**LAB # 05**

**PORT SECURITY**

**OBJECTIVE**

Demonstration of Port Security Mechanism on Ethernet Switch of each port and define violation methods

**Lab Task:**

Switch>en

Switch#sh

Switch#sh mac-address-table

Switch#sh ip interface brief

Switch#config t

Switch(config)#interface range fastEthernet0/1-6

Switch(config-if-range)#switchport mode access

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

Switch(config-if-range)#switch port-security maximum 6

Switch(config-if-range)#switchport port-security maximum 6

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

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

Switch(config-if-range)#exit

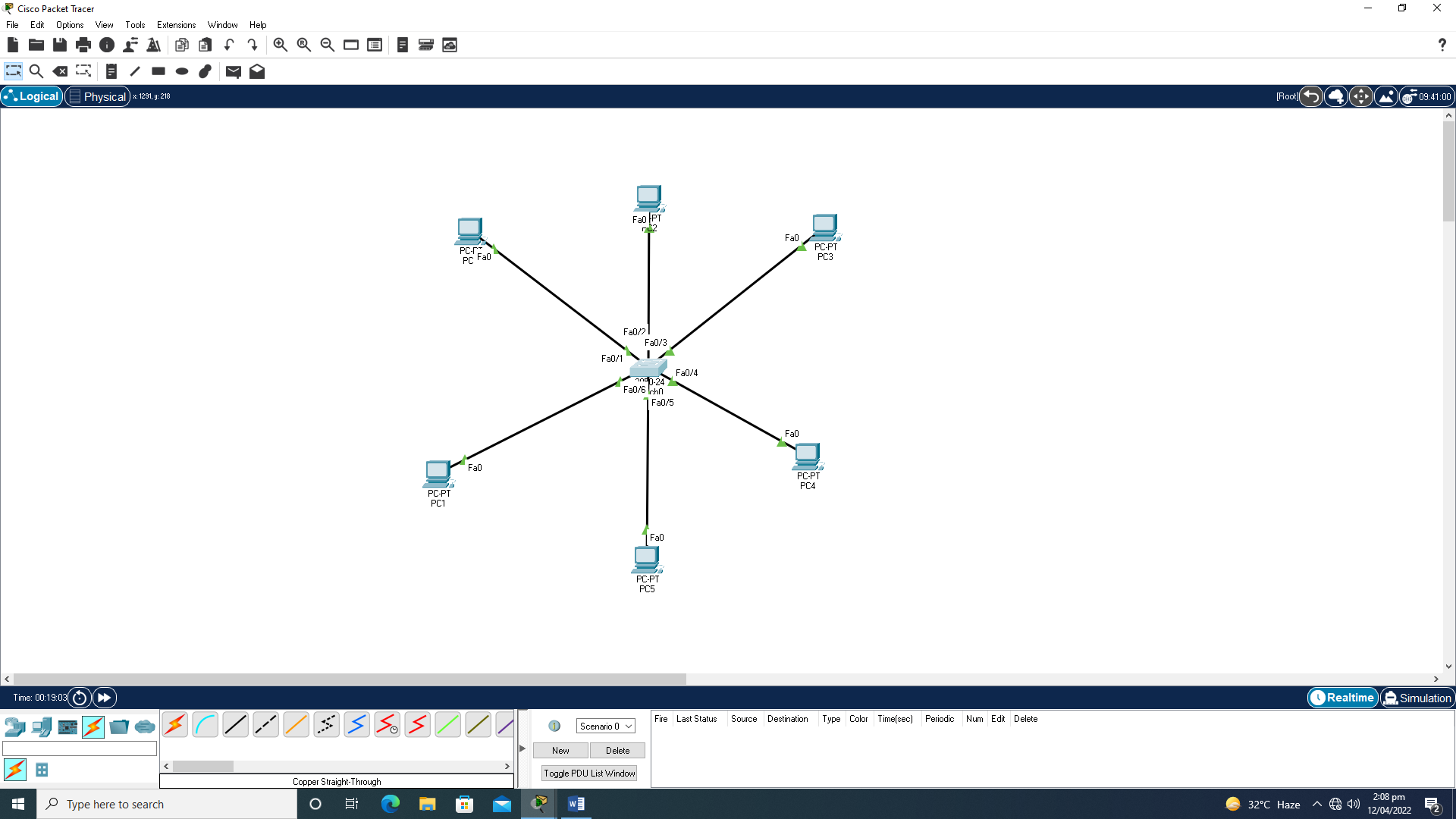
Switch(config)#exit

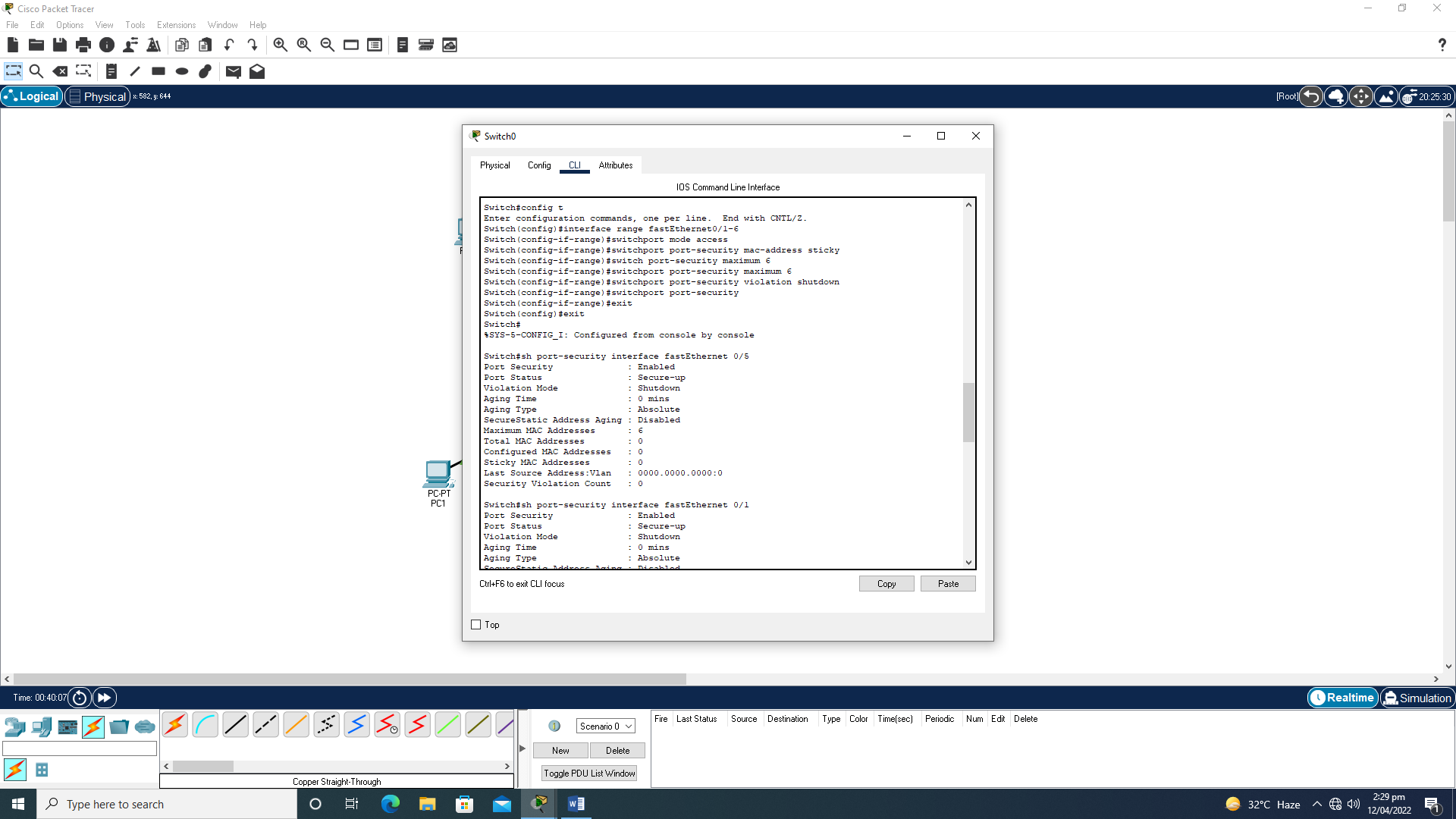
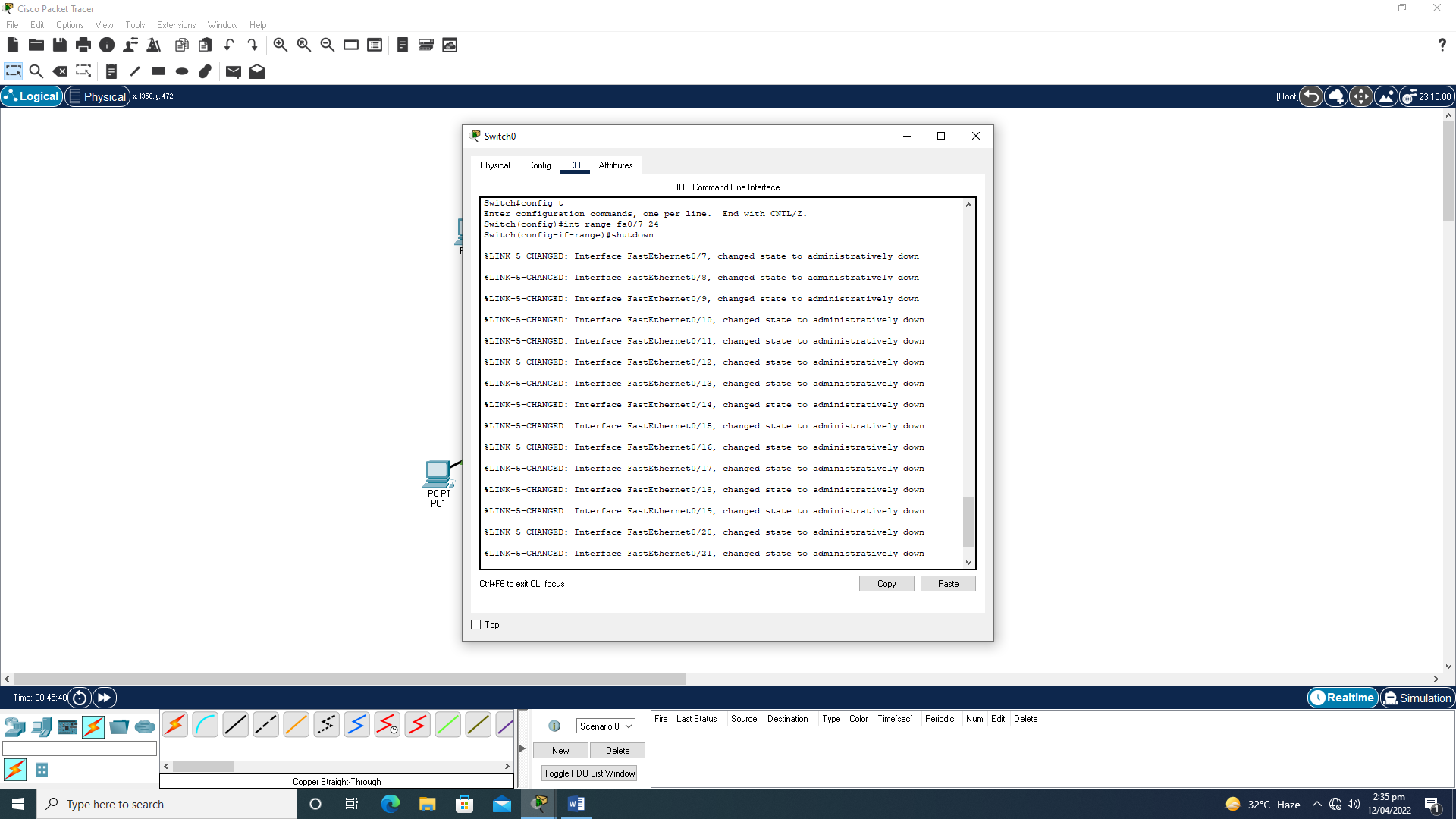
Switch#

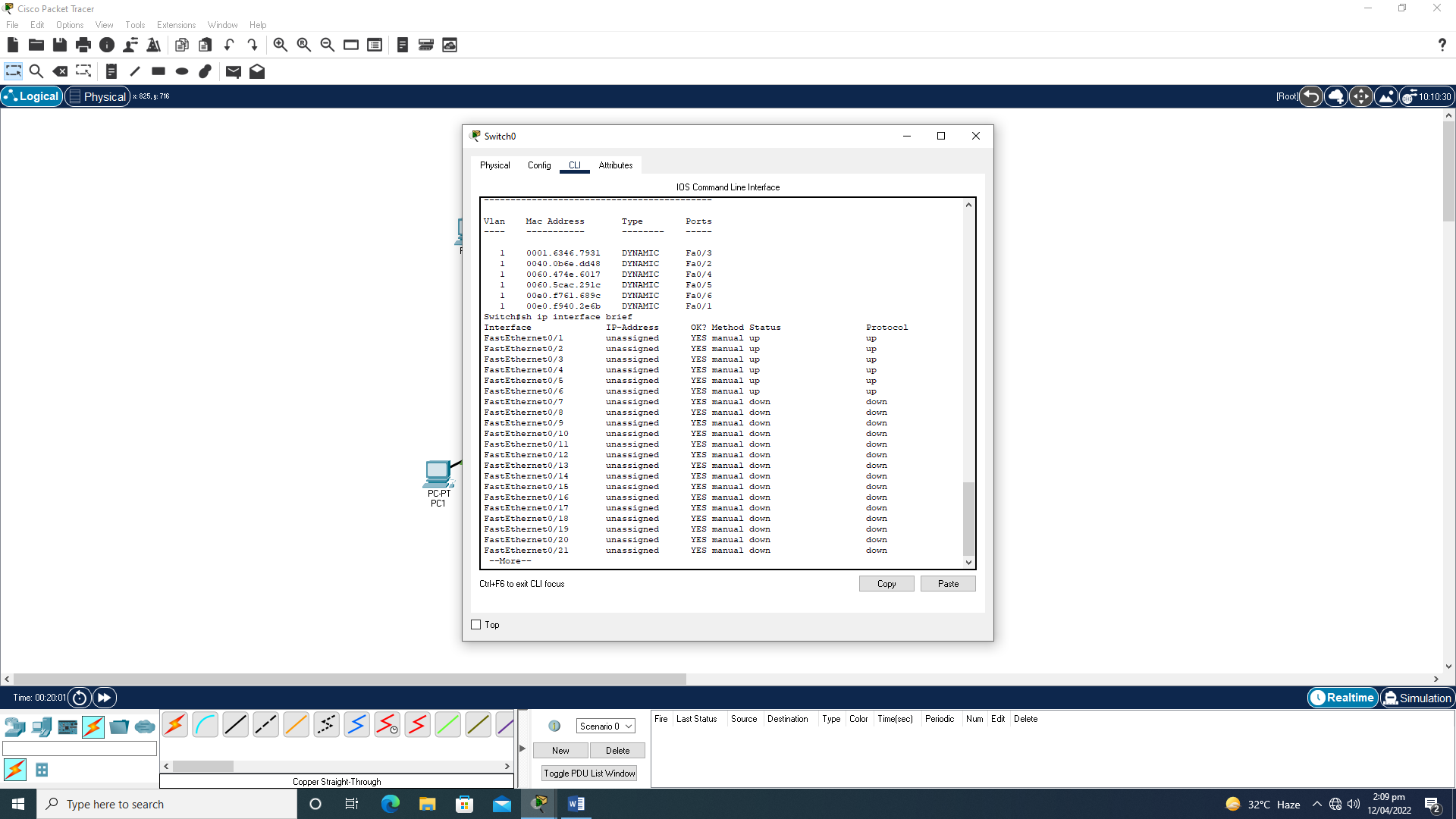
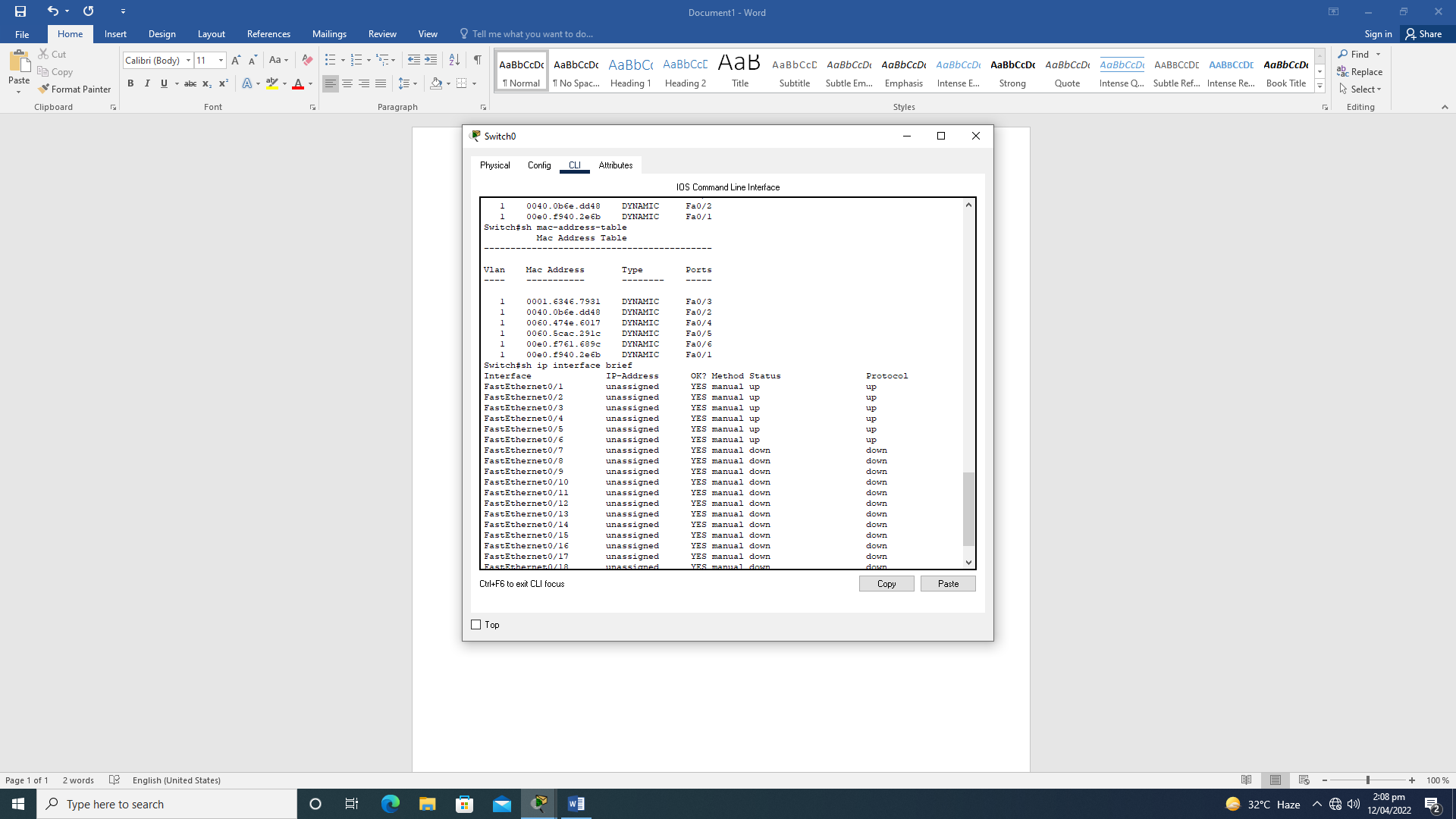
Switch#sh port-security interface fastEthernet 0/5

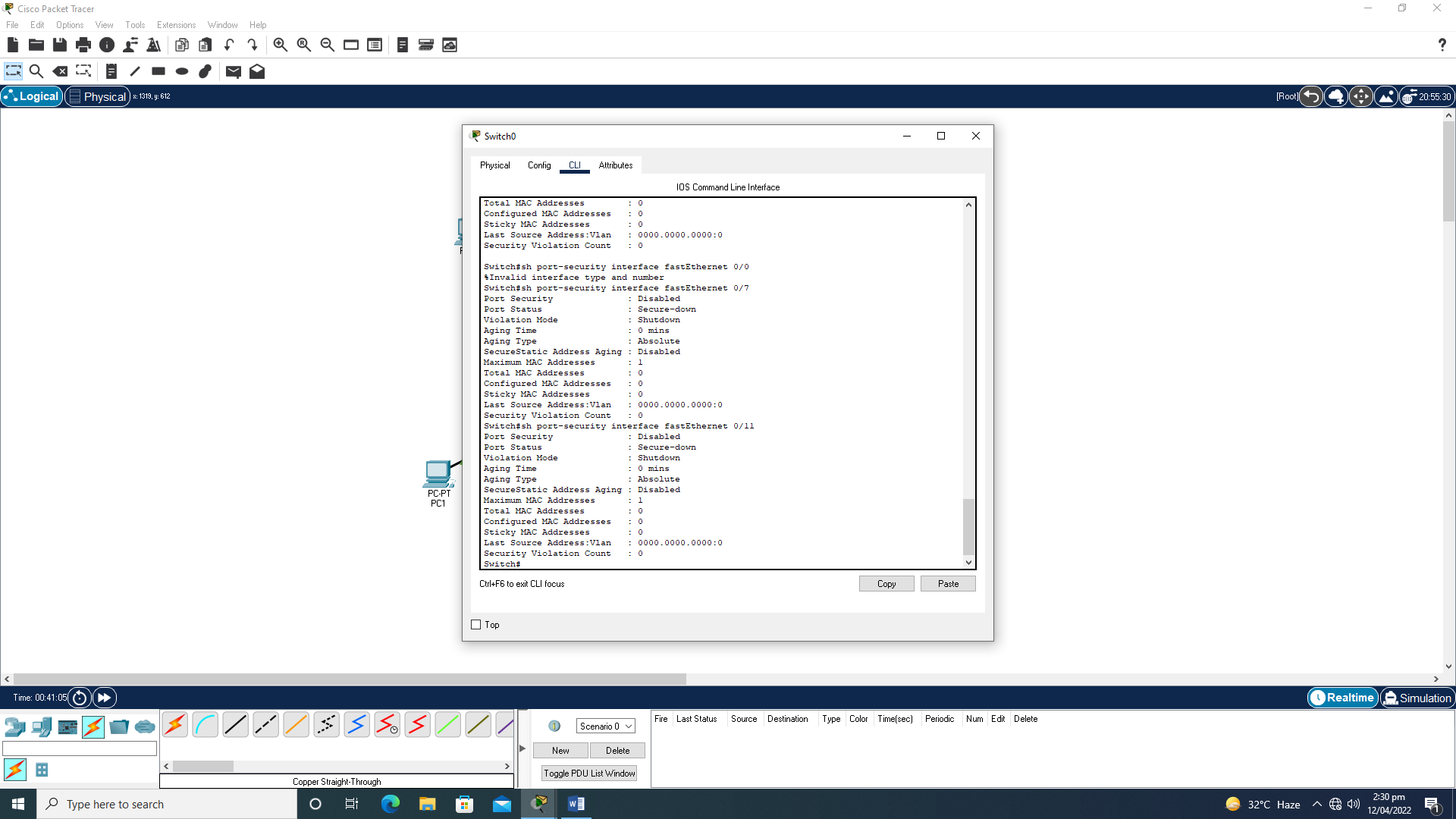
Switch(config)#int range fa0/7-24

Switch(config-if-range)#shutdown









**HOME ASSIGNMENTS**

Q1: Explain MAC address Learning.Also Perform other violation modes on other ports.

**Answer:**

A media access control address is a unique identifier assigned to a network interface controller for use as a network address in communications within a networksegment ans all the Modes are performed above.

Q2: Define inbound ports, outbound ports and well known ports.

**Answer:**

Inbound refers to connections coming-in to a specific device (host/server) from a remote location. e.g. A Web Browser connecting to your Web Server is an inbound connection (to your Web Server) Outbound refers to connections going-out to a specific device from a device/host.

Q3: Differentiate b/w these ports, open, closed, filtered, unfiltered, open filtered, And closed filtered.

**Answer:**

Filtered means that a firewall, filter, or other network obstacle is blocking the port so that Nmap cannot tell whether it is open or closed**.**Closed ports have no application listening on them, though they could open up at any time.