Configuring IP Source Guard (CLI Procedure)

You can use the IP source guard access port security feature on EX-series switches to mitigate the effects of source IP address spoofing and source MAC address spoofing. If IP source guard determines that a host connected to an access interface has sent a packet with an invalid source IP address or source MAC address in the packet header, it ensures that the switch does not forward the packet—that is, the packet is discarded.

You enable the IP source guard feature on VLANs. You can enable it on a specific VLAN, on all VLANs, or on a VLAN range.

NOTE: IP source guard applies only to access interfaces and only to untrusted interfaces. If you enable IP source guard on a VLAN that includes trunk interfaces or an interface set to dhcp-trusted, the CLI shows an error when you try to commit the configuration.

Before you configure IP source guard, be sure that you have:

Enabled DHCP snooping on the VLAN or VLANs on which you will configure IP source guard. See Enabling DHCP Snooping (CLI Procedure).

To enable IP source guard on a VLAN, all VLANs, or a VLAN range (a series of tagged VLANs) by using the CLI:

NOTE: Replace values displayed in italics with values for your configuration.

- On a specific VLAN:

```
[edit ethernet-switching-options secure-access port]
user@switch#set vlan default ip-source-guard
```

- On all VLANs:

```
[edit ethernet-switching-options secure-access port]
user@switch# set vlan all ip-source-guard
```

- On a VLAN range:

  a. Set the VLAN range (the VLAN name is employee):

```
[edit vlans]
user@switch# set employee vlan-range 100-101
```

  b. Associate an interface with a VLAN-range number (100 in the following example) and set the port mode to access:

```
[edit interfaces]
user@switch# set ge-0/0/6 unit 0 family ethernet-switching port-mode access
vlan members 100
```

  c. Enable IP source guard on the VLAN employee:

```
[edit ethernet-switching-options secure-access port]
user@switch# set vlan employee ip-source-guard
```

NOTE: You can use the no-ip-source-guard statement to disable IP source guard for a specific VLAN after you have enabled the feature for all VLANs.

To view results of the configuration steps before committing the configuration, type the show command at the user prompt.

To commit these changes to the active configuration, type the commit command at the user prompt.

Related Topics

- Verifying That IP Source Guard Is Working Correctly
- Example: Configuring IP Source Guard on a Data VLANThat Shares an Interface with a Voice VLAN

- Example: Configuring IP Source Guard with Other EX-series Switch Features to Mitigate Address-Spoofing Attacks on Untrusted Access Interfaces
- Understanding IP Source Guard for Port Security on EX-series Switches