**VIT-AP UNIVERSITY, ANDHRA PRADESH**

**CSE3003 – Computer Networks - Lab Sheet: 4**

**Academic year:** 2023-2024  **Branch/ Class:** B.Tech

**Semester:** Fall  **Date: 16/02/24**

**Faculty Name:** Prof. S.Gopikrishnan  **School:** SCOPE

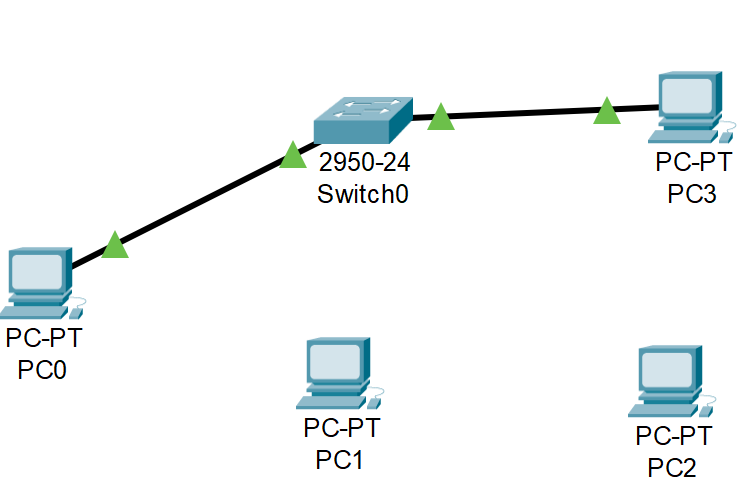
**Student name: Aman Sahu Reg. no.:22BCE7224**

**LAB 4**

1. **Port Security: Port-Security Configuration to prevent MAC flooding attack**

Procedure:

1. Build the network topology: PC1  connects to fa0/1  and  PC2 to fa0/2 of the switch



**Addressing Table:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Device** | **Interface** | **IP Address** | **Subnet Mask** |
| PC0 | NIC | 192.168.1.1 | 255.255.255.0 |
| PC1 | NIC | 192.168.1.2 | 255.255.255.0 |
| PC2 | NIC | 192.168.1.3 | 255.255.255.0 |
| PC3 | NIC | 192.168.1.4 | 255.255.255.0 |

1. Now configure switch port security on switch interfaces.

We’ll configure port security interfaces on fa0/1 and fa0/2.

To do this, we’ll:

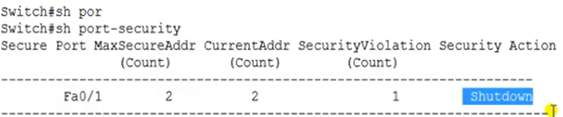
* Configure the port as an **access port**
* Enable **port security**
* Define which **MAC addresses** are allowed to send frames through this interface.

**Objective:**

Configure switch should connect only two devices and verify port security using:

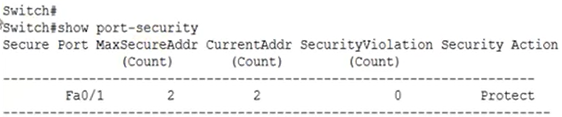
Case 1:

* Default MAC address to learn is 2
* Default violation mode is shut down.
* Expected output:



Case 2:

* Default MAC address to learn is 2
* Change violation mode to protect mode.
* Expected output:



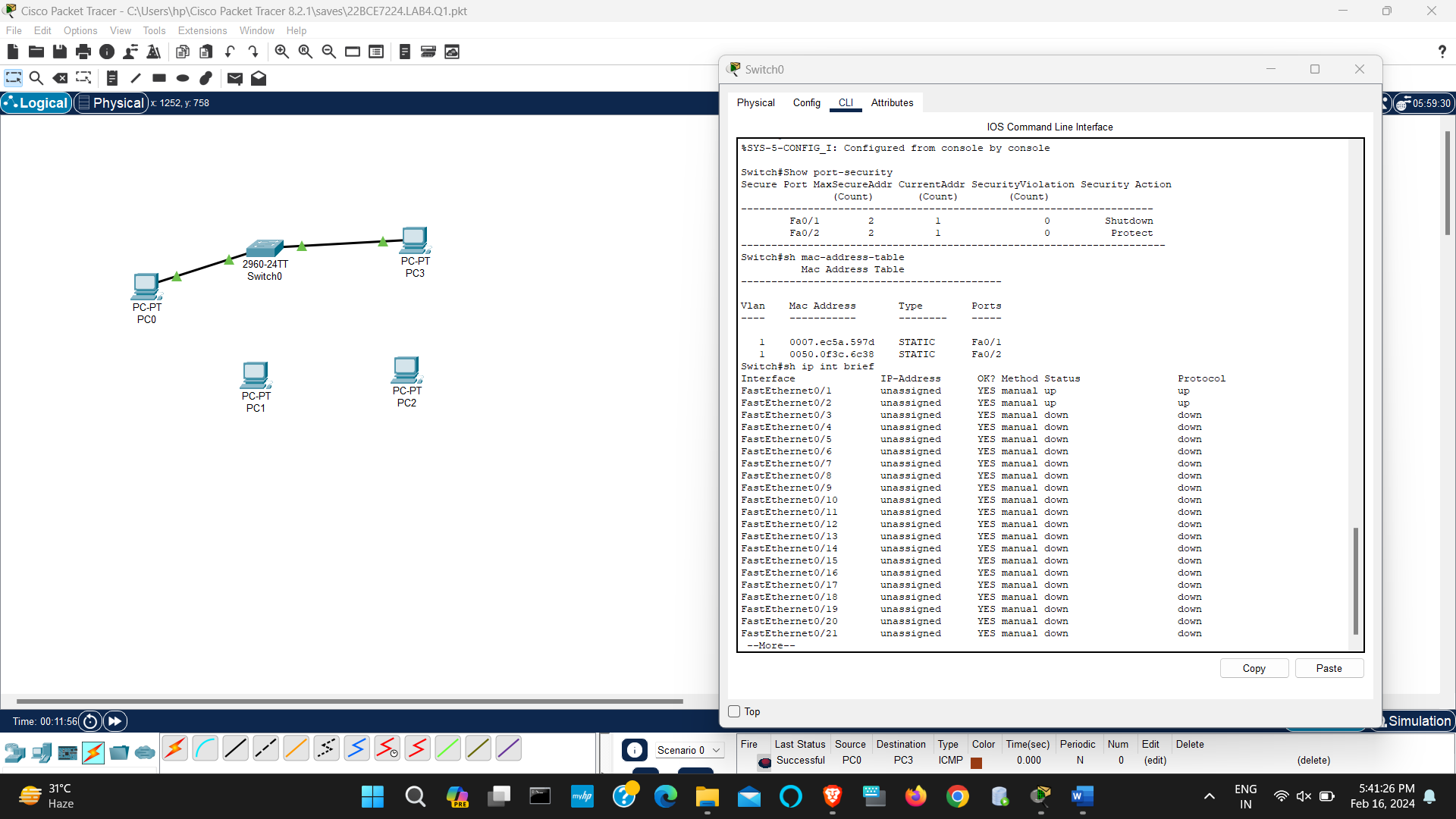
**Note:**

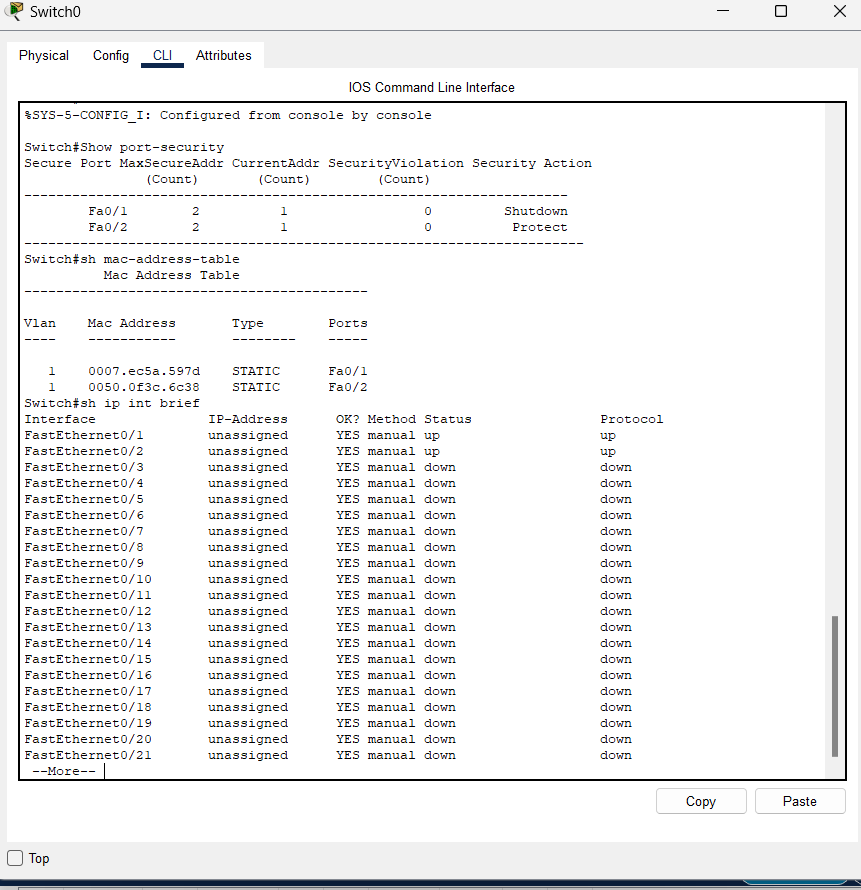
**Use the following comments to get your outputs for each case**

Switch# Show port-security

Switch# sh mac-address-table

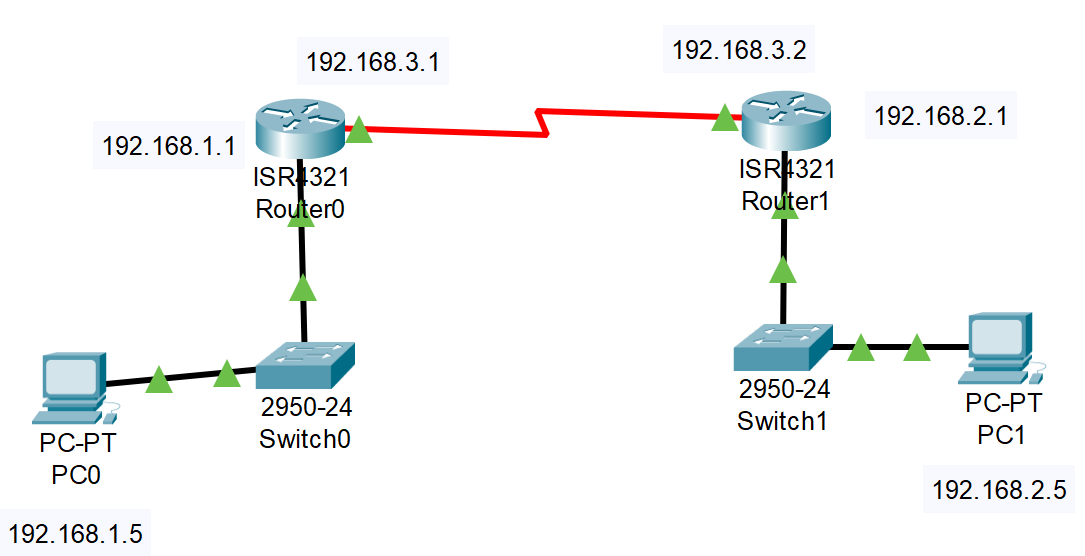
Switch# sh ip int brief

+

****

**2. HDLC (High-level Data Link Control) and PPP (****Point to Point Protocol):**

1. Desing the network given below:



**Addressing Table:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Device** | **Interface** | **IP Address** | **Subnet Mask** |
| PC1 | NIC | 192.168.1.5 | 255.255.255.0 |
| PC2 | NIC | 192.168.2.5 | 255.255.255.0 |
| Router1 Fast Ethernet 0/1 | NIC | 192.168.1.1 | 255.255.255.0 |
| Router1 Serial 0/0 | NIC | 192.168.3.1 | 255.255.255.0 |
| Router2 Fast Ethernet 0/1 | NIC | 192.168.2.1 | 255.255.255.0 |
| Router2 Serial 0/0 | NIC | 192.168.3.2 | 255.255.255.0 |

**Objectives:**

**Case 1:**

1. Design a WAN with 2 Routers
2. Configure the Routers
3. Apply HDLC (PAP and CHAP) authentication on it.
4. Verify Connection.

**Case 2:**

1. Design a WAN with 2 Routers
2. Configure the Routers
3. Apply PPP (PAP and CHAP) authentication on it.
4. Verify Connection.

**Router Configuration:**

Router> enable

Router# configure terminal

Router(config)# interface gigabitethernet 0/1

Router(config-if)# ip address 192.168.1.2 255.255.255.0

Router(config)# ip route 192.168.1.0 255.255.0.0 192.168.2.2

Router(config-if)# no shutdown

Router#show interfaces serial 0/0/0

Router#configure terminal

Router(config)#interface serial 0/0/0

Router(config-if)#encapsulation ppp

Router(config)#exit

Router#show interfaces serial 0/0/0

Router#configure terminal

Router(config)#interface serial 0/0/0

Router(config-if)#encapsulation hdlc

Router(config-if)#shutdown

Router(config-if)#no shutdown

Router(config-if)#exit

Router(config)#exit

Router#show interfaces serial 0/0/0

Router>enable

Router#configure terminal

Router(config)#hostname R1

R1(config)#username R2 password vinita

R1(config)#interface serial 0/0/0

R1(config-if)#encapsulation ppp

R1(config-if)#ppp authentication chap

R1(config-if)#exit

R1(config)#

Router>enable

Router#configure terminal

Router(config)#hostname R2

R2(config)#username R1 password vinita

R2(config)#interface serial 0/0/0

R2(config-if)#encapsulation ppp

R2(config-if)#ppp authentication chap

R2(config-if)#exit

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,

changed state to up

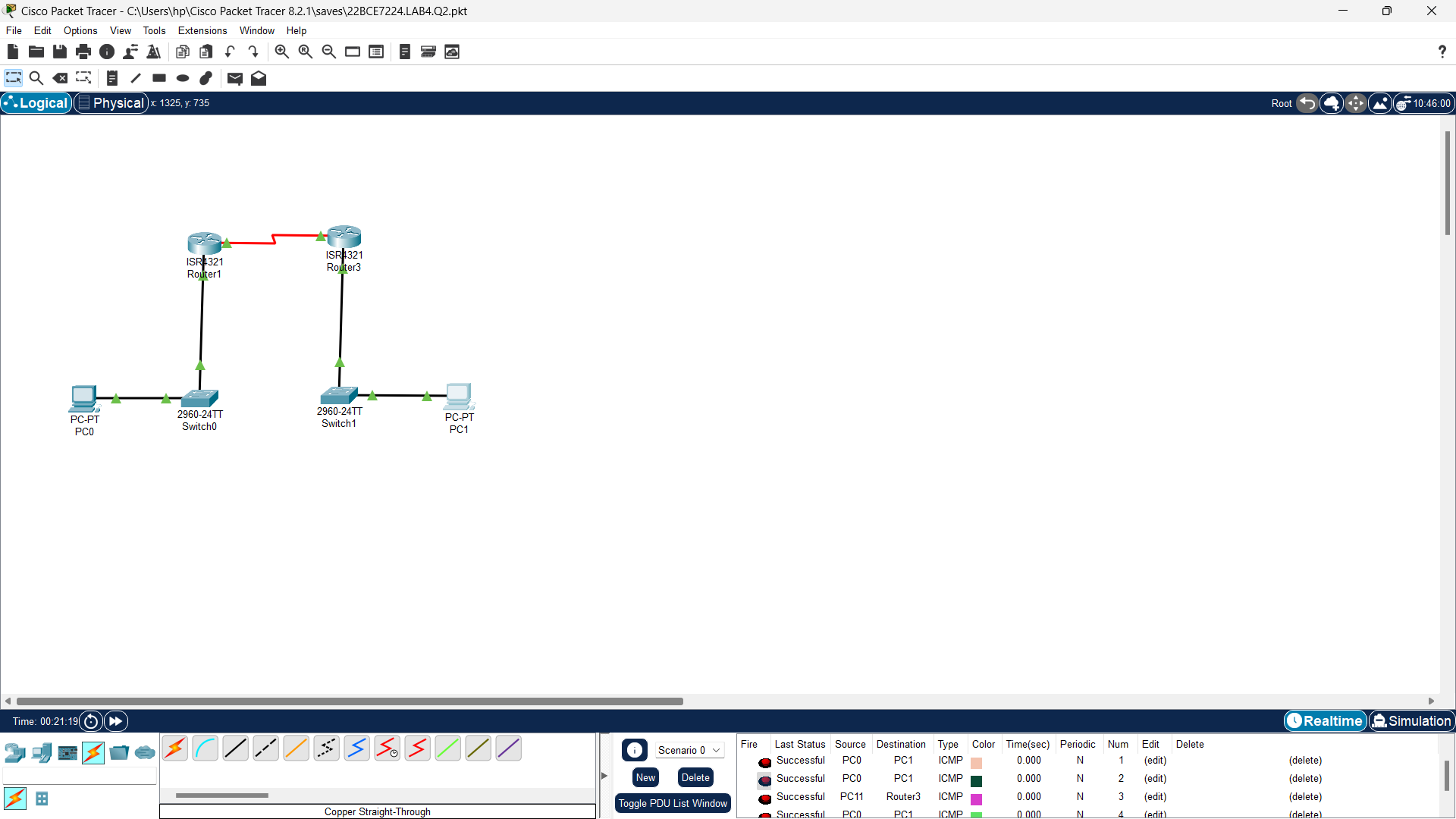
R2(config)#

**References:**

<https://www.packettracernetwork.com/labs/lab11-hdlc.html>

<https://www.packettracernetwork.com/labs/lab12-ppp.html>

1.HDLC



2.PPP