Configuración de la detección IGMP en los switches de la serie CBS220

Objetivo

El objetivo de este documento es mostrarle cómo configurar el Snooping del protocolo de administración de grupos de Internet (IGMP) en los switches Cisco Business serie 220.

Dispositivos aplicables | Versión de software

- Serie CBS220 (Ficha técnica) |2.0.0.17

Introducción

La multidifusión es la técnica de capa de red utilizada para transmitir paquetes de datos de un host a hosts seleccionados en la red. En la capa inferior, el switch transmite el tráfico multicast en todos los puertos, incluso si sólo un host necesita recibirlo. El snooping del protocolo de administración de grupos de Internet (IGMP) se utiliza para reenviar el tráfico multidifusión del protocolo de Internet versión 4 (IPv4) al host deseado.

Cuando se habilita IGMP, detecta los mensajes IGMP intercambiados entre el router IPv4 y los hosts multicast conectados a las interfaces. A continuación, mantiene una tabla que restringe el tráfico de multidifusión IPv4 y los reenvía dinámicamente a las partes que necesitan recibirlos.

Las siguientes configuraciones son prerrequisitos para configurar IGMP:

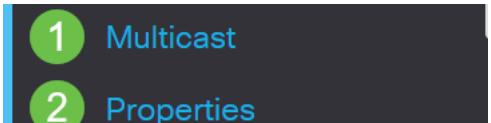
- Configuración de la red de área local virtual (VLAN)
- Habilitar el filtrado de multidifusión de puente (pasos que se muestran en la siguiente sección)

Habilitar la indagación IGMP y la acción de multidifusión

Para que la indagación IGMP funcione, se debe habilitar el filtrado de multidifusión de puente. La función IGMP Snooping debe habilitarse globalmente y para cada VLAN relevante en la página IGMP Snooping.

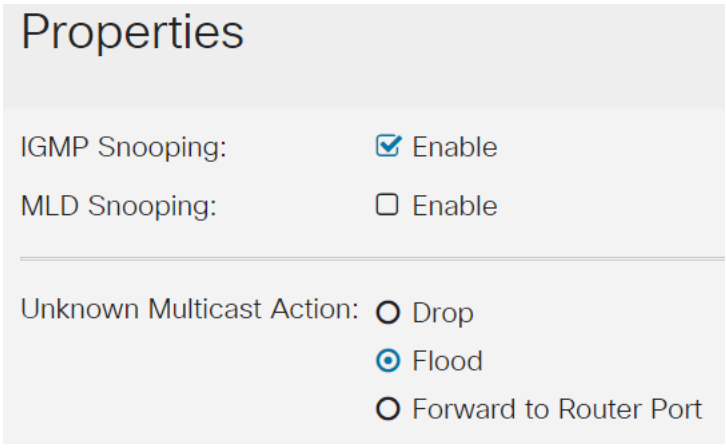
Paso 1

Inicie sesión en la utilidad de configuración web y elija **Multicast > Properties**.



Paso 2

Asegúrese de que IGMP Snooping esté habilitado. Seleccione el procedimiento para *Acción de multidifusión desconocida*. Las opciones son *Drop*, *Flood* o *Forward to Router Port*.



Paso 3

Haga clic en Apply (Aplicar).

Configuración de IGMP Snooping

Paso 1

Inicie sesión en la utilidad basada en Web y elija **Multicast > IGMP Snooping**.

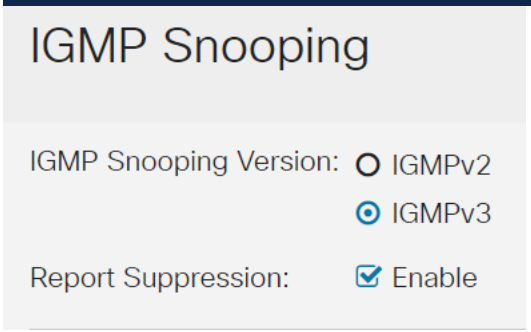
Paso 2

Seleccione el botón de opción de la versión de IGMP que desea utilizar. Sus opciones son IGMPv2 o IGMPv3.

La supresión de informes está activada de forma predeterminada. Si desactiva esta función, todos los informes IGMP se reenviarán a los routers de multidifusión.

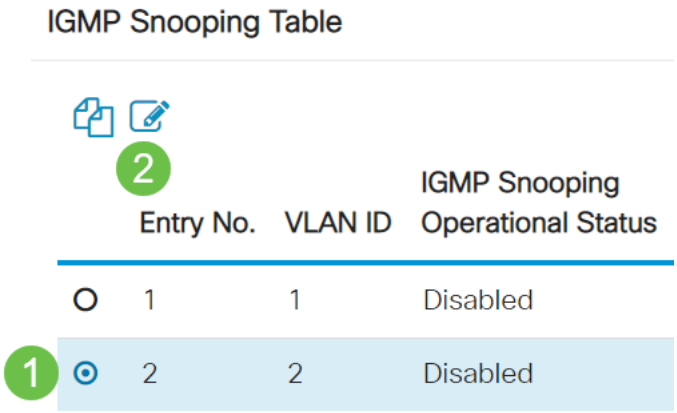
La supresión de informes IGMP se soporta solamente cuando la consulta de multidifusión tiene informes IGMPv1 e IGMPv2. Esta función no se soporta cuando la consulta incluye

informes IGMPv3. El switch utiliza la supresión de informes IGMP para reenviar solamente un informe IGMP por consulta de router de multidifusión a los dispositivos de multidifusión. Cuando se habilita la supresión de informes IGMP, el switch envía el primer informe IGMP de todos los hosts para un grupo a todos los routers de multidifusión. El switch no envía los informes IGMP restantes para el grupo a los routers de multidifusión. Esta función evita que se envíen informes duplicados a los dispositivos de multidifusión. El switch siempre reenvía solamente el primer informe IGMPv1 o IGMPv2 de todos los hosts de un grupo a todos los routers de multidifusión, independientemente de la consulta del router de multidifusión también incluye solicitudes de informes IGMPv3.



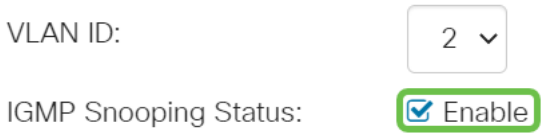
Paso 3

Seleccione una VLAN y haga clic en el **icono de edición**.



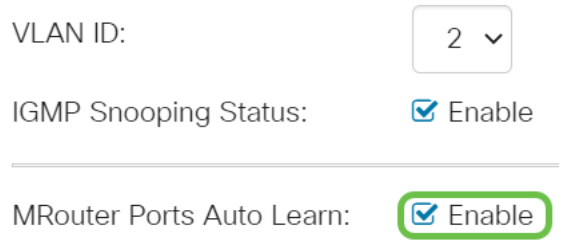
Paso 4

Marque la casilla de verificación Enable para *IGMP Snooping Status*. Esto habilitará la indagación IGMP en la VLAN. El dispositivo monitorea el tráfico de red para determinar qué hosts han solicitado que se envíe tráfico de multidifusión.



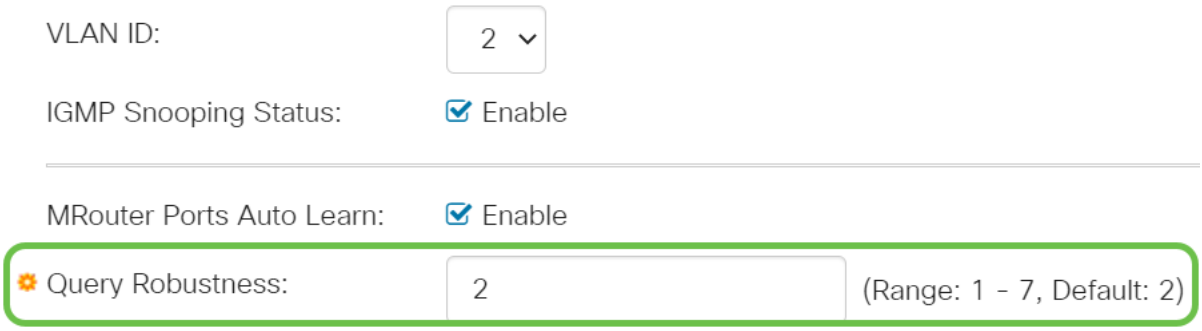
Paso 5 (opcional)

Para permitir que el router multicast aprenda automáticamente los puertos conectados, marque la casilla de verificación Enable para *MRouter Ports Auto Learn*.



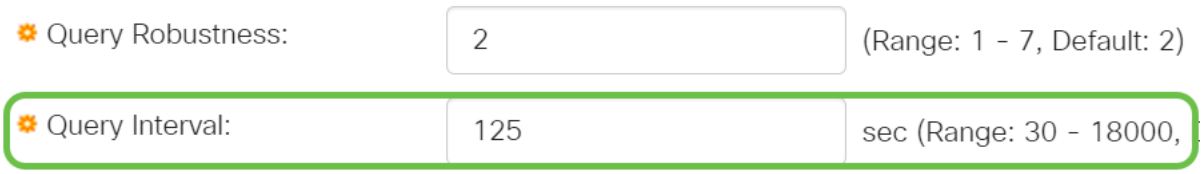
Paso 6

Query Robustness (Solidez de la consulta): introduzca la variable de solidez que se utilizará si este switch es el consultor seleccionado.



Paso 7

Intervalo de consulta: introduzca el intervalo entre las consultas generales que se utilizarán si este switch es el consultor seleccionado.



Paso 8

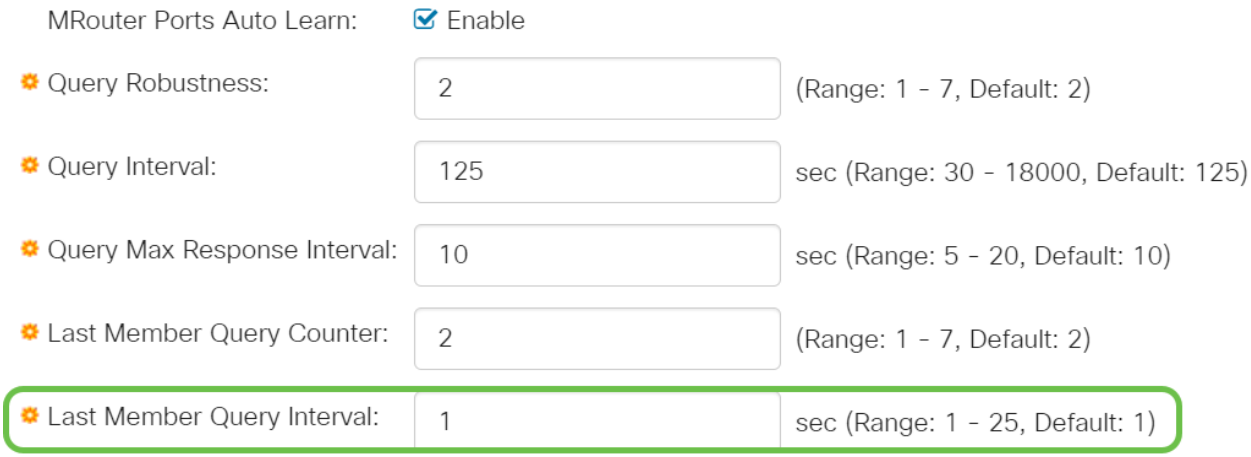
Intervalo máximo de respuesta de consulta: introduzca el retraso utilizado para calcular el código máximo de respuesta insertado en las consultas generales periódicas.

Paso 9

Contador de consulta de último miembro: el número de consultas específicas de grupo IGMP enviadas antes de que el dispositivo asuma que no hay más miembros para el grupo si el dispositivo es el consultor elegido.

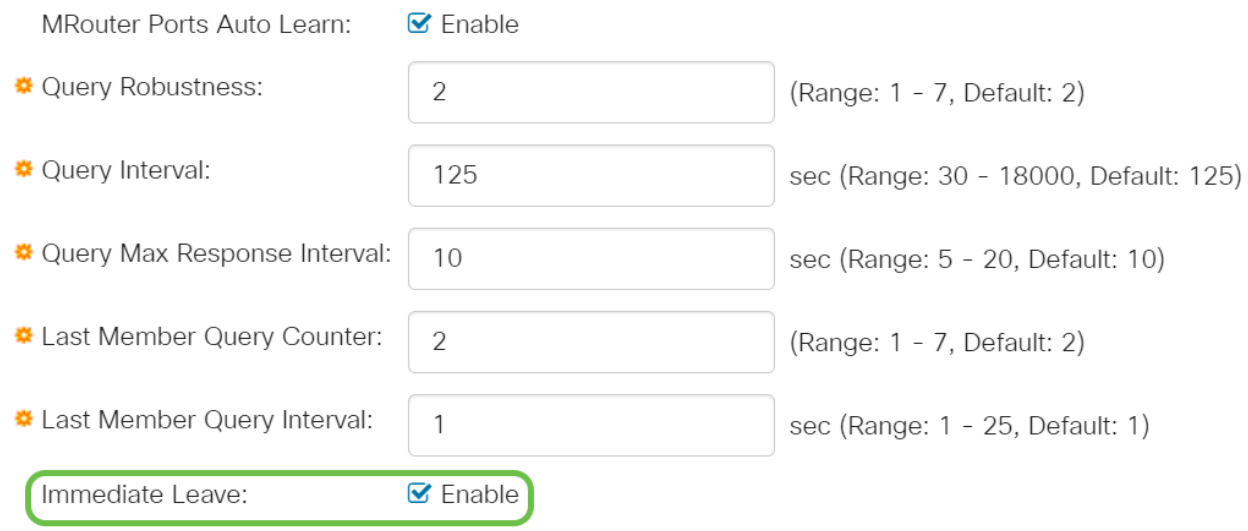
Paso 10

Last Member Query Interval (Intervalo de consulta del último miembro): introduzca el retraso máximo de respuesta que se utilizará si el switch no puede leer el valor máximo de tiempo de respuesta de las consultas específicas del grupo enviadas por el consultor seleccionado.



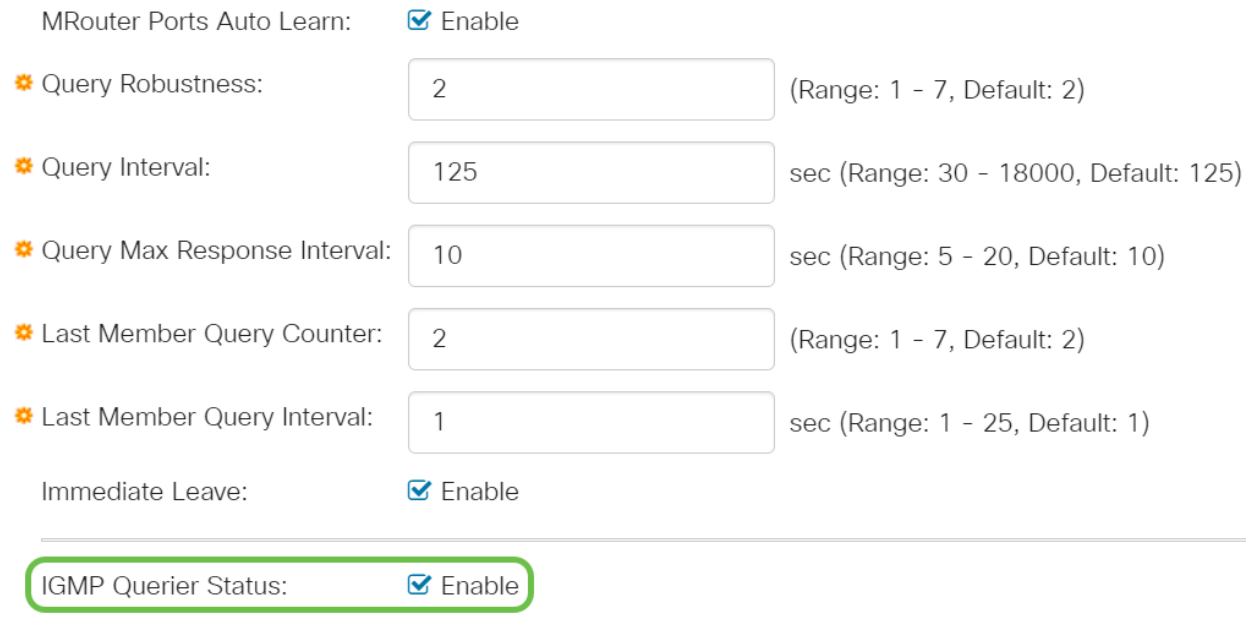
Paso 11

Abandono inmediato: seleccione esta opción para permitir que el switch elimine una interfaz que envía un mensaje de ausencia de la tabla de reenvío sin antes enviar consultas generales basadas en MAC a la interfaz. Cuando se recibe un mensaje de ausencia inmediata de un grupo de abandono de IGMP desde un host, el sistema quita el puerto host de la entrada de tabla. Después de transmitir las consultas IGMP del router Multicast, elimina las entradas periódicamente si no recibe ningún informe de afiliación IGMP de los clientes Multicast. Cuando está activada, esta función reduce el tiempo que se tarda en bloquear el tráfico IGMP innecesario enviado a un puerto de dispositivo.



Paso 12 (opcional)

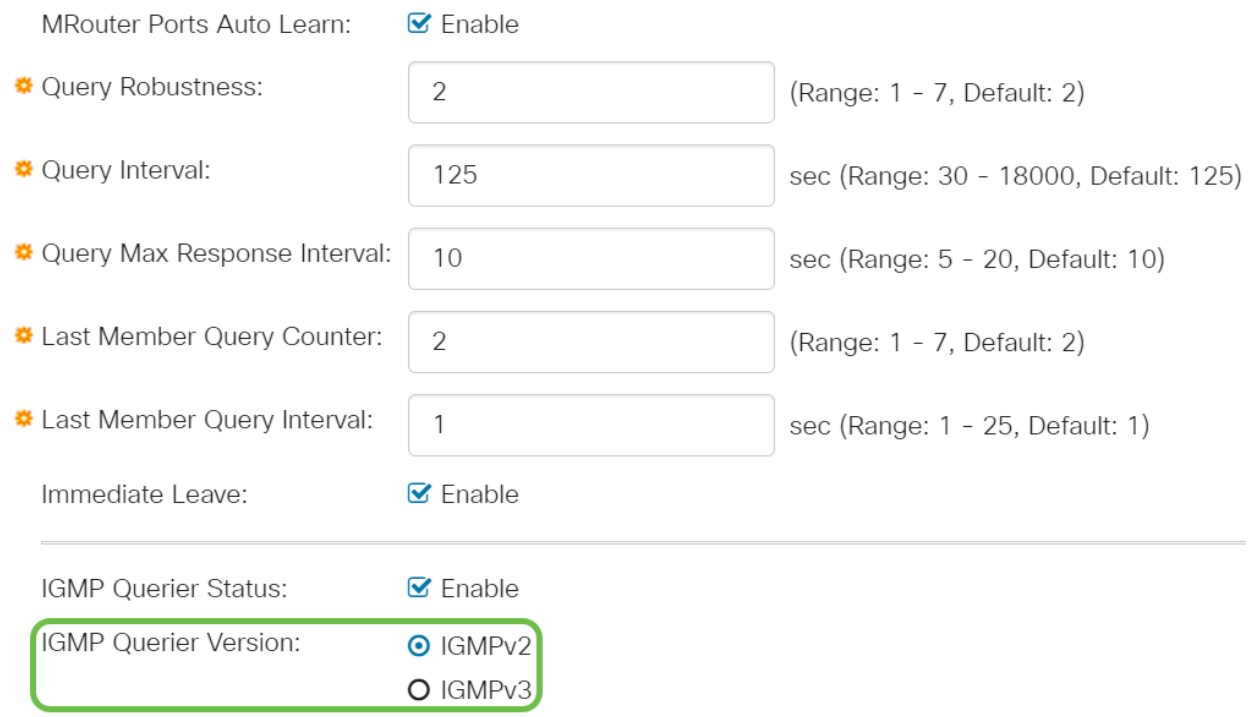
Estado del solicitante IGMP: seleccione esta opción para activar esta función. Esta función es necesaria si no hay ningún router de multidifusión.



Paso 13

Versión del solicitante IGMP: seleccione la versión de IGMP que se utilizará si el dispositivo se convierte en el consultor seleccionado. Seleccione IGMPv3 si hay switches y/o routers de multidifusión en la VLAN que realizan el reenvío de multidifusión IP específico de origen. De lo contrario, seleccione IGMPv2.

En este ejemplo, se elige la versión 2. Permite que la consulta de pertenencia sea general y específica del grupo. La consulta de pertenencia general se utiliza para determinar todos los grupos de multidifusión a los que se suscriben las estaciones. La consulta de pertenencia específica de grupo se utiliza para determinar si hay un suscriptor para un grupo determinado.



Paso 14

Haga clic en Apply (Aplicar). Se actualiza el archivo de configuración en ejecución.

Los cambios en la configuración del temporizador de indagación IGMP (incluidos la solidez de consultas, el intervalo de consultas, etc.) no surten efecto en los temporizadores que ya se han creado.

Paso 15

Para guardar esta configuración de la configuración en ejecución en la configuración de inicio, haga clic en el **icono Guardar** en la esquina superior derecha de la pantalla.

Conclusión

Así de sencillo, ahora ha configurado IGMP Snooping.

Para obtener más configuraciones, refiérase a la Guía de Administración de Switches Cisco Business 220 Series.

Si desea ver más artículos sobre los switches CBS220, consulte la página de soporte de la serie 220.