Configuración de la Base de Datos de Enlace de IP Source Guard en los Switches Stackables de la Serie Sx500

Objetivo

IP Source Guard es una función de seguridad que se puede utilizar para prevenir ataques de tráfico causados cuando un host intenta utilizar la dirección IP de un host vecino. Cuando se habilita IP Source Guard, el switch sólo transmite el tráfico IP del cliente a las direcciones IP contenidas en la base de datos DHCP Snooping Binding. Si el paquete que envía un host coincide con una entrada en la base de datos, el switch reenvía el paquete. Si el paquete no coincide con una entrada en la base de datos, se descarta.

En un escenario en tiempo real, una forma en la que se utiliza IP Source Guard es ayudar a evitar ataques de intrusos en los que un tercero no confiable intenta disfrazarse de usuario genuino. Según las direcciones configuradas en la base de datos de enlace de la protección de origen de IP, sólo se permite el tráfico del cliente con esa dirección IP y se descarta el resto de los paquetes.

Nota: Para que IP Source Guard funcione, debe estar habilitado DHCP Snooping. Para obtener más detalles sobre cómo habilitar la indagación DHCP, consulte el artículo *Configuración de la Base de Datos de Vinculación de Indagación DHCP en los Switches Apilables de la Serie Sx500*. También es necesario configurar la base de datos de enlace para especificar qué direcciones IP se permiten.

En este artículo se explica cómo configurar la base de datos de enlace para la protección de origen IP en los switches apilables de la serie Sx500.

Dispositivos aplicables

Switches apilables · Sx500 Series

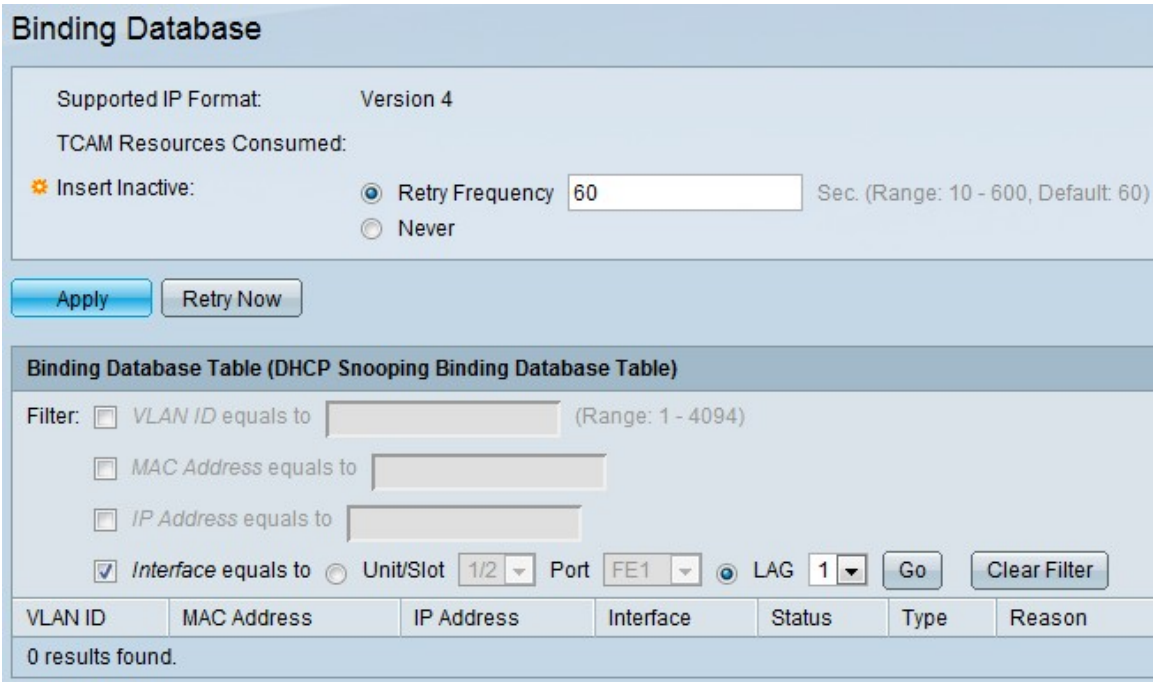
Versión del software

•v1.2.7.76

Configuración de IP Source Guard Binding Database

Base de datos de enlace

Paso 1. Inicie sesión en la utilidad de configuración web y elija **Security > IP Source Guard > Binding Database**. Se abre la página *Base de datos de enlace*:



Paso 2. Haga clic en la entrada correspondiente de las siguientes opciones en el campo Insertar inactivo para elegir la frecuencia con la que el switch debe activar las entradas inactivas. La base de datos de enlace de detección DHCP utiliza la memoria direccionable de contenido ternario (TCAM) para mantener la base de datos.

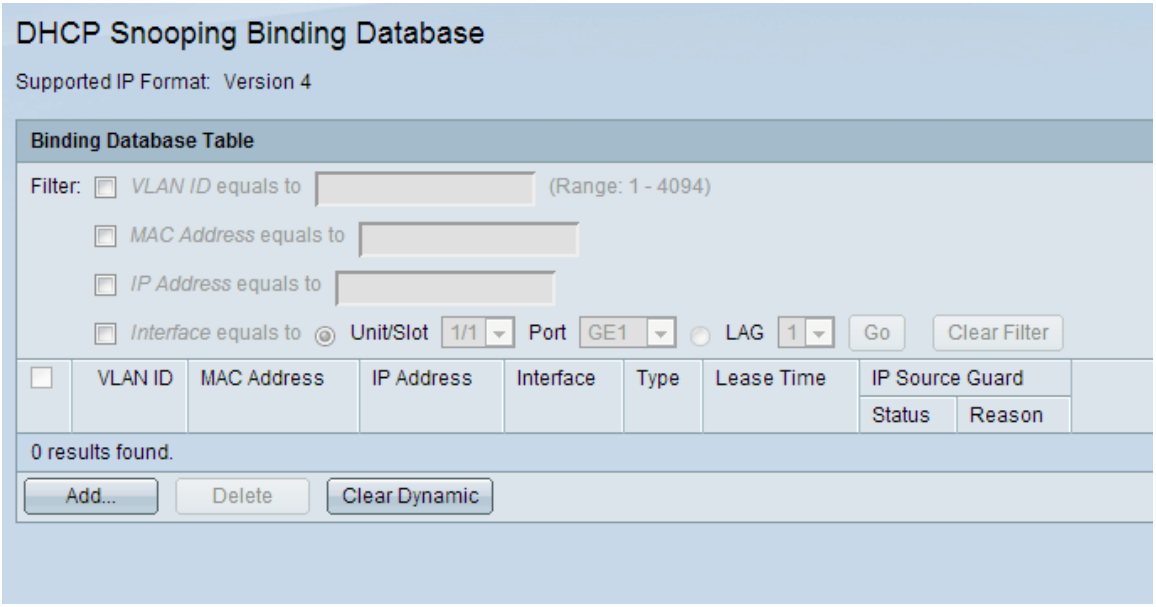
Frecuencia de reintento ·: indica la frecuencia con la que se comprueban los recursos TCAM. El valor predeterminado es 60.

·Nunca: nunca intente activar las direcciones inactivas.

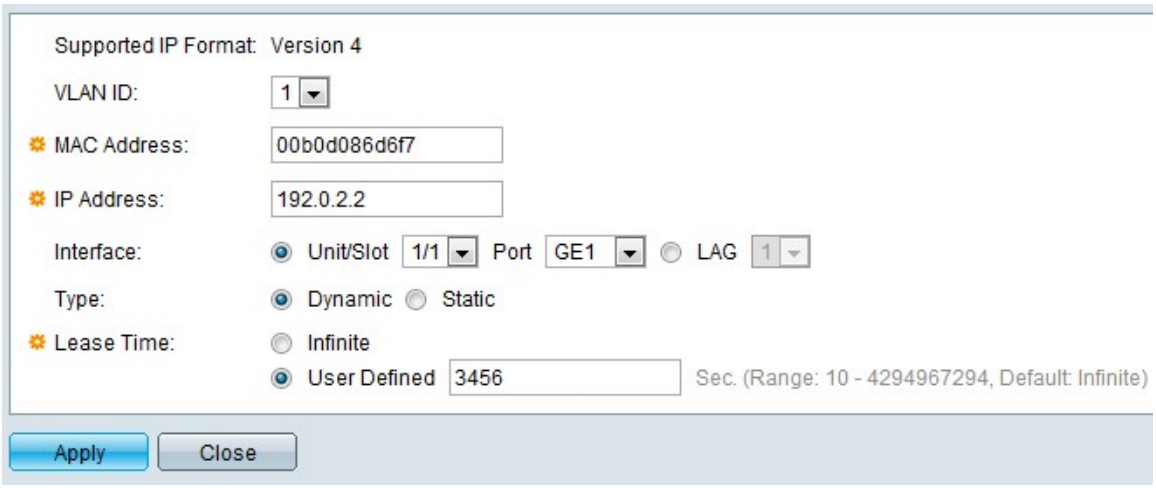
Paso 3. Haga clic en **Aplicar** para actualizar el archivo de configuración en ejecución.

Agregar entrada de base de datos de enlace

Paso 1. Inicie sesión en la utilidad de configuración web y elija **IP Configuration > DHCP > DHCP Snooping Binding Database** que abre la página *DHCP Snooping Binding Database*.



Paso 2. Haga clic en **Add** para ingresar las entradas en la página *Add DHCP Snooping Entry*.

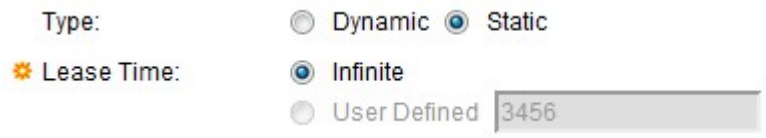


Paso 3. Elija el ID de VLAN de la lista desplegable en la que se espera el paquete en el campo ID de VLAN.

Paso 4. Introduzca la dirección MAC que debe coincidir en el campo Dirección MAC.

Paso 5. Introduzca la dirección IP que se debe buscar en el campo IP Address (Dirección IP).

Paso 6. Elija la interfaz de la lista desplegable Interfaz para mostrar si se muestran los puertos o los LAG en los que se espera el paquete.

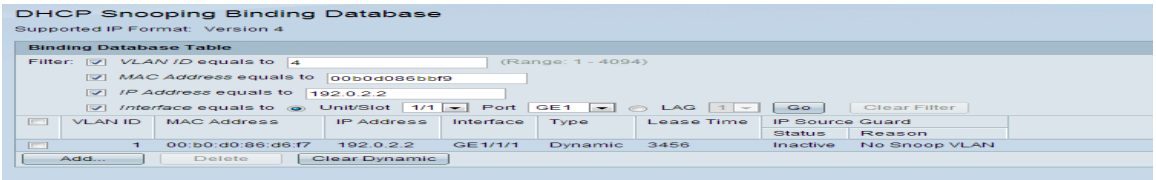


Paso 7. Haga clic en el tipo para mostrar si la entrada es dinámica o estática en el campo Tipo.

·dinámica: la entrada tiene un tiempo de arrendamiento limitado.

·Estático: la entrada se configura estáticamente.

Paso 8. Introduzca el tiempo de concesión en el campo Tiempo de concesión. Si la entrada es dinámica, introduzca la duración del tiempo que la entrada permanecerá activa. Si no hay tiempo de arrendamiento, haga clic en **Infinite**.



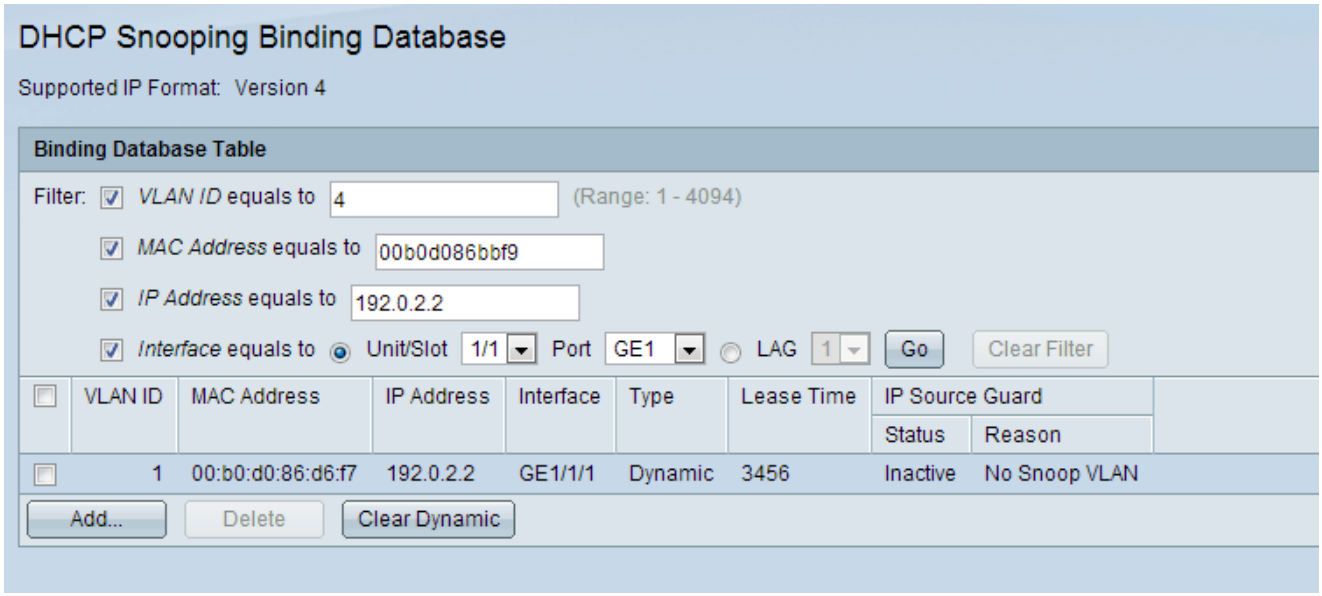
La razón si la interfaz no está activa se muestra en el campo Motivo. Las razones pueden ser las siguientes:

·No hay problema: la interfaz está activa.

·No Snoop VLAN: la función DHCP Snooping no está habilitada en la VLAN.

·puerto de confianza: el puerto es de confianza.

Problema · recurso: se consumen los recursos TCAM.



Paso 9. Para ver un subconjunto de las entradas, introduzca los criterios de búsqueda apropiados en la tabla de base de datos de enlace y haga clic en **Ir**. Las casillas de verificación de filtro se utilizan para filtrar una entrada determinada de la tabla de base de datos de enlace DHCP.

Paso 10. (Opcional) Para quitar los valores introducidos e introducir nuevos valores, haga clic en **Borrar dinámica**.

Paso 11. Haga clic en **Aplicar** para actualizar el archivo de configuración en ejecución.