Configure Port Security

Note To achieve simplification and consistency, the Cisco SD-WAN solution has been rebranded as Cisco Catalyst SD-WAN. In addition, from Cisco IOS XE SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Release 20.12.1, the following component changes are applicable: **Cisco vManage** to **Cisco Catalyst SD-WAN Manager**, **Cisco vAnalytics** to **Cisco Catalyst SD-WAN Analytics**, **Cisco vBond** to **Cisco Catalyst SD-WAN Validator**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

Table 1: Feature History Table

Feature Name	Release Information	Description
Port Security Support for Switchports on Cisco IOS XE Catalyst SD-WAN Devices	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	The feature allows you to configure switchports on Edge platforms with switching modules to restrict input to an interface by limiting and identifying MAC addresses of the workstations that are allowed to access the port.

Supported Devices for Port Security

Cisco ISR4000 series Edge platforms with SM-X-16G4M2X, and SM-X-40G8M2X switching modules:

- ISR4461
- ISR4451
- ISR4351

- ISR4331

Cisco C8300 series Edge platforms with SM-X-16G4M2X, and SM-X-40G8M2X switching modules:

- C8300-1N1S-6T
- C8300-1N1S-4T2X
- C8300-2N2S-6T
- C8300-2N2S-4T2X

Information About Port Security

You can use the port security feature to configure switch ports on routing platforms, to restrict input to an interface by limiting and identifying MAC addresses of the workstations that are allowed to access the port. When you assign secure MAC addresses to a secure port, the port does not forward packets with source addresses outside the group of defined addresses.

The secure addresses are included in an address table in one of these ways:

- You can allow the port to dynamically configure secure MAC addresses with the MAC addresses of connected devices.
- You can configure several addresses and allow the rest to be dynamically configured.

Note If the port shuts down, all dynamically learned addresses are removed.

- You can configure MAC addresses to be sticky. These can be dynamically learned or manually configured, stored in the address table, and added to the running configuration. If these addresses are saved in the configuration file, the interface does not need to dynamically relearn them when the switch restarts. Although sticky secure addresses can be manually configured, it is not recommended.

Enable *sticky learning* to configure an interface to convert the dynamic MAC addresses to sticky secure MAC addresses and to add them to the running configuration. To enable sticky learning, enter the **switchport port-security mac-address sticky** command. When you enter this command, the interface converts all the dynamic secure MAC addresses, including those that were dynamically learned before sticky learning was enabled, to sticky secure MAC addresses.

The sticky secure MAC addresses do not automatically become part of the configuration file, which is the startup configuration used each time the switch restarts. If you save the sticky secure MAC addresses in the configuration file, when the switch restarts, the interface does not need to relearn these addresses. If you do not save the configuration, they are lost.

If sticky learning is disabled, the sticky secure MAC addresses are converted to dynamic secure addresses and are removed from the running configuration.

Restrictions for Port Security

- Secure port and static MAC address configuration are mutually exclusive.

Note **switchport port-security** and **switchport port-security mac-address sticky** configuration commands are validated. There are other port-security commands available, but we recommend not to use them for Cisco SD-WAN Release 20.3.1.

Configure Port Security Using the CLI

Configure Port Security on an Interface

To restrict traffic through a port by limiting and identifying MAC addresses of the stations allowed to access the port, perform this task:

1. Enters physical interface mode for configurations, for example **gigabitethernet 1/0/1**.

   ```
   Device(config)# interface interface_id
   ```

2. Enables port security on the interface.

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

3. (Optional) Enable sticky learning on the interface.

   ```
   Device(config-if)# switchport port-security mac-address sticky
   ```

4. Returns to privileged EXEC mode.

   ```
   Device(config-if)# end
   ```

Configuration Example

The following example shows how to configure a secure MAC address on GigabitEthernet 1/0/1:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# switchport port-security
Device(config-if)# switchport port-security mac-address sticky
Device(config-if)# end
```