Enabling DHCP Snooping (CLI Procedure)

DHCP snooping allows the switch to monitor and control DHCP messages received from untrusted devices connected to the EX Series 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 a VLAN or all VLANs by using the CLI:

- On a specific VLAN (here, the VLAN is default):

```
[edit ethernet-switching-options secure-access port]
user@switch# set vlan default examine-dhcp
```

- On all VLANs:

```
[edit ethernet-switching-options secure-access port]
user@switch# set vlan all examine-dhcp
```

TIP: By default, the IP-MAC bindings are lost when the switch is rebooted and DHCP clients (the network devices, or hosts) must reacquire bindings. However, you can configure the bindings to persist by setting the dhcp-snooping-file statement to store the database file either locally or remotely.

TIP: For private VLANs (PVLANs), enable DHCP snooping on the primary VLAN. If you enable DHCP snooping only on a community VLAN, DHCP messages coming from PVLAN trunk ports are not snooped.

Related Topics

- Enabling DHCP Snooping (J-Web 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: 2009-09-24