Experiment 2: Configuring Port Security in Cisco Packet Tracer

Date: 16/7/25

Aim: To configure and observe port security violation modes (Shutdown, Restrict, Protect) on a Cisco Packet Tracer switch.

Procedure:

1. Network Setup and Initial Connectivity:
* Build a single network topology in Packet Tracer.
* Connect PC1, PC2, PC3, and a Router with wired connections.
* Assign IP addresses and default gateway addresses to PC1, PC2, PC3, and the Router.
* Verify connectivity by pinging between all PCs from their respective command prompts.

2. Configuring Shutdown Mode (fa0/1):
* Access Switch 0 CLI.
* Enter global configuration mode.
* Configure interface fa0/1:
* `switchport mode access`
* `switchport port-security`
* `switchport port-security mac-address sticky`
* `switchport port-security maximum 1`
* `switchport port-security violation shutdown`
* Apply the same shutdown configuration to interfaces fa1/1 and fa2/1.
* Verify connectivity by pinging all PCs.

3. Testing Shutdown Mode:
* Assign an IP address to Rogue PC0.
* Ping PC1, PC2, and PC3 from Rogue PC0.
* Disconnect PC1 and connect Rogue PC0.
* Ping PC2 (192.168.5.15) from Rogue PC0.
* On the Switch, verify port security status:
* `show port-security`
* `show port-security int fa0/1`
* `show mac address-table`
* Disconnect Rogue PC0 and reconnect PC1 (it will remain red, indicating the port is down).
* On the Switch, re-enable the interface fa0/1:
* `configure terminal`
* `int fa0/1`
* `shutdown`
* `no shutdown`
* `end`
* `show mac address-table`
* From PC1, ping 192.168.5.15 and 192.168.5.20.

* Review the running configuration: `show running-config`

4. Configuring Restrict Mode (fa1/1):
* On the Switch, configure interface fa1/1:
* `enable`
* `configure terminal`
* `int fa1/1`
* `switchport mode access`
* `switchport port-security`
* `switchport port-security violation restrict`
* `exit`
* `end`
* Verify port security status:
* `show port-security`
* `show port-security int fa1/1`

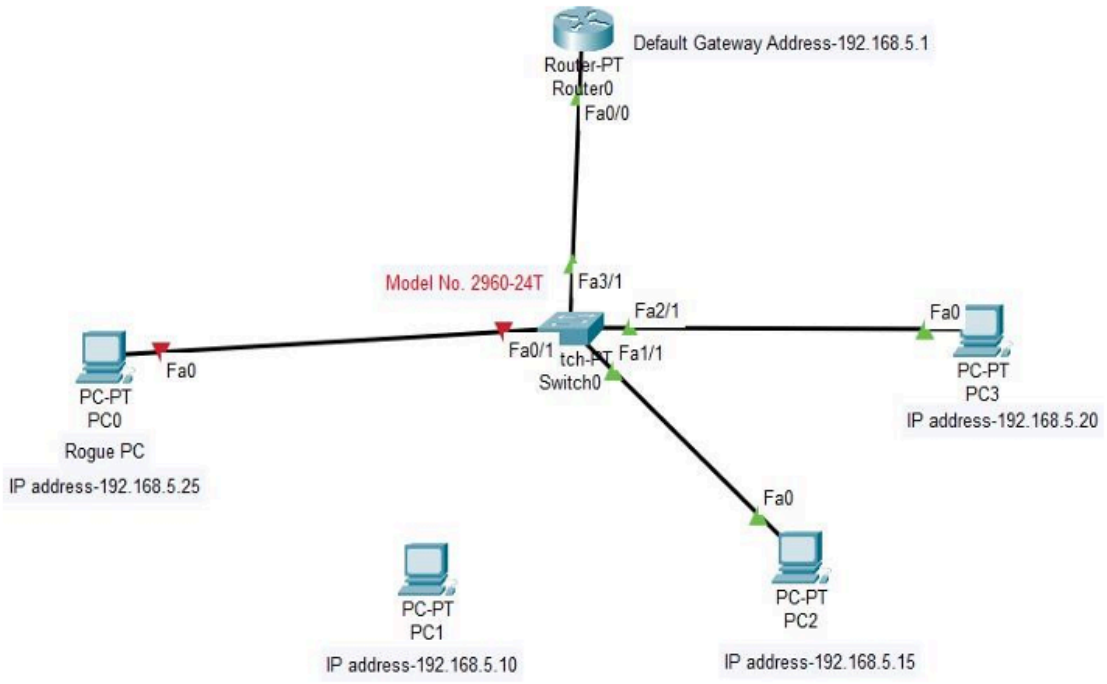
5. Testing Restrict Mode:
* Disconnect PC2 and connect Rogue PC0.
* Ping 192.168.5.10 and 192.168.5.20 (expect request timeout).
* Verify port security status on the Switch:
* `show port-security`
* `show port-security int fa1/1`
* Remove Rogue PC0 and reconnect PC2.
* Ping PC1 and PC3 from PC2.
* Review the running configuration: `show running-config`

6. Configuring Protect Mode (fa2/1):
* On the Switch, configure interface fa2/1:
* `enable`
* `configure terminal`
* `int fa2/1`
* `switchport mode access`
* `switchport port-security`
* `switchport port-security violation protect`
* `exit`
* `end`
* Verify port security status:
* `show port-security`
* `show port-security int fa2/1`

7. Testing Protect Mode:
* Check ping connectivity from PC1 to PC2 and PC3.
* Check ping connectivity from PC3 to PC2 and PC1.
* Disconnect PC3 and connect Rogue PC0.

* Ping 192.168.5.10 and 192.168.5.20 (expect request timeout).
* On the Switch, examine network status:
* `show port-security`
* `show port-security int fa1/1` (Note: Typo in original document, likely intended for fa2/1)
* `show mac address-table`
* `show ip int br`
* Start a continuous ping to 192.168.5.10 (`Ping -t 192.168.5.10`) and stop with Ctrl + C.

Output: Port security was successfully configured. The behavior of each violation mode (Shutdown, Restrict, Protect) was observed as expected during unauthorized access attempts.



Result: The experiment successfully demonstrated the implementation of port security on the switch and the effects of each violation mode when an unauthorized device attempted to connect to the network.