Seguridad de puertos en los switches Cisco Business 220

Objetivo

En este artículo se explican sus opciones de seguridad de puertos en el Cisco Business 220 Series Switch.

Dispositivos aplicables | Versión del firmware

- Serie CBS220 (Ficha técnica) |2.0.0.17

Introducción

La seguridad de la red se puede aumentar limitando el acceso en un puerto a los usuarios con direcciones MAC específicas. Las direcciones MAC pueden aprenderse dinámicamente o configurarse estáticamente. La seguridad de los puertos monitorea los paquetes recibidos y aprendidos. El acceso a los puertos bloqueados está limitado a los usuarios con direcciones MAC específicas.

La seguridad de puerto no se puede habilitar en los puertos en los que está habilitado 802.1X o en los puertos definidos como destino SPAN.

Port Security tiene dos modos:

- **Bloqueo clásico**: todas las direcciones MAC aprendidas del puerto están bloqueadas y el puerto no aprende ninguna dirección MAC nueva. Las direcciones aprendidas no están sujetas al envejecimiento ni al reaprendizaje.
- **Bloqueo dinámico limitado**: el dispositivo aprende las direcciones MAC hasta el límite configurado de direcciones permitidas. Una vez alcanzado el límite, el dispositivo no aprende direcciones adicionales. En este modo, las direcciones están sujetas a envejecimiento y reaprendizaje.

Cuando se detecta una trama de una nueva dirección MAC en un puerto en el que no está autorizada (el puerto está bloqueado de forma clásica y hay una nueva dirección MAC o el puerto está bloqueado de forma dinámica y se ha superado el número máximo de direcciones permitidas), se invoca el mecanismo de protección y se puede realizar una de las siguientes acciones:

- La trama se descarta.
- La trama se reenvía.
- La trama se descarta y se genera un mensaje SYSLOG.
- El puerto está apagado.

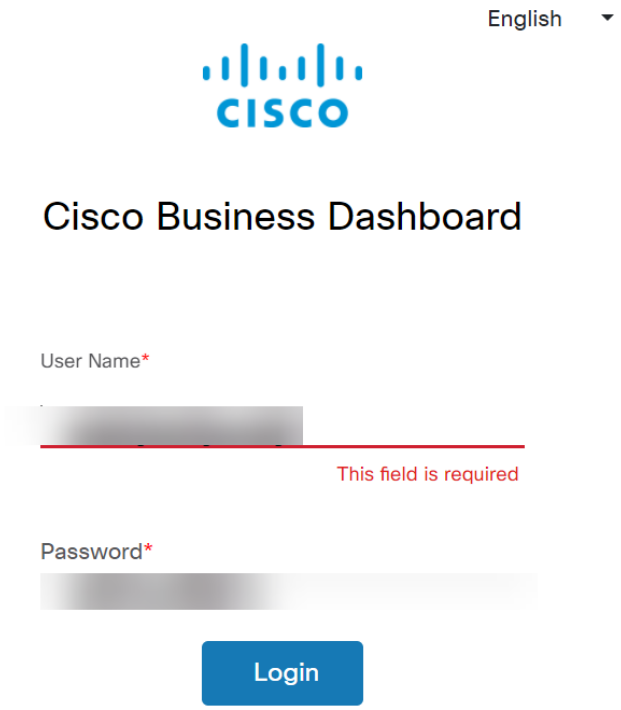
Cuando la dirección MAC segura se ve en otro puerto, la trama se reenvía, pero la dirección MAC no se aprende en ese puerto.

Además de una de estas acciones, también puede generar trampas y limitar su frecuencia y número para evitar sobrecargar los dispositivos.

Configuración de la seguridad del puerto

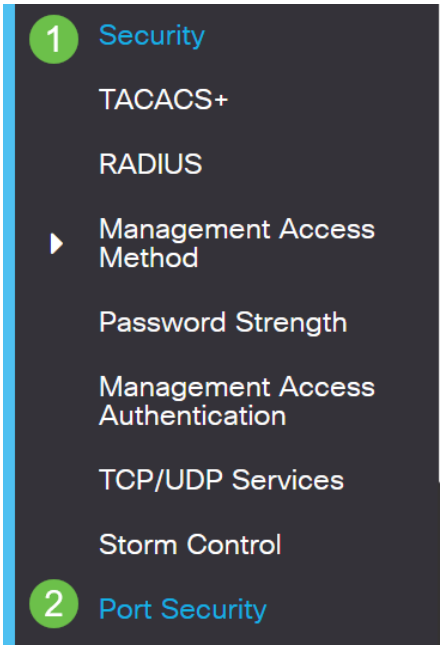
Paso 1

Inicie sesión en la interfaz de usuario web (IU).



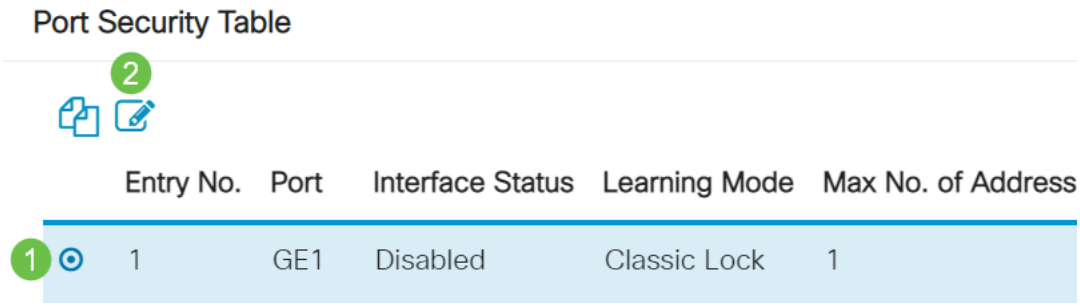
Paso 2

En el menú de la izquierda, seleccione **Seguridad > Seguridad de puerto**.



Paso 3

Seleccione una interfaz para modificar y luego haga clic en el **icono de edición**.



Paso 4

Introduzca los parámetros.

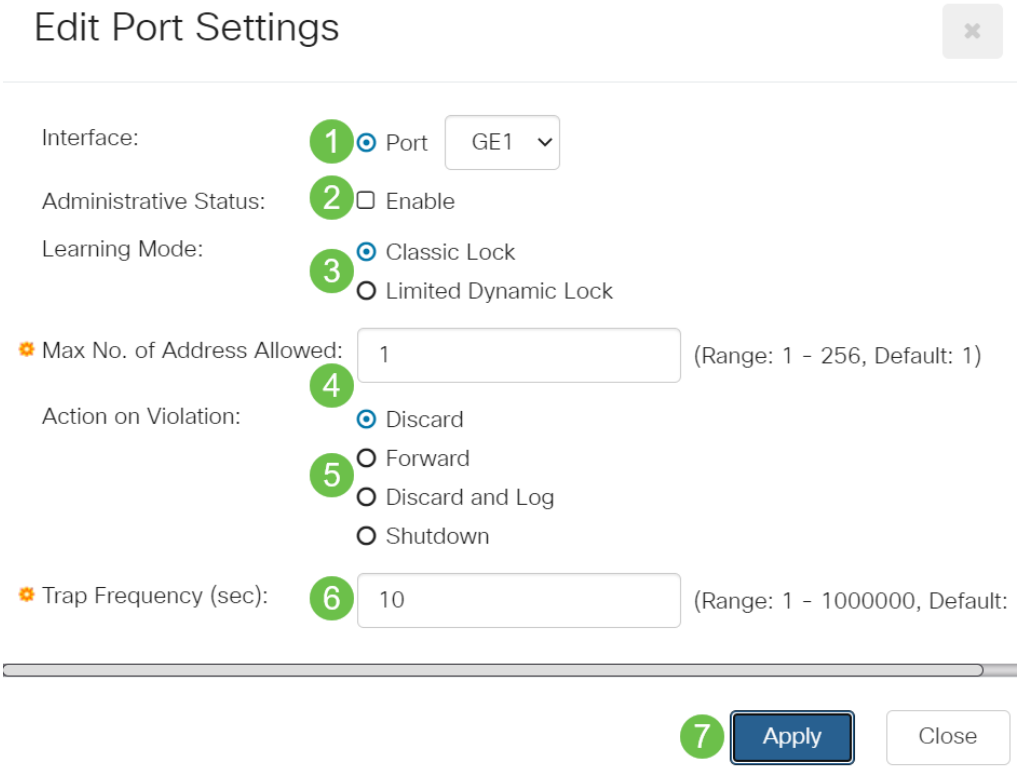
- **Interfaz**: seleccione el nombre de la interfaz.
- **Estado administrativo**: seleccione esta opción para bloquear el puerto.
- **Modo de aprendizaje**: seleccione el tipo de bloqueo de puerto. Para configurar este campo, el estado de la interfaz debe estar desbloqueado. El campo Modo de aprendizaje sólo se habilita si el campo Estado de la interfaz está bloqueado. Para cambiar el modo de aprendizaje, se debe borrar la interfaz de bloqueo. Después de cambiar el modo, se puede restablecer la interfaz de bloqueo. Las opciones son:
  - **Bloqueo clásico**: bloquea el puerto inmediatamente, independientemente del número de direcciones que ya se hayan aprendido.
  - **Bloqueo dinámico limitado**: bloquea el puerto eliminando las direcciones MAC dinámicas actuales asociadas al puerto. El puerto aprende hasta las direcciones máximas permitidas en el puerto. Se habilita tanto el reaprendizaje como el envejecimiento de las direcciones MAC.

- **Nº máximo de direcciones permitidas**: introduzca el número máximo de direcciones MAC que se pueden aprender en el puerto si se selecciona el modo de aprendizaje de bloqueo dinámico limitado. El número 0 indica que sólo se admiten direcciones estáticas

en la interfaz.

- **Acción sobre la violación**: seleccione una acción que se aplicará a los paquetes que lleguen a un puerto bloqueado. Las opciones son:
    - **Descartar**: descarta paquetes de cualquier · de origen no aprendido
    - **Reenvío**: reenvía paquetes de una fuente desconocida sin aprender la dirección MAC
    - **Descarte y Registro**: descarta paquetes de cualquier origen no aprendido, cierra la interfaz, registra los eventos y envía trampas a los receptores de trampa especificados Shutdown: descarta paquetes de cualquier origen no aprendido y cierra el puerto. El puerto permanece apagado hasta que se reactiva o hasta que se reinicia el dispositivo.
    - **Frecuencia de trampa**: introduzca el tiempo mínimo (en segundos) que transcurre entre trampas

Haga clic en Apply (Aplicar).



Si desea ver un ejemplo del comportamiento predeterminado para la seguridad de puerto en su CBS220, desproteja Port Security Behavior.

Conclusión

Es tan simple como eso. Disfrute de su red segura

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

Si desea ver otros artículos, consulte la página de soporte de switches Cisco Business

serie 220.