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—When the limit is exceeded, 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 and the switch logs the message.

NOTE: If you do not want the switch to log messages received for invalid MAC addresses on an interface that has been configured for specific "allowed" MAC addresses, you can disable the logging by configuring the no-allowed-mac-log statement.

You configure MAC limiting per interface, not per VLAN. You can specify the maximum number of dynamic MAC addresses that can be learned on a single Layer 2 access interface or on all Layer 2 access interfaces.

You can choose to have one of the following actions performed when the limit of MAC addresses is exceeded:

- drop—Drop the packet and generate an alarm, an SNMP trap, or a system log entry. This is the default.
- log—Do not drop the packet but generate an alarm, an SNMP trap, or a system log entry.
- none—Take no action.
- shutdown—Disable the interface and generate an alarm. If you have configured the switch with the port-error-disable statement, the disabled interface recovers automatically upon expiration of the specified disable timeout. If you have not configured the switch for autorecovery from port error disabled conditions, you can bring up the disabled interfaces by running the clear ethernet-switching port-error command.

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.

   The action is not specified, so the switch performs the default action 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
```

- On all interfaces:

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

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 MAC Limiting, Including Dynamic and Allowed MAC Addresses, to Protect the Switch from Ethernet Switching Table Overflow 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)
- Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure)
- Understanding MAC Limiting and MAC Move Limiting for Port Security on EX Series Switches
- no-allowed-mac-log

Published: 2009-07-23