

在SPA100系列上配置簡單網路管理協定(SNMP)設定

目標

簡易網路管理通訊協定(SNMP)是一種工具，用於監控和調控網路上的裝置，以及維護組態。它的統計資訊收集、效能和安全性使您能夠快速解決網路問題。SNMP託管網路由託管裝置、代理和網路管理器組成。受管裝置是具備SNMP功能的裝置。代理是受管裝置上的SNMP軟體。網路管理器是從SNMP代理接收資料的實體。您必須安裝SNMP v3管理器程式才能檢視SNMP通知。在裝置上，使用者可以調整陷阱配置設定。陷阱是在網路中發生錯誤時傳送到特定IP地址的錯誤消息。

本文的目的是向您展示如何在SPA100系列模擬電話介面卡(ATA)上配置SNMP設定。

適用裝置

- SPA100系列類比電話配接器

軟體版本

- v1.1.0

SNMP組態

步驟1.登入到Web配置實用程式，然後選擇Administration > Management > SNMP。SNMP頁面隨即開啟：

SNMP

SNMP Setting

SNMP: Enabled Disabled

Trusted IP: Any

Address: . . .

Netmask: . . .

Get / Trap Community:

Set Community:

SNMPV3: Enabled Disabled

R/W User:

Auth- Protocol: ▾

Auth- Password :

PrivProtocol: ▾

Privacy Password:

Trap Configuration

IP Address: . . . (Hint:192.168.15.100)

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

SNMP Version: ▾

Submit

Cancel

步驟2.在SNMP欄位的右側，按一下Enabled單選按鈕以啟用SNMP，或按一下Disabled單選按鈕以停用裝置上的SNMP。

SNMP Setting

SNMP: Enabled Disabled

Trusted IP: Any

Address: 192 . 168 . 10 . 1

Netmask: 255 . 255 . 255 . 0

Get / Trap Community: public

Set Community: private

步驟3.在 *Trusted IP* 欄位中，按一下 **Any** 以允許透過SNMP從任何IP位址存取ATA，或按一下 **Address** 以允許一系列IP位址透過SNMP存取ATA。

步驟4.在 *Get Community* 欄位中，輸入短語作為SNMP社群中GET命令的密碼。

步驟5.在 *Set Community* 欄位中，輸入短語作為SNMP社群中SET命令的密碼。

SNMPV3: Enabled Disabled

R/W User: v3rwuser

Auth- Protocol: HMAC-SHA

Auth- Password :

PrivProtocol: CBC-DES

Privacy Password:

步驟6. SNMPV3是SNMP更安全的實施。它支援使用更高級的身份驗證和加密機制，以確保只有經過授權的裝置才能通過SNMP讀取和寫入網路裝置。按一下 **Enabled** 單選按鈕使用SNMPv3，或按一下 **Disabled** 單選按鈕禁用它。

步驟7.在 *R/W User* 欄位中，輸入SNMPv3身份驗證的使用者名稱。

步驟8.從 *Auth-Protocol* 下拉選單中，選擇SNMPv3的身份驗證協定。可用選項定義如下：

- MD5 - Message-Digest 5(MD5)是一種接受輸入並產生128位輸入消息摘要的演算法。
- SHA — 安全雜湊演演算法(SHA)是一種接受輸入並產生160位元輸入訊息摘要的演演算法。

附註： HMAC-SHA被認為比HMAC-MD5更安全，建議使用。

步驟9.在 *Auth-Password* 欄位中，輸入驗證密碼。

步驟10.從 *PrivProtocol* 下拉選單中，選擇隱私身份驗證協定。建議使用者必須具有隱私功能才能保護資料。可用選項定義如下：

- 無 — 不使用隱私演算法。郵件資料將以未加密方式傳送。
- CBC-DES — 此選項使用DES加密消息的資料。

步驟11.在 *Privacy Password* 欄位中，輸入隱私身份驗證協定的密碼。

Trap Configuration

IP Address: . . . (Hint: 192.168.15.100)

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

SNMP Version: ▼

步驟12.在 *IP Address* 欄位中，輸入將接收陷阱訊息的IP位址。

步驟13.在 *Port* 欄位中，輸入將接收陷阱訊息的連線埠號碼。預設埠為162。

步驟14.從 *SNMP* 版本下拉式清單中選擇用於查詢陷阱消息的SNMP版本。可用的選項如下：

- v1 — 使用SNMPv1陷阱。SNMPv1陷阱使用社群字串來驗證陷阱消息，並且不加密資料。
- v2 — 使用SNMPv2陷阱。SNMPv2陷阱使用社群字串來驗證陷阱消息，並且不加密資料。
- v3 — 使用SNMPv3陷阱。SNMPv3陷阱可以設定為使用使用者名稱和密碼來驗證陷阱的來源，並可以加密陷阱的資料。必須如步驟6所述啟用和配置SNMPv3才能使用此選項。

步驟15.按一下 **Submit** 應用更改，或按一下 **Cancel** 放棄更改。