Enabling DHCP Snooping (J-Web Procedure)

DHCP snooping allows the EX Series switch to monitor and control DHCP messages received from untrusted devices connected to the switch. It builds and maintains a database of valid IP-address/MAC-address (IP-MAC) bindings called the DHCP snooping database.

You configure DHCP snooping for each VLAN, not for each interface (port). By default, DHCP snooping is disabled for all VLANs.

To enable DHCP snooping on one or more VLANs by using the J-Web interface:

1. Select Configure>Security>Port Security.
2. Select one or more VLANs from the VLAN list.
3. Click the Edit button. If a message appears asking if you want to enable port security, click Yes.
4. Select the Enable DHCP Snooping on VLAN check box and then click OK.
5. Click OK after the command 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), the message asking if you want to enable port security appears.

Related Topics

- Enabling DHCP Snooping (CLI Procedure)
- Example: Configuring Port Security, with DHCP Snooping, DAI, MAC Limiting, and MAC Move Limiting, on an EX Series Switch
- Example: Configuring DHCP Snooping, DAI , and MAC Limiting on an EX Series Switch with Access to a DHCP Server Through a Second Switch
- Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks
- Verifying That DHCP Snooping Is Working Correctly
- Monitoring Port Security
- Understanding DHCP Snooping for Port Security on EX Series Switches

Published: 2009-07-23