Experiment -2

Date: 16/7/25

Configure Port Security in Cisco Packet Tracer

AIM:

To configure port security on a switch in Cisco Packet Tracer and observe the behavior of different security violation modes.

PROCEDURE:

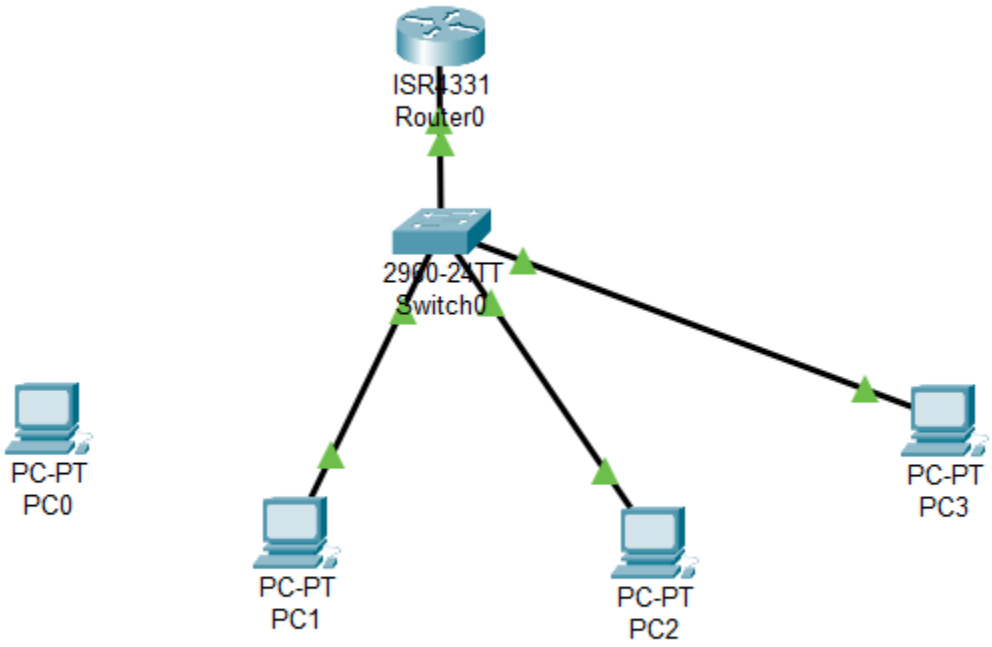
1. Step-1: Build the network single network topology in Packet Tracer.
2. Step-2: Give wired connections for all the devices of PC1, PC2, PC3 and Router.
3. Step-3: Give IP addresses for PC1, PC2, PC3 and Router with default gateway address.
   Click on PC1, go to command prompt and ping the IP address of other PCs.
   Repeat this step-3 for PC2 and PC3.
4. Step-5: Click on Switch 0 and go to CLI. Enter the following commands:
   #enable
   #configure terminal
   #int fa0/1
   #switchport mode access
   #switchport port-security
   #switchport port-security mac-address sticky
   #switchport port-security maximum 1
   #switchport port-security violation shutdown
5. Step-6: Configure shutdown mode for all other ports fa1/1 and fa2/1 using the same commands.
6. Step-7: Ping all PCs to verify connectivity.
7. Step-8: Assign IP address to Rogue PC0.
8. Step-9: Ping PC1, PC2 and PC3.
   Remove connection from PC1 and connect Rogue PC0.
   Ping the IP of PC2 (192.168.5.15).
9. Step-11: On Switch, use:
   #enable
   #show port-security
   #show port-security int fa0/1
   #show mac address-table
10. Step-12: Disconnect Rogue PC0 and reconnect PC1 (it remains red).
11. Step-13: On Switch, run:
    #enable
    #configure terminal
    #int fa0/1
    #shutdown

#no shutdown
#end
#show mac address-table

12. Step-14: From PC1, ping 192.168.5.15 and 192.168.5.20.
    #show running-config
13. Restrict Mode:
    Step-1: Configure restrict mode on fa1/1:
    #enable
    #configure terminal
    #int fa1/1
    #switchport mode access
    #switchport port-security
    #switch port-security violation restrict
    #exit
    #end
    #show port-security
    #show port-security int fa1/1
14. Step-2: Remove connection from PC2 and connect Rogue PC0.
15. Step-3: Ping 192.168.5.10 and 192.168.5.20 (expect request timeout).
16. Step-4: #show port-security
    #show port-security int fa1/1
17. Step-5: Remove Rogue PC0 and reconnect PC2.
    Ping PC1 and PC3.
    #show running-config
18. Protect Mode:
    Step-1: Configure protect mode on fa2/1:
    #enable
    #configure terminal
    #int fa2/1
    #switchport mode access
    #switchport port-security
    #switch port-security violation protect
    #exit
    #end
    #show port-security
    #show port-security int fa2/1
19. Step-2: Check ping from PC1 to PC2 and PC3. Also ping from PC3 to PC2 and PC1.
20. Step-3: Disconnect PC3 and connect Rogue PC0.
21. Step-4: Ping 192.168.5.10 and 192.168.5.20 (expect request timeout).
22. Step-5: On Switch:
    #show port-security
    #show port-security int fa1/1
    #show mac address-table

#show ip int br
Ping -t 192.168.5.10
Ctrl + C to stop ping.

OUTPUT:



Port security configured successfully. Observed the behavior of each violation mode (Shutdown, Restrict, Protect) as expected during unauthorized access attempts.

RESULT:

Port security was successfully implemented on the switch. The experiment demonstrated the effects of each violation mode when an unauthorized device attempted to connect to the network.