Configurazione di SNMP su router RV160 e RV260

Obiettivo

L'obiettivo di questo articolo è mostrare come configurare le impostazioni SNMP (Simple Network Management Protocol) sui router RV160 e RV260.

Introduzione

Il protocollo SNMP è uno standard Internet per la raccolta e l'organizzazione di dati su dispositivi gestiti sulle reti IP. Consente agli amministratori di rete di gestire, monitorare, ricevere notifiche di eventi critici che si verificano sulla rete e risolvere i problemi.

Il quadro SNMP è costituito da tre elementi: un manager SNMP, un agente SNMP e un MIB (Management Information Base). La funzione di SNMP Manager è quella di controllare e monitorare le attività degli host di rete che utilizzano SNMP. L'agente SNMP è incluso nel software del dispositivo e contribuisce alla manutenzione dei dati per consentire la gestione del sistema. MIB è infine un'area di storage virtuale per le informazioni sulla gestione della rete. Questi tre dispositivi si combinano per monitorare e gestire i dispositivi in una rete.

I dispositivi RV160/260 supportano le versioni SNMP v1, v2c e v3. Fungono da agenti SNMP che rispondono ai comandi SNMP dei sistemi di gestione di rete SNMP. I comandi supportati sono i comandi SNMP standard get/next/set. I dispositivi generano anche messaggi trap per notificare al manager SNMP quando si verificano condizioni di allarme. ad esempio riavvii, cicli di alimentazione ed eventi di collegamento alla WAN.

Dispositivi interessati

- RV160
- RV260

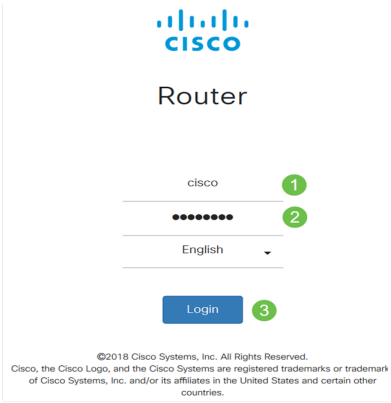
Versione del software

- 1.0.00.13

Configurazione di SNMP

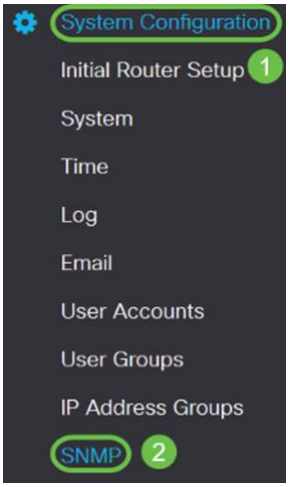
Per configurare il protocollo SNMP del router, attenersi alla seguente procedura.

Passaggio 1. Accedere alla pagina di configurazione Web del router.



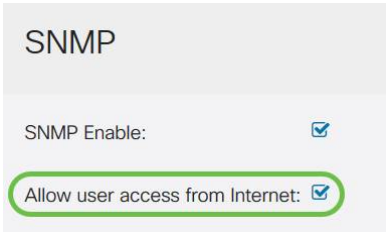
Nota: In questo articolo, utilizzeremo l'RV260W per configurare il protocollo SNMP. La configurazione può variare a seconda del modello in uso.

Passaggio 2. Passare a **Configurazione di sistema > SNMP**.



Passaggio 3. Selezionare la casella di controllo **SNMP Enable** per abilitare il protocollo SNMP.

Passaggio 4. (Facoltativo) Selezionare la casella di controllo **Consenti accesso utente da Internet** per consentire agli utenti autorizzati all'esterno della rete tramite applicazioni di gestione come Cisco FindIT Network Management.

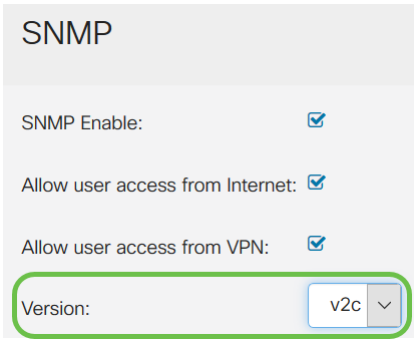


Passaggio 5. (Facoltativo) Selezionare la casella di controllo **Consenti accesso utente da VPN** per consentire l'accesso autorizzato da una rete privata virtuale (VPN).

Passaggio 6. Dal menu a discesa *Versione*, scegliere una versione SNMP da utilizzare sulla rete. Le opzioni sono:

- v1 - Opzione meno sicura. Utilizza testo normale per le stringhe della community.
- v2c - Il supporto migliorato per la gestione degli errori fornito da SNMPv2c include codici di errore estesi che distinguono i diversi tipi di errore; tutti i tipi di errori vengono segnalati tramite un singolo codice di errore in SNMPv1.
- v3 - SNMPv3 fornisce accesso sicuro ai dispositivi tramite l'autenticazione e la crittografia dei pacchetti di dati sulla rete. Gli algoritmi di autenticazione includono MD5 (Message Digest Algorithm) e SHA (Secure Hash Algorithm). I metodi di crittografia includono DES (Data Encryption Standard) e AES (Advanced Encryption Standard).

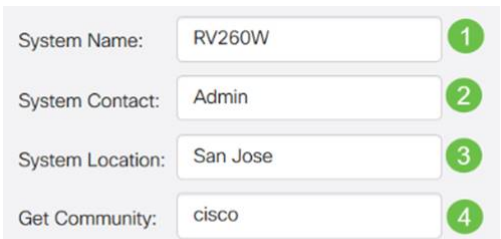
Per ulteriori informazioni su SNMPv3, fare clic qui.



In questo esempio, **v2c** è stato selezionato come *Versione*.

Passaggio 7. Inserire i seguenti campi

- **Nome sistema**: immettere un nome per il router per semplificarne l'identificazione nelle applicazioni di gestione della rete.
- **Contatto di sistema**: immettere il nome di un utente o di un amministratore da identificare con il router in caso di emergenza.
- **Percorso di sistema**: immettere il percorso del router. In questo modo l'individuazione di un problema risulta molto più semplice per l'amministratore.
- **Get Community** - Immettere il nome della community SNMP nel campo *Get Community*. Crea una community di sola lettura che viene utilizzata per accedere e recuperare le informazioni per l'agente SNMP.
- **Set Community** - Nel campo *Set Community*, immettere un nome di community SNMP. Crea una community di lettura/scrittura utilizzata per accedere e modificare le informazioni per l'agente SNMP. Vengono accettate solo le richieste dei dispositivi che si identificano con questo nome community. Nome creato dall'utente. Il valore predefinito è private.



Configurazione trap

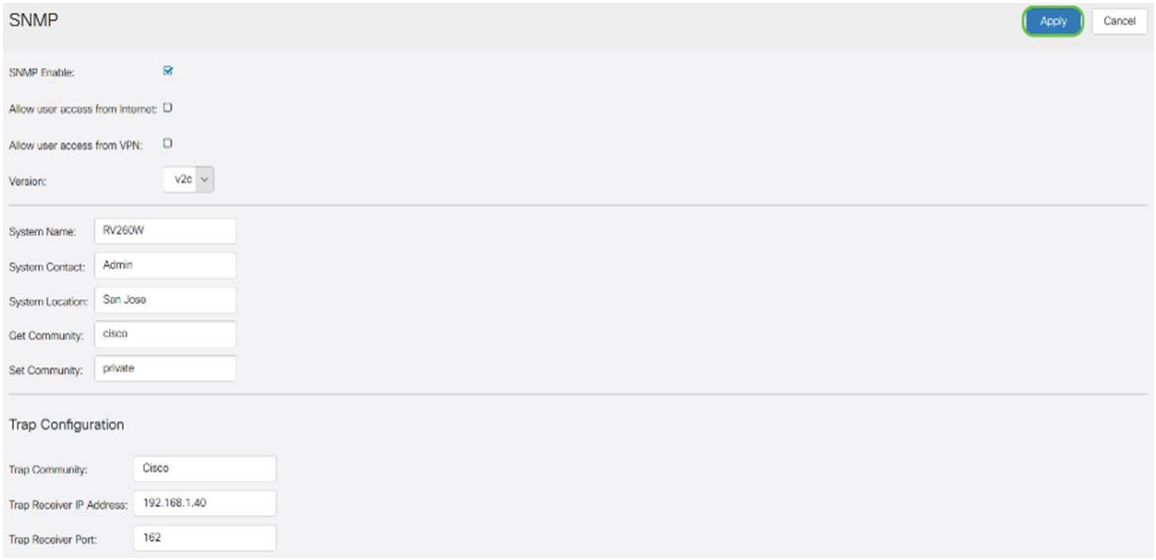
Utilizzando le configurazioni Trap, è possibile impostare l'indirizzo di origine di ogni pacchetto trap SNMP inviato dal router su un singolo indirizzo, indipendentemente dall'interfaccia in uscita.

Passaggio 8. Per configurare la trap SNMP, immettere le informazioni seguenti.

Trap Community	Immettere il nome della comunità trap
Indirizzo IP ricevitore trap	Immettere l'indirizzo IP
Porta del ricevitore Trap	Immettere il numero di porta

Nota: In genere, SNMP utilizza il protocollo UDP (User Datagram Protocol) come protocollo di trasporto e le porte UDP predefinite per il traffico SNMP sono 161 (SNMP) e 162 (SNMP Trap).

Passaggio 9. Fare clic su **Applica**.



A questo punto, è necessario aver abilitato e configurato correttamente il protocollo SNMP sul router RV160/RV260.