

Switch Port Security

- Switch Port Security, on page 1

Switch Port Security

Note Always shutdown interface before port security configurations.

Port security is not supported on port channel interfaces.

Restrictions

- Dynamic secure mac address are not retained over reboot and only delete-on-reset secure mode is supported.
- Static mac address must be set after port is in shutdown, and other port security commands are configured and enabled.
- Only ethernet ports are supported for port security configuration.
- Does not support trap and **show switch interface port-security** command does not show information about trap.
- If port-security violation shutdown mode is configured on a secure port and violation traffic is received, the port changes to error state. A manual interface shutdown and no shutdown is required to recover the port.

Configuring Port Security

To configure port security:

1. Shutdown the interface:

```
configure terminal
switch
    interface gigabitEthernet 1/1
    shutdown
    commit
```

2. Disable port security:

```
configure terminal
switch
    interface gigabitEthernet 1/1
    no port-security enable
    commit
```

3. Configure max mac address:

```
configure terminal
switch
    interface gigabitEthernet 1/1
    port-security max 5
    commit
```

4. Configure violation handling:

```
configure terminal
switch
    interface gigabitEthernet 1/1
    port-security violation discard
    commit
```

5. Enable port security:

```
configure terminal
switch
    interface gigabitEthernet 1/1
    port-security enable
    commit
```

6. Add static secure mac address:

```
configure terminal
switch
    mac address-table static 18:65:90:cb:e6:08 vlan 1 interface gigabitEthernet 1/1
secure
    commit
```

7. Restart the disabled interface:

```
configure terminal
switch
    interface gigabitEthernet 1/1
    no shutdown
    commit
```

8. Use **show switch interface port-security** to verify the configuration:

```
nfvis# show switch interface port-security
MAC
VIOLATION ADDRESS MAX MAC
PORT STATUS LEARNING HANDLING COUNT ADDRESS
-------------------------------------------------------------
1/0 Disabled Delete-On-Reset Discard 0 0
1/1 Enabled Delete-On-Reset Discard 1 5
1/2 Disabled Delete-On-Reset Discard 0 0
1/3 Disabled Delete-On-Reset Discard 0 0
```

```
1/4 Disabled Delete-On-Reset Discard 0 0
1/5 Disabled Delete-On-Reset Discard 0 0
1/6 Disabled Delete-On-Reset Discard 0 0
1/7 Disabled Delete-On-Reset Discard 0 0
```

9. Use **show switch mac addr-table** command to check static configured or dynamic learnt secure mac addresses:

```
nfvis# show switch mac addr-table
VLAN MAC ADDRESS PORT TYPE
---------------------------------------
1 18:65:90:cb:e6:08 gi1/1 secure
```



Note If traffic with a secure MAC address that is configured on one secure port attempts to access another secure port in the same VLAN, ENCS switch port security responds to the violation by discarding the traffic always.