Configuring MAC Limiting (CLI Procedure)

MAC limiting protects against flooding of the Ethernet switching table on the EX-series switch. MAC limiting sets a limit on the number of MAC addresses that can be learned on a single Layer 2 access interface (port).

JUNOS software provides two MAC limiting methods:

- Maximum number of dynamic MAC addresses allowed per interface—As soon as the limit is reached, incoming packets with new MAC addresses are dropped.
- Specific "allowed" MAC addresses for the access interface—Any MAC address that is not in the list of configured addresses is not learned.

You configure MAC limiting for each interface, not for each VLAN. In the default configuration, the limit for dynamically learned MAC addresses for each interface is 5 and the action that the switch will take if that limit is exceeded is none.

To configure MAC limiting on a specific interface or on all interfaces, using the CLI:

1. For limiting the number of dynamic MAC addresses, set a MAC limit of 5 with an action of drop if the limit is exceeded:
   - 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
```

2. For specifying specific 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
```

Related Topics

- Configuring MAC Limiting (J-Web Procedure)
- Example: Configuring Allowed MAC Addresses to Protect the Switch from DHCP Snooping Database Alteration Attacks

- Example: Configuring MAC Limiting, Including Dynamic and Allowed MAC Addresses, to Protect the Switch from Ethernet Switching Table Overflow Attacks
- Example: Configuring MAC Limiting to Protect the Switch from DHCP Starvation Attacks
- Verifying That MAC Limiting Is Working Correctly
- Setting the none Action on an Interface to Override a MAC Limit Applied to All Interfaces (CLI Procedure)
- Understanding MAC Limiting and MAC Move Limiting for Port Security on EX-series Switches