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. It prevents hosts whose MAC addresses have not been learned by the switch from accessing the network. 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. As soon as the limit is reached, incoming packets with new MAC addresses are dropped.
- 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. 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.

MAC Move Limiting

MAC move limiting prevents hosts whose MAC addresses have not been learned by the switch from accessing the network. Initial learning results when the host sends DHCP requests. If a new MAC address is detected on an interface, the packet is trapped to the switch. In general, when a host moves from one interface to another, the host has to renegotiate its IP address and lease (or be reauthenticated if 802.1X is configured on the switch). The DHCP request sent by the host can be one for a new IP address or one to validate the old IP address. If 802.1X is not configured, the Ethernet switching table entry is flushed from the original interface and added to the new interface. These MAC movements are tracked, and if more than the configured number of moves happens within one second, the configured action is performed.

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 reached:

- drop—Drop the packet and generate an alarm, an SNMP trap, or a system log entry.
- log—Do not drop the packet but generate an alarm, an SNMP trap, or a system log entry.
- none—Take no action.
- shutdown—Block data traffic on the interface and generate an alarm.

If you do not set an action, then the action is drop.

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

If you 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 view log messages that indicate the MAC limit or MAC move limit is exceeded, you can view 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 Port Security, with DHCP Snooping, DAI, MAC Limiting, and MAC Move Limiting, on an EX-series Switch
- 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
- Configuring MAC Limiting (CLI Procedure)
- Configuring MAC Limiting (J-Web Procedure)