

RV215W上的简单网络管理协议(SNMP)配置

目标

简单网络管理协议(SNMP)是用于管理和监控网络的应用层协议。网络管理员使用SNMP来管理网络性能、检测和纠正网络问题，以及收集网络统计信息。SNMP托管网络由受管设备、代理和网络管理器组成。受管设备是支持SNMP功能的设备。代理是受管设备上的SNMP软件。网络管理器是从SNMP代理接收数据的实体。用户必须安装SNMP v3管理器程序才能查看SNMP通知。

本文介绍如何在RV215W上配置SNMP。

适用设备

- RV215W

软件版本

- 1.1.0.5

SNMP配置

步骤1. 登录Web配置实用程序，然后选择Administration > SNMP。SNMP页面打开：

SNMP

SNMP System Information

SNMP: Enable

Engine ID: 80000009033CCE738E0126

SysContact:

SysLocation:

SysName:

SNMPv3 User Configuration

UserName: guest admin

Access Privilege: Read Write User

Security level:

Authentication Algorithm Server: MD5 SHA

Authentication Password:

Privacy Algorithm: DES AES

Privacy Password:

Trap Configuration

IP Address: (Hint: 192.168.1.100 or fec0::64)

Port: (Range: 162 or 1025 - 65535, Default: 162)

Community:

SNMP Version:

SNMP系统信息

SNMP System Information

SNMP: Enable

Engine ID: 80000009033CCE738E0126

SysContact:

SysLocation:

SysName:

步骤1.在SNMP字段中选**Enable**以允许在RV215W上进行SNMP配置。

注意：RV215W代理的引擎ID显示在“引擎ID”(Engine ID)字段中。引擎ID用于唯一标识受管设备上的代理。

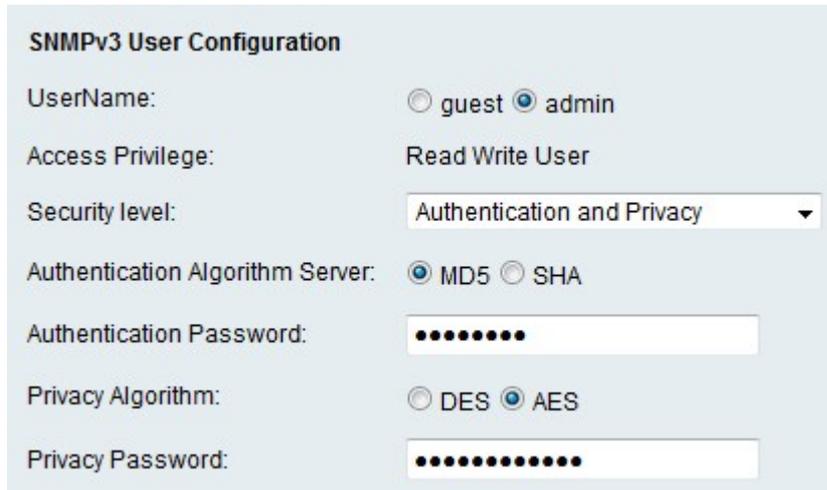
步骤2.在SysContact字段中输入系统联系人的姓名。通常的做法是包括系统联系人的联系信息。

步骤3.在SysLocation字段中输入RV215W的物理位置。

步骤4.在SysName字段中输入RV215W的标识名称。

步骤5.单击Save。

SNMPv3用户配置



The image shows a configuration window titled "SNMPv3 User Configuration". It contains several fields and options:

- UserName:** Radio buttons for "guest" and "admin", with "admin" selected.
- Access Privilege:** A text field containing "Read Write User".
- Security level:** A dropdown menu showing "Authentication and Privacy".
- Authentication Algorithm Server:** Radio buttons for "MD5" and "SHA", with "MD5" selected.
- Authentication Password:** A password input field with 8 dots.
- Privacy Algorithm:** Radio buttons for "DES" and "AES", with "AES" selected.
- Privacy Password:** A password input field with 12 dots.

步骤1.点击与UserName字段中要配置的所需帐户对应的单选按钮。用户的访问权限显示在“访问权限”(Access Privilege)字段中。

- 访客 — 访客用户仅具有读取权限。
- 管理员 — 管理员用户具有读写权限。

步骤2.从Security level下拉列表中选择所需的安全性。身份验证用于验证和允许用户查看或管理SNMP功能。隐私是另一个可用于提高SNMP功能安全性的密钥。

- 无身份验证和无隐私 — 用户不需要身份验证或隐私密码。
- 身份验证和无隐私 — 用户只需要身份验证。
- 身份验证和隐私 — 用户需要身份验证和隐私密码。

步骤3.如果安全级别包括身份验证，请点击Authentication Algorithm Server字段中与所需服务器对应的单选按钮。此算法是哈希函数。散列函数用于将密钥转换为指定的比特消息。

- MD5 — 消息摘要5(MD5)是一种算法，它采用输入并生成输入的128位消息摘要。
- SHA — 安全散列算法(SHA)是一种算法，它采用输入并生成输入的160位消息摘要。

步骤4.在Authentication Password字段中为用户输入密码。

步骤5.如果安全级别包括隐私，请点击与Privacy Algorithm字段中所需算法对应的单选按钮。

- DES — 数据加密标准(DES)是一种使用相同方法加密和解密消息的加密算法。DES算法的处理速度比AES快。
- AES — 高级加密标准(AES)是一种使用不同方法加密和解密消息的加密算法。这使AES成

为比DES更安全的加密算法。

步骤6.在Privacy Password字段中为用户输入隐私密码。

步骤7.单击“保存”。

陷阱配置

陷阱是生成用于报告系统事件的SNMP消息。陷阱将强制受管设备向网络管理器发送SNMP消息，该消息会将系统事件通知网络管理器。



The image shows a 'Trap Configuration' form with the following fields and values:

Field	Value	Hint/Range
IP Address:	192.168.1.100	(Hint: 192.168.1.100 or fec0::64)
Port:	162	(Range: 162 or 1025 - 65535, Default: 162)
Community:	community1	
SNMP Version:	v1	

步骤1.在IP地址字段中输入陷阱通知将发送到的IP地址。

步骤2.在Port字段中输入陷阱通知将发送到的IP地址的端口号。

步骤3.在Community字段中输入陷阱管理器所属的社区字符串。社区字符串是用作密码的文本字符串。SNMP使用它对代理和网络管理器之间发送的消息进行身份验证。

注意：此字段仅在SNMP陷阱版本不是版本3时适用。

步骤4.从SNMP Version下拉列表中，为SNMP陷阱消息选择SNMP管理器版本。

- v1 — 使用社区字符串对陷阱消息进行身份验证。
- v2c — 使用团体字符串对陷阱消息进行身份验证。
- v3 — 使用加密密码对陷阱消息进行身份验证。

步骤5.单击Save。