

Configuración del protocolo simple de administración de red (SNMP) en los routers VPN RV320 y RV325

Objetivo

El protocolo simple de administración de red (SNMP) es un protocolo de capa de aplicación que se utiliza para administrar y supervisar el tráfico de red. SNMP mantiene todos los registros de actividad de varios dispositivos en la red para ayudarle a encontrar rápidamente el origen de los problemas en la red cuando sea necesario. En la serie RV32x del router VPN, puede habilitar SNMPv1/v2c, SNMPv3, o ambos al mismo tiempo para tener el rendimiento deseado de la red.

El objetivo de este documento es explicar cómo configurar el SNMP en la serie RV32x del router VPN.

Dispositivo aplicable

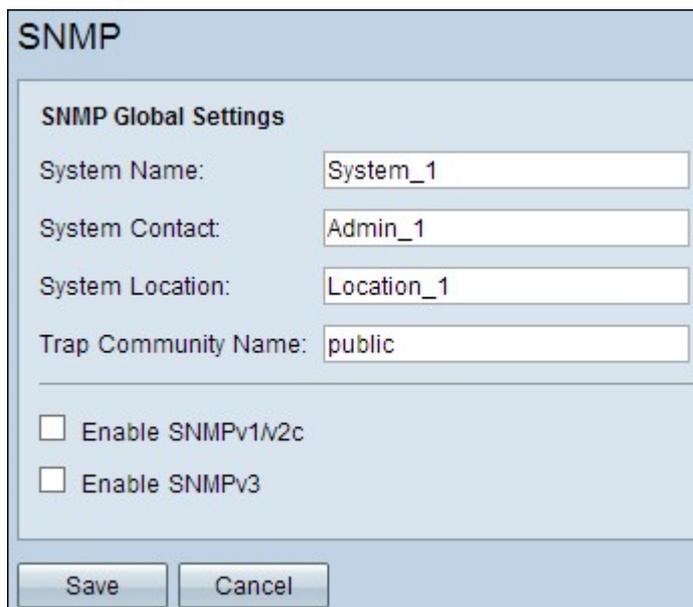
Router VPN Dual WAN · RV320
Router VPN Dual WAN · RV325 Gigabit

Versión del software

•v1.1.0.09

Configuración SNMP

Paso 1. Inicie sesión en la utilidad de configuración web y elija **Administración del sistema > SNMP**. Se abre la *página SNMP*:



The screenshot shows the 'SNMP' configuration page. It has a title bar 'SNMP' and a section 'SNMP Global Settings'. There are four text input fields: 'System Name' with 'System_1', 'System Contact' with 'Admin_1', 'System Location' with 'Location_1', and 'Trap Community Name' with 'public'. Below these are two checkboxes: 'Enable SNMPv1/v2c' and 'Enable SNMPv3', both of which are unchecked. At the bottom are 'Save' and 'Cancel' buttons.

Paso 2. Ingrese el nombre de host en el campo *System Name*.

Paso 3. Ingrese el nombre o la información de contacto de la persona responsable del router en el campo *Contacto del sistema*.

Paso 4. Ingrese la ubicación física del router en el campo *Ubicación del sistema*.

Nota: La información ingresada en los campos *Contacto del sistema* y *Ubicación del sistema* no modifica el comportamiento del dispositivo. Puede introducirlos como desee para ayudar a administrar mejor sus dispositivos (por ejemplo, puede que le resulte conveniente incluir un número de teléfono en el campo *Contacto del sistema*).

Paso 5. Introduzca el nombre de comunidad de trampa al que pertenece el agente en el campo *Trap Community Name*. Una trampa es un mensaje que el dispositivo envía cuando se produce un evento específico. El nombre de comunidad de trampa puede tener hasta 64 caracteres alfanuméricos. El nombre de comunidad de trampa predeterminado es *público*.

Paso 6. Haga clic en **Guardar para guardar la configuración**.

Configuración de SNMPv1/SNMPv2c

SNMPv1 es la primera versión de SNMP y ahora se considera inseguro. SNMPv2c es una versión mejorada de SNMP. Proporciona más seguridad que SNMPv1 y mejora la gestión de errores.

SNMP

SNMP Global Settings

System Name:

System Contact:

System Location:

Trap Community Name:

Enable SNMPv1/2c

Get Community Name:

Set Community Name:

SNMPv1/2c Trap Receiver IP Address: (For IPv4)

Enable SNMPv3

Paso 1. Marque **Enable SNMPv1/2c** para habilitar SNMPv1/2c.

SNMP

SNMP Global Settings

System Name: System_1

System Contact: Admin_1

System Location: Location_1

Trap Community Name: public

Enable SNMPv1/v2c

Get Community Name: community_1

Set Community Name: setcommunity_1

SNMPv1/v2c Trap Receiver IP Address: 192.168.1.2 (For IPv4)

Enable SNMPv3

Save Cancel

Paso 2. Introduzca un nombre de comunidad en el campo *Obtener nombre de comunidad*. Get Community Name es la cadena de comunidad de sólo lectura para autenticar el comando SNMP Get. El comando Get se utiliza para recuperar la información del dispositivo SNMP. El nombre de la comunidad Get puede tener hasta 64 caracteres alfanuméricos. El valor predeterminado Get Community Name es *público*.

Paso 3. Introduzca un nombre de comunidad en el campo *Establecer nombre de comunidad*. Es la cadena de comunidad de lectura/escritura para autenticar el comando SNMP Set. El comando Set se utiliza para modificar o establecer las variables en el dispositivo. El nombre de la comunidad puede tener hasta 64 caracteres alfanuméricos. El valor predeterminado Set Community Name es *private*.

Paso 4. Ingrese la dirección IP o el nombre de dominio del servidor específico donde se ejecuta el software de administración SNMP en el campo *Dirección IP del Receptor de Trampa* SNMPv1/v2c. Se envía un mensaje de trampa al administrador desde el servidor para notificar al administrador si se produce algún error o fallo.

Paso 5. Haga clic en **Guardar** para guardar la configuración.

Configuración de SNMPv3

SNMPv3 es la última versión de SNMP y proporciona el mayor nivel de seguridad entre las tres versiones SNMP. También proporciona configuración remota.

SNMP

SNMP Global Settings

System Name:

System Contact:

System Location:

Trap Community Name:

Enable SNMPv1/v2c

Enable SNMPv3

Group Table

Group Name	Security	Access MIBs
0 results found!		

User Table

Enable	User Name	Authentication	Privacy	Group
0 results found!				

SNMPv3 Trap Receiver IP Address: (For IPv4)

SNMPv3 Trap Receiver User:

Paso 1. Marque **Enable SNMPv3** para habilitar SNMPv3.

Administración de grupos SNMPv3

La administración de grupos SNMPv3 permite crear grupos con diferentes niveles de acceso al dispositivo. A continuación, puede asignar usuarios a estos grupos según lo considere oportuno.

SNMP

SNMP Global Settings

System Name:

System Contact:

System Location:

Trap Community Name:

Enable SNMPv1/v2c

Enable SNMPv3

Group Table

Group Name	Security	Access MIBs
0 results found!		
<input type="button" value="Add"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>

User Table

Enable	User Name	Authentication	Privacy	Group
0 results found!				
<input type="button" value="Add"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>		

SNMPv3 Trap Receiver IP Address: (For IPv4)

SNMPv3 Trap Receiver User:

Paso 1. Haga clic en **Agregar** en la tabla de grupo para agregar un nuevo grupo en la tabla de administración de grupo SNMPv3. Se abre la página *SNMPv3 Group Management*.

SNMP

SNMPv3 Group Management

Group Name:

Group1

Security Level:

No Authentication, No Privacy

MIBs

- | | | |
|---|--|------------------------------------|
| <input type="checkbox"/> 1 | <input checked="" type="radio"/> Read Only | <input type="radio"/> Read / Write |
| <input type="checkbox"/> 1.3.6.1.2.1 | <input checked="" type="radio"/> Read Only | <input type="radio"/> Read / Write |
| <input type="checkbox"/> 1.3.6.1.2.1.1 | <input checked="" type="radio"/> Read Only | <input type="radio"/> Read / Write |
| <input type="checkbox"/> 1.3.6.1.2.1.2 | <input checked="" type="radio"/> Read Only | <input type="radio"/> Read / Write |
| <input type="checkbox"/> 1.3.6.1.2.1.3 | <input checked="" type="radio"/> Read Only | <input type="radio"/> Read / Write |
| <input type="checkbox"/> 1.3.6.1.2.1.4 | <input checked="" type="radio"/> Read Only | <input type="radio"/> Read / Write |
| <input type="checkbox"/> 1.3.6.1.2.1.5 | <input checked="" type="radio"/> Read Only | <input type="radio"/> Read / Write |
| <input type="checkbox"/> 1.3.6.1.2.1.6 | <input checked="" type="radio"/> Read Only | <input type="radio"/> Read / Write |
| <input type="checkbox"/> 1.3.6.1.2.1.7 | <input checked="" type="radio"/> Read Only | <input type="radio"/> Read / Write |
| <input type="checkbox"/> 1.3.6.1.2.1.8 | <input checked="" type="radio"/> Read Only | <input type="radio"/> Read / Write |
| <input type="checkbox"/> 1.3.6.1.2.1.10 | <input checked="" type="radio"/> Read Only | <input type="radio"/> Read / Write |
| <input type="checkbox"/> 1.3.6.1.2.1.11 | <input checked="" type="radio"/> Read Only | <input type="radio"/> Read / Write |
| <input type="checkbox"/> 1.3.6.1.2.1.31 | <input checked="" type="radio"/> Read Only | <input type="radio"/> Read / Write |
| <input type="checkbox"/> 1.3.6.1.2.1.47 | <input checked="" type="radio"/> Read Only | <input type="radio"/> Read / Write |
| <input type="checkbox"/> 1.3.6.1.2.1.48 | <input checked="" type="radio"/> Read Only | <input type="radio"/> Read / Write |
| <input type="checkbox"/> 1.3.6.1.2.1.49 | <input checked="" type="radio"/> Read Only | <input type="radio"/> Read / Write |
| <input type="checkbox"/> 1.3.6.1.2.1.50 | <input checked="" type="radio"/> Read Only | <input type="radio"/> Read / Write |
| <input type="checkbox"/> 1.3.6.1.2.1.88 | <input checked="" type="radio"/> Read Only | <input type="radio"/> Read / Write |
| <input type="checkbox"/> 1.3.6.1.4.1 | <input checked="" type="radio"/> Read Only | <input type="radio"/> Read / Write |
| <input type="checkbox"/> 1.3.6.1.6.3 | <input checked="" type="radio"/> Read Only | <input type="radio"/> Read / Write |

Paso 2. Introduzca el nombre del grupo en el campo *Group Name*.

SNMP

SNMPv3 Group Management

Group Name:

Group1

Security Level:

No Authentication, No Privacy

No Authentication, No Privacy

Authentication, No Privacy

Authentication, Privacy

MIBs

1

1.3.6.1.2.1

Read Only

Read / Write

1.3.6.1.2.1.1

Read Only

Read / Write

1.3.6.1.2.1.2

Read Only

Read / Write

1.3.6.1.2.1.3

Read Only

Read / Write

1.3.6.1.2.1.4

Read Only

Read / Write

1.3.6.1.2.1.5

Read Only

Read / Write

1.3.6.1.2.1.6

Read Only

Read / Write

1.3.6.1.2.1.7

Read Only

Read / Write

1.3.6.1.2.1.8

Read Only

Read / Write

1.3.6.1.2.1.10

Read Only

Read / Write

1.3.6.1.2.1.11

Read Only

Read / Write

1.3.6.1.2.1.31

Read Only

Read / Write

1.3.6.1.2.1.47

Read Only

Read / Write

1.3.6.1.2.1.48

Read Only

Read / Write

1.3.6.1.2.1.49

Read Only

Read / Write

1.3.6.1.2.1.50

Read Only

Read / Write

1.3.6.1.2.1.88

Read Only

Read / Write

1.3.6.1.4.1

Read Only

Read / Write

1.3.6.1.6.3

Read Only

Read / Write

Paso 3. Elija el tipo de seguridad en la lista desplegable *Nivel de seguridad*. Los tipos de seguridad se describen de la siguiente manera:

- Sin autenticación, Sin privacidad: los usuarios de este grupo no tendrán que establecer una contraseña de autenticación ni establecer una contraseña de privacidad. Los mensajes no se cifrarán y los usuarios no se autenticarán

Autenticación ; Sin privacidad: los usuarios deberán establecer una contraseña de autenticación, pero no una contraseña de privacidad. Los usuarios se autenticarán cuando se reciban mensajes, pero los mensajes no se cifrarán.

Privacidad de autenticación de : los usuarios deberán establecer una contraseña de autenticación y una contraseña de privacidad. Los usuarios se autenticarán cuando se reciban mensajes. Los mensajes también se cifrarán mediante la contraseña de privacidad.

SNMP

SNMPv3 Group Management

Group Name:

Security Level: ▼

MIBs

<input type="checkbox"/> 1	<input checked="" type="radio"/> Read Only	<input type="radio"/> Read / Write
<input checked="" type="checkbox"/> 1.3.6.1.2.1	<input type="radio"/> Read Only	<input checked="" type="radio"/> Read / Write
<input checked="" type="checkbox"/> 1.3.6.1.2.1.1	<input checked="" type="radio"/> Read Only	<input type="radio"/> Read / Write
<input type="checkbox"/> 1.3.6.1.2.1.2	<input checked="" type="radio"/> Read Only	<input type="radio"/> Read / Write
<input type="checkbox"/> 1.3.6.1.2.1.3	<input checked="" type="radio"/> Read Only	<input type="radio"/> Read / Write
<input checked="" type="checkbox"/> 1.3.6.1.2.1.4	<input type="radio"/> Read Only	<input checked="" type="radio"/> Read / Write
<input checked="" type="checkbox"/> 1.3.6.1.2.1.5	<input checked="" type="radio"/> Read Only	<input type="radio"/> Read / Write
<input checked="" type="checkbox"/> 1.3.6.1.2.1.6	<input type="radio"/> Read Only	<input checked="" type="radio"/> Read / Write
<input type="checkbox"/> 1.3.6.1.2.1.7	<input checked="" type="radio"/> Read Only	<input type="radio"/> Read / Write
<input type="checkbox"/> 1.3.6.1.2.1.8	<input checked="" type="radio"/> Read Only	<input type="radio"/> Read / Write
<input type="checkbox"/> 1.3.6.1.2.1.10	<input checked="" type="radio"/> Read Only	<input type="radio"/> Read / Write
<input type="checkbox"/> 1.3.6.1.2.1.11	<input checked="" type="radio"/> Read Only	<input type="radio"/> Read / Write
<input type="checkbox"/> 1.3.6.1.2.1.31	<input checked="" type="radio"/> Read Only	<input type="radio"/> Read / Write
<input type="checkbox"/> 1.3.6.1.2.1.47	<input checked="" type="radio"/> Read Only	<input type="radio"/> Read / Write
<input type="checkbox"/> 1.3.6.1.2.1.48	<input checked="" type="radio"/> Read Only	<input type="radio"/> Read / Write
<input type="checkbox"/> 1.3.6.1.2.1.49	<input checked="" type="radio"/> Read Only	<input type="radio"/> Read / Write
<input type="checkbox"/> 1.3.6.1.2.1.50	<input checked="" type="radio"/> Read Only	<input type="radio"/> Read / Write
<input type="checkbox"/> 1.3.6.1.2.1.88	<input checked="" type="radio"/> Read Only	<input type="radio"/> Read / Write
<input type="checkbox"/> 1.3.6.1.4.1	<input checked="" type="radio"/> Read Only	<input type="radio"/> Read / Write
<input type="checkbox"/> 1.3.6.1.6.3	<input checked="" type="radio"/> Read Only	<input type="radio"/> Read / Write

Paso 4. Active las casillas de verificación para seleccionar la Base de información de administración (MIB) específica a la que desea que el grupo tenga acceso. Las MIB se utilizan para definir la información necesaria del sistema administrado. Se representa como iso.org.dod.internet.mgmt.mib. Al establecer MIB específicas, puede permitir que los grupos tengan acceso a diferentes partes del dispositivo.

Paso 5. Haga clic en el botón de opción específico para cada MIB verificada para elegir el nivel de permiso disponible para el grupo. Los niveles de permisos se definen de la siguiente manera:

- de sólo lectura: los usuarios de este grupo podrán leer de la MIB, pero no modificarla.
- Lectura/Escritura: los usuarios de este grupo podrán leer la MIB y modificarla.

Paso 6. Desplácese hacia abajo y haga clic en **Guardar** para guardar los parámetros. Esto agrega el grupo a la tabla de grupo.

The screenshot shows the SNMP configuration page. Under 'SNMP Global Settings', there are input fields for System Name (System_1), System Contact (Admin_1), System Location (Location_1), and Trap Community Name (public). Below these are checkboxes for 'Enable SNMPv1v2c' (unchecked) and 'Enable SNMPv3' (checked). The 'Group Table' section contains a table with one group, 'Group1', which is selected with a radio button. The group has a security level of 'Authentication,Privacy' and access to five MIBs: 1.3.6.1.2.1[W], 1.3.6.1.2.1.1[R], 1.3.6.1.2.1.4[W], 1.3.6.1.2.1.5[R], and 1.3.6.1.2.1.6[W]. Below the table are 'Add', 'Edit', and 'Delete' buttons, with 'Edit' circled in red. The 'User Table' section shows '0 results found!' and also has 'Add', 'Edit', and 'Delete' buttons. At the bottom, there are fields for 'SNMPv3 Trap Receiver IP Address' (empty) and 'SNMPv3 Trap Receiver User' (set to 'No User').

Paso 7. (Opcional) Si desea cambiar el grupo configurado, haga clic en el botón de opción del grupo deseado y, a continuación, haga clic en **Editar** y cambie los campos respectivos.

Paso 8. (Opcional) Si desea eliminar el grupo configurado, haga clic en el botón de opción deseado del grupo y, a continuación, haga clic en **Eliminar**.

Administración de usuarios SNMPv3

Los usuarios SNMP son los usuarios remotos para los que se ejecutan los servicios SNMP.

Nota: Debe agregar un grupo a la tabla de grupos para poder agregar un usuario a la tabla de usuarios.

SNMP

SNMP Global Settings

System Name:

System Contact:

System Location:

Trap Community Name:

Enable SNMPv1/v2c

Enable SNMPv3

Group Table

	Group Name	Security	Access MIBs
<input type="radio"/>	Group1	Authentication,Privacy	1.3.6.1.2.1[W] 1.3.6.1.2.1.1[R] 1.3.6.1.2.1.4[W] 1.3.6.1.2.1.5[R] 1.3.6.1.2.1.6[W]

User Table

	Enable	User Name	Authentication	Privacy
0 results found!				

SNMPv3 Trap Receiver IP Address: (For IPv4)

SNMPv3 Trap Receiver User:

Paso 1. Haga clic en **Agregar** desde la tabla de usuario para agregar un nuevo usuario en la tabla de administración de usuarios SNMPv3. Se abre la página *Administración de usuarios SNMPv3*:

SNMP

SNMPv3 User Management

Enable :

User Name:

Group:

Authentication Method: MD5 SHA None Authentication Password:

Privacy Method: DES AES None Privacy Password:

Paso 2. Marque **Enable** para habilitar la administración del usuario para SNMP.

Paso 3. Introduzca un nombre de usuario en el campo *User Name*.

Paso 4. Elija el grupo deseado de la lista *desplegable Grupo*. El nuevo usuario se agrega a este grupo específico.

Paso 5. Haga clic en el botón de opción específico para elegir un método de autenticación. Los métodos de autenticación se describen de la siguiente manera:

- MD5: Message Digest Algorithm-5 (MD5) es una función hash hexadecimal de 32 dígitos.
- SHA: el algoritmo hash seguro (SHA) es una función hash de 160 bits considerada más segura que MD5.

Paso 6. Ingrese una contraseña para la autenticación en el campo *Authentication Password*. La contraseña de autenticación es la contraseña que se comparte de antemano entre los dispositivos. Cuando intercambian tráfico, utilizan la contraseña específica para autenticar el tráfico.

Paso 7. Haga clic en el botón de opción específico para elegir el método de cifrado deseado en el campo *Método de privacidad*.

- DES: el estándar de cifrado de datos (DES) es un método de encriptación de 56 bits. Se considera inseguro, pero puede ser necesario cuando el dispositivo se utiliza junto con otros dispositivos que no admiten AES.
- AES: el estándar de cifrado avanzado (AES) utiliza un método de encriptación de 128 bits, 192 bits o 256 bits. Se considera más seguro que DES.

Paso 8. Introduzca una contraseña para la privacidad en el campo *Privacy Password*. La contraseña de privacidad es la contraseña que se utiliza para cifrar mensajes.

Paso 9. Haga clic en **Guardar para guardar la configuración**. Esto agrega el usuario a la tabla de usuario.

Enable SNMPv3

Group Table			
	Group Name	Security	Access MIBs
<input type="radio"/>	Group1	Authentication,Privacy	1.3.6.1.2.1[W] 1.3.6.1.2.1.1[R] 1.3.6.1.2.1.4[W] 1.3.6.1.2.1.5[R] 1.3.6.1.2.1.6[W]

User Table					
	Enable	User Name	Authentication	Privacy	Group
<input type="radio"/>	<input checked="" type="checkbox"/>	USER1	SHA	AES	Group1

SNMPv3 Trap Receiver IP Address: (For IPv4)

SNMPv3 Trap Receiver User:

Enable SNMPv3

Group Table			
Group Name	Security	Access MIBs	
<input type="radio"/> Group1	Authentication,Privacy	1.3.6.1.2.1[W] 1.3.6.1.2.1.1[R] 1.3.6.1.2.1.4[W] 1.3.6.1.2.1.5[R] 1.3.6.1.2.1.6[W]	

Add Edit Delete

User Table				
Enable	User Name	Authentication	Privacy	Group
<input checked="" type="radio"/>	USER1	SHA	AES	Group1

Add Edit Delete

SNMPv3 Trap Receiver IP Address: (For IPv4)

SNMPv3 Trap Receiver User:

Save Cancel

Paso 10. (Opcional) Si desea cambiar el usuario configurado, haga clic en el botón de opción del usuario deseado y, a continuación, haga clic en **Editar** y cambie el campo correspondiente.

Paso 11. (Opcional) Si desea eliminar el usuario configurado, haga clic en el botón de opción del usuario deseado y, a continuación, haga clic en **Eliminar**.

Enable SNMPv1v2c

Get Community Name:

Set Community Name:

SNMPv1v2c Trap Receiver IP Address: (For IPv4)

Enable SNMPv3

Group Table			
Group Name	Security	Access MIBs	
<input type="radio"/> Group1	Authentication,Privacy	1.3.6.1.2.1[W] 1.3.6.1.2.1.1[R] 1.3.6.1.2.1.4[W] 1.3.6.1.2.1.5[R] 1.3.6.1.2.1.6[W]	

Add Edit Delete

User Table					
Enable	User Name	Authentication	Privacy	Group	
<input type="radio"/>	<input checked="" type="checkbox"/>	USER1	SHA	AES	Group1

Add Edit Delete

SNMPv3 Trap Receiver IP Address: (For IPv4)

SNMPv3 Trap Receiver User:

Save Cancel

Paso 12. Ingrese la dirección IP del receptor de trampas SNMPv3 en el campo *Dirección IP del receptor de trampas SNMPv3*.

Paso 13. Elija el usuario de trampa respectivo de la lista desplegable *SNMPv3 Trap Receiver User*. Este es el usuario que recibe el mensaje de trampa cuando se produce un

evento de trampa.

Paso 14. Haga clic en **Guardar para guardar la configuración.**