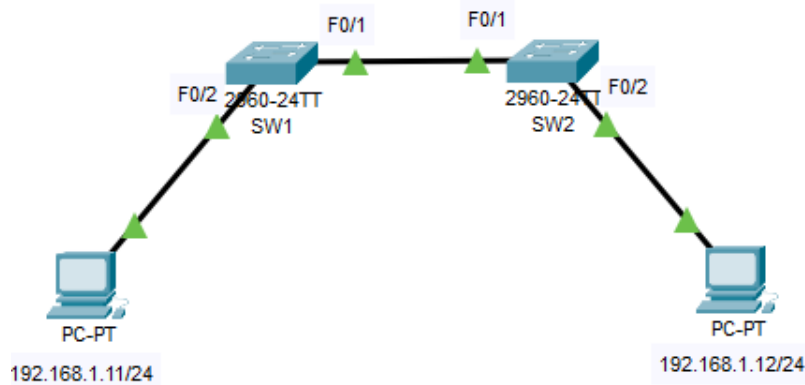


ACTIVITY 17: Port Security (Part 1)



1. From SW1, find the MAC address of SW2. From the CLI of SW2, find the MAC address of SW1.

```
SW1#show mac-address-table
      Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -
1       0001.9626.4101   DYNAMIC Fa0/1   -> SW2's mac address is 001.9626.4101.

SW2#show mac-address-table
      Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -
1       0006.2a8c.e501   DYNAMIC Fa0/1   -> SW1's mac address is 006.2a8c.e501.
```

2. Why don't the MAC addresses of PC1 and PC2 appear in the MAC address tables of SW1 and SW2
The MAC addresses of the two PCs don't appear because there was no traffic before from them.

3. Ping from PC1 to PC2 to generate traffic. Check the MAC address tables of the switches again

```
C:\>ping 192.168.1.12

Pinging 192.168.1.12 with 32 bytes of data:

Reply from 192.168.1.12: bytes=32 time<1ms TTL=128
Reply from 192.168.1.12: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.12:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Now we get their Mac addresses on both of the switches

SW1#show mac-address-table				SW2#show mac-address-table			
Mac Address Table				Mac Address Table			
Vlan	Mac Address	Type	Ports	Vlan	Mac Address	Type	Ports
1	0001.9626.4101	DYNAMIC	Fa0/1	1	0002.16e2.2193	DYNAMIC	Fa0/1
1	0002.16e2.2193	DYNAMIC	Fa0/2	1	0006.2a8c.e501	DYNAMIC	Fa0/1
1	0007.ec28.0631	DYNAMIC	Fa0/1	1	0007.ec28.0631	DYNAMIC	Fa0/2

4. Enable port security on the switch interfaces connected to PCs.

```
SW1(config)#interface f0/2
SW1(config-if)#switchport mode access
SW1(config-if)#switchport port-security
```

```
SW2(config)#interface f0/2
SW2(config-if)#switchport mode access
SW2(config-if)#switchport port-security
```

5. How many MAC addresses are allowed on a port-security enabled interface by default? Explicitly configure this setting on each switch.

By default, the maximum is 1. Let's configure it.

```
SW1(config-if)#switchport port-security maximum 1
```

```
SW2(config-if)#switchport port-security maximum 1
```

6. What is the default action in the event of a port-security violation? Explicitly configure this setting on each switch.

By default, the action in the event of a port-security violation is shutdown. Let's configure it.

```
SW1(config-if)#switchport port-security violation shutdown
```

```
SW2(config-if)#switchport port-security violation shutdown
```

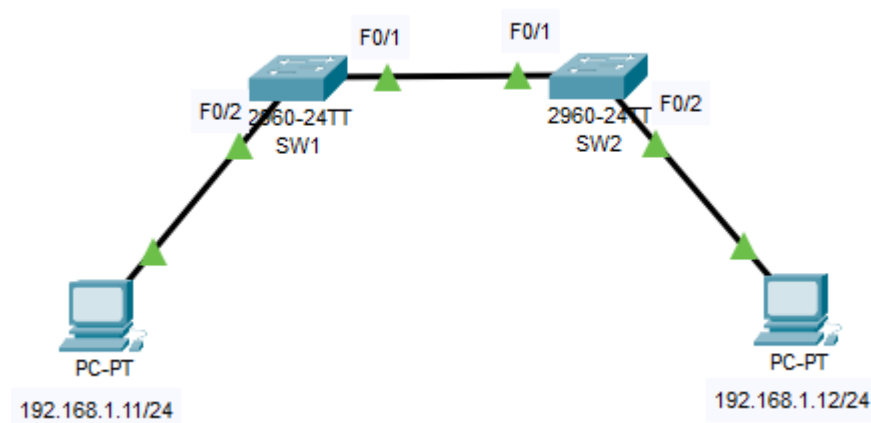
7. Manually configure the MAC address of PC1 as a secure MAC address for SW1 F0/2

Manually configure the MAC address of PC2 as a secure MAC address for SW2 F0/2

```
SW1(config-if)#switchport port-security mac-address 0002.16E2.2193
```

```
SW2(config-if)#switchport port-security mac-address 0007.EC28.0631
```

ACTIVITY 18: Port Security (Part 2)



1. Enable port security on the switchports connected to end hosts.

```
SW1(config)#interface f0/2
SW1(config-if)#switchport mode access
SW1(config-if)#switchport port-security
```

```
SW2(config)#interface f0/2
SW2(config-if)#switchport mode access
SW2(config-if)#switchport port-security
```

2. Ping from PC1 to PC2 to generate traffic between them.

```
C:\>ping 192.168.1.12

Pinging 192.168.1.12 with 32 bytes of data:

Reply from 192.168.1.12: bytes=32 time<1ms TTL=128
Reply from 192.168.1.12: bytes=32 time=12ms TTL=128
Reply from 192.168.1.12: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.12:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 12ms, Average = 4ms
```

3. View the secure MAC addresses on SW1. PC1's MAC address should be in the table.

```
SW1#show port-security address
      Secure Mac Address Table
-----
Vlan    Mac Address      Type                               Ports    Remaining Age
      (mins)
-----
1        0002.16E2.2193    DynamicConfigured                FastEthernet0/2

Total Addresses in System (excluding one mac per port)    : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

4. Check the configuration of SW1's F0/2 interface in the running configuration.

```
SW1#show running-config
interface FastEthernet0/2
 switchport mode access
 switchport port-security
```

5. Save the running configuration of SW1, and reload the switch.

```
SW1#wr
Building configuration...
[OK]
SW1#reload
```

6. View the secure MAC addresses on SW1 again. Is PC1's MAC address still present?

No it disappeared.

```
SW1#show port-security address
      Secure Mac Address Table
-----
Vlan    Mac Address      Type                               Ports    Remaining Age
      (mins)
-----
Total Addresses in System (excluding one mac per port)    : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

7. Enable sticky secure MAC addresses on the F0/2 interface of SW1, and ping from PC1 to PC2 to generate traffic.

```
SW1(config)#interface f0/2
SW1(config-if)#switchport port-security mac-address sticky
```

```
C:\>ping 192.168.1.12

Pinging 192.168.1.12 with 32 bytes of data:

Reply from 192.168.1.12: bytes=32 time<1ms TTL=128
Reply from 192.168.1.12: bytes=32 time=12ms TTL=128
Reply from 192.168.1.12: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.12:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 12ms, Average = 4ms
```

8. View the secure MAC addresses on SW1, then view the configuration of F0/2 in the running configuration. What is different?

```
SW1#show port-security address
      Secure Mac Address Table
-----
Vlan    Mac Address      Type                Ports    Remaining Age
(mins)
----    -
1       0002.16E2.2193    SecureSticky        Fa0/2    -
-----

Total Addresses in System (excluding one mac per port)    : 0
Max Addresses limit in System (excluding one mac per port) : 1024

interface FastEthernet0/2
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0002.16E2.2193
!
```

9. Save the running configuration and reload the switch.

SW1#wr

Building configuration...

[OK]

SW1#reload

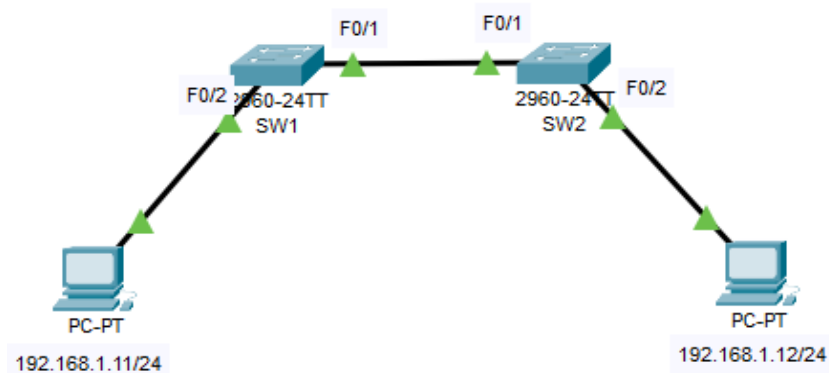
10. View the secure MAC addresses on SW1 again. Is PC1's MAC address still present?

Yes, it is.

```
SW1#show port-security address
      Secure Mac Address Table
-----
Vlan    Mac Address      Type                Ports    Remaining Age
(mins)
----    -
1       0002.16E2.2193    SecureSticky        Fa0/2    -
-----

Total Addresses in System (excluding one mac per port)    : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

ACTIVITY 19: Port Security (Part 3)



1. Ping from PC1 to PC2 to generate traffic between them.

```
C:\>ping 192.168.1.12

Pinging 192.168.1.12 with 32 bytes of data:

Reply from 192.168.1.12: bytes=32 time<1ms TTL=128
Reply from 192.168.1.12: bytes=32 time<1ms TTL=128
Reply from 192.168.1.12: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.12:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

2. View the MAC address table of SW1, and take note of the MAC address of PC1.

```
SW1#show mac-address-table
```

Mac Address Table			
Vlan	Mac Address	Type	Ports
1	0001.9626.4101	DYNAMIC	Fa0/1
1	0002.16e2.2193	DYNAMIC	Fa0/2
1	0007.ec28.0631	DYNAMIC	Fa0/1

3. Enable port security on SW1's F0/2 interface, and manually configure PC1's MAC address as a secure MAC address.

```
SW1(config)#interface f0/2
```

```
SW1(config-if)#switchport mode access
```

```
SW1(config-if)#switchport port-security
```

```
SW1(config-if)#switchport port-security mac-address 0002.16e2.2193
```

4. Repeat the process on SW2 for PC2.

```
SW2#show mac-address-table
```

Mac Address Table			
Vlan	Mac Address	Type	Ports
1	0002.16e2.2193	DYNAMIC	Fa0/1
1	0006.2a8c.e501	DYNAMIC	Fa0/1
1	0007.ec28.0631	DYNAMIC	Fa0/2

```
SW2(config)#interface f0/2
```

```
SW2(config-if)#switchport mode access
```

```
SW2(config-if)#switchport port-security
```

```
SW2(config-if)#switchport port-security mac-address 0007.ec28.0631
```

5. Ping between PC1 and PC2 to test.

```
C:\>ping 192.168.1.12
```

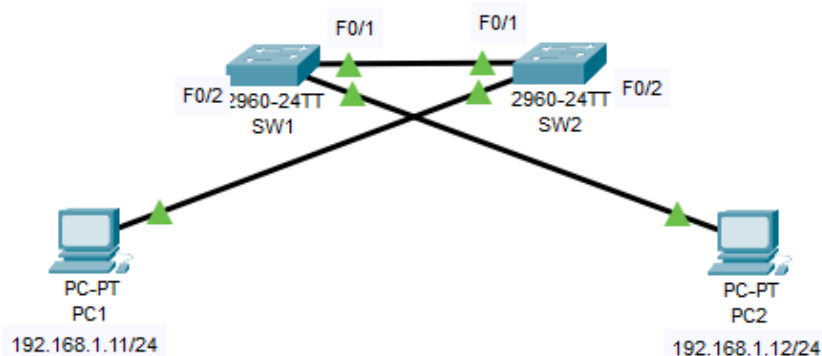
Pinging 192.168.1.12 with 32 bytes of data:

```
Reply from 192.168.1.12: bytes=32 time<1ms TTL=128
Reply from 192.168.1.12: bytes=32 time<1ms TTL=128
```

Ping statistics for 192.168.1.12:

```
Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

6. Remove the cables connecting the PCs to the switches, and then connect PC1 to SW2's F0/2 interface, and PC2 to SW1's F0/2 interface.



7. Ping from PC1 to PC2. What happens?

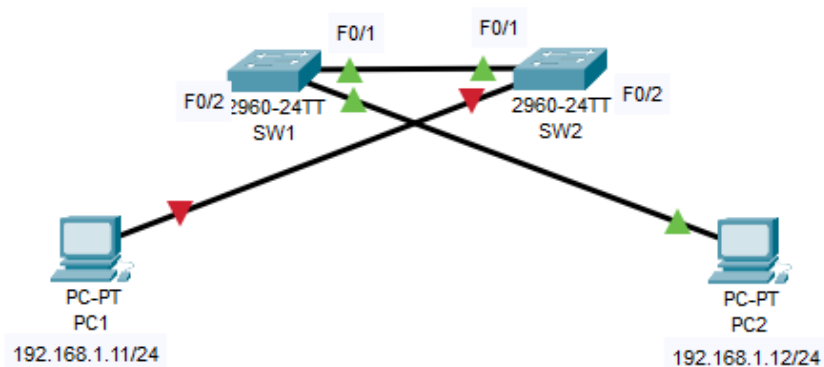
The connection between the PCs doesn't work.

```
C:\>ping 192.168.1.12

Pinging 192.168.1.12 with 32 bytes of data:

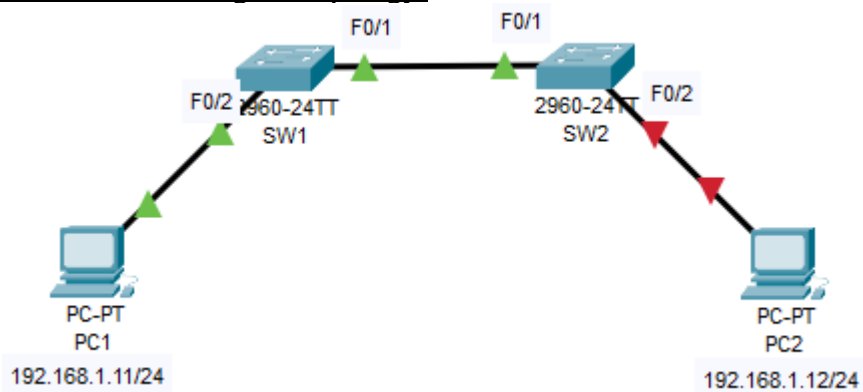
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```



And the port shutdown

8. Reconnect the cables as in the original topology.



9. Ping from PC1 to PC2. What happens?

Still no connection as the port is still shutdown on SW2 because of the security-violation.

10. Fix the problem and try to ping from PC1 to PC2 once more.

```
SW2(config)#interface f0/2
SW2(config-if)#shutdown
SW2(config-if)#no shutdown
```

```
C:\>ping 192.168.1.12

Pinging 192.168.1.12 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 192.168.1.12: bytes=32 time<1ms TTL=128
Reply from 192.168.1.12: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

It works again.