

# Konfiguration der IP Source Guard Binding Database auf Stackable Switches der Serie Sx500

## Ziel

IP Source Guard ist eine Sicherheitsfunktion, mit der Datenverkehrsangriffe verhindert werden können, die entstehen, wenn ein Host versucht, die IP-Adresse eines benachbarten Hosts zu verwenden. Wenn IP Source Guard aktiviert ist, überträgt der Switch nur den Client-IP-Datenverkehr an IP-Adressen, die in der DHCP Snooping Binding-Datenbank enthalten sind. Wenn das Paket, das ein Host sendet, mit einem Eintrag in der Datenbank übereinstimmt, leitet der Switch das Paket weiter. Wenn das Paket nicht mit einem Eintrag in der Datenbank übereinstimmt, wird es verworfen.

In einem Echtzeit-Szenario kann IP Source Guard beispielsweise eingesetzt werden, um Man-in-the-Middle-Angriffe zu verhindern, bei denen ein nicht vertrauenswürdiger Dritter versucht, sich als legitimer Benutzer zu tarnen. Basierend auf den in der IP Source Guard-Bindungsdatenbank konfigurierten Adressen ist nur der Datenverkehr vom Client mit dieser IP-Adresse zulässig, und die restlichen Pakete werden verworfen.

**Hinweis:** DHCP-Snooping sollte aktiviert sein, damit IP Source Guard funktioniert. Weitere Informationen zur Aktivierung von DHCP Snooping finden Sie im Artikel [DHCP Snooping Binding Database Configuration auf Stackable Switches der Serie Sx500](#). Außerdem muss die Bindungsdatenbank so konfiguriert werden, dass angegeben wird, welche IP-Adressen zulässig sind.

In diesem Artikel wird erläutert, wie Sie Bindungsdatenbank für IP Source Guard auf Stackable Switches der Serie Sx500 konfigurieren.

## Anwendbare Geräte

- Stackable Switches der Serie Sx500

## Softwareversion

- v1.2.7.76

## Konfiguration der IP Source Guard Binding Database

### Bindungsdatenbank

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Security > IP Source Guard > Binding Database** aus. Die Seite *Bindungsdatenbank* wird geöffnet:

### 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.						

Schritt 2: Klicken Sie in den folgenden Optionen im Feld Inaktiv einfügen auf den entsprechenden Eintrag, um festzulegen, wie oft der Switch inaktive Einträge aktivieren soll. Die DHCP Snooping Binding Database verwendet den Ternary Content Addressable Memory (TCAM), um die Datenbank zu verwalten.

- Häufigkeit erneut eingeben - Gibt die Häufigkeit an, mit der die TCAM-Ressourcen überprüft werden. Der Standardwert ist 60.

- Nie - Versuchen Sie nie, die inaktiven Adressen zu aktivieren.

Schritt 3: Klicken Sie auf **Apply**, um die aktuelle Konfigurationsdatei zu aktualisieren.

## Hinzufügen von Bindungsdatenbankeinträgen

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **IP Configuration > DHCP > DHCP Snooping Binding Database** aus, die die Seite *DHCP Snooping Binding Database* öffnet.

### 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.								

Schritt 2: Klicken Sie auf **Hinzufügen**, um die Einträge auf der Seite *DHCP-Snooping-Eintrag*

hinzufügen einzugeben.



Supported IP Format: Version 4

VLAN ID: 1

MAC Address: 00b0d086d6f7

IP Address: 192.0.2.2

Interface:  Unit/Slot 1/1 Port GE1  LAG 1

Type:  Dynamic  Static

Lease Time:  Infinite  User Defined 3456 Sec. (Range: 10 - 4294967294, Default: Infinite)

Apply Close

Schritt 3: Wählen Sie die VLAN-ID aus der Dropdown-Liste aus, in der das Paket im Feld "VLAN ID" erwartet wird.

Schritt 4: Geben Sie im Feld MAC Address (MAC-Adresse) die abzugleichende MAC-Adresse ein.

Schritt 5: Geben Sie die IP-Adresse ein, die im Feld "IP Address" (IP-Adresse) zugeordnet werden soll.

Schritt 6: Wählen Sie in der Dropdown-Liste "Interface" (Schnittstelle) die Schnittstelle aus, um anzuzeigen, ob Ports oder LAGs angezeigt werden sollen, für die das Paket erwartet wird.



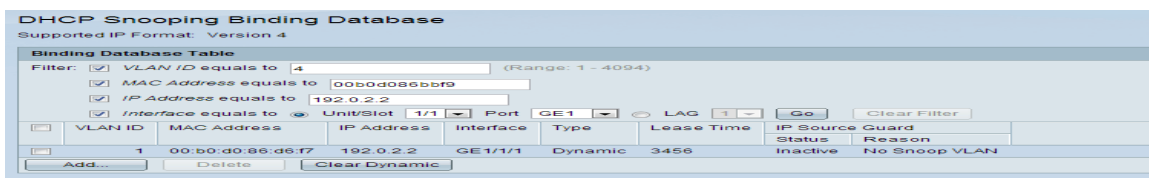
Type:  Dynamic  Static

Lease Time:  Infinite  User Defined 3456

Schritt 7: Klicken Sie im Feld Typ auf den Typ, um anzuzeigen, ob der Eintrag dynamisch oder statisch ist.

- Dynamic (Dynamisch): Der Eintrag hat eine begrenzte Leasing-Zeit.
- Statisch - Der Eintrag ist statisch konfiguriert.

Schritt 8: Geben Sie die Leasingzeit in das Feld Leasingzeit ein. Wenn der Eintrag dynamisch ist, geben Sie die Dauer der Zeit ein, die der Eintrag aktiv bleibt. Wenn keine Leasedauer vorhanden ist, klicken Sie auf **Unbegrenzt**.



DHCP Snooping Binding Database

Supported IP Format: Version 4

Binding Database Table

Filter:  VLAN ID equals to 4 (Range: 1 - 4094)  
 MAC Address equals to 00b0d086d6f7  
 IP Address equals to 192.0.2.2

VLAN ID  Unit/Slot 1/1 Port GE1  LAG 1

VLAN ID	MAC Address	IP Address	Interface	Type	Lease Time	IP Source Guard Status	Reason
1	00-b0:d0:86:d6:f7	192.0.2.2	GE1/1/1	Dynamic	3456	Inactive	No Snoop VLAN

Der Grund, warum die Schnittstelle nicht aktiv ist, wird im Feld "Grund" angezeigt. Die Gründe hierfür können wie folgt sein:

- Kein Problem - Schnittstelle ist aktiv.

- Kein Snoop-VLAN - DHCP-Snooping ist im VLAN nicht aktiviert.
- Vertrauenswürdiger Port - Port ist vertrauenswürdig.
- Ressourcenproblem - TCAM-Ressourcen werden genutzt.

### 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

Schritt 9: Um eine Teilmenge der Einträge anzuzeigen, geben Sie die entsprechenden Suchkriterien in der Binding Database Table ein, und klicken Sie auf **Go**. Mit den Filterkästchen wird ein bestimmter Eintrag aus der DHCP-Binding-Datenbanktabelle herausgefiltert.

Schritt 10: (Optional) Um die eingegebenen Werte zu entfernen und neue Werte einzugeben, klicken Sie auf **Clear Dynamic (Dynamisch löschen)**.

Schritt 11: Klicken Sie auf **Apply**, um die aktuelle Konfigurationsdatei zu aktualisieren.