Configurando SNMP em roteadores RV160 e RV260

Objetivo

O objetivo deste artigo é mostrar a você como configurar as configurações do Protocolo de Gerenciamento de Rede Simples (SNMP - Simple Network Management Protocol) nos roteadores RV160 e RV260.

Introduction

O SNMP é um protocolo padrão da Internet para coletar e organizar dados em dispositivos gerenciados nas redes IP. Ele permite que os administradores de rede gerenciem, monitorem, recebam notificações de eventos críticos à medida que eles ocorrem na rede e solucionem problemas.

A estrutura SNMP consiste em três elementos; um gerenciador SNMP, um agente SNMP e uma Base de Informações de Gerenciamento (MIB - Management Information Base). A função do gerenciador SNMP é controlar e monitorar as atividades dos hosts de rede que utilizam SNMP. O agente SNMP está dentro do software do dispositivo e auxilia na manutenção de dados para gerenciar o sistema. Por fim, a MIB é uma área de armazenamento virtual para informações de gerenciamento de rede. Esses três se combinam para monitorar e gerenciar os dispositivos em uma rede.

Os dispositivos RV160/260 suportam SNMP versão v1, v2c e v3. Eles atuam como agentes SNMP que respondem aos comandos SNMP dos sistemas de gerenciamento de rede SNMP. Os comandos suportados são os comandos SNMP padrão get/next/set. Os dispositivos também geram mensagens de interceptação (trapping) para notificar o gerenciador SNMP quando ocorrem condições de alarme. Os exemplos incluem reinicializações, ciclos de energia e eventos de enlace de WAN.

Dispositivos aplicáveis

- RV160
- RV260

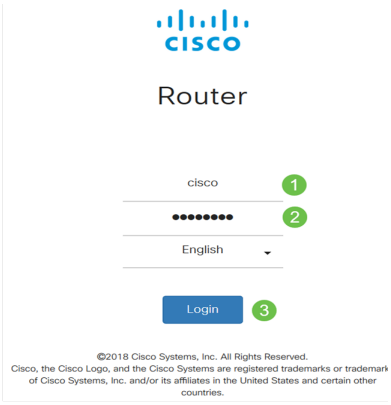
Versão de software

- 1.0.00.13

Configurar SNMP

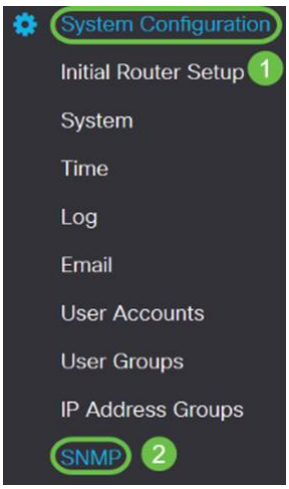
Para configurar o SNMP do roteador, execute as seguintes etapas.

Etapa 1. Faça login na página de configuração da Web do roteador.



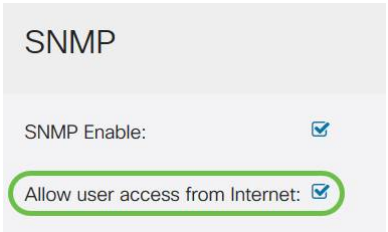
Note: Neste artigo, usaremos o RV260W para configurar o SNMP. A configuração pode variar dependendo do modelo que você está usando.

Etapa 2. Navegue até **Configuração do sistema > SNMP**.



Etapa 3. Marque a caixa de seleção **SNMP Enable** para habilitar o SNMP.

Etapa 4. (Opcional) Marque a caixa de seleção **Permitir acesso de usuário da Internet** para permitir acesso de usuário autorizado fora da rede por meio de aplicativos de gerenciamento, como o Cisco FindIT Network Management.

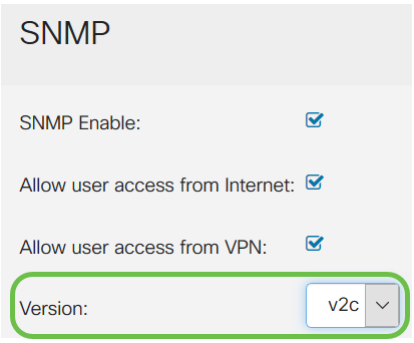


Etapa 5. (Opcional) Marque a caixa de seleção **Permitir acesso de usuário da VPN** para permitir acesso autorizado de uma VPN (Virtual Private Network).

Etapa 6. No menu suspenso *Version*, escolha uma versão SNMP para usar na rede. As opções são:

- v1 - opção menos segura. Usa texto simples para community strings.
- v2c - o melhor suporte para tratamento de erros fornecido pelo SNMPv2c inclui códigos de erro expandidos que distinguem diferentes tipos de erros; todos os tipos de erros são relatados por meio de um único código de erro em SNMPv1.
- v3 - O SNMPv3 fornece acesso seguro a dispositivos autenticando e criptografando pacotes de dados pela rede. Os algoritmos de autenticação incluem o algoritmo de resumo de mensagens (MD5 - Message digest Algorithm) e o algoritmo de hash seguro (SHA - Secure Hash Algorithm). Os métodos de criptografia incluem o Data Encryption Standard (DES) e o Advanced Encryption Standard (AES).

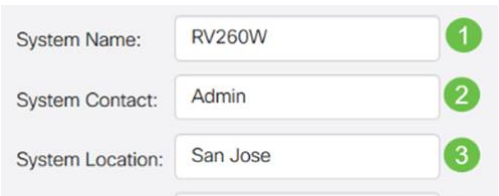
Para obter mais informações sobre SNMPv3, clique aqui.



Neste exemplo, **v2c** foi selecionado como a *Versão*.

Passo 7. Insira os seguintes campos

- **System Name** - (Nome do sistema) Insira um nome para o roteador para facilitar a identificação em aplicativos de gerenciamento de rede.
- **System Contact** - (Contato com o sistema) Insira o nome de um indivíduo ou administrador para se identificar com o roteador em caso de emergência.
- **System Location** - (Local do Sistema) Insira o local do roteador. Isso torna a localização de um problema muito mais fácil para um administrador.
- **Get Community** - Insira o nome da comunidade SNMP no campo *Get Community*. Cria uma comunidade somente leitura que é usada para acessar e recuperar as informações do agente SNMP.
- **Set Community** - No campo *Set Community*, insira um nome de comunidade SNMP. Ele cria uma comunidade de leitura e gravação que é usada para acessar e modificar as informações do agente SNMP. Somente as solicitações dos dispositivos que se identificam com esse nome de comunidade são aceitas. Este é um nome criado pelo usuário. O padrão é privado.



Configuração de armadilha

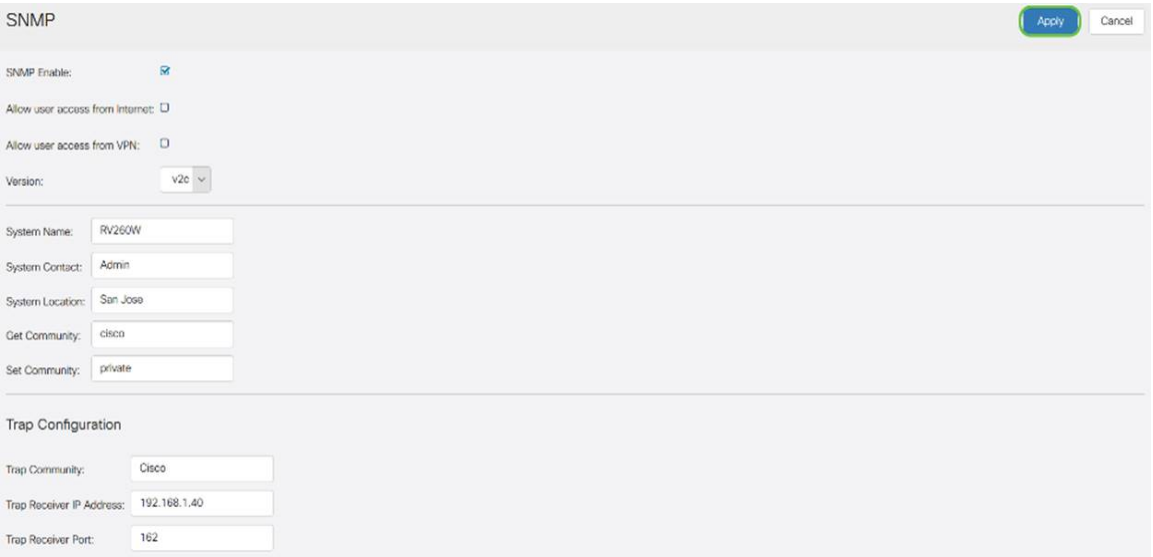
Usando as configurações Trap, você pode definir o endereço de origem de cada pacote de trap SNMP enviado pelo roteador para um único endereço, independentemente da interface de saída.

Etapa 8. Para configurar a armadilha SNMP, insira as seguintes informações.

comunidade trap	Insira o nome da comunidade de armadilhas
Endereço IP do receptor de interceptação	Insira o endereço IP
Porta do receptor de interceptação	Insira o número da porta

Note: Geralmente, o SNMP usa UDP (User Datagram Protocol) como protocolo de transporte e as portas UDP padrão para tráfego SNMP são 161 (SNMP) e 162 (SNMP Trap).

Etapa 9. Clique em Apply.



Agora você deve ter habilitado e configurado o SNMP com êxito no roteador RV160/RV260.