Configuring MAC Limiting (J-Web Procedure)

MAC limiting protects against flooding of the Ethernet switching table on an 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—If 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.

You configure MAC limiting for each interface, not for each 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. The default action that the switch will take if that maximum number is exceeded is drop—drop the packet and generate an alarm, an SNMP trap, or a system log entry.

To enable MAC limiting on one or more interfaces using the J-Web interface:

1. Select Configure>Security>Port Security.
2. Select one or more interfaces from the Interface List.
3. Click the Edit button. If a message appears asking whether you want to enable port security, click Yes.
4. To set a dynamic MAC limit:
    1. Type a limit value in the MAC Limit box.
    2. Select an action from the MAC Limit Action box (optional). The switch takes this action when the MAC limit is exceeded. If you do not select an action, the switch applies the default action, drop.
        - Log—Generate a system log entry, an SNMP trap, or an alarm.
        - Drop—Drop the packets and generate a system log entry, an SNMP trap, or an alarm. (Default)
        - Shutdown—Shut down the VLAN and generate an alarm. You can mitigate the effect of this option by configuring the switch for autorecovery from the disabled state and specifying a disable timeout value. See Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) . If you have not configured autorecovery from the disabled state, you can bring up the interfaces by running the clear ethernet-switching port-error command.
        - None— No action to be taken.
5. To add allowed MAC addresses:
    1. Click Add.
    2. Type the allowed MAC address and click OK.

Repeat this step to add more allowed MAC addresses.

6. Click OK when you have finished setting MAC limits.
7. Click OK after the configuration has been successfully delivered.

NOTE: You can enable or disable port security on the switch at any time by clicking the Activate or Deactivate button on the Port Security Configuration page. If security status is shown as Disabled when you try to edit settings for any VLANs or interfaces (ports), a message asking whether you want to enable port security appears.

Related Topics

- Configuring MAC Limiting (CLI Procedure)
- 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
- 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)
- Understanding MAC Limiting and MAC Move Limiting for Port Security on EX Series Switches

Published: 2009-07-23