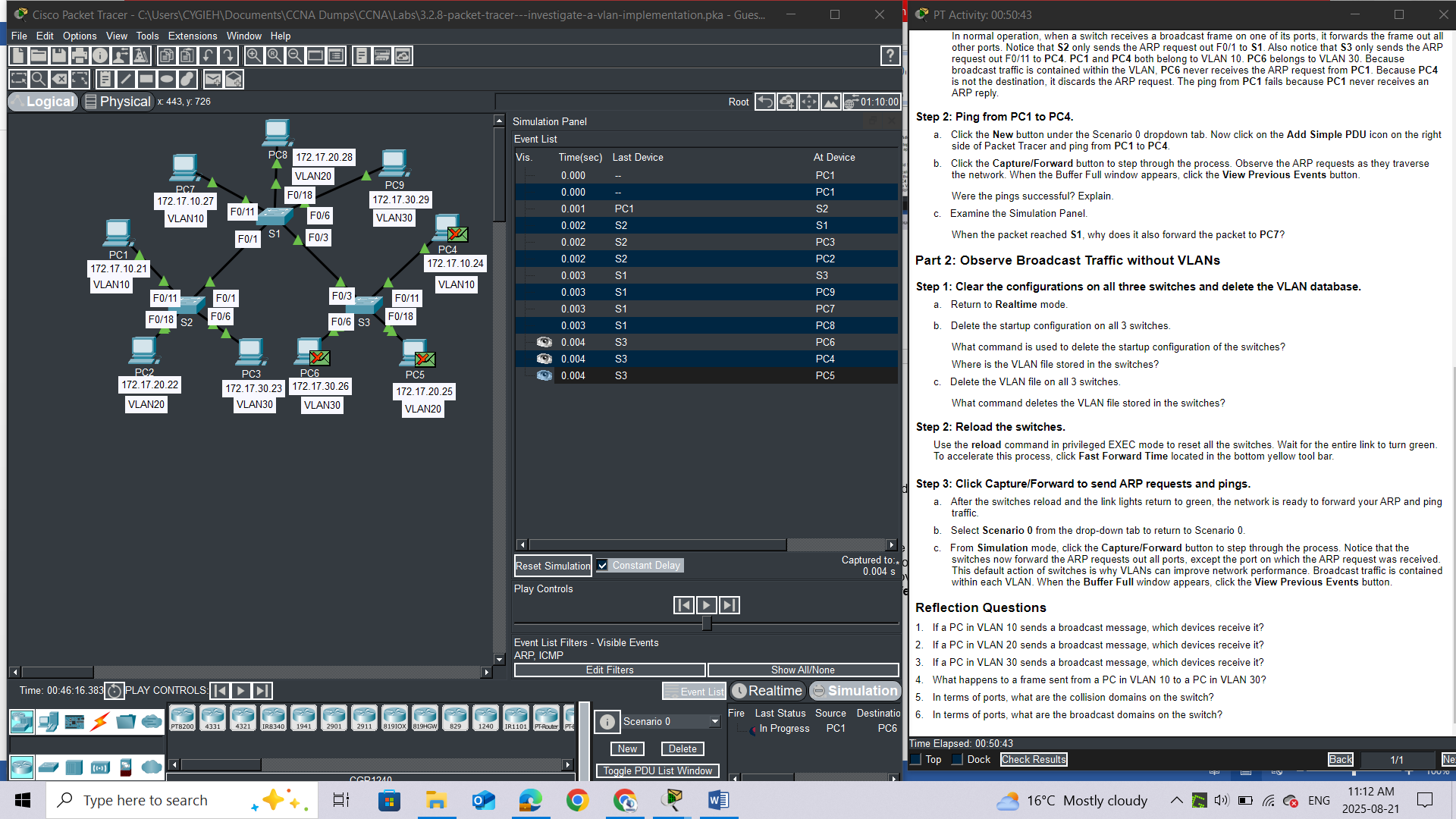
*Close configuration window*

### Step 3: Click Capture/Forward to send ARP requests and pings.

a.     After the switches reload and the link lights return to green, the network is ready to forward your ARP and ping traffic.

b.     Select **Scenario 0** from the drop-down tab to return to Scenario 0.

c.     From **Simulation**mode, click the **Capture/Forward** button to step through the process. Notice that the switches now forward the ARP requests out all ports, except the port on which the ARP request was received. This default action of switches is why VLANs can improve network performance. Broadcast traffic is contained within each VLAN. When the **Buffer Full** window appears, click the **View Previous Events** button.



## Reflection Questions

1.     If a PC in VLAN 10 sends a broadcast message, which devices receive it? All devices

2.     If a PC in VLAN 20 sends a broadcast message, which devices receive it? All devices

3.     If a PC in VLAN 30 sends a broadcast message, which devices receive it? All devices

4.     What happens to a frame sent from a PC in VLAN 10 to a PC in VLAN 30?

5.     In terms of ports, what are the collision domains on the switch?

6.     In terms of ports, what are the broadcast domains on the switch?

# LAB 3: Packet Tracer - VLAN Configuration

## Addressing Table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device** | **Interface** | **IP Address** | **Subnet Mask** | **VLAN** |
| PC1 | NIC | 172.17.10.21 | 255.255.255.0 | 10 |
| PC2 | NIC | 172.17.20.22 | 255.255.255.0 | 20 |
| PC3 | NIC | 172.17.30.23 | 255.255.255.0 | 30 |
| PC4 | NIC | 172.17.10.24 | 255.255.255.0 | 10 |
| PC5 | NIC | 172.17.20.25 | 255.255.255.0 | 20 |
| PC6 | NIC | 172.17.30.26 | 255.255.255.0 | 30 |

## Objectives

**Part 1: Verify the Default VLAN Configuration**

**Part 2: Configure VLANs**

**Part 3: Assign VLANs to Ports**

## Background

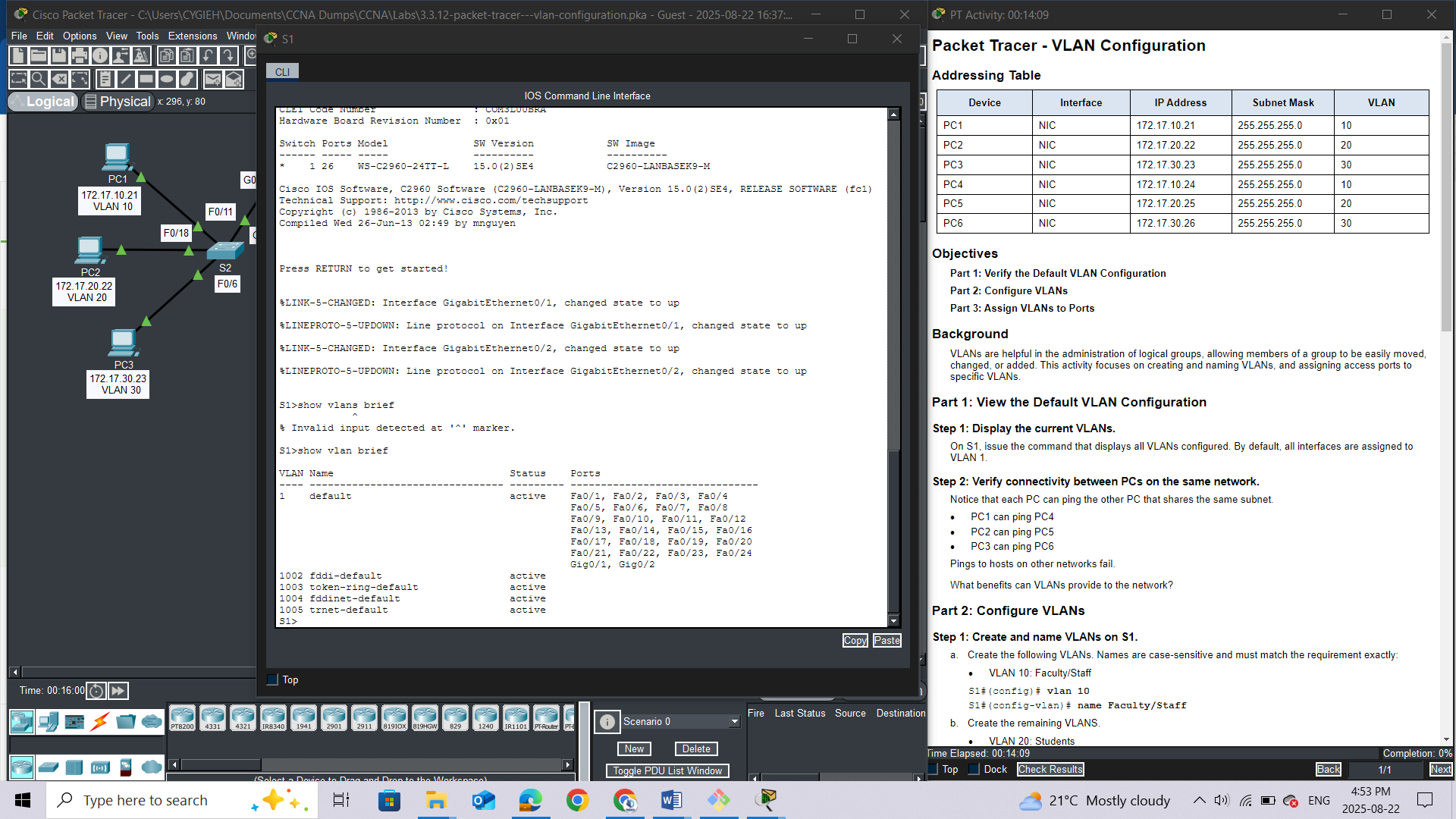
VLANs are helpful in the administration of logical groups, allowing members of a group to be easily moved, changed, or added. This activity focuses on creating and naming VLANs, and assigning access ports to specific VLANs.

## Instructions

### Part 1: View the Default VLAN Configuration

#### Step 1: Display the current VLANs.

On S1, issue the command that displays all VLANs configured. By default, all interfaces are assigned to VLAN 1.



#### Step 2: Verify connectivity between PCs on the same network.

Notice that each PC can ping the other PC that shares the same subnet.

·         PC1 can ping PC4

·         PC2 can ping PC5

·         PC3 can ping PC6

Pings to hosts on other networks fail.

Question:

What benefits can VLANs provide to the network?

1. **Enhanced Security:**
   * **Segmentation:** VLANs divide a large network into smaller, isolated virtual networks, creating "virtual walls" that prevent unauthorized users and traffic from crossing into sensitive areas.
   * **Reduced Attack Surface:** By limiting the broadcast domain, VLANs decrease the chances of a successful data breach or an attack propagating throughout the entire network.
2. **Improved Network Performance:**
   * **Reduced Broadcast Traffic:** VLANs contain broadcasts within their respective segments, preventing excessive broadcast traffic from consuming network resources and causing congestion.
   * **Optimized Traffic Flow:** Each VLAN can be configured to handle only relevant traffic, allowing devices to process information more efficiently.
3. **Simplified Network Management:**
   * **Logical Grouping:** VLANs allow you to group devices logically by function, department, or application, rather than by their physical location.
   * **Ease of Administration:** This logical grouping simplifies network administration tasks, such as applying configurations, security policies, and updates to specific groups of users or devices.
4. **Flexibility and Scalability:**
   * **Adaptable to Changes:** When users or devices move to new physical locations but perform the same function, their VLAN membership can be changed without requiring physical reconfigurations.
   * **Easy Expansion:** VLANs provide a pathway for seamless network expansion, making it easier to add new users or services as the network grows.
5. **Cost-Effectiveness:**
   * **Hardware Optimization:** VLANs allow multiple logical networks to operate on a single physical network infrastructure, reducing the need for additional switches and hardware.
6. **Policy Enforcement:**
   * **Tailored Rules:** Administrators can define and enforce specific Quality of Service (QoS) rules, access control lists (ACLs), and other security policies for individual VLANs

### Part 2: Configure VLANs

#### Step 1: Create and name VLANs on S1.

a.     Create the following VLANs. Names are case-sensitive and must match the requirement exactly:

·         VLAN 10: Faculty/Staff

*Open configuration window*

S1#(config)# **vlan 10**

S1#(config-vlan)# **name Faculty/Staff**

b.     Create the remaining VLANS.

·         VLAN 20: Students

·         VLAN 30: Guest(Default)

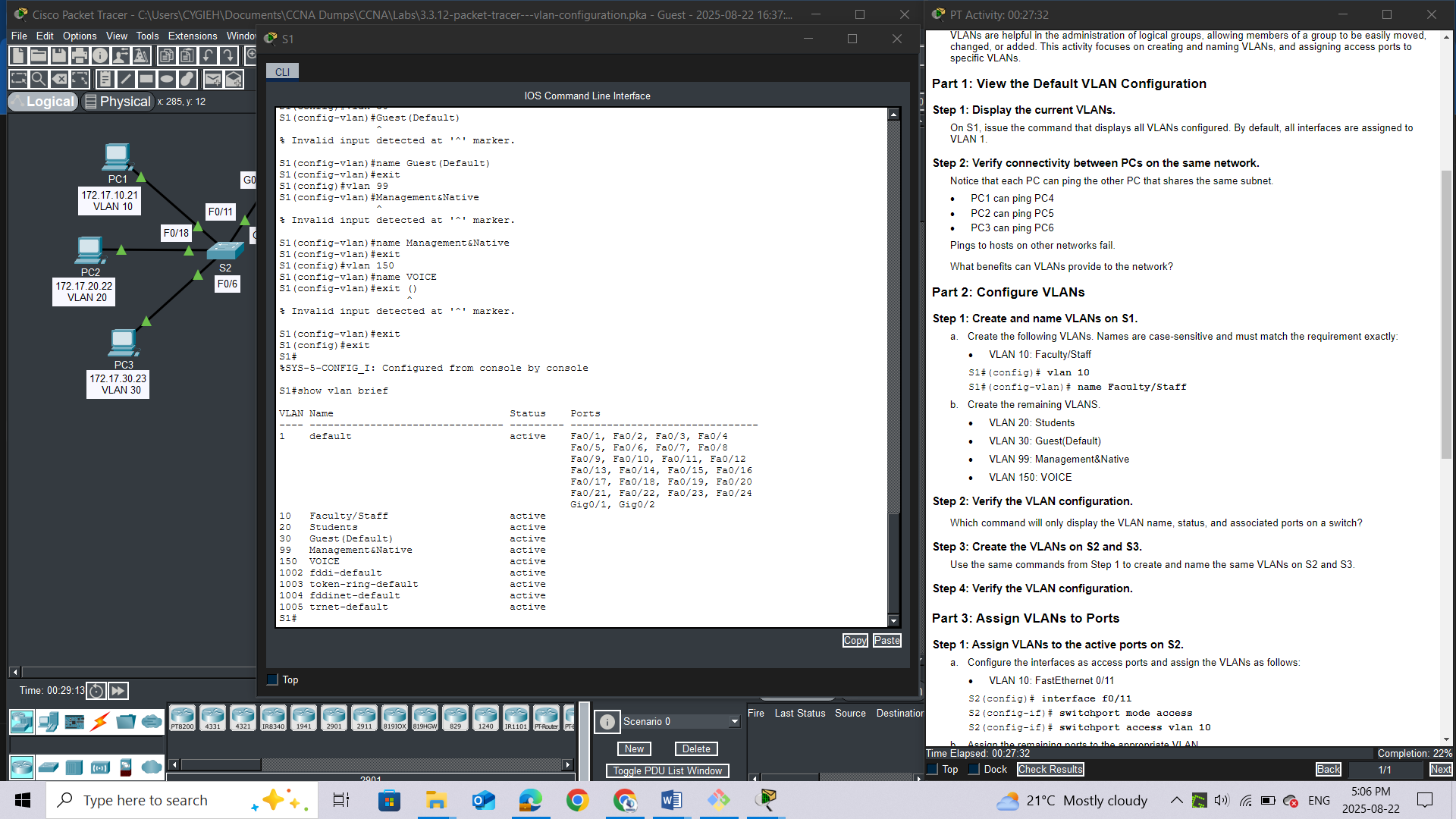
·         VLAN 99: Management&Native

·         VLAN 150: VOICE

#### Step 2: Verify the VLAN configuration.

Question:

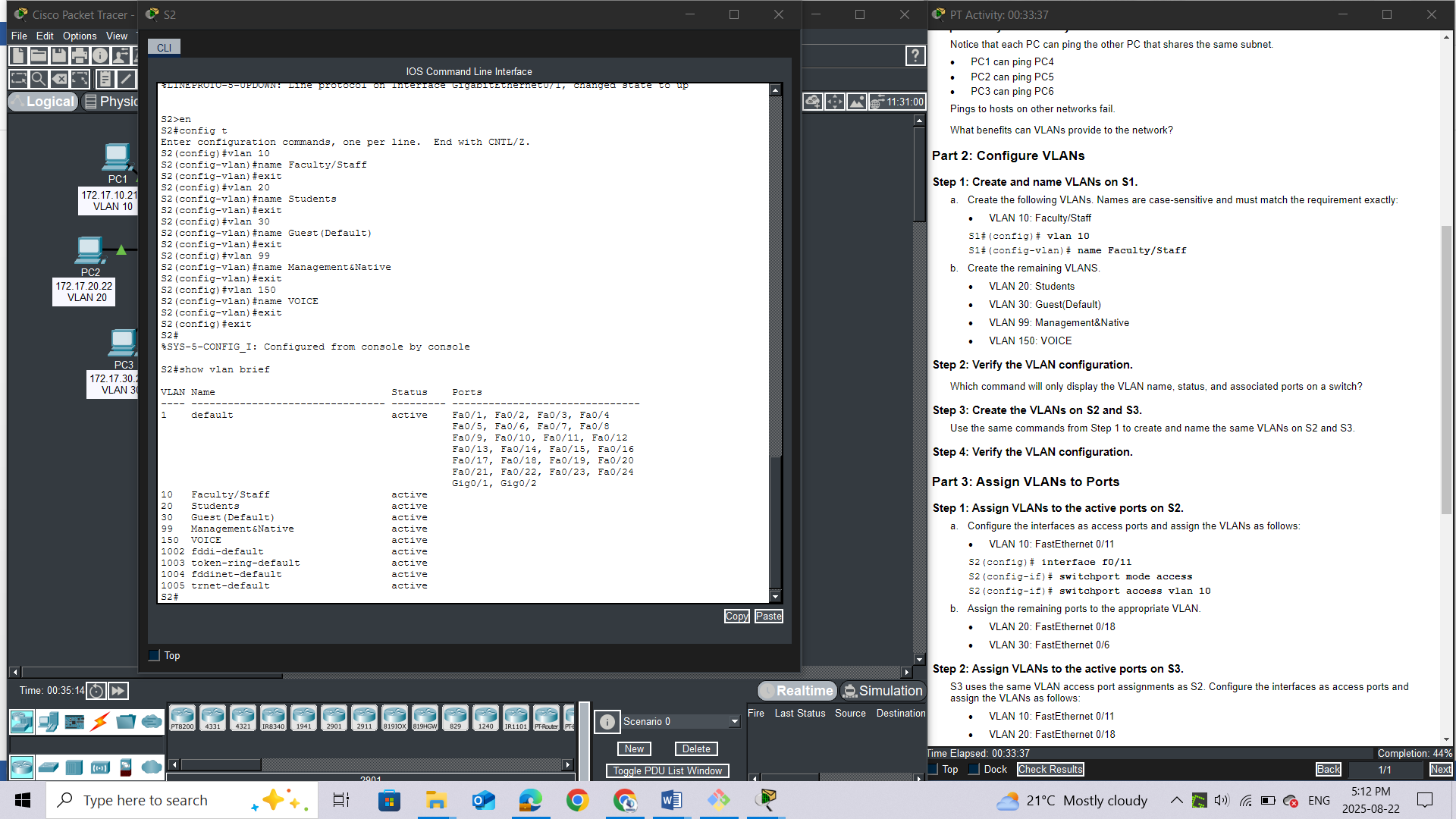
Which command will only display the VLAN name, status, and associated ports on a switch? **Show vlan brief**

****

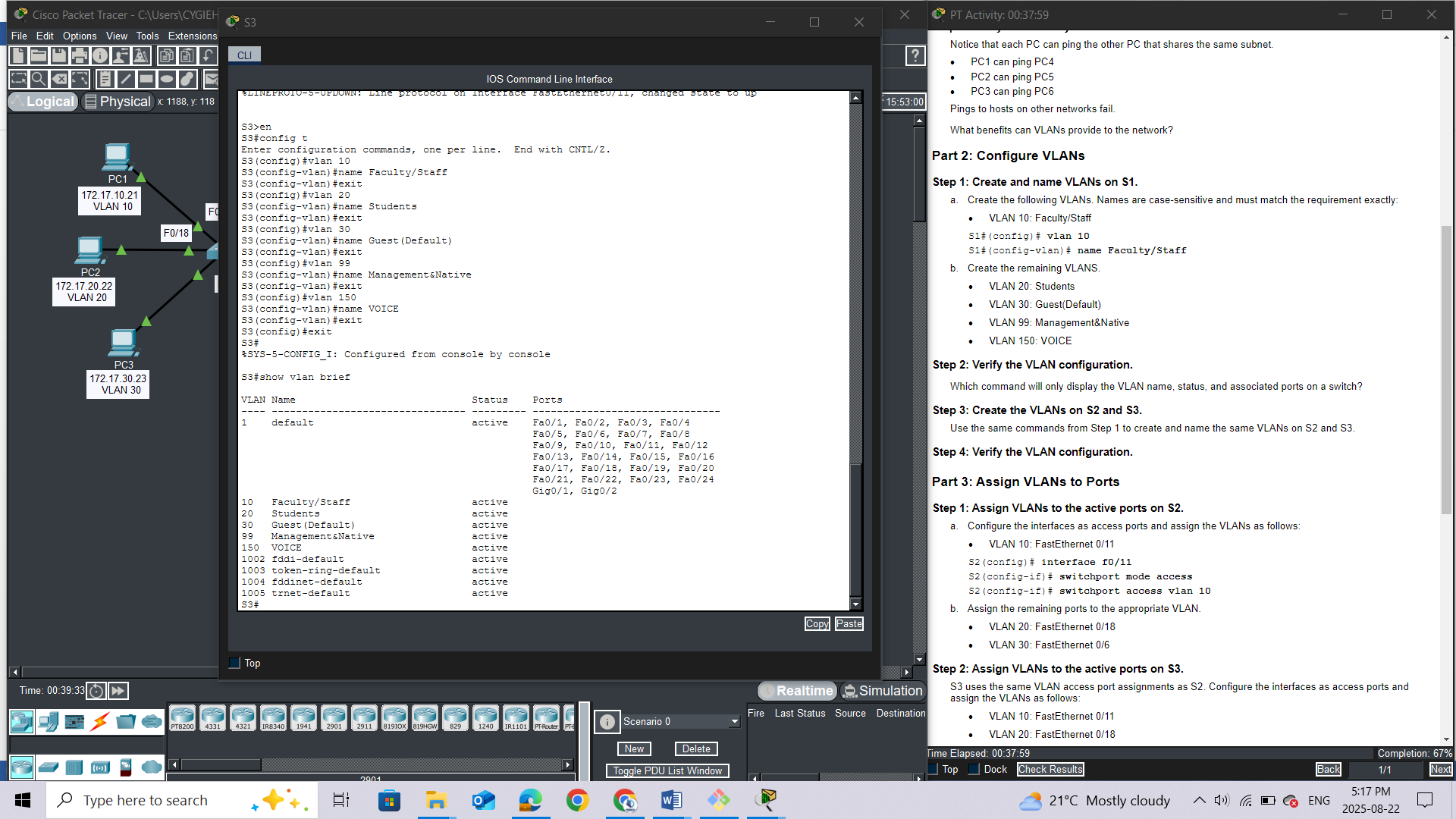
#### Step 3: Create the VLANs on S2 and S3.

Use the same commands from Step 1 to create and name the same VLANs on S2 and S3.

**S2**



**S3**

****

#### Step 4: Verify the VLAN configuration.

*Close configuration window*

### Part 3: Assign VLANs to Ports

#### Step 1: Assign VLANs to the active ports on S2.

a.     Configure the interfaces as access ports and assign the VLANs as follows:

·         VLAN 10: FastEthernet 0/11

*Open configuration window*

S2(config)# **interface f0/11**

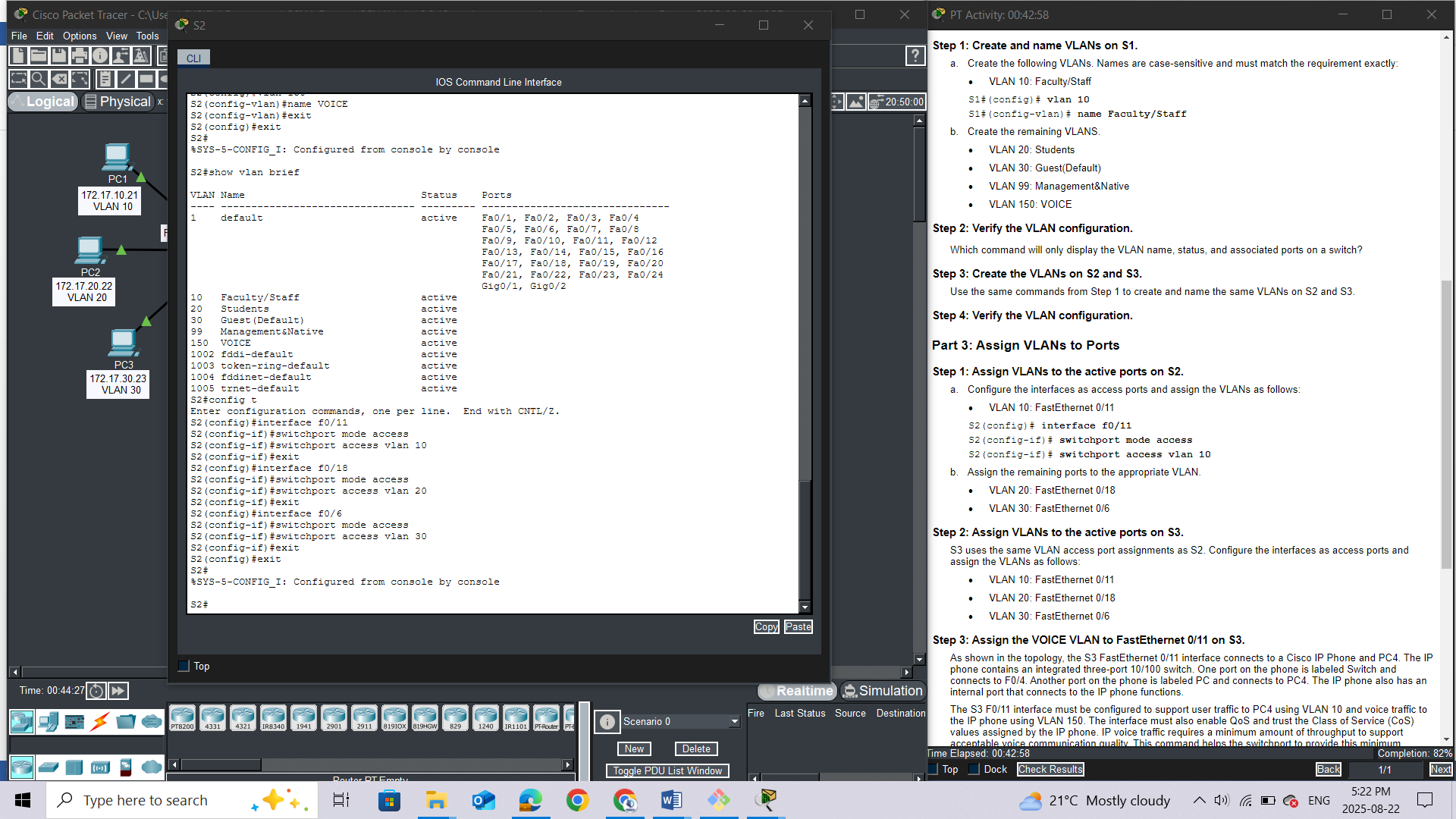
S2(config-if)# **switchport mode access**

S2(config-if)# **switchport access vlan 10**

b.     Assign the remaining ports to the appropriate VLAN.

·         VLAN 20: FastEthernet 0/18

·         VLAN 30: FastEthernet 0/6



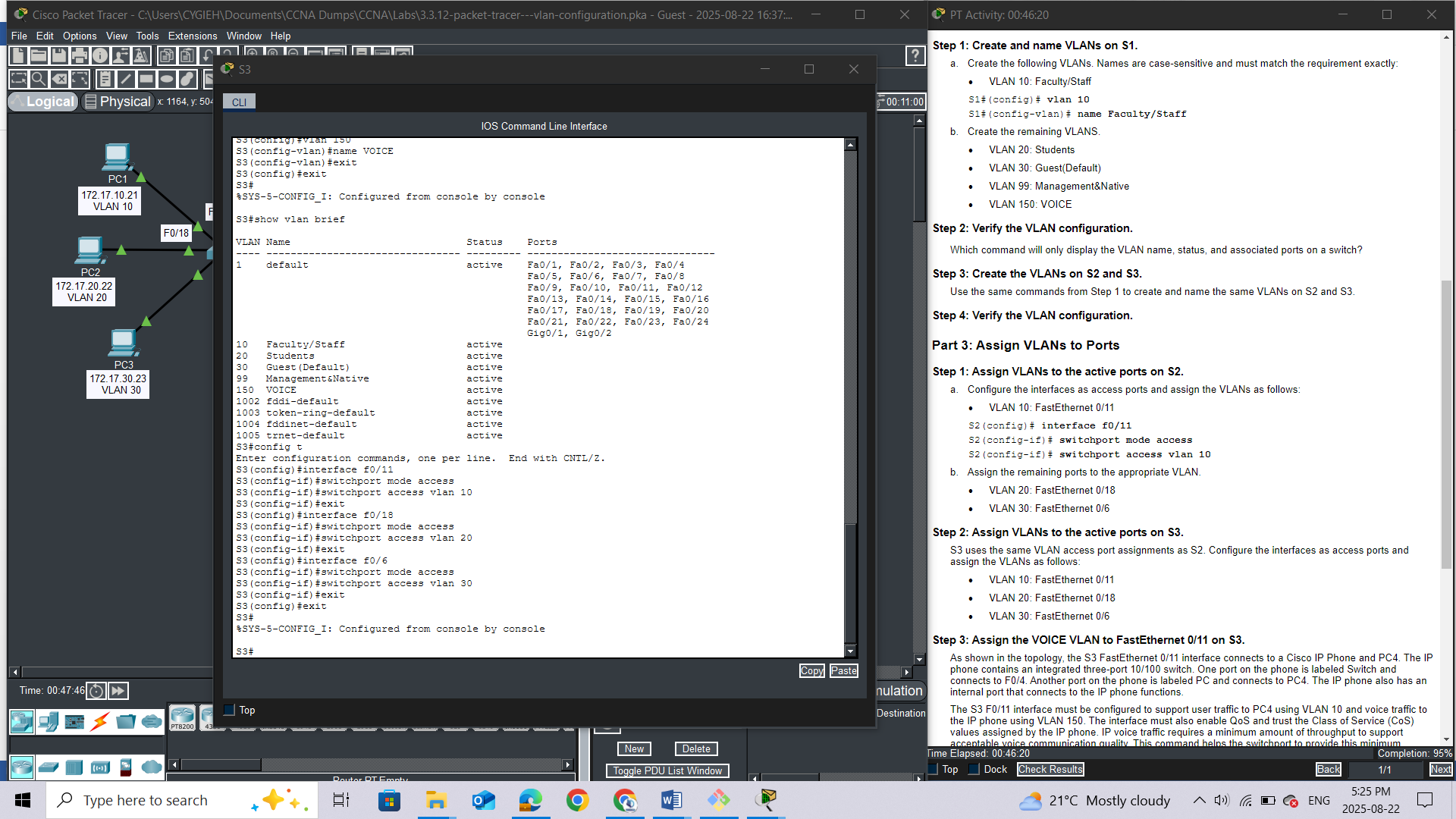
#### Step 2: Assign VLANs to the active ports on S3.

S3 uses the same VLAN access port assignments as S2. Configure the interfaces as access ports and assign the VLANs as follows:

·         VLAN 10: FastEthernet 0/11

·         VLAN 20: FastEthernet 0/18

·         VLAN 30: FastEthernet 0/6



#### Step 3: Assign the VOICE VLAN to FastEthernet 0/11 on S3.

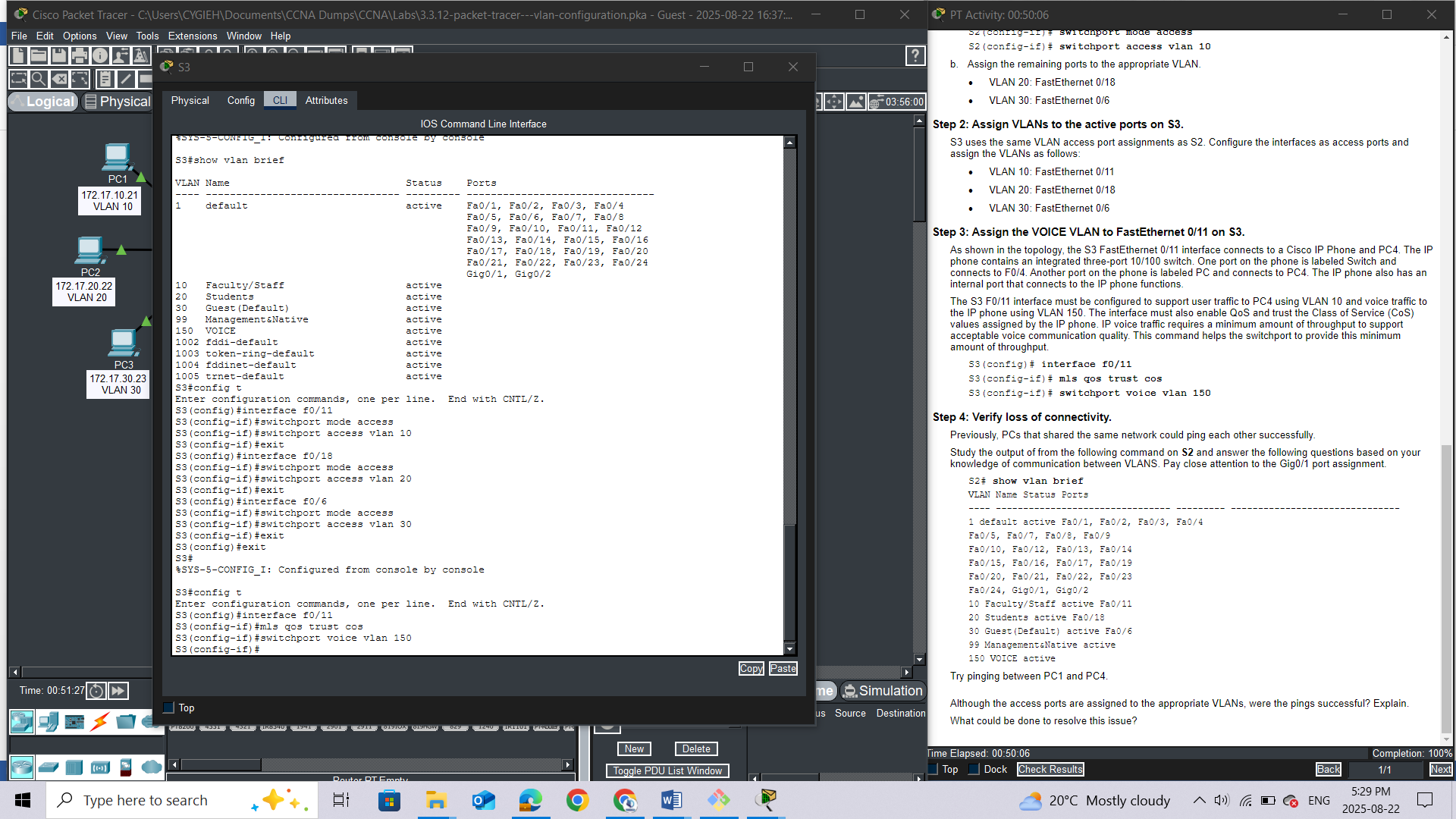
As shown in the topology, the S3 FastEthernet 0/11 interface connects to a Cisco IP Phone and PC4. The IP phone contains an integrated three-port 10/100 switch. One port on the phone is labeled Switch and connects to F0/4. Another port on the phone is labeled PC and connects to PC4. The IP phone also has an internal port that connects to the IP phone functions.

The S3 F0/11 interface must be configured to support user traffic to PC4 using VLAN 10 and voice traffic to the IP phone using VLAN 150. The interface must also enable QoS and trust the Class of Service (CoS) values assigned by the IP phone. IP voice traffic requires a minimum amount of throughput to support acceptable voice communication quality. This command helps the switchport to provide this minimum amount of throughput.

S3(config)# **interface f0/11**

S3(config-if)# **mls qos trust cos**

S3(config-if)# **switchport voice vlan 150**



#### Step 4: Verify loss of connectivity.

Previously, PCs that shared the same network could ping each other successfully.

Study the output of from the following command on **S2** and answer the following questions based on your knowledge of communication between VLANS. Pay close attention to the Gig0/1 port assignment.

S2# **show vlan brief**

VLAN Name Status Ports

---- -------------------------------- --------- -------------------------------

1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4

Fa0/5, Fa0/7, Fa0/8, Fa0/9

Fa0/10, Fa0/12, Fa0/13, Fa0/14

Fa0/15, Fa0/16, Fa0/17, Fa0/19

Fa0/20, Fa0/21, Fa0/22, Fa0/23

Fa0/24, Gig0/1, Gig0/2

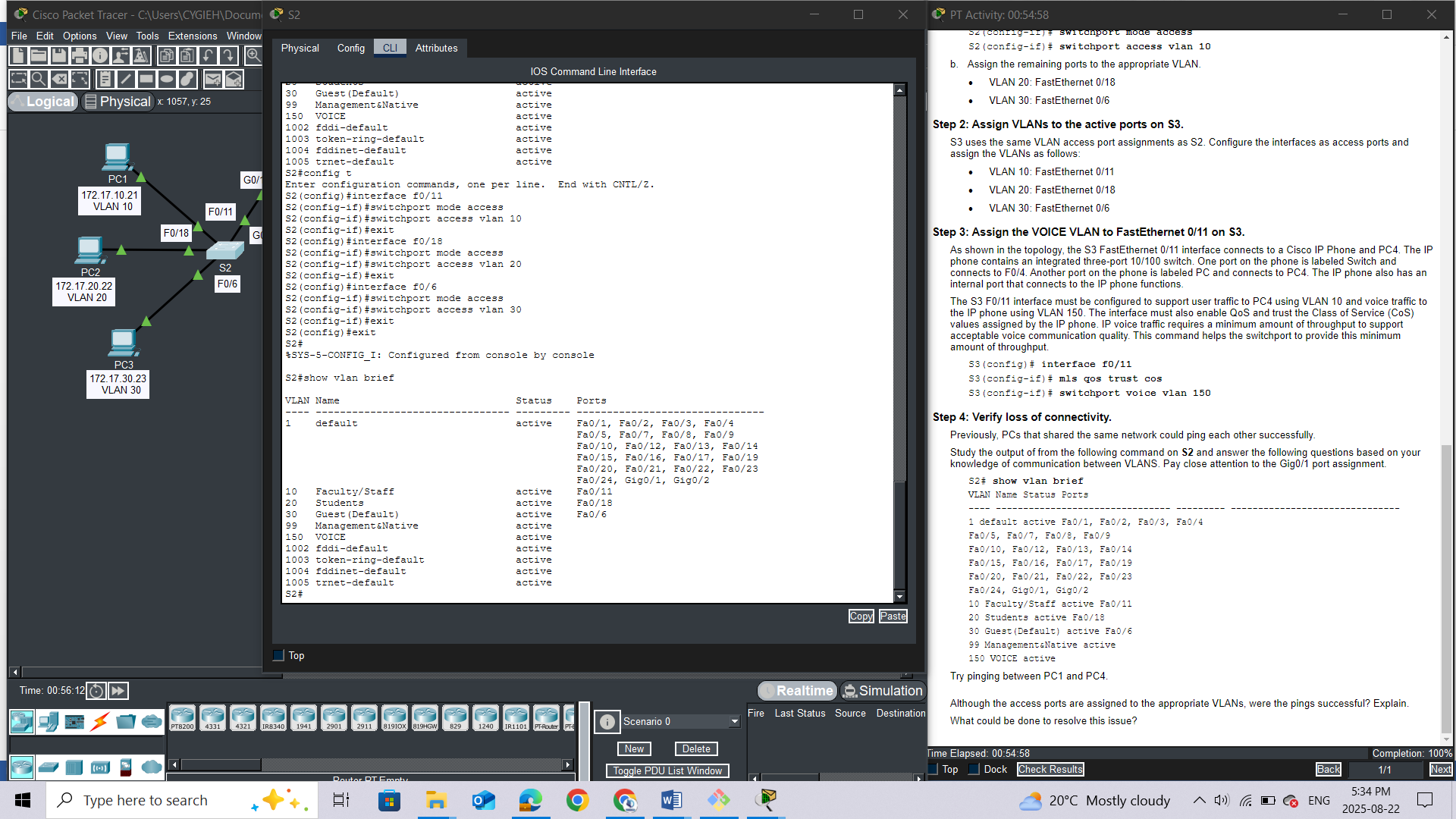
10 Faculty/Staff active Fa0/11

20 Students active Fa0/18

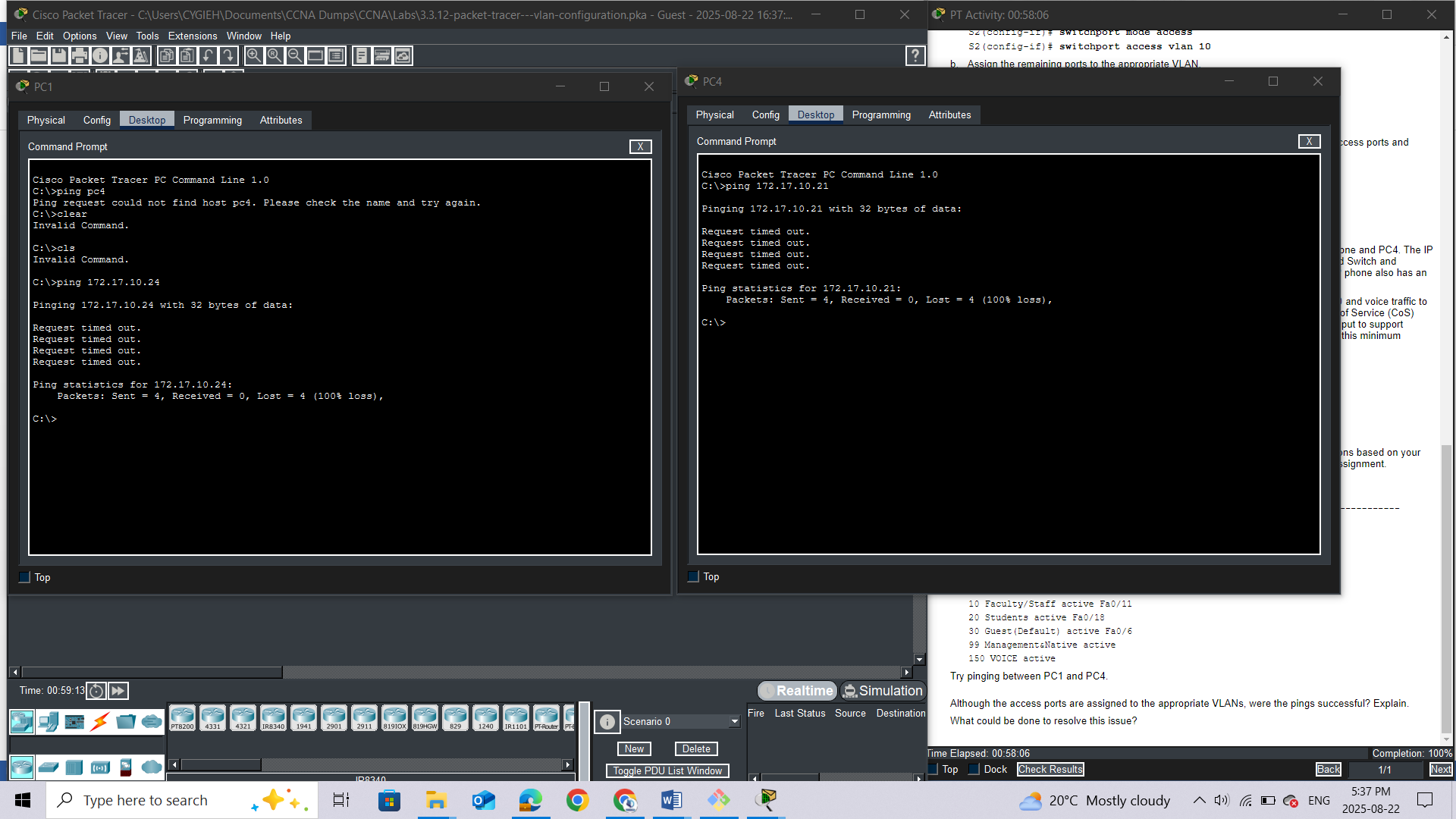
30 Guest(Default) active Fa0/6

99 Management&Native active

150 VOICE active



Try pinging between PC1 and PC4.



## Questions:

Although the access ports are assigned to the appropriate VLANs, were the pings successful? Explain.

What could be done to resolve this issue?