

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 protect 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

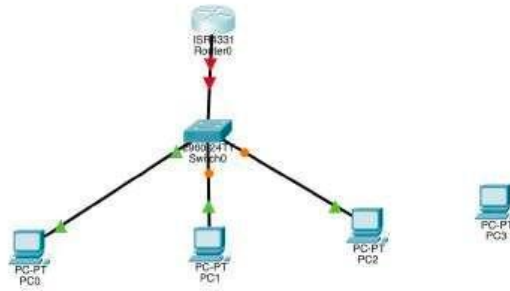
Switch(config-if)#switchport port-security violation shutdown

Switch(config-if)#

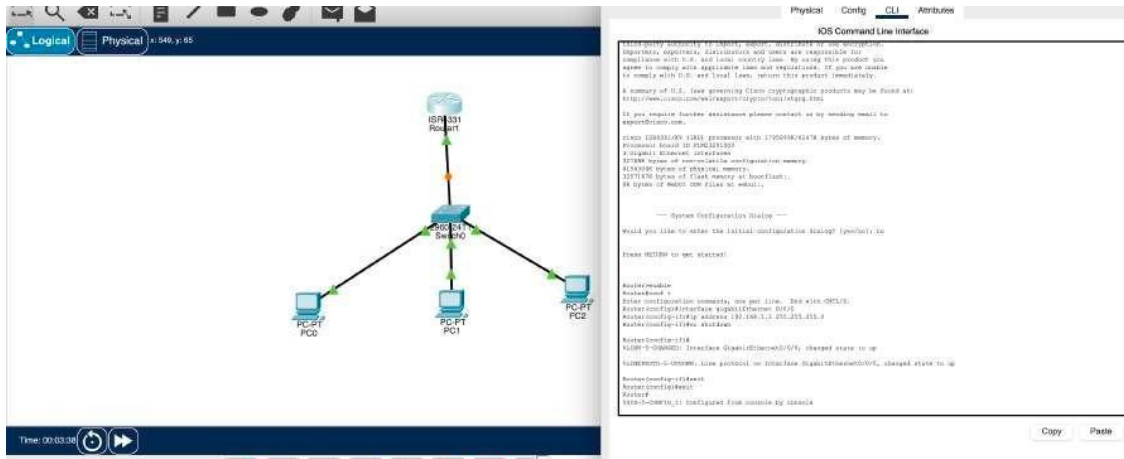
Switch(config-if)#end

Switch#

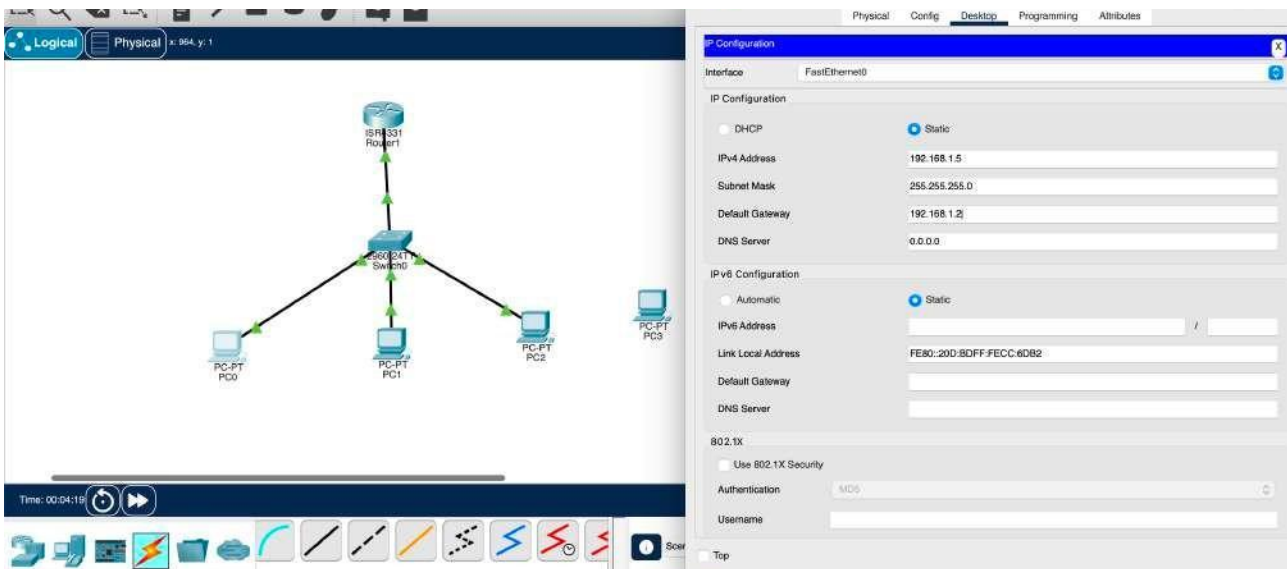
1.



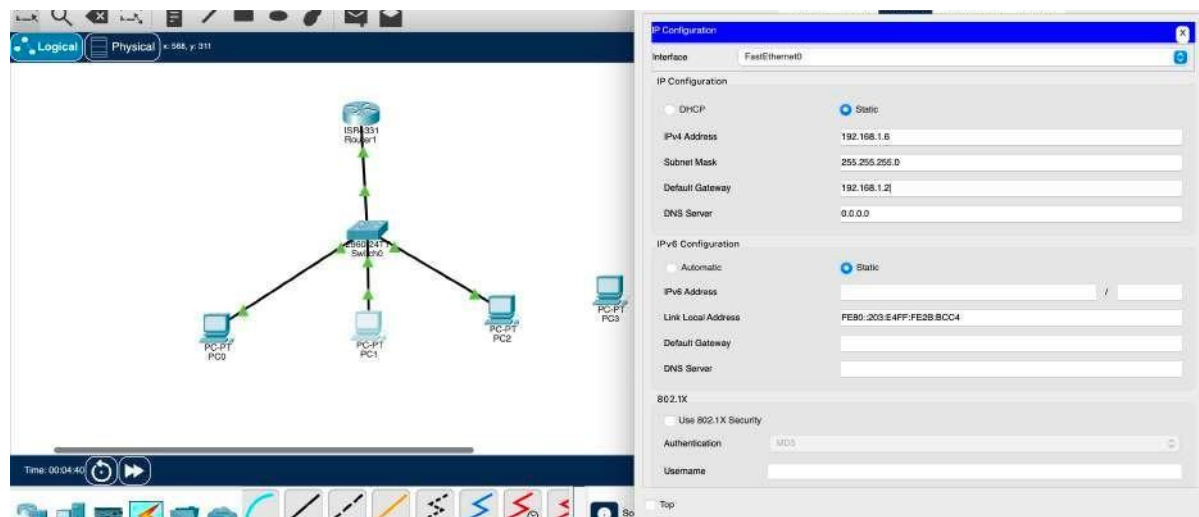
Router Configuration:



IP-Address to PC-1:



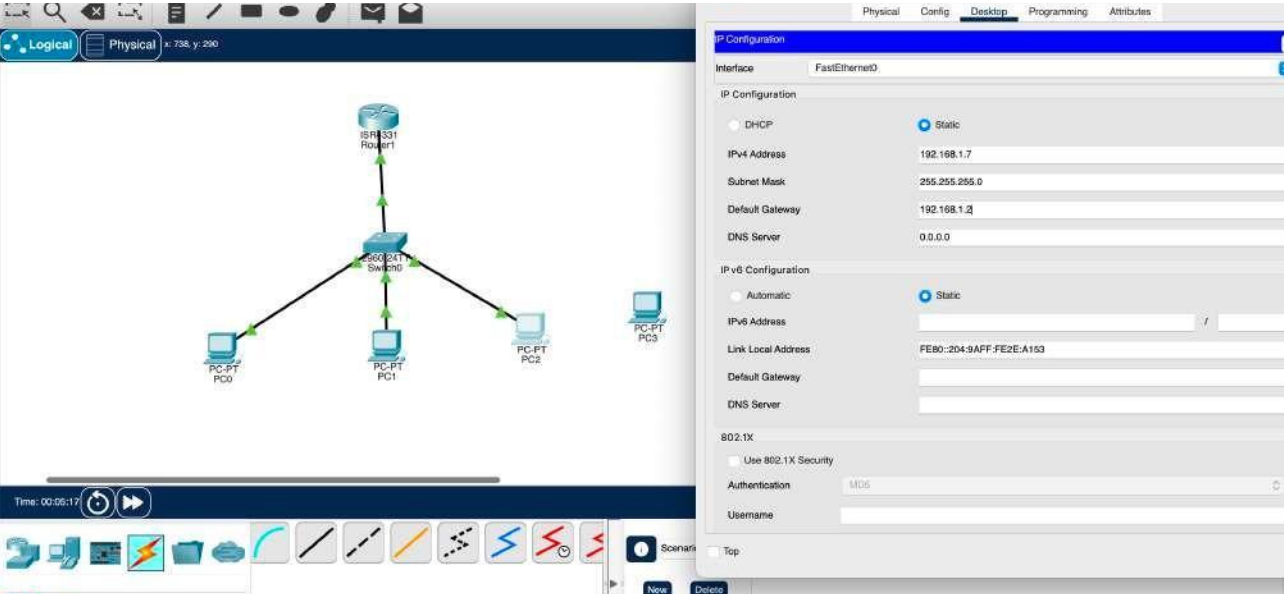
IP-Address to PC-2:



The image shows a network diagram on the left and an IP configuration window on the right. The network diagram features a central 2500 24T Switch connected to an ISR 4331 Router. Three PCs are connected to the switch: PC-PT PC0, PC-PT PC1, and PC-PT PC2. The IP configuration window is for the FastEthernet0 interface, showing the following settings:

Interface	FastEthernet0
IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.1.6
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.2
DNS Server	0.0.0.0
IPv6 Configuration	
<input type="radio"/> Automatic	<input checked="" type="radio"/> Static
IPv6 Address	
Link Local Address	FE80::203:E4FF:FE2B:8CC4
Default Gateway	
DNS Server	
802.1X	
<input type="radio"/> Use 802.1X Security	
Authentication	MD5
Username	

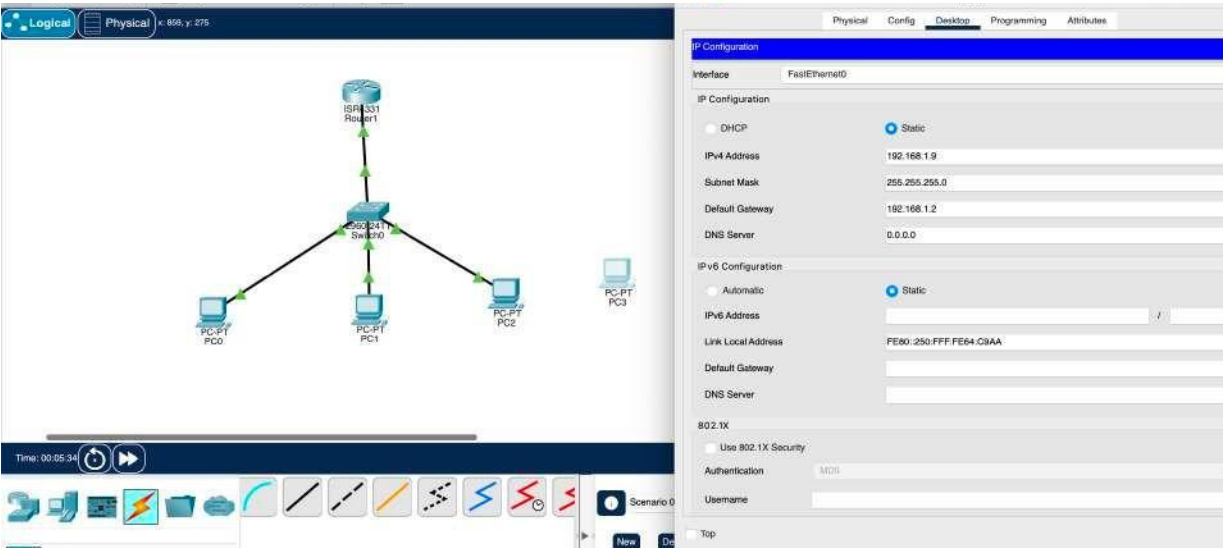
IP-Address to PC-3:



The image shows a network diagram on the left and an IP configuration window on the right. The network diagram features a central 2500 24T Switch connected to an ISR 4331 Router. Three PCs are connected to the switch: PC-PT PC0, PC-PT PC1, and PC-PT PC2. The IP configuration window is for the FastEthernet0 interface, showing the following settings:

Interface	FastEthernet0
IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.1.7
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.2
DNS Server	0.0.0.0
IPv6 Configuration	
<input type="radio"/> Automatic	<input checked="" type="radio"/> Static
IPv6 Address	
Link Local Address	FE80::204:9AFF:FE2E:A153
Default Gateway	
DNS Server	
802.1X	
<input type="radio"/> Use 802.1X Security	
Authentication	MD5
Username	

IP-Address to PC-4:



The image shows a network diagram on the left and an IP configuration window on the right. The network diagram features a central 2500 24T Switch connected to an ISR 4331 Router. Three PCs are connected to the switch: PC-PT PC0, PC-PT PC1, and PC-PT PC2. The IP configuration window is for the FastEthernet0 interface, showing the following settings:

Interface	FastEthernet0
IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.1.9
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.2
DNS Server	0.0.0.0
IPv6 Configuration	
<input type="radio"/> Automatic	<input checked="" type="radio"/> Static
IPv6 Address	
Link Local Address	FE80::250:FFF:FE64:C9AA
Default Gateway	
DNS Server	
802.1X	
<input type="radio"/> Use 802.1X Security	
Authentication	MD5
Username	

Ping from PC-1 to all PC's:

The network diagram shows a central 2600-AT Switch connected to three PCs (PC-PT PC0, PC-PT PC1, and PC-PT PC2) and an ISR331 Router. The command prompt shows the results of a ping command from PC-1 to all other PCs.

```
Command Prompt
C:\>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=128
Reply from 192.168.1.1: bytes=32 time=1ms TTL=128
Reply from 192.168.1.1: bytes=32 time=1ms TTL=128
Reply from 192.168.1.1: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milliseconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milliseconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.1.3
Pinging 192.168.1.3 with 32 bytes of data:
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milliseconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Ping from PC-2 to all PC's:

The network diagram shows a central 2600-AT Switch connected to three PCs (PC-PT PC0, PC-PT PC1, and PC-PT PC2) and an ISR331 Router. The command prompt shows the results of a ping command from PC-2 to all other PCs.

```
Command Prompt
C:\>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=128
Reply from 192.168.1.1: bytes=32 time=1ms TTL=128
Reply from 192.168.1.1: bytes=32 time=1ms TTL=128
Reply from 192.168.1.1: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milliseconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milliseconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.1.3
Pinging 192.168.1.3 with 32 bytes of data:
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milliseconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Ping from PC-3 to all PC's:

The network diagram shows a central 2600-AT Switch connected to three PCs (PC-PT PC0, PC-PT PC1, and PC-PT PC2) and an ISR331 Router. The command prompt shows the results of a ping command from PC-3 to all other PCs.

```
Command Prompt
C:\>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=128
Reply from 192.168.1.1: bytes=32 time=1ms TTL=128
Reply from 192.168.1.1: bytes=32 time=1ms TTL=128
Reply from 192.168.1.1: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milliseconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128

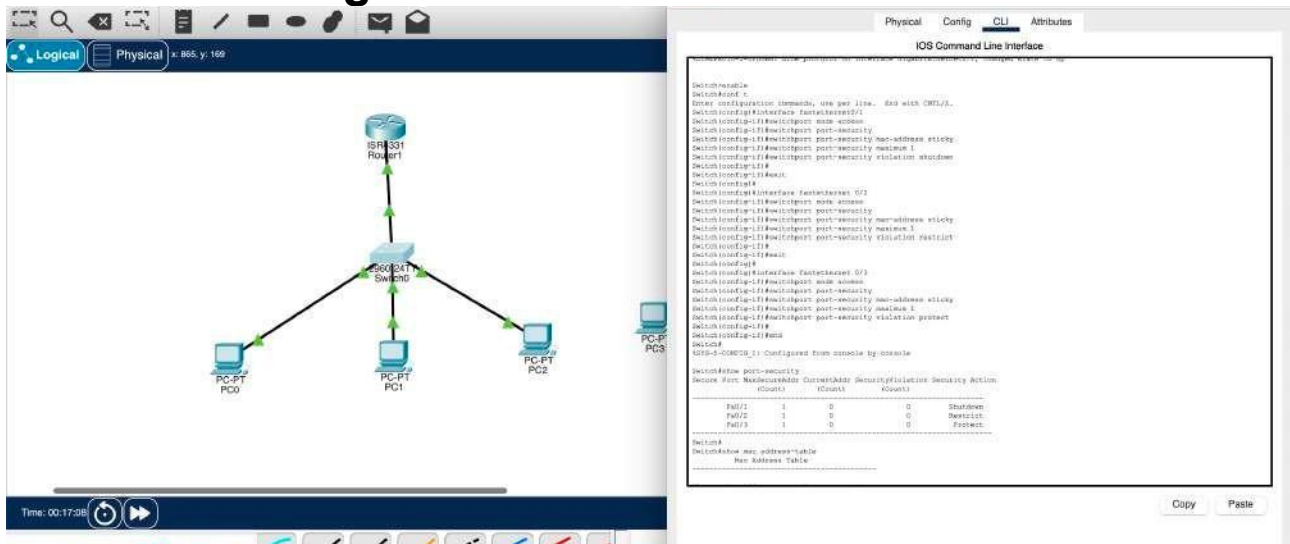
Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milliseconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.1.3
Pinging 192.168.1.3 with 32 bytes of data:
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128

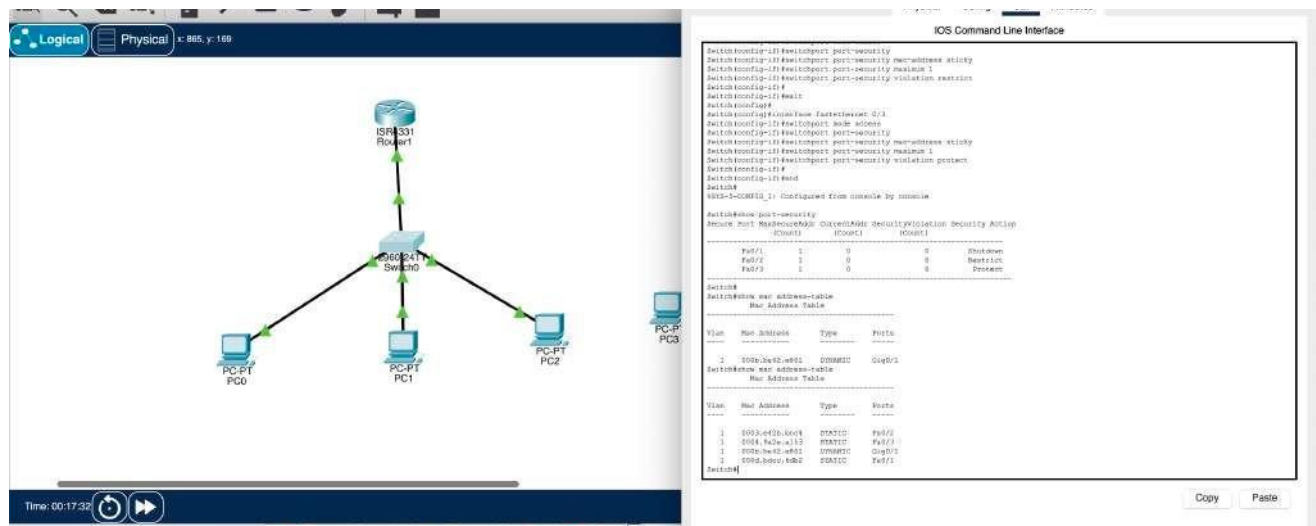
Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milliseconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

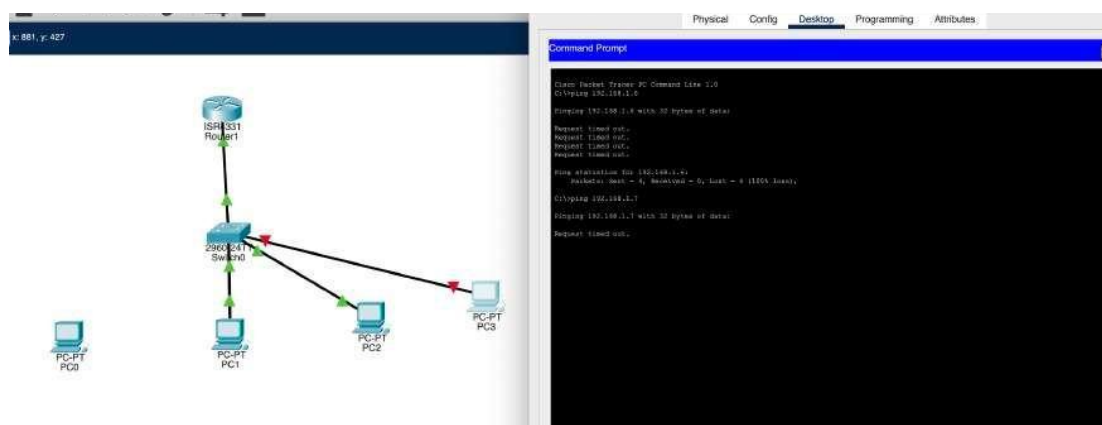
Interface Configuration Shutdown/Restrict/Protected:



Interface Modes and Mac-address table:



Shutdown:



Physical Config CLI Attributes

IOS Command Line Interface

```

Switch(config-if)#switchport port-security violation protect
Switch(config-if)#
Switch(config-if)#end
Switch#
%SYS-5-CONFIG_1: Configured from console by console

Switch#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
-----
Fa0/1      1      0      0      Shutdown
Fa0/2      1      0      0      Restrict
Fa0/3      1      0      0      Protect

Switch#
Switch#show mac address-table
Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----
1       000b.be42.e801   DYNAMIC   Gig0/1
Switch#show mac address-table
Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----
1       0003.e42b.bcc4   STATIC    Fa0/2
1       0004.9a2e.a153   STATIC    Fa0/3
1       000b.be42.e801   DYNAMIC   Gig0/1
1       000d.bdc6.6db2   STATIC    Fa0/1

Switch#
%LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINK-3-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINK-3-CHANGED: Interface FastEthernet0/1, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
  
```

Copy Paste

Line protocol is down in the shutdown

IOS Command Line Interface

```

Switch#show mac address-table
Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----
1       0003.e42b.bcc4   STATIC    Fa0/2
1       0004.9a2e.a153   STATIC    Fa0/3
1       000b.be42.e801   DYNAMIC   Gig0/1
1       000d.bdc6.6db2   STATIC    Fa0/1

Switch#
%LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINK-3-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINK-3-CHANGED: Interface FastEthernet0/1, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

Switch#show ip interface brief
Interface IP-Address OK? Method Status Protocol
FastEthernet0/1 unassigned YES manual down down
FastEthernet0/2 unassigned YES manual up up
FastEthernet0/3 unassigned YES manual up up
FastEthernet0/4 unassigned YES manual down down
FastEthernet0/5 unassigned YES manual down down
FastEthernet0/6 unassigned YES manual down down
FastEthernet0/7 unassigned YES manual down down
FastEthernet0/8 unassigned YES manual down down
FastEthernet0/9 unassigned YES manual down down
FastEthernet0/10 unassigned YES manual down down
FastEthernet0/11 unassigned YES manual down down
FastEthernet0/12 unassigned YES manual down down
FastEthernet0/13 unassigned YES manual down down
FastEthernet0/14 unassigned YES manual down down
FastEthernet0/15 unassigned YES manual down down
FastEthernet0/16 unassigned YES manual down down
FastEthernet0/17 unassigned YES manual down down
FastEthernet0/18 unassigned YES manual down down
FastEthernet0/19 unassigned YES manual down down
FastEthernet0/20 unassigned YES manual down down
FastEthernet0/21 unassigned YES manual down down
  
```

Copy Paste

Interface Status-down

Physical Config CLI Attributes

IOS Command Line Interface

Interface	Line	Protocol	Admin	Oper	Line	Protocol	Admin	Oper
FastEthernet0/1	unassigned	FE3	manual	down	down			
FastEthernet0/2	unassigned	FE3	manual	down	down			
FastEthernet0/3	unassigned	FE3	manual	down	down			
FastEthernet0/4	unassigned	FE3	manual	down	down			
FastEthernet0/5	unassigned	FE3	manual	down	down			
FastEthernet0/6	unassigned	FE3	manual	down	down			
FastEthernet0/7	unassigned	FE3	manual	down	down			
FastEthernet0/8	unassigned	FE3	manual	down	down			
FastEthernet0/9	unassigned	FE3	manual	down	down			
FastEthernet0/10	unassigned	FE3	manual	down	down			
FastEthernet0/11	unassigned	FE3	manual	down	down			
FastEthernet0/12	unassigned	FE3	manual	down	down			
FastEthernet0/13	unassigned	FE3	manual	down	down			
FastEthernet0/14	unassigned	FE3	manual	down	down			
FastEthernet0/15	unassigned	FE3	manual	down	down			
FastEthernet0/16	unassigned	FE3	manual	down	down			
FastEthernet0/17	unassigned	FE3	manual	down	down			
FastEthernet0/18	unassigned	FE3	manual	down	down			
FastEthernet0/19	unassigned	FE3	manual	down	down			
FastEthernet0/20	unassigned	FE3	manual	down	down			
FastEthernet0/21	unassigned	FE3	manual	down	down			
FastEthernet0/22	unassigned	FE3	manual	down	down			
FastEthernet0/23	unassigned	FE3	manual	down	down			

Switch#show port-security

Secure Port	MaxSecureAddr	CurrentAddr	SecurityViolation	Security Action
(Count)	(Count)	(Count)		
Fast0/1	2	2	2	Shutdown
Fast0/2	2	2	0	Restrict
Fast0/3	2	2	0	Protect

Switch#show interface Fast0/1

```

FastEthernet0/1
  Vlan1 input: detected at *** marker.
Switch#show fast0/1
  Vlan1 input: detected at *** marker.
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int fast0/1
Switch(config-if)#shutdown
VLAN5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
Switch(config-if)#no shutdown
VLAN5-CHANGED: Interface FastEthernet0/1, changed state to up
Switch(config-if)#
VLAN5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
  
```

Manually changing the interface from shutdown to no shutdown

Restrict:

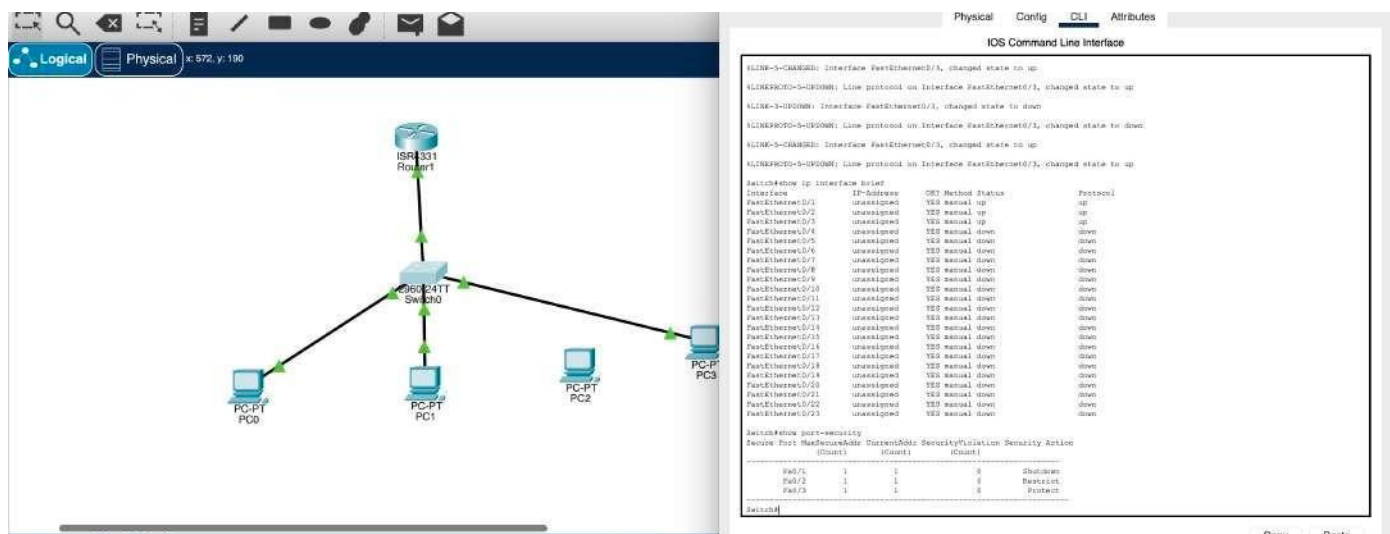
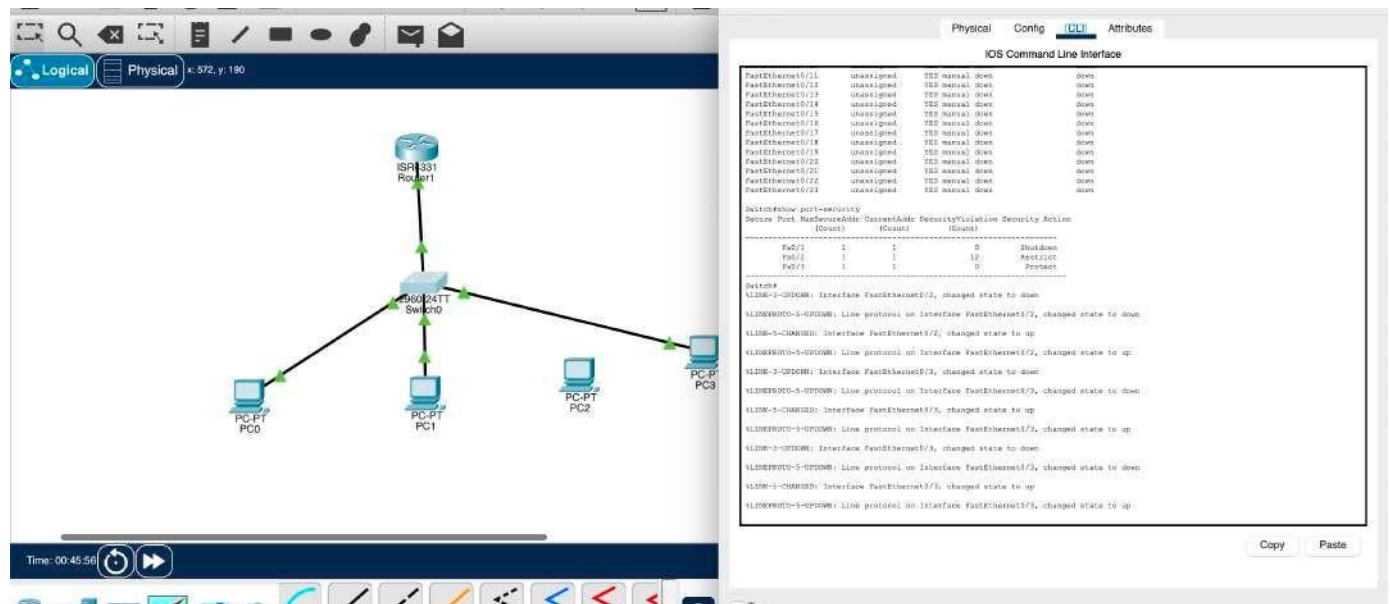
Physical Config Desktop Programming Attributes

Command Prompt

```

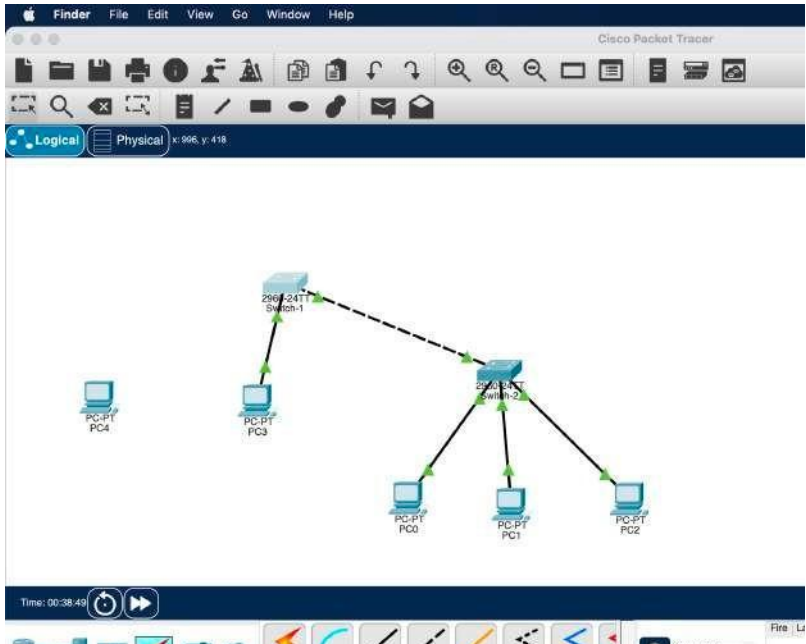
C:\Users\PC>ipconfig /all
IP Configuration
Ethernet adapter Ethernet0:
. . .
IP Address. . . : 192.168.1.1
Subnet Mask . . . : 255.255.255.0
Default Gateway . . . : 192.168.1.1
. . .
C:\Users\PC>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    . . .
C:\Users\PC>ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    . . .
C:\Users\PC>ping 192.168.1.3
Pinging 192.168.1.3 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    . . .
  
```


Line Interface is up



Count =0 for all.

2.



Switch-1 IP Address configuration:

The screenshot shows the Cisco Packet Tracer interface with the 'CLI' tab selected for 'Switch-1'. The 'IOS Command Line Interface' window displays the following configuration commands and status messages:

```
Press RETURN to get started!

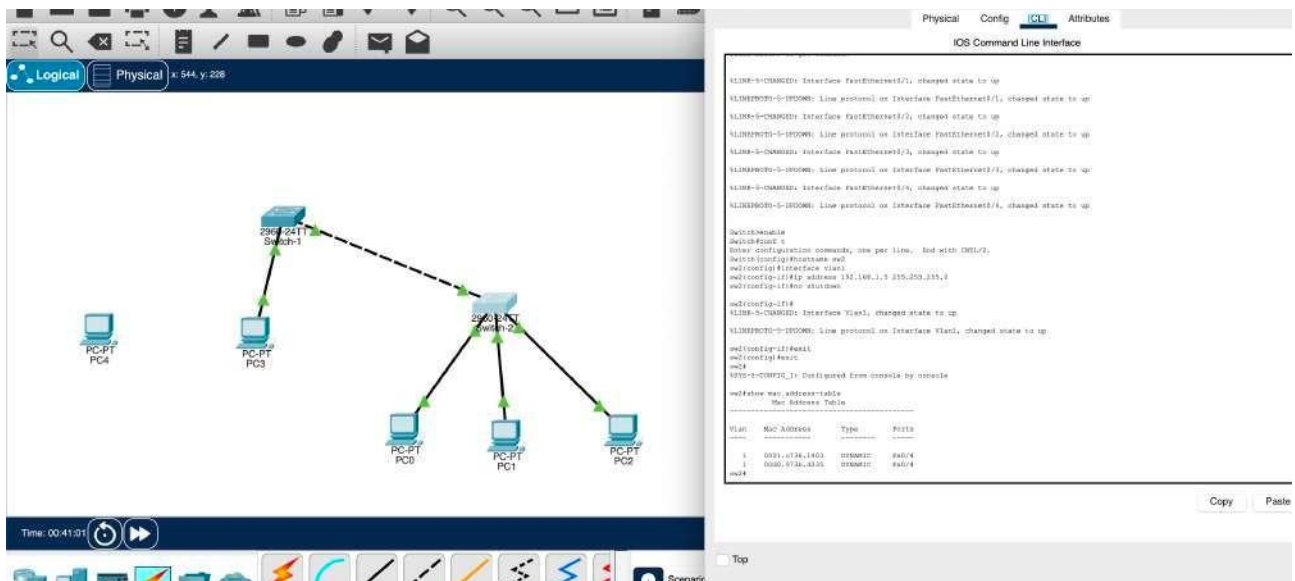
Switch-1>
Switch-1>enable
Switch-1#configure terminal
Switch-1(config)#hostname sw1
Switch-1(config)#
Switch-1(config)#interface Vlan1
Switch-1(config-if)#ip address 192.168.1.6 255.255.255.0
Switch-1(config-if)#no shutdown
Switch-1(config-if)#
Switch-1(config-if)#exit
Switch-1(config)#exit
Switch-1#show ip interface brief
Switch-1#
Switch-1#show ip address-table
Switch-1#
```

The status messages indicate that the interfaces are up and the configuration is successful. Below the CLI window, a 'New Address Table' is displayed:

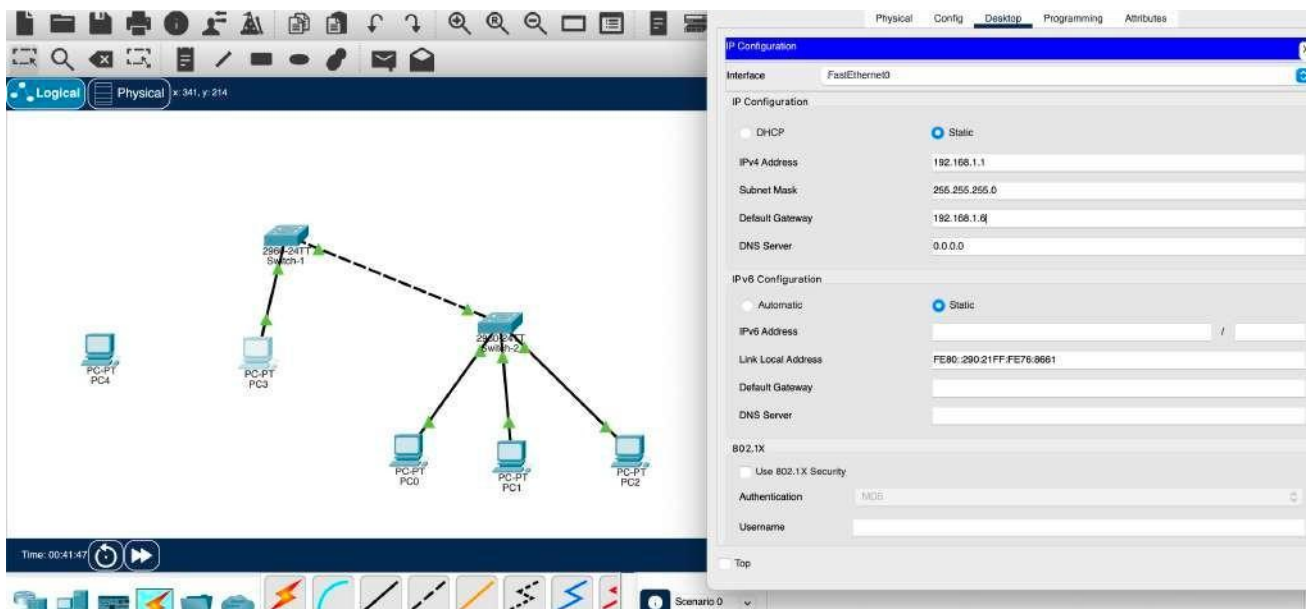
Vlan	Mac Address	Type	Ports
1	9846.8531.2394	DMZ	Port 1

The bottom status bar shows 'Time: 00:38:17'.

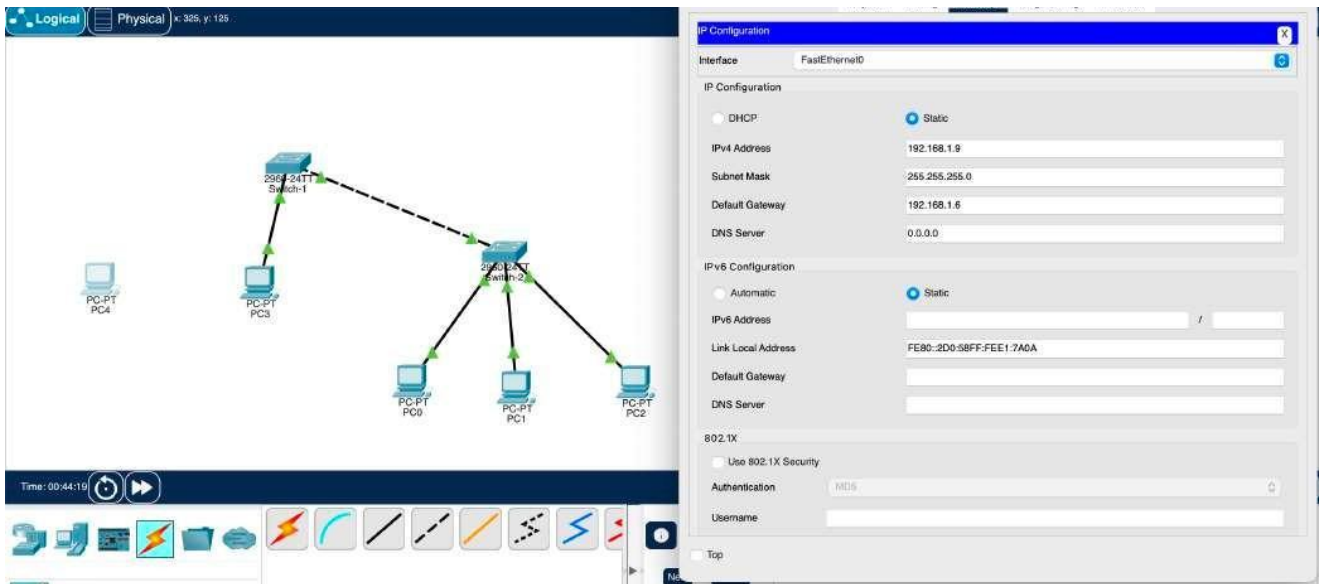
Switch-2 IP Address:



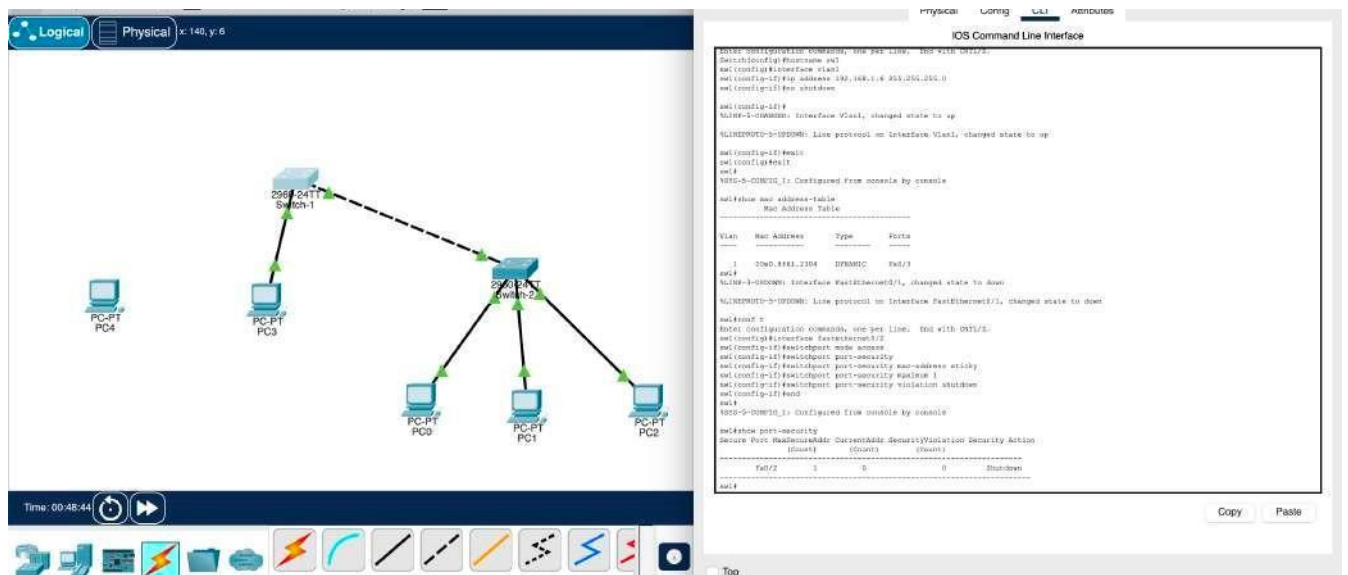
PC IP-Address Configuration:

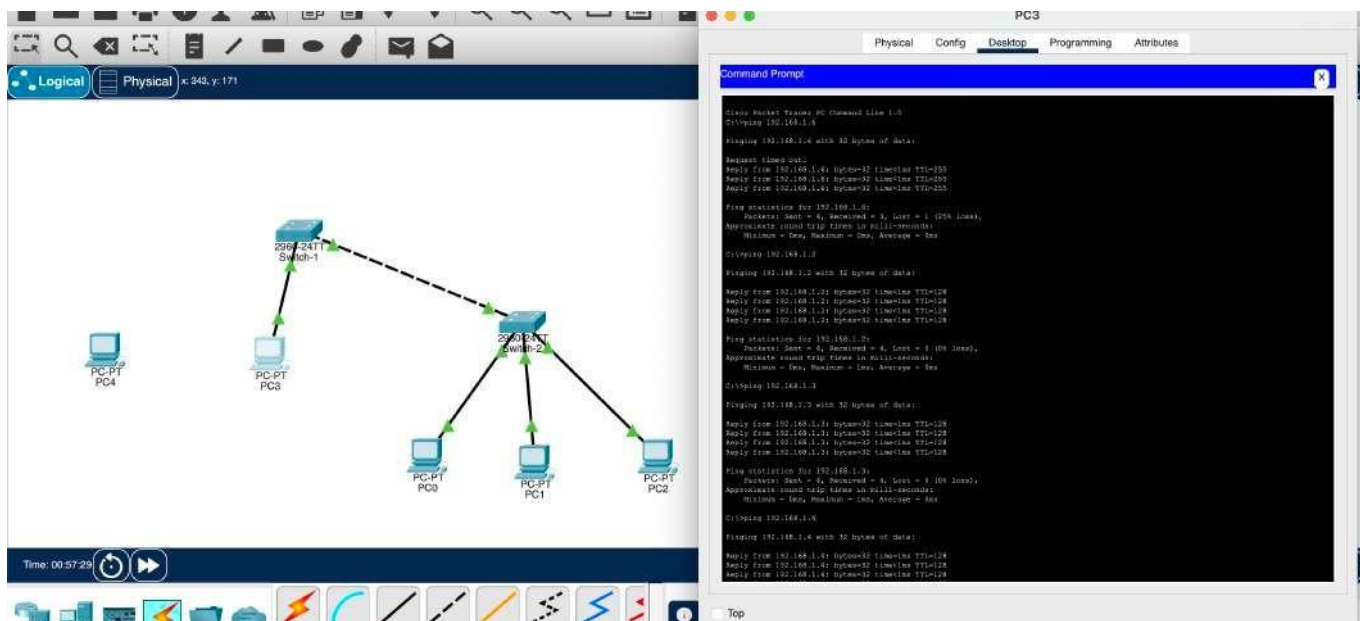
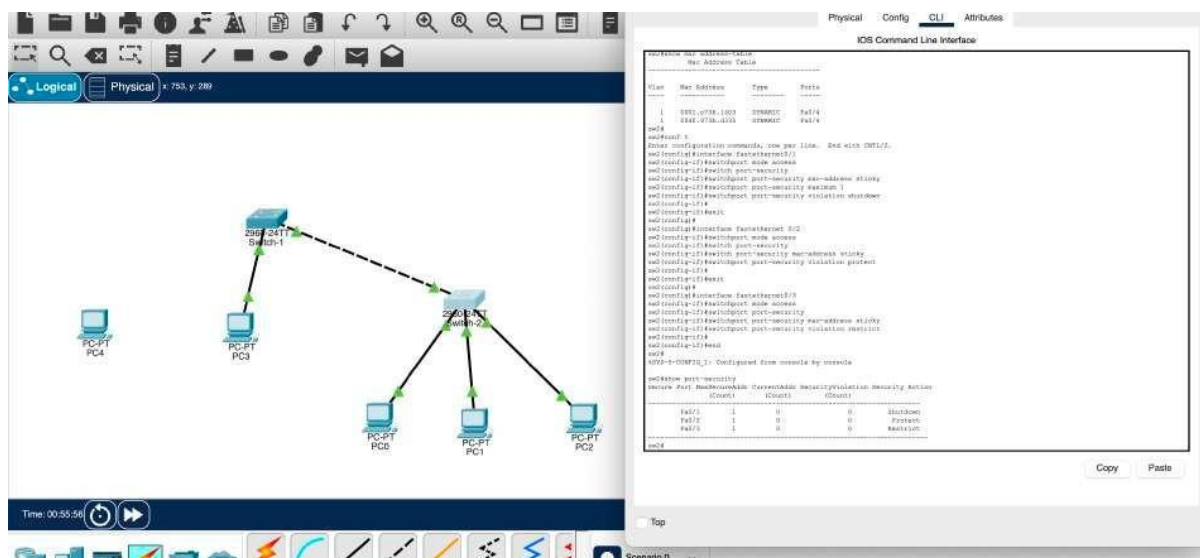


Switch-1:

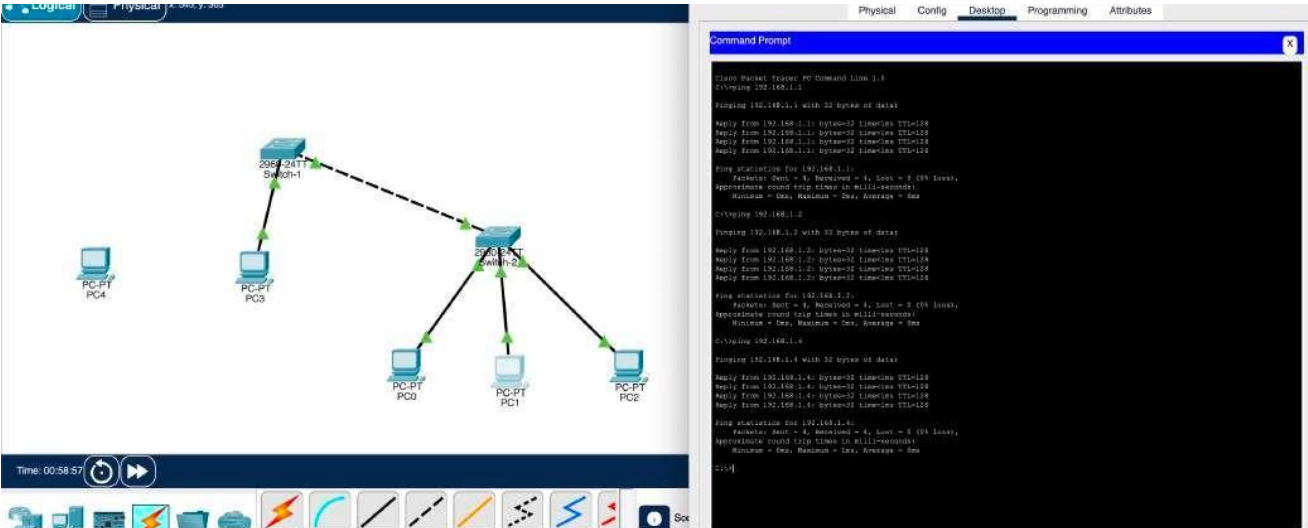


Switch-2:

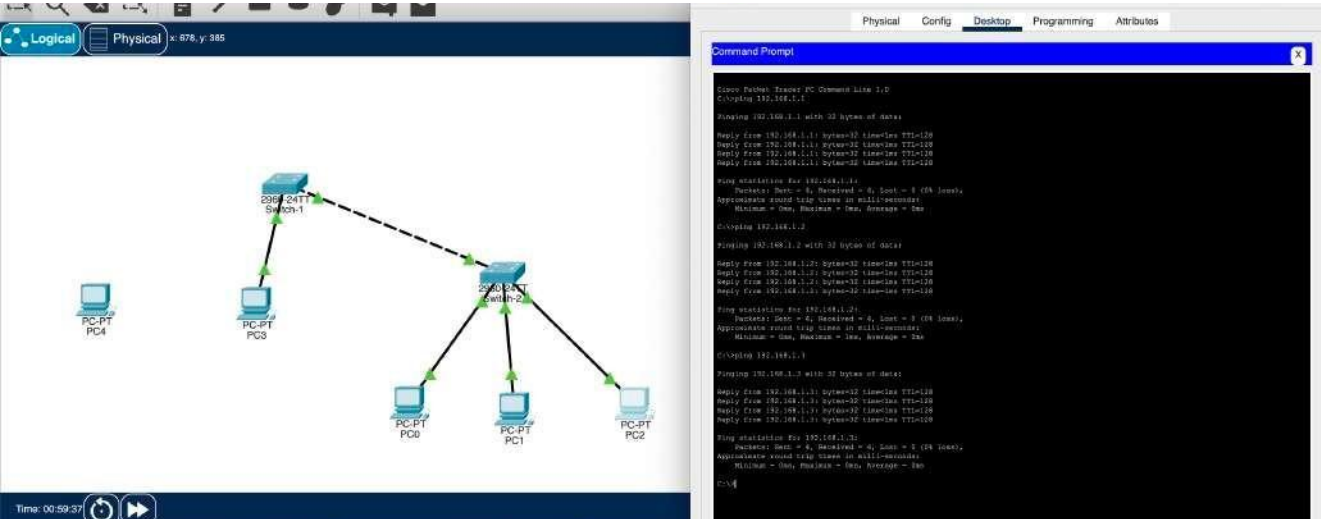




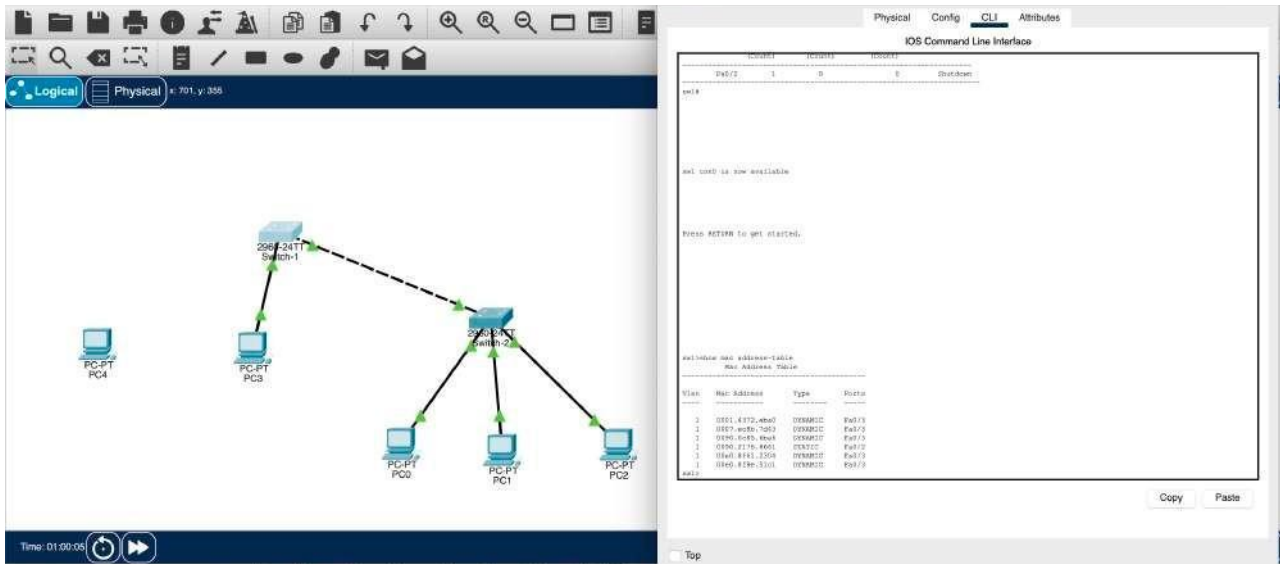
Ping from PC-1 to other devices:



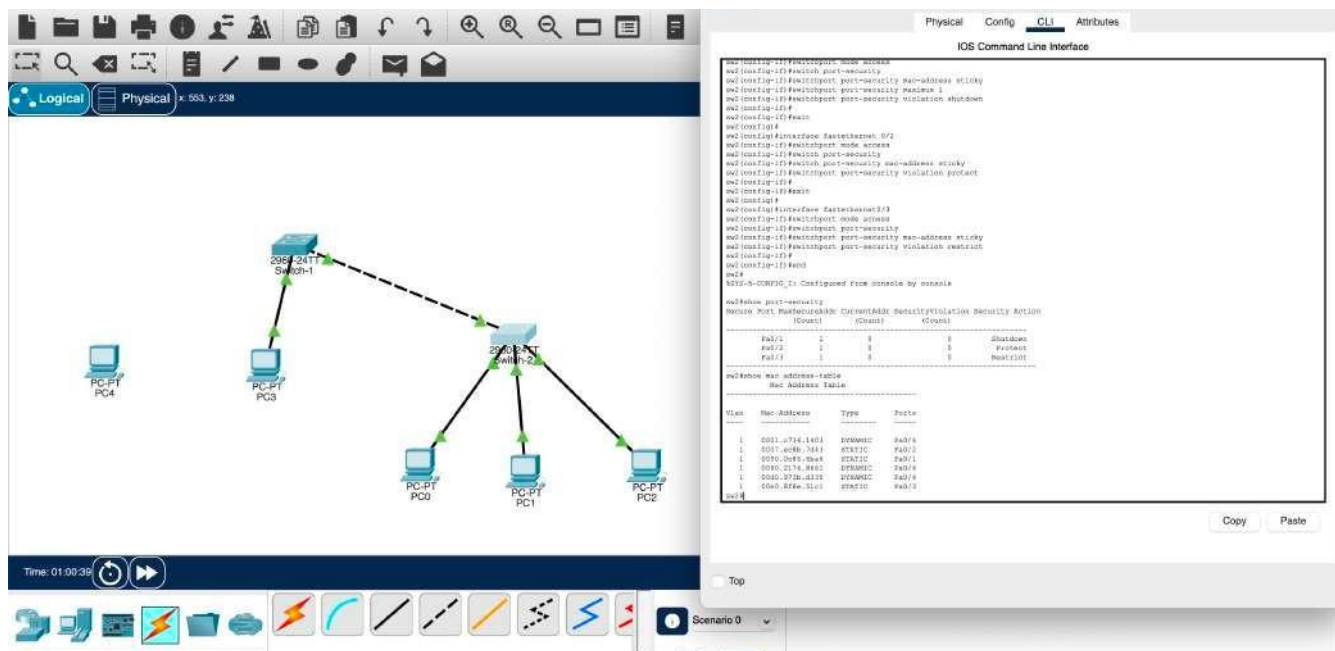
Ping from PC-2 to other devices:



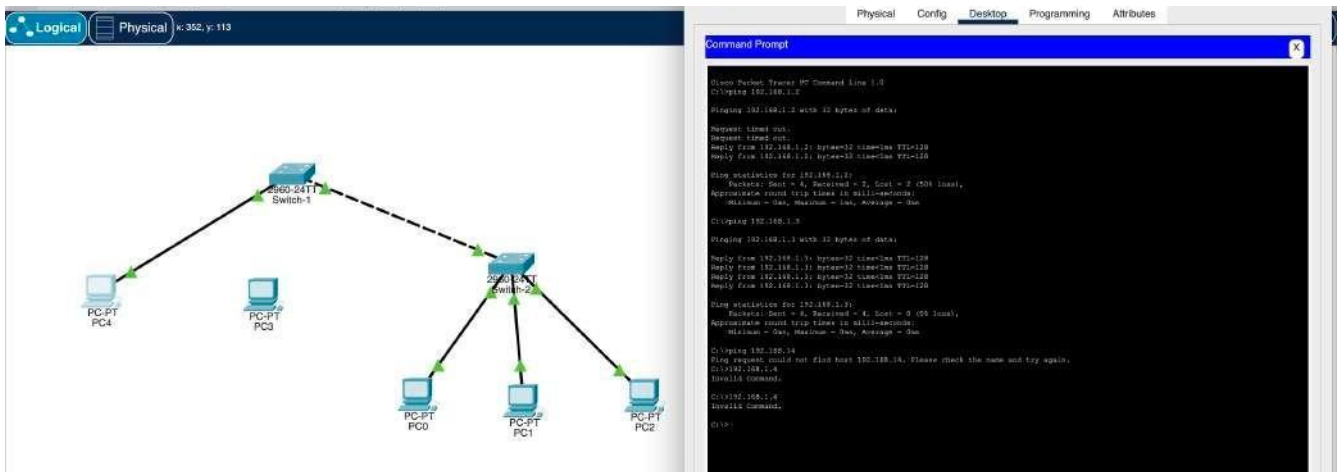
Switch-1:



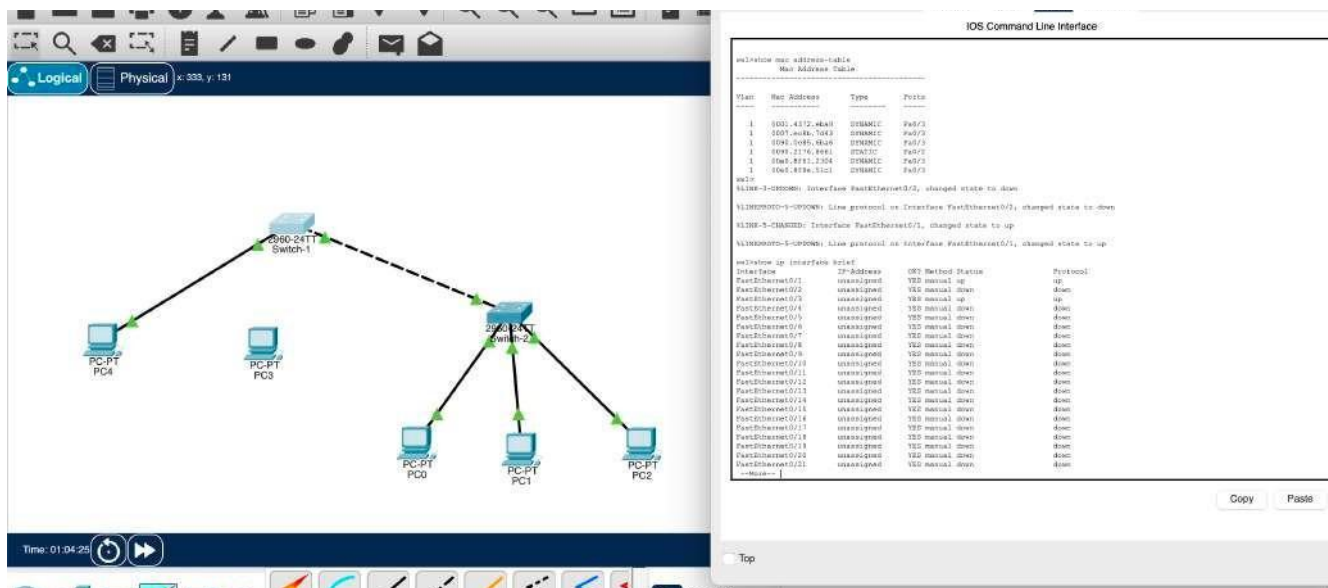
Switch-2:



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 protect 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.

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

