P15/145186/2022

VLANs LAB1

PART 1

- **Reading assignment**
  - Read the notes (slides) in the VLANs folder (of Corporate network Technologies section). Read the following sections and then answer the questions that follow..
    - Breaking networks into subnetworks
    - Subnetting
    - Subnetting without VLANs
    - Mapping VLANs to subnets
  - What is a VLAN? How is it related to broadcast domains and subnets?

A **VLAN** (Virtual Local Area Network) is a network technology that allows for the segmentation of a physical network into multiple logical networks. Each VLAN functions as a separate **broadcast domain**, which means that broadcast traffic within one VLAN is isolated and not forwarded to other VLANs. This segmentation happens at **Layer 2** (Data Link Layer) of the OSI model.

Relation to broadcast domains and subnets: VLANs limit the size of broadcast domains, and in most configurations, each VLAN is typically mapped to a **single IP subnet**. The broadcast traffic is restricted within the VLAN, preventing unnecessary broadcasts across the entire network. This separation improves network performance and security.

  - Why do you think the VLAN technology was developed?

VLAN technology was developed to address issues of network segmentation, broadcast traffic control, and resource management. reasons include:

- **Improving performance**: By reducing broadcast traffic and isolating it within specific VLANs.
- **Enhancing security**: VLANs allow administrators to separate sensitive traffic (like different departments) even within the same physical network.
- **Scalability**: VLANs make it easier to manage and scale networks without physically restructuring them.
- **Flexibility**: VLANs allow devices from different locations to be logically grouped, making network management simpler.

  - Does the use of VLANs improve or worsen the performance of a Switched LAN? Explain! What are its other advantages/disadvantages?

Improves performance: VLANs reduce the size of broadcast domains, which can reduce congestion and improve overall network efficiency. Only devices within a VLAN receive broadcast traffic, preventing unnecessary broadcast storms.

- **Advantages**:
  - Limits the size of broadcast domains, improving network performance and scalability.

  - Enhances security by isolating traffic in different VLANs.
  - Simplifies management by logically grouping devices across a network.
  - Enables the creation of virtual workgroups and differentiation between traffic types (e.g., data and voice).
- **Disadvantages**:
  - Inter-VLAN communication requires routing, which can introduce complexity and additional latency.
  - Misconfigurations can lead to connectivity issues or security vulnerabilities.
  - VLANs can be complex to manage in very large networks

  - Distinguish between an access link and a trunk link in a VLAN. Identify the access and trunk links in the networks described in (a) and (b) of Part 2
    Access link: Connects a switch to an end device (e.g., a computer, printer) and carries traffic for a single VLAN. It does not tag frames with VLAN IDs.
    Trunk link: Connects switches or a switch to a router and carries traffic for multiple VLANs. Frames on trunk links are tagged with VLAN IDs to differentiate traffic from different VLANs.

  - Distinguish between (i) VLANs created on a single switch and (ii) VLANs which span multiple switches. Which of the above two methods is preferable today? Explain! In which circumstances (Name just one) is the non preferred one useful? Explain!
- **VLANs on a single switch**: VLANs created on a single switch are confined to that switch. This is simpler but only applicable for small, localized networks.
- **VLANs spanning multiple switches**: VLANs can span multiple switches by using trunk links between the switches, allowing devices on different switches but within the same VLAN to communicate as if they are on the same network.

Preferable method today: VLANs spanning multiple switches are preferable today, especially in large or distributed networks, because they provide greater flexibility and scalability.

Single-switch VLAN use case: In small networks (like a single office floor), VLANs created on a single switch can be sufficient and simpler to manage

  - Why and when is a tag added to a frame when VLANs are in use?
    A **VLAN tag** is added to Ethernet frames when they pass through **trunk links** to distinguish traffic from different VLANs. The tag is necessary because trunk links carry traffic from multiple VLANs, and the tag ensures that the traffic is routed correctly within the correct VLAN. When a frame exits a switch to an access link, the VLAN tag is removed since the end device does not need to interpret VLAN information.
  - Is it possible to use VLANs without mapping them to subnets? Use the diagrams in subnetting without VLANs and Mapping subnets to VLANs to answer this question.

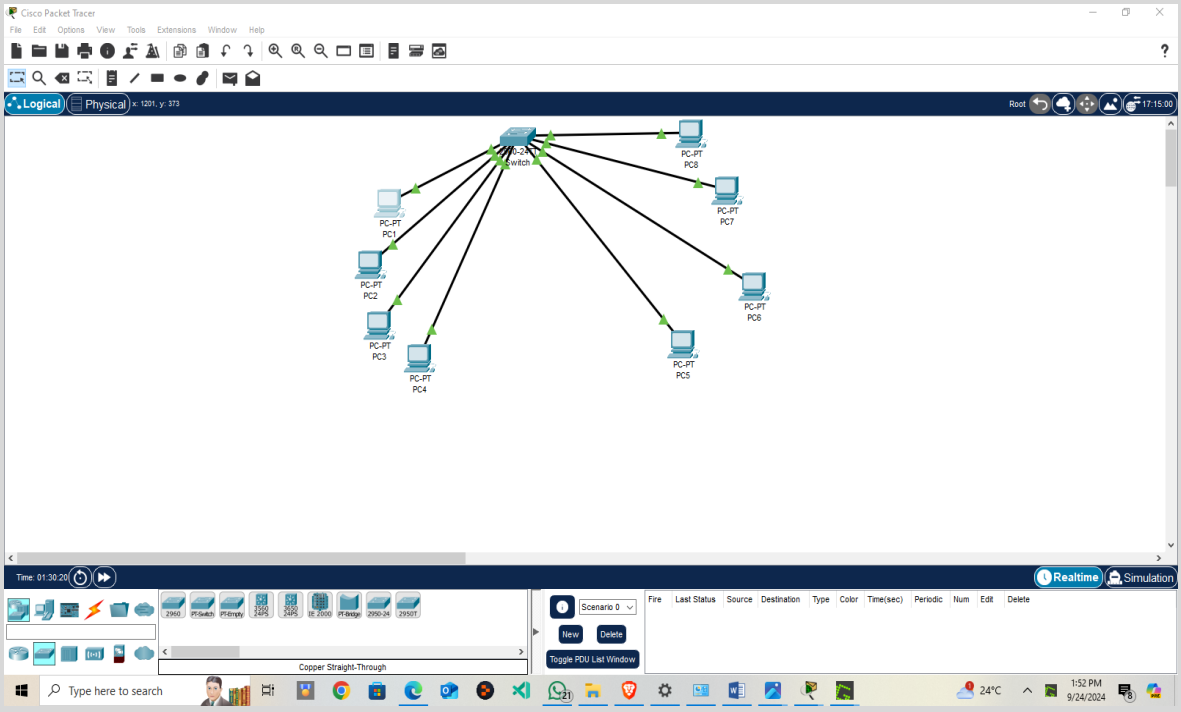
No, VLANs are mapped to subnets to ensure that broadcast traffic is limited within a VLAN and that routing between VLANs can occur efficiently. **Subnetting without VLANs** leads to all devices being part of the same broadcast domain, which defeats the purpose of VLAN segmentation. However, **mapping VLANs to subnets** ensures broadcast traffic remains within a VLAN and allows for routing between subnets (and VLANs) as needed.

PART 2

- Read the notes (VLAN configuration) about how to configure VLANs on a switch. Use that information to create and configure VLANs in questions (a) and (b) below. Use packet tracer.

(a) A switch is configured with two Fast Ethernet switched LANs (VLANs), VLAN 10 and VLAN 20. Each of the VLANs has four hosts (PC1 to PC4 & PC5 to PC8 respectively). VLAN 10 is mapped to netID 192.168.1.0/24 while VLAN 20 is mapped to NetID 192.168.2.0/24

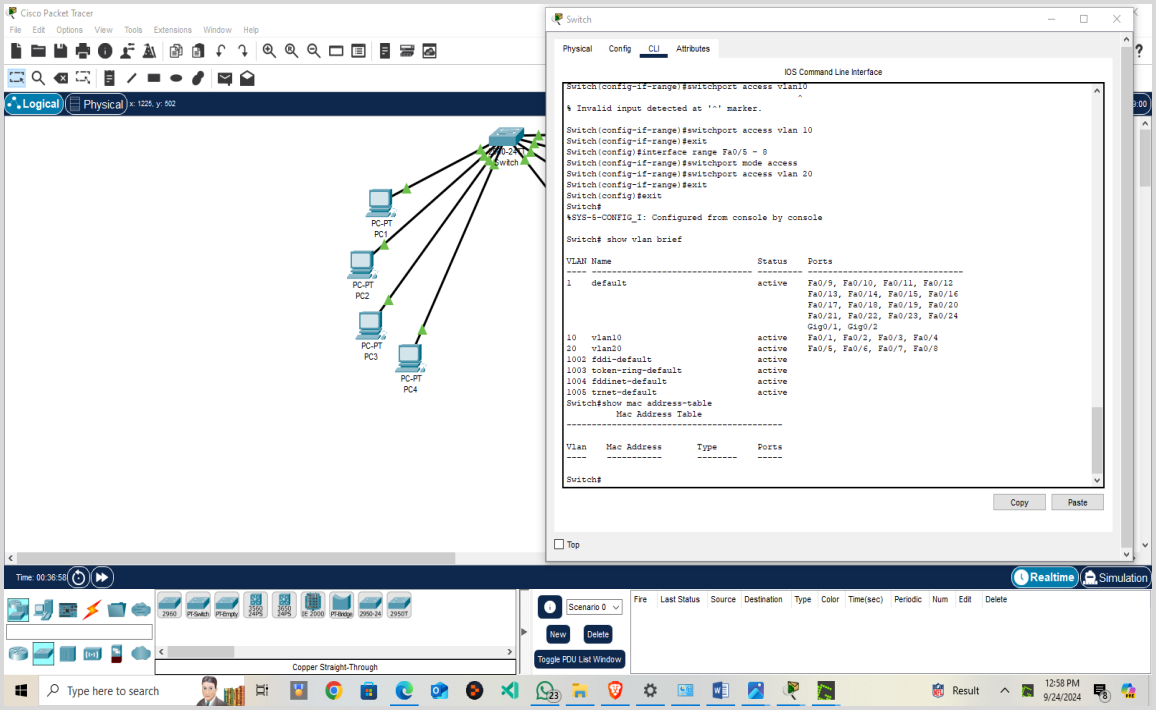
- Using Packet tracer, create a Fast Ethernet switched LAN with 8 PCs (PC1 to PC8). This should be based on the 2960 cisco switch



- List the MAC addresses of the 8 PCs in your network

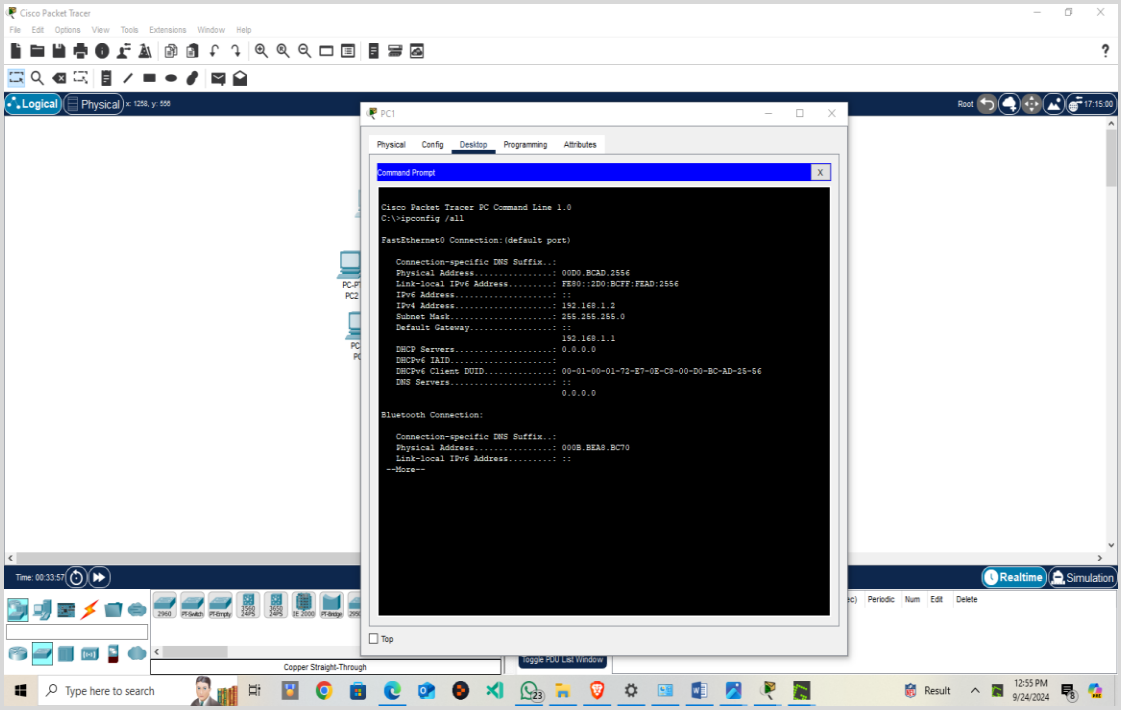
Switched not learned yet about my pcs mac addresses

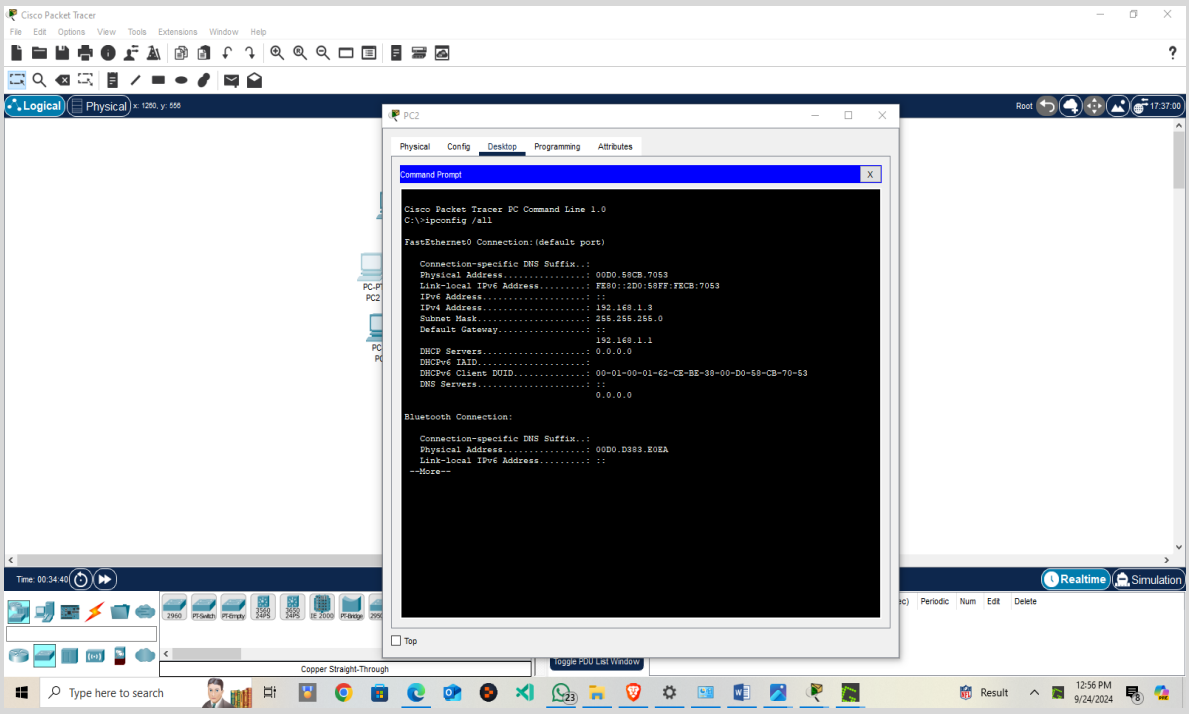
P15/145186/2022



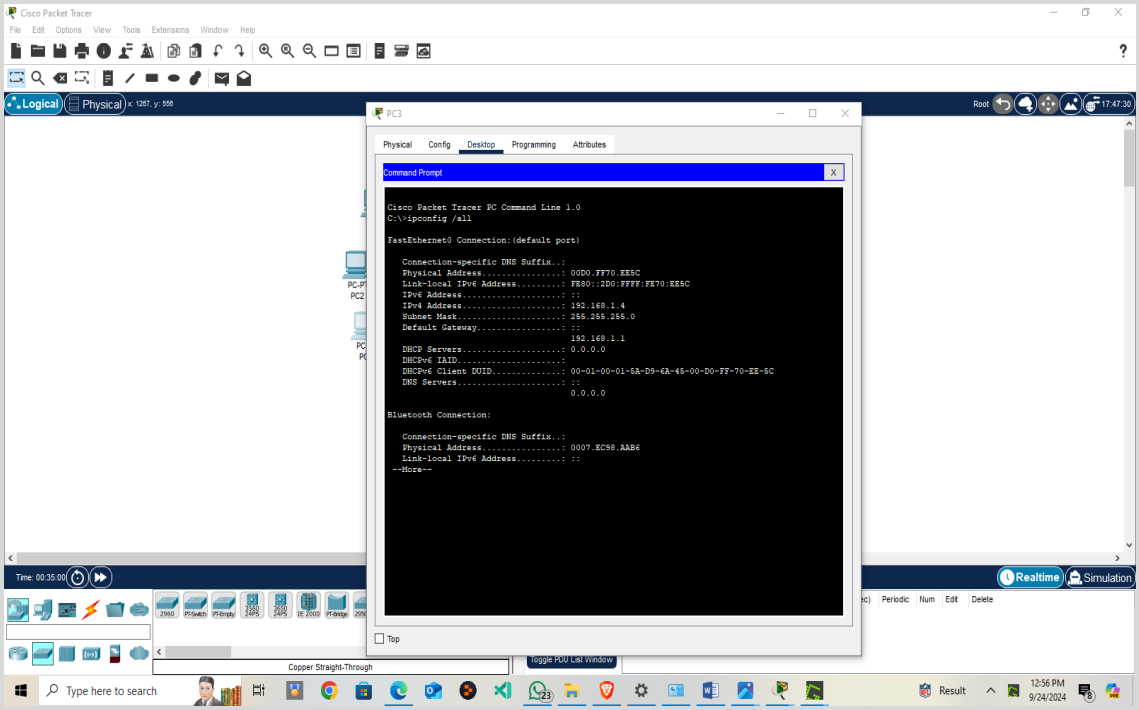
P15/145186/2022

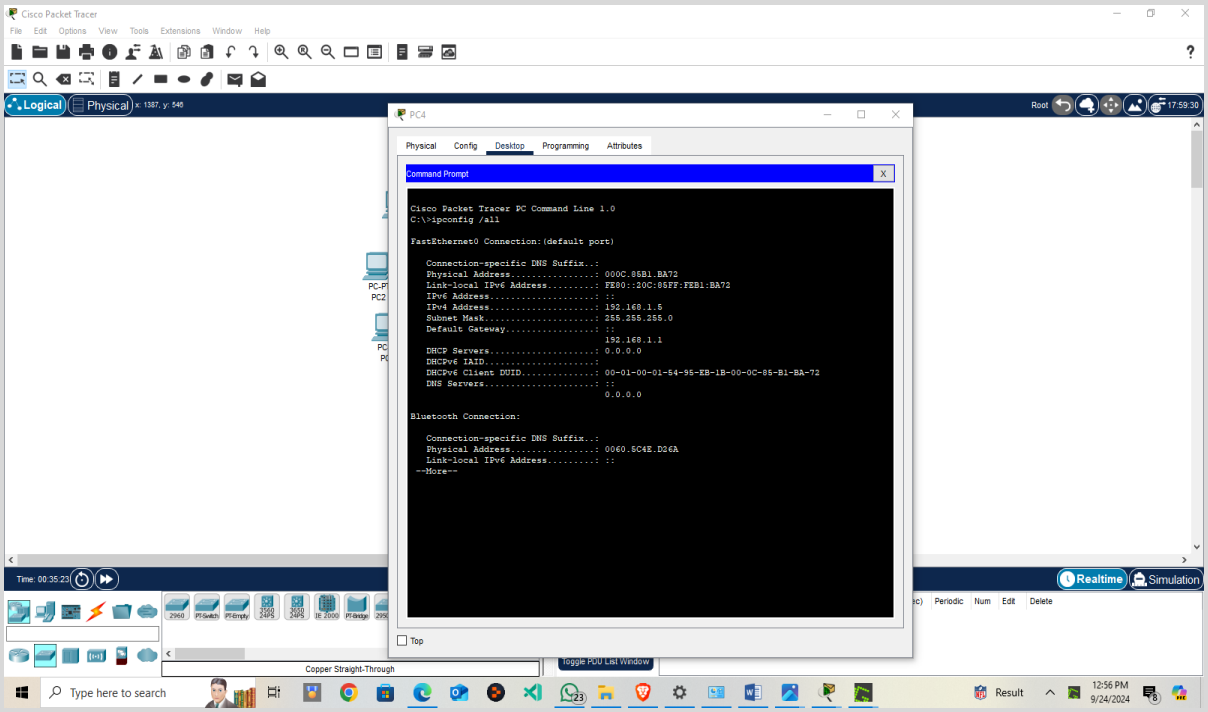
The list of each pcs mac address



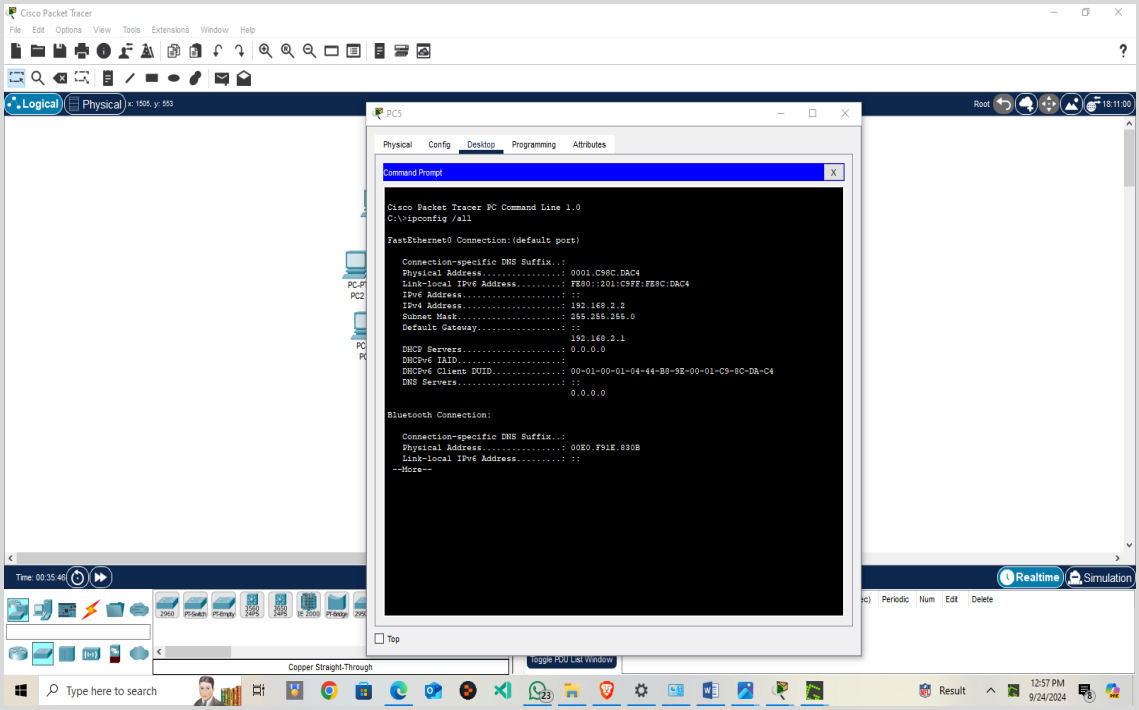


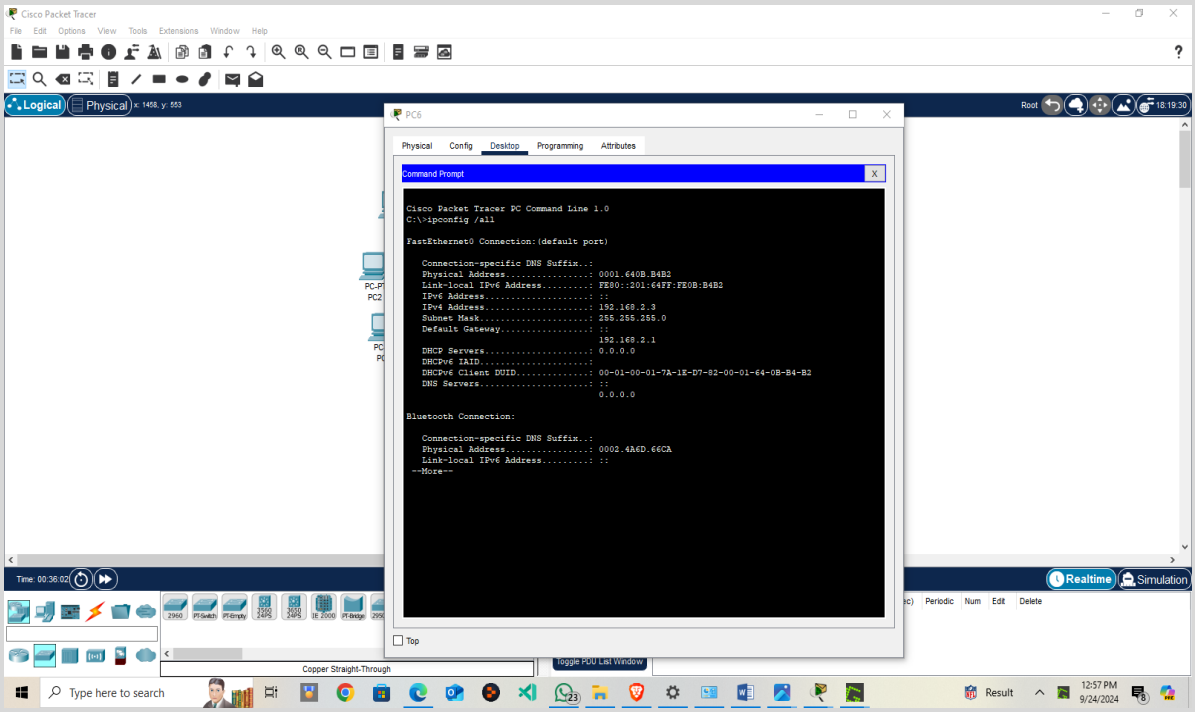
P15/145186/2022

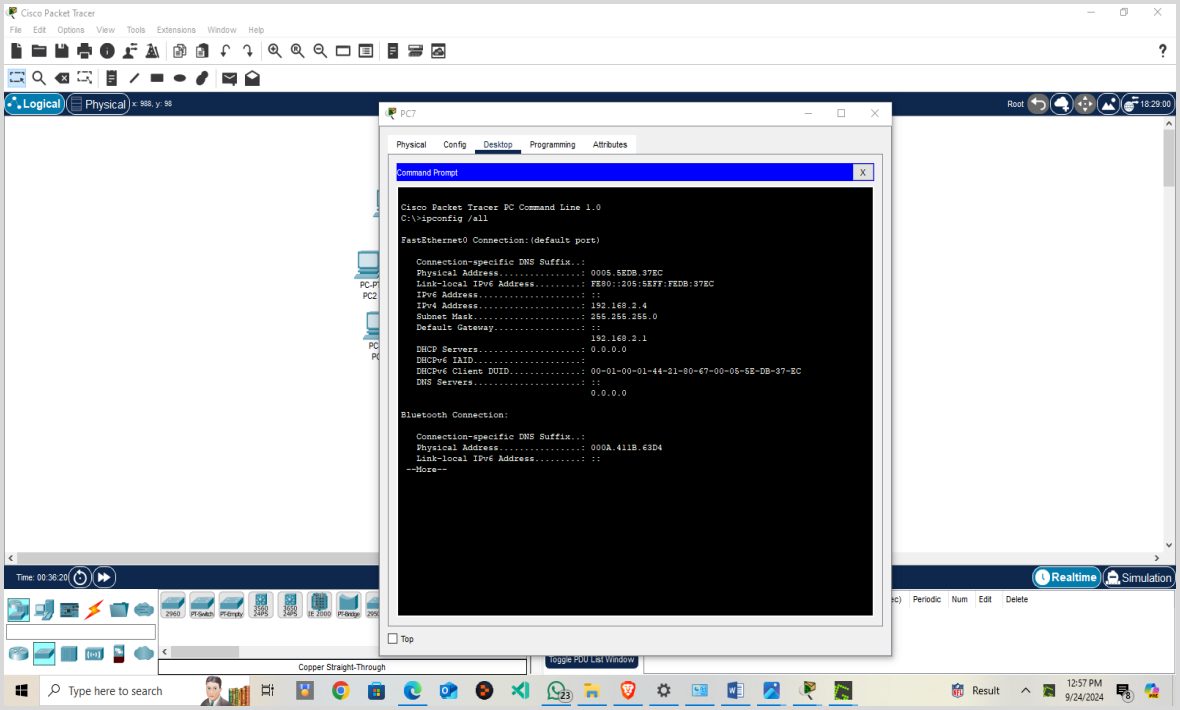


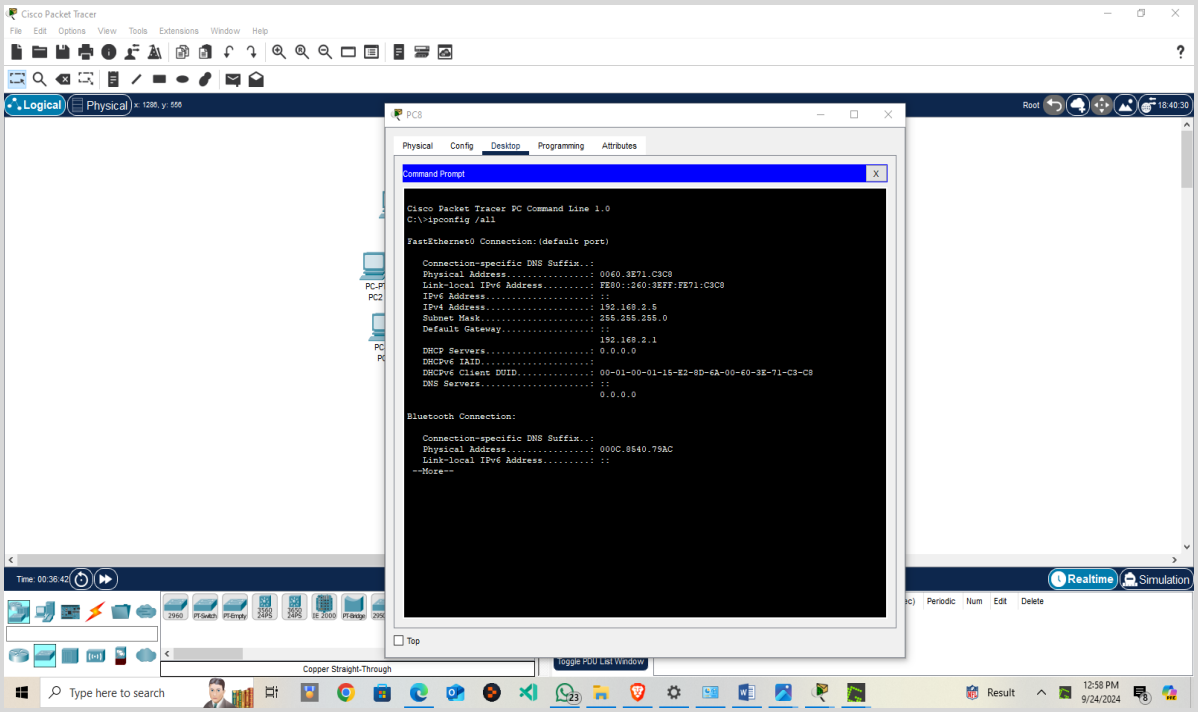


P15/145186/2022









- Create the two VLANs.
    - Explain the configurations you made on the switch to achieve the desired goal.

Configure the Switch:

- Click on the Cisco 2960 switch and enter the **CLI**.

  Enter global configuration mode:

```
Switch> enable
Switch# configure terminal
```

-

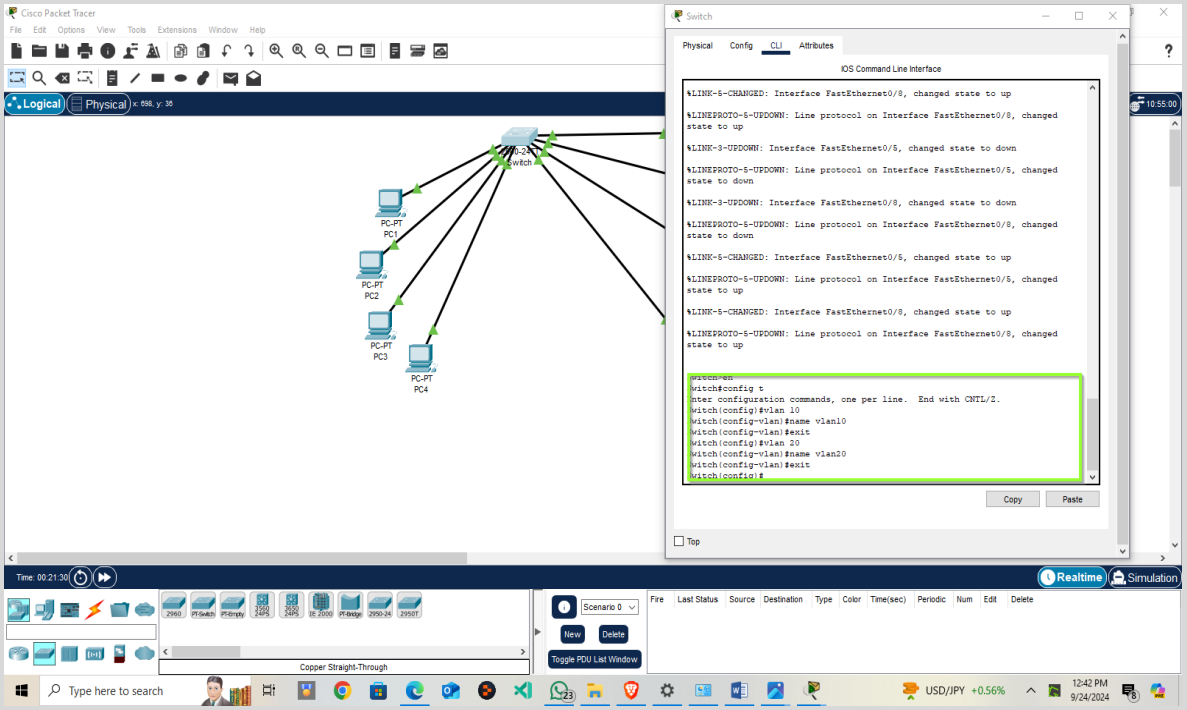
  Create VLANs:

  Create VLAN 10 and VLAN 20:

```
Switch(config)# vlan 10
Switch(config-vlan)# name VLAN10
Switch(config-vlan)# exit
Switch(config)# vlan 20
Switch(config-vlan)# name VLAN20
```

  - `Switch(config-vlan)# exit`

P15/145186/2022



:

- **Assign Switch Ports to VLANs**

  Assign ports **Fa0/1 to Fa0/4** to **VLAN 10** (PC1 to PC4):

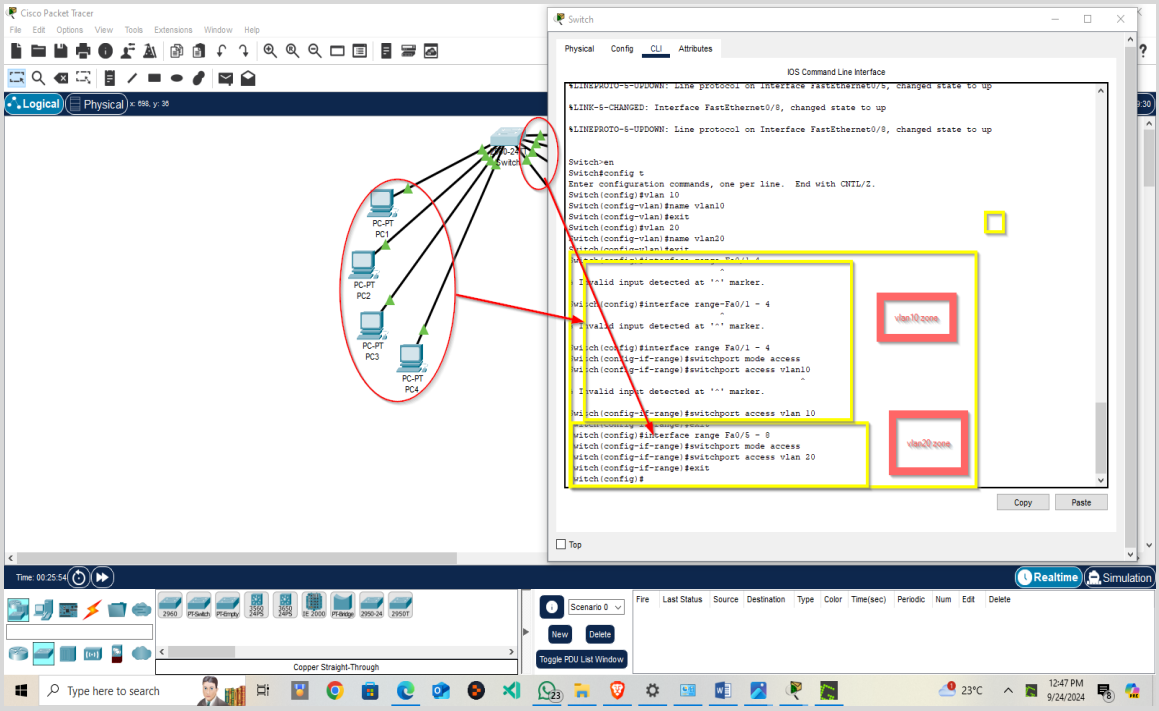
```
Switch(config)# interface range Fa0/1 - 4
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# exit
```

-

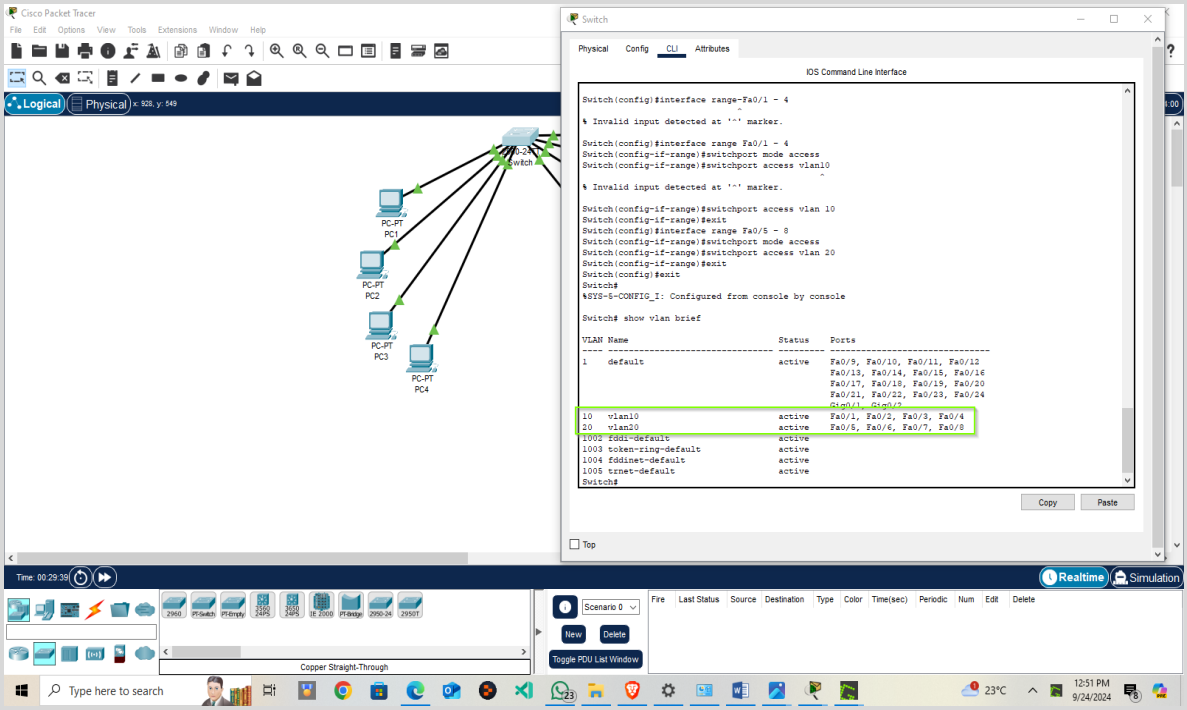
Assign ports **Fa0/5 to Fa0/8** to **VLAN 20** (PC5 to PC8):

```
Switch(config)# interface range Fa0/5 - 8
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 20
```

- `Switch(config-if-range)# exit`



Verify VLAN Configuration:



- Are you creating VLAN membership by (i) port grouping or(ii) MAC address grouping? Explain!

  I used port grouping ,as seen above screenshots;

- **Ports Fa0/1 to Fa0/4** are assigned to **VLAN 10**, which means that all devices connected to these ports (PC1 to PC4) will be part of VLAN 10.
- **Ports Fa0/5 to Fa0/8** are assigned to **VLAN 20**, meaning devices connected to these ports (PC5 to PC8) will be part of VLAN 20.

- **Show** the VLANs created (use show vlan command) on the switch and the ports configured to be in each VLAN. (video)
- Video
- https://drive.google.com/file/d/1VtCY4MIfj-DSnQ9w1PMvmoA0_Eh5CBEf/view?usp=sharing

- Using real time simulation, demonstrate the following. In each case trace the flow of frames from source to destination.

    - Unicast frame from PC 1 to PC 3

      . Unicast Frame from PC1 to PC3 (Both in VLAN 10):

      - **PC1 (192.168.1.2)** is sending a unicast frame to **PC3 (192.168.1.4)**, both in the same VLAN.

        `ping 192.168.1.4`

        Video

        https://drive.google.com/file/d/11vptVDYzvH030GQWRutaZ25-RJeVGrhf/view?usp=sharing

    - Unicast Frame from PC 5 to PC7

      Unicast Frame from PC5 to PC7 (Both in VLAN 20):

- **PC5 (192.168.2.2)** sends a unicast frame to **PC7 (192.168.2.4)**, both in VLAN 20.

  `ping 192.168.2.4`

Video

https://drive.google.com/file/d/1HVAtNJ4zRAsfm4InhI-bug4GkvCpBHZI/view?usp=sharing

- Broadcast message from PC2

. Broadcast Message from PC2 (Within VLAN 10):

- **PC2 (192.168.1.3)** sends a broadcast message within VLAN 10.

```
ping 192.168.1.255
```

Video
https://drive.google.com/file/d/16k3OaxtbnalmSnkbgLWeOVCioC6VFUpr/view?usp=sharing

- Broadcast frame from PC6

Broadcast Frame from PC6 (Within VLAN 20):

- **PC6 (192.168.2.3)** sends a broadcast frame within VLAN 20.

```
ping 192.168.2.255
```

Video

https://drive.google.com/file/d/1_QSfHivtznrdKcxCMjrq2fpGcLgldEPS/view?usp=sharing

- Unicast frame from PC1 to PC5

Unicast Frame from PC1 to PC5 (Different VLANs):

- **PC1 (192.168.1.2)** sends a unicast frame to **PC5 (192.168.2.2)**, which are in **different VLANs** (VLAN 10 and VLAN 20).

```
ping 192.168.2.2
```

Video
https://drive.google.com/file/d/1v3sPko2dGX6puUq8-lC3N_sTeFY3ei4_/view?usp=sharing

- Is it possible to have frame transmission (Unicast, broadcast) within a VLAN. Explain!

Yes, it is possible to have both **unicast** and **broadcast** frame transmission within a VLAN. VLANs operate at **Layer 2** (Data Link Layer) of the OSI model and can transmit various types of traffic, including unicast, broadcast, and multicast frames, just like traditional LANs. Here's an explanation of how unicast and broadcast traffic works within a VLAN:

1. Unicast Frame Transmission within a VLAN

- **Unicast communication** within a VLAN is a one-to-one form of communication. It occurs when a frame is sent from one device to another specific device within the same VLAN.
- **How it works in a VLAN**:
  - **Source and destination devices**: The source device sends a frame directly to a destination device using its **port address**.in ourr case using ip addresses
  - **Switch behavior**:
    - When the switch receives the unicast frame, it checks its **MAC address table** to determine the port associated with the destination MAC address.
    - The frame is then forwarded only to the specific port where the destination device is connected.
  - **VLAN isolation**: The unicast traffic is confined to devices within the same VLAN. Devices in other VLANs cannot receive or forward the traffic unless inter-VLAN routing is configured.

P15/145186/2022

- Is it possible to have frame transmission (Unicast, broadcast) between different VLANs?Explain!

No, it is **not possible** to have frame transmission (either **unicast** or **broadcast**) between different VLANs on a **Layer 2 switch alone**.

Explanation:

A **Layer 2 switch** operates at the Data Link Layer of the OSI model, which means it handles switching and forwarding of frames based on **MAC addresses**. It does **not perform routing** or any kind of IP-based decision-making. Here's how frame transmission works for both unicast and broadcast traffic:

1. Unicast Transmission Between Different VLANs

- **Unicast transmission** is one-to-one communication between two specific devices.
- On a Layer 2 switch, devices in different VLANs are isolated from each other. Even if they are connected to the same switch, they cannot communicate with each other unless they are in the same VLAN.
-

Broadcast Transmission Between Different VLANs

- **Broadcast transmission** is when a frame is sent to all devices within the same broadcast domain (VLAN).

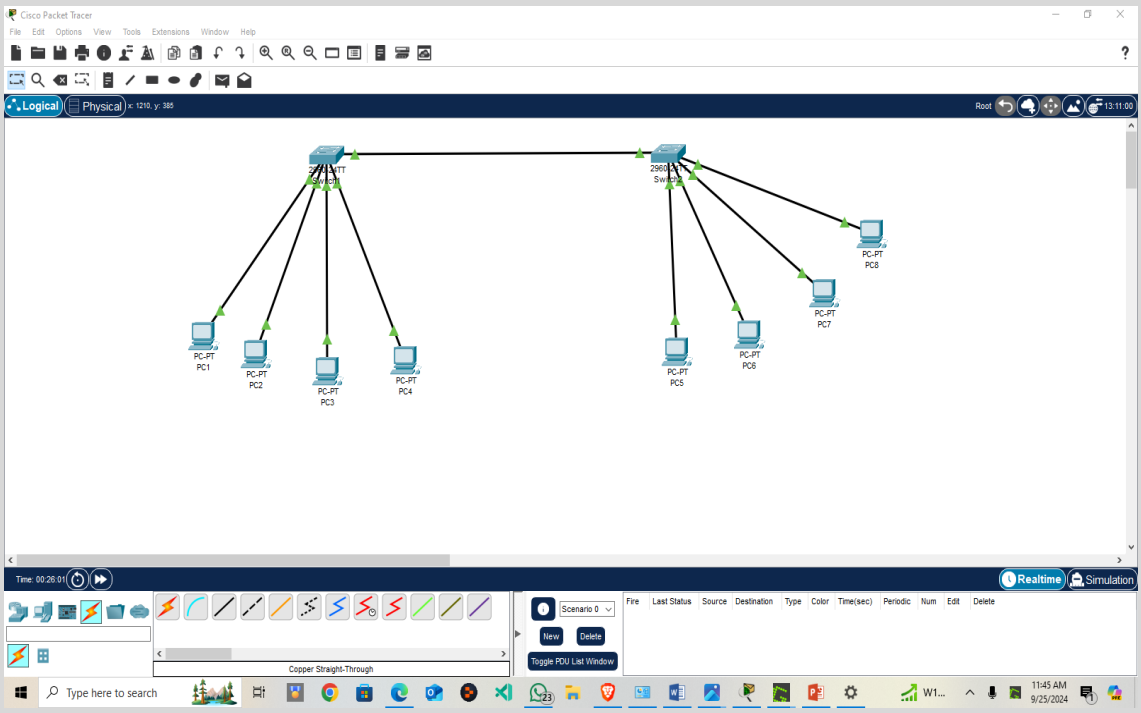
(b) A Fast Ethernet switched LAN based on two switches (SW1 and SW2) is created. Two VLANs, VLAN 10 and VLAN 20 are created with **each** VLAN **spanning** the two switches. VLAN 10 has four PCs (PC1 to PC4 and PC5 to PC8 respectively). Each VLAN has the first two hosts on switch1 and the last two hosts on switch 2. The two switches are mirror images of each other as each switch connects the two PCs on ports Fa0/2 and Fa0/3 respectively. VLAN 10 is mapped to netID 192.168.1.0/24 while VLAN 20 is mapped to NetID 192.168.2.0/24.

- Using Packet tracer, create the network topology described above- with two switches and 8 PCs (PC1 to PC8). T his switched LANshould be based on the cisco 2960 switch
- **Add Two Cisco 2960 Switches (SW1 and SW2)** to the workspace.
- **Add Eight PCs** (PC1 to PC8).
- **Connect PCs to Switches:**
    - PC1 and PC2 connect to SW1 on ports Fa0/2 and Fa0/3, respectively.
    - PC3 and PC4 connect to SW1 on ports Fa0/4 and Fa0/5, respectively.

- PC5 and PC6 connect to SW2 on ports Fa0/2 and Fa0/3, respectively.
- PC7 and PC8 connect to SW2 on ports Fa0/4 and Fa0/5, respectively.

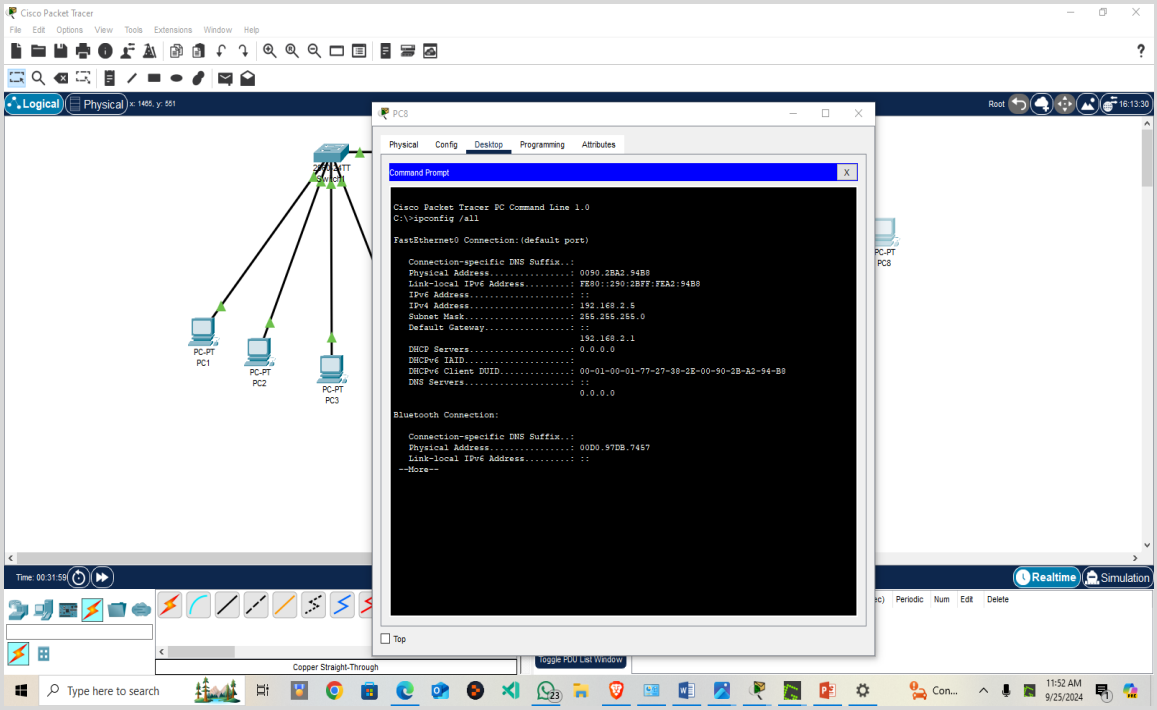
2. Configure IP Addresses for PCs

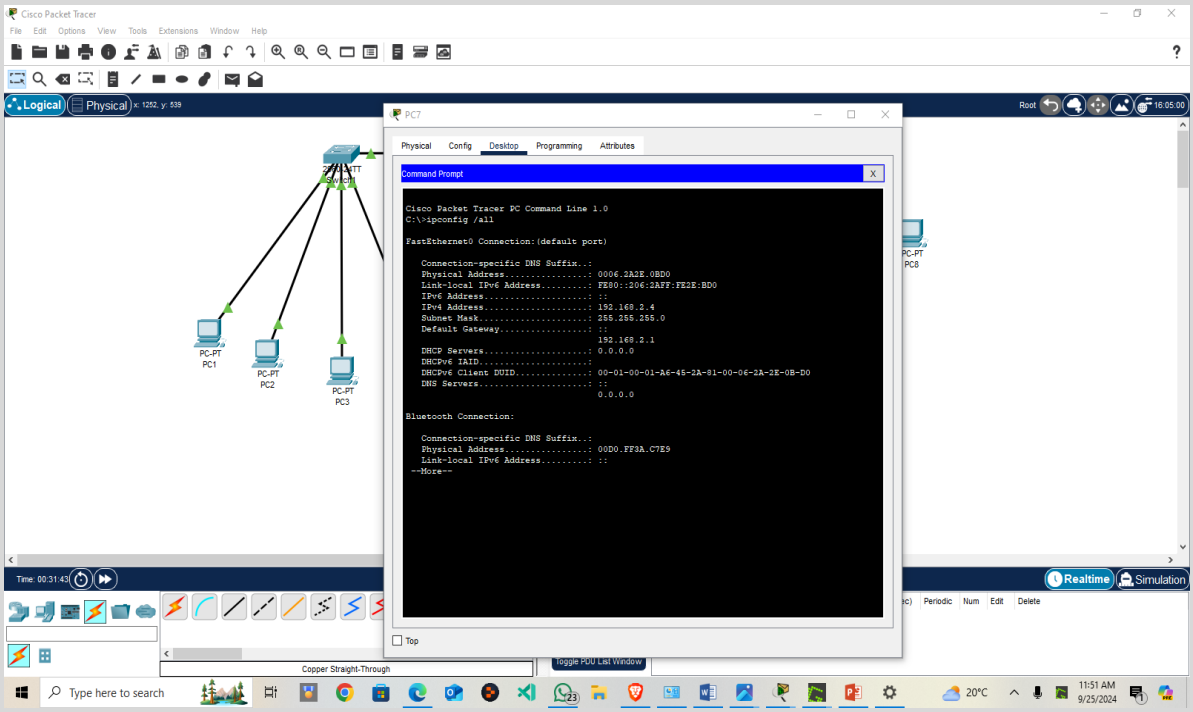
- Assign IP addresses to PCs based on the VLAN they belong to.
- For **VLAN 10** (Network ID 192.168.1.0/24):
  - PC1: 192.168.1.2 /24
  - PC2: 192.168.1.3 /24
  - PC3: 192.168.1.4 /24
  - PC4: 192.168.1.5 /24
- For **VLAN 20** (Network ID 192.168.2.0/24):
  - PC5: 192.168.2.2 /24
  - PC6: 192.168.2.3 /24
  - PC7: 192.168.2.4 /24
  - PC8: 192.168.2.5 /24
  -



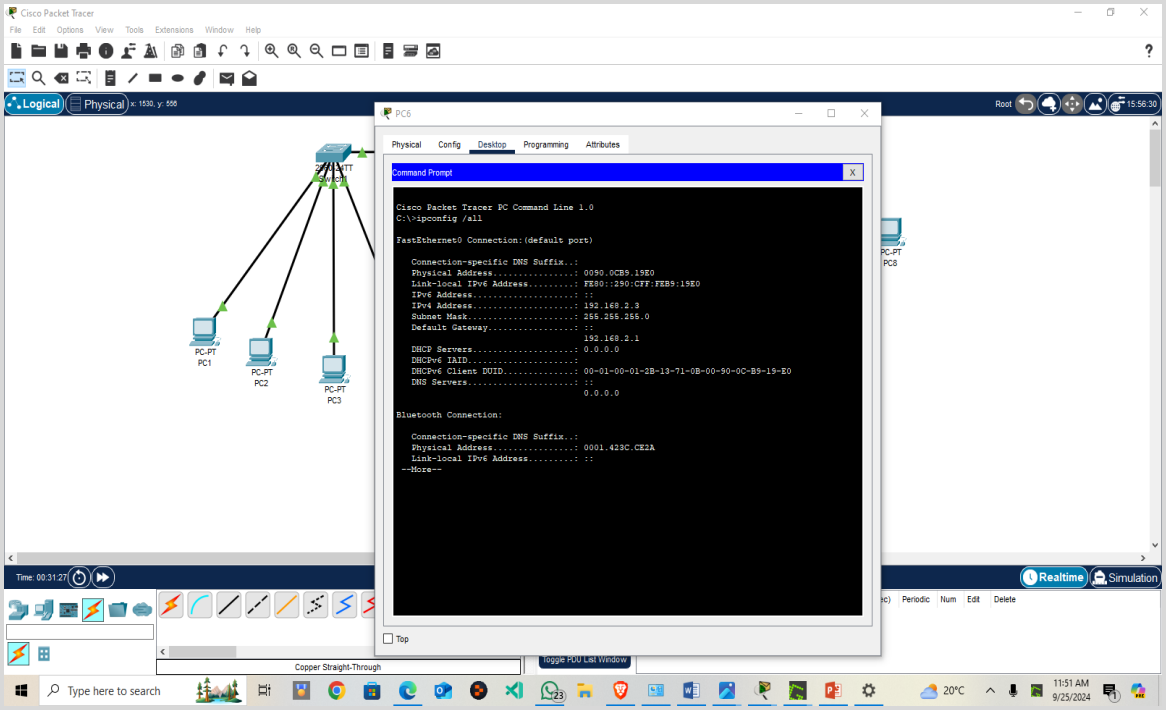
- List the MAC addresses of the 8 PCs in your network

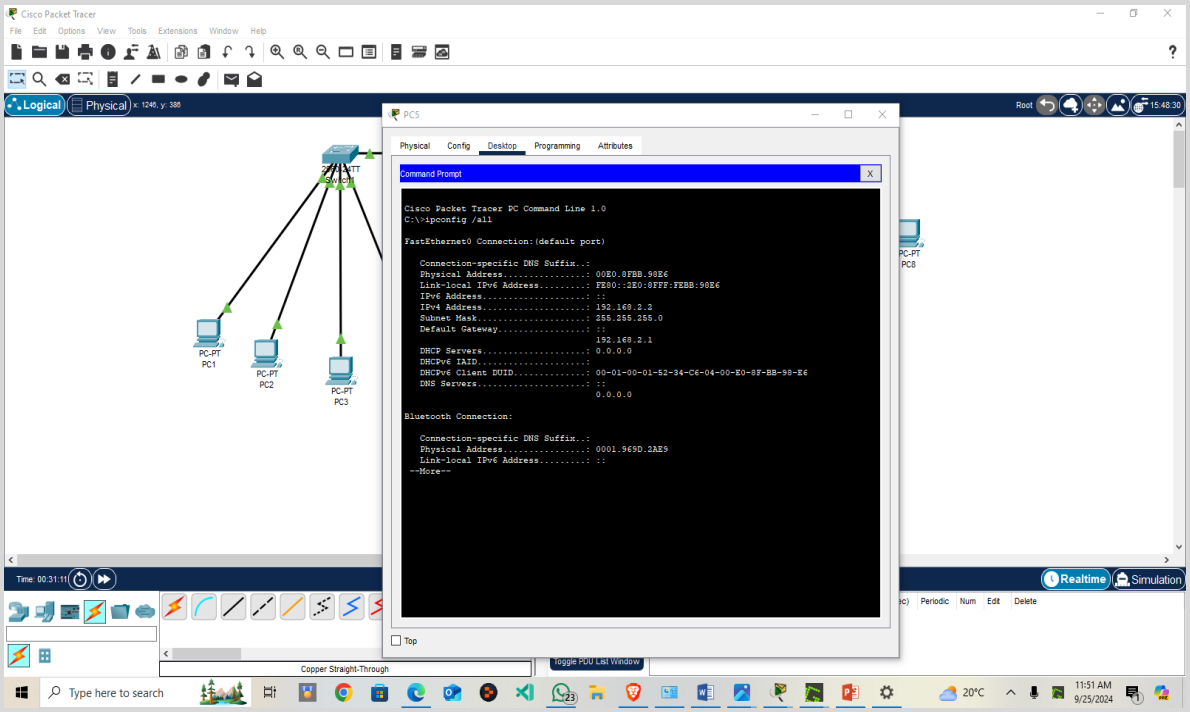
P15/145186/2022



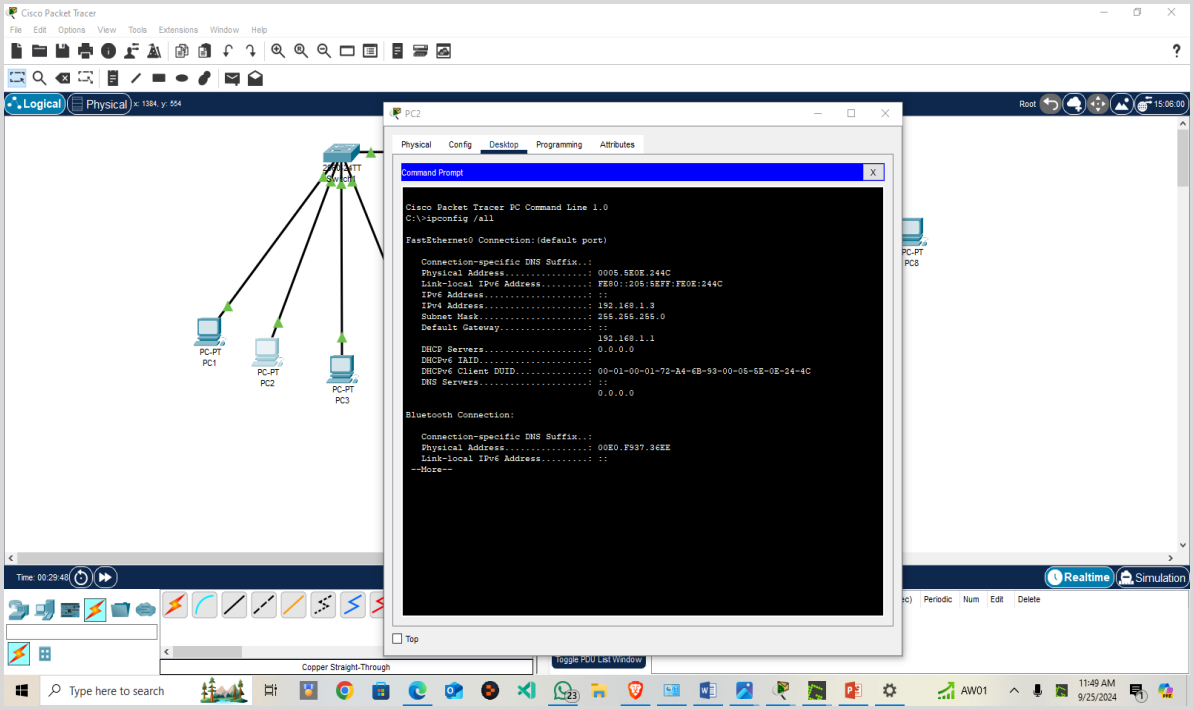


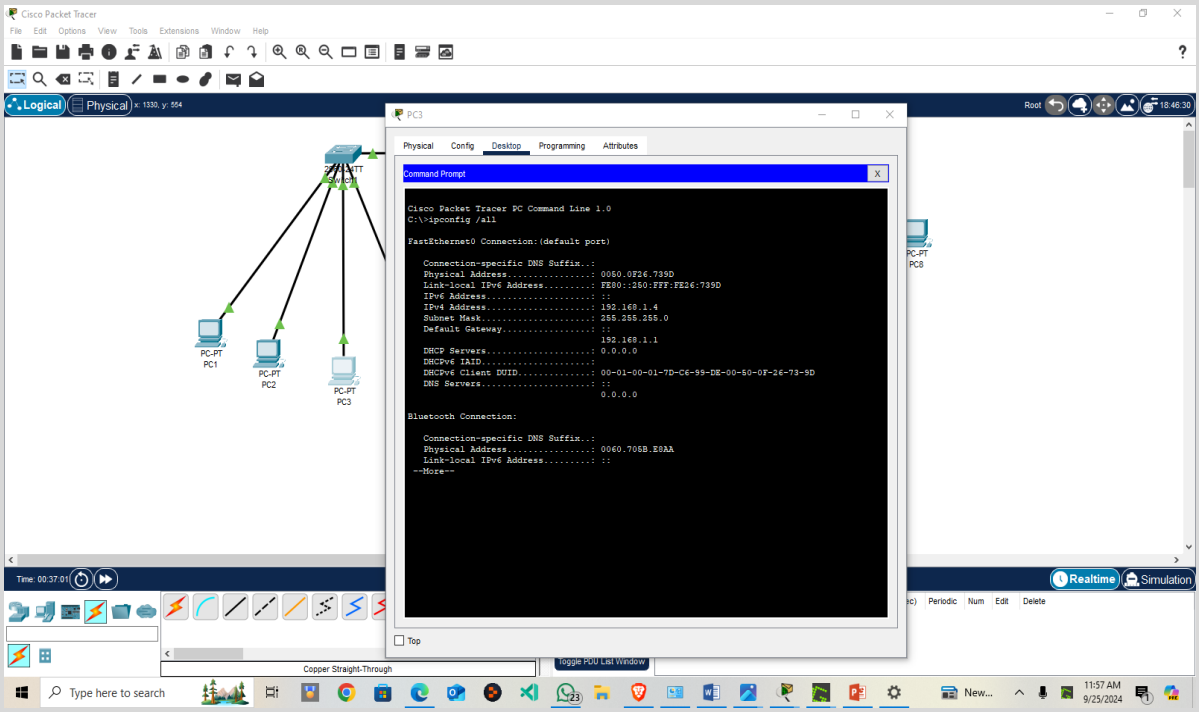
P15/145186/2022

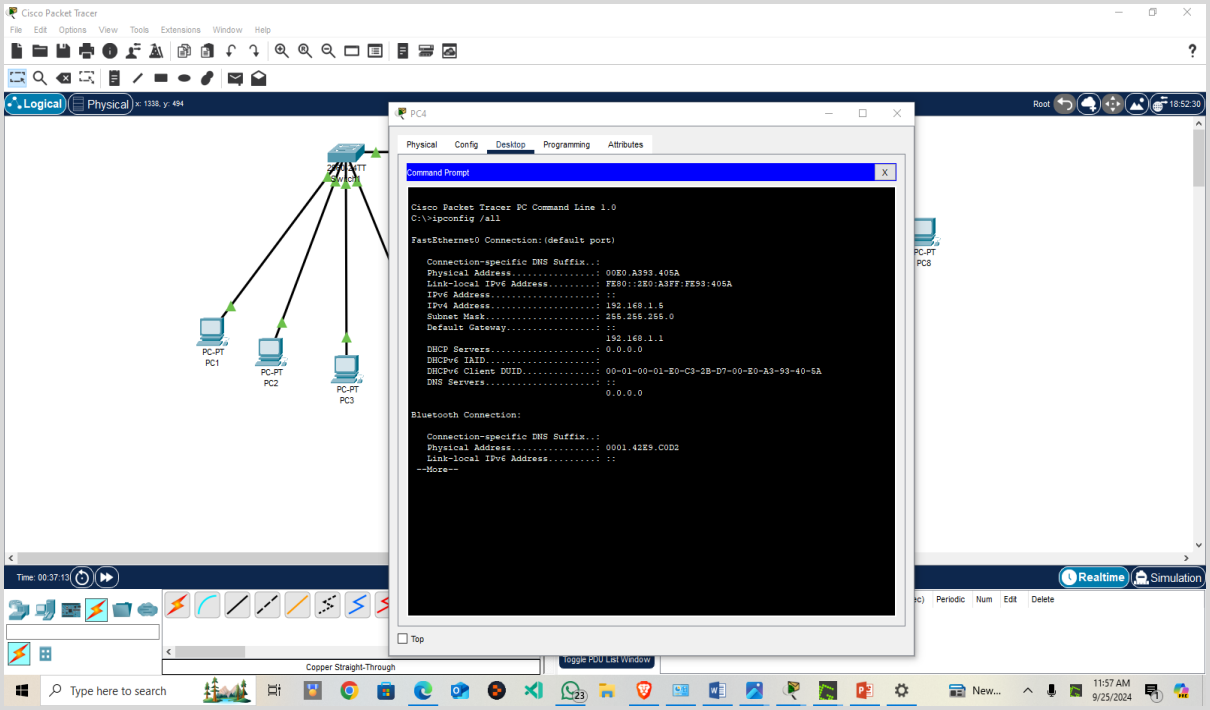


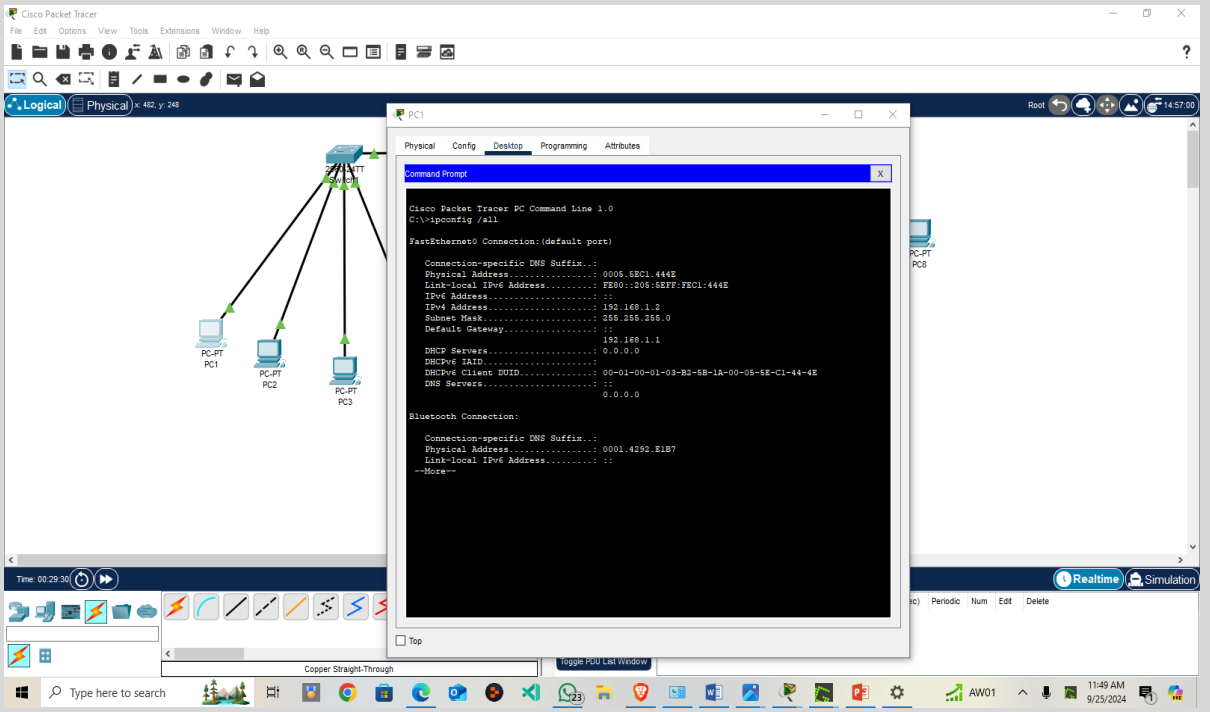


P15/145186/2022









- Create the two VLANs.
    - Explain the configurations you made on each switch to achieve the desired goal.

Create VLANs on Switches

- **On Switch 1 (SW1):**

  Enter the switch CLI, then enter global configuration mode:

```
Switch> enable
Switch# configure terminal
```

  -

  Create VLAN 10 and VLAN 20

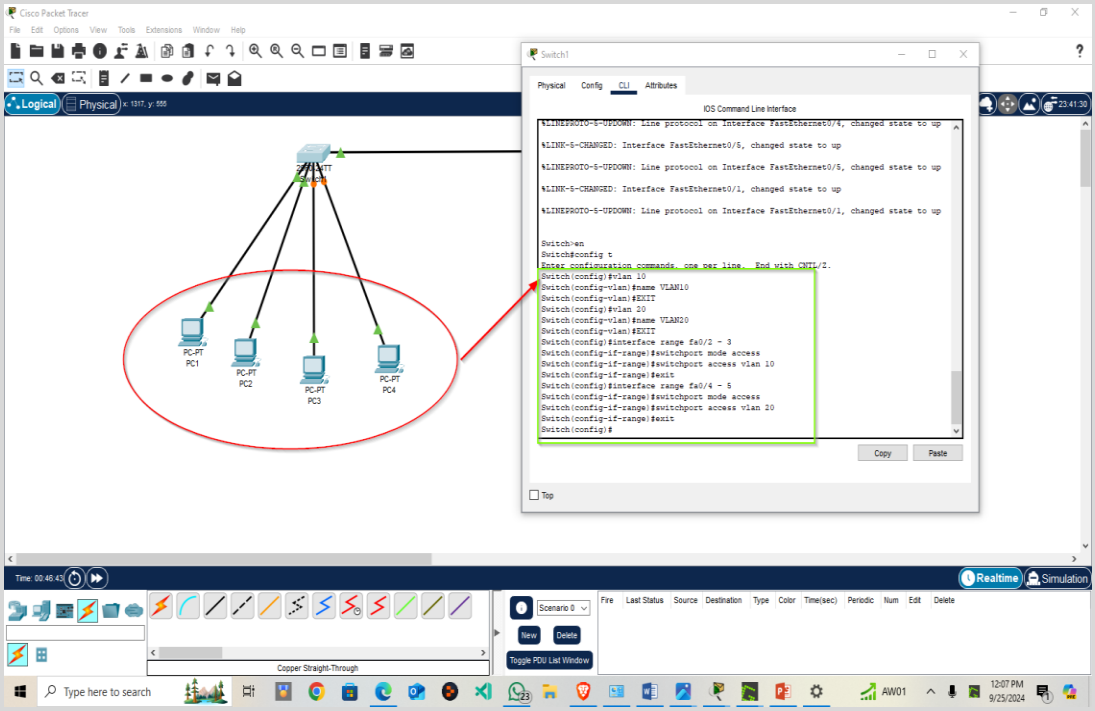
```
Switch(config)# vlan 10
Switch(config-vlan)# name VLAN10
Switch(config-vlan)# vlan 20
Switch(config-vlan)# name VLAN20
```

  -

  Assign VLANs to ports:

```
Switch(config)# interface range fa0/2 - 3
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config)# interface range fa0/4 - 5
Switch(config-if-range)# switchport mode access
```

  - `Switch(config-if-range)# switchport access vlan 20`



On Switch 2 (SW2):

- create VLAN 10 and VLAN 20.

```
Switch> enable
Switch# configure terminal
```

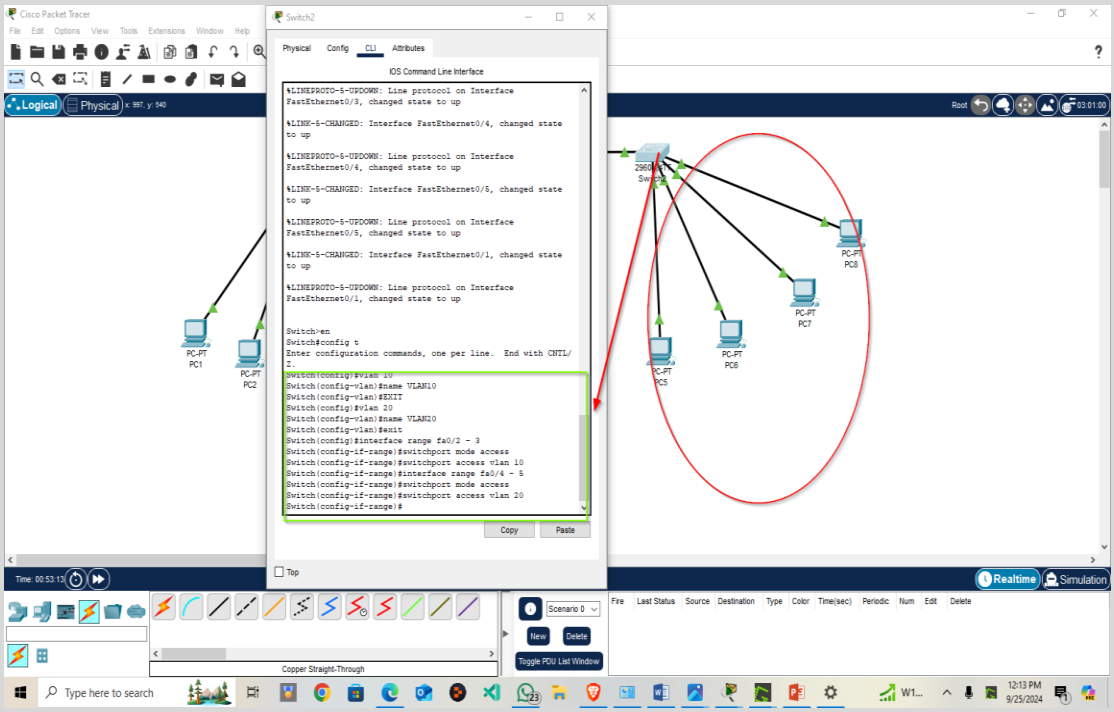
Create VLAN 10 and VLAN 20:

```
Switch(config)# vlan 10
Switch(config-vlan)# name VLAN10
Switch(config-vlan)# vlan 20
Switch(config-vlan)# name VLAN20
```

Assign the ports as follows:

```
Switch(config)# interface range fa0/2 - 3
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config)# interface range fa0/4 - 5
Switch(config-if-range)# switchport mode access
```

- `Switch(config-if-range)# switchport access vlan 20`



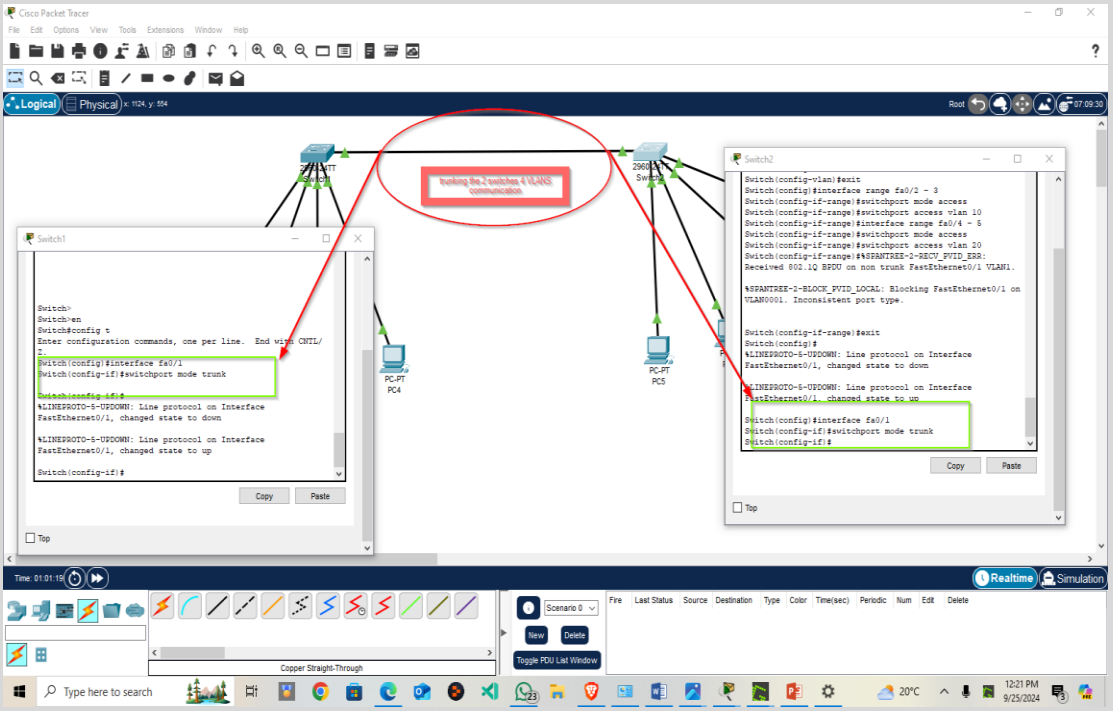
. Trunk Link Between SW1 and SW2

- To allow VLANs to span across both switches, you need to configure a trunk link:
  - Use an available port on each switch (e.g., Fa0/1) to connect the switches.

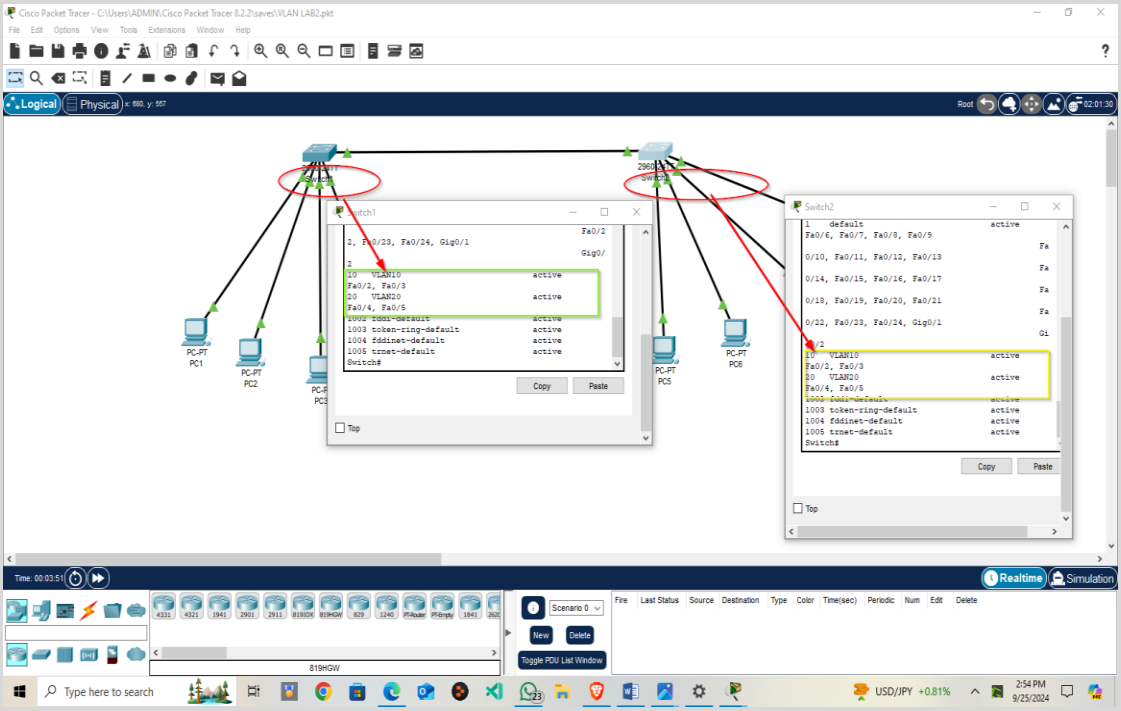
Configure the trunk:

Switch(config)# interface fa0/1

- Switch(config-if)# switchport mode trunk
- The cli must be applied to **both switches** to enable VLAN traffic to pass between them
- **NB: we are doing spanning VLANs across switches.,but strictly not "(Inter-VLAN Communication which Requires Layer 3 Routing)"**



- **Show** the VLANs created on each switch (use show vlan command) on each switch and the ports configured to be in each VLAN. (video)
- Video
- https://drive.google.com/file/d/1uJEUzycM2p3pwTZSFgIkrCWPzdQP-1mz/view?usp=sharing



- Using real time simulation, demonstrate the following. In each case trace the flow of frames from source to destination.
    - Unicast frame from PC 1 to PC 3

      From **PC1 (192.168.1.2)**, try to ping **PC3 (192.168.1.4)**

      ```
      ping 192.168.1.4
      ```

      ```
      This must fail, because both are in different vlans,vlans isolate traffics.
      ```

      Video

      https://drive.google.com/file/d/1IUL1xdyS3-59dIUGYmzSs6WvsVT4I1jQ/view?usp=sharing

    - Unicast Frame from PC 5 to PC7

      PC5 (192.168.1.6) is in **VLAN 10** and **PC7 (192.168.2.4)** is in **VLAN 20, ping 192.168.2.4**

      Video

https://drive.google.com/file/d/1m_yLy6eCBYaLi_Mo5KRFnCekw6IahQnD/view?usp=sharing

- Broadcast message from PC2

- **PC2 (192.168.1.3)** is in **VLAN 10**.
- The broadcast address for VLAN 10 (192.168.1.0/24) is **192.168.1.255**.

```
ping 192.168.1.255
```

- Broadcast frame from PC6

- **PC6 (192.168.2.1)** is in **VLAN 20**.
- The broadcast address for VLAN 20 (192.168.2.0/24) is **192.168.2.255**.

```
ping 192.168.2.255
```

- Unicast frame from PC1 to PC5

  Both **PC1 (192.168.1.2)** and **PC5 (192.168.1.6)** are in **VLAN 10**.

  ping 192.168.1.6

  Video

  https://drive.google.com/file/d/1E94265b0VAQh0TOTzh9fbfXk1MdE1wo2/view?usp=sharing

- Is it possible to have frame transmission (Unicast, broadcast) within a VLAN. Explain!

Yes, it is possible to have both **unicast** and **broadcast** frame transmission within a VLAN. VLANs operate at **Layer 2** (Data Link Layer) of the OSI model and can transmit various types of traffic, including unicast, broadcast, and multicast frames, just like traditional LANs. Here's an explanation of how unicast and broadcast traffic works within a VLAN:

1. Unicast Frame Transmission within a VLAN

- **Unicast communication** within a VLAN is a one-to-one form of communication. It occurs when a frame is sent from one device to another specific device within the same VLAN.
- **How it works in a VLAN**:
  - **Source and destination devices**: The source device sends a frame directly to a destination device using its **port address**.in ourr case using ip addresses
  - **Switch behavior**:
    - When the switch receives the unicast frame, it checks its **MAC address table** to determine the port associated with the destination MAC address.
    - The frame is then forwarded only to the specific port where the destination device is connected.
  - **VLAN isolation**: The unicast traffic is confined to devices within the same VLAN. Devices in other VLANs cannot receive or forward the traffic unless inter-VLAN routing is configured.
- Is it possible to have frame transmission (Unicast, broadcast) between different VLANs?Explain!

No, it is **not possible** to have frame transmission (either **unicast** or **broadcast**) between different VLANs on a **Layer 2 switch alone**.

Explanation:

A **Layer 2 switch** operates at the Data Link Layer of the OSI model, which means it handles switching and forwarding of frames based on **MAC addresses**. It does **not perform routing** or any kind of IP-based decision-making. Here's how frame transmission works for both unicast and broadcast traffic:

1. Unicast Transmission Between Different VLANs

- **Unicast transmission** is one-to-one communication between two specific devices.
- On a Layer 2 switch, devices in different VLANs are isolated from each other. Even if they are connected to the same switch, they cannot communicate with each other unless they are in the same VLAN.
-

Broadcast Transmission Between Different VLANs

- **Broadcast transmission** is when a frame is sent to all devices within the same broadcast domain (VLAN).

P15/145186/2022

Part 1 Summary:

- **VLAN Definition:** VLANs are virtual local area networks that logically segment a physical network into separate broadcast domains.
- **Purpose of VLANs:** Developed to enhance network performance, scalability, flexibility, and security by reducing broadcast traffic and logically segmenting networks.
- **VLAN and Broadcast Domain:** Each VLAN functions as its own broadcast domain, with traffic limited to the devices within that VLAN, typically mapping each VLAN to its own IP subnet.
- **Access and Trunk Links:**
    - **Access Links**: Connect a switch to an end device and carry traffic for only one VLAN.
    - **Trunk Links**: Carry traffic for multiple VLANs between switches or between switches and routers.
- **Configuration of VLANs in Packet Tracer:**
    - **VLAN 10** and **VLAN 20** were created, with devices assigned to the respective VLANs through specific port groupings. No MAC address-based grouping was used.
    - You successfully demonstrated **unicast** and **broadcast** traffic within the same VLAN, and the inability for devices in different VLANs to communicate directly without Layer 3 routing.

Part 2 Summary:

In Part 2, you extended the setup across two switches:

1. **Two Cisco 2960 Switches** were configured with VLAN 10 and VLAN 20 spanning both switches. The PCs on **SW1** and **SW2** were connected across the ports as described, and the VLANs were successfully created and verified.
2. **Trunk Link Configuration:** A trunk link between SW1 and SW2 was set up using port Fa0/1 on both switches, allowing VLAN traffic to pass between the switches.
3. **IP Addressing:** IP addresses for each PC were configured based on the respective VLAN subnet mappings.
4. **Frame Flow Simulations:**
    - **Unicast** communication between PCs within the same VLAN was shown to work correctly.
    - Communication between VLANs (e.g., PC1 in VLAN 10 and PC5 in VLAN 20) was blocked, as expected, without Layer 3 routing.