Configuración de SNMP en routers RV160 y RV260

Objetivo

El objetivo de este artículo es mostrarle cómo configurar los parámetros del protocolo simple de administración de red (SNMP) en los routers RV160 y RV260.

Introducción

SNMP es un protocolo estándar de Internet para recopilar y organizar datos en dispositivos administrados en las redes IP. Permite a los administradores de red gestionar, supervisar, recibir notificaciones de eventos críticos a medida que se producen en la red y solucionar problemas.

El marco SNMP consta de tres elementos; un administrador SNMP, un agente SNMP y una base de información de administración (MIB). La función del administrador SNMP es controlar y monitorear las actividades de los hosts de red que utilizan SNMP. El agente SNMP se encuentra dentro del software del dispositivo y ayuda en el mantenimiento de los datos para administrar el sistema. Por último, MIB es un área de almacenamiento virtual para la información de administración de red. Estos tres se combinan para supervisar y gestionar los dispositivos de una red.

Los dispositivos RV160/260 admiten SNMP versión v1, v2c y v3. Actúan como agentes SNMP que responden a los comandos SNMP de los Sistemas de administración de red SNMP. Los comandos soportados son los comandos estándar SNMP get/next/set. Los dispositivos también generan mensajes de trampa para notificar al administrador SNMP cuando se producen condiciones de alarma. Algunos ejemplos son los reinicios, los ciclos de alimentación y los eventos de link WAN.

Dispositivos aplicables

- RV160
- RV260

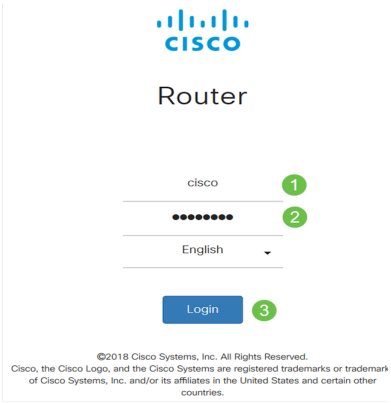
Versión del software

- 1.0.00.13

Configuración de SNMP

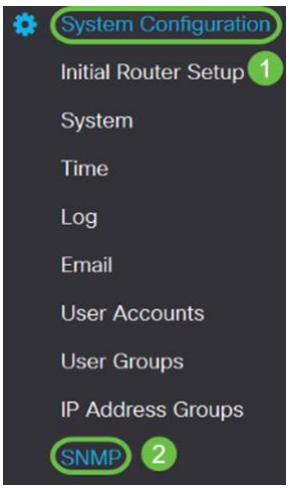
Para configurar el SNMP del router, realice los pasos siguientes.

Paso 1. Inicie sesión en la página de configuración web del router.



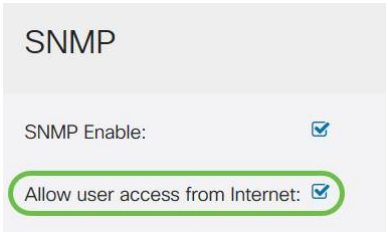
Nota: En este artículo, utilizaremos el RV260W para configurar SNMP. La configuración puede variar en función del modelo que esté utilizando.

Paso 2. Vaya a **Configuración del sistema > SNMP**.



Paso 3. Marque la casilla de verificación **SNMP Enable** para habilitar SNMP.

Paso 4. (Opcional) Marque la casilla de verificación **Permitir acceso de usuario desde Internet** para permitir el acceso de usuario autorizado fuera de la red a través de aplicaciones de administración como Cisco FindIT Network Management.

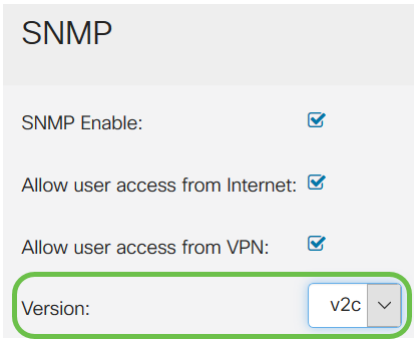


Paso 5. (Opcional) Marque la casilla de verificación **Permitir acceso de usuario desde VPN** para permitir el acceso autorizado desde una red privada virtual (VPN).

Paso 6. En el menú desplegable *Versión*, elija una versión SNMP para usar en la red. Las opciones son:

- v1: opción menos segura. Utiliza texto sin formato para cadenas de comunidad.
- v2c - El soporte mejorado de manejo de errores proporcionado por SNMPv2c incluye códigos de error expandidos que distinguen diferentes tipos de errores; todos los tipos de errores se informan a través de un solo código de error en SNMPv1.
- v3 - SNMPv3 proporciona acceso seguro a los dispositivos mediante la autenticación y el cifrado de paquetes de datos a través de la red. Los algoritmos de autenticación incluyen el algoritmo de resumen de mensajes (MD5) y el algoritmo hash seguro (SHA). Los métodos de cifrado incluyen el estándar de cifrado de datos (DES) y el estándar de cifrado avanzado (AES).

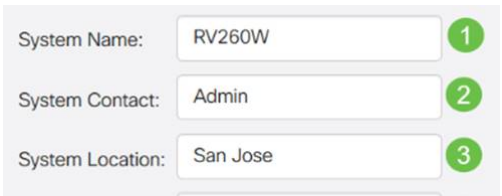
Para obtener más información sobre SNMPv3, haga clic aquí.



En este ejemplo, **v2c** se ha seleccionado como la *versión*.

Paso 7. Introduzca los campos siguientes

- **Nombre del sistema**: introduzca un nombre para el router para facilitar la identificación en las aplicaciones de administración de red.
- **Contacto del sistema** : introduzca el nombre de una persona o administrador para identificarse con el router en caso de emergencia.
- **Ubicación del sistema**: introduzca una ubicación del router. Esto facilita la localización de un problema para un administrador.
- **Obtener comunidad**: introduzca el nombre de la comunidad SNMP en el campo *Obtener comunidad*. Crea una comunidad de sólo lectura que se utiliza para acceder y recuperar la información del agente SNMP.
- **Establecer comunidad**: en el campo *Establecer comunidad*, ingrese un nombre de comunidad SNMP. Crea una comunidad de lectura y escritura que se utiliza para acceder y modificar la información del agente SNMP. Solo se aceptan las solicitudes de los dispositivos que se identifican con este nombre de comunidad. Este es un nombre creado por el usuario. El valor predeterminado es private (privado).

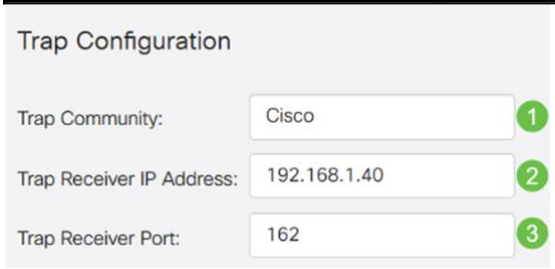


Configuración de trampa

Con las configuraciones Trap, puede establecer la dirección de origen de cada paquete de trampa SNMP enviado por el router en una sola dirección independientemente de la interfaz saliente.

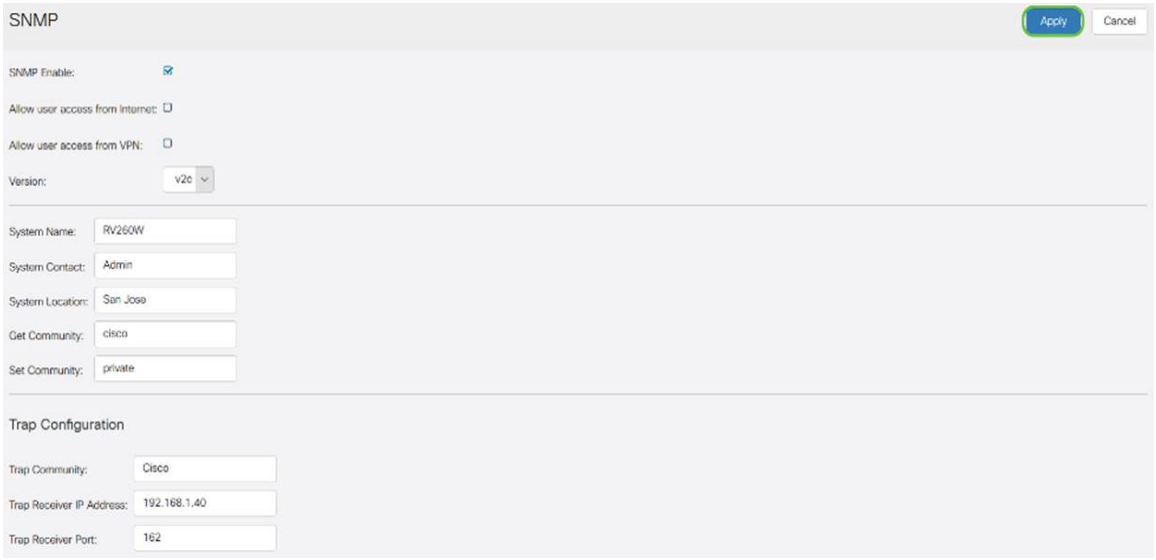
Paso 8. Para configurar la trampa SNMP, introduzca la siguiente información.

comunidad de trampa	Introduzca el nombre de la comunidad de trampa
Dirección IP del receptor de trampas	Introduzca la dirección IP
Puerto del receptor de trampas	Introduzca el número de puerto



Nota: Normalmente, SNMP utiliza el protocolo de datagramas de usuario (UDP) como protocolo de transporte y los puertos UDP predeterminados para el tráfico SNMP son 161 (SNMP) y 162 (SNMP Trap).

Paso 9. Haga clic en Apply (Aplicar).



Ahora debería haber activado y configurado correctamente SNMP en el router RV160/RV260.