21BCE7371
RADHA KRISHNA GARG

COMPUTER NETWORKS ASSIGNMENT - 4

Port-Security

Port security is a dynamic Cisco Catalyst switch feature that secures switch ports, and ultimately the CAM table, by limiting the number of MAC addresses that can be learned on a particular port or interface. Port security can be implemented in the following three ways:

- Static Secure MAC Addresses
- Dynamic Secure MAC Addresses
- Sticky Secure MAC Addresses

Static secure MAC addresses are statically configured by network administrators and are stored in the MAC address table, as well as in the switch configuration. When static secure MAC addresses are assigned to a secure port, the switch will not forward frames that do not have a source MAC address that matches the configured static secure MAC address or addresses.

Dynamic secure MAC addresses are dynamically learned by the switch and are stored in the MAC address table. However, unlike static secure MAC addresses, dynamic secure MAC address entries are removed from the switch when the switch is reloaded or powered down.

Sticky secure MAC addresses are a combination of static secure MAC addresses and dynamic secure MAC addresses. These addresses can be learned dynamically or configured statically and are stored in the MAC address table, as well as in the switch configuration. This means that when the switch is powered down or rebooted, it will not need to dynamically discover the MAC addresses again because they will already be saved in the configuration file.

Once port security has been enabled, administrators can define the actions the switch will take in case of a port security violation. Cisco IOS

software allows administrators to specify three different actions to take when a violation occurs:

- Protect
- Shutdown
- Restrict

The project option forces the port into a protected port mode. In this mode, all Unicast or Multicast frames with unknown source MAC addresses, i.e. MAC addresses not presently in the CAM table, are discarded by the switch. When the switch is configured to protect a port, it will not send out a notification when operating in protected port mode, meaning that administrators would never know when an attack was prevented in this mode.

The shutdown option places a port in an error-disabled state when a security violation occurs. The corresponding LED on the switch port is also turned off in this state. In shutdown mode, the switch sends out an SNMP trap and a Syslog message, and the violation counter is incremented.

The restrict option is used to drop packets with unknown MAC addresses, i.e. MAC addresses not presently in the CAM table, when the number of secure MAC addresses reaches the administrator-defined maximum limit for the port. In this mode, the switch will continue to restrict additional MAC addresses from sending frames until a sufficient number of secure MAC addresses is removed, or the number of maximum allowable addresses is increased. As is the case with the shutdown option, the switch sends out an SNMP trap and a Syslog message, and the violation counter is incremented.

Command to Configure Interface:

Switch#configure terminal

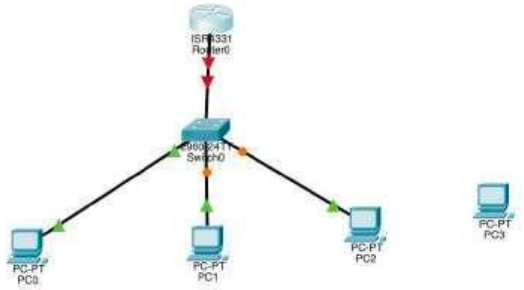
Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#interface fastethernet0/1

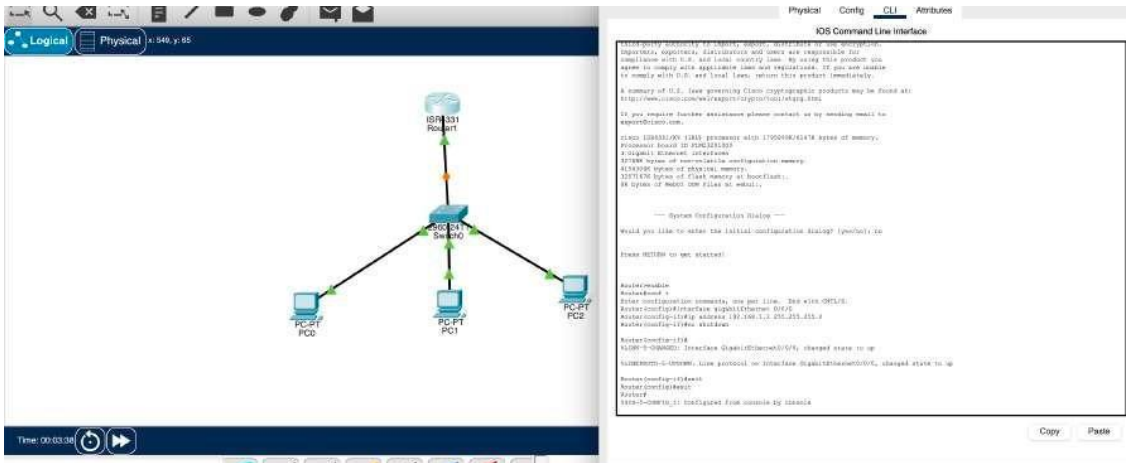
Switch(config-if)#switchport mode access

```
Switch(config-if)#switchport port-security

Switch(config-if)#switchport port-security mac-address sticky

Switch(config-if)#switchport port-security maximum 1

Switch(config-if)#switchport port-security violation shutdown

Switch(config-if)#

Switch(config-if)#exit

Switch(config)#

Switch(config)#interface fastethernet0/2

Switch(config-if)#switchport mode access

Switch(config-if)#switchport port-security

Switch(config-if)#switchport port-security mac-address sticky

Switch(config-if)#switchport port-security maximum 1

Switch(config-if)#switchport port-security violation shutdown

Switch(config-if)#

Switch(config-if)#end

Switch#
```

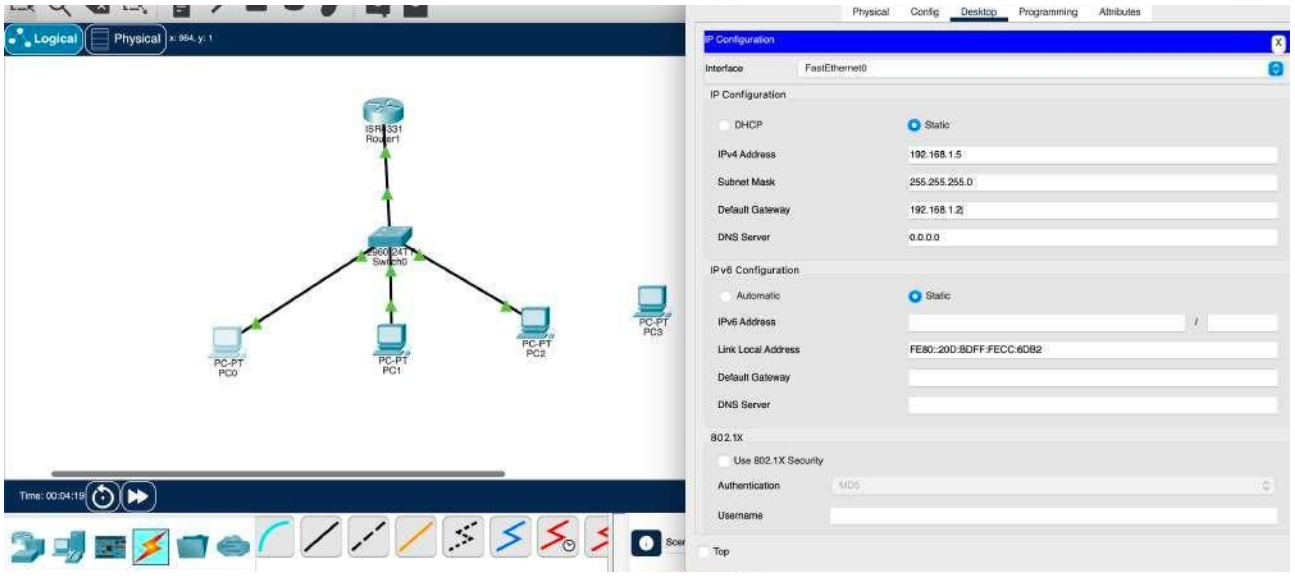
1.



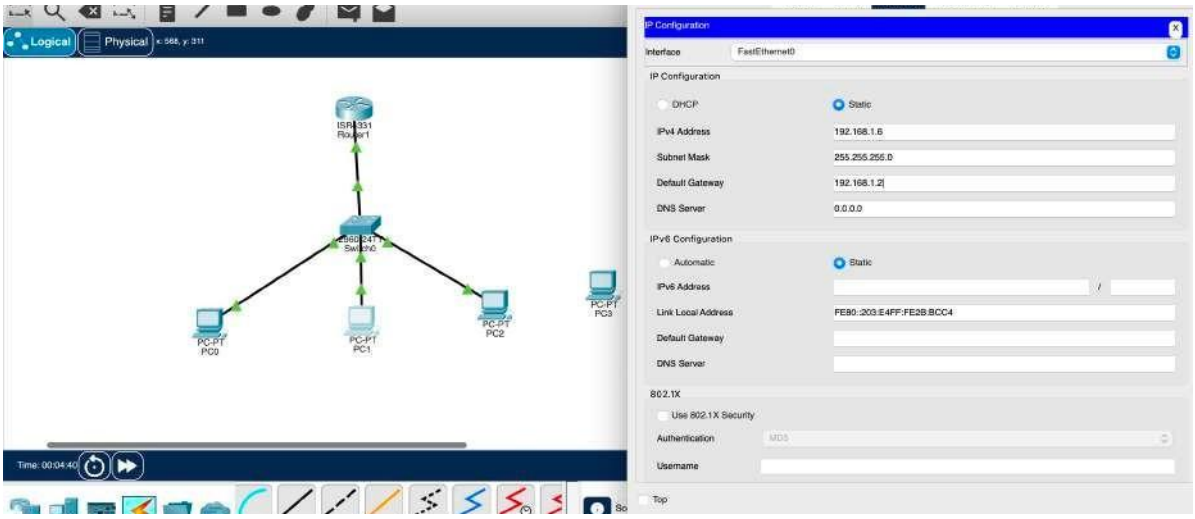
Router Configuration:



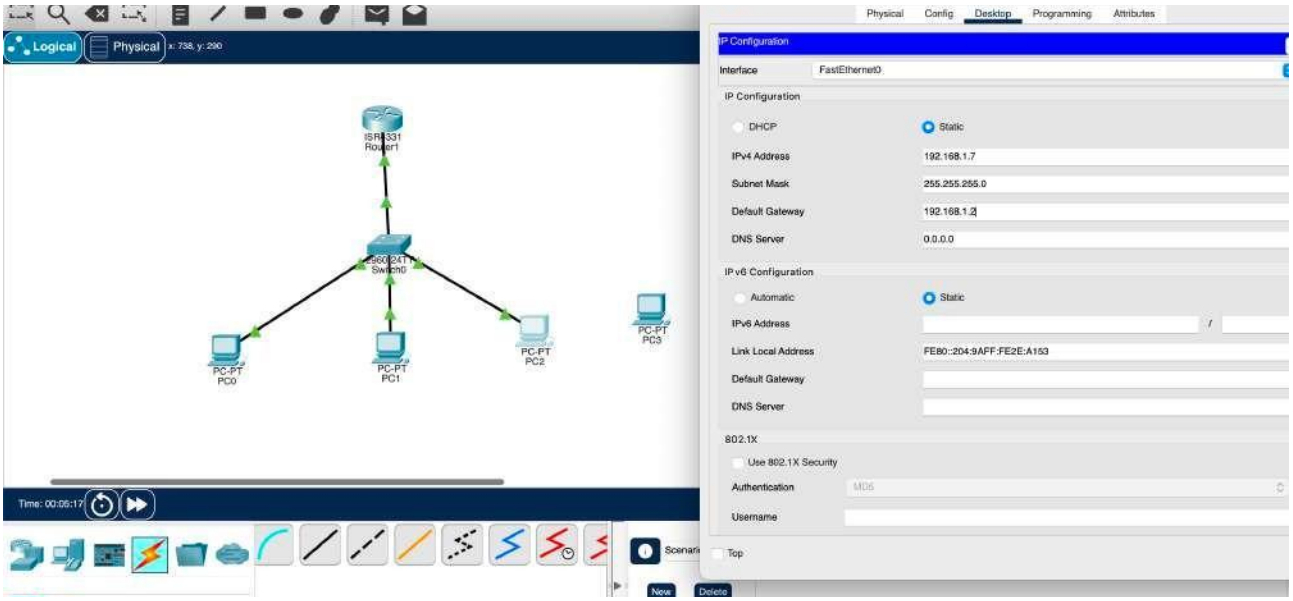
IP-Address to PC-1:



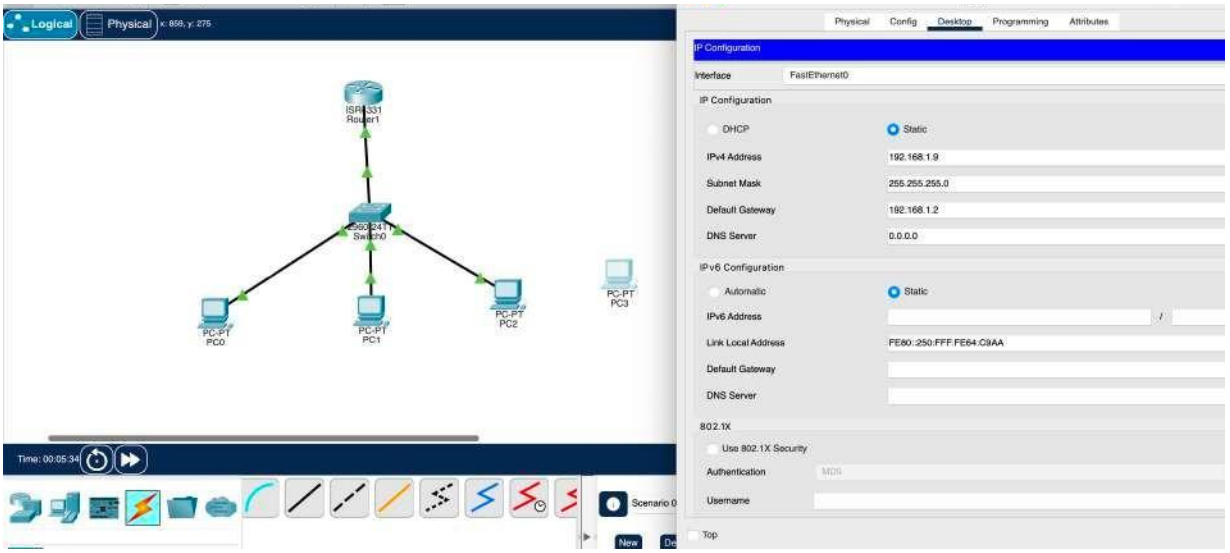
IP-Address to PC-2:



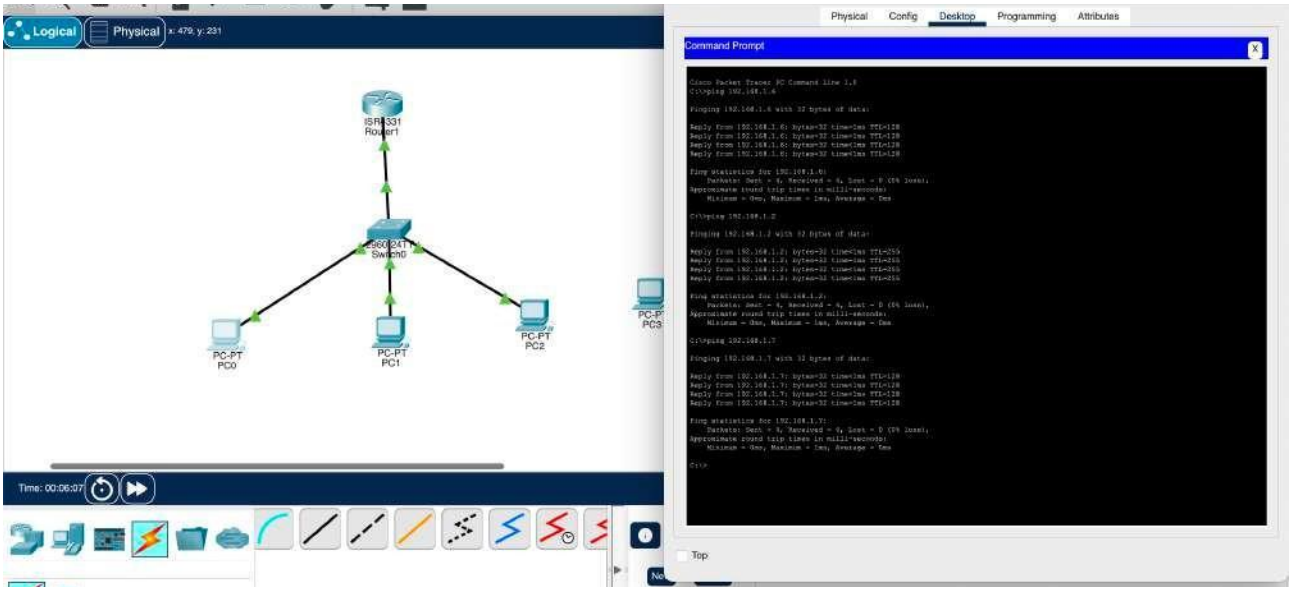
IP-Address to PC-3:



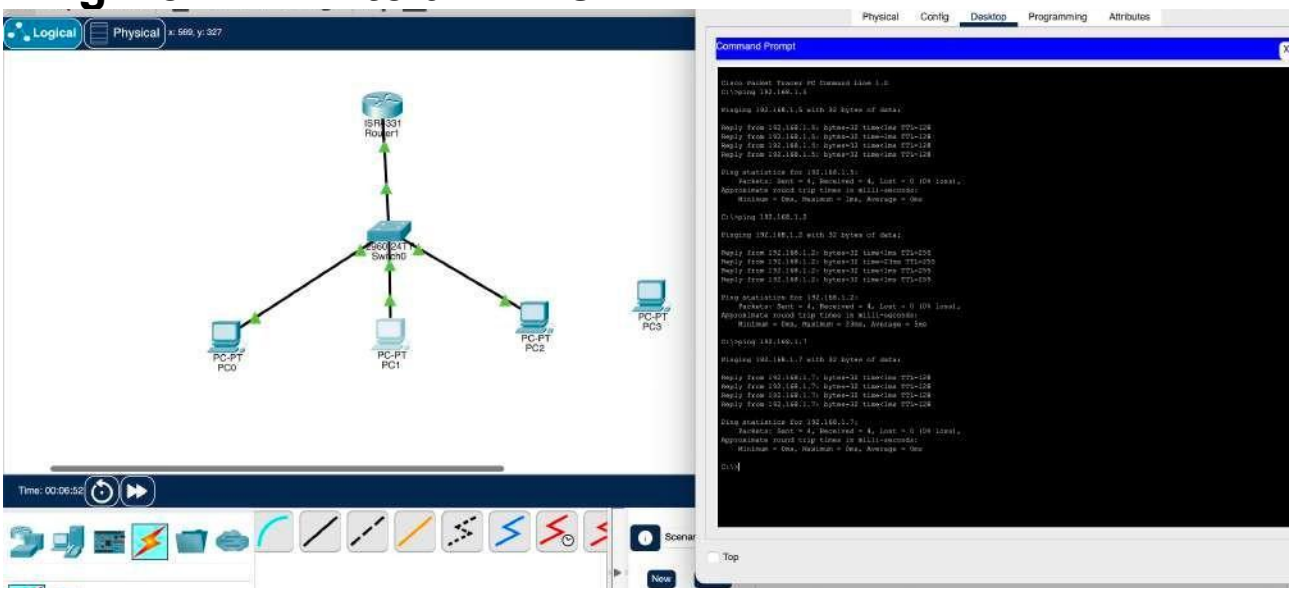
IP-Address to PC-4:



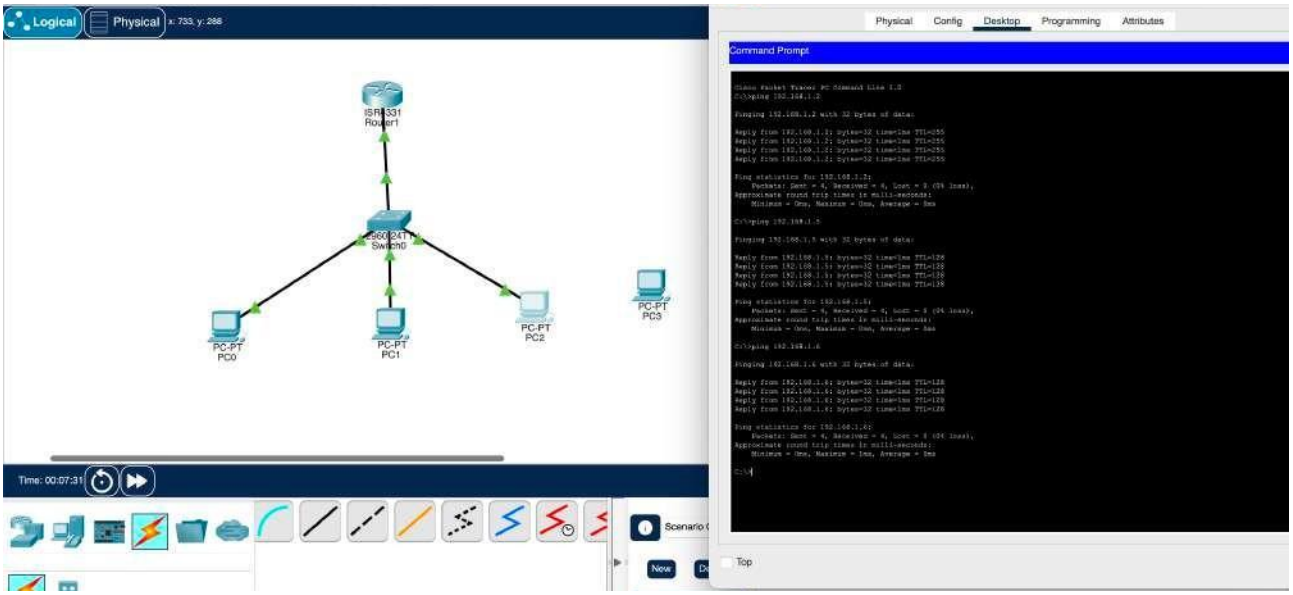
Ping from PC-1 to all PC's:



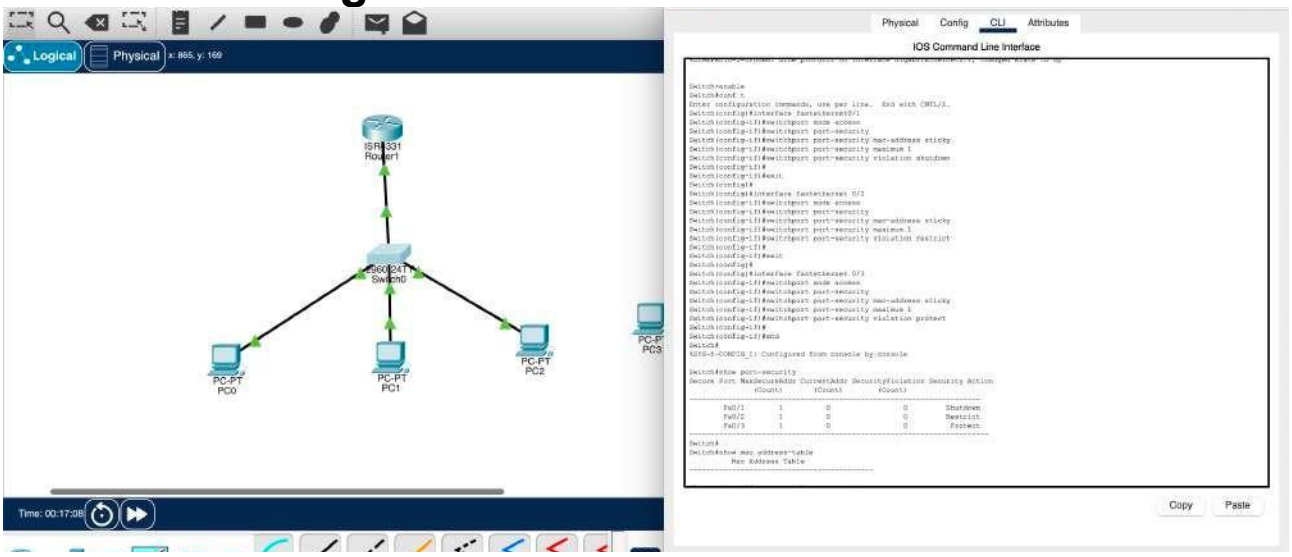
Ping from PC-2 to all PC's:



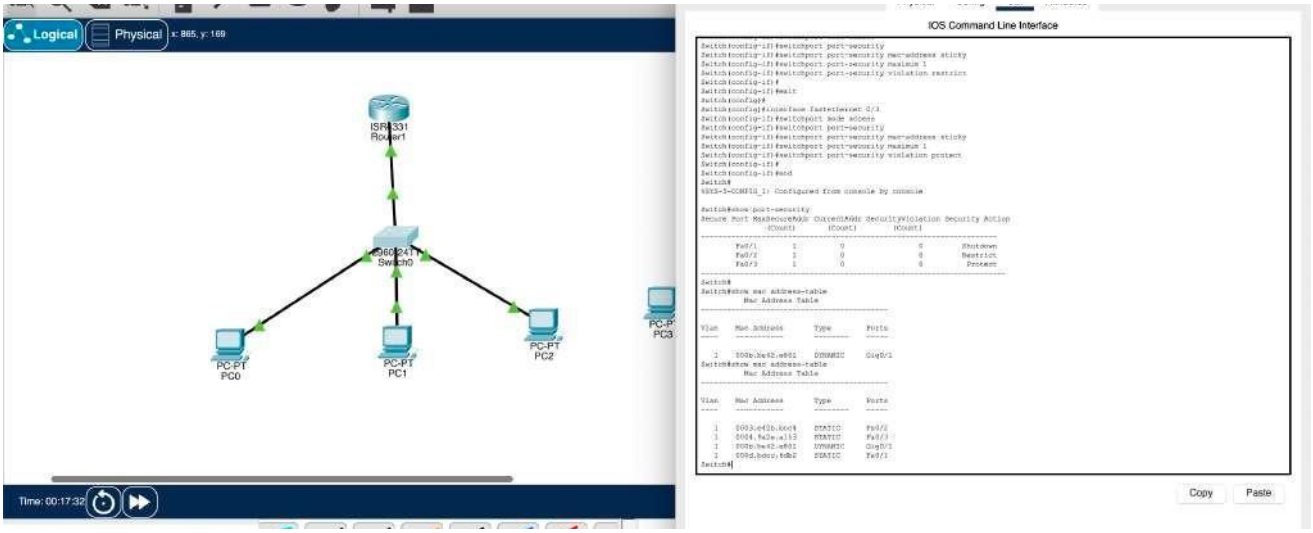
Ping from PC-3 to all PC's:



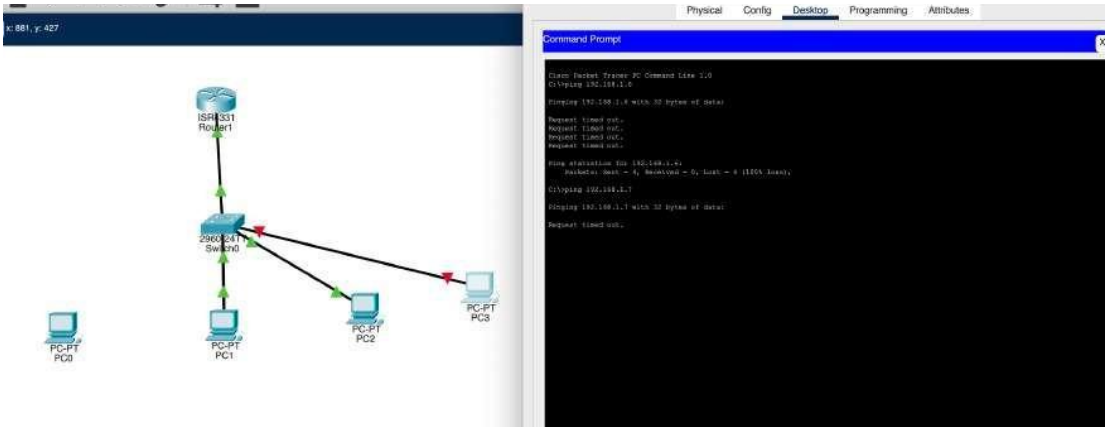
Interface Configuration Shutdown/Restrict/Protected:

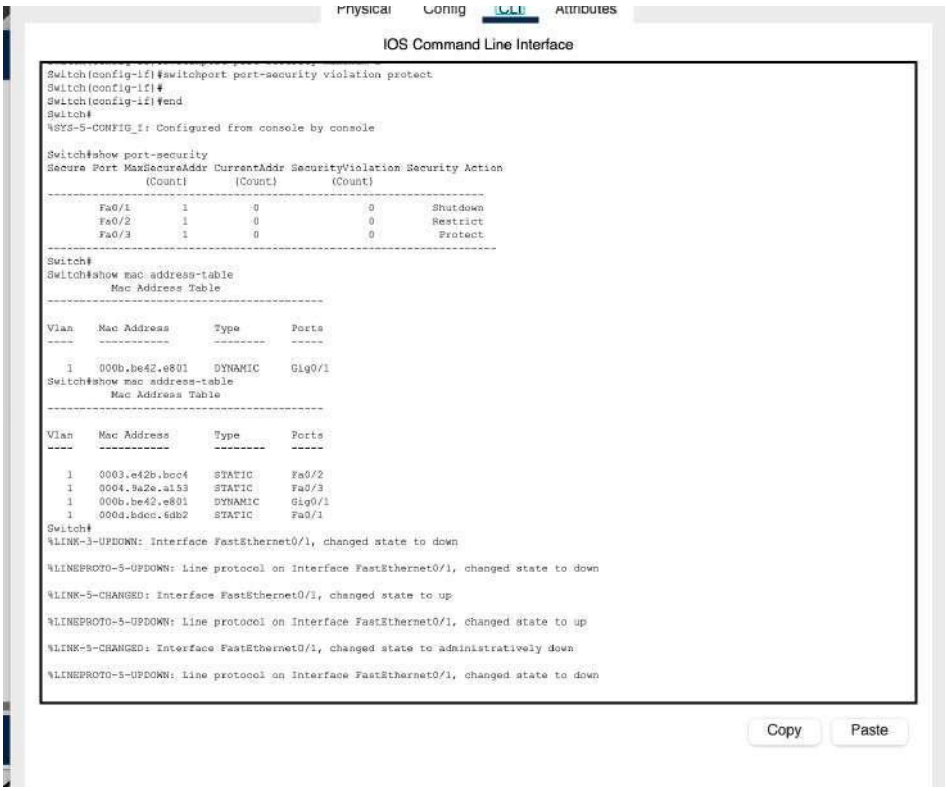


Interface Modes and Mac-address table:

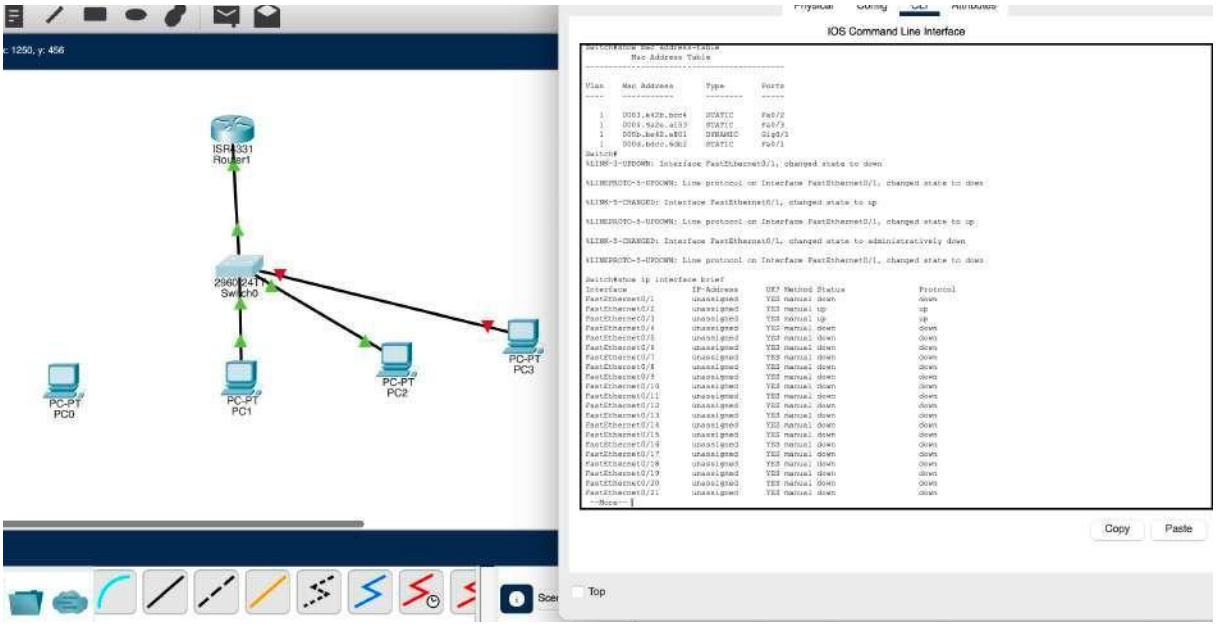


Shutdown:

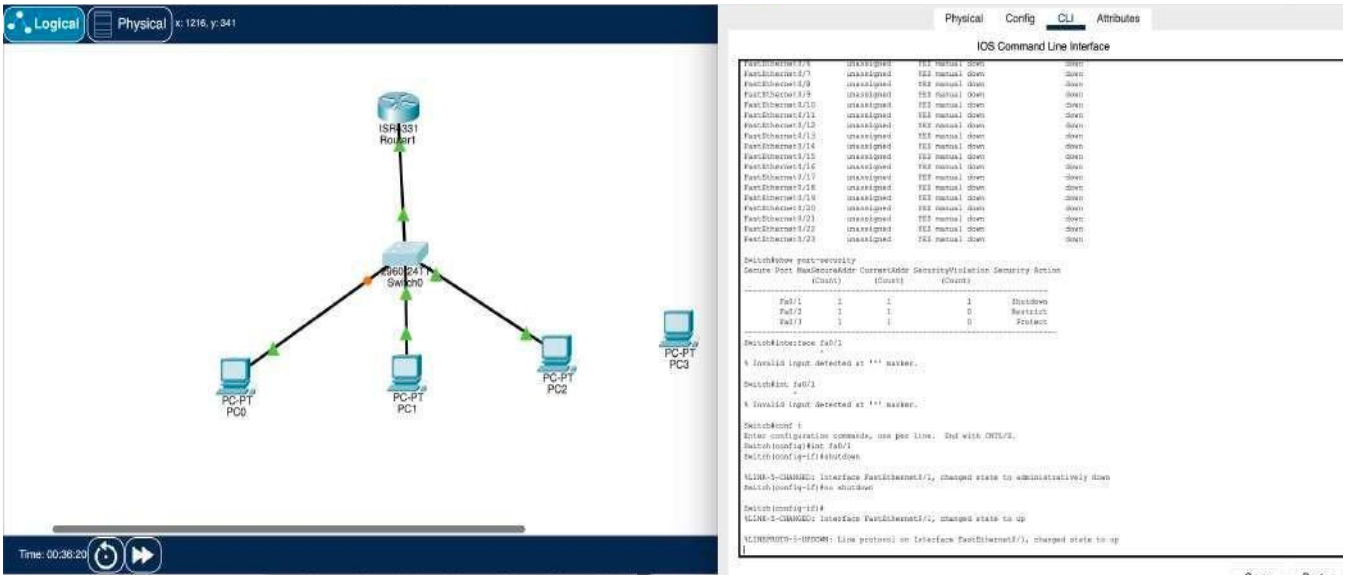




Line protocol is down in the shutdown

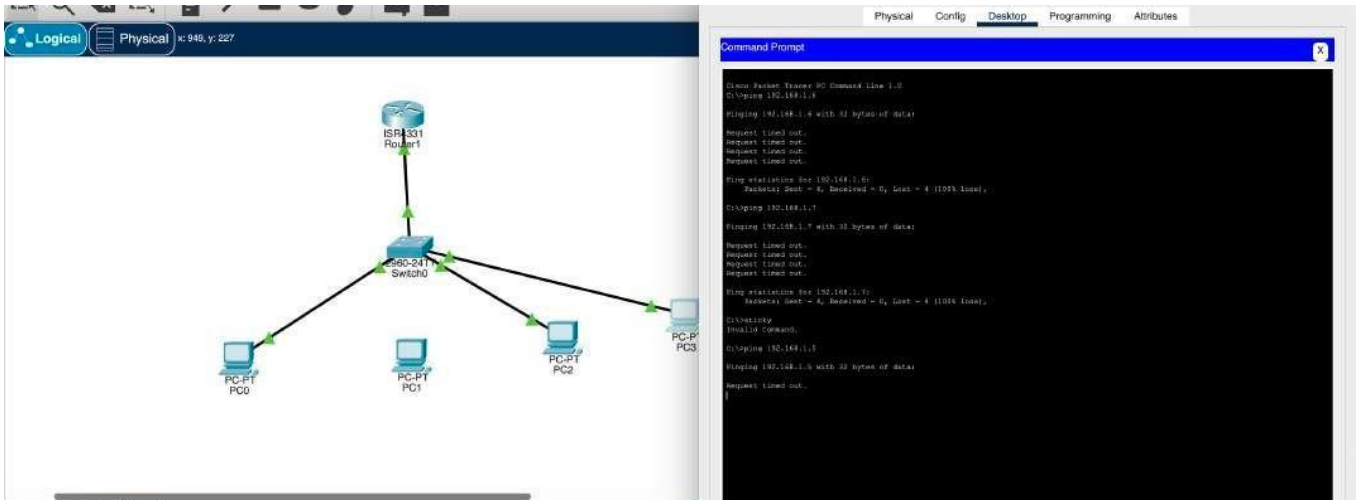


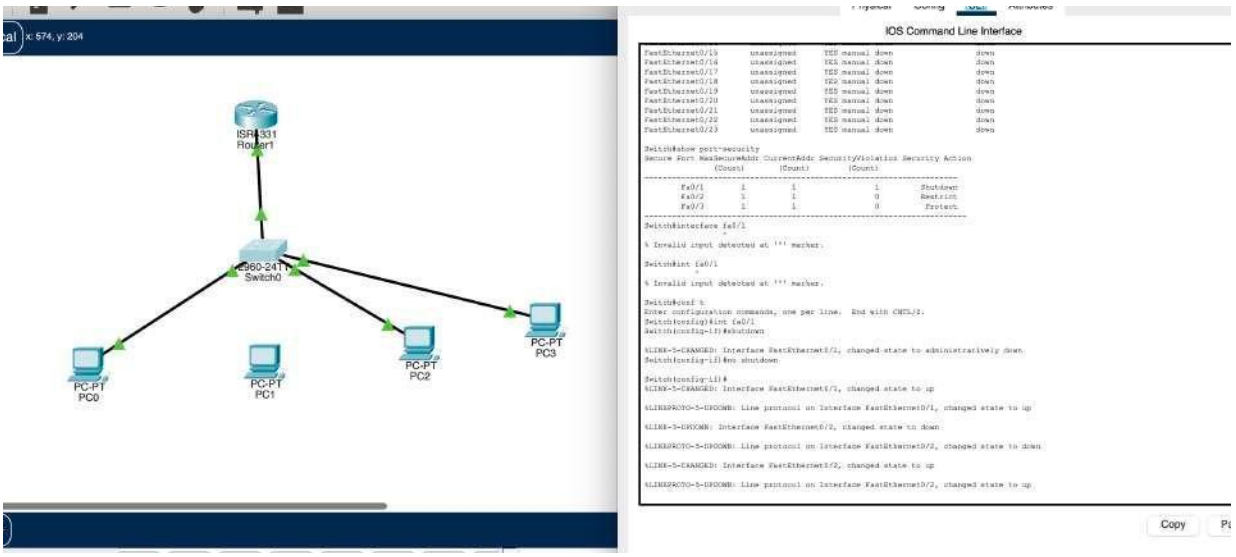
Interface Status-down



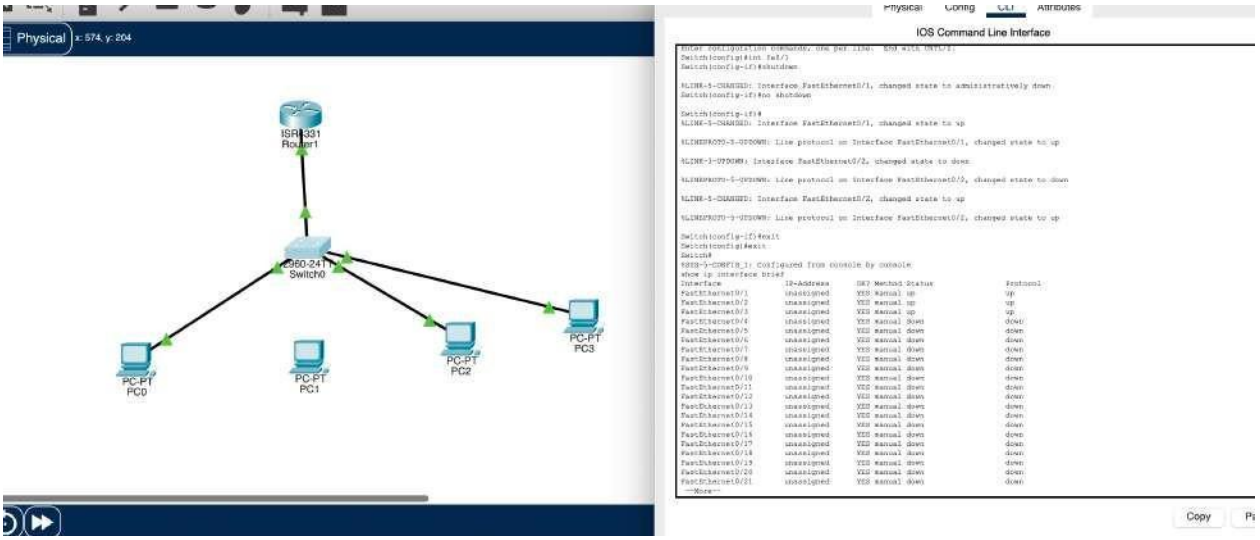
Manually changing the interface from shutdown to no shutdown

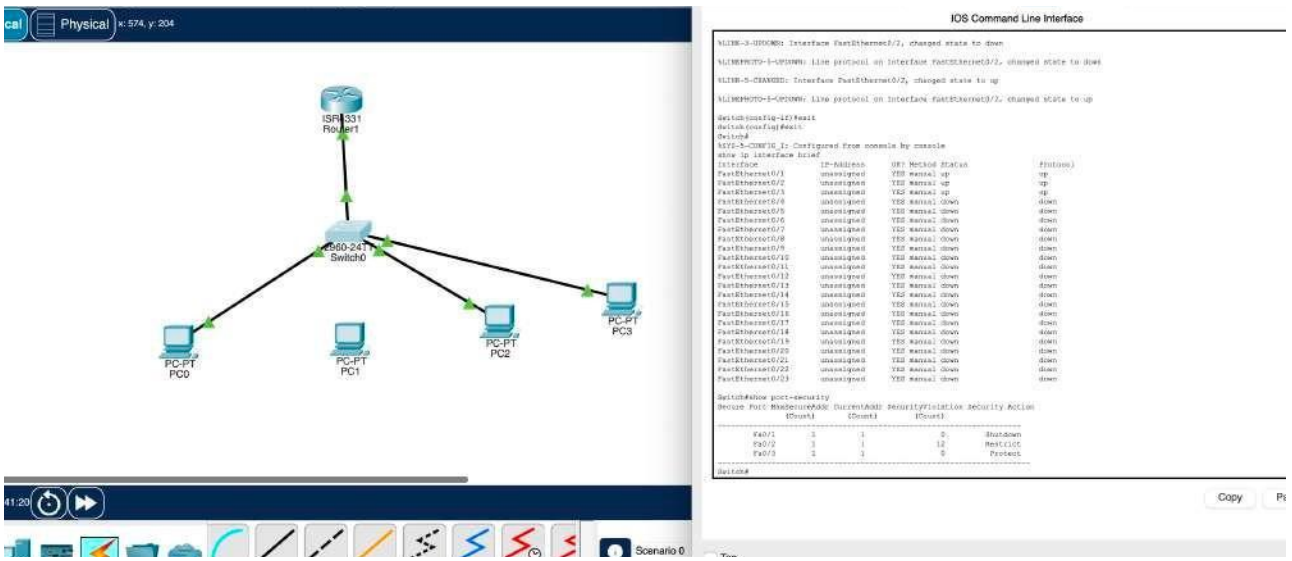
Restrict:





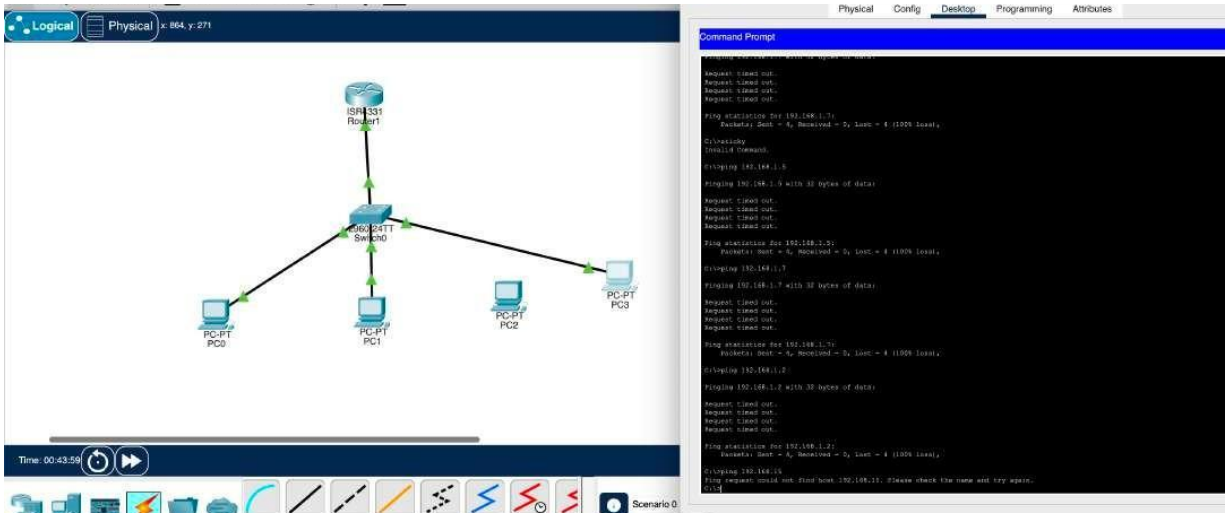
Line interface is up

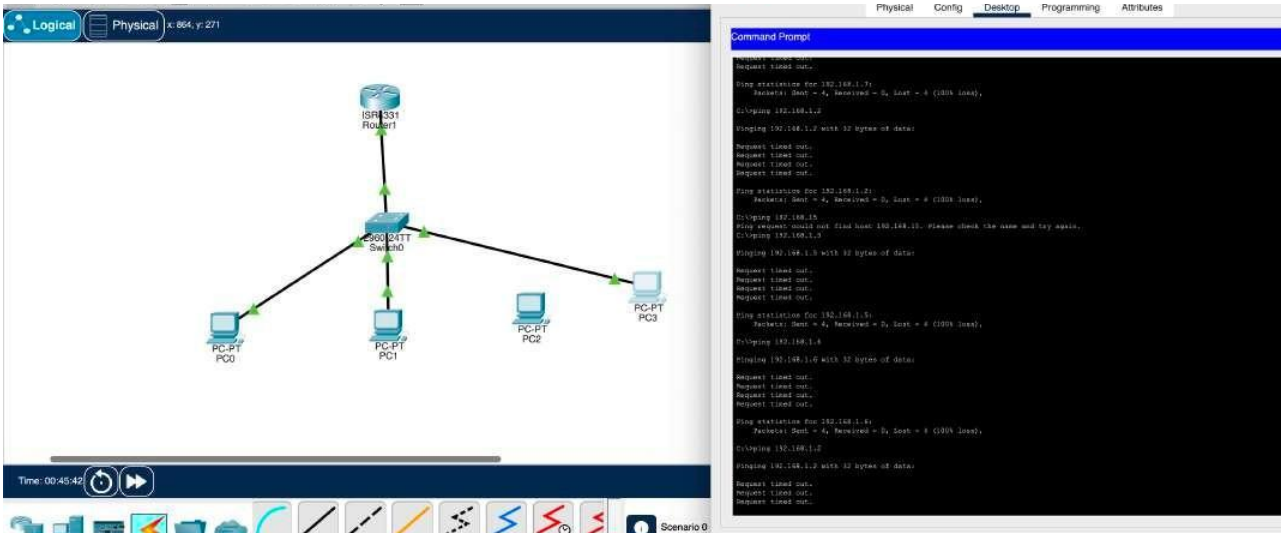




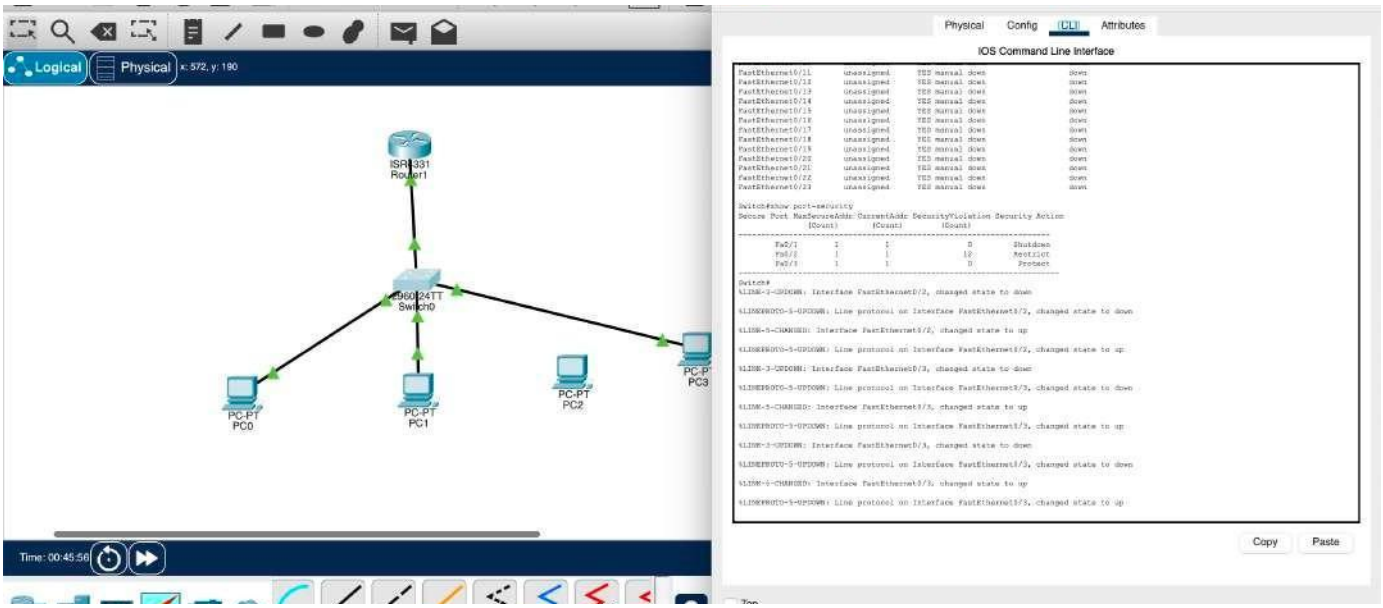
Port-Security count=12

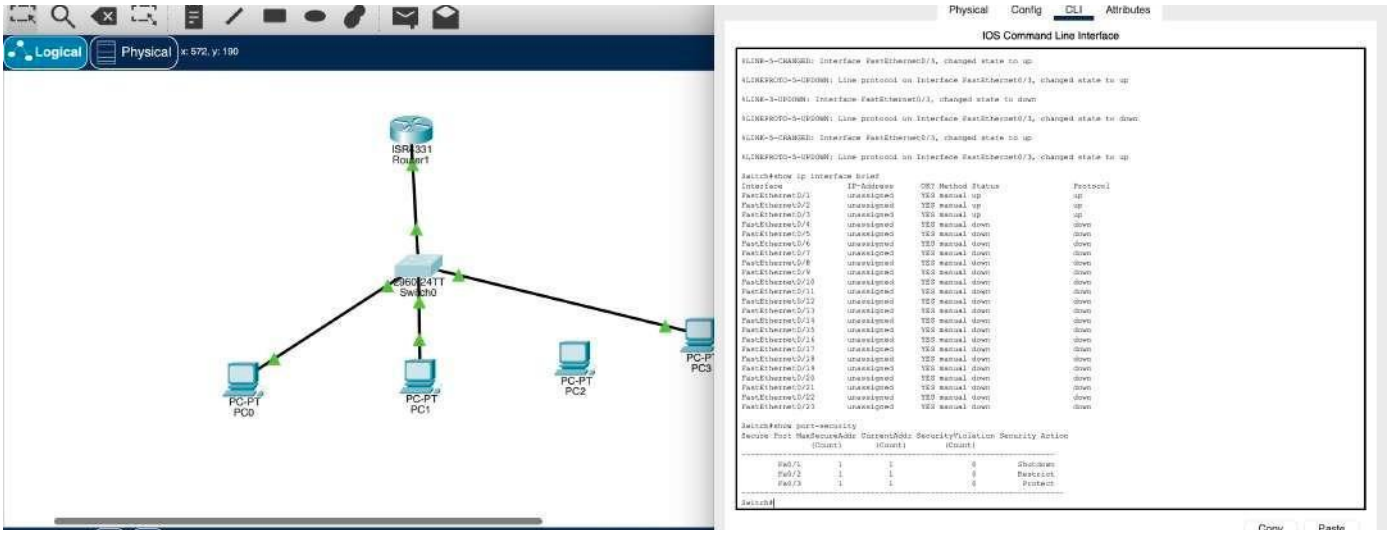
Protect





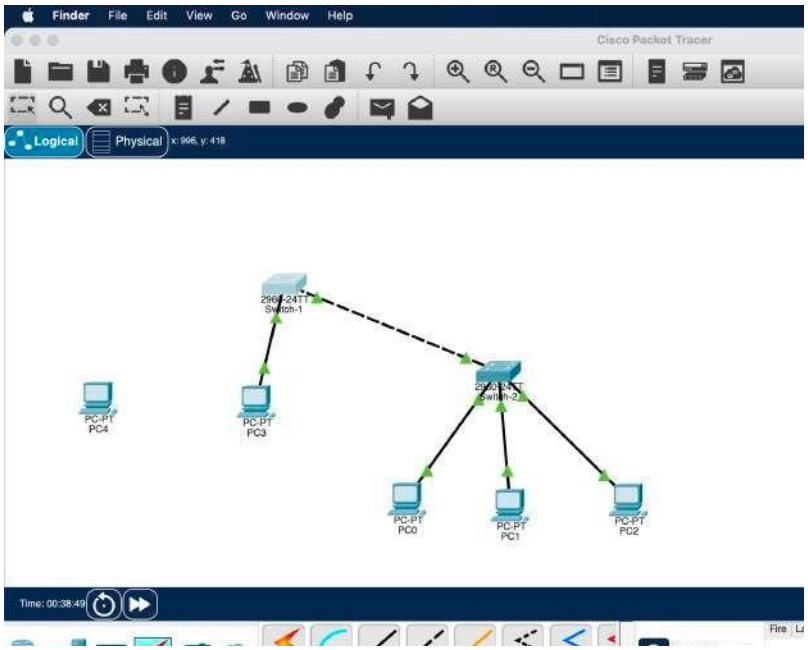
Line Interface is up



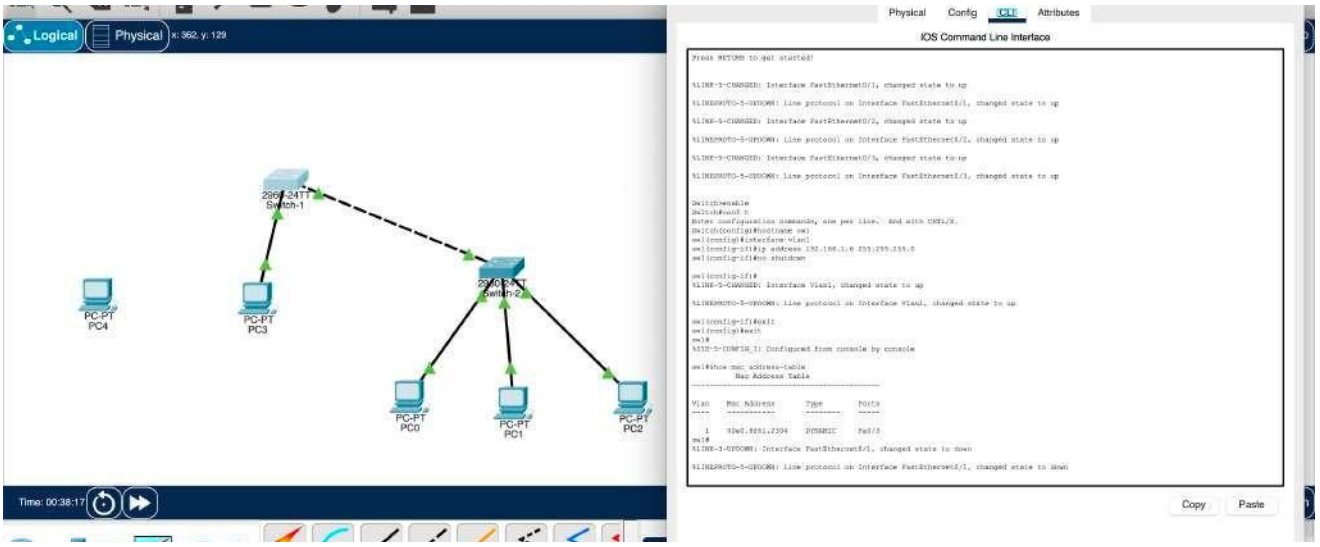


Count =0 for all.

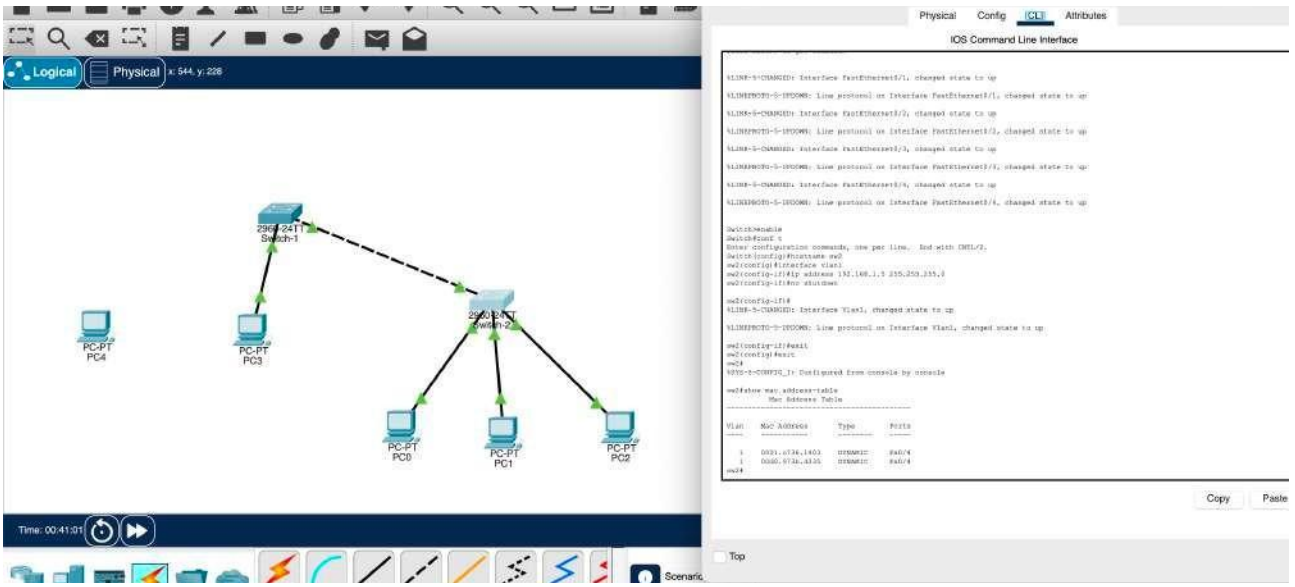
2.



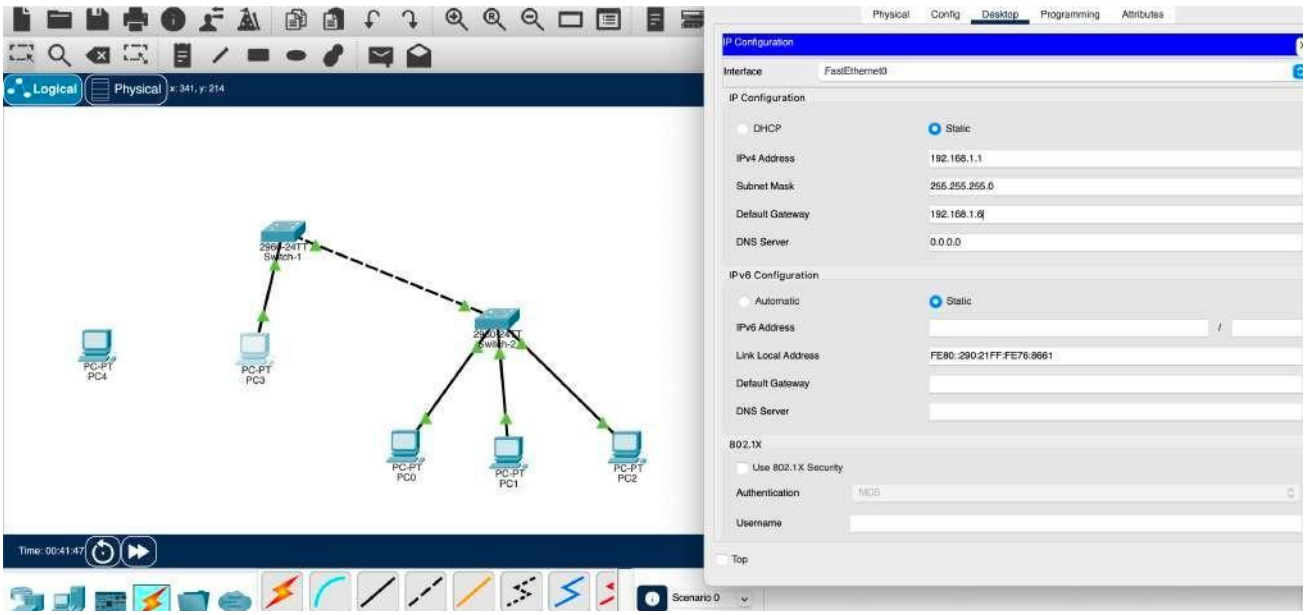
Switch-1 IP Address configuration:



Switch-2 IP Address:

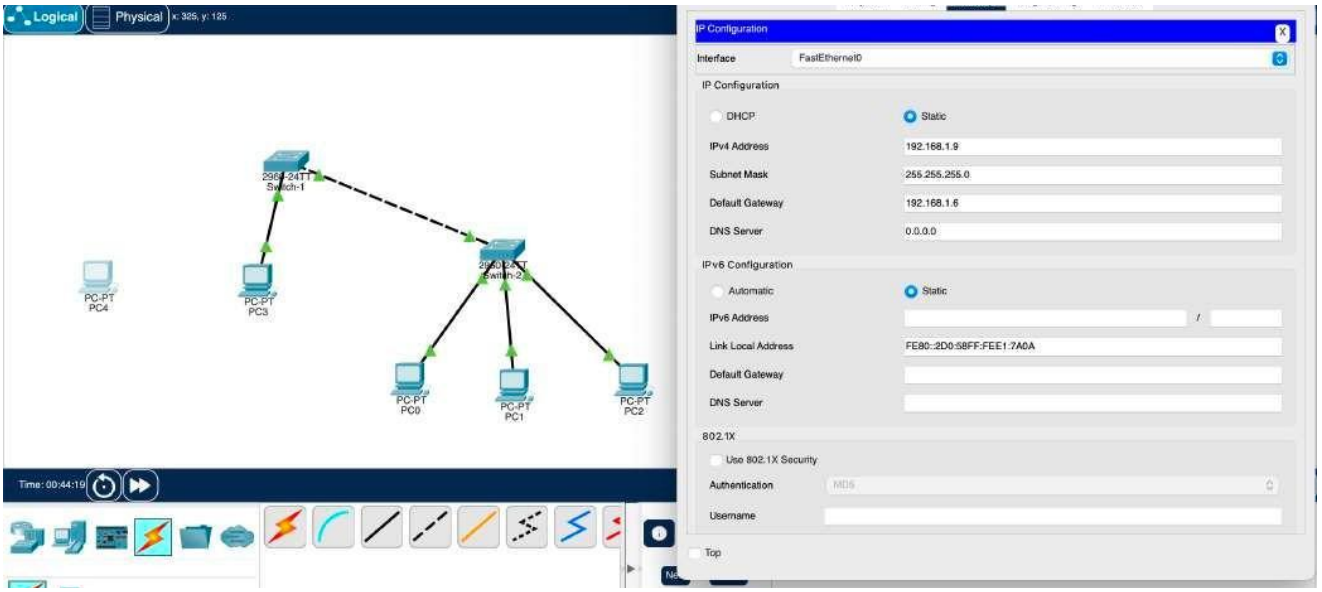


PC IP-Address Configuration:

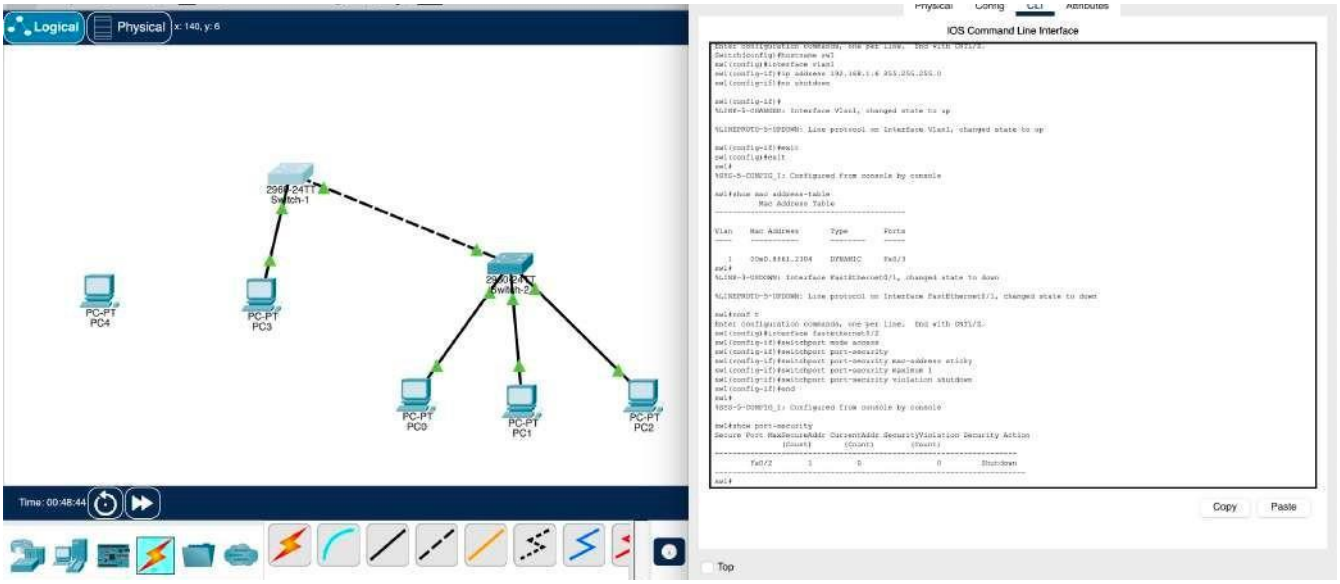


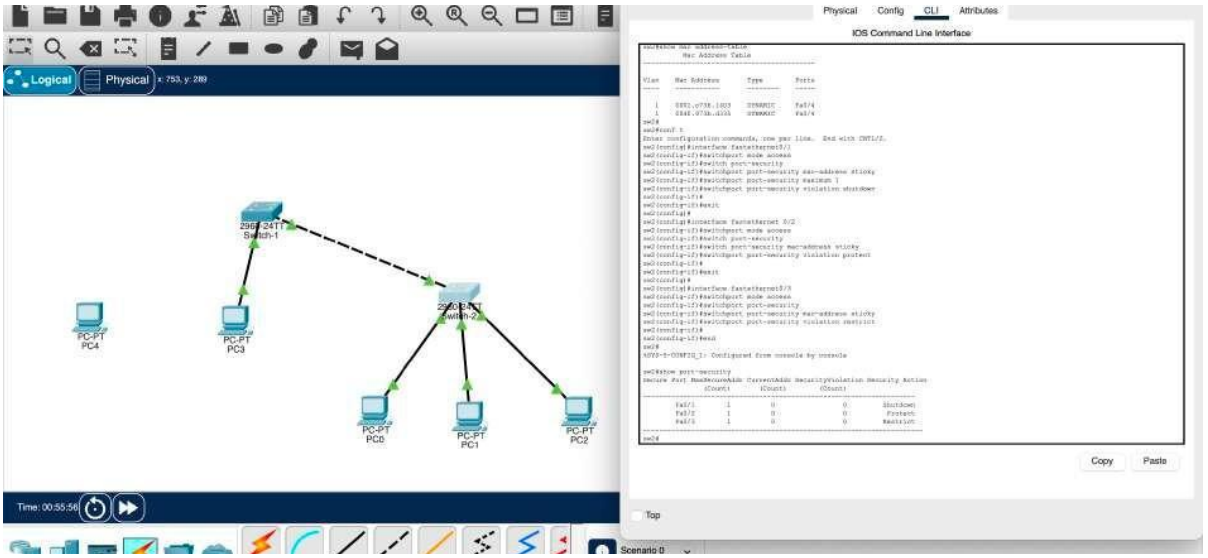
Switch Interface Configuration:

Switch-1:

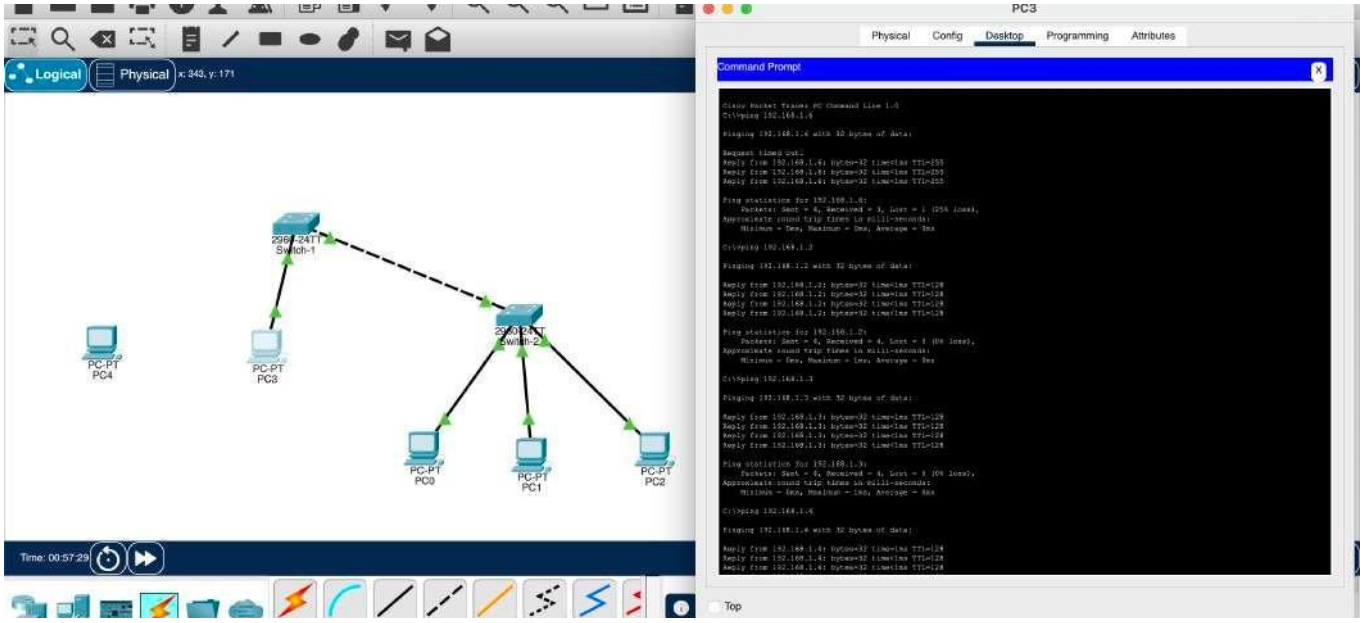


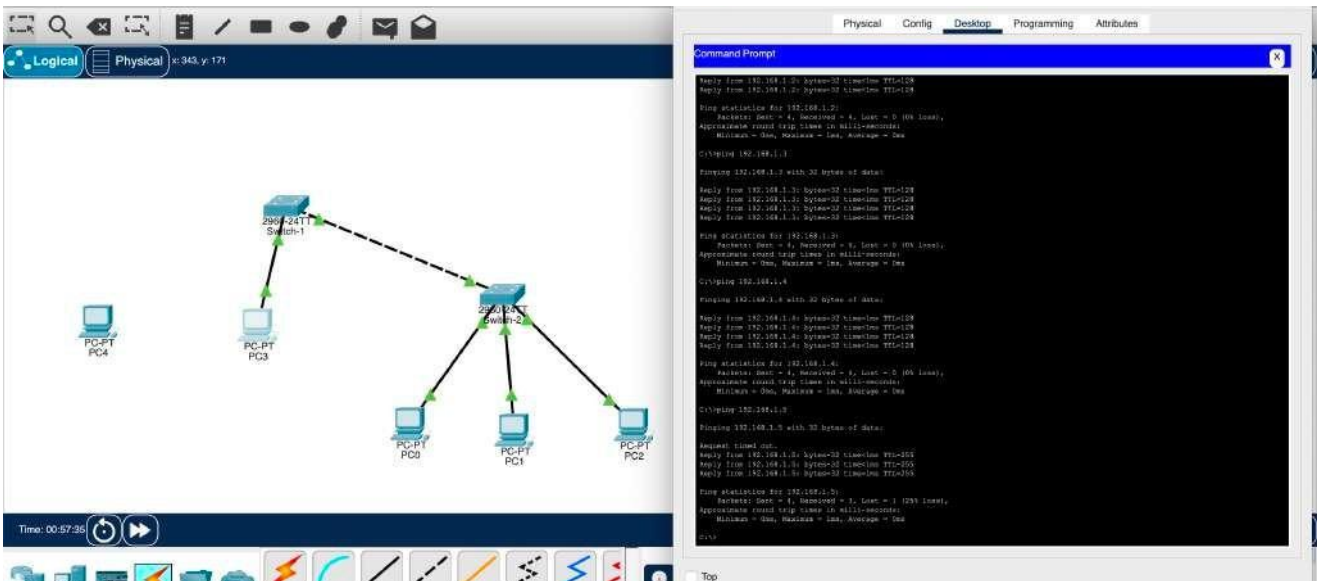
Switch-2:



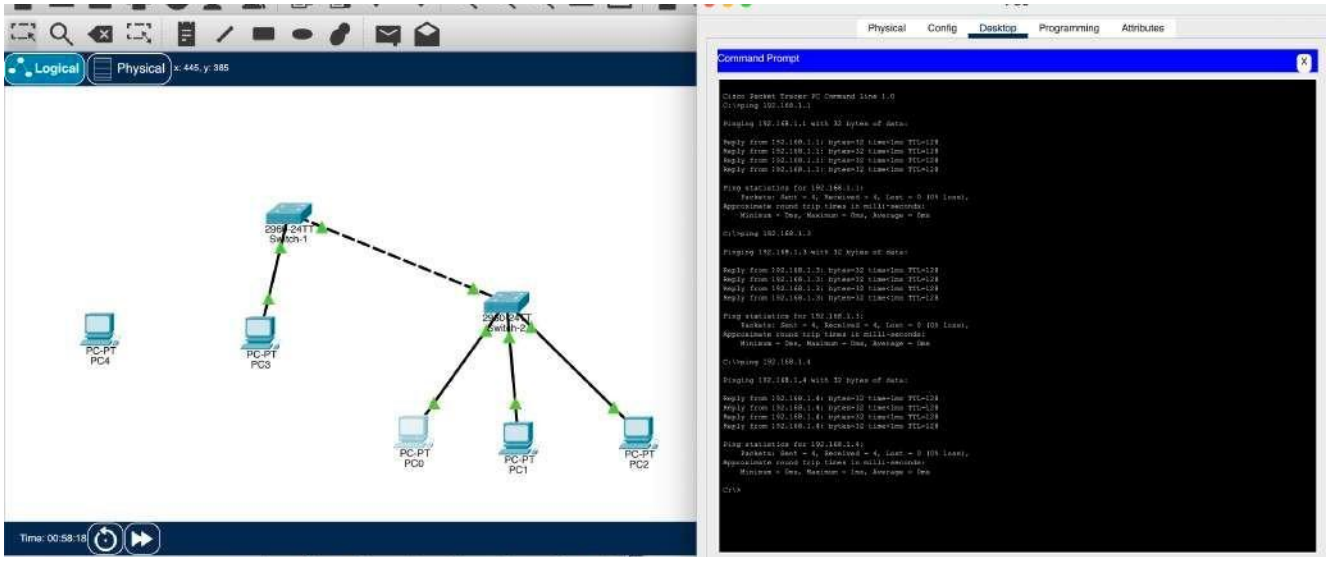


Ping from PC-3 to other devices:

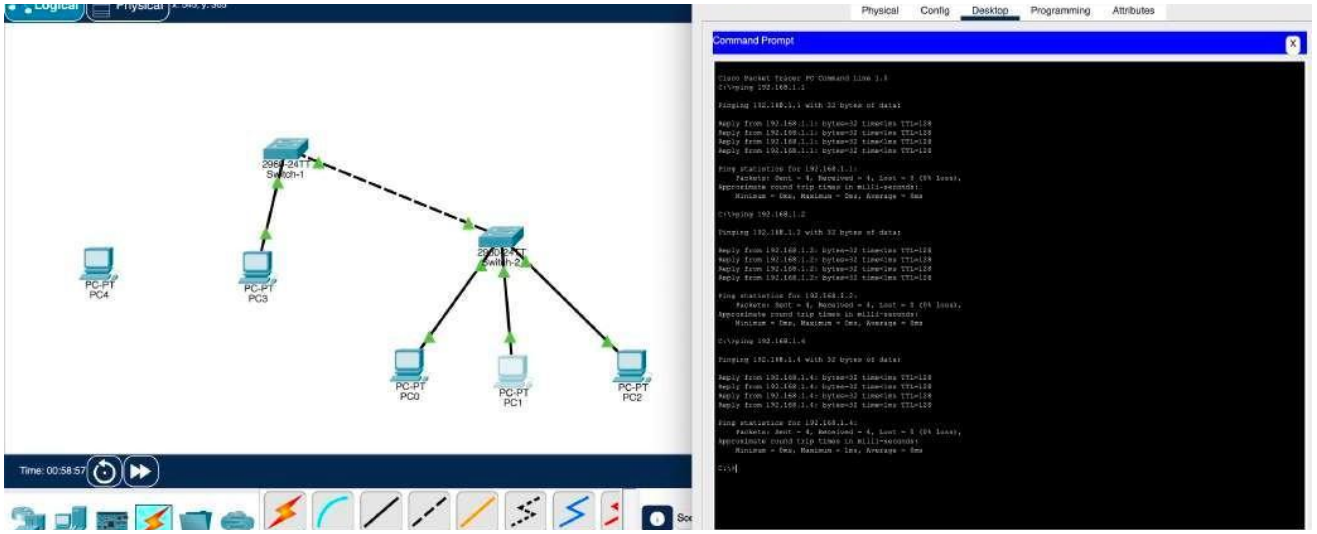




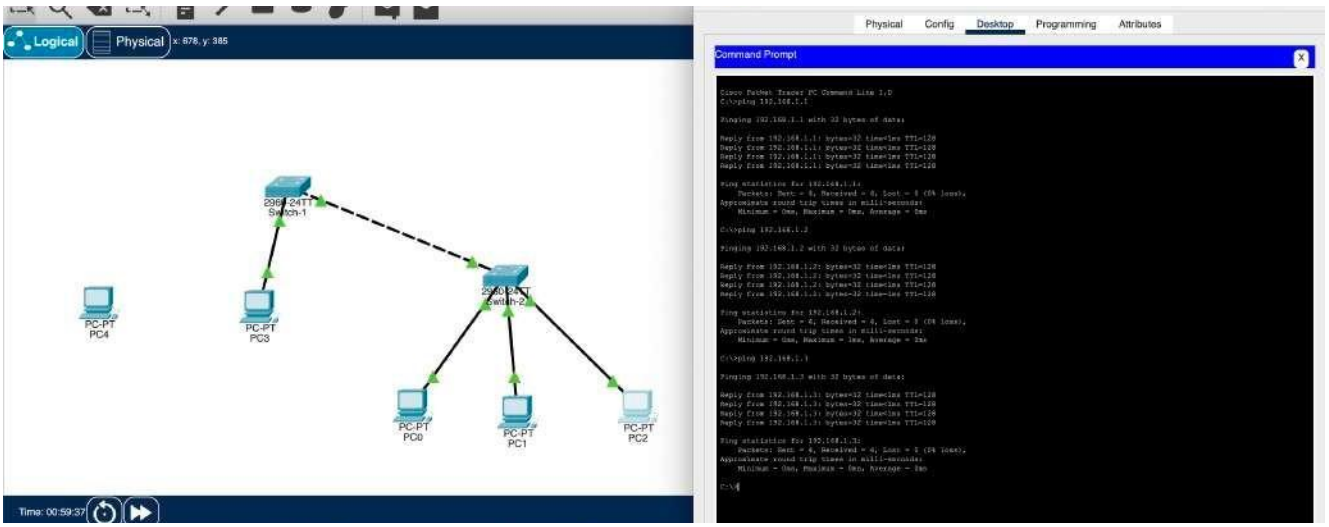
Ping from PC-0 to other devices:



Ping from PC-1 to other devices:

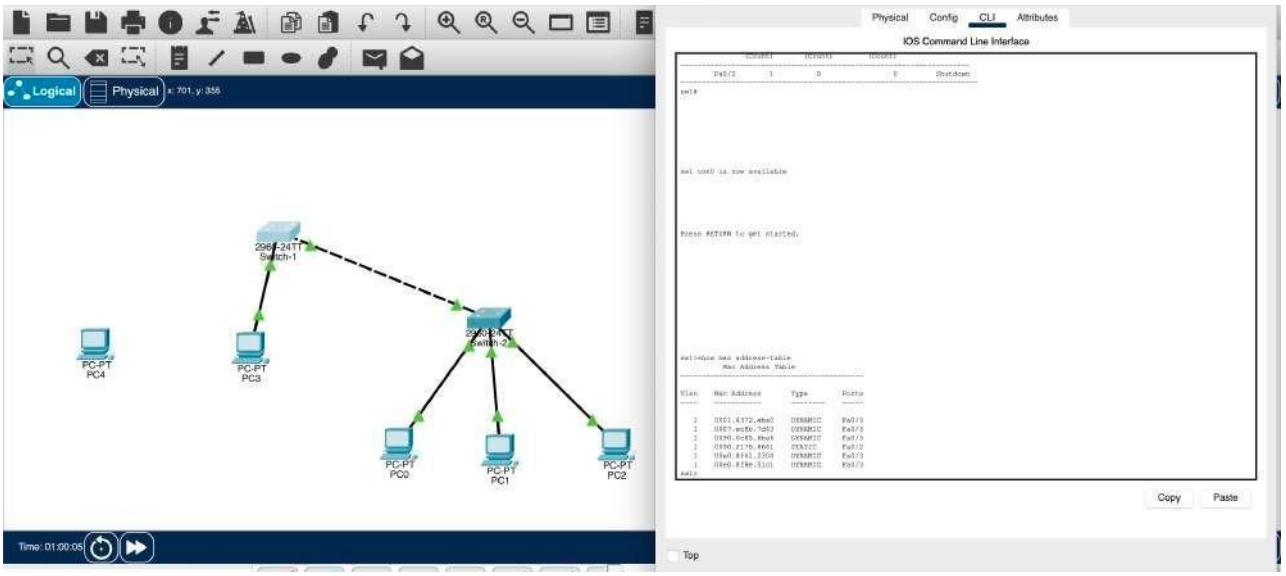


Ping from PC-2 to other devices:

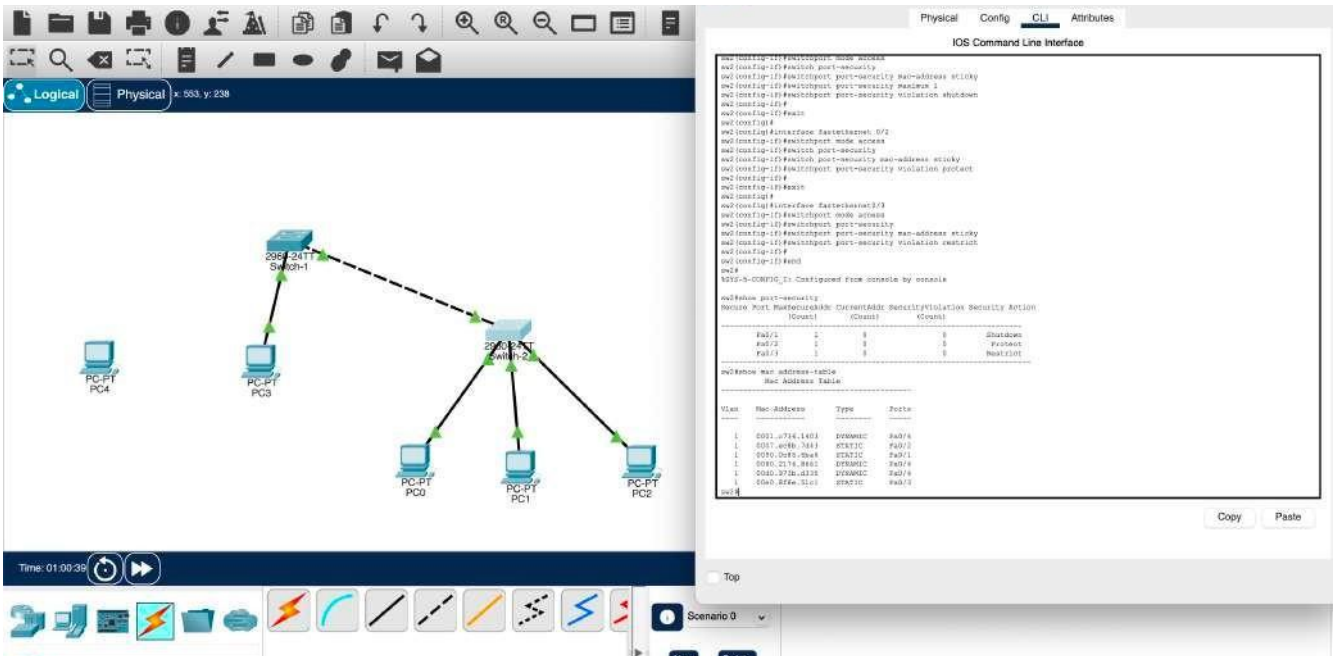


Mac-address table:

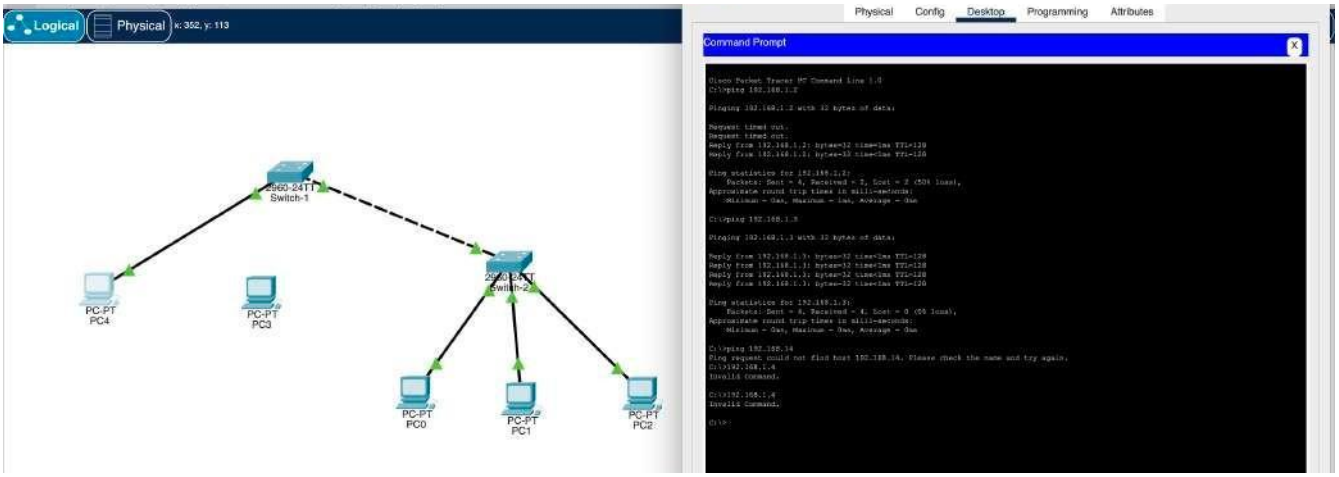
Switch-1:



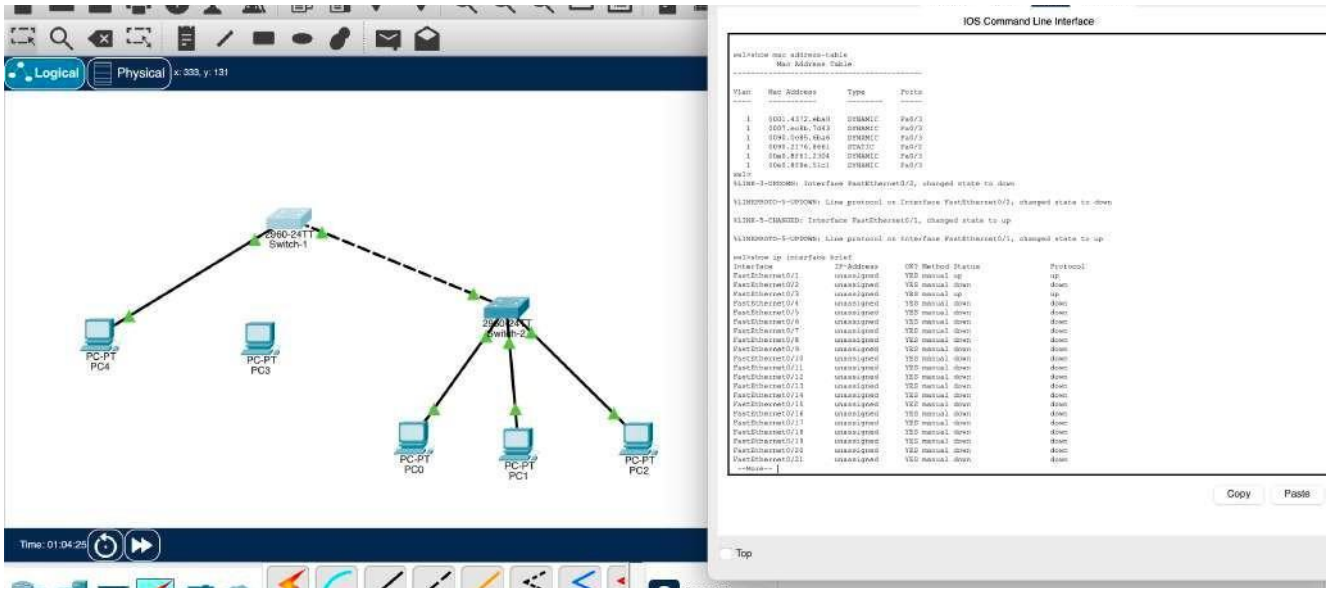
Switch-2:



Ping from PC that is not connected to PC's configured with Shutdown/Protect/Restrict:



Switch CLI:



Q1 How many MAC addresses are visible in the table?

ANS -1

5 Mac addresses are visible in the 1st table and **6** in the 2nd table.

Q2 Other than the sticky command what other approach can be used for identifying MAC address?

Ans -2

IP config/all can be used other than sticky for identifying MAC address.

Q3 Observe the transmission difference between notation methods

Ans -3

a. **Protect**
b. **Restrict**
c. **Shutdown**

The project option forces the port into a protected port mode. In this mode, all Unicast or Multicast frames with unknown source MAC addresses, i.e. MAC addresses not presently in the CAM table, are discarded by the switch. When the switch is configured to protect a port, it will not send out a notification when operating in protected port mode, meaning that administrators would never know when an attack was prevented in this mode.

The shutdown option places a port in an error-disabled state when a security violation occurs. The corresponding LED on the switch port is also turned off in this state. In shutdown mode, the switch sends out an SNMP trap and a Syslog message, and the violation counter is an increment.

The restrict option is used to drop packets with unknown MAC addresses, i.e. MAC addresses not presently in the CAM table when the number of secure MAC addresses reaches the administrator-defined maximum limit for the port. In this mode, the switch will continue to restrict additional MAC addresses from sending frames until a sufficient number of secure MAC addresses is removed, or the number of maximum allowable addresses is increased. As is the case with the shutdown option, the switch sends out an SNMP trap and a Syslog message, and the violation counter is incremented.

The screenshots showing the difference between Protect, Shutdown and Restrict are present above in the pdf.