Configuring MAC Move Limiting (CLI Procedure)

MAC move limiting detects MAC address movement and MAC address spoofing on access ports. MAC address movements are tracked, and if a MAC address moves more than the configured number of times within one second, the configured (or default) action is performed. You enable this feature on VLANs.

NOTE: Although you enable this feature on VLANs, the MAC move limitation pertains to the number of movements for each individual MAC address rather than the total number of MAC address moves in the VLAN. For example, If the MAC move limit is set to 1, the switch allows an unlimited number of MAC address movements within the VLAN as long as the same MAC address does not move more than once.

You configure MAC move limiting per VLAN, not per interface (port). In the default configuration, the number of MAC moves permitted is unlimited.

You can choose to have one of the following actions performed when the MAC move limit 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 interfaces in the VLAN and generate an alarm. If you have configured the switch with the port-error-disable statement, the disabled interfaces recover 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 a MAC move limit for MAC addresses within a specific VLAN or for MAC addresses within all VLANs, using the CLI:

- On a single VLAN: To limit the number of MAC address movements that can be made by an individual MAC address within the VLAN employee-vlan, set a MAC move limit of 5:

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

  The action is not specified, so the switch performs the default action drop if it tracks that an individual MAC address within the employee-vlan has moved more than 5 times within one second.

- On all VLANs: To limit the number of MAC movements that can be made by individual MAC addresses within all VLANs, set a MAC move limit of 5:

```
[edit ethernet-switching-options secure-access-port]
set vlan all mac-move-limit 5
```

  The action is not specified, so the switch performs the default action drop if it tracks that an individual MAC address within any of the VLANs has moved more than 5 times within one second.

Related Topics

- Configuring MAC Move Limiting (J-Web Procedure)
- Example: Configuring Port Security, with DHCP Snooping, DAI, MAC Limiting, and MAC Move Limiting, on an EX Series Switch
- Verifying That MAC Move Limiting Is Working Correctly
- Monitoring Port Security
- 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

---

Published: 2009-07-23