

Configuration of IP Source Guard Binding Database on Sx500 Series Stackable Switches

Objective

IP Source Guard is a security feature that can be used to prevent traffic attacks caused when a host tries to use the IP address of a neighboring host. When IP Source Guard is enabled, the switch only transmits client IP traffic to IP addresses contained in the DHCP Snooping Binding database. If the packet that a host sends matches an entry in the database, the switch forwards the packet. If the packet does not match an entry in the database, it is dropped.

In a real time scenario, one way in which IP Source Guard is used is to help prevent man-in-the-middle attacks where an untrusted third party attempts to masquerade as a genuine user. Based on the addresses which are configured in the IP source guard binding database, only the traffic from the client with that IP address is allowed and the rest of the packets are dropped.

Note: DHCP Snooping should be enabled for IP Source Guard to function. In order to get more details on how to enable DHCP Snooping please refer to the article [DHCP Snooping Binding Database Configuration on Sx500 Series Stackable Switches](#). It is also necessary to configure the binding database to specify which IP addresses are allowed.

This article explains how to configure binding database for IP source guard on Sx500 Series Stackable Switches.

Applicable Devices

- Sx500 Series Stackable Switches

Software Version

- v1.2.7.76

Configuration of IP Source Guard Binding Database

Binding Database

Step 1. Log in to the web configuration utility, and choose **Security > IP Source Guard > Binding Database**. The *Binding Database* page opens:

Binding Database

Supported IP Format: Version 4

TCAM Resources Consumed:

☀ Insert Inactive: ☒ Retry Frequency Sec. (Range: 10 - 600, Default: 60)
☐ Never

Binding Database Table (DHCP Snooping Binding Database Table)

Filter: ☐ VLAN ID equals to (Range: 1 - 4094)
☐ MAC Address equals to
☐ IP Address equals to
☒ Interface equals to ☐ Unit/Slot Port ☒ LAG

VLAN ID	MAC Address	IP Address	Interface	Status	Type	Reason
0 results found.						

Step 2. Click the appropriate entry from the following options in the Insert Inactive field to choose how often the inactive entries should be made active by the switch. DHCP Snooping Binding Database uses Ternary Content Addressable Memory (TCAM) to maintain the database.

- **Retry Frequency** — Gives the frequency which the TCAM resources are checked. The default value is 60.
- **Never** — Never try to activate the inactive addresses.

Step 3. Click **Apply** to update the running configuration file.

Add Binding Database Entry

Step 1. Log in to the web configuration utility, and choose **IP Configuration > DHCP > DHCP Snooping Binding Database** which opens the *DHCP Snooping Binding Database* page.

DHCP Snooping Binding Database

Supported IP Format: Version 4

Binding Database Table

Filter: ☐ VLAN ID equals to (Range: 1 - 4094)
☐ MAC Address equals to
☐ IP Address equals to
☐ Interface equals to ☒ Unit/Slot Port ☐ LAG

<input type="checkbox"/>	VLAN ID	MAC Address	IP Address	Interface	Type	Lease Time	IP Source Guard	Status	Reason
0 results found.									

Step 2. Click **Add** to enter the entries in the *Add DHCP Snooping Entry* page.

Supported IP Format: Version 4

VLAN ID:

MAC Address:

IP Address:

Interface: ☒ Unit/Slot Port ☐ LAG

Type: ☒ Dynamic ☐ Static

Lease Time: ☐ Infinite ☒ User Defined Sec. (Range: 10 - 4294967294, Default: Infinite)

Step 3. Choose the VLAN ID from the drop-down list on which the packet is expected in the VLAN ID field.

Step 4. Enter the MAC address to be matched in the MAC Address field.

Step 5. Enter the IP address to be matched in the IP Address field.

Step 6. Choose the interface from the Interface drop-down list to show whether to display ports or LAGs on which the packet is expected.

Type: ☐ Dynamic ☒ Static

Lease Time: ☒ Infinite ☐ User Defined

Step 7. Click the type to show whether the entry is Dynamic or Static in the Type field.

- Dynamic — Entry has a limited lease time.
- Static — Entry is statically configured.

Step 8. Enter the Lease time in the Lease time field. If the entry is dynamic enter the duration of time the entry will remain active. If there is no lease time then click **Infinite**.

<input type="checkbox"/>	VLAN ID	MAC Address	IP Address	Interface	Type	Lease Time	IP Source Guard	
							Status	Reason
<input type="checkbox"/>	1	00:b0:d0:86:d6:f7	192.0.2.2	GE1/1/1	Dynamic	3405	Inactive	No Snoop VLAN
<input type="button" value="Add..."/> <input type="button" value="Delete"/> <input type="button" value="Clear Dynamic"/>								

The reason if the interface is not active is displayed in the Reason field. The reasons can be as follows:

- No problem — Interface is active.
- No Snoop VLAN — DHCP Snooping is not enabled on the VLAN.
- Trusted Port — Port is trusted.
- Resource Problem — TCAM resources are consumed.

DHCP Snooping Binding Database

Supported IP Format: Version 4

Binding Database Table

Filter: ☒ VLAN ID equals to (Range: 1 - 4094)

☒ MAC Address equals to

☒ IP Address equals to

☒ Interface equals to ☒ Unit/Slot Port ☐ LAG

<input type="checkbox"/>	VLAN ID	MAC Address	IP Address	Interface	Type	Lease Time	IP Source Guard	
							Status	Reason
<input type="checkbox"/>	1	00:b0:d0:86:d6:f7	192.0.2.2	GE1/1/1	Dynamic	3456	Inactive	No Snoop VLAN

Step 9. To see a subset of the entries, enter the appropriate search criteria in the Binding Database Table and click **Go**. The filter check boxes are used to filter out a particular entry from the DHCP Binding Database Table.

Step 10. (Optional) To remove the values which have been entered and to enter new values, click **Clear Dynamic**.

Step 11. Click **Apply** to update the running configuration file.