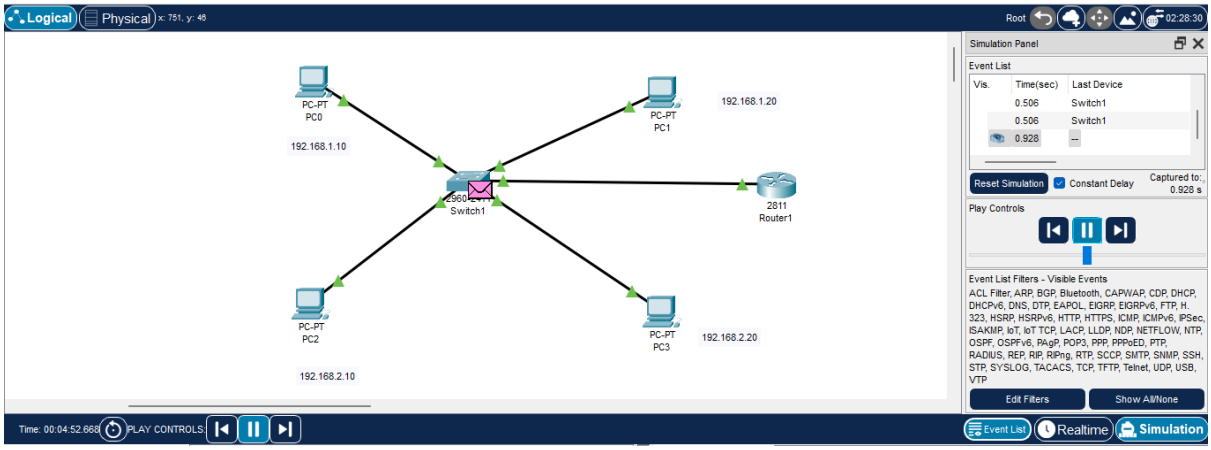
Q5. Change the native VLAN on a trunk port. Test for VLAN mismatches and troubleshoot.

**Network Setup:**




**Native VLAN:**

A Native VLAN is the default VLAN assigned to an untagged frame on a trunk port in an 802.1Q VLAN network. Unlike other VLANs, which carry tagged traffic, the native VLAN does not add a VLAN tag to the frames.By default, VLAN 1 is the native VLAN on Cisco switches, but it can be changed for security reasons.

**Uses of a Native VLAN**

**Handling Untagged Traffic on a Trunk**

- If a switch receives an **untagged Ethernet frame** on a trunk port, it assumes the frame belongs to the **native VLAN**.
- This allows devices that **do not support VLAN tagging** (e.g., some VoIP phones, older network devices) to communicate in a VLAN environment.

**Backward Compatibility with Legacy Devices**

- Some older devices or unmanaged switches **do not support VLAN tagging**. The **native VLAN** ensures these devices can still communicate over the network.

**Reducing Processing Overhead**

- Since native VLAN traffic is **untagged**, there is no need for additional VLAN tagging and processing, reducing the load on networking hardware.

**Interoperability Between Different Vendors**

- Different network vendors use different VLAN tagging mechanisms. The **native VLAN ensures smooth interoperability** between switches from Cisco, HP, Juniper, etc.

```
Switch>show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/5       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/5       1-1005

Port        Vlans allowed and active in management domain
Fa0/5       1,10,20

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/5       1,10,20
```

**When to Change the Native VLAN?**

### To Improve Security (Prevent VLAN Hopping Attacks)

- VLAN **hopping attacks** occur when an attacker exploits the native VLAN to gain unauthorized access to other VLANs.

### To Prevent VLAN Mismatches

- If two connected switches have **different native VLANs**, a **VLAN mismatch** occurs, leading to connectivity issues and spanning-tree errors.

### To Separate Management Traffic from Data Traffic

- VLAN 1 is the default VLAN for **management traffic** (e.g., CDP, STP, VTP). Keeping it as the native VLAN exposes the network to attacks.

**Changed Native VLAN:**

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface FastEthernet 0/5
Switch(config-if)#switchport trunk native vlan 100
Switch(config-if)#exit
```

```
Switch#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/5       on           802.1q         trunking      100

Port        Vlans allowed on trunk
Fa0/5       1-1005

Port        Vlans allowed and active in management domain
Fa0/5       1,10,20

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/5       1,10,20

Switch#
```