

RV315W VPN路由器上的SNMP配置

目標

簡單網路管理協定(SNMP)是用於網路管理的TCP/IP協定。SNMP允許管理員監控網路效能、錯誤率。SNMP還可以對映網路可用性。SNMP框架包含三個要素：SNMP管理器、SNMP代理和MIB。SNMP管理器的功能是控制和監控使用SNMP的網路主機的活動。SNMP代理位於裝置的軟體中，它幫助維護資料以便管理系統。最後，管理資訊庫(MIB)是網路管理資訊的虛擬儲存區域。這三種方法相結合，可監控和管理網路中的裝置。

本文有助於解釋如何在RV315W VPN路由器上配置SNMP。

適用的裝置

·RV315W

軟體版本

•1.01.03

設定SNMP

SNMP v1是SNMP的原始版本，缺乏某些功能，只適用於TCP/IP網路，SNMP v2是v1的改進版本。SNMP v1&v2隻應選擇使用SNMPv1或SNMPv2的網路。SNMP v3是SNMP的最新標準，解決了SNMP v1和v2的許多問題。特別是，它解決了v1和v2的許多安全漏洞。SNMP v3還允許管理員遷移到一個常用的SNMP標準。

步驟1.登入到Web配置實用程式並選擇**System Management > SNMP**。SNMP頁面隨即開啟：

SNMP configuration page showing the following settings:

- SNMP: Enable Disable
- SNMP Version: SNMP v1&v2 SNMP v3
- System Contact: (1-200 characters)
- System Name: RV315W *(1-30 characters)
- System Location: Office *(1-200 characters)
- Security Username: (1-32 characters)
- Authentication Password: (8-64 characters)
- Authentication Method: HMAC-MD5 HMAC-SHA
- Encrypted Password: (8-64 characters)
- Encryption Method: None CBC-DES
- SNMP Read-Only Community: public *(1-32 characters)
- SNMP Read-Write Community: private *(1-32 characters)
- Trap Community: public *(1-32 characters)
- SNMP Trusted Host: 0.0.0.0
- Trap Receiver Host: 192.168.1.100 *

* indicates a mandatory option.

步驟2.按一下**Enable**單選按鈕以啟用SNMP。

步驟3.按一下所需的SNMP版本單選按鈕。

·SNMP v1&v2 — SNMP v1是SNMP的原始小版本，缺少某些功能，SNMP v2是改進功能的

較新版本，但只應針對運行SNMP v1或SNMP v2的網路選擇此選項。

·SNMP v3 — SNMP 3是最新版本，允許管理員使用一個標準。應選擇此選項，因為它修復了v1和v2中的許多安全缺陷。

為SNMP v1&v2配置SNMP

The screenshot shows the SNMP configuration window with the following settings:

- SNMP: Enable Disable
- SNMP Version: SNMP v1&v2 SNMP v3
- System Contact: (1-200 characters)
- System Name: RV315W *(1-30 characters)
- System Location: Office *(1-200 characters)
- Security Username: (1-32 characters)
- Authentication Password: (8-64 characters)
- Authentication Method: HMAC-MD5 HMAC-SHA
- Encrypted Password: (8-64 characters)
- Encryption Method: None CBC-DES
- SNMP Read-Only Community: public *(1-32 characters)
- SNMP Read-Write Community: private *(1-32 characters)
- Trap Community: public *(1-32 characters)
- SNMP Trusted Host: 0.0.0.0
- Trap Receiver Host: 192.168.1.100 *

* indicates a mandatory option.

步驟4. (可選) 在「系統聯絡人」欄位中輸入聯絡人資訊。這是聯絡以取得網路協助的個人。

步驟5.在「系統名稱」欄位中輸入名稱。這是分配給SNMP設定的名稱。

步驟6.在「系統位置」欄位中輸入位置。這是系統所在的位置。

步驟7.在SNMP Read-Only Community欄位中輸入一個社群。這是用於對SNMP設定進行只讀訪問的客戶端引數。

步驟8.在SNMP讀取/寫入社群欄位中輸入社群。這是用於對SNMP設定進行讀寫訪問的客戶端引數。

步驟9.在「陷阱社群」欄位中輸入社群。這是能夠使用SNMP陷阱的社群。陷阱是傳送給管理員的定向通知。陷阱允許管理員通過允許其使用者使用陷阱來通知裝置來管理每台裝置。

步驟10.在SNMP Trusted Host欄位中輸入主機。這是SNMP設定的信任主機的IP地址。

步驟11.在Trap Receiver Host欄位中輸入主機。這是接收陷阱的管理員的IP地址。

步驟12.按一下**Save**以套用設定。

為SNMP v3配置SNMP

步驟4. (可選) 在「系統聯絡人」欄位中輸入聯絡人資訊。這是聯絡以取得網路協助的個人。

步驟5.在「系統名稱」欄位中輸入名稱。這是分配給SNMP設定的名稱。

步驟6.在「系統位置」欄位中輸入位置。這是系統所在的位置。

SNMP configuration interface showing the following fields and values:

- SNMP: Enable Disable
- SNMP Version: SNMP v1&v2 SNMP v3
- System Contact: (1-200 characters)
- System Name: RV315W *(1-30 characters)
- System Location: Office *(1-200 characters)
- Security Username: Profile1 (1-32 characters)
- Authentication Password: ***** (8-64 characters)
- Authentication Method: HMAC-MD5 HMAC-SHA
- Encrypted Password: ***** (8-64 characters)
- Encryption Method: None CBC-DES
- SNMP Read-Only Community: public *(1-32 characters)
- SNMP Read-Write Community: private *(1-32 characters)
- Trap Community: public *(1-32 characters)
- SNMP Trusted Host: 0.0.0.0
- Trap Receiver Host: 192.168.1.100 *

* indicates a mandatory option.

步驟7。(可選)在Security Username欄位中輸入使用者名稱。這是使用者名稱，用於取得SNMP設定的存取許可權。

步驟8。(可選)在Authentication Password欄位中輸入密碼。這是用於取得對SNMP設定程式存取的密碼。

步驟9.按一下Authentication Method欄位中的HMAC-MD5或HMAC-SHA單選按鈕。基於雜湊的消息驗證碼(HMAC)是將驗證碼和金鑰組合在一起的加密代碼。HMAC的主要用途是保證報文安全。HMAC將根據生成的金鑰對資料進行身份驗證。

- HMAC MD5 — 此雜湊演算法存在幾個安全缺陷，資料可能受到危害。HMAC MD5是一種使用加密雜湊函式的消息驗證機制。MD5用於系統效能速度優異的關鍵點，儘管安全性較低。

- HMAC SHA — 此雜湊演算法比加密方法更安全。這是使用加密雜湊函式的消息身份驗證更加安全的機制。當安全性至關重要時，應使用HMAC SHA。

SNMP configuration interface showing the following fields and values:

- SNMP: Enable Disable
- SNMP Version: SNMP v1&v2 SNMP v3
- System Contact: (1-200 characters)
- System Name: RV315W *(1-30 characters)
- System Location: Office *(1-200 characters)
- Security Username: Profile1 (1-32 characters)
- Authentication Password: ***** (8-64 characters)
- Authentication Method: HMAC-MD5 HMAC-SHA
- Encrypted Password: ***** (8-64 characters)
- Encryption Method: None CBC-DES
- SNMP Read-Only Community: public *(1-32 characters)
- SNMP Read-Write Community: private *(1-32 characters)
- Trap Community: public *(1-32 characters)
- SNMP Trusted Host: 0.0.0.0
- Trap Receiver Host: 192.168.1.100 *

* indicates a mandatory option.

步驟10.在Encrypted Password欄位中輸入密碼。

步驟11.點選Encryption Method欄位中的CBC-DES單選按鈕。CBC和DES是結合起來保護傳輸資料的加密標準。

步驟12.在SNMP Read-Only Community欄位中輸入一個社群。這是用於對SNMP設定進行只讀訪問的客戶端引數。

步驟13.在SNMP讀取/寫入社群欄位中輸入社群。這是用於對SNMP設定進行讀寫訪問的客戶端引數。

步驟14.在「陷阱社群」欄位中輸入社群。這是能夠使用SNMP陷阱的社群。陷阱是傳送給管理員的定向通知。陷阱允許管理員通過允許其使用者使用陷阱來通知裝置來管理每台裝置。

步驟15.在SNMP Trusted Host欄位中輸入主機。這是SNMP設定的信任主機的IP地址。

步驟16.在Trap Receiver Host欄位中輸入主機。這是接收陷阱的管理員的IP地址。

步驟17.按一下「**Save**」以套用設定。