

# 在RV34x系列路由器上配置简单网络管理协议(SNMP)设置

## 目标

简单网络管理协议(SNMP)用于网络管理、故障排除和维护。SNMP记录、存储和共享信息时，需要借助以下两个关键软件：在管理器设备上运行的网络管理系统(NMS)和在受管设备上运行的代理。RV34x系列路由器支持SNMP版本1、2和3。

SNMP v1是SNMP的原始版本，它缺乏某些功能，仅在TCP/IP网络上运行，而SNMP v2是v1的改进版本。SNMP v1和v2c只应选择用于使用SNMPv1或SNMPv2c的网络。SNMP v3是SNMP的最新标准，可解决SNMP v1和v2c的许多问题。特别是，它可解决v1和v2c的许多安全漏洞。SNMP v3还允许管理员迁移到一个通用SNMP标准。

本文介绍如何在RV34x系列路由器上配置SNMP设置。

## 适用设备

- RV34x系列

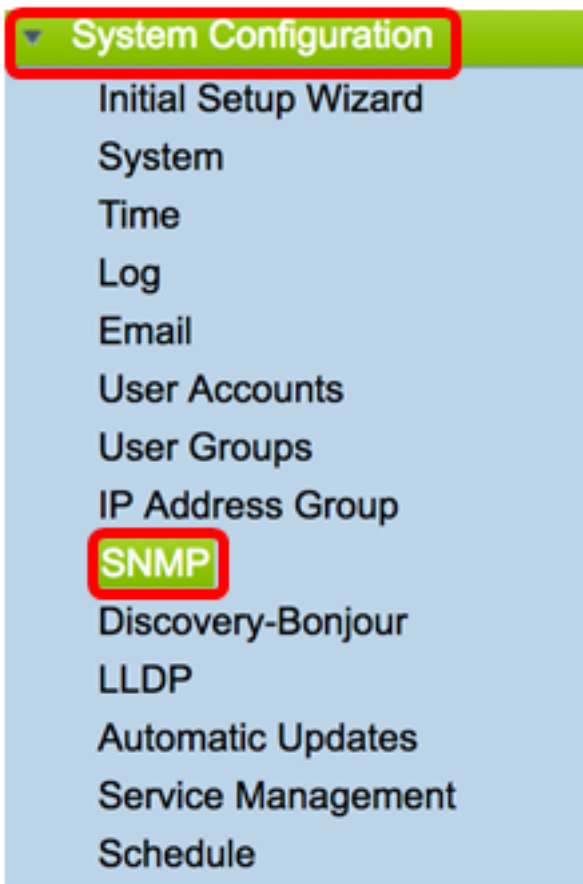
## 软件版本

- 1.0.1.16

## 在RV34x系列路由器上配置SNMP设置

### 配置SNMP设置

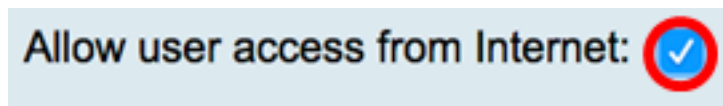
步骤1.登录到路由器的基于Web的实用程序，然后选择System Configuration > SNMP。



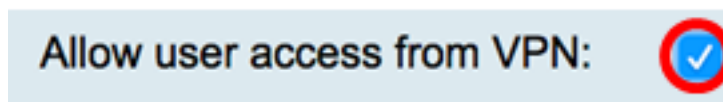
步骤2.选中SNMP Enable复选框以启用SNMP。



步骤3. ( 可选 ) 选中Enable Allow user access from Internet复选框，以允许授权用户通过Cisco FindIT Network Management等管理应用访问网络外部。



第4步。( 可选 ) 选中Allow user access from VPN(允许用户从VPN访问)复选框，以允许从VPN进行授权访问。



步骤5.从Version下拉菜单中，选择要在网络上使用的SNMP版本。选项有：

- v1 — 安全性最低的选项。对社区字符串使用明文。
- v2c - SNMPv2c提供的改进错误处理支持包括区分不同类型错误的扩展错误代码；所有类型的错误都通过SNMPv1中的一个错误代码报告。
- v3 - SNMPv3是一种安全模型，其中为用户和用户所在的组设置了身份验证策略。安全级别是安全模型中允许的安全级别。安全模型和安全级别的组合确定在处理SNMP数据包时使用的安全机制。

**注意：**在本例中，选择v2c。

Allow user access from VPN:

Version:

System Name:

A dropdown menu for selecting the SNMP version. The options are v1, v2c (which is selected with a checkmark), and v3. The entire menu is enclosed in a red rounded rectangle.

v1  
✓ v2c  
v3

步骤6.在System Name字段中，输入路由器名称，以便在网络管理应用程序中更轻松地识别。

**注意：**在本例中，ArkHives用作系统名称。

System Name:

ArkHives

步骤7.在System Contact字段中，输入在紧急情况下与路由器进行标识的个人或管理员的姓名。

**注意：**在本例中，Noah用作系统联系人。

System Contact:

Noah

步骤8.在System Location字段中，输入路由器的位置。这使管理员更容易找到问题。

**注意：**在本例中，FloodPlains用作系统位置。

System Location:

FloodPlains

要继续配置，请点击步骤5中选择的SNMP版本。

- [配置SNMP 1或v2c](#)
- [配置SNMP v3](#)

### [配置SNMP 1或v2c](#)

步骤1.如果在步骤5中选择了SNMP v2c，请在Get Community字段中输入SNMP社区名称。它创建只读社区，用于访问SNMP代理的信息。发送方发送的请求数据包中发送的社区字符串必须与代理设备上的社区字符串匹配。只读的默认字符串为public。

**注意：**只读密码授予仅检索信息的权限。在本例中，使用pblick。

Get Community:

pblick

步骤2.在Set Community字段中输入SNMP社区名称。它创建读写社区，用于访问SNMP代理的信息。仅接受来自使用此社区名称标识自己的设备的请求。这是用户创建的名称。默认为私有。

**注意：**建议将两个密码都更改为更自定义的密码，以避免外部人员的安全攻击。在本例中，使用pribado。

Set Community:

pribado

您现在应该已成功配置SNMP v1或v2设置。继续进入“[陷阱配置](#)”区域。

### [配置SNMP v3](#)

步骤1.如果选择了SNMP v3，请点击Username区域中的单选按钮以选择访问权限。选项有：

- guest — 只读权限
- admin — 读写权限

**注意：**在本例中，选择访客。

Access Privilege区域根据单击的单选按钮显示权限类型。

Username:

guest  admin

Access Privilege:

Read

步骤2.单击Authentication Algorithm区域中的单选按钮，选择SNMP代理用于进行身份验证的方法。选项有：

- 无 — 不使用用户身份验证。
- MD5 — 消息摘要算法5使用128位哈希值进行身份验证。需要用户名和密码。
- SHA1 — 安全散列算法(SHA-1)是一种单向散列算法，可生成160位摘要。SHA-1计算速度比MD5慢，但比MD5更安全。

**注意：**在本例中，选择MD5。

Authentication Algorithm:

None  MD5  SHA1

Authentication Password:

**注意：**如果选择None，请跳至Trap Configuration [区域](#)。

步骤3.在Authentication Password 字段中输入密码。

Authentication Algorithm:

None  MD5  SHA1

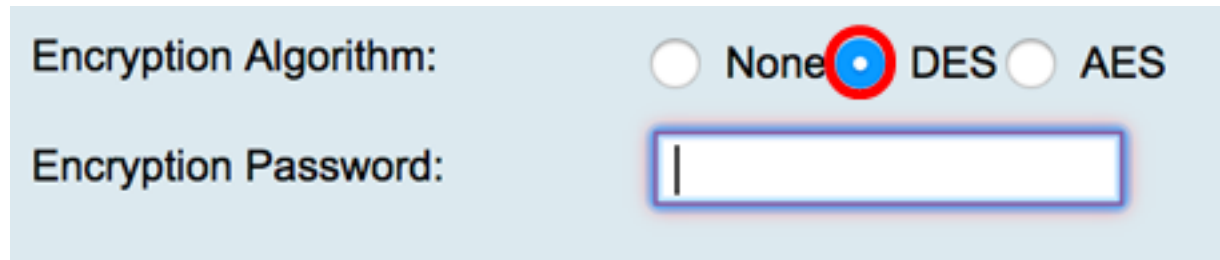
Authentication Password:

步骤4. ( 可选 ) 在Encryption Algorithm区域，点击单选按钮以选择SNMP信息的加密方式。选项有：

- 无 — 不使用加密。如果选择此步骤，请跳至“[陷阱配置](#)”区域。

- DES — 数据加密标准(DES)是一种56位加密方法，它不太安全，但可能需要向后兼容。
- AES — 高级加密标准(AES)。如果选择此选项，则需要加密密码。


**注意：**在本例中，选择DES。



Encryption Algorithm:  None  DES  AES

Encryption Password:

步骤5. ( 可选 ) 如果选择了DES或AES，请在Encryption Password字段中输入加密密码。



Encryption Algorithm:  None  DES  AES

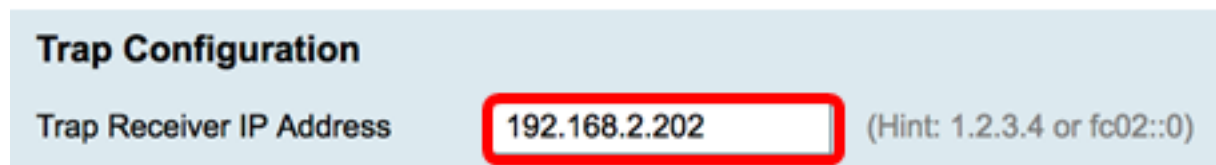
Encryption Password:

您现在应该已成功配置SNMP v3设置。现在继续到陷阱配置区。

## 陷阱配置

步骤1.在Trap Receiver IP Address 字段中，输入将接收SNMP陷阱的IPv4或IPv6 IP地址。

**注意：**在本例中，使用192.168.2.202。

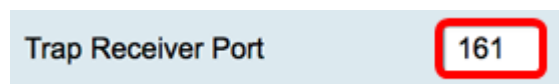


**Trap Configuration**

Trap Receiver IP Address  (Hint: 1.2.3.4 or fc02::0)

步骤2.在Trap Receiver Port字段中输入用户数据报协议(UDP)端口号。SNMP代理检查此端口的访问请求。

**注意：**在本例中，使用161。



Trap Receiver Port

步骤3.单击“应用”。

## Trap Configuration

Trap Receiver IP Address

192.168.2.100

Trap Receiver Port

161

Apply

Cancel

## SNMP



Success. To permanently save the configuration, Go to [Configuration Management](#) page or click Save icon.

SNMP Enable:



Allow user access from Internet:



Allow user access from VPN:



Version:

v3

System Name:

Ark Hives

System Contact:

Noah

System Location:

FloodPlains

Username:



guest



admin

Access Privilege:

Read

Authentication Algorithm:



None



MD5



SHA1

Authentication Password:

.....

Encryption Algorithm:



None



DES



AES

Encryption Password:

.....

### Trap Configuration

Trap Receiver IP Address

192.168.2.100

(Hint: 1.2.3.4 or fc02::0)

Trap Receiver Port

161

Apply

Cancel

步骤4. ( 可选 ) 要永久保存配置，请转至“复制/保存配置”页面，或单



击页面上部的图标。

现在，您应该已成功配置RV34x系列路由器上的SNMP设置。