Configuration du protocole SNMP sur les routeurs RV160 et RV260

Objectif

L'objectif de cet article est de vous montrer comment configurer les paramètres SNMP (Simple Network Management Protocol) sur les routeurs RV160 et RV260.

Introduction

SNMP est un protocole standard Internet permettant de collecter et d'organiser des données sur les périphériques gérés sur les réseaux IP. Elle permet aux administrateurs réseau de gérer, surveiller, recevoir des notifications d'événements critiques lorsqu'ils se produisent sur le réseau et de résoudre les problèmes.

Le cadre SNMP se compose de trois éléments ; un gestionnaire SNMP, un agent SNMP et une base MIB (Management Information Base). Le gestionnaire SNMP a pour fonction de contrôler et de surveiller les activités des hôtes réseau qui utilisent SNMP. L'agent SNMP se trouve dans le logiciel du périphérique et facilite la maintenance des données afin de gérer le système. Enfin, MIB est une zone de stockage virtuelle pour les informations de gestion de réseau. Ces trois fonctions permettent de surveiller et de gérer les périphériques d'un réseau.

Les périphériques RV160/260 prennent en charge les versions SNMP v1, v2c et v3. Ils agissent en tant qu'agents SNMP qui répondent aux commandes SNMP des systèmes de gestion de réseau SNMP. Les commandes prises en charge sont les commandes SNMP standard get/next/set. Les périphériques génèrent également des messages de déroutement pour avertir le gestionnaire SNMP en cas d'alarme. Par exemple, les redémarrages, les cycles d'alimentation et les événements de liaison WAN.

Périphériques pertinents

- RV160
- RV260

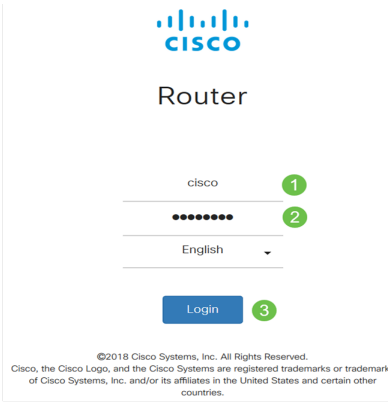
Version du logiciel

- 1.0.00.13

Configurer SNMP

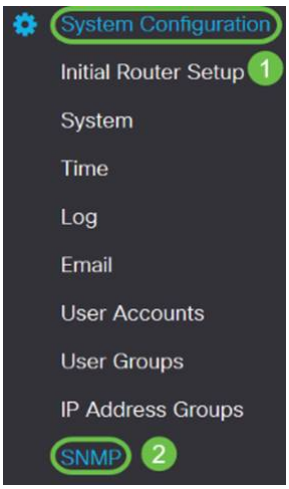
Pour configurer le protocole SNMP du routeur, procédez comme suit.

Étape 1. Connectez-vous à la page de configuration Web de votre routeur.



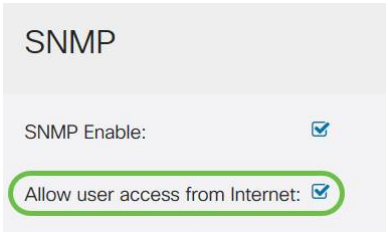
Note: Dans cet article, nous allons utiliser le RV260W pour configurer SNMP. La configuration peut varier en fonction du modèle que vous utilisez.

Étape 2. Accédez à **Configuration du système > SNMP**.



Étape 3. Cochez la case **SNMP Enable** pour activer SNMP.

Étape 4. (Facultatif) Cochez la case **Autoriser l'accès utilisateur à partir d'Internet** pour autoriser l'accès utilisateur autorisé en dehors du réseau via des applications de gestion telles que Cisco FindIT Network Management.

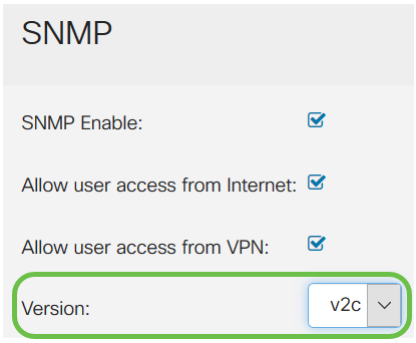


Étape 5. (Facultatif) Cochez la case **Autoriser l'accès utilisateur à partir du VPN** pour autoriser l'accès autorisé à partir d'un réseau privé virtuel (VPN).

Étape 6. Dans le menu déroulant *Version*, sélectionnez une version SNMP à utiliser sur le réseau. Les options sont les suivantes :

- v1 - Option la moins sécurisée. Utilise du texte clair pour les chaînes de communauté.
- v2c - La prise en charge améliorée de la gestion des erreurs fournie par SNMPv2c inclut des codes d'erreur étendus qui distinguent différents types d'erreurs ; tous les types d'erreurs sont signalés via un code d'erreur unique dans SNMPv1.
- v3 - SNMPv3 fournit un accès sécurisé aux périphériques en authentifiant et en cryptant les paquets de données sur le réseau. Les algorithmes d'authentification incluent l'algorithme MD5 (Message Digest Algorithm) et l'algorithme SHA (Secure Hash Algorithm). Les méthodes de cryptage incluent les normes DE (Data Encryption Standard) et AES (Advanced Encryption Standard).

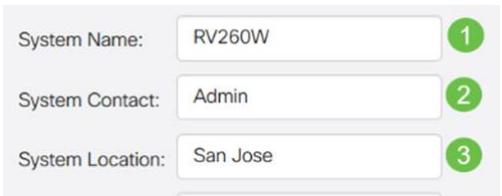
Pour plus d'informations sur SNMPv3, cliquez ici.



Dans cet exemple, **v2c** a été sélectionné comme *Version*.

Étape 7. Saisissez les champs suivants :

- **Nom du système** - Entrez un nom pour le routeur afin de faciliter l'identification dans les applications de gestion de réseau.
- **Contact système** : saisissez le nom d'une personne ou d'un administrateur à identifier au routeur en cas d'urgence.
- **Emplacement du système** : saisissez l'emplacement du routeur. Cela facilite la recherche d'un problème pour un administrateur.
- **Get Community** - Entrez le nom de la communauté SNMP dans le champ *Get Community*. Il crée une communauté en lecture seule qui est utilisée pour accéder aux informations de l'agent SNMP et les récupérer.
- **Set Community** - Dans le champ *Set Community*, saisissez un nom de communauté SNMP. Il crée une communauté en lecture-écriture qui est utilisée pour accéder aux informations de l'agent SNMP et les modifier. Seules les demandes des périphériques qui s'identifient avec ce nom de communauté sont acceptées. Il s'agit d'un nom créé par l'utilisateur. La valeur par défaut est private.



Configuration du déroutement

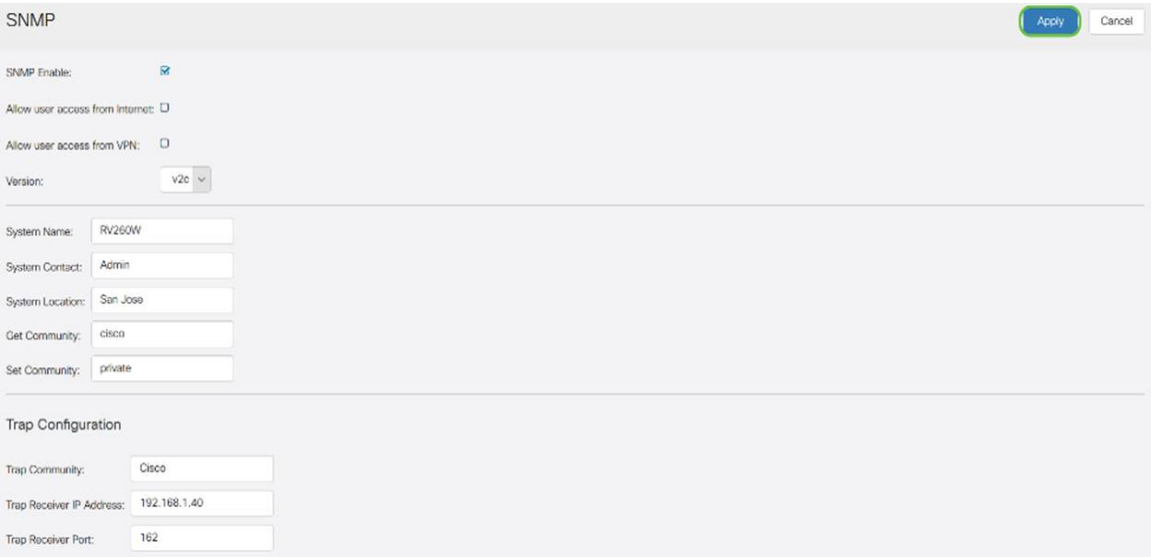
Àl'aide des configurations de déroutement, vous pouvez définir l'adresse source de chaque paquet de déroutement SNMP envoyé par le routeur sur une seule adresse, quelle que soit l'interface sortante.

Étape 8. Pour configurer le déroutement SNMP, saisissez les informations suivantes.

Communauté de déroutement	Entrez le nom de la communauté de déroutement
Adresse IP du récepteur de déroutement	Saisissez l'adresse IP.
Port récepteur de déroutement	Entrez le numéro de port

Note: En règle générale, SNMP utilise le protocole UDP (User Datagram Protocol) comme protocole de transport et les ports UDP par défaut pour le trafic SNMP sont 161 (SNMP) et 162 (SNMP Trap).

Étape 9. Cliquez sur Apply.



Vous devez maintenant avoir activé et configuré SNMP sur votre routeur RV160/RV260.