Understanding MAC Limiting and MAC Move Limiting for Port Security on EX Series Switches

MAC limiting protects against flooding of the Ethernet switching table (also known as the MAC forwarding table or Layer 2 forwarding table). You enable this feature on interfaces (ports). MAC move limiting detects MAC movement and MAC spoofing on access interfaces. You enable this feature on VLANs.

MAC Limiting

MAC limiting sets a limit on the number of MAC addresses that can be learned on a single Layer 2 access interface or on all the Layer 2 access interfaces on the switch. JUNOS Software provides two MAC limiting methods:

- Maximum number of MAC addresses—You configure the maximum number of dynamic MAC addresses allowed per interface. When the limit is exceeded, incoming packets with new MAC addresses are treated as specified by the configuration. The incoming packets with new MAC addresses can be ignored, dropped, logged, or the interface can be shut down or temporarily disabled.
- Allowed MAC—You configure 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. Allowed MAC binds MAC addresses to a VLAN so that the address does not get registered outside the VLAN. If an allowed MAC setting conflicts with a dynamic MAC setting, the allowed MAC setting takes precedence.

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.

MAC Move Limiting

MAC move limiting causes the switch to track the number of times a MAC address can move to a new interface (port). It can help to prevent MAC spoofing, and it can also detect and prevent loops.

If a MAC address moves more than the configured number of times within one second, the switch performs the configured action. You can configure MAC move limiting to apply to all VLANs or to a specific VLAN.

Actions for MAC Limiting and MAC Move Limiting

You can choose to have one of the following actions performed when the limit of MAC addresses or the limit of MAC moves 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.

See descriptions of results of these various action settings in Verifying That MAC Limiting Is Working Correctly .

If you have set a MAC limit to apply to all interfaces on the switch, you can override that setting for a particular interface by specifying action none. See Setting the none Action on an Interface to Override a MAC Limit Applied to All Interfaces (CLI Procedure).

MAC Addresses That Exceed the MAC Limit or MAC Move Limit

If you have configured the port-error-disable statement, you can view which interfaces are temporarily disabled due to exceeding the MAC limit or MAC move limit in the output for the show ethernet-switching interfaces command.

The log messages that indicate the MAC limit or MAC move limit has been exceeded include the offending MAC addresses that have exceeded the limit. See Troubleshooting Port Security for details.

Related Topics

- Port Security for EX Series Switches Overview
- 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
- Configuring MAC Limiting (CLI Procedure)
- Configuring MAC Limiting (J-Web Procedure)

- Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure)
- no-allowed-mac-log

Published: 2009-07-27