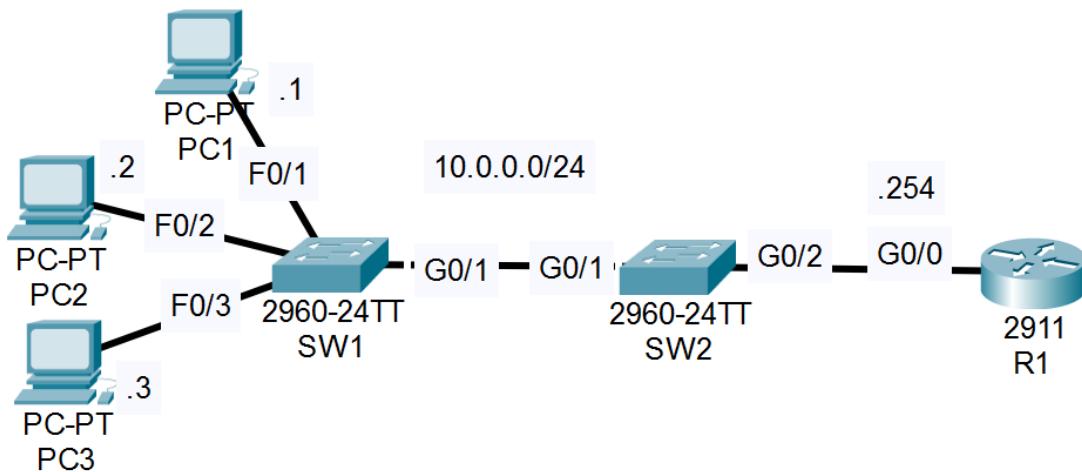


Network Topology:



Instructions and actions:

Configure port security on the following interfaces

1. SW1 F0/1, F0/2, F0/3 –
Violation mode: Shutdown
Maximum addresses: 1
Sticky learning: Disabled
Ageing time: 1 hour

By default, the first three conditions will be implemented. I have to enable port security for the interfaces and the ageing timer.

SW1 CLI:

```
SW1(config-if)#int f0/2
SW1(config-if)#switchport mode access
SW1(config-if)#switchport port-security
SW1(config-if)#do sh port-security int f0/2
Port Security          : Enabled
Port Status             : Secure-up
Violation Mode          : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 0
Configured MAC Addresses: 0
Sticky MAC Addresses    : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count: 0

SW1(config-if)#switchport port-security aging time 60
```

(These commands were configured to the interface range f0/1-3)

2. SW2 G0/1

Violation mode: Restrict

Maximum addresses: 4

Sticky learning: Enabled

SW2 CLI:



The screenshot shows a Windows application window titled "SW2". The tab bar at the top has "Physical", "Config", "CLI" (which is selected and highlighted in blue), and "Attributes". Below the tab bar is the title "IOS Command Line Interface". The main area of the window contains the output of several CLI commands related to port security on interface G0/1 of switch SW2.

```
SW2(config-if)#switchport port-security
SW2(config-if)#do sh port-security int g0/1
Port Security          : Enabled
Port Status             : Secure-up
Violation Mode          : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 0
Configured MAC Addresses: 0
Sticky MAC Addresses    : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count: 0

SW2(config-if)#switchport port-security max?
maximum
SW2(config-if)#switchport port-security maximum mac addresses ?
% Unrecognized command
SW2(config-if)#switchport port-security maximum ?
<1-132> Maximum addresses
SW2(config-if)#switchport port-security maximum 4
SW2(config-if)#switchport port-security violation restrict
SW2(config-if)#do sh port-security interface g0/1
Port Security          : Enabled
Port Status             : Secure-up
Violation Mode          : Restrict
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 4
Total MAC Addresses     : 1
Configured MAC Addresses: 0
Sticky MAC Addresses    : 0
Last Source Address:Vlan : 0060.471C.1D19:1
Security Violation Count: 0

SW2(config-if)#switchport port-security mac address sticky
^
% Invalid input detected at '^' marker.

SW2(config-if)#switchport port-security mac-address sticky
SW2(config-if)#do sh switchport port-security int g0/1
sh switchport port-security int g0/1
^
% Invalid input detected at '^' marker.

SW2(config-if)#do sh port-security int g0/1
Port Security          : Enabled
Port Status             : Secure-up
Violation Mode          : Restrict
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 4
Total MAC Addresses     : 1
Configured MAC Addresses: 0
Sticky MAC Addresses    : 1
Last Source Address:Vlan : 0060.471C.1D19:1
Security Violation Count: 0
```

3. Checking:

When PC1, PC2 and PC3 pinged their default gateway, we could observe the following MAC address table on SW2 –

```
SW2#show mac address-table
      Mac Address Table
-----
Vlan   Mac Address        Type      Ports
----  -----
  1    0001.0001.0001    STATIC    Gig0/1
  1    0002.0002.0002    STATIC    Gig0/1
  1    0003.0003.0003    STATIC    Gig0/1
  1    0060.471c.1d19    STATIC    Gig0/1
  1    00e0.b0d8.7e01    DYNAMIC  Gig0/2
SW2#
```

As a maximum of 4 MAC addresses were allowed on the g0/1 interface of SW2, one more can't ping through it.

SW1 CLI:

```
SW1>en
SW1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#int vlan 1
SW1(config-if)#ip address 10.0.0.10 255.255.255.0
SW1(config-if)#do ping 10.0.0.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.254, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Same for SW1, after manipulating the MAC address of PC1 from configuration mode, PC1 is not able to ping through SW1 as SW1 can't recognise the MAC.

PC1 Command Prompt:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.254

Pinging 10.0.0.254 with 32 bytes of data:

Reply from 10.0.0.254: bytes=32 time<1ms TTL=255

Ping statistics for 10.0.0.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 10.0.0.254

Pinging 10.0.0.254 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.0.254:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```