

WAP121和WAP321接入點上的簡單網路管理協定(SNMP)常規設定

目標

簡單網路管理協定(SNMP)是用於網路管理、故障排除和維護的協定。SNMP在兩款重要軟體的幫助下記錄、儲存和共用資訊：在管理器裝置上運行的網路管理系統(NMS)和在受管裝置上運行的代理。WAP121和WAP321支援SNMPv2和SNMPv3。

本文說明如何在WAP121和WAP321接入點上配置常規SNMP設定。

適用裝置

- WAP121
- WAP321

軟體版本

- 1.0.3.4

SNMP常規設定

步驟1.登入到Access Point Configuration Utility，然後選擇**SNMP > General**。*General*頁面隨即開啟：

The screenshot shows the 'General' configuration page for SNMP. It includes the following sections and fields:

- Global Settings:**
 - SNMP: Enable
 - UDP Port: (Range: 1025-65535, Default: 161)
- SNMPv2c Settings:**
 - Read-only Community: (Range: 1 - 256 Characters. Alphanumeric and special characters are allowed.)
 - Read-write Community: (Range: 1 - 256 Characters. Alphanumeric and special characters are allowed.)
 - Management Station: All, User Defined
 - NMS IPv4 Address/Name: (xxx.xxx.xxx.xxx / Hostname max 253 Characters)
 - NMS IPv6 Address/Name: (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx / Hostname Max 253 Characters)
- SNMPv2c Trap Settings:**
 - Trap Community: (Range: 1 - 80 Characters.. Alphanumeric and special characters are allowed.)
- Trap Destination Table:**

	Host IP Address Type	Hostname/IP Address	
<input type="checkbox"/>	IPv4	<input type="text"/> (xxx.xxx.xxx.xxx / Hostname max 253 Characters)	
<input type="checkbox"/>	IPv4	<input type="text"/> (xxx.xxx.xxx.xxx / Hostname max 253 Characters)	
<input type="checkbox"/>	IPv4	<input type="text"/> (xxx.xxx.xxx.xxx / Hostname max 253 Characters)	

A 'Save' button is located at the bottom left of the configuration area.

Global Settings

SNMP: Enable

UDP Port: (Range: 1025-65535, Default: 161)

步驟2.在Global Settings區域中，選中**Enable**覈取方塊以啟用SNMP。

步驟3.在「UDP埠」欄位中，輸入SNMP代理將偵聽訪問請求的UDP埠號。

時間分配器：如果您不想配置SNMPv2，請跳至**步驟12**。如果未配置SNMPv2，則使用SNMPv3。要配置SNMPv3設定，請參閱WAP121和WAP321接入點上的**簡單網路管理協定(SNMP)檢視配置**。

SNMPv2c Settings

Read-only Community: (Range: 1 - 256 Characters. Alphanumeric and special characters are allowed.)

Read-write Community: (Range: 1 - 256 Characters. Alphanumeric and special characters are allowed.)

Management Station: All User Defined

NMS IPv4 Address/Name: (xxx.xxx.xxx.xxx / Hostname max 253 Characters)

NMS IPv6 Address/Name: (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx / Hostname Max 253 Characters)

步驟4.在「只讀社群」欄位中輸入只讀社群名稱。團體名稱是使用者建立的有效名稱，用作簡單身份驗證機制或密碼，以限制網路上可向SNMP代理請求資料的裝置。傳送方傳送的請求資料包中傳送的社群字串必須與代理裝置上的社群字串匹配。只讀密碼授予僅檢索資訊的許可權。

步驟5.在「讀取/寫入社群」欄位中輸入允許的SNMP集操作的讀取/寫入社群名稱。僅接受來自使用此社群名稱標識自己的裝置的請求。這是使用者建立的名稱。此密碼允許您從代理檢索資訊並修改該代理裝置上的設定。

附註：最好將兩個密碼都更改為自定義的密碼，以避免外部人員的安全攻擊。

步驟6.點選適當的單選按鈕，在Management Station欄位中選擇管理站首選項。管理站監視和更新管理資訊庫(MIB)中的值。

- 所有 — 允許網路中的所有站點通過SNMP作為管理站點訪問WAP。
- 使用者定義 — 限制對特定站點或站點組的訪問。

時間分配器：如果在上一步中選擇了「全部」，請跳至步驟9。

SNMPv2c Settings

Read-only Community: (Range: 1 - 256 Characters. Alphanumeric and special characters are allowed.)

Read-write Community: (Range: 1 - 256 Characters. Alphanumeric and special characters are allowed.)

Management Station: All User Defined

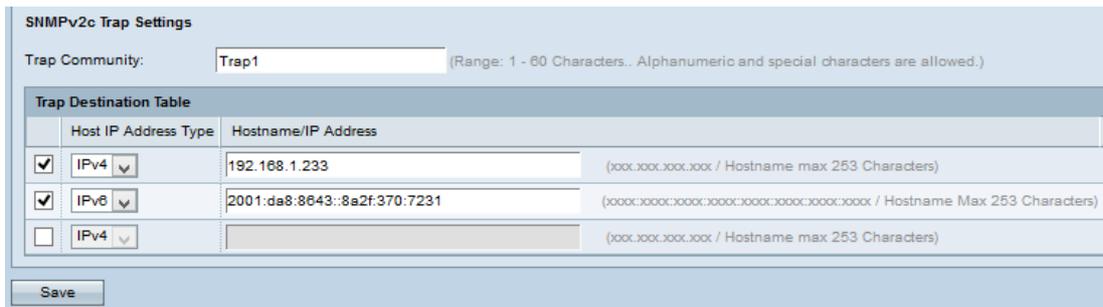
NMS IPv4 Address/Name: (xxx.xxx.xxx.xxx / Hostname max 253 Characters)

NMS IPv6 Address/Name: (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx / Hostname Max 253 Characters)

步驟7.如果已在在上一步中選擇「使用者定義」，請在「NMS IPv4地址/名稱」欄位中輸入要訪問WAP的管理工作站的IPv4地址。網路管理系統(NMS)是指執行應用程式以監視和控制受管裝置的管理站。

步驟8. (可選) 如果WAP使用IPv6地址，則在NMS IPv6 Address/Name欄位中輸入要訪問

WAP的管理站的IPv6地址。



The image shows a configuration window titled "SNMPv2c Trap Settings". At the top, there is a "Trap Community" field with the value "Trap1" and a note "(Range: 1 - 60 Characters. Alphanumeric and special characters are allowed.)". Below this is a "Trap Destination Table" with three rows. The first row is checked and has "IPv4" selected in the "Host IP Address Type" column and "192.168.1.233" in the "Hostname/IP Address" column. The second row is also checked and has "IPv6" selected and "2001:da8:8643::8a2f:370:7231" in the address field. The third row is unchecked and has "IPv4" selected. A "Save" button is located at the bottom left of the table area.

	Host IP Address Type	Hostname/IP Address	
<input checked="" type="checkbox"/>	IPv4	192.168.1.233	(xxx.xxx.xxx.xxx / Hostname max 253 Characters)
<input checked="" type="checkbox"/>	IPv6	2001:da8:8643::8a2f:370:7231	(xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx / Hostname Max 253 Characters)
<input type="checkbox"/>	IPv4		(xxx.xxx.xxx.xxx / Hostname max 253 Characters)

步驟9.在Trap Community欄位中輸入與SNMP陷阱關聯的全域性社群名稱。陷阱是從代理傳送到包含代理資訊的管理器的通知。從裝置傳送的陷阱使用輸入的字串作為社群名稱。

步驟10.在Trap Destination表中，選中主機IP地址覈取方塊，然後從Host IP Address Type欄位的下拉選單中選擇適當型別的主機IP地址（IPv4或IPv6）。這是指從受管裝置接收陷阱的相應管理站的地址或名稱。

步驟11.在主機名/IP地址欄位中輸入陷阱的主機名或IP地址。

附註：您最多可以重複步驟10和11三次。

步驟12.按一下**Save**以儲存組態。