

Configurazione di SNMP (Simple Network Management Protocol) su router VPN RV320 e RV325

Obiettivo

Il protocollo SNMP (Simple Network Management Protocol) è un protocollo a livello di applicazione utilizzato per gestire e monitorare il traffico di rete. L'SNMP conserva tutti i record di attività di vari dispositivi nella rete per consentire all'utente di trovare rapidamente la fonte dei problemi nella rete quando necessario. Nella serie RV32x VPN Router è possibile abilitare SNMPv1/v2c, SNMPv3 o entrambi contemporaneamente per ottenere le prestazioni desiderate per la rete.

L'obiettivo di questo documento è spiegare come configurare il protocollo SNMP sulla serie RV32x VPN Router.

Dispositivo applicabile

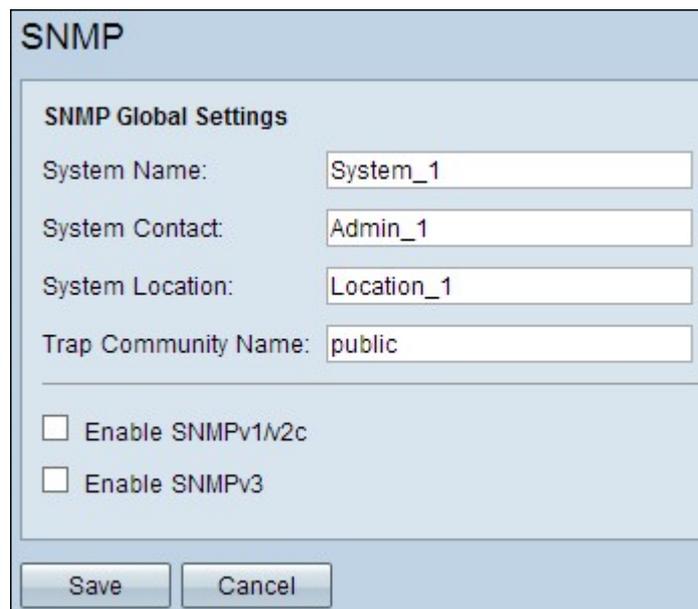
- RV320 Dual WAN VPN Router
- RV325 Gigabit Dual WAN VPN Router

Versione del software

·v1.1.0.09

Configurazione SNMP

Passaggio 1. Accedere all'utility di configurazione Web e scegliere **Gestione sistema > SNMP**. Viene visualizzata la pagina *SNMP*:



SNMP

SNMP Global Settings

System Name:

System Contact:

System Location:

Trap Community Name:

Enable SNMPv1/v2c

Enable SNMPv3

Passaggio 2. Inserire il nome dell'host nel campo *Nome sistema*.

Passaggio 3. Inserire il nome o le informazioni di contatto della persona responsabile del router nel campo *Contatto sistema*.

Passaggio 4. Immettere la posizione fisica del router nel campo *Posizione sistema*.

Nota: Le informazioni immesse nei campi *Contatto di sistema* e *Percorso di sistema* non modificano il comportamento del dispositivo. È possibile inserirli nel modo desiderato per facilitare la gestione dei dispositivi (ad esempio, potrebbe essere utile includere un numero di telefono nel campo *Contatto di sistema*).

Passaggio 5. Inserire il nome della comunità trap a cui appartiene l'agente nel campo *Nome comunità trap*. Una trap è un messaggio inviato dal dispositivo quando si verifica un evento specifico. Il nome della comunità trap può contenere un massimo di 64 caratteri alfanumerici. Il nome della comunità trap predefinita è *public*.

Passaggio 6. Fare clic su **Save** per salvare le impostazioni.

Configurazione SNMPv1/SNMPv2c

SNMPv1 è la prima versione di SNMP ed è ora considerato non sicuro. SNMPv2c è una versione migliorata di SNMP. Offre una maggiore protezione rispetto a SNMPv1 e una migliore gestione degli errori.

SNMP

SNMP Global Settings

System Name:

System Contact:

System Location:

Trap Community Name:

Enable SNMPv1/v2c

Get Community Name:

Set Community Name:

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

Enable SNMPv3

Passaggio 1. Selezionare **Enable SNMPv1/v2c** per abilitare 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

Passaggio 2. Inserire un nome di comunità nel campo *Ottieni nome comunità*. Get Community Name è la stringa della community di sola lettura per autenticare il comando SNMP Get. Il comando Get viene utilizzato per recuperare le informazioni dal dispositivo SNMP. Il nome della community Get può contenere un massimo di 64 caratteri alfanumerici. Il nome della community di recupero predefinito è *public*.

Passaggio 3. Inserire un nome di comunità nel campo *Imposta nome comunità*. È la stringa della community di lettura/scrittura per autenticare il comando SNMP Set. Il comando Set viene utilizzato per modificare o impostare le variabili sul dispositivo. Il nome della community può contenere un massimo di 64 caratteri alfanumerici. Il valore predefinito di Imposta nome comunità è *private*.

Passaggio 4. Immettere l'indirizzo IP o il nome di dominio del server specifico in cui viene eseguito il software di gestione SNMP nel campo *Indirizzo IP ricevitore trap SNMPv1/v2c*. Il server invia un messaggio trap all'amministratore per informarlo in caso di errori o errori.

Passaggio 5. Fare clic su **Save** per salvare le impostazioni.

Configurazione SNMPv3

SNMPv3 è la versione più recente di SNMP e fornisce il livello di sicurezza più elevato tra le tre versioni di SNMP. Fornisce anche la configurazione 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:

Passaggio 1. Selezionare **Enable SNMPv3** per abilitare SNMPv3.

Gestione gruppi SNMPv3

La gestione dei gruppi SNMPv3 consente di creare gruppi con diversi livelli di accesso al dispositivo. È quindi possibile mappare gli utenti in questi gruppi in base alle esigenze.

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:

Passaggio 1. Fare clic su **Add** nella tabella Group per aggiungere un nuovo gruppo nella tabella Group Management di SNMPv3. Viene visualizzata la pagina *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 |

Passaggio 2. Inserire il nome del gruppo nel campo *Nome gruppo*.

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

Passaggio 3. Scegliere il tipo di protezione dall'elenco a discesa *Livello di protezione*. I tipi di protezione sono descritti come segue:

- Nessuna autenticazione, Nessuna privacy: agli utenti di questo gruppo non verrà richiesto di impostare una password di autenticazione o una password per la privacy. I messaggi non verranno crittografati e gli utenti non verranno autenticati

·Autenticazione, nessuna privacy: agli utenti verrà richiesto di impostare una password di autenticazione, ma non una password per la privacy. Gli utenti verranno autenticati alla ricezione dei messaggi, ma i messaggi non verranno crittografati.

·Privacy dell'autenticazione: agli utenti verrà richiesto di impostare sia una password di autenticazione che una password di privacy. Gli utenti verranno autenticati alla ricezione dei messaggi. I messaggi verranno inoltre crittografati utilizzando la password per la privacy.

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

Passaggio 4. Selezionare le caselle di controllo per selezionare il database MIB (Management Information Base) specifico a cui si desidera che il gruppo abbia accesso. I MIB vengono utilizzati per definire le informazioni necessarie del sistema gestito. È rappresentato come iso.org.dod.internet.mgmt.mib. Impostando MIB specifici, è possibile consentire ai gruppi di accedere a parti diverse del dispositivo.

Passaggio 5. Fare clic sul pulsante di opzione specifico per ogni MIB selezionato per scegliere il livello di autorizzazione disponibile per il gruppo. I livelli di autorizzazione sono definiti come segue:

- Sola lettura — gli utenti di questo gruppo potranno leggere dal MIB, ma non modificarlo.
- Lettura/scrittura: gli utenti di questo gruppo potranno sia leggere dal MIB sia modificarlo.

Passaggio 6. Scorrere verso il basso e fare clic su **Save** per salvare le impostazioni. Il gruppo verrà aggiunto alla tabella dei gruppi.

The screenshot shows the SNMP configuration page. At the top, there are 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 SNMPv1/v2c' (unchecked) and 'Enable SNMPv3' (checked). The 'Group Table' section contains a table with one group, 'Group1', which is selected. The table has columns for Group Name, Security, and Access MIBs. The Security column for Group1 is 'Authentication,Privacy'. The Access MIBs column lists five MIBs with their respective access levels: 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 buttons for 'Add', 'Edit' (highlighted with a red circle), and 'Delete'. The 'User Table' section below it shows '0 results found!' and buttons for 'Add', 'Edit', and 'Delete'. At the bottom, there are fields for 'SNMPv3 Trap Receiver IP Address' (empty) and 'SNMPv3 Trap Receiver User' (set to 'No User').

Passaggio 7. (Facoltativo) Se si desidera modificare il gruppo configurato, fare clic sul pulsante di opzione del gruppo desiderato, quindi su **Modifica** e modificare i rispettivi campi.

Passaggio 8. (Facoltativo) Se si desidera eliminare il gruppo configurato, fare clic sul pulsante di opzione desiderato del gruppo e quindi su **Elimina**.

Gestione utente SNMPv3

Gli utenti SNMP sono gli utenti remoti per i quali vengono eseguiti i servizi SNMP.

Nota: prima di poter aggiungere un utente nella tabella utente, è necessario aggiungere un gruppo alla tabella gruppo.

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:

Passaggio 1. Fare clic su **Add** dalla tabella User per aggiungere un nuovo utente nella tabella User Management di SNMPv3. Viene visualizzata la pagina *Gestione utente SNMPv3*:

SNMP

SNMPv3 User Management

Enable :

User Name:

Group:

Authentication Method: MD5 SHA None Authentication Password:

Privacy Method: DES AES None Privacy Password:

Passaggio 2. Selezionare **Enable** per abilitare la gestione degli utenti per SNMP.

Passaggio 3. Inserire un nome utente nel campo *Nome utente*.

Passaggio 4. Scegliere il gruppo desiderato dall'elenco a discesa *Gruppo*. Il nuovo utente viene aggiunto a questo gruppo specifico.

Passaggio 5. Fare clic sul pulsante di opzione specifico per scegliere un metodo di autenticazione. I metodi di autenticazione sono descritti come segue:

- MD5 — Message Digest Algorithm-5 (MD5) è una funzione hash esadecimale a 32 cifre.
- SHA: Secure Hash Algorithm (SHA) è una funzione hash a 160 bit considerata più sicura di MD5.

Passaggio 6. Immettere una password per l'autenticazione nel campo *Password autenticazione*. La password di autenticazione è la password che viene condivisa in anticipo tra i dispositivi. Quando si scambiano traffico, utilizzano la password specifica per autenticare il traffico.

Passaggio 7. Fare clic sul pulsante di opzione specifico per scegliere il metodo di crittografia desiderato nel campo *Privacy Method*.

- DES: Data Encryption Standard (DES) è un metodo di crittografia a 56 bit. È considerato non sicuro, ma potrebbe essere necessario quando il dispositivo viene usato insieme ad altri dispositivi che non supportano AES.
- AES - Advanced Encryption Standard (AES) utilizza un metodo di crittografia a 128 bit, 192 bit o 256 bit. È considerato più sicuro di DES.

Passaggio 8. Immettere una password per la privacy nel campo *Password privacy*. La password per la privacy è la password utilizzata per crittografare i messaggi.

Passaggio 9. Fare clic su **Save** per salvare le impostazioni. L'utente verrà aggiunto alla tabella utente.

The screenshot shows the configuration interface for SNMPv3. At the top, there is a checkbox labeled "Enable SNMPv3" which is checked. Below this, there are two tables: "Group Table" and "User Table".

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]

Buttons: Add, Edit, Delete

User Table:

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

Buttons: Add, Edit, Delete

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

Passaggio 10. (Facoltativo) Se si desidera modificare l'utente configurato, fare clic sul pulsante di opzione dell'utente desiderato, quindi su **Modifica** e modificare il campo corrispondente.

Passaggio 11. (Facoltativo) Se si desidera eliminare l'utente configurato, fare clic sul pulsante di opzione dell'utente desiderato e quindi su **Elimina**.

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

Passaggio 12. Immettere l'indirizzo IP del ricevitore di trap SNMPv3 nel campo *Indirizzo IP del ricevitore di trap SNMPv3*.

Passaggio 13. Selezionare l'utente di trap corrispondente dall'elenco a discesa *SNMPv3 Trap Receiver User* (Utente di trap SNMPv3). Utente che riceve il messaggio di trap quando

si verifica un evento di trap.

Passaggio 14. Fare clic su **Save** per salvare le impostazioni.