Configuring MAC Move Limiting (CLI Procedure)

MAC move limiting detects MAC address movement and MAC address spoofing on access ports. It prevents hosts whose MAC addresses have not been learned by the EX-series switch from accessing the network. The MAC movements are tracked, and if more than the configured number of moves happens within one second, the configured (or default) action is performed.

You configure MAC move limiting per VLAN, not per interface (port). In the default configuration, the number of MAC moves permitted is unlimited. The default action that the switch will take if that limit is exceeded is drop—drop the packet and generate an alarm, an SNMP trap, or a system log entry.

To configure a MAC move limit on a specific VLAN or on all VLANs, using the CLI:

- On a single VLAN, to limit the number of MAC movements that can be made within VLAN employee-vlan, set a MAC limit of 5. The action is not specified, so the switch performs the default action drop if it tracks more than 5 MAC moves within the employee-vlan within one second:

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

- On all VLANs, to limit the number of MAC movements that can be made, set a MAC limit of 5. The action is not specified, so the switch performs the default action drop if it tracks more than 5 MAC moves within all VLANs within one second:

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

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
- Understanding MAC Limiting and MAC Move Limiting for Port Security on EX-series Switches