Port Security

Port Security Overview

The port security feature allows you to restrict input to an interface by limiting and identifying MAC addresses of the workstations that are allowed to access the port. It helps you to control the learning and storing of MAC addresses for each interface. It is used to protect against CAM overflow attacks and rogue equipment, such as hubs and switches, being plugged in. A port security enabled port is called a secure port, and the MAC addresses allowed on that port are called secure MAC addresses.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. If you limit the number of secure MAC addresses to one and assign a single secure MAC address to a secure port, the workstation attached to that port is assured the full bandwidth of the port.

After you have set the maximum number of secure MAC addresses on a port, you can include secure MAC addresses in an address table in one of these ways:

- Configure all secure MAC addresses by using the switchport port-security mac-address *mac_address* interface configuration command.
- Allow the port to dynamically configure secure MAC addresses with the MAC addresses of connected devices.
- Configure a number of addresses and allow the rest to be dynamically configured.

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

- 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.

MAC Learning

After port security is enabled on an interface and a new MAC address is seen on the interface, a security validation is done for the new MAC address. Based on this validation, the MAC address will be added to the address table - either as a normal entry or a drop entry.

Port Security Violations

A port security violation occurs in either of these situations:

- When the maximum number of secure MAC addresses is reached on a secure port and the source MAC address of the ingress traffic is different from any of the identified secure MAC addresses, port security applies the configured violation mode.
- If traffic with a secure MAC address that is configured or learned on one secure port attempts to access another secure port in the same VLAN, port security applies the configured violation mode. This is also known as a MAC move violation.

There are three violation actions for port security. You can configure the port for one of these violation actions:

- **Shutdown**—A port security violation causes the port to shut down immediately.
- **Restrict**—A port security violation restricts data, causes the SecurityViolation counter to increment, and causes an SNMP Trap to be generated. In the Restrict action, learning is disabled on the port after 10 violations. Restrict is the default action for port security violations.
- **Protect**—A port security violation causes data from unknown MAC addresses to be dropped. The SecurityViolation counter is not incremented, and no SNMP Trap is generated.

Guidelines for Port Security on UCS 6454 Fabric Interconnects

The following guidelines apply when you configure port security for UCS 6454 Fabric Interconnect ports:

- Port security can be configured only on NIV ports. It is not supported on BIF ports.
- Only one MAC address per VLAN can be secured for an NIV port.
- For port security violations on virtual interfaces, Restrict is the default violation action.
- MAC learning is disabled on a secure port after 10 violations.
- Secure MAC addresses never age out.
- The maximum number of secure MAC addresses that can be configured are as follows:
    - On a Device—A maximum of 8000 secure MAC addresses in addition to one MAC address per port
    - On an Interface—A maximum of 1000 MAC addresses per interface
    - In a VLAN—Only one secure MAC address per port for a VLAN

Configuring Port Security

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

Procedure

	Command or Action	Purpose
Step 1	switch(config)# **interface** *interface_id*	Enters interface configuration mode.
Step 2	switch(config-if)# **switchport mode access**	Sets the interface mode as access; an interface in the default mode (dynamic desirable) cannot be configured as a secure port.
Step 3	switch(config-if)# [**no**] **switchport port-security**	Enables port security on the interface. To return the interface to the default condition as not a secure port, use the no switchport port-security interface configuration command.
Step 4	switch(config-if)# **switchport port-security maximum** *value*	Sets the maximum number of secure MAC addresses for the interface. The range is 1 to 1000. To return the interface to the default number of secure MAC addresses, use the no switchport port-security maximum *value* interface configuration command.
Step 5	switch(config-if)# **switchport port-security violation** {**restrict** | **shutdown** | **protect**}	Sets the action to be taken when a security violation is detected. The action can be one of the following: • **Shutdown**—A port security violation causes the port to shut down immediately. • **Restrict**—A port security violation restricts data, causes the SecurityViolation counter to increment, and causes an SNMP Trap to be generated. In the Restrict action, learning is disabled on the port after 10 violations. Restrict is the default action for port security violations. • **Protect**—A port security violation causes data from unknown MAC addresses to be dropped. The SecurityViolation counter is not incremented, and no SNMP Trap is generated. To return the violation mode to the default condition (restrict), use the no switchport

	Command or Action	Purpose
		port-security violation {restrict | shutdown | protect} interface configuration command.
Step 6	switch(config-if)# **switchport port-security mac-address** *mac_address*	Enters a secure MAC address for the interface. You can use this command to enter the maximum number of secure MAC addresses. If you configure fewer secure MAC addresses than the maximum, the remaining MAC addresses are dynamically learned. To delete a MAC address from the address table, use the no switchport port-security mac-address *mac_address* interface configuration command.