Port Security

The purpose of port security is to prevent any unauthorized endpoint from access to the corporate network. For example, plugging an unauthorized laptop from home or a switch into the Ethernet jack at work could affect network operations. The switch port enabled with port security would deny access based on the unknown MAC address.

It is a Layer 2 security feature configured on network access switches. Cisco switches support sticky, static or dynamic port security modes. Switch ports configured with port security will only accept frames from addresses that have been dynamically learned or manually configured. Note that port security feature cannot be enabled on trunk interfaces or EtherChannel port interfaces.

Sticky Address

The **sticky** keyword saves the dynamically learned MAC address to the running configuration script. In addition sticky MAC addresses do not age out of the MAC address table. The switch does have to relearn the MAC addresses after every reboot unless the running configuration is saved to startup configuration. Removing the **sticky** keyword causes dynamically learned the MAC addresses to persist in the MAC address table only for the connected session. The following IOS commands enable port security on a switch port interface with sticky method.

```
interface fastethernet 0/1
switchport port-security
switchport port-security mac-address sticky
```

Static Address

The static address option enables a switch interface to only accept frames from a host endpoint with a specific MAC address. The static MAC is manually assigned to the switch port and must match to allow frames. The switch port would deny access based on an unknown MAC address. The default setting is to allow only one MAC address per switch port.

```
interface fastethernet 0/1
switchport port-security
switchport port-security mac-address 0000.1234.5678
```

Dynamic Address

This is the default setting for port security on a switch interface when it is enabled. The MAC address of the connected host or device is learned dynamically and added to the MAC address table. The MAC address persists in the switch address table until the switch is powered off or deleted when host disconnects from switch. The MAC address is flushed at regular intervals based on the aging timer. That will trigger MAC learning to discover and dynamically add to MAC address table again.

Maximum MAC Addresses

The following port security interface command allows connecting only a single host or network device to a switch port. There is support however for allowing multiple hosts (MAC addresses) to a single switch port. The switch interface can add a maximum of five MAC addresses to the switch MAC address table.

switchport port-security maximum 1

Violation Modes

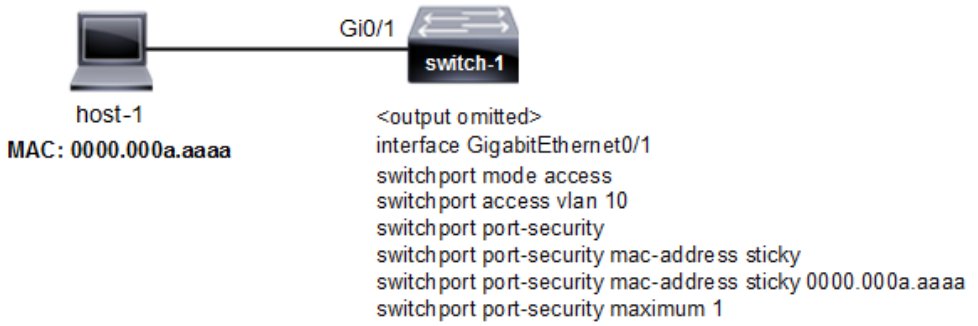
The four configurable violation modes include protect, restrict, shutdown and shutdown VLAN. It describes what the switch does in response to a port violation. The Cisco default port security violation mode is shutdown. There are various different events that could trigger a port violation action. The switch interface can add up to the maximum number of allowed MAC addresses to the address table. The switch port shuts down only when the maximum number of secure MAC addresses is exceeded. The switch then sends an SNMP trap notification. The security violation could trigger when there is an attempt from a host with a MAC address not in the MAC address table. Duplicate MAC address error cause a port violation action as well. The restrict mode causes the switch to drop all packets from an unknown source. SNMP trap alert is sent, Syslog message is logged and the violation counter is incremented. An advantage of restrict mode is listing the number of violations. Protect mode only sends a security violation notification.

Example: Port Security

Refer to the port security configuration on switch-1 interface Gi0/1. Ethernet frames with source MAC address **0000.000a.aaaa** arrives at switch-1 interface Gi0/1. What events occur when frames arrive on Gi0/1?

switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1

Figure 1 Port Security Sticky Address



Answer

Port security configuration allows host-1 connected to switch-1 interface Gi0/1 access to the network. The source MAC address **0000.000a.aaaa** is assigned to the host-1. Ethernet frames with destination MAC address **0000.000a.aaaa** are forwarded out of Gi0/1 to host-1 as well.

switchport port-security *(enable port security)*

switchport port-security mac-address sticky

(MAC address 0000.000a.aaaa added to running configuration)

switchport port-security maximum 1 *(one host connection only)*

Operational Commands

Each of the following IOS commands verify that port security is configured on a switch port. the operational command **show port-security** provides status information of an interface. The switch will errdisable any switch port interface where there is a port security violation.

show port-security interface gigabitethernet 1/1

show running-config