VLAN ( VIRTUAL LOCAL AREA NETWORK )

1. A VLAN (Virtual Local Area Network) is a logically segmented network that groups devices together, regardless of their physical location, as if they were on the same LAN.
2. VLANs improve network efficiency, security, and manageability by reducing broadcast domains and segregating traffic.
3. Devices in different VLANs cannot communicate directly unless explicitly allowed.
4. Broadcast traffic remains within a VLAN, preventing unnecessary traffic from affecting other VLANs.
5. Reducing the number of devices in a broadcast domain helps optimize network performance.
6. Devices can be grouped based on function, department, or security policies rather than physical location.
7. VLANs operate at Layer 2 (Data Link Layer) of the OSI model.
8. However, inter-VLAN routing requires layer-3 switch or Router-on-a-Stick (RoaS) which has physically only one interface but logically that interface can be segmented as per requirement.
9. It follows 802.1Q standard which defines the way VLAN can be configured in managed switches, routers with vlan tag etc.
10. Access port -> Connection between end hosts and switch . these ports carry untagged traffic since switches takes care of vlan tagging and priority fixing.
11. Trunk port -> connection between switches and switch-router that carries tagged traffic since it takes up multiple vlan traffic across switched networks to associated vlan.
12. Default VLAN -> by default, all switch ports belong to VLAN-1.
13. Native VLAN -> any untagged traffic (like broadcast messages) via trunk port will be assigned with this VLAN tag (by default 99, but advisable to change).
14. Data VLAN -> Used for carrying user-generated.
15. Voice VLAN -> Dedicated VLAN for VoIP traffic to ensure quality of service (QoS).
16. Management VLAN ->Used for network administration and management access.
17. To declare VLAN in switch :

Switch(config)# vlan 10

Switch(config-vlan)# name Sales

Switch(config-vlan)# exit

1. To assign ports to declared VLAN :

Switch(config)# interface fa0/1

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 10

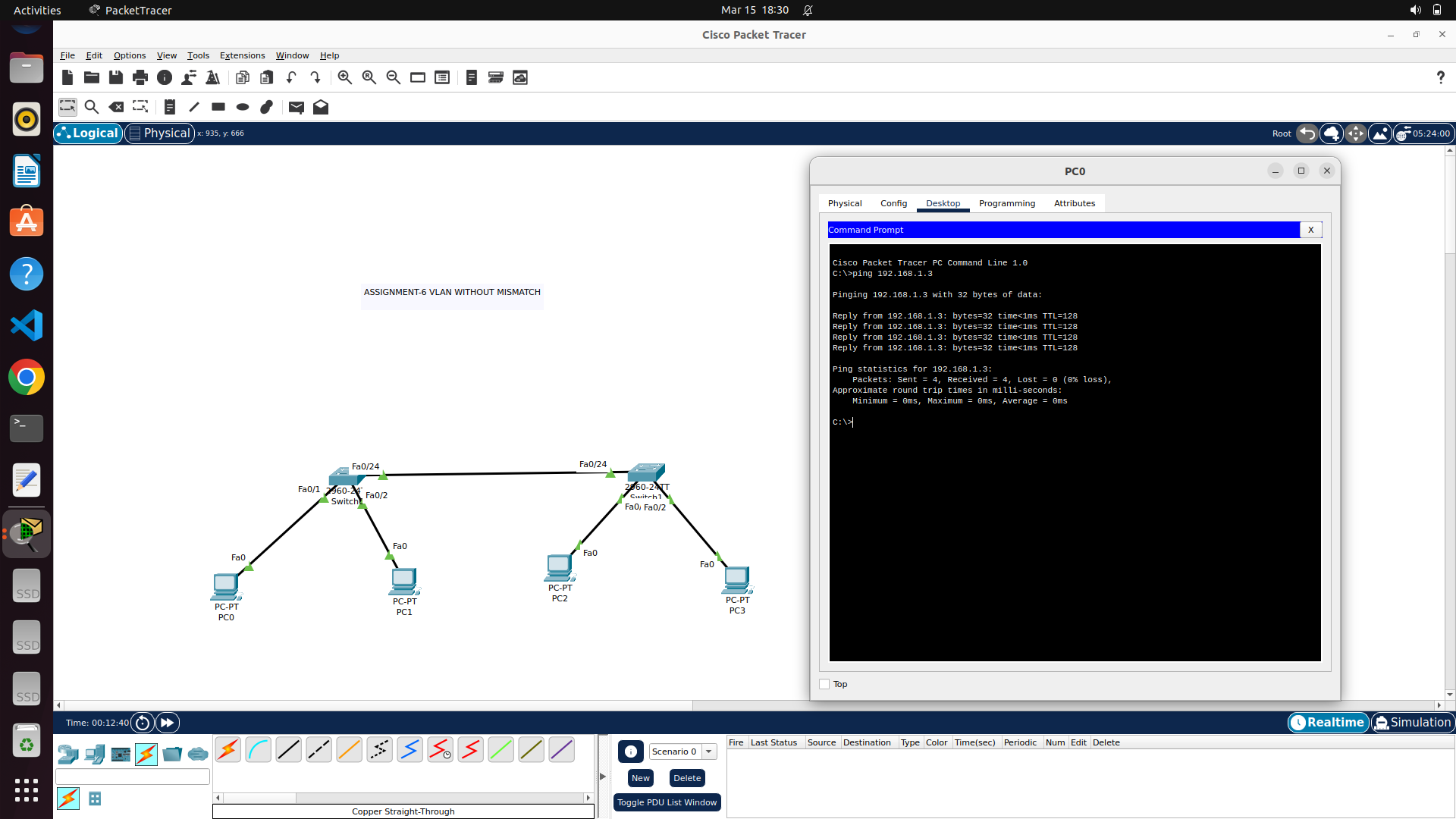
OR

Switch(config-if)# switchport mode trunk <native vlan <vlan number>>

Switch(config-if)# exit

1. If any packet arrives at switch, it checks in its mac table for the destination learnt, if so, it tags and sends out if destination is under other switch. If not so, it just sends to the intended device under same VLAN. If broadcast packets, it will be broadcasted to all same vlan and to trunk port if allowed.

DEMONSTRATION :



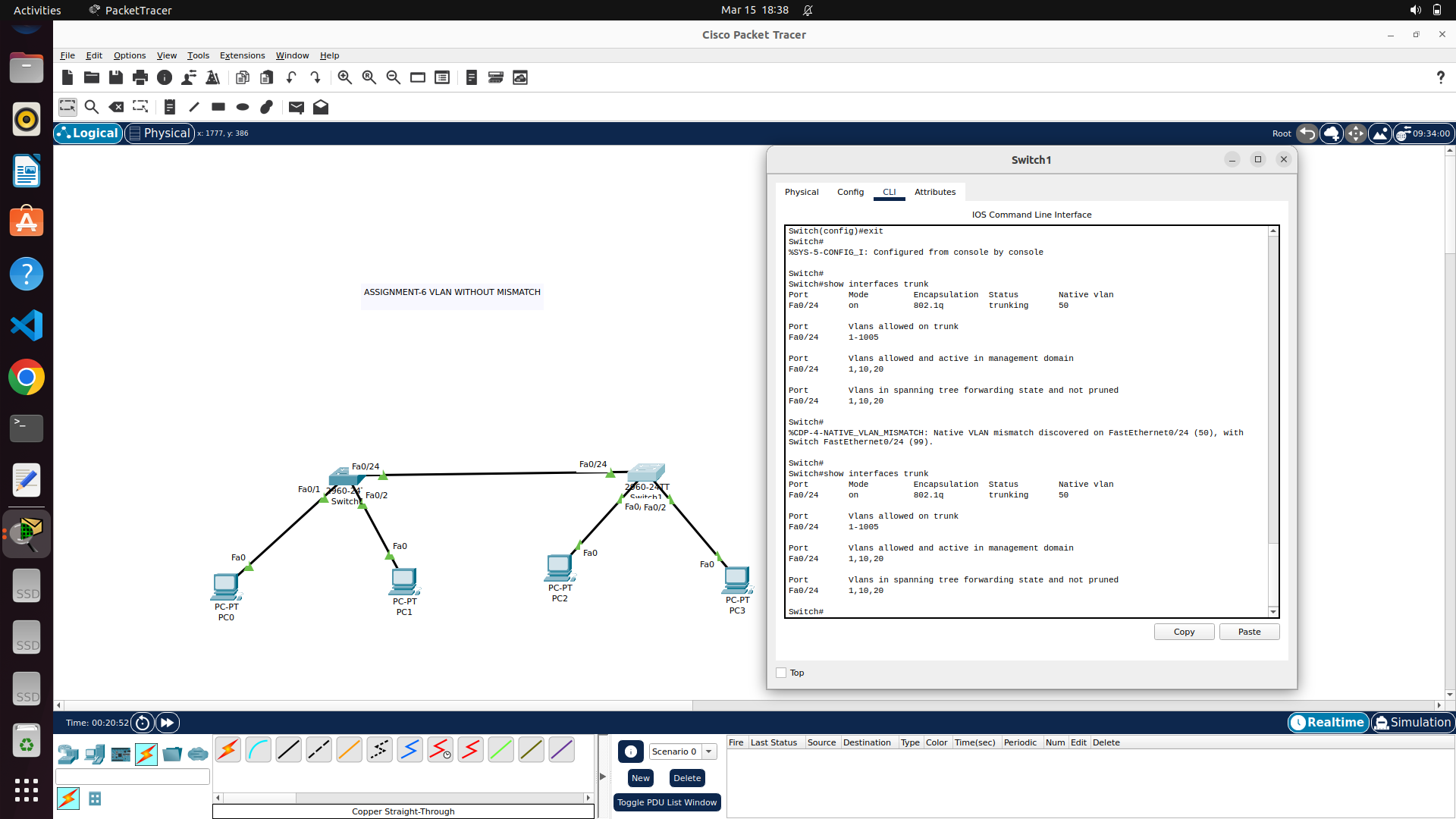
Here, to prove that vlan considers logical segmentation of network regardless of physical location,

PC0 – 192.168.1.2/24

PC1 – 192.168.2.2/24

PC2 – 192.168.1.3/24

PC3 – 192.168.2.3/24 are assigned. Now, naturally it is possible to ping from pc0 to pc2 and from pc1 to pc3 alone. Since, vlan shrinks broadcast domain. Both the interfaces of switches contributing trunk port should have same native vlan to avoid mismatches.



Above, using “switchport mode trunk native vlan <new vlan number> helps in changing native vlan in router. Commands might not show error as sender device and switch would have already learnt mac address of it. No direct tagging will take place instead of sending ARP broadcasts and letting the packet get dropped.

TROUBLESHOOTING : in router enable mode, execute “show vlan brief” and “show interfaces trunk” to get to know about vlan configuration

Since, layer-2 switch will not have idea on IP addresses, it is not possible to have Inter-VLAN routing without layer-3 switch or RoAS as discussed above.

INTER-VLAN ROUTING WITH ROUTER-ON-A-STICK :

To demonstrate a network address 10.0.0.0/24 is split into four subnets as follows and from each subnet, one device is represented to create 4 vlan with managed switch and a vlan router.

First subnet : (00 000000 to 00 111111) -> 10.0.0.0 to 10.0.0.63

* Network address = 10.0.0.0/26
* Usable ip = 10.0.0.1/26 to 10.0.0.62/26
* Broadcast address = 10.0.0.63/26

Second subnet : (01 000000 to 01 111111) -> 10.0.0.64 to 10.0.0.127

* Network address = 10.0.0.64/26
* Usable ip = 10.0.0.65/26 to 10.0.0.126/26
* Broadcast address = 10.0.0.127/26

Third subnet : (10 000000 to 10 111111) -> 10.0.0.128 to 10.0.0.191

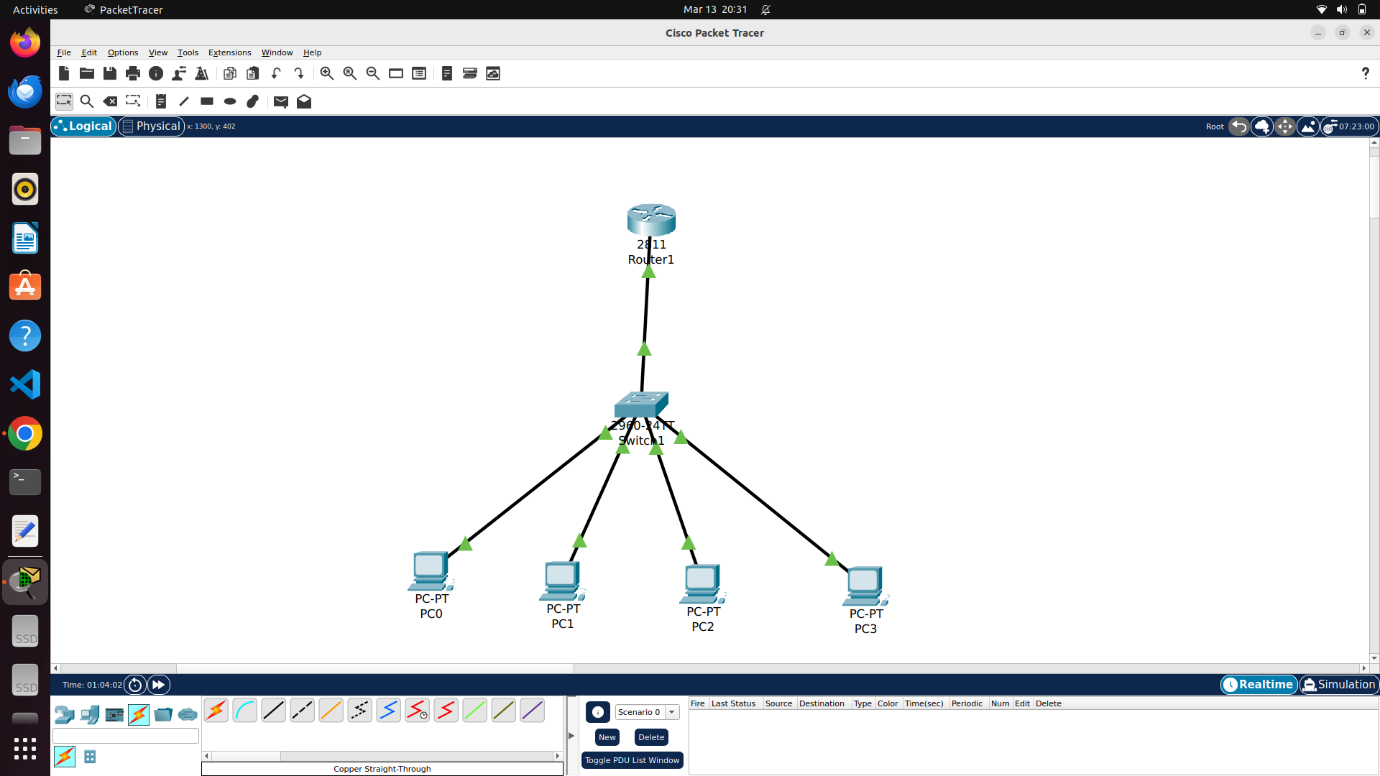
* Network address = 10.0.0.128/26
* Usable ip = 10.0.0.129/26 to 10.0.0.190/26
* Broadcast address = 10.0.0.191/26

Fourth subnet : (11 000000 to 11 111111) -> 10.0.0.192 to 10.0.0.255

* Network address = 10.0.0.192/26
* Usable ip = 10.0.0.193/26 to 10.0.0.254/26
* Broadcast address = 10.0.0.255/26

Image below is the demonstration of implementing four different subnets using VLAN (Virtual LAN) concept. Traffic within same VLAN can be managed by switch but inter-VLAN traffic is maintained by router (vlan enabled).

VLAN BASED NETWORK CONSTRUCTION FOR IMPLEMENTING ALL THE CREATED SUBNETS USING SINGLE SWITCH AND ROUTER



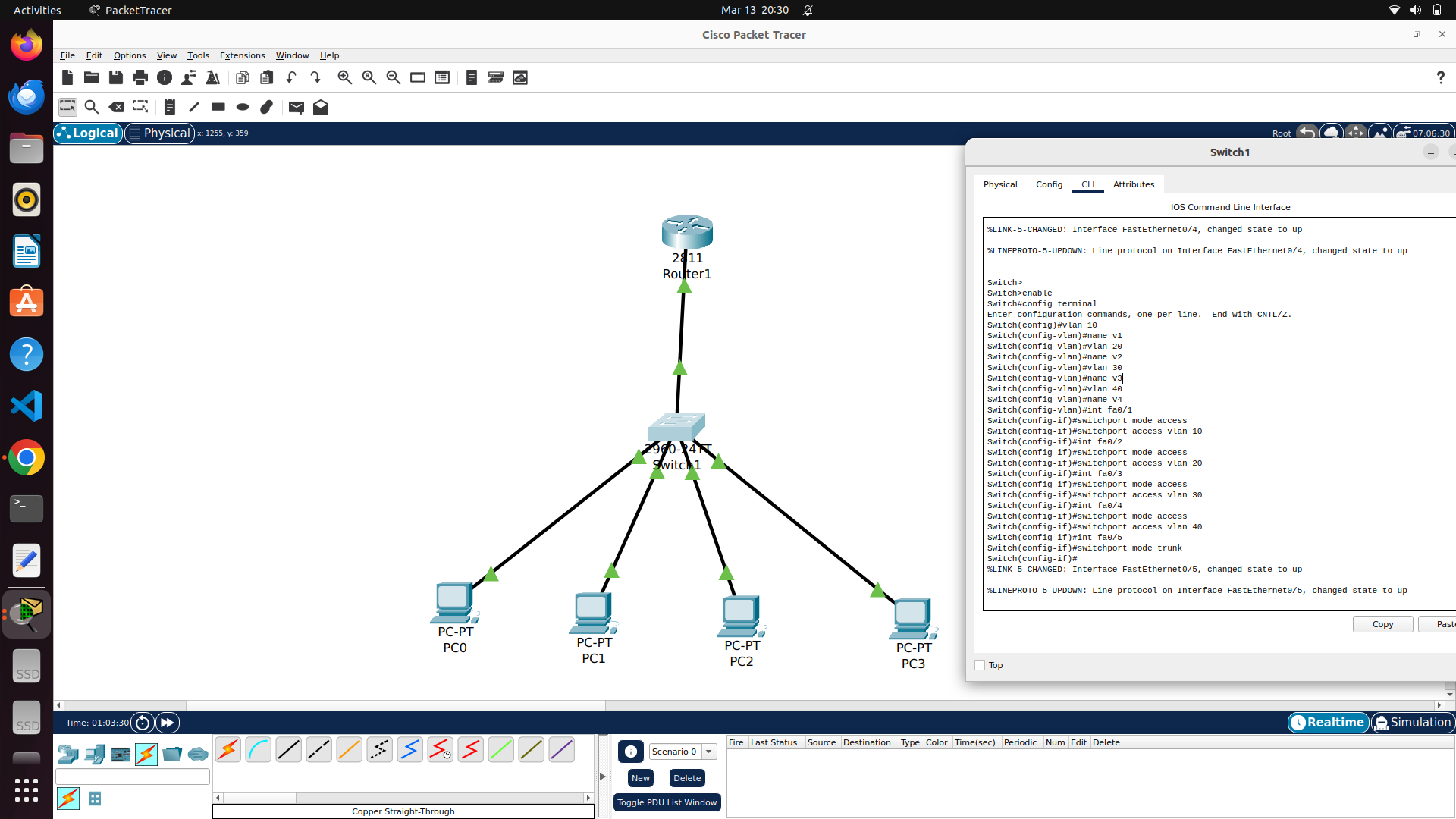
PC0 – 10.0.0.2

PC1 – 10.0.0.66

PC2 – 10.0.0.130

PC3 – 10.0.0.194

For switch, individual VLAN to be declared with its tag and each switch port to be either marked as access or trunk port.



For router, each interface to be defined and should made up , followed by creating sub interfaces as per IEEE 802.1Q and assigning with available vlan and provide IP and subnet mask.

