Configuring Port Security (CLI Procedure)

Ethernet LANs are vulnerable to attacks such as address spoofing and Layer 2 denial of service (DoS) on network devices. Port security features such as DHCP snooping, DAI (dynamic ARP inspection), MAC limiting, and MAC move limiting, as well as trusted DHCP server, help protect the access ports on your EX Series switch against the losses of information and productivity that can result from such attacks.

To configure port security features using the CLI:

1. Enable DHCP snooping:
   - On a specific VLAN:

     ```
     [edit ethernet-switching-options secure-access port]
     user@switch# set vlan default examine-dhcp
     ```

   - On all VLANs:

     ```
     [edit ethernet-switching-options secure-access port]
     user@switch# set vlan all examine-dhcp
     ```

2. Enable DAI:
   - On a single VLAN (here, the VLAN is employee-vlan):

     ```
     [edit ethernet-switching-options secure-access-port]
     user@switch# set vlan employee-vlan arp-inspection
     ```

   - On all VLANs:

     ```
     [edit ethernet-switching-options secure-access-port]
     user@switch# set vlan all arp-inspection
     ```

3. Limit the number of dynamic MAC addresses and specify the action to take if the limit is exceeded—for example, set a MAC limit of 5 with an action of drop:
   - On a single interface (here, the interface is ge-0/0/1):

     ```
     [edit ethernet-switching-options secure-access-port]
     user@switch# set interface ge-0/0/1 mac-limit 5 action drop
     ```

   - On all interfaces:

     ```
     [edit ethernet-switching-options secure-access-port]
     user@switch# set interface all mac-limit 5 action drop
     ```

4. Specify allowed MAC addresses:
   - On a single interface (here, the interface is ge-0/0/2):

     ```
     [edit ethernet-switching-options secure-access-port]
     user@switch# set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:80
     user@switch# set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:81
     ```

```
user@switch# set interface ge-0/0/2 allowed-mac 00:05:85:3A:82:83
```

- On all interfaces:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set interface all allowed-mac 00:05:85:3A:82:80
user@switch# set interface all allowed-mac 00:05:85:3A:82:81
user@switch# set interface all allowed-mac 00:05:85:3A:82:83
```

5. Limit the number of times a MAC address can move from its original interface in one second—for example, set a MAC move limit of 5 with an action of drop if the limit is exceeded:

   - On a single VLAN (here, the VLAN is employee-vlan):

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan employee-vlan mac-move-limit 5 action drop
```

   - On all VLANs:

```
[edit ethernet-switching-options secure-access-port]
user@switch# set vlan all mac-move-limit 5 action drop
```

6. Configure a trusted DHCP server on an interface (here, the interface is ge-0/0/8):

```
[edit ethernet-switching-options secure-access port]
user@switch# set interface ge-0/0/8 dhcp-trusted
```

Related Topics

- Configuring Port Security (J-Web Procedure)
- Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure)
- Example: Configuring Port Security, with DHCP Snooping, DAI, MAC Limiting, and MAC Move Limiting, on an EX Series Switch
- Example: Configuring DHCP Snooping, DAI , and MAC Limiting on an EX Series Switch with Access to a DHCP Server Through a Second Switch
- Monitoring Port Security
- Port Security for EX Series Switches Overview

Published: 2010-04-05