27-1 Port Security Configuration Answer Key

In this lab you will configure Port Security on a small campus network.

Disable Unused Ports

1) Disable all unused ports on SW1. This prevents unauthorised hosts plugging in to them to gain access to the network.

'show ip interface brief' shows ports FastEthernet 0/1 – 24 and GigabitEthernet0/1 – 2. Interfaces FastEthernet 0/1 and 0/2 are in use.

```
SW1#sh ip int brief
Interface IP-Address OK? Method Status Protocol
FastEthernet0/1 unassigned YES manual up up
FastEthernet0/2 unassigned YES manual up up
FastEthernet0/3 unassigned YES manual down down
! truncated
FastEthernet0/24 unassigned YES manual down down
GigabitEthernet0/1 unassigned YES manual down down
GigabitEthernet0/2 unassigned YES manual down down
Vlan1 unassigned YES manual administratively down down
```

Interfaces FastEthernet 0/1 and 0/2 are in use. Shutdown all other interfaces:

```
SW1(config)#interface range f0/3 - 24
SW1(config-if-range)#shutdown

SW1(config-if-range)#interface range g0/1 - 2
SW1(config-if-range)#shutdown
```

Port Security Configuration

2) Configure Port Security on interface FastEthernet 0/1. Allow a maximum of two MAC addresses and manually add PC1's MAC address to the configuration.

   Important: After enabling Port Security, do not send traffic between the PCs (for example 'ping') until you have manually added PC1's MAC address to the configuration. If you do, Port Security will learn PC1's MAC address dynamically and Packet Tracer has no function to remove it.

   This results in the error "Found duplicate mac-address". In this case you have to shutdown interface Fa0/1, save the configuration, reload then add PC1's MAC address before enabling interface Fa0/1 again.

   Shutting down the interface is necessary because PC1 sends gratuitous ARPs when its interface comes up.

We need to discover PC1's MAC address. We can get this information from the PC itself or from the switch. Use 'ipconfig /all' to find it on the PC.

```
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address................: 0000.1111.1111
   Link-local IPv6 Address.........: FE80::200:CFF:FEA0:A359
   IP Address......................: 10.10.10.10
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: 0.0.0.0
   DNS Servers.....................: 0.0.0.0
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................: 28262
   DHCPv6 Client DUID..............:
00-01-00-01-61-91-76-98-00-00-11-11-11-11
```

Use ‘show mac address-table’ to find it on the switch. Use ping to generate some traffic from the PC if it does not show up in the MAC address table.

```
C:\>ping 10.10.10.11

Pinging 10.10.10.11 with 32 bytes of data:

Reply from 10.10.10.11: bytes=32 time=14ms TTL=128
Reply from 10.10.10.11: bytes=32 time<1ms TTL=128
Reply from 10.10.10.11: bytes=32 time=19ms TTL=128
Reply from 10.10.10.11: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 19ms, Average = 8ms
```

```
SW1#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0000.1111.1111    DYNAMIC     Fa0/1
   1    0000.2222.2222    DYNAMIC     Fa0/2
```

You need to make the interface an access port before the switch will accept Port Security configuration. No VLANs are configured on the switch or specified in the lab task so leave it in the default VLAN 1.

```
SW1(config)#interface f0/1
SW1(config-if)#switchport mode access
```

Add the Port Security configuration.

```
SW1(config-if)#switchport port-security
SW1(config-if)#switchport port-security maximum 2
SW1(config-if)#switchport port-security mac-address
0000.1111.1111
```

3) Enable Port Security on interface FastEthernet 0/2 with the default settings.

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

4) From PC1 or PC2, generate some traffic between the PCs.

Ping from PC2 to PC1 or vice versa:

```
C:\>ping 10.10.10.10

Pinging 10.10.10.10 with 32 bytes of data:

Reply from 10.10.10.10: bytes=32 time=1ms TTL=128
Reply from 10.10.10.10: bytes=32 time<1ms TTL=128
Reply from 10.10.10.10: bytes=32 time=13ms TTL=128
Reply from 10.10.10.10: bytes=32 time=17ms TTL=128

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 17ms, Average = 7ms
```

5) On SW1, use a 'show port-security' command to verify if the MAC address of PC2 has been learned by Port Security.

```
SW1#show port-security address
                    Secure Mac Address Table
------------------------------------------------------------------------
Vlan   Mac Address   Type                Ports         Remaining Age
                                                       (mins)
----   -----------   ----                -----         -------------
1      0000.1111.1111      SecureConfigured    FastEthernet0/1
1      0000.2222.2222      DynamicConfigured   FastEthernet0/2
------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

PC2's MAC address is 0000.2222.2222

6) Verify the full Port Security configuration on both interfaces. Do not use the ‘show running-config’ command in this task.

```
SW1#show port-security interface f0/1
Port Security : Enabled
Port Status : Secure-up
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 2
Total MAC Addresses : 1
Configured MAC Addresses : 1
Sticky MAC Addresses : 0
Last Source Address:Vlan : 0000.1111.1111:1
Security Violation Count : 0

SW1#show port-security interface 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 : 1
Configured MAC Addresses : 0
Sticky MAC Addresses : 0
Last Source Address:Vlan : 0000.2222.2222:1
Security Violation Count : 0
```