EtherWAN

工業級行動通訊 LTE 閘道器

EW50

使用手冊

免責聲明

本文件中包含的資訊如有更改，恕不另行通知。EtherWAN 對於本手冊中包含的任何錯誤、遺漏或與本手冊中提供的資訊有關的損害概不負責。

所有其他商標均為其各自所有者的財產。

保證

有關 EtherWAN 保固更新政策的詳細信息，請登入我們的網站：

https://kb.etherwan.com/index.php?CategoryID=13

本手冊適用的產品：

EW50

前言

讀者

本手冊專為安裝、配置、部署和維護網路的人員而設計。 本文認定讀者俱有相當的電腦硬體和網路技能。

文件修訂記錄

本節提供本文件修訂更改的歷史記錄

修訂	文件版本	日期	描述
A	版本 2	1/15/2018	修正了幾個拼寫和語法錯誤
A	3	2/9/2018	修正文字
A	4	6/18/2019	改正圖片
A	5	8/7/2019	修正連接 DI/DO 和序列設備說明

此版本的更改

這是本文件的第一個版本。

目錄

第 1 章 簡介

1.1 簡介

恭喜您購買此產品：工業行動通訊閘道器。EtherWAN 行動通訊閘道器是應用於 M2M 正確的選擇。

其內建的世界級4G LTE模組，只需插入當地通信公司的SIM卡即可上網。雙SIM卡設計為重要的應用提供備援和可靠的WAN連接。透過VPN通道技術，遠程的站點很容易即可成為本地網路的一部分，所有資料都採用安全(256位AES加密)傳輸。而DI/DO 功能讓閘道器能即時警示偵測器檢測到的事件。

這款EW50配備了許多安全功能，包括VPN，Firewall防火牆，NAT網路位址轉換，埠轉發，DHCP動態分配IP伺服器以及其他用於外部IP監控的應用功能。12-48 VDC雙電源備援和雙SIM卡確保資料的傳輸和網路連接無損。

主要特點：

- 內建雙 SIM 卡 LTE modem 支援行動通訊備援。
- 配備 gigabit 網路埠連接其他 IP 設備。
- RS-232 序列埠用於控制傳統序列設備或 Modbus 設備。
- Digital I/O 埠用於結合偵測器、開關或其他警報設備。
- 可選擇 802.11a/b/g/ac 2T2R 2.4G/5GHz 的 Wi-Fi AP 模式。
- 採用堅固且易於安裝的金屬主體設計，適用於工業環境及各種 M2M(機器對機器)應用。

在安裝和使用本產品之前，請詳細閱讀本手冊。

1.2 包裝清單

1.2.1 包裝內容

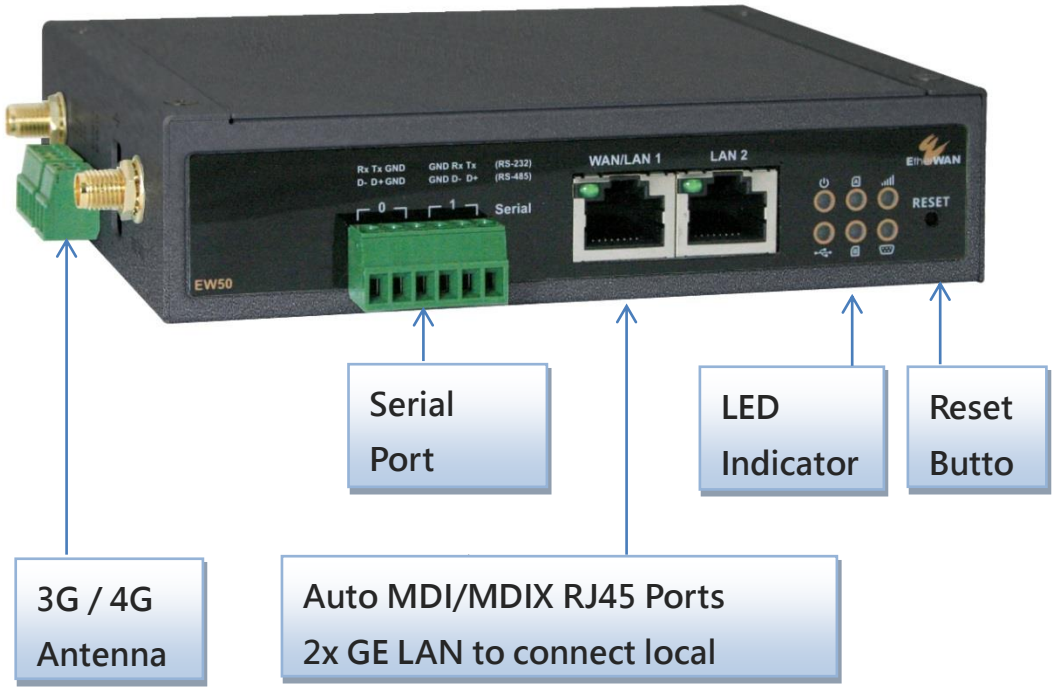
#標準包裝

項目	描述	內容	數量
1	**EW50** **工業行動通訊閘道器**		1pcs
2	**Cellular Antenna**		2pcs
3	**Power Adapter** **(DC 12V/2A)** (*[1])		1pcs
3	**2針接線盒**		**1pcs**
4	**4針接線盒**		1pcs
5	**6針接線盒**		1pcs
7	**DIN-Rail**		1pcs

1 The maximum power consumption of EW50 series products is 7 Watts.

1.3 硬體設定

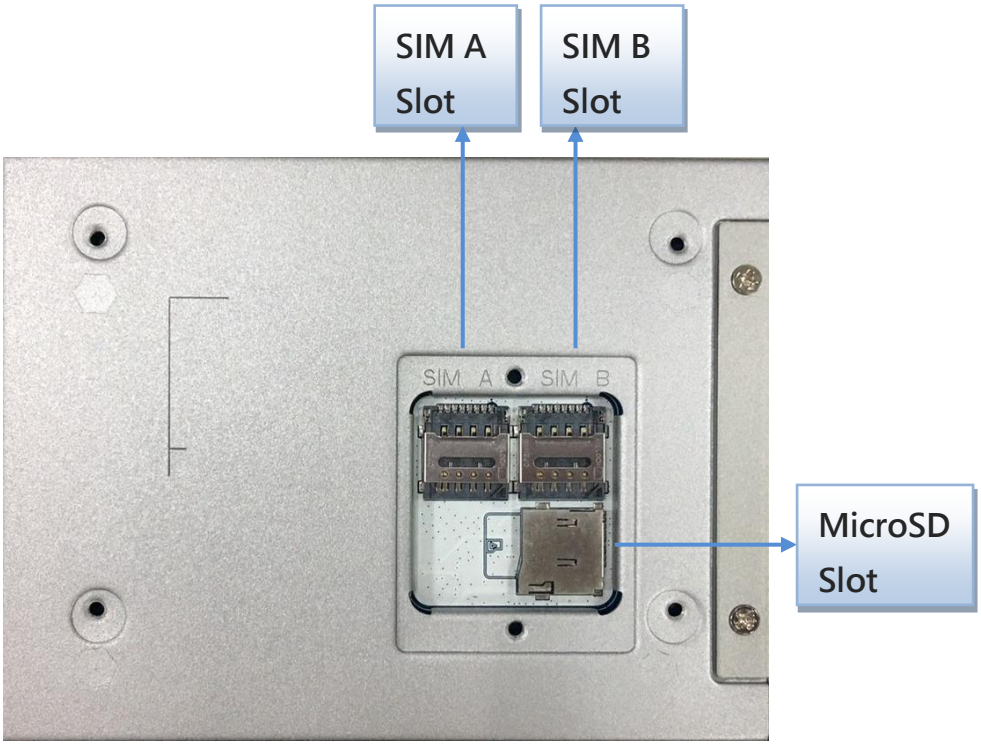
➢ 前視圖



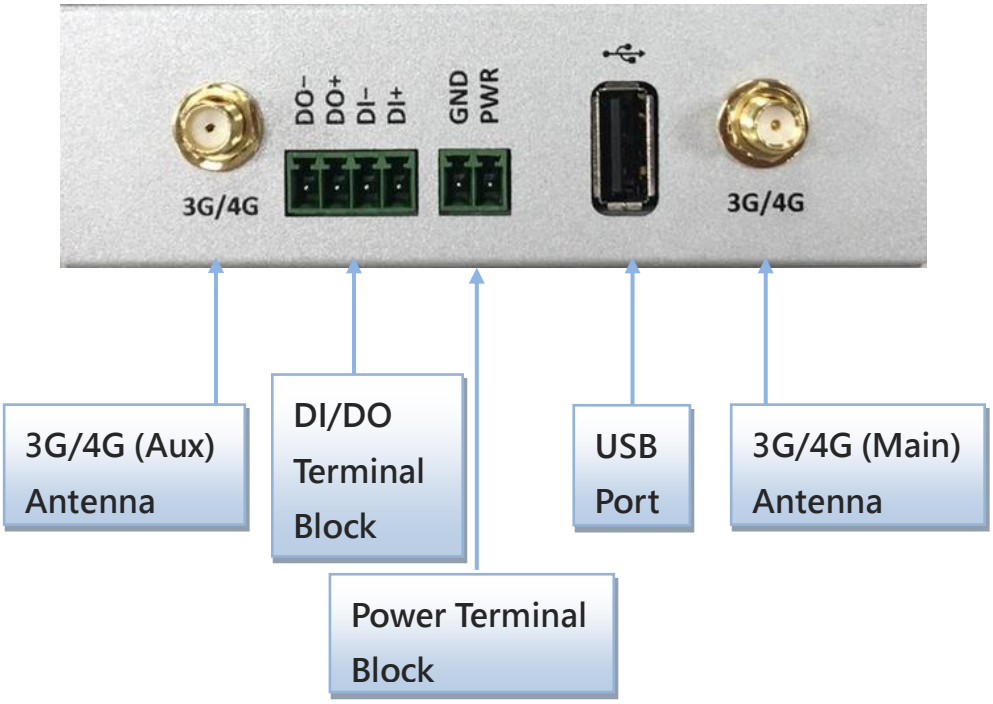
※重置按鈕

重置按鈕提供了一種快速簡單的方法來恢復預設置。持續按住重置按鈕 6 秒鐘，然後鬆開。該設備將重置為出廠預設值。

➢ 底視圖


SIM A Slot
SIM B Slot
SIM A
SIM B
MicroSD Slot

➢ 左視圖


DO-
DO+
DI-
DI+
GND
PWR
3G/4G
3G/4G
3G/4G (Aux) Antenna
DI/DO Terminal Block
Power Terminal Block
USB Port
3G/4G (Main) Antenna

1.4 LED 顯示器

LED 圖示	顯示	LED 顏色	說明
	電源 1	藍色	**恆亮**：設備由電源 1 供電
	訊號 (Cellular)	藍色	**恆亮:** 訊號強度 61~100% **慢閃(每秒)**：信號強度 31~60% **快閃(每 0.5 秒)**：信號強度 0~30%
	USB	藍色	**不亮**：沒有資料封包通過 USB 埠傳輸 **閃爍**：資料封包通過 USB 埠傳輸
	LAN 1 ~ LAN 2/WAN	綠色	**恆亮**： LAN 區域網連接或 WAN 網路連接。 **閃爍**：正在傳輸資料封包。 **不亮**：未連接網路線或未連接設備。
	序列	藍色	**不亮**：無序列埠資料傳輸。 **閃爍**：序列資料封包通過序列埠傳輸。
Status	狀態	藍色	**慢閃(每秒)**：設備正常工作 **非常快速的閃爍**：設備處於恢復模式或異常狀態
	SIM A/B	藍色	**不亮**：未偵測到 SIM **慢閃(每秒)**：選擇 SIM A/B 進行連接 **恆亮**：Cellular 連接成功建立(在 SIM A/B 下)

1.5 安裝和維護

1.5.1 系統需求

網路需求	• Gigabit 網路 RJ45 線 • 3G/4G行動通訊用戶 • IEEE 802.11 a/b/g/ac 無線網路客戶端 • 10/100/1000 網卡電腦
網頁設定工具需求	**具有以下內容的電腦:** • Windows®、Macintosh 或基於 Linux 的作業系統 • 安裝網路網卡 **瀏覽器需求:** • Internet Explorer 6.0 或更高版 • Chrome 2.0 或更高版 • Firefox 3.0 或更高版 • Safari 3.0 或更高版

1.5.2 警告

注意

- 只能使用符合閘道器電源規格的電源供應器。使用超出額定電壓規格的電源是危險的，可能會損壞產品。
- 請勿自行打開或修理外殼。如果產品過熱，請立即關閉電源，並在合格的服務中心進行維修。

1.5.3 發熱表面警示

警告: 金屬外殼的表面溫度可能非常高! 特別是經過長時間的操作後、安裝在沒有空調的密閉機櫃中、或在環境溫度較高的地方。

請勿觸摸發熱表面!!

1.5.4 CE RED 要求的產品資訊

必須在產品使用者手冊中顯示以下產品資訊, 以瞭解最新的 CE RED 要求[2]

(1) 頻帶 & 最大功率

1.a 行動通訊連結的頻帶

頻帶號	工作頻率	最大輸出功率
LTE FDD BAND 1	上傳: 1920-1980 MHz 下載: 2110-2170 MHz	23 ±2.7 dBm
LTE FDD BAND 3	上傳: 1710-1785 MHz 下載: 1805-1880 MHz	
LTE FDD BAND 7	上傳: 2500-2570 MHz 下載: 2620-2690 MHz	
LTE FDD BAND 8	上傳: 880-915 MHz 下載: 925-960 MHz	
LTE FDD BAND 20	上傳: 832-862 MHz 下載: 791-821 MHz	
WCDMA BAND 1	上傳: 1920-1980 MHz 下載: 2110-2170 MHz	24 +1/-3 dBm
WCDMA BAND 8	上傳: 880-915 MHz 下載: 925-960 MHz	
E-GSM	上傳: 880-915 MHz 下載: 925-960 MHz	33 ±2 dBm
DCS	上傳: 1710-1785 MHz 下載: 1805-1880 MHz	30 ±2 dBm

2本節介紹的信息僅適用於歐盟/歐洲自由貿易區 EU/EFTA 地區版本。 對於非 CE/EFTA 版本，請參閱相應的產品規格。

1.b Wi-Fi 連結的頻帶

頻帶	操作頻率	最大輸出功率 (EIRP)
2.4G	2.4 – 2.4835 GHz	100 mW
5G	5.15 – 5.25 GHz	200 mW

(2) 5150 ~ 5350MHz 室內使用環境

本產品配備 IEEE 802.11ac 相容 5GHz 無線射頻模組。根據 RED 要求, 5150 ~ 5350 MHz 頻帶覆蓋的通道僅供室內使用。

(3) 限制的國家清單(用於具有 5GHz 的無線產品)

對於歐盟/歐洲自由貿易區 EU/EFTA, 此產品可以使用在全歐盟成員國和歐洲自由貿易區國家。

AT	BE	BG	CH	CY	CY	DK
DE	EE	EL	ES	FI	FR	HR
HU	IE	IT	LT	LU	LV	MT
NL	NO	PL	PT	RO	SI	SK
SE	TR	UK				

(4) RF 射頻曝露環境

在正常使用條件下, 該產品的天線應至少離使用者身體 20 公分。

1.6 硬體安裝

本章介紹如何安裝和配置硬體

1.6.1 安裝設備

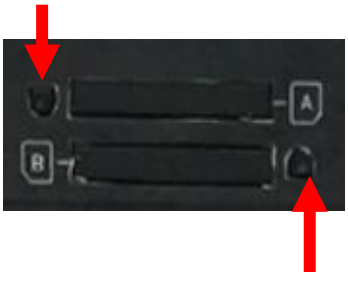
EW50 系列產品可以使用安裝配件 (托架或 DIN Rail 套件) 用來安裝在牆上、水平機架或機櫃內的 DIN Rail 導軌上。安裝配件在出廠時未鎖在產品上。請先將壁掛式套件或 DIN Rail 套件安裝在產品上。

1.6.2 插入 SIM 卡

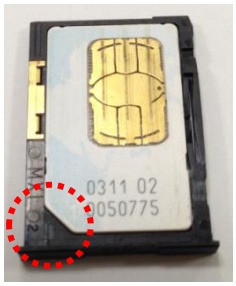
警告: 插入或更換 SIM 卡前, 請確保設備電源已關閉。

SIM 卡插槽位於設備外殼的前端。按下按鈕並拉出 SIM 卡載入盒以安裝或卸下 SIM 卡。將 SIM 卡放入載入盒後, 將 SIM 卡載入盒推入其插槽中。

步驟 1:
按下按鈕解鎖並退出 SIM 卡載入盒。



步驟 2:
將 SIM 卡平穩放入載入盒。



步驟 3:
將 SIM 卡安裝回插槽。

1.6.3 連接電源

EW50 系列產品可通過連接一個或兩個電源到終端連接盒來供電。**支援雙 12 到 48 伏特 DC 直流電源輸入** 。下圖顯示電源端子盒針腳配置。請仔細檢查並連接到正確的電源需求和極性.

雙電源 PWR1 和 PWR2 可用於主要/備援或同步模式, 具體取決於 PWR1 和 PWR2 的電壓。

如果 PWR1 和 PWR2 之間的電壓差大於 5.0 伏 (這是使用兩個不同外部規格的電源的情況, 如 48V 和 24V), 則電源控制電路在主要/備援用電源模式下工作。具有較高電壓的電源被視為主要功率, 另一種為備援電源。通常, 只有主電源供電給閘道器和連接 PoE 設備;只有當主電源出現故障時, 備援用電源才會為閘道器供電並連接 PoE 設備。

如果 PWR1 和 PWR2 之間的電壓差小於 0.5 伏 (這是使用相同外部規範的兩個電源的情況, 如 48V), 則電源控制電路在同步模式下工作。PWR1 和 PWR2 都需要電源, 同時連接 PoE 設備。

請確保外部電源可以提供系統所需的電源量。如果出現故障, 可能會導致電源控制電路切換到同步模式, 從而使 PWR1 和 PWR2 電源同時供電。

1.6.4 安裝電源供應器

電源供應器是選配，不包括在標準包裝中。您必須額外購買或準備外部電源，以供電到閘道器。以下爲工業爲電源安裝範例。

➢ 安裝 AC 交流電源線

電源供應器應使用 100-240 伏 AC 直流, 50/60 赫茲電源輸入線。建議使用 AWG 18 電源線。

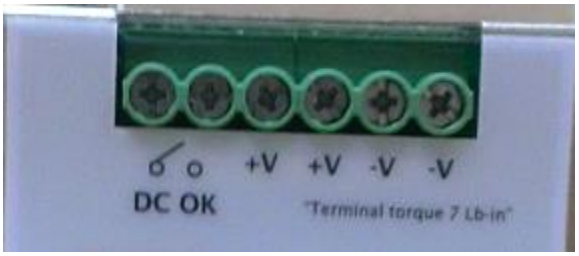
終端腳位編號配置如下所示

Pin No.	Assignment
1	FG ⏚
2	AC/N
3	AC/L

將帶電線、中性線和接地線連接到相應的位置。

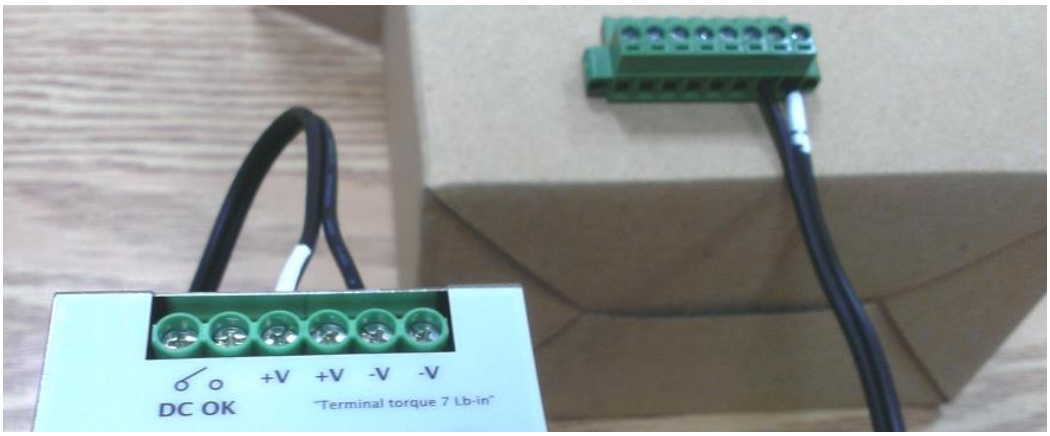
➢ 安裝 DC 直流電源終端盒

電源供應器可由單組或兩組直流電源輸出接點組成。



您可以用電線連接 DC 直流電源和閘道器的終端盒電源針腳, 如下所示。建議使用 AWG 18 電源線。

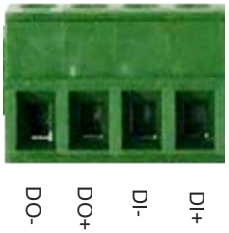
將直流電源線插入 PWR1 或 PWR2。+V 連接到 PWR, 然後-V 連接到 GND 地線。然後, 將終端盒插入閘道器側邊的插槽。



最後，將電源線的插頭連接到插座上。電源供應器將會開啓並為連接的設備提供直流電源。

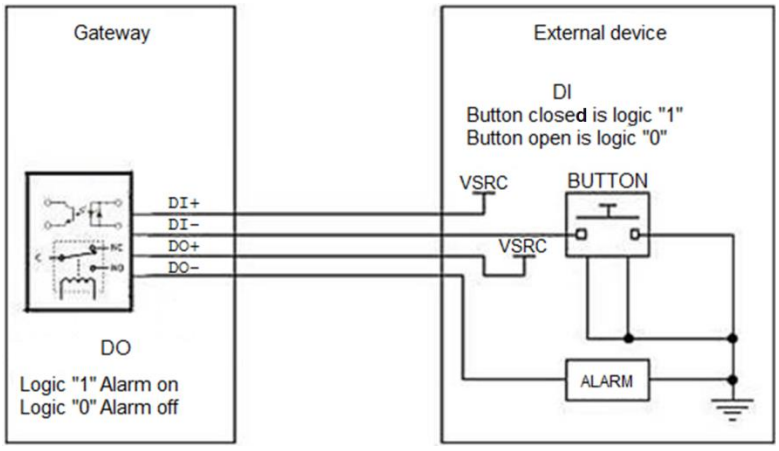
1.6.5 連接 DI/DO 設備

在電源終端盒(Terminal Block)旁邊有一個 DI (digital input 數位輸入) 和一個 DO (digital output 數位輸出) 埠，請參閱以下有關 DI 和 DO 設備連接的規格。



模式	規範	
數位輸入	觸發電壓 (高)	邏輯等級 1: 5 v ~ 30 v
	正常電壓 (低)	邏輯等級 0: 0 v ~ 2 v
數位輸出	電壓 (中繼模式)	取決於外部設備，最大電壓為 30V
	最大電流	1A

連接圖



1.6.6 連接序列設備

EW50 具有用於連接到序列設備的 6 針串口終端盒。使用符合 RS-232/485 的正確針腳配置將序列設備連接到終端盒 (如下所示)。

Pin 1 2 3 4 5 6

	Pin1	Pin2	Pin3	Pin4	Pin5	Pin6
Port	SPort-0			SPort-1		
RS-232	RXD	TXD	GND	GND	RXD	TXD
RS-485	DATA-	DATA+	GND	GND	DATA-	DATA+

1.6.7 連接到網路或 Host 主機

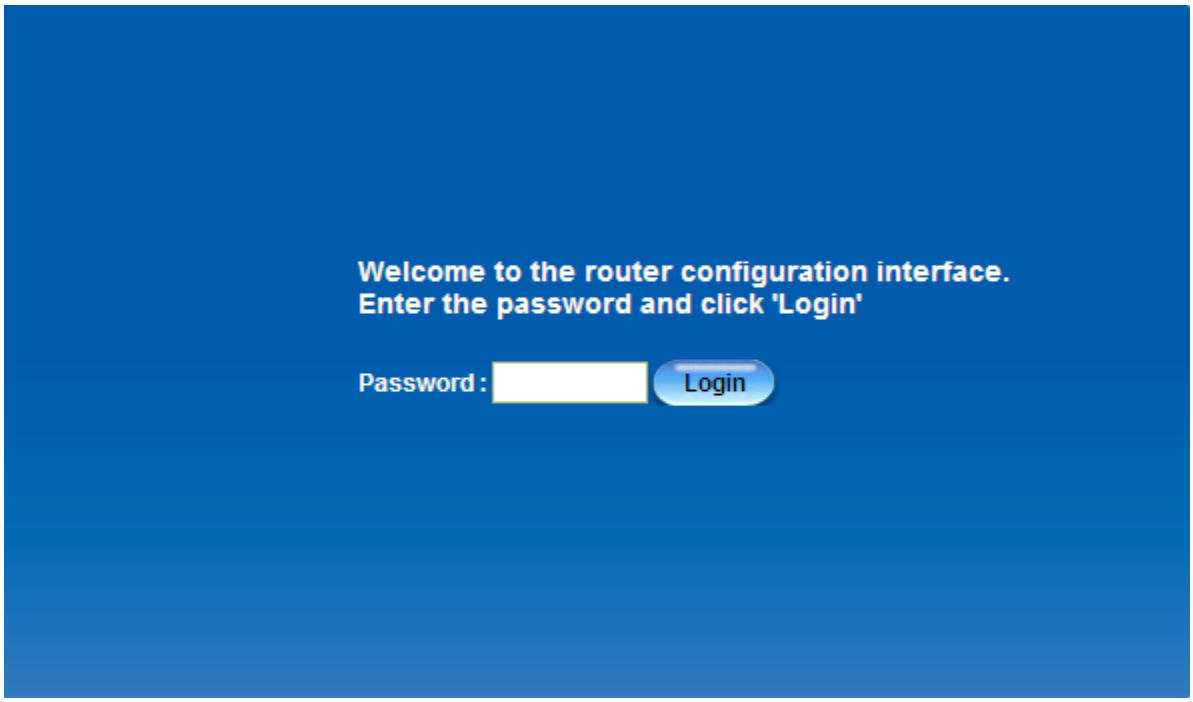
EW50 提供 RJ45 埠以連接 10/100/1000 Mbps 網路。其可以自動檢測網路上的傳送速率並自動進行設定。將一條網路線連接到設備的 RJ45 埠 (LAN), 然後將網路線的另一端插入電腦的網路埠。如此，您可以用 RJ45 網路線連接到 Host 主機 電腦 PC 的網路埠以設定設備。

1.6.8 由網頁介面進行設定

您可以透過網頁介面來設定設備。

IP 地址爲 (**http://192.168.123.254**)[3]

當你看到登入頁面，輸入帳號 ‘**admin**’ , 密碼 ‘**admin**’[4] 並按下 ‘**Login**’ 按鈕。

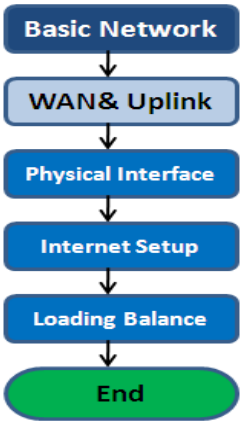


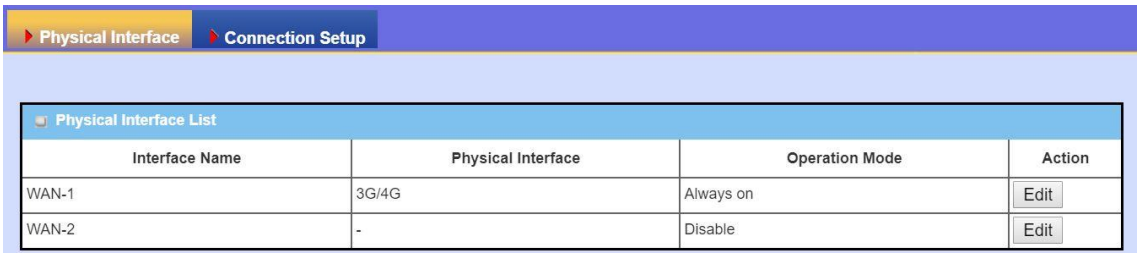
3 該閘道器的預設 LAN IP 地址是 192.168.123.254。 如果您更改過，您將需要使用新的 IP 地址登錄。

4 強烈建議您將預設的登錄密碼修改爲不同密碼。

第 2 章 基本網路

2.1 WAN & Uplink 上傳

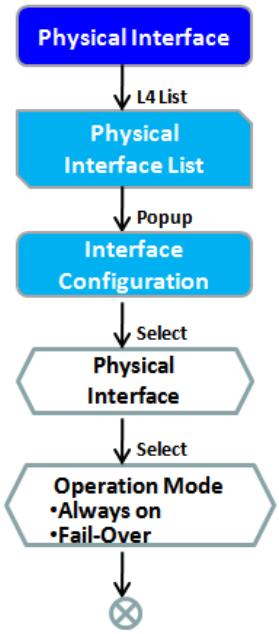


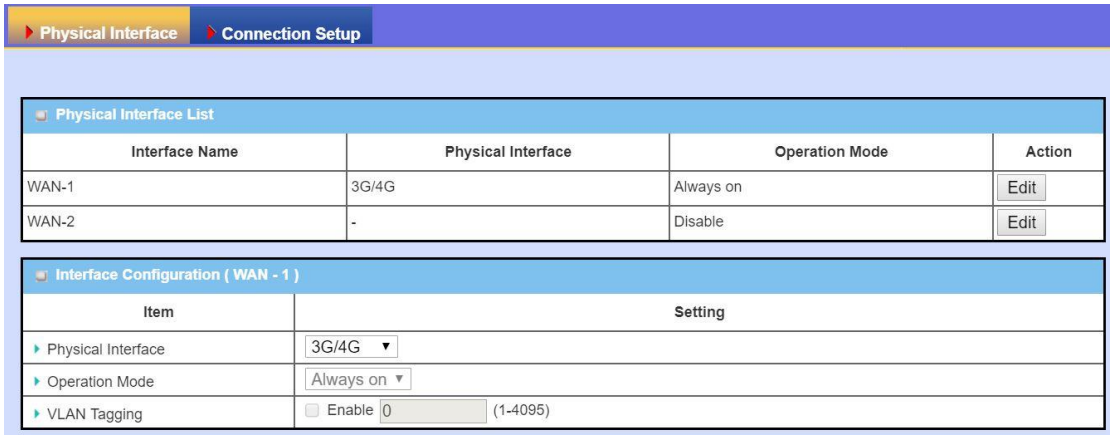


閘道器提供多個 WAN 介面, 允許閘道器 Intranet 網中的客戶端主機通過 ISP 連上網際網路。但世界各地的 ISP 有各種不同的通信協定, 讓閘道器或使用者的設備撥入 ISP, 然後通過不同類型的媒體連結到網際網路。

因此, WAN 連接允許您指定 WAN 網路的實體介面(Physical Interface)、WAN 網路設置 (Connection Setup)和 WAN 網路負載平衡(Load Balance), 以便使內網連接到網際網路。對於每個 WAN 介面, 您必須先指定其實體介面, 然後才能設定將內網連接到 ISP 。由於閘道器具有多個 WAN 介面, 因此可以分配實體介面來參與負載平衡功能。

2.1.1 實體介面





M2M 閘道器通常配置各種 WAN 介面以支援不同的 WAN 連接方案。可以將 WAN 介面一個接一個設定為適合連接網際網路的設置。**參考您型號的規格表以獲得 WAN 介面的規格。**

設定一個 WAN 介面的首先要為 WAN 連接指定該使用哪種類型的連接媒體, 如 "實體介面" 頁面所示。

在 "Physical Interface (實體介面)" 頁面中, 有兩個設定視窗, "Physical Interface List (實體介面清單)" 和 "Interface Configuration (介面設定)"。"Physical Interface List (實體介面清單)" 視窗顯示所有可用的實體介面。在 "Physical Interface List (實體介面清單)" 視窗中按一下介面的 "Edit (編輯)" 按鈕後, 將出現 "Interface Configuration (介面設定)" 視窗。

實體介面:

- **網路 WAN:** 閘道器有一個或多個 RJ45 WAN 埠可設定用來連接 WAN。您可以直接連接外部 DSL 資料機或設置在防火牆後。
- **3G/4G WAN:** 閘道器內建一個 3G/4G 行動式網路作為 WAN 連接。每個行動式 WAN 有 1 或 2 個 SIM 卡插槽。

注意

- 插入或取出 SIM 卡前，請先**關閉**閘道器電源。
- 如果在閘道器運行時插入或拔出 SIM 卡，SIM 卡可能會損壞。

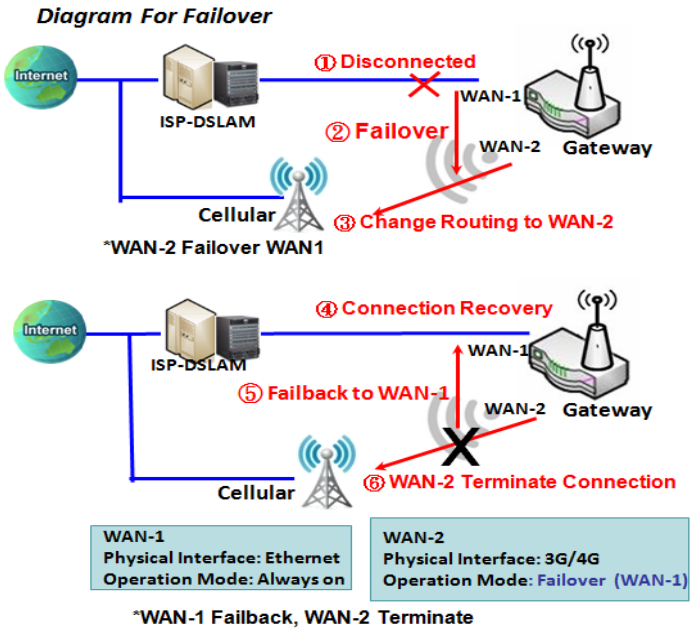
操作模式:

有三種操作模式 “Always on 永遠開啓”， “Failover 容錯移轉”，和 “Disable 關閉” 操作模式設定。

Always on 永遠開啓：設置此 WAN 介面一直處於活動狀態。當兩個或多個 WAN 是已建立"永遠開啓"模式, 傳出資料將通過 WAN 連接並基於負載平衡的策略。

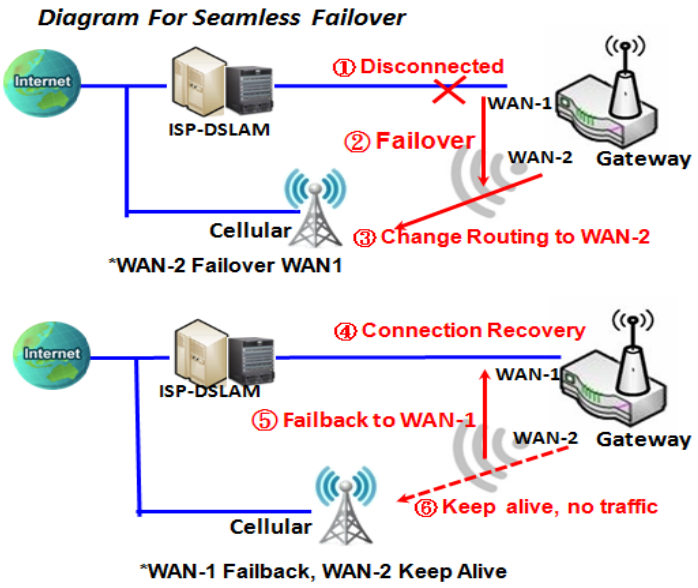
Failover 容錯移轉：

Failover 介面是做爲主要連接的備援連接。這表示將只有當主 WAN 連接斷線時, 備援連接才會啟動以替代主要連接。



如圖中所示, WAN-2 是備援 WAN-1. WAN-1 為操作模式 "永遠開啓" 的主要連接。WAN-2 不會啓動除非 WAN-1 已中斷連線。當 WAN-1 連接恢復時, 它將再次接管資料通訊。此時, WAN-2 連接將被終止。

Seamless Failover 無縫容錯移轉:



此外, 還有在 Failover 操作模式的 "Seamless " 選項。在勾選設定視窗中的 "Seamless " 框啟動無縫選項時, 主要 Primary 連接和 Failover 連接都將在系統重新開機後啟動。但只有主要連接才會執行資料傳輸, 而 Failover 容錯移轉則只是保持連接的存在狀態。一旦失去主連接(Primary), 系統將切換到容錯移轉(Failover)連接。

當 "Seamless" 核取方塊被啟動之後, 它可以允許容錯移轉介面從系統啟動連續連接。在 WAN 介面 不傳輸資料通信的情況下維護連接。這是在容錯移轉(Failover)過程中縮短切換時間，當主要連接已中斷連線, 容錯移轉介面將接手資料轉移任務立即透過只更改資料傳輸路徑到容錯移轉介面。容錯移轉連接的撥號時間因為它已事先連接而減少。

VLAN Tagging 標記

有時, 您的 ISP 需要由閘道器將 VLAN Tag 標記插入到 WAN 資料包中以進行特定 VLAN 傳輸服務。請啟用 VLAN 標記(vlan tagging)並在 WAN 實體介面中設定標記。請注意, 只有網路和 ADSL 實體介面支援此功能。無法適用於只有 3G/4G WAN 的介面資料傳輸。

Physical Interface 實體介面設定

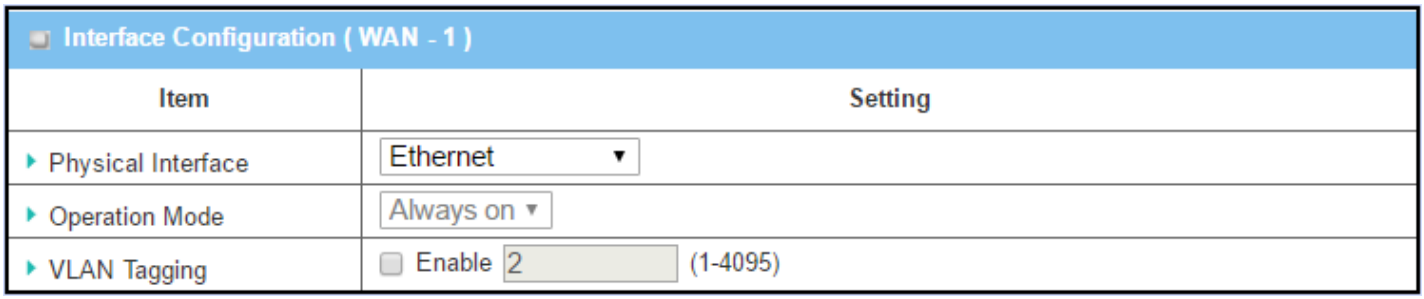
到 Basic Network > WAN > Physical Interface 頁面。

實體介面允許設定實體 WAN 介面和調整 WAN 的行為。
注意: 可用的 WAN 介面數量因型號而異。

Physical Interface List			
Interface Name	Physical Interface	Operation Mode	Action
WAN-1	3G/4G	Always on	Edit
WAN-2	-	Disable	Edit

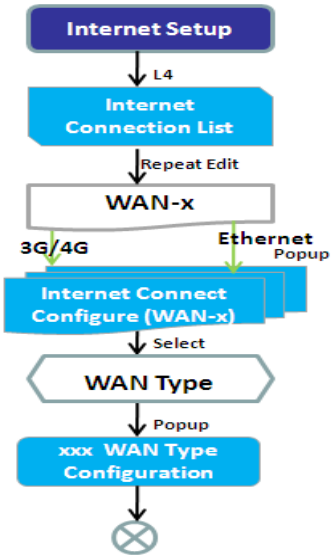
當按下 **Edit (編輯)** 按鈕，會出現 **Interface Configuration (介面設定)** 畫面。這邊用 WAN-1 介面做範例。

Interface Configuration (介面設定):



介面設定		
項目	**設定值**	**描述**
Physical Interface (實體介面)	1. 必要設定 2. WAN-1 是主要介面， 出廠設置為 **Always on (永遠開啓)**。	從可用介面下拉清單中選擇一個預期的介面。 取決於閘道器型號，**Disable(禁用)**和 **Failover(容錯移轉)**選項僅可用於多個 WAN 的閘道器。WAN-2 ~ WAN-4 介面僅可用於多 WAN 的閘道器。
Operation Mode (操作模式)	必要設定	定義介面的操作模式。 選擇**永遠 Always on** 使此 WAN 永遠處於活動狀態。 選擇**禁用 Disable** 禁用此 WAN 介面。 選擇**容錯移轉 Failover**,選擇 WAN 2 為 Failover Operation Mode。當 WAN1 介面為主 WAN 介面連線失敗時會切換到 WAN-2 的連接介面(請參考下列圖示)。 注意: 對於 WAN-1, 只有 **alway on(永遠開啓)**選項可用。
VLAN 標記	可選設定	勾選 **Enable(啟用)** 框可輸入 ISP 提供的標記值。否則取消選擇該選項。 ***範圍值***: 1 ~ 4095. 注意: 此功能無法用於 3G/4G WAN 連線資料傳輸。

2.1.2 Internet Setup (網際網路設定)



Internet Connection List

Interface Name	Physical Interface	Operation Mode	WAN Type	Action
WAN-1	Ethernet	Always on	Dynamic IP	Edit
WAN-2	3G/4G	Always on	3G/4G	Edit

Internet Connection Configuration (WAN - 1)

Item	Setting
WAN Type	Dynamic IP

Dynamic IP WAN Type Configuration

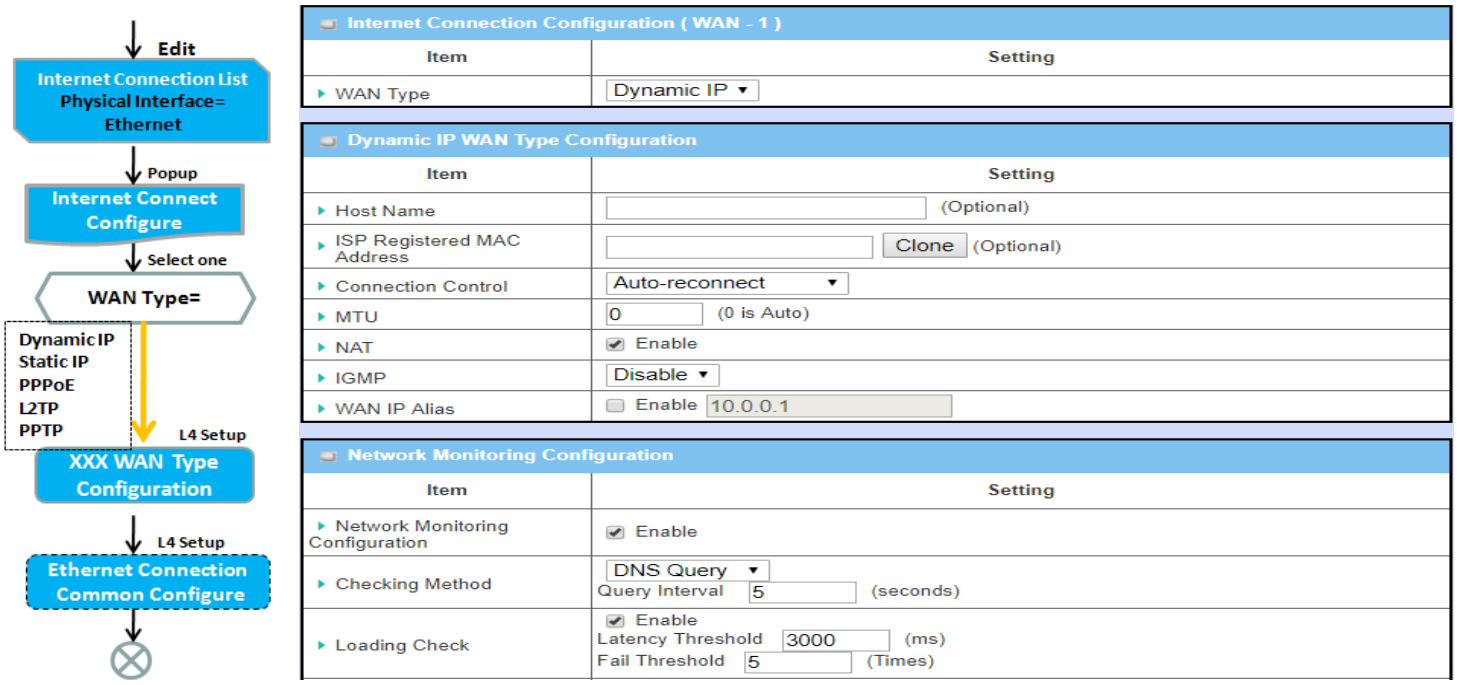
Item	Setting
Host Name	(Optional)
ISP Registered MAC Address	Clone (Optional)
Connection Control	Auto-reconnect
MTU	0 (0 is Auto)
NAT	Enable

為每個 WAN 連接指定實體介面後, 必須設定連接 profile, 以便閘道器內網的所有客戶端主機都可以連接網際網路。

在 "Internet Setup (網際網路設置)" 頁面上有一些設定視窗: "Internet Connection List (網際網路連接清單)"、"Internet Connection Configuration (網際網路連接設定)", "WAN Type Configuration (WAN 類型設定)" 以及每個 WAN 類型的相關設定視窗。關於每個 WAN 介面的網際網路設定, 您必須首先指定其 WAN 類型的實體介面, 然後為該 WAN 類型定義相關的參數設定。

按一下 "Internet Connection List (網際網路連接清單)" 視窗中實體介面的 "Edit (編輯)" 按鈕後, 將顯示 "Internet Connection Configuration (網際網路連接設定)" 視窗, 用以讓您指定將用於該實體介面的 WAN 類型, 使其成為網際網路連接。根據所選的 WAN 類型, 可以在每個相應的設定視窗中設定必要的參數。

Internet Connection List (網際網路連接清單) - WAN 網路



用於區域網介面的 WAN 類型:

Ethernet 是 M2M 閘道器最常見的 WAN 和上傳介面。通常與 xDSL 或有線資料機連接, 您可以設定 WAN 連接。有多種類型 WAN 用來與 ISP 進行連接。

- **Static IP(靜態 IP):** 如果 ISP 提供固定 IP，請選擇此選項。這通常比較昂貴，但對於重要應用要求很重要。
- **Dynamic IP (動態 IP):** DHCP 伺服器為 WAN 分配的 IP 位址每次都不同。這比較便宜, 通常為消費者所使用。
- **PPP over Ethernet (區域網 PPP):** 稱為 PPPoE。此 WAN 類型廣泛用於 ADSL 的連接。每次撥號獲得的 IP 通常是不同的。
- **PPTP:** 此 WAN 類型在一些國家 (如俄羅斯) 很受歡迎.
- **L2TP:** 此 WAN 類型在某些國家 (如以色列) 很受歡迎.

Ethernet WAN 設定

按下 **Edit(編輯)** 按鈕時, 會出現 **"Internet Connection Configuration (網際網路連接設定)"** 畫面。這邊用 WAN-1 介面做範例。

WAN 類型 = Dynamic IP (動態 IP)

Internet Connection Configuration (WAN - 1)	
Item	Setting
WAN Type	Dynamic IP ▾

選擇後, 將出現 " Dynamic IP WAN Type Configuration (動態 IP 地址 WAN 配置)"。項目和設定如下所示:

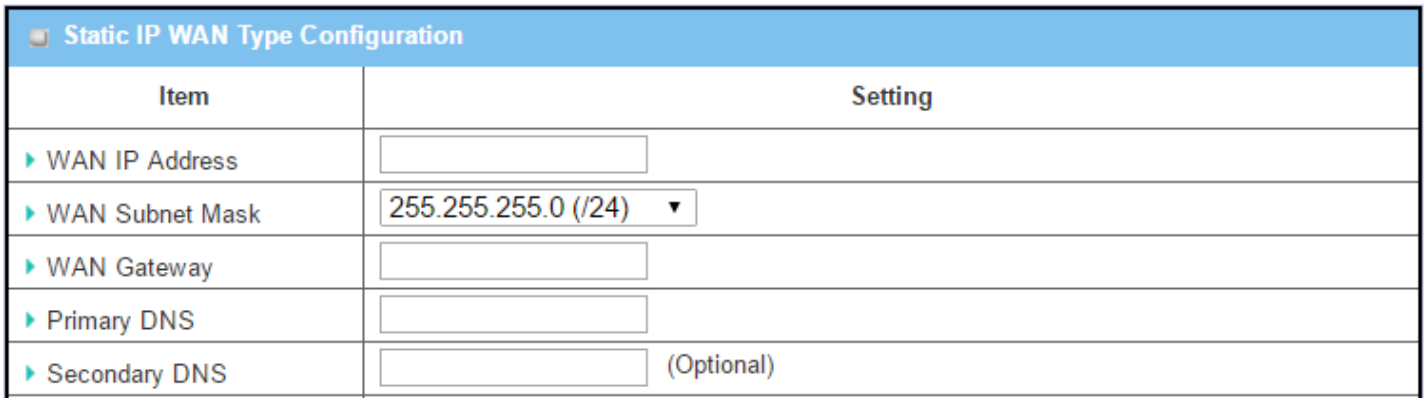
Dynamic IP WAN Type Configuration	
Item	Setting
Host Name	(Optional)
ISP Registered MAC Address	Clone (Optional)

Dynamic IP WAN Type Configuration (動態 IP WAN 類型配置)		
項目	設定值	說明
Host Name (主機名稱)	可選設定	輸入服務提供者提供的主機名稱。
ISP Registered MAC Address (ISP 註冊的 MAC 位址)	可選設定	輸入您已向服務提供者註冊的 MAC 位址。或者按一下 **Clone(複製)**按鈕將 PC 或機器設備 的 MAC 複製到此欄位。 這通常是 PC 的 MAC 位址分配, 讓您連接到網際網路。

WAN 類型= Static IP (靜態 IP)

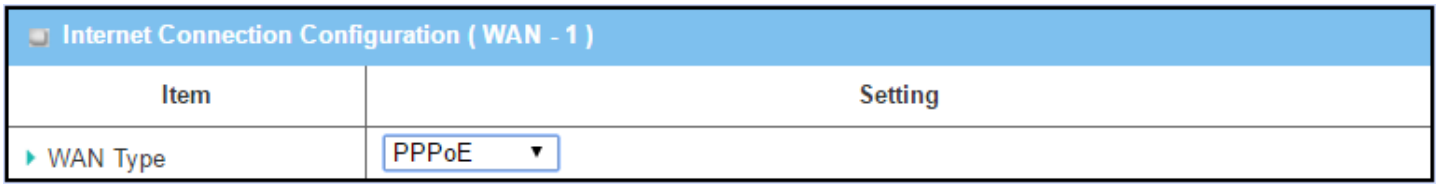
Internet Connection Configuration (WAN - 1)	
Item	Setting
WAN Type	Static IP ▾

選擇後, 將出現 " Static IP WAN Type Configuration (靜態 IP 地址 WAN 類型配置)"。項目和設定如下所示:

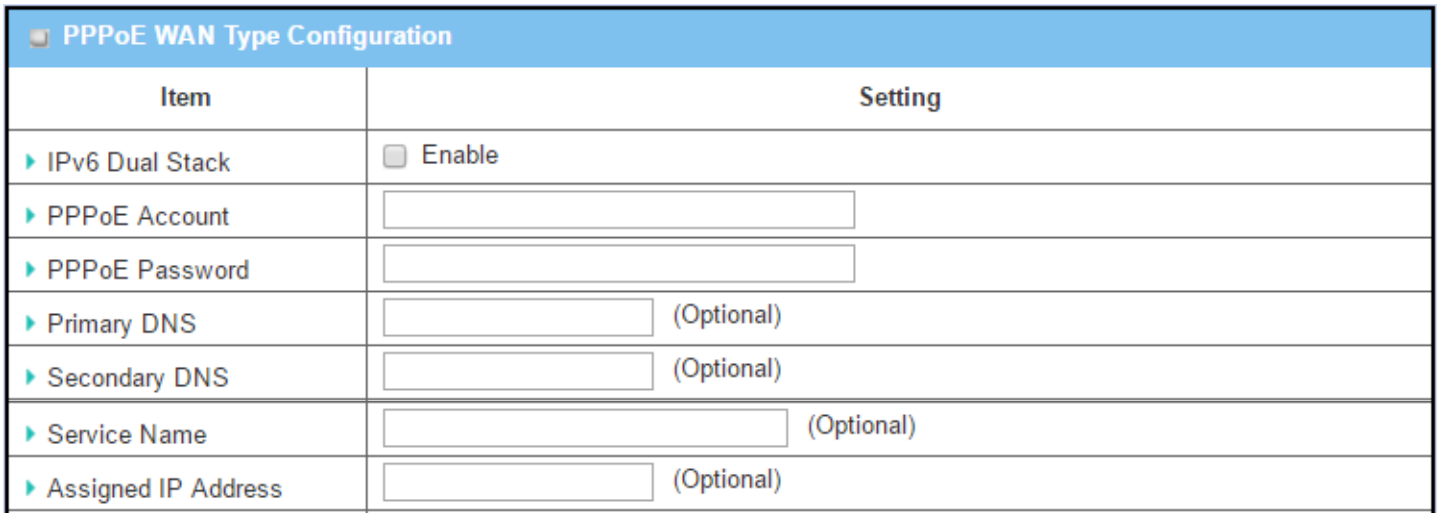


Static IP WAN Type Configuration (靜態 IP WAN 類型配置)		
項目	設定值	說明
WAN IP Address (WAN 網路 IP 位址)	必要設定	輸入服務提供者提供的 WAN IP 位址
WAN Subnet Mask (WAN 子網路遮罩)	必要設定	輸入服務提供者提供的 WAN 子網路遮罩
WAN Gateway (WAN 網路閘道)	必要設定	輸入服務提供者提供的 WAN 閘道 IP 位址
Primary DNS (主 DNS)	必要設定	輸入服務提供者提供的主 WAN DNS IP 位址
Secondary DNS (次 DNS)	可選設定	輸入服務提供者提供的次 WAN DNS IP 位址

WAN 類型= PPPoE



選擇後, 將出現 " PPPoE WAN Type Configuration (PPPoE WAN 類型配置)"。項目和設定如下所示:



PPPoE WAN Type Configuration (PPPoE WAN 類型配置)		
項目	設定值	說明
IPv6 Dual Stack (IPv6 雙協議棧)	1. 可選設定 2. 預設未選	按一下核選方塊啓動 IPv6 雙協議棧功能。
PPPoE Account (PPPoE 帳戶)	必要設定	輸入您的服務供應商提供的 PPPoE 用戶名。
PPPoE Password (PPPoE 密碼)	必要設定	輸入您的服務供應商提供的 PPPoE 密碼。
Primary DNS (主 DNS)	可選設定	輸入主 DNS 的 IP 地址。
Secondary DNS (次 DNS)	可選設定	輸入次 DNS 的 IP 地址。
Service Name (伺服器名稱)	可選設定	輸入伺服器名稱，如果您的 ISP 有要求。
Assigned IP Address (分配的 IP 位址)	可選設定	輸入您的服務供應商分配的 IP 地址。

WAN 類型= PPTP

Internet Connection Configuration (WAN - 1)	
Item	Setting
WAN Type	PPTP ▼

選擇後, 將出現 " PPTP WAN Type Configuration (PPTP WAN 類型配置)"。項目和設定如下所示:

PPTP WAN Type Configuration	
Item	Setting
IP Mode	Dynamic IP Address ▼
Server IP Address / Name	
PPTP Account	
PPTP Password	
Connection ID	(Optional)
MPPE	Enable

PPTP WAN Type Configuration (PPTP WAN 類型配置)		
項目	設定值	說明
IP Mode (IP 模式)	必要設定	當 PPTP 網路連接選擇靜態或動態 IP 位址。 ● 當選擇 **Static IP Address(靜態 IP 位址)**時, 您需要輸入 **WAN IP Address (WAN IP 位址)**、 **WAN Subnet Mask (WAN 子網路遮罩)**、和 **WAN Gateway (WAN 閘道)**. ■ **WAN IP Address (WAN IP 位址)**(必要設定)：輸入服務供應商提供的 WAN IP 位址. ■ **WAN Subnet Mask (WAN 子網路遮罩)**(必要設定)：輸入服務供應商提供的 WAN 子網路遮罩. ■ **WAN Gateway (WAN 閘道)**(必要設定)： 輸入服務供應商提供的 WAN 閘道 IP 位址. ● 當選擇 **Dynamic IP(動態 IP)** 時, 不需要上述設定。
Server IP Address/Name (伺服器 IP 位址/名稱)	必要設定	輸入 PPTP 伺服器名稱或 IP 位址。
PPTP Account	必要設定	輸入服務供應商提供的 PPTP 使用者名。

(PPTP 帳戶)		
PPTP Password (PPTP 密碼)	必要設定	輸入服務供應商提供的 PPTP 連接密碼。
Connection ID (連接 ID)	可選設定	輸入標識 PPTP 連接的名稱。
MPPE	可選設定	選擇 **Enable(啟用)** 可為 PPTP 連接啟用 MPPE (Microsoft Point-to-Point Encryption , Microsoft 點對點加密) 安全性。

WAN 類型= L2TP

Internet Connection Configuration (WAN - 1)	
Item	Setting
WAN Type	L2TP ▼

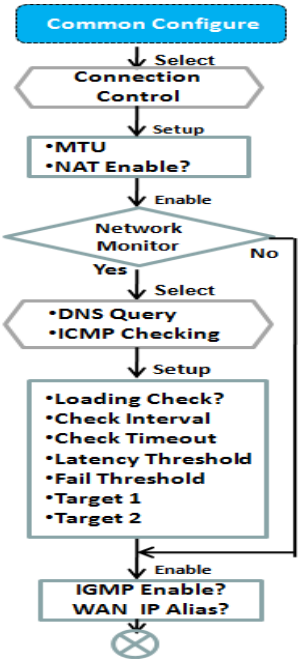
選擇後, 將出現 " L2TP WAN Type Configuration (L2TP WAN 類型配置)"。項目和設定如下所示:

L2TP WAN Type Configuration	
Item	Setting
IP Mode	Dynamic IP Address ▼
Server IP Address / Name	
L2TP Account	
L2TP Password	
Service Port	User-defined ▼ 1702
MPPE	Enable

L2TP WAN Type Configuration (L2TP WAN 類型配置)		
項目	**設定值**	**說明**
IP Mode (IP 模式)	必要設定	當 L2TP 網路連接選擇靜態或動態 IP 位址。 ● 當選擇 **Static IP Address(靜態 IP 位址)**時, 您需要輸入 **WAN IP Address (WAN IP 位址)**、 **WAN Subnet Mask (WAN 子網路遮罩)**、和 **WAN Gateway (WAN 閘道)**. ■ **WAN IP Address (WAN IP 位址)**(必要設定)：輸入服務供應商提供的 WAN IP 位址. ■ **WAN Subnet Mask (WAN 子網路遮罩)**(必要設定)：輸入服務供應商提供的 WAN 子網路遮罩. ■ **WAN Gateway (WAN 閘道)**(必要設定)： 輸入服務供應商提供的 WAN 閘道 IP 位址. ● 當選擇 **Dynamic IP(動態 IP)** 時, 不需要上述設定。
Server IP Address/Name (伺服器 IP 位址/名稱)	必要設定	輸入 L2TP 伺服器名稱或 IP 位址。
L2TP Account (L2TP	必要設定	輸入 L2TP 服務供應商提供的使用者名稱。

帳戶)		
L2TP Password (L2TP 密碼)	必要設定	輸入 L2TP 服務供應商提供的密碼。
Service Port (服務埠)	必要設定	輸入網路服務的服務埠。 有三種選擇: ● **Auto (自動):** 埠將被自動分配. ● **1701 (用於 Cisco)** : 將服務埠設置為 1701 埠以連接到 CISCO 伺服器。 ● **User-defined (使用者定義的)**: 輸入服務供應商提供的服務埠。
MPPE	可選設定	選擇 **Enable(啟用)** 可為 PPTP 連接啟用 MPPE (Microsoft Point-to-Point Encryption , Microsoft 點對點加密) 安全性。

區域網連接通用配置

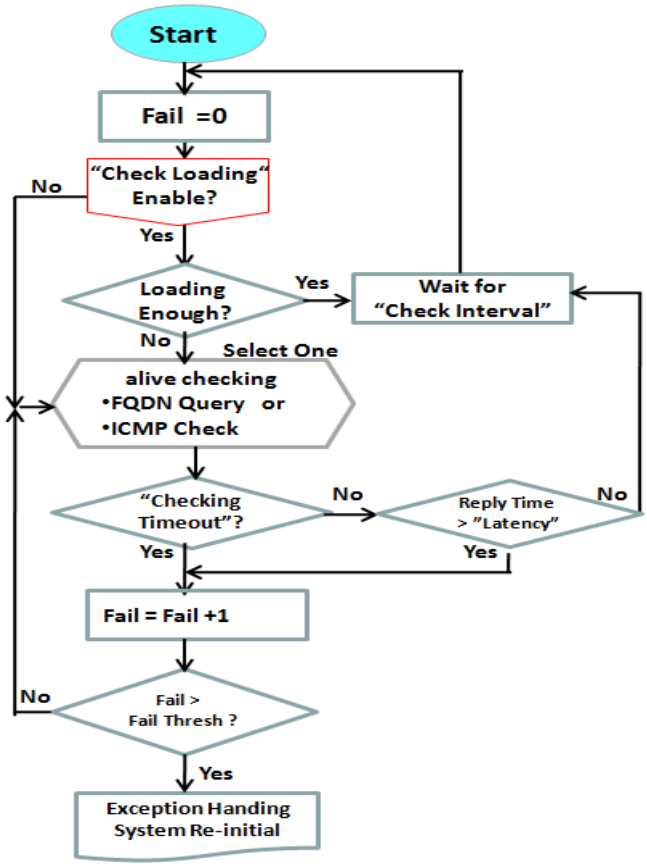


Connection Control	Auto-reconnect
MTU	0 (0 is Auto)
NAT	Enable
IGMP	Disable
WAN IP Alias	Enable 10.0.0.1

Network Monitoring Configuration

Item	Setting
Network Monitoring Configuration	Enable
Checking Method	DNS Query Query Interval 5 (seconds)
Loading Check	Enable Latency Threshold 3000 (ms) Fail Threshold 5 (Times)
Target1	DNS1
Target2	None

Network Monitoring Configuration(網路監控)



當需要連續監視連接狀態時，使用“ICMP 檢查”和“FQDN 查詢”。當連接流量較大時，檢查封包會浪費頻寬，回應報告的反應時間也可能增加。為了防止“網路監控”工作異常，啟用“Checking Loading(檢查負荷)”選項將在高流量時停止檢查連線。它會等待另一個“檢查間隔”，然後再次檢查負荷。

當您進行“網路監控”時，如果回复時間長於“延遲”或無回應時間超過“檢查超時”，則“失敗”計數將會增加。如果連續且“失敗”計數大於設定的“失敗閾值”，則閘道器將執行異常處理程序並再次重新初始化連接。否則，網路監視過程將重新啟動。

設定 “Ethernet Common Configuration (區域網通用配置)”

Ethernet WAN Common Configuration (區域網通用配置)		
項目	**設定值**	**說明**
MTU	1. 必要設定 2. **Auto(0)** 爲預設設定 3. 手動設定範圍 1200~1500	**MTU** 指的是最大傳輸單元，它指定允許網路傳輸的最大資料封包大小。 當設置為 **Auto** (值 "0") 時, 路由器將選擇最佳的 MTU 以最佳化網路連線性能。
NAT	1. 可選設定 2. NAT 預設設定爲啓動	在 WAN 連線上啟用 NAT (Network Address Translation 網路位址轉譯)。取消選擇該選項以禁用 NAT。

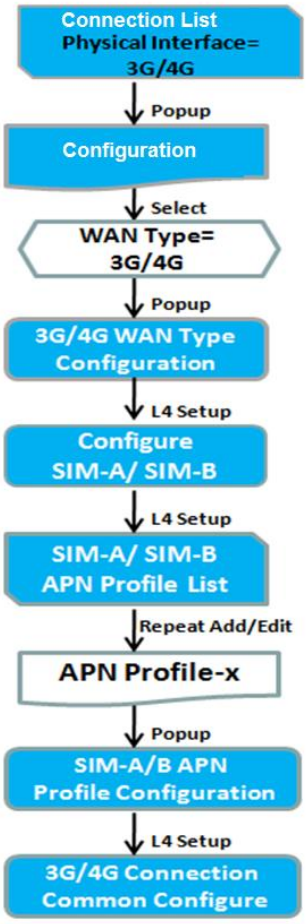
Network Monitoring (網路監控)	1. 可選設定
	2. 預設爲啓動
		當啟用網路監控功能時, 閘道器將使用 DNS 查詢或 ICMP 定期檢查網路 連接狀態.
		• 選擇 **DNS Query (DNS 查詢)** 或 **ICMP Checking (ICMP 檢查)** 以檢測 WAN 連結。通過 **DNS 查詢**，系統透過 DNS 查詢資料封包發送到目標 1 和目標 2 中指定的目標來檢查連線。透過 **ICMP 檢查**，系統將透過向目標 1 和目標 2 中指定的目標發送 ICMP 請求資料封包來檢查連線。
		• **Loading Check(負荷檢查)**
		  ■ 啟用負荷檢查允許路由器在 WAN 頻寬完全佔用時忽略未回復的 DNS 查詢或 ICMP 請求。這是為了防止錯誤的斷線狀態。
		• **Check Interval(檢查間隔)** 定義兩個 DNS 查詢或 ICMP 檢查資料封包之間的傳輸間隔。
		• **Check Timeout(檢查超時)** 定義每個 DNS 查詢/ICMP 的超時時間。
		• **Latency Threshold (延隔時間閾值)** 定義回應時間的公差閾值。
		• **Fail Threshold (失敗閾值)** 指定在路由器識別 WAN 斷線狀態之前檢測到的斷線狀態。在確認斷線之前， 輸入多個檢測斷線時間為閾值。
		• **Target1 目標 1(DNS1 爲預設設定)** 指定發送 DNS 查詢/ICMP 請求的第一個目標。
		  ■ **DNS1** : 將主 DNS 設置為目標。
		  ■ **DNS2** : 將次 DNS 設置為目標。
		  ■ **Gateway(閘道)**: 將目前閘道設置為目標。
		  ■ **Other Host(其他主機)**: 輸入要成為目標的 IP 位址。

		• **Target2 (None 爲預設設定)** 指定發送 DNS 查詢/ICMP 請求的第二個目標。 ■ **None(無)**: 禁用 **Target2** ■ **DNS1** : 將主 DNS 設置為目標。 ■ **DNS2** : 將次 DNS 設置為目標。 ■ **Gateway(閘道)**: 將目前閘道設置為目標。 ■ **Other Host(其他主機)**: 輸入要成為目標的 IP 位址。
WAN IP Alias (別名)	1. 可選設定 2. 預設爲未勾選	啟用 **WAN IP Alias (別名)**, 然後輸入服務供應商提供的 IP 位址。 **WAN IP Alias(別名)** 由路由器使用, 並被視為第二組 WAN IP, 以便為 LAN 網路提供雙 WAN IP 位址。
Save (保存) (保存)	*無*	按一下 **Save (保存)**以保存設定。
Undo (還原) (還原)	*無*	按一下 **Undo (還原)**取消設定。

Network Monitoring Configuration (網路監視配置) 項目	設定值	說明
Network Monitoring Configuration (網路監視配置)	1. 可選設定 2. 預設爲未勾選	勾選 **Enable** 方框以啟動網路監視功能。
Checking Method (檢查方法)	1. 可選設定 2. 預設爲 **DNS Query (DNS 查詢)**	選擇 **DNS Query (DNS 查詢)** 或 **ICMP Checking (ICMP 檢查)**以檢測 WAN 連結。通過 **DNS 查詢**，系統透過 DNS 查詢資料封包發送到目標 1 和目標 2 中指定的目標來檢查連線。透過 **ICMP 檢查**，系統將透過向目標 1 和目標 2 中指定的目標發送 ICMP 請求資料封包來檢查連線。 **Query Interval (查詢間隔)**定義兩個 DNS 查詢或 ICMP 檢查資料包之間的傳輸間隔.
Loading Check (負荷檢查)	1. 可選設定 2. 預設爲未勾選	勾選 **Enable** 方框啟用負荷檢查允許路由器在 WAN 頻寬完全佔用時忽略未回復的 DNS 查詢或 ICMP 請求。這是為了防止錯誤的斷線狀態。 **Latency Threshold (延隔時間閾值)** 定義回應時間的公差閾值。 **Fail Threshold (失敗閾值)** 指定在路由器識別 WAN 斷線狀態之前檢測到的斷線狀態。在確認斷線之前， 輸入多個檢測斷線時間為閾值。
Target 1 (目標 1)	1. 可選設定 2. 預設爲 **DNS1**	**Target1 specifies** 指定**目標 1** 指定發送 DNS 查詢/ICMP 請求的第一個目標。

		DNS1：將主 DNS 設置為目標。 **DNS2**：將次 DNS 設置為目標。 **Gateway(閘道)**: 將目前閘道設置為目標。 **Other Host(其他主機)**: 輸入要成為目標的 IP 位址。
Target 2 (目標 2)	1. 可選設定 2. 預設爲 **None (無)**	**Target2 specifies** 指定**目標 2** 指定發送 DNS 查詢/ICMP 請求的第二個目標。 **DNS1**：將主 DNS 設置為目標。 **DNS2**：將次 DNS 設置為目標。 **Gateway(閘道)**: 將目前閘道設置為目標。 **Other Host(其他主機)**: 輸入要成為目標的 IP 位址
Save (保存) (保存)	*無*	按一下 **Save (保存)**以保存設定。
Undo (還原) (還原)	*無*	按一下 **Undo (還原)**取消設定。

Internet Connection (網際網路連接) – 3G/4G WAN



Internet Connection Configuration (WAN - 2)

Item	Setting
WAN Type	3G/4G

3G/4G WAN Type Configuration

Item	Setting
Preferred SIM Card	SIM-A First ▾ Failback : Enable

Connection with SIM-A Card

Item	Setting
Network Type	Auto

SIM-A APN Profile List Add Delete

ID	Profile Name	APN	Account	Password	Authentication	Priority	Enable	Actions

SIM-A APN Profile Configuration

Item	Setting
Profile Name	Profile-1

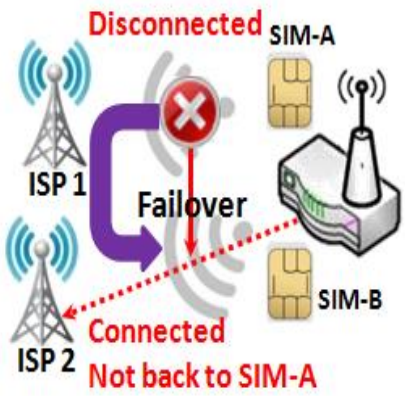
3G/4G Connection Common Configuration

Item	Setting
Connection Control	Auto-reconnect
Time Schedule	(0) Always
MTU	0 (0 is Auto)
NAT	Enable

優先 SIM 卡 - 雙卡容錯移轉 Dual SIM Failover

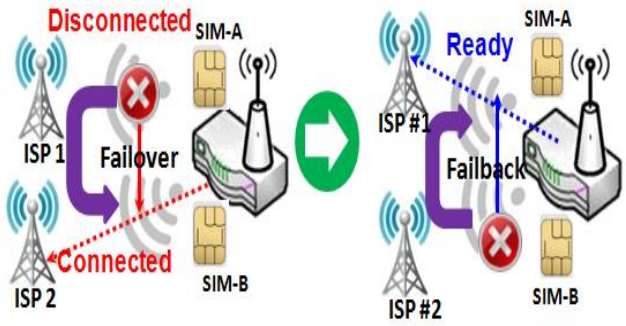
對於 3G/4G 嵌入式設備來說，一個嵌入式行動通訊模組只能建立一個 WAN 埠。該設備具有用於特殊容錯移轉(Failover)機制的一個雙 SIM 卡模組。它被稱為雙 SIM Failover 容錯移轉。此功能在位置變動時可用於切換 ISP。在 "雙 SIM 容錯移轉" 中, 有各種使用方案, 包括 "SIM-A First (SIM-A 優先)"、"SIM-B First (SIM-B 優先)" 和 "Failback (容錯回復)" 啟用與否, 以及 "SIM-A Only (僅限 SIM-A)" 和 "SIM-B Only (僅限 SIM-B)"。

SIM-A / SIM-B first without enable Failback 無容錯回復 SIM-A / SIM-B 優先



在預設"SIM-A 優先" 方案適用於連接到行動通訊 ISP 進行資料傳輸。在 "SIM-A 優先" 或 "SIM-B 優先" 的情況下, 閘道器將嘗試透過使用 SIM-A 卡或 SIM-B 卡來連線到網路。如果斷線, 閘道器將自動切換為使用其他 SIM 卡作為備用, 不會切換回使用原來的 SIM 卡, 除非目前的 SIM 卡也斷線 ，即 SIM-A 和 SIM-B 是反覆相互使用的, 但在目前連線仍然存在時, 任何一種方式都將繼續傳輸資料。

SIM-A / SIM-B first with Failback enable 有容錯回復 SIM-A / SIM-B 優先



啟用容錯回復選項後, "SIM-A 優先" 方案於斷線時, 閘道系統將切換到使用 SIM-B。當 SIM-A 恢復連線時, 它會切換回原來使用的 SIM 卡。

配置 3G/4G WAN 設定

當按下 **Edit(編輯)** 按鈕時，將出現 **Internet Connection Configuration** (網路連接設定) 和 **3G/4G WAN Configuration** (3G/4G WAN 設定) 畫面。 本例中使用 WAN-1 埠。

Internet Connection Configuration (WAN - 1)

Item	Setting
WAN Type	3G/4G

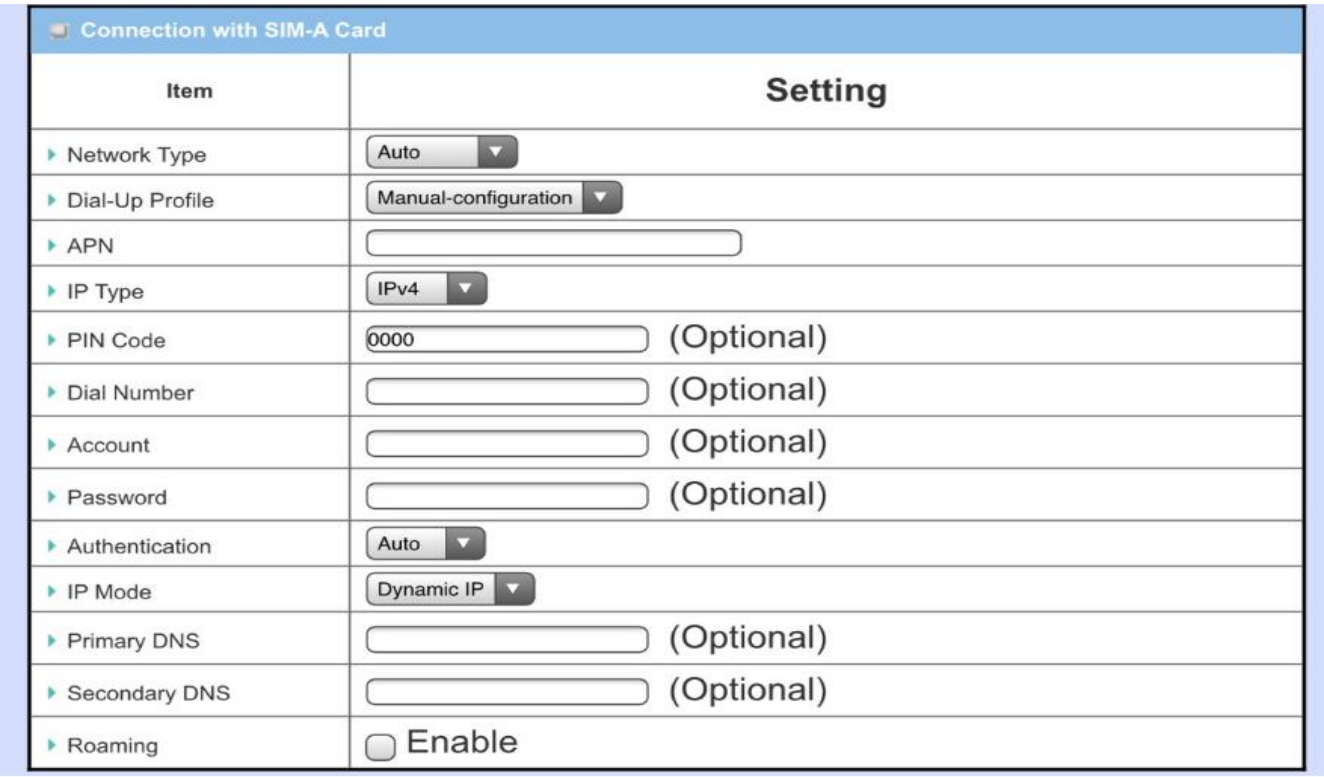
3G/4G WAN Type Configuration

Item	Setting
Preferred SIM Card	SIM-A First Failback : Enable
Auto Flight Mode	Enable

3G/4G Connection Configuration (3G/4G 連線設定)		
項目	**設定值**	**說明**
WAN Type (WAN 類型)	1. 必要設定 2. 預設爲 **3G/4G**	從下拉清單中, 選擇 3G/4G WAN 連接的網路連接方法。只有 3G/4G 可用。
Preferred SIM Card (優先的 SIM 卡)	1. 必要設定 2. 預設選擇 **SIM-A First** 3. 預設未勾選 **Failback**	選擇用於連接的 SIM 卡。 當 **SIM-A First (SIM-A 優先)** 或 **SIM-B First (SIM-B 優先)**被勾選時, 表示連線是優先使用 SIM A/SIM B 建立的。如果連線失敗，系統將切換到其他 SIM 卡， 並嘗試再次撥號，直到連接接通。 如果勾選了僅 **SIM-A only (僅限 SIM-A)** 或 **SIM-B only (僅限 SIM-B)** , 系統將嘗試僅使用所選的 SIM 卡撥號。 當勾選 **Failback(容錯回復)**時，意味著如果未使用所選的主 SIM 卡撥號連線，系統將嘗試切回到主 SIM 卡建立連接。 **註_1**：對於具有單個 SIM 設計的產品, 只有 **SIM-A Only** 選項可用。 **註_2**：**Failback** 只有在 **SIM-A First** 個或 **SIM-B First** 被勾選時才可用。

設定 SIM-A / SIM-B 卡

在此, 您可以根據所需要的行動通訊連接設定配置。



註_1: SIM-B 卡的設定遵循和 SIM-A 卡相同的規則，這裡我們 SIM-A 列表作為例子。

註_2: 只有在 **SIM-A First (SIM-A 優先)** 或 **SIM-B First(SIM-B 優先)**被勾選時, **Connection with SIM-A Card (用 SIM-A 卡連線)** 和 **Connection with SIM-B Card (用 SIM-B 卡連線)** 才會彈出, 否則只會彈出一個。

Connection with SIM-A/-B Card (用 SIM-A/-B 卡連線)		
項目	**設定值**	**說明**
Network Type (網路類型)	1. 必要設定 2. 預設選擇 **Auto (自動)**	選擇 **Auto(自動)**自動註冊網路, 而不考慮網路類型。 選擇 **2G Only (僅 2G)** 僅註冊 2G 網路。 選擇 **2G Prefer (2G 優先)** 如果可以，優先註冊 2G 網路。 選擇 **3G Only (僅 3G)** 僅註冊 3G 網路。 選擇 **3G Prefer (3G 優先)** 如果可以，優先註冊 3G 網路。 選擇 **LTE Only (僅 LTE)** 僅註冊 LTE 網路。 **注意:** 選項可能因型號而異。
Dial-Up Profile (撥接設定檔)	1. 必要設定 2. 預設選擇 **Manual-**	指定您的 3G/4G 網路的撥號配設定檔案類型。可以爲 **Manual-configuration(手動設定)**、 **APN Profile List (APN 配置檔案清單)** 或

	configuration (手動設定)	**Auto-detection(自動偵測)**。 選擇 **Manual-configuration(手動設定)** 可將 **APN** (Access Point Name 登入點名稱)、**Dial Number(撥號號碼)**、**Account (帳戶)**和 **Password(密碼)**設置為您的營運商提供的內容。 選擇 **APN Profile List (APN 配置檔案清單)**, 將多個設定檔設定為依序撥號， 直到建立連線為止。將彈出一個新欄位。有關詳細資訊，請轉到 **Basic Network > WAN & Uplink > Internet Setup > SIM-A APN Profile List**。 選擇自動偵測可在撥號時自動顯示所需的所有設定，方法是將 SIM 卡的 IMSI 與製造商資料庫中列出的記錄進行比對。 **註_1:** 強烈建議選擇 **Manual(手動)**或 **APN Profile List (APN 配置檔案清單)**指定用戶的網路。您的 ISP 應提供此類網路設定。 **註_2:** 如果選擇 **Auto-detection(自動偵測)**，將可能會連接到不正確的網路, 或者無法為 ISP 找到有效的 APN。
APN	1. 必要設定 2. 字串格式: 任意文字	輸入要用於建立連接的 **APN** 。 如果您選擇 **Manual-configuration(手動設定)**作為撥號設定檔方案則必須選擇此設定。
PIN code (PIN 碼)	1. 可選設定 2. 字串格式: 整數	如果需要解鎖 SIM 卡, 請輸入 PIN (Personal Identification Numbe 個人識別碼) 碼。
Dial Number (撥號號碼), **Account (帳號),** **Password (密碼)**	1. 可選設定 2. 字串格式: 任意文字	如果 ISP 提供了這些設置, 請輸入可選的**撥號號碼**、**帳號**和**密碼**。 注意: 這些設置僅在選擇**手動設定**時顯示。
Authentication (認證)	1. 必要設定 2. 預設選擇 **Auto (自動)**	選擇 **PAP** (Password Authentication Protocol 密碼認證協議)並使用此協議與營運商的服務器進行認證。 選擇 **CHAP** (Challenge Handshake Authentication Protocol 質詢握手認證協議)並使用此協議與營運商的服務器進行認證。 選擇 **Auto(自動)**時，表示系統將使用 PAP 或 CHAP 向服務器進行身份驗證。
IP Mode (IP 模式)	1. 必要設定 2. 預設選擇 **Dynamic IP** (動態IP)。	當選擇 **Dynamic IP (動態 IP)**時，意味著系統將從營運商的伺服器獲取所有 IP 配置並直接設置到設備。 如果您有由營運商提供的特定應用程式，並且希望自己設置 IP 配置,

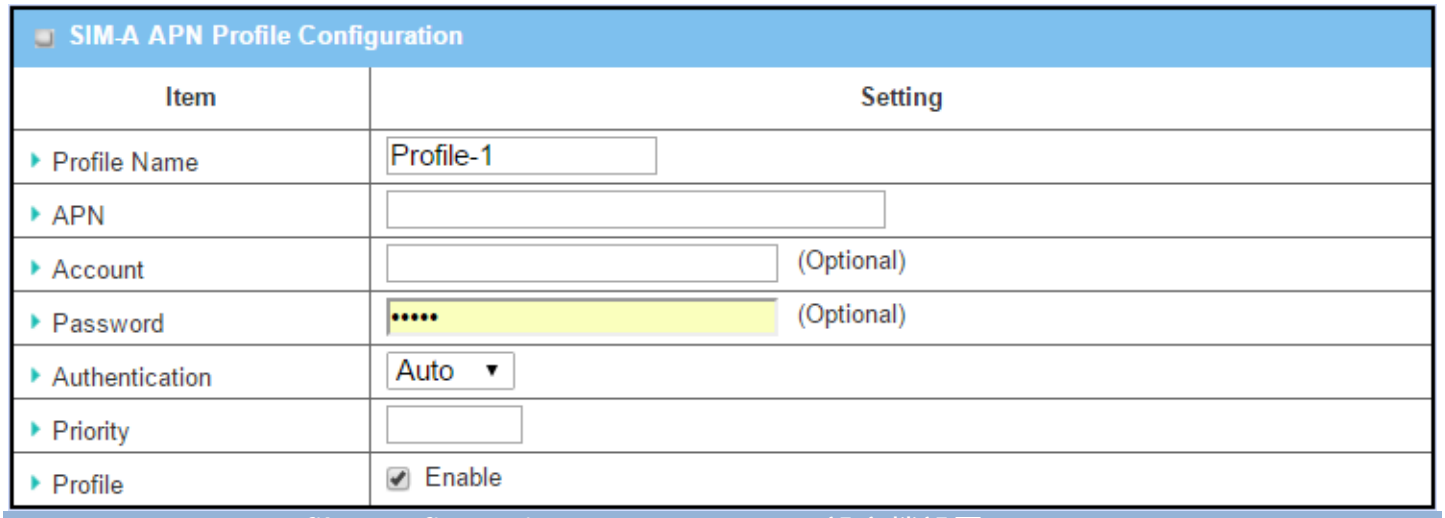
		則可以切換到 **Static IP(靜態 IP)**模式, 並填寫所需的所有參數, 如 IP 位址、子網路遮罩和閘道。 **注意: IP Subnet Mask(子網路遮罩)**是必要設定。請確認您的設定正確。
Primary DNS (主 DNS)	1. 可選設定 2. 字串格式: IP 位址 (IPv4 類型)	輸入 IP 位址以更改主 DNS (Domain Name Server 網域名稱伺服器) 設置。如果未填寫, 伺服器位址由營運商在撥號時提供。
Secondary DNS (次 DNS)	1. 可選設定 2. 字串格式: IP 位址 (IPv4 類型)	輸入 IP 位址以更改次 DNS (Domain Name Server 網域名稱伺服器) 設置。如果未填寫, 伺服器位址由營運商在撥號時提供。
Roaming (漫遊)	預設未勾選	勾選該框以建立連線，即使註冊狀態為漫遊，而不是在家用網路中。 **注釋**: 如果連線設定為漫遊, 則可能會產生附加費用。

建立/編輯 SIM-A / SIM-B APN Profile List (設定檔清單)

您可以為連線添加新的 APN 設定檔, 或者修改新增的 APN 設定檔的內容。僅當您選擇 **Dial-Up Profile (撥號設定檔)**作為 **APN Profile List (APN 設定檔清單)**時才可用。

這將列出您建立的所有 APN 設定檔, 從而便於檢查和修改。僅當您選擇 Dial-Up Profile(撥號設定檔)作為 APN Profile List (APN 設定檔清單)時才可用。

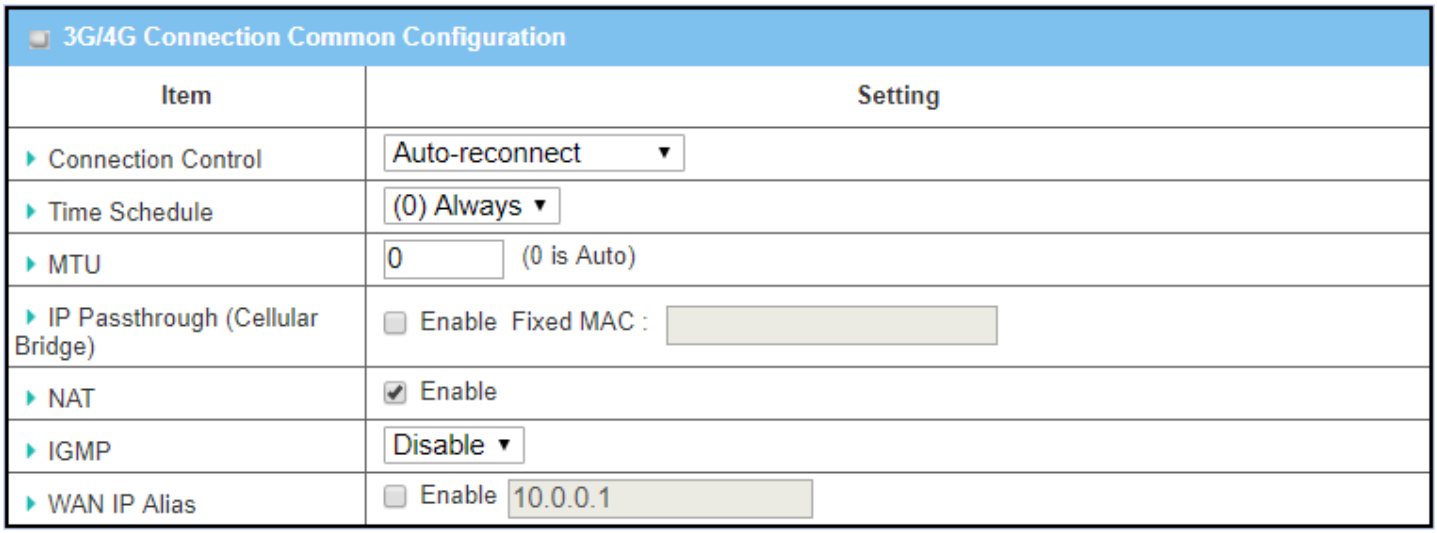
當按下 Add 按鈕時, 將顯示 APN Profile List (APN 設定檔清單)畫面。



SIM-A/-B APN Profile Configuration (SIM-A/-B APN 設定檔設置)		
項目	**設定值**	**說明**
Profile Name (設定檔名稱)	1. **Profile-x** 爲預設 2. 字串格式: 任意文字	輸入要為該設定檔描述的設定檔名稱。
APN	字串格式: 任意文字	輸入要用於建立連線的 APN 。
Account (帳戶)	字串格式: 任意文字	輸入要用於身份驗證的帳戶名稱。 ***範圍值***: 0 ~ 53 個字元。
Password (密碼)	字串格式: 任意文字	輸入要用於身份驗證的密碼。
Authentication (認證)	1. 必要設定 2. 預設選擇 **Auto(自動)**	選擇 3G/4G 連線的身份驗證方法。 設定值有 **Auto**, **PAP**, **CHAP**, 或 **None**.
Priority (優先順序)	1. 必要設定 2. 字串格式: 整數	輸入撥號的順序。有效值從 1 到 16。系統將從分配最小號的設定檔開始撥號。 ***範圍值***: 1 ~ 16.
Profile (設定檔)	預設勾選此方框	勾選該框以啟用此設定檔。 取消勾選該框以在撥號操作中禁用此設定檔。
Save (保存) (保存)	無	按下 **Save (保存)** 按鈕以保存設定值。
Undo (還原) (還原)	無	按下 **Undo (還原)** 按鈕可將剛剛設定的內容還原回上一個設定。
Back (返回)	無	按一下 **Back (返回)** 按鈕時，畫面將返回到上一個頁面。

設定 3G/4G Connection Common Configuration (3G/4G 連線通用設置)

在此, 您可以更改 3G/4G WAN 的通用設置。

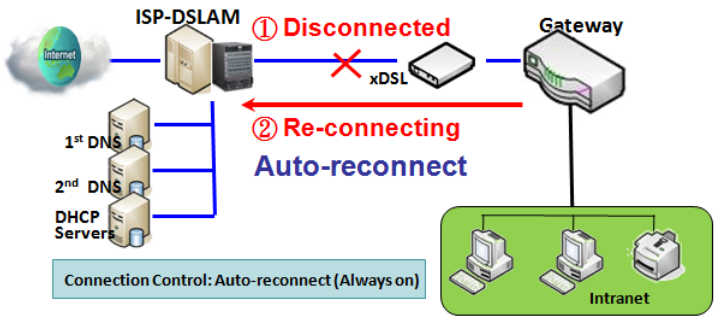


3G/4G Connection Common Configuration (3G/4G 連線通用設置)		
項目	**設定值**	**說明**
Connection Control (連接控制)	預設選擇 **Auto-reconnect (自動重新連線)**	當選擇 **Auto-reconnect(自動重新連線)**時，意味著無論何時有實體連線，設備都將永遠嘗試保持網路連線。 如果勾選了 **Connect-on-demand (按需連線)**，則表示只有在偵測到資料通信時才建立網路連線。 勾選 **Connect Manually (手動連線)**時，意味著必須按一下 **Connect (連線)**按鈕才能手動撥號連線。有關詳細資訊，請轉到 **Status > Basic Network > WAN & Uplink** 頁面。 **注意:** 如果 WAN 介面作為容錯移轉角色中另一個 WAN 介面的主節點 (反之亦然)，則連線控制參數在兩個 WAN 上都不可用，因為系統必須將其設置為 "Auto-reconnec (自動重新連線)"。
Maximum Idle Time (最大閒置時間)	1. 可選設定 2. 預設輸入 **600** 秒	指定在連線閒置超時斷開網路連線的最大閒置時間設定。 ***範圍值***: 300 ~ 86400. **注意:** 只有在(**Connect-on-demand 需要時連線)** 或 **Connect Manually (手動連接)**被選擇為連線控制方案時，此欄位才可用
Time Schedule (時程表)	1. 必要設定 2. 預設選擇 **(0) Always**	選擇**(0) Always** 表示此 WAN 一直在運行。設定其他時程計畫後， 將有其他選項可供選擇。有關詳細資訊，請轉到 **Object Definition > Scheduling**。
MTU	1. 必要設定	指定 3G/4G 連線的 **MTU** (Maximum Transmission Unit 最大傳輸單

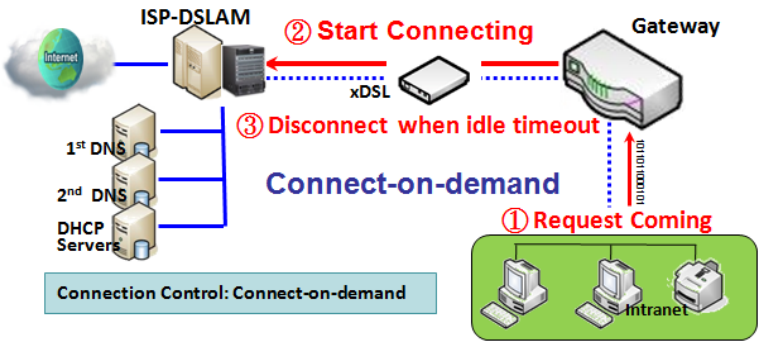
	2. 預設 **0** is filled-in	元) ***範圍值***: 512 ~ 1500, 0 爲自動
IP Pass-through (Cellular Bridge) **IP 直通 (蜂巢橋)**	1. 預設未勾選 2. 固定 **Fixed MAC** 字串格式: MAC 位址, 例如 00:50:18:aa:bb:cc	選擇 **Enable(啟用)**框後, 這表示將設備將直接將 WAN IP 分配給第一個連線的本地 LAN 客戶端。 但是，當可選的 **Fixed MAC(固定 MAC)** 爲非零值時，代表只有具有此 MAC 位址的客戶端才能獲得 WAN IP 位址。 **注意:** 當 **IP Pass-through (IP 直通)**處於啟用狀態時，**NAT** 和 **WAN IP Alias (別名)** 將不可用，直到該功能再次被停用。
NAT	預設勾選	取消勾選該框以停用 **NAT** (Network Address Translation 網路位址轉譯) 功能。
IGMP	預設選擇 **Disable** (停用)	選擇 **Auto (自動)** 以啓動 **IGMP** 功能。 勾選 **Enable (啓動)** 方框以啓動 **IGMP Proxy (代理)**。
WAN IP Alias	1. 預設未勾選 2. IP 位址字串格式. (IPv4 格式)	勾選該框以啟用 **WAN IP Alias** (別名), 然後填寫要分配的 IP 位址。

無論選擇哪種類型的 WAN, 都需要設定一些重要的參數。

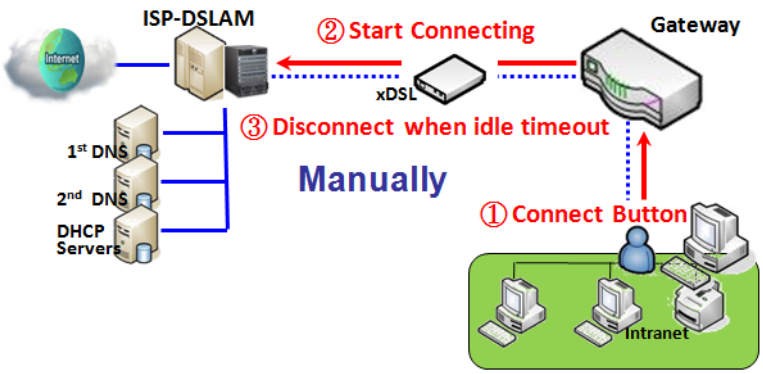
Connection Control (連接控制)



Auto-reconnect (自動重新連接): 一旦啟動, 閘道器將自動建立網路連線, 並在連接斷線後嘗試重新連接。建議為關鍵型應用程式選擇此方案, 以便確保全時網路連線。



Connect-on-demand (需要時連接): 在將本地資料發送到 WAN 端之前, 閘道器不會開始建立網路連接。在 LAN 和 WAN 之間進行正常資料傳輸後, 如果閒置時間達到最大閒置時間的值, 則此閘道器將斷開 WAN 連接..



Manually (手動): 在按下網頁介面中的 "連接" 按鈕之前，此閘道不會開始建立 WAN 連接。在 LAN 和 WAN 之間進行正常資料傳輸後, 如果閒置時間達到最大閒置時間的值，此閘道將斷開連接。

Network Monitoring Configuration

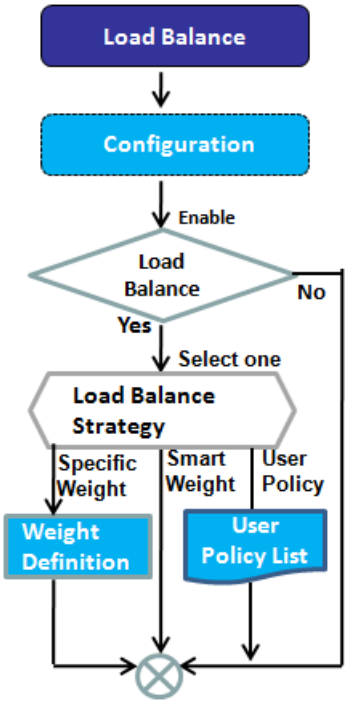
Item	Setting
Network Monitoring Configuration	Enable
Checking Method	DNS Query Query Interval 5 (seconds)
Loading Check	Enable Latency Threshold 3000 (ms) Fail Threshold 5 (Times)
Target1	DNS1
Target2	None

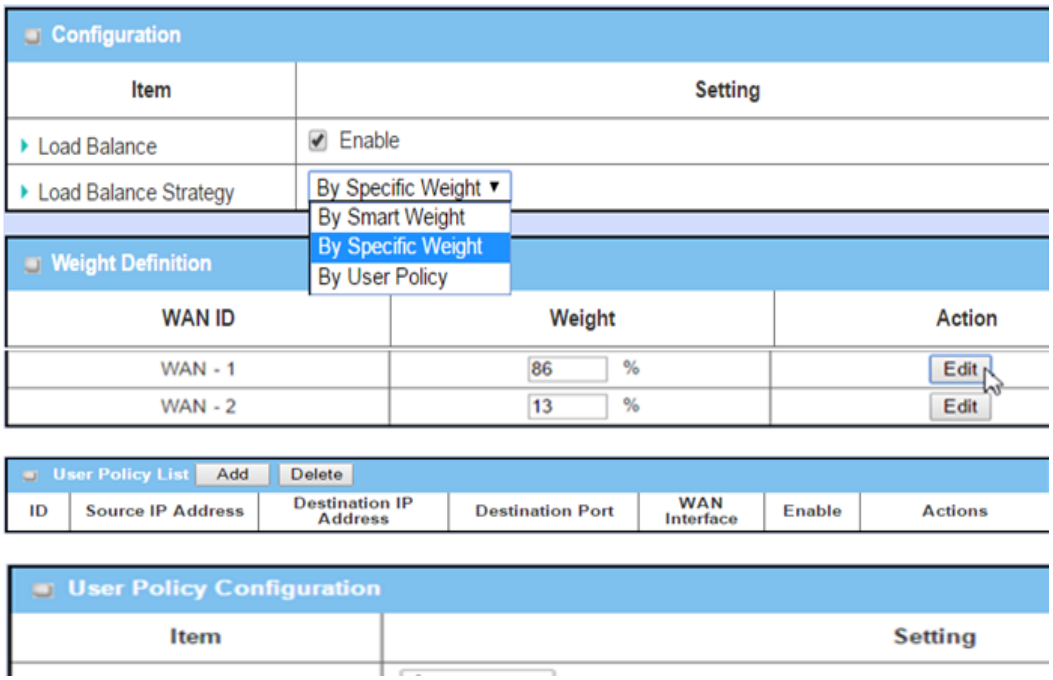
Network Monitoring Configuration(網路監控設置)

項目	設定值	說明
Network Monitoring Configuration (網路監視配置)	1. 可選設定 2. 預設爲未勾選	勾選 **Enable** 方框以啟動網路監視功能。
Checking Method (檢查方法)	1. 可選設定 2. 預設爲 **DNS Query (DNS 查詢)**	選擇 **DNS Query (DNS 查詢)** 或 **ICMP Checking (ICMP 檢查)**以檢測 WAN 連結。通過 **DNS 查詢**，系統透過 DNS 查詢資料封包發送到目標 1 和目標 2 中指定的目標來檢查連線。透過 **ICMP 檢查**，系統將透過向目標 1 和目標 2 中指定的目標發送 ICMP 請求資料封包來檢查連線。 **Query Interval (查詢間隔)**定義兩個 DNS 查詢或 ICMP 檢查資料包之間的傳輸間隔.

Loading Check (負荷檢查)	1. 可選設定 2. 預設爲未勾選	勾選 **Enable** 方框啟用負荷檢查允許路由器在 WAN 頻寬完全佔用時忽略未回復的 DNS 查詢或 ICMP 請求。這是為了防止錯誤的斷線狀態。 **Latency Threshold (延隔時間閾值)** 定義回應時間的公差閾值。 **Fail Threshold (失敗閾值)** 指定在路由器識別 WAN 斷線狀態之前檢測到的斷線狀態。在確認斷線之前， 輸入多個檢測斷線時間為閾值。
Target 1 (目標 1)	1. 可選設定 2. 預設爲 **DNS1**	**Target1 specifies** 指定**目標 1** 指定發送 DNS 查詢/ICMP 請求的第一個目標。 **DNS1**：將主 DNS 設置為目標。 **DNS2**：將次 DNS 設置為目標。 **Gateway(閘道)**: 將目前閘道設置為目標。 **Other Host(其他主機)**: 輸入要成為目標的 IP 位址。
Target 2 (目標 2)	1. 可選設定 2. 預設爲 **None (無)**	**Target2 specifies** 指定**目標 2** 指定發送 DNS 查詢/ICMP 請求的第二個目標。 **DNS1**：將主 DNS 設置為目標。 **DNS2**：將次 DNS 設置為目標。 **Gateway(閘道)**: 將目前閘道設置為目標。 **Other Host(其他主機)**: 輸入要成為目標的 IP 位址
Save (保存) (保存)	*無*	按一下 **Save (保存)**以保存設定。
Undo (還原) (還原)	*無*	按一下 **Undo (還原)**取消設定。

2.1.3 負載平衡

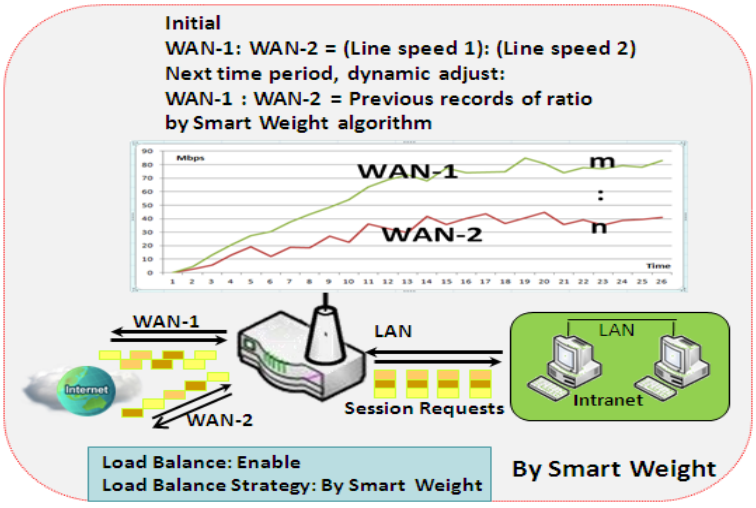




當有多個 WAN 介面，並且一個 WAN 連線的頻寬不足以支援從內網到網際網路的通信負載，則可以使用 WAN 負載平衡功能來擴大總 WAN 的頻寬。

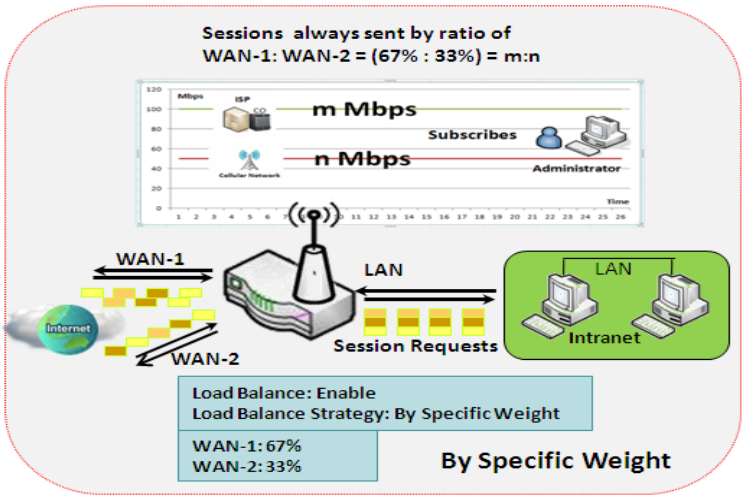
負載平衡策略

有三種可選的負載平衡策略：*"By Smart Weight (依照智慧權重)"*，*"By Specific Weight (依照指定權重)"* 和 *"By User Policy (依照用戶自訂規則)"*。根據應用要求和環境選擇策略。策略說明如下。



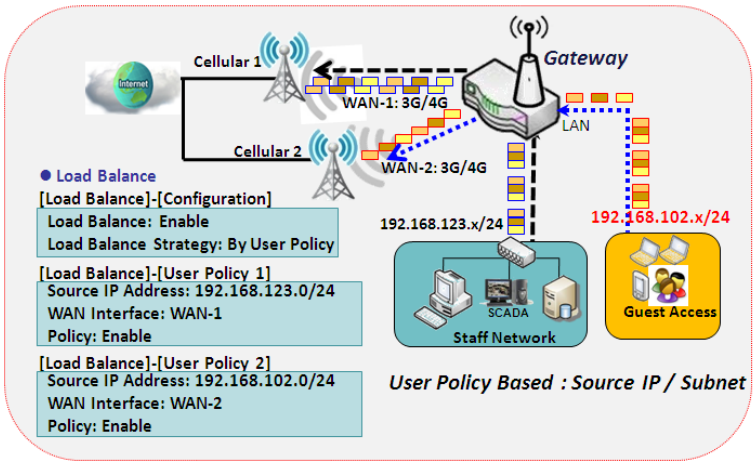
By Smart Weight (依照智慧權重)

如果基於 "依照智慧權重"，閘道器將採用 "實體介面" 配置頁面中指定的所有 WAN 介面的線路速度設定作為資料傳輸的預設比率。根據過去一段時間內(可能是 5 分鐘)通過這些 WAN 介面傳輸的資料封包的比率，系統會決定下一時段通過每個 WAN 介面的傳輸階段。管理員可以將其作為一種快速的方法來最大限度提高閘道器中多個 WAN 介面的頻寬利用率



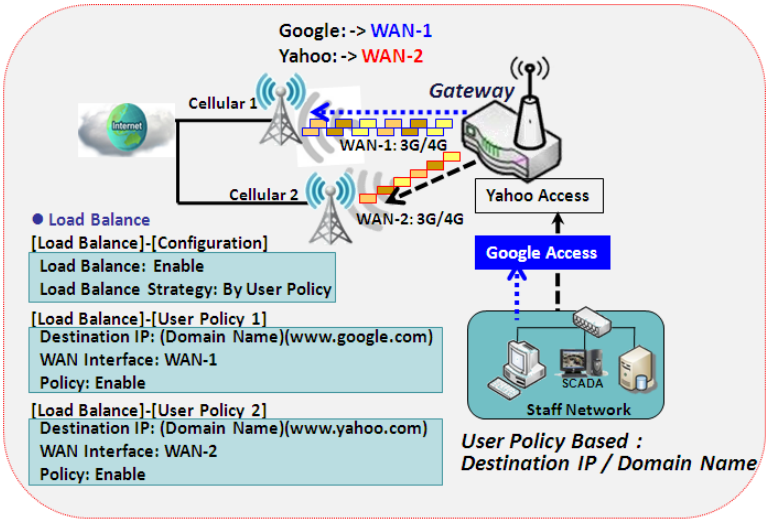
By Specific Weight (依照指定權重)

當選擇 “依照指定權重” 時，您需要設定 WAN-1 / WAN-2 的比率來決定階段的發送比率。 總比例應為 100%。該比率通常基於環境實際的 WAN 速度來定義。閘道器的流量控製程序將根據所有 WAN 介面上的專用權重比進行路由操作。



By User Policy (依照自訂規則)

如果選擇 “依照用戶策略” 負載平衡策略，則可以將來源 IP、目標 IP 或目標埠映射到指定的 WAN 介面。 該 IP 地址不一定是單一個 IP; 也可能是子網或 IP 範圍。目標埠可能是單一個埠或埠的範圍。 您可以為一個映射選擇一個目標來設定 IP 位址，並將其他設定為 “any (任意)” / “All (全部)” 。 除此之外，您還可以將協定設定為 TCP、UDP 或兩者。



左側顯示的圖表是用戶自訂規則示意圖。第一個圖說明了將各種來源 IP 子網域映射到不同 WAN 介面的示意圖。 來自不同子網域的所有資料封包將被路由到指定的 WAN 介面。管理員可以依據此管理和平衡可用 WAN 介面之間的負載。

第二個圖說明了將具有指定目的地 IP 或域名的資料封包路由到特定 WAN 介面的另一個示意圖。如果封包不符合用戶自定的規則，則閘道器只根據智慧權重算法(smart weight)對這些封包進行路由傳送。

設定負載平衡

轉到 Basic Network > WAN & Uplink > Load Balance 頁面

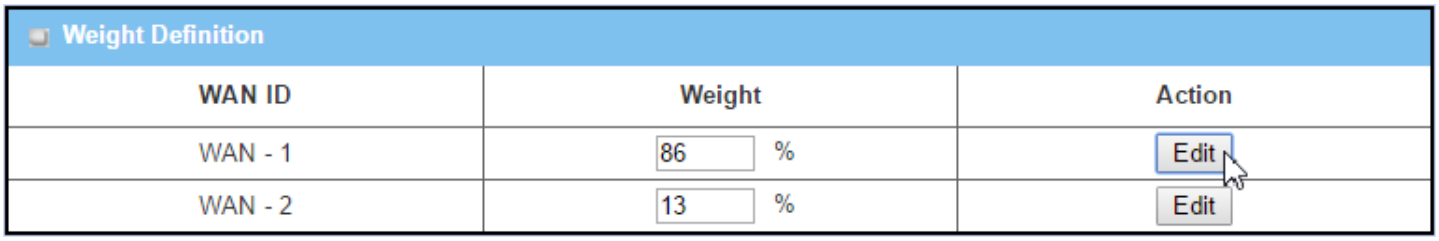
負載平衡功能用於管理多個 WAN 連線之間的頻寬平衡。當選擇 “By Smart Weight (依照智慧權重)” 時，系統將根據嵌入式智慧權重演算法自動操作負載平衡。但是，當選擇 “By Specific Weight (依照指定權重)” 時，隨後的 “Weight Definition (權重定義)” 設定畫面將允許您定義所有 WAN 介面之間傳輸階段的資料傳輸比率。最後，當選擇 “By User Policy (依照用戶規則定義)” 時， “User Policy List (用戶策略定義列表)” 將顯示所有已定義用戶的使用規則，並且 “User Policy Configuration (用戶策略配置)” 畫面將允許您建立並定義一條使用者定義使用規則用於透過特定一個 WAN 介面路由傳送特定封包資料。

啓動/選擇負載平衡策略

Configuration 項目	設定值	說明
Load Balance (負載平衡)	預設未勾選	勾選 Enable 啓動負載平衡
Load Balance Strategy	1. 必要設定 2. **By Smart Weight** 預設選擇.	有三負載平衡策略: **By Smart Weight (依照智慧權重)**: 系統將基於嵌入式智慧權重演算法自動操作負載平衡功能. **By Specific Weight (依照指定權重)**: 系統將基於指定的每個 WAN 的權重調整所有 WAN 中傳輸階段的比率 。 **By User Policy (依照用戶自訂規則)**: 系統將根據使用者定義的規則, 通過可用的 WAN 介面路由通信.
Save (保存) (保存)	無	按下 **Save (保存)** 按鈕以保存設定值。
Undo (還原)	無	按下 **Undo (還原)** 按鈕以還原上一個設定值.

(還原)

當選擇 **By Specific Weight (依照指定權重)**時，您需要調整 WAN 負荷的百分比。 系統會根據每個 WAN 的頻寬比率提供初始值，並在 **Save (保存) (保存)**按鈕被點擊後保留該值。

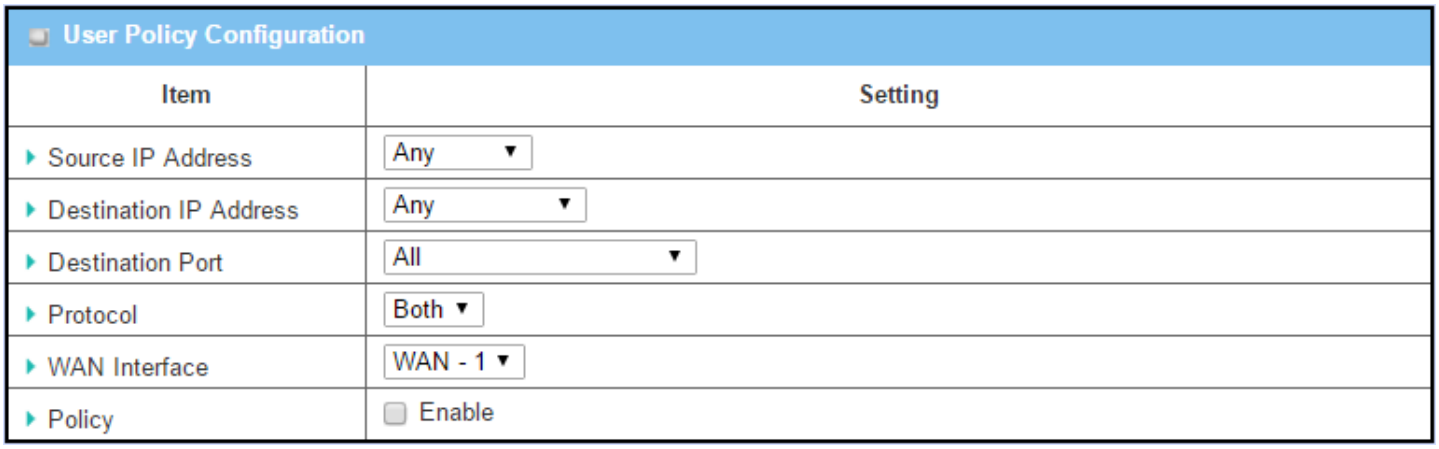


Weight Definition (權重定義) 項目	設定值	說明
WAN ID	無	每個可用 WAN 介面的識別碼
Weight (權重)	1. 必要設定 2. 預設設置每個 WAN 的頻寬比率。	輸入每個 WAN 介面的權重比率。 初始 預設情況下設置每個 WAN 的頻寬比率。 ***範圍值***: 1 ~ 99. 注意: 權重的總和不能大於 100%。
Save (保存) (保存)	無	按下 **Save (保存)** 按鈕以保存設定值
Undo (還原) (還原)	無	按下 **Undo (還原)** 按鈕以還原上一個設定值

當選擇 **By User Policy (依照用戶策略)** 時，將出現 **User Policy List (用戶策略列表)** 畫面。 請正確配置的策略規則，系統將根據這些規則通過路由可用的 WAN 介面流量

建立用戶策略

當按下 Add (增加)按鈕，將出現 User Policy Configuration (用戶策略配置) 畫面



User Policy Configuration (用戶策略配置)		
項目	**設定值**	**說明**
Source IP Address (來源 IP 位址)	1. 必要設定 2.預設爲 **Any (隨意)**	有四種選擇: **Any (隨意)**: 未提供特定的來源 IP。通信可能來自任何來源。 **Subnet (子網域)**: 指定通信來源的 subnet。輸入格式為: xxx/xx, 如 192.168.123.0/24. **IP Range (IP 範圍)**: 指定通信來源的 IP 範圍 **Single IP (單一個 IP)** : 指定通信來源唯一的 IP 位址。輸入格式為: xxx.xxx.xxx.xxx 例如 192.168.123.101.
Destination IP Address (目標 IP 位址)	1. 必要設定 2.預設爲 **Any (隨意)**	有五種選擇: **Any (隨意)**: 未提供特定的目標 IP。通信可能轉向任何目標。 **Subnet (子網域)**: 指定通信目標的 subnet。輸入格式為: xxx/xx, 如 192.168.123.0/24. **IP Range (IP 範圍)**: 指定通信目標的 IP 範圍 **Single IP (單一個 IP)** : 指定通信目標唯一的 IP 位址。輸入格式為: xxx.xxx.xxx.xxx 例如 192.168.123.101. **Domain Name (網域名稱)**: 指定通信目標的網域名稱。
Destination Port (目標埠)	1. 必要設定 2.預設爲 **All (全部)**	有四種選擇: **All (全部)** : 沒有提供特定的目標埠。 **Port Range (埠範圍)**: 指定通信的目標埠範圍 **Single Port(單一個埠)** : 指定傳輸唯一的目標埠 **Well-known Application(已知應用程式)**: 在下來選單選擇所定義的已知應用程式的服務埠 。

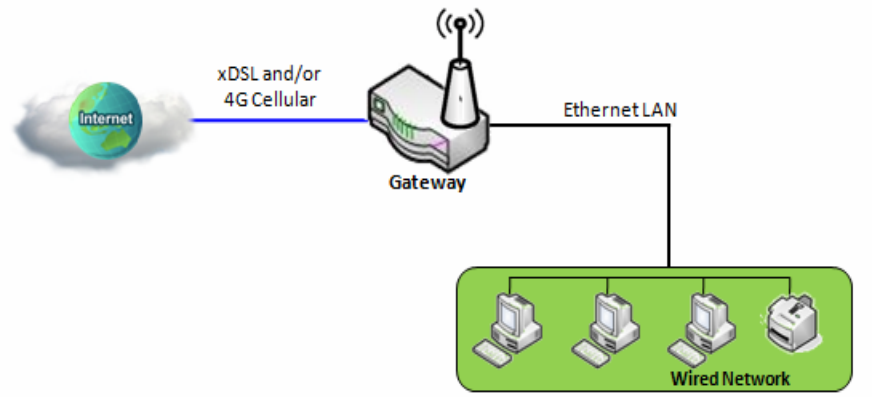
Protocol (目標埠)	1. 必要設定 2. 預設 **Both (兩者)**	有三個選項，包含 **Both**、**TCP** 和 **UDP**。
WAN Interface (WAN 介面)	1. 必要設定 2. 預設爲 **WAN-1**	選擇傳輸通過的介面。 請注意, WAN 介面下拉選單將只顯示可用的 WAN 介面。
Policy (策略)	預設未勾選	勾選 **Enable** 方框啓動策略規則
Save (保存) (保存)	無	按下 **Save (保存)** 按鈕以保存設定值
Undo (還原) (還原)	無	按下 **Undo (還原)** 按鈕可將剛剛設定的內容還原回上一個設定.

2.2 LAN & VLAN

本章節介紹LAN和VLAN的設定。閘道器型號決定是否有VLAN功能。

2.2.1 區域網 LAN

區域網 Local Area Network(LAN)可用於連線到網路的電腦之間分享資料或文件。下圖說明了有線網路和互連電腦的網路。



按照以下說明設定IPv4以太網LAN。

Configuration

Item	Setting
LAN IP Address	192.168.123.254
Subnet Mask	255.255.255.0 (/24)

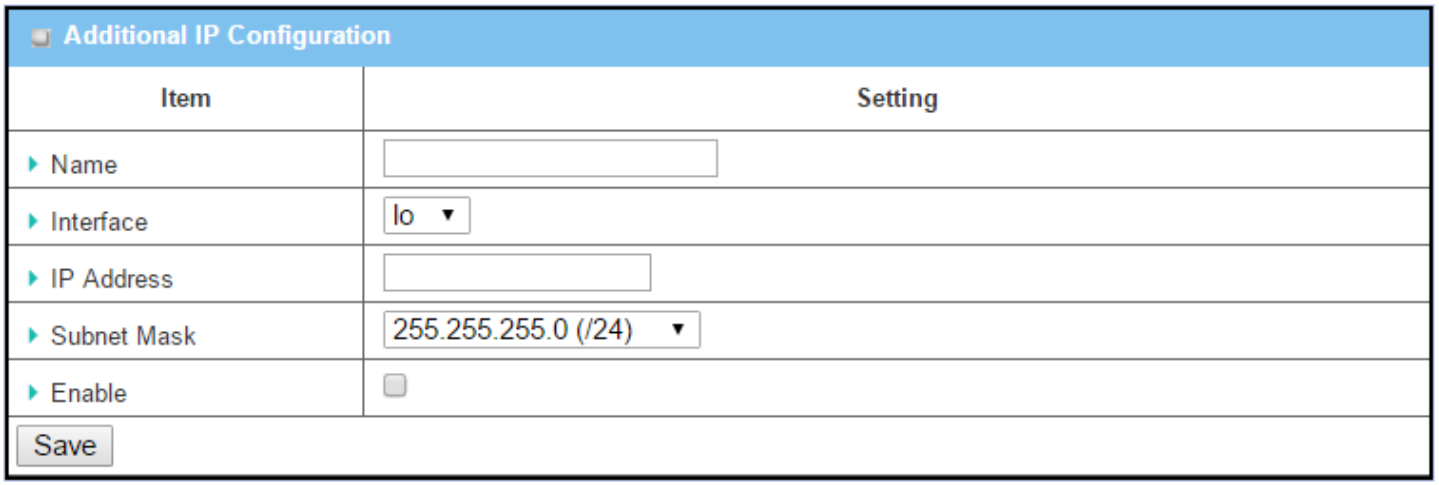
Configuration (設定) 項目	設定值	說明
LAN IP Address (網路 IP 位址)	1. 必要設定 2. 預設 192.168.123.254	輸入該設備的本地 IP 位址 網路設備在網路上必須使用此設備的 LAN IP 位址作為其預設閘道.如果需要, 可以對其進行更改. **注意:** *這也是 web UI(網頁介面) 的 IP 位址。如果更改之後需要在瀏覽器中輸入新的 IP 位址以登入 web UI .*
Subnet Mask (子網路	1. 必要設定 2. 255.255.255.0 (/24) is set 預設	在下來選單中爲閘道選擇子網路遮罩 子網路遮罩定義在一個網路或子網中允許的客戶端數量。預設子網路遮罩

遮罩)		為 255.255.255.0(/24), 這表示在此子網中允許最大 254 個 IP 位址。但是, 其中一個被該閘道的 LAN IP 位址佔用, 因此 LAN 網路中最多允許有 253 個客戶端. ***範圍值***: 255.0.0.0 (/8) ~ 255.255.255.252 (/30).
Save (保存)	無	按下 **Save (保存)** 按鈕以保存設定值
Undo (還原)	無	按下 **Undo (還原)** 按鈕以還原上一個設定值.

建立/編輯額外 IP (Create / Edit Additional IP)

此閘道器提供 LAN IP 別名功能，用於特殊管理的考量。 您可以為此閘道器新增 LAN IP，並透過新增 IP 登入此閘道器。

當按下 Add (增加)按鈕，將出現 Additional IP Configuration (額外 IP 設定) 畫面



Configuration (設定) 項目	設定值	說明
Name (名稱)	1. 可選設定	輸入別名 IP 位址的名稱。
Interface (介面)	1. 必要設定 2. **lo** is set 預設	指定介面類型。可能是 **lo** 或 **br0**.
IP Address (IP 位址)	1. 可選設定 2. **預設爲** 192.168.123.254	輸入設備的其他 IP 位址
Subnet	1. 必要設定 2. **255.255.255.0 (/24)** is	在下來選單中爲閘道選擇子網路遮罩

Mask (子網路遮罩)	set 預設	子網路遮罩定義在一個網路或子網中允許的客戶端數量。預設子網路遮罩為 255.255.255.0(/24), 這表示在此子網中允許最大 254 個 IP 位址。但是, 其中一個被該閘道的 LAN IP 位址佔用, 因此 LAN 網路中最多允許有 253 個客戶端. ***範圍值***: 255.0.0.0 (/8) ~ 255.255.255.255 (/32)
Save (保存)	無	按下 Save (保存) 按鈕以保存設定值

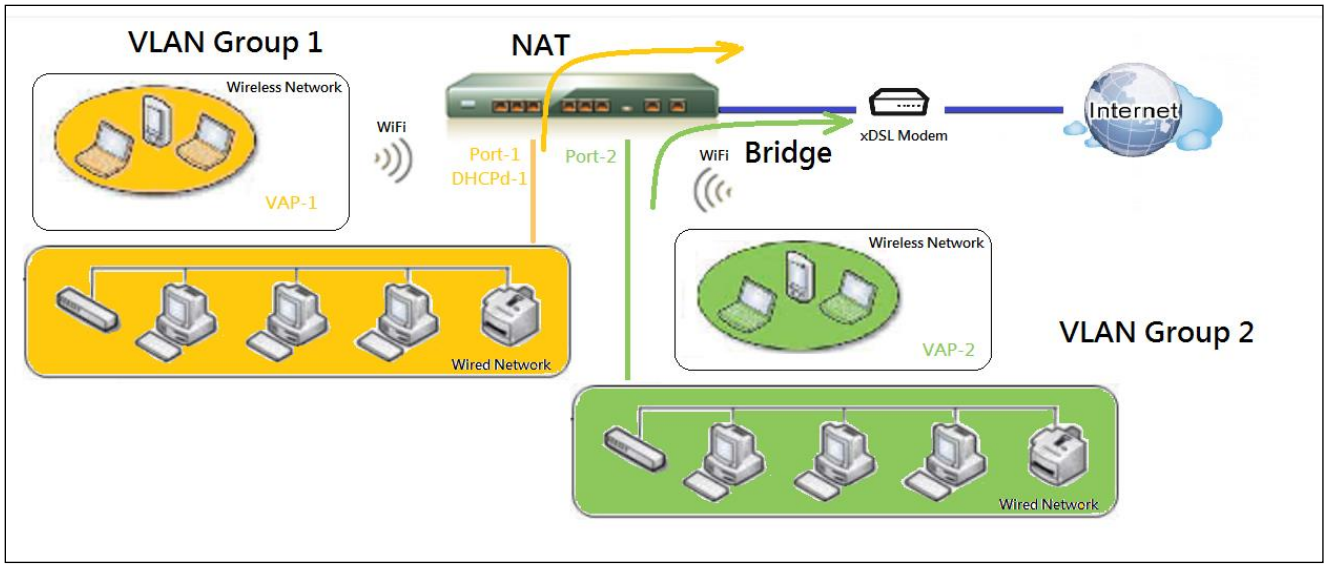
2.2.2 VLAN

VLAN(Virtual 虛擬 LAN)是交換器或路由器設備下的邏輯網路，用於將具有特定 VLAN ID 的客戶端主機分組。 該閘道器支援 Port-based 埠基礎的 VLAN 和 Tag-based 標籤基礎的 VLAN。 這些功能允許您將本地網路劃分為不同的 “virtual LANs 虛擬區域網” 。 這是一些應用方案的常見要求。 例如 SMB 中有各個部門，同一部門中的所有客戶端主機都應擁有共同的登入權限和 QoS 屬性。 您可以透過埠基礎的 VLAN 或標籤基礎的 VLAN 將多個部門分配為一個組，然後依據需要進行設定。 在某些情況下，ISP 可能要求路由器支援某些類型的服務(如 IPTV)的 “VLAN tags 標記” 。 您可以在一個標籤基礎的 VLAN 中將需要此服務的所有設備分組。

如果閘道器只有一個實體以太網 LAN 埠，則啟用埠基礎的 VLAN 時只有非常有限的設定可用。

➢Port-based 埠基礎 VLAN

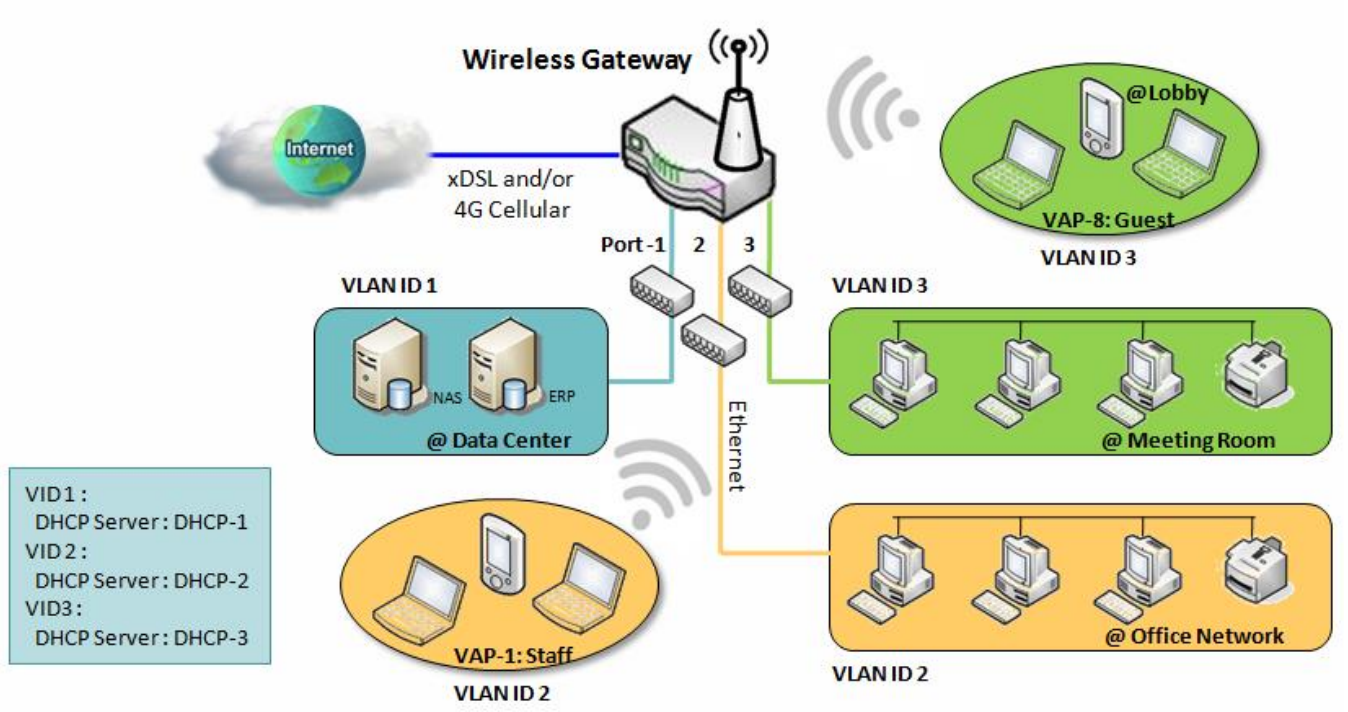
埠基礎的 VLAN 可以將以太網埠 Port-1～Port-4 和 Wi-Fi 虛擬接入點 VAP-1～VAP-8 集中在一起進行網路瀏覽、多媒體娛樂、VoIP 等差異化服務。兩種操作模式，即 NAT 和橋接器，可以應用於每個 VLAN 羣組。 可以為一個 NAT VLAN 羣組分配一台 DHCP 服務器，以便羣組主機成員獲得 IP 位址。這樣，每台主機都可以透過商業接入閘道器的 NAT 機制接入網際網路。在橋接器模式下，內網資料封包流量透過帶有 VLAN 標籤的 WAN 中繼埠傳送到不同服務的上層鏈路。



埠基礎的 VLAN 是以太網或有線或無線閘道器的虛擬 AP 上的一羣組埠，以構成邏輯 LAN 段。以下爲一個例子。

在一家公司，管理員設計了 3 個網段：大廳/會議室，辦公室和資料中心。在無線閘道器中，管理員可

以設定具有 VLAN ID 3 的大廳/會議室段。VLAN 羣組包括配備 NAT 模式和 DHCP-3 服務器的 Port-3 和 VAP-8(SSID：Guest)。 辦公室設定爲 VLAN ID 2，VLAN 羣組包括配備了 NAT 模式和 DHCP-2 服務器的 Port-2 和 VAP-1(SSID：Staff)。最後，管理員還設定 VLAN ID 為 1 的資料中心網段。VLAN 羣組包括 WAN 介面的 NAT 模式的 Port-1，如下圖所示。

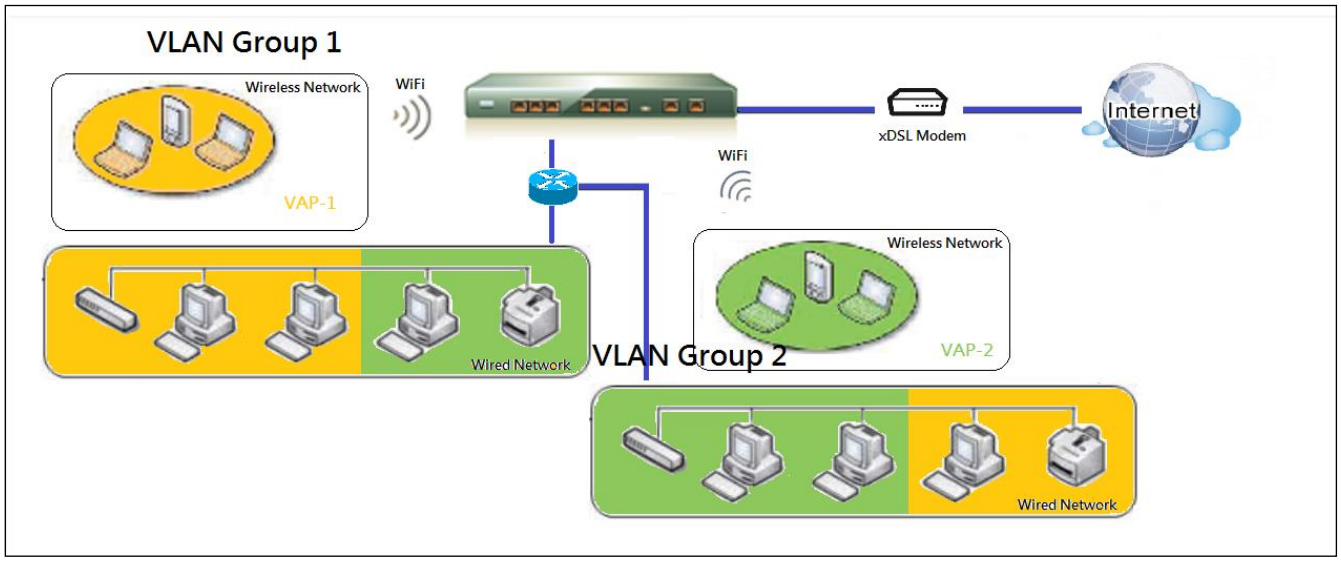


以上顯示了具有 3 個以太網 LAN 埠的閘道器的一般情況。如果設備只有一個以太網 LAN 埠，則設備只有一個 VLAN 羣組。 在這種情況下仍然支援埠基礎的 VLAN 設定的 NAT 和橋接模式。

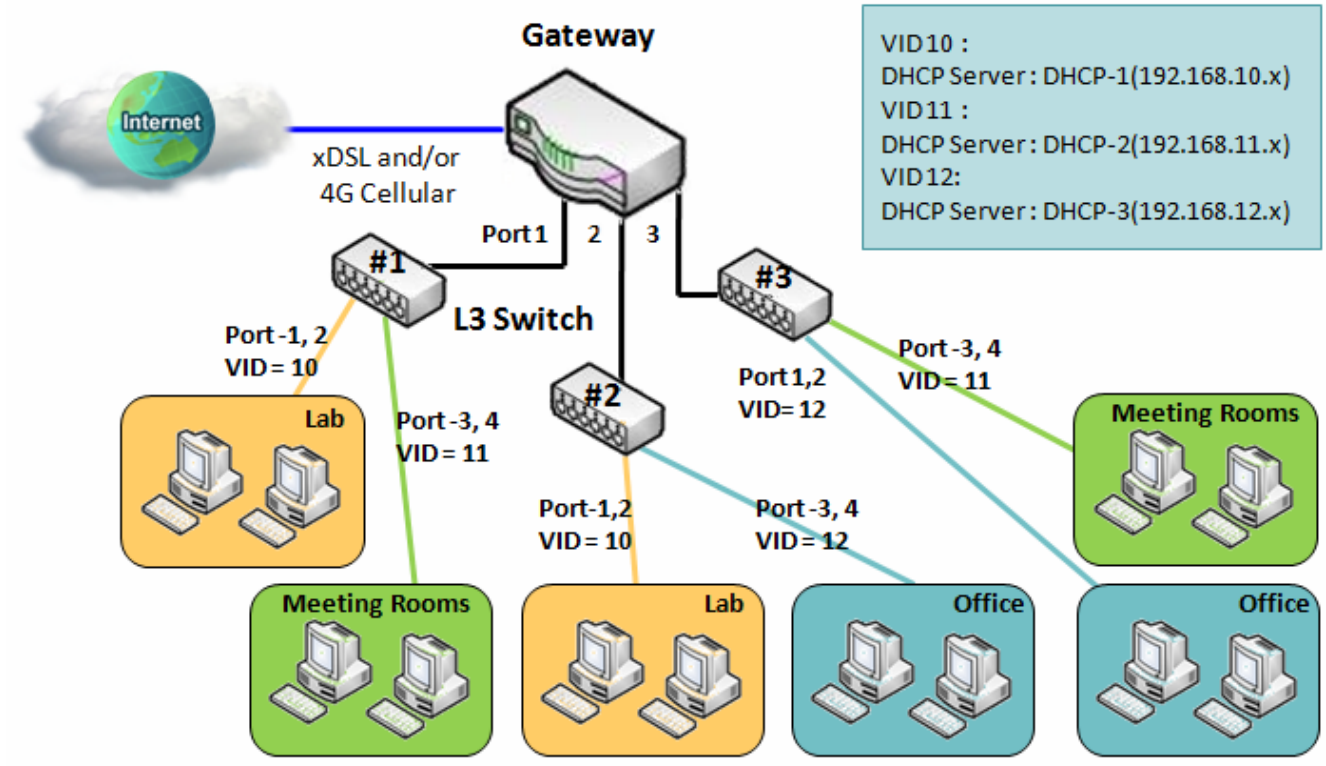
➢Tag-based 標籤基礎 VLAN

標籤基礎的 VLAN 功能可以將以太網埠 Port-1～Port-4 和 Wi-Fi 虛擬接入點 VAP-1～VAP-8 分組在不同的 VLAN 標籤中，以便在子網中部署。即使在相同的實體以太網埠，所有資料封包流也可以攜帶不同的 VLAN 標籤。 這些資料流可以被引導到不同的目的地，因為它們具有不同的標籤。 該方法將不同地理位置的主機分組到同一工作羣組非常有用。

標籤基礎的 VLAN 也稱為 VLAN 中繼。 VLAN Trunk 從路由器收集具有不同 VLAN ID 的所有資料封包，並將它們傳送到內網中。標記 VLAN 中的 VLAN 成員資格取決於埠上接收到的分組中的 VLAN ID 信息。管理員可以進一步使用 VLAN 交換器依據 VLAN ID 將 VLAN 中繼分為不同的羣組。 以下是一個例子。



管理員設計了 3 個網段，實驗室、會議室和辦公室。在安全 VPN 閘道器中，管理員可以設定帶有 VLAN ID 12 的辦公室環境。該 VLAN 羣組配備 DHCP-3 伺服器以建立 192.168.12.x 子網。他還使用 VLAN ID 11 設立會議室區段。該 VLAN 羣組配備 DHCP-2 伺服器，僅為內網建立 192.168.11.x 子網。也就是說，VLAN 11 羣組中的客戶端主機無法登入網際網路。 最後，他將實驗室網段設定為 VLAN ID 10。該 VLAN 羣組配備 DHCP-1 伺服器以建立 192.168.10.x 子網。

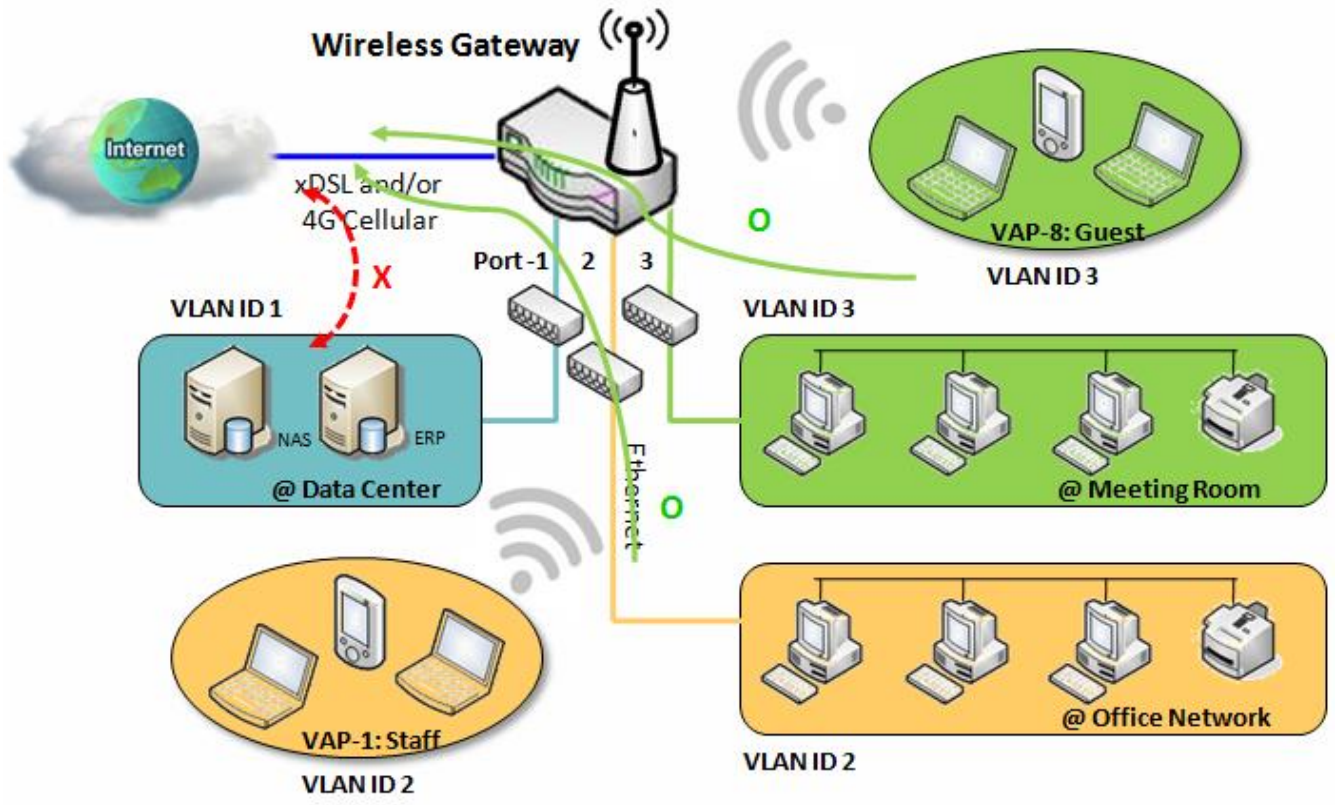


➢VLAN 羣組登入控制 (VLAN Groups Access Control)

管理員可以為所有 VLAN 羣組指定網際網路登入權限。他還可以設定允許哪些 VLAN 羣組相互溝通。

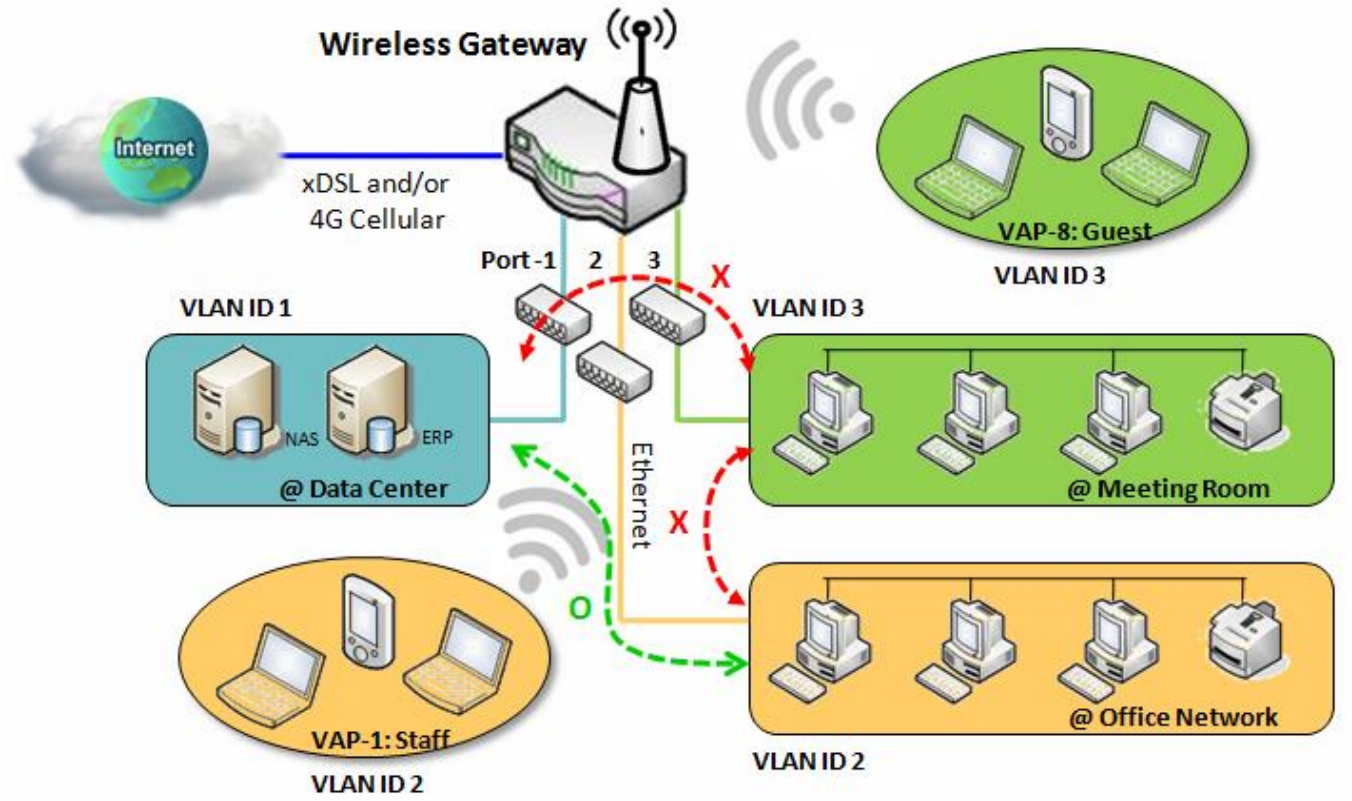
VLAN 羣組網際網路登入 (VLAN Group Internet Access)

管理員可以指定一個 VLAN 羣組的成員是否可以登入網際網路。以下示意圖說明 VLAN 羣組 VID 為 2 和 3 可以登入網際網路，但 VID 為 1 的用戶無法登入網際網路。也就是說，會議室的訪客和辦公室的工作人員可以登入網際網路。但由於安全考慮，資料中心中的電腦/伺服器無法登入網際網路。資料中心的伺服器僅供可信任人員使用，或者透過安全通道進行登入。



VLAN 間羣組路由:

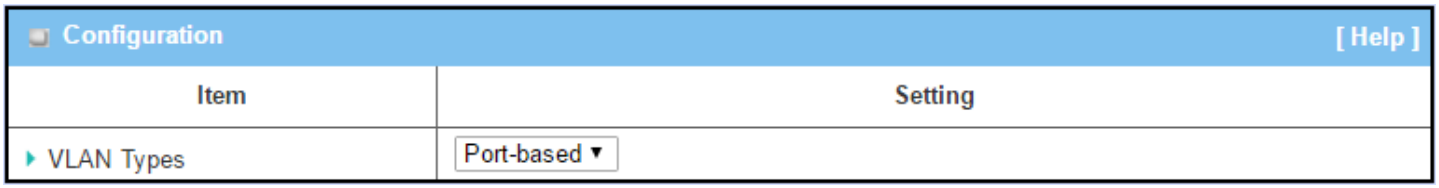
在 Port-Based Vlan 的標記中，管理員可以指定一個 VLAN 羣組的成員主機能夠或不能與另一個 VLAN 羣組進行通信。這是一個通訊配對，一個 VLAN 羣組可以加入多個通訊配對。但通訊配對沒有傳遞性。也就是說，如果 A 可以與 B 通信，並且 B 可以與 C 通信，那麼並不代表 A 可以與 C 通信。下面的圖表顯示了一個示意圖。 VID 1 和 2 的 VLAN 羣組可以互相登入，但 VID 1 和 VID 3 之間以及 VID 2 和 VID 3 之間的 VLAN 羣組不能登入。



設定 VLAN

轉到 Basic Network > LAN & VLAN > VLAN 頁面

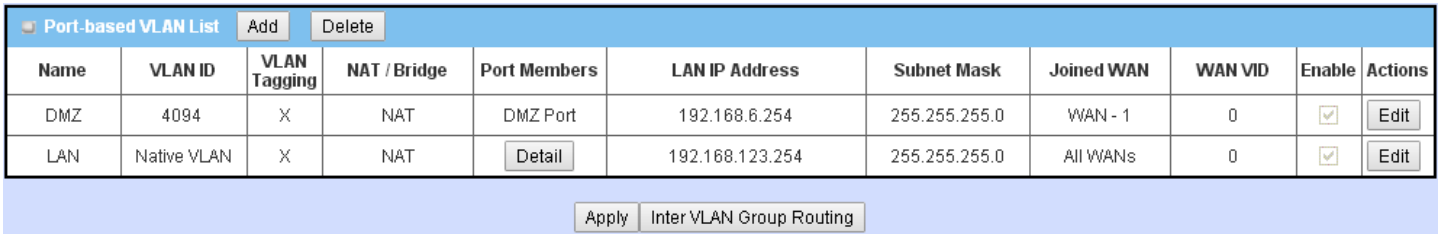
VLAN 功能允許您將本地網路劃分為不同的虛擬區域網，無論是埠基礎還是標籤基礎的。



Configuration (設定)		
項目	**設定值**	**說明**
VLAN Type (類型)	預設選擇 **Port-based**	選擇要使用的 VLAN 類型。 **Port-based (埠基礎)**: 埠基礎的 VLAN 允許您為每個 LAN 埠添加規則, 並且可以使用 VLAN ID 進行進階控制 **Tag-based(標籤基礎)**: 標籤基礎 的 VLAN 允許您添加 VLAN ID, 並為此 VLAN ID 選擇成員和 DHCP 伺服器。轉到 **Tag-based VLAN List (標籤基礎的 VLAN 清單)**頁面
Save (保存)	無	按下 **Save (保存)** 按鈕以保存設定值

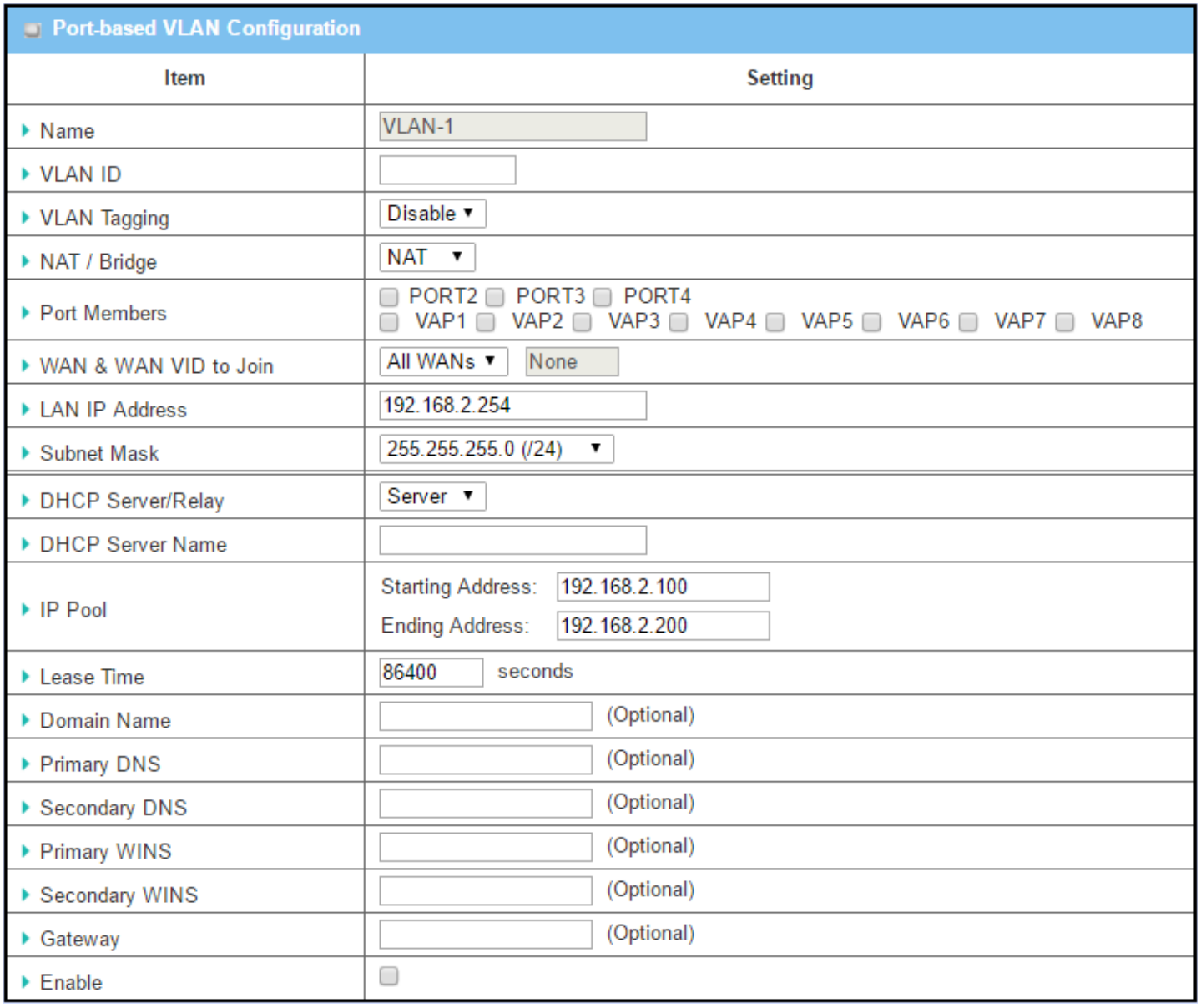
埠基礎 VLAN – 建立/編輯 VLAN 規則

埠基礎的 VLAN 允許您自定義每個 LAN 埠。預設規則顯示所有 LAN 埠的設定。如果您的設備有 DMZ 埠，您也會看到 DMZ 設定。規則的最大數目取決於 LAN 埠的數量。



當按下 Add (增加) 按鈕，將出現 Port-based VLAN Configuration (埠基礎 VLAN 設定) 畫面，包括 3 部分: Port-based VLAN Configuration (埠基礎 VLAN 設定), IP Fixed Mapping Rule List (IP 固定映射規則列表), 和 Inter VLAN Group Routing (VLAN 間羣組路由)(按鈕進入)。

Port-based VLAN – Configuration (埠基礎 VLAN 設定)

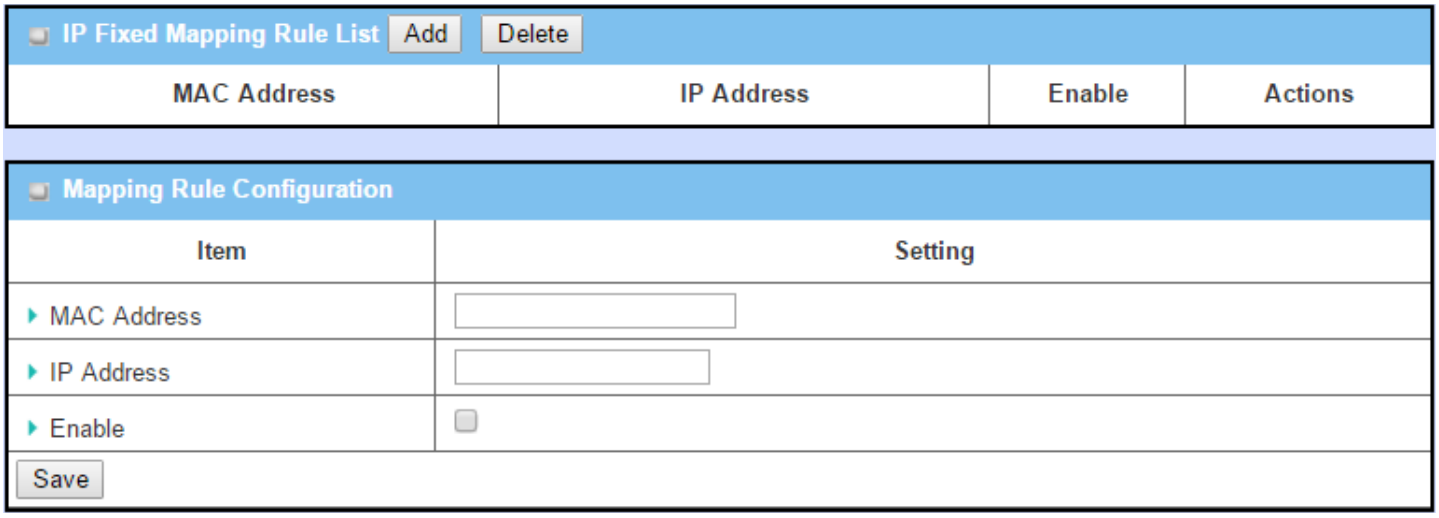


Port-based VLAN Configuration (埠基礎 VLAN 設定)		
項目	**設定值**	**說明**
Name (名稱)	1. 必要設定 2. 字串格式.: 已有預設文字	定義此規則的名稱 。具有預設文本, 無法修改。
VLAN ID	必要設定	定義 VLAN ID 編號, 範圍為 1 ~ 4094。
VLAN	預設爲 **Disable(禁用)**.	選則 **Enable 啟用**時, 將根據 **VLAN ID** 和 **Port Members(埠成員)**設定啟

Tagging (標記)		動規則。 選則 **Disable 禁用**時, 將根據 **Port Members(埠成員)**設定啟動該規則。
NAT / Bridge	預設選擇 **NAT**.	為此規則選擇 **NAT** 模式或 **Bridge 橋接**模式。
Port Members(埠成員)	預設未勾選.	選擇要添加到規則中的 LAN 埠和 VAP。 注意: 可用成員清單將取決於產品型號。
WAN & WAN VID to Join (加入)	預設選擇 **All WANs**.	選擇某個 **WAN** 或 **All WAN** 允許登入網際網路 。 注意: 如果選擇了**橋接**模式, 則需要選擇 WAN 並輸入 VID。
LAN IP Address (位址)	必要設定	分配 IP 位址給使用該規則的 DHCP 伺服器, 此 IP 位址為閘道 IP。
Subnet Mask (子網路遮罩)	預設選擇.**255.255.255.0(/24)**	為 DHCP 伺服器選擇**子網路遮罩**。
DHCP Server /Relay (伺服器/中繼)	預設選擇 **Server**.	定義 **DHCP 伺服器**類型。 有三種類型: **Server 伺服器**、**Relay 中繼**和 **Disable 禁用**. **中繼**: 選擇**中繼**為 VLAN 羣組啟用 DHCP 中繼功能。您只需要填入 **DHCP 伺服器 IP 位址** 欄位。 **伺服器**: 選擇**伺服器**為 VLAN 羣組啟用 DHCP 伺服器功能。您需要指定 DHCP 伺服器定。 **禁用**: 選擇**禁用**以禁用 VLAN 羣組的 DHCP 伺服器功能.
DHCP Server IP Address (伺服器 IP 位址) (僅供 DHCP **中繼**)	必要設定	如果選擇**中繼**類型的 DHCP 伺服器，請指定一個 **DHCP 伺服器 IP 位址**, 閘道將 DHCP 請求中繼到指派的 DHCP 伺服器。
DHCP Server Name (伺服器名稱)	必要設定	定義 DHCP 伺服器的名稱。
IP Pool	必要設定	定義 IP 池範圍。 有 **Starting Address 起始位址**和 **Ending Address 結束位址**欄位。如果客

		戶端從該 DHCP 伺服器請求 IP 位址, 將會在 **IP 池**的範圍內分配 IP 位址。.
Lease Time (租約時間)	必要設定	設定 設備到 DHCP 伺服器租用 IP 位址的到期時間。預設**租約時間**為 86400 秒。
Domain Name (網域名稱)	字串格式., 任何文字	此 DHCP 伺服器的網域名稱。 ***範圍值***: 0 ~ 31 個字元。
Primary DNS	IPv4 格式	此 DHCP 伺服器的主 DNS。
Secondary DNS	IPv4 格式	此 DHCP 伺服器的次 DNS。
Primary WINS	IPv4 格式	此 DHCP 伺服器的主 WINS。
Secondary WINS	IPv4 格式	此 DHCP 伺服器的次 WINS。
Gateway	IPv4 格式	此 DHCP 伺服器的閘道。
Enable	預設未勾選	勾選 **Enable (啓動)** 方框以啓動這個規則。
Save (保存)	無	按下 **Save (保存)** 按鈕以保存設定值。
Undo (還原)	無	按下 **Undo (還原)** 按鈕以還原上一個設定值。

另外，如果需要VLAN羣組的DHCP伺服器，則可以將一些IP規則添加到 **IP Fixed Mapping Rule List (IP固定映射規則列表)** 中。



當按下Add (增加)按鈕，將出現 **Mapping Rule Configuration (映射規則設定) 畫面**

Mapping Rule Configuration 項目	設定值	說明
MAC Address (位	必要設定	定義 DHCP 伺服器要分配的 **MAC 位址**目標。

址)		
IP Address (位址)	必要設定	定義 DHCP 伺服器分配的 **IP 位址**。 如果在上面的欄位中填入了 MAC 位址的請求, DHCP 伺服器則會將此 **IP 位址**分配給符合 **MAC 位址**的客戶端。
Enable (啓動)	預設未勾選	勾選 Enable (啓動) 方框以啓動這個規則。
Save (保存)	無	按下 Save (保存) 按鈕以保存設定值

注意：當瀏覽器更新頁面將您帶回VLAN頁面後都要點擊**Apply(套用)**按鈕以套用更改。

Port-based VLAN List Add Delete

Name	VLAN ID	VLAN Tagging	NAT / Bridge	Port Members	LAN IP Address	Subnet Mask	Joined WAN	WAN VID	Enable	Actions
DMZ	4094	X	NAT	DMZ Port	192.168.6.254	255.255.255.0	WAN - 1	0	☑	Edit
LAN	Native VLAN	X	NAT	Detail	192.168.123.254	255.255.255.0	All WANs	0	☑	Edit
VLAN-1	2	X	NAT	Detail	192.168.2.254	255.255.255.0	All WANs	0	☑	Edit ☐ Select

Apply Inter VLAN Group Routing

Please Click Apply button to take effect.

埠基礎 VLAN – VLAN 羣組間路由 (Port-Based VLAN-Inter VLAN Group Routing)

點擊 **VLAN Group Routing** (羣組路由) 按鈕, 將出現 **VLAN Group Internet Access Definition (VLAN 羣組登入網際網路定義)** 和 **Inter VLAN Group Routing (羣組間路由)** 畫面。

VLAN Group Internet Access Definition

VLAN IDs	Members	Internet Access(WAN)
1	**Port :** 2,3,4 ; **VAP :** 1,2,3,4,5,6,7,8	Allow Edit

Inter VLAN Group Routing

VLAN IDs	Members	Action
		Edit
		Edit
		Edit
		Edit

Save Back

當按下 Edit (編輯) 按鈕，將出現類似這個畫面。

VLAN Group Internet Access Definition

VLAN IDs	Members	Internet Access(WAN)
☑ 1, ☑ 2	**Port :** 2,3,4 ; **VAP :** 1,2,3,4,5,6,7,8	Allow Edit

Inter VLAN Group Routing

VLAN IDs	Members	Action
☐ 1, ☐ 2		Edit

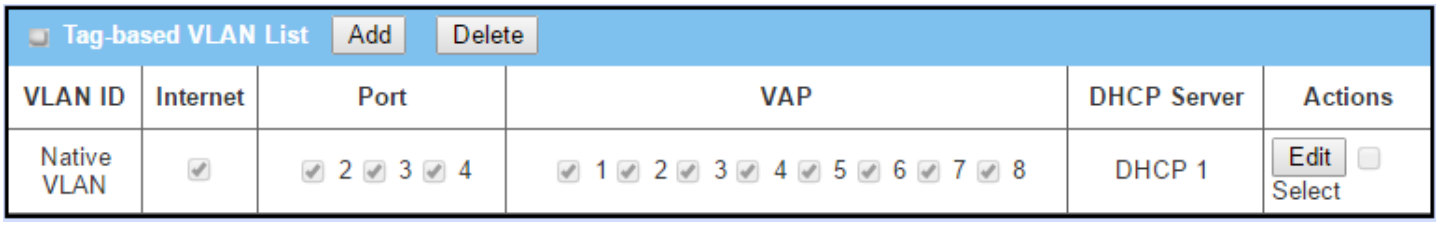
Inter VLAN Group Routing (VLAN 羣組間路由)

項目	設定值	說明
VLAN Group Internet Access Definition	預設勾選全部方框	預設勾選所有方框, 這表示將允許所有 **VLAN ID** 成員登入 WAN 介面。 如果未勾選 **VLAN ID**, 則表示 VLAN ID 成員無法登入網際網路。 注意: **VLAN ID 1** 永遠可用。其爲 **LAN** 的預設 VLAN ID。其他 **VLAN ID** 僅在啟用時才可用。

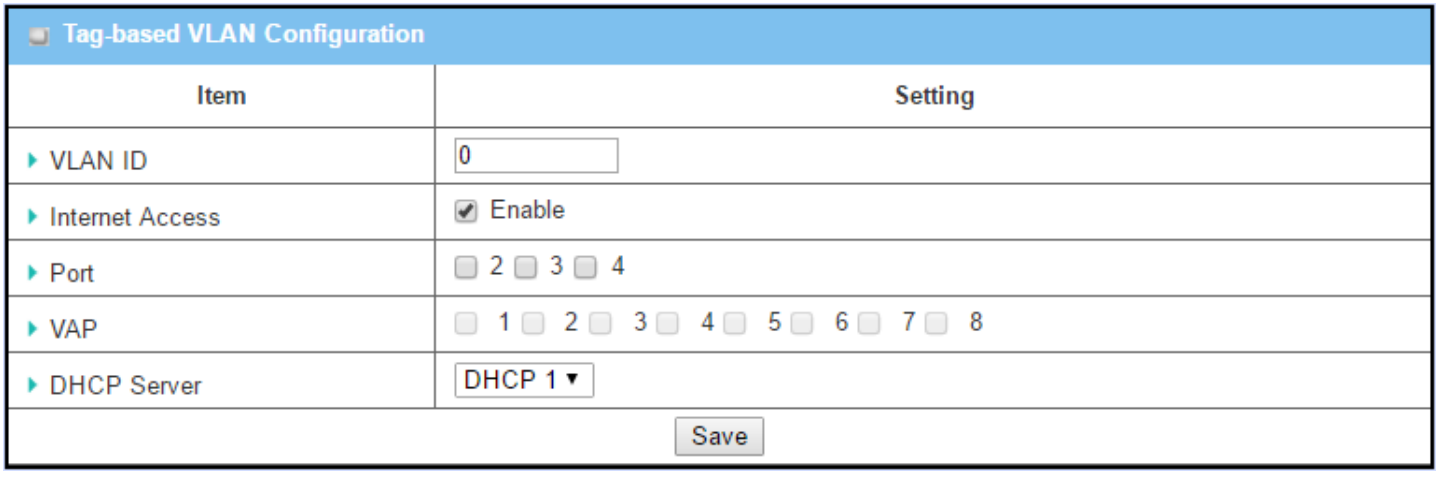
(網路登入定義)		
Inter VLAN Group Routing (羣組間路由)	預設未勾選	按一下 VLAN ID 方框以啟用 VLAN 登入功能。 預設不同 VLAN ID 中的成員無法相互登入。閘道最多支援 4 條 **VLAN 羣組路由**規則。 例如,如果勾選了 ID_1 和 ID_2, 則表示 VLAN ID_1 中的成員可以登入 VLAN ID_2 的成員, 反之亦然。
Save (保存)	無	按下 Save (保存) 按鈕以保存設定值

標籤基礎 Tag-based VLAN – 建立/編輯 VLAN 規則

標籤基礎的 VLAN 允許您依據 VLAN ID 客製化每個 LAN 埠。預設規則顯示所有 LAN 埠和所有 VAP 的設定。 如果您的設備有 DMZ 埠，您也會看到 DMZ 設定。 該路由器最多支援 128 個標籤基礎的 VLAN 規則集。



當按下 Add (增加)按鈕，將出現 **Tag-based VLAN Configuration** (標籤基礎 VLAN 設定) 畫面



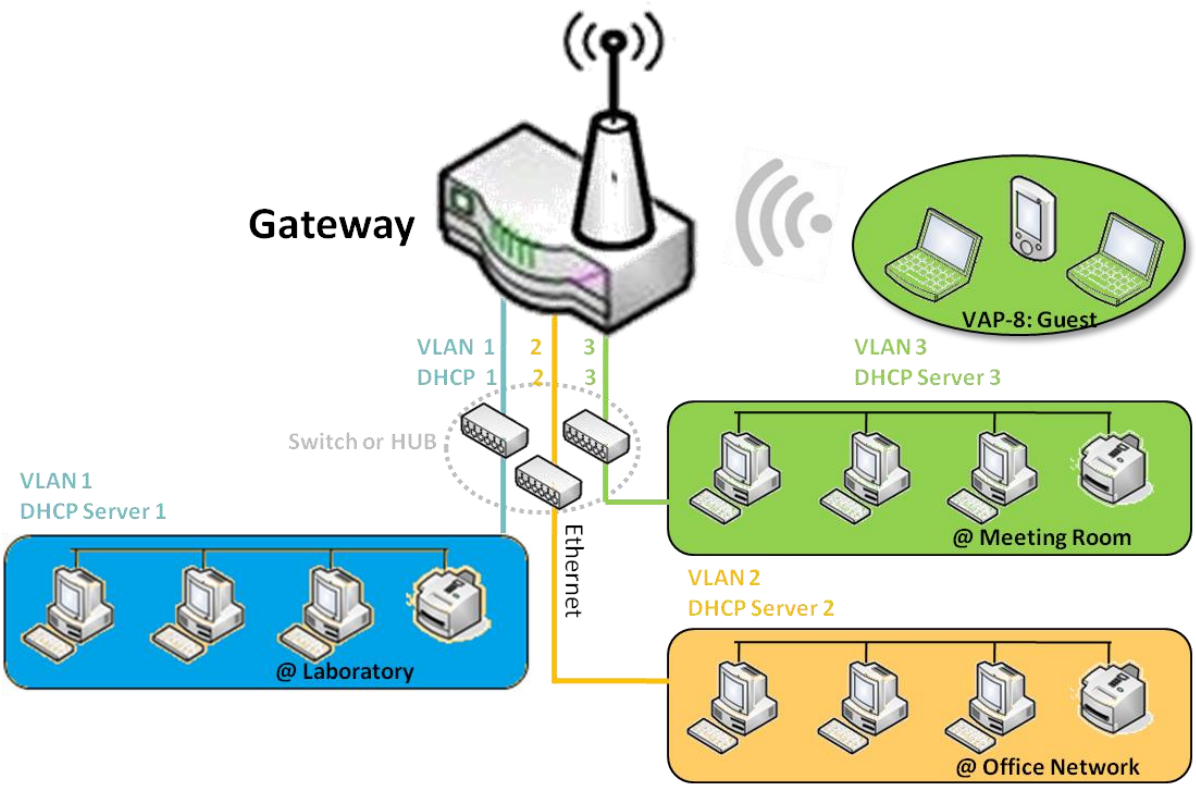
Tag-based VLAN Configuration (標籤基礎 VLAN 設定)		
項目	**設定值**	**說明**
VLAN ID	必要設定	定義 **VLAN ID** 編號, 範圍為 6 ~ 4094。

Internet Access (登入網路)	預設勾選此方框.	按一下 **Enable 啟用**方框允許 VLAN 羣組中的成員登入網際網路。
Port (埠)	預設未勾選	檢查 LAN 埠方框 以加入 VLAN 羣組。
VAP	預設未勾選	勾選 "VAP"方框加入 VLAN 羣組。 注意: 只有無線閘道有 VAP 清單。
DHCP Server	**DHCP 1** 預設選擇.	為此 VLAN 羣組的成員選擇 **DHCP 伺服器**。 要建立或編輯 VLAN 的 DHCP 伺服器, 請參閱 **Basic Network > LAN & VLAN > DHCP Server**
Save (保存)	無	點擊 Save (保存) 按鈕以保存設定 注意: 按一下 **Save (保存)**按鈕後, 請都再按一下 **Apply (套用)**按鈕以套用設置。

2.2.3 DHCP 伺服器

➢DHCP 伺服器

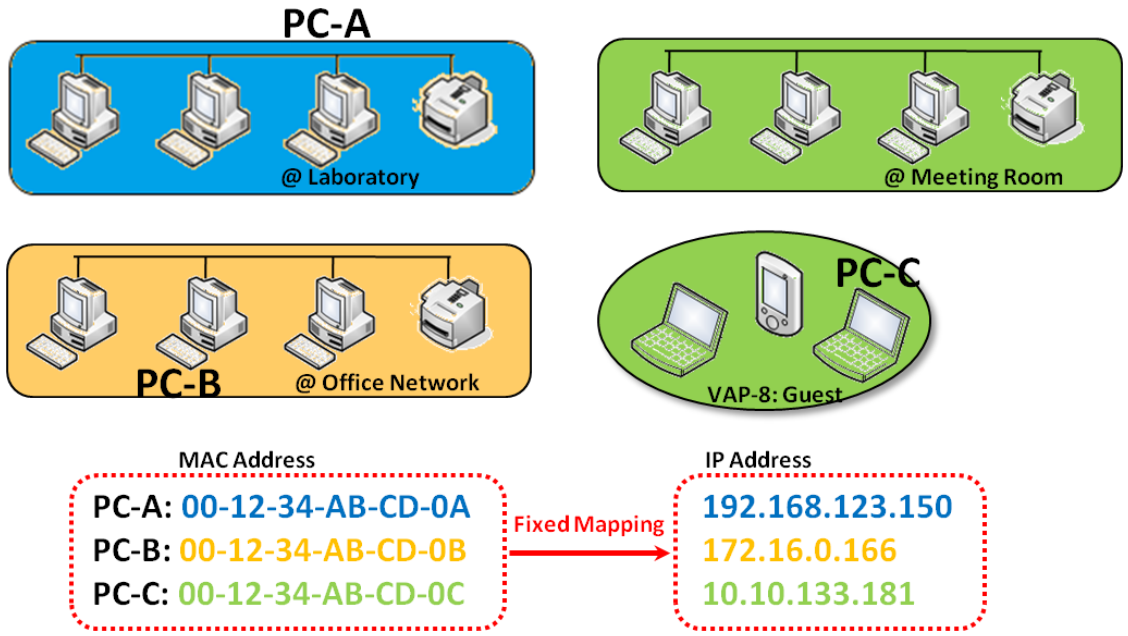
閘道器最多支援 4 台 DHCP 伺服器，以滿足來自不同 VLAN 羣組的 DHCP 請求(有關詳細資訊，請參閱 VLAN 的部分)。預設設定 LAN IP 位址與閘道器 LAN 介面相同，其預設子網路遮罩設定為 “255.255.255.0” ，顯示在閘道器的 Web UI 上的 DHCP 伺服器列表頁面上預設 (IP Pool) IP 池範圍從 “.100” 到 “.200” 。



點擊 “DHCP Server List (DHCP 伺服器列表)” 後面的 “Add(新增)” 按鈕即可添加更多 DHCP 伺服器設定，或點擊每個 DHCP 伺服器列表尾端的 “Edit (編輯)” 按鈕，以編輯目前設定。此外，您可以選擇一個 DHCP 伺服器並透過單擊 “Select (選擇)” 方框和 “Delete (刪除)” 按鈕將其刪除。

➢Fixed Mapping (固定映射)

當目標已存在於 *DHCP Client List (DHCP 客戶端列)*表中時，用戶可以將固定 IP 位址分配給特定客戶端 MAC 位址，或者預先手動增加其他映射規則。



DHCP 伺服器設定

轉到 Basic Network > LAN & VLAN > DHCP Server 頁面。

DHCP 伺服器設定允許用戶建立和客製化 DHCP 伺服器策略，為區域網(LAN)上的設備分配 IP 位址。

建立/編輯 DHCPServerMapping 規則列表

閘道器允許您在 DHCP Server 上客製化 Mapping rules。最多支持 64 個規則集。當按下 **Fixed Mapping** 按鈕時，將出現 **Mapping Rule List** 畫面。

DHCP Server List | Add | Delete | DHCP Client List | [Help]

DHCP Server Name	LAN IP Address	Subnet Mask	IP Pool	Lease Time	Domain Name	Primary DNS	Secondary DNS	Primary WINS	Secondary WINS	Gateway	Enable	Actions
DHCP 1	192.168.123.254	255.255.255.0	192.168.123.100-192.168.123.200	3600		0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	☑	Edit / Fixed Mapping

當按下 Add (增加)按鈕，將出現 **DHCP Server Configuration** (DHCP 伺服器設定) 畫面

DHCP Server Configuration

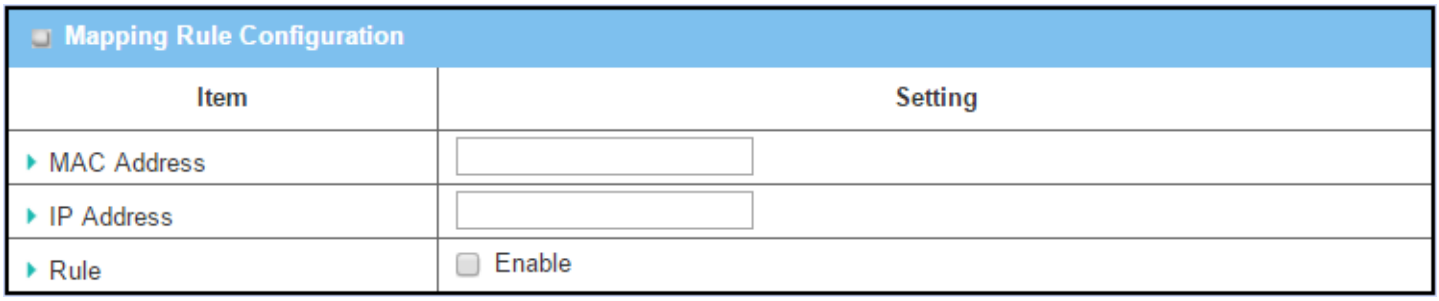
Item	Setting
DHCP Server Name	DHCP 2
LAN IP Address	192.168.2.254
Subnet Mask	255.0.0.0 (/8)
IP Pool	Starting Address: Ending Address:
Lease Time	86400 seconds
Domain Name	(Optional)
Primary DNS	(Optional)
Secondary DNS	(Optional)
Primary WINS	(Optional)
Secondary WINS	(Optional)
Gateway	(Optional)
Server	Enable

DHCP Server Configuration (DHCP 伺服器設定)		
項目	**設定值**	**說明**
DHCP Server Name	1. 字串格式., 任何文字 2. 必要設定	輸入 DHCP 伺服器名稱。
LAN IP Address (位址)	1. IPv4 格式. 2. 必要設定	此 DHCP 伺服器的 LAN IP 位址。
Subnet Mask	255.0.0.0 (/8) is set 預設	此 DHCP 伺服器的子網路遮罩。
IP Pool	1. IPv4 格式. 2. 必要設定	此 DHCP 伺服器的 IP 池。在此欄位中輸入起始位址和此欄位中輸入的結束位址組成。
Lease Time	1. 數字字串格式. 2. 必要設定	此 DHCP 伺服器的租用時間。 ***範圍值***: 300 ~ 604800 seconds.
Domain Name	字串格式., 任何文字	此 DHCP 伺服器的網域名稱。
Primary DNS	IPv4 格式	此 DHCP 伺服器的主 DNS。
Secondary DNS	IPv4 格式	此 DHCP 伺服器的次 DNS。
Primary WINS	IPv4 格式	此 DHCP 伺服器的主 WINS。
Secondary WINS	IPv4 格式	此 DHCP 伺服器的次 WINS。
Gateway	IPv4 格式	此 DHCP 伺服器的閘道。
Server	預設未勾選	勾選 Enable (啓動) 方框以啓動 DHCP 伺服器。
Save (保存)	無	按下 Save (保存) 按鈕以保存設定值
Undo (還原)	無	按下 Undo (還原) 按鈕可將剛剛設定的內容還原回上一個設定.
Back(返回)	無	按一下 **Back(返回)**按鈕後, 畫面將返回到 DHCP 伺服器設定頁面。

建立/編輯 DHCP 服務器映射規則列表

閘道器允許您在 DHCP 服務器上客製化映射規則列表。最多支持 64 個規則集。當按下 **Fix Mapping(g 固定映射)**按鈕時，將出現 **Mapping Rule List(**映射規則列表) 畫面。

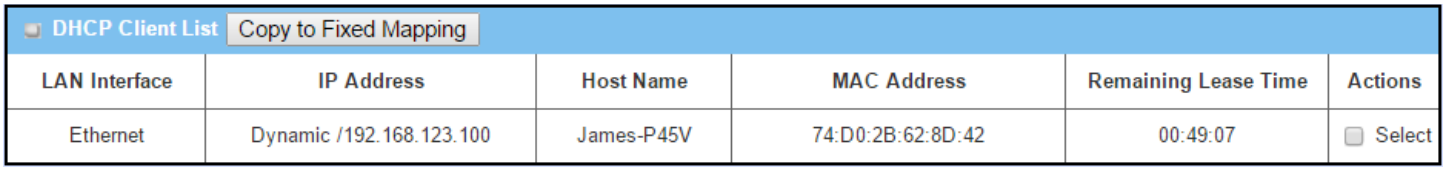
當按下 Add (新增) 按鈕，將會出現 Mapping Rule Configuration (映射規則設定) 畫面



Mapping Rule Configuration (映射規則設定)		
項目	設定值	說明
MAC Address	1. MAC 位址字串格式. 2. 必要設定	此映射規則的 MAC 位址。
IP Address	1. IPv4 格式. 2. 必要設定	此映射規則的 IP 位址。
Rule	預設未勾選	勾選 **Enable (啓動)** 方方框啓動這個規則。
Save (保存)	無	按下 **Save (保存)** 按鈕以保存設定值
Undo (還原)	無	按下 **Undo (還原)** 按鈕以還原上一個設定值.
Back (返回)	無	按一下 Back (返回)按鈕後, 畫面將返回 DHCP 伺服器設定頁面。

檢視/複製 DHCP 客戶端列表 (DHCP Server Option List)

當按下 DHCP Client List (DHCP 客戶端列表)按鈕將會出現 DHCP Client List 畫面

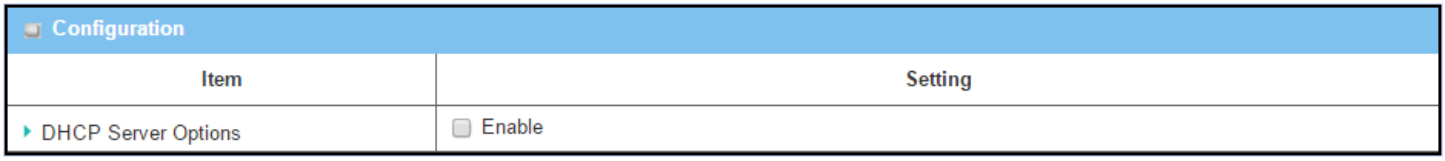


當選擇 DHCP 客戶端，並按下 **Copy to Fixed Mapping (複製到固定映射)** 按鈕時。 DHCP 客戶端的 IP 位址和 MAC 位址將自動套用於特定 DHCP 伺服器上的映射規則列表。

啓動/關閉 DHCP 伺服器選項

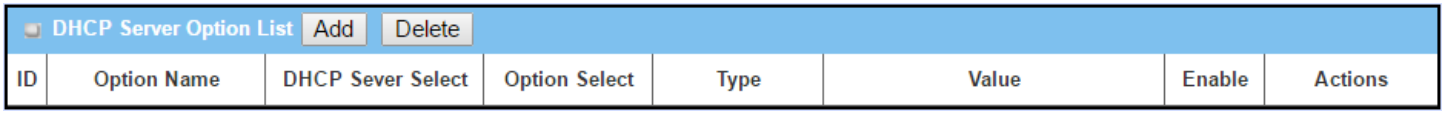
DHCP Server Options (DHCP 伺服器選項) 設定允許用戶設定 DHCP 選項 66,72 或 114。點擊 **Enable (啟用)**按鈕以啓動 DHCP 選項功能，DHCP 伺服器將在發送 DHCPOFFER DHCPACK 封包時增加設定的選項。

Option	Meaning	RFC
66	TFTP server name	[RFC 2132]
72	Default World Wide Web Server	[RFC 2132]
114	URL	[RFC 3679]

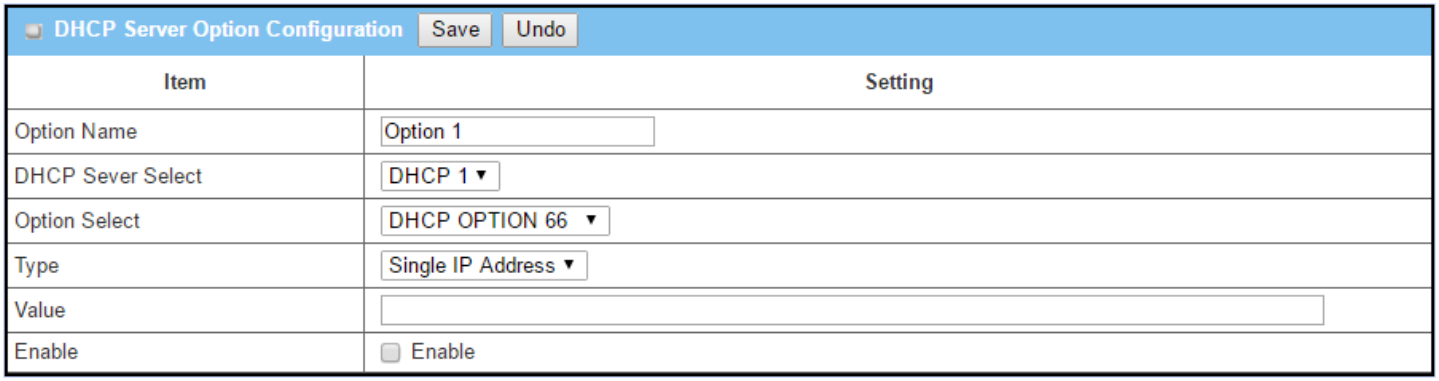


建立/編輯 DHCP 伺服器選項

閘道器最多支援 99 個選項設定。



當按下 Add/Edit(新增/編輯) 按鈕時，將出現 DHCP Server Option Configuration (DHCP 伺服器選項設定)畫面。



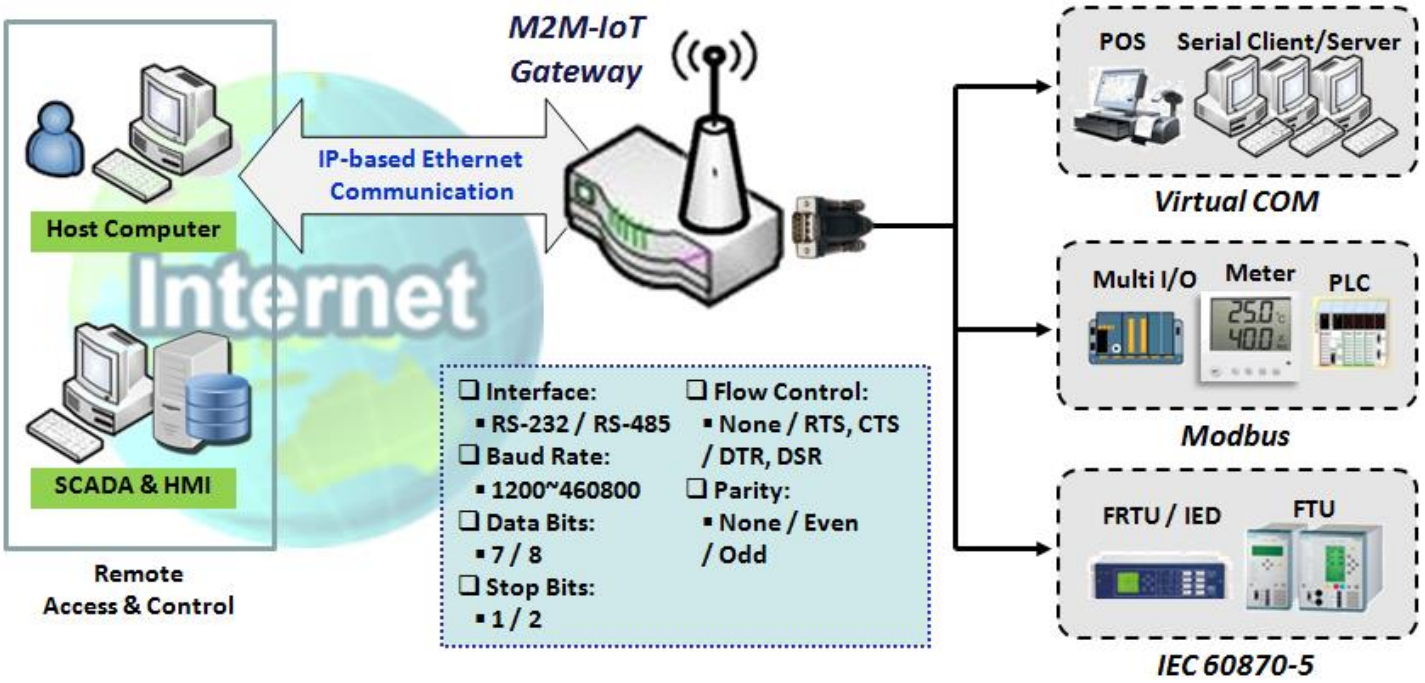
DHCP Server Option Configuration (DHCP 伺服器選項設定)		
項目	**設定值**	**說明**
Option Name (選項名稱)	1. 字串格式., 任何文字 2. 必要設定.	輸入 DHCP 伺服器選項名稱。
DHCP Server	所有可用 DHCP 伺服器的	選擇此選項套用到 DHCP 伺服器。

<table>
<tr><td>Select
(DHCP 伺服器選擇)</td><td colspan="4">下拉清單。</td></tr>
<tr><td>Option Select (選項選擇)</td><td>1. 必要設定.
2. 預設選擇 Option 66。</td><td colspan="3">從下拉清單中選擇選項。可以選擇 Option 66、Option 72 或 Option 144.
Option 66 用於 TFTP;
Option 72 用於 www;
Option 144 用於 URL.</td></tr>
<tr><td rowspan="5">Type</td><td rowspan="5">DHCP 伺服器選擇的下拉清單</td><td colspan="3">每個選項都有不同的數值型別。</td></tr>
<tr><td rowspan="2">66</td><td colspan="2">單一 IP 位址</td></tr>
<tr><td colspan="2">單一 FQDN</td></tr>
<tr><td>72</td><td colspan="2">IP 位址清單, 由 “,” 分隔</td></tr>
<tr><td>114</td><td colspan="2">單一 URL</td></tr>
<tr><td rowspan="6">Value</td><td rowspan="6">1. IPv4 格式
2. FQDN 格式
3. IP 列表
4. URL 格式
5. 必要設定</td><td colspan="3">符合類型:</td></tr>
<tr><td></td><td>類型</td><td>值</td></tr>
<tr><td rowspan="2">66</td><td>單一 IP 位址</td><td>IPv4 格式</td></tr>
<tr><td>單一 FQDN</td><td>FQDN 格式</td></tr>
<tr><td>72</td><td>IP 位址清單, 由 “,” 分隔</td><td>IPv4 格式, 由 “,” 分隔</td></tr>
<tr><td>114</td><td>單一 URL</td><td>URL 格式</td></tr>
<tr><td>Enable(啓動)</td><td>預設未勾選</td><td colspan="3">勾選 Enable (啓動) 方框啓動此設定。</td></tr>
<tr><td>Save (保存)</td><td>無</td><td colspan="3">點擊 Save (保存) 按鈕以保存設定。</td></tr>
<tr><td>Undo (還原)</td><td>無</td><td colspan="3">按下 Undo (還原)按鈕, 畫面將返回, 但沒有任何更改。</td></tr>
</table>

第 4 章 場域通訊

4.1 匯流排(Bus)& 協定(Protocol)

將 RS-232 或 RS-485 序列設備連線到 IP 基礎的區域網 LAN，閘道可以為序列通信配備序列埠。透過這些通訊協定，可以方便地進入區域網路或網際網路上任何地方的序列設備。這些可能是 " Virtual COM)" 和 " Modbus"。



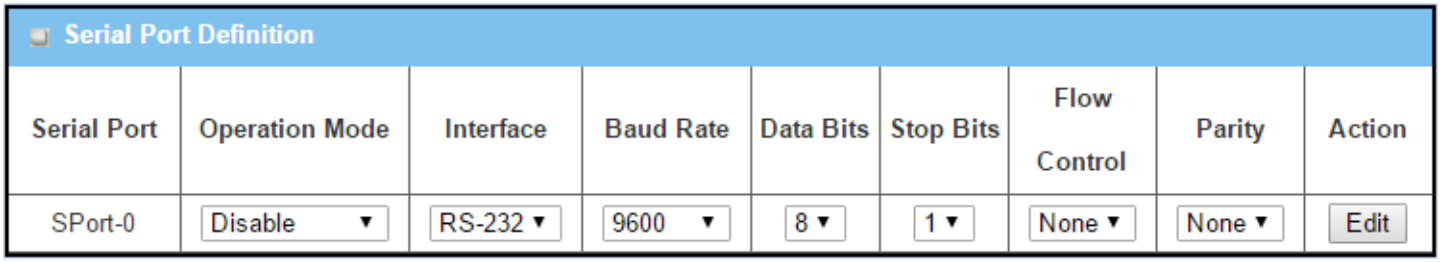
4.1.1 埠的設定

在使用受支援的場域通信功能 (如虛擬 COM 或 Modbus) 之前，您需要先設定實體通訊連線埠。
埠設定畫面允許使用者為每個序列介面設定操作模式和實體層設定, 還可以快速從一個通訊協定切換到序列埠。受支援的協定的埠數和類型將因閘道器型號而異。

設定埠設定

轉到 Field Communication > Bus & Protocol > Port Configuration 頁面

在 " Port Configuration (埠設定)" 頁面中，序列埠設定只有一個設定視窗。使用 " Configuration (設定)" 視窗，您可以指定序列埠參數，包括操作模式為 " Virtual COM (虛擬 COM)"、"Modbus"或停用，介面為 “RS-232” 或 “RS-485” 、鮑率、資料位長度、停止位長度，流量控制為 “RTS/CTS” ，“DTS/DSR” 或 “None (無)” 以及校驗。

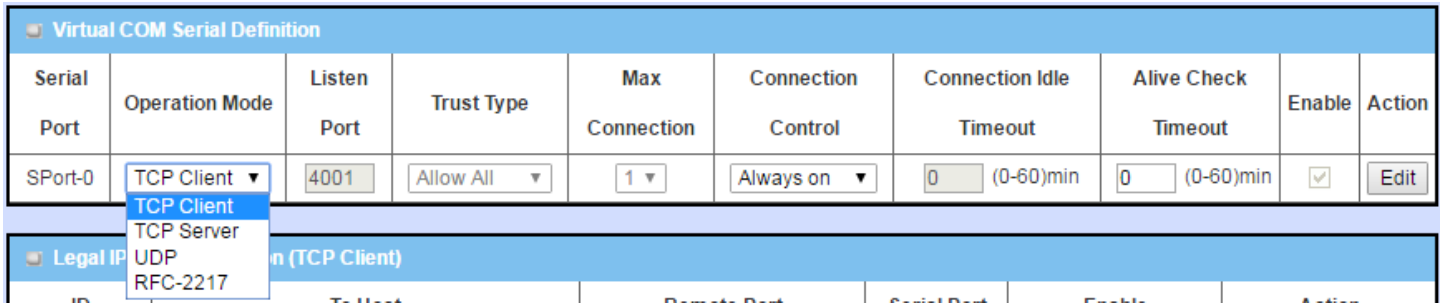


Port Configuration Window (埠設定視窗)		
項目	**設定值**	**說明**
Serial Port (序列埠)	*無*	顯示序列埠 ID。 序列埠的數量將因閘道器型號而異。
Operation Mode (操作模式)	預設設定 Disable (禁用)	顯示序列介面目前選擇的操作模式。根據型號的不同, 可用的模式可能是 Virtual COM、Modbus, 和 IEC 60870-5.。
Interface (介面)	預設設定RS-232	選擇 RS-232 或 RS-485 實體介面以連接到具有相同介面規範的登入設備。
Baud Rate (鮑率)	預設設定19200	為序列設備通信選擇適當的鮑率。 RS-232: 1200/2400/4800/9600/19200/38400/57600/115200 RS-485 可以使用較高的 230400 和 460800 鮑率。取決於電纜長度和安裝環境。
Data Bits	預設設定8	選擇 8 或 7。
Stop Bits	預設設定1	選擇 1 或 2。
Flow Control (流量控制)	預設設定None (無)	選擇 None/RTS、CTS/DTS、DSR RS-232 模式中的流量控制。 依型號支援流量控制。
Parity (奇偶校	預設設定None (無)	選擇 None(無) / Even(偶數) / Odd(奇數)/用於奇偶校驗。

驗)		
Action (行動)	無	按一下**Edit(編輯)**按鈕以更改操作模式，或修改上面列出用於序列介面通信的參數。
Save (保存)	無	點擊 **Save (保存)** 按鈕以保存設定值。
Undo (還原)	無	點擊 **Undo (還原)** 按鈕以取消設定值。

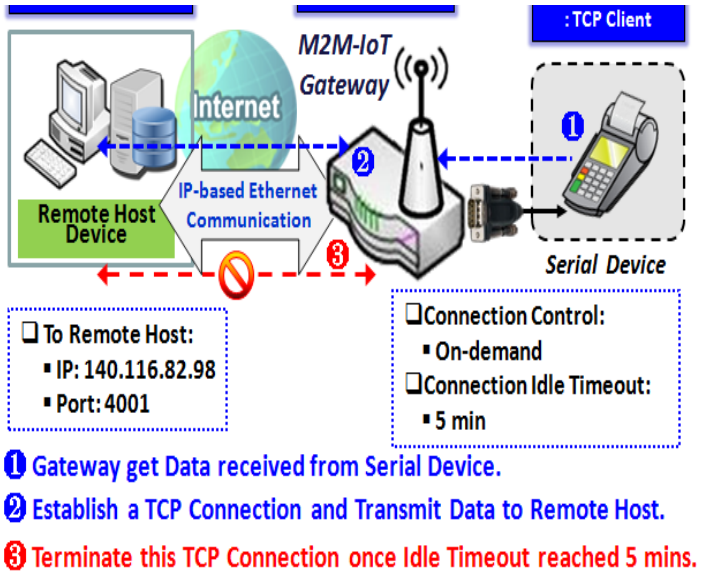
4.1.2 Virtual COM (虛擬 COM)

在用戶的PC /主機上建立一個虛擬COM埠，以提供連線到閘道器序列埠的序列設備。這將允許透過Internet(固網或行動通訊網路)來控制和管理連線的序列設備。這也被稱為乙太網直通通訊。



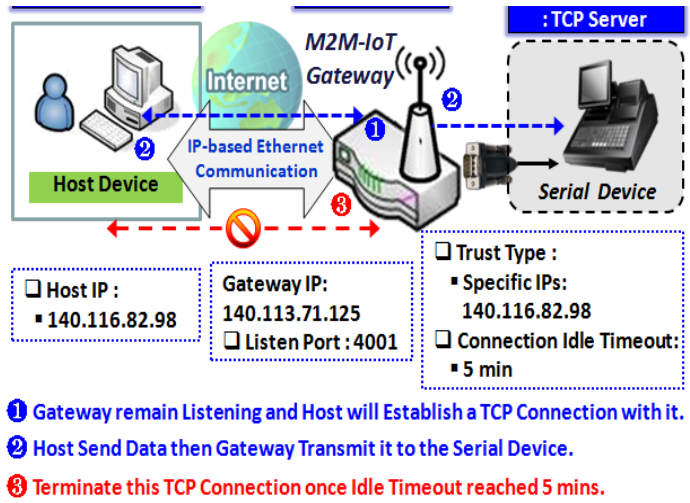
虛擬 COM 設定畫面允許用戶將虛擬 COM 埠的設備連線到網路，以便可以遠端登入序列資料。可用於遠端登入連線的序列設備的停用、TCP 客戶端、TCP 伺服器、UDP 和 RFC2217 模式。這些操作模式如下圖所示。

TCP Client 客戶端模式



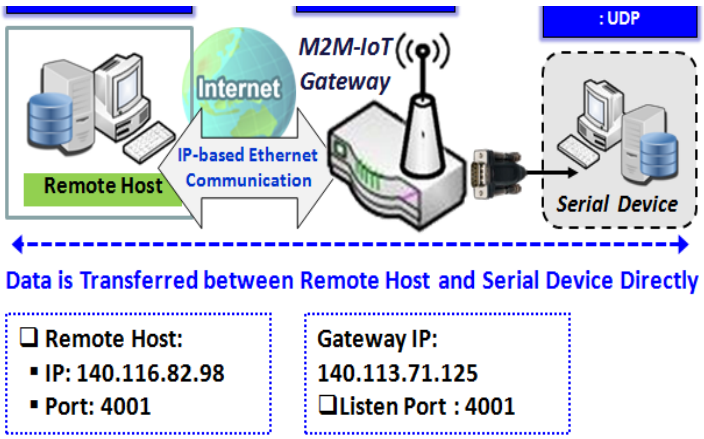
當管理員希望閘道器在序列資料到達時主動建立與預定主機的 TCP 連線時，“虛擬 COM”功能的操作模式需要為“TCP Client (TCP 客戶端)”，並且當虛擬 COM 的連線控制是“On-demand (需要時)”，一旦閘道器從連線的序列設備接收到資料，建會立 TCP 連線並將接收到的序列資料傳送到遠端主機。資料傳送完成後，閘道器會自動使用 TCP 存活檢查逾時或空閒逾時設定，切斷 TCP 通訊和主機的連線。

TCP Server 伺服器模式



當管理員希望閘道器為主機設備的序列資料請求被動等待時，且主機將建立 TCP 連線以從序列設備獲取資料時，“Virtual COM”功能的操作模式需設為“TCP Server”。在這種模式下，閘道器在 TCP/IP 網路上提供唯一的“IP：埠”位址。其最多支援 4 個同時連線，因此多個主機可以同時從同一個序列設備收集資料。資料傳送完成後，將使用 TCP 活動檢查逾時或空閒逾時的設定，將 TCP 連線自動從主機斷線。

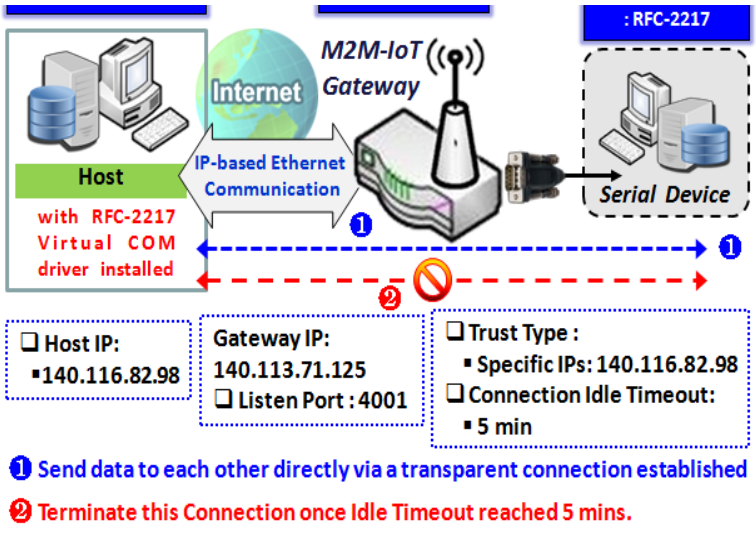
UDP 模式



如果遠端主機和序列設備都需要在需要時啟動資料傳送，則閘道器中“Virtual COM”功能的操作模式必須為“UDP”。在這種模式下，UDP 資料可以在閘道器和多台主機之間傳送，這種模式非常適合用來顯示訊息。

遠端主機可以透過閘道器直接發送 UDP 資料到序列設備，同時也可以透過閘道器從序列設備接收 UDP 資料。閘道器最多支援 4 台合法主機同時透過閘道器連線到序列設備。

RFC-2217 模式



RFC-2217 定義了 Telnet 基礎協定的通用 COM 埠控制選項。安裝有 RFC-2217 驅動程式的主機可以監視和管理連線到閘道器序列埠的遠端序列設備，就像連線到本地序列埠一樣。當本地序列設備上的虛擬序列埠建立時，需要指定與之建立連線主機的 IP 位址。

任何支援 RFC-2217 的第三方驅動程式都可以安裝在主機中。驅動程式透過將閘道器序列埠的 IP 埠映射到主機上的虛擬本地 COM 埠 (IP:Port)，在主機和序列設備之間建立通透連線。

主機可以透過閘道器直接向序列設備發送資料，同時也可以透過閘道器從序列設備接收資料。閘道器最多支援 4 台網路主機。

設定虛擬 COM

虛擬 COM 設定畫面允許用戶將虛擬 COM 埠的設備連線到網路，允許用戶遠登入序列資料。包含有遠登入連線的序列設備的禁用、TCP 客戶端、TCP 伺服器、UDP 和 RFC2217 模式。預設設定為禁用模式。

若要使用虛擬 COM 功能，首先請設定多功能序列埠的操作模式。進入 **Field Communication > Bus & Protocol > Port Configuration** 頁面，選擇虛擬 COM 作為預設操作模式，並完成相關埠設定。然後再從左邊 Menu 先點選 **Field Communication > Bus & Protocol >再點選頁面上方 Virtual COM** Tab 獲得關於虛擬 COM 設定的詳細設定。

啓動 TCP Client 模式

您可以將閘道器設定為 TCP (Transmission Control Protocol 傳送控制協定)客戶端。在 TCP 客戶端模式下，當有資料要傳送時，設備會啟動與 TCP 伺服器的 TCP 連線。當連線處於空閒狀態且達到指定的時間時，設備將從伺服器斷線。您也可以啟用 TCP 伺服器全時連線。

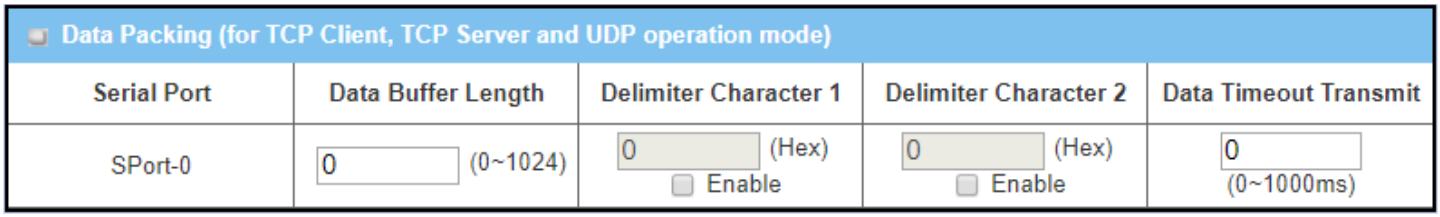
Operation Mode Definition for each Serial Port

Serial Port	Operation Mode	Listen Port	Trust Type	Max Connection	Connection Control	Connection Idle Timeout	Alive Check Timeout	Enable	Action
SPort-0	TCP Client	N/A	N/A	N/A	Always on	N/A	N/A	☐	Edit

Enable TCP Client Mode Window (啓動 TCP 客戶端視窗)		
項目	**設定值**	**說明**
Operation Mode (操作模式)	必要設定	選擇 **TCP 客戶端**.
Connection Control (連線控制)	預設 **Always on (保持啓動)**	選擇 Always on 保存 TCP 連線。否則選擇 On-Demand (依照需求)僅在需要傳輸時啟動 TCP 連線，並在空閒超時時斷開連線。
Connection Idle Timeout (連線空閒超時)	1. 預設設定 0 2. 範圍 0 至 60 分鐘.	輸入空閒超時 (分鐘)。 超過空閒超時斷開 TCP 連線。 只有在 **Connection Control (連線控制)**欄位中選擇了 **On-Demand (依照需求)**時，空閒超時才可用。
Alive Check Timeout (活動檢	1. 預設設定 0 2. 範圍 0 至 60 分鐘.	輸入活動檢查超時的時間段。如果 TCP 連線沒有收到活動檢查的回應時間超過此超時設定， 將會被終止

查超時)		
Enable (啓動)	預設未勾選	勾選 **Enable (啟用)**方框指定的操作模式啟動相應的序列埠。
Save (保存)	*無*	按下 Save (保存) 按鈕以保存設定值

指定資料封包(Data Packing)參數



Data Packing Configuration (資料封包參數設定)		
項目	**設定值**	**說明**
Data Buffer Length (資料緩衝區長度)	1. 可選設定 2. 預設值 0	輸入序列埠的資料緩衝區長度。 ***範圍值*** : 0 ~ 1024.
Delimiter Character 1 (分隔符號字元 1)	1. 可選設定 2. 預設值 0	勾選 **Enable(啟用)**方框啟動分隔符號字元 1, 然後輸入十六進位代碼。 ***範圍值*** : 0x00 ~ 0xFF.
Delimiter Character 2 (分隔符號字元 2)	1. 可選設定 2. 預設值 0	勾選 **Enable(啟用)**方框啟動分隔符號字元 2, 然後輸入十六進位代碼。 ***範圍值*** : 0x00 ~ 0xFF.
Data Timeout Transmit (資料超時傳輸)	1. 可選設定 2. 預設值 0	輸入傳輸序列資料的資料超時間隔。 預設設定為 0，禁用超時功能。 ***範圍值*** : 0 ~ 1000ms.
Save (保存)	*無*	按下 Save (保存) 按鈕以保存設定值

指定遠端 TCP Server 伺服器

Legal Host IP/ FQDN Definition (for TCP Client operation mode)

ID	To Remote Host	Remote Port	Serial Port	Definition Enable	Action
1		4001	SPort-0	☐	Edit
2		4001	SPort-0	☐	Edit
3		4001	SPort-0	☐	Edit
4		4001	SPort-0	☐	Edit

Specify TCP Server Window (指定 TCP 伺服器視窗)		
項目	**設定值**	**說明**
To Remote Host (到遠端主機)	必要設定	按 **Edit (編輯)**按鈕可輸入遠端 TCP 伺服器的 IP 位址或 FQDN 以傳輸序列資料。
Remote Port (遠端埠)	1. 必要設定 2. 預設設定 4001	輸入 TCP 埠編號。這是遠端 TCP 伺服器的監聽埠。 ***範圍值*** : 1 ~ 65535.
Serial Port (序列埠)	預設設定 SPort-0	套用 TCP 伺服器連線到選擇的序列埠。每個序列埠可同時配置多達 4 個 TCP 伺服器。
Definition Enable (定義啟用)	預設未勾選	勾選 **Enable (啟用)**方框啟用 TCP 伺服器設定。
Save (保存)	*無*	按下 Save (保存) 按鈕以保存設定值

啓動 TCP Server 伺服器模式

將閘道器設定為 TCP(Transmission Control Protocol 傳送控制協定)伺服器。 TCP 伺服器等待由遠端 TCP 客戶端設備發起連線以接收序列資料。該設定允許用戶指定特定的 TCP 客戶端或允許任何序列資料傳送頻寬控制和登入控制發送序列資料。 TCP 伺服器最多支援 4 個同步連線來接收來自多個 TCP 客戶端的序列資料。

Operation Mode Definition for each Serial Port

Serial Port	Operation Mode	Listen Port	Trust Type	Max Connection	Connection Control	Connection Idle Timeout	Alive Check Timeout	Enable	Action
SPort-0	TCP Server	4001	Allow All	1	N/A	0	0	☐	Edit

Enable TCP Server Mode Window (啓動 TCP 伺服器模式視窗)		
項目	**設定值**	**說明**
Operation Mode (操作模式)	必要設定	選擇 **TCP Server (TCP 伺服器)**模式。
Listen Port (監聽埠)	預設 4001	顯示 TCP 連線的監聽埠。 ***範圍值*** : 1 ~ 65535.
Trust Type (信任類型)	預設 **Allow Al**	選擇 **Allow All(允許全部)**允許任何 TCP 客戶端連線。否則請選擇 **Specific IP(特定 IP)**限制某些 TCP 客戶端。
Max Connection (最大連線)	1. 最大 4 個連線 2. 預設 1	設定 TCP 同時連線的最大數目。可以建立多達 4 個 TCP 同時連線。 ***範圍值*** : 1 ~ 4.
Connection Idle Timeout (連線空閒超時)	預設值 0	輸入空閒超時 (分鐘)。 超過空閒超時斷開 TCP 連線。 只有在 **Connection Control (連線控制)**欄位中選擇了 **On-Demand (依照需求)**時，空閒超時才可用。
Alive Check Timeout (活動檢查超時)	預設值 0	輸入活動檢查超時的時間段。如果 TCP 連線沒有收到活動檢查的回應時間超過此超時設定， 將會被終止
Enable (啓動)	預設未勾選	勾選 **Enable (啟用)**方框指定的操作模式啟動相應的序列埠。
Save (保存)	*無*	點擊 **Save (保存)** 按鈕以保存設定值。

為登入 TCP Server 伺服器指定 TCP Client 客戶端

如果您選擇特定 IP 作為信任的類型，則會出現 “Trusted IP Definition (可信任 IP 定義)” 畫面。 這些設定對 TCP 伺服器和 RFC-2217 模式都有效。

Trusted IP Definition (for TCP Server & RFC-2217 operation mode)

ID	Host	Serial Port	Definition Enable	Action
1			☐	Edit
2			☐	Edit
3			☐	Edit
4			☐	Edit
5			☐	Edit
6			☐	Edit
7			☐	Edit
8			☐	Edit

Specify TCP Clients Window (指定 TCP 客戶端視窗)		
項目	**設定值**	**說明**
Host (主機)	必要設定	輸入允許的 TCP 客戶端的 IP 位址範圍。
Serial Port (序列埠)	預設未勾選	勾選該方框指定所選序列埠的規則。
Definition Enable (定義啟動)	預設未勾選	勾選 **Enable(啟用)**方框啟用該規則。
Save (保存)	無	點擊 **Save (保存)** 按鈕以保存設定值
Undo (還原)	無	點擊 **Undo (還原)** 按鈕以取消設定

啓動 UDP 模式

UDP (User Datagram Protocol)可使 UDPSocket 程式能夠與序列伺服器 Serial Server 上的序列埠 Serial Port 進行通信。 UDP 模式提供非連接協議的通信模式，使您能夠將資料從序列設備羣組播 Multicast 送到多台主機，反之亦然，因此這種模式非常適用套用於顯示訊息。

Operation Mode Definition for each Serial Port

Serial Port	Operation Mode	Listen Port	Trust Type	Max Connection	Connection Control	Connection Idle Timeout	Alive Check Timeout	Enable	Action
SPort-0	UDP	4001	N/A	N/A	N/A	N/A	N/A	☐	Edit

Enable UDP Mode Window (啓動 UDP 模式視窗)		
項目	設定值	說明
Operation Mode(操作模式)	必要設定	選擇 **UDP** 模式。
Listen Port (監聽埠)	預設值 4001	顯示 UDP 連線的監聽埠。 ***範圍值*** : 1 ~ 65535
Enable (啓動)	預設未勾選	勾選 Enable (啓動)方框指定的操作模式啟動對應的序列埠。
Save (保存)	無	點擊 Save (保存) 按鈕以保存設定值
Undo (還原)	無	點擊 Undo (還原) 按鈕以取消設定

指定遠端 UDP

Legal Host IP Definition (for UDP operation mode)

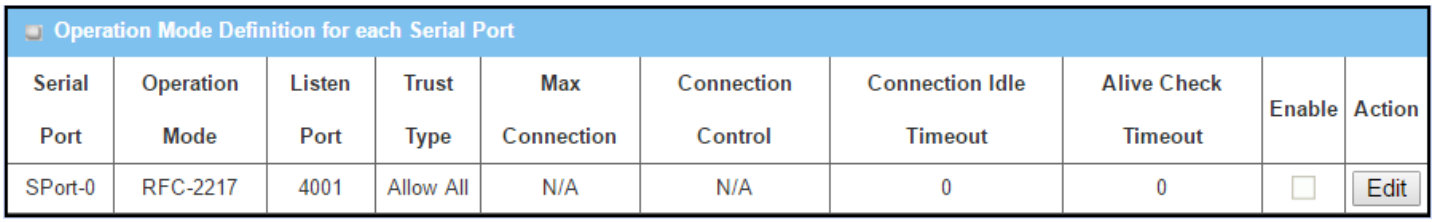
ID	Remote Host	Remote Port	Serial Port	Definition Enable	Action
1		4001	SPort-0	☐	Edit
2		4001	SPort-0	☐	Edit
3		4001	SPort-0	☐	Edit
4		4001	SPort-0	☐	Edit

Specify Remote UDP hosts Window (指定遠端 UDP 主機視窗)		
項目	設定值	說明
Host (主機)	必要設定	按 **Edit(編輯)**按鈕可輸入遠端 UDP 主機的 IP 位址範圍。
Remote Port (遠端埠)	預設值 4001	顯示節點 UDP 主機的 UDP 埠。 ***範圍值*** : 1 ~ 65535
Serial Port (序列埠)	預設設定 SPort-0	套用 UDP 主機到選擇的序列埠。每個序列埠同時配置多達 4 個 UDP 伺服器。
Definition Enable (定義啟動)	預設未勾選	勾選 **Enable(啟用)**方框啟用該規則。

Save (保存)	無	點擊 Save (保存) 按鈕以保存設定值
Undo (還原)	無	點擊 Undo (還原) 按鈕以取消設定

啓動 RFC-2217 Mode 模式

RFC-2217 定義了 Telnet 基礎協定的通用 COM 埠控制選項。使用 RFC-2217 模式，遠端主機可以監視和管理遠端序列連線的設備，就像連線到本地序列埠一樣。當建立本地序列設備上的虛擬序列埠時，需要指定建立連線的遠端主機的 IP 位址。



Operation Mode Definition for each Serial Port

Serial Port	Operation Mode	Listen Port	Trust Type	Max Connection	Connection Control	Connection Idle Timeout	Alive Check Timeout	Enable	Action
SPort-0	RFC-2217	4001	Allow All	N/A	N/A	0	0	☐	Edit

Enable RFC-2217 Mode Window		
項目	**設定值**	**說明**
Operation Mode (操作模式)	必要設定	選擇 **FC-2217** 模式。
Listen Port (監聽埠)	4001 is set 預設	顯示 **FC-2217** 連線的監聽埠。 ***範圍值*** : 1 ~ 65535.
Trust Type (信任類型)	**Allow All** is set 預設	選擇 **Allow All(允許全部)**允許任何客戶端連線。否則請選擇 **Specific IP(特定 IP)**限制某些客戶端。
Connection Idle Timeout (連線空閒超時)	預設值 0	輸入空閒超時 (分鐘)。 超過空閒超時斷開 TCP 連線。 只有在 **Connection Control (連線控制)**欄位中選擇了 **On-Demand (依照需求)**時，空閒超時才可用。
Alive Check Timeout (活動檢查超時)	預設值 0	輸入活動檢查超時的時間段。如果 TCP 連線沒有收到活動檢查的回應時間超過此超時設定， 將會被終止
Enable (啓動)	預設未勾選	勾選 **Enable (啟用)**方框指定的操作模式啟動相應的序列埠。
Save (保存)	無	點擊 **Save (保存)** 按鈕以保存設定值
Undo (還原)	無	點擊 **Undo (還原)** 按鈕以取消設定

指定登入的遠端主機

如果您選擇特定 IP 作為信任類型，則出現 “Trusted IP Definition (可信任 IP 定義)” 畫面。這些設定對 TCP 伺服器和 RFC-2217 模式都有效。

Trusted IP Definition (for TCP Server & RFC-2217 operation mode)

ID	Host	Serial Port	Definition Enable	Action
1			☐	Edit
2			☐	Edit
3			☐	Edit
4			☐	Edit
5			☐	Edit
6			☐	Edit
7			☐	Edit
8			☐	Edit

Specify RFC-2217 Clients for Access Window (指定 RFC-2217 客戶端登入視窗)		
項目	**設定值**	**說明**
Host (主機)	必要設定	輸入允許的客戶端的 IP 位址範圍。
Serial Port (序列埠)	預設未勾選	勾選該方框指定所選序列埠的規則。
Definition Enable (定義啟動)	預設未勾選	勾選 **Enable(啟用)**方框啟用該規則。
Save (保存)	無	點擊 **Save (保存)** 按鈕以保存設定值
Undo (還原)	無	點擊 Undo (還原) 按鈕以取消設定

.1.3 Modbus

Modbus 是世界上最流行的自動化協定之一，支援傳統的 RS-232/422/485 設備和最新開發的網路設備。許多工業設備，如 PLC、DCS、HMI、儀表和智慧儀表都使用 Modbus 協定作為通信標準。其用於建立人工智慧設備之間的主從通信。

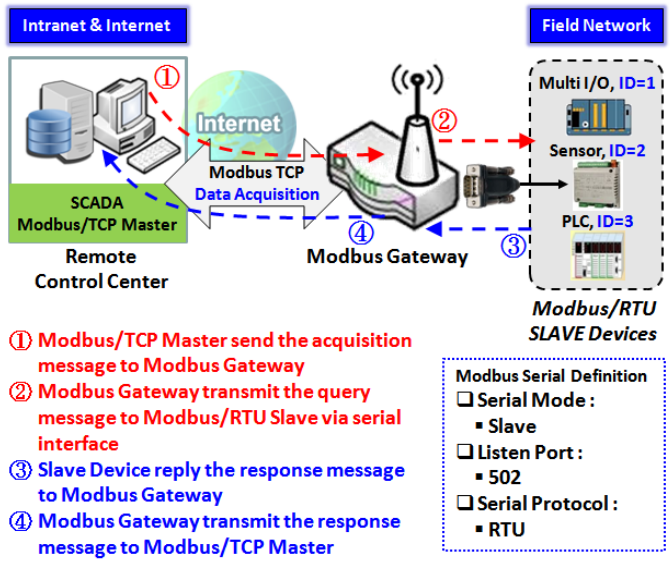
但是，網路基礎的 Modbus 協定與原始的序列基礎協定不同。為了合成 Modbus 網路，物聯網閘道器(包括一個或多個支援 RS-232 和 RS-485 通信介面的序列埠)可以在 Modbus TCP(Ethernet)和 Modbus RTU / ASCII(Serial)協定之間自動並智慧地進行轉換，允許網路基礎的 PLC 透過 RS-485 控制儀器，無需額外的程序或工作。

Serial Port Definition

Serial Port	Operation Mode	Interface	Baud Rate	Data Bits	Stop Bits	Flow Control	Parity	Action
SPort-0	Modbus	RS-485	115200	8	1	None	None	Edit

注意：當 Modbus 設備連線到和物聯網 Modbus 閘道器的同一序列埠時，這些 Modbus 設備必須使用具有相同設定的相同協定(即具有相同 Baud Rate 設定的 Modbus RTU 或 Modbus ASCII)。

Modbus 閘道器應用案例

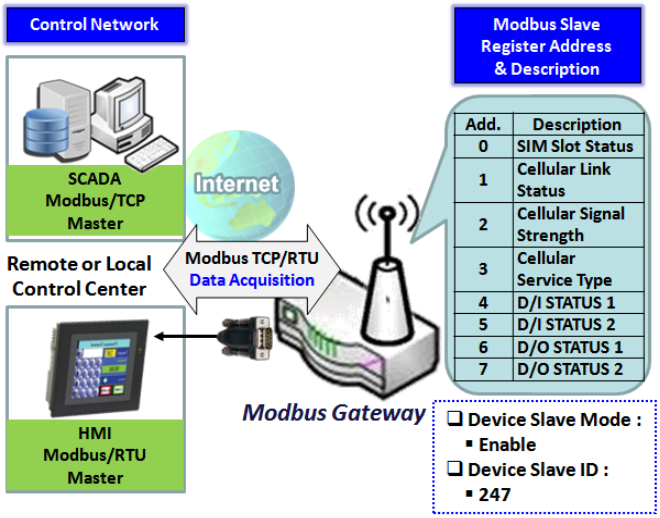


IoT 閘道器充當 Modbus 閘道器和位於遠端控制中心的 Modbus TCP Master (SCADA 伺服器)進行通信，以便登入擷取 Modbus 設備資料。

Modbus TCP Master 請求 IoT Gateway 閘道器透過 Internet access 去讀取或設定 Modbus 設備的資訊，例如資料採集或登錄器 Register/值的修改，IoT 閘道器做為資料轉發的閘道器。

在這種設定下，Modbus TCPMaster 向連接在 Modbus 閘道器的各種 Modbus / RTUSlave 設備請求資訊或發送控制命令。 Modbus 閘道器執行相關的指令將結果回覆給 Modbus / TCPMaster。

Modbus Slave(Modbus TCP Slave) Scenario



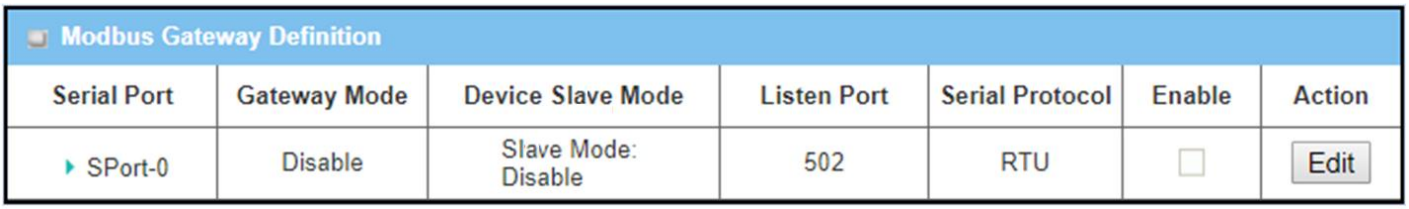
除了作爲 Modbus 閘道器之外，還有一個內建的 Modbus Slave 選項，用於透過 Modbus protocol 向遠端 Modbus Master 提供設備狀態，如 Cellular 和 DI/DO 狀態。啟用 Slave 選項後，Modbus TCP Master 可以向 IoT 閘道器即 Modbus TCP / RTU Slave (EW50)設備請求資訊或發送控制命令。物聯網閘道器執行相關程序並回覆 Modbus TCP Master。

Modbus 設定

轉到 Field Communication > Bus & Protocol > Modbus 頁面。

用戶可以在 Modbus 設定頁面面將閘道器設定作為 Modbus 閘道器執行，並允許在連線到區域網網路的 Modbus TCP 設備和連線到閘道器序列埠的 Modbus RTU / ASCII 設備之間進行登入。 一旦完成了本章節中的 Modbus 設定，請在埠設定畫面中選擇 Modbus 操作模式。

為每個序列埠定義 Modbus Gateway 閘道功能



Modbus Gateway Definition (Modbus 閘道定義)		
項目	**設定值**	**說明**
Serial Port (序列埠)	無	顯示所使用的序列埠的名稱。例如 SPort-0。 序列埠的數量因型號而異。
Gateway Mode (閘道模式)	**預設設定 Disable (禁用)**	指定.Modbus 閘道模式選擇的序列埠。 可設定爲 **Disable (禁用)**, **Serial as Slave (隨從序列)**或 **Serial as Master (主控序列)**。 一個序列埠可以連線至一個 Modbus 主伺服器,，或菊鏈在一組的多個隨從設備。 **Disable (禁用)**: 禁用所選序列埠的 Modbus 閘道函數。 **Serial as Slave (隨從序列)**: 當於連線的序列設備全部是 Modbus 隨從設備時。 **Serial as Master (主控序列)**: 當所連線的序列設備是一個 Modbus 主設備時.
Device Slave Mode (設備隨從模式)	預設未勾選	勾選 Enable(**啟用)**框到啟動 Modbus 隨從功能，並輸入整合的的預選 ID，這功能可以作爲 Modbus 隨從設備，並且可以通過來自 SCADA 管理系統的傳統 Modbus 功能代碼進行登入。 下表中列出了支援的 Modbus 命令。。 ***範圍值***: 1 ~ 247.

Listen Port (監聽埠)	1. 預設 **502** 2. 範圍 1 到 65535	指定監聽埠編號 ，如果隨隨從設備已加到選擇的序列埠。如果連線了主控設備，則不需要設定。 ***範圍值***: 1 ~ 65535. 注意: 爲多個序列埠的產品，設定不同的序列埠編號。
Serial Protocol (序列協定)	預設設定 **RTU**	選擇所連線的周邊設備所採用的序列協定. 可能是 **RTU** 或 **ASCII**.
Enable (啓動)	無	顯示指定的 Modbus 為已啟用或禁用。要啟用或禁用 Modbus 支援, 轉到 **欄 Field Communication > Bus & Protocol > Port Configuration** 頁面, 並將操作模式設定為 **Modbus**。

指定閘道設定

Gateway Mode Configuration for SPort-0

Item	Setting
Response Timeout	1000 ms (1~65535)
Timeout Retries	0 times (0~5)
0Bh Exception	Enable
Tx Delay	Enable
TCP Connection Idle Time	300 sec (1~65535)
Maximum TCP Connections	1 connections (1~4)
TCP Keep-alive	Enable
Modbus Master IP Access	Allow All
Message Buffering	Enable

Gateway Mode Configuration for SPort-n (SPort-n 的閘道模式設定)		
項目	**設定值**	**說明**
Response Timeout (回覆超時)	預設設定 **1000 ms**	設定主控發送請求到隨從伺服器的回覆超時。 如果隨從在指定時間內未回覆，則將丟棄資料。 這適用於序列連線的主控發送請求到遠端隨從，或從遠端主伺服器發送請求到序列連線的隨從. ***範圍值***: 1 ~ 65535.
Timeout Retries (超時重試次數)	預設值 **0**	如果隨從伺服器未回覆主控請求, 則閘道將重新發送存儲在緩衝區中的請求。如果超時重試設定為 null (值為 0)，則閘道不會緩衝主控請求。如果指

		定了零以外的值，閘道會將主控請求存儲在緩衝區中，然後重試發送請求至指定的次數。 一旦重試用盡，閘道將向主控伺服器發送一條錯誤訊息。但是，如果勾選了 "0Bh Exception (0Bh 異常)" 方框 (見下列)，將會發送一個 0Bh 十六進位代碼的錯誤訊息。 ***範圍值***: 0 ~ 5.
0Bh Exception (0Bh 異常)	預設未勾選	勾選 **Enable(啟用)**方框可啟用，閘道將 0Bh 異常代碼訊息發送到 Modbus 主機以顯示隨從設備在超時間隔內未回覆。
Tx Delay (Tx 延遲)	預設未勾選	勾選 **Enable(啟用)**方框可以啟動在收到回覆之前的到發送下一條訊息的最短時間。 啟用 tx 延遲時, 閘道器將在主請求之間插入 tx 延遲。延遲給了足夠的時間為隨從設備轉動他們的發射機和他們的接收器回到。 閘道器在主控請求之間插入一個 Tx 延遲。該延遲給予隨從設備足夠的時間來關閉它們的發射機並收回它們的接收機。

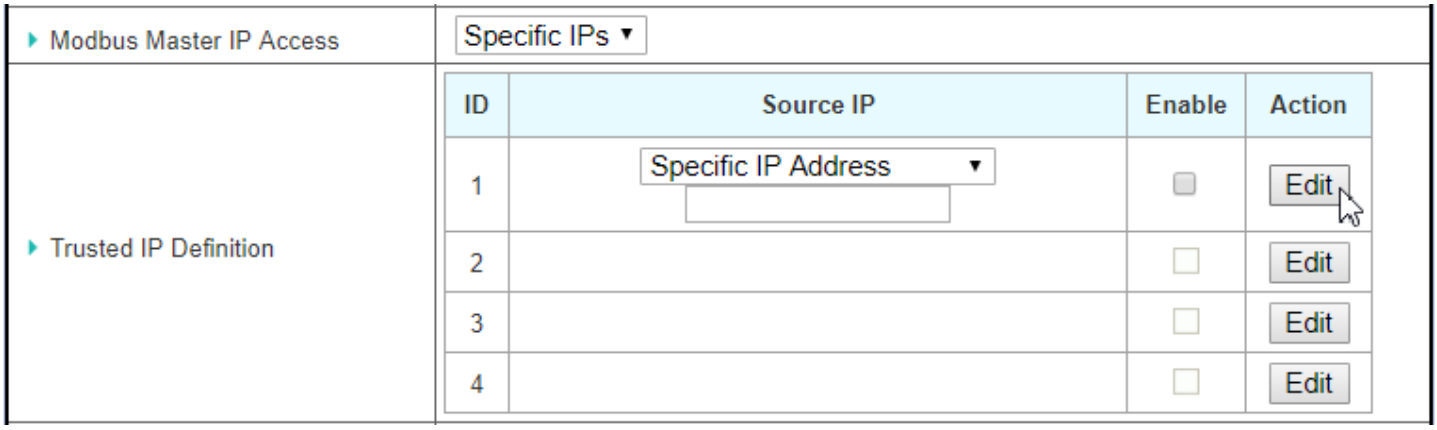
設定用於接收 Modbus Master 請求的 TCP / IP 連線

以下 Modbus TCP 設定項允許用戶設定 TCP 連線，以便遠端 Modbus 主站可以登入 Modbus 閘道器。也可讓用戶在 TCP 網路上指定授權的主設備。

項目	設定值	說明
TCP Connection Idle Time (TCP 連線閒置時間)	1. 預設設定 **300** 2. 範圍 1 到 65535	輸入空閒超時 (以秒為單位)。如果閘道器在執行空閒超時之前未收到其他 TCP 請求，將自動終止 TCP 連線。 ***範圍值***: 1 ~ 65535.
Maximum TCP Connections (最大 TCP 連線數)	1. 預設值 4 2. 範圍 1 至 4	輸入允許同時 TCP 連線的最大數目。 ***範圍值***: 1 ~ 4.
TCP Keep-alive (TCP 保持生存狀態)	預設未勾選	勾選 **Enable (啟用)**方框確保 TCP 保持連線。
Modbus Master IP Access (Modbus 主控 IP 登入)	預設選擇 **Allow All (允許全部)**。	指定 TCP 網路上的主控授權。 選擇 " **Allow All (全部允許)**" 允許任何主控主機到達附加的隨從伺服器。否則僅限特定主控經由設定 **Specific IPs(特定 IP)**連到達隨從。 當 **Specific IPs(特定 IP)**被勾選時，將出現 Trusted IP Definition(受信任的 IP 定義) 對話框。

在 TCP 網絡上指定可信任的 Modbus 主站

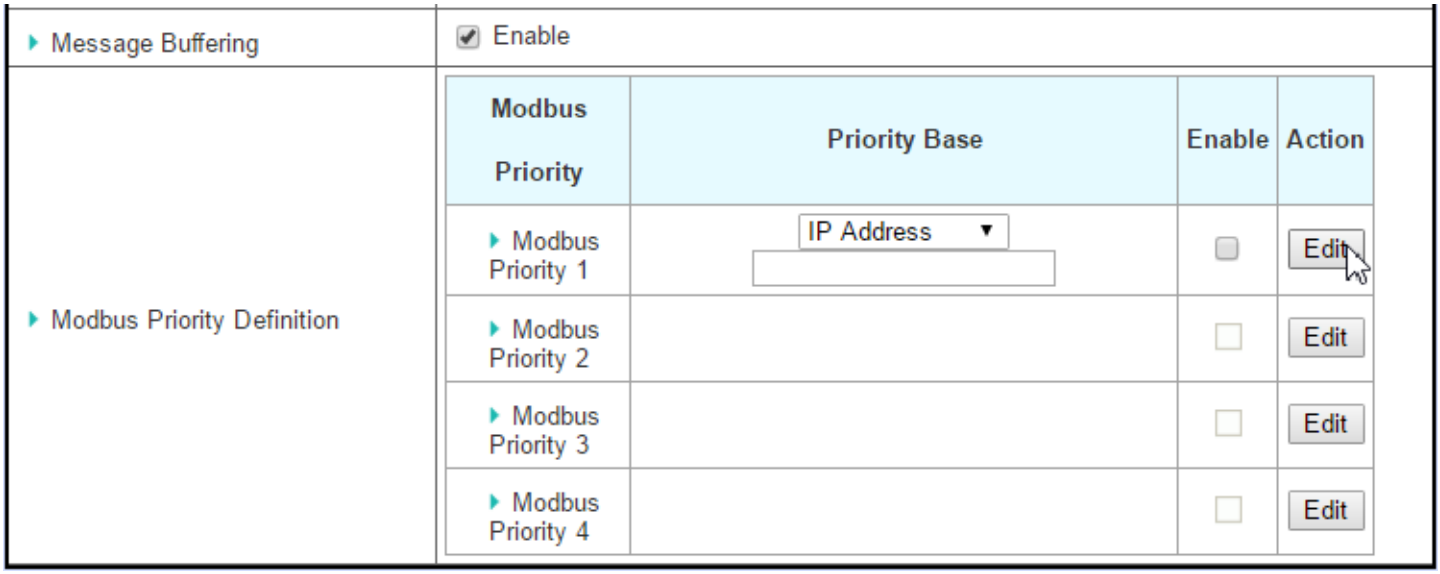
選擇特定 IP 時，使用者必須使用其 IP 地址指定主設備才能連線序列連線的隨從設備。



項目	設定值	說明
Source IP (來源 IP)	必要設定	選擇 **Specific IP Address (特定 IP 位址)**只讓允許的主控 IP 位址登入附加的隨從伺服器。 選擇 **IP Range (IP 範圍)**只讓允許的 IP 範圍 位址的主控登入附加的隨從伺服器。 選擇 **IP Address-based Group (IP 位址羣組)**, 只允許預先定義的主機 IP 位址羣組登入附加的隨從伺服器。 注意: 羣組必須預先定義， 然後此選項才可用。請參閱 **Object Definition > Grouping > Host grouping**。您還可以通過 增加規則捷徑按鈕登入羣組建立畫面。增加規則按鈕的設定也將出現在主機分組設定畫面中。 勾選 **Enable (啟用)**方框啟用此規則。
Enable	預設未勾選	勾選 **Enable (啟用)**方框啟用此規則。

定義 Modbus 順序

如上所述，必須啟用訊息緩衝才能優先排列發送主要請求至 Modbus 隨從站。點擊 **Edit(**編輯)按鈕以填寫優先設定。

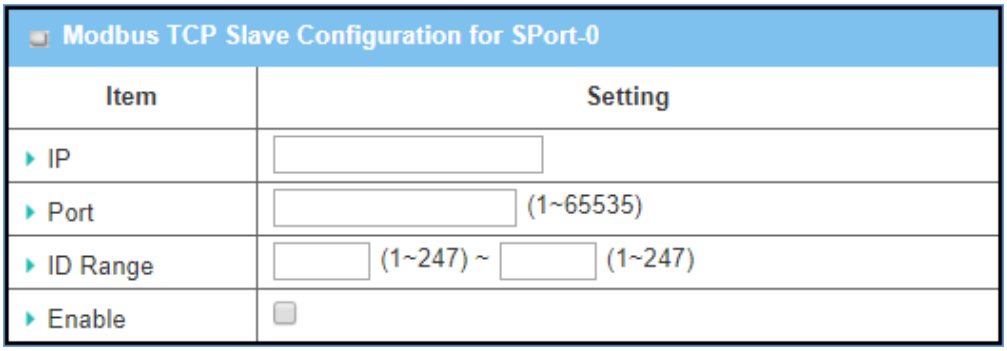


項目	設定值	說明
Message Buffering (訊息緩衝)	1. 預設未勾選 2. 緩衝多達 32 個請求	勾選 **Enable(啟用)**方框可緩衝多達 32 個來自該主機的請求。 如果勾選了 **Enable(啟用)**方框則會出現使用一個 " Modbus Priority Definition 優先順序定義 "對話框。如果請求來自遠端主機，或是遠端隨從 ID (如果請求來自序列連線的主控)，則可以進一步配置緩衝的主請求，以便將請求佇列優先順序設定為主控 IP 位址的隨從伺服器; 或者依照 **Function Code** 代碼。
Modbus Priority (優先順序)	無	用於設定指定的 Modbus 的優先順序清單。 Modbus Priority 1 ~ Modbus Priority 4。
Priority Base (優先權基數)	預設爲 IP Address	指定一個具有 **IP Address (IP 位址)**、**Slave ID (隨從 ID)**或 **Function Code(函數代碼)**。符合指定標識的緩衝 Modbus 訊將按照設定的優先級別進行處理。 如果請求來自遠端主控設備，則 Modbus 主控設備請求可根據主控設備的 IP 地址緩存到特定的優先佇列，如果請求來自序列連接的主控設備，或者由遠端主控設備發送的特定 **Function Code(函數代碼)**。
Enable (啓動)	預設未勾選	勾選 **Enable (啓動)** 方框以啓動優先設定。
Save (保存)	無	點擊 **Save (保存)** 按鈕以保持設定。

指定 Modbus TCP 隨從設備

如果 Modbus 主站設備連線到 Modbus 閘道器的序列埠，則使用者必須進一步指定 Modbus TCP 隨從站設備以向連線的 Modbus RTU/ASCII 主設備發送請求或從連線的 Modbus RTU/ASCII 主設備發送請求。

當按下 Add (新增) 按鈕，將會出現 **Modbus TCP Slave Configuration** (隨從站設定)畫面



Modbus Remote Slave Configuration (Modbus 遠端隨從設定)		
項目	**設定值**	**說明**
IP	必要設定	輸入遠端 Modbus TCP 隨從設備的 IP 位址。
Port (埠)	1. 必要設定 2. 範圍 1 到 65535	輸入遠端 Modbus TCP 隨從設備監聽的 TCP 埠(TCP 客戶端連線請求)。 ***範圍值***: 1 ~ 65535.
ID Range (ID 範圍)	範圍 1 到 247	輸入回應主控站請求的 Modbus TCP 隨從的 Modbus ID 範圍。 除了指定隨從站 IP 和埠，對於登入位於另一個 Modbus 閘道後面的遠端 Modbus RTU 隨從站，使用者還必須指定 Modbus RTU 隨從站的 Modus ID 範圍。 ***範圍值***: 1 ~ 247.
Enable (啓動)	預設未勾選.	勾選 Enable (啓動) 方框以啓動這個規則。
Save (保存)	無	點擊 Save (保存) 按鈕以保持設定。

支援整合 Modbus TCP Slave 的 Function Code

此用途可將閘道器設定為獨立的 Modbus Slave 設備。本地 SCADA 管理系統可將閘道器視為 Slave 設備，因此能夠讀取其資訊以進行設備監控。

目前整合 Modbus Modbus Slave 可支援下列登入閘道器的 3G/4G Modem 狀態的命令。

功能代碼：0x03(/讀)0×06(/寫)
位址：0 ~ 9999

Register Address	Register Name	Read/ Write	Register Range / Description
0	WAN-1 連線狀態	R	0 ~ 6, 0=已斷線, 1=連線中, 2=已連線, 3=斷線中, 5=等待傳輸, 6=已斷線
1	WAN-2 連線狀態	R	0 ~ 6, 0=已斷線, 1=連線中, 2=已連線, 3=斷線中, 5=等待傳輸, 6=已斷線
2	WAN-3 連線狀態	R	0 ~ 6, 0=已斷線, 1=連線中, 2=已連線, 3=斷線中, 5=等待傳輸, 6=已斷線
3	WAN-4 連線狀態	R	0 ~ 6, 0=已斷線, 1=連線中, 2=已連線, 3=斷線中, 5=等待傳輸, 6=已斷線
10	3G/4G_服務狀態	R	0 ~ 7, 0=2G, 1=無, 2=3G, 3=3.5G, 4~6=3.75G, 7=LTE
11	3G/4G_連線狀態	R	0 ~ 6, 0=已斷線, 1=連線中, 2=已連線, 3=斷線中, 5=等待傳輸, 6=已斷線
12	3G/4G_訊號強度	R	0 ~ 100
13	3G/4G_SIM_狀態	R	0: SIM 卡內建 PIN 碼 1: SIM 卡可用 2: 無 SIM 卡
14	3G/4G_MCC	R	MCC 值
15	3G/4G_MNC	R	MNC 值
16	3G/4G_CS 註冊器狀態	R	0: 未註冊, 1: 已註冊
17	3G/4G_PS 註冊器狀態	R	0: 未註冊, 1: 已註冊
18	3G/4G_漫遊狀態	R	0: 未漫遊, 1: 漫遊中
19	3G/4G_RSSI	R	RSSI 值
20	3G/4G_RSRP	R	RSRP 值

Register Address	Register Name	Read/ Write	Register Range / Description
21	3G/4G_RSRQ	R	RSRQ 值
30	3G/4G_模組-2_服務狀態	R	0 ~ 7, 0=2G, 1=無, 2=3G, 3=3.5G, 4~6=3.75G, 7=LTE
31	3G/4G_模組-2_連線狀態	R	0 ~ 6, 0=已斷線, 1=連線中, 2=已連線, 3=斷線中, 5=等待傳輸, 6=已斷線
32	3G/4G_模組-2_訊號強度	R	0 ~ 100
33	3G/4G_模組-2_SIM_狀態	R	0: SIM 卡內建 PIN 碼 1: SIM 卡可用 2: 無 SIM 卡
34	3G/4G_模組-2_MCC	R	MCC 值
35	3G/4G_模組-2_MNC	R	MNC 值
36	3G/4G_模組-2_CS 註冊器狀態	R	0: 未註冊, 1: 已註冊
37	3G/4G_模組-2_PS 註冊器狀態	R	0: 未註冊, 1: 已註冊
38	3G/4G_模組-2_漫遊狀態	R	0: 未漫遊, 1: 漫遊中
39	3G/4G_模組-2_RSSI	R	RSSI 值
40	3G/4G_模組-2_RSRP	R	RSRP 值
41	3G/4G_模組-2_RSRQ	R	RSRQ 值
70	ADSL_下載速度	R	ADSL 下載速度值 (kbps)
71	ADSL_上傳速度	R	ADSL 上傳速度值 (kbps)
72	ADSL SNR_下載	R	ADSL SNR 下載值 (dB)
73	ADSL SNR_上傳	R	ADSL SNR 上傳值 (dB)
74	ADSL 數據機連線狀態	R	0: 已斷線, 1: 已連線
101	VPN IPsec 通道 1 狀態	R	1: 已連線, 2: 等待傳輸, 3: 已斷線, 9: 連線中
102	VPN IPsec 通道 2 狀態	R	1: 已連線, 2: 等待傳輸, 3: 已斷線, 9: 連線中
103	VPN IPsec 通道 3 狀態	R	1: 已連線, 2: 等待傳輸, 3: 已斷線, 9: 連線中
104	VPN IPsec 通道 4 狀態	R	1: 已連線, 2: 等待傳輸, 3: 已斷線, 9: 連線中
105	VPN IPsec 通道 5 狀態	R	1: 已連線, 2: 等待傳輸,

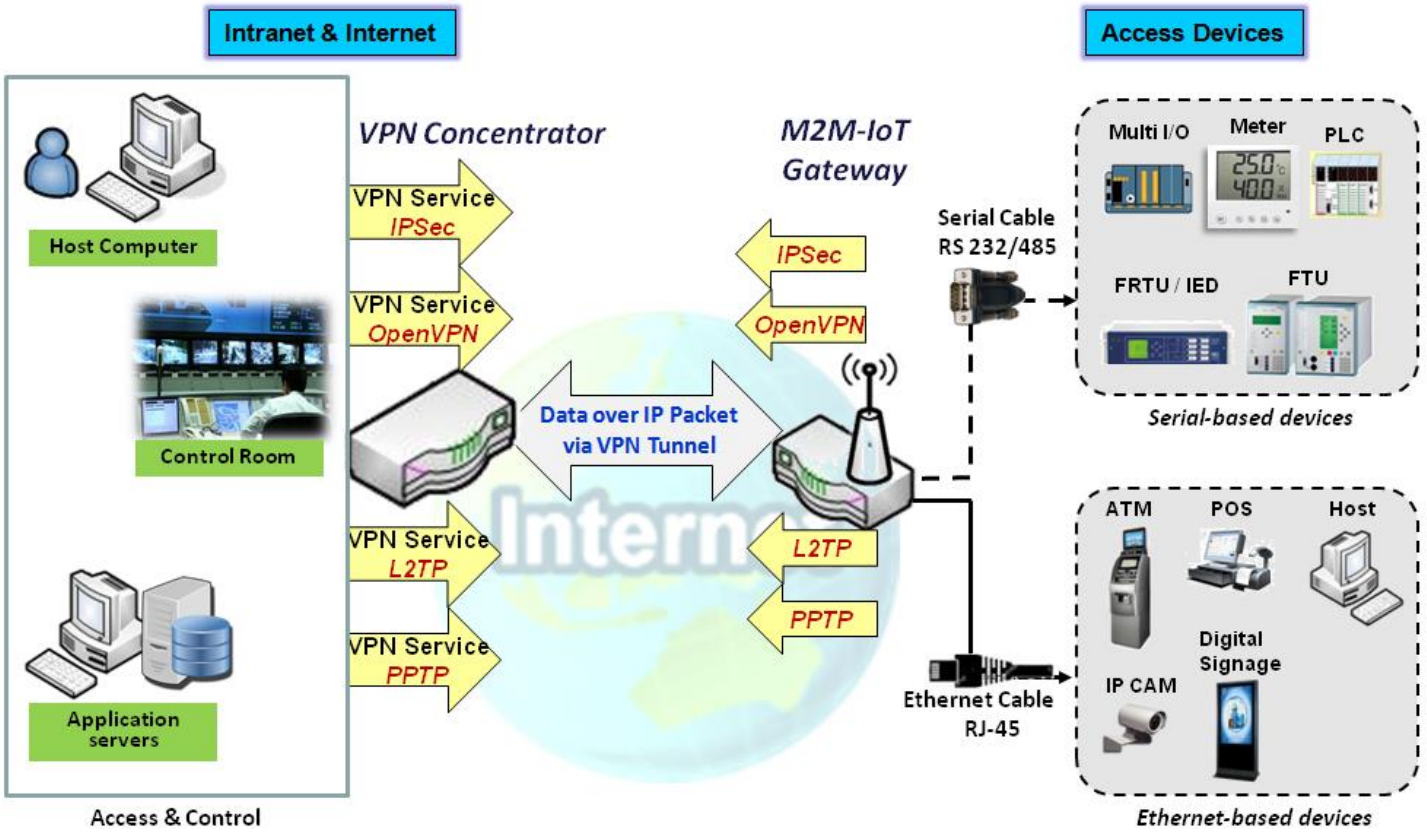
Register Address	Register Name	Read/ Write	Register Range / Description
			3: 已斷線, 9: 連線中
106	VPN IPsec 通道 6 狀態	R	1: 已連線, 2: 等待傳輸, 3: 已斷線, 9: 連線中
107	VPN IPsec 通道 7 狀態	R	1: 已連線, 2: 等待傳輸, 3: 已斷線, 9: 連線中
108	VPN IPsec 通道 8 狀態	R	1: 已連線, 2: 等待傳輸, 3: 已斷線, 9: 連線中
109	VPN IPsec 通道 9 狀態	R	1: 已連線, 2: 等待傳輸, 3: 已斷線, 9: 連線中
110	VPN IPsec 通道 10 狀態	R	1: 已連線, 2: 等待傳輸, 3: 已斷線, 9: 連線中
111	VPN IPsec 通道 11 狀態	R	1: 已連線, 2: 等待傳輸, 3: 已斷線, 9: 連線中
112	VPN IPsec 通道 12 狀態	R	1: 已連線, 2: 等待傳輸, 3: 已斷線, 9: 連線中
113	VPN IPsec 通道 13 狀態	R	1: 已連線, 2: 等待傳輸, 3: 已斷線, 9: 連線中
114	VPN IPsec 通道 14 狀態	R	1: 已連線, 2: 等待傳輸, 3: 已斷線, 9: 連線中
115	VPN IPsec 通道 15 狀態	R	1: 已連線, 2: 等待傳輸, 3: 已斷線, 9: 連線中
116	VPN IPsec 通道 16 狀態	R	1: 已連線, 2: 等待傳輸, 3: 已斷線, 9: 連線中
150	DI_狀態_1	R	0: OFF, 1: ON
151	DO_狀態_1	R / W	0: OFF, 1: ON
152	DI_狀態_2	R	0: OFF, 1: ON
153	DO_狀態_2	R / W	0: OFF, 1: ON
154	DI_狀態_3	R	0: OFF, 1: ON
155	DO_狀態_3	R/W	0: OFF, 1: ON

Register Address	Register Name	Read/ Write	Register Range / Description
156	DI_狀態_4	R	0: OFF, 1: ON
157	DO_狀態_4	(R/W)	0: OFF, 1: ON
201	序列埠-0_介面	R	1: RS-232, 3: RS-485
202	序列埠-0_ Baud Rate	R	Baud Rate 值
203	序列埠-0_Data Bits	R	7 或 8
204	序列埠-0_Stop Bits	R	1 或 2
205	序列埠-0_流量控制	R	0: 無, 2: RTS,CTS, 3: DTR,DSR
206	序列埠-0_奇偶校驗	R	0: 無, 1: 奇數, 2: 偶數
211	序列埠-1_介面	R	1: RS-232, 3: RS-485
212	序列埠-1_ Baud Rate	R	Baud Rate
213	序列埠-1_Data Bits	R	7 或 8
214	序列埠-1_Stop Bits	R	1 或 2
215	序列埠-1_流量控制	R	0: 無, 2: RTS,CTS, 3: DTR,DSR
216	序列埠-1_奇偶校驗	R	0: 無, 1: 奇數, 2: 偶數
221	序列埠-2_介面	R	1: RS-232, 3: RS-485
222	序列埠-2_ Baud Rate	R	Baud Rate 值
223	序列埠-2_Data Bits	R	7 或 8
224	序列埠-2_Stop Bits	R	1 或 2
225	序列埠-2_流量控制	R	0: 無, 2: RTS,CTS, 3: DTR,DSR
226	序列埠-2_奇偶校驗	R	0: 無, 1: 奇數, 2: 偶數
231	序列埠-3_介面	R	1: RS-232, 3: RS-485
232	序列埠-3_BaudRate	R	BaudRate 值
233	序列埠-3_Data Bits	R	7 或 8
234	序列埠-3_Stop Bits	R	1 或 2
235	序列埠-3_流量控制	R	0: 無, 2: RTS,CTS, 3: DTR,DSR
236	序列埠-3_奇偶校驗	R	0: 無, 1: 奇數, 2: 偶數
9999	重新開機	W	設定 1 爲系統重新開機

第 5 章 Security

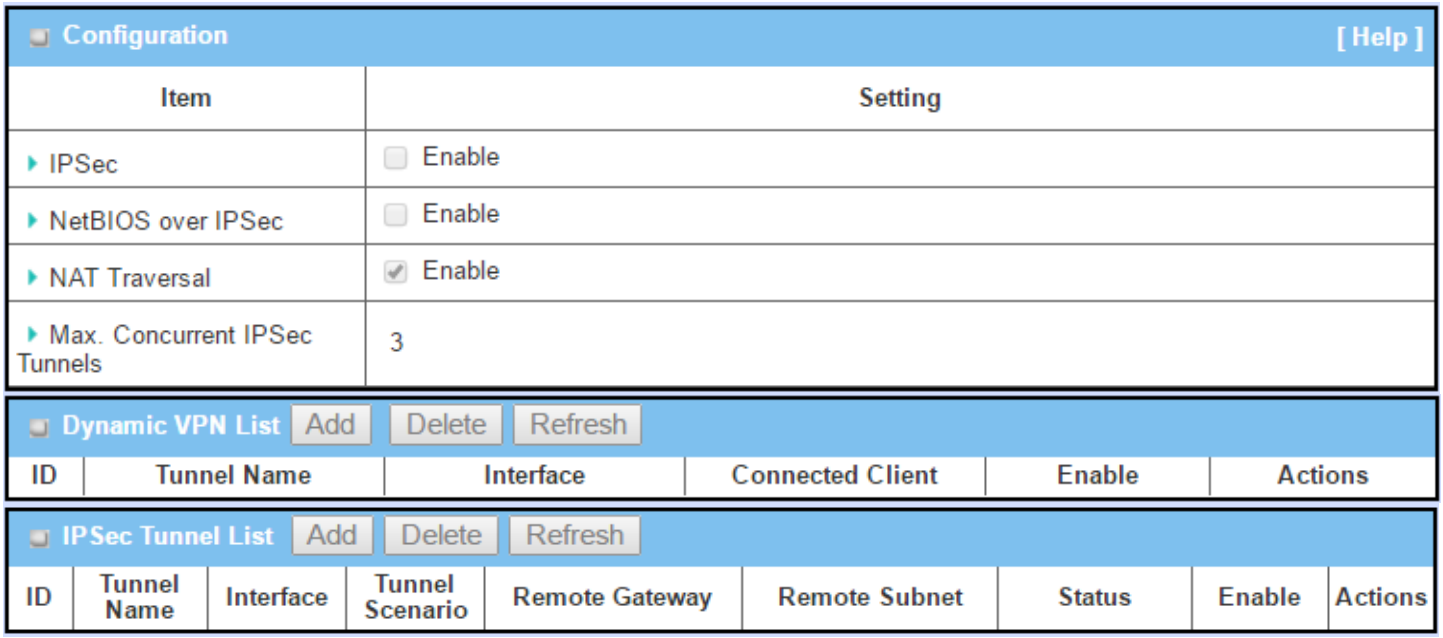
5.1 VPN

虛擬私人網路(VPN)透過公用網路(如網際網路)擴展私人網路。它使電腦能夠透過分享或公共網路發送和接收資料，就好像直接連線到私人網路一樣，同等於私人網路的功能、安全和管理策略。這是透過使用專屬連線、加密或兩者的組合來建立虛擬的點對點連線來完成。通道技術利用封裝協定、加密演算法和Hash演算法來支援資料機密性、資料來源認證和網路資訊的資料完整性。



該產品系列支援不同的通道技術，以在多個站點之間建立用於資料傳輸的安全通道，例如IPsec、OpenVPN、L2TP(over IPsec)，PPTP和GRE。 此外還支援一些進階功能，如全通道、Tunnel Failover通道容錯移轉、通道負載平衡Tunnel Load Balance、IPsec上的NetBIOS、NATTraversal和動態Dynamic VPN。

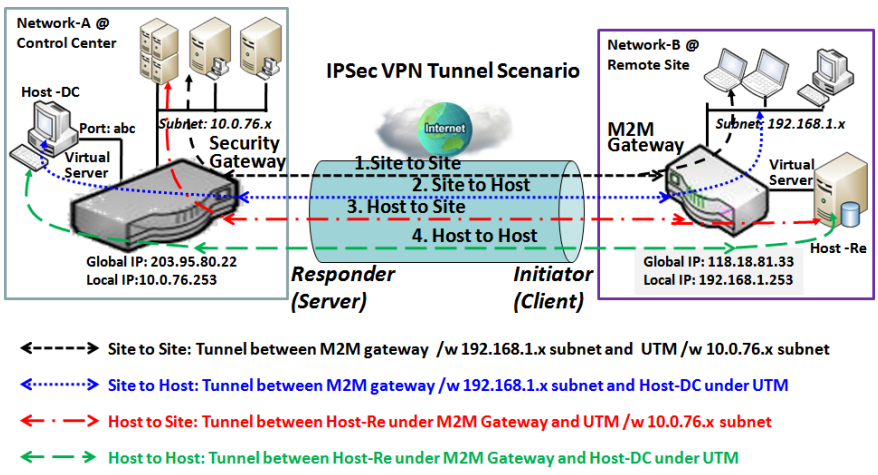
5.1.1 IPsec



網際網路協定安全(Internet Protocol Security IPsec)是一種透過驗證和加密每個 IP 通信階段資料封包來保護網際網路協定(IP)通信的協定套件。IPsec 包括協定於階段開始時建立代理之間的身份驗證，並協議在階段期間使用的密鑰。

在 IPsec 客戶端和伺服器之間建立 IPsec VPN 通道。有時稱 IPsec VPN 客戶端為發起者，IPsec VPN 伺服器為響應者。可以將此閘道器設定為不同的角色，並與各種遠端設備建立大量通道。在建立 VPN 連線之前，您可能需要決定通道的方案類型。

IPsec 通道方案



建立 IPsec 通道時，如果 IPsec 節點後面的主機可以登入遠端站點或主機，則需要輸入遠端閘道器全域 IP 和可選的子網。 在這種設定下，有四種情況：

Site to Site：您需要在兩個閘道器設定遠端閘道器 IP 和子網。IPsec 通道建立後，兩個閘道器後面的主機可以

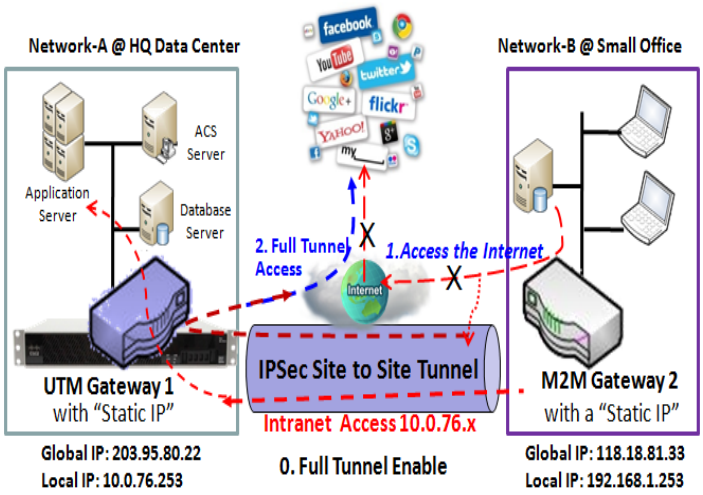
透過通道相互通信。

Site to Host：站點到主機適用於在子網中的客戶端和伺服器(主機)之間進行通道傳輸。如圖所示，M2M 閘道器後面的客戶端可以透過站點到主機 VPN 通道登入位於控制中心的主機 “Host-DC” 。

Host to Site：用於單一主機(或移動使用者)登入位於內網中的資源，可應用於主機到站點方案。

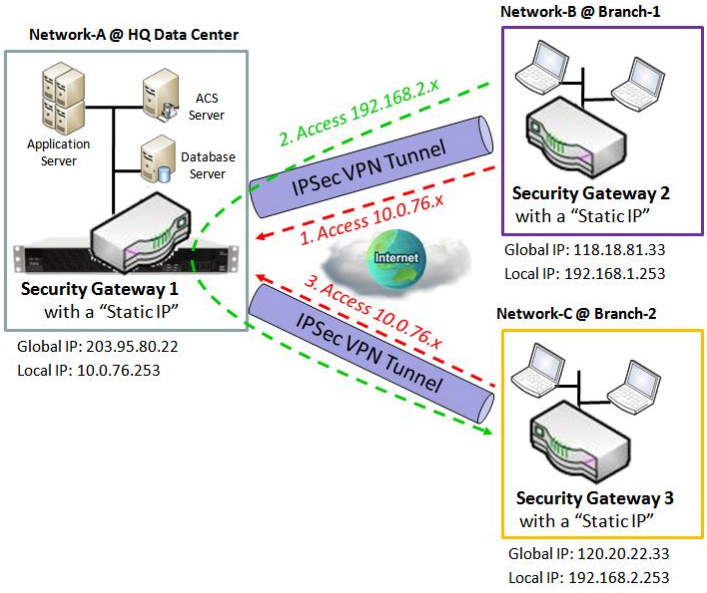
Host to Host：主機到主機是用於在兩台主機之間建立 VPN 通道的特殊設定。

啟用 “Full Tunnel 全通道” 站點到站點



在 “Site to Site” 方案中，遠端站點的客戶端主機可以透過已建立的 IPsec 通道登入企業總部的閘道器，如上所述。但是，遠端站點的網際網路登入仍然透過常規 WAN 來連線。如果您希望來自遠端站點的所有資料封包透過此 IPsec 通道路由(包括 HQ 伺服器登入和網際網路登入)，請啟用 “全部通道” 設定。

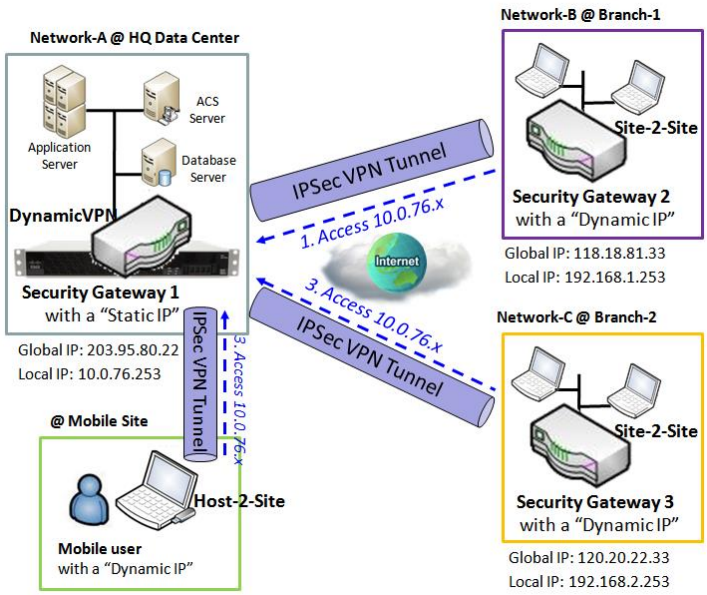
Site to Site 的 “Hub and Spoke” 機制



為了讓控制中心在所有遠端站點間管理內網安全，整個 VPN 網路都有一個簡單的設定，稱為軸輻式(Hub and Spoke)。 軸輻式 VPN 網路建立在擁有集中控制中心的所有遠端站點(如商店或辦公室)的羣組織中。 控制中心充當 Hub，遠端商店或辦公室充當 Spokes。 來自遠端站點的所有 VPN 通道終止於此集線器，該集線器充當集中器。輻條之間的站點到站點連線不存在。 資訊流從一個 Spoke 發起往另一個 Spoke 必須透過 Hub。在這種設定下，您不需要維護遠端客戶端之間的

VPN 通道。

Dynamic VPN Server 案例



動態 VPN 伺服器方案是與遠端站點建立多個通道的有效方式，特別是對於具有動態 IP 的移動客戶端。在這種情況下，閘道器只能作為伺服器(響應者)的角色，並且必須具有“靜態 IP”或“FQDN”。可以允許許多 VPN 客戶端(啟動器)連線至各種通道方案。簡而言之，透過簡單的動態 VPN 伺服器設定可讓許多 VPN 客戶端都可以連線到伺服器。但是與軸輻式機制相比，不允許透過動態 VPN 伺服器在任何兩個客戶端之間直接通信。

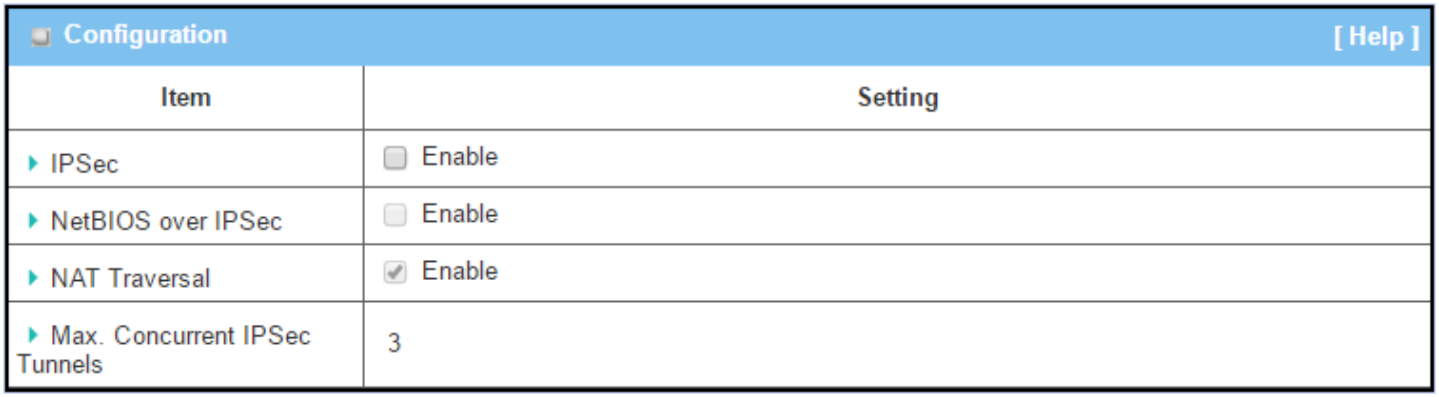
對於閘道器，您可以為每個 WAN 介面設定一個動態 VPN 伺服器。

設定 IPsec

轉到 Security > VPN > IPsec 頁面。

IPsec 設定允許使用者建立和設定 IPsec 通道。

啓動 IPsec

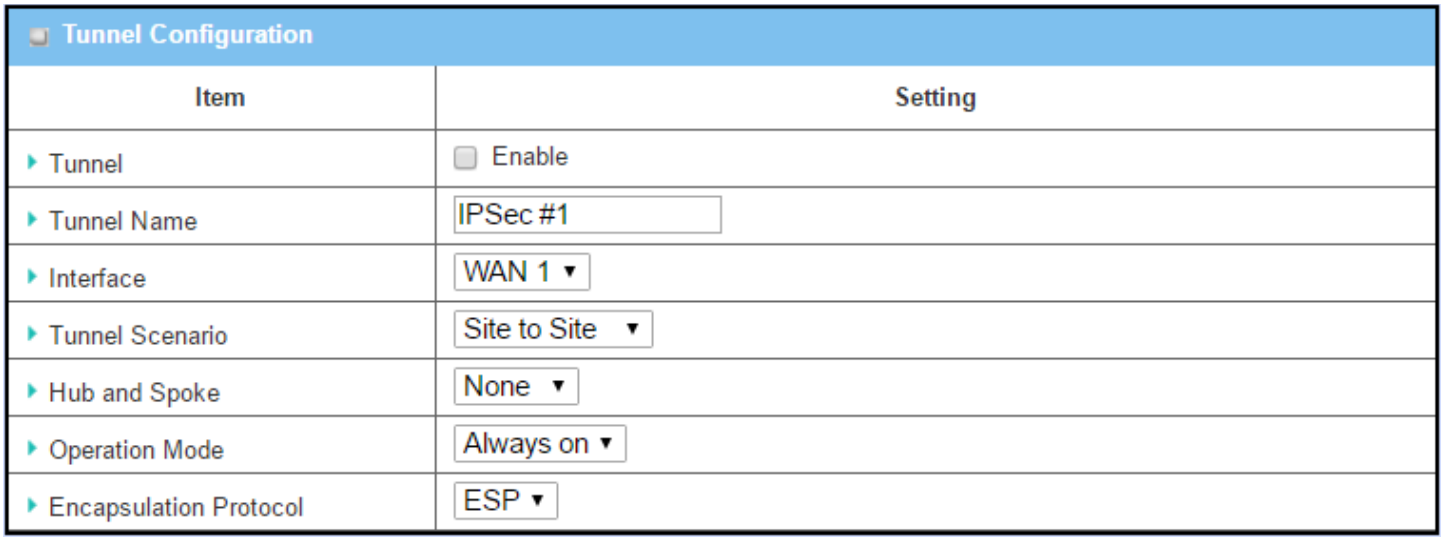


Configuration Window (設定視窗)		
項目	設定值	說明
IPsec	預設未勾選	勾選 **Enable (啓動)** 方框以啓動 IPsec 功能。
NetBIOS over IPsec	預設未勾選	勾選 **Enable (啓動)** 方框以啓動 NetBIOS over IPsec 功能。
NAT Traversal	預設勾選	勾選 **Enable (啓動)** 方框以啓動 NAT Traversal 功能。
Max. Concurrent IPsec Tunnels	取決於產品規格。	指定的值將限制同時發生的 IPsec 通道連接的最大數量。預設值可能會因設備型號而異。
Save (保存)	無	點擊 **Save (保存)** 按鈕以保存設定值
Undo (還原)	無	點擊 **Undo (還原)** 按鈕以取消設定

建立/編輯 IPsec tunnel

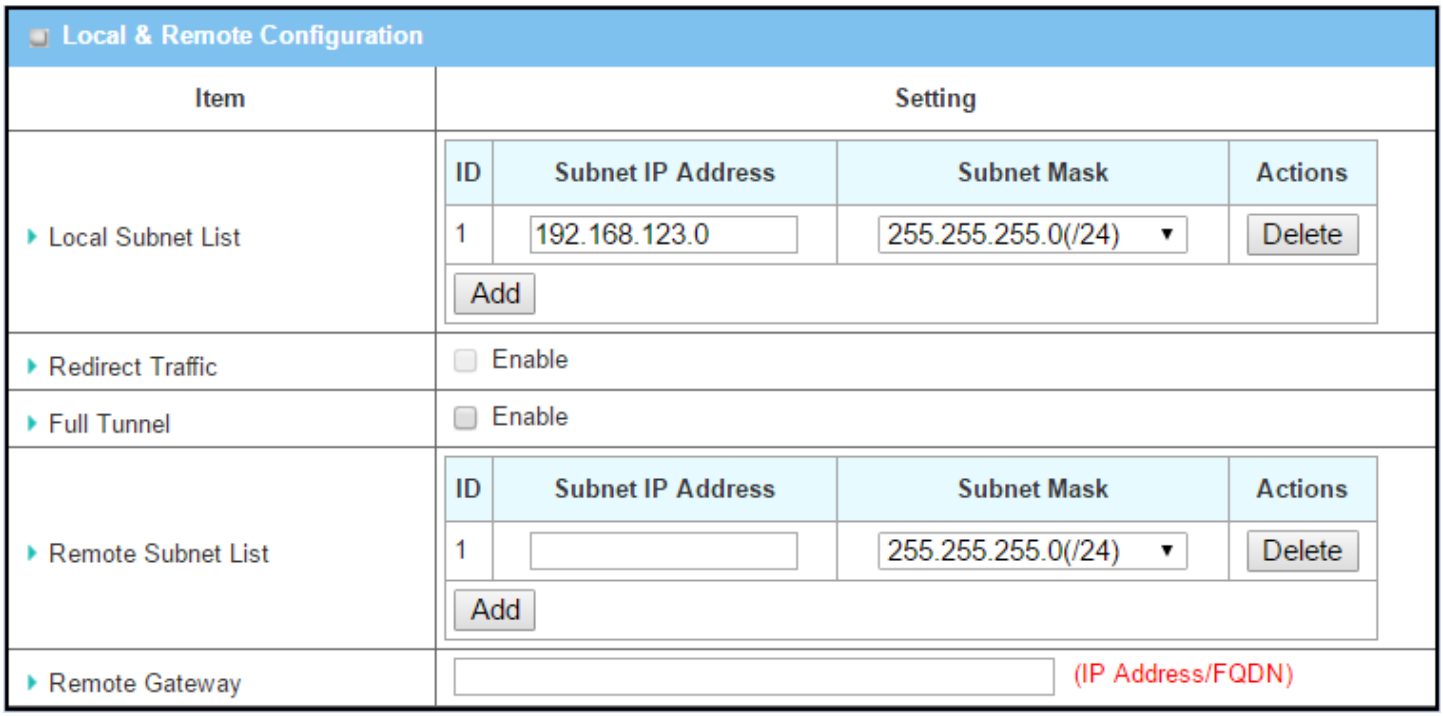
在進一步設定 IPsec 通道設定之前，請確認已勾選 IPsec 方方框啟用。

當按下 **Add/Edit(**增加/編輯)按鈕時，會出現通道設定、本地和遠端設定、認證、IKE 階段、IKE 建議定義、IPsec 階段和 IPsec 建議定義的一系列設定畫面。本地和遠端 VPN 設備的通道詳細設定。



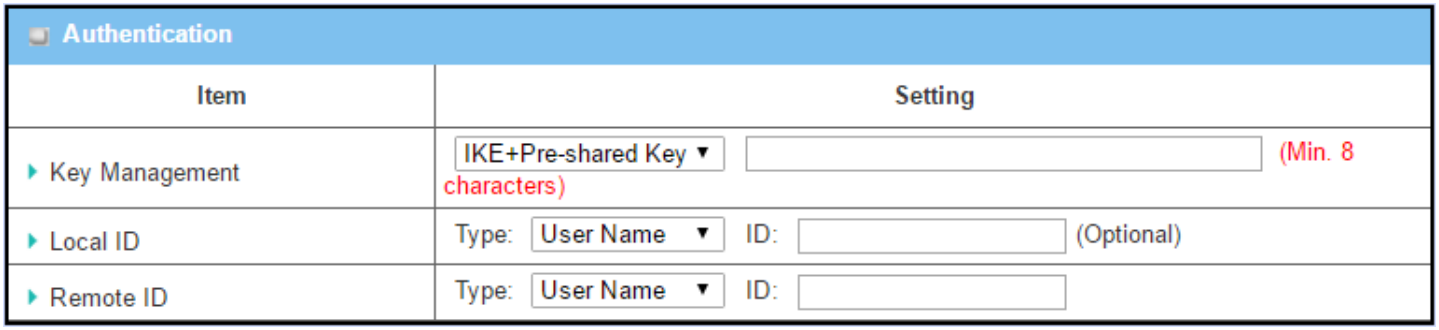
Tunnel Configuration Window (通道設定視窗) 項目	設定值	說明
Tunnel (通道)	預設未勾選	勾選**啟用**啟動 IPsec 通道的框
Tunnel Name (通道名稱)	1. 必要設定 2. 字串格式，文字	輸入通道名稱。 ***範圍值***: 1 ~ 19 個字元.
Interface (介面)	1. 必要設定 2. 預設選擇 **WAN 1**	選擇要在其中建立 IPsec 通道的介面，可能是任何可用的 WAN 和 LAN 介面。
Tunnel Scenario (通道方案)	1. 必要設定 2. 預設選擇 **Site to site (站點到站點)**	從應用程式的下拉清單中選擇 IPsec 通道方案。選擇 **Site-to-Site (站點到站點)**、**Site-to-Host (站點到主機)**、**Host-to-Site (主機到站點)** 或 **Host-to-Host (主機到主機)**。如果選擇了 LAN 介面。則只有**主機到主機**的方案可用。 使用**站點到站點**或**站點到主機**或**主機到站點**，IPsec 在通道模式下運行。 區別在於子網的數目。使用**主機到主機**, IPsec 在傳輸模式下運行。
Hub and Spoke (軸輻式)	1. 可選設定 2. 預設定設 **None (沒有)**	從下拉清單中選擇集線器和分支 IPsec VPN 部署設定閘道。 如果部署不支援集線器或分支加密, 請選擇 **None** (無)。 在 IPsec 設計中的集線器角色選擇 **Hub(集線器)**。 在 IPsec 設計中的分支角色選擇 **Spoke(分支)**。 注意: 集線器和分支僅適用於通道方案中指定的站點到站點 VPN 通道。不可用於動態 VPN 通道。

Operation Mode (操作模式)	1. 必要設定 2. 預設選擇 **Always on**	定義 IPsec 通道的操作模式。可能是 **Always On(永遠 On)** 或 **Failover(容錯移轉)**。 如果此通道是設定為容錯移轉通道，您需要進一步選擇要從故障切換到的主通道。 注意: **容錯移轉**模式為不可用於單 WAN 的閘道器。
Encapsulation Protocol (封裝協定)	1. 必要設定 2. 預設選擇 **ESP**	從該 IPsec 通道的下拉清單中選擇封裝協定。可用的為 **ESP** 和 **AH**。



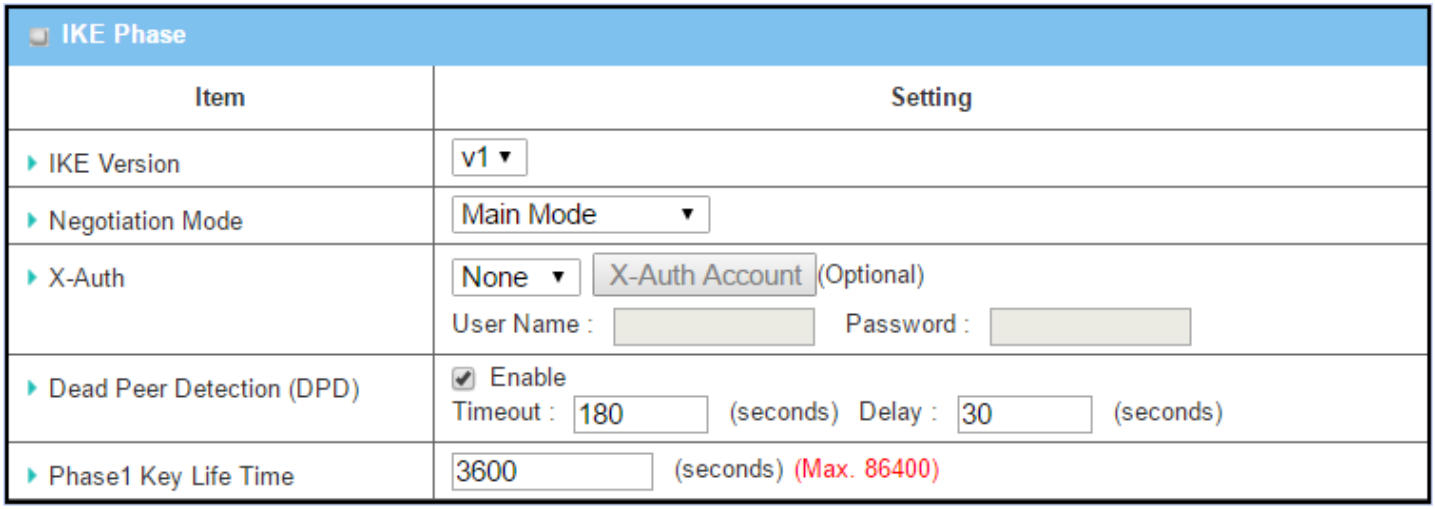
Local & Remote Configuration Window (本地&遠端設定視窗)		
項目	**設定值**	**說明**
Local Subnet List (本地子網清單)	必要設定	指定本地子網 IP 位址和子網路遮罩。 按一下 **Add (增加)**或**刪除 (Delete)**按鈕以增加或刪除本地子網。 註_1: 當選擇通道方案中的動態 VPN 選項時，將只有一個子網可用。 註_2: 當選擇 通道方案中的 "主機到站點" 或 "主機到主機" 選項時, 本地子網將不可用。 註_3: 選擇 Hub and Spoke (軸輻式)中的 " Hub and Spoke " 選項後, 將只有一個子網可用。

Redirect Traffic (轉向通信)	預設未勾選	按一下 **Enable(啟用)**方框以啟動轉向通信功能。 注意:轉向通信僅適用於在通道方案中指定的主機到站點。預設爲禁用，以防止意外和危險登入節點的子網。如果啟用此功能，VPN 主機後面的所有網路設備 (實際上是 NAT 閘道) 都可以使用主機 IP 登入節點子網。
Full Tunnel (全通道)	預設未勾選	按一下 **Enable(啟用)**方框啟用全通道。 注意: 全通道僅適用於通道方案中指定站點到站點。
Remote Subnet List (遠端子網列表)	必要設定	指定遠端子網 IP 位址和子網路遮罩。 按一下 " Add(增加)" 或 " Delete(刪除)" 按鈕以增加或刪除遠端子網設定。
Remote Gateway (遠端閘道)	1. 必要設定. 2. 格式可能是 IPV4 位址或 FQDN	指定遠端閘道。



Authentication Configuration Window (身份驗證設定視窗) 項目	設定值	說明
Key Management(密鑰管理)	1. 必要設定 2. 預共用密鑰 8 到 32 個字元。	從該 IPsec 通道的下拉清單中選擇 "密鑰管理"。 **IKE+Pre-shared Key (IKE + 預共用密鑰) :** 使用者需要設定一個密鑰 (8 ~ 32 字元)。 **IKE + x 509 :** 使用者需要用於驗證的憑證。只有在正確設定憑證時, 才可用 IKE+X.509。請參閱本手冊的 "憑證" 部分以及網頁工具程式中的 **Object Definition > Certificate** 。 **Manually (手動) :** 使用者需要輸入密鑰 ID 進行身份驗證。手動密鑰設定將在之後的 **手動密鑰管理**中解釋。
Local ID (本地 ID)	可選設定	指定此 IPsec 通道的本地 ID 以進行身份驗證。 選擇本地 ID 的 **User Name(使用者名稱)**, 然後輸入使用者名。使用者名可以包含數字但不能全部都是數字。 選擇本地 ID 的 **FQDN** , 然後輸入 fqdn。

		選擇本地 ID 的 **User@FQDN**， 然後輸入 **User@FQDN**。 選擇本地 ID 的 **Key ID (密鑰 ID)**， 然後輸入密鑰 ID (英文字母或數字)。
Remote ID (遠端 ID)	可選設定	指定此 IPsec 通道的遠端 ID 以進行身份驗證。 選擇 **User Name(使用者名稱)**用於遠端 ID 並輸入使用者名稱。使用者名可以包含數字但不能全部都是數字。 選擇本地 ID 的 **FQDN** , 然後輸入 fqdn。 選擇本地 ID 的 **User@FQDN**， 然後輸入 **User@FQDN**。 選擇本地 ID 的 **Key ID (密鑰 ID)**， 然後輸入密鑰 ID (英文字母或數字)。 注意: 選擇 "通道方案" 中的 "動態 VPN" 選項時, 遠端 ID 將不可用。



IKE Phase Window (IKE 階段視窗)		
項目	**設定值**	**說明**
IKE Version (IKE 版本)	1. 必要設定 2. 預設選擇 v1	指定此 IPsec 通道的 IKE 版本。選擇 v1 或 v2 注意: 如果選擇了 "通道方案" 中的 " Dynamic VPN 動態 VPN" 選項, 或者在 " Encapsulation Protocol 封裝協定" 中選擇了 AH 選項，IKE 版本將不可用。
Negotiation Mode (協商模式)	預設 Main Mode	指定此 IPsec 通道的協商模式。選擇 Main Mode(主模式)或 Aggressive Mode(野蠻模式)。
X-Auth (X-認證)	預設選擇 None	指定此 IPsec 通道的 X-驗證角色。選擇 "Server(伺服器)"、" Client(客戶端)" 或 " None(無)"。 此閘道選擇伺服器將成爲 X-認證伺服器。按一下 " X-Auth Account

		(X-驗證帳戶)" 按鈕以建立遠端 X-身份驗證客戶端的帳戶。 此閘道選擇客戶端將成爲 X-認證客戶端。輸入要由 X-認證伺服閘道器驗證的使用者名和密碼。 注意: 在通道方案中選擇的 "動態 VPN" 選項將無法使用 X-身份驗證客戶端。
Dead Peer Detection (DPD 死節點偵測)	1. 預設勾選 2. 預設 Timeout 180s 和 Delay 30s	按一下 Enable (啓動)方框啟用 **DPD** 函數。指定**超時**和**延遲**時間 (以秒為單位)。 ***範圍值***: 0 ~ 999 秒**超時**和**延遲**.
Phase1 Key Life Time (階段 1 密鑰存活時間)	1. 必要設定 2. 預設 3600s 3. 最大 86400s	指定 Phase1 密鑰存活時間。 ***範圍值***: 30 ~ 86400.

IKE Proposal Definition

ID	Encryption	Authentication	DH Group	Definition
1	AES-auto	SHA1	Group 2	Enable
2	AES-auto	MD5	Group 2	Enable
3	DES	SHA1	Group 2	Enable
4	3DES	SHA1	Group 2	Enable

IKE Proposal Definition Window (IKE 提議定義視窗)

項目	設定值	說明
IKE Proposal Definition (IKE 提議定義)	必要設定	指定階段 1 加密方法。可以是 DES / 3DES / AES-auto / AES-128 / AES-192 / AES-256。 指定認證方法。可以是 None / MD5 / SHA1 / SHA2-256。 指定 DH 羣組。可以是 None / Group1 / Group2 / Group5 / Group14 / Group15 / Group16 / Group17 / Group18。 勾選 Enable 啟用(啟動)方框以啟動此設定。

IPSec Phase

Item	Setting
Phase2 Key Life Time	28800 (seconds) (Max. 86400)

IPsec Phase Window (IPsec 階段視窗)

項目	設定值	說明
Phase2 Key Life	1. 必要設定	指定 Phase2 的密鑰存活時間 (以秒為單位)。

Time (階段 2 密鑰存活時間)	2. 預設 28800s 3. 最大 86400s	***範圍值***: 30 ~ 86400.

IPSec Proposal Definition

ID	Encryption	Authentication	PFS Group	Definition
1	AES-auto	SHA1	Group 2	Enable
2	AES-auto	MD5		Enable
3	DES	SHA1		Enable
4	3DES	SHA1		Enable

IPsec Proposal Definition Window (IPsec 提議定義視窗)		
項目	**設定值**	**說明**
IPsec Proposal Definition (IPsec 提議定義)	必要設定	指定加密方法。 可以是 None/ DES / 3DES / AES-auto / AES-128 / AES-192 / AES-256。 注意：只有在封裝協議設置為 AH 時才可用; 不適用於 ESP 封裝。 指定認證方法。 可以是 None / MD5 / SHA1 / SHA2-256。 注意：只有當封裝協議設定為 ESP 時，None 和 SHA2-256 才可用; 不適用於 AH 封裝。 指定 PFS 羣組。可以是 None / Group1 / Group2 / Group5 / Group14 / Group15 / Group16 / Group17 / Group18。 點擊 **Enable** 啟用此設置。
Save (保存)	無	點擊 **Save (保存)** 按鈕以保存設定值
Undo (還原)	無	點擊 **Undo (還原)** 按鈕以取消設定
Back (返回)	無	點擊 **Back (返回)** 按鈕以返回上一頁。

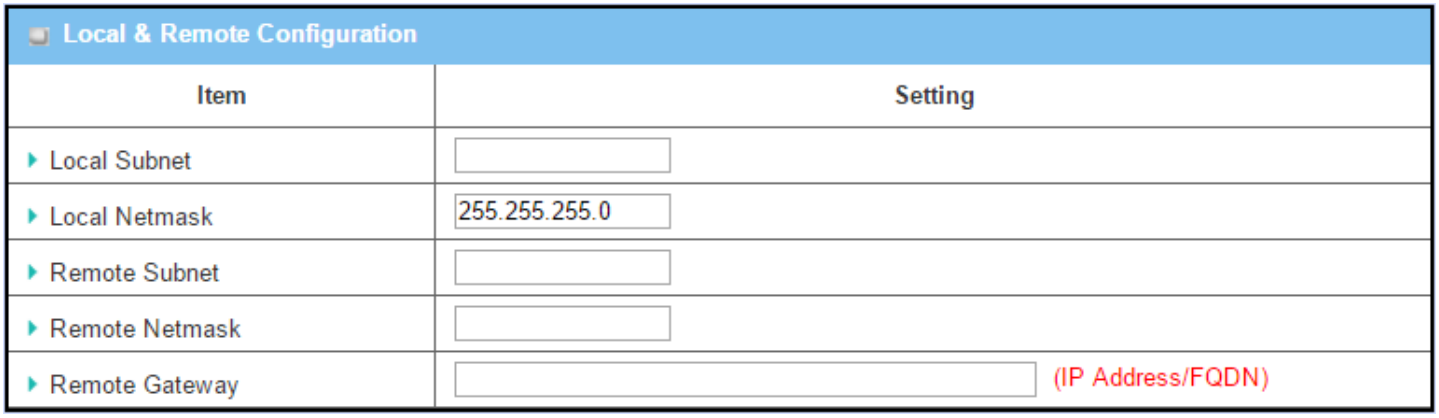
手動密鑰(Key)管理

如認證設定畫面中所述為密鑰管理選擇手動選項時，將出現本地和遠端設定、身份驗證和手動建議的手動 IPsec 通道設定畫面。

Authentication

Item	Setting
Key Management	Manually
Local ID	Type: KEY ID ID: (Optional)
Remote ID	Type: KEY ID ID:

Authentication Window (身份驗證視窗)		
項目	設定值	說明
Key Management (密鑰管理)	必要設定	從該 IPsec 通道的下拉清單中選擇 " Key Management 密鑰管理"。 **Manually(手動)** 是已選擇的選項。
Local ID (本地 ID)	可選設定	指定 **Local ID(本地 ID)**爲 此 IPsec 通道進行身份驗證。 選擇 **key ID (密鑰 ID)**用於本地 ID 並輸入密鑰 ID (字母或數字)。
Remote ID (遠端 ID)	可選設定	指定 **Remote ID(遠端 ID)** 為此 IPsec 通道進行身份驗證. 選擇 **Key ID(密鑰 ID)**用於遠端 ID 並輸入密鑰識別碼 (字母或數字)。



Local & Remote Configuration Window (本地 & 遠端設定視窗)		
項目	設定值	說明
Local Subnet (本地子網)	必要設定	指定本地子網 IP 位址和子網路遮罩。
Local Netmask (本地網路遮罩)	必要設定	指定本地子網路遮罩。
Remote Subnet (遠端子網)	必要設定	指定遠端子網 IP 位址
Remote Netmask (遠端網路遮罩)	必要設定	指定遠端 子網路遮罩.
Remote Gateway (遠端閘道)	1. 必要設定 2. IPv4 位址或 FQDN 格式	指定遠端閘道。

在手動密鑰管理身份驗證設定下，本地和遠程 IPsec 節點僅支援一個子網。

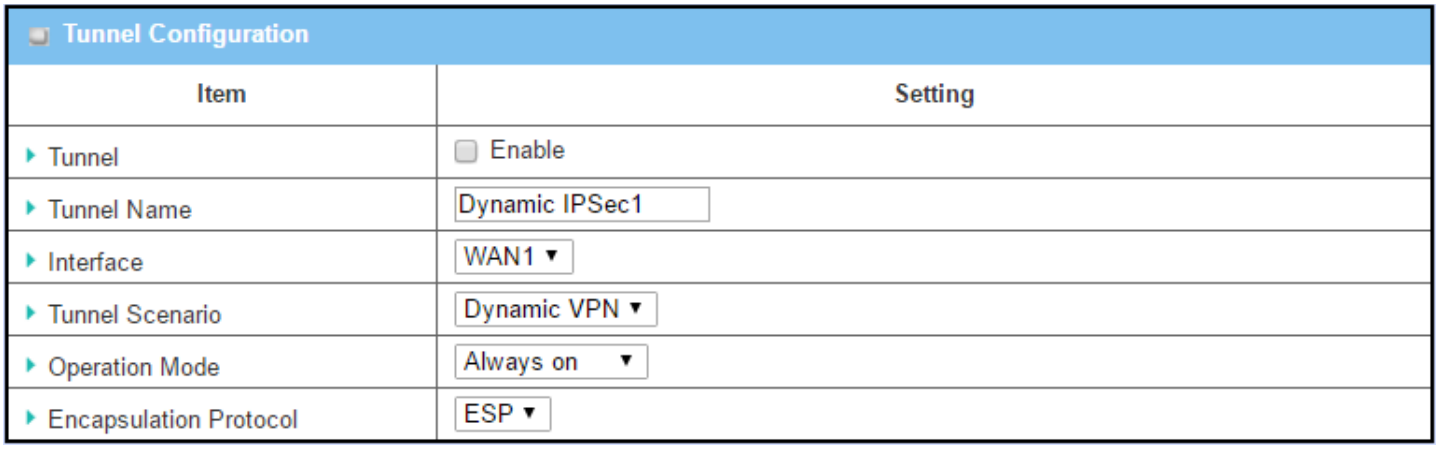
Manual Proposal Window (手動提議視窗) 項目	設定值	說明
Outbound SPI (出站 SPI)	十六進位格式	指定此 IPsec 通道的出站 SPI。 *範圍值*:0 ~ FFFF
Inbound SPI (入站 SPI)	十六進位格式	指定此 IPsec 通道的入站 SPI。 *範圍值*:0 ~ FFFF
Encryption (加密)	1. 必要設定 2. 十六進位格式	指定加密方法和加密密鑰. 可用的加密方法為 DES/3DES/AES-128/AES-192/AES-256. DES 的密鑰長度為 16、3DES 為 48、AES-128 為 32, AES-192 為 48, AES-256 為 64. 注意: 如果選擇了封裝中的 **AH** 選項, 則加密將不可用。
Authentication (認證)	1. 必要設定 2. 十六進位格式	指定身份驗證方法和身份驗證密鑰. 可用的加密是 None/MD5/SHA1/SHA2-256. MD5 的密鑰長度為 32, SHA1 為 40, SHA2-256 為 64。 注意: 如果選擇了封裝協定中的 **AH** 選項, 則身份驗證中的 **None** 選項將不可用。
Save (保存)	無	點擊 Save (保存) 按鈕以保存設定值
Undo (還原)	無	點擊 Undo (還原) 按鈕以取消設定
Back (返回)	無	Click **Back (返回)** to return to the previous page.

建立/編輯 Dynamic VPN Server List (動態 VPN 伺服器列表)

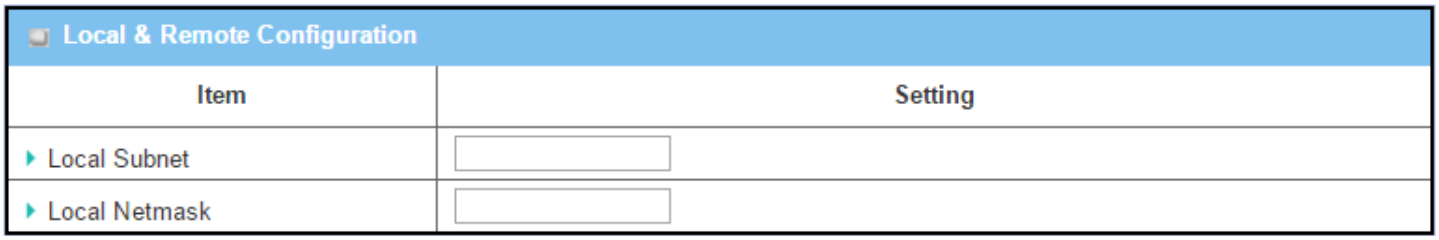
與 站點/主機 到 站點/主機 方案建立 IPsec VPN 通道類似，當按下 **Edit(編輯)**按鈕時，將出現通道設定、本地和遠端設定、認證、IKE 階段、IKE 建議定義、IPsec 階段和 IPsec 建議定義設定畫面。詳細設定動

態 VPN 伺服器的閘道器通道。

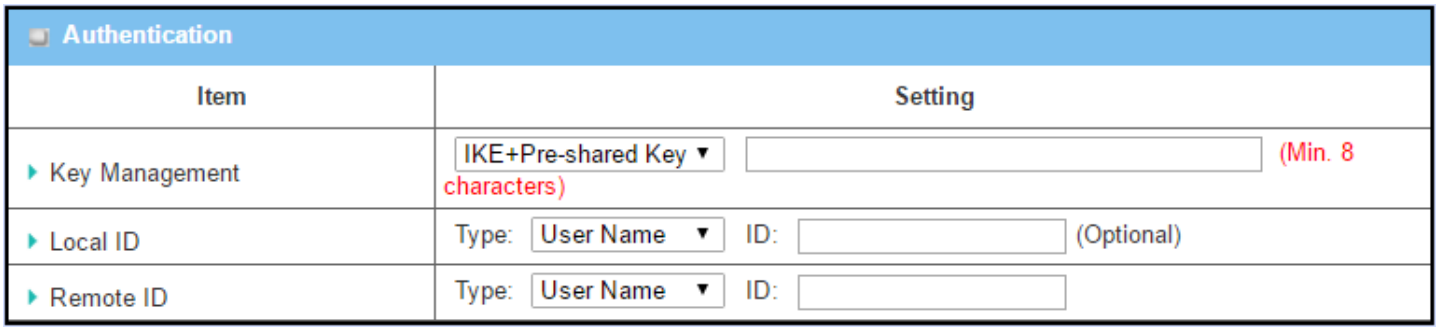
注意：您可以為每個 WAN 介面設定一個動態 VPN 伺服器。



Tunnel Configuration Window (通道設定視窗)		
項目	**設定值**	**說明**
Tunnel (通道)	預設未勾選	勾選 **Enable(啟用)**方框啟動動態 IPsec VPN 通道。
Tunnel Name (通道名稱)	1. 必要設定 2. 字串格式., 任何文字	輸入通道名稱。 ***範圍值***: 1 ~ 19 個字元.
Interface (介面)	1. 必要設定 2. 預設選擇 **WAN 1**	選擇要在其中建立 IPsec 通道的 WAN 介面。
Tunnel Scenario (通道方案)	1. 必要設定 2. 預設選擇 **Dynamic VPN**	IPsec 通道方案固定在動態 VPN 上。
Operation Mode (操作模式)	1. 必要設定 2. 預設選擇 **Always on**	可用的操作模式爲 **Always On(永遠啓動)**。動態 IPsec 方案不可用 Failover(容錯轉換)。
Encapsulation Protocol (封裝協定)	1. 必要設定 2. 預設選擇 **ESP**	從該 IPsec 通道的下拉清單中選擇封裝協定。可用的封裝為 **ESP** 和 **AH**.



Local & Remote Configuration Window (本地 & 遠端設定視窗)		
項目	設定值	說明
Local Subnet (本地子網)	必要設定	指定本地子網 IP 位址。
Local Netmask (本地網路遮罩)	必要設定	指定本地子網路遮罩。



Authentication Configuration Window (身份驗證設定視窗)		
項目	設定值	說明
Key Management(密鑰管理)	1. 必要設定 2. 預共用密鑰 8 到 32 個字元。	從該 IPsec 通道的下拉清單中選擇 "密鑰管理"。 **IKE+Pre-shared Key (IKE + 預共用密鑰) :** 使用者需要設定一個密鑰 (8 ~ 32 字元)。 **IKE + x 509 :** 使用者需要用於驗證的憑證。只有在正確設定憑證時, 才可用 IKE+X.509。請參閱本手冊的 "憑證" 部分以及網頁工具程式中的 **Object Definition > Certificate** 。 **Manually (手動) :** 使用者需要輸入密鑰 ID 進行身份驗證。手動密鑰設定將在之後的 **手動密鑰管理**中解釋。
Local ID (本地 ID)	可選設定	指定此 IPsec 通道的本地 ID 以進行身份驗證。 選擇本地 ID 的 **User Name(使用者名稱)**, 然後輸入使用者名。使用者名可以包含數字但不能全部都是數字。 選擇本地 ID 的 **FQDN** , 然後輸入 fqdn。 選擇本地 ID 的 **User@FQDN**， 然後輸入 **User@FQDN**。 選擇本地 ID 的 **Key ID (密鑰 ID)**， 然後輸入密鑰 ID (英文字母或數字)。
Remote ID (遠端 ID)	可選設定	指定此 IPsec 通道的遠端 ID 以進行身份驗證。 選擇 **User Name(使用者名稱)**用於遠端 ID 並輸入使用者名稱。使用者名可以包含數字但不能全部都是數字。 選擇本地 ID 的 **FQDN** , 然後輸入 fqdn。 選擇本地 ID 的 **User@FQDN**， 然後輸入 **User@FQDN**。

	選擇本地 ID 的 **Key ID (密鑰 ID)**， 然後輸入密鑰 ID (英文字母或數字)。注意: 選擇 "通道方案" 中的 "動態 VPN" 選項時, 遠端 ID 將不可用。

剩餘的 IKE 階段、IKE 建議定義、IPsec 階段和 IPsec 建議定義設定與上一部分中介紹的建立 IPsec 通道的設定相同。 請參考相關說明。

5.1.2 OpenVPN

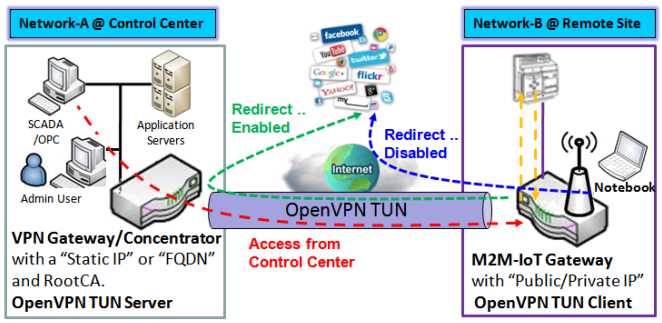
OpenVPN 是一種進行虛擬私人網路(VPN)技術的應用，用於在路由或橋接設定和遠端登入設施中建立安全的點對點或站點到站點連線。利用 SSL/TLS 進行密鑰交換來客製化安全協定。它能夠穿越網路位址轉換器(NAT)和防火牆。

OpenVPN 允許同行使用靜態密鑰(預分享密鑰)或憑證相互認證。在多客戶端伺服器設定中使用時，允許伺服器為每個客戶端發布身份驗證憑證，適用於簽名和憑證頒發機構。其廣泛使用 OpenSSL 加密資料庫以及 SSLv3/TLSv1 協定，並含有許多安全和控制功能。

OpenVPN 通道是適用於客戶端和伺服器的通道技術。OpenVPN 伺服器必須具有靜態 IP 或 FQDN，並維護客戶端列表。OpenVPN 客戶端可能是具有公共 IP 或專用 IP 的移動使用者或移動站點，並請求 OpenVPN 通道連線。該產品支援 OpenVPN 伺服器和 OpenVPN 客戶端的功能，以滿足不同的應用需求。

有 TAP 和 TUN 兩個 OpenVPN 連線方案。該產品可以建立三層的 IP 通道(TUN)，也可以建立承載任何類型的以太網流量的二層以太網 TAP。除了將設備設定為伺服器或客戶端之外，還要指定要採用哪種類型的 OpenVPN 連線方案。

OpenVPN TUN 方案



1. M2M-IoT Gateway (as OpenVPN TUN Client) connects to peer VPN Gateway/Concentrator (as OpenVPN TUN Server).
2. M2M-IoT Gateway will be assigned 10.8.0.2 IP Address after OpenVPN TUN Connection estabilshed. (10.8.0.x is a virtual subnet)
3. Local networked device will get a virtual IP 10.8.0.x if its traffic goes through the OpenVPN TUN connection (when NAT disabled & Redirect Internet Traffic enabled).
4. SCADA Server in Control Center can access remote attached device(s) with the assigned IP Address 10.8.0.2.

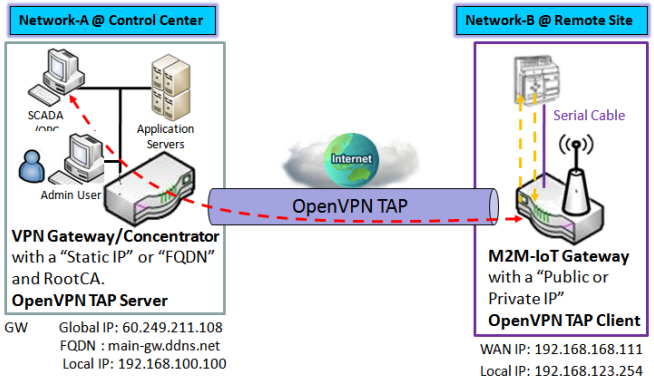
TUN 模式是最簡單的解決方案。

"TUN" 模式又被稱為路由模式並且與第 3 層封包一起操作。在路由模式下，VPN 客戶端在與 OpenVPN 伺服器的本地 LAN 不同子網上獲得 IP 位址。爲連線到任何遠端 VPN 的電腦建立虛擬子網。在路由模式下，OpenVPN 伺服器建立一個 "TUN" 介面，其自身的 IP 位址池與本地 LAN 不同。撥入的遠端主機將在虛擬網路中獲得 IP 位址，並且只能登入 OpenVPN 所在的伺服器。

如果您想要從客戶端遠端登入 VPN 伺服器，並禁止登入 VPN 伺服器下的遠端 LAN 資源，則 OpenVPN

如圖所示，M2M-IoT 閘道器設定為 OpenVPN TUN 客戶端，並連線到 OpenVPN UN 伺服器。 一旦建立了 OpenVPN TUN 連線，連線的 TUN 客戶端將被分配一個虛擬 IP(10.8.0.2)，該虛擬 IP 屬於與控制中心的本地子網不同的虛擬子網。透過這樣的連線，當啟用重定向網際網路流量設定時，如果本地網路設備的流量透過 OpenVPN TUN 連線，則本地聯網設備將獲得虛擬 IP 10.8.0.x; 控制中心的 SCADA 伺服器可以使用虛擬 IP 位址(10.8.0.2)登入遠端連線的序列設備。

OpenVPN TAP 方案



1. M2M-IoT Gateway (as OpenVPN TAP Client) connects to peer VPN Gateway/Concentrator (as OpenVPN TAP Server).
2. M2M-IoT Gateway will be assigned 192.168.100.210 IP Address after OpenVPN TAP Connection estabilshed. (same subnet as in Control Center)
3. SCADA Server in Control Center can access remote attached device(s) with the assigned IP Address 192.168.100.210.

"TAP" 也稱爲橋接模式並與第 2 層一起操作。在橋接模式下，VPN 客戶端會獲得與 OpenVPN 伺服器的 LAN 同一子網的 IP 位址。 在這種設定下，OpenVPN 客戶端可以直接登入區域網。如需要為 VPN 客戶端提供對整個遠端 LAN 的遠端登入，請在 "TAP" 橋接模式下設定 OpenVPN。

如圖所示，M2M-IoT 閘道器設定為 OpenVPN TAP 客戶端，並連線到 OpenVPN TAP 伺服器。 一旦建立了 OpenVPN TAP 連線，連線的 TAP 客戶端將被分配一個虛擬 IP(192.168.100.210)，該虛擬 IP 與控制中心中的本地子網處於同一子網。透過此連線，控制中心的 SCADA 伺服器可以使用虛擬 IP 位址(192.168.100.210)登入遠端連線的序列設備。

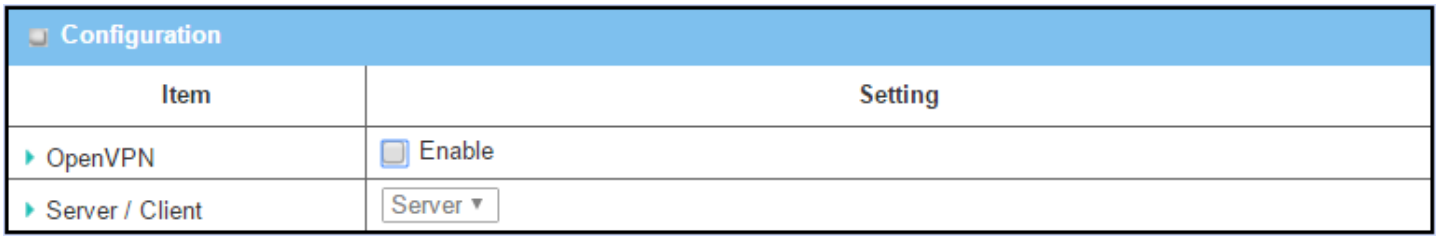
設定 Open VPN

轉到 Security > VPN > OpenVPN 頁面。

OpenVPN 設定允許使用者建立和設定 OpenVPN 通道。

啓動 OpenVPN

啟用 OpenVPN 並選擇需要的設定(伺服器或客戶端)以供閘道器運行。

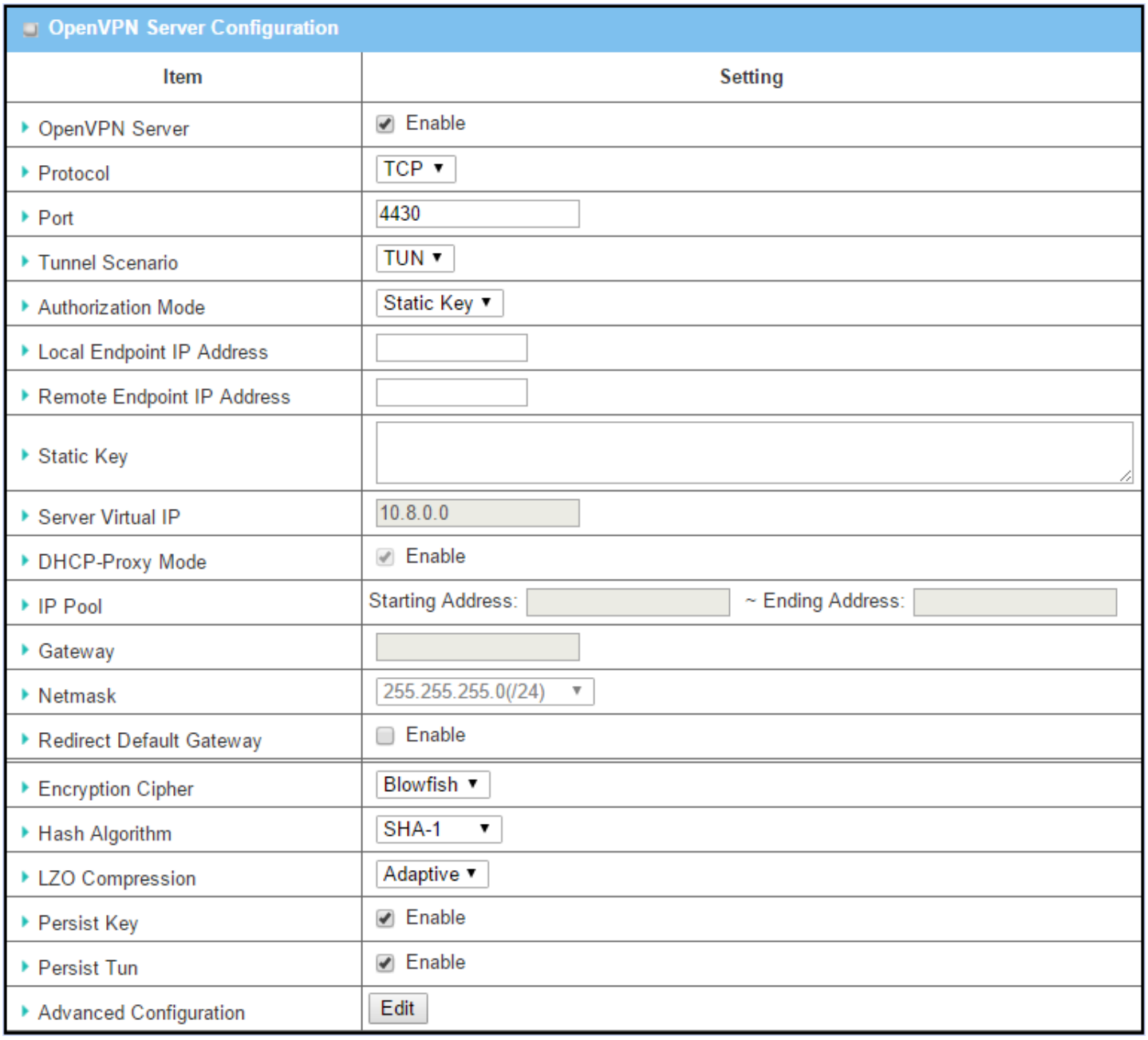


Configuration (設定)		
項目	**設定值**	**說明**
OpenVPN	預設未勾選	勾選 Enable 啓動 OpenVPN 功能。
Server/ Client (伺服器/ 客戶端)	預設選擇. Server Configuration	選擇 **Server (伺服器)**時，下面將顯示進一步的伺服器設定設置。 選擇 **Client(客戶端)**時，您可以在另一個客戶端設定窗口中指定客戶端設置。

作為 OpenVPN 伺服器

如果選擇了 Server(伺服器)，將會出現 OpenVPN 伺服器設定畫面。OpenVPN 伺服器設定畫面允許您啟用 OpenVPN 伺服器功能，並在遠端 OpenVPN 客戶端撥入時指定 OpenVPN 伺服器的虛擬 IP 位址以及身份驗證協定。

OpenVPN 伺服器同時支援最多 4 個 TUN / TAP 通道。



OpenVPN Server Configuration

Item	Setting
OpenVPN Server	Enable
Protocol	TCP
Port	4430
Tunnel Scenario	TUN
Authorization Mode	Static Key
Local Endpoint IP Address	
Remote Endpoint IP Address	
Static Key	
Server Virtual IP	10.8.0.0
DHCP-Proxy Mode	Enable
IP Pool	Starting Address: ~ Ending Address:
Gateway	
Netmask	255.255.255.0(/24)
Redirect Default Gateway	Enable
Encryption Cipher	Blowfish
Hash Algorithm	SHA-1
LZO Compression	Adaptive
Persist Key	Enable
Persist Tun	Enable
Advanced Configuration	Edit

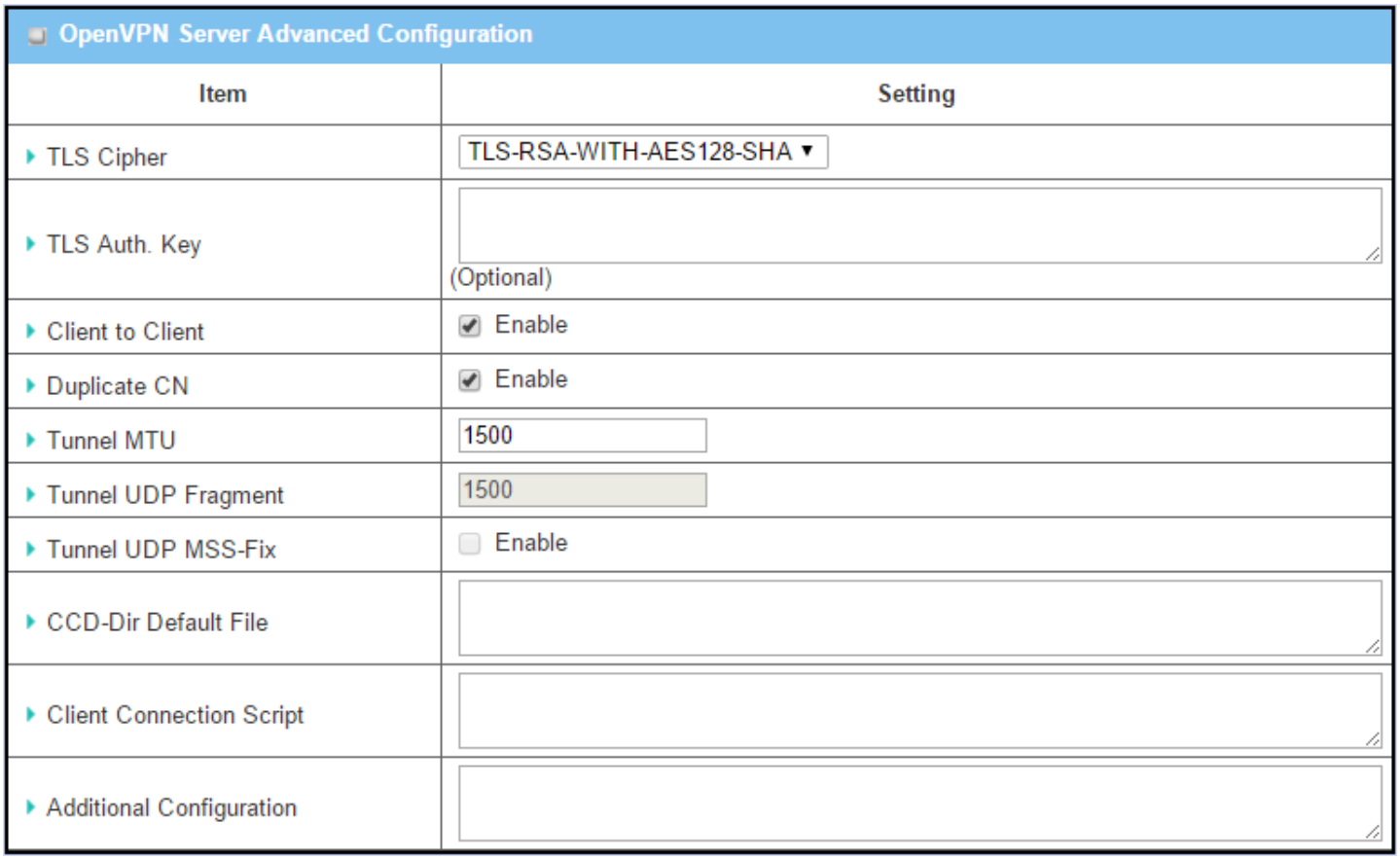
OpenVPN Server Configuration (OpenVPN 伺服器設定)		
項目	**設定值**	**說明**
OpenVPN Server (伺服器)	預設未勾選	按一下 " **Enable(啟用)**" 以啟動 OpenVPN 伺服器功能。
Protocol (協	1. 必要設定	定義連接到 OpenVPN 伺服器選定的**協定**。

定)	2. 預設選擇 **TCP**	• **選擇 TCP 或 UDP** -> TCP 將用於登入 OpenVPN 伺服器，將設置為 443 **埠**。 • **選擇 UDP** -> UDP 將用於登入 OpenVPN 伺服器，將設置為 1194 **埠**。
Port (埠)	1. 必要設定 2. 預設設定 **4430**	指定連接到 OpenVPN 伺服器的**埠**。. ***範圍值***: 1 ~ 65535.
Tunnel Scenario (通道方案)	1. 必要設定 2. 預設選擇 **TUN**	指定連接到 OpenVPN 伺服器**通道方案**的類型 。可以是 **TUN** 通道方案或 **TAP** 通道方案.
Authorization Mode (授權模式)	1. 必要設定 2. 預設選擇 **Static Key**	指定 OpenVPN 伺服器的授權模式。. • **TLS** -> OpenVPN 將使用 TLS 授權模式, 以下將顯示 **CA Cert.**, **Server Cert.** 和 **DH PEM**。 **CA Cert** 可以在憑證中產生。請參閱**物件定義>憑證>受信任的憑證**。 **Server Cert** 可以在憑證中產生。請參閱**物件定義>憑證>我的憑證**。 • **Static Key (靜態密鑰)** -> OpenVPN 將使用靜態密鑰 (預共用) 授權模式, 並將顯示 **Local Endpoint IP Address (本地端點 ip 位址)**、**Remote Endpoint IP Address (遠端端點 IP 位址)** 和 **Static Key (靜態密鑰)**。 注意: 只有在通道方案中選擇 TUN 時，才可用靜態密鑰。
Local Endpoint IP Address (本地端點 IP 位址)	必要設定	指定此 OpenVPN 閘道的虛擬**本地端點 IP 位址**。 ***範圍值***: IP 格式為 10.8.0.x, x 的範圍為 1 ~ 254. 注意: 僅當在授權模式下選擇靜態密鑰時, 本地端點 IP 位址才可用。
Remote Endpoint IP Address (遠端端點 IP 位址)	必要設定	指定對等 OpenVPN 閘道的虛擬**遠端端點 IP 位址**。 ***範圍值***: IP 格式為 10.8.0.x, x 的範圍為 1 ~ 254. 注意: 只有在授權模式下選擇靜態密鑰時, 遠端端點 IP 位址才可用。
Static Key (靜態密鑰)	必要設定	指定**靜態密鑰**. 注意: 只有在授權模式下選擇靜態密鑰時，靜態密鑰才可用。
Server Virtual IP (伺服器虛擬 IP)	必要設定	指定**伺服器虛擬 IP** . ***範圍值***: IP 格式為 10, y 0.0, y 的範圍為 1 ~ 254. 注意: 伺服器虛擬 IP 僅在授權模式下選擇 TLS 才可用。
DHCP-Proxy Mode (DHCP	1. 必要設定 2. 預設勾選此方框.	勾選 " **Enable(啟用)**" 方框以啟動 **DHCP 代理模式**. 注意: 只有在通道設備中選擇了 TAP 時，DHCP 代理模式才可用。

代理模式)		
IP Pool (IP 池)	必要設定	設定 OpenVPN 伺服器的 IP 池， 指定 **起始位址** 和**結束位址**作為 OpenVPN 用戶端的 IP 位址池。 注意: IP 池將僅可用在通道設備中選擇 TAP 和 DHCP-代理模式未勾選 (禁用)時。
Gateway (閘道)	必要設定	指定 OpenVPN 伺服器的閘道設置。它將被分配給連接 OpenVPN 的用戶端。 注意: 只有在通道設備中選擇 TAP 並未勾選 (禁用)DHCP 代理模式，閘道才可用。
Netmask (網路遮罩)	預設選擇 - **select one** -	指定 OpenVPN 伺服器的網路遮罩。它將被分配給連接 OpenVPN 的用戶端。 ***範圍值*** : 255.255.255.0/24 (僅支援 class C) 註_1: 只有在通道設備中選擇 TAP 並未勾選 (禁用)DHCP 代理模式，網路遮罩才可用。 註_2: 通道設備中選擇 TUN 時也可用網路遮罩。
Redirect Default Gateway (轉向預設閘道)	1. 可選設定. 2. 預設未勾選	勾選 " **Enable(啟用)**" 方框以啟動**轉向預設閘道**功能。
Encryption Cipher (加密密碼)	1. 必要設定. 2. 預設選擇 **Blowfish**	從下拉清單中選擇**加密密碼**。 選擇 **Blowfish/AES-256/AES-192/AES-128/None** 。
Hash Algorithm (雜湊演算法)	預設選擇 **SHA-1**	從下拉清單中選擇**雜湊演算法**。 選擇 **SHA-1/MD5/MD4/SHA2-256/SHA2-512/None/Disable.**
LZO Compression (壓縮)	預設選擇 **Adaptive**	指定 **LZO 壓縮** 計畫。 選擇 **Adaptive/YES/NO/Default**
Persis Key	1. 可選設定. 2. 預設勾選此方框.	勾選 " **Enable(啟用)**" 方框以啟動 **Persis Key** 功能。
Persis Tun	1. 可選設定. 2. 預設勾選此方框.	勾選 " **Enable(啟用)**" 方框以啟動 **Persis TUN** 功能。
Advanced Configuration	無	按一下 " **Edit (編輯)**" 按鈕進階設定 OpenVPN 伺服器。 如果按了按鈕則**階設定級**將顯示在下面。

(進階設定)		
Save (保存)	無	點擊 **Save (保存)** 按鈕以保存設定值.
Undo (還原)	無	點擊 **Undo (還原)** 以取消更改。

當選擇 Advanced Configuration (進階設定)時，會出現 OpenVPN 伺服器進階設定畫面。



OpenVPN Server Advanced Configuration (OpenVPN 伺服器進階設定)		
項目	**設定值**	**說明**
TLS Cipher (TLS 密碼)	1. 必要設定. 2. **TLS-RSA-WITH-AES128-SHA** 預設選擇	從下拉清單中指定 **TLS: None / TLS-RSA-WITH-RC4-MD5 / TLS-RSA-WITH-AES128-SHA / TLS-RSA-WITH-AES256-SHA / TLS-DHE-DSS-AES128-SHA / TLS-DHE-DSS-AES256-SHA.** 注意: TLS 密碼僅可用於授權模式選擇 TLS 時。
TLS Auth. Key (TLS 驗證金鑰)	1. 可選設定. 2. 字串格式: 任意文字	指定 **TLS 驗證密鑰.** 注意: TLS 密碼僅可用於授權模式選擇 TLS 時。
Client to Client (用戶端到用戶端)	預設勾選此方框	勾選 " **Enable(啟用)**" 方框可啟用不同 OpenVPN 客戶端之間的通信。 注意: 用戶端到用戶端僅可用於授權模式選擇 TLS 時。
Duplicate CN (複製 CN)	預設勾選此方框	勾選 " **Enable(啟用)**" 方框以啟動**複製 CN** 功能.

		注意: **複製 CN** 僅可用於授權模式選擇 TLS 時。
Tunnel MTU (Ope 通道 MTU)	1. 必要設定 2. 預設 **1500**	指定**通道 MTU**。 ***範圍值*** : 0 ~ 1500.
Tunnel UDP Fragment (Ope 通道 UDP 片段)	1. 必要設定 2. 預設 **1500**	指定**通道 UDP 片段**，預設等於**通道 MTU**。 ***範圍值*** : 0 ~ 1500. 注意: 通道 UDP 片段僅可用於選擇 UDP 協定時。
Tunnel UDP MSS-Fix (Ope 通道 UDP MSS 修復)	1. 可選設定. 2. 預設未勾選	勾選 " **Enable(啟用)**" 方框以啟動**通道 UDP MSS 修復**功能。 注意: **通道 UDP MSS 修復**僅可用於選擇 UDP 協定時。
CCD-Dir Default File (CCD-Dir 預設檔)	1. 可選設定. 2. 字串格式: 任意文字	指定 **CCD-Dir 預設檔.** ***範圍值*** : 0 ~ 256 個字元.
Client Connection Script (用戶端連接腳本)	1. 可選設定. 2. 字串格式: 任意文字	指定**用戶端連接腳本.** ***範圍值*** : 0 ~ 256 個字元.
Additional Configuration (附加設定)	1. 可選設定. 2. 字串格式: 任意文字	指定**附加設定.** ***範圍值*** : 0 ~ 256 個字元.

作爲 OpenVPN Client 客戶端

如果選擇了 **Client(客戶端)**，則會出現 OpenVPN 客戶端列表畫面。

OpenVPN Client List | Add | Delete

ID	Client Name	Interface	Protocol	Port	Tunnel Scenario	Remote IP/FQDN	Remote Subnet	Redirect Internet Traffic	NAT	Authorization Mode	Encryption Cipher	Hash Algorithm	Enable	Actions

當按下 **Add (增加)**按鈕，將出現 **OpenVPN Client Configuration (OpenVPN 客戶端設定)**畫面，OpenVPN 客戶端設定畫面允許您指定 OpenVPN VPN 客戶端所需的參數，例如 “OpenVPN 客戶端名稱” 、 “介面” 、 “協定” 、 “通道方案” 、 “遠端 IP/FQDN” 、 “遠端子網” 、 “ 授權模式 ”、” 加密密碼 “、” 散列算法 “和通道啓動。

OpenVPN Client Configuration

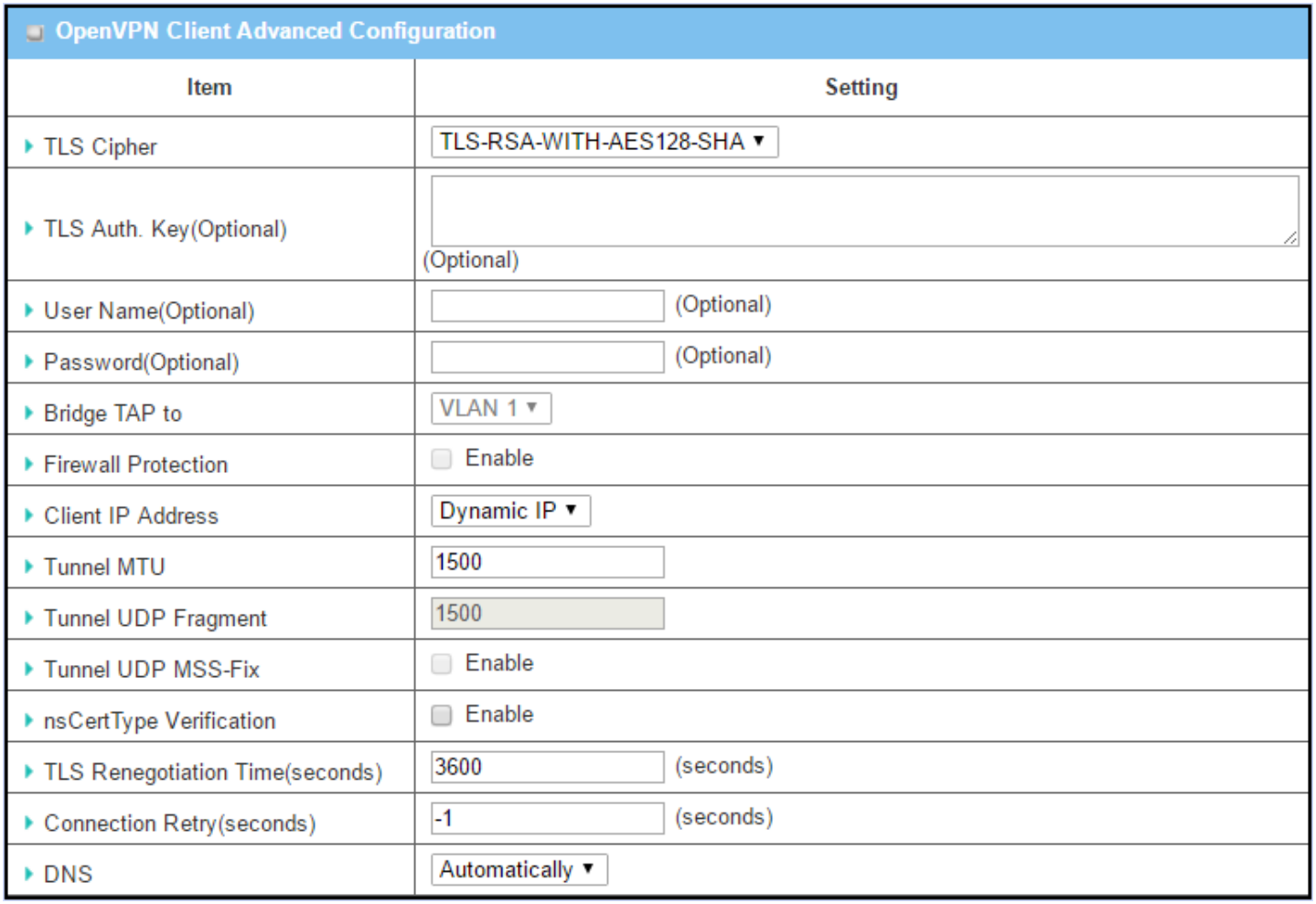
Item	Setting
OpenVPN Client Name	OpenVPN Client #1
Interface	WAN 1
Protocol	TCP Port: 443
Tunnel Scenario	TUN
Remote IP/FQDN	
Remote Subnet	255.255.255.0(/24)
Redirect Internet Traffic	Enable
NAT	Enable
Authorization Mode	TLS CA Cert.: Client Cert.: Client Key.: Please set the Certificate.
Encryption Cipher	Blowfish
Hash Algorithm	SHA-1
LZO Compression	Adaptive
Persist Key	Enable
Persist Tun	Enable
Advanced Configuration	Edit
Tunnel	Enable

OpenVPN Client Configuration (OpenVPN 客戶端設定)		
項目	**設定值**	**說明**
OpenVPN Client Name (OpenVPN 客戶端名稱)	必要設定	**OpenVPN 用戶端名稱**將用於標識通道清單中的客戶端。 ***範圍值***: 1 ~ 32 字元
Interface (介面)	1. 必要設定 2. 預設選擇 **WAN-1**	定義用於此 OpenVPN 客戶端通道的實體介面。
Protocol (協定)	1. 必要設定 2. 預設選擇 **TCP**	定義連接到 OpenVPN 客戶端選定的**協定**。 • **選擇 TCP 或 UDP** -> TCP 將用於 OpenVPN，將設置為 443 **埠**。 • **選擇 UDP** -> UDP 將用於 OpenVPN，將設置為 1194 **埠**。
Port (埠)	1. 必要設定 2. 預設設定 **4430**	指定連接到 OpenVPN 客戶端的**埠**。. ***範圍值***: 1 ~ 65535.
Tunnel Scenario (通道方案)	1. 必要設定 2. 預設選擇 **TUN**	指定連接到 OpenVPN 客戶端**通道方案**的類型 。可以是 **TUN** 通道方案或 **TAP** 通道方案.
Remote IP/FQDN (遠端 IP/FQDN)	必要設定	指定此 OpenVPN 用戶端通道的節點 OpenVPN 伺服器的**遠端 IP/FQDN** 。輸入 IP 位址或 FQDN。
Remote Subnet (遠端子網)	必要設定	指定此 OpenVPN 用戶端通道的節點 OpenVPN 伺服器的**遠端子網**。 補入遠端子網位址和遠端子網路遮罩.
Redirect Internet Traffic (轉向網路通信)	1. 可選設定. 2. 預設未勾選	勾選**Enable (啟用)** 方框以啟動**Redirect Internet Traffic (轉向網路通信)** 功能。
NAT	1. 可選設定. 2. 預設未勾選	勾選**Enable (啟用)** 方框以啟動**NAT**功能。
Authorization Mode (授權模式)	1. 必要設定 2. 預設選擇 **Static Key**	指定 OpenVPN 伺服器的授權模式。. • **TLS** -> OpenVPN 將使用 TLS 授權模式, 以下將顯示 **CA Cert.**, **Server Cert.** 和

		DH PEM。 **CA Cert** 可以在憑證中產生。請參閱**物件定義>憑證>受信任的憑證**。 **Server Cert** 可以在憑證中產生。請參閱**物件定義>憑證>我的憑證**。 • **Static Key (靜態密鑰)** -> OpenVPN 將使用靜態密鑰 (預共用) 授權模式, 並將顯示 **Local Endpoint IP Address (本地端點 ip 位址)**、**Remote Endpoint IP Address (遠端端點 IP 位址)** 和 **Static Key (靜態密鑰)**。 注意: 只有在通道方案中選擇 TUN 時，才可用靜態密鑰。
Local Endpoint IP Address (本地端點 IP 位址)	必要設定	指定此 OpenVPN 閘道的虛擬**本地端點 IP 位址**。 ***範圍值***: IP 格式為 10.8.0.x, x 的範圍為 1 ~ 254. 注意: 僅當在授權模式下選擇靜態密鑰時, 本地端點 IP 位址才可用。
Remote Endpoint IP Address (遠端端點 IP 位址)	必要設定	指定對等 OpenVPN 閘道的虛擬**遠端端點 IP 位址**。 ***範圍值***: IP 格式為 10.8.0.x, x 的範圍為 1 ~ 254. 注意: 只有在授權模式下選擇靜態密鑰時, 遠端端點 IP 位址才可用。
Static Key (靜態密鑰)	必要設定	指定**靜態密鑰**. 注意: 只有在授權模式下選擇靜態密鑰時，靜態密鑰才可用。
Encryption Cipher (加密密碼)	1. 必要設定. 2. 預設選擇 **Blowfish**	從下拉清單中選擇**加密密碼**。 選擇 **Blowfish/AES-256/AES-192/AES-128/None** 。
Hash Algorithm (雜湊演算法)	預設選擇 **SHA-1**	從下拉清單中選擇**雜湊演算法**。 選擇 **SHA-1/MD5/MD4/SHA2-256/SHA2-512/None/Disable.**
LZO Compression (壓縮)	預設選擇 **Adaptive**	指定 **LZO 壓縮** 計畫。 選擇 **Adaptive/YES/NO/Default**
Persis Key	1. 可選設定. 2. 預設勾選此方框.	勾選 " **Enable(啟用)**" 方框以啟動 **Persis Key** 功能。
Persis Tun	1. 可選設定. 2. 預設勾選此方框.	勾選 " **Enable(啟用)**" 方框以啟動 **Persis TUN** 功能。
Advanced Configuration (進階設定)	無	按一下 " **Edit (編輯)**" 按鈕進階設定 OpenVPN 客戶端。 如果按了按鈕則**階設定級**將顯示在下面。
Tunnel (通道)	預設未勾選	勾選 **Enable (啓動)**以啓動 OpenVPN 通道。

Save (保存)	無	點擊 **Save (保存)** 按鈕以保存設定值.
Undo (還原)	無	點擊 **Undo (還原)** 以取消更改。
Back (返回)	無	點擊 **Back (返回)** 以回到最後一頁。

當選擇了 **Advanced Configuration (進階設定)** 會出現 OpenVPN Client Advanced Configuration (OpenVPN 進客戶端進階設定) 畫面

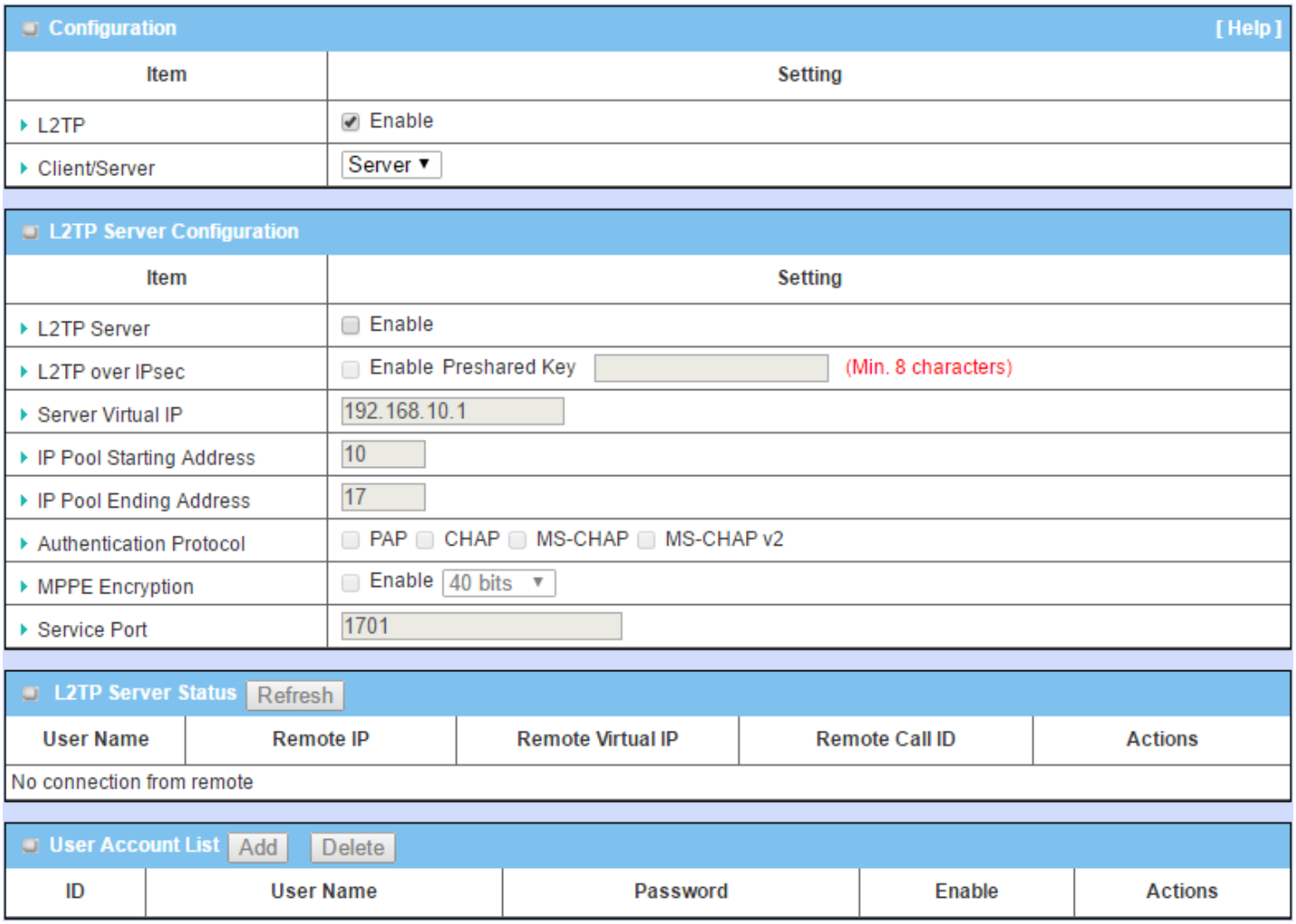


OpenVPN Client Advanced Configuration (OpenVPN 客戶端進階設定)		
項目	**設定值**	**說明**
TLS Cipher (TLS 密碼)	1. 必要設定. 2. **TLS-RSA-WITH-AES128-SHA** 預設選擇	從下拉清單中指定 **TLS: None / TLS-RSA-WITH-RC4-MD5 / TLS-RSA-WITH-AES128-SHA / TLS-RSA-WITH-AES256-SHA / TLS-DHE-DSS-AES128-SHA / TLS-DHE-DSS-AES256-SHA.**

		注意: TLS 密碼僅可用於授權模式選擇 TLS 時。
TLS Auth. Key (TLS 驗證金鑰)	1. 可選設定. 2. 字串格式: 任意文字	指定 **TLS 驗證密鑰.** 注意: TLS 密碼僅可用於授權模式選擇 TLS 時。
User Name (使用者名稱)	可選設定	如果伺服器要求，請輸入用於連接到 OpenVPN 伺服器的**使用者帳戶**。 注:使用者名稱僅可用於授權模式選擇 TLS 時。
Password (密碼)	可選設定	如果伺服器需要, 請輸入連接到 OpenVPN 伺服器的**密碼**。 注:密碼僅可用於授權模式選擇 TLS 時。
Bridge TAP to (橋接 TAP 至)	預設選擇 **VLAN 1**	指定 "**橋接 TAP 至**"將 TAP 介面橋接到某個本地網路介面或 VLAN。 注: **橋接 TAP 至**僅可用也 TAP 未選擇通道方案和 NAT 時。
Firewall Protection (防火牆保護)	預設未勾選	勾選該方框以啟動 **防火牆保護** 功能 . 注意: 防火牆保護僅可用於啟用 NAT 時。.
Client IP Address (用戶端 IP 位址)	預設選擇 **Dynamic IP**	指定虛擬 OpenVPN 用戶端的 IP 位址. 選擇 **Dynamic IP/Static IP (動態 IP /靜態 IP)**
Tunnel MTU (Ope 通道 MTU)	1. 必要設定 2. 預設 **1500**	指定**通道 MTU** . ***範圍值*** : 0 ~ 1500.
Tunnel UDP Fragment (Ope 通道 UDP 片段)	1. 必要設定 2. 預設 **1500**	指定**通道 UDP 片段**，預設等於**通道 MTU**。 ***範圍值*** : 0 ~ 1500. 注意: 通道 UDP 片段僅可用於選擇 UDP 協定時。
Tunnel UDP MSS-Fix (Ope 通道 UDP MSS 修復)	1. 可選設定. 2. 預設未勾選	勾選 " **Enable(啟用)**" 方框以啟動**通道 UDP MSS 修復**功能。 注意: **通道 UDP MSS 修復**僅可用於選擇 UDP 協定時。
nsCerType Verification (nsCerType 驗證)	預設未勾選	勾選 **Enable (啓動)**以啓動 **nsCerType 驗證**功能。 注:nsCerType 驗證僅可用於授權模式選擇 TLS 時。
TLS Renegotiation Time (seconds) (TLS 重新協商時間	預設值 3600	指定 **TLS 重新協商時間**間隔。 ***範圍值*** : -1 ~ 86400.

(秒))		
Connection Retry(seconds) (連接重試 (秒))	預設值爲 -1	指定**連接重試**間隔。 預設-1 表示不需要執行連接重試。 ***範圍值***：-1 ~ 86400, -1 表示不需要重試。
DNS	預設選擇 **Automatically**	指定 **DNS** 的設定。 選擇 **Automatically/Manually(自動 /手動)**。

5.1.3 L2TP

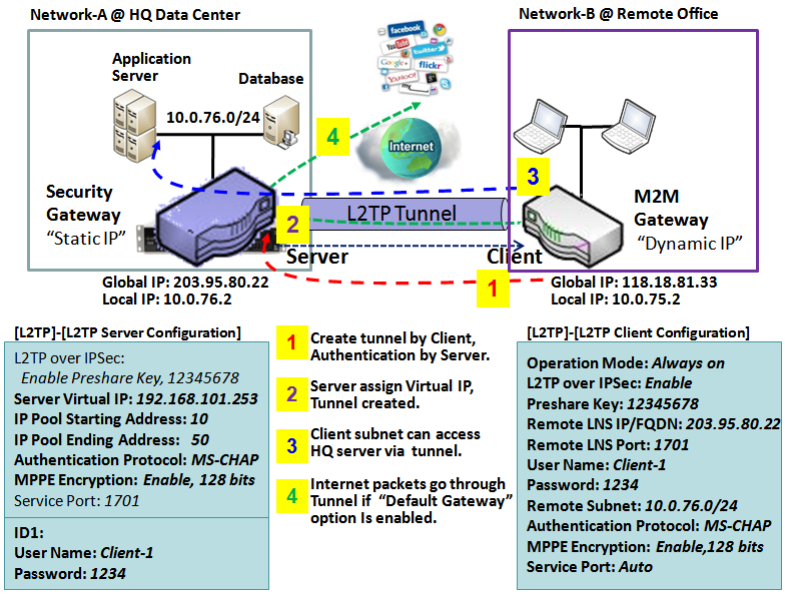


Layer 2 Tunneling Protocol 第二層通道協定(L2TP)是一種通道協定，用於支援虛擬私人網路(VPN)或作為 ISP 提供服務的一部分。它本身不提供任何加密或機密性。相反的依靠它在通道內傳遞的加密協定來提供隱私。該閘道器可以同時充當 L2TP 伺服器和 L2TP 客戶端。

L2TP 伺服器：客戶端必須具有靜態 IP 或 FQDN 才能建立 L2TP 通道。它還維護用於客戶端登錄認證的“使用者帳戶列表”(使用者名/密碼); 有一個虛擬 (IP Pool) IP 池為每個連線的 L2TP 客戶端分配虛擬 IP。

L2TP 客戶端：它可能是具有動態 IP 的遠端辦公室的移動使用者或閘道器。如要建立通道，請增加“使用者名稱”、“密碼”和伺服器的全局 IP。另外，將每個通道的操作模式視爲為主連線，爲另一個通

道容錯移轉，或平衡通道負載以增加總頻寬。將資料封包選擇 “Default Gateway (預設閘道器)” 或 “Remote Subnet (遠端子網)” 。您還可以定義通過 L2TP 通道的通信類型的 “預設閘道器/遠端子網” 參數。



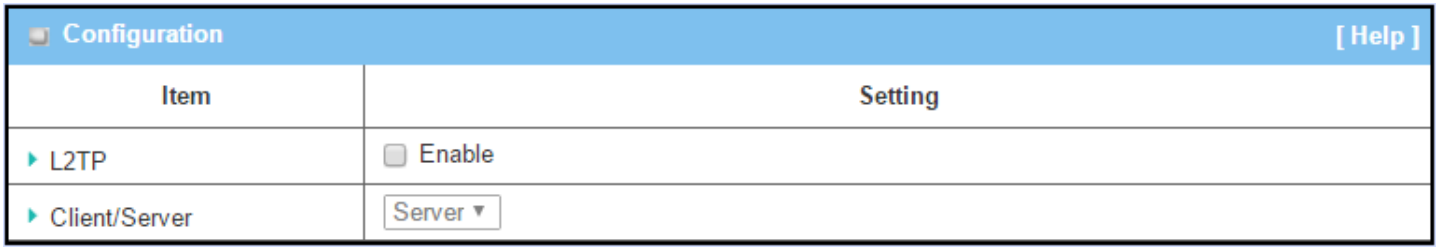
關於 L2TP 客戶端，L2TP 伺服器對節點的內網需要設定遠端子網項目。在 L2TP 客戶端，目標位於專用子網的資料封包將透過 L2TP 通道傳輸。其他人將依據 L2TP 客戶端節點閘道器的路由策略進行傳輸。但是，如果在遠端子網字段中輸入 0.0.0.0/0，則會被視為 L2TP 客戶端節點設備的 “預設閘道器” 設定，並且所有資料封包(包括 L2TP 客戶端節點設備的網際網路登入)都將透過 建立 L2TP 通道。 這表示將遠端 L2TP 伺服器節點體控制來自 L2TP 客戶機節點體的任何資料封包的流動。 這些資料封包透過 L2TP 通道。

設定 L2TP

轉到 Security > VPN > L2TP 頁面。

L2TP 設定允許使用者建立和設定 L2TP 通道。

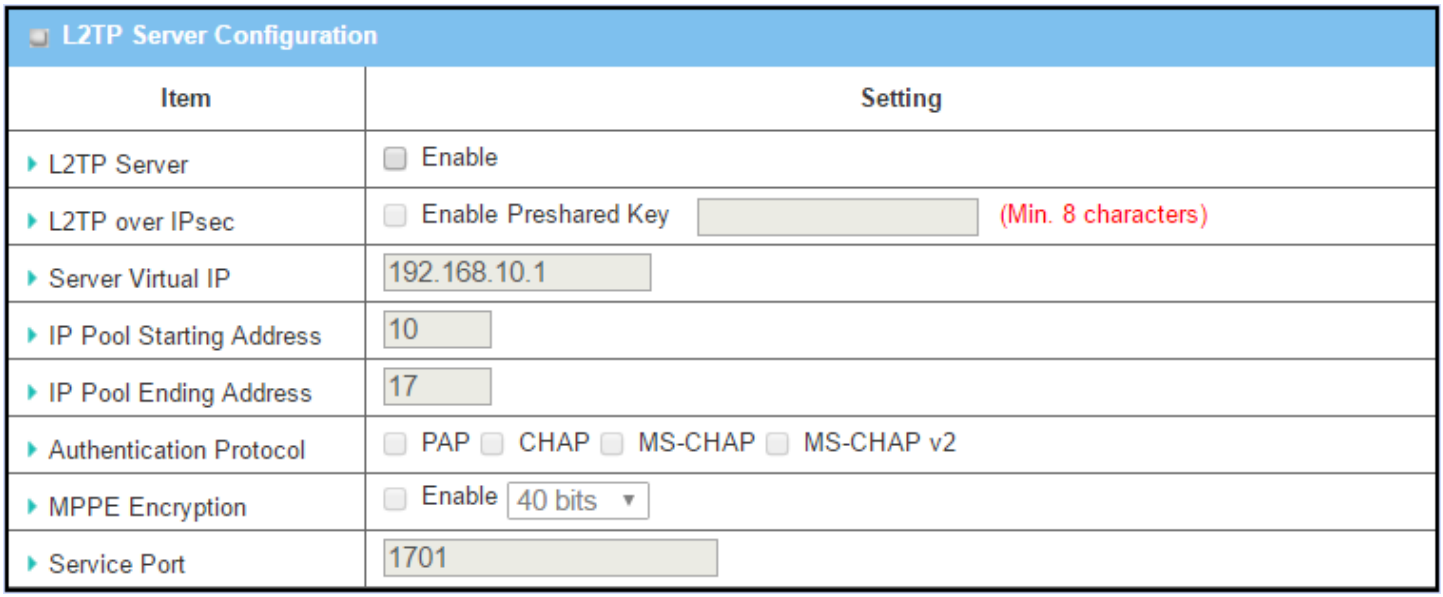
啓動 L2TP



Enable L2TP Window (啟動 L2TP 視窗)		
項目	**設定值**	**說明**
L2TP	預設未勾選	勾選 " **Enable(啟用)**" 方框以啟動 L2TP 功能。
Client/Server (客戶端/伺服器)	必要設定	爲閘道選擇 L2TP" **Server(伺服器)**" 或 "**Client (客戶端)**" 角色。以下是 L2TP 伺服器和客戶端的設定視窗。
Save (保存)	無	點擊 **Save (保存)** 按鈕以保存設定。

作爲 L2TP 伺服器

當在 **Server(伺服器)**選擇了 Client/Server(客戶端/伺服器)時，將出現 L2TP 伺服器設定。

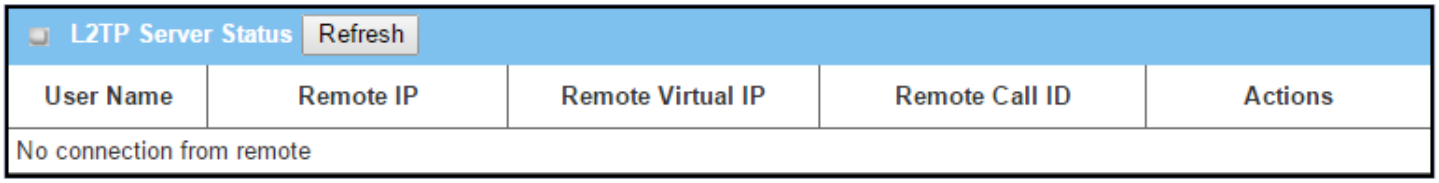


L2TP Server Configuration

Item	Setting
L2TP Server	Enable
L2TP over IPsec	Enable Preshared Key (Min. 8 characters)
Server Virtual IP	192.168.10.1
IP Pool Starting Address	10
IP Pool Ending Address	17
Authentication Protocol	PAP CHAP MS-CHAP MS-CHAP v2
MPPE Encryption	Enable 40 bits
Service Port	1701

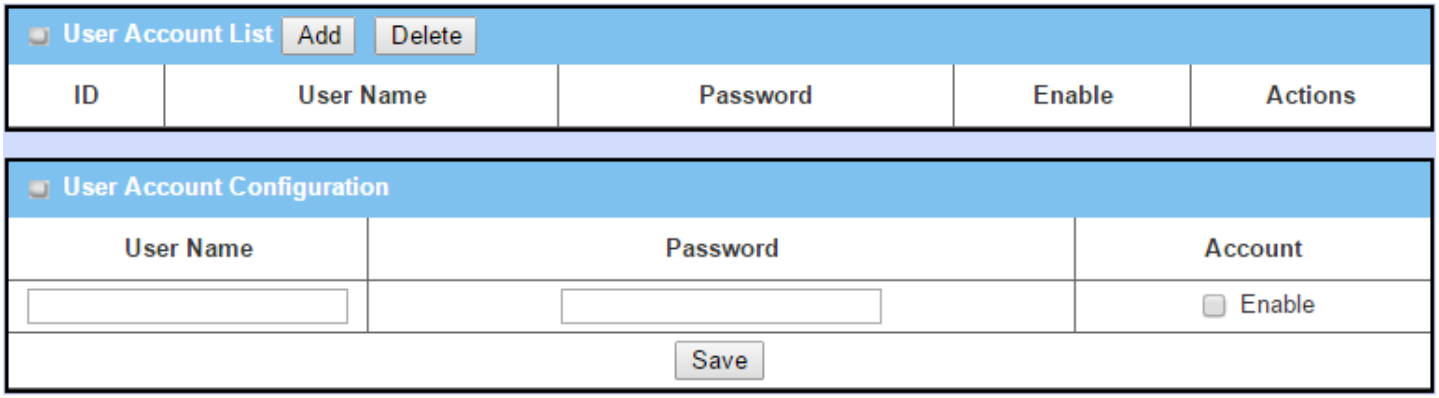
L2TP Server Configuration 項目	設定值	說明
L2TP Server (L2TP 伺服器)	預設未勾選	勾選 **Enable (啓動)** 方框以啓動 L2TP 伺服器
L2TP over IPsec	預設未勾選	勾選 Enable (啓動) 方框以啓動 L2TP over IPsec 並需要填寫預共用密鑰 (8 ~ 32 個字元)。
Server Virtual IP (伺服器虛擬 IP)	必要設定	指定 L2TP 伺服器虛擬 IP。
IP Pool Starting Address (IP 池起始位址)	1. 必要設定 2. 預設值 10.	指定虛擬 IP 池的 L2TP 伺服器啟動 IP。 ***範圍值***:1 ~ 254.
IP Pool Ending Address (IP 池結束位址)	1. 必要設定 2. 預設值 17.	指定虛擬 IP 池的 L2TP 伺服器結束 IP。 ***範圍值***:> = 起始位址且 < (起始位址 + 8) 或 254.
Authentication Protocol (身份驗證協定)	必要設定	為 L2TP 伺服器選擇單個或多個身份驗證協定身份驗證的 L2TP 客戶端。可用的身份驗證協定是 **PAP / CHAP / MS-CHAP / MS-CHAP v2**..
MPPE Encryption (MPPE 加密)	必要設定	指定是否支援 MPPE 協定。勾選 **Enable (啓動)** 方框啟用 MPPE 和從下拉清單中選擇 **40 bits / 56 bits / 128 bits**. 注意: 啟用 MPPE 加密時, 身份驗證協定 **PAP / CHAP** 選項將不可用.
Service Port (服務埠)	必要設定	指定 L2TP 伺服器使用的**服務埠**。 ***範圍值***:1 ~ 65535.

Save (保存)	無	按下 **Save (保存)** 按鈕以保存設定值.
Undo (還原)	無	點擊 **Undo (還原)** 按鈕以還原設定。.



L2TP Server Status (L2TP 伺服器狀態)

項目	設定值	說明
L2TP Server Status (L2TP 伺服器狀態)	無	顯示連線 L2TP 客戶端的使用者名、遠端 IP、遠端虛擬 IP 和遠端撥號 ID。 點擊 **Refresh(刷新)**按鈕以更新 L2TP 客戶端資訊。

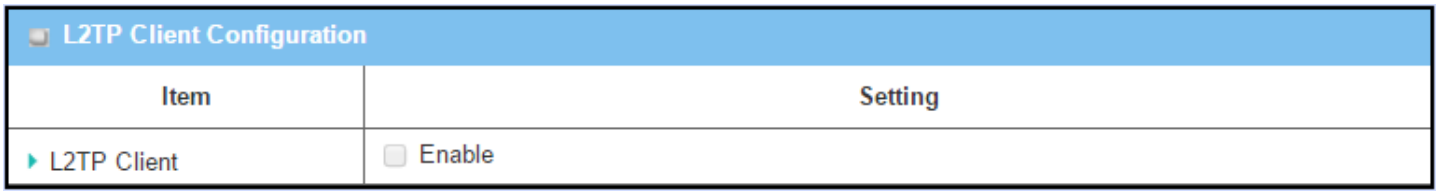


User Account List Window (使用者帳戶清單視窗)

項目	設定值	說明
User Account List (使用者帳戶清單)	最大 10 個使用者帳戶	這是 L2TP 身份驗證的使用者帳戶條目。可以為 L2 TP VPN 連線閘道的遠端客戶端建立和增加帳戶。 點擊 **Add(增加)**按鈕增加使用者帳戶。輸入使用者名和密碼。然後勾選 **enable(啟用)**方框以啟用使用者。 點擊 **Save(保存)**按鈕以保存新使用者帳戶。 點擊 **Delete(刪除)**按鈕, 可以永久刪除選擇的使用者帳戶。 ***範圍值***: 1 ~ 32 個字元.

作爲 L2TP 客戶端

當選擇了 Client/Server (客戶端/伺服器) 將會出現 L2TP Client Configuration (L2TP 客戶端設定)畫面。



L2TP Client Configuration (L2TP 客戶端設定)		
項目 Setting	設定值	說明
L2TP Client (L2TP 客戶端)	預設未勾選	勾選 Enable (啓動) 方框以啓動閘道器的 L2TP 客戶端。
Save (保存)	無	點擊 Save (保存) 按鈕以保存設定值。
Undo (還原)	無	點擊 Undo (還原) 按鈕以取消設定值。

建立/編輯 L2TP 客戶端

L2TP Client List & Status | Add | Delete | Refresh

ID	Tunnel Name	Interface	Virtual IP	Remote IP/FQDN	Remote Subnet	Status	Enable	Actions

當按下 **Add/Edit**(增加/編輯)按鈕時，會出現一系列的設定畫面。您最多可以增加 8 個 L2TP 客戶端。

L2TP Client Configuration

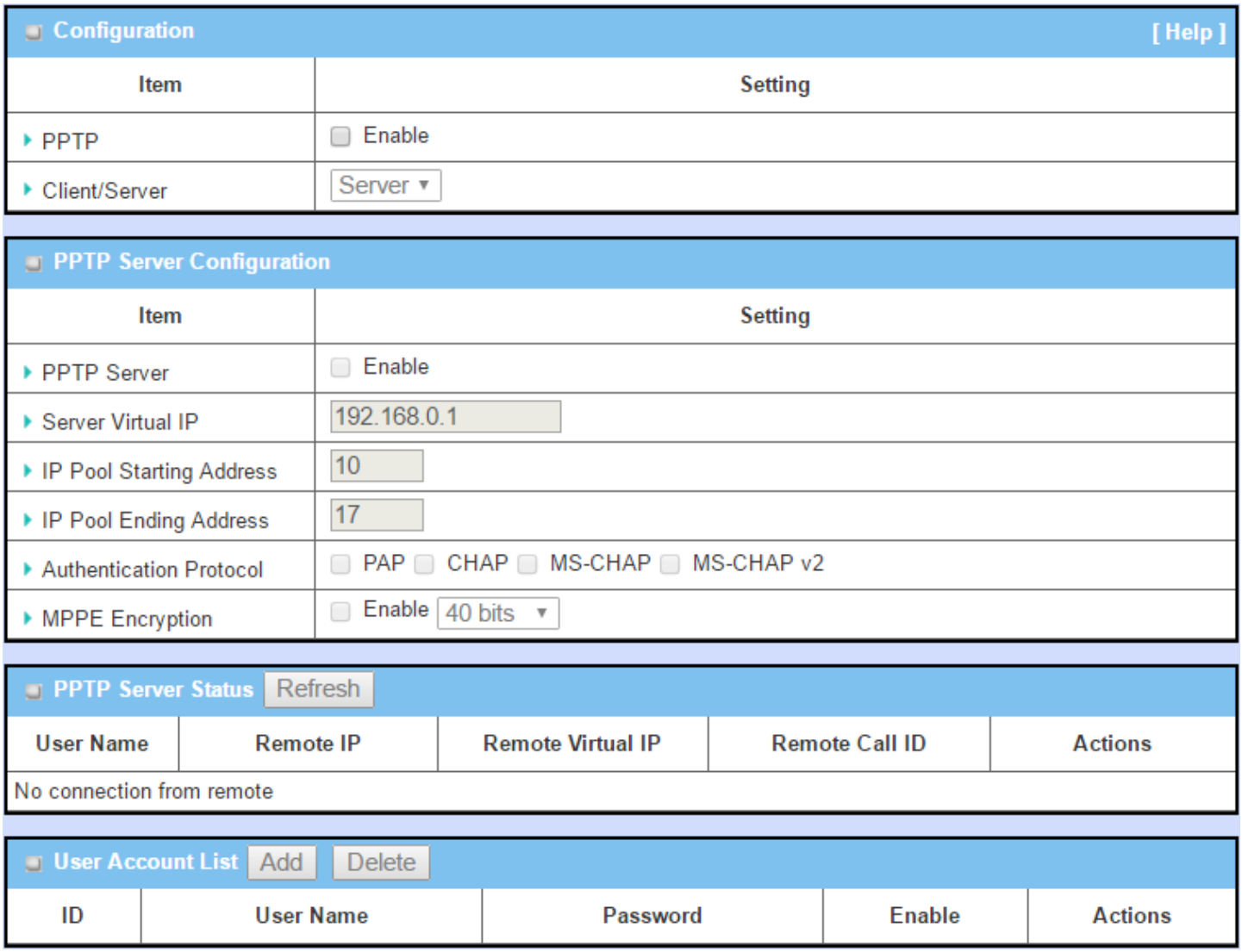
Item	Setting
Tunnel Name	L2TP #1
Interface	WAN1
Operation Mode	Always on
L2TP over IPsec	Enable Preshared Key (Min. 8 characters)
Remote LNS IP/FQDN	
Remote LNS Port	1701
User Name	
Password	
Tunneling Password (Optional)	
Remote Subnet	
Authentication Protocol	PAP CHAP MS-CHAP MS-CHAP v2
MPPE Encryption	Enable
LCP Echo Type	Auto Interval 30 seconds Max. Failure Time 6 times
Service Port	Auto 0
Tunnel	Enable

L2TP Client Configuration (L2TP 客戶端設定)		
項目 Setting	設定值	說明
Tunnel Name (隧道名稱)	必要設定	輸入通道名稱。 ***範圍值***: 1 ~ 32 個字元.

Interface (介面)	必要設定	定義此 L2TP 通道的選擇介面 (僅當啟用 WAN-1 介面時, **WAN-1** 才可用) 同樣適用於其他 WAN 介面 (例如 **WAN-2).**
Operation Mode (操作模式)	1. 必要設定 2. 預設選擇 **Always on**	定義 L2TP 通道的操作模式。可能是 **Always On(永遠啓動)**或 **Failover(容錯移轉)**。. 如果此通道設定為容錯移轉通道，您需要進一步選擇要轉移的主通道. 注意:單 WAN 的閘道器不能選**容錯移轉**。.
L2TP over IPsec	預設未勾選	勾選 **Enable (啓動)**方框啓 L2TP over IPsec, 並進一步指定預共用密鑰(8 ~ 32 個字元).
Remote LNS IP/FQDN (遠端 LNS IP/FQDN)	必要設定	輸入公共 IP 位址或的 L2TP 伺服器的 FQDN。
Remote LNS Port (遠端 LNS 埠)	1. 必要設定 2. 預設 **1701**	輸入此 L2TP 通道的遠端 LNS 埠。 ***範圍值***:1 ~ 65535.
User Name (使用者名稱)	必要設定	輸入此 L2TP 隧道的**使用者稱**以在連接到 L2TP 服務器時進行身份驗證。 ***範圍值*** : 1 ~ 32 個字元.
Password (密碼)	必要設定	輸入此 L2TP 隧道的**密碼**以在連接到 L2TP 服務器時進行身份驗證。
Tunneling Password(Optional) (隧道密碼 (可選))	預設未勾選	輸入此 L2TP 隧道的**隧道密碼**進行認證。
Remote Subnet (遠端子網)	必要設定	指定此 L2TP 通道的遠程子網以連到 L2TP 服務器。 遠程子網格式必須是 IP 地址/網路遮罩(例如 10.0.0.2/24)。 用於 L2TP VPN 伺服器的內網。因此在 L2TP 客戶端目標位於專用子網的數據封包將通過 L2TP VPN 通道傳輸。其他人將根據 L2TP 客戶端的安全閘道的當前路由策略進行傳輸。 如果在遠程子網段中輸入 0.0.0.0/0，將被視為 L2TP 客戶端節點設備的預設閘道設定，所有數據封包(包括 L2TP 客戶端節點設備的網際網路登入)都將通過建立的 L2TP VPN 通道。這表示遠程 L2TP VPN 伺服器控制來自 L2TP 客戶端的任何數據包的流量。
Authentication Protocol (身份驗證協定)	1. 必要設定 2. 預設未勾選	為此 L2TP 通道指定一個或多個認證協議。 可用的身份驗證方法是 **PAP / CHAP / MS-CHAP / MS-CHAP v2**。
MPPE Encryption (MPPE 加密)	1. 預設未勾選 2. 可選設定	指定 L2TP 伺服器是否支援 MPPE 協議。 點擊 **Enable(啟用)**方框啟用 MPPE。 注意：啟用 MPPE 加密時，認證協定 **PAP / CHAP** 選項將不可用。

LCP Echo Type (LCP 回聲類型)	1. 預設 Auto	為此 L2TP 通道指定 LCP 回聲類型。 選擇 **Auto(自動)**、**User-defined(使用者定義)**或 **Disable(禁用)**。 **Auto(自動)**：系統設置間隔和最大失敗次數。 **User-defined(使用者定義)**：輸入時間間隔和最大 失敗次數。 間隔的預設值是 30 秒，最大失敗次數是 6 次。 **Disable(禁用)**：禁用 LCP 回聲。 ***範圍值*** **:** 間隔時間為 1 ~ 99999, 故障時間為 1 ~ 999.
Service Port (服務埠)	必要設定	指定要使用的此 L2TP 通道的**服務埠**，可以選 **Auto(自動), (1701) for Cisco)** 或 **User-defined(使用者定義)**. **Auto(自動)**:由系統偵測服務埠。 **1701 (for Cisco):** 系統使用 1701 埠連線 CISCO L2TP 伺服器. **User-defined(使用者定義的) :** 輸入隨從服務埠，預設值為 0 ***範圍值*** :0 ~ 65535.
Tunnel (通道)	預設未勾選	勾選 **Enable (啓動)** 方框以啓動 L2TP 通道。
Save (保存)	無	點擊 **Save (保存)** 按鈕以保存設定值。
Undo (還原)	無	點擊 **Undo (還原)** 按鈕以取消設定值。
Back (返回)	無	點擊 **Back (返回)**按鈕以返回前一頁。

5.1.4 PPTP

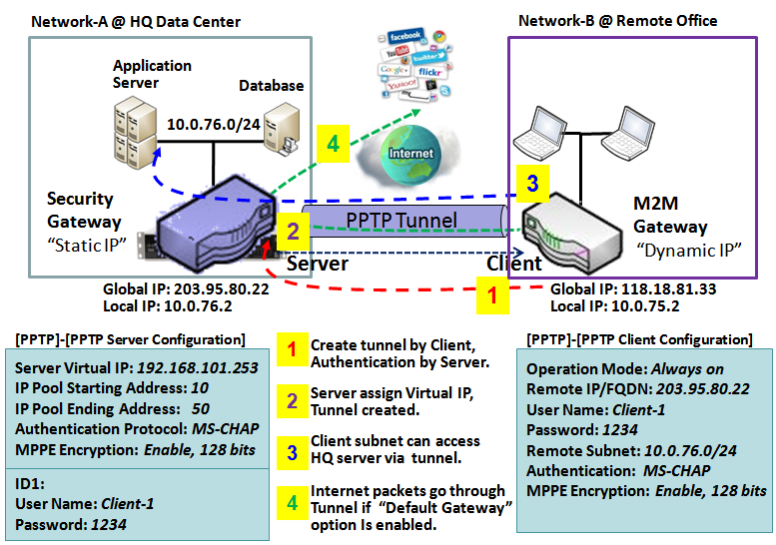


Point-to-Point Tunneling Protocol 點對點通道協定(PPTP)是一種進行虛擬私人網路的方法。PPTP 使用 TCP 上的控制通道和 GRE 通道來封裝 PPP 資料封包。它是一種客戶端和伺服器的技術。對於 PPTP 通道，有各種級別的身份驗證和加密，通常本身就是 Windows PPTP 堆棧的標準功能。對於不同的通道，安全閘道器可以扮演 PPTP VPN 通道的 “PPTP 伺服器” 角色或 “PPTP 客戶端” 角色，或同時扮演這兩個角色。 PPTP 通道的程序幾乎與 L2TP 相同。

PPTP 伺服器：它必須具有靜態 IP 或 FQDN 以供客戶端建立 PPTP 通道。它還維護用於客戶端登錄認證的 “使用者帳戶列表” (使用者名/密碼); 有一個虛擬 (IP Pool) IP 池為每個連線的 PPTP 客戶端分配虛

擬 IP。

PPTP 客戶端：它可能是具有動態 IP 的遠端辦公室的移動使用者或閘道器。要建立通道，請增加“使用者名”、“密碼”和伺服器的全局 IP。此外還需要將每個通道的操作模式視爲為主要連線，對另一個通道進行容錯移轉或平衡通道負載增加總體頻寬。將資料封包選擇“Default Gateway (預設閘道器)”或“Remote Subnet (遠端子網)”。您還可以定義通過 PPTP 通道的通信類型的“預設閘道器/遠端子網”參數。



這些資料封包透過 PPTP 通道

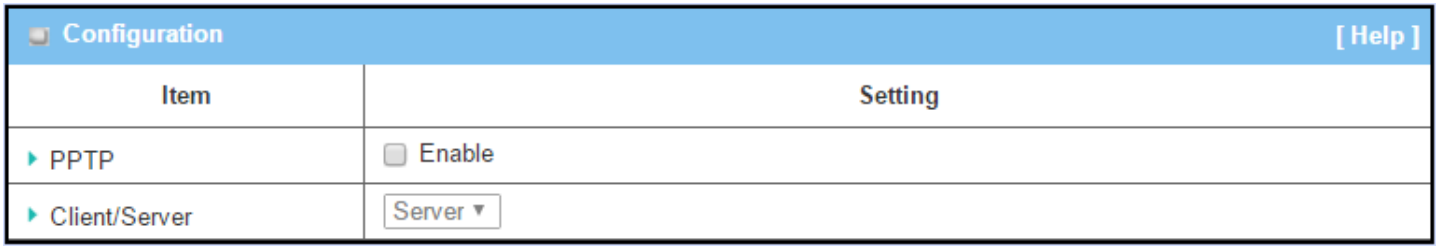
關於 PPTP 客戶端，PPTP 伺服器對節點的內網需要設定遠端子網項目。在 PPTP 客戶端，目標位於專用子網的資料封包將透過 PPTP 通道傳輸。其他人將依據 PPTP 客戶端節點閘道器的路由策略進行傳輸。但是，如果在遠端子網字段中輸入 0.0.0.0/0，則會被視為 PPTP 客戶端節點設備的“預設閘道器”設定，並且所有資料封包(包括 PPTP 客戶端節點設備的網際網路登入)都將透過 建立 PPTP 通道。這表示將遠端 PPTP 伺服器節點體控制來自 PPTP 客戶機節點體的任何資料封包的流動。

設定 PPTP

轉到 Security > VPN > PPTP 頁面。

PPTP 設定允許使用者建立和設定 PPTP 通道。

啓動 PPTP

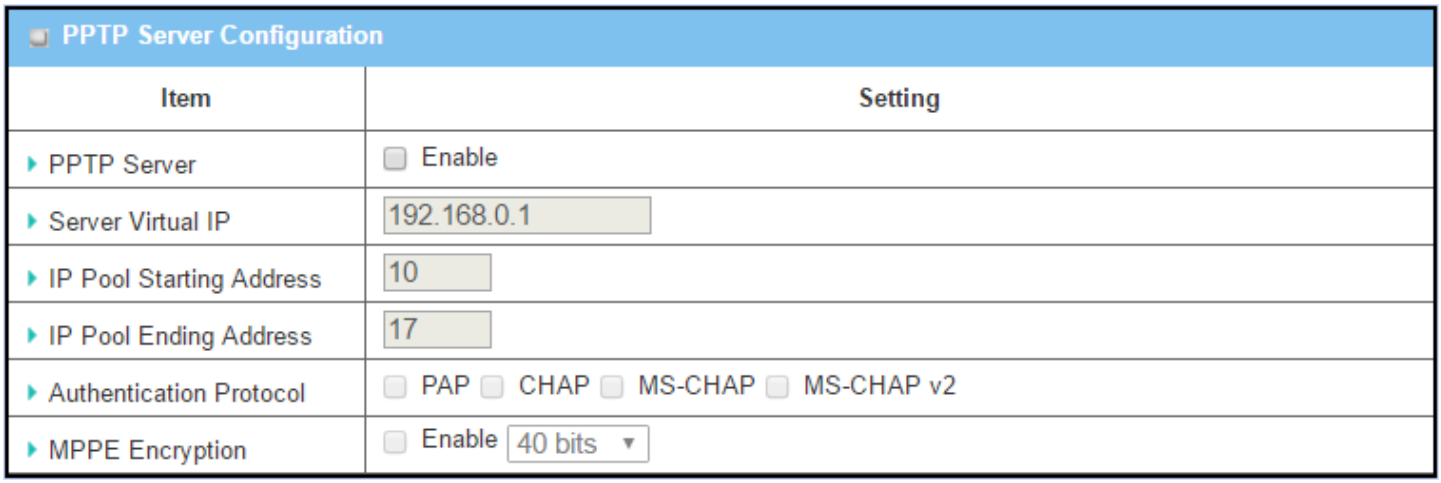


Enable PPTP Window (啓動 PPTP 視窗)		
項目	**設定值**	**說明**
PPTP	預設未勾選	勾選 Enable (啓動)以啓動 PPTP 功能。
Client/Server (客戶端/伺服器)	必要設定	指定 PPTP 的角色。選擇 **Server(伺服器)**或 **Client(用戶端)**角色。下面是 PPTP 伺服器和用戶端的設定視窗。
Save (保存)	無	點擊 Save (保存) 按鈕以保存設定值。

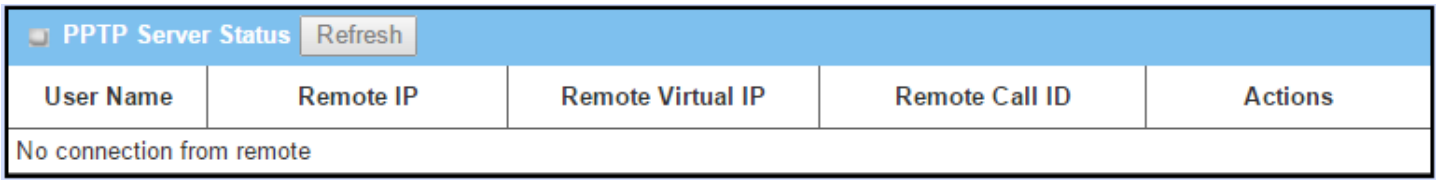
作爲 PPTP 伺服器

閘道器最多支援 10 個 PPTP 使用者帳戶。

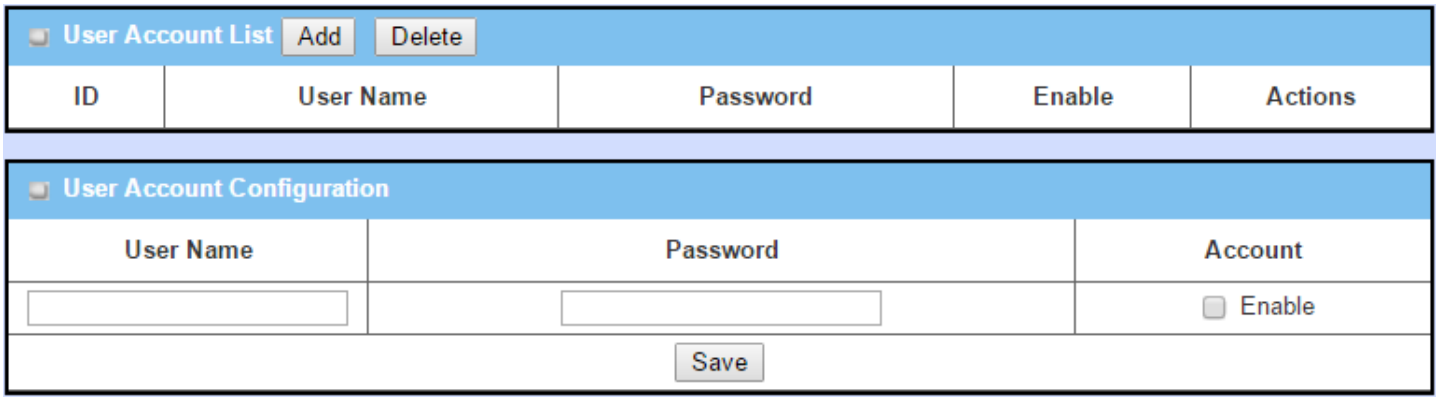
當在 **Server(伺服器)**選擇了 Client/Server(客戶端/伺服器)時，將出現 PPTP 伺服器設定。



PPTP Server Configuration Window (PPTP 伺服器設定視窗)		
項目	設定值	說明
PPTP Server (PPTP 伺服器)	預設未勾選	勾選 Enable (啓動) 方框以啓動 PPTP server role of the gateway.
Server Virtual IP (伺服器虛擬 IP)	1. 必要設定 2. 預設 192.168.0.1	指定 PPTP 伺服器虛擬 IP 位址。虛擬 IP 位址將作為 PPTP 客戶端的虛擬 DHCP 伺服器。在建立 PPTP 通道後, 客戶端將分配到一個虛擬 IP 位址。
IP Pool Starting Address (IP 池起始位址)	1. 必要設定 2. 預設值 10.	這是 PPTP 伺服器的虛擬 IP DHCP 伺服器。使用者可以指定要分配 PPTP 客戶端 IP 位址子網的初始 IP 位址。 ***範圍值***:1 ~ 254.
IP Pool Ending Address (IP 池結束位址)	1. 必要設定 2. 預設值 17.	這是 PPTP 伺服器的虛擬 IP DHCP 伺服器。使用者可以指定要分配 PPTP 客戶端 IP 位址子網的最後 IP 位址。 ***範圍值***:> = 起始位址且 < (起始位址 + 8) 或 254.
Authentication Protocol (身份驗證協定)	1. 必要設定 2. 預設未勾選	為 L2TP 伺服器選擇單個或多個身份驗證協定身份驗證的 PPTP 客戶端。可用的身份驗證協定是 **PAP / CHAP / MS-CHAP / MS-CHAP v2**..
MPPE Encryption (MPPE 加密)	1. 必要設定 2. 預設未勾選	指定是否支援 MPPE 協定。勾選 **Enable (啓動)** 方框啟用 MPPE 和從下拉清單中選擇 **40 bits / 56 bits / 128 bits**. 注意: 啟用 MPPE 加密時, 身份驗證協定 **PAP / CHAP** 選項將不可用.
Save (保存)	無	點擊 Save (保存) 按鈕以保存設定值。
Undo (還原)	無	點擊 Undo (還原) 按鈕以取消設定值。



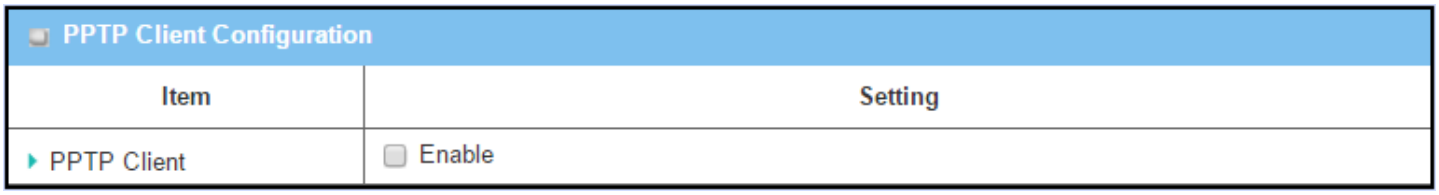
PPTP Server Status Window(PPTP 伺服器狀態視窗)		
項目	設定值	說明
PPTP Server Status	無	顯示連線 PPTP 客戶端的使用者名、遠端 IP、遠端虛擬 IP 和遠端撥號 ID。 點擊 **Refresh(刷新)**按鈕以更新 L2TP 客戶端資訊。



User Account List Window (使用者帳戶清單視窗)		
項目	設定值	說明
User Account List (使用者帳戶清單)	最大 10 個使用者帳戶	這是 PPTP 身份驗證的使用者帳戶條目。可以為 PPTP VPN 連線閘道的遠端客戶端建立和增加帳戶。 點擊 **Add(增加)**按鈕增加使用者帳戶。輸入使用者名和密碼。然後勾選 **enable(啟用)**方框以啟用使用者。 點擊 **Save(保存)**按鈕以保存新使用者帳戶。 點擊 **Delete(刪除)**按鈕, 可以永久刪除選擇的使用者帳戶。 ***範圍值***: 1 ~ 32 個字元

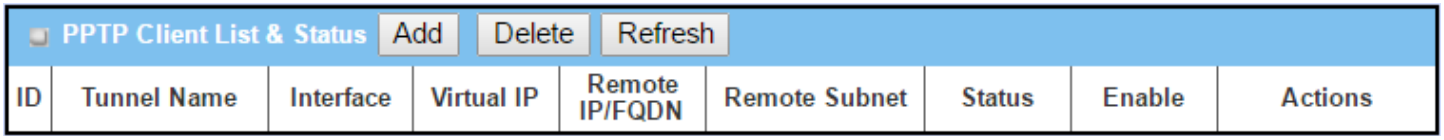
作爲 PPTP 客戶端

在 Client/Server(客戶端/伺服器)中選擇 Client(客戶端)時，將出現一系列 PPTP 客戶端配置。

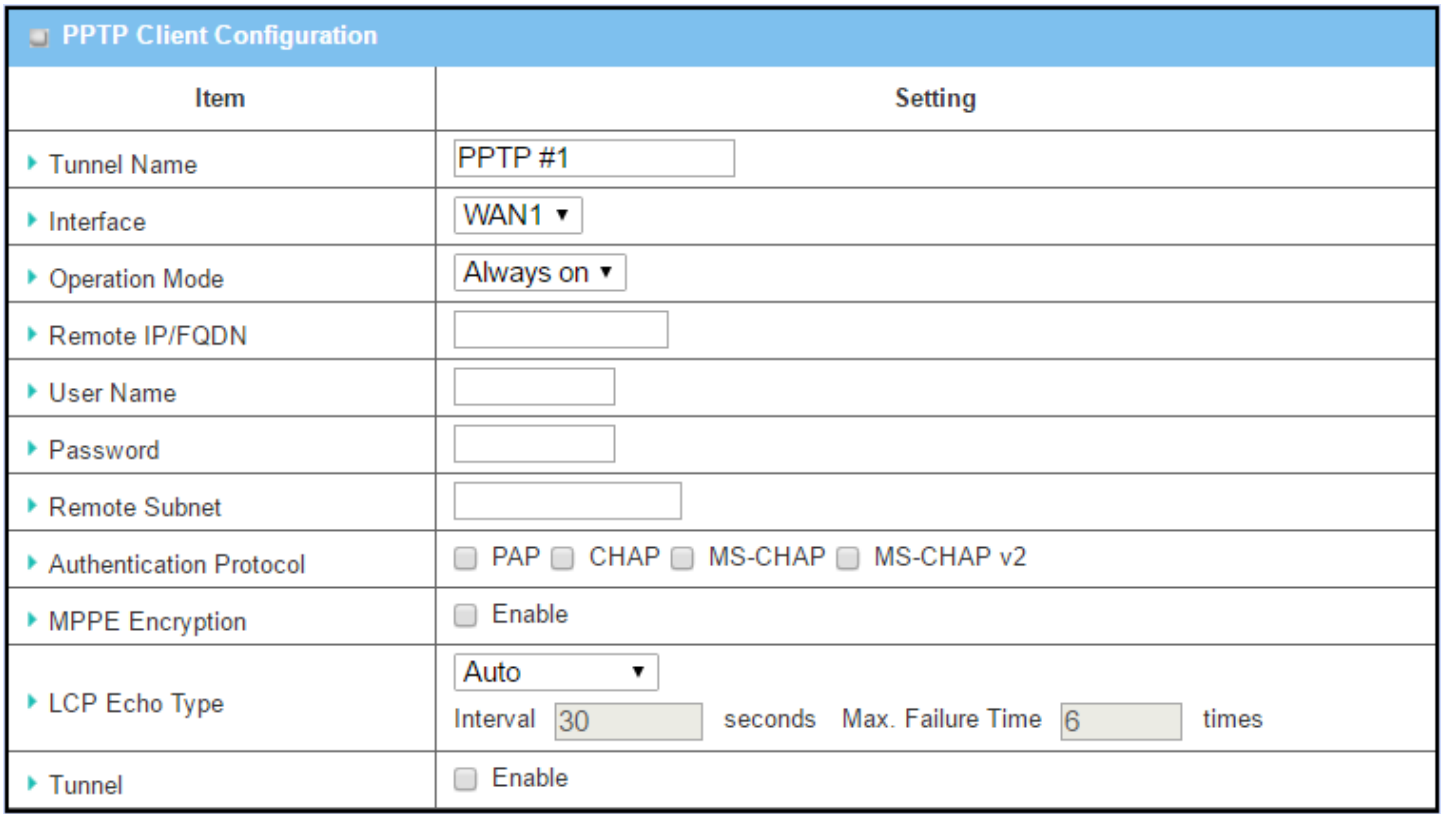


PPTP Client Configuration (PPTP 客戶端設定)		
項目	設定值	說明
PPTP Client (PPTP 客戶端)	預設未勾選	勾選 Enable (啓動) 方框以啓動閘道器的 PPTP 客戶端。
Save (保存)	無	點擊 Save (保存) 按鈕以保存設定值。
Undo (還原)	無	點擊 Undo (還原) 按鈕以取消設定值。

建立/編輯 PPTP 客戶端



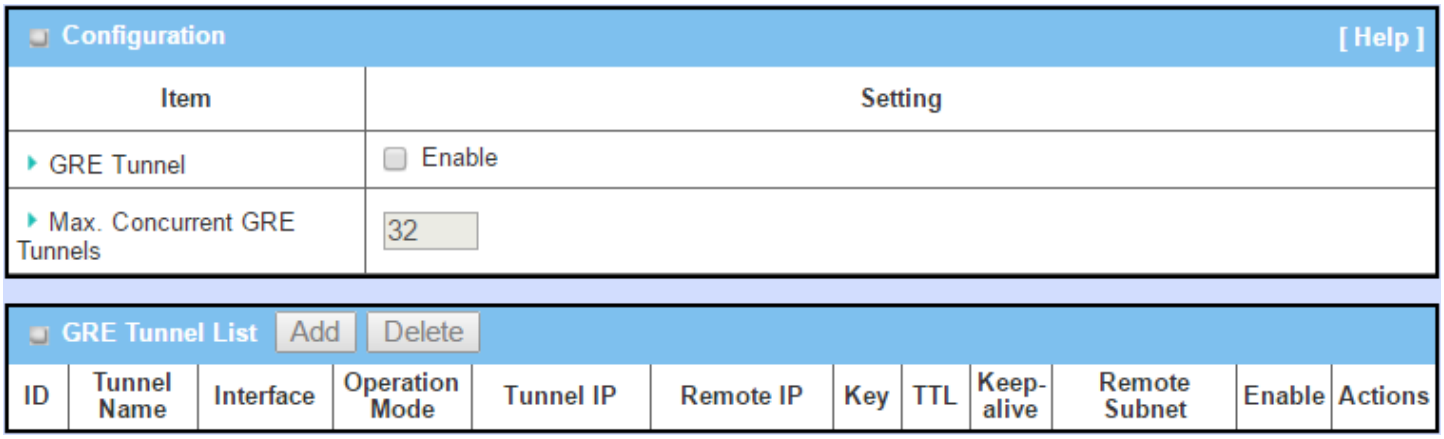
當按下 **Add/Edit(增加/編輯)**按鈕時，將出現一系列 PPTP 客戶端設定畫面。



PPTP Client Configuration Window (PPTP 客戶端設定視窗)		
項目	**設定值**	**說明**
Tunnel Name (隧道名稱)	必要設定	輸入通道名稱。 ***範圍值***: 1 ~ 32 個字元.
Interface (介面)	必要設定	定義此 PPTP 通道的選擇介面 (僅當啟用 WAN-1 介面時, **WAN-1** 才可用) 同樣適用於其他 WAN 介面 (例如 **WAN-2).**
Operation Mode (操作模式)	1. 必要設定 2. 預設選擇 **Always on**	定義 PPTP 通道的操作模式。可能是 **Always On(永遠啓動)**或 **Failover(容錯移轉)**。. 如果此通道設定為容錯移轉通道，您需要進一步選擇要轉移的主通道. 注意:單 WAN 的閘道器不能選**容錯移轉**。.
Remote IP/FQDN (遠端 IP/FQDN)	1. 必要設定. 2. 格式可以是 ipv4 位址或 FQDN	輸入公共 IP 位址或的 PPTP 伺服器的 FQDN。
User Name (使用者名稱)	必要設定	輸入此 PPTP 隧道的**使用者稱**以在連接到 PPTP 服務器時進行身份驗證。 ***範圍值***: 1 ~ 32 個字元.
Password (密碼)	必要設定	輸入此 PPTP 隧道的**密碼**以在連接到 PPTP 服務器時進行身份驗證。
Remote Subnet	必要設定	指定此 PPTP 通道的遠程子網以連到 PPTP 服務器。

(遠端子網)		遠程子網格式必須是 IP 地址/網路遮罩(例如 10.0.0.2/24)。 用於 PPTP VPN 伺服器的內網。因此在 PPTP 客戶端目標位於專用子網的數據封包將通過 PPTP VPN 通道傳輸。其他人將根據 PPTP 客戶端的安全閘道的當前路由策略進行傳輸。 如果在遠程子網段中輸入 0.0.0.0/0，將被視為 PPTP 客戶端節點設備的預設閘道設定，所有數據封包(包括 PPTP 客戶端節點設備的網際網路登入)都將通過建立的 PPTP VPN 通道。這表示遠程 PPTP VPN 伺服器控制來自 PPTP 客戶端的任何數據包的流量。
Authentication Protocol (身份驗證協定)	1. 必要設定 2. 預設未勾選	為此 PPTP 通道指定一個或多個認證協議。 可用的身份驗證方法是 **PAP / CHAP / MS-CHAP / MS-CHAP v2**。
MPPE Encryption (MPPE 加密)	1. 預設未勾選 2. 可選設定	指定 PPTP 伺服器是否支援 MPPE 協議。 點擊 **Enable(啟用)**方框啟用 MPPE。 注意：啟用 MPPE 加密時，認證協定 **PAP / CHAP** 選項將不可用。
LCP Echo Type (LCP 回聲類型)	1. 預設 Auto	為此 PPTP 通道指定 LCP 回聲類型。 選擇 **Auto(自動)**、**User-defined(使用者定義)**或 **Disable(禁用)**。 **Auto(自動)**：系統設置間隔和最大失敗次數。 **User-defined(使用者定義)**：輸入時間間隔和最大 失敗次數。 間隔的預設值是 30 秒，最大失敗次數是 6 次。 **Disable(禁用)**：禁用 LCP 回聲。 ***範圍值***: 間隔時間為 1 ~ 99999, 故障時間為 1 ~ 999.
Tunnel (通道)	預設未勾選	勾選 **Enable (啓動)** 方框以啓動 PPTP 通道。
Save (保存)	無	點擊 **Save (保存)** 按鈕以保存設定值。
Undo (還原)	無	點擊 **Undo (還原)** 按鈕以取消設定值。
Back (返回)	無	點擊 **Back (返回)**按鈕以返回前一頁。

5.1.5 GRE

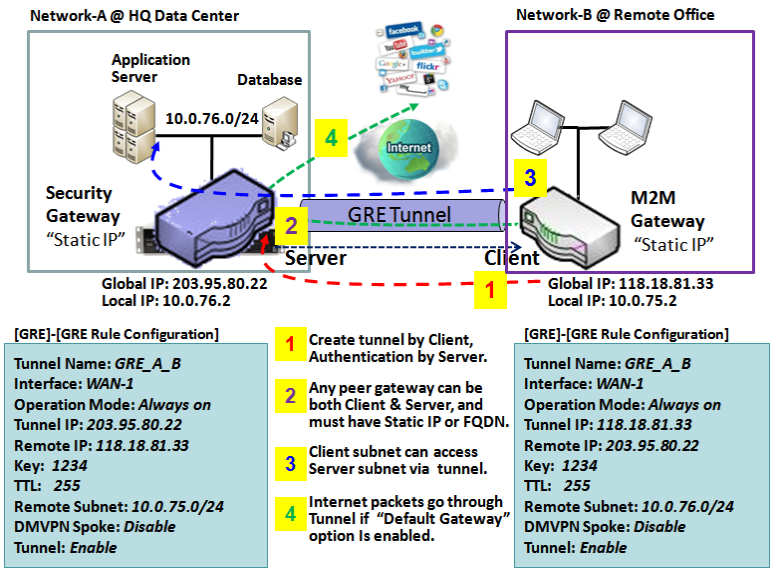


Generic Routing Encapsulation 通用路由封裝(GRE)是 Cisco 思科系統公司開發的通道協定，它透過網際網路協定網際網路路在虛擬點對點鏈路內封裝了各種各樣的網路層協定。

為遠端站點部署 M2M 閘道器，並使用 GRE 通道與控制中心建立虛擬私人網路。使 M2M 閘道器後面的所有客戶端主機都可以與控制中心閘道器後面的伺服器主機進行資料通信。

GRE 通道與 IPsec 通道類似，客戶端請求與伺服器建立通道。客戶端和伺服器都必須具有靜態 IP 或 FQDN。 任何節點閘道器即使是使用同一羣組設定的規則都可以作為客戶端或伺服器使用。

GRE 通道方案



為了建立 GRE 通道，每個節點體需要將其全局 IP 設定為通道 IP，並登入對方的全局 IP 作為遠端 IP。

每個節點必須進一步指定 GRE 伺服器節點的內部網的遠端子網項目。在 GRE 客戶端，目的地在專用子網中的資料封包將透過 GRE 通道傳輸。 其他人將依據 GRE 客戶端節點閘道器的目前路由策略進行傳輸。 但是，如果在遠端子網字段中輸入了 0.0.0.0/0，則它將被視為 GRE 客戶端節點設備的" Default Gateway (預設閘道器)" 設定，並且所有資

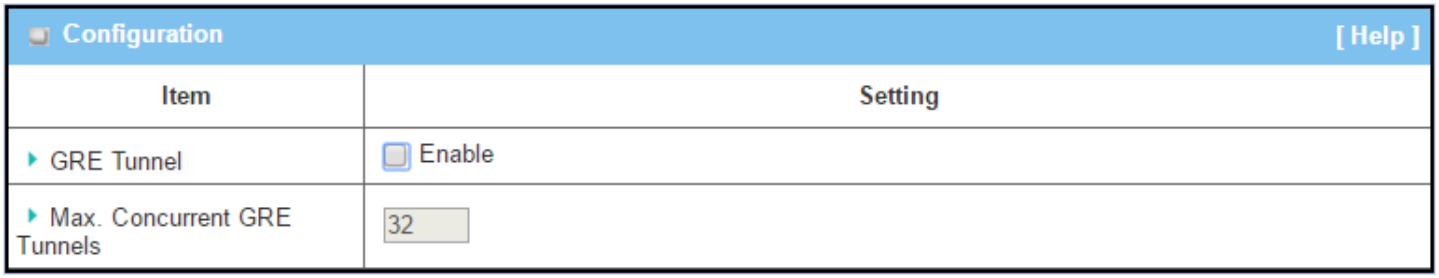
料封包(包括 GRE 客戶端節點設備的網際網路登入)將透過 建立了 GRE 通道。這表示遠端 GRE 伺服器節點控制來自 GRE 客戶節點的任何資料封包的流動。
如果 GRE 伺服器支援 DMVPN Hub 功能(如 Cisco 路由器作為 VPN 集中器)，則 GRE 客戶端可以在此啓動 DMVPN 分支功能，因為它是透過 GRE over IPsec 通道進行的。

設定 GRE

轉到 Security > VPN > GRE 頁面。

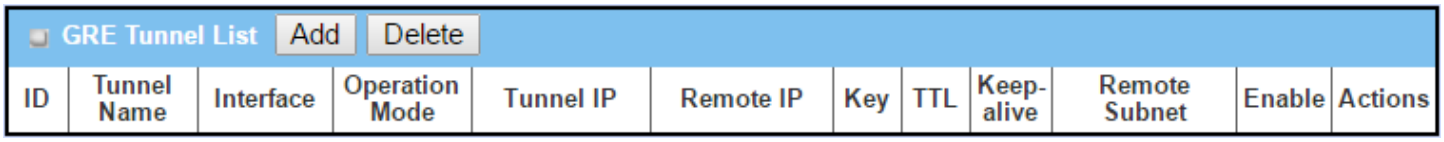
GRE 設定允許使用者建立和設定 GRE 通道。

啓動 GRE

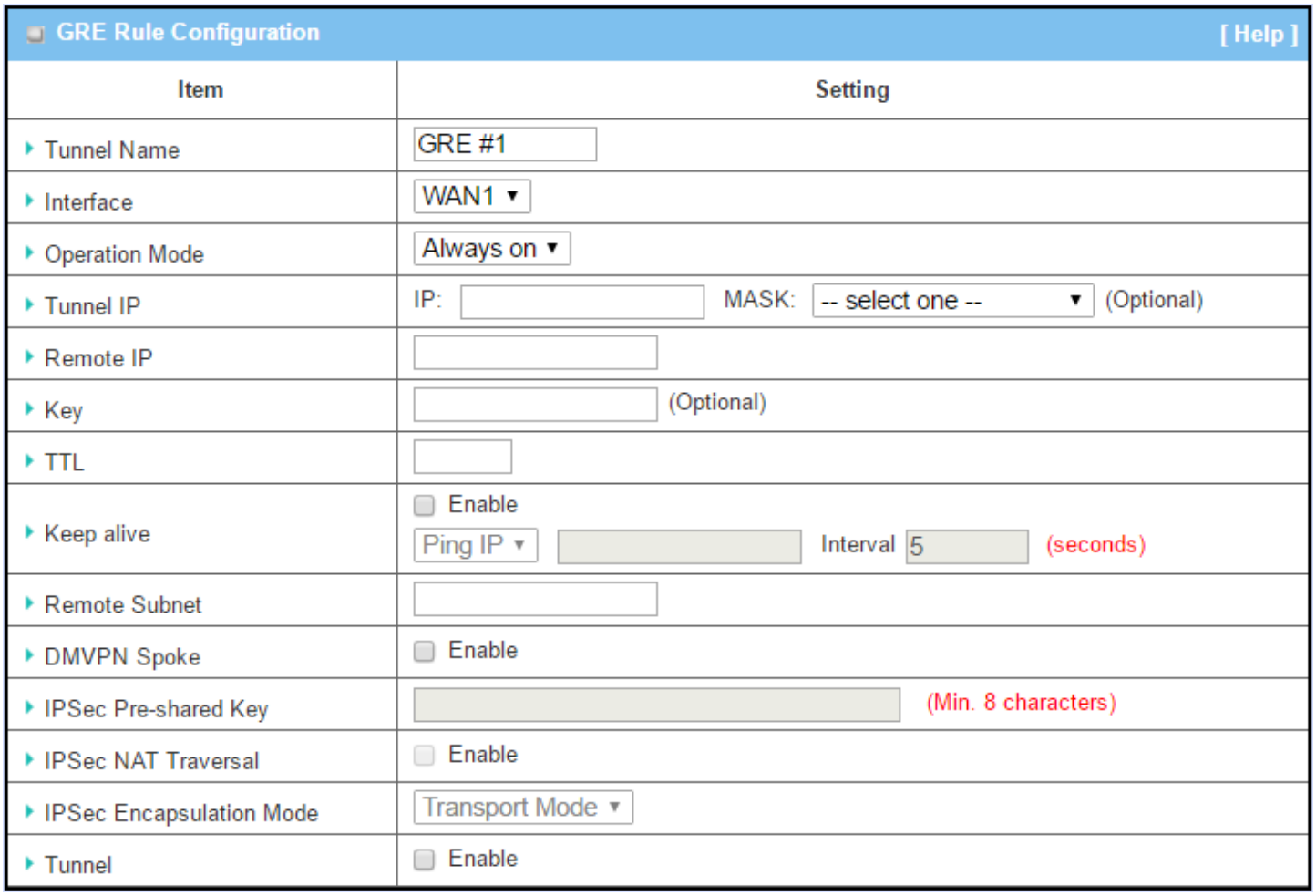


Enable GRE Window (啟動 GRE 視窗)		
項目	設定值	說明
GRE Tunnel (GRE 通道)	預設未勾選	勾選 **Enable (啓動)** 方框以啓動 GRE 功能。
Max. Concurrent GRE Tunnels (最大並行 GRE 通道)	依據產品型號	指定最大同時連線 GRE 通道的數值限制根據設備型號而不同。
Save (保存)	無	點擊 **Save (保存)** 按鈕以保存設定。
Undo (還原)	無	點擊 **Undo (還原)** 按鈕以取消設定。

建立/編輯 GRE 通道



當按下 Add/Edit (新增/編輯) 按鈕將出現 GRE Rule Configuration (GRE 規則設定) 畫面

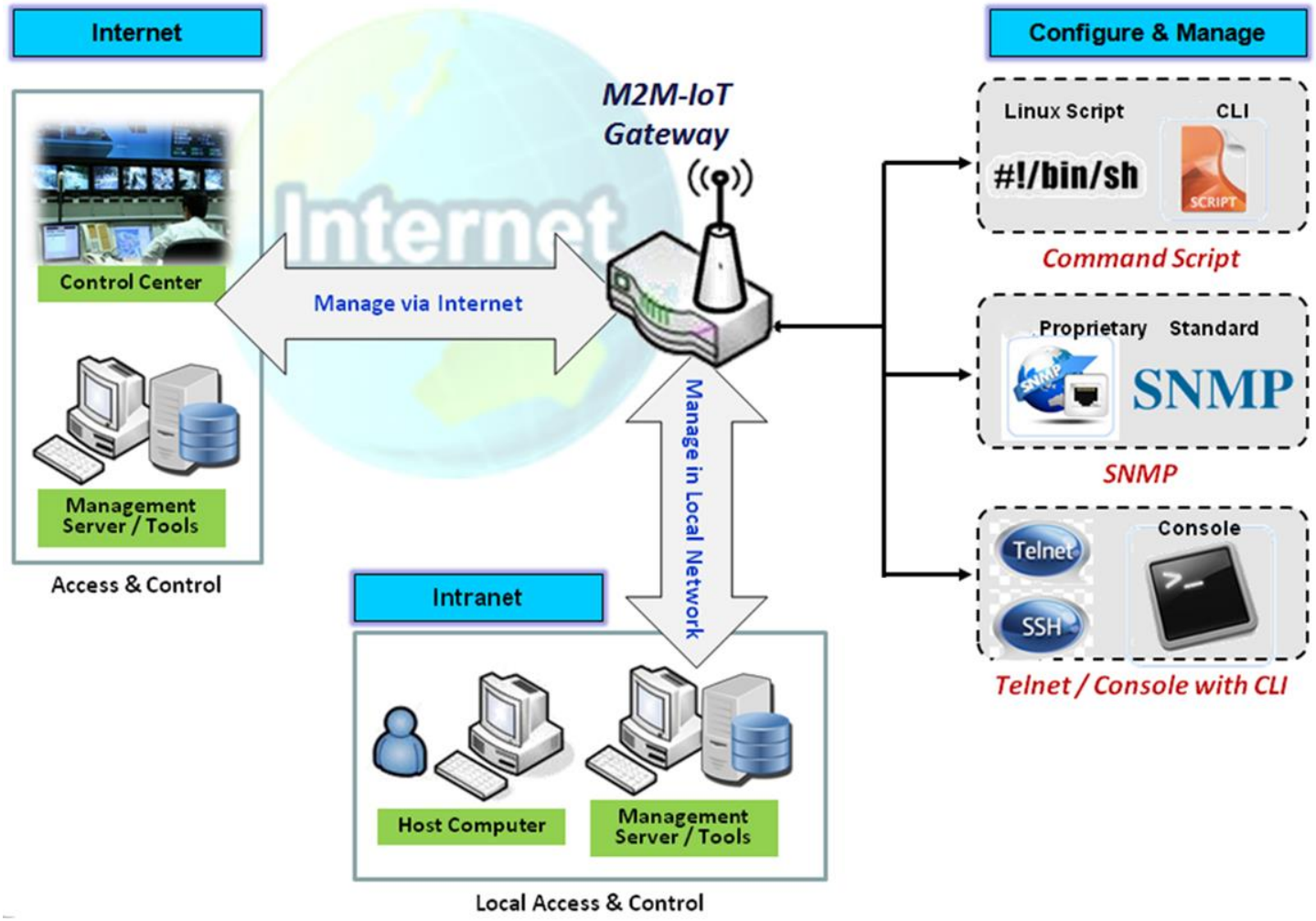


GRE Rule Configuration Window (GRE 規則設定視窗)		
項目	設定值	說明
Tunnel Name (隧道名稱)	必要設定	輸入通道名稱. ***範圍值***: 1 ~ 9 個字元.
Interface (介面)	1. 必要設定 2. **WAN 1** 預設選擇	選擇要建立 GRE 通道的介面，可能是任何可用的 WAN 和 LAN 介面。
Operation Mode (操作模式)	1. 必要設定 2. 預設選擇 **Always on**	定義 GRE 通道的操作模式。可能是 **Always On(永遠啓動)**或 **Failover(容錯移轉)**。. 如果此通道設定為容錯移轉通道，您需要進一步選擇要轉移的主通道. 注意:單 WAN 的閘道器不能選**容錯移轉**。.
Tunnel IP (隧道 IP)	可選設定	輸入通道 IP 位址和相應的子網路遮罩.
Remote IP (遠端 IP)	必要設定	輸入遠端 GRE 通道閘道的遠端 IP 位址。通常這是遠端 GRE 閘道的公共 IP 位址。

Key(密鑰)	可選設定	輸入 GRE 連線的密鑰。 ***範圍值***: 0 ~ 9999999999.
TTL	1. 必要設定 2. 1 to 255 range	指定此 GRE 通道的 **TTL** 躍點(hop-count)數值。 ***範圍值***:1 ~ 255.
Keep alive (保存生存)	1. 預設未勾選 2. 5s is set 預設	勾選 **Enable(啟用)**方框啟用 "保持生存" 功能. 選擇 Ping IP 以保持活動狀態, 並將 IP 位址輸入 Ping。 輸入 Ping 時間間隔 (以秒為單位)。 ***範圍值***: 5 ~ 999 秒.
Remote Subnet (遠端子網)	必要設定	指定此 GRE 通道遠端子網. 遠端子網格式必須是 IP 位址/網路遮罩 (例如 10.0. 0.2/24)。 用於 GRE 伺服器節點。 GRE 客戶端節點目標位於專用子網中的資料封包將通過 GRE 通道傳輸。其他將根據 GRE 客戶端節點的安全閘道的目前路由策略進行傳輸。 如果在遠端子網欄位中輸入 0.0. 0.0/0, 則將被視為 GRE 客戶端的預設閘道設定，並且所有數據封包(包括 GRE 客戶端節點設備的網際網路登入)都將通過建立的 GRE 通道。 這表示遠端 GRE 伺服器節點控制來自 GRE 客戶端節點的任何數據封包的流動。
DMVPN Spoke (DMVPN 分支)	預設未勾選	指定閘道是否支援 DMVPN GRE 通道的分支。勾選 **Enable(啟用)**方框以啟用 DMVPN 分支。
IPsec Pre-shared Key (IPsec 預共用金鑰)	必要設定	輸入 DMVPN 分支身份驗證預共用密鑰 (8 ~ 32 個字元). 注意: 預共用密鑰僅可用於啟用 DMVPN 分支時.
IPsec NAT Traversal	預設未勾選	勾選 **Enable(啟用)**框可啟用 NAT Traversal。 注意:IPsec 如果未啟用 DMVPN, 則 NAT Traversal 將不可用.
IPsec Encapsulation Mode (IPsec 封裝模式)	預設未勾選	從下拉框中指定 IPsec 封裝模式。支援 **Transport mode (傳輸模式)**和 **Tunnel mode**(隧道模式)。 注意：當 DMVPN 未啟用時，IPsec 封裝模式將不可用。
Tunnel (通道)	預設未勾選	勾選支持方框以啓動 GRE 通道。
Save (保存)	無	點擊 **Save (保存)** 按鈕以保存設定值。
Undo (還原)	無	點擊 **Undo (還原)** 按鈕以取消設定值。
Back (返回)	無	點擊 **Back (返回)**按鈕以返回前一頁。

第 6 章 管理

6.1 配置&管理



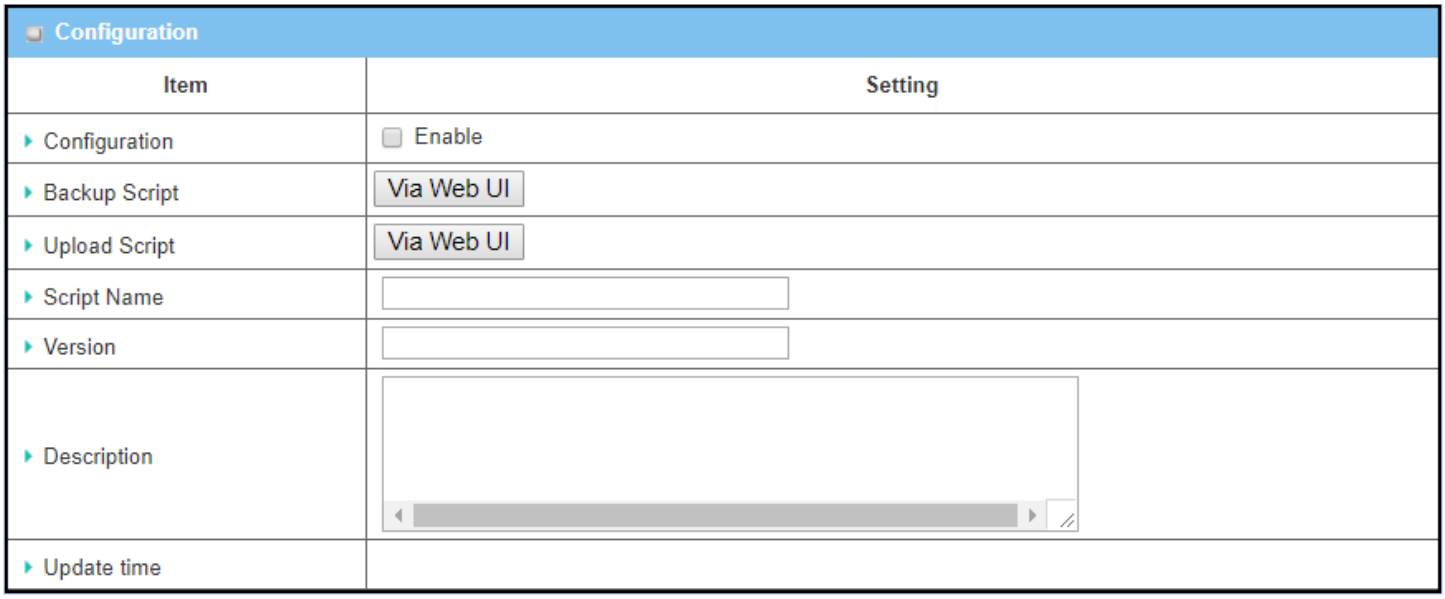
配置 & 管理是指企業範圍內分散式系統的管理, 包括 (通常在運作中) 電腦系統。集中式管理需要與公司規模、IT 員工的專業知識和所使用的技術總量相關的時間和精力。此設備支援許多系統管理協定, 如 Command Script 指令、 SNMP 和透過Telnet 下CLI指令 的. 您可以在 “配置和管理” 這部分的Web UI中做這些設定。

6.1.1 Command Script 指令腳本

Command Script 指令設定是允許管理員以純文字設定預設定義並在啟動時套用設定的應用。

轉到 Administration > Command Script > Configuration 頁面。

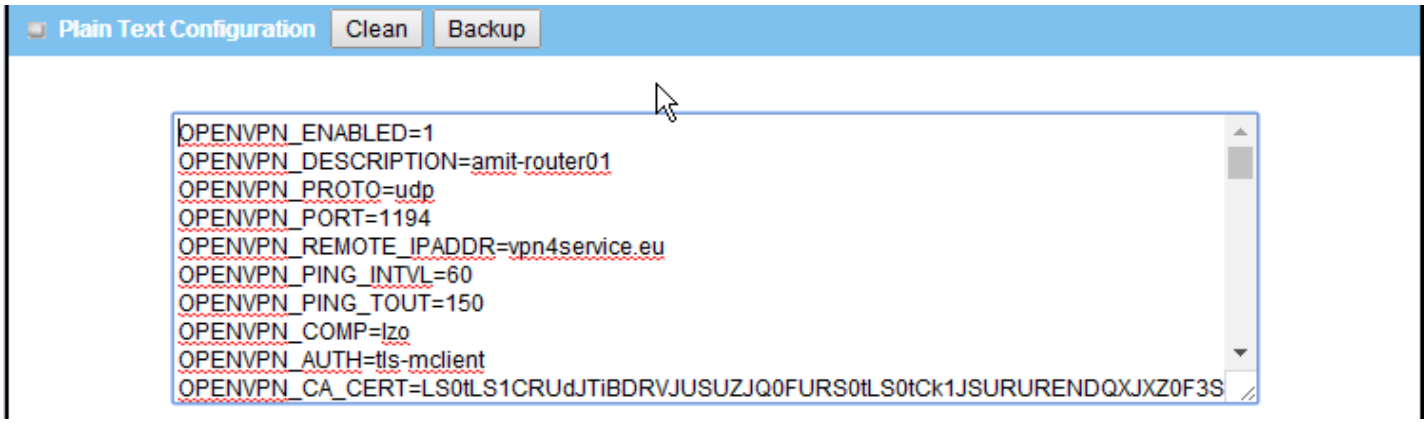
啓動 Command Script 設定



Configuration (設定) 項目	設定值	說明
Configuration (設定)	預設未勾選	勾選 **Enalbe(啟用)**方框啟動命令腳本功能.
Backup Script (備份腳本)	無	點擊 Via Web UI 或 Via Storage 按鈕以備份 .txt 檔中的現有命令腳本。可以在下面的**腳本名稱**中指定指令檔名。
Upload Script (上傳腳本)	無	點擊 Via Web UI 或 Via Storage 按鈕按鈕從指定的 .txt 檔上傳現有的命令腳本。
Script Name (腳本名稱)	1. 可選設定 2. 任何有效的檔案名	指定腳本備份指令檔名, 或顯示選擇的上傳指令檔名稱。 ***範圍值***: 0 ~32 個字元.
Version (版本)	1. 可選設定 2. 任何字串	指定應用的命令腳本的版本號。 ***範圍值***: 0 ~32 個字元.
Description(說明)	1. 可選設定 2. 任何字串	為應用的命令腳本輸入簡短說明。

Update time (更新時間)	無	記錄上次命令腳本的上傳時間。

編輯/備份 純文字指令腳本



您可以在設定畫面中編輯純文字配置設定，如上所示。

Plain Text Configuration (純文字設定)		
項目	**設定值**	**說明**
Clean (清除)	*無*	清除文字區域。(點擊 **Save 保存**按鈕可進一步清除系統中已保存的設定)。
Backup (備份)	*無*	備份和下載設定。
Save (保存)	*無*	保存設定

支援的純文字設定項目顯示在以下列表中。你可以將標準 Linux 命令執行的設定置於 script 文件中，並使用 **STARTUP** 命令套用於系統設定。對於沒有相對應 Linux 命令集的設定，可以使用專有 Proprietary Command Set 命令集對其進行設定。

Configuration Content (設定內容)		
Key	**設定值**	**說明**
OPENVPN_ENABLED	1: 啓動 0: 禁用 e	啟動或禁用 OpenVPN 客戶端功能。
OPENVPN_說明	必要設定	指定 OpenVPN 客戶端連線的通道名稱。
OPENVPN_PROTO	UDP TCP	為 OpenVPN 客戶端定義**協定**。 • **TCP 或 TCP/UDP** -> OpenVPN 將使用 TCP 協定設定為

		443 **埠**. • **UDP** -> OpenVPN 將使用 UDP 協定設定為 1194 **埠**
OPENVPN_PORT	必要設定	指定要使用的 OpenVPN 客戶端的**埠**。
OPENVPN_REMOTE_IPADDR	IP 或 FQDN	指定此 OpenVPN 客戶端通道的節點 OpenVPN 伺服器的**遠端 IP/FQDN** 。輸入 IP 位址或 FQDN。
OPENVPN_PING_INTVL	秒	指定 OpenVPN 保持生存狀態檢查的時間間隔。
OPENVPN_PING_TOUT	秒	指定 OpenVPN 客戶端保持生存狀態檢查的超時值。
OPENVPN_COMP	自適應	指定 OpenVPN 客戶端的 **LZO Compression 壓縮**演算法
OPENVPN_AUTH	靜態金鑰/TLS	為 OpenVPN 通道指定授權模式. • **TLS** -> OpenVPN 將使用 TLS 授權模式，需要指定 **CA Cert.**, **Client Cert.** 和 **Client Key**
OPENVPN_CA_CERT	必要設定	指定 OpenVPN 客戶端受信任的 CA 憑證。透過 Base64 轉換。
OPENVPN_LOCAL_CERT	必要設定	指定 OpenVPN 客戶端本地憑證。透過 Base64 轉換。
OPENVPN_LOCAL_KEY	必要設定	指定 OpenVPN 客戶端的本地密鑰。透過 Base64 轉換。
OPENVPN_EXTRA_OPTS	選項	指定 OpenVPN 客戶端的額外選項
IP_ADDR1	IP	區域網 LAN IP
IP_NETM1	網路遮罩	區域網 LAN 遮罩
PPP_MONITORING	1: 啓動 0: 禁用	啟用網路監視功能後, 路由器將使用 DNS 查詢或 ICMP 定期檢查網路連線。
PPP_PING	0: DNS Query (DNS 查詢) 1: ICMP Query (ICMP 查詢)	通過 **DNS 查詢**，系統將 DNS 查詢資料封包發送到 PPP_PING_IPADDR 中指定的目標來檢查連線。 使用 **ICMP 查詢**，系統將向 PPP_PING_IPADDR 中指定的目標發送 ICMP 請求資料封包來檢查連線。
PPP_PING_IPADDR	IP	指定 IP 位址作為發送 DNS 查詢/ICMP 請求的目標。
PPP_PING_INTVL	秒	指定時間間隔檢查兩個 DNS 查詢或 ICMP 檢查資料封包之間。
STARTUP	指令檔	使用標準 Linux 命令的設定, 將它們放在指令檔中, 並將指令檔應用於 STARTUP 啟動命令。 例如, STARTUP=#!/bin/sh STARTUP=echo “startup done” > /tmp/demo

使用 Telnet 進行純文字系統設定

除了上面提到的網頁風格的純文字設定外，閘道器系統還允許使用 Telnet CLI 進行設定。管理員可以使用專有的 Telnet 命令“txtConfig”和相關操作項目來執行簡單的系統設定。

命令格式為：txtConfig(action)[option]

行動	選項	說明
Clone (複製)	*輸出檔案*	複製資料庫中的設定內容, 並將其存儲為設定檔。 (例: *txtConfig clone /tmp/config*) 設定檔中的內容與上面提到的純文字命令相同。此操作與執行 "備份" 純文字配設定完全相同。
Commit (提交)	*現有的檔案*	將設定內容提交到資料庫。 (例: *txtConfig commit /tmp/config*)
Enable (啓動)	*無*	啟用純文字系統組態。 (例: *txtConfig enable*)
Disable (禁用)	*無*	禁用純文字系統組態。 (例: *txtConfig disable*)
run_immediately	*無*	套用在資料庫中提交的設定內容。 (例: *txtConfig run_immediately*)
run_immediately	*現有的檔案*	分配要應用的設定檔。 (例: *txtConfig run_immediately /tmp/config*)

6.1.2 SNMP

Simple Network Management Protocol 簡單網路管理協定 SNMP，是一種旨在透過polling和設定終端值以及監控網路事件的協定，為使用者提供遠端管理電腦網路的能力。

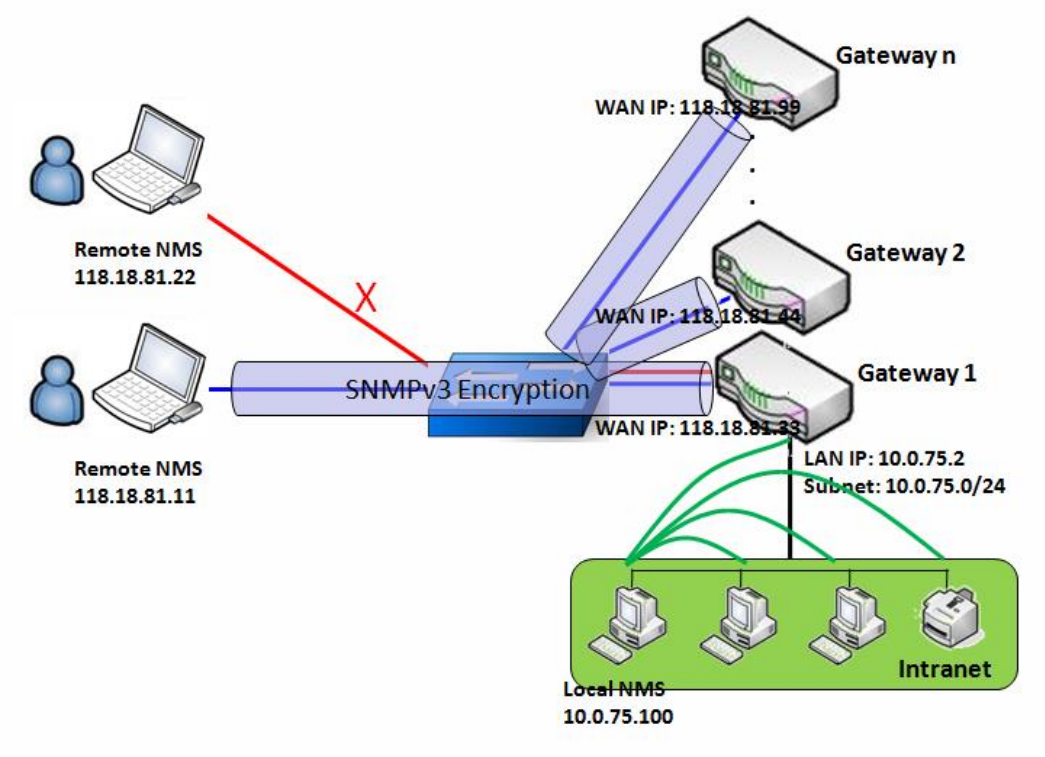
典型的 SNMP 使用, 一個或多個管理電腦 (稱為Manager) 負責監視或管理電腦網路上的一羣組主機或設備。每個託管系統在任何時候都執行一個稱為代理的軟體元件(Agent)透過 SNMP 向管理器報告資訊。

SNMP 代理將管理資料作為變數提供SNMP Manger。該協定還允許主動管理工作，例如透過遠端修改這些變數來修改和應用新的設定。通過 SNMP 登入的變數是在層次結構中組織的。這些層次結構和其他中繼資料 (如變數的類型和描述) 由Management Information Bases 管理資訊庫 (MIBs) 描述。

該設備支援多個公用 MIBs 和一個 SNMP 代理的專用 MIB。支援的 MIBs 如下: MIB-II (RFC 1213, 包含 IPv6)、IF-MIB、IP-MIB、TCP-MIB、UDP-MIB、SMIv1 和 SMIv2、SNMPv2-TM 和 SNMPv2-

MIB、 和 AMIB (ETHERWAN 專用 MIB)

SNMP 管理方案



方案應用程式計時

、SNMP 網路管理系統 (NMS) 有兩種應用程式方案。本地 NMS 位於網際網路中，並管理所有支援 SNMP 的設備。另一種方法是使用遠端 NMS 來管理其 WAN 介面由交換器或帶有 UDP 轉發的路由器連線在一起的設備。

方案說明

NMS 伺服器可以使用 SNMP 協定監視和配置受控設備，這些設備位於可以從 NMS 獲得 UDP 資料封包的位置。

受控設備將緊急陷阱(trap)事件報告給 NMS 伺服器。

使用 SNMPv3 版本的協定可以保護 SNMP 命令和回覆的傳輸。

具有最高權限 IP 位址的遠端 NMS 可以管理設備, 但另一個遠端 NMS 則不行。

參數設定示意圖

下表列出了參數設定，作為上圖中的閘道器 1 的一個示意圖，並在 LAN 和 WAN 介面上啟用 "SNMP"。表中未提及的參數使用預設值。

Configuration Path	[SNMP]-[Configuration]
SNMP Enable	■ *LAN* ■ *WAN*
Supported Versions	■ *v1* ■ *v2c* ■ *v3*
Get / Set Community	*ReadCommunity / WriteCommunity*
Trap Event Receiver 1	*118.18.81.11*
WAN Access IP Address	*118.18.81.11*

Configuration Path	[SNMP]-[User Privacy Definition]		
ID	1	2	3
User Name	*UserName1*	*UserName2*	*UserName3*
Password	*Password1*	*Password2*	*Disable*
Authentication	*MD5*	*SHA-1*	*Disable*
Encryption	*DES*	*Disable*	*Disable*
Privacy Mode	*authPriv*	*authNoPriv*	*noAuthNoPriv*
Privacy Key	*12345678*	*Disable*	*Disable*
Authority	*Read/Write*	*Read*	*Read*
Enable	■ *Enable*	■ *Enable*	■ *Enable*

方案操作程序

在上圖中，NMS 伺服器可以管理內網中的多個設備或 UDP-reachable (UDP 可達)網路。 “Gateway 1” 是託管設備之一，LAN 介面的 IP 位址為 10.0.75.2，WAN-1 介面的 IP 位址為 118.18.81.33。作爲 NAT 路由器。

在第一階段，NMS 管理人員為所有託管設備準備相關資訊並將其記錄在 NMS 系統中。然後 NMS 系統透過使用 SNMP get 命令獲取所有託管設備的狀態。

當管理員想要設定託管理設備時，NMS 系統允許使用 SNMP 設定命令。如果管理員使用 SNMPv3 協定設定 “Gateway 1” ，則使用 “UserName1” 帳戶。由於帳戶的權限為 “Read/Write(讀/寫)” ，因

此只有“UserName1”帳戶可以讓“Gateway 1”接受來自 NMS 的設定。

一旦託管設備發送緊急事件，設備將向 Trap 陷阱事件接收器發出 Trap 陷阱。NMS 本身可能是其中之一。

如果要保護在 NMS 和託管設備之間傳輸的 SNMP 命令和響應，請使用 SNMPv3。

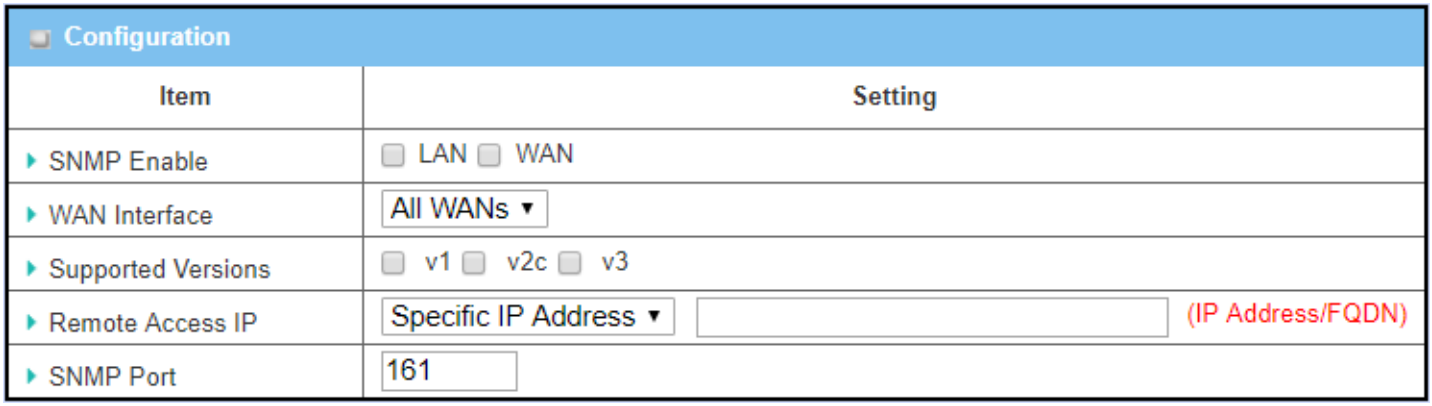
無最高權限 IP 位址的遠端網管無法管理“Gateway 1”，因為“Gateway 1”只允許具有最高權限 IP 位址的網管透過其 WAN 介面進行管理。

設定 SNMP

轉到 Administration > Configure & Manage > SNMP 頁面。

SNMP 頁面卡允許使用者設定 SNMP 相關設定, 包括介面、版本、存取控制和 trap 陷阱接收器。

啓動 SNMP



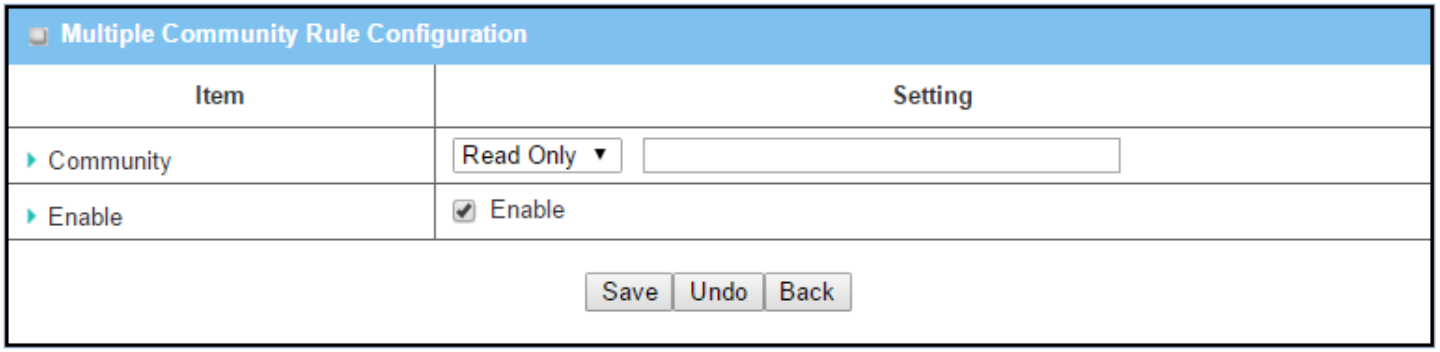
SNMP 項目	設定值	說明
SNMP Enable (SNMP 啟動)	1. 預設未勾選	選擇 SNMP 的介面並啟用 SNMP 功能。 勾選 **LAN** 方框時, 將啟動 SNMP 功能和您可以由 LAN 登入 SNMP。 勾選 **WAN** 方框時, 將啟動 SNMP 功能和您可以由 WAN 登入 SNMP。.
WAN Interface (WAN 介面)	1. 必要設定 2. 預設選擇 ALL WANs	指定遠端 SNMP 主機可用於登入設備的 WAN 介面。 預設勾選,**All WANs**, 並且 WAN 介面沒有限制。
Supported Versions (支援的版本)	1. 必要設定 2. 預設未勾選	選擇 SNMP 的版本 **v1** 方框被勾選時， 您可以登入 SNMP 版本 1. **v2** 方框被勾選時， 您可以登入 SNMP 版本 2. **v3** 方框被勾選時， 您可以登入 SNMP 版本 3.
Remote Access IP (遠端存取 IP)	1. 字串格式.: 任何 IPv4 位址 2. 可選項目	指定 WAN 的**遠端存取 IP** 。 選擇 **Specific IP Address (特定的 IP 位址)**和輸入 IP 位址。僅此 IP 位址可以由 LAN/WAN 登入 SNMP 選擇 **IP Range (IP 範圍)**，填入的一個範圍的 IP 位址，此範圍內的 IP 位址可以由 LAN/WAN 登入 SNMP 如果留空，表示任何 IP 位址都可以由 LAN/WAN 登入 SNMP.
SNMP Port	1. 字串格式.: 任何埠	指定 **SNMP 埠**.

(SNMP 埠)	號碼 2. 預設 SNMP 埠 161. 3. 必要設定	輸入任何埠編號。但您必須確定不會使用這個埠編號。 *範圍值*:1 ~ 65535.
Save (保存)	無	點擊 Save (保存) 按鈕以保存設定值
Undo (還原)	無	點擊 Undo (還原) 按鈕以取消設定

建立/編輯多個羣體

SNMP 允許您為版本 1 和版本 2 的使用者定制您的登入控制。 該路由器最多支援 10 個羣體集。

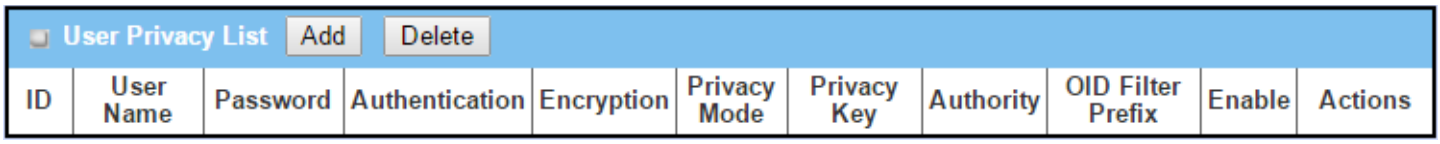
當按下 Add (增加)按鈕，將出現 Multiple Community Rule Configuration (多羣體規則設定)畫面



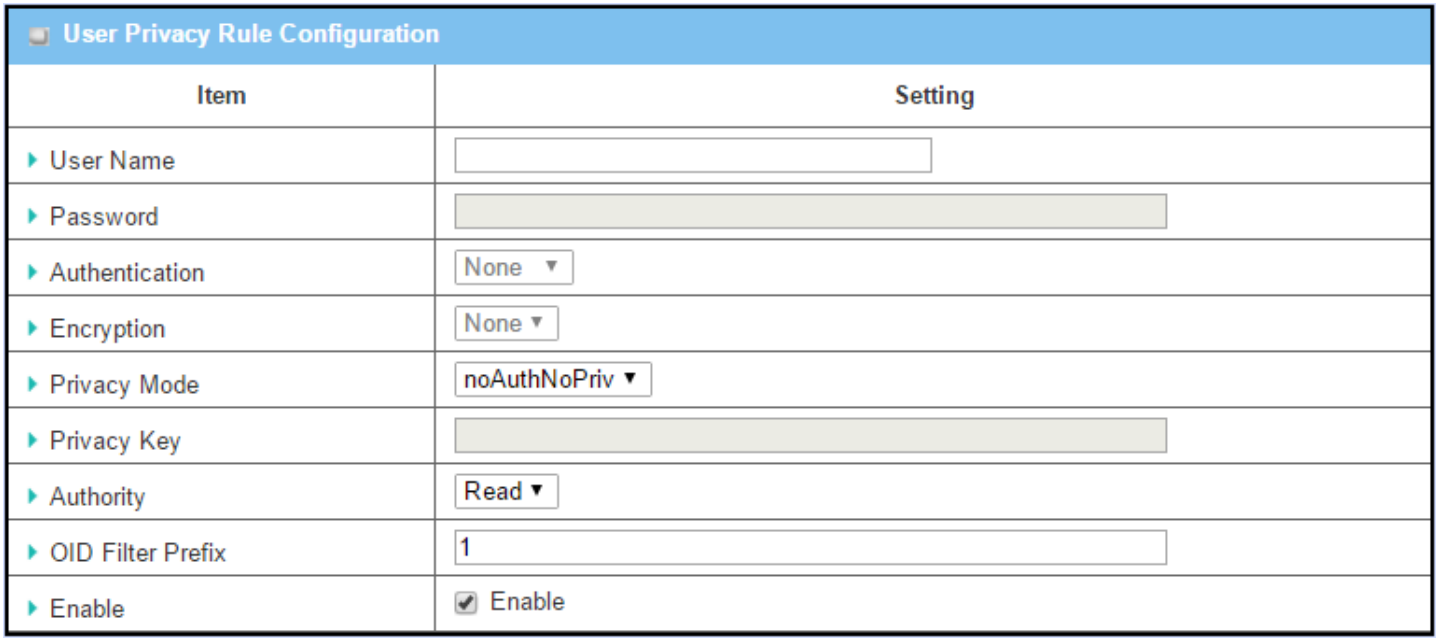
Multiple Community Rule Configuration (多羣體規則設定) 項目	設定值	說明
Community (羣體)	1. 預設選擇 Read Only 2. 必要設定 3. 字串格式: 任意文字	指定此版本 1 或版本 v2c 使用者的羣體，將被允許唯讀(GET 和 GETNEXT) 或讀寫(GET、GETNEXT 和 SET) 分別登入. 羣體的最大長度是 32。
Enable (啓動)	1. 預設勾選	點擊 Enable 啟用此版本 1 或版本 v2c 使用者.
Save (保存)	無	點擊 **Save(保存)**按鈕以保存設定。但不適用於 SNMP 功能。返回 SNMP 主頁時將顯示 " Click on save button to apply your changes(點擊保存按鈕以套用您的更改)" 以提醒使用者點擊保存按鈕。
Undo (還原)	無	點擊 **Undo (還原)** 按鈕取消設定.
Back (返回)	無	點擊 **Back (返回)**按鈕返回最後一頁

建立/編輯使用者隱私

SNMP 允許您為第 3 版使用者定制您的登入控制。該路由器最多支持 128 個使用者隱私設定。



當按下 Add (增加)按鈕，將出現 User Privacy Rule Configuration (使用者隱私規則設定)畫面

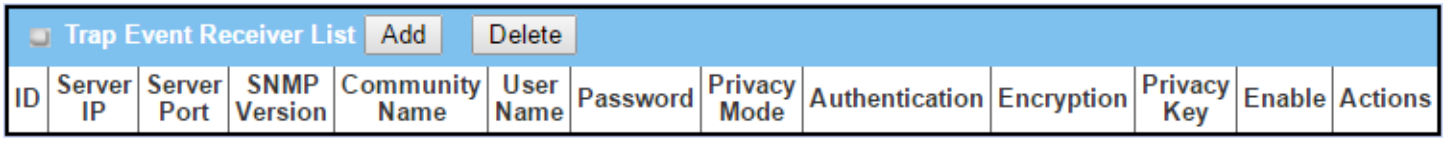


User Privacy Rule Configuration (使用者隱私規則設定)		
項目	設定值	說明
User Name (使用者名稱)	1. 必要設定 2. 字串格式: 任意文字	指定版本 3 使用者的**使用者名稱**。 ***範圍值***: 1 ~ 32 個字元.
Password (密碼)	1. 字串格式: 任意文字	當**隱私模式**為 **authNoPriv** 或 **authPriv** 時, 請為版本 3 使用者指定**密碼**。 ***範圍值***: 8 ~ 64 個字元.
Authentication (認證)	1. 預設選擇 **None**	當**隱私模式**為 **authNoPriv** 或 **authPriv** 時, 請為版本 3 使用者指定**身份驗證**類型。 選擇使用 **MD5/SHA-1** 的身份驗證類型 。
Encryption (加密)	1. 預設選擇 **None**	當**隱私模式**為 **authPriv** 時, 請為版本 3 使用者指定**加密**協定。 選擇 **DES/AES** 爲加密協定 。
Privacy Mode (隱私模式)	1. 預設選擇 **noAuthNoPriv**	指定版本 3 使用者的**隱私模式**。 **noAuthNoPriv**.

		不使用身份驗證類型或加密協定。 **authNoPriv**. 指定**身份驗證**和**密碼**. **authPriv**. 指定身份驗證、密碼、加密和隱私密鑰。
Privacy Key (隱私金鑰)	1. 字串格式: 任意文字	當您的**隱私模式**為 **authPriv** 時, 請指定版本 3 使用者的**隱私密鑰**(8 ~ 64 個字元) 。
Authority (權力)	1. 預設選擇 **Read**	指定版本 3 使用者的**頒發機構**，允許**唯讀**(GET 和 GETNEXT) 或**讀寫**(GET、GETNEXT 和 SET) 分別登入.
OID Filter Prefix (OID 篩選前綴)	1. 預設 1 2. 必要設定 3. 字串格式.: 任何合法 OID	**OID 篩選前綴**將版本 3 使用者的登入限制為給定 OID 的子樹根(sub-tree rooted)。 ***範圍值***: 1 ~ 2080768.
Enable (啓動)	1.預設勾選此方框	點擊 **Enable(啟用)**啟用版本 3 使用者。
Save (保存)	無	點擊 **Save(保存)**按鈕以保存設定。不適用於 SNMP 功能。返回 SNMP 主頁時將顯示 " Click on save button to apply your changes (點擊保存按鈕以套用您的更改)" 以提醒使用者點擊主頁**保存**按鈕。
Undo (還原)	無	點擊 **Undo (還原)** 按鈕取消設定.
Back (返回)	無	點擊 **Back (返回)**按鈕返回最後一頁

建立/編輯 Trap 陷阱事件接收器

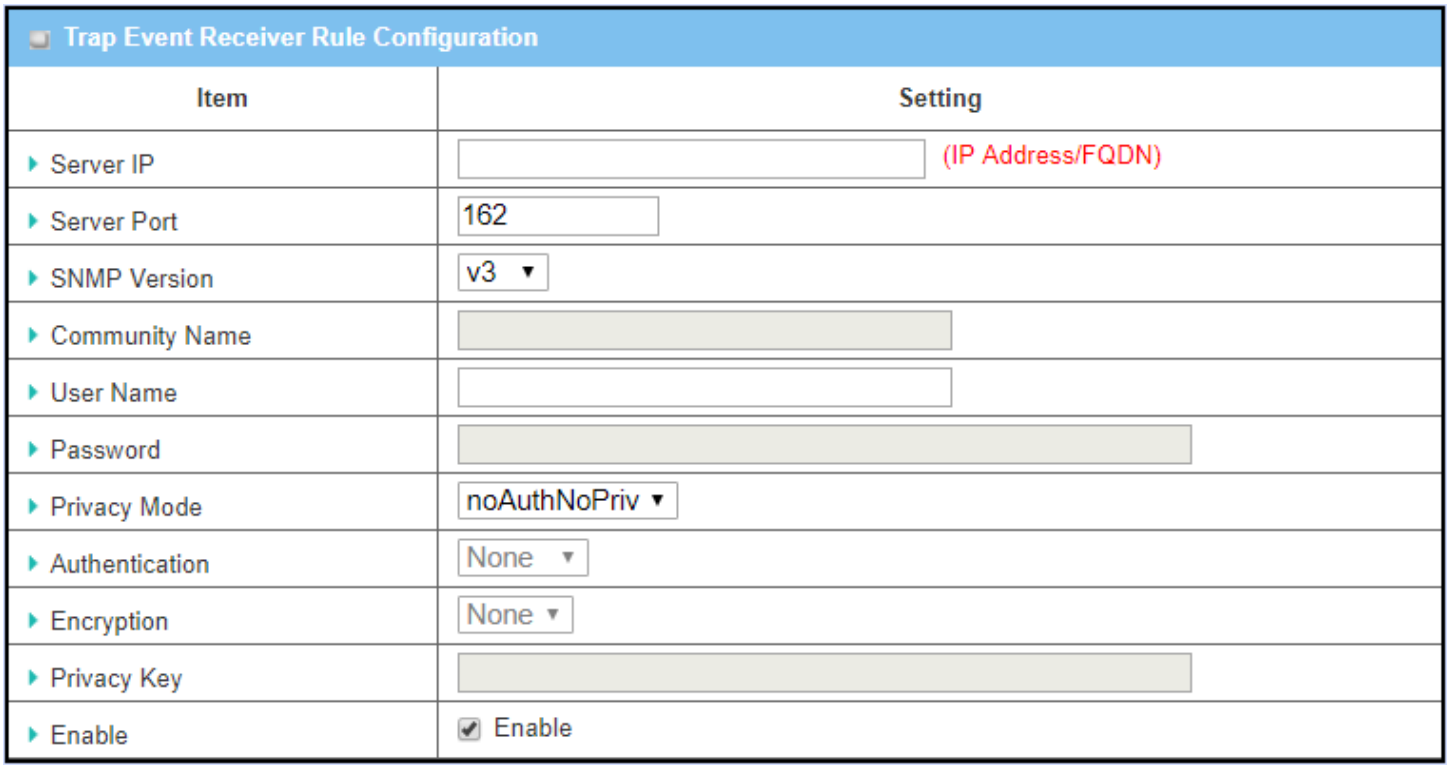
SNMP 允許您客製化您的 Trap 陷阱事件接收器。 該路由器最多支援 4 個 Trap 陷阱事件接收器集。



當按下 Add (增加)按鈕，將出現 **Trap Event Receiver Rule Configuration** (陷阱事件接收器規則設定)畫面，預設的 SNMP 版本是 v1。設定畫面將提供版本 1 所需的項目。

當選擇 v2c 時，除了版本不同外，設定畫面與 v1 完全相同。

當選擇 v3 時，設定畫面將為版本 3 Trap 陷阱提供更多設定項目。



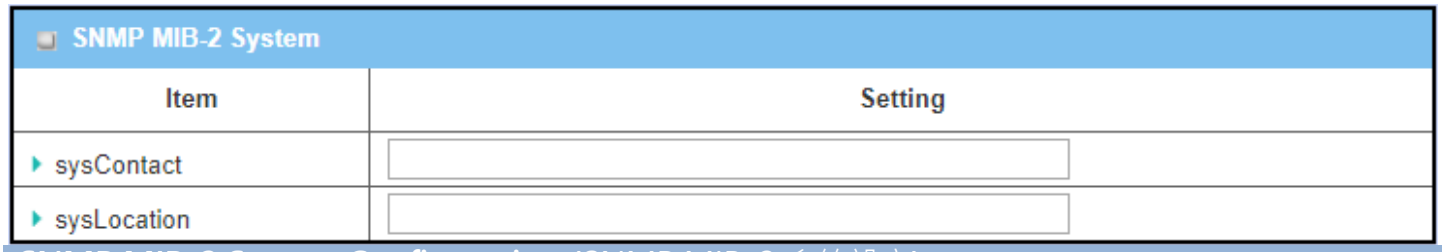
Trap Event Receiver Rule Configuration (陷阱事件接收器規則設定)		
項目	設定值	說明
Server IP (伺服器 IP)	1. 必要設定 2. 字串格式: 任意 IPv4 位址或 FQDN	指定 Trap 陷阱**伺服器 IP** 或 **FQDN**。 Trap 陷阱將被發送到伺服器 IP/FQDN。
Server Port (伺服器埠)	1. 字串格式: 任意埠編號 2. 預設 SNMP trap 埠 162	指定 Trap 陷阱 **伺服器埠** 輸入任何埠編號。但您必須確認不會使用此埠編號。 *範圍值*:1 ~ 65535.

	3. 必要設定	
SNMP Version (SNMP 版本)	1. **v1** 預設選擇	選擇 Trap 陷阱版本 **v1** 設定畫面將提供版本 1 所需的專案。 **v2c** 設定畫面將提供版本 2c 所需的專案。 **v3** 設定畫面將提供版本 3 所需的專案。
Community Name (群體名稱)	1. **v1** and **v2c** 必要設定 2. 字串格式: 任意文字	為版本 1 或版本 v2c Trap 陷阱指定**群體名稱**。 ***範圍值***: 1 ~ 32 個字元
User Name (使用者名)	1. **v3** 必要設定 2. 字串格式: 任意文字	為版本 3 Trap 陷阱指定**使用者名稱**。 ***範圍值***: 1 ~ 32 個字元
Password (密碼)	1. **v3** 必要設定 2. 字串格式: 任意文字	當**隱私模式**為 **authNoPriv** 或 **authPriv** 時, 必須為版本 3 Trap 陷阱指定**密碼**。 ***範圍值***: 8 ~ 64 個字元
Privacy Mode (隱私模式)	1. **v3** 必要設定 2. **noAuthNoPriv** 預設選擇	指定版本 3 Trap 陷阱的**隱私模式**。 選擇 **noAuthNoPriv** . 不使用任何身份驗證類型和加密協定。 選擇 **authNoPriv**. 必須指定 **身份驗證**和**密碼**. 選擇 **authPriv**. 必須指定身份驗證、密碼、加密和隱私密鑰。
Authentication (認證)	1. **v3** 必要設定 2. **None** 預設選擇	當**隱私模式**為 **authNoPriv** 或 **authPriv** 時, 必須為版本 3 Trap 陷阱指定 **身份驗證**類型。 選擇 **MD5/SHA-1** 爲使用的身份驗證類型 。
Encryption (加密)	1. **v3** 必要設定 2. **None** 預設選擇	當**隱私模式**為 **authPriv** 時, 必須為版本 3 陷阱指定 **加密**協定。 已選擇要使用的加密協定 **DES/AES** 。
Privacy Key (隱私金鑰)	1. **v3** 必要設定 2. 字串格式: 任意文字	當您的**隱私模式**為 **authPriv** 時, 必須指定**隱私密鑰** (8 ~ 64 個字元) 用於版本 3 Trap 陷阱。
Enable (啓用)	預設勾選方框	點擊 **Enable(啟用)**啟用此陷阱接收器.
Save (保存)	無	**點擊 Save(保存)按鈕以保存設定。不適用於 SNMP 功能。返回 SNMP 主頁時將顯示 " Click on save button to apply your changes (點擊保存按鈕以套用您的更改)" 以提醒使用者點擊主頁保存按鈕。**

Undo (還原)	無	點擊 **Undo (還原)** 按鈕取消設定。
Back (返回)	無	點擊 **Back (返回)**按鈕返回最後一頁。

指定 SNMP MIB-2 系統

如果需要，您還可以指定 MIB-2 系統所需的資訊。

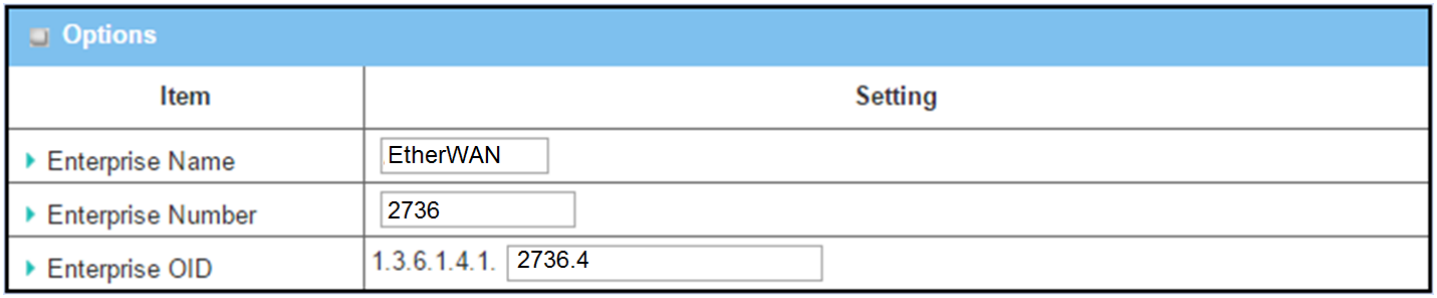


SNMP MIB-2 System Configuration (SNMP MIB-2 系統設定)

項目	設定值	說明
sysContact	1. 可選設定 2. 字串格式: 任意文字	指定 MIB-2 系統連絡人資訊。 ***範圍值***: 0 ~ 64 字元.
sysLocation	1. 可選設定 2. 字串格式: 任意文字	指定 MIB-2 系統位置資訊。 ***範圍值***: 0 ~ 64 字元.

編輯 SNMP 選項

如果您使用某個特定的專用 MIB，則必須輸入企業名稱、編號和 OID。



Options (選項)

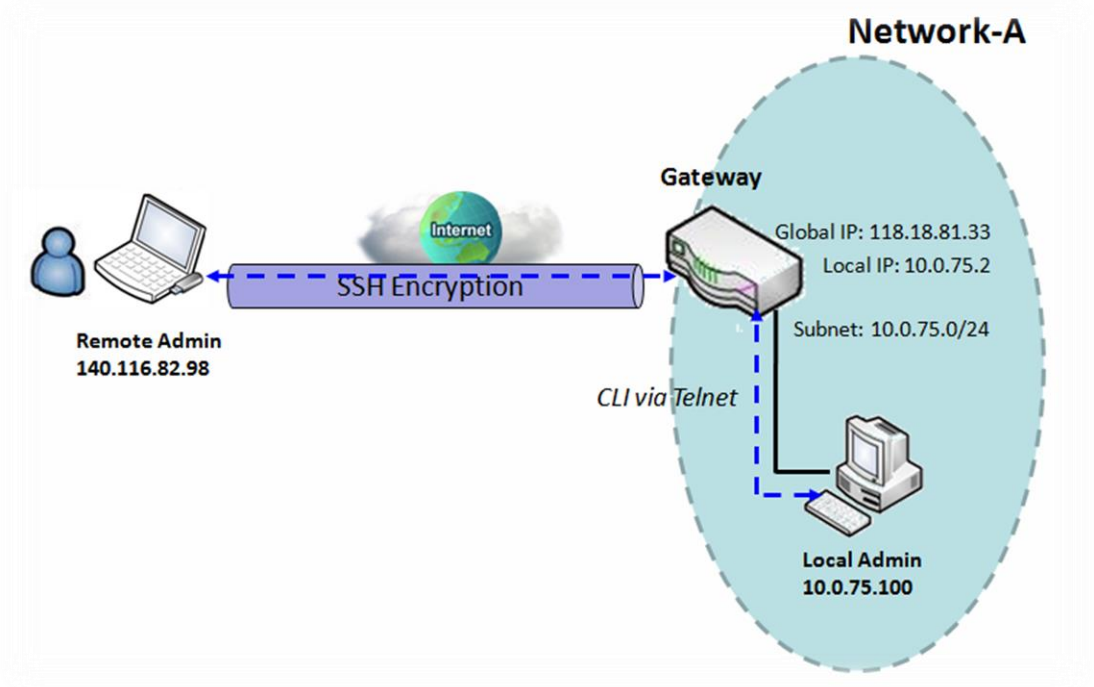
項目	設定值	說明
Enterprise Name (企業名稱)	1. 預設值為 Etherwan 2. 必要設定 3. 字串格式: 任意文字	為特定的 MIB 指定**企業名稱**。 ***範圍值***: 1 ~ 10 個字元, 且只有 A~Z、a~z、0~9、' – '、 '_' 的字串.

Enterprise Number (企業編號)	預設值爲 2736 2. 必要設定 3. 字串格式.: any number	為特定的 MIB 指定**企業編號**。 ***範圍值***: 1 ~ 2080768.
Enterprise OID (企業 OID)	1. 預設值爲 1.3.6.1.4.1.2736.4 2. 必要設定 3. 字串格式.: 任意合法 OID	為特定的 MIB 指定**企業 OID**。 每個 OID 的範圍是 1-2080768。 企業 OID 的最大長度為 31. 第七個數字必須與企業編號相同。
Save (保存)	無	點擊 **Save(保存)**按鈕以保存設定並將更改套用於 SNMP 功能。
Undo (還原)	無	點擊 **Undo (還原)** 按鈕取消設定.

6.1.3 Telnet 模式的 CLI

command-line interface 命令列介面 (CLI) 也稱為命令列使用者介面和主控台使用者介面，是與電腦程式進行交談的方式, 使用者 (或客戶端) 以連續的文字列形式向程式發出命令 (命令列)。介面通常使用命令列 shell 進行, 該命令列 shell 是一個接受命令作為文字輸入並將命令轉換為適當的操作系統功能的程式。使用命令列界面的程序通常更容易透過腳本自動化。該設備分別支援 Telnet 和 SSH (安全 Shell) CLI 和預設服務埠 23 和 22。

Telnet & SSH 方案



方案應用程式計時

當閘道器管理員希望透過內網或網際網路從遠端站點進行管理時，可以使用“Telnet 模式的 CLI”功能透過 Telnet 或 SSH 工具來進行。

情景說明

本地管理員或遠端管理員可以使用具有最高權限使用者名稱和密碼的 Telnet 或 SSH 程式來管理閘道器。本地管理員和閘道器之間或遠端管理員和閘道器之間的資料封包可能是純文字或加密文件。 建議本地管理員在內網使用 Telnet 和純文字，遠端管理員在網際網路上使用 SSH 和加密文件。

參數設定示意圖

下表列出了上述示意圖中的參數設定，在 LAN 和 WAN 介面上啟用了“Telnet 模式的 CLI”。
表中未提及的參數使用預設值。

Configuration Path (設定路徑)	[Telnet with CLI]-[Configuration]
Telnet with CLI (Telnet 模式的 CLI)	LAN: ■ ***Enable*** WAN: ■ ***Enable***
Connection Type (連線類型)	Telnet: Service Port (服務埠) ***23*** ■ ***Enable*** SSH: Service Port (服務埠) ***22*** ■ ***Enable***

方案操作程序

在上圖中，“Local Admin 本地管理員”或“Remote Admin 遠端管理員”可以從內部網或網際網路管理“Gateway 閘道器”。 “Gateway 閘道器”是 Network-A 的閘道器，其內網的子網為 10.0.75.0/24。其具有 LAN 介面的 IP 位址 10.0.75.2 和 WAN-1 介面的 IP 位址 118.18.81.33。作爲 NAT 閘道器。

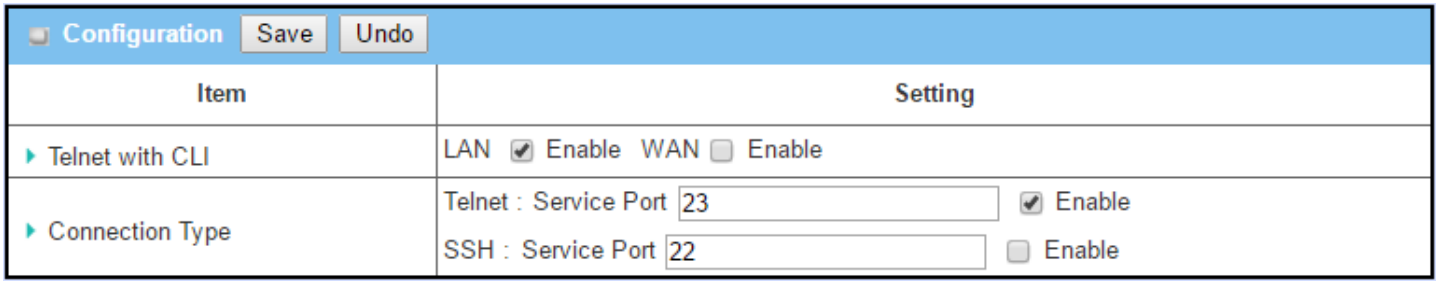
內網中的“Local Admin 本地管理員”使用具有最高權限帳戶的 Telnet 登錄到閘道器。

網際網路中的“Remote Admin 遠端管理員”使用具有最高權限帳戶的 SSH 登錄到閘道器。

設定 Telnet 模式的 CLI

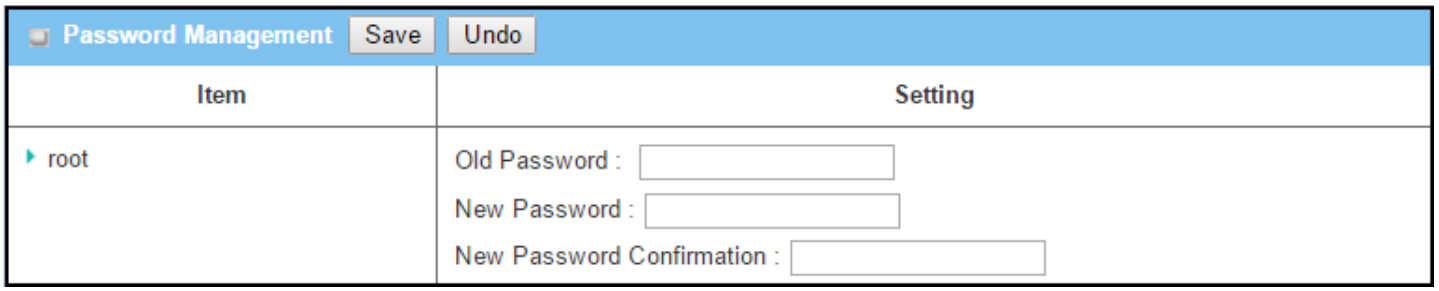
轉到 Administration > Configure & Manage > Telnet with CLI 頁面。

Telnet 模式的 CLI 允許管理員透過傳統的 Telnet 程式登入此設備。在 Telnet(登錄)到設備之前，請仔細設定相關設定和密碼。密碼管理部分允許您設定用於使用 Telnet 和 SSH 登錄的 root 密碼。



Configuration (設定)		
項目	**設定值**	**說明**
Telnet with CLI (Telnet 模式的 CLI)	1. 預設勾選 LAN 2. 預設未勾選 WAN	勾選 **Enable(啟用)**方框啓動 Telnet 模式的 CLI，以便從 WAN/LAN 介面進行連線。
Connection Type (連線類型)	1. 預設勾選 Telnet **Service Port** 預設 23 2. 預設未勾選 SSH **Service Port** 預設 22	勾選 Telnet 的 **Enable** 啟動 Telnet 服務。勾選 SSH 的 **Enable** 啟動 SSH 服務。您可以設定要為相應服務提供的**服務埠**數目。 ***範圍值*** : 1 ~ 65535.
Save (保存)	無	點擊 **Save (保存)** 按鈕以保存設定值
Undo (還原)	無	點擊 **Undo (還原)** 按鈕以取消設定

預設 CLI 登入帳號”root”，密碼為”wirelessm2m”



Configuration (設定)		
項目	**設定值**	**說明**
Root (根)	1. 字串: 任何文字 , 但不能有空白字元 2. Telnet 的預設密碼為 "m2metherwan"	輸入舊密碼並指定新密碼以更改根密碼。 ***注意: 強烈建議在部署設備之前更改預設的 Telnet 密碼。***
Save (保存)	無	點擊 **Save (保存)** 按鈕以保存設定值
Undo (還原)	無	點擊 **Undo (還原)** 按鈕以取消設定

6.2 系統操作

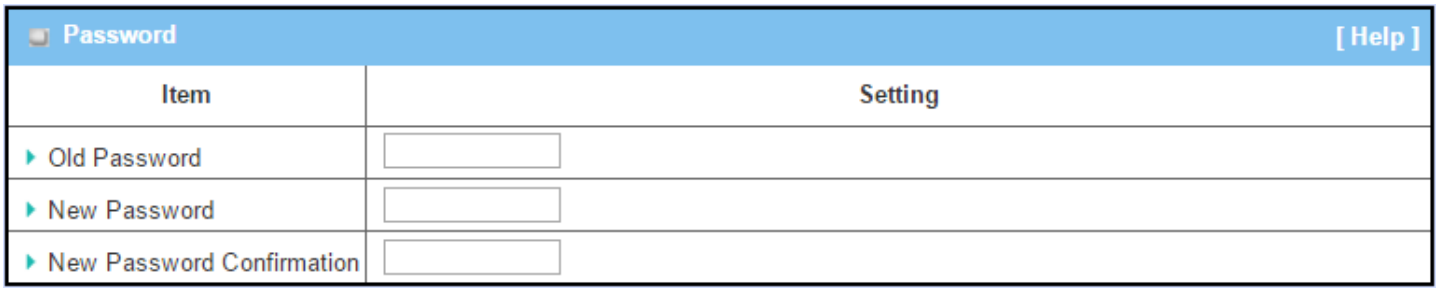
系統操作允許網路管理員管理系統和設定，如 Web 工具軟體、密碼更改、系統資訊、系統時間、系統日誌、韌體/設定備份和恢復，以及重置和重新開機。

6.2.1 密碼 & MMI (人機界面)

轉到 Administration > System Operation > Password & MMI 頁面。

變更密碼

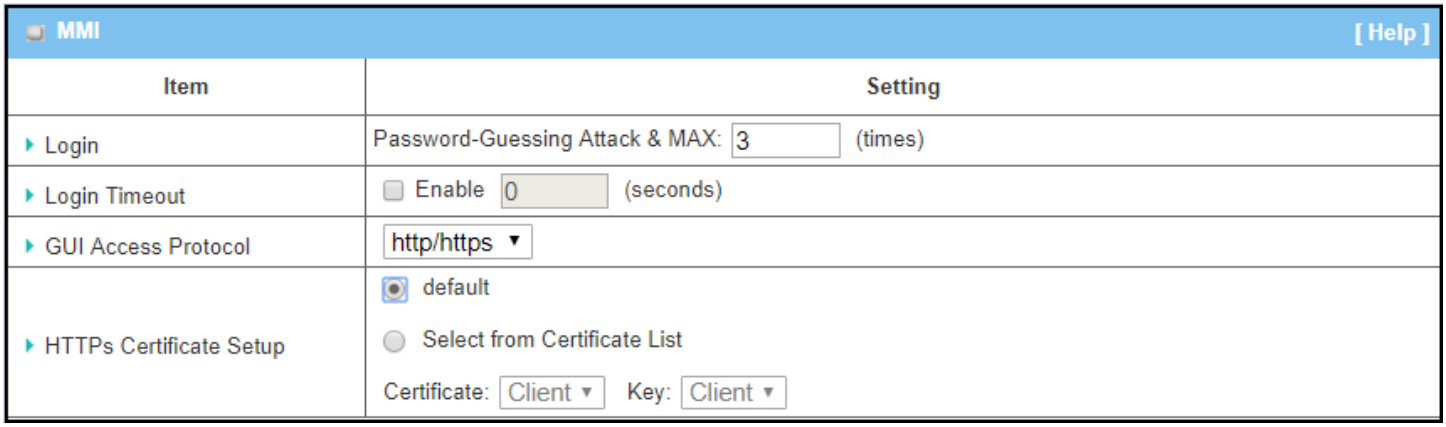
變更密碼畫面允許網路管理員更改 Web 的 MMI(Man-machine interface 人機界面)登錄密碼。



Change Password (更改密碼)		
項目	設定值	說明
Old Password (舊密碼)	1. 字串: 任何文字 2. 預設密碼為 "admin"。	輸入目前密碼。
New Password (新密碼)	字串: 任何文字	輸入新密碼
New Password Confirmation (新密碼確認)	字串: 任何文字	再次輸入新密碼作爲確認
Save (保存)	無	點擊 Save (保存) 按鈕以保存設定
Undo (還原)	無	點擊 Undo (還原) 按鈕以取消設定

更改登入 MMI 的設定

它允許管理員使用網頁人機介面登入閘道器進行管理。閘道器的網頁人機介面將在閒置時間結束後自動登出。該設定允許管理員啟用自動登出並設定登出閒置時間。



Web UI 項目	設定值	說明
Login (登錄)	預設設定 3 次	輸入登錄試用次數。 ***範圍值***:3 ~ 10 如果有人嘗試使用不正確的密碼登錄到 web GUI 中，會出現警告訊息 "*Already reaching maximum Password-Guessing times, please wait a few seconds! (已經達到了密碼猜測的最大次數，請稍候幾秒鐘!)*"
Login Timeout (登錄超時)	預設未勾選 Enable	勾選 " Enable(啟用)" 方框啟動自動登出功能, 同時指定最大閒置時間。 ***範圍值***:30 ~ 65535.
GUI Access Protocol (GUI 訪問協定)	**http/https** 預設選擇.	選擇用於 GUI 登入的協定。可能是 **http/https**, **http only**, 或 **https only**..
HTTPs Certificate Setup (HTTPs 證書設定)	預設勾選 **default**	如果選擇 HTTPs 登入協定，則將更進一步設定 HTTPs 憑證選項。 您可以將其保留為預設值，或從下拉選單中選擇憑證和密鑰。 有關憑證設定，請參閱物件 **Definition > Certificate** 部分。
Save (保存)	無	點擊 **Save (保存)** 按鈕以保存設定。
Undo (還原)	無	點擊 **Undo (還原)** 按鈕以取消設定

6.2.2 系統資訊 System Information

系統資訊畫面使網路管理員能夠快速查看閘道器的設備資訊。

轉到 Administration > System Operation > System Information 頁面。

System Information

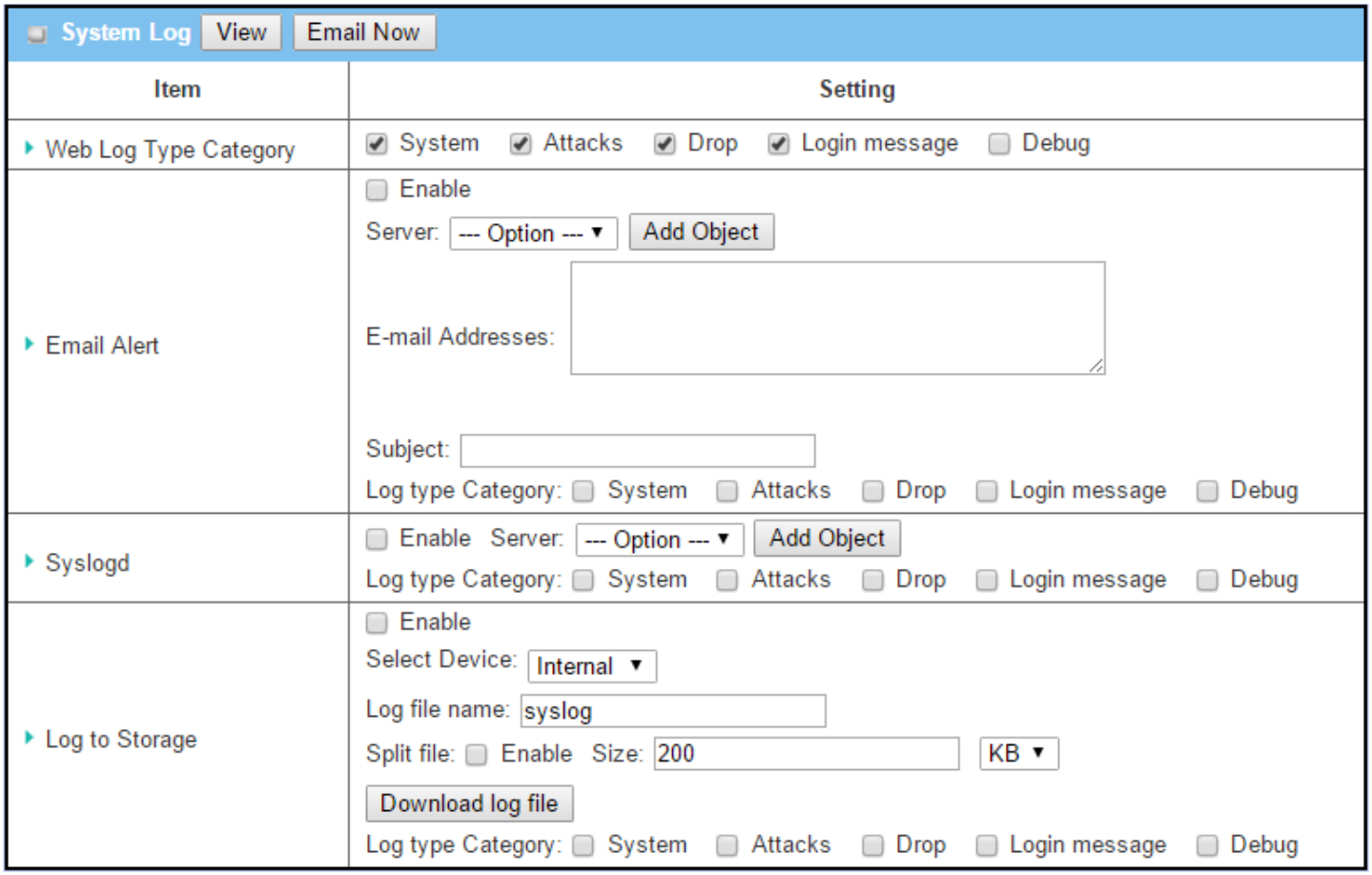
Item	Setting
Model Name	
Device Serial Number	
Kernel Version	2.6.36
FW Version	0000TE0.H81_e81.0000_08021800
CPU Usage	9.80%
Memory Usage	60%
System Time	Mon, 07 Aug 2017 15:45:25 +0800
Device Up-Time	4day 3hr 22min 24sec

System Information (系統資訊)		
項目	**設定值**	**說明**
Model Name (型號名稱)	無	顯示此產品的型號名稱。
Device Serial Number (設備序號)	無	顯示此產品的序號。
Kernel Version (內核版本)	無	顯示產品的 Linux 內核版本
FW Version (韌體版本)	無	顯示產品的韌體版本
CPU Usage (CPU 使用率)	無	顯示 CPU 利用率的百分比。
Memory Usage (記憶體使用率)	無	顯示裝置記憶體利用率百分比。
System Time (系統時間)	無	顯示您流覽網頁時的當前系統時間。
Device Up-Time (設備開機)	無	顯示自上次開機以來設備運行的時間統計資訊。
Refresh (刷新)	無	點擊 Refresh(**刷新)** 按鈕更新系統資訊。

6.2.4 系統日誌 System Log

系統日誌畫面包含各種事件日誌工具，以便於本地事件記錄和遠端報告。

轉到 Administration > System Operation > System Log 頁面。

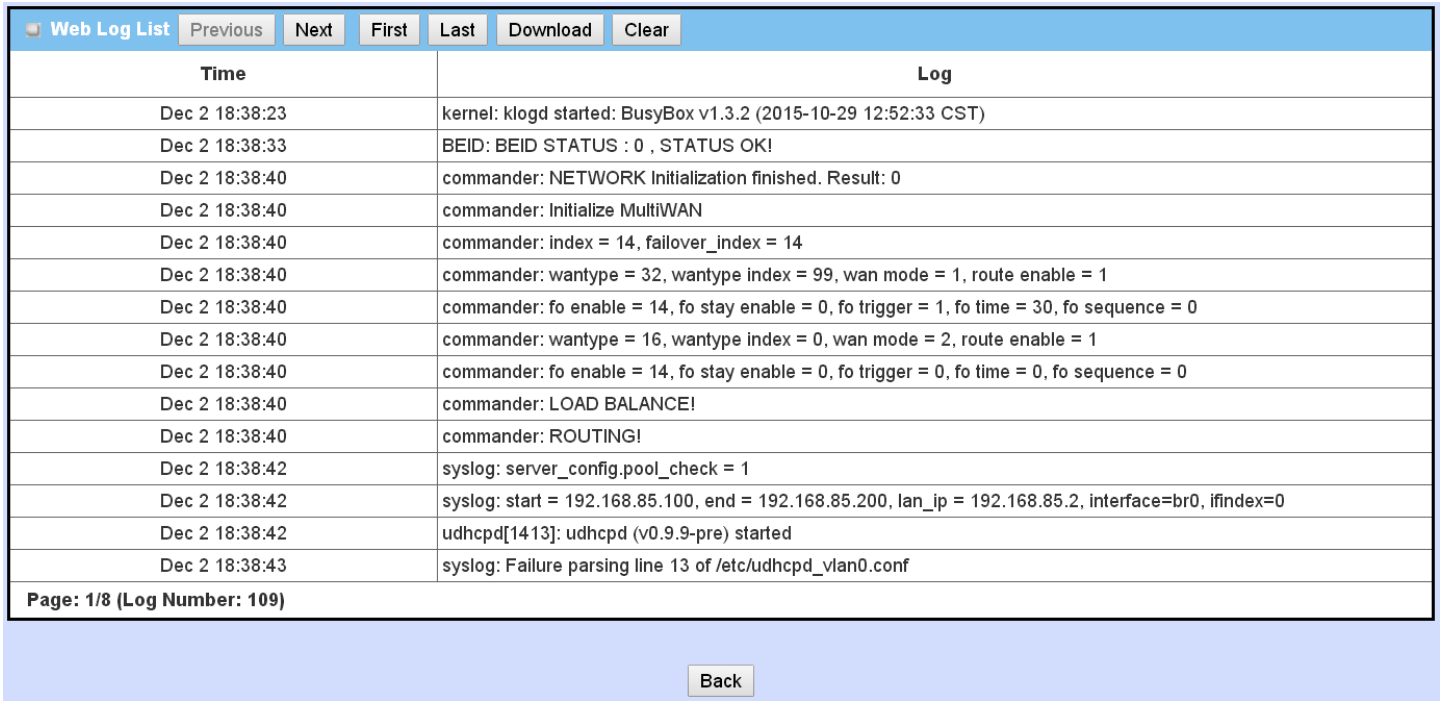


查看 & 以電子郵件寄出日誌歷史記錄

View(查看)按鈕允許查看日誌歷史記錄。 **Email Now** 按鈕可讓管理員發送即時電子郵件進行分析。

View & Email Log History (查看 & 電子郵件傳送日誌歷史)		
項目	**設定值**	**說明**
View button (查看按鈕)	無	點擊 **View (查看)** 按鈕在 "網頁日誌清單" 視窗中查看日誌歷史記錄。

Email Now button (立即傳送按鈕)	無	點擊 **Email Now (立即傳送按鈕)**按鈕，立刻寄出日誌電子郵件。



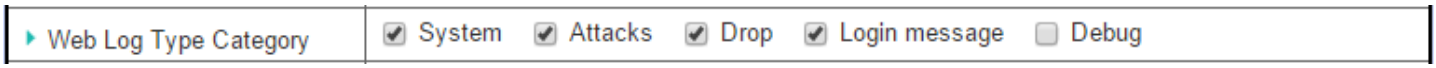
Web Log List Window (網頁日誌清單視窗)		
項目	**設定值**	**說明**
Time column (時間列)	無	顯示事件時間戳記
Log column (日誌列)	無	顯示日誌訊息

Web Log List Button (網頁日誌清單按鈕)		
項目	**設定值**	**說明**
Previous	無	點擊 Previous(**上一個**)按鈕移動到上一頁。
Next	無	點擊 Next(**下一步**)按鈕移動到下一頁。
First	無	點擊 First(**第一個**)按鈕跳轉到第一頁。
Last	無	點擊 Last(**最後一個**)按鈕跳轉到最後一頁。
Download	無	點擊 Download(**下載**)按鈕以 tar 檔案格式將日誌下載到您的 PC 上。

Clear	無	點擊 Clear(**清除**)按鈕清除所有日誌。
Back	無	點擊 Back(**返回**)按鈕返回上一頁。

網頁日誌類型類別

網頁日誌類型類別畫面允許網路管理員選擇要記錄的事件類型，並按照上一節所述在網頁日誌列表畫面中顯示。 點擊 View 查看按鈕在網頁日誌列表畫面中查看日誌歷史記錄。



Web Log Type Category Setting Window (網頁日誌類型設定視窗)		
項目	**設定值**	**說明**
System	預設勾選	記錄系統事件並在 "網頁日誌清單" 視窗中顯示。
Attacks	預設勾選	記錄攻擊事件並在 "網頁日誌清單" 視窗中顯示。
Drop	預設勾選	記錄資料封包丟失事件並顯示在 "網頁日誌清單" 視窗中。
Login message	預設勾選	記錄系統登錄事件並在 "網頁日誌清單" 視窗中顯示。
Debug	預設未勾選	記錄除錯事件並在 "網頁日誌清單" 視窗中顯示。

電子郵件警報

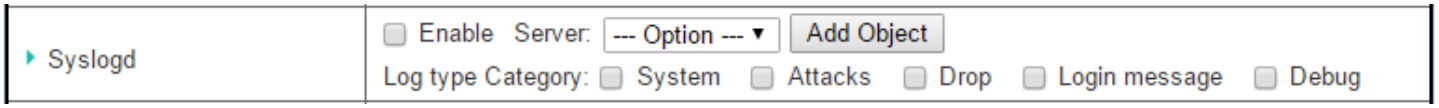
電子郵件警報畫面允許網路管理員選擇要記錄的事件類型同步送到指定的電子郵件帳戶。

Email Alert Setting Window (電子郵件警報設定視窗)		
項目	**設定值**	**說明**
Enable	預設未勾選	勾選 Enable(**啟用**)方框將事件日誌訊息發送到電子郵件地址中定義的指定電子郵件帳戶。
Server	無	從 "Server(伺服器)" 下拉選單中選擇一個電子郵件伺服器以發送郵件。如果沒有可用的，點擊 **Add Object(增加物件)**按鈕以建立傳出電子郵件伺服器。

		您還可以從 Object Definition > External Server > External Server 頁面增加傳出電子郵件伺服器。
E-mail address (電子郵件地址)	字串: 電子郵件格式	輸入收件者的電子郵件地址。用逗號 "," 或分號 ";" 分隔電子郵件地址 輸入電子郵件地址格式為 *'myemail@domain.com'*
Subject (標題)	字串: 任何文字	輸入電子郵件標題，讓您可以很容易地在電子郵件客戶端上識別。
Log type category (日誌類型類別)	預設未勾選	選擇要記錄的事件種類同時送到指定的電子郵件帳戶，可用的事件爲 System、Attacks、Drop、Login message 和 Debug。

Syslogd

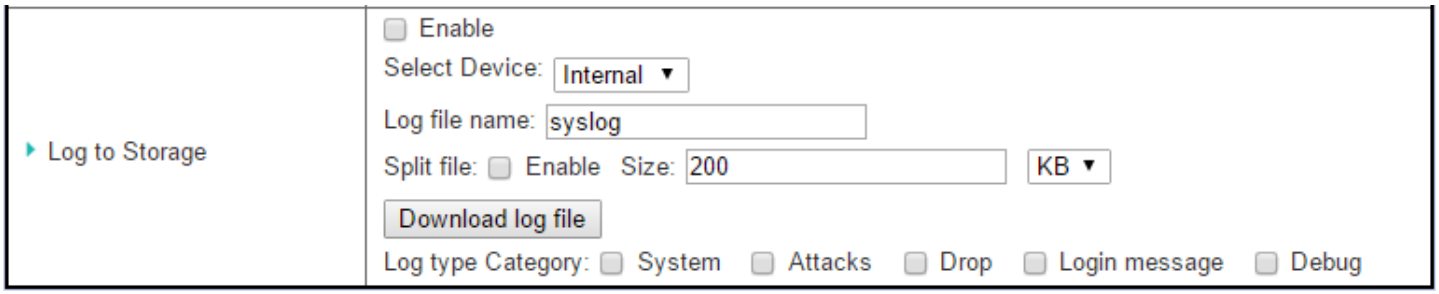
Syslogd 畫面允許網路管理員選擇要記錄的事件類型並將其發送到指定的 Syslog 伺服器。



Syslogd Setting Window (Syslogd 設定視窗) 項目	設定值	說明
Enable	預設未勾選	勾選 **Enable(**啟用)方框啟動 Syslogd 功能，將事件日誌發送到日誌伺服器
Server	無	從 " **Server(**伺服器)" 下拉清單中選擇一個日誌伺服器，將事件日誌發送過去。 如果沒有可用的, 點擊 **Add Object(增加物件)**按鈕以建立系統日誌伺服器。 也可以從 Object Definition > External Server > External Server 頁面增加系統日誌伺服器。
Log type category (日誌類型類別)	預設未勾選	選擇要記錄的事件種類並將其發送到預定的日誌伺服器.可用事件是 System、Attacks、Drop、Login message 和 Debug

日誌儲存 Log to Storage

日誌存儲畫面允許網路管理員選擇要記錄的事件類型並存儲在內部或外部存儲設備中。



Log to Storage Setting Window (日誌到存儲設定視窗) 項目	設定值	說明

Enable	預設未勾選	勾選方框以啟用將日誌發送到存儲設備。
Select Device	Internal 預設選擇	選擇內部或外部存儲設備。
Log file name	預設未勾選	輸入要保存日誌的檔案名稱。
Split file Enable	預設未勾選	勾選 **Enable(啟用)**方框之後每到日誌檔到達大小限制時拆分檔案。
Split file Size	**200 KB** is set 預設	輸入每個拆分日誌檔的檔案大小限制。 ***範圍值*** :10 ~ 1000.
Log type category **(日誌類型類別)**	預設未勾選	勾選要發送的日誌類型: System、Attacks、Drop、Login message 和 Debug

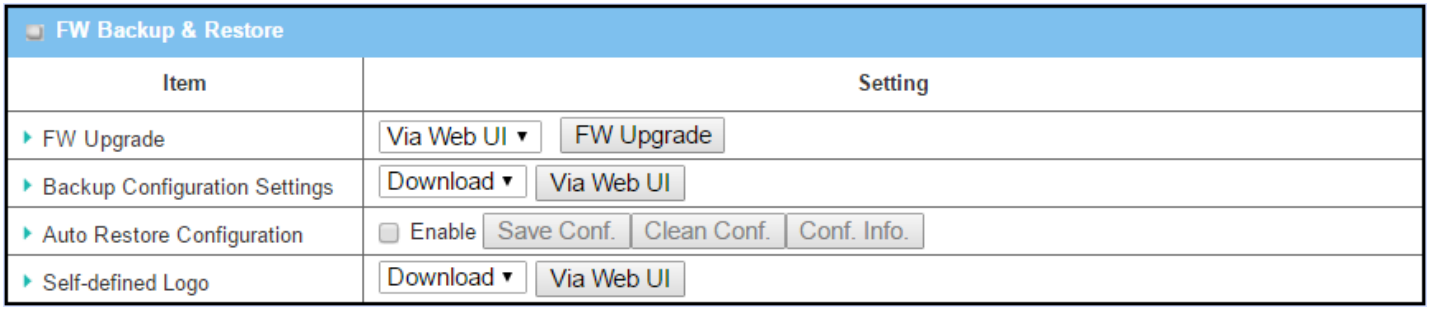
Log to Storage Button Description (日誌到存儲按鈕說明)		
項目	**設定值**	**說明**
Download log file (下載日誌檔)	無	點擊 **Download log file(下載日誌檔)**按鈕下載日誌檔到日誌. tar 檔。

6.2.5 備份 & 恢復 Backup & Restore

在 “Backup& Restore 備份和恢復” 畫面中，可以在有新韌體時升級設備韌體，也可以備份/恢復設備設定。

除了出廠預設設定之外，您還可以將特殊設定設作爲客製化預設值。您可以使用此客製化預設值將設備依照需求重置為預設設定。

轉到 Administration > System Operation > Backup& Restore 頁面。



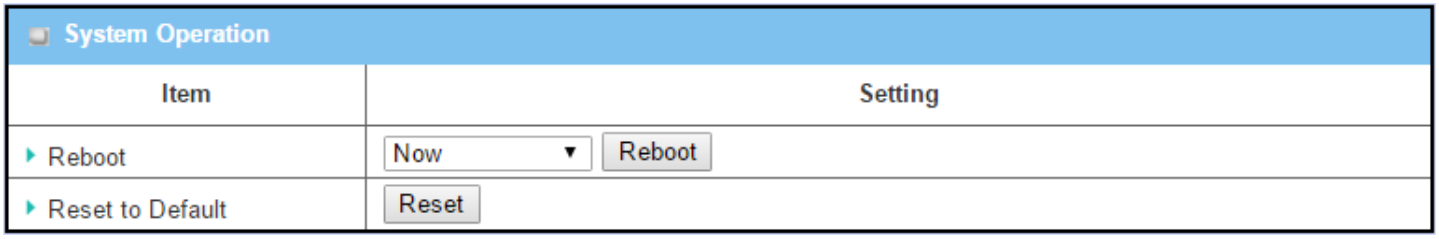
FW Backup& Restore (韌體備份 & 恢復) 項目	設定值	說明
FW Upgrade (韌體升級)	預設選擇 Via Web UI	如果有新韌體可用, 請點擊 **FW Upgrade(韌體升級)**按鈕以升級設備韌體 可選 **via Web UI(通過 Web UI)**或 **Via Storage(通過存儲設備)**。 點擊 " FW Upgrade(韌體升級)" 按鈕後, 使用 " Browse(流覽)" 按鈕指定新韌體的檔案名稱，然後點擊 " Upgrade(升級)" 按鈕啟動韌體升級程序。如果要升級來自 GPL 策略的韌體，請勾選 " Accept unofficial firmware(接受非官方韌體)"
Backup Configuration Settings (備份配置設定)	預設選擇 Download	你可以通過點擊 ***Via Web UI(通過 Web UI)*** 按鈕來備份或還原設備配置設定。 **Download(下載)**: 用於將設備配置備份到配置. bin 檔。 **Upload(上傳)**: 用於將指定的配置檔案還原到設備。 **Via Web UI(通過 Web UI)** : 通過 Web GUI 檢索設定檔。
Auto Restore Configuration (自動還原設定)	預設未勾選 Enable	點擊 **Enable(啟用)**按鈕以啟動自訂的預設設定功能。 啟動該功能後，可以通過點擊 " **Save Conf.(保存**配置)" 按鈕, 或點擊” **Clean Conf.(清除**配置)" 按鈕保存設定為自訂預設設定。

6.2.6 重新開機 & 重新設定

在某些特殊原因或情況下，您可能需要將閘道器重新開機或將設備重新設定為預設設定。除了透過電源開啟/關閉或按下設備面板上的 Reset 重置按鈕來執行這些操作外，您還可以透過網頁界面執行此操作。

轉到 Administration > System Operation > Reboot & Reset 頁面。

在 Reboot＆Reset(重新開機 & 重新設定)畫面中，您可以透過點擊 “Reboot 重新開機” 按鈕來重新啟動該設備，並透過點擊 “Reset 重新設定” 按鈕將該設備重置為預設設定。



System Operation Window (系統操作視窗) 項目	設定值	說明
Reboot (重新開機)	預設選擇 Now	點擊 Reboot(**重新開機)**按鈕可立即或依照預定時間安排重新開機閘道器。 **Now(現在)** : 立即重新開機 **Time Schedule(時間安排)**: 選擇預定自動重新開機的時間計畫規則, 以便在指定時間自動重新開機。轉到 **Object Definition > Scheduling > Configuration** 頁面。
Reset to Default (重設爲預設)	無	點擊 **Reset(重置)**按鈕, 將設備的設定重置為預設值。

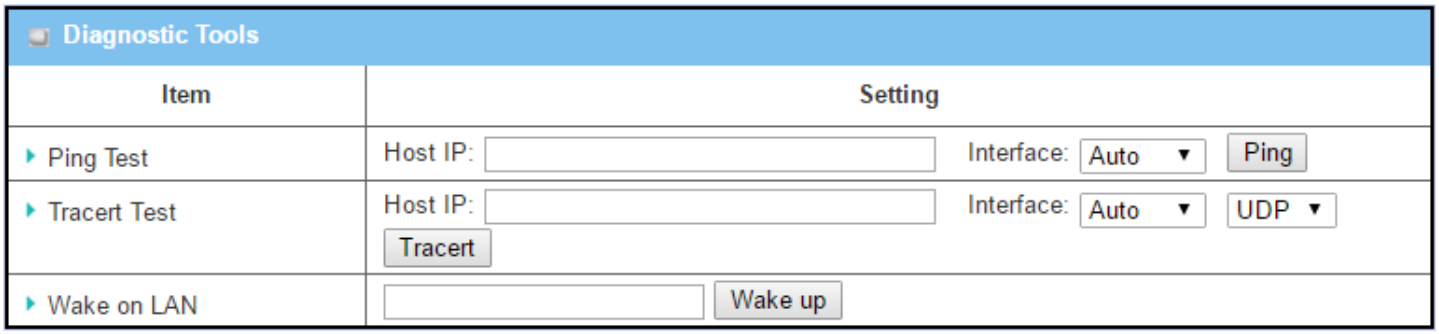
6.4 診斷 Diagnostics

該閘道器支援簡單的網路診斷工具，供管理員故障排除和分析閘道器的異常行為或流量。

6.4.1 診斷工具

診斷工具為網路管理員提供了一些常用的網路連線工具(方法)來檢查設備連線。

轉到 Administration > Diagnostic > Diagnostic Tools 頁面。

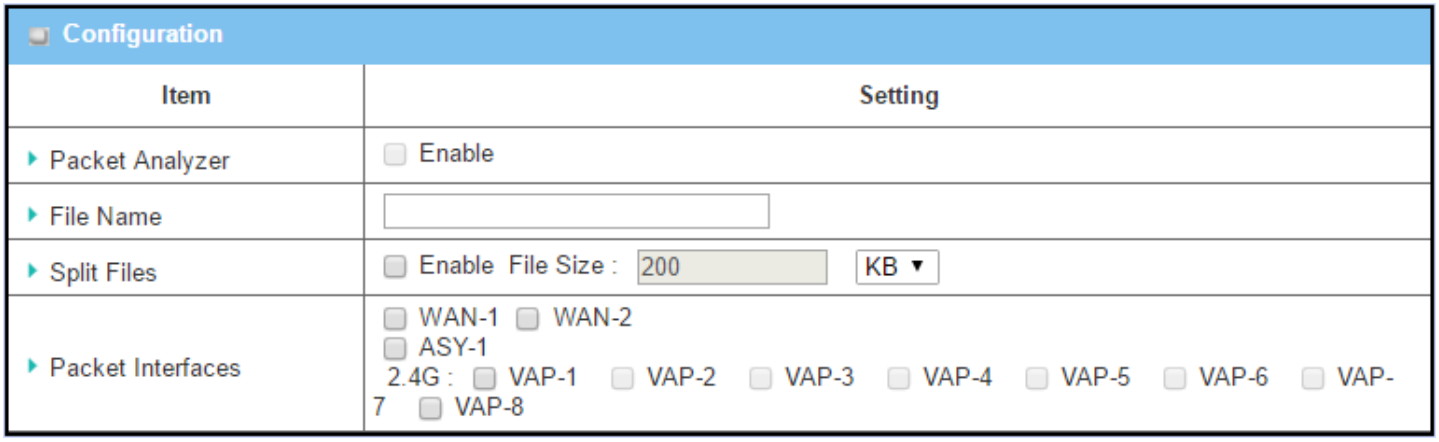


Diagnostic Tools (診斷工具)		
項目	設定值	說明
Ping Test (Ping 測試)	可選設定	此允許您指定 IP/FQDN 和測試介面(LAN、WAN 或 Auto)，系統將嘗試 去 ping 您指定的設備，點擊 **Ping** 按鈕後測試它是否存在。測試結果將顯示在下面的視窗。
Tracert Test (路由追蹤測試)	可選設定	Trace route (tracert) 命令是一個網路診斷工具, 用於顯示路由 (路徑) 並通過 IP 網路測量資料封包的傳輸延遲。追蹤路由直到所有 (三個) 發送的資料封包丟失兩次以上、連線丟失而且無法計算路由。 指定 IP/FQDN、測試介面(LAN、WAN 或 Auto)和協定 (UDP 或 ICMP)。預設是 **UDP**。系統將嘗試追蹤指定的主機 ，點擊 **Tracert** 按鈕後測試它是否存在。測試結果將顯示在下面視窗。
Wake on LAN (網路喚醒)	可選設定	Wake on LAN (WOL)(網路喚醒)是一個區域網網路標準，允許電腦由網路開機或。您可以通過點擊 Wake up(**喚醒**)命令按鈕，指定電腦在 LAN 網路中的 MAC 位址，以便在遠端開機。
Save (保存)	無	按下 Save (保存) 按鈕以保存設定值.

6.4.2 封包分析器 Packet Analyzer

封包分析器可以依據客製化設定捕捉封包。使用者可以指定介面來捕捉資料封包並透過設定規則進行過濾。請確認日誌存儲可用(嵌入式 SD 卡或外部 USB 存儲裝置)，否則無法啟用封包分析器。

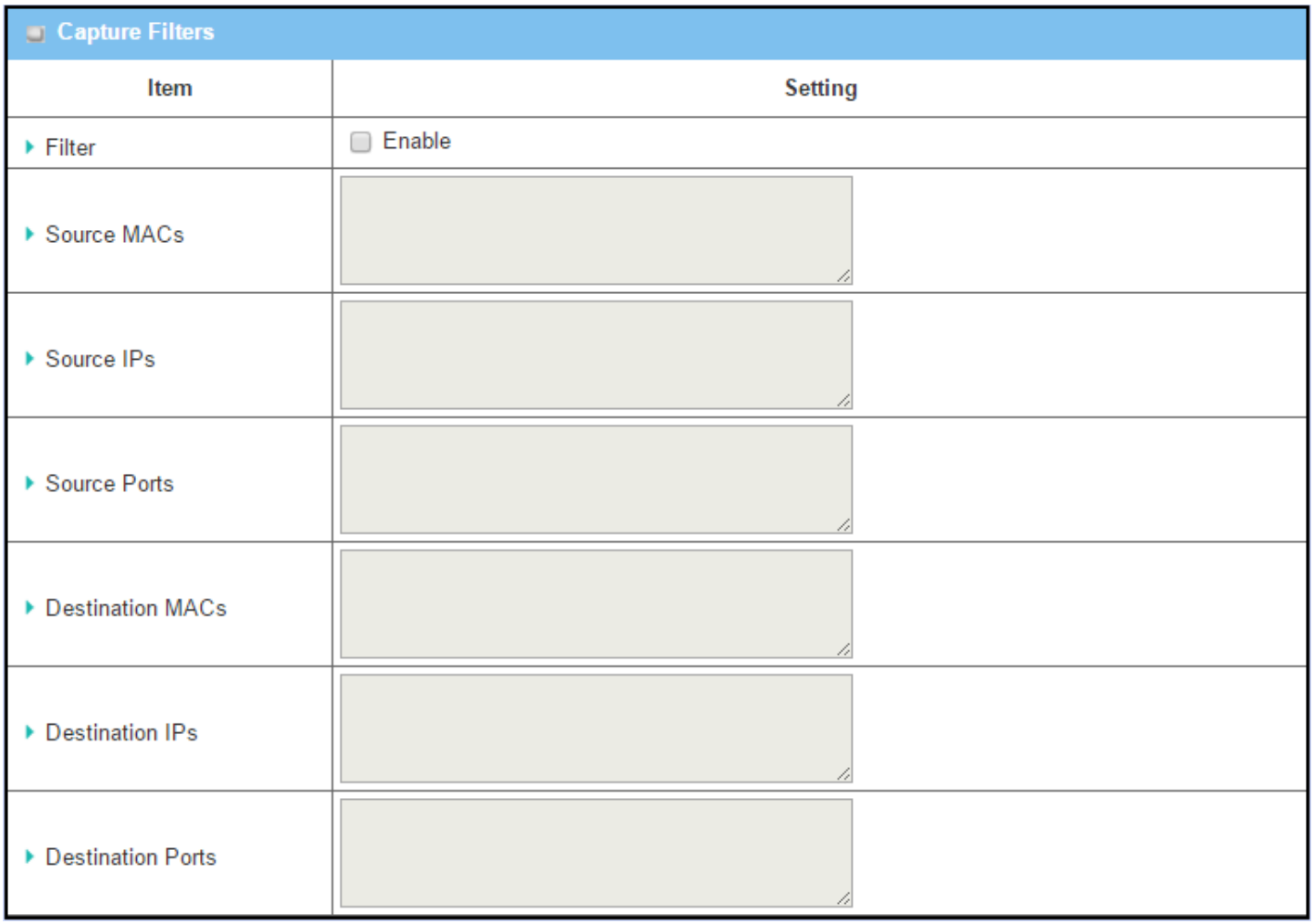
轉到 Administration > Diagnostic > Packet Analyzer 頁面。



Configuration (設定)		
項目	**設定值**	**說明**
Packet Analyzer (封包分析器)	預設未勾選	勾選 **Enable(啟用)**方框啟動資料封包分析器功能。 如果無法啟用該核取方框，請檢查存儲設備是否可用。插入 USB 存儲碟，然後啟用封包分析器功能。
File Name (檔案名稱)	1. 可選設定 2. 預設為空, 預設檔案名為 **<介面> _ <日期> _ <索引>**	輸入檔案名稱以儲存捕獲的資料封包日誌。 如果還啟用了 **Split Files 拆分檔案**選項，檔案名稱將追加一個索引代碼 "_ < **索引** >"，檔副檔名為**. pcap**
Split Files (拆分檔案)	1. 可選設定 2. **檔案大小**的預設值為 200 KB。	勾選 **Enable(啟用)**方框指定日誌檔拆分指定的大小限制， 如果啟用了**拆分檔案**選項，則可以進一步指定拆分檔的**檔案大小**和**單位**。 ***範圍值*** **:** 10 ~ 99999.注意:**檔案大小**不能小於 10 KB
Packet Interfaces (封包介面)	可選設定	定義**資料封包分析器**應處理的介面。 至少需要一個介面，但也接受複選。支援的介面有: **WAN**：當在**實體介面**上啟用 WAN 時, 可以在此處選擇它。 **ASY**：代表序列通信介面。用於捕獲出現在 **Field Communication(場域通訊)**中的資料封包。只有當啟用了

		特定的欄位通訊協定 (如 " Modbus ") 時, 才能選擇它。 **VAP** : 代表虛擬 AP。當啟用 Wi-Fi 和 VAP 時，可以在這裡選擇它。
Save (保存)	無	按下 **Save (保存)** 按鈕以保存設定值.
Undo (還原)	無	按下 **Undo (還原)** 按鈕以還原上一個設定值.

在特定介面上啟用了封包分析器功能之後，可以進一步指定一些過濾規則來捕捉符合規則的封包。

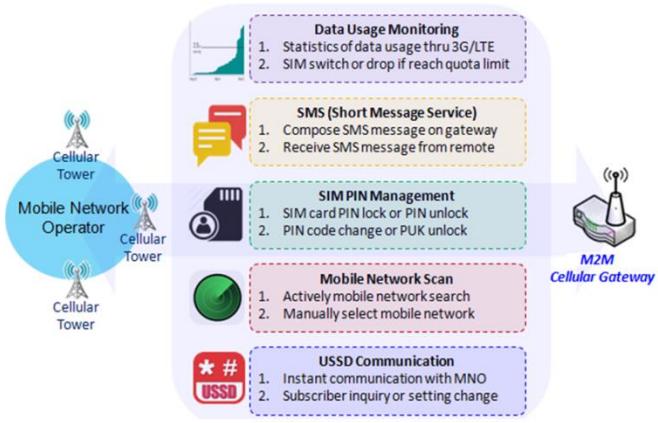


Capture Fitters (截取篩選)		
項目	**設定值**	**說明**
Filter (過濾器)	可選設定	勾選 Enable(**啟用**)方框啟動**過濾器**功能。
Source MACs (來源 MAC)	可選設定	定義**來源 MAC** 作爲篩選規則 , 資料封包的來源 MAC 位址。 將抓取源 MAC 位址的資料封包。

		支援多達 10 個 MAC, 但必須用 ";"分隔開。 例如 AA:BB:CC:DD:EE:FF;11:22:33:44:55:66 資料封包將在符合規則其中的任何一個 MAC 時抓取。
Source IPs (來源 IP)	可選設定	定義**來源 IP** 作爲篩選規則，資料封包的來源 IP 位址。 將抓取符合規則的資料封包。 支援多達 10 個 IP, 但必須用 ";"分隔開。 如 192.168.1.1;192.168.1.2 資料封包將在符合規則其中的任何一個 IP 時抓取。
Source Ports (來源埠)	可選設定	定義**來源埠**，資料封包的來源埠。 將抓取符合規則的資料封包。 支援多達 10 個埠, 但必須用 ";"分隔開。 例如 80;53 ***範圍值*** : 1 ~ 65535.
Destination MACs (目標 MAC)	可選設定	定義**目標 MAC** 作爲篩選規則 , 資料封包的目標 MAC 位址。 將抓取源 MAC 位址的資料封包。 支援多達 10 個 MAC, 但必須用 ";"分隔開。 例如 AA:BB:CC:DD:EE:FF;11:22:33:44:55:66 資料封包將在符合規則其中的任何一個 MAC 時抓取。
Destination IPs (目標 IP)	可選設定	定義**目標 IP** 作爲篩選規則，資料封包的目標 IP 位址。 將抓取符合規則的資料封包。 支援多達 10 個 IP, 但必須用 ";"分隔開。 如 192.168.1.1;192.168.1.2 資料封包將在符合規則其中的任何一個 IP 時抓取。
Destination Ports (目標埠)	可選設定	定義**目標埠**，資料封包的目標埠。 將抓取符合規則的資料封包。 支援多達 10 個埠, 但必須用 ";"分隔開。 例如 80;53 ***範圍值*** : 1 ~ 65535.

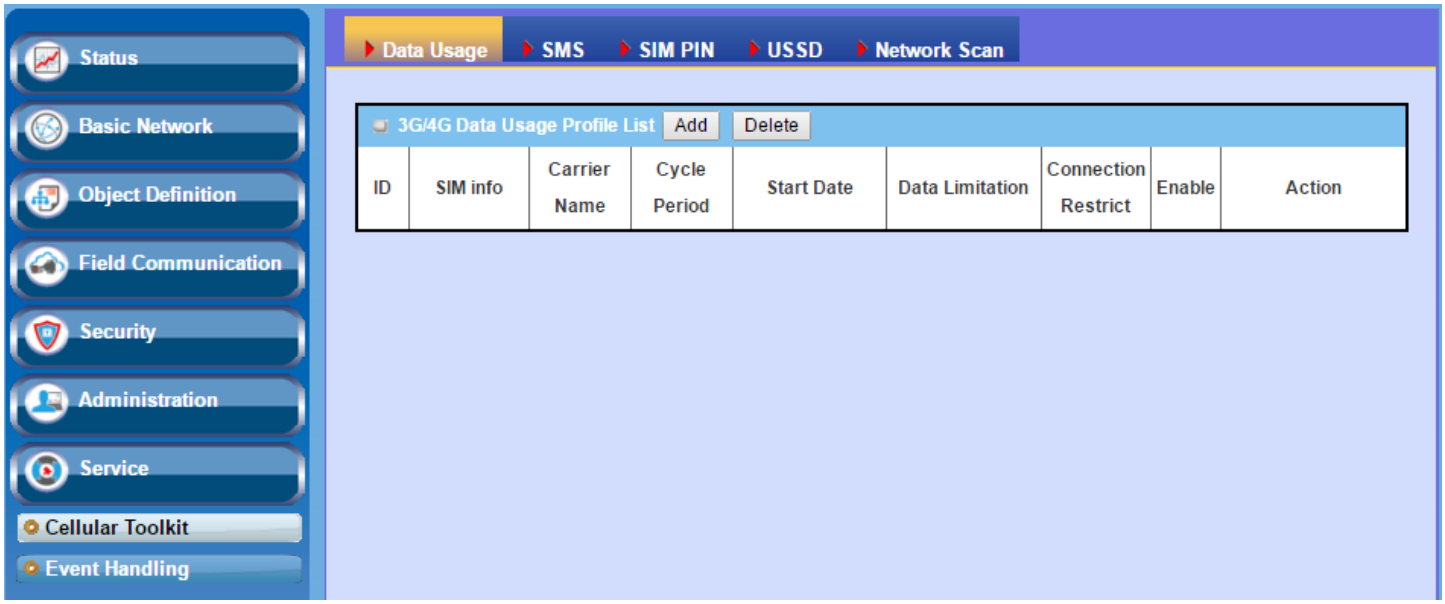
第 7 章 服務 Serverice

7.1 蜂巢工具組 Cellular Toolkit



除了Cellular資料連線之外，您還可能需要監控Cellular WAN的資料使用情況，透過SMS發送文字訊息、更改SIM卡的PIN碼、使用USSD(Unstructured Supplementary Service Data)命令與Carrier/ ISP 進行通信，或執行蜂巢網路掃描作爲診斷。

Cellular Toolkit工具組包括幾個與Cellular設定或應用有關的功能。您可以在此設定資料使用、SMS、SIM PIN、USSD和網路掃描的設定。 請注意，在繼續本節中的設定之前，需要將有效的SIM卡插入設備。



7.1.1 資料使用

大多數 Cellular 連線的資料方案都有資料上限。如果資料使用量超過設定的限制，可能會導致資料吞吐量低得多，從而影響您的操作，或者超過額度的高額賬單。

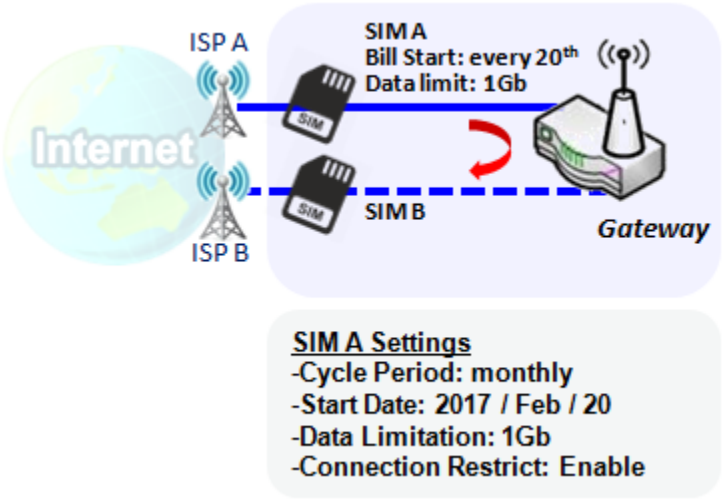
透過資料使用功能，設備將持續監控手機資料使用情況並採取預設操作。設備可以設定為立即取消蜂巢資料連線，或者如果插入了副 SIM 卡，設備將切換到副 SIM 並自動建立另一個蜂巢資料連線。

如果啟用了資料使用功能，則可以在 **Status** > **Statistics & Reports** > **Cellular Usage** 頁面上查看蜂巢資料使用的整個歷史記錄。

3G/4G Data Usage Profile List | Add | Delete

ID	SIM info	Carrier Name	Cycle Period	Start Date	Data Limitation	Connection Restrict	Enable	Action
1	3G/4G SIM A	ISP A	1 Monthly	Mon Feb 20 2017 00:00:00 GMT+0800	1GB	☑	☑	Edit ☐ Select

3G/4G 資料使用



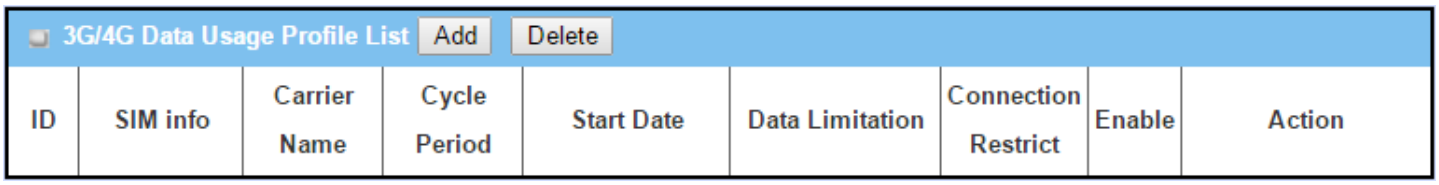
資料使用功能允許閘道器設備持續監控 Cellular 資料使用並採取行動。在該圖中，SIM A 的限制為每月 1Gb，並且計費開始日期為每個月的 20 日。該設備可以在本月 20 日開始新的資料使用計算。 當資料使用量達到 1Gb 時，啟用連線限制將強製閘道器將 SIM A 的 Cellular 斷線。如果在網際網路安裝程序中設定了 SIM 故障切換功能，則閘道器將切換到 SIM B 並自動建立新的 Cellular 資料連線。

設定資料使用

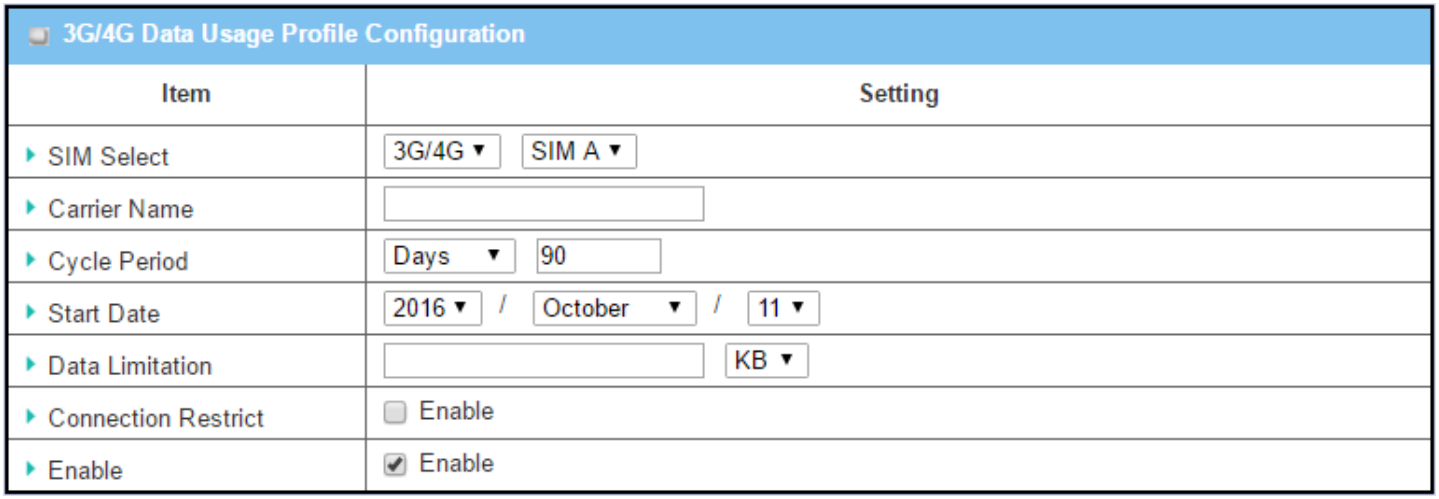
轉到 **Service** > **Cellular Toolkit** > **Data Usage** 頁面。

如要設定資料使用，您需要知道資料方案的結算和開始日期、帳單週期和資料額度。

建立/編輯 3G/4G 資料使用專案



當按下 Add (增加)按鈕，將出現 3G/4G Data Usage Profile Configuration (資料使用專案設定)畫面, 您最多可以建立四個資料使用設定，即閘道器中使用的每個 SIM 卡爲一個專案。



3G/4G Data Usage Profile Configuration (3G/4G 資料使用專案設定)		
項目 Setting	設定值	說明
SIM Select **(SIM 選擇)**	預設 **3G/4G-1** 和 **SIM A**	選擇一個蜂巢介面 (**3G/4G-1** 或 **3G/4G-2**)，綁定選擇的蜂巢介面 SIM 卡以配置其資料使用設定檔。 **注意:** 3G/4G-2 僅適用於具有雙蜂巢模組的產品。
Carrier Name **(營運商名稱)**	可選項目.	填寫 SIM 卡的營運商名稱作爲識別。

Cycle Period (迴圈週期)	預設 **Days**	三種類型的週期為 **Days(天)**、**Weekly(每周)** 和 **Monthly(每月)** **Days(天)**: 選擇每天的週期，您必須進一步指定第二個框中的天數。 ***範圍值*** : 1 ~ 90 天. **Weekly(每周)** 和 **Monthly(每月)**: 迴圈週期為一周或一個月.
Start Date (開始日期)	無	指定開始測量網路通信量的日期。 不要選擇過去日期。這將導致交通統計資料不正確。
Data Limitation (資料限制)	無	指定週期期間允許的資料量限制。
Connection Restrict (連接限制)	預設未勾選.	勾選 **Enable(啟用)**方框啟動連線限制功能。 在指定的週期期間，如果實際資料使用量超過允許的資料量限制，則將強制斷開蜂巢連線。
Enable (啓動)	預設未勾選.	勾選 **Enable(啟用)**方框啟動資料使用設定檔。

7.1.2 SMS

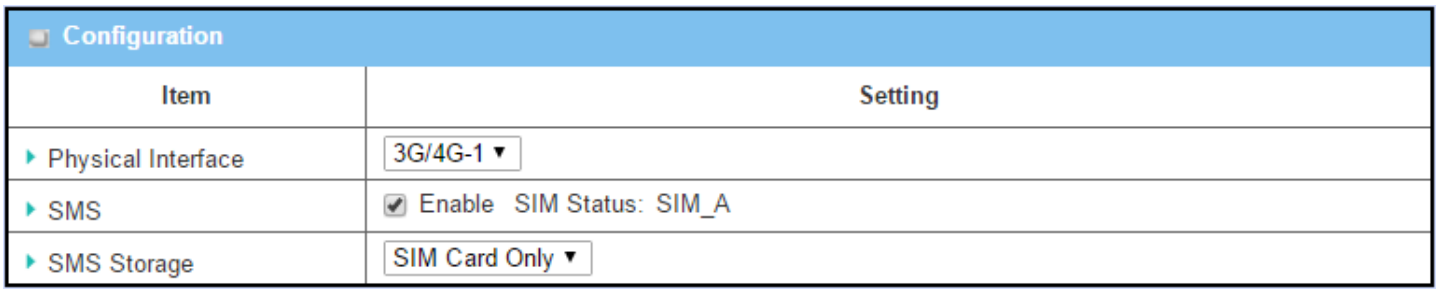
簡訊服務(SMS)是一種在手機上廣泛使用的簡訊服務。使用標準化的通信協定使手機或手機設備以即時便捷的方式交換短資訊。

設定SMS

轉到**Service** > **Cellular Toolkit** > **SMS** 頁面

使用這款閘道器設備，您可以像手機一樣發送簡訊或瀏覽收到的簡訊。

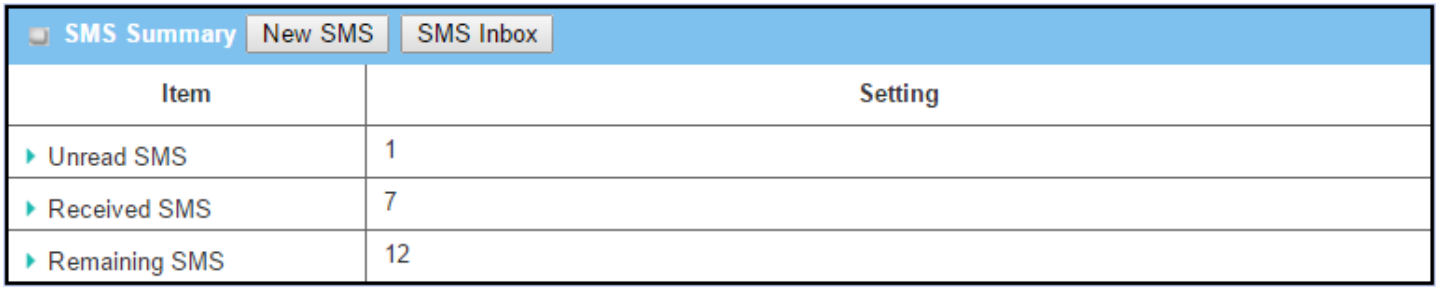
設定 SMS 配置



Configuration (設定)		
項目	**設定值**	**說明**
Physical Interface (實體介面)	預設 **3G/4G-1**	選擇一個蜂巢介面 (**3G/4G-1** 或 **3G/4G-2**)用於以下 SMS 功能設定 **注意: 3G/4G-2** 僅適用於具有雙蜂巢模組的產品。
SMS	預設勾選	勾選以啟用 SMS 功能。
SIM Status	無	根據於目前 SIM 的狀態。可能的值為 **SIM_A** 或 **SIM_B**。
SMS Storage	預設選擇 **SIM Card Only**	這是 SMS 存儲位置。目前唯一的選項是 **SIM 卡**。
Save (保存)	無	點擊 **Save (保存)**按鈕保存設定

SMS 簡訊摘要

顯示未讀簡訊、已收簡訊、剩餘簡訊，並允許編輯簡訊發送、從 SIM 卡讀取簡訊。

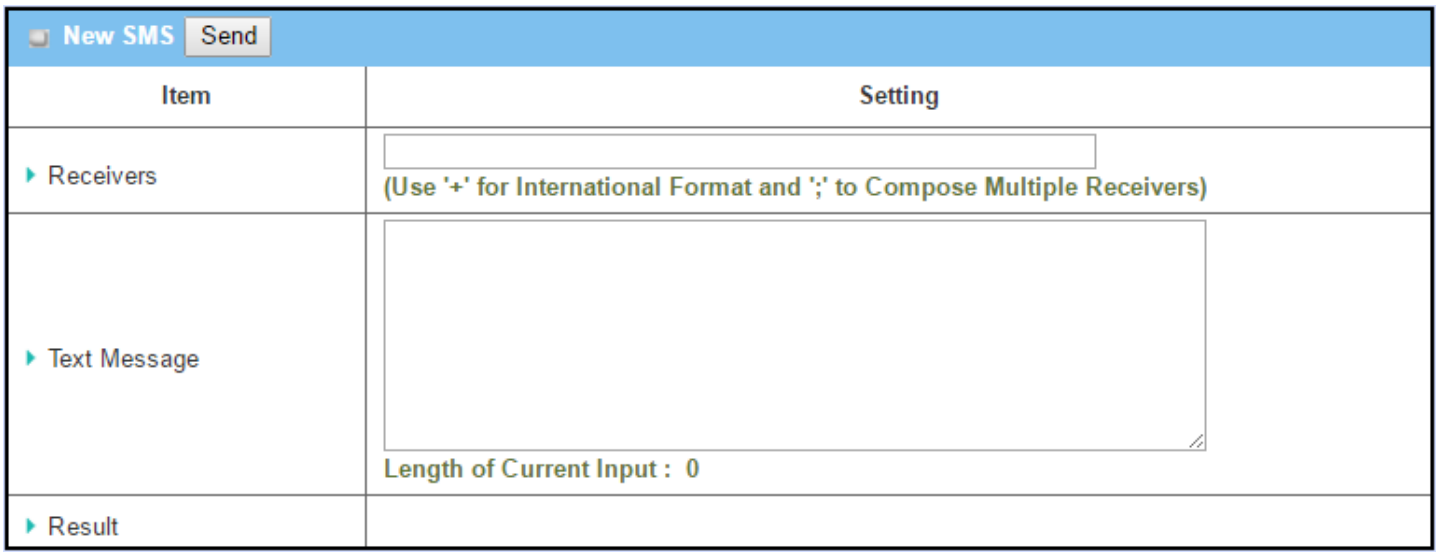


SMS Summary (簡訊摘要)		
項目	**設定值**	**說明**
Unread SMS (未讀簡訊)	無	如果是第一次插入 SIM 卡，則未讀的 SMS 值為零。當收到新的 SMS 但未讀取時，此值會增加。
Received SMS (收到的簡訊)	無	此值記錄來自 SIM 卡的 SMS 的數量。
Remaining SMS (剩餘簡訊容量)	無	此值為 SMS 總容量數減去收到的 SMS 數量。
New SMS (新建簡訊)	無	點擊 **New SMS(新建 SMS)**按鈕, 將顯示 **New SMS** 畫面。請參閱下一頁中的新 SMS。

SMS Inbox(簡訊收件匣)	無	點擊 **SMS Inbox (SMS 收件匣)**按鈕, 將顯示 **SMS Inbox** 畫面。使用者從這個畫面可以閱讀或刪除簡訊、回復簡訊或轉發簡訊。請參閱下一頁的 " SMS Inbox List (SMS 收件匣清單)" 。
Refresh (刷新)	無	點擊 **Refresh(刷新)** 按鈕更新 SMS 摘要。

新簡訊 SMS

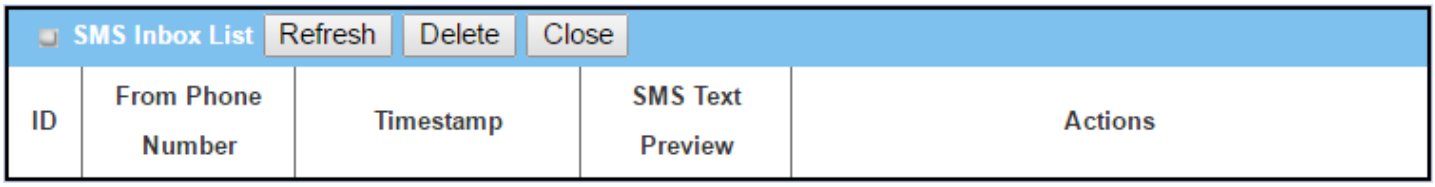
由此畫面設定 SMS。



New SMS (新建 SMS) 項目	設定值	說明
Receivers (接收器)	無	輸入 SMS 將送出的接收器。增加分號以分隔多個接收器。
Text Message (訊息內容)	無	編寫 SMS 內容。支援最大 1023 個字元的長度。
Send (送出)	無	點擊 **Send(送出)**按鈕，將文字訊息作為 SMS 發送。
Result (結果)	無	如果 SMS 已成功送出，則會顯示 **Send OK**, 否則將顯示 **Send Failed**。

SMS 簡訊收件匣列表

您可以由此列表讀取簡訊、回覆簡訊或是轉寄簡訊。



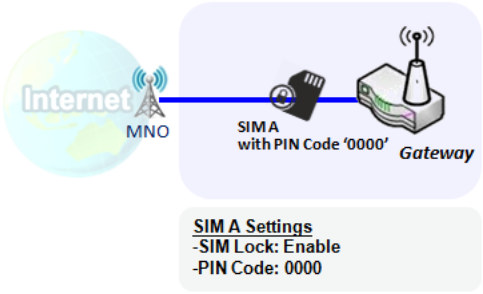
SMS Inbox List (簡訊收件匣清單) 項目	設定值	說明
ID	無	簡訊的編號。
From Phone Number (從電話號碼)	無	簡訊來源的電話號碼。
Timestamp (時間戳記)	無	收到簡訊的時間
SMS Text Preview (預覽簡訊內容)	無	預覽簡訊內容。點擊 **Detail(詳細資訊)**按鈕可閱讀內容。
Action (行動)	預設未勾選	點擊 **Detail(詳細資訊)**按鈕以讀取簡訊詳細資訊，點擊 **Reply / Forward C(回覆 / 轉發)** 按鈕以回覆 / 轉發簡訊。 勾選方框，然後點擊 Delete(**刪除)** 按鈕刪除簡訊。
Refresh (刷新)	無	刷新 "SMS 收件匣" 清單。
Delete (刪除)	無	刪除所有 Action (行動)中勾選方框的簡訊 。
Close (關閉)	無	關閉簡訊訊息詳細資訊畫面。

7.1.3 SIM PIN

在大多數情況下，使用者需要將 SIM 卡(又名 UICC)插入連線到蜂巢網路的終端設備。SIM 卡通常由移動 Mobile Operators 或 Service Provider 提供。每個 SIM 卡都有一個唯一的號碼(所謂的 ICCID)，供網路所有者或服務供應商識別每個使用者。由於 SIM 卡在服務供應商和使用者之間扮演著重要角色，SIM 卡上需要一些安全機制來防止未經授權的登入。

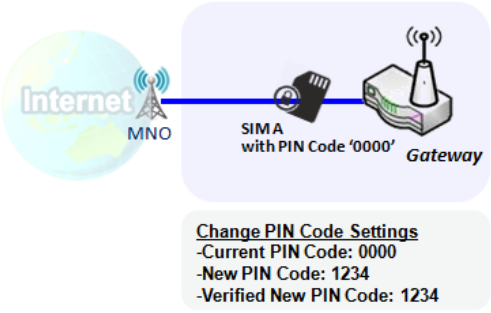
在 SIM 卡中啟用 PIN 碼是保護 Cellular 設備免受未經授權登入的簡單而有效的方式。該閘道器設備允許您透過網頁介面啓動和管理 SIM 卡的 PIN 碼。

啓用SIM卡的 PIN碼



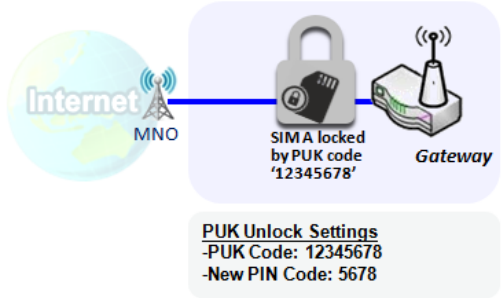
此閘道器設備允許您啓動 SIM 卡上的 PIN 碼。此示意圖顯示如何使用預設 PIN 碼 “0000” 在 3G / 4G-1 的 SIM-A 上啓用 PIN 碼。

更換SIM卡的 PIN碼



此閘道器設備允許您更改 SIM 卡上的 PIN 碼。按照示意圖，您需要輸入原始 PIN 碼 “0000” ，然後輸入新的 PIN 碼：'1234'以將新的 PIN 碼設定為'1234'。 如需要確認新的 PIN 碼，請再次在驗證的新 PIN 碼欄位中重新輸入新的 PIN 碼。

用PUK碼解鎖 SIM卡



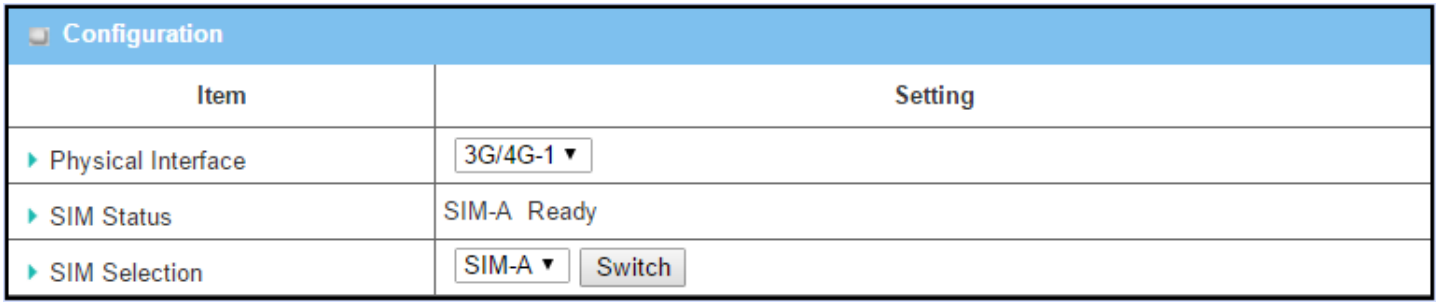
如果您在 3G / 4G-1 WAN 的設定頁面中輸入了錯誤的 PIN 碼三次以上，則 SIM 卡將被 PUK(personal unlocking key 個人解鎖密鑰)代碼鎖住。您將必須撥打服務電話獲取 PUK 碼以解鎖 SIM 卡。在圖中 PUK 碼是 “12345678” ，新的 PIN 碼是 “5678” 。

設定 SIM PIN

轉到 Service > Cellular Toolkit > SIM PIN 頁面

使用 SIM PIN 功能畫面，可以啟用或禁用 SIM 鎖定(即受 PIN 碼保護)或更改 PIN 碼。如前所述，您還可以查看有關失敗檢驗剩餘時間的資訊。如果您用完這些失敗檢驗，您將需要獲取 PUK 碼才能解鎖 SIM 卡。

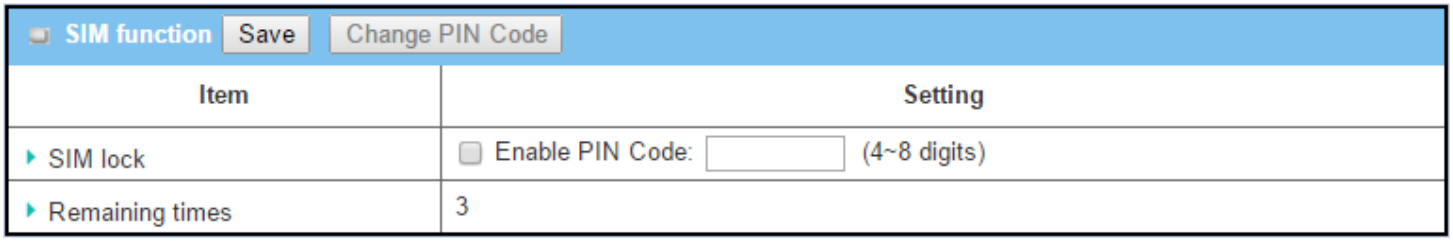
選擇 SIM 卡



Configuration Window (設定視窗)		
項目	**設定值**	**說明**
Physical Interface (實體介面)	預設選擇 **3G/4G-1**	選擇一個蜂巢介面(**3G/4G-1** 或 **3G/4G-2**) 以更改所選 SIM 卡的 SIM PIN 設定。 **注意: 3G/4G-2** 僅適用於具有雙蜂巢模組的產品。
SIM Status (SIM 狀態)	無	顯示所選的 SIM 卡和 SIM 卡的狀態。 **Ready (就緒)**、**Not Insert (未插入)**或 **SIM PIN** **Ready (就緒)**- 已插入 SIM 卡並準備使用。可能是沒有 PIN 保護的 SIM 卡, 或者 SIM 卡已經被正確的 PIN 碼解鎖。 **Not Insert (未插入)**- SIM 插槽中沒有插入 SIM 卡。 **SIM PIN** --SIM 卡受 PIN 碼的保護，而且還沒有通過正確的 PIN 碼解鎖。SIM 卡仍處於鎖定狀態。
SIM Selection (SIM 選擇)	無	選擇 SIM 卡以進一步設定 SIM PIN。 按 **Switch(開關)**按鈕, 然後閘道器會將 SIM 卡切換到另一張。

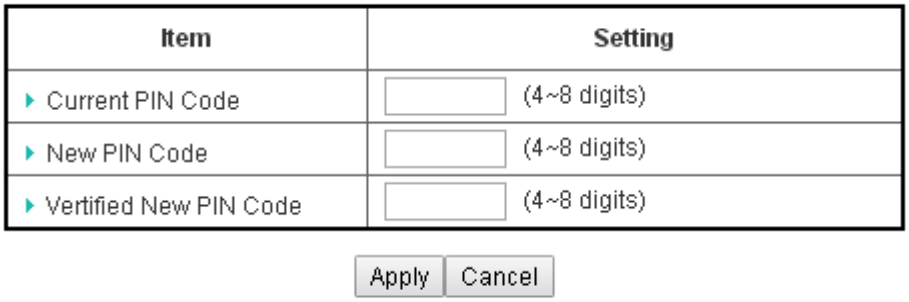
啓動/更改 PIN 碼

啟用或禁用 PIN 碼 (密碼) 功能，或甚至更改 PIN 碼功能。



SIM function Window (SIM 功能視窗)		
項目 Setting	設定值	說明
SIM lock (SIM 卡鎖)	取決於 SIM 卡	點擊 **Enable(啟用)**按鈕以啟動 SIM 卡鎖功能。 第一次要啟用 SIM 卡鎖功能時，請填寫 PIN 碼，然後點擊 **Save(保存)**按鈕以套用該設定。
Remaining times (剩餘次數)	取決於 SIM 卡	表示 SIM PIN 解鎖的剩餘試用次數。
Save (保存)	無	點擊將按鈕**保存**到應用設定.
Change PIN Code	無	點擊 **Change PIN code(更改 PIN 碼)**按鈕以更改 PIN 碼 (密碼)。 如果未啟用 **SIM 鎖**功能, 則禁用**更改 PIN 碼**按鈕。如果仍然要更改 PIN 代碼, 請首先啟用 SIM 卡鎖功能，填寫 PIN 代碼，然後點擊 Save(**保存)**按鈕以啟用。之後，您可以點擊 **Change PIN code(更改 PIN 碼)**按鈕來更改 PIN 碼。

當點擊 **Change PIN Code** (更改 PIN 碼)按鈕，出現如下畫面

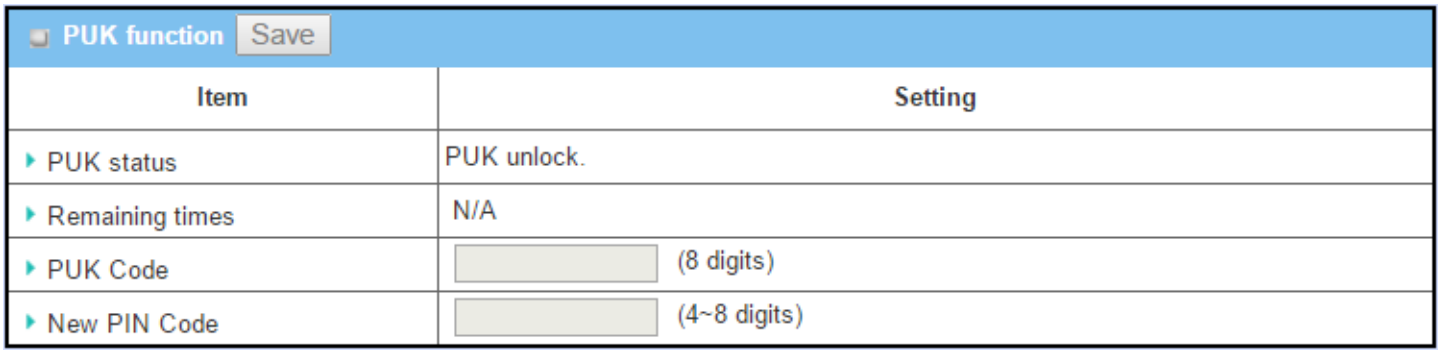


項目	設定值	說明
Current PIN Code (目前的 PIN 碼)	必要設定	輸入 SIM 卡的目前 (舊) PIN 碼。
New PIN Code(新的 PIN 碼)	必要設定	輸入新的 PIN 碼。
Verified New PIN Code (驗證新 PIN 碼)	必要設定	再次確認新的 PIN 碼。
Apply (套用)	無	點擊 **Apply(套用)**按鈕以使用新 PIN 碼更改舊 PIN 碼。
Cancel (取消)	無	點擊 **Cancel(取消)**按鈕以取消更改並保留目前 PIN 代碼。

注意：如果您更改了特定 SIM 卡的 PIN 碼，還必須更改 **Basic Network > WAN & Uplink > Internet Setup > Connection with SIM Card** 頁面中指定的 PIN 碼。否則可能會導致使用無效(舊)PIN 碼進行錯誤的 SIM PIN 碼檢驗。

用 PUK 碼解鎖

PUK 功能畫面僅可用於設定當 SIM 卡被 PUK 碼鎖定的情況。通常情況下，在使用不正確的 PIN 碼進行過多次嘗試後，SIM 卡功能表中的剩餘時間將變為 0。在此情況下，您需要聯繫服務供應商並請求獲得 SIM 卡的 PUK 碼，並使用提供的 PUK 碼解鎖 SIM 卡。透過 PUK 碼成功解鎖 SIM 卡後，SIM 鎖定功能將自動啓動。



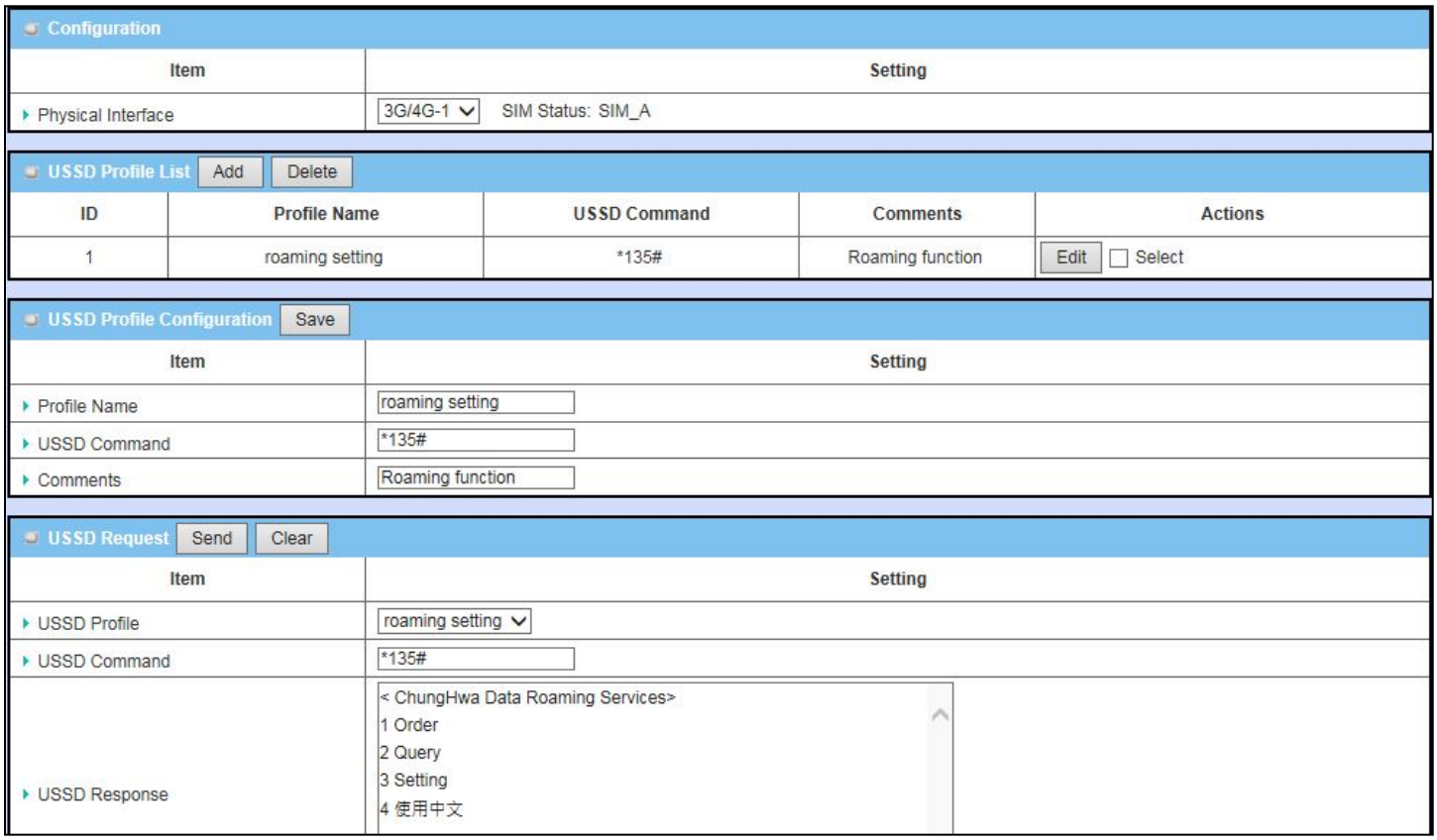
PUK Function Window (PUK 功能視窗)		
項目	**設定值**	**說明**
PUK status (PUK 狀態)	**PUK Unlock (PUK 解鎖)** / **PUK Lock (PUK 鎖住)**	顯示 PUK 狀態: **PUK Lock (PUK 鎖)**或 **PUK Unlock (PUK 解鎖)**。如前所述，SIM 卡將在過多以不正確的 PIN 碼嘗試後鎖定。在這種情況下，PUK 狀態將變為 PUK **Lock**。在正常情況下，將顯示 **PUK Unlock (PUK 解鎖)**。
Remaining times (剩餘次數)	取決於 SIM 卡	PUK 解鎖試用剩餘次數。 注意:**不允許剩餘次數達到零，它將永遠損壞 SIM 卡!** 如果你沒有的 PUK 碼，請打電話給您的 ISP 尋求協助獲得一個正確的 PUK 以解鎖 SIM。
PUK Code	必要設定	輸入可在 PUK 解鎖狀態中解鎖 SIM 卡的 PUK 碼 (8 位數位)。
New PIN Code (新的 PIN 碼)	必要設定	輸入 SIM 卡的新 PIN 碼 (4 ~ 8 位數字)。 你必須確認新的 PIN 碼以取代舊的、遺忘的。小心保管 PIN 碼 (密碼)。
Save (保存)	無	點擊 Save(**保存)**按鈕以應用該設定。

注意：如果您更改了某個 SIM 卡的 PUK 碼和 PIN 碼，還必須更改 **Basic Network** > **WAN & Uplink** > **Internet Setup** > **Connection with SIM Card** 頁面中指定的相應 PIN 碼。 否則可能會導致使用無效(舊)PIN 碼進行錯誤的 SIM PIN 碼檢驗。

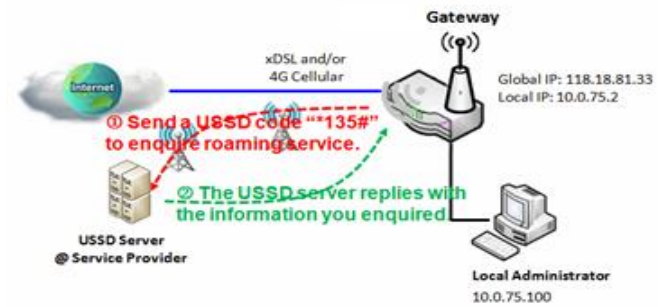
7.1.4 USSD

Unstructured Supplementary Service Data 非結構化補充服務資料(USSD)是GSM蜂巢電話用於與服務供應商電腦通信的協定。USSD可用於WAP瀏覽、預付回撥服務、行動錢包服務、本地的內容服務、選單資訊服務以及作為網路設定電話的一部分。

USSD訊息長度最多為182個字元。與簡訊服務(SMS)訊息不同，USSD訊息在USSD通信期間建立即時連線。連線保持打開狀態，允許雙向交換序列資料。 這使得USSD比使用SMS的服務更具響應能力。



USSD 方案



USSD允許您與營運商/ISP進行即時雙向通信。在該圖中，USSD命令'* 135 # '是指資料漫遊服務。將USSD命令發送給營運商後，您可以在USSD Response視窗中獲得回覆。請注意USSD命令因不同的營運商/ISP而

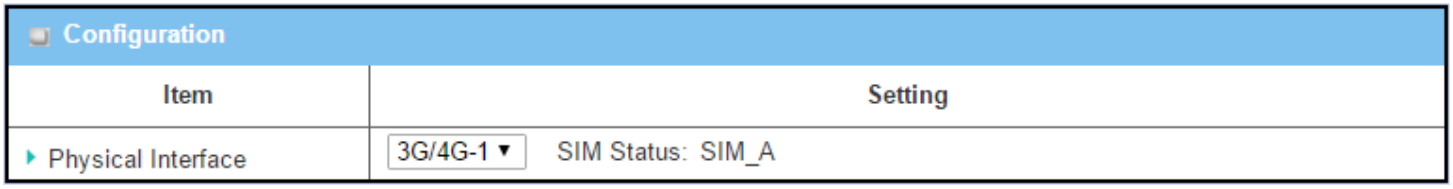
異。

設定USSD

轉到 Service > Cellular Toolkit > USSD 頁面。

在“USSD”頁面中，有四個用於USSD功能的畫面。在“Configuration (設定)”畫面中，您可以指定使用USSD的哪個3G/4G模組(實體介面)，系統將顯示模組中哪個SIM卡是目前的SIM卡。第二個畫面是“USSD Profile List (USSD 專案列表)”，顯示了所有定義的USSD專案，用於存儲用於啓動USSD階段的預命令。透過畫面中的“Add (增加)”按鈕，您可以增加一個新的USSD專案，並在第三個畫面“USSD Profile Configuration (USSD專案設定)”中定義該專案的命令。當您想要啟動USSD伺服器的USSD連線階段時，請選擇USSD專案或輸入正確的預命令，然後點擊該階段的“Send (發送)”按鈕。USSD伺服器的回覆將顯示在“USSD Command (USSD命令)”行下。當發送“USSD Command (USSD命令)”字段中輸入的命令時，收到的回覆將顯示在“USSD Response (USSD回覆)”的空白處。使用者可以透過發送USSD命令和透過閘道器獲取USSD回覆來與USSD伺服器通信。

USSD 設定

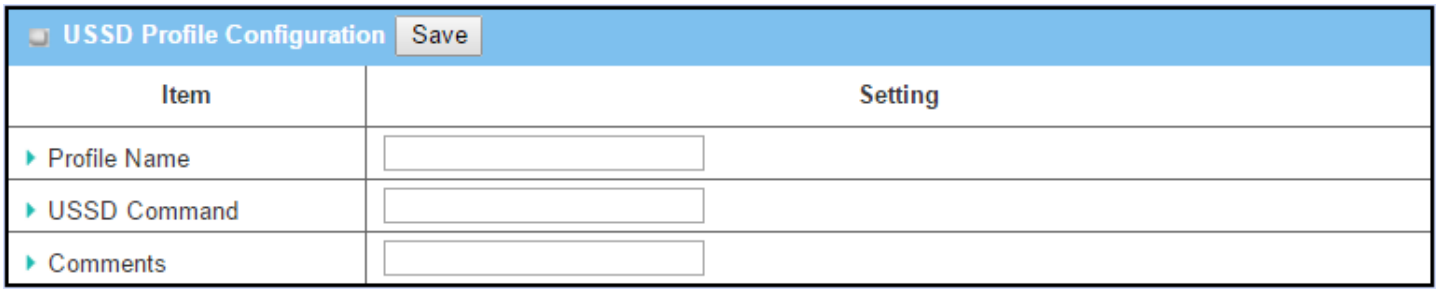


Configuration (設定) 項目	設定值	說明
Physical Interface (實體介面)	預設爲 **3G/4G-1**	選擇蜂巢介面 (**3G/4G-1** 或 **3G/4G-2**)為連線的蜂巢服務設定 USSD (標識為 **SIM_A** 或 **SIM_B**) 。 **注意: 3G/4G-2** 僅適用於具有雙蜂巢模組的產品。
SIM Status (SIM 狀態)	無	顯示已連線的蜂巢服務 (標識為 **SIM_A** 或 **SIM_B**)。

建立/編輯 USSD 專案

蜂巢閘道器允許您客製化您的 USSD 專案。 最多支援 35 個 USSD 專案。

當按下 Add (增加)按鈕，將出現 USSD Profile Configuration (USSD 專案設定)畫面

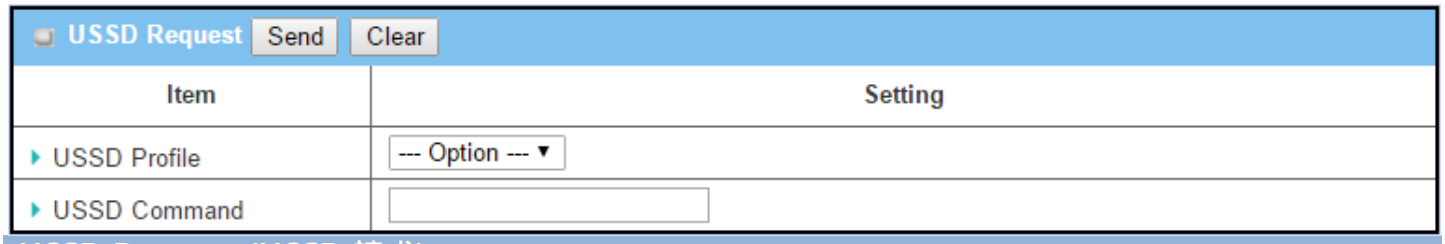


USSD Profile Configuration (USSD 專案設定)		
項目	設定值	說明
Profile Name (專案名稱)	無	輸入 USSD 專案的名稱。
USSD Command (USSD 指令)	無	輸入為專案定義的 USSD 命令。 通常是一個由數字鍵盤 "0 ~ 9", "*" 和 "#" 組成的命令字串。USSD 命令與蜂巢服務高度相關，請與聯絡服務提供者以瞭解詳細資訊。
Comments (註解)	無	為專案輸入簡短註解。

發送 USSD 請求

當您發送 USSD 命令時，將出現 USSD 回覆畫面。

當點擊 **Clear** (清除)按鈕時，USSD 回覆將消失。



USSD Request (USSD 請求) 項目	設定值	說明
USSD Profile (USSD 專案)	無	從下拉清單中選擇一個 USSD 的專案名稱。
USSD Command (USSD 指令)	無	所選專案的 USSD 命令字串將顯示在此處。
USSD Response (USSD 回應)	無	點擊 Send(**發送)**按鈕發送 USSD 命令，將顯示 **USSD Response (USSD 回覆)**畫面。您將看到相關服務的回覆訊息，接收服務簡訊。

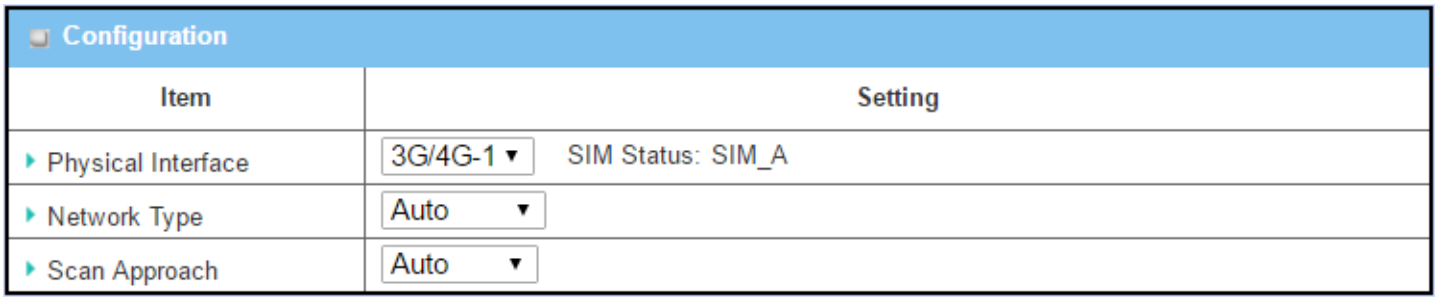
7.1.5 網路掃描

“Network Scan 網路掃描” 功能可讓管理員指定設備如何連線到行動通信系統，以便為每個3G/4G介面進行資料通信。例如，管理員可以指定使用哪一代行動通信系統進行連線，即2G，3G或LTE。此外可以定義連線順序以連線到行動通信系統。管理員還可以手動掃描可用的行動通信系統，然後選擇操作目標系統並套用它。

設定網路掃描

轉 **Service** > **Cellular Toolkit** > **Network Scan** 頁面。
在 “Network Scan (網路掃描)” 頁面中，有兩個網路掃描功能畫面。在 “Configuration (設定)” 畫面中，您可以選擇使用哪個3G/4G模組(實體介面)來執行網路掃描，系統將在模組中顯示目前使用的SIM卡。您可以一個一個地執行網路掃描來設定每個3G/4G WAN介面。您還可以指定2G/3G/LTE行動通信系統的連線順序。

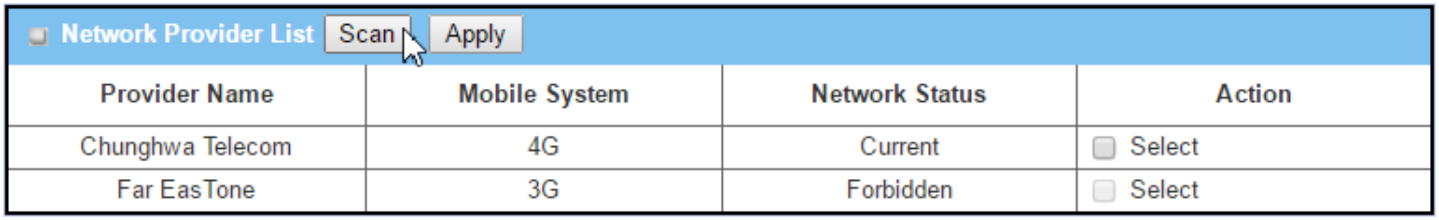
網路掃描配置



Configuration (設定) 項目	設定值	說明
Physical Interface (實體介面)	預設勾選 **3G/4G-1**	選擇一個蜂巢介面 (**3G/4G-1** 或 **3G/4G-2**)用於網路掃描功能。 注意: **3G/4G-2** 僅適用於具有雙蜂巢模組的產品。
SIM Status	無	顯示已連線的蜂巢服務 (標識為 **SIM_A** 或 **SIM_B**)。
Network Type	預設選擇 **Auto(自動)**.	指定網路掃描功能的網路類型。 可能是 Auto、2G Only 、2G prefer、3G Only、3G prefer 或 LTE Only。 當選擇 Auto(**自動)**後，網路將自動註冊; 如果選擇 **prefer(優先)**時，將首先以您的選項註冊網路; 如果選擇 Only(**僅)**時，則只以您的選項註冊網路。
Scan	預設選擇 **Auto(自動)**.	當選擇 **Auto(自動)**時，蜂巢模組將自動註冊。

Approach		如果選擇 **Manually(手動)**選項，將出現 **Network Provider List** (網路供應商列表)畫面。按 **Scan(掃描)**按鈕掃描最近的站點。選擇 (勾選該框) 想選的站點然後點擊 **Apply(套用)**按鈕套用設定。
Save (保存)	無	點擊 Save(**保存)**保存設定。

在設定畫面中選擇手動掃描方式時出現第二個畫面 “Network Provider List (網路供應商列表)” 。 點擊 “Scan (掃描)” 按鈕並等待1到3分鐘，找到的行動作業系統將顯示供您選擇。再次點擊 “Apply (套用)” 按鈕，讓系統連線到專用3G / 4G介面的行動營運商系統。



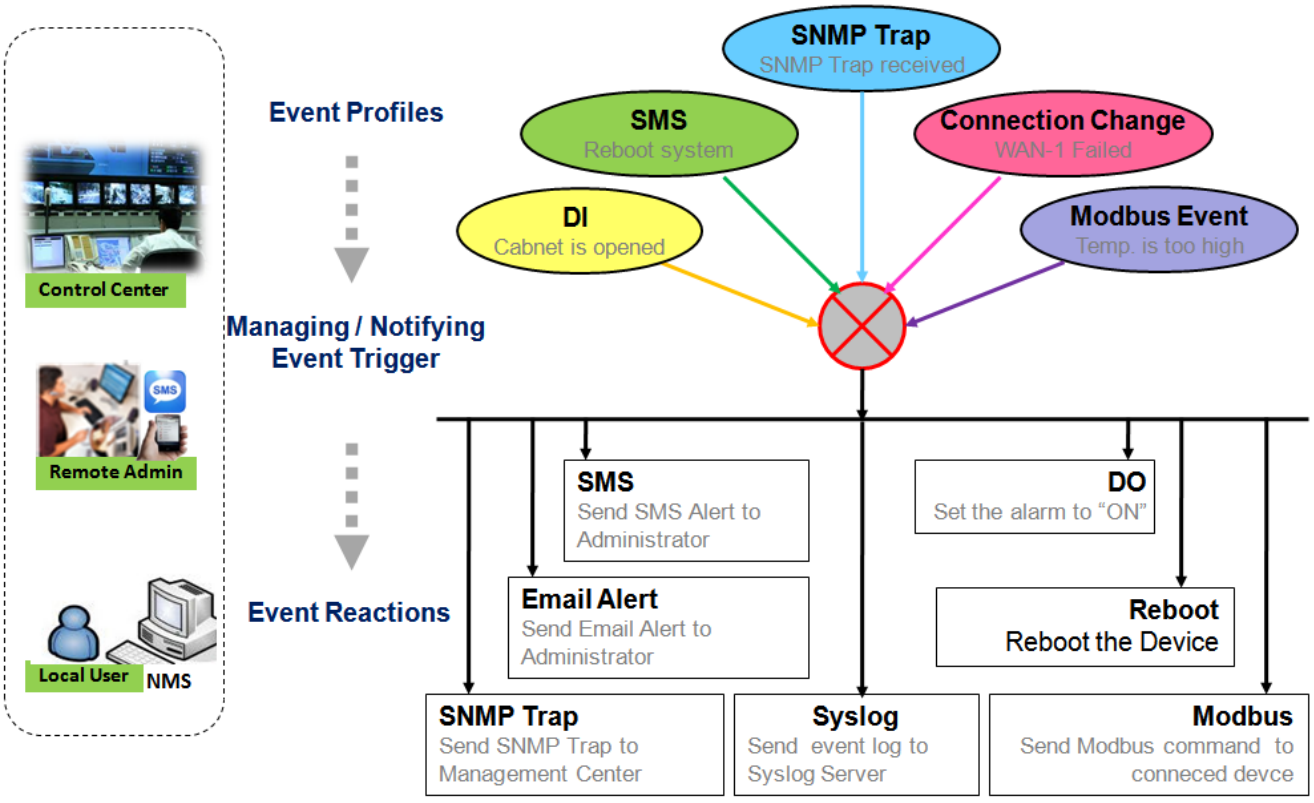
7.2 事件處理

事件處理是允許管理員設定預定義的事件，處理程序或個別專案的回覆行為的應用。透過適當的設定，管理員可以透過閘道器輕鬆地遠端獲取狀態和資訊。此外還可以處理和管理一些重要的系統相關功能，甚至連線field bus設備和D/O設備。

事件支援兩種組合：**管理事件**和**通知事件**。

管理事件是用於管理閘道器或更改閘道器特定功能的”設定/狀態”的事件。在收到管理事件後，閘道器將採取措施更改功能，收集所需的管理狀態，並更改連線的field bus設備的狀態。

通知事件是觸發某些相關物件並採取相應操作的事件。這可能是由連線的感應器或某個連線的field bus設備生成的事件。警報可以透過簡訊、電子郵件和SNMP Trap陷阱發送。



為了便於設定，管理員可以建立和編輯常見的預定義管理/通知事件專案，以便對特定事件進行即時操作或管理設備以進行進階目的。例如，閘道器日常維護、field bus設備狀態監測、數字感應器檢測控制

等發送/接收遠端管理簡訊。 所有這些管理和通知功能都可以透過事件處理功能有效地進行。

以下是提供的專案和事件的摘要列表：

(注意：可用的專案和事件會因產品型號而異。)

- 專案(規則):
  - SMS 簡訊設定和帳戶
  - 電子郵件帳戶
  - 數位輸入(DI)專案
  - 數位輸出(DO)專案
  - Modbus 管理事件專案
  - Modbus 通知事件專案

- 管理事件:
  - 觸發類型：SMS、SNMP Trap 陷阱和數位輸入(DI)。
  - 操作：獲取網路狀態; 或設定 LAN/VLAN 行為、Wi-Fi 行為、NAT 行為、防火牆行為、VPN 行為、系統管理、Administration 管理、數位輸出行為以及連線的 Modbus 設備。

- 通知事件:
  - 觸發類型：數位輸入、電源更改、連線更改(WAN、LAN & VLAN、Wi-Fi、DDNS)，Administration 管理、Modbus 和資料使用。
  - 操作：簡訊通知管理員、Syslog、SNMP Trap 陷阱或電子郵件警報通知管理員; 更改連線的數位量輸出或 Modbus 設備的狀態。

要使用事件處理功能，請啟用事件管理設定並使用提供的專案設定事件詳細資訊。您可以建立或編輯個人管理/通知事件的預定義專案。專案設定分為幾個項目; 分別是SMS帳戶定義、電子郵件服務定義、數位輸入(DI)專案設定、數位輸出(DO)專案設定和Modbus定義。

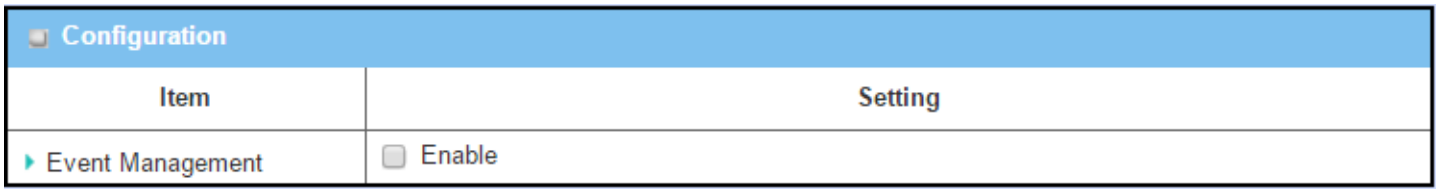
然後透過設定事件的觸發條件和事件的相對應操作來設定每個管理/通知事件。每個事件都可以同時啓動多個動作。

7.2.1 設定

轉到 Service > Event Handling > Configuration 頁面。

事件處理是允許管理員設定預先定義的事件、處理程序或個別專案的回覆行為的服務。

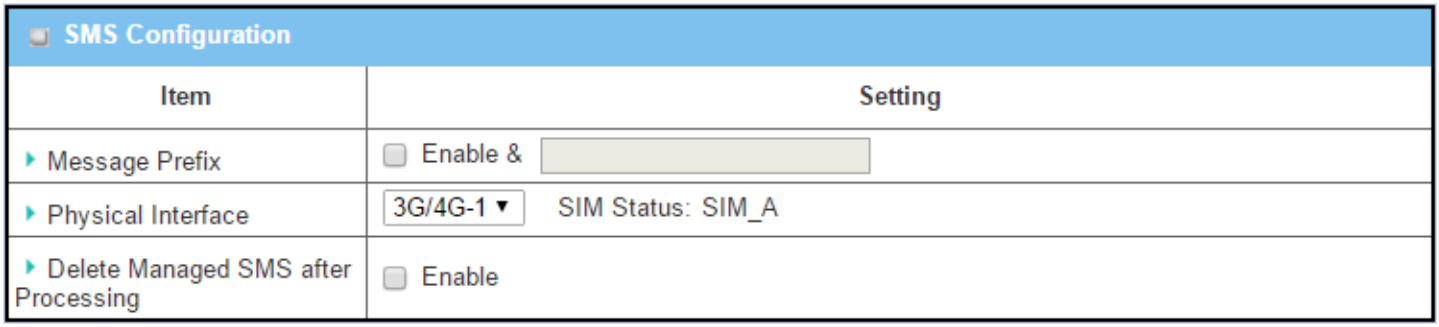
啓動事件管理



Configuration		
項目	設定值	說明
Event Management	預設未勾選	勾選 Enable 啓動 Event Management 功能。

啓動簡訊管理

要使用簡訊管理功能，請先設定這些設定。

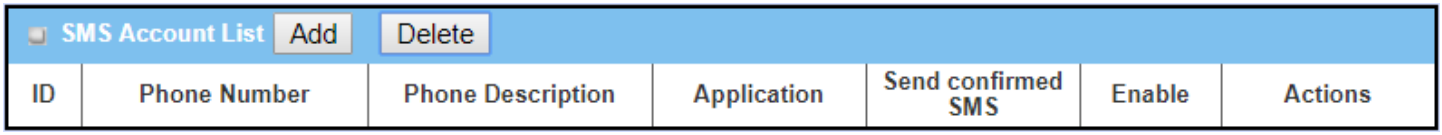


SMS Configuration (簡訊設定)		
項目	設定值	說明

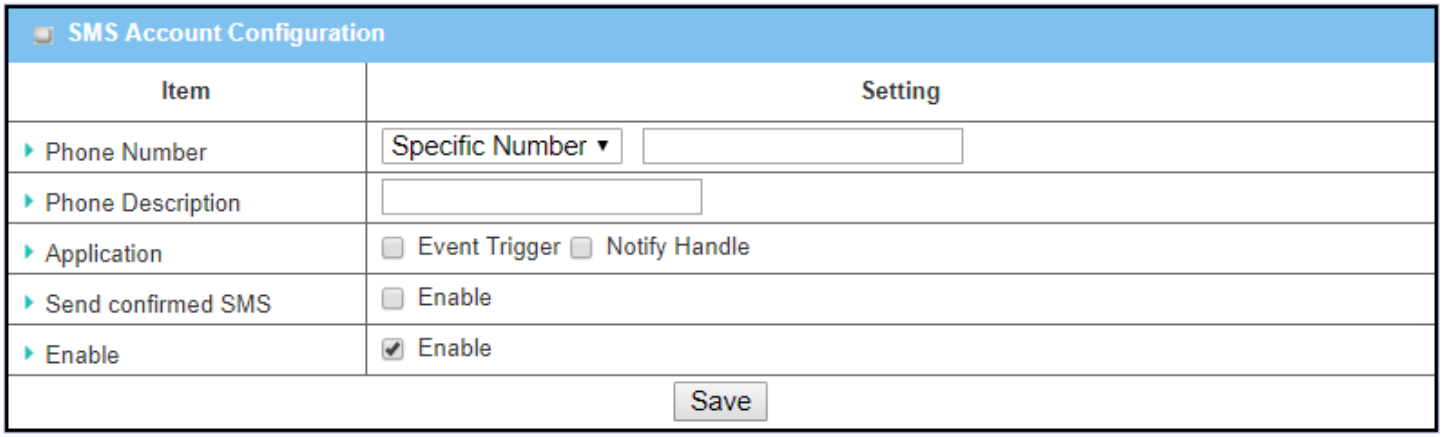
Message Prefix (訊息前綴)	預設未勾選	點擊 **Enable(啟用)**方框啟用簡訊前綴詞以驗證接收的簡訊。啟用該功能後，請在核取方框後面輸入前綴詞。 已接收管理事件的簡訊必須將指定的前綴詞作為初始識別碼，然後相對應的處理着將令未來處理的方式更有效率。
Physical Interface (實體介面)	預設勾選 3G/4G-1	選擇一個蜂巢介面 (**3G/4G-1** 或 **3G/4G-2**). 注意: **3G/4G-2** 僅適用於具有雙蜂巢模組的產品。
SIM Status (SIM 狀態)	無	顯示已連線的蜂巢服務 (標識為 **SIM_A** 或 **SIM_B**)。
Delete Managed SMS after Processing (處理後刪除簡訊)	預設未勾選	勾選 Enable(**啟用)**框可在處理後刪除收到的管理事件簡訊

建立/編輯 簡訊帳戶

設定簡訊帳戶以管理閘道器。最多支持 5 個賬戶。



點擊 **Add / Edit** (新增/編輯)按鈕以設定簡訊帳戶。

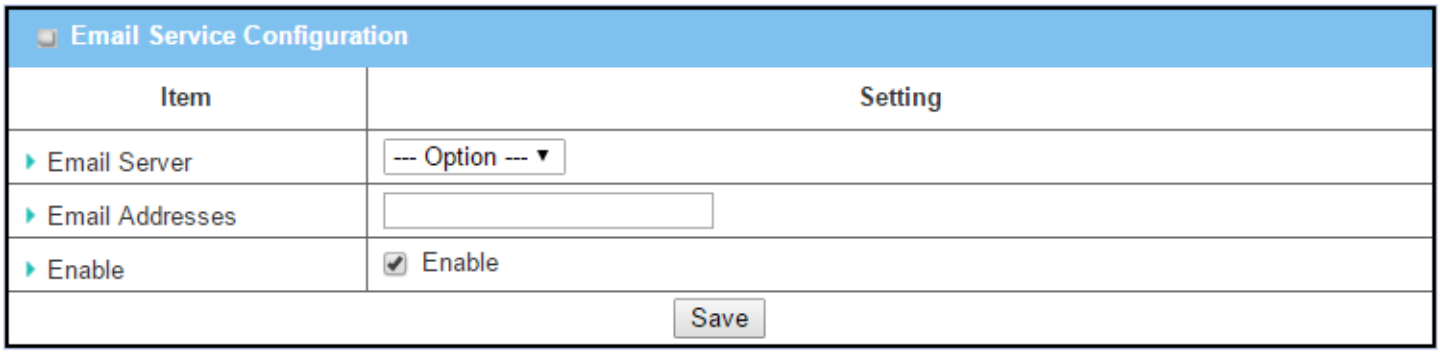


SMS Account Configuration (SMS 帳戶設定)		
項目	**設定值**	**說明**
Phone Number (電話號碼)	1. 手機電話號碼格式 2. 必要設定	從下拉清單中選擇電話號碼，如果需要，可將行動電話號碼指定為 SMS 帳戶識別碼。 可能是 **Specific Number(特定數字)**或 **Allow Any(允許任何)**。如果勾選 **Specific Number(特定編號)**，請將電話號碼指定為 SMS 帳戶識別碼。 ***範圍值*** : -1 ~ 32 位數位.
Phone Description (電號描述)	1. 任何字 2. 可選設定	簡短說明 SMS 帳戶。
Application(應用)	必要設定	指定應用程式類型。可能是 **Event Trigger (事件觸發器)**、**Notify Handle(通知控制碼)**或 **both(兩個)**。 如果電話號碼策略為 **Allow Any(允許任何)**，則 Notify Handle(通知控制)將無法勾選。
Send confirmed SMS (傳送確認簡訊)	1. 可選設定 2. 預設未勾選	點擊 Enable(**啟用)**方框啟動簡訊回覆功能。 在收到 SMS 管理事件時，閘道器將向寄件者發送確認訊息。確認的訊息類似於以下格式: " *Device received a SMS with command xxxxx. (設備接收到帶有指令的 簡訊)*"
Enable (啓動)	預設未勾選	點擊 Enable(**啟用)**方框啟動此帳戶。
Save (保存)	*無*	按下 Save (保存) 按鈕以保存設定值.

建立/編輯電子郵件服務帳戶

設定電子郵件服務帳戶以進行事件通知。最多支持 5 個賬戶。

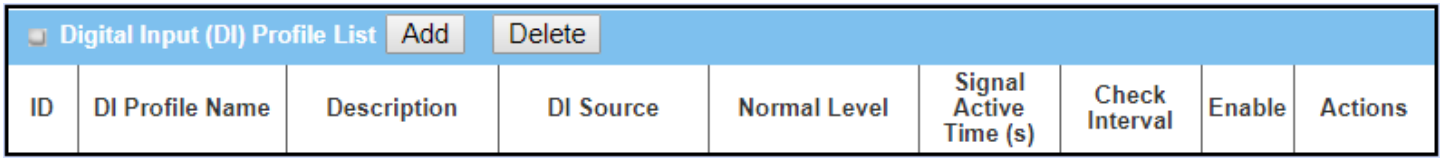
點擊 **Add / Edit** (新增/編輯) 按鈕以設定電子郵件帳戶。



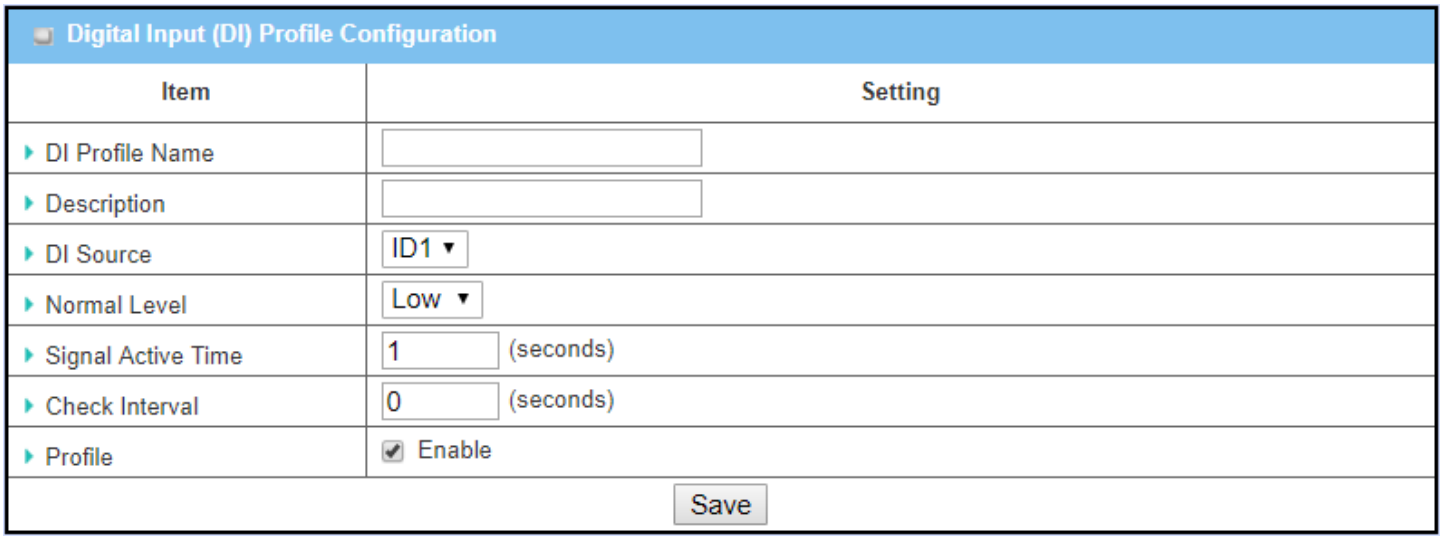
Email Service Configuration (電子郵件服務設定)		
項目	**設定值**	**說明**
Email Server	--- Option ---	從**外部伺服器**設定中選擇電子郵件帳戶設定的電子郵件伺服器設定檔。
Email Addresses	1. 網際網路 E-mail address format 2. 必要設定	指定目標電子郵件地址。
Enable	預設未勾選	點擊**啟用**方框啟動此帳戶。
Save (保存)	*無*	按下 Save (保存) 按鈕以保存設定值

建立/編輯數位輸入(DI)專案規則 (需支援 DI/DO)

設定數位輸入(DI)專案規則。最多支援 10 個專案。



當按下 Add (新增) 按鈕，將會出現 Digital Input (DI) Profile Configuration (數位輸入(DI)專案設定)畫面

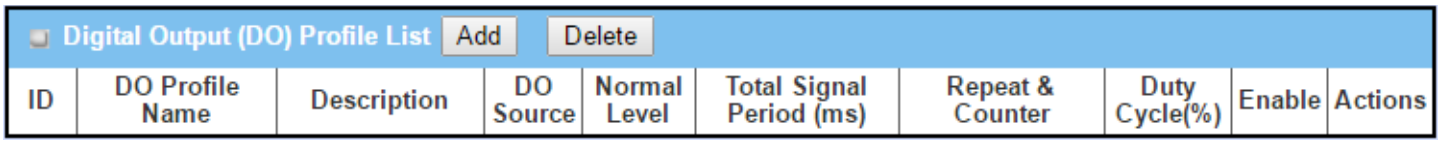


Digital Input (DI) Profile Configuration (數位輸入(DI)專案設定)		
項目	**設定值**	**說明**
DI Profile Name (DI 專案名稱)	1. 字串格式. 2. 必要設定	指定 DI 專案名稱。 ***範圍值*** : -1 ~ 32 個字元.
Description(描述)	1. 任何文字 2. 可選設定	簡要說明專案指。
DI Source (DI 來源)	預設 **ID1**	指定 DI 來源。可能是 **ID1** 或 **ID2**. 可用 DI 來源的數量將取決於產品型號。
Normal Level (正常級別)	預設 Low	指定正常級別: **Low(低)**或 **High(高)**。
Signal Active Time (信號有效時間)	1. 數字字串格式. 2. 必要設定	指定信號啟用時間。 ***範圍值*** : 1 ~ 10 秒.
Check Interval (檢查間隔)	1. 數字字串格式. 2. 必要設定 3. 預設 0	指定 DI 事件的檢查間隔。如果事件在長時間間隔內保持活動狀態，則閘道器將為每個檢查間隔發送重複的事件通知。 ***範圍值*** : 0 ~ 8640 0 秒. **注意:** 若要防止在相同情況下接收太多通知，可以將檢查間隔調整為適合您的應用程式的值。
Profile (專案)	預設未勾選	點擊 **Enable(啟用)**方框啟動此專案設定。

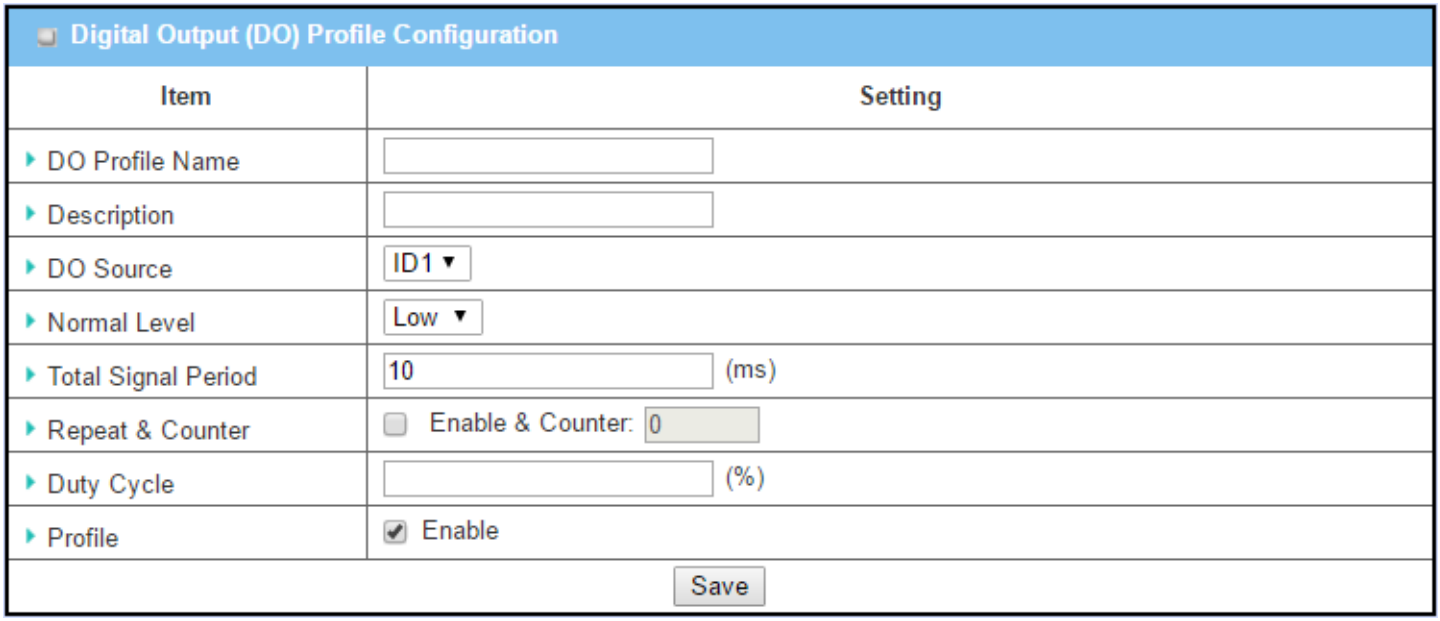
Save (保存)	*無*	按下 **Save (保存)** 按鈕以保存設定值.

建立/編輯數位輸出(DO)專案規則 **(需支援 DI/DO)**

設定數位輸出(DO)專案規則。最多支援 10 個專案。



當按下 Add (增加)按鈕，將出現 Digital Output (DO) Profile Configuration (數位輸出(DO)專案設定)畫面。



Digital Output (DO) Profile Configuration (數位輸出 (DO) 設定檔配置)		
項目	**設定值**	**說明**
DO Profile Name (DO 專案名稱)	1. 字串格式. 2. 必要設定	指定 DO 專案名稱。 ***範圍值***：-1 ~ 32 個字元.
Description(描述)	1. 任何文字 2. 可選設定	簡要說明專案指。
DO Source (DO 來源)	**ID1** 預設	指定執行來源。
Normal Level (正常級別)	預設 Low	指定正常級別: **Low(低)**或 **High(高)**。

Total Signal Period (總信號週期)	1. 數字字串格式. 2. 必要設定	指定總信號週期。 ***範圍值*** : 10 ~ 10000 毫秒
Repeat & Counter (重複 & 計數器)	預設未勾選	勾選 " Enable(啟用)" 方框啟動重複的數位輸出，並指定重複時間。 ***範圍值*** : 0 ~ 65535
Duty Cycle (工作週期)	1. 數字字串格式. 2. 必要設定	指定數位輸出的工作週期。 ***範圍值*** : 1 ~100%
Profile (專案)	預設未勾選	點擊 **Enable(啟用)**方框啟動此設定檔設定。
Save (保存)	無	按下 Save (保存) 按鈕以保存設定值.

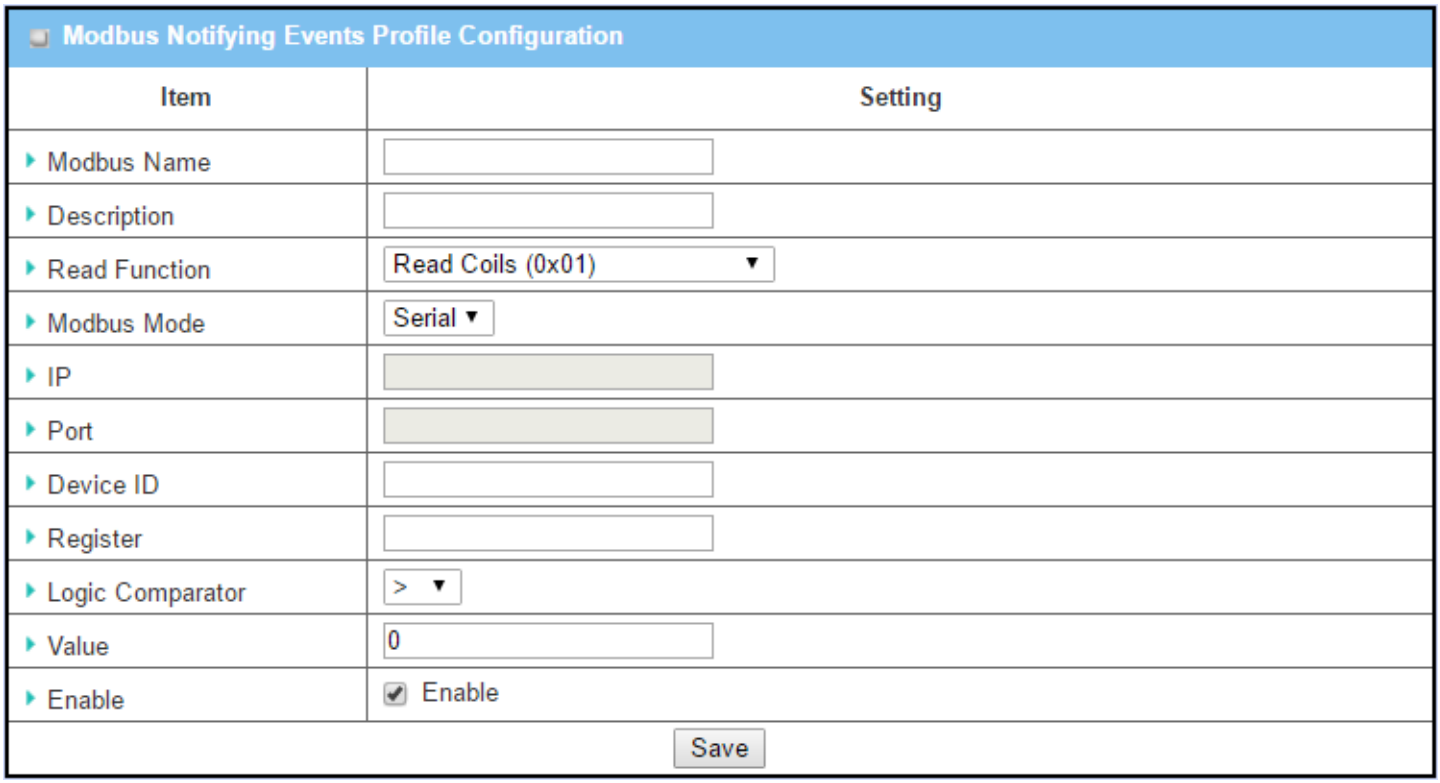
建立/編輯 Modbus 通知事件專案 (需支援 Modbus)

設定 Modbus 通知事件專案。最多支援 10 個專案。

Modbus Notifying Events Profile List [Add] [Delete]

ID	Modbus Name	Description	Read Function	Modbus Mode	IP	Port	Device ID	Register	Logic Comparator	Value	Enable	Actions
1	co2_level	read co2 level to check if it bigger than 60	Read Holding Registers (0x03)	TCP	122.22.33.44	987	78	3	>	60	☑	Edit ☐ Select

點擊 **Add / Edit(增加/編輯)**按鈕來設定專案。



Modbus Notifying Events Profile (通知事件設定檔)		
項目	**設定值**	**說明**
Modbus Name (Modbus 名稱)	1. 字串格式. 2. 必要設定	指定 Modbus 專案名稱。 ***範圍值*** : -1 ~ 32 個字元.
Description (描述)	1. 任何文字 2. 可選設定	簡要說明專案。
Read Function (讀取功能)	預設 Read Holding Registers	指定 **Notifying Events(通知事件)**的讀取功能.
Modbus Mode (Modbus 模式)	預設 **Serial**	指定 Modbus 模式: **Serial(序列)**或 **TCP**.
IP	1. Modbus 模式的序列爲無	指定 Modbus 模式 TCP 的 IP。IPv4 格式。

	2. Modbus 模式的 TCP 爲必要設定	
Port (埠)	1. Modbus 模式的序列爲無 2. Modbus 模式的 TCP 爲必要設定	指定 Modbus 模式下 TCP 埠。 ***範圍值*** : 1 ~ 65535.
Device ID (設備識別碼)	1. 數字字串格式. 2. 必要設定	指定該設備的裝置識別碼。可以從 1 到 247。
Register (註冊器)	1. 數字字串格式. 2. 必要設定	指定該設備的註冊器編號。 ***範圍值*** : 0 ~ 65535.
Logic Comparator (邏輯比較器)	預設 '>'	為**通知事件**指定邏輯比較器。可能是 ' > ', ' < ', ' = ', ' > = ', 或 ' < = '。
Value (數值)	1. 數字字串格式. 2. 必要設定	指定數值。 ***範圍值*** : 0 ~ 65535.
Enable (啓動)	預設未勾選	點擊 Enable(**啟用**)方框啟動此設定檔設定。
Save (保存)	*無*	按下 Save (保存) 按鈕以保存設定值。
Undo (還原)	*無*	按下 Undo (還原) 按鈕可將剛剛設定的內容還原回上一個設定。

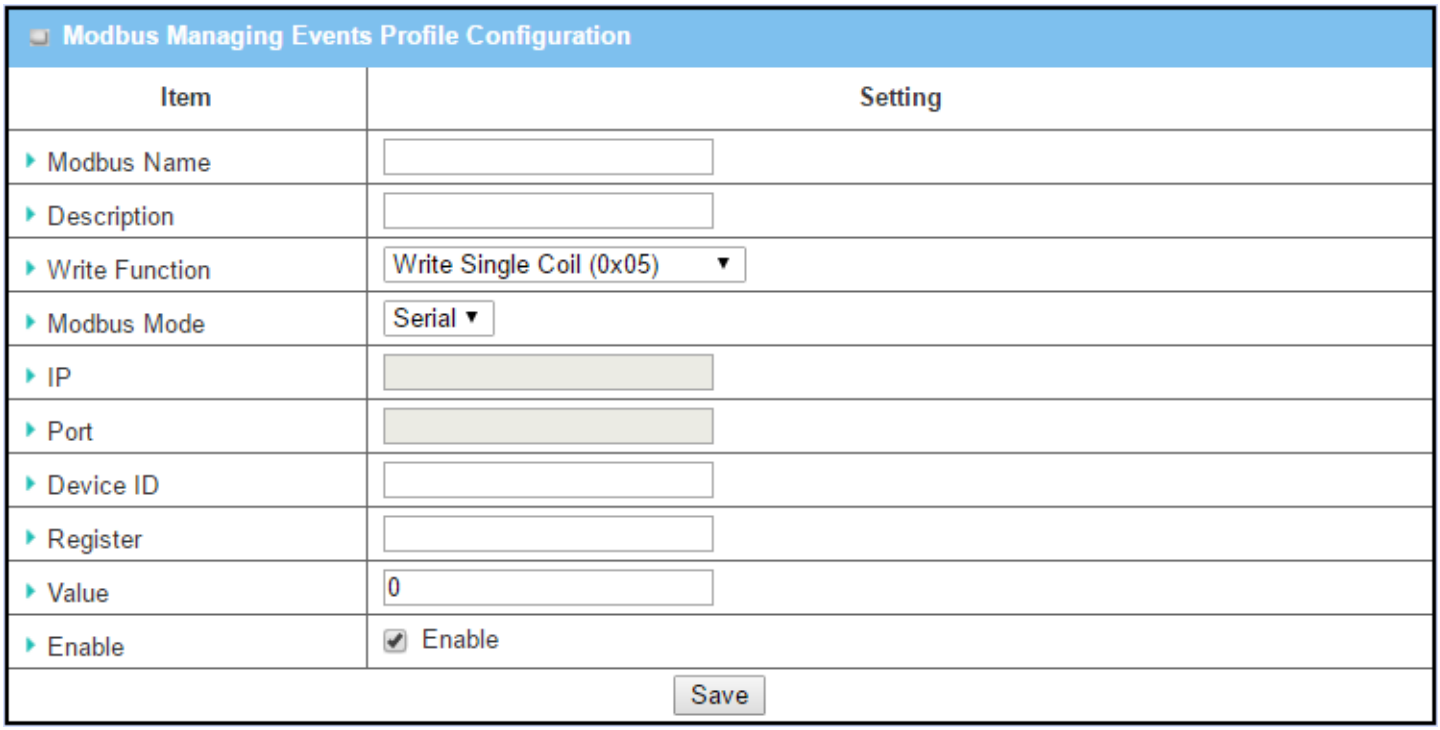
建立/編輯 Modbus 管理事件專案 (需支援 Modbus)

設定 Modbus 管理事件專案。最多支援 10 個專案。

Modbus Managing Events Profile List [Add] [Delete]

ID	Modbus Name	Description	Write Function	Modbus Mode	IP	Port	Device ID	Register	Value	Enable	Actions
1	water_pump	write water pump to control the motor speed high-low	Write Single Register (0x06)	TCP	233.44.55.66	876	247	44	5678	☑	Edit ☐ Select

您可以點擊 **Add / Edit**(增加/編輯)按鈕來設定專案。



Modbus Managing Events Profile (Modbus 管理事件設定檔)		
項目	**設定值**	**說明**
Modbus Name (Modbus 名稱)	1. 字串格式. 2. 必要設定	指定 Modbus 專案名稱。 ***範圍值*** : -1 ~ 32 個字元.
Description(說明)	1. 任何文字 2. 可選設定	簡要說明專案。
Write Function (寫入功能)	預設 Write Single Registers	指定 **Managing Events(管理事件)**的寫入功能。
Modbus Mode (Modbus 模式)	預設 **Serial**	指定 Modbus 模式: **Serial(序列)**或 **TCP**.
IP	1. Modbus 模式的序列爲無 2. Modbus 模式的 TCP	指定 Modbus 模式 TCP 的 IP。IPv4 格式。

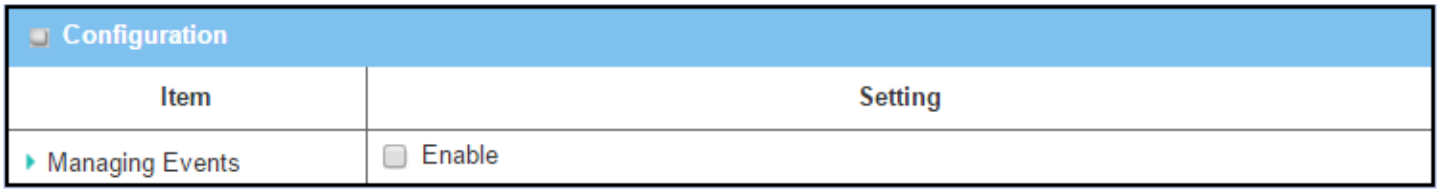
	爲必要設定	
Port (埠)	1. Modbus 模式的序列爲無 2. Modbus 模式的 TCP 爲必要設定	指定 Modbus 模式下 TCP 埠。 ***範圍值*** : 1 ~ 65535.
Device ID (設備識別碼)	1. 數字字串格式. 2. 必要設定	指定該設備的裝置識別碼。可以從 1 到 247。
Register (註冊器)	1. 數字字串格式. 2. 必要設定	指定該設備的註冊器編號。 ***範圍值*** : 0 ~ 65535.
Value (數值)	1. 數字字串格式. 2. 必要設定	指定數值。 ***範圍值*** : 0 ~ 65535.
Enable (啓動)	預設未勾選	點擊 Enable(**啟用**)方框啟動此設定檔設定。
Save (保存)	*無*	按下 Save (保存) 按鈕以保存設定值。
Undo (還原)	*無*	按下 Undo (還原) 按鈕可將剛剛設定的內容還原回上一個設定。

7.2.2 管理事件

管理事件允許管理員定義事件觸發器、處理程序和回覆之間的關係(規則)。

轉到 Service > Event Handling > Managing Events 頁面。

啓動管理事件



Configuration (設定)		
項目	**設定值**	**說明**
Managing Events (管理事件)	預設未勾選	勾選 Enable (啓動)Managing Events (管理事件)功能。

建立/編輯管理事件規則

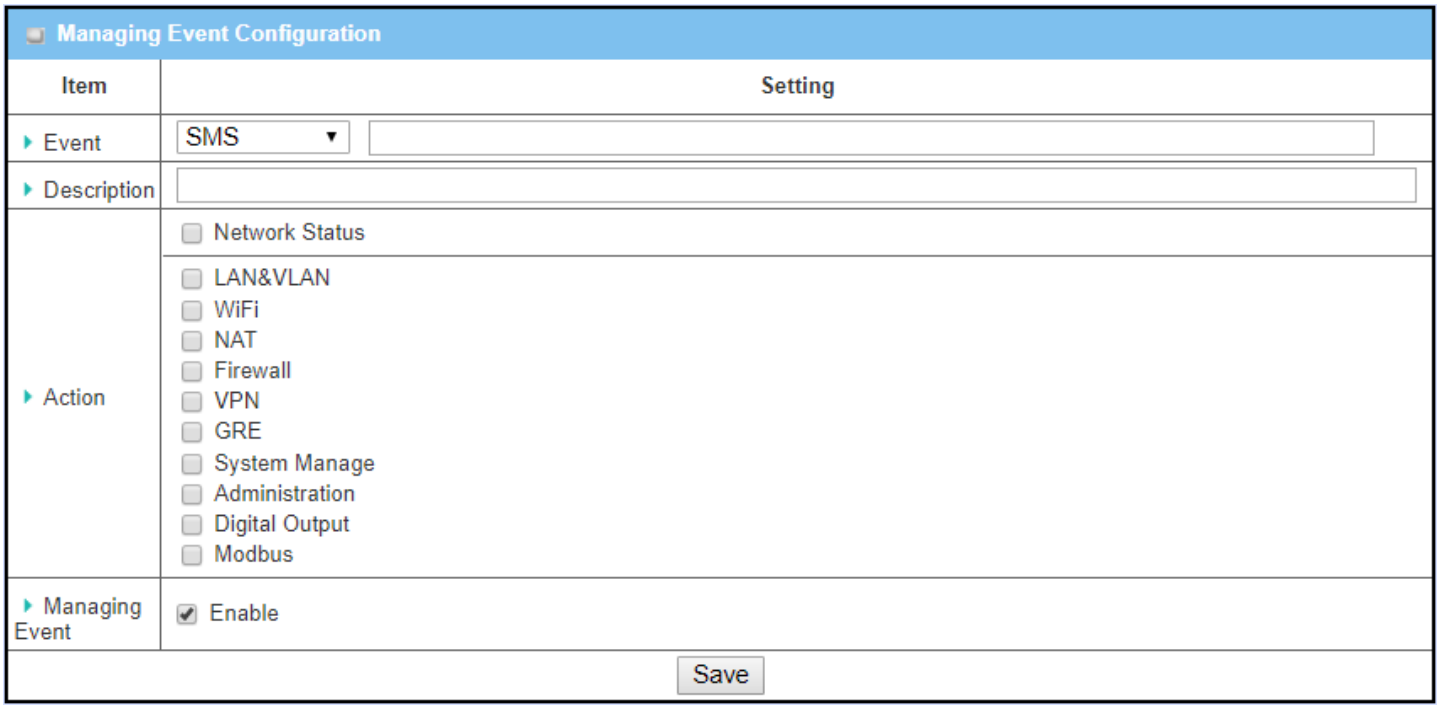
設定管理事件規則。最多支援 128 條規則。

Managing Event List Add Delete

ID	Event	Description	Enable	Actions
1	SMS	Get the Network Status from device	☑	Edit Select
2	SMS	Connect cellular WAN connection	☑	Edit Select
3	SMS	Disconnect cellular WAN connection	☑	Edit Select
4	SMS	Switch Cellular WAN Connecting by SIM-A	☑	Edit Select
5	SMS	Switch Cellular WAN Connecting by SIM-B	☑	Edit Select
6	SMS	Turn On the WiFi	☐	Edit Select
7	SMS	Turn Off the WiFi	☐	Edit Select
8	SMS	Enable SSH login from WAN	☐	Edit Select
9	SMS	Disable SSH login from WAN	☐	Edit Select
10	SMS	Enable TR-069 manage function	☐	Edit Select
11	SMS	Disable TR-069 manage function	☐	Edit Select
12	SMS	Backup config	☑	Edit Select
13	SMS	Restore specific config	☑	Edit Select
14	SMS	Reboot System Immediately	☑	Edit Select
15	SMS	Save current configuration as default	☑	Edit Select

如上面的畫面所示，有一些預先定義的 SMS 事件規則。您可以透過點擊 Edit(編輯)按鈕來設定，並啟用或禁用每個相應的規則。

當按下 Add(增加)或 Edit(編輯)按鈕時，將出現 Managing Event Configuration (管理事件設定)畫面。



Managing Event Configuration (管理事件設定)		
項目	**設定值**	**說明**
Event (事件)	預設 **SMS** (或 **SNMP Trap**)	指定事件種類 (**SMS**、 **SNMP Trap 陷阱**或 **Digital Input 數位輸入**) 和事件識別碼/專案。 **SMS**：選擇 **SMS** 並在文字方塊中輸入訊息作為事件的觸發條件; **SNMP**：選擇 **SNMP Trap 陷阱**並在文字方塊中輸入訊息以指定 SNMP Trap 陷阱事件; **Digital Input(數位輸入)**: 選擇**數位輸入**，您定義用於指定某個 DI 數位輸入事件的 DI 專案; *注意: 可用的事件種類將取決於產品型號。*
Description(說明)	字串格式: 任意文字.	簡要說明管理事件。
Action (動作)	預設未勾選.	指定 **Network Status(網路狀態)**， 或者至少在觸發預期您定義用於指定某個 DI 數位輸入事件的 DI 專案;事件時採取某個操作。 **Network Status(網路狀態)**: 選擇 **Network Status(網路狀態)**核取方框以網路狀態作為事件的動作; **LAN & VLAN**：選擇 **LAN & VLAN** 核取方框和相關的子項 (On/Off(開/關)), 閘道將更改設定作為事件的動作;

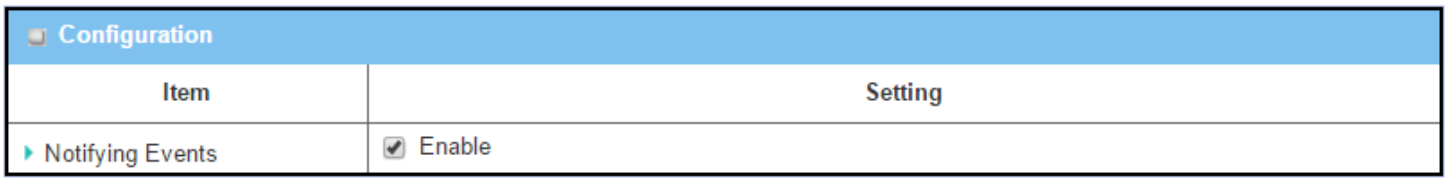
		Wi-Fi : 選擇 **Wi-Fi** 核取方框和相關的子項 (Wi-Fi radio On/Off (**Wi-Fi** 無線電開/關)), 閘道將更改設定為事件的動作; **NAT** : 選擇 **NAT** 核取方框和相關的子項 (Virtual Server Rule On/Off(虛擬伺服器規則開/關), DMZ On/Off(DMZ 開/關))，閘道器將更改設定作為事件的動作; **Firewall(防火牆)**: 選擇 **Firewall(防火牆)**核取方框和相關的子項 (Remote Administrator Host ID On/Off(遠端系統管理員主機識別碼 開/關))，閘道器將設定更改為事件的動作; **VPN** : 選擇 **VPN** 核取方框和相關子項 (IPsec Tunnel ON/Off(IPsec 通道開/關)、PPTP Client On/Off(PPTP 客戶端開/關)、 L2TP Client On/Off(L2TP 客戶端開/關)、OpenVPN Client On/Off(OpenVPN 客戶端開/關))，閘道將更改設定作為事件的動作; **GRE** : 選擇 **GRE** 核取方框和相關子項 (GRE Tunnel On/Off (GRE 通道開/關)), 閘道器將更改設定作為事件的動作; **System Manage(系統管理)**: 選擇 **System Manage(系統管理)**核取方框和相關的子項 (WAN SSH Service On/Off(**WAN SSH** 伺服器開/關)), 閘道將更改設定作為事件的動作; **Administration(管理)**: 選擇 **Administration(管理)**核取方框和相關的子項 (Backup Config(備份設定)、Restore Config(還原設定)、Reboot(重新開機)、Save Current Setting as Default(將目前設定保存為預設值)), 閘道將將設定更改為事件的動作; **Digital Output(數位輸出)**: 選擇 **Digital Output(數位輸出)**核取方框，您定義用於指定某個 DO 數位輸出事件的 DO 專案; **Modbus**: 選擇 **Modbus** 核取方框和 Modbus 管理事件專案，將設定更改為事件的動作; *注意: 可用的事件種類將取決於產品型號。*
Managing Event (管理事件)	預設未勾選	點擊 **Enable(啟用)**方框啟動此管理事件設定。
Save (保存)	*無*	按下 Save (保存) 按鈕以保存設定值
Undo (還原)	*無*	按下 Undo (還原) 按鈕以還原上一個設定值.

7.2.3 通知事件

轉到 Service > Event Handling > Notifying Events 頁面。

通知事件設定允許管理員定義事件觸發器和處理程序之間的關係(規則)。

Enable Notifying Events



Configuration		
項目	設定值	說明
Notifying Events	預設未勾選	勾選 Enable 啓動 Notifying Events 功能。

建立/編輯通知事件規則

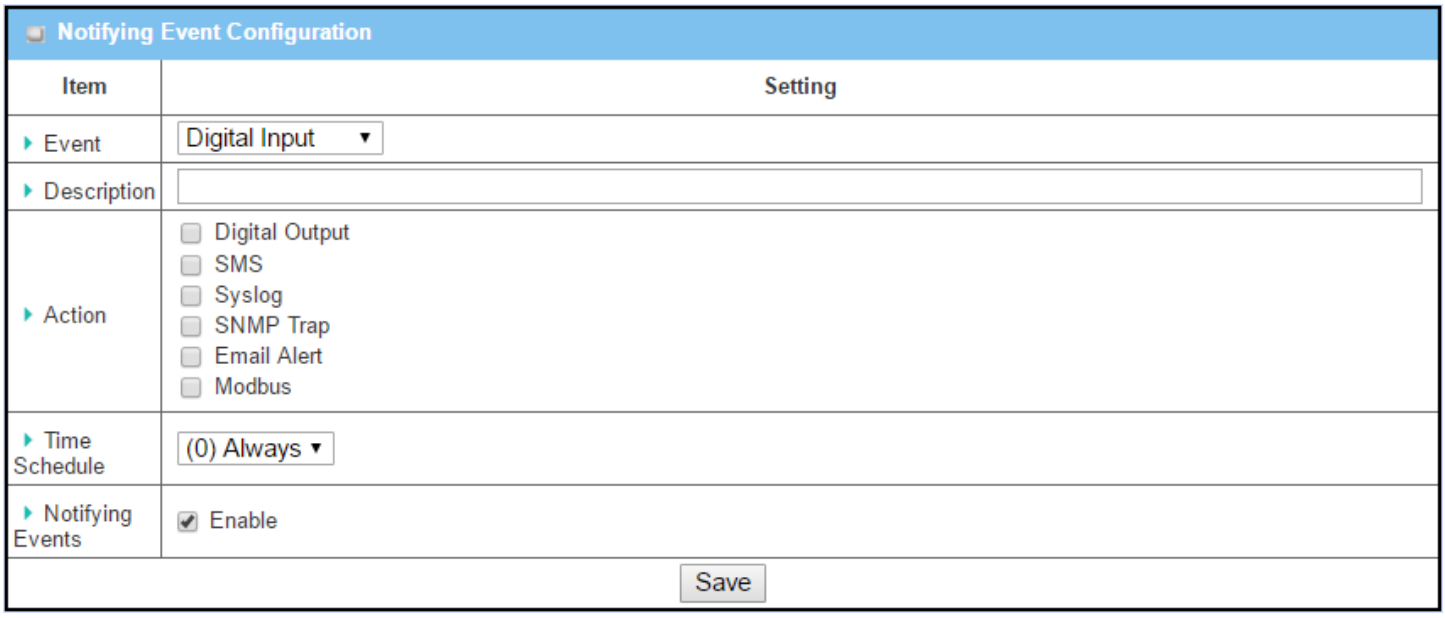
設定您的通知事件規則。 支援多達 128 條規則。

Notifying Event List Add Delete

ID	Event	Description	Action	Enable	Actions
1	WAN	Send alert SMS to Admin once the Primary WAN link is Up	SMS		Edit Select
2	WAN	Send alert SMS to Admin once the Primary WAN link is Down	SMS		Edit Select
3	WAN	Send alert SMS to Admin once the Backup WAN link is Up	SMS		Edit Select
4	WAN	Send alert SMS to Admin once the Backup WAN link is Down	SMS		Edit Select
5	WAN	Send alert SMS to Admin once the Dial-up Fail 5 Times	SMS		Edit Select
6	WAN	Send alert SMS to Admin once the SIM Switching occurred	SMS		Edit Select
7	WiFi	Send the SMS and SNMP Trap out to Admin when WiFi Module Up	SMS ; SNMP Trap		Edit Select
8	WiFi	Send the SMS and SNMP Trap out to Admin when WiFi Module Down	SMS ; SNMP Trap		Edit Select
9	Administration	Send the SMS to Admin when Firmware Upgrade is under processing	SMS		Edit Select

如上面的畫面所示，有一些預先定義的通知事件規則。您可以透過點擊 Edit(編輯)按鈕來設定，並啟用或禁用每個相應的規則。

當按下 Add(增加)或 Edit(編輯)按鈕時，將出現 **Notifying Event Configuratio**(通知事件設定)畫面。



Notifying Event Configuration (通知事件設定)		
項目	**設定值**	**說明**
Event (事件)	預設 **Digital Input** (或 **WAN**)	指定事件種類和相應的事件配置。支援的事件種類為: **Digital Input(數位輸入)**: 選擇 **Digital Input(數位輸入)**，您定義用於指定某個 DI 數位輸入事件的 DI 專案; **Power Change 電源更改**: 選擇 **Power Change(電源更改)**和觸發條件以指定電源上的事件。 **WAN** : 選擇 **WAN** 和一個觸發條件來指定某個 WAN 事件; **LAN & VLAN** : 選擇 **LAN & VLAN** 和觸發條件以指定特定的 LAN & VLAN 事件; **Wi-Fi** : 選擇 **Wi-Fi** 和觸發條件以指定某種 Wi-Fi 事件; **DDNS** : 選擇 **DDNS** 和一個觸發條件來指定特定的 DDNS 事件; **Administration(管理)**: 選擇 **Administration(管理)**和觸發條件以指定特定的管理事件; **Modbus**: 選擇您所定義的 Modbus 和 Modbus 通知事件專案以指定某個 Modbus 事件; **Data Usage(資料使用)**: 選擇**資料使用**，SIM 卡 (蜂巢伺服器) 和觸發條件以指定某一資料使用事件; *注意: 可用的事件種類將取決於產品型號。*
Description(說	字串格式: 任意文字.	輸入通知事件的簡短說明。

明)		
Action (動作)	預設未勾選.	指定在觸發預期事件時至少要執行的一個動作。 **Digital Output(數位輸出)**: 選擇 **Digital Output(數位輸出)**核取方框，您定義用於指定某個 DO 數位輸出事件的 DO 專案; **SMS**：選擇 **SMS**, 閘道將向所有已定義的 SMS 帳戶發送簡以作為事件的動作; **Syslog(日誌)**：選擇 **Syslog（日誌)**並勾選/取消勾選 " Enable(啟用)" 核取方框作為事件的動作; **SNMP Trap(陷阱)**: 選擇 **SNMP Trap(陷阱)**, 閘道器將向已定義的 SNMP 事件接收器發送 SNMP Trap 陷阱作為事件的動作; **Email Alert (電子郵件警報通知)**: 選擇 **Email Alert (電子郵件警報通知)**，閘道將發送電子郵件到已定義的電子郵件帳戶作為事件的動作; **Modbus**: 選擇您所定義的 Modbus 和 Modbus 通知事件專案以指定某個 Modbus 事件; *注意: 可用的事件種類將取決於產品型號。*
Time Schedule (時程表)	預設選擇**(0) Always**	選擇通知事件時程表規則。
Notifying Events (通知事件)	預設未勾選	點擊 **Enable(啟用)**方框啟動此通知事件設定。
Save (保存)	*無*	按下 Save (保存) 按鈕以保存設定值
Undo (還原)	*無*	按下 Undo (還原) 按鈕以還原上一個設定值.

規格

行動通訊介面	
標準	Cellular 頻段: (參閱訂單資訊中的選配頻段) 4G LTE: FDD-LTE, TDD-LTE 3G: WCDMA 2G: GSM/EDGE
天線接頭	2 x SMA 公
SIM Slots	2

WLAN 介面	
WiFi	802.11 a/b/g/無 c 2T2R (2.4G/5GHz 可選)
頻率 Frequency Band	歐洲 / CE 2.4 GHz (13 個通道) 5GHz (4 個通道) 美國 / FCC 2.4GHz (11 個通道) 5GHz (9 個通道) 臺灣 / NCC 2.4GHz(11 個通道) 5GHz (9 個通道) 新加坡 / iDA 2.4GHz (13 個通道) 5GHz (9 個通道)
加密安全性	WEP、WPA 1/2-PAK & WPA 1/2 (8 x VAP / SSID)
天線接頭	2 x SMA 母

EW50 行動通訊 LTE 閘道器

區域網	
Standard	IEEE 802.3 10Base-T IEEE802.3u 100BASE-TX/100BASE-FX IEEE802.3ab 1000BASE-T IEEE802.1x, 全雙工流控制
Ports	1 x RJ45 GE (WAN/LAN configurable) + 4*RJ45 GE
Physical Layer	10/100/1000Base-T
序列	
埠 Ports	1 x RS-232/RS-485

I/O	
Digital I/O	1 x DI (“Logic 0”: 0~2V, “Logic 1”: 5V~30V), 1 x DO (中繼模式, 最高 30V / 1A)

USB	
標準	USB 2.0
Ports	1 x USB Type A

功能	
Wi-Fi LAN	AP 路由器, WDS, WDS 混合模式
VLAN	埠基礎, 標記基礎 VLAN
Port Forwarding	虛擬伺服器/電腦, DMZ 主機, PPTP/L2TP/IPSec 直通
路由	靜態, 動態: RIP1/RIP2, OSPF, BGP
QoS	策略基礎的頻寬控制和 資料封包優先順序
虛擬 COM	RFC 2217, TCP 使用者端, TCP 伺服器, UDP
Modbus	Modbus 從站; Modbus 閘道 於 Modbus TCP,

	Modbus RTU/ASCII 主/從 登入
VPN	IPSec, OpenVPN, PPTP, L2TP, GRE
防火牆	具有隱形模式的 SPI 防火牆, IPS
事件處理	管理/通知事件; DI, DO, Modbus, SMS, 系統日誌, SNMP 陷阱, Email 警報, 重新開機
裝置管理解決方案	eVue (Q4, 2018)

電源	
備援輸入電源	2 x DC 12V ~ 48V (終端輸入盒)
功耗	最大 20W

EW50 行動通訊 LTE 閘道器

實體	
尺寸 (W x D x H)	62 x 125 x 160mm (不含掛載套件) 62 x 135 x 160mm (含 DIN Rail 導軌套件) 200 x 125 x 65mm (含 Bracket 套件)
重量	1.2 公斤 (2.64 磅)
掛載	DIN-導軌 / 壁掛

環境	
工作溫度	-30 至+70°C (-22 至 +158°F)
貯存溫度	-40 至 +85°C (-40 至 +185°F)
相對濕度	5% 至 95% (non-condensing)

法規批准	
GSM/UMTS	PTCRB (Q4, 2018)
Emissions/ Immunity	CE / FCC / NCC BSMI / iDA
安規	EN 60950-1 EN 62368-1:2014

聯絡資訊

益網科技股份有限公司

EtherWAN System, Inc.

www.etherwan.com

USA Office

2301 E. Winston Road
Anaheim, CA 9280
Tel: +1-714-779-3800
Email: info@etherwan.com

環太平洋辦公室

231 新北市新店區寶橋路 235 巷 6 弄 2 號 8 樓
Tel: +886 -2- 6629-8986
Email: info@etherwan.com.tw

EW50 行動通訊 LTE 閘道器
2019/08/07