

# SX500系列堆叠式交换机上IP源防护绑定数据库的配置

## 目标

IP源防护是一种安全功能，可用于防止主机尝试使用相邻主机的IP地址时引起的流量攻击。启用IP源防护后，交换机仅将客户端IP流量传输到DHCP监听绑定数据库中包含的IP地址。如果主机发送的数据包与数据库中的条目匹配，交换机将转发该数据包。如果数据包与数据库中的条目不匹配，则会将其丢弃。

在实时场景中，使用IP源防护的一种方式是帮助防止不受信任的第三方试图伪装成正版用户的中间人攻击。根据在IP源防护绑定数据库中配置的地址，仅允许来自具有该IP地址的客户端的流量，并丢弃其余数据包。

**注意：**应启用DHCP监听，IP源防护才能正常工作。要获取有关如何启用DHCP监听的更多详细信息，请参阅Sx500系列可堆叠交换机上的[DHCP监听绑定数据库配置文章](#)。还需要配置绑定数据库以指定允许哪些IP地址。

本文介绍如何在Sx500系列堆叠式交换机上为IP源防护配置绑定数据库。

## 适用设备

- Sx500系列堆叠式交换机

## 软件版本

- v1.2.7.76

## IP源防护绑定数据库的配置

### 绑定数据库

步骤1. 登录到Web配置实用程序，然后选择Security > IP Source Guard > Binding Database。将打开“绑定数据库”页：

### 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.						

步骤2.在Insert Inactive字段中，从以下选项中点击适当的条目，以选择交换机应激活非活动条目的频率。DHCP监听绑定数据库使用三态内容可寻址存储器(TCAM)来维护数据库。

- 重试频率 — 提供检查TCAM资源的频率。默认值为 60。
- 从不 — 从不尝试激活非活动地址。

步骤3.单击“应用”更新运行配置文件。

## 添加绑定数据库条目

步骤1.登录Web配置实用程序，然后选择IP Configuration > DHCP > DHCP Snooping Binding Database，打开DHCP Snooping Binding Database页。

### 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.								

步骤2.单击Add以在Add DHCP Snooping Entry页中输入条目。

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)

步骤3.从VLAN ID字段中数据包预期所在的下拉列表中选择VLAN ID。

步骤4.在MAC Address字段中输入要匹配的MAC地址。

步骤5.在IP Address字段中输入要匹配的IP地址。

步骤6.从Interface下拉列表中选择接口，以显示是显示端口还是LAG，其上应有数据包。

Type:  Dynamic  Static

Lease Time:  Infinite  User Defined

步骤7.在“类型”字段中单击类型以显示条目是“动态”还是“静态”。

- 动态 — 条目的租用时间有限。
- 静态 — 条目是静态配置的。

步骤8.在Lease time字段中输入Lease time。如果条目是动态的，请输入条目保持活动状态的持续时间。如果没有租用时间，请单击Infinite。

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

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

接口未处于活动状态的原因显示在原因字段中。原因如下：

- 无问题 — 接口处于活动状态。
- 无监听VLAN - VLAN上未启用DHCP监听。
- 受信任端口 — 端口受信任。
- 资源问题 — TCAM资源被消耗。

## 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

步骤9.要查看条目的子集，请在绑定数据库表中输入适当的搜索条件，然后单击**开始**。过滤器复选框用于从DHCP绑定数据库表中过滤特定条目。

步骤10. ( 可选 ) 要删除已输入的值并输入新值，请单击“**清除动态**”。

步骤11.单击“**应用**”更新运行配置文件。