

# 在RV320和RV325 VPN路由器上配置简单网络管理协议(SNMP)

## 目标

简单网络管理协议(SNMP)是一种应用层协议，用于管理和监控网络流量。SNMP会保留网络中各种设备的所有活动记录，以帮助您在需要时快速查找网络中问题的根源。在RV32x VPN路由器系列中，您可以同时启用SNMPv1/v2c、SNMPv3或两者，以获得所需的网络性能。

本文档的目的是说明如何在RV32x VPN路由器系列上配置SNMP。

## 适用设备

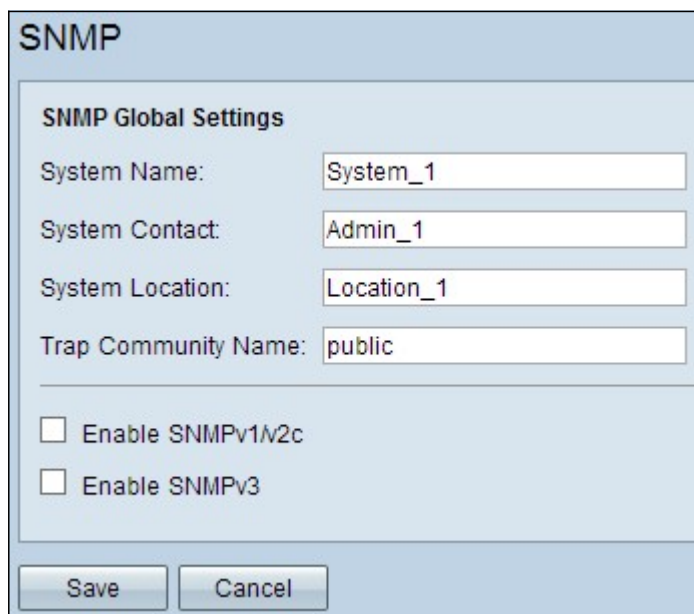
- RV320双WAN VPN路由器
- RV325千兆双WAN VPN路由器

## 软件版本

- v1.1.0.09

## SNMP配置

步骤1.登录Web配置实用程序并选择System Management > **SNMP**。SNMP页面打开：



步骤2.在System Name字段中输入主机名。

步骤3.在“系统联系人”字段中输入负责路由器的人员的姓名或联系信息。

步骤4.在System Location字段中输入路由器的物理位置。

**注意：**在“系统联系人”和“系统位置”字段中输入的信息不会修改设备的行为。您可以根据需要输入它们，以帮助最好地管理您的设备(例如，您可能认为最好在“系统联系人”字段中包含电话

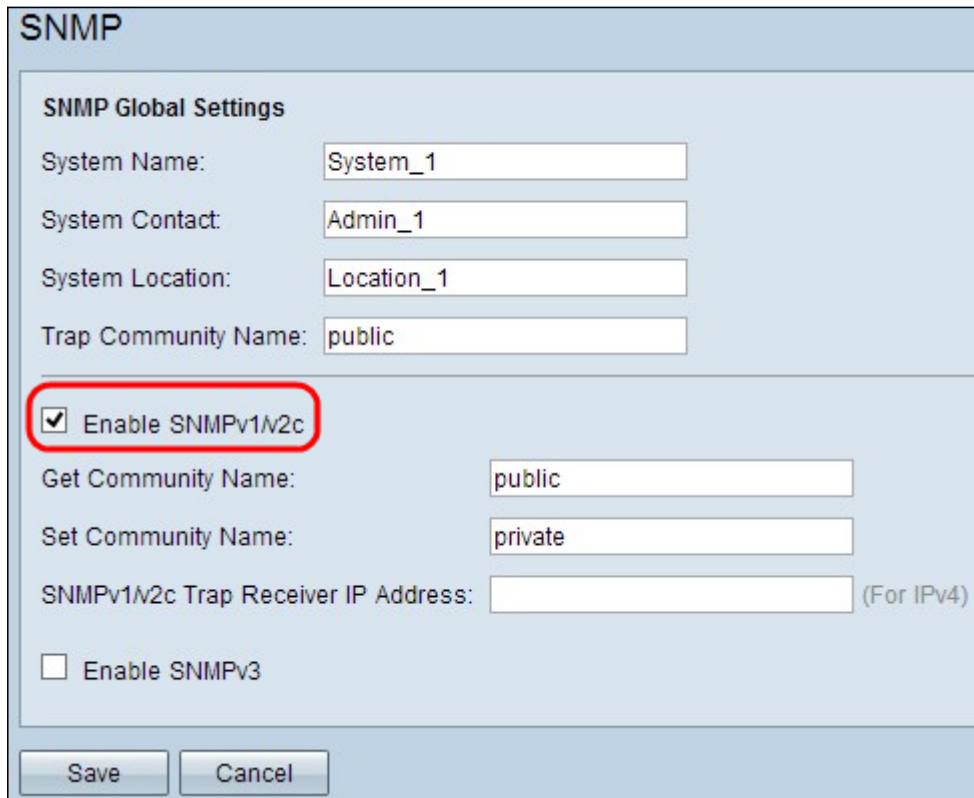
号码)。

步骤5.在Trap Community Name字段中输入座席所属的陷阱社区名称。陷阱是设备在发生特定事件时发送的消息。陷阱社区名称最多可包含64个字母数字字符。默认陷阱社区名称为 *public*。

步骤6.单击“保存”以保存设置。

## SNMPv1/SNMPv2c配置

SNMPv1是SNMP的第一个版本，现在被视为不安全。SNMPv2c是SNMP的改进版本。它比SNMPv1提供更高的安全性，并改进了错误处理。



The image shows a configuration window titled "SNMP". Under the "SNMP Global Settings" section, there are four text input fields: "System Name" (System\_1), "System Contact" (Admin\_1), "System Location" (Location\_1), and "Trap Community Name" (public). Below this, there is a checkbox labeled "Enable SNMPv1/v2c" which is checked and highlighted with a red circle. Further down, there are two more text input fields: "Get Community Name" (public) and "Set Community Name" (private). Below these is a text input field for "SNMPv1/v2c Trap Receiver IP Address" with the note "(For IPv4)". At the bottom, there is an unchecked checkbox for "Enable SNMPv3". At the very bottom of the window are two buttons: "Save" and "Cancel".

步骤1.选中Enable SNMPv1/v2c以启用SNMPv1/2c。

The image shows a configuration window titled "SNMP". It is divided into two main sections. The top section, "SNMP Global Settings", contains four text input fields: "System Name" (System\_1), "System Contact" (Admin\_1), "System Location" (Location\_1), and "Trap Community Name" (public). Below this is a checkbox for "Enable SNMPv1/v2c" which is checked. A red rectangular box highlights the "SNMPv1/v2c" configuration fields: "Get Community Name" (community\_1), "Set Community Name" (setcommunity\_1), and "SNMPv1/v2c Trap Receiver IP Address" (192.168.1.2) with a "(For IPv4)" label. At the bottom, there is a checkbox for "Enable SNMPv3" which is unchecked, and two buttons labeled "Save" and "Cancel".

步骤2.在Get Community Name字段中输入社区名称。Get Community Name是用于验证SNMP Get命令的只读社区字符串。Get命令用于从SNMP设备检索信息。“获取社区名称”最多可包含64个字母数字字符。默认的获取社区名称为*public*。

步骤3.在Set Community Name字段中输入社区名称。对SNMP Set命令进行身份验证的是读/写社区字符串。Set命令用于修改或设置设备上的变量。“设置社区名称”最多可包含64个字母数字字符。默认的“设置社区名称”为私有。

步骤4.在SNMPv1/v2c陷阱接收器IP地址字段中输入SNMP管理软件运行的特定服务器的IP地址或域名。从服务器向管理员发送陷阱消息，以便在发生错误或故障时通知管理员。

第 5 步：点击 **Save (保存)**，以保存设置。

## SNMPv3配置

SNMPv3是SNMP的最新版本，它在三个SNMP版本中提供最高级别的安全性。它还提供远程配置。

**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:

步骤1.选中**Enable SNMPv3**以启用SNMPv3。

## SNMPv3组管理

SNMPv3组管理允许您创建具有不同级别访问设备的组。然后，您可以根据您认为适当的情况将用户映射到这些组。

### 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:

步骤1.在组表中单击添加，在SNMPv3组管理表中添加新组。SNMPv3组管理页面打开：

# 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 |

步骤2.在Group Name字段中输入组名称。

# 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

步骤3.从Security Level下拉列表中选择安全类型。安全类型描述如下：

·无身份验证、无隐私 — 此组中的用户无需设置身份验证密码或设置隐私密码。消息不会加密，用户也不会通过身份验证

·身份验证，无隐私 — 用户需要设置身份验证密码，但不需要设置隐私密码。收到消息时

，用户将通过身份验证，但消息不会加密。

·身份验证隐私 — 用户需要设置身份验证密码和隐私密码。收到消息时，用户将通过身份验证。邮件也将使用隐私密码进行加密。

## 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

步骤4.选中复选框以选择您希望组访问的特定管理信息库(MIB)。MIB用于定义托管系统的必要



信息。它表示为iso.org.dod.internet.mgmt.mib。通过设置特定MIB，您可以允许组访问设备的不同部分。

步骤5.单击每个选中的MIB的特定单选按钮，以选择该组可用的权限级别。权限级别定义如下：

- 只读 — 此组中的用户将能够从MIB读取，但无法修改它。
- 读/写 — 此组中的用户将能够从MIB中读取并修改它。

步骤6.向下滚动并单击“保存”以保存设置。这会将组添加到组表。

The image shows a web-based configuration interface for SNMP. It is divided into several sections:

- SNMP Global Settings:** Includes input fields for System Name (System\_1), System Contact (Admin\_1), System Location (Location\_1), and Trap Community Name (public). There are checkboxes for "Enable SNMPv1/v2c" (unchecked) and "Enable SNMPv3" (checked).
- Group Table:** A table with columns for Group Name, Security, and Access MIBs. A row for "Group1" is highlighted in green, with Security set to "Authentication, Privacy" and five MIBs selected with radio buttons: 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 "Add", "Edit" (circled in red), and "Delete" buttons.
- User Table:** A table with columns for Enable, User Name, Authentication, Privacy, and Group. It currently shows "0 results found!" and has "Add", "Edit", and "Delete" buttons.
- SNMPv3 Trap Receiver IP Address:** An input field with "(For IPv4)" next to it.
- SNMPv3 Trap Receiver User:** A dropdown menu currently set to "No User".

步骤7. ( 可选 ) 如果要更改已配置的组，请单击所需组的多选按钮，然后单击编辑并更改相应字段。

第8步。 ( 可选 ) 如果要删除已配置的组，请单击该组所需的多选按钮，然后单击删除。

## SNMPv3用户管理

SNMP用户是为其执行SNMP服务的远程用户。

**注意：**必须先将组添加到组表，然后才能在用户表中添加用户。

### 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:

步骤1.从User Table中单击**Add**，在SNMPv3 User Management Table中添加新用户。系统将打开“SNMPv3用户管理”页：

### SNMP

**SNMPv3 User Management**

Enable:

User Name:

Group:

Authentication Method:  MD5  SHA  None Authentication Password:

Privacy Method:  DES  AES  None Privacy Password:

步骤2.选中**Enable**以启用SNMP的用户管理。

步骤3.在“用户名”字段中输入用户名。

步骤4.从Group下拉列表中选择所需组。新用户将添加到此特定组。

步骤5.点击特定单选按钮以选择Authentication Method。身份验证方法如下所述：

- MD5 — 消息摘要算法5(MD5)是32位十六进制哈希函数。
- SHA — 安全散列算法(SHA)是160位散列函数，被认为比MD5更安全。

步骤6.在Authentication Password字段中输入身份验证的密码。身份验证密码是设备之间预先共享的密码。当它们交换流量时，它们使用特定密码对流量进行身份验证。

步骤7.单击特定单选按钮，在Privacy Method字段中选择所需的加密方法。

·DES — 数据加密标准(DES)是一种56位加密方法。它被视为不安全，但是当设备与不支持AES的其他设备一起使用时，可能需要它。

·AES — 高级加密标准(AES)使用128位、192位或256位加密方法。它被认为比DES更安全。

步骤8.在Privacy Password字段中输入隐私密码。隐私密码是用于加密消息的密码。

第 9 步： 点击 **Save ( 保存 )**，以保存设置。这会将用户添加到用户表。

The screenshot displays 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

第10步。(可选)如果要更改已配置的用户,请单击所需用户的单选按钮,然后单击编辑并更改相应的字段。

第11步。(可选)如果要删除已配置的用户,请单击所需用户的单选按钮,然后单击删除。

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

步骤12.在SNMPv3陷阱接收器IP地址字段中输入SNMPv3陷阱接收器的IP地址。

步骤13.从SNMPv3陷阱接收器用户下拉列表中选择相应的陷阱用户。这是发生陷阱事件时接收陷阱消息的用户。

步骤14.单击“保存”以保存设置。