How to Configure Cisco Port Security

by Bilal Ibrahim, Senior Network Engineer, UncommonX

Port security is a layer two traffic control feature on Cisco Catalyst switches. It enables administrators to configure individual switch ports to allow only a specified number of source MAC addresses ingressing the port. This helps improve security by filtering traffic that is destined to or received from a specific host based on their MAC address.

By default, there is no limit to the number of MAC addresses a switch can maintain on an interface and all MAC addresses are allowed. If you want, you can change this behavior with port security. For your organization's internal network, you do not want an employee to bring their own switch and connect to the network. That could cause outages like a SPT topology change in a case where the new switch has a lower bridge ID or a VTP VLAN overwrites if the plugged switch has a higher revision number.

Port security can also help with:
MAC base attacks like MAC address flooding
STP attacks like STP topology change (TCN) if the plugged switch has a lower bridge ID
VTP VLAN overwrites if the plugged switch has a higher revision number

To avoid all the above harmful scenarios, we can use port security command. Configuring the port security feature is easy and there are no prerequisites for the configuration. Use **switchport port security** command to enable port security:

```
Switch(config)# interface f0/1
Switch(config-if)# switchport port-security
```

Below is a useful command to check port security configuration. You can tell that the security feature is enabled, and you can verify the source MAC address along with the VLAN (see highlighted lines).

```
Switch#show port-security interface FastEthernet 0/1
Port Security           : Enabled
Port Status            : Secure-down
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   : aaaa.bbbb.cccc:10
Security Violation Count   : 0
```

There are multiple configurations that you can set using port security. First, you can set the maximum number of MAC addresses so that once the switch detects another MAC address on the interface, it will trigger the violation that was predefined by the administrator.

Second, you can filter the MAC address (hardcoding MAC address), and when the switch once again detects that this MAC address is not what has been configured, then it will trigger a violation action.

Below is an example of a violation penalty that was triggered because of a breach in port security settings:

```
%PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/1, putting Fa0/1 in err-disable
state
%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC
address dddd.eeee.ffff on port FastEthernet0/1
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down
```

As we can see, the port goes into err-disable mode. We can use **show port security interface** command to get more details. Let's take a close look at the output below:

```
Switch# show port security interface f0/1
Port Security               : Enabled
Port Status                 : Secure-shutdown
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      : dddd.eeee.ffff:10
Security Violation Count      : 1
```

You can enable the interface again after **err-disable** by either typing “**shutdown”** followed by “**no shutdown”** or even easier if the interface could recover automatically after a certain time (by default, 300 seconds) by using **errdisable recovery cause pscure-violation.**

You can decrease the waiting time and make it much faster. For example, instead of 300 seconds (about five minutes), we can set the time to 30 seconds using **errdisable recovery interval 30**.

Instead of manually typing the MAC address (hardcoding), you can make the switch automatically and use the first MAC address on the interface for the port security by adding the word **Sticky** at the end**.**

Instead of **switchport port-security mac-address aaaa.bbbb.cccc,** you can use **switchport port-security mac-address sticky**.

Here are violation predefined modes you can use:

Shutdown: This is the default mode. The interface will be placed in err-disable mode where all traffic will be blocked and SNMP messages sent.
Protect: This will discard traffic from MAC addresses that are not allowed but keeps the port up and does not send SNMP messages.
Restrict: This is the same as protect except this mode will send SNMP messages.

```
Switch(config-if)#switchport port-security violation?
 protect   Security violation protect mode
 restrict  Security violation restrict mode
 shutdown  Security violation shutdown mode
```

About the author

Bilal Ibrahim is an IT professional with more than 16 years of experience in the vast area of networking technologies. His background has largely been in financial services with hands-on experience in enterprise networks specializing in Cisco LAN/WAN/backbone/data center and security environments. Bilal leads the internal network design and automation for UncommonX.