# CERIO Corporation

# CS-34816XG

## 4 埠 SFP+10Gigabit + 16 埠 SFP Gigabit + 8 埠 Combo Gigabit L2/L3 Lite 加強管理型光纖網路交換器

# 使用手冊

| Web管理頁面 / 登入資訊 | |
|---|---|
| 預設IP位址 | 192.168.2.200 |
| 使用者名稱 | root |
| 登入密碼 | default |

**FCC Warning**

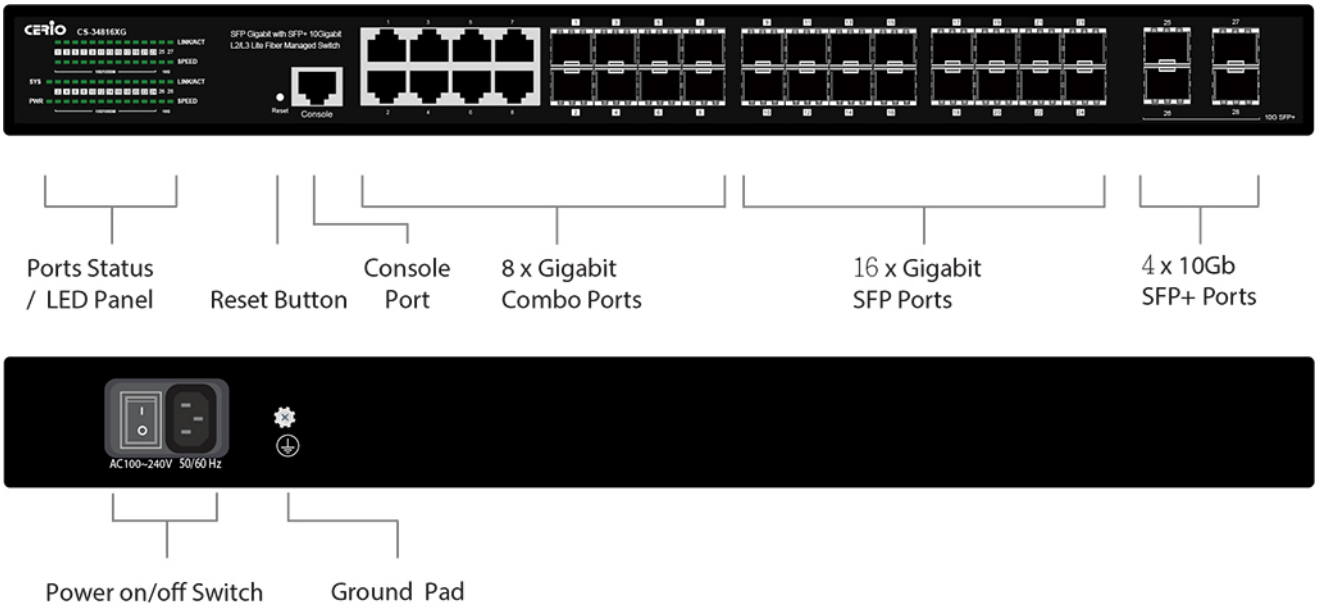
This device has been tested and found to comply with limits for a Class A digital device, pursuant to Part 2 and 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiates radio frequency energy and, if not installed and used in accordance with the user's manual, may cause interference in which case user will be required to correct the interference at his own expense.

**CE Mark Warning**

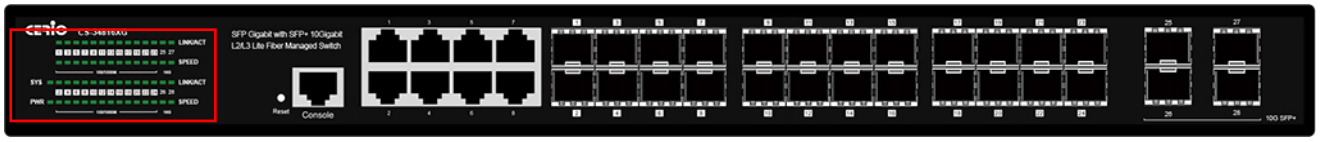
This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user many be required to take adequate measures.

# 1.產品外觀

## 1.1 前面板




## 1.2 後面板



**LED 狀態指示燈：4 x SFP+10Gigabit 乙太網路連接埠 和 16 埠 SFP Gigabit 乙太網路連接埠 和 8 x Gigabit Combo 連接埠**

**Per Port :** Link/ACT 狀態 LED 指示燈。

**Per Port :** 1000M/Gigabit 狀態指示燈。

**Per Unit :** 系統狀態 LED 指示燈。

**Per Unit :** 電源 LED 指示燈。


1) AC 電源 交換器控制開/關。
2) AC 輸入(100-240V/AC, 50-60Hz)。
3) 接地螺絲鎖點。

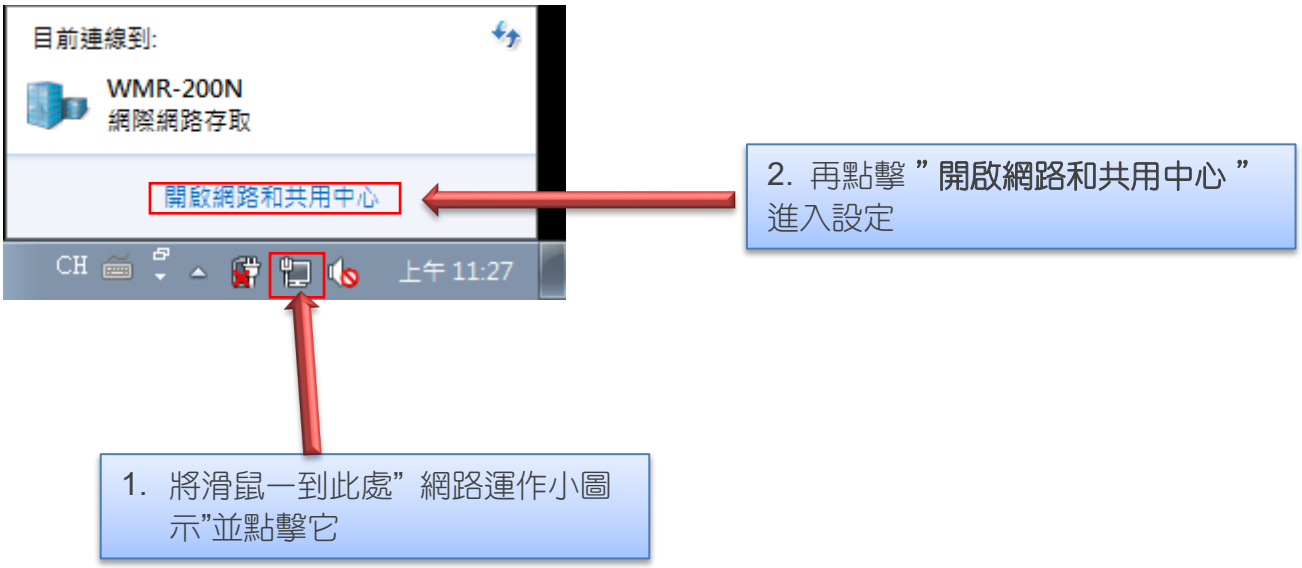
# 2.軟體設定

CS-34816XG 採用 Web 網頁管理方式。當架構建置完成，可以透過 Web 瀏覽器(如 Microsoft Edge 或 Google Chrome 或 Firefox)藉由桌上型 PC / NB 筆記型電腦來管理設定 CS-34816XG。
請將使用者管理員的桌上型 PC / NB 筆記型電腦的網路 IP 區段設定為與 CS-34816XG 相同的網路 IP 區段範圍，以便於同網路 IP 區段可以順利訪問 CS-34816XG 的網頁管理系統。

**注意，請勿將電腦設定並與使用 CS-34816XG 的 IP 相同 IP 位址或於環境網路中的任何其他網路設備的使用的 IP 重複衝突位址。** ***請參閱以下步驟：***

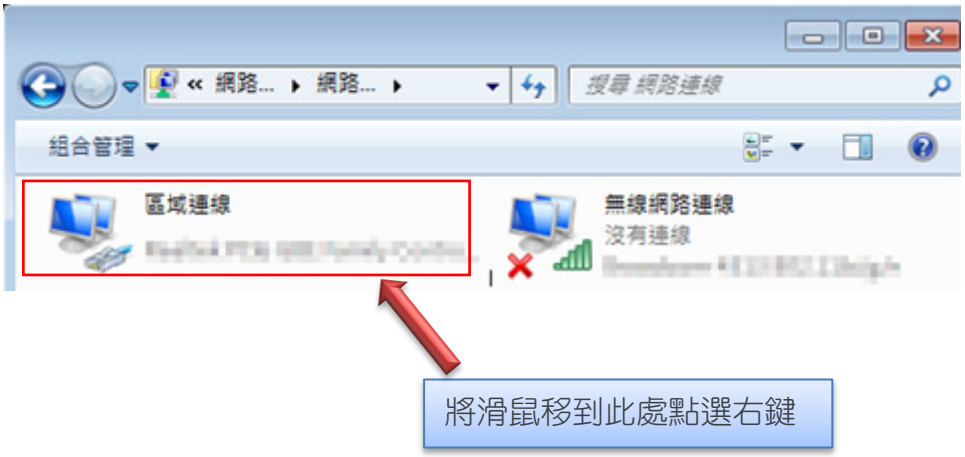
## 2.1 Windows OS 作業系統為例

**步驟 1：** 請點擊螢幕右下方的網路運作小圖示，如下圖，再點擊 **" 開啟網路和共用中心 "** ，進入設定頁面。

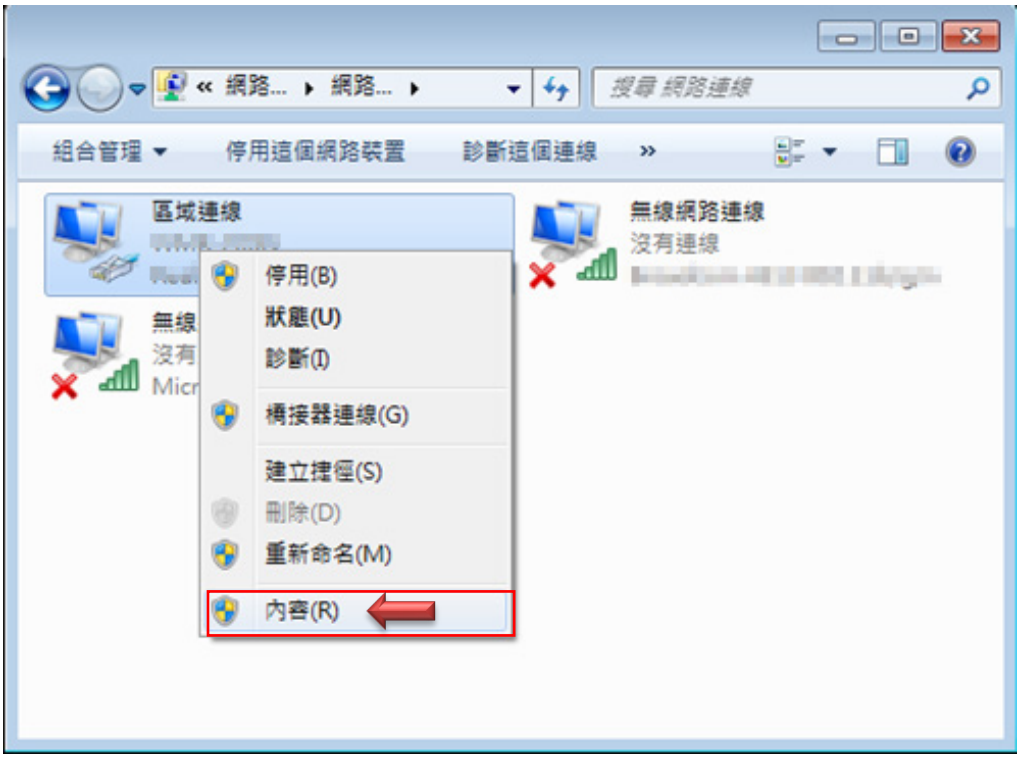


**步驟 2：**當進入網路共用中心後，在左邊目錄部分找出＂**變更介面卡設定**＂點擊進入。


**步驟 3：**進入變更介面卡設定則會出現以下圖示，將滑鼠移到＂**區域連線**＂後按下右鍵點擊內容。

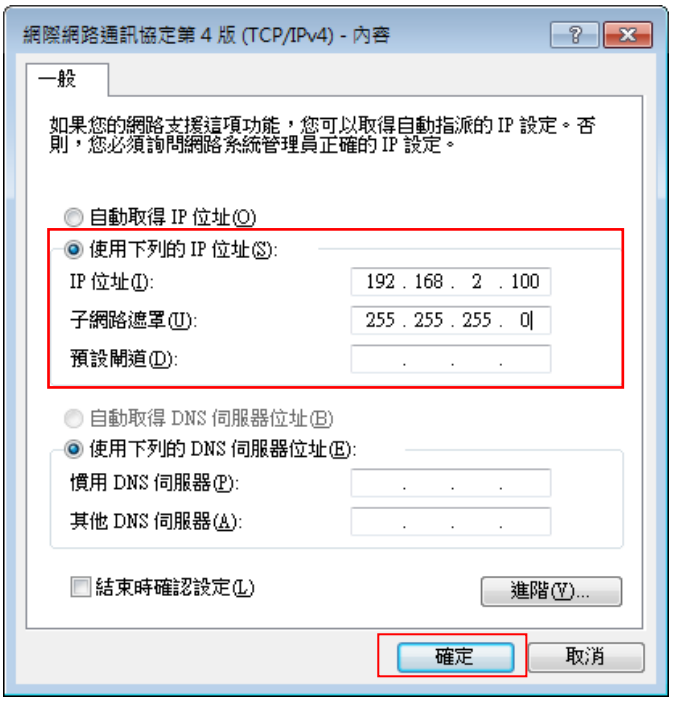


**步驟 4：**出現右鍵選單後，點擊選單下方的＂**內容**＂(如下圖所示)將進入設定 TCP/IP。



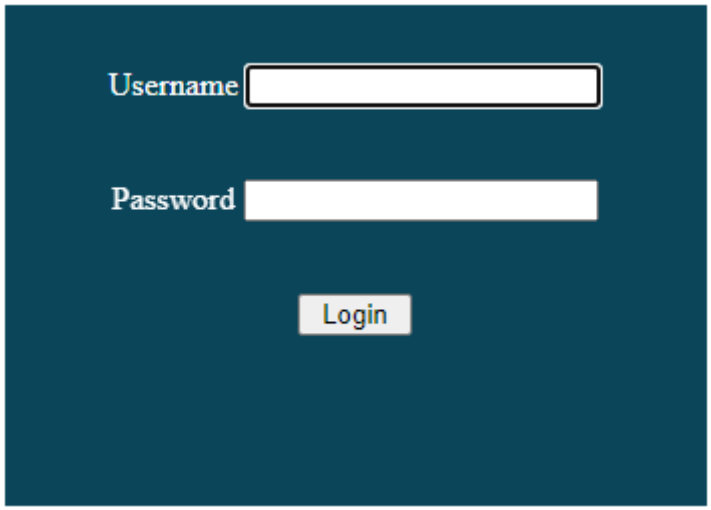

**步驟 5：**進入後再＂**這個連線使用下列項目**＂內找出＂**網際網路通訊協定第 4 版(TCP/IPv4)**＂選項點擊兩下進入編輯。

**步驟 6：**點擊 TCP/IPv4 將進入 PC 或筆電的 IP 位址設定頁面，預設為自動取得 IP 位址，我們將它改為”使用以下的 IP 位址”，並在 IP 欄位打入與 CS-34816XG 的同網段 IP 位址，例如 CS-34816XG 網頁管理的預設 IP 為 192.168.2.200，則 PC 或筆電的 IP 為者可以設定 192.168.2.x ，x 可設定 1~至 253 之間的數值。以下圖為例，完成設定。




**步驟 7：開啟 Web 瀏覽器**

接下來請開啟您的如 Microsoft Edge 或 Google Chrome 或 Firefox 瀏覽器並於 URL 網址列中輸入 CS-34816XG 網頁 Web 管理的預設的 IP 位址 ：
http://192.168.2.200，開啟 CS-34816XG 的 WEB 管理介面。




*成功進入管理登入介面後，在使用者名稱欄位中輸入「root」，密碼鍵入「default」，按「確定」即可登入管理介面。*

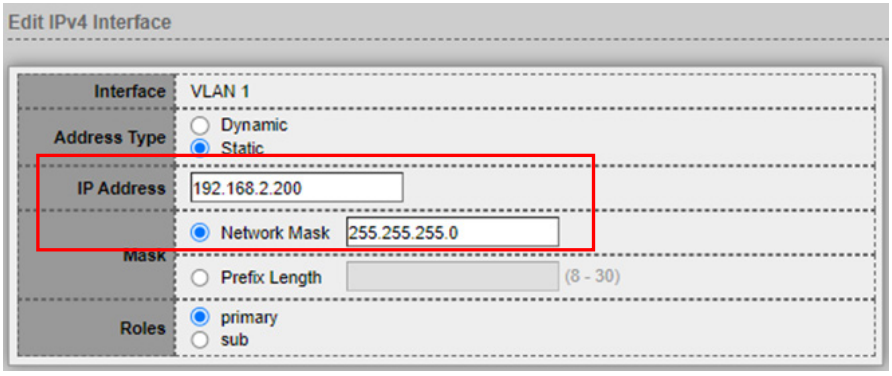
## 2.2 系統登錄使用者名稱與密碼資訊

- 預設的 IP 位置 : **192.168.2.200**
- 預設的使用者名稱與密碼 : **root /default**

| | |
|---|---|
| **預設登入位址** | 192.168.2.200 |
| **登入帳號** | root |
| **登入密碼** | default |

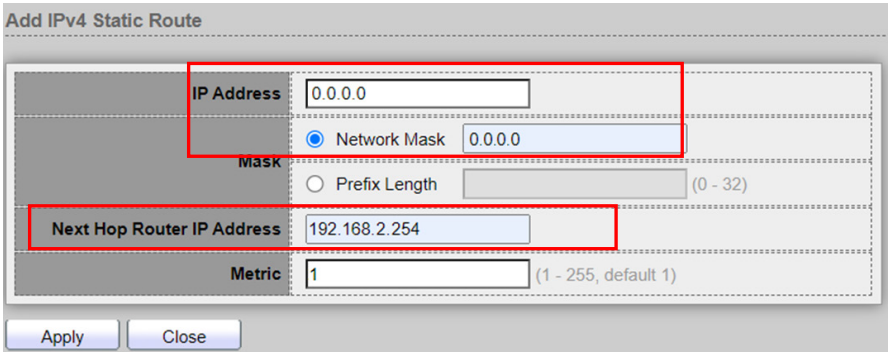
在通過使用者/密碼驗證通過之後，將顯示管理介面的主頁，可以開始進行下一步管理設定。

## 預設 IP 設定:




| Note | 如果要變更 POE 交換器的預設 IP(VLAN IP)位址，<br>請參閱章節：13.1.1。 “IP Configuration > IPv4 Interface & Default IP Configure >”(請參閱第 147 頁 )。 |
|---|---|

## Layer3 預設路由設定：(該功能與 Layer2 交換器的"Default Gateway Configure"相同 )



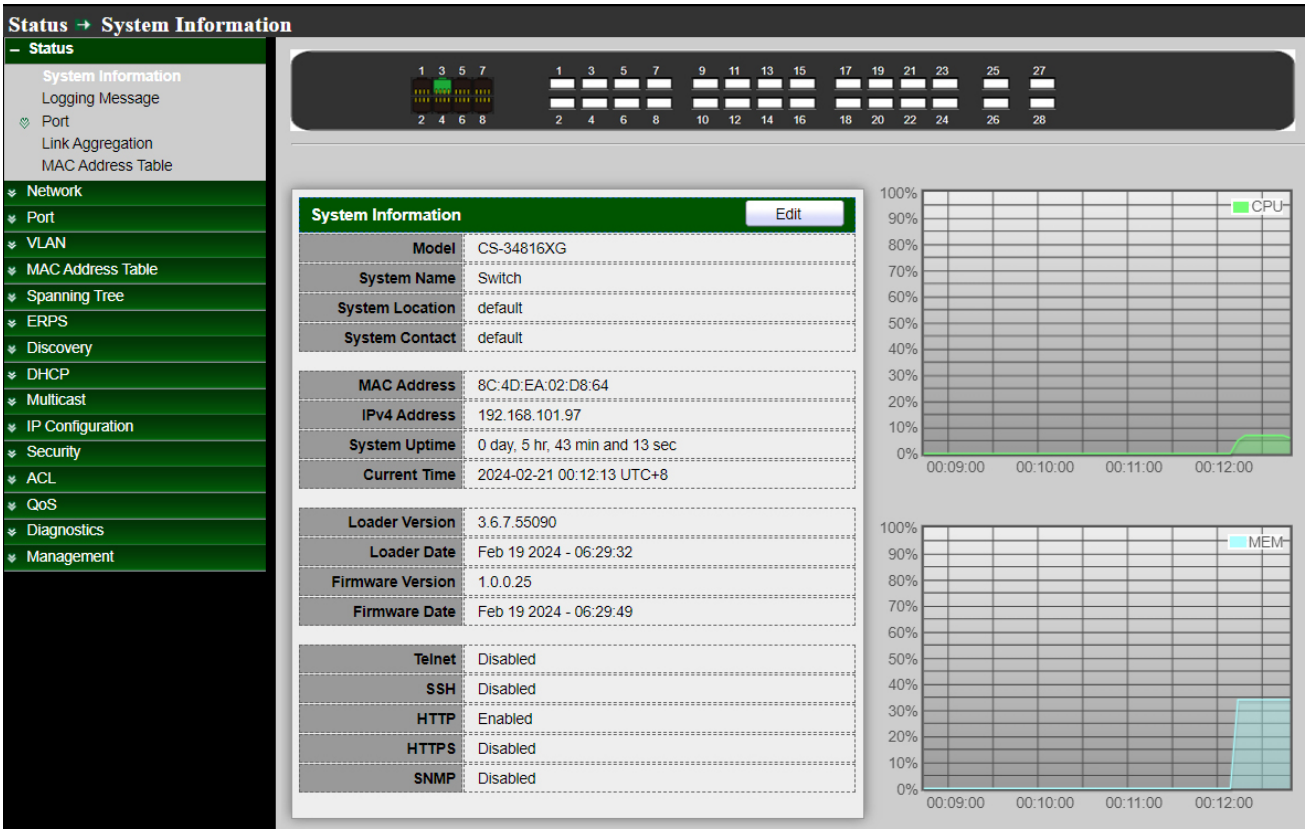

| Note | 如果要設定 L3 POE 交換器的預設 Router IP 位址，<br>請參閱章節：14.1.2。 “IP Configuration > IPv4 Interface & Default IP Configure >”(請參閱第 151 頁 )。 |
|---|---|

# 3.Status

## 3.1 系統資訊(System Information)

使用者管理員可以查看此頁面顯示的交換器面板、CPU 使用率、記憶體使用率和其他系統當前資訊。允許使用者編輯一些系統資訊。

| Note | 在 Web UI 中，左欄顯示設定選單。頂行顯示交換器目前的連結狀態，點選連接埠圖形時可快速顯示連結狀態等資訊，埠圖形顯示綠色表示連接埠已連結成功，埠圖形顯示黑色表示連接埠未有連結成功。在交換器面板下方，配有常用工具欄，為使用者提供有用的功能。螢幕的其餘部分顯示設定。 |
|---|---|

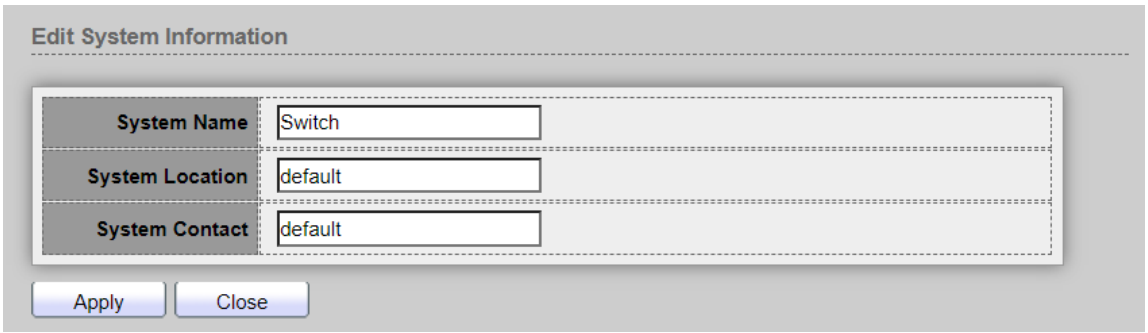



| 欄位 | 描述 |
|---|---|
| Model | 顯示交換器的型號 |
| System Name | 顯示交換器的系統名稱。該名稱也用作每行的CLI前綴（“Switch>” or “Switch#”） |
| System Location | 顯示交換器的位置資訊 |

| | |
|---|---|
| System Contact | 顯示交換器的聯繫資訊 |
| MAC Address | 顯示交換器的基本MAC位址 |
| IPv4 Address | 目前系統IPV4位址 |
| IPv6 Address | 目前系統IPV6位址 |
| System OID | SNMP系統對象ID |
| System Uptime | 顯示以開機運行累積時間 |
| Current Time | 當前系統時間 |
| Loader Version | 裝載版本 |
| Loader Date | 裝載版本日期 |
| Firmware Version | 當前韌體版本 |
| Firmware Date | 當前韌體版本日期 |
| Telnet | 顯示目前Telnet服務開啓/關閉狀態 |
| SSH | 顯示目前SSH服務開啓/關閉狀態 |
| HTTP | 顯示目前HTTP服務開啓/關閉狀態 |
| HTTPS | 顯示目前HTTPS服務開啓/關閉狀態 |
| SNMP | 顯示目前SNMP服務開啓/關閉狀態 |

## Edit System Information

使用者管理員可以點擊表格標題上的“Edit”編輯以下系統資訊。

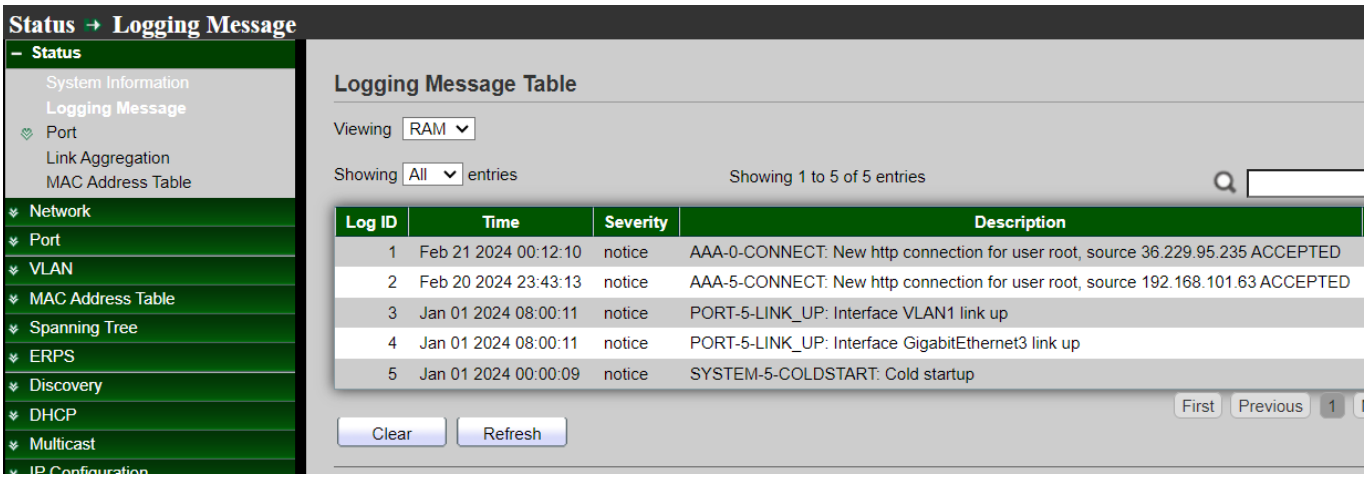


- **System Name :** 顯示交換器的系統名稱。該名稱也用作每行的 CLI 前綴（“Switch>” or “Switch#”）。
- **System Location :** 顯示交換器的位置資訊。
- **System Contact :** 顯示交換器的聯繫資訊。

*點擊應用”**Apply**”加入保存設定，或**“Close”**關閉設定。*

## 3.2 日誌訊息(Logging Message)

使用者管理員可以使用此工具頁面檢查系統 RAM 和 FLASH 狀態。




- **Viewing :** 可檢視日誌包括：
  - **RAM :** 顯示儲存在 RAM 上的日誌訊息。
  - **Flash :** 顯示儲存在 FLASH 上的日誌訊息。

| 欄位 | 描述 |
|---|---|
| Log ID | 日誌標識符 |
| Time | 日誌訊息的時間戳記 |
| Severity | 日誌訊息的嚴重程度 |
| 描述 | 描述日誌訊息 |

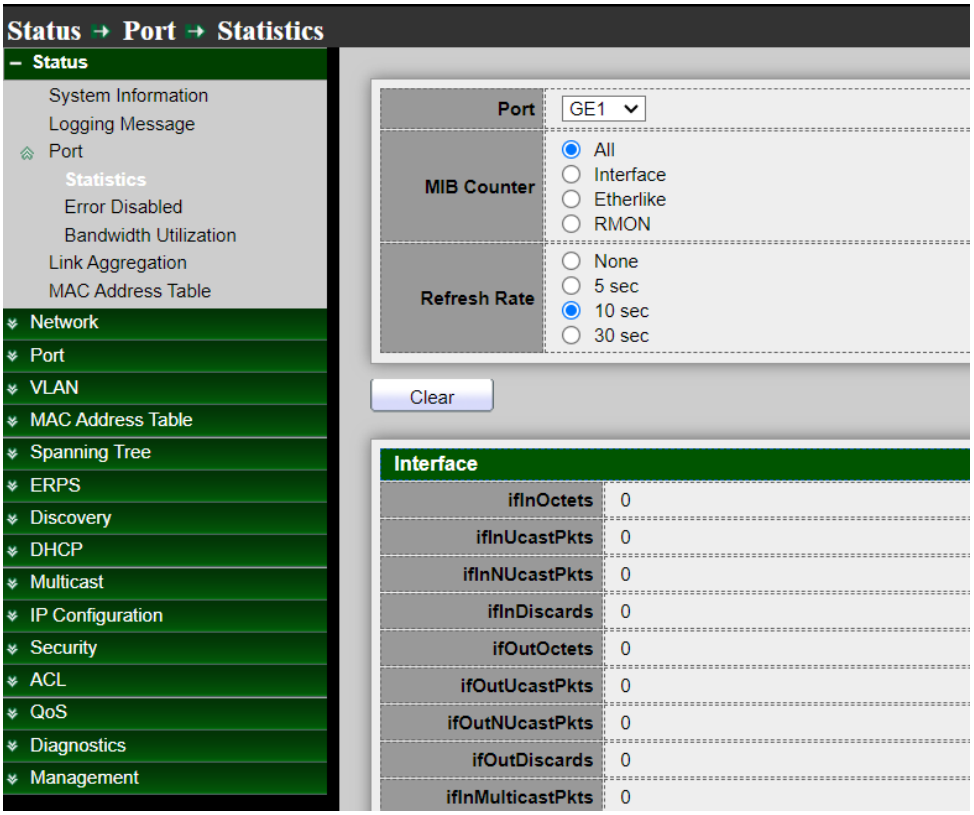
*點擊 "Clear" 加入並清除頁面或點擊 "Refresh" 加入並重新整理刷新頁面。*

## 3.3 埠(Port)

顯示每個連接埠的詳細埠摘要和狀態資訊。

### 3.3.1 統計數據(Statistics)

使用者管理員可以選擇檢視介面、乙太網路和 RMON MIB 的網路流量的標準計數器。介面和乙太網路的計數器顯示通過每個連接埠的流量錯誤。RMON 計數器提供通過每個連接埠的不同訊框類型和大小的總計數。 "Clear" 將清除目前所選連接埠的 MIB 計數器。




*點擊 "Clear" 加入並清除此頁面。*

| Interface | |
|---|---|
| ifInOctets | 1226044 |
| ifInUcastPkts | 8677 |
| ifInNUcastPkts | 343 |
| ifInDiscards | 0 |
| ifOutOctets | 2813449 |
| ifOutUcastPkts | 5587 |
| ifOutNUcastPkts | 194 |
| ifOutDiscards | 0 |
| ifInMulticastPkts | 226 |
| ifInBroadcastPkts | 117 |
| ifOutMulticastPkts | 194 |
| ifOutBroadcastPkts | 0 |

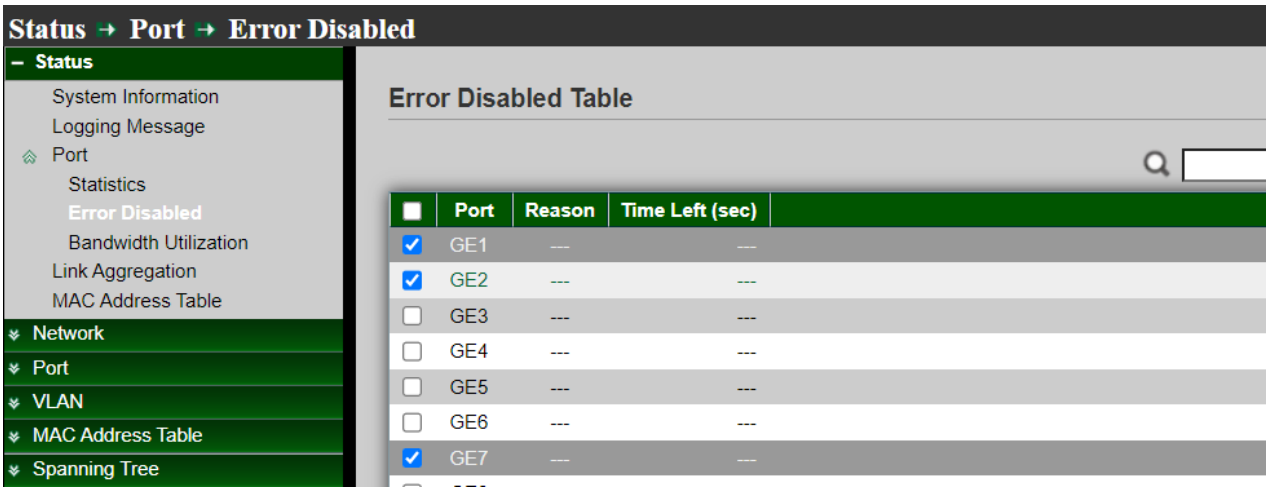
| Etherlike | |
|---|---|
| dot3StatsAlignmentErrors | 0 |
| dot3StatsFCSErrors | 0 |
| dot3StatsSingleCollisionFrames | 0 |
| dot3StatsMultipleCollisionFrames | 0 |
| dot3StatsDeferredTransmissions | 0 |
| dot3StatsLateCollisions | 0 |
| dot3StatsExcessiveCollisions | 0 |
| dot3StatsFrameTooLongs | 0 |
| dot3StatsSymbolErrors | 0 |
| dot3ControlInUnknownOpcodes | 0 |
| dot3InPauseFrames | 0 |
| dot3OutPauseFrames | 0 |

| RMON | |
|---|---|
| etherStatsDropEvents | 0 |
| etherStatsOctets | 1236728 |
| etherStatsPkts | 9117 |
| etherStatsBroadcastPkts | 117 |
| etherStatsMulticastPkts | 226 |
| etherStatsCRCAlignErrors | 0 |
| etherStatsUnderSizePkts | 0 |
| etherStatsOverSizePkts | 0 |
| etherStatsFragments | 0 |
| etherStatsJabbers | 0 |
| etherStatsCollisions | 0 |
| etherStatsPkts64Octets | 6502 |
| etherStatsPkts65to127Octets | 1080 |
| etherStatsPkts128to255Octets | 122 |
| etherStatsPkts256to511Octets | 1251 |
| etherStatsPkts512to1023Octets | 150 |
| etherStatsPkts1024to1518Octets | 12 |

- **Port :** 選擇一個連接埠顯示計數器統計資料。
- **MIB Counter :** 選擇 MIB 計數器以顯示不同的計數器類型。
  - **All :** 所有計數器。
  - **Interface :** 介面相關的 MIB 記數器。
  - **Etherlike :** 乙太網路相關的 MIB 計數器。
  - **RMON :** 相關的 MIB 計數器。
- **Refresh Rate :** 以每隔 “None , 5 sec , 10 sec , 30 sec” 秒數重新整理網頁，以取得指定連接埠的新計數器。

### 3.3.2 錯誤停用(Error Disabled)

如果使用者管理員設定了錯誤停用功能，則可以監控頁面資訊。



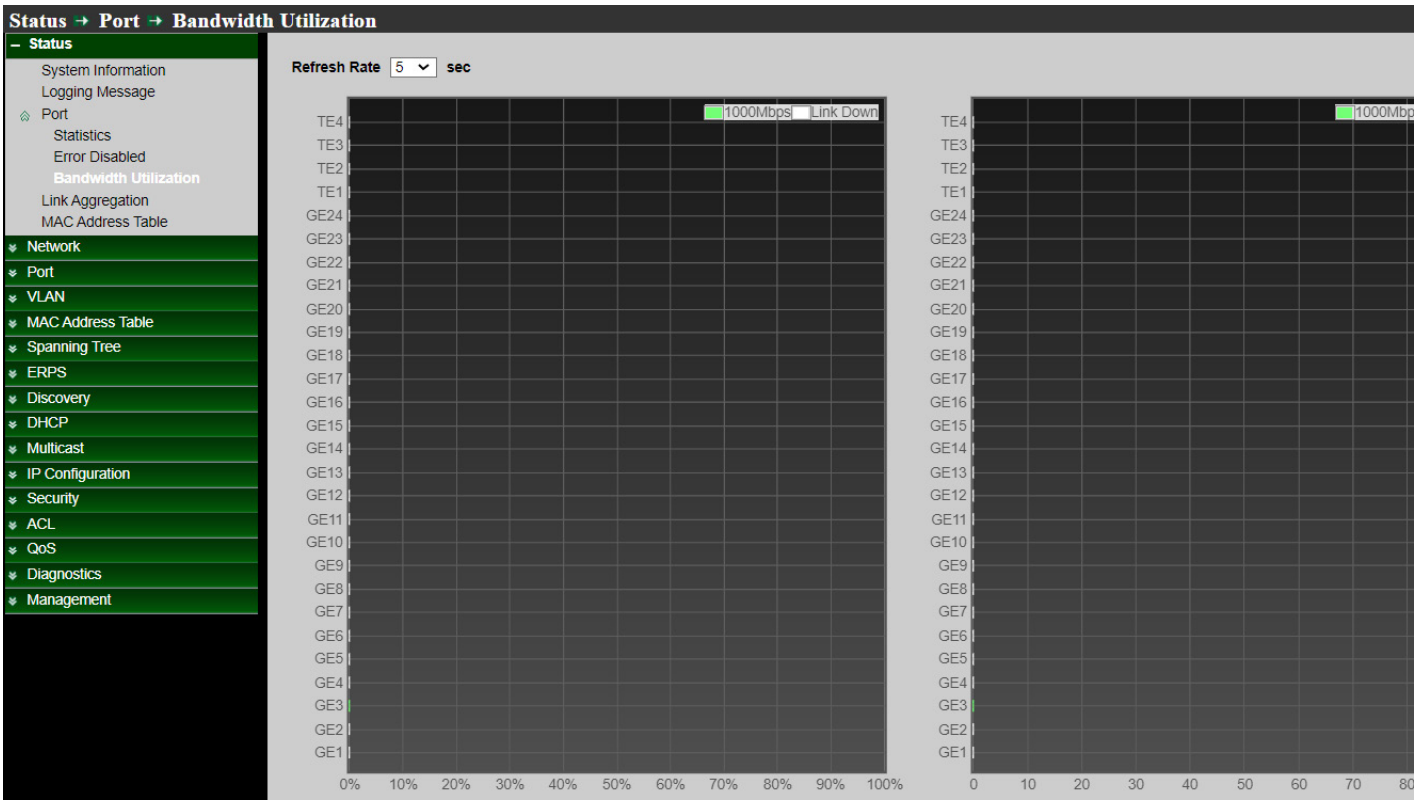

| 欄位 | 描述 |
|---|---|
| Port | 介面或埠編號 |
| Reason | 連接埠會因以下錯誤原因之一被停用：<br>• BPDU Guard(BPDU防護)<br>• UDLD(單向鏈路檢測)<br>• Self Loop(自循環)<br>• Broadcast Flood(廣播氾濫)<br>• Unknown Multicast Flood(未知多播氾濫)<br>• Unicast Flood(單播氾濫)<br>• ACL(訪問控制表) |

- Port Security Violation(埠安全違規)
- DHCP rate limit(DHCP速率限制)
- ARP rate limit(ARP速率限制)

| | |
|---|---|
| **Time Left (sec)** | 錯誤恢復剩餘時間(秒) |

### 3.3.3 頻寬利用率(Bandwidth Utilization)

此頁面可以顯示每個連接埠的 Tx/Rx 即時頻寬資訊。(每個連接埠的即時使用率，此頁面會在每個刷新週期自動刷新)

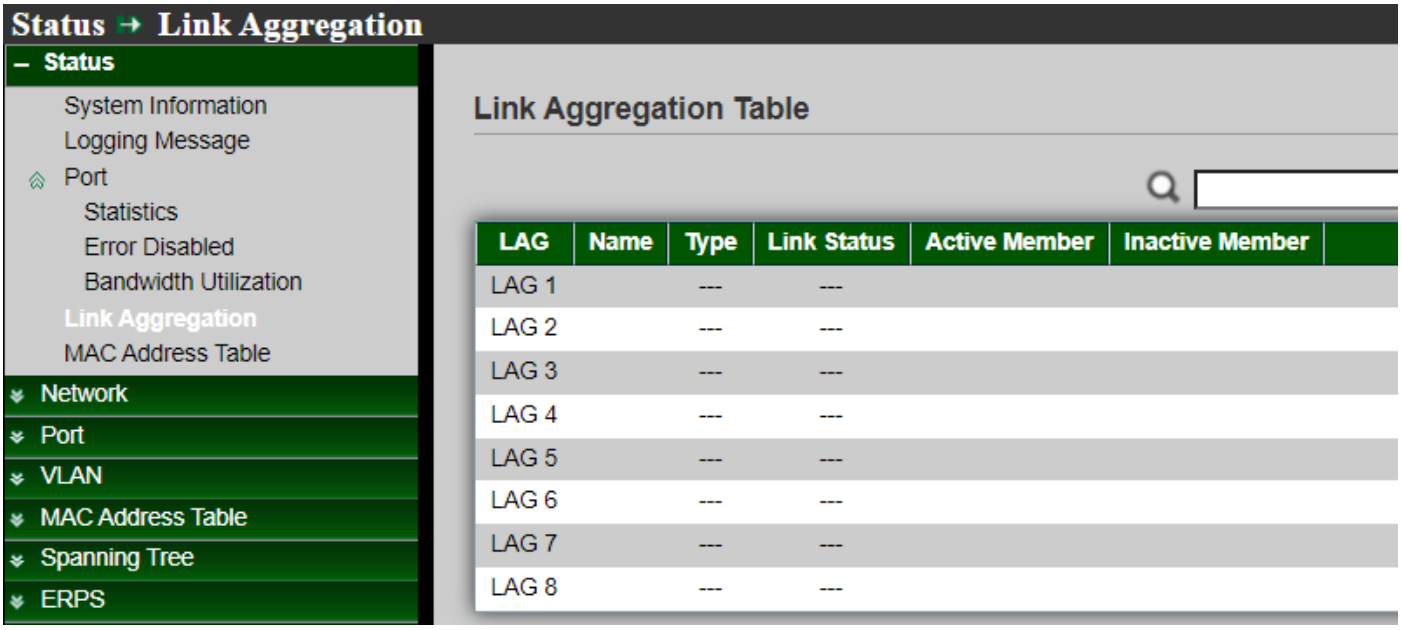



➢ **Refresh Rate :** 每隔幾秒刷新網頁，以獲取新的頻寬利用率。

- **2 :** 從下拉式選單中選擇 2 秒週期，刷新顯示頁面
- **5 :** 從下拉式選單中選擇 2 秒週期，刷新顯示頁面
- **10 :** 從下拉式選單中選擇 2 秒週期，刷新顯示頁面

## 3.4 鏈路聚合(Link Aggregation)

如果使用者管理員設定了 LACP 功能，則可以顯示 LACP 資訊。本系統支援 8 個鏈路聚合組(Link Aggregation Group,LAG)。管理員可以啟用 8 個 LAG。

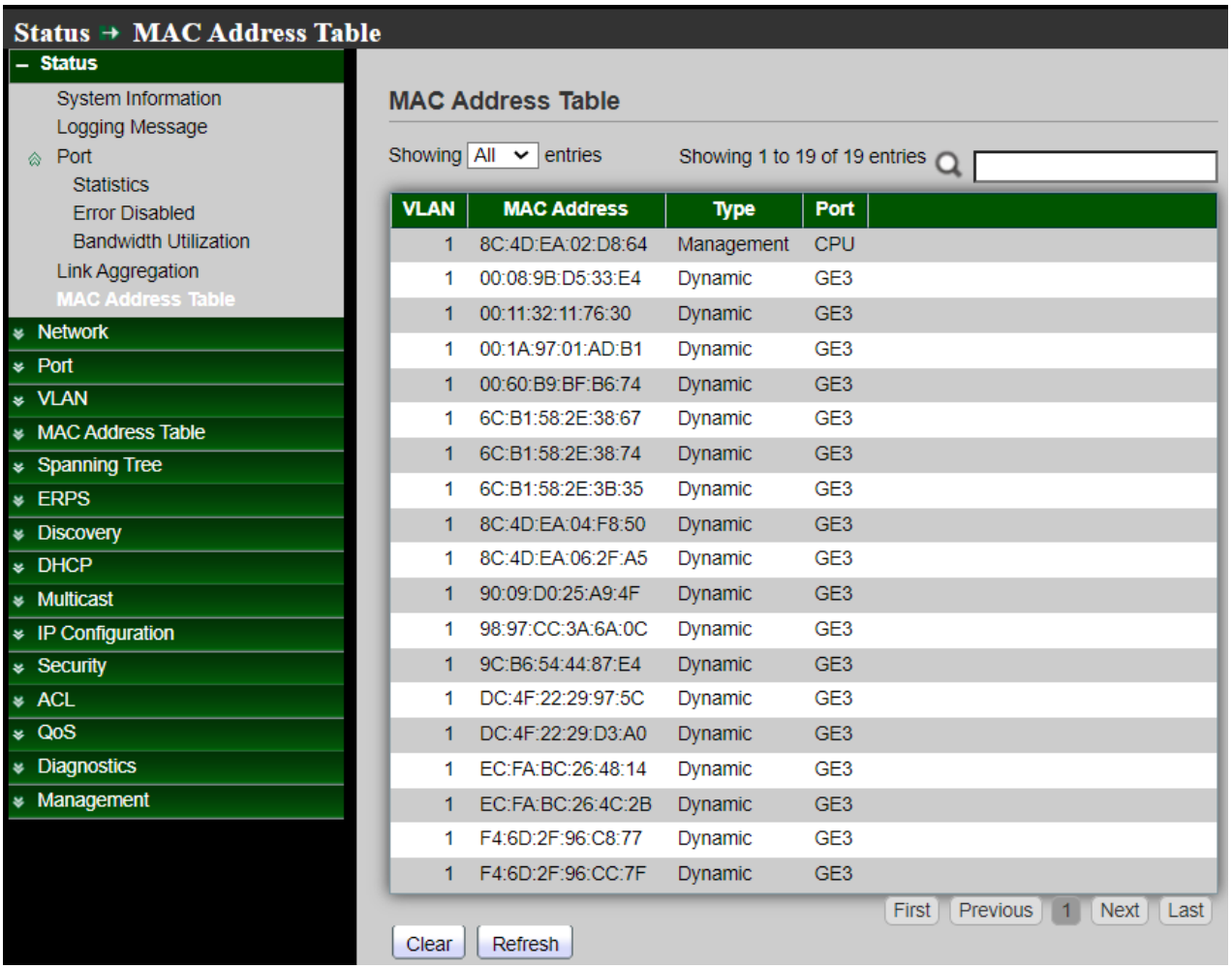



| 欄位 | 描述 |
|---|---|
| LAG | LAG編號 |
| Name | LAG連接埠描述 |
| Type | LAG類型<br>• **Static :** 分配給靜態LAG的連接埠組始終是設定啟用的成員<br>• **LACP :** 分配給動態LAG的連接埠組為候選埠。LACP決定哪些連接埠是設定啟用的成員埠 |
| Link Status | LAG的連接埠鏈路狀態 |
| Active Member | LAG的設定啟用的成員連接埠 |
| Inactive Member | LAG的非設定啟用的成員連接埠 |

# 3.5 MAC 位址表(MAC Address Table)

MAC 位址表頁面顯示交換器上的所有 MAC 位址清單，包括使用者管理員創建的靜態 MAC 位址或從硬體自動學習到的 MAC 位址。

“Clear”會清除所有動態清單，“Refresh”將檢索最新的 MAC 位址顯示在頁面上。




| 欄位 | 描述 |
|---|---|
| VLAN | MAC位址關聯的VLAN ID |
| MAC Address | 靜態轉發封包到的MAC位址 |
| Type | MAC位址的類型<br>• **Management:**用於管理的被測器件基本MAC位址<br>• **Static:**位址由使用者管理員手動設定<br>• **Dynamic:**位址由硬體自動學習 |

| | |
|---|---|
| Port | 連接埠類型<br>• CPU:用於管理的被測器件CPU連接埠<br>• Other:正常交換器連接埠 |

*點擊“Clear”清除資訊頁面，點擊“Refresh”重新整理頁面。*

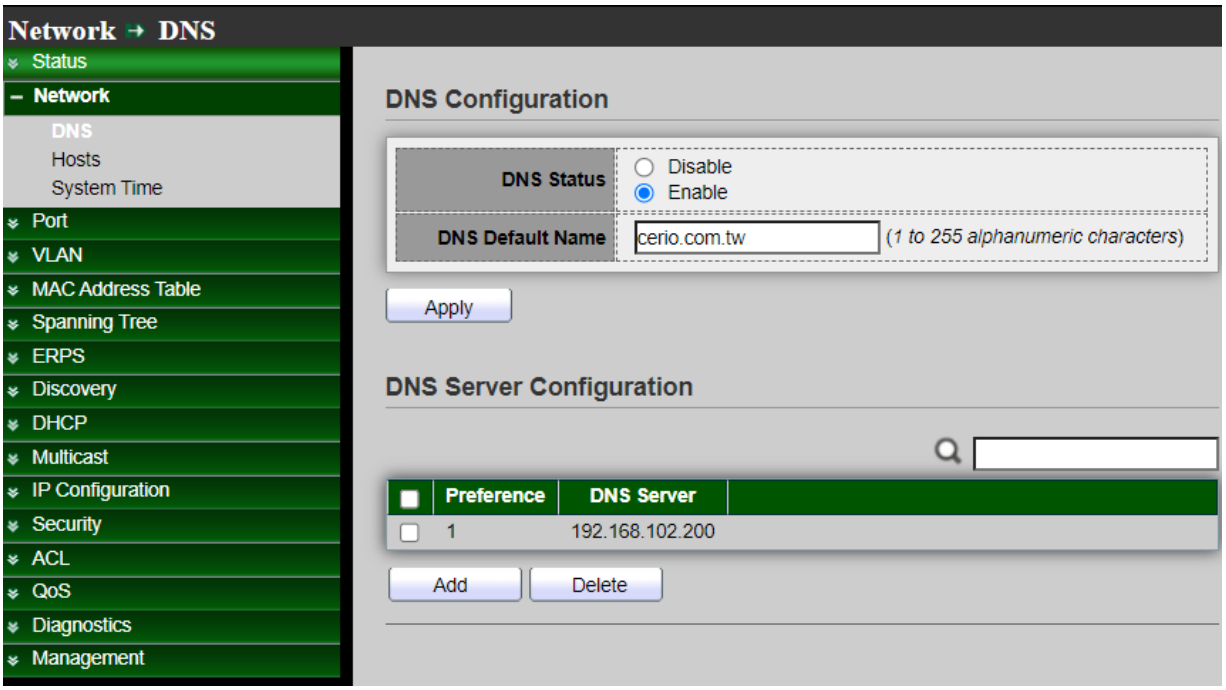
# 4.Network

## 4.1 網域名稱系統(DNS)

DNS(網域名稱系統)用於將網域名稱和 IP 位址相對映。使用 DNS 畫面可設定和檢視交換器上的預設 DNS 伺服器。使用這些頁面可設定有關網路使用的 DNS 伺服器以及交換器作為 DNS 用戶端運作的資訊。

本交換器的 DNS 服務允許使用靜態表清單或透過重新導向到網路上的其他名稱伺服器，將主機名稱映射到 IP 位址。當用戶端設備指定此交換器為 DNS 伺服器時，用戶端將透過向交換器轉送 DNS 查詢並等待回應，嘗試將主機名稱解析為 IP 位址。
您可以手動設定 DNS 表中用於將映射網域名稱到 IP 位址的清單、設定預設網域名稱或指定一個或多個名稱伺服器用於網域名稱到位址的轉換。

您可以使用這些頁面設定有關網路使用的 DNS 伺服器和交換器作爲 DNS 用戶端運行的資訊。
使用該頁面設定全域 DNS 設定和 DNS 伺服器資訊。



**DNS Configuration**

選擇“Disable”或“Enable”指定開啓或關閉 DNS 用戶端的管理狀態：

- **DNS Status:**
  - **Disable :** 阻止交換器發送 DNS 查詢。
  - **Enable :** 允許交換器向 DNS 伺服器轉送 DNS 查詢以解析 DNS 網域名稱。
- **DNS Default Name :** 輸入要包含 DNS 查詢中的預設 DNS 網域名稱。

| | |
|---|---|
| Note | 當系統對不合格主機名稱執行查找時，此欄位提供網域名稱(例如，如果預設網域為 cerio.cc，而使用者輸入 oem，則“oem”將變更為 oem.cerio.cc，以解析名稱)。網域名稱長度不得超過 255 個字母字元。 |

*點擊 **“Apply”** 儲存您的變更。*

## DNS Server Configuration

使用者管理員可以通過 **“add”** 和 **“Delete”** 設定 DNS Server Setting 管理功能。

| 欄位 | 描述 |
|---|---|
| Preference | Preference欄位顯示伺服器首選項順序。首選項會依照輸入首選項的順序設定 |
| DNS Server | 顯示伺服器已新增至列表 |

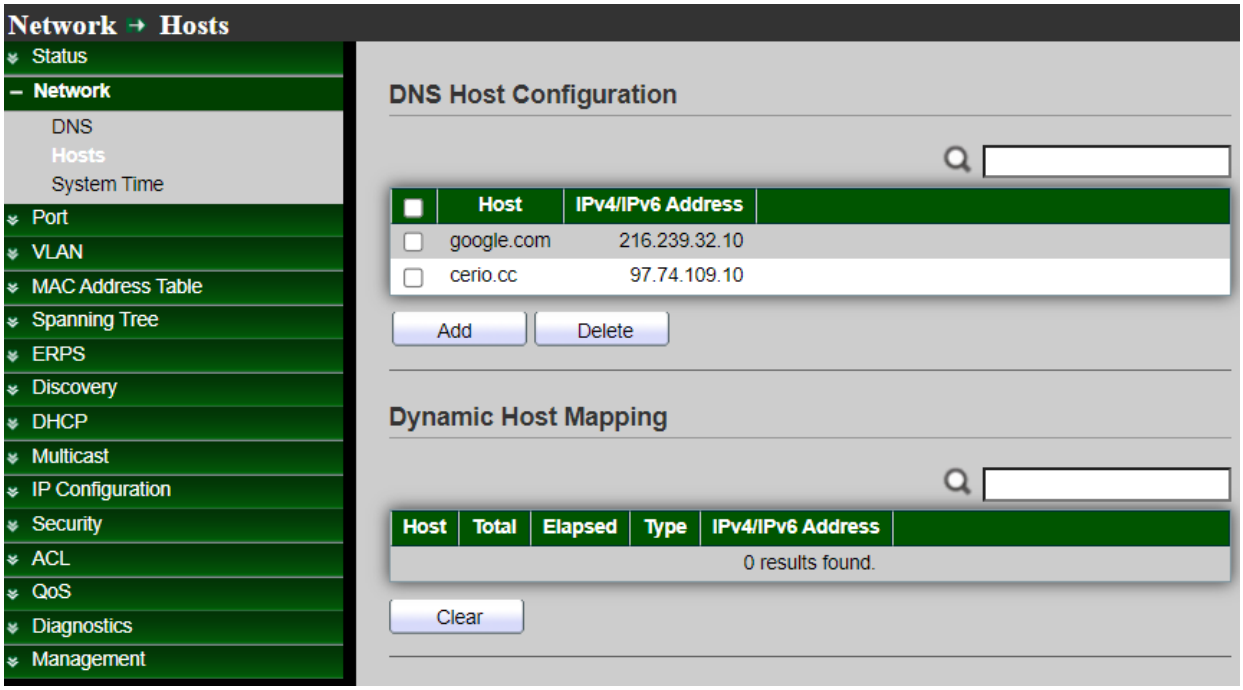
| | |
|---|---|
| Note | 伺服器的“preference”：首選項由輸入順序決定。最多可以指定八個 DNS 伺服器。 |

- **Add :** 要指定交換器向其發送 DNS 查詢的 DNS 伺服器，請在 DNS Server Address 中以標準 IPv4 點標記法輸入 IP 位址，然後點擊”Add”。伺服器會出現在下麵的清單中。您最多可以指定八個 DNS 伺服器。首選項按照創建的順序設定。
- **Delete :** 要從清單中移除 DNS 伺服器，點選想要移除的伺服器旁的複選框，然後點擊“Delete”。如果沒有指定 DNS 伺服器，複選框會全選並刪除清單中所有 DNS 伺服器。

使用者管理員可以在螢幕上設定 DNS Server Configuration 的“**Apply**”和“**Cancel**”，並將螢幕上的資料重設為交換器的最新值。

## 4.2 主機(Host)

該頁面為使用者管理員提供查看主機名稱到 IP 位址的資訊，使用者管理員可以設定此頁面手動映射主機名稱到 IP 位址或查看動態主機映射。

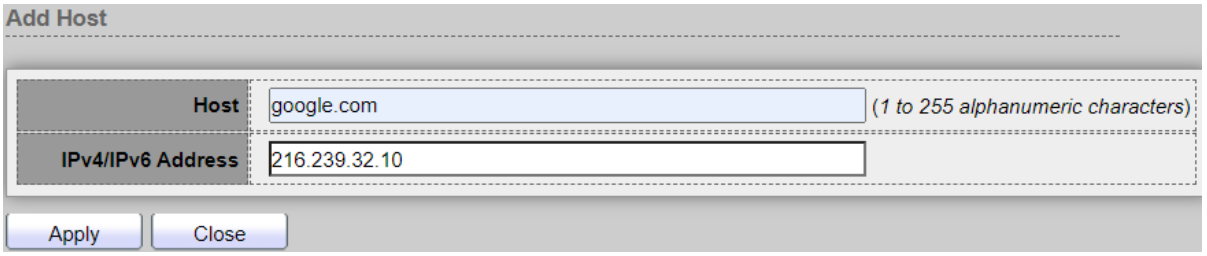



*點擊“Clear”清除該頁面資訊。*

### DNS Host Configuration

使用者管理員可以通過“**add**”和“**Delete**“為本地動態主機映射表的靜態清單設定功能管理。

| 欄位 | 描述 |
|---|---|
| Host | 顯示分配給指定IP位址的“host name” |
| IPv4/IPv6 Address | 與“host name”相關聯的IP位址 |




- **Host :** 使用者管理員可以設定 Host Name 欄位，指定要新增的靜態主機名稱。
- **IPv4/IPv6 Address :** 輸入與主機名稱關聯的 IP 位址到該 "IPv4/IPv6 Address" 欄位，應用 **"Apply"** 創建後清單將顯示在頁面列表中。

| Note | 對於 Host Name 欄位,必須為 1 至 255 個字母數字字元，長度不能超過 158 個字元，且為必填欄位。 |
|---|---|

*點擊 **"Apply"** 儲存您的變更，或點擊 **"Close"** 關閉設定。*

## Dynamic Host Mapping

使用者管理員可以清除列表中的所有動態主機名稱清單，只需點擊 "Clear" 。

Dynamic Host Mapping 表顯示交換器學習到的主機名稱-到-IP 位址的清單。

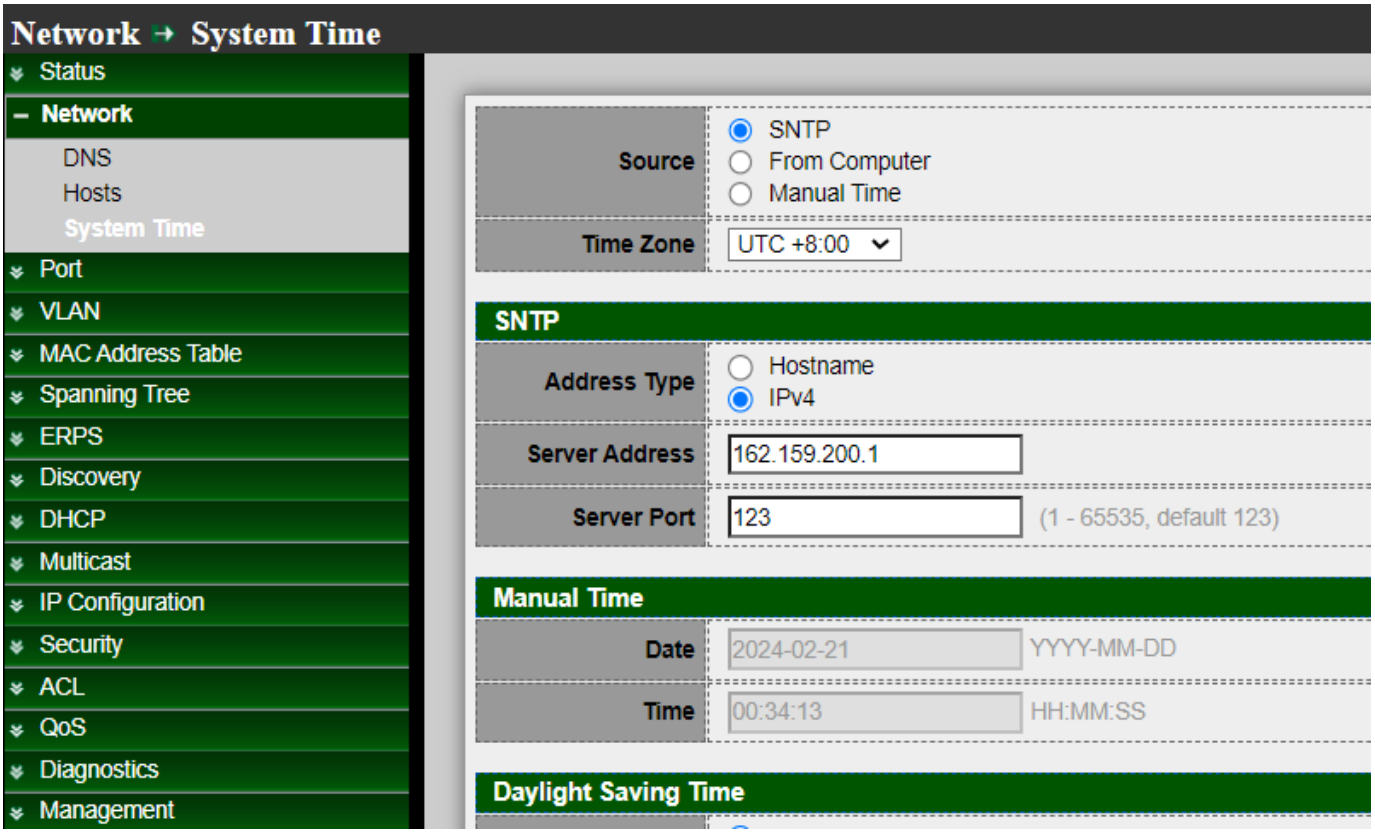
| 欄位 | 描述 |
|---|---|
| Host | 顯示分配給指定IP位址的主機名稱的清單 |
| Total | 顯示自動態清單首次新增到表中以來的時間 |
| Elapsed | 顯示自最後更新動態清單以來的時間 |
| Type | 顯示動態清單類型 |
| IPv4/IPv6 Address | 顯示與主機名稱相關聯的IPv4或IPv6位址列表 |

*點擊 **"Apply"** 儲存您的變更，或點擊 **"Clear"** 重新整理頁面。*

# 4.3 系統時間(System Time)

可以透過此頁面設定係統時間。使用者管理員可以選擇 SNTP Server 或從電腦更新系統時間，也可以手動設定系統時間。

注意。如果管理員選擇 SNTP Server 來同步更新時間，則必須確認系統閘道和 DNS 是否正確，且交換器系統必須能夠連線到 SNTP Server。




### System Time

- **Source :** 選擇時間來源。
  - **SNTP :** 從 NTP 伺服器同步時間。
  - **From Computer :** 從瀏覽器主機設定時間。
  - **Manual Time :** 手動設定時間。
- **Time Zone :** 從地區清單選擇時區。

### SNTP

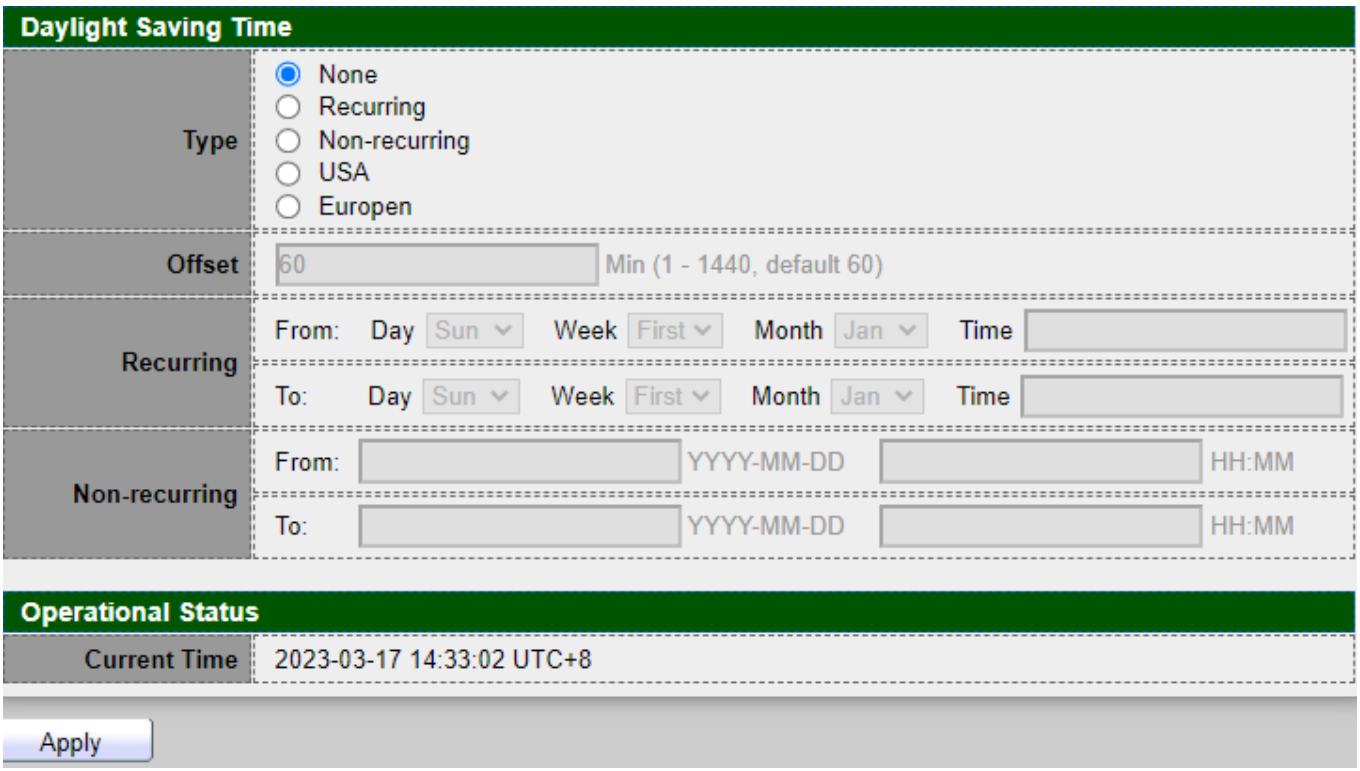
- **Address Type :** 選擇 NTP 伺服器的位址類型。當時間來源為 SNTP 時啓用此功能。
- **Server Address :** 輸入 NTP 伺服器的 IPv4 位址或主機名稱。當時間來源為 SNTP 時啟用此功能。
- **IPv6 Address :** 輸入 NTP 伺服器的 NTP 埠。預設值為 123。當時間來源為 SNTP 時啟用此功能。

## Manual Time

- **Date :** 輸入手動日期。當時間來源為手動時啟用此功能。
- **Time :** 輸入手動時間。當時間來源為手動時啟用此功能。

## Daylight Saving Time

交換器支援夏令時功能，如果使用者管理員需要啟用並設定夏令時功能則可以啟用此功能。




- **Type :** 選擇夏令時模式。
  - **Disable :** 關閉夏令時功能。
  - **Recurring :** 使用循環夏令時模式。
  - **Non-Recurring :** 使用非循環夏令時模式。
  - **USA :**使用美國夏令時，從三月的第二個星期日開始，到十一月的第一個星期天結束。
  - **European :** 使用歐洲夏令時，從三月的最後一個星期日開始，到最後一個星期日結束。
- **Offset :** 指定夏令時的調整偏移量。
- **Recurring From :** 指定循環夏令時的起始時間。當選擇”Recurring”模式時此位元欄位元可用。
- **Recurring To :** 指定循環夏令時的結束時間。當選擇”Recurring”模式時此欄位元可用。
- **Non-recurring From :** 指定非循環夏令時的起始時間。當選擇” Non-Recurring”模式時此位元欄位元可用。

➢ **Non recurring To :** 指定非循環夏令時的結束時間。當選擇" Non-Recurring" 模式時此欄位元可用。

### Operational Status

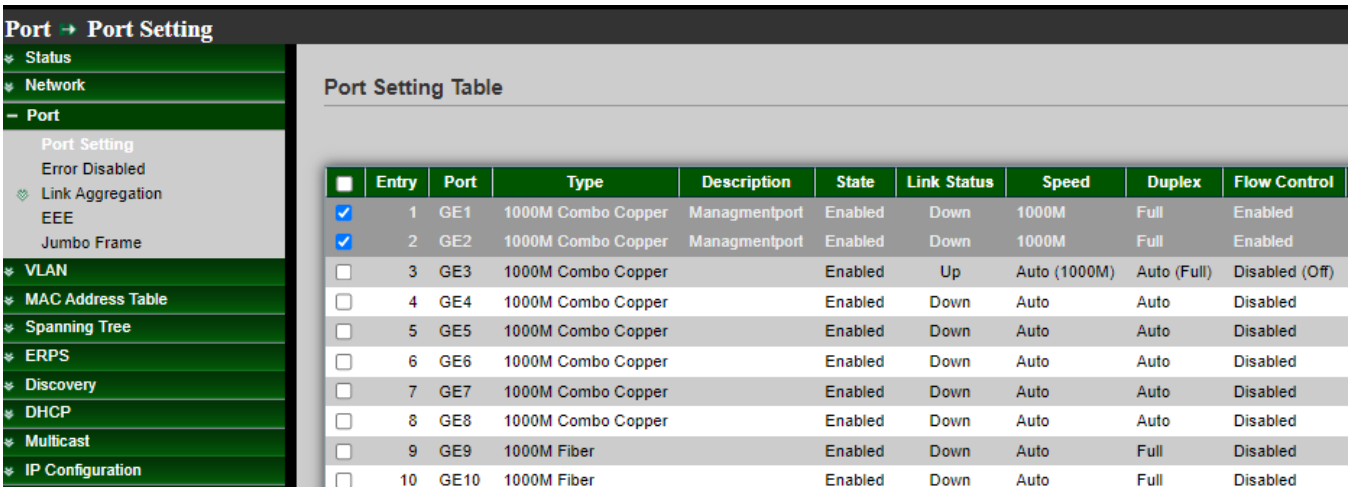
**Current Time :** 顯示目前運行時間。

*點擊 "Apply" 儲存您的變更設定。*

# 5. Port

## 5.1 網路埠設定(Port setting)

該頁面顯示網路埠目前狀態，允許使用者修改網路埠設定。選擇網路埠清單然後點擊 **"Edit"** 修改網路埠設定。

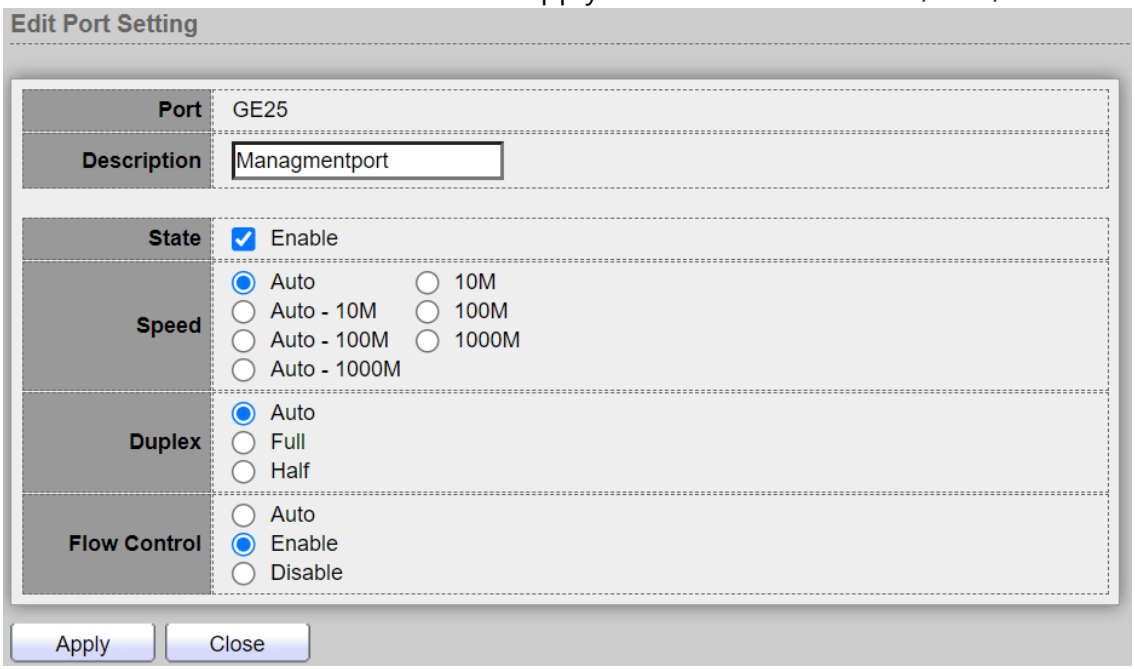



| 欄位 | 描述 |
|---|---|
| Port | 顯示本交換器的網路埠編號 |
| Type | 顯示連接埠媒體類型 |
| Description | 顯示自訂連接埠的描述 |
| State | 顯示網路埠管理狀態<br>• **Enabled :** 網路埠狀態開啟<br>• **Disabled :** 網路埠狀態關閉 |
| Link Status | 目前連接埠鏈路狀態<br>• **Up :** 連接埠鏈路已連接<br>• **Down :** 連接埠鏈路已關閉 |

| | |
|---|---|
| Speed | 目前連接埠速度設定和鏈路速度狀態 |
| Duplex | 目前連接埠雙工設定和鏈路雙工狀態 |
| Flow Control | 目前連接埠流量控制設定和連線的流量控制狀態 |

使用者管理員可以設定每個連接埠的速度/雙工/流量控制。

選擇複選框的連接埠編號，然後點擊應用 “Apply” 設定每個連接埠的速度/雙工/流量控制。




- **Port :** 選定的網路埠清單。
- **Description :** 自訂連接埠的描述。
- **State :** 網路埠管理狀態。
  - **Enabled :** 網路埠狀態開啟。
  - **Disabled :** 網路埠狀態關閉。
- **Speed :** 網路埠的速率。
  - **Auto :** 自協商所有速率。
  - **Auto-10M :** 自動判別到 10M。
  - **Auto-100M :** 自動判別到 100M。
  - **Auto-1000M :** 自動判別到 1000M。
  - **Auto-10M/100M :** 自動判別到 10M/100M。
  - **10M :** 強制速率為 10M。
  - **100M :** 強制速率為 100M。

- **1000M :** 強制速率為 1000M。

➢ **Duplex :** 網路埠雙工模式。

- **Auto :** 自動判別所有雙工模式。
- **Half :** 自動為半雙工模式。
- **Full :** 自動為全雙工模式。

➢ **Flow Control :** 網路埠的流量控制。

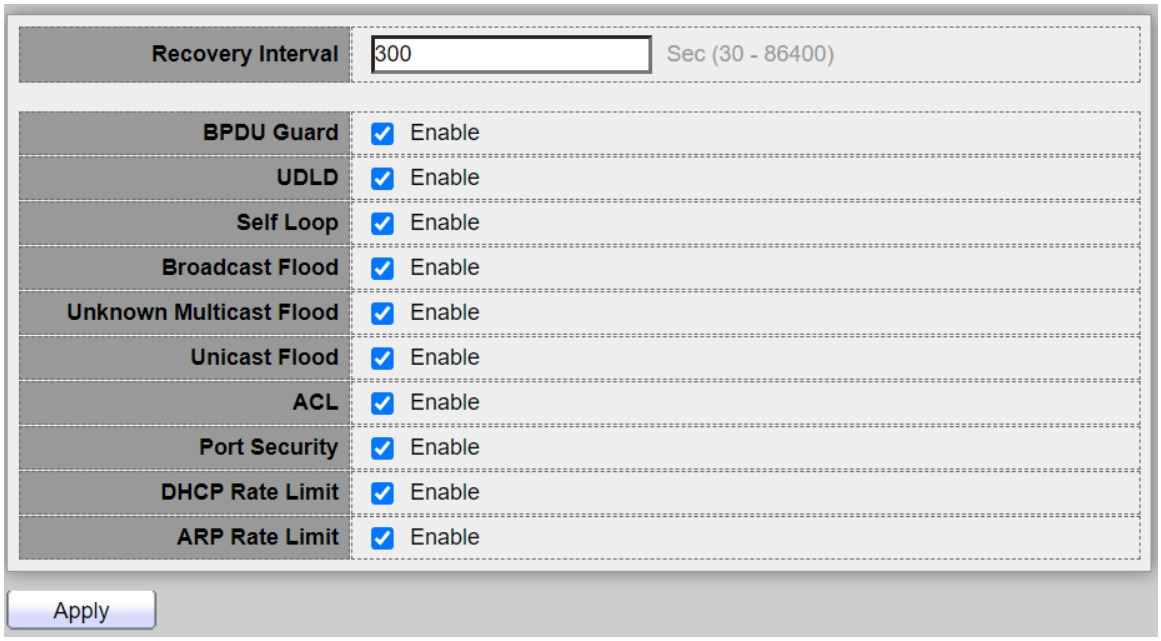
- **Auto :** 自動判別流量控制。
- **Enabled :** 啓用流量控制。
- **Disabled :** 關閉流量控制。

*點擊 "Apply" 儲存您的變更，或 "Close" 關閉設定。*

## 5.2 錯誤停用(Error Disabled)

該功能可阻止錯誤操作，包括 BPDU Guard(BPDU 防護)/UDLD(單向鏈路檢測)/Self Loop(自循環)/Broadcast Flood(廣播氾濫)/Unknown Multicast Flood(未知多播氾濫)/Unicast Flood(單播氾濫)/ACL(訪問控制表)/Port Security(埠安全)/DHCP Rate Limit(DHCP 速率限制)/ARP Rate Limit(ARP 速率限制)等。

使用者管理員啟用此功能後，如果表中的功能發生錯誤，系統將自動立即阻止錯誤操作，直到設定的時間過後，系統才會自動重新啟用。



- **Recovery Interval :** 錯誤停用連接埠在此時間間隔後自動恢復。
- **BPDU Guard :** 啓用後當發生 BPDU Guard 原因時自動關閉連接埠。
  *該原因是由 STP BPDU Guard 機制引起的。
- **UDLD :** 啓用後發生 UDLD 違規時自動關閉連接埠。
- **Self Loop :** 啓用後發生 Self Loop 原因時自動關閉連接埠。
- **Broadcast Flood :** 啓用後發生 Broadcast Flood 原因時自動關閉連接埠。
  *該原因是廣播速率超過廣播風暴控制速率所造成的。
- **Unknown Multicast Flood :** 啓用後發生 Unknown Multicast Flood 原因時自動關閉連接埠。
  *該原因是未知多播速率超過未知多播風暴控制速率所造成的。
- **Unicast Flood :** 啓用後發生 Unicast Flood 原因時自動關閉連接埠。
  *該原因是單播速率超過單播風暴控制速率所造成的。
- **ACL :** 啓用後發生 ACL 關閉連接埠原因時自動關閉連接埠。
  *該原因是封包匹配 ACL 關閉連接埠的操作造成的。
- **Port Security :** 啓用後發生 Port Security Violation 原因時自動關閉連接埠。
  *該原因是違反連接埠安全規則造成的。
- **DHCP rate limit :** 啓用後發生 DHCP 速率限制時自動關閉連接埠。
  *該原因是 DHCP 封包速率超過 DHCP 速率限制造成的。
- **ARP rate limit :** 啓用後發生 ARP 速率限制原因時自動關閉連接埠。
  *該原因是 ARP 封包速率超過 ARP 速率限制造成的。

*點擊 "Apply" 儲存您的變更設定。*

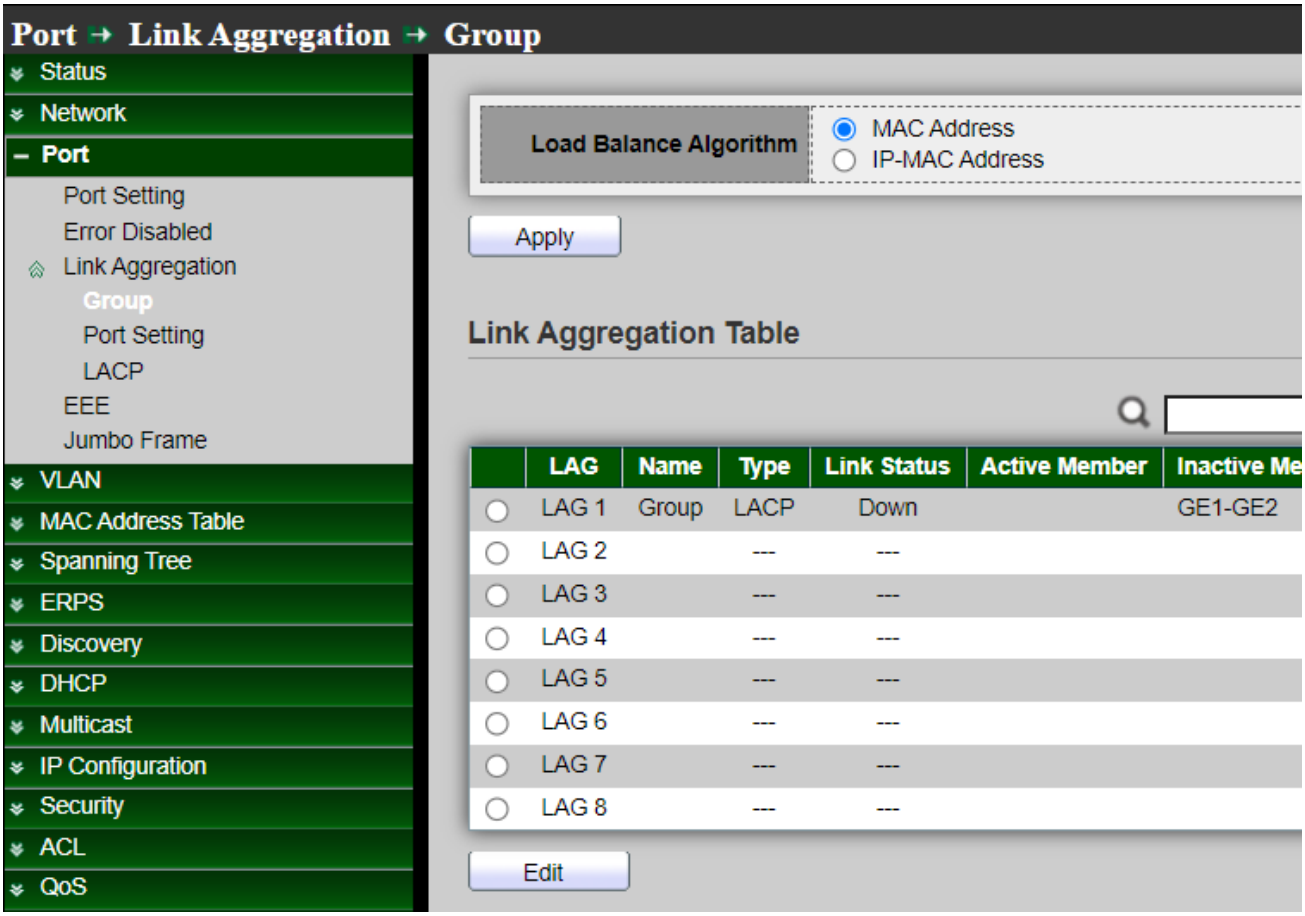
# 5.3 鏈路聚合(Link Aggregation)

Link Aggregation(LA)也稱爲 802.3ad (LACP,鏈路聚合控制協定)的鏈路聚合、分組連接埠埠和連接埠聚合, Port Aggregation 可以將多個物理乙太網埠匯聚一起形成邏輯聚合組。對於上層實體而言，聚合組中的所有物理鏈路當作一條邏輯鏈路。

## 5.3.1 聚合組設定(Group Configuration)

使用者管理員可以選擇使用 MAC 位址或 IP-MAC 位址的負載平衡演算法。

本系統預設可以設定 8 個 LA 組，使用者管理員可以選擇 LAG 編號並點擊 "Edit" 去設定 LA 使用的連接埠。

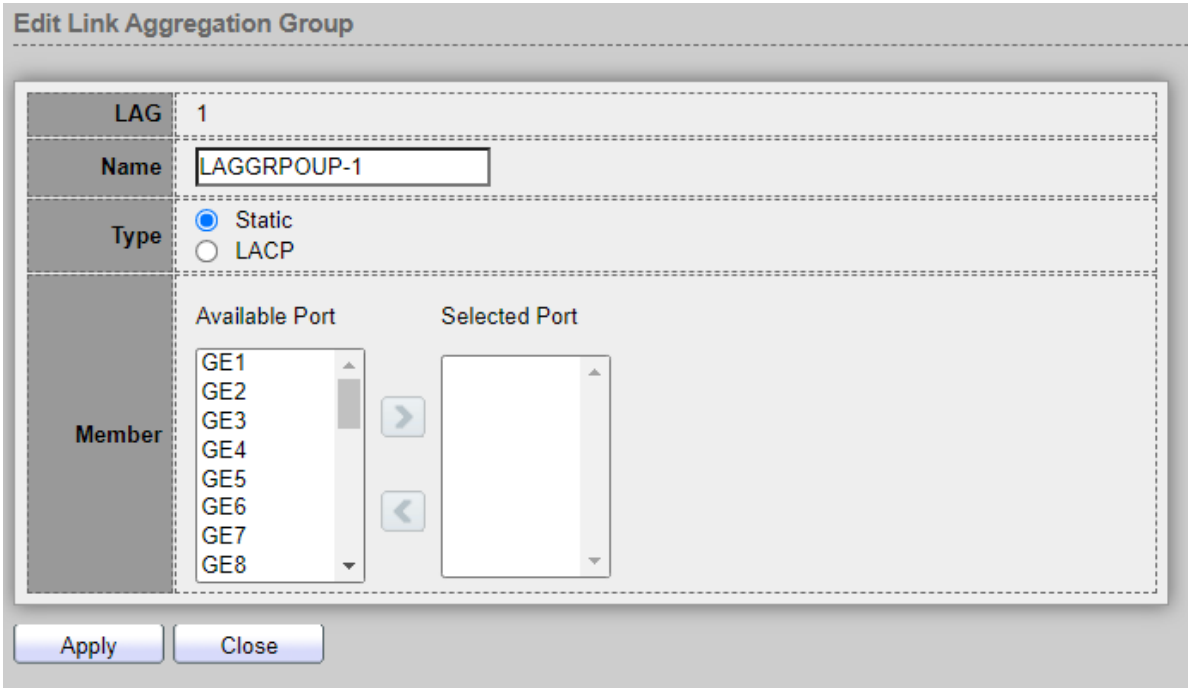



- **Load Balance Algorithm :** LAG 負載平衡演算法。
  - **MAC Address :** 基於 MAC 位址。
  - **IP-MAC Address :** 基於 MAC 位址和 IP 位址。

*點擊 "Apply" 儲存您的變更設定。*

| 欄位 | 描述 |
|---|---|
| LAG | LAG編號 |
| Name | LAG連接埠描述 |
| Type | LAG類型<br>• **Static :** 分配給靜態LAG的連接埠組始終是設定啟用的 |

| | |
|---|---|
| | 成員<br>• **LACP :** 分配給動態LAG的連接埠組為候選埠。LACP決定哪些連接埠是設定啟用的成員埠 |
| Link Status | LAG的連接埠鏈路狀態 |
| Active Member | LAG的設定啟用的成員連接埠 |
| Inactive Member | LAG的非設定啟用的成員連接埠 |

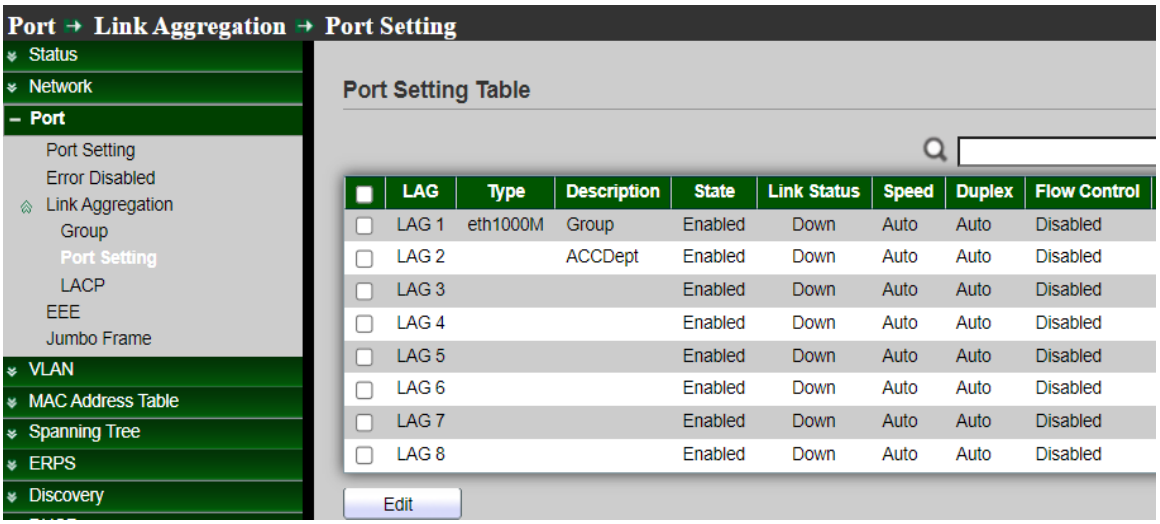



- **LAG :** 選定的 LAG 組 ID。
- **Name :** LAG 連接埠描述。
- **Type :** LAG 類型。
  - **Static :** 分配給靜態 LAG 的連接埠組始終是設定啟用的成員。
  - **LACP :** 分配給動態 LAG 的連接埠組為候選埠。LACP 決定哪些連接埠是設定啟用的成員埠。
- **Member :** 選擇可用連接埠成爲 LAG 組成員埠。

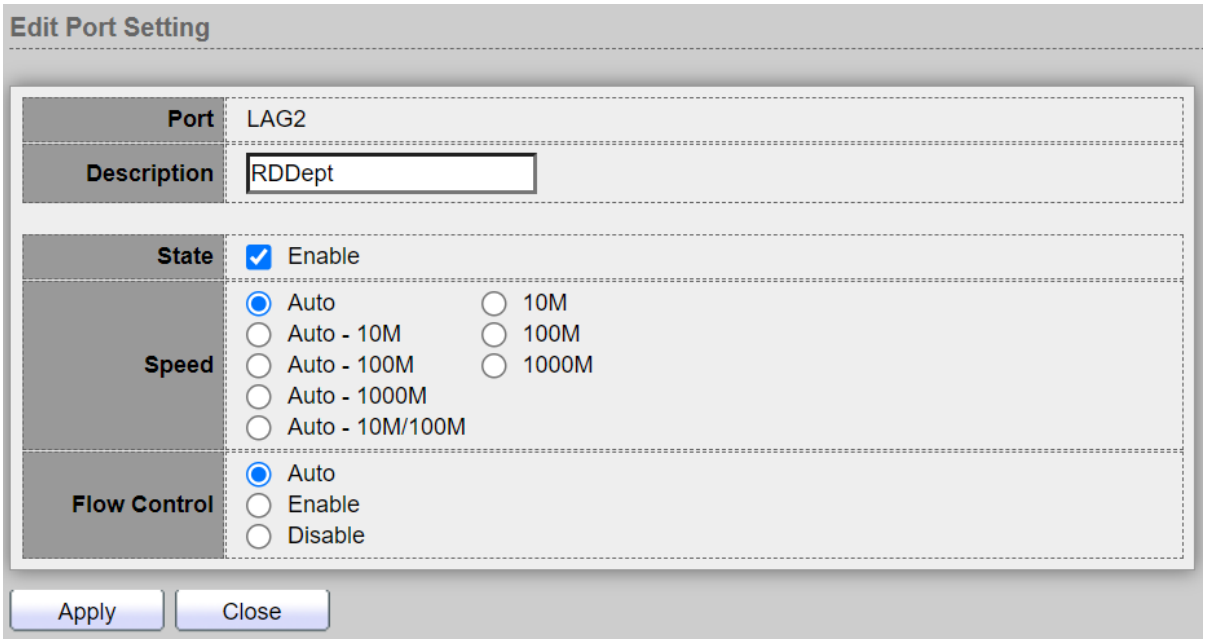
*點擊 **"Apply"** 儲存您的變更，或 **"Close"** 關閉設定。*

### 5.3.2 連接埠設定(Port Setting)

此頁面顯示 LAG 連接埠目前狀態，並允許使用者編輯 LAG 連接埠設定。選擇 LAG 清單並點擊 "Edit" 以編輯 LAG 連接埠設定。




| 欄位 | 描述 |
|---|---|
| LAG | 顯示LAG連接埠編號 |
| Type | 顯示LAG連接埠媒體類型 |
| Description | 顯示自訂LAG連接埠描述 |
| State | LAG連接埠管理狀態<br>• **Enabled :** 埠狀態開啟<br>• **Disabled :** 埠狀態關閉 |
| Link Status | 目前LAG連接埠鏈路狀態<br>• **Up :** 連接埠鏈路已連接<br>• **Down :** 連接埠鏈路已關閉 |
| Speed | 目前 LAG連接埠速度設定和鏈路速度狀態 |
| Duplex | 目前連LAG連接埠雙工設定和鏈路雙工狀態 |
| Flow Control | 目前LAG連接埠流量控制設定和連線的流量控制狀態 |



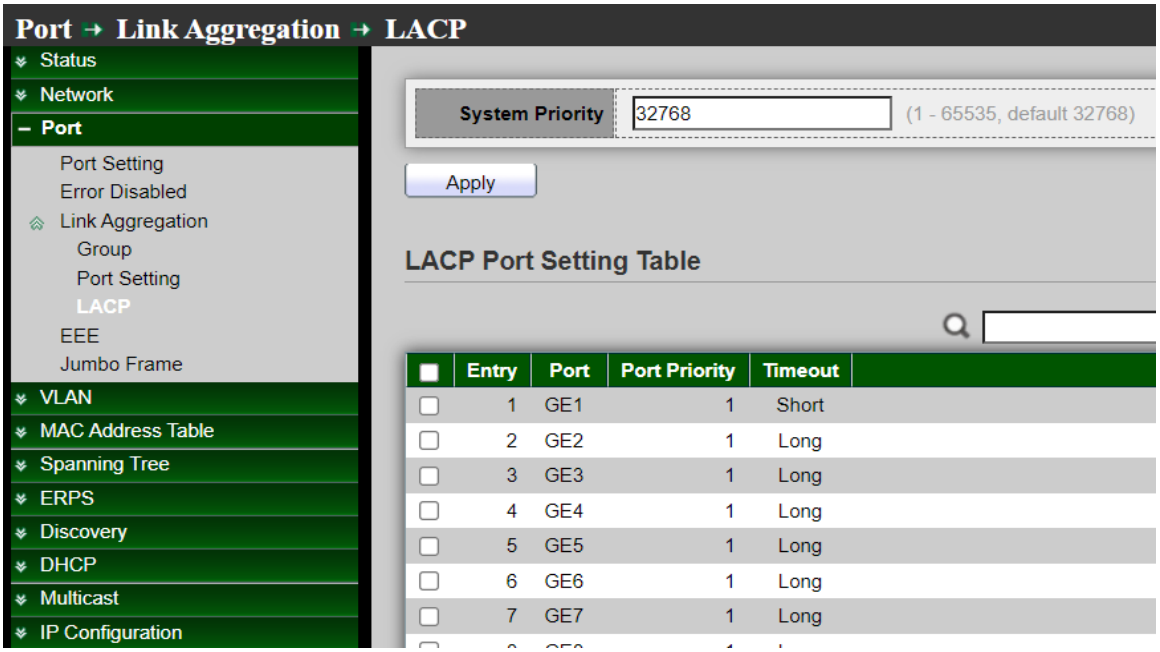

- **Port :** 選定的網路埠清單。
- **Description :** 自訂 LAG 連接埠的描述。
- **State :** 網路埠管理狀態。
  - **Enabled :** 網路埠狀態開啟。
  - **Disabled :** 網路埠狀態關閉。
- **Speed :** 網路埠的速率。
  - **Auto :** 自動判別所有速率。
  - **Auto-10M :** 自動判別到 10M。
  - **Auto-100M :** 自動判別到 100M。
  - **Auto-1000M :** 自動判別到 1000M。
  - **Auto-10M/100M :** 自動判別到 10M/100M。
  - **10M :** 強制速率為 10M。
  - **100M :** 強制速率為 100M。
  - **1000M :** 強制速率為 1000M。
- **Flow Control :** 網路埠的流量控制。
  - **Auto :** 自動判別流量控制。
  - **Enabled :** 啓用流量控制。
  - **Disabled :** 關閉流量控制。

*點擊 "Apply" 儲存您的變更，或 "Close" 關閉設定。*

### 5.3.3 LACP

鏈路聚合控制協議(LACP)可以將多個物理乙太網埠匯聚一起形成邏輯鏈路聚合群組。對於上層實體而言，鏈路聚合群組中的所有物理鏈路當作一條邏輯鏈路。

使用者管理員可以設定 LACP 全域和連接埠設定。選擇連接埠並點擊 “Edit” 來編輯連接埠設定。

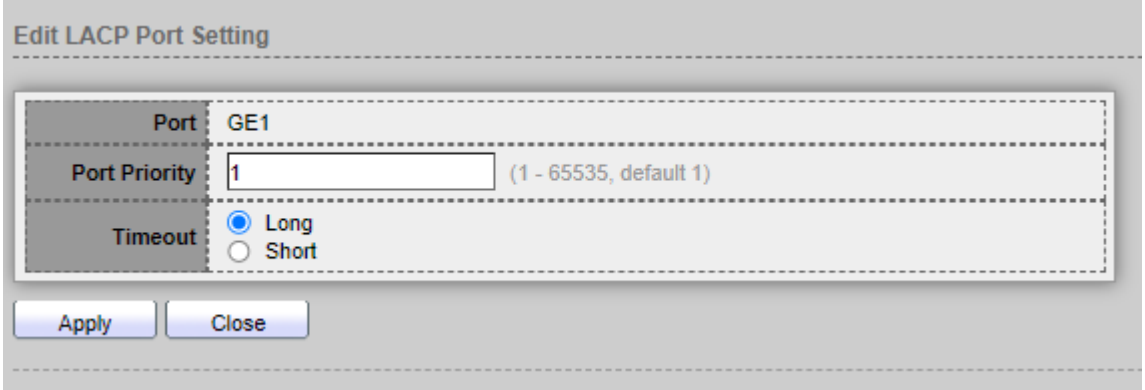



- **System Priority :** 使用者管理員在每台運行 LACP 的交換器上設定 LACP 系統優先級別。LACP 使用系統優先級別和交換器 MAC 位址來形成系統 ID，在與其他交換器協商時使用。這決定了 LACP PDU 中的系統優先級別欄位。

*點擊 **“Apply”** 儲存您的變更設定。*

| Note | 該功能讓系統優先級別值最低的決定每個 LACP 組的 LACP 對象設備之間的鏈路哪些處於設定啟用的狀態，哪些處於待機狀態。鏈路控制端的設備使用連接埠優先級別來確定哪些連接埠到聚合捆綁，哪些連接埠置於待機模式。其他設備(鏈路的非控制端)上的連接埠優先級別將被忽略。在優先級別比較中，數值越低，優先級別越高。因此，LACP 系統優先級別數值低(優先值高)的系統將成為控制系統。如果兩台設備的 LACP 系統優先級別相同(例如，它們都設定為預設設定 32768)，則設備 MAC 位址決定哪個交換器處於控制狀態。 |
|---|---|

| 欄位 | 描述 |
|---|---|
| Port | 連接埠編號 |
| Port Priority | 連接埠的LACP優先級別值 |
| Timeout | LACP PDU的週期性傳輸類型<br>• **Long :** 以慢速週期(30秒)傳送LACP PDU<br>• **Short :** 以快速週期(1秒)傳送LACP PDU |



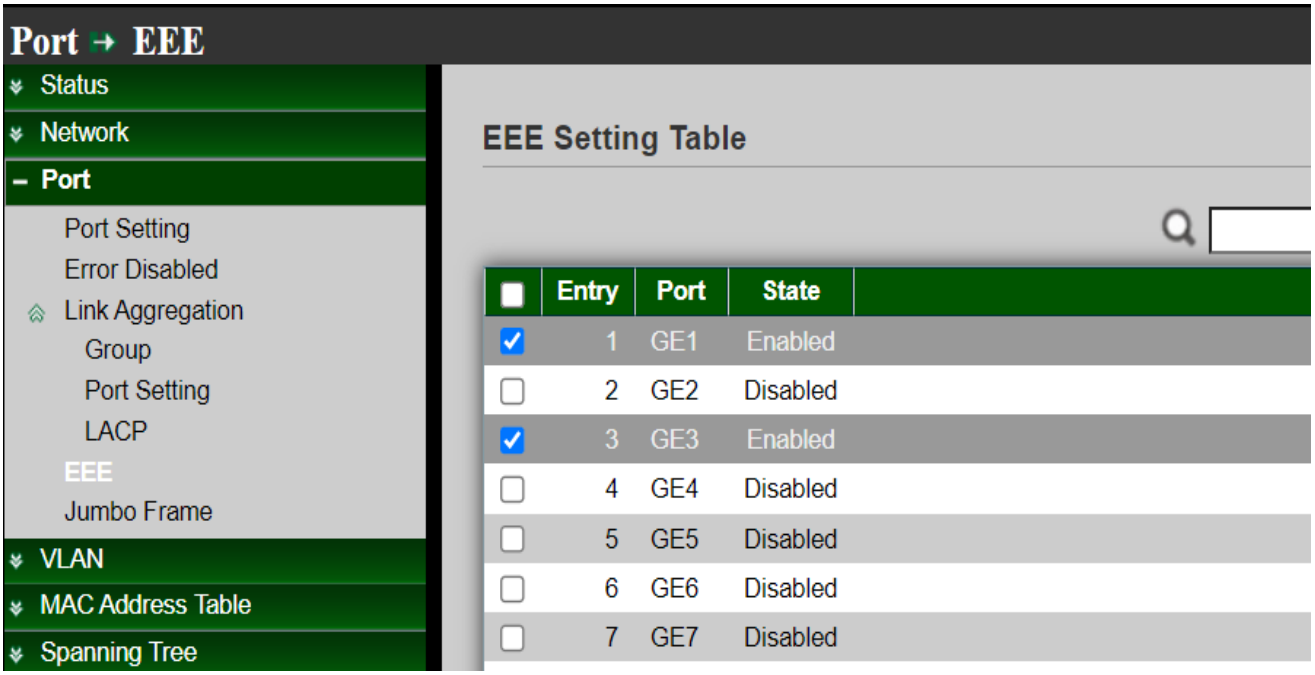

- **Port :** 選定的連接埠清單。
- **Port Priority :** 輸入連接埠的 LACP 優先級別數值。
- **Timeout :** LACP PDU 的週期性傳輸類型。
  - **Long :** 以慢速週期(30 秒)傳送 LACP PDU。
  - **Short :** 以快速週期(1 秒)傳送 LACP PDU。

*點擊 "Apply" 儲存您的變更，或 "Close" 關閉設定。*

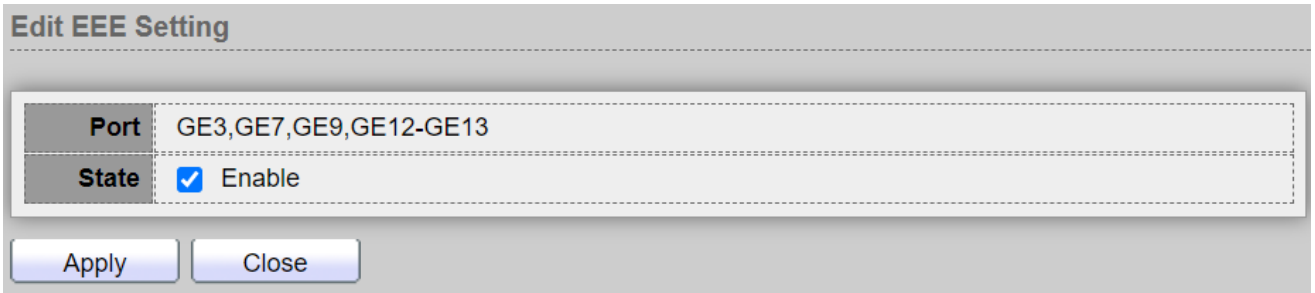
## 5.4 節能乙太網路(EEE)

節能乙太網路(EEE)將 MAC 與一系列支援低功耗模式運行的實體層結合。它由 IEEE 802.3az 節能工作群組定義。低功耗模式使鏈路的發送端和接收端可以在輕負載時停用某些功能，以節省功耗。轉換到低功耗模式不會改變鏈路狀態。轉換到低功耗模式不會遺失或損壞傳輸中的訊框。 轉換時間對於上層協定和應用是透明的。

此交換器支援節能乙太網(EEE)功能。使用者管理員可以透過連接埠設定 EEE 功能的開啓或關閉。預設為“Disable” 。




| 欄位 | 描述 |
|---|---|
| Port | 連接埠編號 |
| State/Operational Status | 連接埠EEE管理狀態<br>• **Enabled** : EEE 已啟用/正在運行<br>• **Disabled** : EEE 已停用/未運行 |

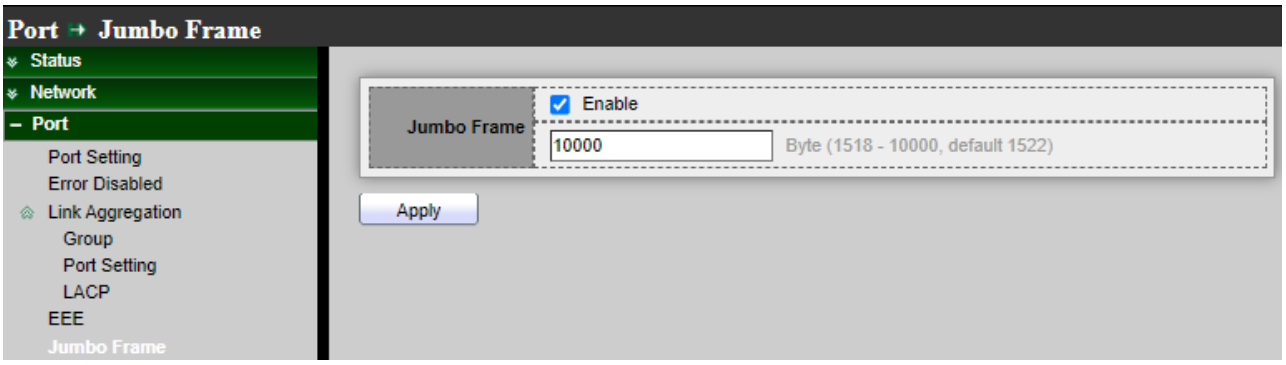


- **Port :** 選定的連接埠清單。
- **State :** 連接埠 EEE 管理狀態。
  - **Enable :** 啓用 EEE。
  - **Disable :** 停用 EEE。

*點擊 "Apply" 儲存您的變更，或 "Close" 關閉設定。*

## 5.5 巨大封包(Jumbo Frame)

使用者管理員可以在此頁面設定巨大封包大小。




- **Jumbo Frame :** 開啓或關閉巨大封包。巨大封包開啓時，交換器允許設定最大封包大小。巨大封包關閉時，將使用預設封包大小 1522。

| Note | 需要使用巨大封包時，交換器允許設定的最大封包大小（10000）。<br>取消應用：<br>當取消選取 "Apply" 後，交換器恢復預設的常規封包大小"1522"。 |
|---|---|

*點擊 "Apply" 儲存您的變更設定。*

# 6.VLAN

虛擬區域網路(VLAN)是指一組具有共同要求的主機，這些主機像連接到同一廣播域一樣進行通訊，無論其實體位置為何。VLAN 與普通區域網路(LAN)有相同的屬性，但 VLAN 允許將終端站分組在一起，即使它們不在同一網路交換器中。

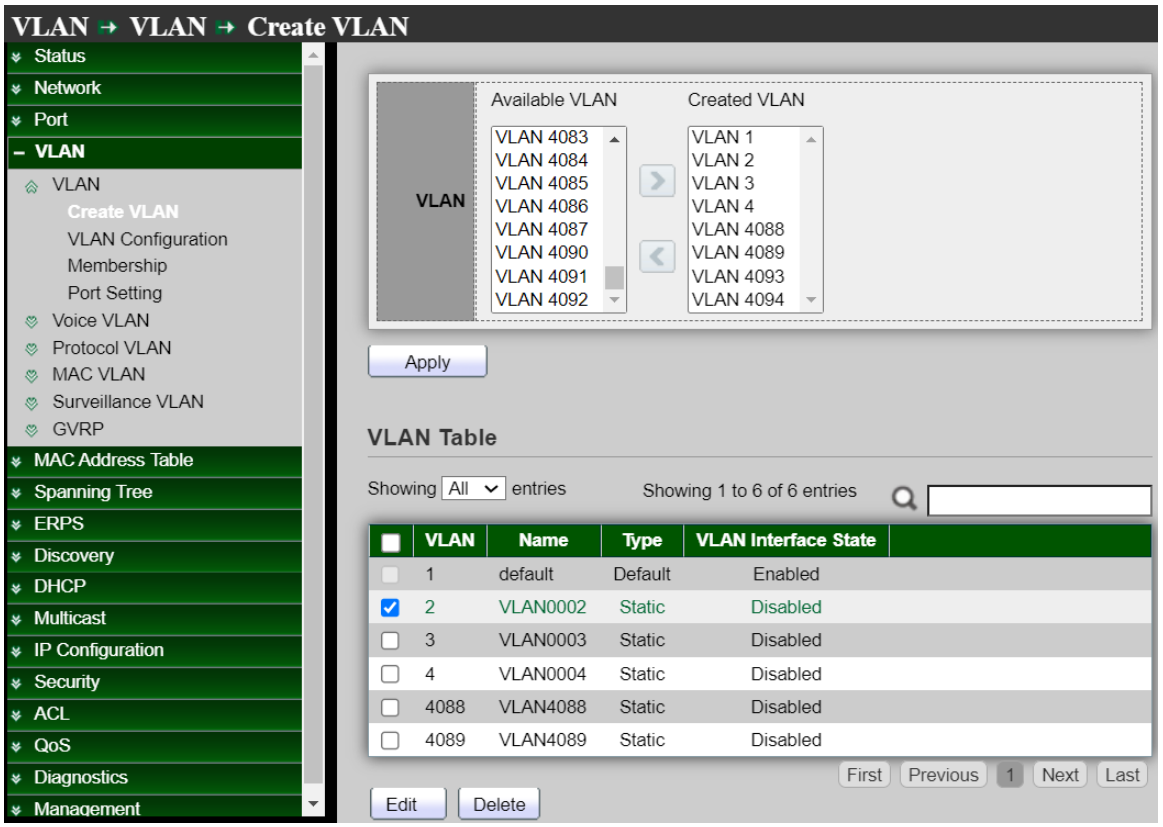
**CS-34816XG** 為第 2 層交換器中新增虛擬區域網(VLAN)支援，提供了橋接和路由的一些優點。像橋接一樣速度很快，VLAN 交換器基於第 2 層表頭轉送流量；並且像路由器一樣，它將網路劃分為邏輯網段，從而提供更好的管理、安全性和多播流量管理

使用者管理員可以設定基於 IEEE 802.1q **標簽**的 VLAN 或基於連接埠的 VLAN。系統預設基於 VLAN1 連接埠(PVID)。

## 6.1 VLAN

### 6.1.1 創建 VLAN(Create VLAN)

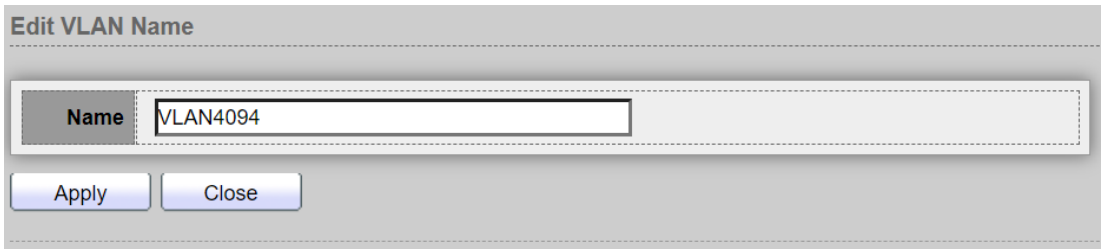
使用者管理員可以在 Available VLAN 清單中選擇 VLAN 編號，該 VLAN 編號基於 IEEE 802.1q 標準。Available VLAN 清單可以多選。



- **VLAN :** 使用者管理員在"Available VLAN"表中選擇 VLAN 編號，移動到"Created VLAN"表，這樣就完成了 802.1q VLAN。

*點擊 **"Apply"** 儲存您的變更設定。*

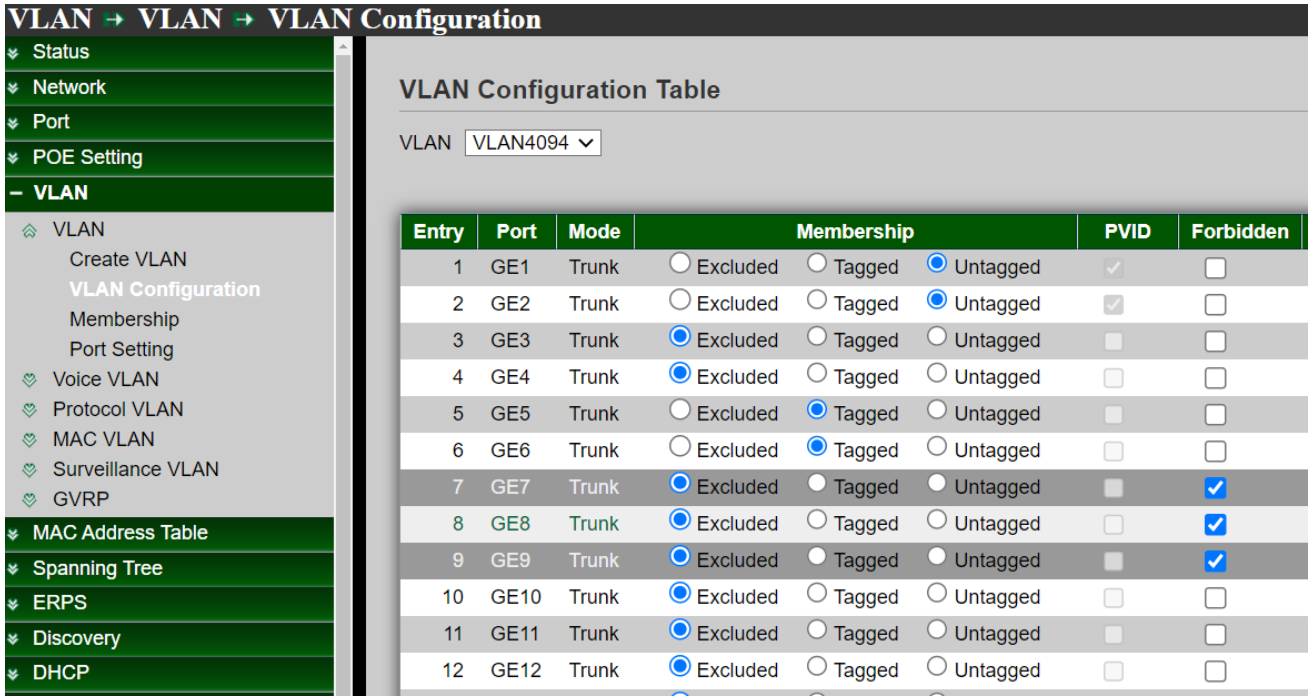
**VLAN Table :** 使用者管理員可以勾選要編輯或刪除的 VLAN，如果選中並點擊"Edit"，則使用者管理員可以手動修改該 VLAN 的名稱描述。




*點擊**"Apply"**儲存您的變更，或**"Close"**關閉設定。*

## 6.1.2 VLAN 設定(VLAN Configuration)

使用者管理員可以選擇在連接埠和 LAG 的成員資格表中設定 Excluded / Forbidden / Tagged / Untagged 功能。



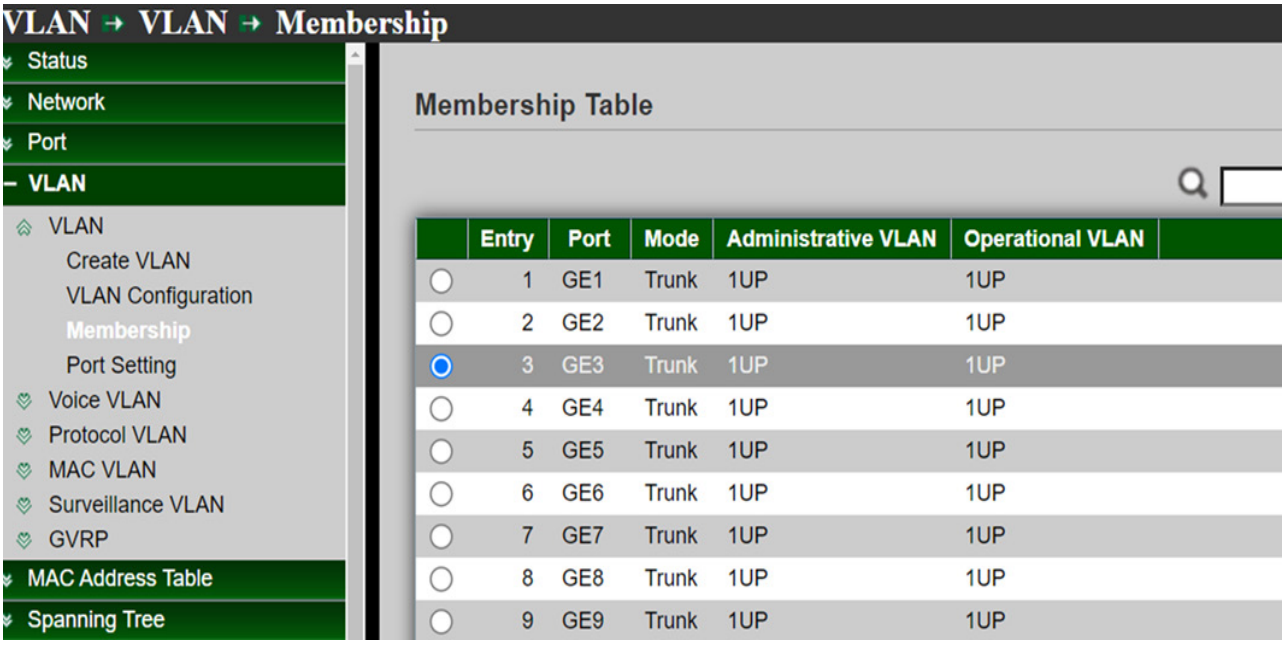
| 欄位 | 描述 |
|---|---|
| VLAN | 選擇指定的 VLAN ID 設定 VLAN |
| Port | 顯示連接埠清單介面 |
| Mode | 顯示連接埠 VLAN 模式介面 |
| Membership | 為該連接埠選擇指定 VLAN ID 的成員資格<br>• **Excluded :** 指定連接埠在 VLAN 中被排除<br>• **Tagged :** 指定連接埠在 VLAN 中是 tagged 成員<br>• **Untagged :** 指定連接埠在 VLAN 是 untagged 成員 |
| PVID | 顯示介面是否爲 PVID |
| Forbidden | 選中後指定連接埠在 VLAN 中被禁用 |

- **VLAN :** 使用者管理員可以點選下拉選單選擇 VLAN 並進行設定。
  - **Excluded :** 該介面目前不是 VLAN 的成員。這是所有連接埠和 LAG 的預設值。
  - **Tagged** : 該介面是 VLAN 的 tagged 成員。
  - **Untagged** : 該介面是 VLAN 的 untagged 成員。VLAN 的封包不加表頭被轉送到介面 VLAN
  - **PVID** : 勾選將介面 PVID 設定為 VLAN 的 VID。PVID 是按每個連接埠設定的。
  - **Forbidden :** 選擇禁用指定連接埠。

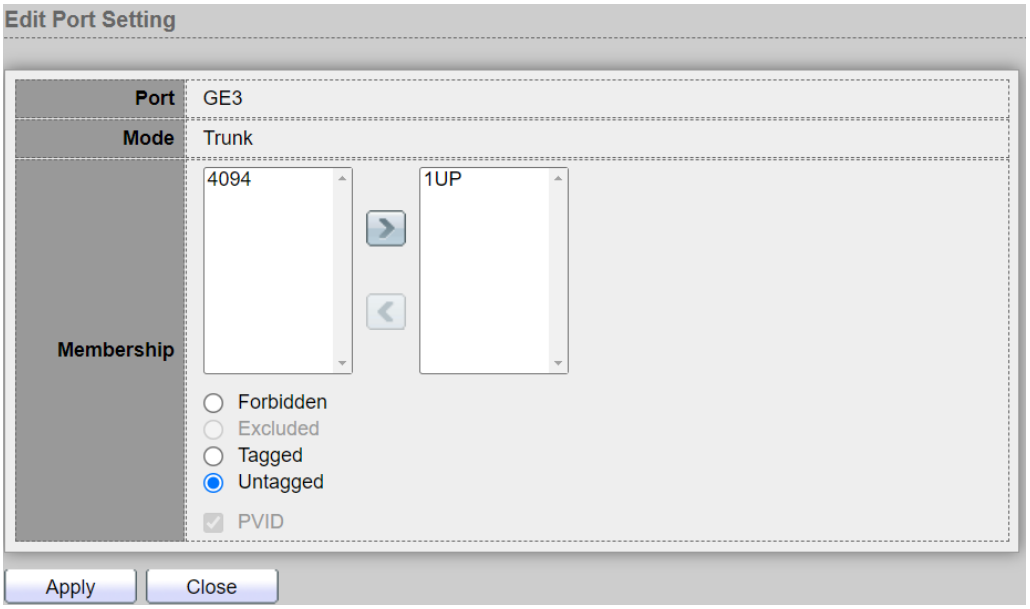
### 6.1.3 成員資格(Membership)

顯示所有連接埠設定資訊。使用者管理員可以勾選複選框並點擊 “Edit” 修改 VLAN 類型。*(Note : Number=VLAN number, F=Forbidden, T=Tagged, U=Untagged, P=PVID)*

當禁止連接埠成爲預設 VLAN 成員時，該連接埠也不允許成為任何其他 VLAN 的成員。將為該連接埠分配內部 VID 4095。如果兩個設備之間的連接埠要向 VLAN 傳送和接收 untagged 封包，則兩個設備之間的連接埠上的 PVID 必須相同。否則，流量可能會從一個 VLAN 洩漏到另一個 VLAN。




| 欄位 | 描述 |
|---|---|
| Port | 顯示連接埠清單介面 |
| Mode | 顯示連接埠 VLAN 模式介面 |
| Administrative VLAN | 顯示該連接埠的 VLAN 管理列表 |
| Operational VLAN | 顯示該連接埠的 VLAN 運行列表。Operational VLAN 是指設備中真正運行的 VLAN 狀態。可能與管理 VLAN 不同 |

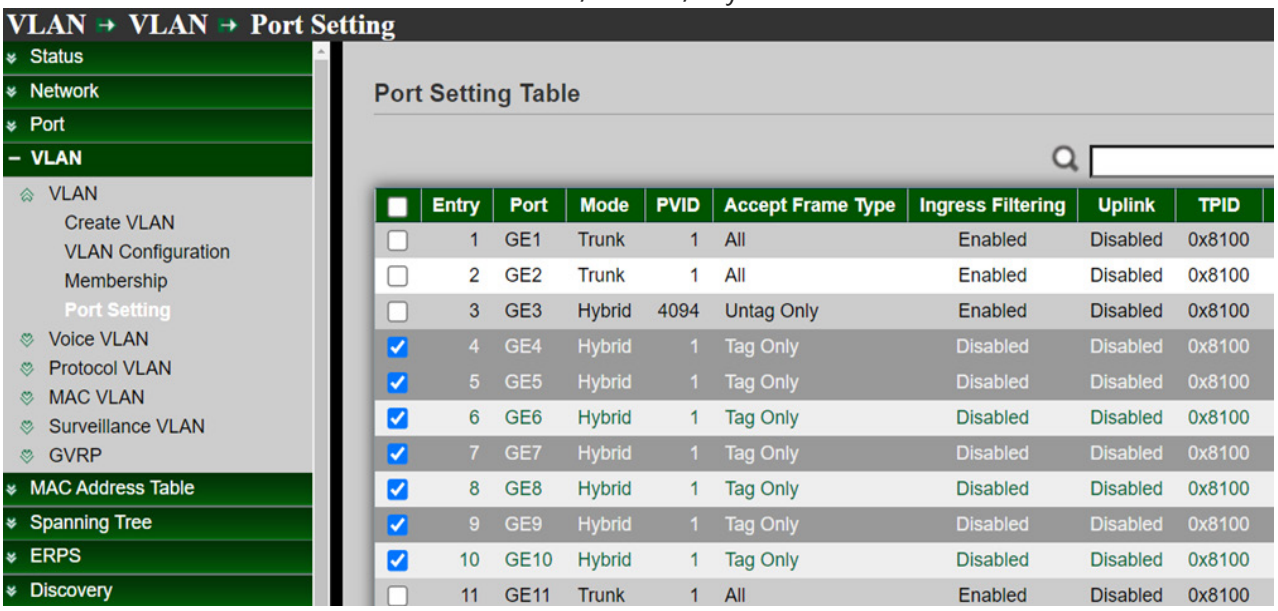


- **Port :** 顯示所選的連接埠編號。
- **Mode :** 顯示在介面設定頁面上所選的連接埠 VLAN 模式。
- **Membership :** 點擊箭頭按鈕將 VLAN ID 從左側列表移至右側列表。如果預設 VLAN 是 tagged，則可能會出現在右側列表中，但無法選中。

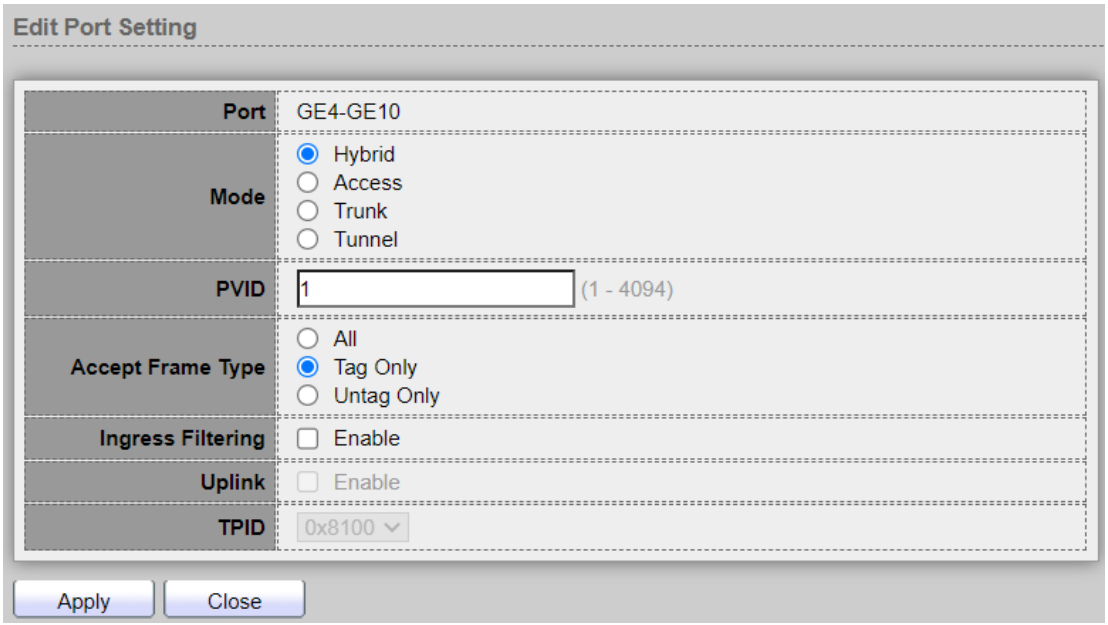
*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

### 6.1.4 Port Setting

使用者管理員可以設定 VLAN 模式 Access / Trunk / Hybrid。




| 欄位 | 描述 |
|---|---|
| Port | 顯示介面 |
| Mode | 顯示連接埠 VLAN 模式 Hybrid/Access/Trunk/Tunnel |
| PVID | 顯示連接埠的 PVID |
| Accept Frame Type | 顯示連接埠的接收封包類型 |
| Ingress Filtering | 顯示連接埠的入口過濾器狀態 |
| Uplink | 顯示上行鏈路狀態 |
| TPID | 顯示介面使用的 TPID |



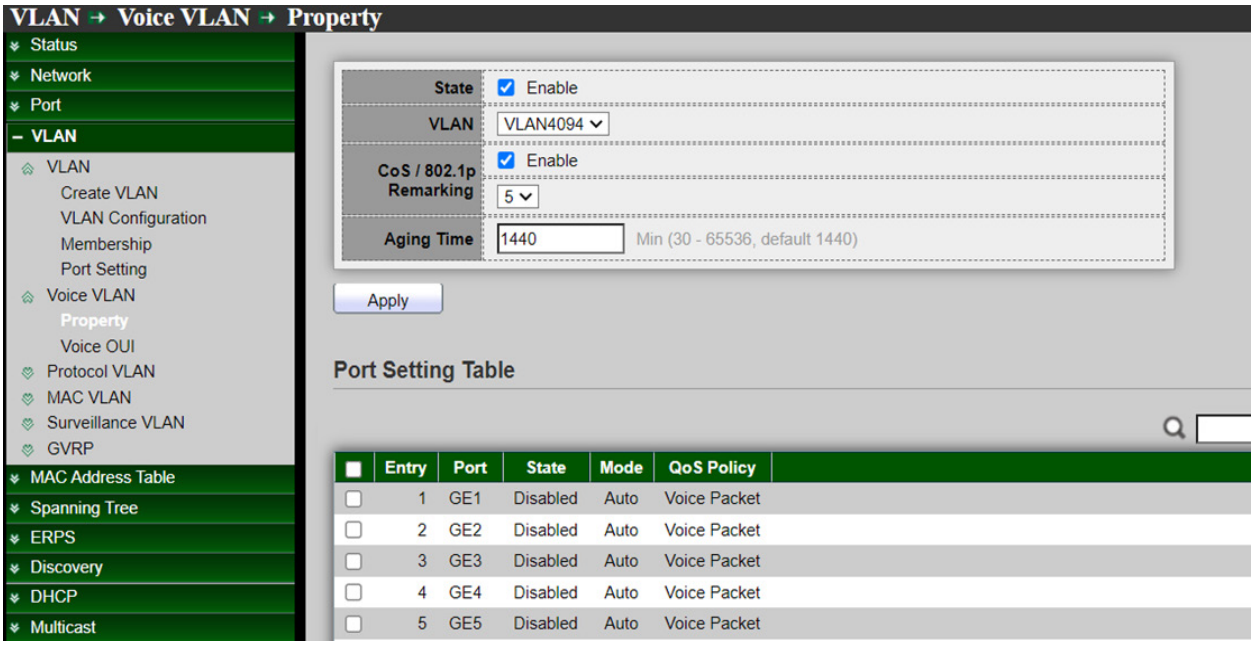

- **Hybrid :** 此介面可以是一個或多個 VLAN 的 tagged 或 untagged 成員。
- **Access :** 此介面是單一 VLAN 的 untagged 成員。以這種模式設定的連接埠被稱為存取連接埠。
- **Trunk :** 此介面是最多一個 VLAN 的 untagged 成員，並且是零個或多個 VLAN 的 tagged 成員。在此模式下設定的連接埠稱為中繼埠。
- **Tunnel :** 這能讓使用者可以在提供者網路中使用自己安排的 VLAN (PVID)。
- **PVID :** 輸入 VLAN 的連接埠 VLAN ID(PVID)，傳入的 untagged 訊框和 priority tagged 訊框歸入該 VLAN。
- **Accept Frame Type :** 選擇介面允許接收的訊框類型。不屬於設定類型的訊框將在入口處被丟棄。這些訊框類型僅在常規模式下可用。如下所示。
  - **All :** 此介面接受所有類型的訊框：untagged 訊框、tagged 訊框和 priority tagged 訊框。
  - **Tag Only :** 介面只接收 tagged 的訊框。
  - **Untag Only :** 介面只接受 untagged 和 priority tagged 的訊框。
- **Ingress Filtering :** 使用者管理員可以選取 “Enable” 以啟用入口過濾。當介面啟用入口過濾時，該介面將丟棄所有分類為不屬於介面成員 VLAN 的傳入訊框。一般連接埠可停用或啟用入口過濾。在存取連接埠和中繼連接埠上總是啟用的。
- **Uplink :** 使用者管理員可以選中” **Enable**” 將介面設定為上行鏈路連接埠。
- **TPID :** 如果 Uplink 已啟用，為介面選擇修改的標簽協定識別符(TPID)值。

*點擊"**Apply**"儲存您的變更，或"**Close**"關閉設定。*

# 6.2 語音 VLAN(Voice VLAN)

語音 VLAN 可讓您透過設定連接埠來傳輸來自特定 VLAN 上 IP 電話的 IP 語音流量，從而增強 VoIP 服務。VoIP 流量在來源 MAC 位址中具有預先設定的 OUI 前綴。 使用者管理員可以在 1 到 4094 範圍內設定 VLAN ID。

## 6.2.1 Property




- **State :** 使用者管理員可以選擇 “Enable” 或” Disable” 該功能。
- **VLAN :** 使用者管理員能夠選擇 VLAN。
- **CoS / 802.1P Remarking :** 使用者管理員可以為 VLAN 設定 CoS 802.1p 優先級別。
- **Port Aging Time :** 使用者管理員可以設定此規則的延遲時間。

*點擊"Apply"儲存您的變更設定。*

| 欄位 | 描述 |
|---|---|
| Port | 顯示連接埠清單 |
| State | 顯示介面打開/關閉狀態 |

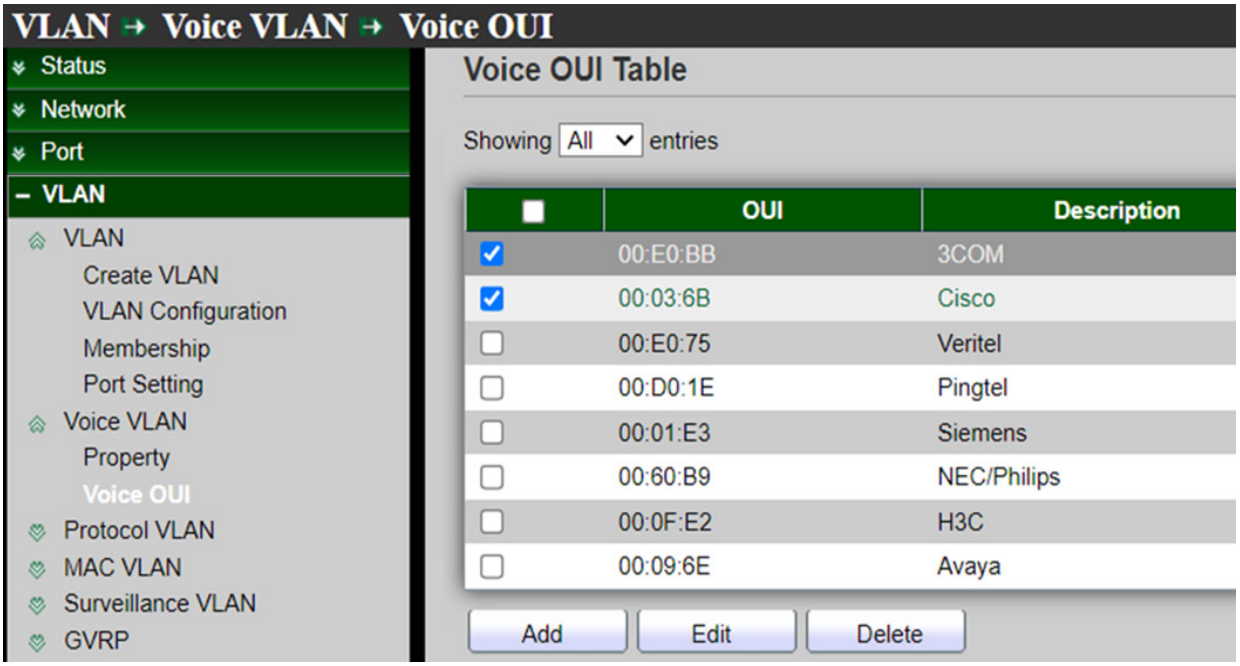
| | |
|---|---|
| **Mode** | 顯示語音VLAN模式 |
| **QoS Policy** | 顯示語音VLAN備註QoS使用策略 |


- **Port :** 顯示連接埠清單。
- **State :** 介面打開/關閉狀態。
- **Mode :** 選擇語音 VLAN 模式。
- **Qos Policy :** 選擇語音 VLAN 備註 QoS 使用策略。

*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

### 6.2.2 語音 OUI(Voice OUI)

組織唯一標識符(OUI)是 MAC 位址的前三個字節，而後三個字節包含獨特的站 ID。使用者管理員可以通過 OUI 新增特定製造商。 新增 OUI 後，語音 VLAN 連接埠從列出的 OUI 特定 IP 電話接收到的所有流量，都會在語音 VLAN 上轉送。與根據電話 OUI 檢測語音設備的電話 OUI 模式不同，自動語音 VLAN 模式依賴自動智慧連接埠將連接埠動態添加到語音 VLAN。預設為語音電話設定了 8 種樣品描述。




| 欄位 | 描述 |
|---|---|
| OUI | 顯示QUI MAC位址 |
| description | 顯示OUI清單描述。 |


使用者管理員可以創建新的 OUI 或修改或刪除表中的 OUI

點擊 **“add”** 加入創建新的 OUI。

點擊 **“Edit”** 修改 OUI 資料。

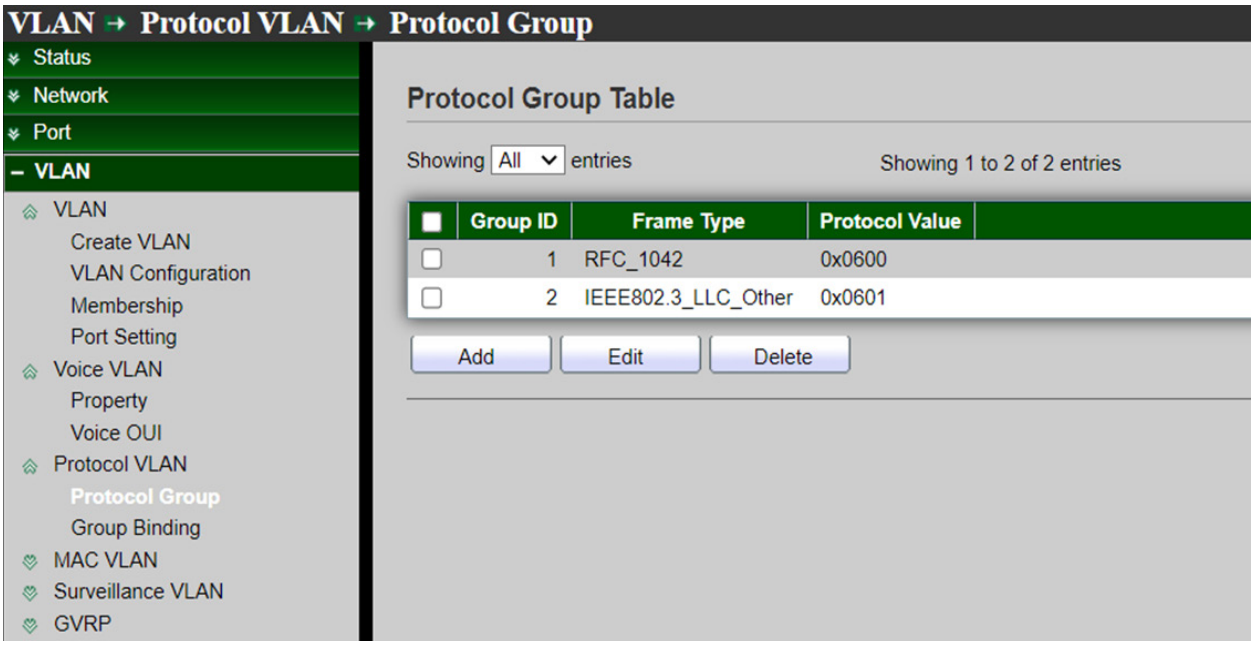
點擊 **“Delete”** 刪除 OUI 資料。

*點擊**"Apply"**儲存您的變更，或**"Close"**關閉設定。*

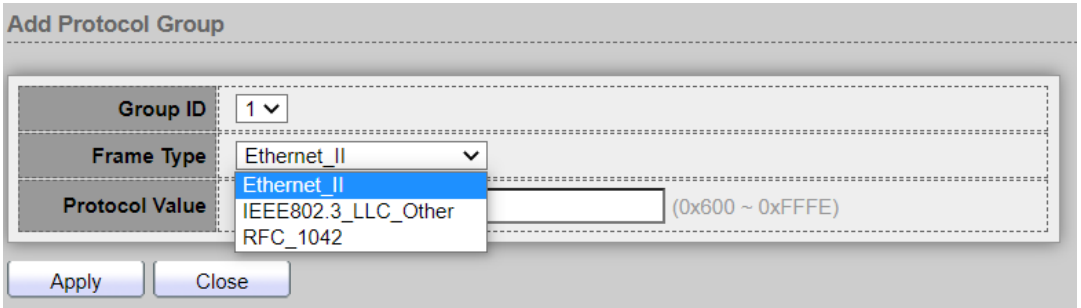
# 6.3 協定 VLAN(Protocol VLAN)

## 6.3.1 協定群組(Protocol Group)

使用者管理員可以在此頁面設定新增或編輯協定 VLAN 的群組，並設定“add”、“Edit”和“Delete”功能進行管理。




| 欄位 | 描述 |
|---|---|
| Group ID | 顯示清單的群組ID |
| Frame Type | 顯示清單的封包類型 |
| Protocol Value | 顯示清單的協定數值 |



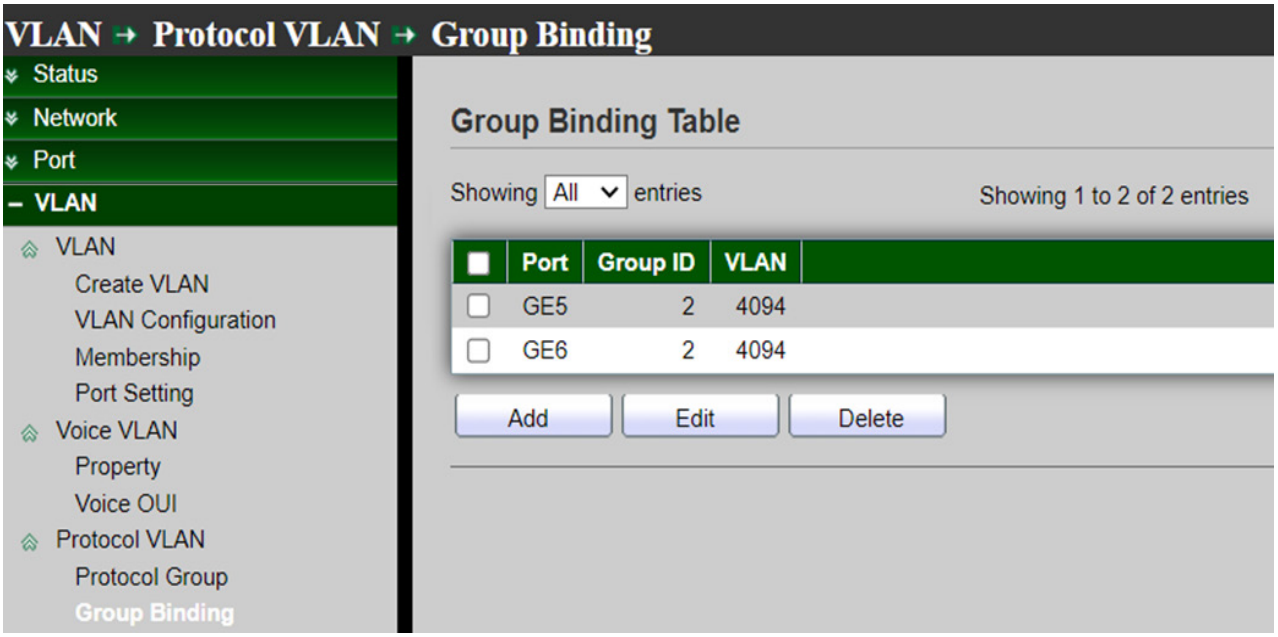

➢ **Group ID**：選擇清單的群組 ID。範圍為從 1 到 8。

- **Frame Type :** 透過檢查封包表頭中的八位元組來發現與其關聯的協定類型，選擇將封包映射到協定定義的 VLAN 的清單的訊框類型。
  - **Ethernet_II :** 封包類型是 Ethernet_II
  - **IEEE802.3_LLC_Other :** 封包類型是 802.3 封包，帶有 LLC 其他表頭。
  - **RFC_1042 :** 封包類型是 rfc 1042 封包。
- **Protocol Value :** 輸入目標協定的協定值。符合此協定值的封包被分類到指定的 VLAN ID。

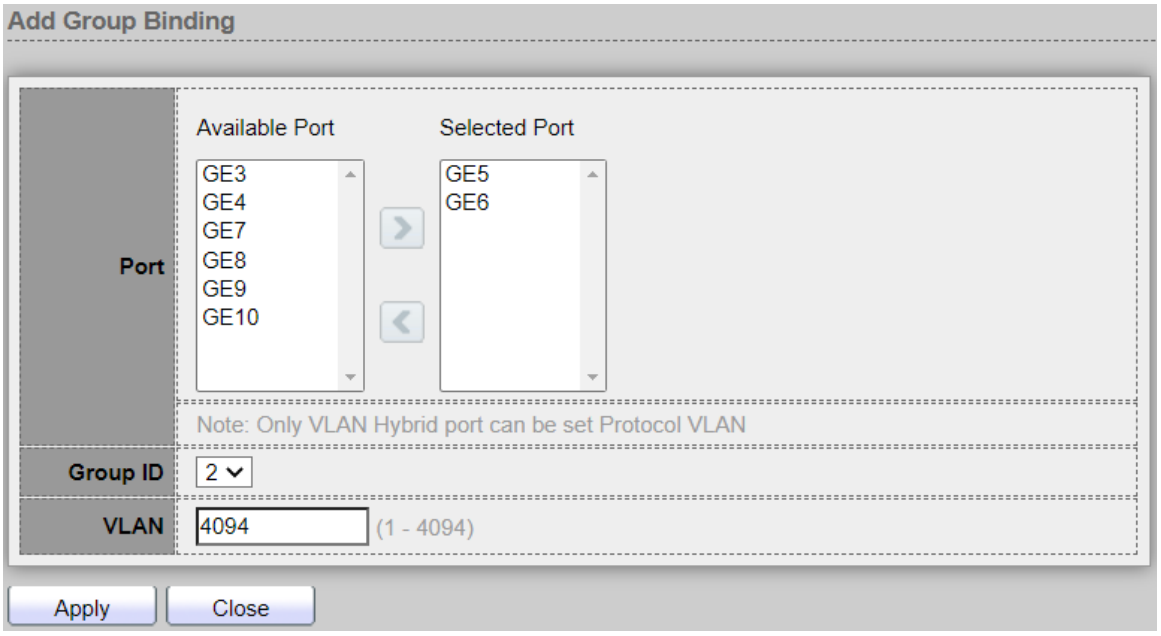
*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

### 6.3.2 群組綁定(Group Binding)

使用者管理員可以為每個連接埠設定帶有 VLAN ID 的綁定協定 VLAN 群組，並設定“**add**”、“**Edit**”和“**Delete**”功能進行管理。




| 欄位 | 描述 |
|---|---|
| Port | 顯示與協定組清單與綁定的連接埠號 |
| Group ID | 顯示連接埠綁定的群組ID |
| VLAN | 顯示分配給符合協定群組的封包的VLAN ID |




- **Port :** 在左側框中選擇連接埠，然後移到右側與協定組綁定。或在右側框中選擇連接埠，然後移到左側解除與協定組的綁定。只能選擇具有混合 VLAN 模式的介面並與協定群組綁定。僅適用於 “Add” 對話框中。
- **Group ID :** 選擇與連接埠相關聯的群組 ID。僅適用於 “Add” 對話框。
- **VLAN :** 輸入分配給符合協定群組的封包的 VLAN ID。

*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

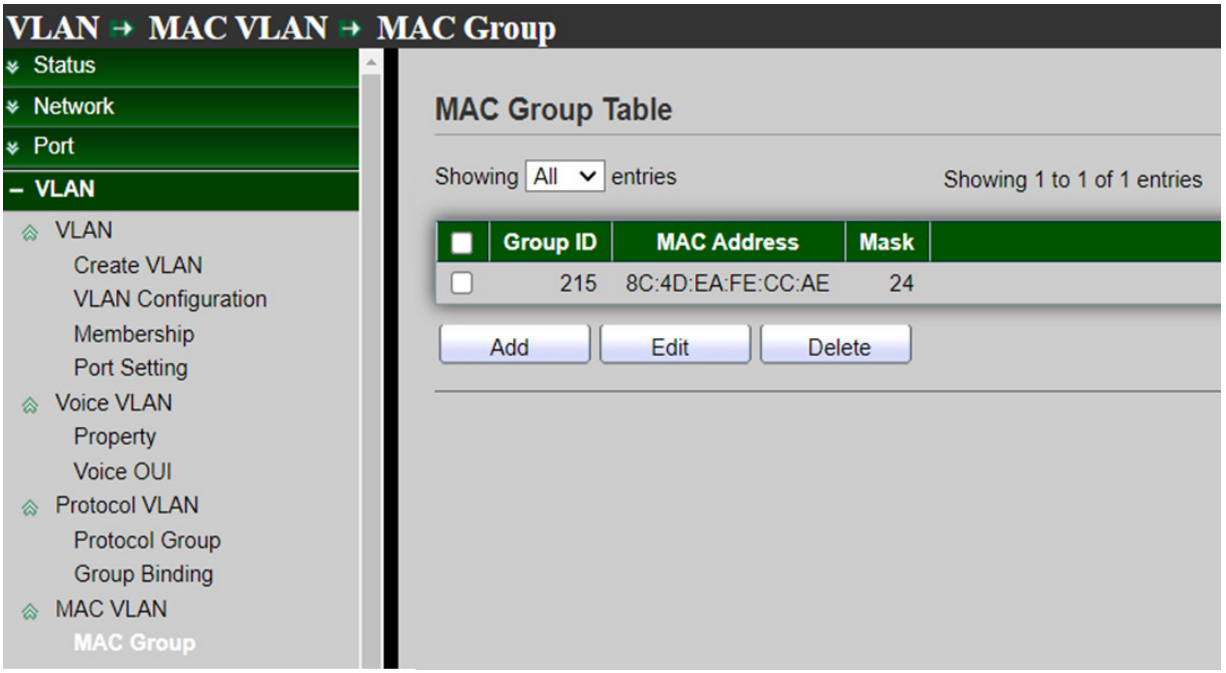
# 6.4 MAC VLAN

## 6.4.1 MAC 群組(MAC Group)

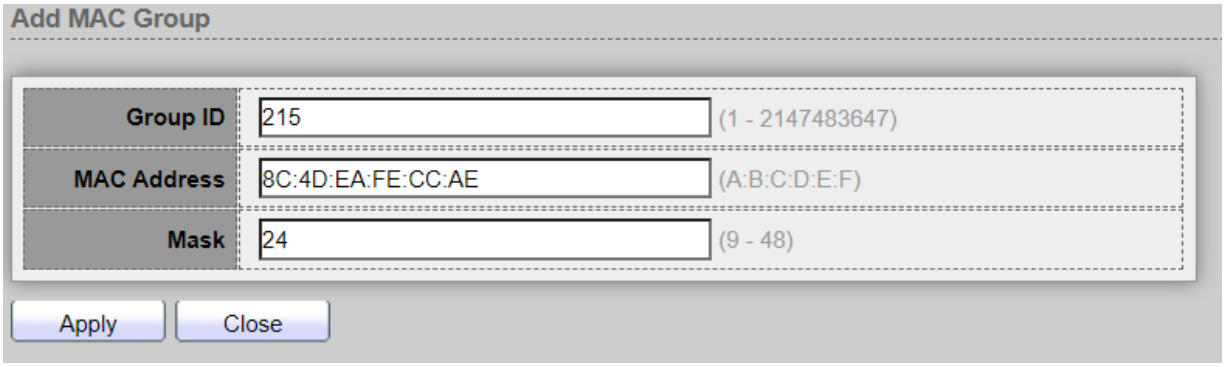
MAC VLAN 功能允許將傳入的 untagged 封包分配到 VLAN，從而根據封包的來源 MAC 位址對流量進行分類。您可以透過設定 MAC 到 VLAN 表中的清單來定義 MAC 到 VLAN 的映射。使用來源 MAC 位址和適當的 VLAN ID 可指定清單。設備的所有連接埠共用 MAC 到 VLAN 設定 ( 即有一個全系統表，其中包含 MAC 位址到 VLAN ID 的映射 )。

當 untagged 或 priority tagged 的封包到達交換器且 MAC 到 VLAN 表中存在清單時，將會尋找封包的來源 MAC 位址。如果找到清單，則將相應的 VLAN ID 指派給封包。如果封包已經 priority tagged，它將保持該值；否則，優先級別將設定為 0(零)。指派的 VLAN ID 將根據 VLAN 表進行驗證。如果 VLAN 有效，則繼續對封包進行入口處理;否則，將丟棄封包。這意味您可以設定 MAC 位址映射到系統上尚未創建的 VLAN，

並設定“add”、“Edit”和“Delete”功能進行管理。




| 欄位 | 描述 |
|---|---|
| Group ID | 顯示清單的群組ID |
| MAC Address | 顯示清單的MAC位址 |
| Mask | 顯示分類封包的MAC位址遮罩 |

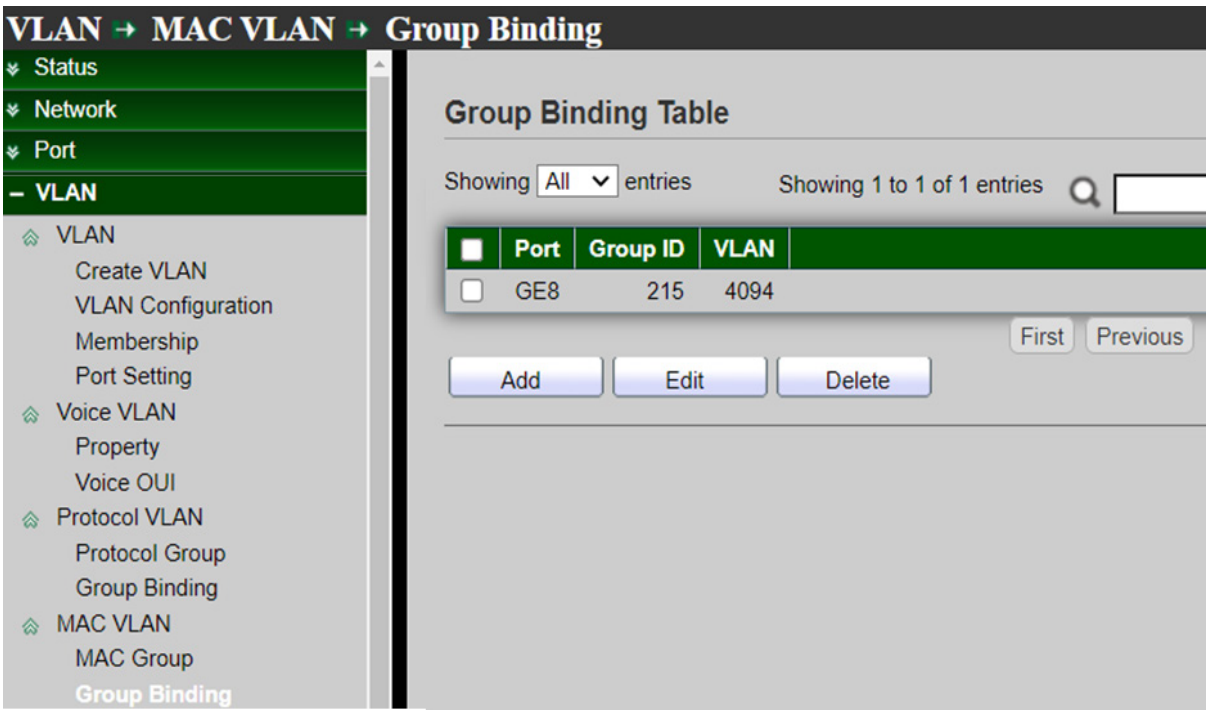



- **Group ID :** 新增群組 ID 號碼。
- **MAC Address :** 輸入 MAC 位址。
- **Mask :** 輸入分類封包的 MAC 位址遮罩。

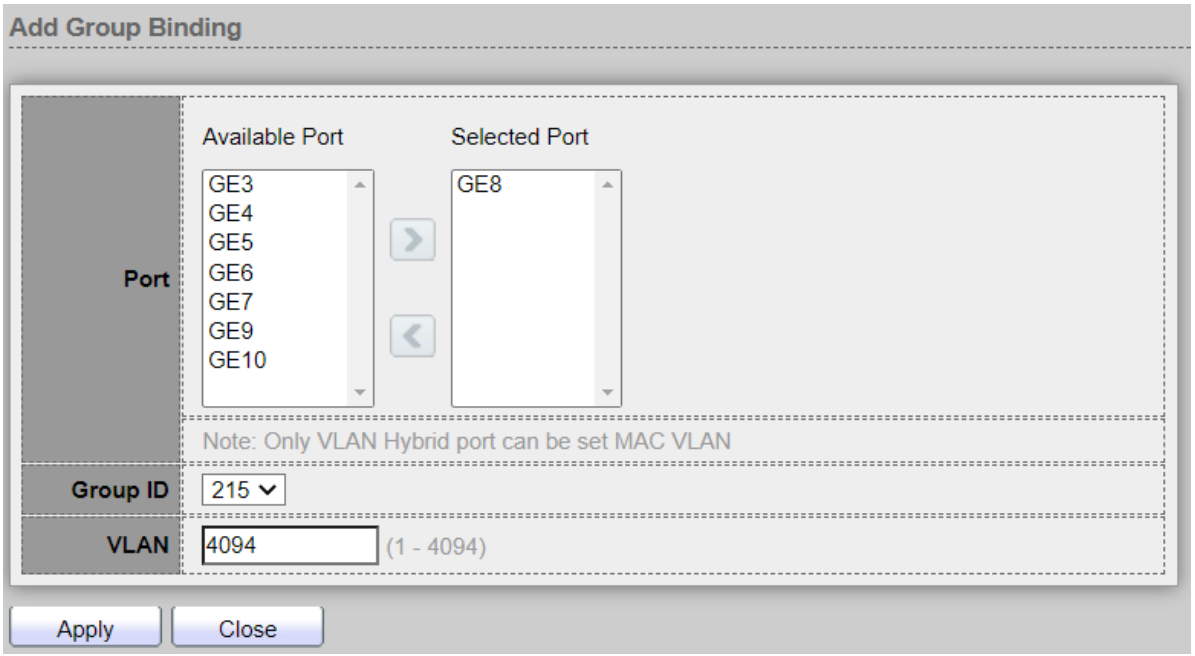
*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

### 6.4.2 群組綁定(Group Binding)

Group Binding 功能允許使用者將 MAC VLAN 群組與每個連接埠的 VLAN ID 綁定， 並設定 **“add”** 、 **“Edit”** 和 **“Delete”** 功能進行管理。




| 欄位 | 描述 |
|---|---|
| Port | 顯示與協定群組清單綁定的連接埠 ID |
| Group ID | 顯示連接埠綁定的群組 ID |
| VLAN | 顯示分配給符合協定群組封包的 VLAN ID |



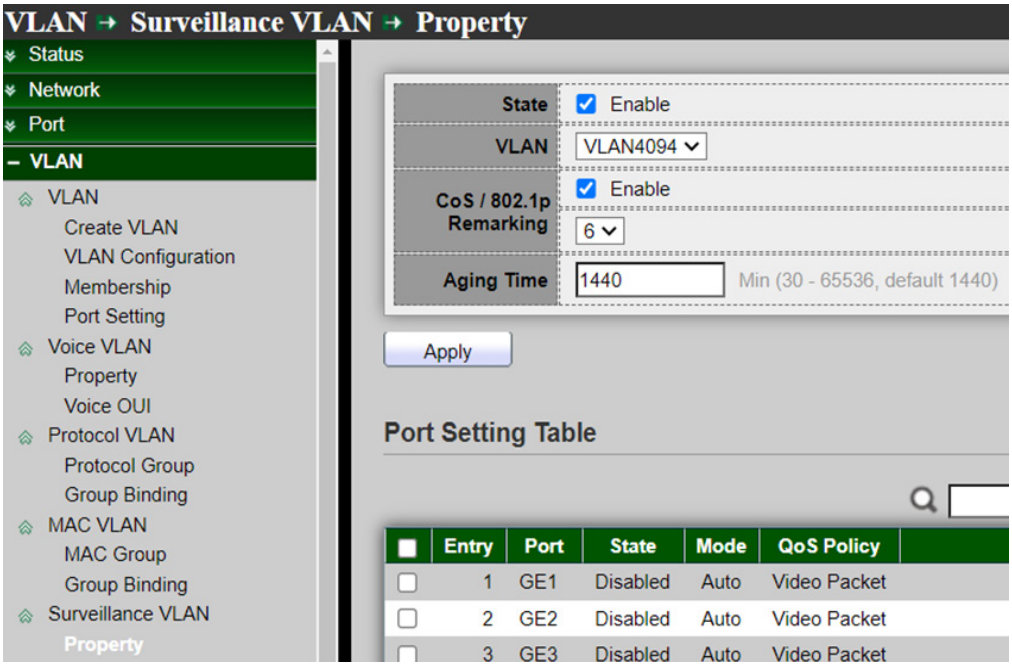

- **Port :** 在左側框中選擇連接埠，然後移到右側與 MAC 組綁定。或在右側框中選擇連接埠，然後移到左側解除與 MAC 組的綁定。只能選擇具有混合 VLAN 模式的介面並與協定群組綁定。
- **Group ID :** 選擇與連接埠相關聯的群組 ID。
- **VLAN :** 輸入分配給符合 MAC 群組的封包的 VLAN ID。

*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

# 6.5 監控 VLAN(Surveillance VLAN)

## 6.5.1 優先級別(Property)

使用者管理員可以透過設定頁面來設定 Surveillance VLAN 的全域和每個介面的設定。




- **State :** 勾選複選框以啟用或停用 Surveillance VLAN 功能。
- **VLAN :** 選擇 Surveillance VLAN ID。Surveillance VLAN ID 不能是預設 VLAN。
- **Cos/802.1p :** 選擇 VPT 值。符合條件的封包會使用此 VPT 值作為內部優先級別。
- **Remarking :** 設定復選框以啟用或停用標記。如果啟用，符合條件的封包會對此值進行標記。
- **Aging Time :** 輸入延遲時間值。預設值為 1440 分鐘。如果沒有任何封包通過，視訊 VLAN 清單會在此時間過後過時。

*點擊"Apply"儲存您的變更設定。*

**Port Setting Table**

| Entry | Port | State | Mode | QoS Policy |
|---|---|---|---|---|
| 1 | GE1 | Disabled | Auto | Video Packet |
| 2 | GE2 | Disabled | Auto | Video Packet |
| 3 | GE3 | Disabled | Auto | Video Packet |
| 4 | GE4 | Disabled | Auto | Video Packet |
| 5 | GE5 | Disabled | Auto | Video Packet |
| 6 | GE6 | Disabled | Auto | Video Packet |
| 7 | GE7 | Disabled | Auto | Video Packet |
| 8 | GE8 | Disabled | Auto | Video Packet |
| 9 | GE9 | Disabled | Auto | Video Packet |
| 10 | GE10 | Disabled | Auto | Video Packet |
| 11 | GE11 | Disabled | Auto | Video Packet |
| 12 | GE12 | Disabled | Auto | Video Packet |

| 欄位 | 描述 |
|---|---|
| Port | 顯示連接埠清單 |
| State | 顯示介面的啟用/停用狀態 |
| Mode | 顯示語音VLAN模式 |
| QoS Policy | 顯示Surveillance VLAN標記會影響哪種封包 |

**Edit Port Setting**

| | |
|---|---|
| Port | GE2-GE4 |
| State | Enable |
| Mode | Auto / Manual |
| QoS Policy | Video Packet / All |

Apply Close

- **Port :** 顯示選擇的要編輯的連接埠。
- **State :** 勾選複選框以啟用或停用介面的 Surveillance VLAN 功能。
- **Mode :** 選擇連接埠 Surveillance VLAN 模式。

- **Auto :** 視訊 VLAN 會自動檢測符合 OUI 表的封包，並將接收的連接埠新增至監控 VLAN ID tagged 成員。
- **Manual :** 使用者需要手動將介面新增到 VLAN ID taggged 成員。

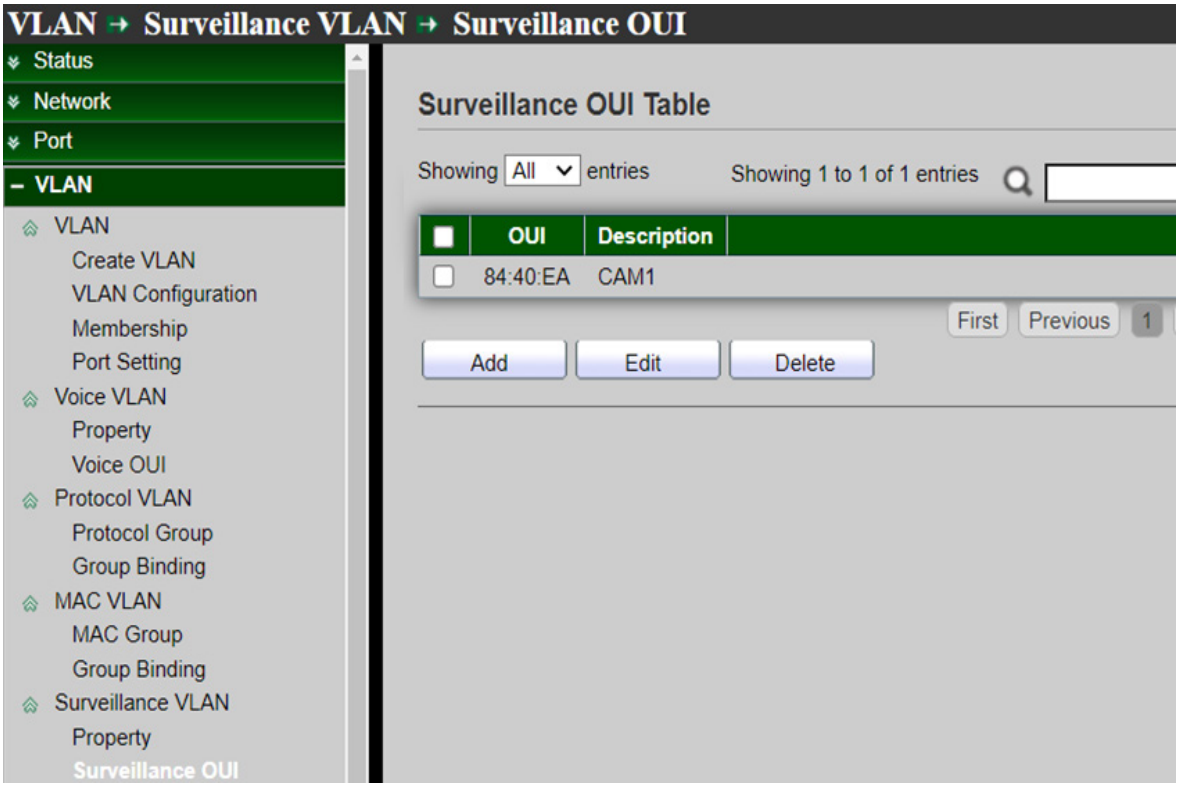
➢ **QoS Policy :** 選擇連接埠的 QoS Policy 模式。

- **Video Packet :** 視訊封包：Qos 屬性適用於來源 MAC 位址中包含 OUI 的封包
- **All :** Qos 屬性適用於分類到 Surveillance VLAN 的封包

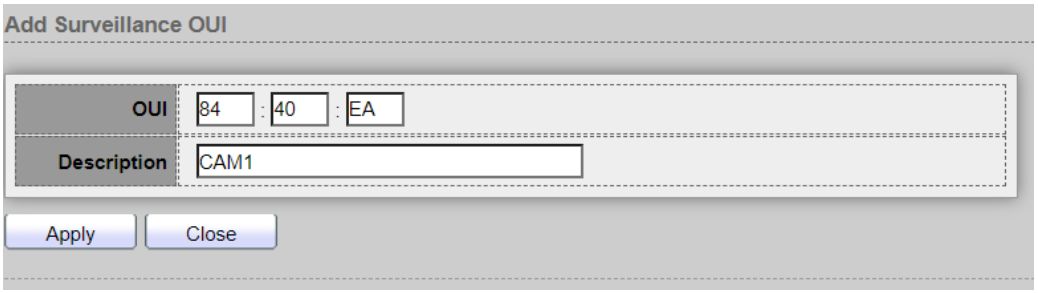
*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

## 6.5.2 監控 OUI(Surveillance OUI)

使用者管理員可以透過設定此頁面新增、編輯或刪除 OUI MAC 位址，設定**"add"**、**"Edit"**和**"Delete"**功能進行管理。



| 欄位 | 描述 |
|---|---|
| OUI | 顯示OUI MAC位址 |
| Description | 顯示OUI清單的描述 |




- **OUI :** 輸入 OUI MAC 位址。無法在編輯對話框中編輯。
- **Description :** 輸入指定 MAC 位址的描述到 Surveillance VLAN OUI 表中。

*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

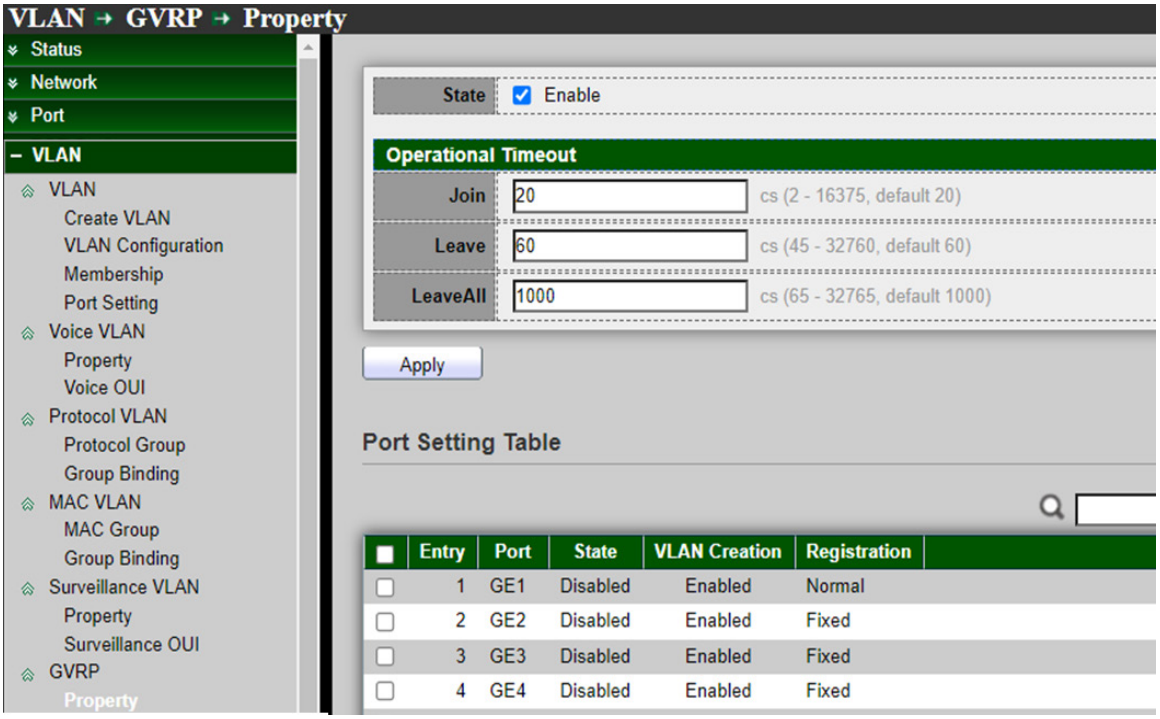
# 6.6 GVRP

GVRP(通用 VLAN 註冊協定)在 IEEE 802.1p 標準中進行描述；它是一種符合 IEEE 802.1Q 標準的方法，用於促進自動(動態)VLAN 成員資格設定。GVRP 支援交換器可以與其他 GVRP 支援交換器交換 VLAN 設定資訊。策略規則或其他網路管理方法可以決定誰可以加入 VLAN。當節點請求加入特定 VLAN 時，GVRP 會處理該節點與 GVRP 支援交換器之間的註冊事宜，並維護該資訊。

GVRP 通過自動提供 VLAN ID(VID)在整個網路的一致性來減少 VLAN 設定中錯誤發生機率。此外，您可以在交換器設定的靜態 VLAN 上,使用 GVRP 動態啟用連接埠成員資格。一旦 GVRP 創建動態 VLAN，還可以減少不必要的廣播流量和單播流量。

## 6.6.1 屬性(Property)

使用者管理員可以啟用 GVRP 功能並設定 GVRP 上每個連接埠的註冊。




- **State :** 設定 GVRP 功能的啟用狀態。
  - **Enable :** 如果勾選則啟用 GVRP，否則為停用 GVRP。
- **Operational Timeout :** Join/Leave/LeaveAll 定時器，用來控制 Join/Leave/LeaveAll 消息發送。
  - **Join :** GVRP 加入超時。
  - **Leave :** GVRP 保留超時。

*點擊"Apply"儲存您的變更設定。*

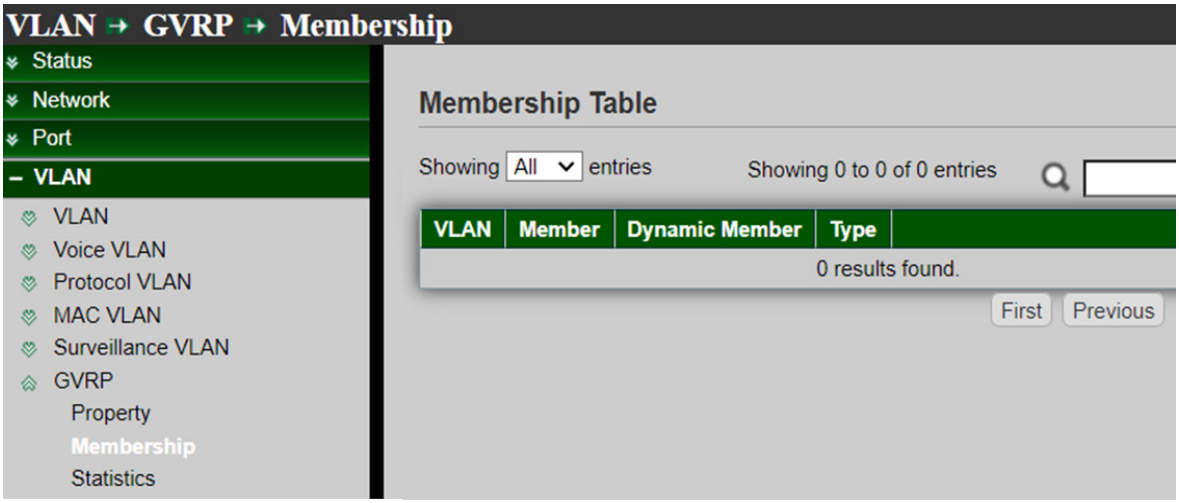
| 欄位 | 描述 |
|---|---|
| Port | 連接埠名稱 |
| State | 顯示連接埠GVRP狀態 |
| VLAN Creation | 顯示連接埠GVRP創建VLAN狀態 |
| Registration | 顯示連接埠GVRP註冊模式 |


- **Port :** 顯示連接埠編號。
- **State :** 顯示介面上的 GVRP 是啟用還是停用。
- **VLAN Creation :** 顯示介面上的動態 VLAN 創建是啟用還是停用。如果停用，GVRP 可以運行，但不會創建新的 VLAN。
- **Registration :** 顯示介面上的 VLAN 註冊模式。
  - **Normal : 正常模式。**允許動態 VLAN 在連接埠上註冊。同時發送動態和靜態 VLAN 資訊，允許動態和靜態 VLAN 封包通過。
  - **Fixed :** 不允許動態 VLAN 在連接埠上註冊。只向鄰近設備發送靜態 VLAN 資訊並允許靜態 VLAN 封包通過。
  - **Forbidden :** 不允許動態 VLAN 在連接埠上註冊並只允許預設 VLAN 封包通過。

*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

### 6.6.2 成員資格(Member ship)

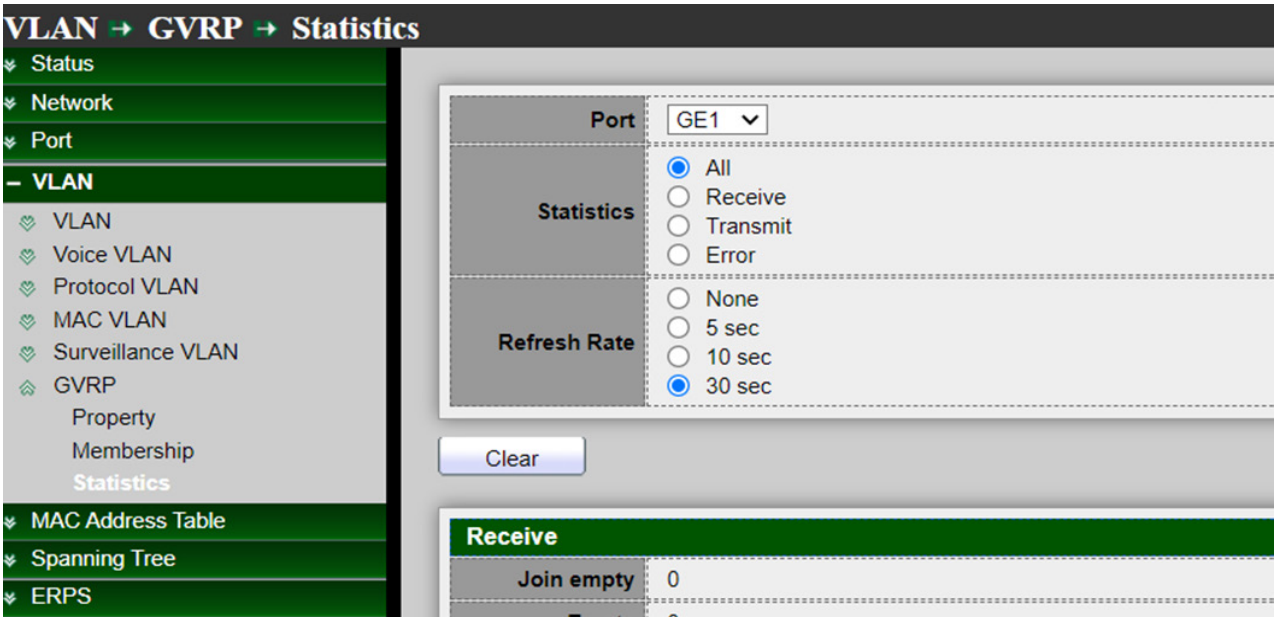
啟用 GVRP 功能並把網路埠設定為 GVRP 狀態後，使用者管理員可以查看 GVRP 成員資訊。




| 欄位 | 描述 |
|---|---|
| VLAN | VLAN編號 |
| Member | VLAN網路埠成員包括靜態成員和動態成員 |
| Dynamic Ports | GVRP註冊的動態網路埠 |
| Type | VLAN類型分為靜態或動態 |

### 6.6.3 統計數據(Statistics)

啟用並設定 GVRP 功能時，使用者管理員可以查看 GVRP 中每個連接埠訊息，包括 Receive、Transmit 和 Error。




*點擊 "Clear" 清除該頁面。*

| Receive | |
|---|---|
| Join empty | 0 |
| Empty | 0 |
| Leave Empty | 0 |
| Join In | 0 |
| Leave In | 0 |
| Leave All | 0 |

| Transmit | |
|---|---|
| Join empty | 0 |
| Empty | 0 |
| Leave Empty | 0 |
| Join In | 0 |
| Leave In | 0 |
| Leave All | 188 |

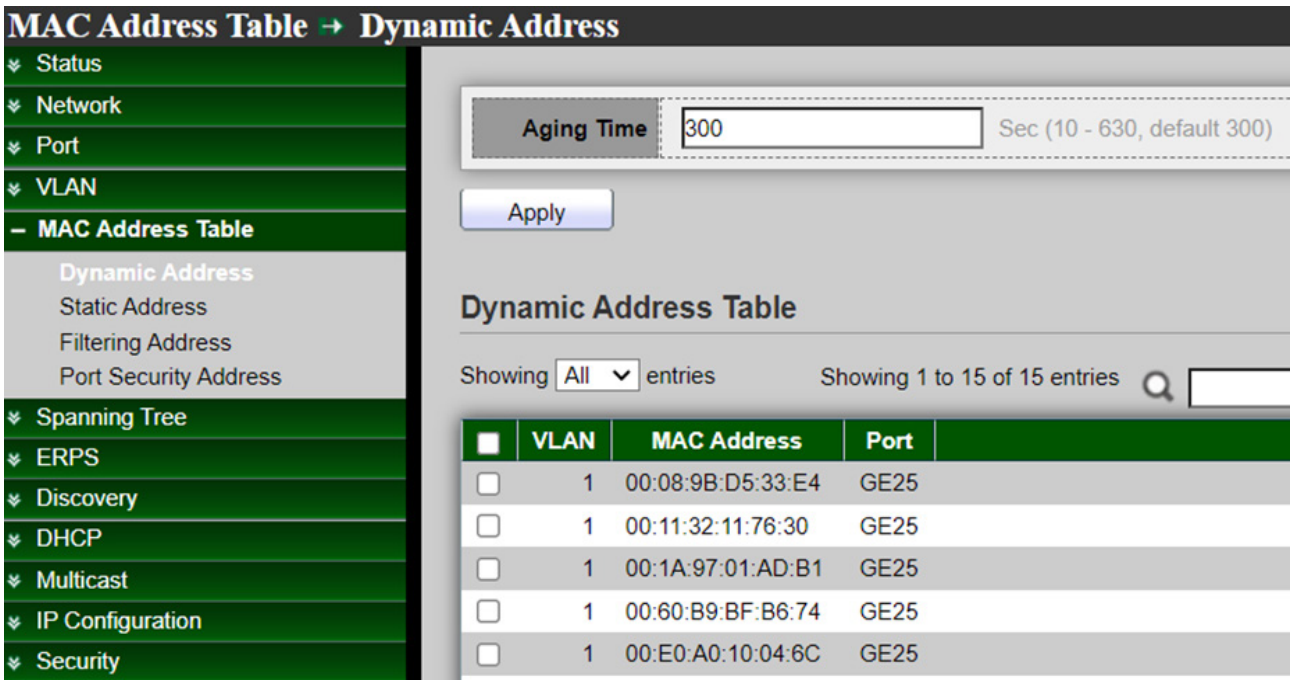
| Error | |
|---|---|
| Invalid Protocol ID | 0 |
| Invalid Attribute Type | 0 |
| Invalid Attribute Value | 0 |
| Invalid Attribute Length | 0 |
| Invalid Event | 0 |

| 欄位 | 描述 |
| --- | --- |
| Join empty | 接收或傳輸Join Empty消息的數量 |
| Empty | 接受或傳輸Empty消息的數量 |
| Leave Empty | 接收或傳輸Leave Empty消息的數量 |
| Join In | 接收或傳輸Join In消息的數量 |
| Leave In | 接收或傳輸Leave In消息的數量 |
| Leave All | 接收或傳輸Leave All消息的數量 |
| Invalid Protocol ID | 接收無效協定ID的數量 |
| Invalid Attribute Type | 接收無效Type的數量 |
| Invalid Attribute Value | 接收無效Value的數量 |
| Invalid Attribute Length | 接收無效Length的數量 |
| Invalid Event | 接收無效Event的數量 |

# 7.MAC Address Table

## 7.1 動態位址(Dynamic Address)

此頁面顯示連接設備的 MAC 位址。使用者管理員可以設定連接埠的延遲時間。




- **Aging Time :** 一個清單可在 MAC 位址表中保留的時間(秒)。有效範圍為 10 至 630 秒，預設值為 300 秒。

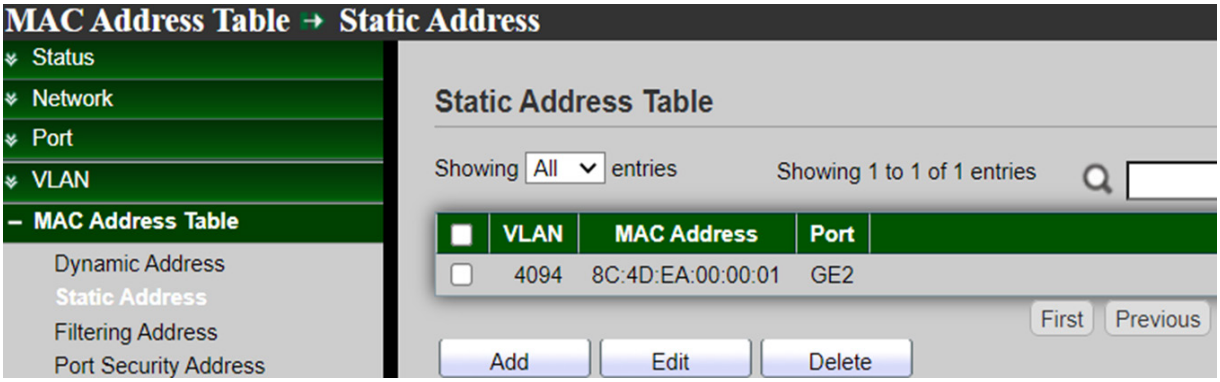
*點擊"Apply"儲存您的變更設定。*

| 欄位 | 描述 |
|---|---|
| MAC Address | 封包被靜態轉送的MAC位址 |
| VLAN | 指定要顯示或清除MAC清單的VLAN |
| Port | 介面或連接埠編號 |

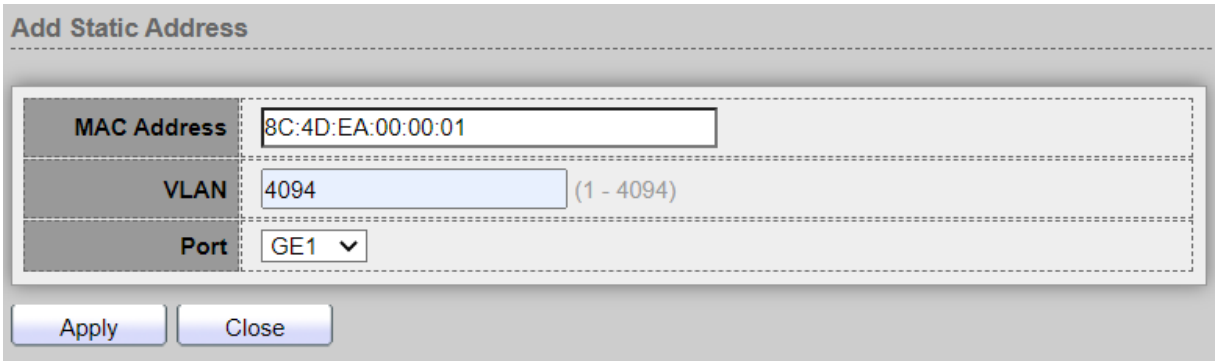
使用者管理員點選 MAC 位址的復選框然後點擊 “**Add Static Address**” 時，選中的 MAC 位址將會移至 “**Static Address**” 功能中。

## 7.2 靜態位址(Static Address)

如果使用者管理員在連接埠中固定了 MAC 位址，則設備 MAC 位址將綁定在該連接埠中，如果設備連接到其他連接埠將無法運作，除非連接到綁定連接埠。設定"**add**"、"**Edit**"和"**Delete**"功能進行管理。




| 欄位 | 描述 |
|---|---|
| MAC Address | 封包被靜態轉送的MAC位址 |
| VLAN | 指定要顯示或清除MAC清單的VLAN |
| Port | 介面或連接埠編號 |

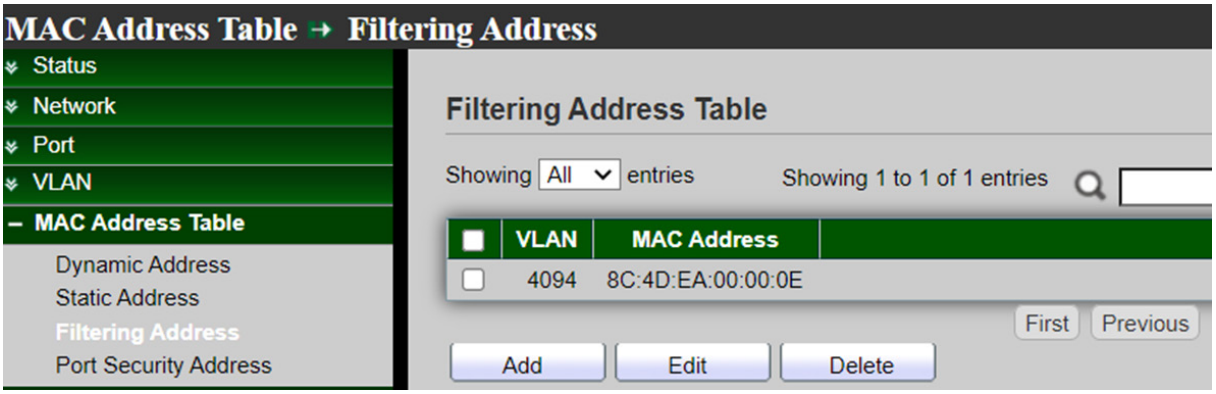



- **MAC Address :** 輸入封包被靜態轉送的 MAC 位址。
- **VLAN :** 輸入靜態 MAC 所屬 VLAN ID。
- **Port :** 選擇一個介面或埠編號。

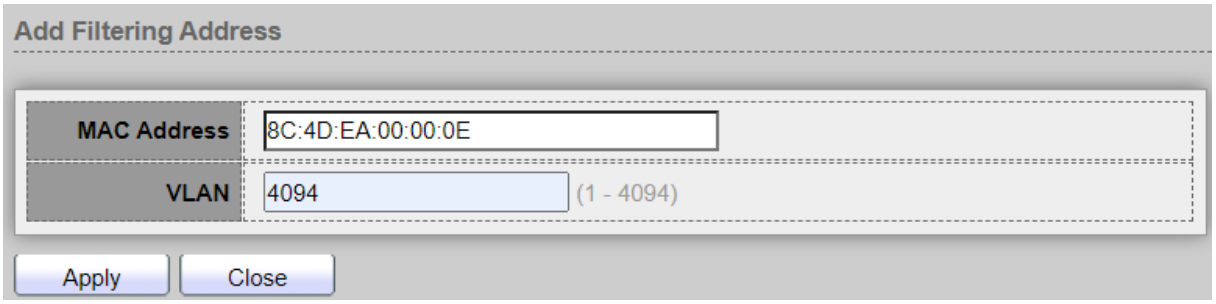
*點擊"**Apply**"儲存您的變更，或"**Close**"關閉設定。*

## 7.3 過濾位址(Filtering Address)

使用者管理員可以在 MAC 表中設定需要過濾的 MAC 位元址。如果表中添加 MAC，該 MAC 將被阻止。設定"**add**"、"**Edit**"和"**Delete**"功能進行管理。




| 欄位 | 描述 |
|---|---|
| MAC Address | 指定要丟棄封包中的單播MAC位址 |
| VLAN | 指定靜態MAC所屬VLAN ID |

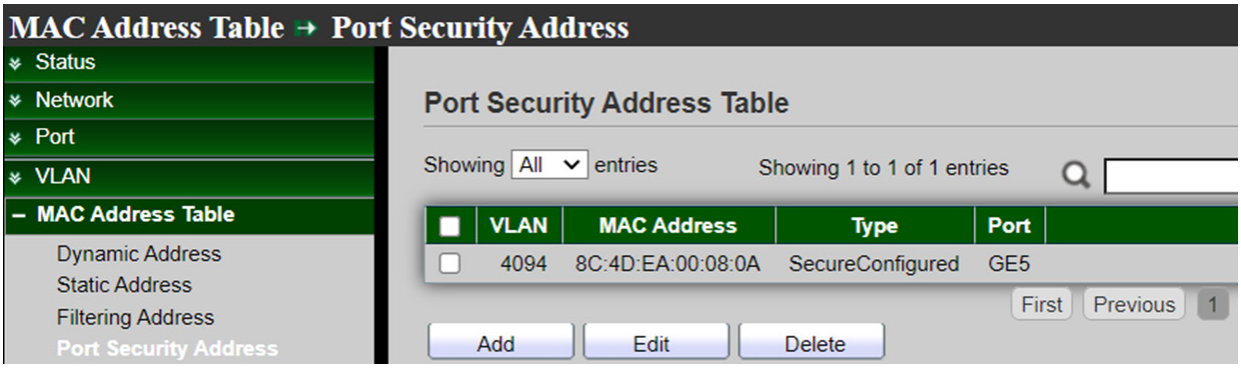



- **MAC Address :** 輸入指定要丟棄封包中的單播 MAC 位址。
- **VLAN :** 輸入指定靜態 MAC 所屬 VLAN ID。

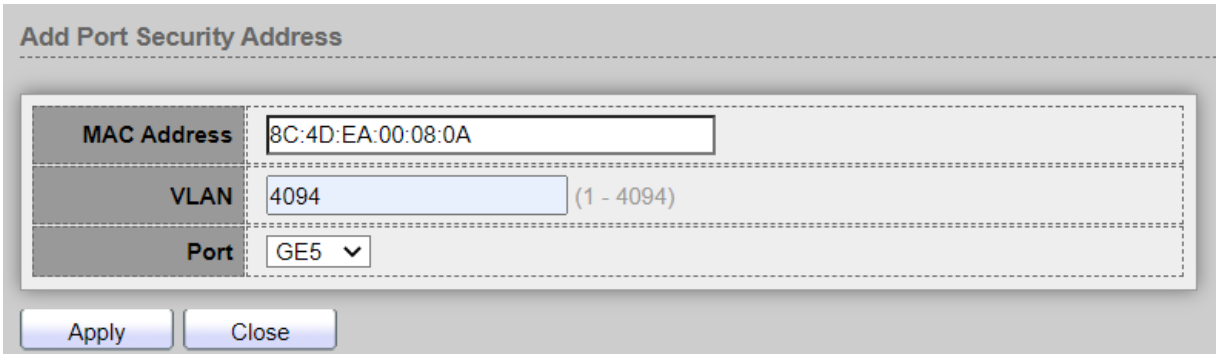
*點擊"**Apply**"儲存您的變更，或"**Close**"關閉設定。*

# 7.4 埠安全位址(Port Security Address)

使用者管理員可以設定 Port Security Address 功能，並設定"**add**"、"**Edit**"和"**Delete**"功能進行管理。




| 欄位 | 描述 |
|---|---|
| VLAN | 指定要顯示埠安全的VLAN |
| MAC Address | 為埠安全指定MAC位址 |
| Type | 為埠安全指定類型 |
| Port | 介面或連接埠編號 |



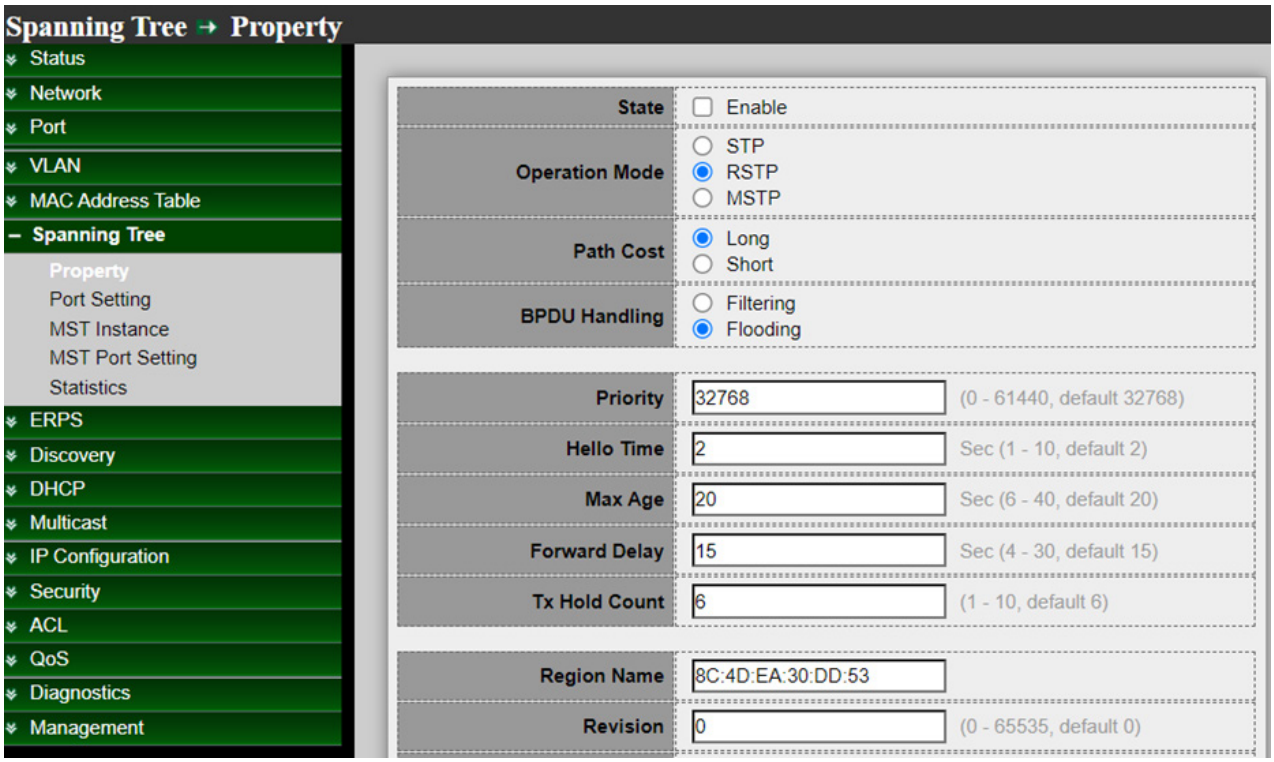

- **MAC Address :** 輸入埠安全的 MAC 位址。
- **VLAN :** 輸入 MAC 位址所屬 VLAN ID。
- **Port :** 介面或連接埠編號。

*點擊"**Apply**"儲存您的變更，或"**Close**"關閉設定。*

# 8.Spanning Tree

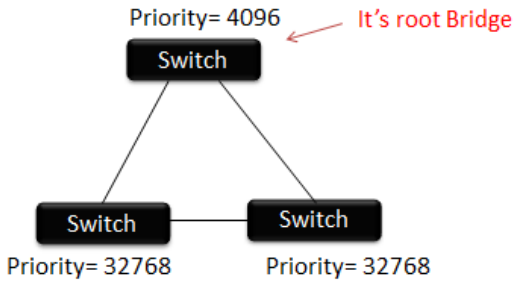
生成樹功能只允許任兩個網路設備之間每次有一條單一的設定啟用的鏈路（這可以防止迴圈），但當初始鏈路失效時會建立多餘鏈路作爲備援。如果生成樹成本發生變化，或網路鏈路無法訪問，生成樹演 演算法會重新設定生成樹拓撲，並啟動備用鏈路重新建立鏈接。如果沒有生成樹，兩端鏈路可能同時 生效，從而導致 LAN 上流量無限循環。

## 8.1 屬性(Property)



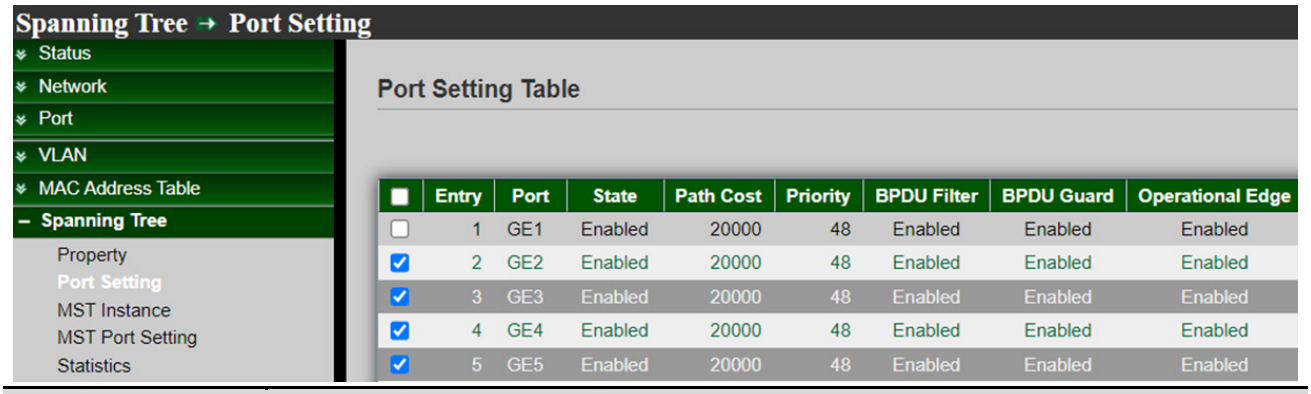

- **State :** 使用者管理員可以選擇啟用或停用該功能。
- **Operation Mode :** 使用者管理員可以選擇 3 種生成樹模式：生成樹(STP)、快速生成樹(RSTP)或多生成樹(MSTP)。
- **Path Cost :** 使用者管理員可以選擇 STP 判斷路徑成本為 Long 或 Short。
  - **Long :** 指定預設連接埠路徑成本在以下範圍內：1-200000000。
  - **Short :** 指定預設連接埠路徑成本在以下範圍內：1-65535。
- **BPDU Handling :** 當交換器接收到 BPDU 訊框時，使用者管理員可以選擇 BPDU 處理模式為 Filtering 或者 Flooding。指定 STP 關閉時的 BPDU 轉送方式。
  - **Filtering :** STP 關閉時過濾 BPDU。
  - **Flooding :**STP關閉時氾濫BPDU。

- **Priority :** 使用者管理員可以設定橋接優先級別，預設值為 32768。數值(橋接優先級別)最低的是 root bridge。指定橋接優先級別，有效範圍為 0 至 61440，並且值應為 4096 的倍數。(總共 16 個等級可選)。這是確保交換器被選為根層的概率，交換器的值越小，越優先被選為拓撲 root bridge。

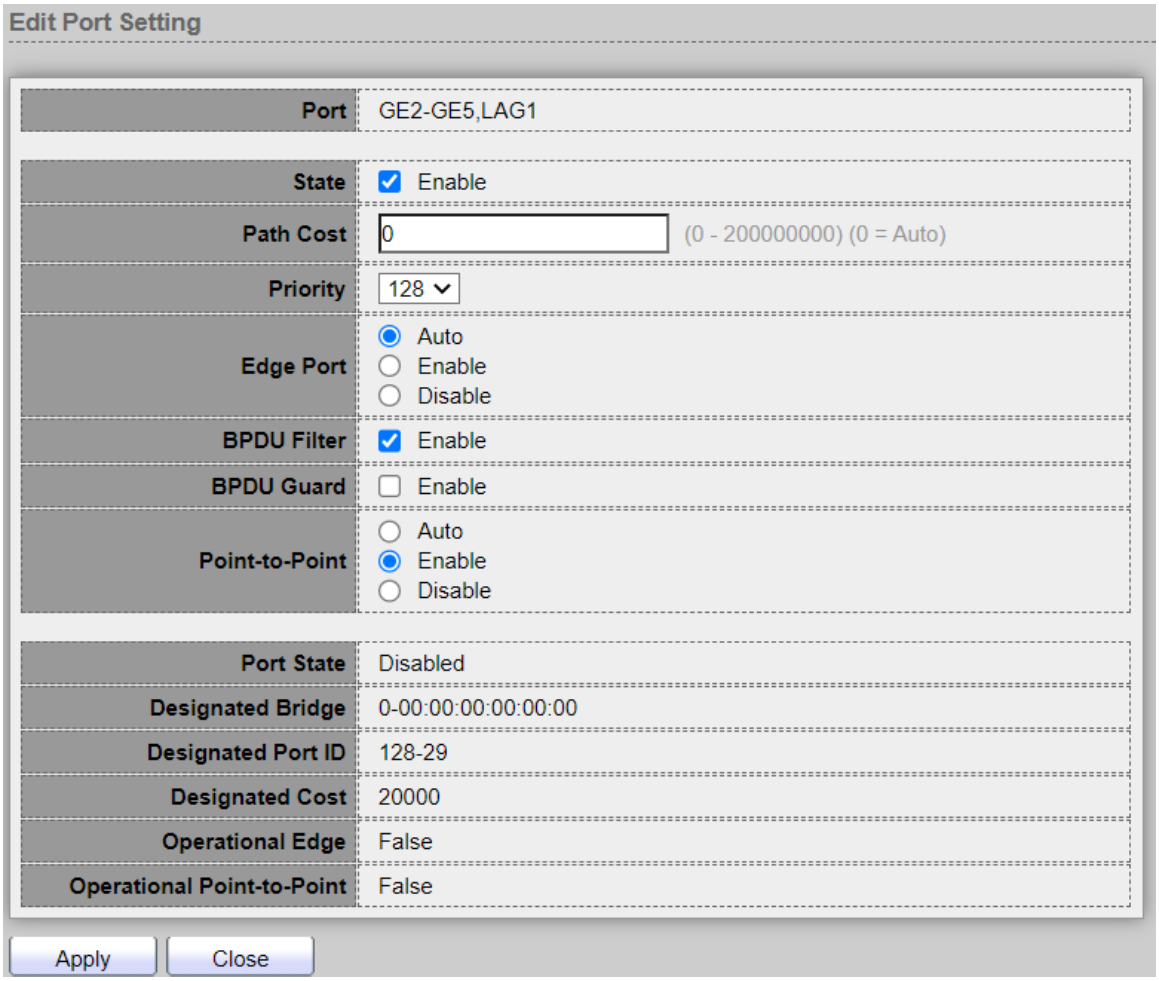



- **Hello Time :** 訪問時間是在連接埠發送每個橋接協議數據 ( BPDU ) 之間的間隔時間。該時間預設為 2 秒(sec)，使用者管理員可將時間調整爲 1 至 10 秒。
- **Max. Age / Forward delay :** 2*(延遲轉發-1s) >=最大延遲時間>= 2*(訪問時間+1s)，交換器等待設定資訊而不嘗試重新設定自己的時間間隔(以秒爲單位)。數值在 6-40 間。
- **Forward Delay :** 指定 STP 轉發延遲，這是連接埠在進入轉發狀態之前保持監聽和學習狀態的時間。有效範圍在 4-30 之間。
- **TX hold Count :** 指定發出保持計數用於限制每秒傳輸的封包數量。有效範圍為 1 到 10。
- **Region Name :** MSTP 實例名稱。最大長度為 32 個子元。預設值為交換器的 MAC 位址。
- **Revision :** 使用者管理員每次變更 MST 數值，習慣性"Revision"值會加 1。這是 MSTP 修訂號。有效範圍為 0 至 65535。
- **Max. Hop :** 設定交換器的最大跳數。指定 BPDU 被丟棄前在 MSTP 域中的跳數。有效範圍為 1 到 40。

## 8.2 連接埠設定(Port Setting)




| 欄位 | 描述 |
|---|---|
| Port | 指定介面ID或介面ID列表 |
| State | 指定埠的運行狀態 |
| Path Cost | 指定埠的STP路徑成本 |
| Priority | 指定埠的STP優先級別 |
| BPDU Filter | 指定埠的BPDU過濾狀態 |
| BPDU Guard | 指定埠的BPDU防護狀態 |
| Operational Edge | 指定埠的邊際埠運行狀態 |
| Operational Point-to-Point | 指定埠的點對點運行狀態 |
| Port Role | 指定埠的當前埠角色。可能為：<br>“關閉”，“主埠”，“根埠”，“指定埠”，“預備埠” 和 “備份埠” |
| Port State | 指定埠的目前狀態。可能為：<br>“關閉”，“丟棄狀態”，“學習狀態” 和 “轉發狀態” |
| Designated Bridge | 指定網橋的網橋ID |
| Designated Port ID | 交換器上的指定埠ID |
| Designated Cost | 交換器上指定埠的路徑成本 |




- **State :** 使用者管理員可以設定啟用或關閉。
- **Path Cost :** 路徑成本(1-200000000)該參數用於決定設備之間的最佳路徑。因此，應將較低的值分配給連接高速媒體的埠，較高的值分配給連接低速媒體的埠。(路徑成本優先於埠優先級別) 請注意當路徑成本模式設定為 short 時，最大路徑成本值為 65535。範圍 : 1-200000000(設定值 0= 自動，預設值為 0)。
- **Priority :** 如果交換器上所有埠的路徑成本相同，則有最高優先級別(即最低值)的埠將會被設定為生成樹中的設定啟用的鏈路。如果多個埠被分配最高優先級別，則有最低數值標識符的埠將被啓用。範圍：0-240，預設值為 128。
- **Edge Port :** 指定邊際模式。
  - **Enable :** 進入啓用狀態(作為主機連接)。
  - **Disable :** 進入關閉狀態(作為橋接連接)。

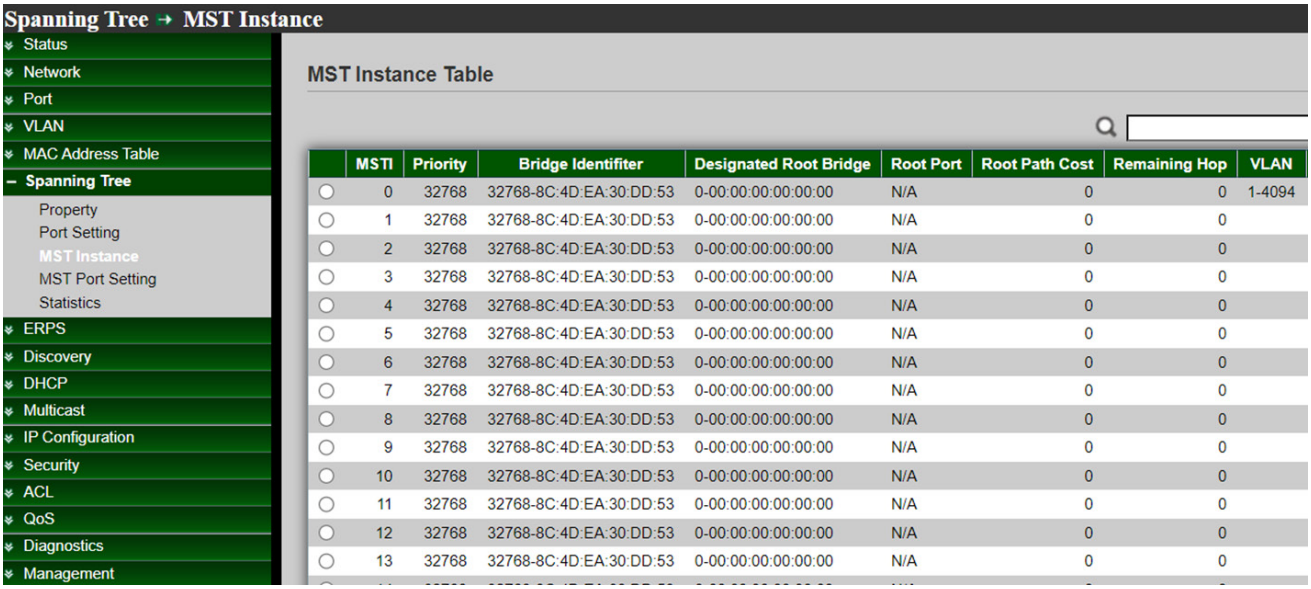
  邊際模式下，埠會在鏈路連接後立即進入轉發狀態。如果埠啓用邊際模式並且接收BPDUs報文，則可能會在STP狀態改變前的短時間內形成迴圈。

- **BPDU Filter :** BPDU 過濾設定可避免從指定連接埠接收/傳送 BPDU。
  - **Enable :** 打開 BPDU 過濾功能。
  - **Disable :** 關閉BPDU過濾功能。
- **BPDU Guard :** BPDU 防護設定直接丟棄接收的 BPDU。
  - **Enable :** 打開 BPDU 防護功能。
  - **Disable :** 關閉BPDU防護功能。
- **Point-to-Point :** 指定點對點埠設定：
  - **Auto :** 該狀態基於埠的雙工設定。
  - **Enable :** 進入關閉狀態。
  - **Disable :** 進入開啓狀態。
- **Port State :** 指定埠的目前狀態。可能為：“關閉”，“丟棄狀態”，“學習狀態”和‘轉發狀態”。
- **Designated Bridge :** 指定網橋的網橋 ID。
- **Designated Port ID :** 交換器上的指定埠 ID。
- **Designated Cost :** 交換器上指定埠的路徑成本。
- **Operational Edge :** 顯示“False”或“True”狀態。
- **Operational Point-to-Point :** 顯示“False”或“True”狀態。

*點擊**"Apply"**儲存您的變更，或**"Close"**關閉設定。*

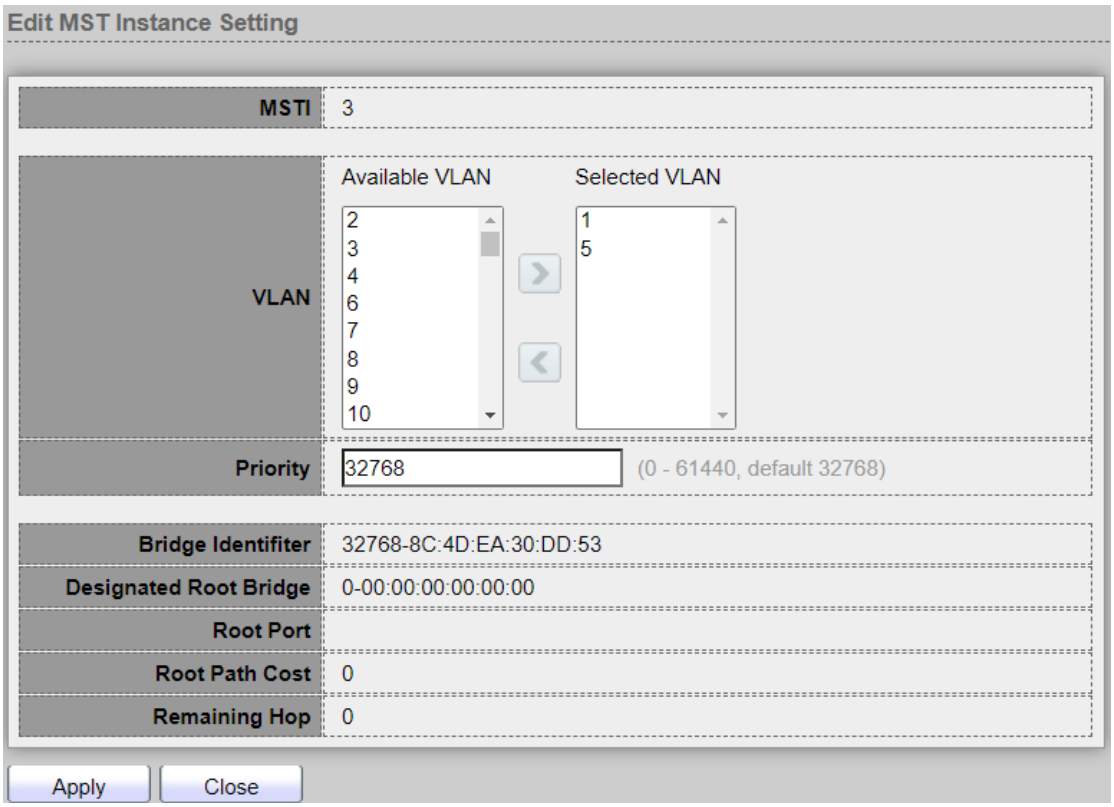
## 8.3 MST 實例(MST Instance)

MST 可以有多組 STP 實例。每個實例獨立形成邏輯生成樹。並且每個實例有自己的 VLAN 和連接埠狀態，可以獨立設定每個連接埠的優先級別。




| MSTI | Priority | Bridge Identifiter | Designated Root Bridge | Root Port | Root Path Cost | Remaining Hop | VLAN |
|---|---|---|---|---|---|---|---|
| 0 | 32768 | 32768-8C:4D:EA:30:DD:53 | 0-00:00:00:00:00:00 | N/A | 0 | 0 | 1-4094 |
| 1 | 32768 | 32768-8C:4D:EA:30:DD:53 | 0-00:00:00:00:00:00 | N/A | 0 | 0 | |
| 2 | 32768 | 32768-8C:4D:EA:30:DD:53 | 0-00:00:00:00:00:00 | N/A | 0 | 0 | |
| 3 | 32768 | 32768-8C:4D:EA:30:DD:53 | 0-00:00:00:00:00:00 | N/A | 0 | 0 | |
| 4 | 32768 | 32768-8C:4D:EA:30:DD:53 | 0-00:00:00:00:00:00 | N/A | 0 | 0 | |
| 5 | 32768 | 32768-8C:4D:EA:30:DD:53 | 0-00:00:00:00:00:00 | N/A | 0 | 0 | |
| 6 | 32768 | 32768-8C:4D:EA:30:DD:53 | 0-00:00:00:00:00:00 | N/A | 0 | 0 | |
| 7 | 32768 | 32768-8C:4D:EA:30:DD:53 | 0-00:00:00:00:00:00 | N/A | 0 | 0 | |
| 8 | 32768 | 32768-8C:4D:EA:30:DD:53 | 0-00:00:00:00:00:00 | N/A | 0 | 0 | |
| 9 | 32768 | 32768-8C:4D:EA:30:DD:53 | 0-00:00:00:00:00:00 | N/A | 0 | 0 | |
| 10 | 32768 | 32768-8C:4D:EA:30:DD:53 | 0-00:00:00:00:00:00 | N/A | 0 | 0 | |
| 11 | 32768 | 32768-8C:4D:EA:30:DD:53 | 0-00:00:00:00:00:00 | N/A | 0 | 0 | |
| 12 | 32768 | 32768-8C:4D:EA:30:DD:53 | 0-00:00:00:00:00:00 | N/A | 0 | 0 | |
| 13 | 32768 | 32768-8C:4D:EA:30:DD:53 | 0-00:00:00:00:00:00 | N/A | 0 | 0 | |

| 欄位 | 描述 |
|---|---|
| MSTI | MST實例ID |
| Priority | 指定MSTI上的橋接優先級別 |
| Bridge Identifier | 指定MSTI上的橋接標識符 |
| Designated Root Bridge | 指定MSTI上的指定根層標識符別 |
| Root Port | 指定MSTI上的指定根埠 |
| Root Path Cost | 指定MSTI上的指定根路徑成本 |
| Remaining Hop | 指定MSTI上的剩餘跳數設定 |
| VLAN | 指定MSTI上的VLAN設定 |

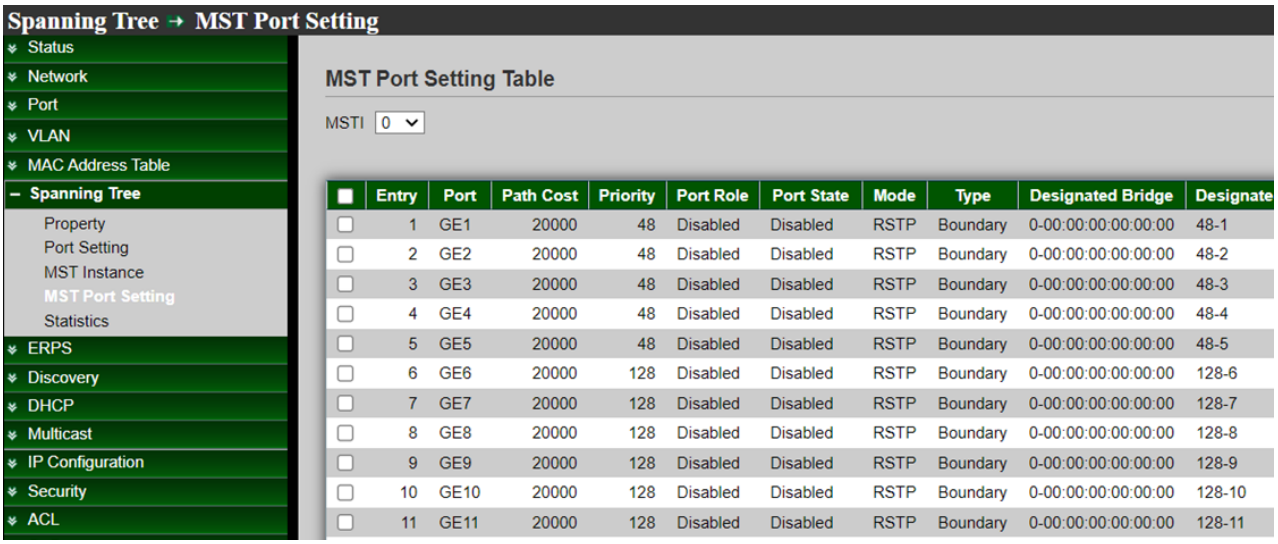



- **VLAN :** 選擇指定 MSTI 的 VLAN 列表。
- **Priority :** 指定 MSTI 上的橋接優先級別。有效範圍為 0 至 61440，並且值應為 4096 的倍數。(總共 16 個等級可選)。這是確保交換器被選為根層的概率，交換器的值越小，越優先被選為拓撲 root bridge。
- **Bridge Identifier :** 顯示所選 MST 實例根層的優先級別和 MAC 位址。
- **Root Port :** 顯示所選 MST 實例的根埠。
- **Root Path Cost :** 顯示所選 MST 實例的根路徑成本。
- **Remaining Hops :** 顯示到下一目的地的剩餘跳數。

*點擊"Apply"儲存您的變更，或"Close"關閉設定。.*

## 8.4 MST 網路埠設定(MST Port Setting)

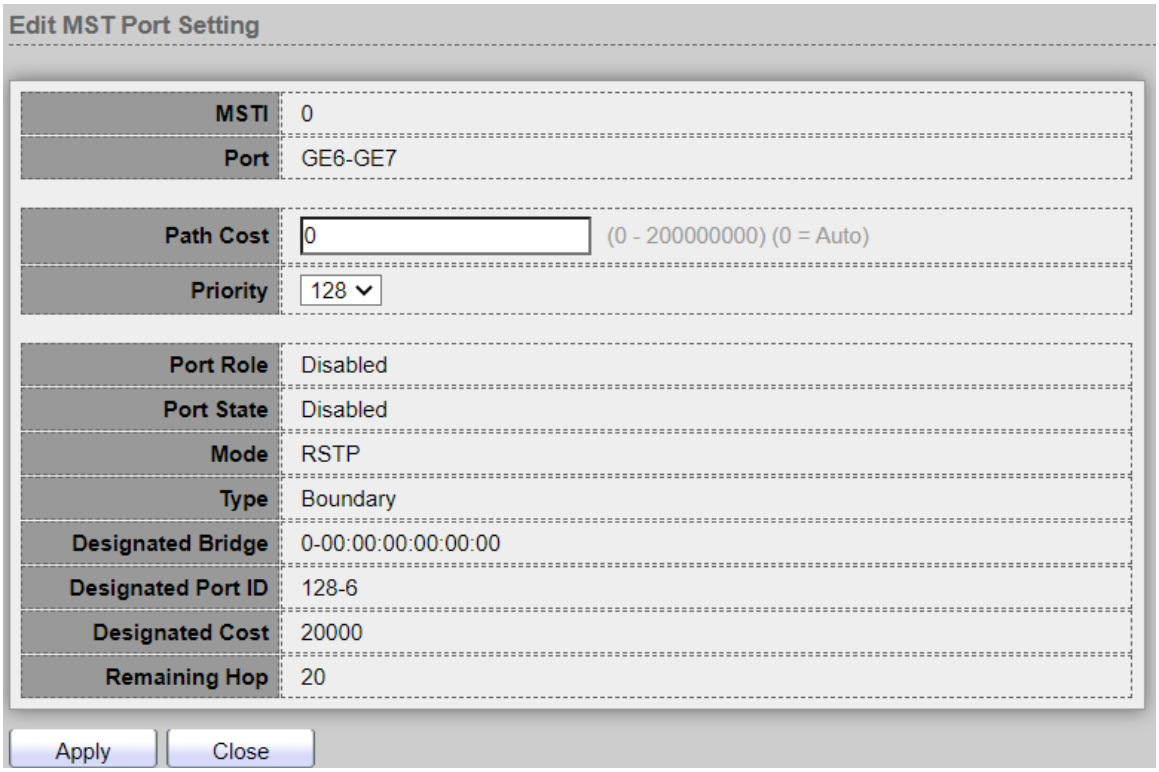
MST(多生成樹)是 RST(快速生成樹)的擴展。MST 進一步開發了 VLAN 的實用性。MST 為每個 VLAN 群組設定一個單獨的生成樹，並在每個生成樹中阻止除一條可能的備用路徑之外的所有路徑。 多生成樹實例(MSTI)演算並創建無環拓撲，以橋接來自映射到該實例的 VLAN 的封包。




MST Port Setting 用於設定每個 MST 實例的連接埠 MSTP 設定。也用於查看從協議學習的統計資料。

| 欄位 | 描述 |
|---|---|
| MSTI | 指定 MSTI 上的連接埠設定 |
| Port | 指定介面 ID 或介面 ID 列表 |
| Path Cost | 指定 MSTI 上的連接埠路徑成本 |
| Priority | 指定 MSTI 上的連接埠優先級別 |
| Port Role | 指定埠的當前埠角色。可能為：<br>"關閉","主埠","根埠","指定埠","預備埠"和"備份埠" |
| Port State | 指定埠的目前狀態。可能為：<br>"關閉","丟棄狀態","學習狀態"和"轉發狀態" |
| Mode | 指定連接埠上運行的 STP 模式 |
| Type | 連接埠類型可能值為：<br>• **Boundary**：將 MST 網橋連接到不在同一區域的 LAN 的連接埠<br>• **Internal**：將 MST 網橋連接到同一區域的 LAN 的連接埠 |
| Designated Bridge | 指定網橋的網橋 ID |

| | |
|---|---|
| **Designated Port ID** | 交換器上的指定連接埠 ID |
| **Designated Cost** | 交換器上的指定埠路徑成本 |
| **Remaining Hop** | 指定埠上的剩餘跳數 |




- **MTSI :** 指定 MSTI 上的指定連接埠設定。
- **Port :** 指定介面 ID 或介面 ID 列表。
- **Path Cost :** 指定 MSTI 上的 STP 連接埠路徑成本，路徑成本預設值為 0(自動)，取決於來源設備速率。

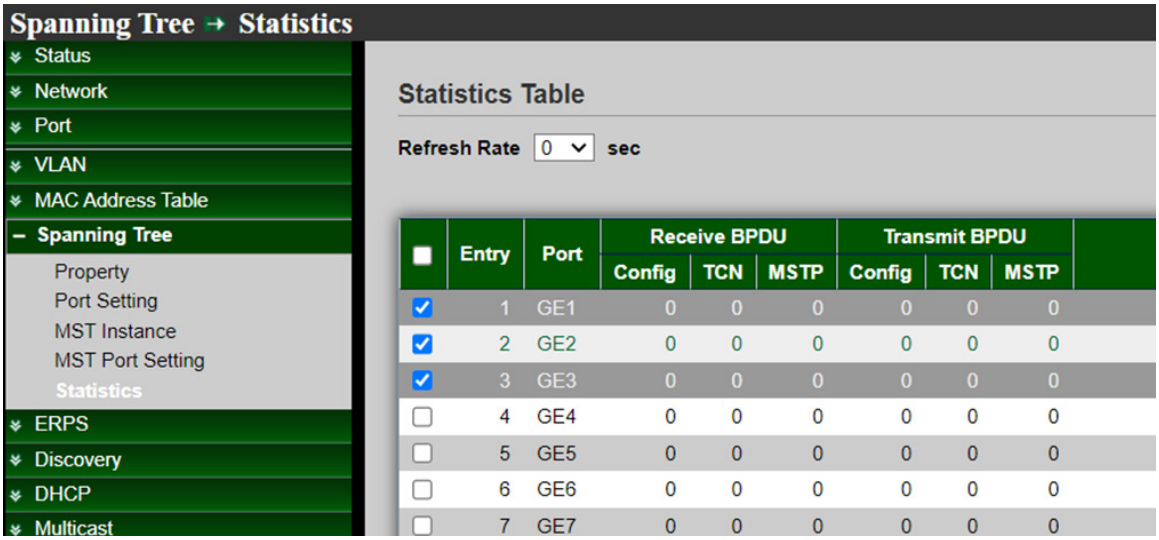
  如果網路發生迴圈，MST 在選擇介面進入轉送狀態時會使用 cost 值。使用者管理員可以為想要優先選擇的介面分配較低的 cost 值，為想要最後選擇的介面分配較高的 cost 值。如果所有介面的 cost 值相同，則 MST 將介面編號最小的介面置於轉送狀態，並阻塞其他介面。
- **Priority :** 指定 MSTI 上的 STP 連接埠優先級別，使用者管理員可以設定 MTP 優先級別，使交換器更有可能被選為根層交換器。
- **Port Role :** 顯示每個實例的埠角色，由 MSTP 演算法分配 STP 路徑。可為：**“Disabled(關閉)”，“Master(主埠)”，“Root(根埠)”，“Designated(指定埠)”，“Alternative(預備埠)”** 和 **“Backup(備份埠)”** 。

- **Port State :** 指定埠的目前狀態。可為：
  **“Disabled(關閉)”，“Discarding(丟棄狀態)”，“Learning(學習狀態)”**,和 **“Forwarding(轉發狀態)”** 。
- **Mode :** 指定埠上的 STP 運行模式。
  - **RSTP :** 連接埠啟用 RSTP。
  - **STP :** 連接埠啟用經典 STP。
  - **MSTP :** 連接埠啟用 MSTP。
- **Type :** 顯示連接埠的 MSTP 類型，連接埠類型可值為：
  - **Boundary :** 將 MST 網橋連接到不在同一區域的 LAN 的連接埠。
  - **Internal :** 將 MST 網橋連接到同一區域的 LAN 的連接埠。
- **Designated Bridge :** 顯示將鏈路或共用 LAN 連接到 root 的網橋 ID 號碼。
- **Designated Port ID :** 顯示將鏈路或共用 LAN 連接到 root 的指定網橋的優先級別和埠 ID。
- **Designated Cost :** 顯示參與 STP 拓撲的連接埠成本。如果 STP 檢測到迴圈，成本越低的連接埠被阻塞的可能性越小。
- **Remaining Hops :** 顯示到下一目的地的剩餘跳數。

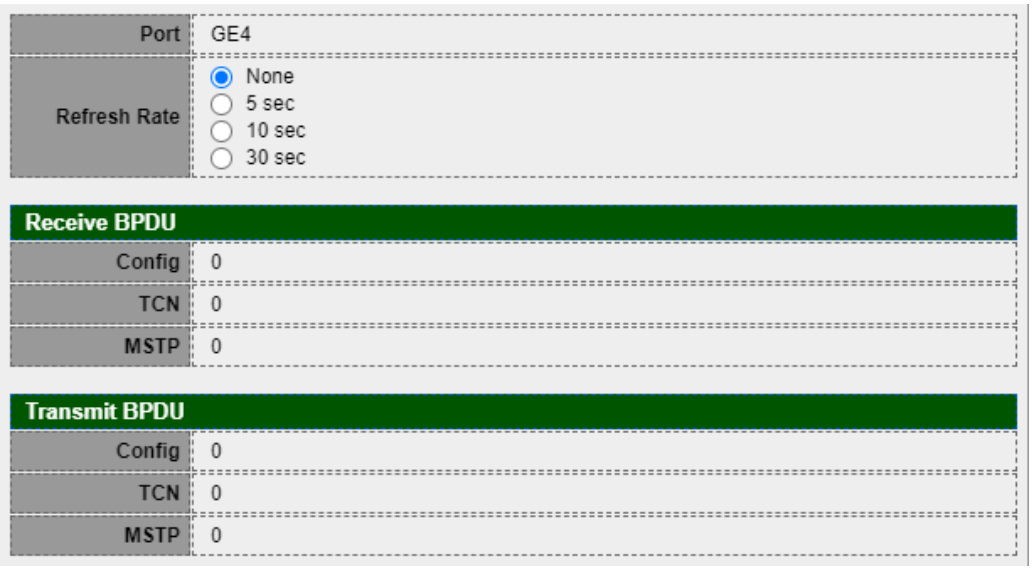
*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

## 8.5 統計數據(Statistics)

該頁面可以查看 STP 埠的 Receive / Transmit BPDU 資訊。



| 欄位 | 描述 |
|---|---|
| Refresh Rate | 自動刷新統計數據的選項 |
| Receive BPDU (Config) | 接收到的CONFIG BPDU計數 |
| Receive BPDU (TCN) | 接收到的TCN BPDU計數 |
| Receive BPDU (MSTP) | 接收到的MSTP BPDU計數 |
| Transmit BPDU (Config) | 傳送的CONFIG BPDU計數 |
| Transmit BPDU (TCN) | 傳送的TCN BPDU計數 |
| Transmit BPDU (MSTP) | 傳送的MSTP BPDU計數 |
| Clear | 清除所選介面的統計數據 |
| View | 查看介面的統計數據 |




- **Refresh Rate :** 自動刷新統計數據的選項：

為刷新級別：None , 5 sec , 10 sec , 30sec。

- **Clear :** 清除所選介面的統計數據

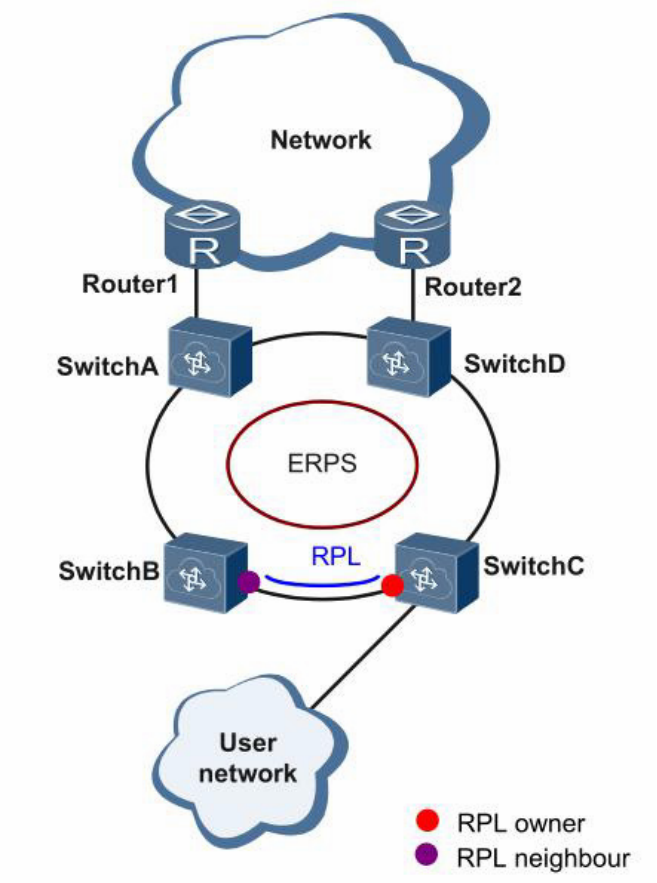
# 9.ERPS

**ERPS (乙太環網保護切換) :**在環網等乙太網路交換網路中，通常採用多餘鏈路來提供鏈路備份和增強網路可靠性。但是，使用多餘鏈路可能會造成網路迴圈、引發廣播風暴並導致 MAC 位址表不穩定。從而導致通訊品質下降，甚至通訊服務中斷。

STP (生成樹協議), RSTP (快速生成樹協議),和 MSTP (多生成樹協議)也能滿足網路的可靠性要求，但收斂速度慢，不符合行業標準要求。

第一個工業標準乙太網多餘協議(ITU-T G.8032)，用於鏈路備份，提高網路可靠性，乙太網路需要更快的 ERPS 功能保護交換器。互補式 STP 無法滿足快速收斂的要求。ERPS 是用於防止環網迴圈的 ITU-T 標準協議。它優化檢測並執行快速收斂。ERPS 允許環網上所有支援 ERPS 的設備進行通訊。

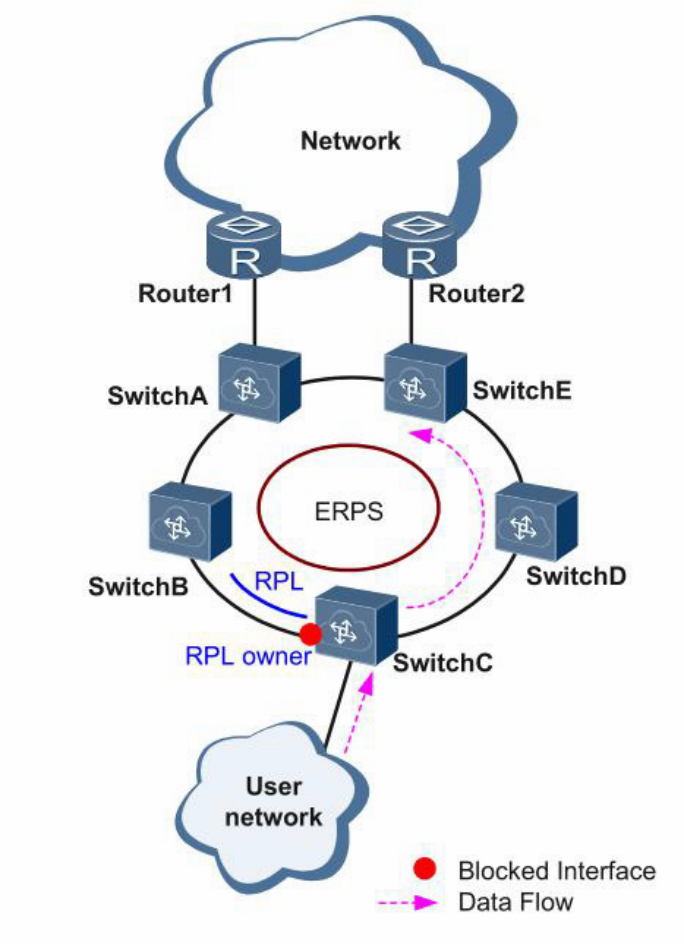
## 如圖例 1 所示　　=>　典型群組網




**圖例 ERPS 鏈路正常**

ERPS 是專用於乙太網路鏈路層的標準環網協議，以 ERPS 環為基本單位。每個二層交換設備上只能有兩個連接埠加入同一個 ERPS 環。在 ERPS 環中，為了防止迴圈，可以啟動破環機制，阻塞 RPL owner 埠。當環網上發生鏈路故障時，運行 ERPS 協議的設備可以快速放開阻塞連接埠，並進行鏈路保護倒換。

**如圖例 2 所示　　=>　鏈路正常**

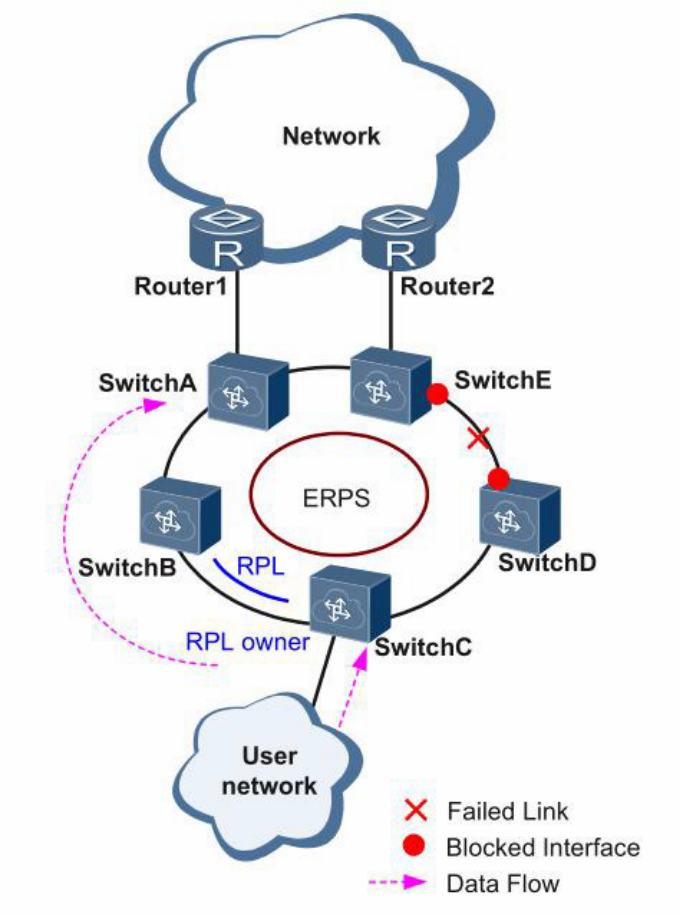



**圖例 ERPS 鏈路正常**

由 Switch A~Switch E 組成的環上所有設備均正常通訊。

為了防止迴圈，ERPS 會先阻塞 RPL owner 埠。如果設定了 RPL neighbor 埠，則該連接埠也會被阻塞，其他連接埠可以正常轉發業務流量。

**如圖例 3 所示　　=>　鏈路故障**




**圖例 ERPS 鏈路故障**

當 Switch D 和 Switch E 之間鏈路發生故障，ERPS 啟用保護倒換機制，阻塞故障鏈路兩端的連接埠，放開 RPL owner 埠。重新恢復使用者流量的接收和發送，從而保證了流量不中斷。

| Note | 鏈路恢復正常後，如果 ERPS 環設定的是回切模式。RPL owner 埠所在設備會重新阻塞 RPL 鏈路上的流量，故障鏈路重新用來完成使用者流量的轉送。 |
|---|---|

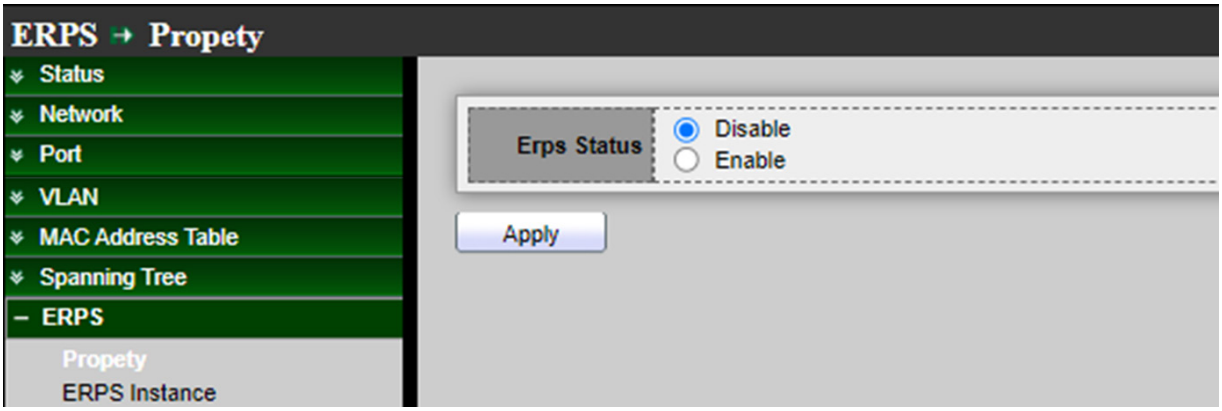
## 9.1 安全(Propety)

在運行 ERPS 的環形拓撲網路中，只有一台交換器被指定為“owner”，負責阻塞 RPL 中的流量，以避免迴圈。與 RPL owner 相鄰的交換器稱為 RPL“neighbor”節點，在正常情況下負責阻塞其 RPL 末端。環中與 RPL owner 或 RPL neighbor 相鄰的其他參與交換器是該拓撲的普通成員或 RPL next-neighbor 節點，通常轉送接收流量。

ERPS 與 STP 一樣，透過使用輪詢封包檢測故障，來提供無迴圈網路。當故障發生時，ERPS 透過在受保護的反向路徑上發送流量(小於 50ms)來進行自我修復，並迅速恢復轉送流量。由於採用這種故障檢測機制，網路廣播風暴問題也可以避免。

乙太環網保護切換(ERPS)是一台網路環網保護協議，用於防止在 LAN 中形成迴圈，從而避免廣播風暴問題。迴圈避免機制確保流量在除 RPL 之外所有環網鏈路上流動。為了實現迴圈避免機制，ITU-T G.8032 定義了 ERPS 三種連接埠角色，分別是“RPL Owner Node”，“RPL Neighbor Node”和“None Node”。

使用者管理員可以設定“ERPS”以啟用/停用 ERPS 功能。

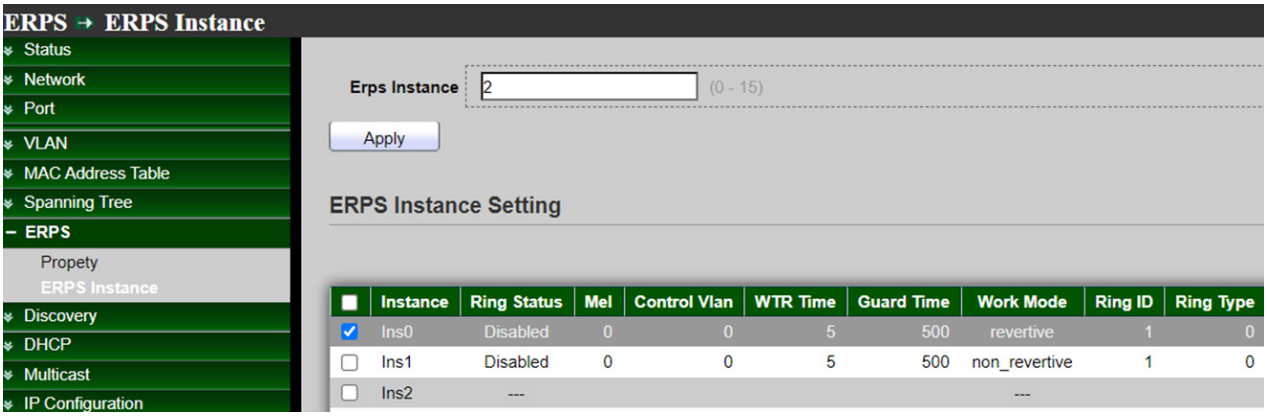



*點擊"Apply"儲存您的變更設定。*

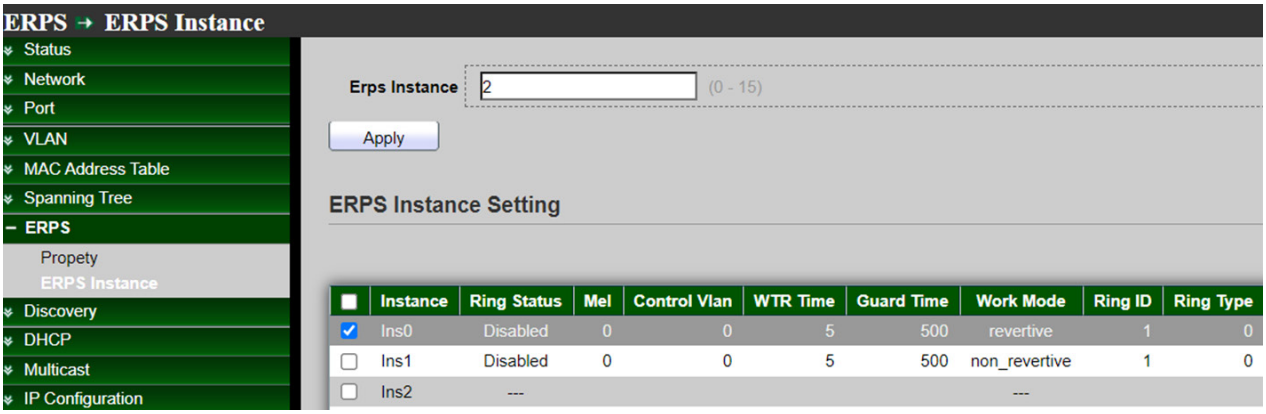
# 9.2 ERPS 實例設定(ERPS Instance Setting)

如下，點擊並編輯設定介面 “Ins” 設定。

使用者管理員可以設定 “ERPS Instance” 為環網實例設定功能。




| Note | 設定 ERPS 之前，需要停用快速生成樹協議(RSTP)或多生成樹協議，因為交換器內只有一種協議是獨佔運行。 |
|---|---|




- **ERPS Instance :** ERPS 介面的 ID。

*點擊"Apply"儲存您的變更設定。*

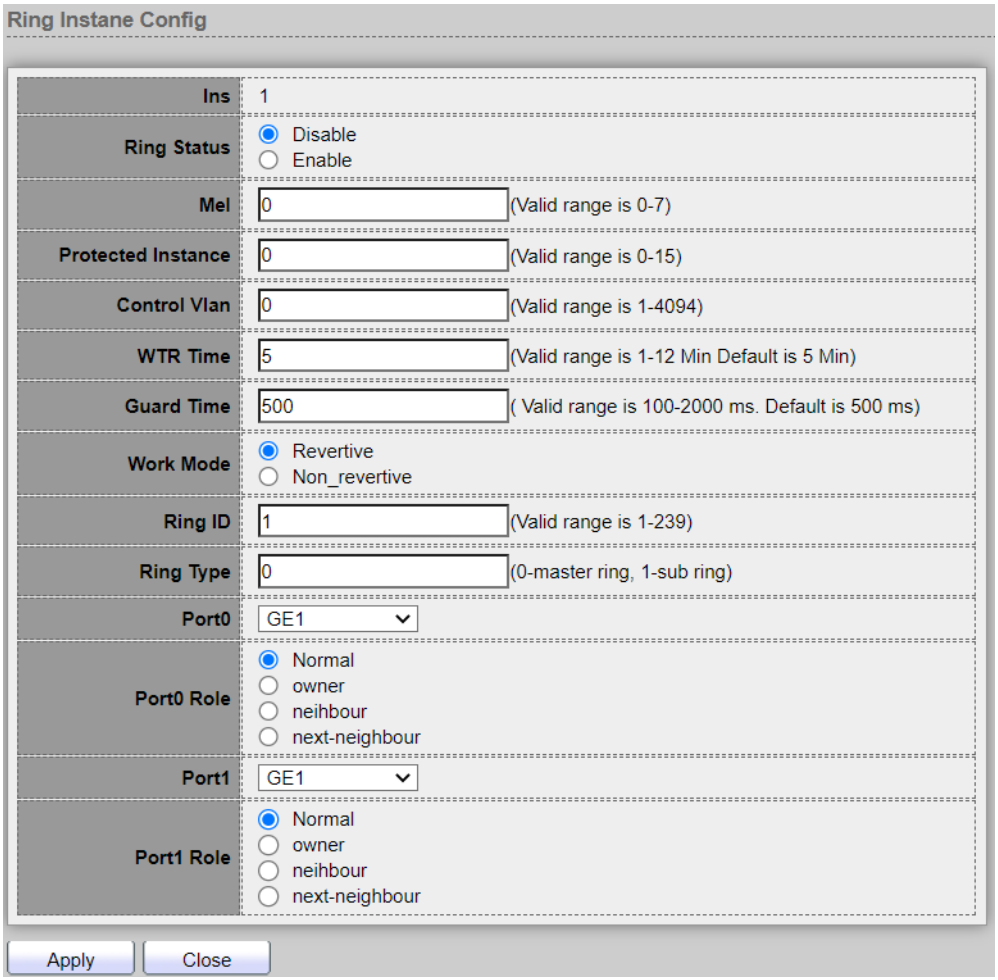
**ERPS Instance Setting**

| | Instance | Ring Status | Mel | Control Vlan | WTR Time | Guard Time | Work Mode | Ring ID | Ring Type |
|---|---|---|---|---|---|---|---|---|---|
| ☑ | Ins0 | Disabled | 0 | 0 | 5 | 500 | revertive | 1 | 0 |
| ☐ | Ins1 | Disabled | 0 | 0 | 5 | 500 | non_revertive | 1 | 0 |
| ☐ | Ins2 | --- | | | | | --- | | |
| ☐ | Ins3 | --- | | | | | --- | | |

| Protected Instance | Port0 | Port Role | Port Status | Port1 | Port Role | Port Status | Node Status |
|---|---|---|---|---|---|---|---|
| --- | gi1 | rpl | disabled | gi1 | rpl | disabled | init |
| --- | gi1 | rpl | disabled | gi1 | rpl | disabled | init |

| 欄位 | 描述 |
|---|---|
| Instance | ERPS的ID ,也是保護實例的ID |
| Ring Status | 顯示啟用或關閉環網 |
| Mel | 顯示環網的MEL(實例維護等級)值 |
| Control VLAN | 顯示控制VLAN ID |
| WTR Time | 等待恢復(Wait To Restore,WTR)定時器值用於恢復倒換<br>操作員可以設定WTR Time定時器為5至12分鐘之間以1分鐘為單位，預設值為5分鐘 |
| Guard Time | 防衛定時器值用於防止環網節點接收過期R-APS訊息<br>可以設定Guard Time定時器為100毫秒至2000毫秒(2秒)之間以100毫秒為單位，預設值為500毫秒 |
| Work Mode | 顯示回切模式/非回切模式<br>• **In Revertive mode :** 導致保護恢復的條件清除後，流量通道恢復到工作傳輸實體，即阻塞 RPL 鏈路<br>• **In Non-Revertive mode :** 導致保護恢復的條件清除後，如果未發生故障，則流量通道繼續使用 RPL 鏈路 |

| | |
|---|---|
| **Ring ID** | 顯示環網ID |
| **Ring Type** | 顯示環網類型:"0"為主環，"1"為子環 |
| **Protected Instance** | ERPS環網實例的保護實例 |
| **Prot0** | 該節點的連接埠0(阻塞的第一個連接埠) |
| **Port Role** | 目前連接埠0的角色狀態 |
| **Port Status** | 顯示連接埠0的連接埠狀態 |
| **Port1** | 該節點的連接埠1(阻塞的第二個連接埠) |
| **Port Role** | 目前連接埠1的角色狀態 |
| **Port Status** | 顯示連接埠1的連接埠狀態. |
| **Node Status** | 顯示以下ERPS狀態 ：<br>**Init :** ERPS環網已啟動但還沒決定環網狀態<br>**Idle :** 如果環網內所有節點都處於該狀態，則表示環網內所有鏈路都處於正常運行狀態。如果發生鏈路故障，該狀態將切換到protection狀態<br>**Protection :** 如果有節點處於此狀態，則表示發生鏈路故障<br>如果所有故障鏈路恢復，此狀態將切換到idle狀態 |




- **Ring Status :** 環網狀態為啟用/禁用。
  - **Disable :** 禁用實例的 ERPS 協議。
  - **Enable :** 啟用實例的 ERPS 協議。
- **Mel :** 設定環網的控制 MEL。有效值為 0 至 7，預設值為 0。

| Note | 環網的實例維護等級(MEL)為環網自動保護倒換(R-APS)訊息提供通訊通道。在運行 ERPS 的第二層網路中，如果啟用了其他故障檢測協議，RAPS PDU 中的 MEL 欄位將決定這些封包是否可以轉發。如果 ERPS 環網的 MEL 值比故障檢測協議的 MEL 值小，則表明該封包優先級別較低而無法通過。此外，MEL 值還可用於與 ERPS 環網中不同廠商的設備進行通訊。相同的 MEL 值可確保多廠商設備之間的通訊順暢。建議將 MEL 設定為 7。在有主環和子環的網路中，兩個環的 MEL 都應設定為 7。 |
|---|---|

- **Protected Instance :** 有效值:0-15。保護實例設定,用於在 ERPS 環網中設定乙太網路環保護(ERP)實例。
- **Control VLAN :** 實例的控制 VLAN 應與控制 VLAN 下的 ERPS 控制 VLAN ID 相同，範圍從 1 到 4094。這是用於發送 ERPS PDU 的 VLAN ID。

| | |
|---|---|
| Note | 在 ERPS 環網中，控制 VLAN 僅用於轉發 RAPS PDU，從而提高了 ERPS 協議的安全性。ERPS 環網內的所有設備必須設定相同的控制 VLAN。其他 VLAN 不能與控制 VLAN 使用相同的 ID。例如,如果 VLAN 設定中已存在標準 VLAN 20,則無法將 VLAN 20 設定為 ERPS 環網的控制 VLAN。 |

- **WTR Time :** 設定環網的 WTR time 定時器。有效值在 1 至 12(以分鐘為單位)之間，預設值為 5 分鐘。
- **Guard Time :** 設定環網的 Guard time 定時器。有效值在 100 至 2000(以毫秒為單位)之間，預設值為 500 毫秒。
- **Work Mode :** 選擇回切模式或非回切模式。
  - **Revertive :** 選擇回切模是並啟用。

| | |
|---|---|
| Note | 得知環網故障恢復後，RPL owner 節點<br>將恢復 RPL 的阻塞狀態，並使網路流量傳輸路徑恢復到故障前的鏈路。 |

  - **Non_revertive :** 選擇並啟用非回切模式。

| | |
|---|---|
| Note | 得知環網故障恢復後，RPL owner 節點<br>不會阻塞 RPL，網路流量傳輸路徑與之前相同。 |

- **Ring ID :** 設定 ERPS 環網 ID。有效值從 1 至 239，用於區分不同的環網拓撲結構。
- **Ring Type :** 設定環網類型:數值"0"為主環，"1"為子環，預設值為 0。

| | |
|---|---|
| Note | 主環(如果該值設定為"0")：是連接互連節點上連接兩個連接埠的環。子環(如果該值設定為"1")：是透過兩個互連節點與其他網路相連的環，它不是環形網絡，只有透過互連節點連接起來才組成環形網路節點。 |

- **Port0 :** ERPS 環網連接埠 0，可以映射到實際交換器連接埠 1(GE1)-連接埠 24(GE24)。

| Note | 請勿設定與環網連接埠 1 相同。 |
|---|---|

- **Port0 Role :** 設定 ERPS 連接埠 0 角色為 “Normal” 、 “Owner” 、 “Neighbour” 或 “Next-Neighbour” 。
  - **Normal :** 除 “Owner” 和 “Neighbour” 節點外，其餘節點定義為 “Normal” 節點。
  - **Owner :** 負責阻塞 RPL 鏈路的一側。它將阻止封包從其阻塞連接埠發出。
  - **Neighbour :** 負責阻塞 RPL 鏈路的另一側。它將阻止封包從其阻塞連接埠發出。
  - **Next-Neighbour :** 負責阻塞下一個 RPL 鏈路的另一側。它將阻止封包從其阻塞連接埠發出。

- **Port1 :** ERPS 環網連接埠 1，可以映射到實際交換器連接埠 1(GE1)-連接埠 24(GE24)。

| Note | 請勿設定與環網連接埠 0 相同。 |
|---|---|

- **Port1 Role :** 設定 ERPS 連接埠 1 角色為 “Normal” 、 “Owner” 、 “Neighbour” 或 “Next-Neighbour” 。
  - **Normal :** 除 “Owner” 和 “Neighbour” 節點外，其餘節點定義為 “Normal” 節點。
  - **Owner :** 負責阻塞 RPL 鏈路的一側。它將阻止封包從其阻塞連接埠發出。
  - **Neighbour :** 負責阻塞 RPL 鏈路的另一側。它將阻止封包從其阻塞連接埠發出。
  - **Next-Neighbour :** 負責阻塞下一個 RPL 鏈路的另一側。它將阻止封包從其阻塞連接埠發出。

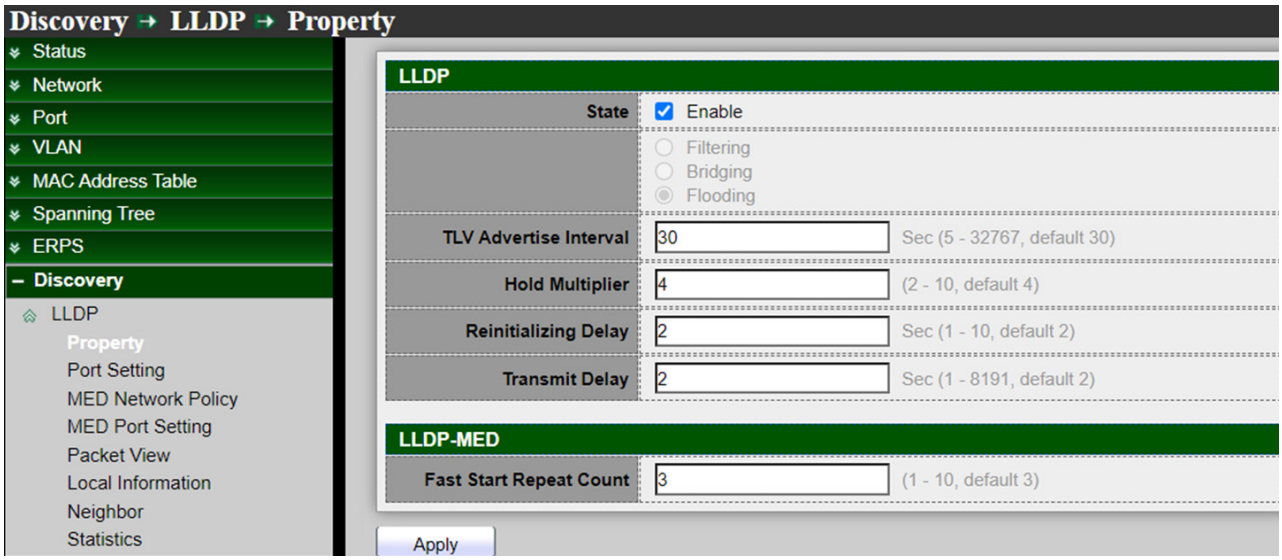
| Note | 在任一網環節點上啟用任何 ERPS 協議之前，請勿將所有交換器連接成迴圈（環網）。在拓撲結構中的所有節點都準備就緒之前，應至少拔掉一個環網連接埠。 |
|---|---|

*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

# 10. Discovery(LLDP)

鏈路層發現協議(Link Layer Discovery Protocol，LLDP)是一種乙太網協議套件中的廠商中立鏈路層協議，用於網路設備在 IEEE 802.1ab 區域網路(主要有線乙太網)上通告其身份、功能和鄰近設備。LLDP 訊息由設備以乙太網訊框的形式，按固定間隔從其每個介面發送。每個訊框都包含一個 LLDP 數據單元(LLDPDU)。每個 LLDPDU 都是一串類型(Tag)-長度(Length)-值(Value)結構(TLV)的序列。

## 10.1 屬性(Property)

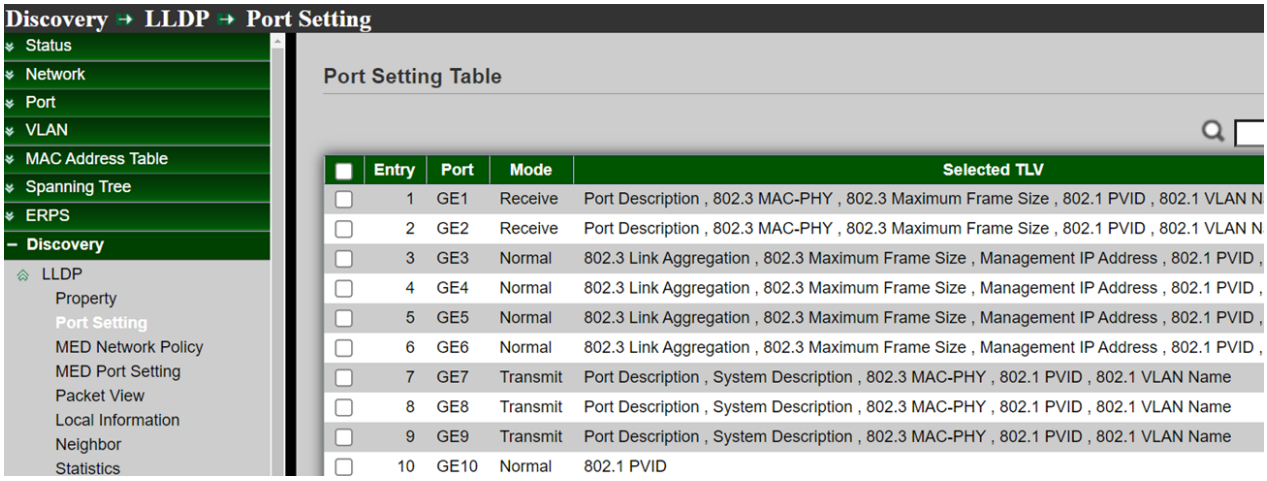



- **State :** 使用者管理員可以選擇開啟或關閉 LLDP 功能。
- **LLDP Handing :** 如果取消復選框，則使用者管理員可以選擇 LLDP 報文處理方式 Filtering(過濾) / Bridging(轉發) / Flooding(氾濫)。LLDP 全區域禁用時，選擇要過濾、轉發或氾濫的 LLDP PDU 處理操作。
  - **Filtering :** 刪除封包。
  - **Bridging :** (VLAN-aware氾濫)將封包轉發給所有VLAN成員。
  - **Flooding :** 將封包轉發給所有連接埠。
- **TLV Advertise Interval :** 選擇封包傳輸的時間間隔(範圍 5-32760 秒，預設 30 秒)。
- **Hold Multiplier :** 設定 Hold 值(範圍 2-10，默認 4)。使用者管理員可以通過設定 Hold 乘積的值，來控制鄰近設備上本地訊息的延遲時間。*TTL(存活時間)=Hold multiplier(發送週期乘積)* TLV Advertise Interval(發送週期)*。
- **Reinitializing Delay :** 選擇重新初始化前的延遲時間(範圍 1-10 秒，預設 2 秒)。
- **Transmit Delay :** 選擇傳送 LLDP 封包後的延遲時間(範圍 1-8191 秒，預設 2 秒)。
- **Fast Start Repeat Count :** 連接埠鏈接時的快速啟動重複次數(範圍 1-10，預設 3)。

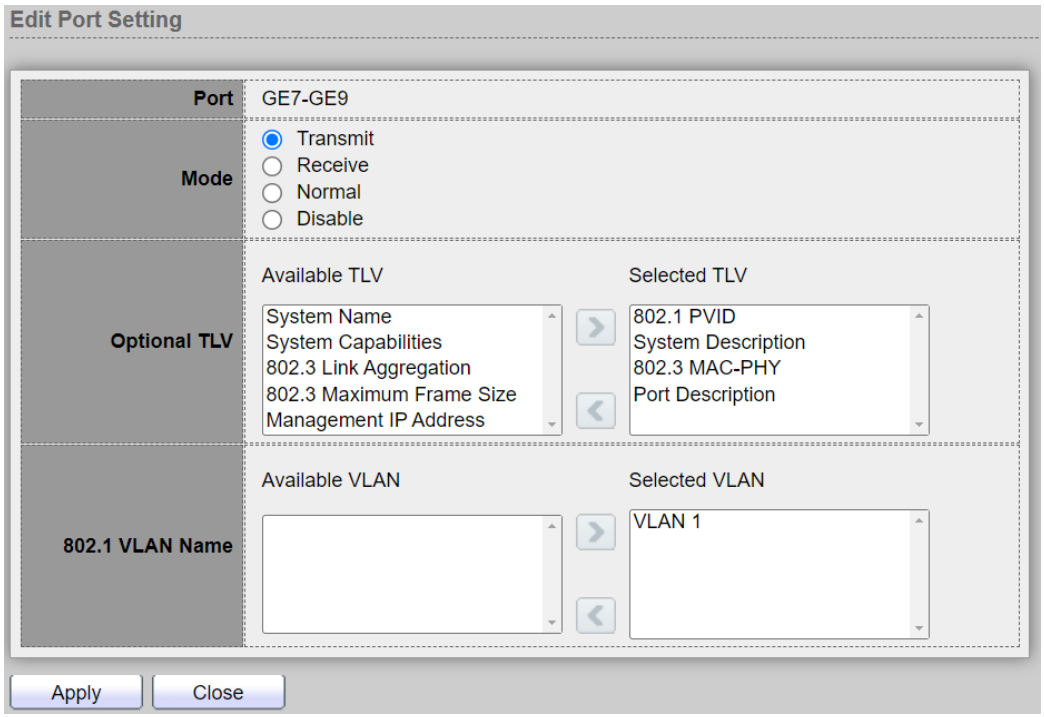
*點擊"Apply"儲存您的變更設定。*

## 10.2 連接埠設定(Port Setting)

使用者管理員可以設定每個連接埠 LLDPDU 的 Transmit(只發) / Receive(只收) / Normal(收發)或 Disable(關閉)模式，並從"Optional TLV"列表選擇發送連接埠的 TLV 類型。




| 欄位 | 描述 |
|---|---|
| **Port** | 顯示連接埠LLDP狀態 |
| **Mode** | 顯示Transmit (只發),Receive (只收),Normal (收發),Disable(關閉) |
| **Selected TLV** | 顯示已選TLV資訊，VLAN資訊 |

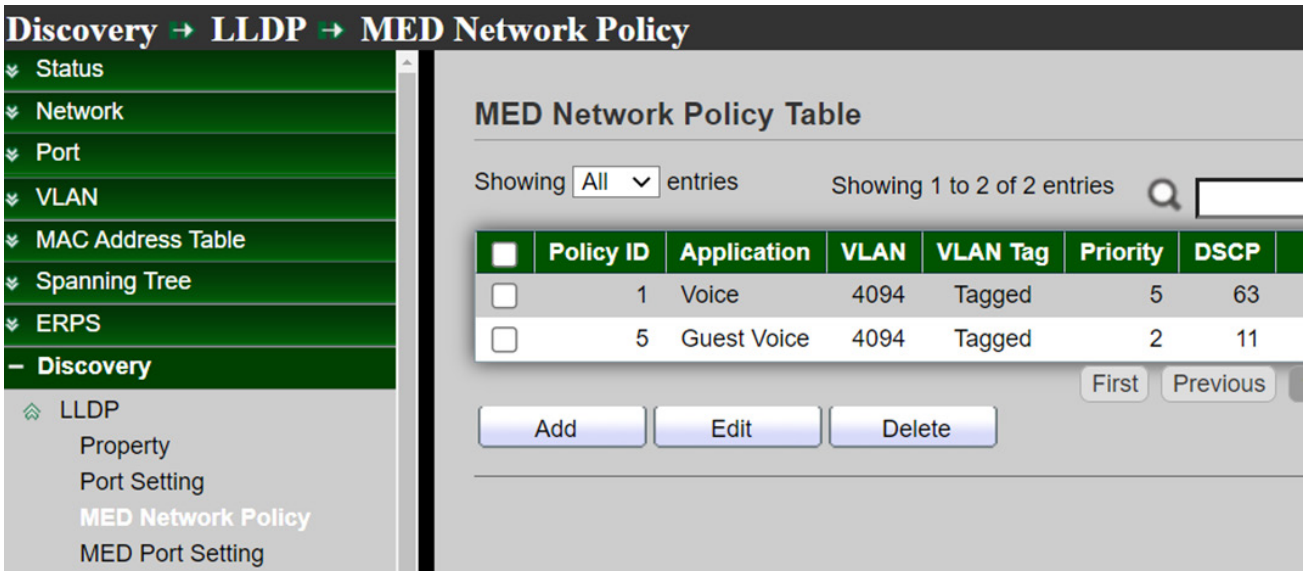



- **Mode :** 使用者管理員可以選擇 Transmit (只發),Receive (只收),Normal (收發),Disable(關閉)，如果選擇關閉將不發送也不接收 LLDPDU。
  - Transmit (TX Only) : 只發 LLDP PDU。
  - Receive (RX Only) : 只收LLDP PDU。
  - Normal (TX And RX) : 既發送也接收 LLDP PDU。
  - Disable : 禁用 LLDP PDU 的傳輸。
- **Optional TLV :** 使用者管理者可以將設定資訊分成不同的 TLV，封裝成 LLDPDU 並傳送給鄰近設備。
  - System Name(系統名稱)
  - Port Description(連接埠描述)
  - System Description(系統描述)
  - System Capability(系統功能)
  - 802.3 MAC-PHY
  - 802.3 Link Aggregation(鏈路聚合)
  - 802.3 Maximum Frame Size(最大封包大小)
  - Management Address(管理地址)
  - 802.1 PVID
- **802.1 VLAN Name :** 選擇要攜帶的 VLAN ID 名稱(允許多選)。

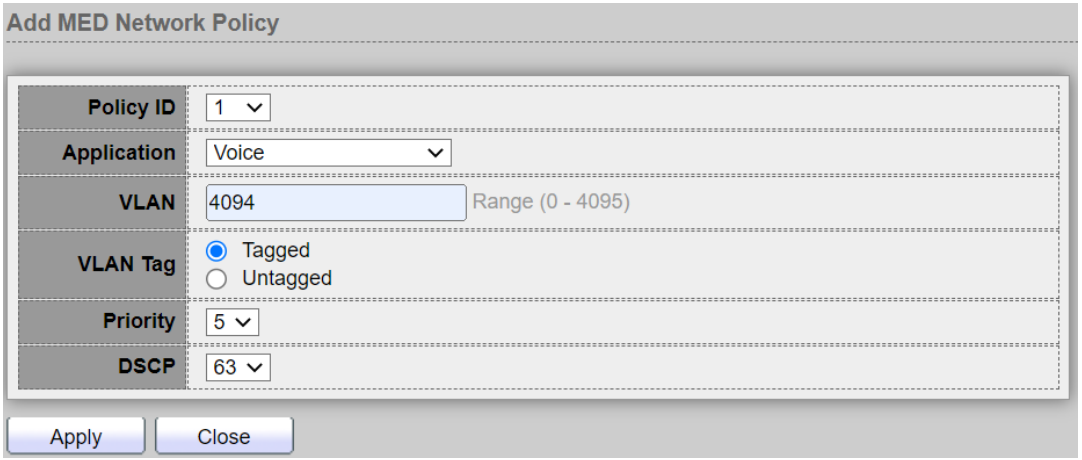
*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

## 10.3 媒體終端發現網路策略(MED Network Policy)

使用者管理員可以看到 LLDP MED 網路策略設定，並設定"**add**"、"**Edit**"和"**Delete**"功能進行管理。




| 欄位 | 描述 |
|---|---|
| Policy ID | 顯示策略ID |
| Application | 顯示網路策略類型 |
| VLAN | 顯示VLAN ID |
| VLAN Tag | 顯示VLAN標籤狀態 |
| Priority | 顯示L2優先級別 |
| DSCP | 顯示DSCP值 |

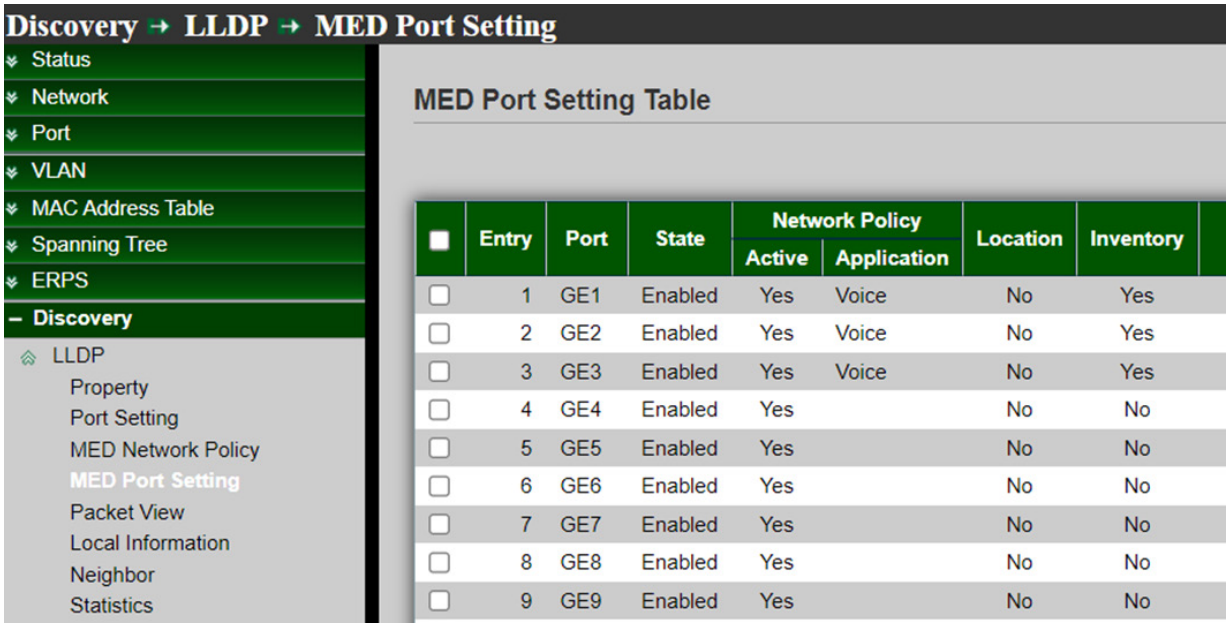



- **Policy ID :** 選擇指定的網路策略 ID 進行設定。
- **Application :** 選擇網路策略應用類型。
  - Voice(語音)
  - Voice Signaling(語音信令)
  - Guest Voice(訪客語音)
  - Guest Voice Signaling(訪客語音信令)
  - Softphone Voice(軟體電話語音)
  - Video Conferencing(視訊會議)
  - App Streaming Video(流影片)
  - Video Signaling(影片信令)
- **VLAN :** 設定 VLAN ID，範圍 1 至 4094。
- **VLAN Tag :** 設定 VLAN 標籤狀態。
  - **Tagged :** 流量為 tagged。
  - **Untagged :** 流量為 untagged。
- **Priority :** 設定 L2 優先級別，範圍 0 至 7。
- **DSCP :** 設定 DSCP 值，範圍 0 至 63。

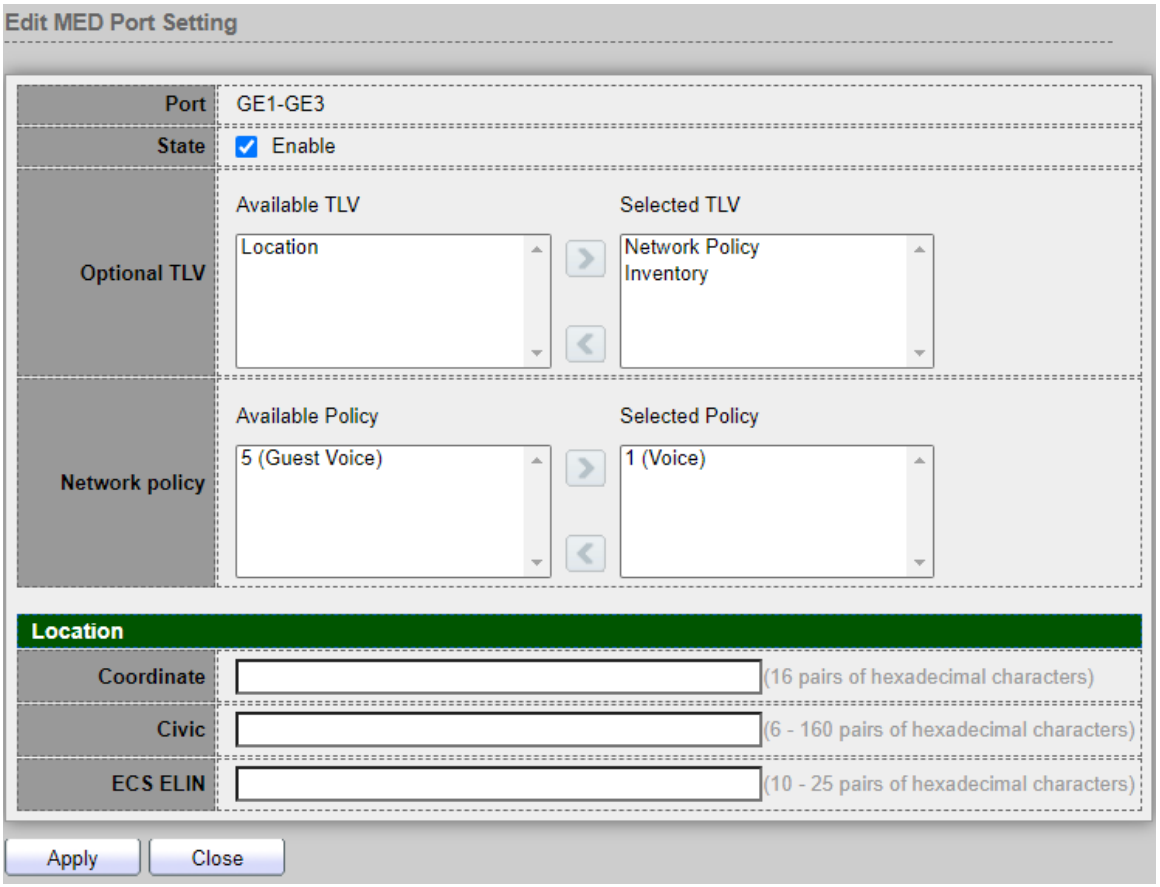
*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

## 10.4 媒體終端發現埠設定(MED Port Setting)

使用者管理員可以查看 LLDP MED 埠設定。




| 欄位 | 描述 |
|---|---|
| Port | 顯示LLDP MED指定連接埠 |
| State | 顯示LLDP MED狀態 |
| Optional TLV | 顯示LLDP MED可選TLV |
| Network Policy | 顯示LLDP MED網路策略Active狀態和應用類型ID |
| Location | 顯示位置狀態 |
| Inventory | 用yes或no顯示清單 |

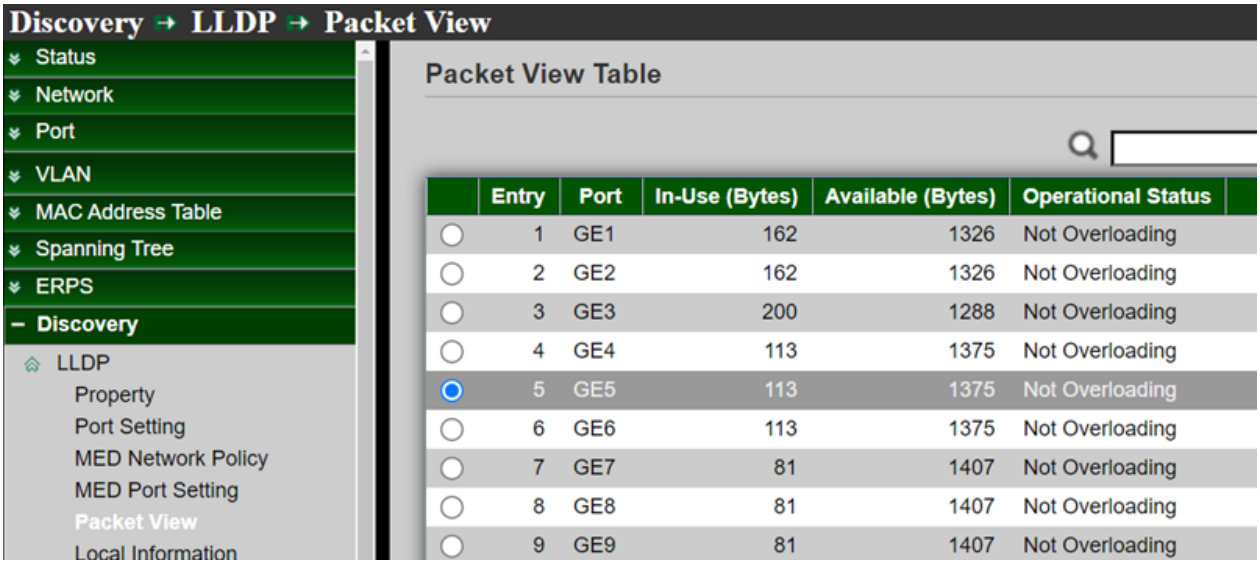



- **Port :** 選擇指定埠或所有埠來設定 LLDP MED。
- **State :** 選擇 LLDP MED 啟用狀態。
- **Optional TLV :** 選擇 LLDP MED 可選 TLV (允許多選)。
  - Network Policy(網路策略)
  - Location(位址)
  - Inventory(清單)
- **Network Policy :** 選擇要與連接埠綁定的網路策略 ID。應先在 MED Network Policy 頁面中創建網路策略。
- **Location :**
  - **Coordinate : 設定坐標位置。**
  - **Civic : 設定中心位址。**
  - **ECS ELIN : 設定緊急呼叫服務緊急位置標識號。**

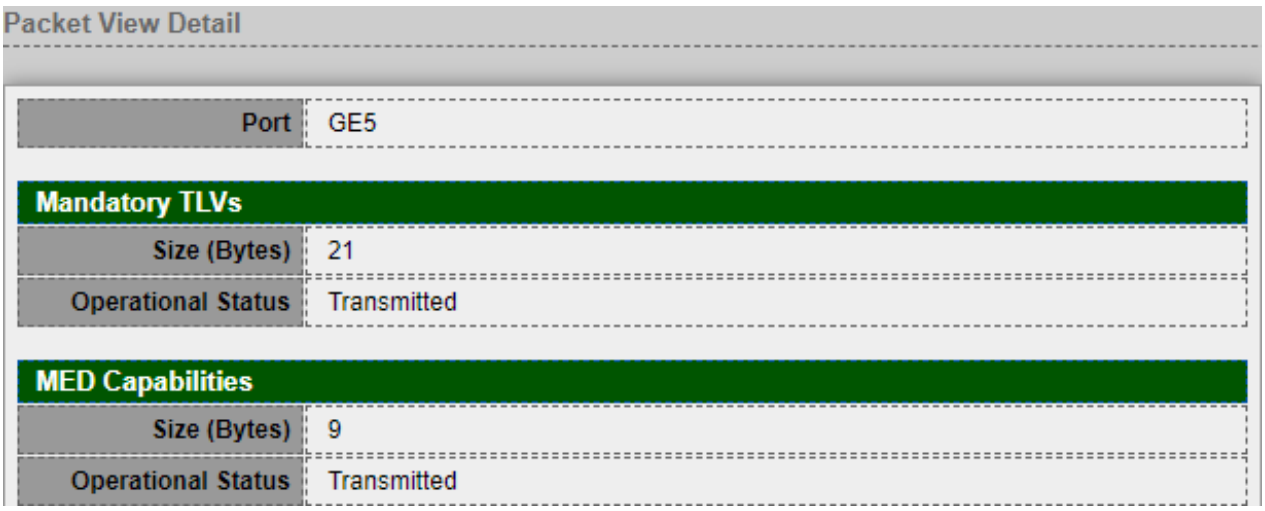
*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

# 10.5 封包查探(Packet View)

使用者管理員可以選擇要查看的連接埠，然後點擊"**Detail**"查看所選連接埠上的 LLDP 封包資訊。




| 欄位 | 描述 |
|---|---|
| Port | 連接埠編號 |
| In-Use (Bytes) | 每個封包中LLDP資訊的位元組總數 |
| Available (Bytes) | 每個封包中留給附加LLDP資訊的可用位元組總數 |
| Operational Status | 是否超載 |



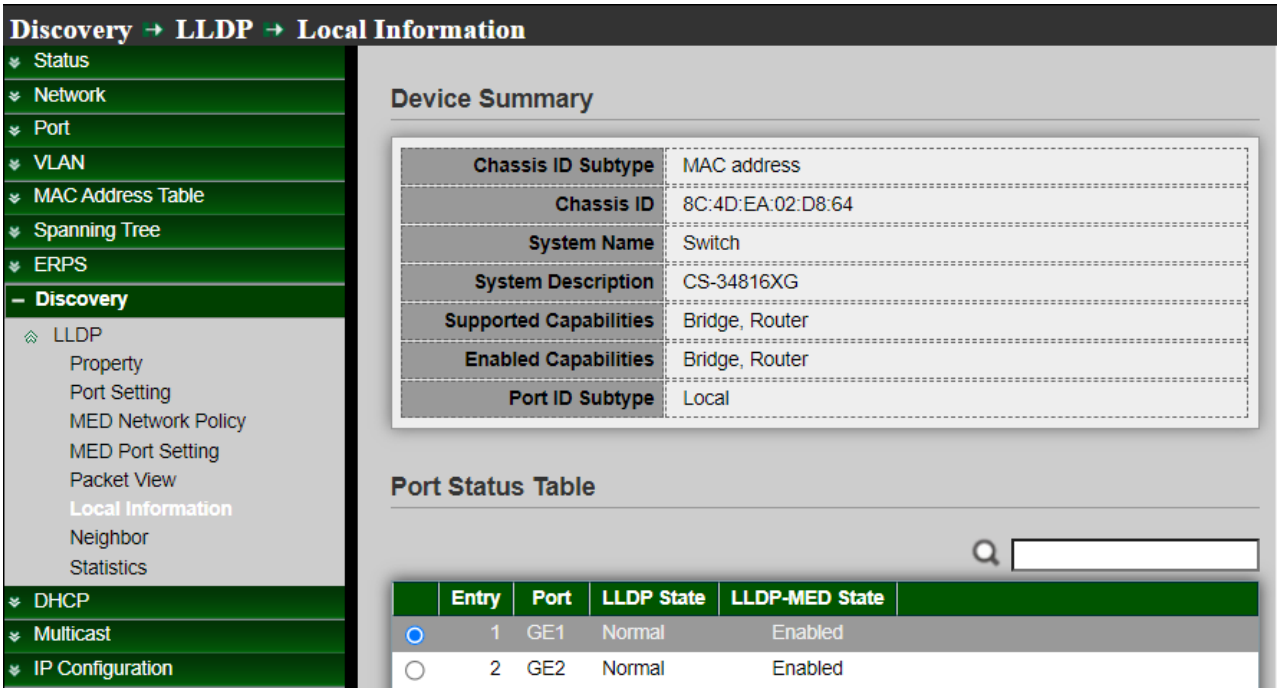

*點擊 "Close" 關閉檢視詳情頁面。*

| 欄位 | 描述 |
|---|---|
| Port | 連接埠編號 |
| Mandatory TLVs | 傳送強制TLV所需的位元組數<br>狀態為轉送或過載 |
| MED Capabilities | MED功能封包位元組總大小<br>狀態為轉送或過載 |
| MED Location | MED位置封包位元組總大小<br>狀態為轉送或過載 |

| | |
|---|---|
| MED Network Policy | MED 網路策略封包位元組總大小<br>狀態為轉送或過載 |
| MED Inventory | MED 庫存位元組總大小<br>狀態為轉送或過載 |
| MED Extended Power via MDI | 通過 MDI 封包位元組大小的 LLDP MED 擴展電源總數<br>狀態為轉送或過載 |
| 802.3 TLVs | MED 802.3封包位元組總大小<br>狀態為轉送或過載 |
| Optional TLVs | 總MED可選TLVs封包位元組大小<br>狀態為轉送或過載 |
| 802.1 TLVs | MED 802.1封包位元組總大小<br>狀態為轉送或過載 |
| Total | 每個封包中LLDP資訊的位元組總數 |

## 10.6 本地資訊(Local Information)

顯示交換器摘要和每個連接埠的 LLDP 狀態。使用者管理員可以選擇要查看的連接埠，然後點擊"**detail**"查看本地設備的資訊以及所選連接埠的 LLDP 屬性資訊。



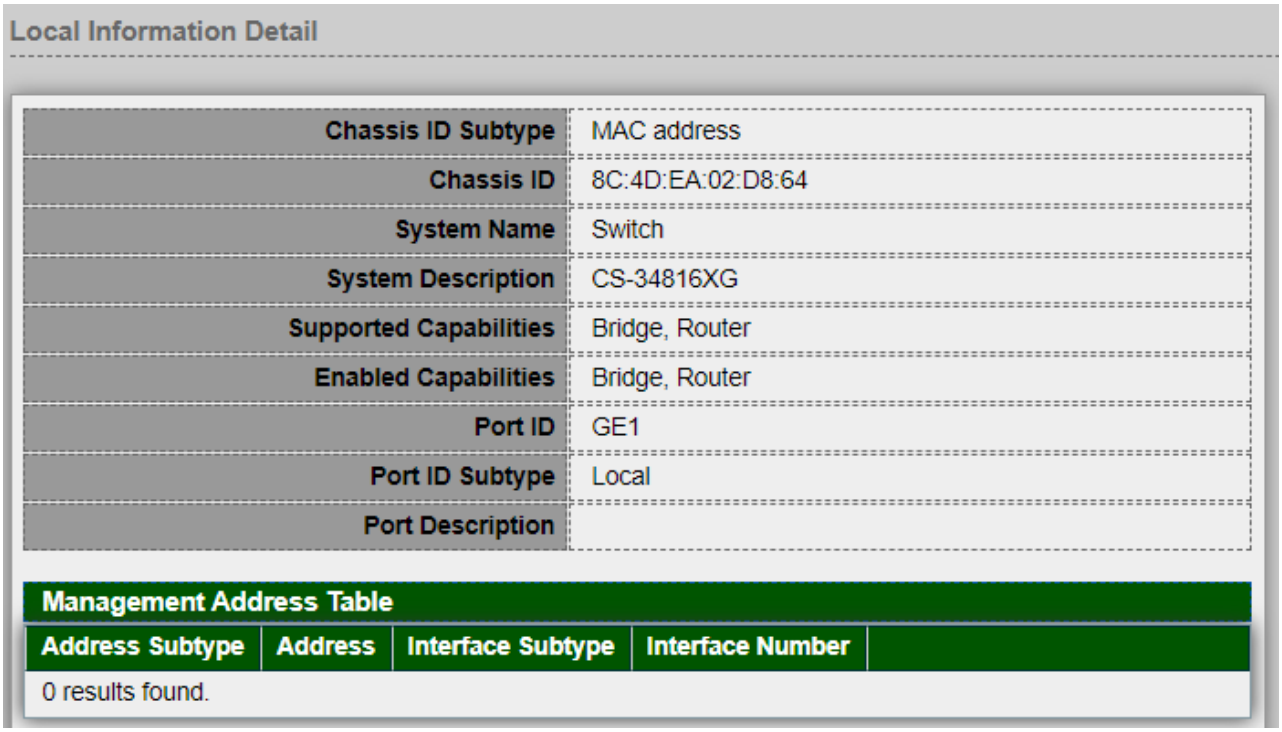
## Device Summary

| 欄位 | 描述 |
|---|---|
| Chassis ID Subtype | 機箱ID的類型，如MAC位址 |
| Chassis ID | 機箱識別碼。如果機箱ID子類型是MAC位址，則顯示交換器的MAC位址 |
| System Name | 交換器系統名稱 |
| System Description | 交換器描述說明 |
| Supported Capabilities | 設備支援的主要功能，如Bridge、WLAN AP或Router |
| Enabled Capabilitie | 設備已啟用的主要功能 |
| Port ID Subtype | 顯示的連接埠標識符類型 |

## Port Status Table

| 欄位 | 描述 |
|---|---|
| Port | 連接埠編號 |
| LLDP Status | LLDP發送和接收狀態 |
| LLDP Med Status | LLDP MED啟用狀態 |

*點擊"**detail**"查看所選連接埠的詳細資訊。*



Local Information Detail

| | |
|---|---|
| Chassis ID Subtype | MAC address |
| Chassis ID | 8C:4D:EA:02:D8:64 |
| System Name | Switch |
| System Description | CS-34816XG |
| Supported Capabilities | Bridge, Router |
| Enabled Capabilities | Bridge, Router |
| Port ID | GE1 |
| Port ID Subtype | Local |
| Port Description | |

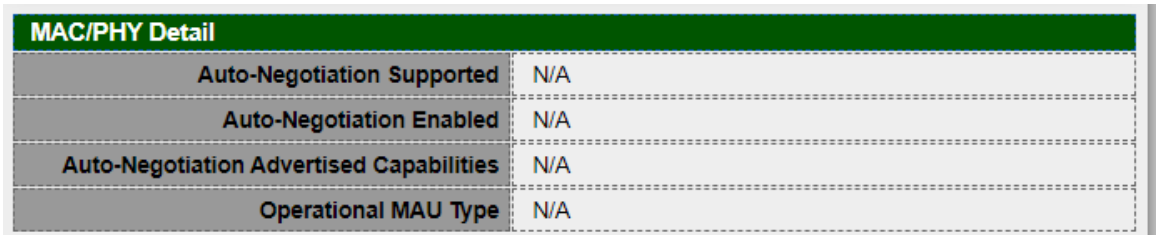
Management Address Table

| Address Subtype | Address | Interface Subtype | Interface Number | |
|---|---|---|---|---|
| 0 results found. | | | | |

## Management Address Table

| 欄位 | 描述 |
|---|---|
| Address Subtype | 連接埠編號類型 |
| Address | 顯示管理IP位址類型 |
| Interface Subtype | 最適合管理使用的傳回位址，通常是第3層位址 |
| Interface number | 與管理位址相關的特定介面 |

## MAC/PHY Details



MAC/PHY Detail

| | |
|---|---|
| Auto-Negotiation Supported | N/A |
| Auto-Negotiation Enabled | N/A |
| Auto-Negotiation Advertised Capabilities | N/A |
| Operational MAU Type | N/A |

| 欄位 | 描述 |
| --- | --- |
| Auto-Negotiation Supported | 連接埠速率自協商支援狀態 |
| Auto-Negotiation Enabled | 連接埠速率自協商啟用狀態 |
| Auto-Negotiation Advertised Capabilities | 連接埠速率自協商功能，例如1000BASE-T半雙工模式、100BASE-TX全雙工模式 |
| Operational MAU Type | 介質連線單元(MAU)類型。MAU執行實體層功能，包括從乙太網路介面的碰撞檢測和將位元注入到網路中進行數位資料轉換，例如100BASE-TX全雙工模式。 |

## 802.3 Detail

| 802.3 Detail | |
| --- | --- |
| 802.3 Maximum Frame Size | 1522 |

| 欄位 | 描述 |
| --- | --- |
| 802.3 Maximum Frame Size | 支援的最大IEEE 802.3訊框大小. |

## 802.3 Link Aggregation

| 802.3 Link Aggregation | |
| --- | --- |
| Aggregation Capability | N/A |
| Aggregation Status | N/A |
| Aggregation Port ID | N/A |

| 欄位 | 描述 |
| --- | --- |
| Aggregation Capability | 表示介面聚合功能 |
| Aggregation Status | 表示介面聚合狀態 |

| | |
|---|---|
| Aggregation Port ID | 發佈的聚合介面ID |

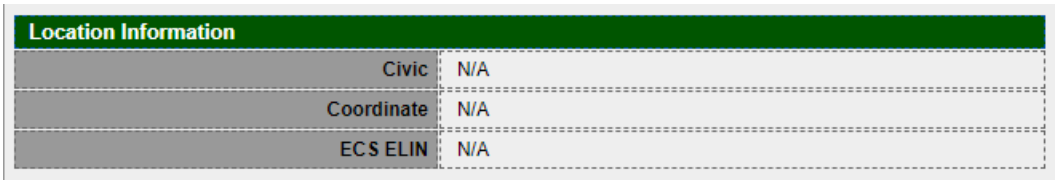
## MED Detail

| MED Detail | |
|---|---|
| Capabilities Supported | Capabilities , Network policy |
| Current Capabilities | Capabilities , Network policy |
| Device Class | Network Connectivity |
| PoE Device Type | N/A |
| PoE Power Source | N/A |
| PoE Power Priority | N/A |
| PoE Power Value | N/A |
| Hardware Revision | N/A |
| Firmware Revision | N/A |
| Software Revision | N/A |
| Serial Number | N/A |
| Manufacturer Name | N/A |
| Model Name | N/A |
| Asset ID | N/A |

| 欄位 | 描述 |
|---|---|
| Capabilities Supported | 連接埠支援的MED功能 |
| Current Capabilities | 連接埠啟用的MED功能 |
| Device Class | LLDP MED端點設備類別 |
| PoE Device Type | 連接埠PoE類型，例如供電(僅支援POE型號) |
| PoE Power Source | 連接埠電源(僅支援POE型號) |
| PoE Power Priority | 連接埠供電優先級(僅支援POE型號) |

| | |
|---|---|
| PoE Power Value | 連接埠功率值(僅支援POE型號) |
| Hardware Revision | 硬體版本 |
| Firmware Revision | 韌體版本 |
| Software Revision | 軟體版本 |
| Serial Number | 設備序列號 |
| Manufacturer Name | 設備晶片組IC製造商名稱 |
| Model Name | 設備晶片組IC型號名稱 |
| Asset ID | 資產ID |

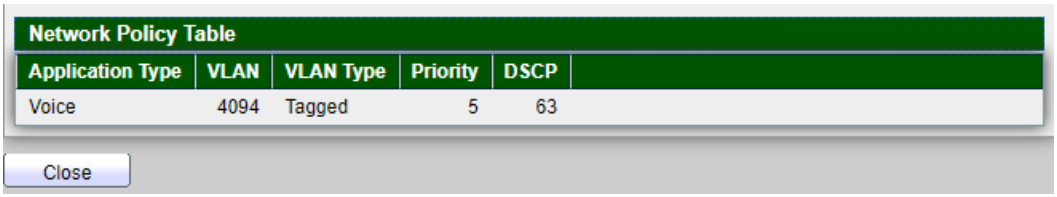
## Location Information



| Location Information | |
|---|---|
| Civic | N/A |
| Coordinate | N/A |
| ECS ELIN | N/A |

| 欄位 | 描述 |
|---|---|
| Coordinate | 設定坐標位置 |
| Civic | 設定中心位址 |
| ECS ELIN | 設定緊急呼叫服務緊急位置標識號 |

## Network Policy Table

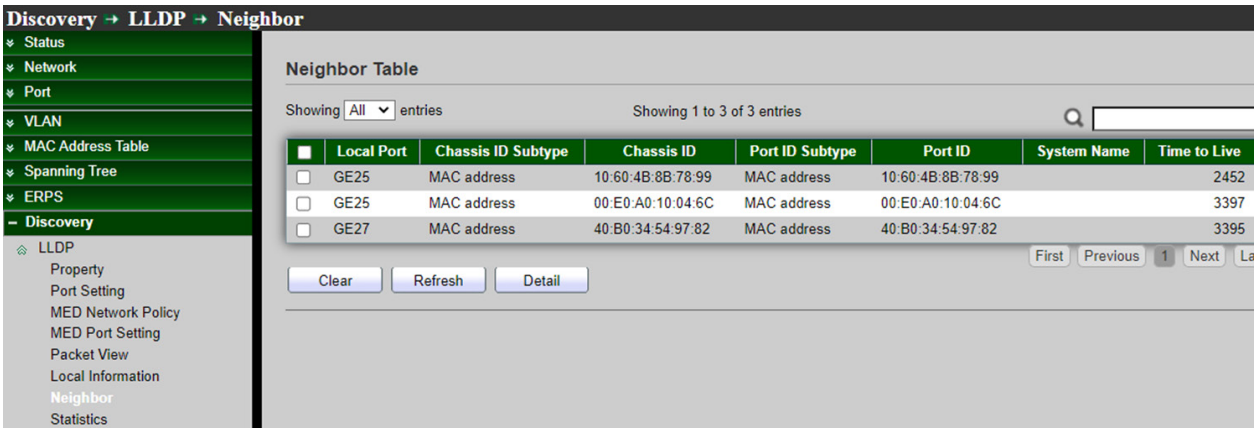



| 欄位 | 描述 |
|---|---|
| Application | 顯示網路策略應用類型：<br>● Voice (語音)<br>● Voice Signaling(語音信令)<br>● Guest Voice(訪客語音)<br>● Guest Voice Signaling(訪客語音信令)<br>● Softphone Voice(軟體電話語音)<br>● Video Conferencing(視訊會議)<br>● App Streaming Video(流影片)<br>● VideoSignaling(影片信令) |
| VLAN | 顯示VLAN ID |
| VLAN Type | VLAN標籤狀態。顯示網路策略應用流量類型是“tagged”或“untagged” |
| Priority | 顯示L2優先級別 |
| DSCP | 顯示DSCP值 |

*點擊“Close”關閉資訊頁面。*

## 10.7 鄰近設備(Neighbor)

該頁面顯示使用LLDP協議從鄰近設備接收到的資訊。超時後資訊會刪除(基於從鄰近設備接收到的生存TLV時間值，在此期間內未從鄰近設備接收到任何 LLDP PDU)，並設定**"add"**、**"Edit"**和**"Delete"**功能進行管理。




| 欄位 | 描述 |
|---|---|
| Local Port | 鄰近設備連接的本地埠編號 |
| Chassis ID Subtype | 機箱ID的類型(如MAC位址) |
| Chassis ID | 802 LAN鄰近設備機箱的識別碼 |
| Port ID Subtype | 顯示連接埠標識符類型 |
| Port ID | 連接埠的標識符 |
| System Name | 交換器的發佈名稱 |
| Time to Live | 超時後刪除此鄰近設備資訊的時間間隔(秒) |

*點擊 "detail" 查看所選鄰近設備的詳細資訊。*

Neighbor Information Detail

| | |
|---|---|
| Local Port | GE25 |

**Basic Detail**

| | |
|---|---|
| Chassis ID Subtype | MAC address |
| Chassis ID | 10:60:4B:8B:78:99 |
| Port ID Subtype | MAC address |
| Port ID | 10:60:4B:8B:78:99 |
| Port Description | |
| System Name | |
| System Description | |
| Supported Capabilities | N/A |
| Enabled Capabilities | N/A |

**Management Address Table**

| Address Subtype | Address | Interface Subtype | Interface Number |
|---|---|---|---|
| 0 results found. | | | |

**MAC/PHY Detail**

| | |
|---|---|
| Auto-Negotiation Supported | True |
| Auto-Negotiation Enabled | True |
| Auto-Negotiation Advertised Capabilities | 1000baseTFD |
| Operational MAU Type | Other |

**802.3 Power via MDI**

| | |
|---|---|
| MDI Power Support Port Class | N/A |
| PSE MDI Power Support | N/A |
| PSE MDI Power State | N/A |
| PSE Power Pair Control Ability | N/A |
| PSE Power Pair | N/A |
| PSE Power Class | N/A |
| Power Type | N/A |
| Power Source | N/A |
| Power Priority | N/A |
| PD Request Power Value | N/A |
| PSE Allocated Power Value | N/A |

| 802.3 Detail | |
|---|---|
| 802.3 Maximum Frame Size | N/A |

| 802.3 Link Aggregation | |
|---|---|
| Aggregation Capability | N/A |
| Aggregation Status | N/A |
| Aggregation Port ID | N/A |

| 802.1 VLAN and Protocol | |
|---|---|
| PVID | |
| VLAN Name | N/A |

| MED Detail | |
|---|---|
| Capabilities Supported | Capabilities |
| Current Capabilities | Capabilities |
| Device Class | Endpoint Class 1 |
| PoE Device Type | N/A |
| PoE Power Source | N/A |
| PoE Power Priority | N/A |
| PoE Power Value | N/A |
| Hardware Revision | N/A |
| Firmware Revision | N/A |
| Software Revision | N/A |
| Serial Number | N/A |
| Manufacturer Name | N/A |
| Model Name | N/A |
| Asset ID | N/A |

| Location Information | |
|---|---|
| Civic | N/A |
| Coordinate | N/A |
| ECS ELIN | N/A |

**Network Policy Table**

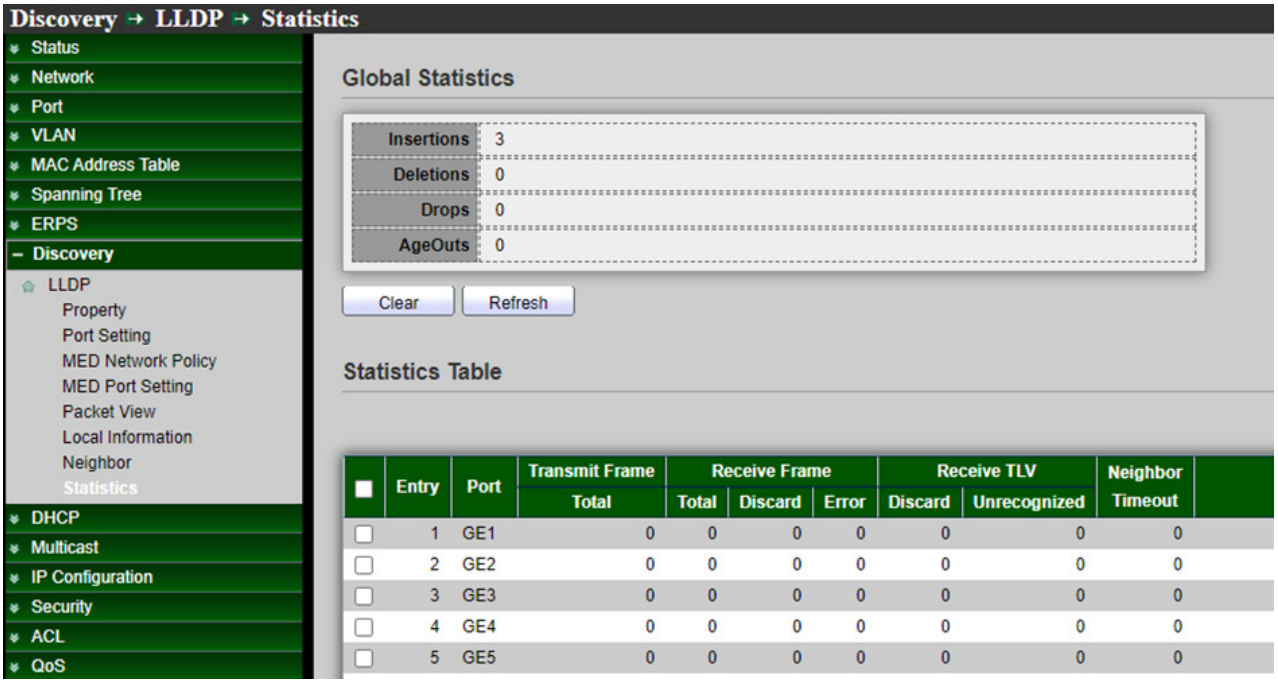
| Application Type | VLAN | VLAN Type | Priority | DSCP |
|---|---|---|---|---|
| 0 results found. | | | | |

Close

*點擊 "Close" 關閉資訊頁面。*

# 10.8 統計數據(Statistics)

此頁面顯示每個連接埠的 LLDP 統計資料。鏈路層發現協議(LLDP)的 Statistics 頁面顯示交換器上傳送和接收的 LLDP 訊框的摘要和每個連接埠資訊。




## Global Statistics

| 欄位 | 描述 |
|---|---|
| Insertions | 由特定MAC服務存取點(MSAP)發佈的完整資訊集插入到與遠端系統關聯的表中的次數 |
| Deletions | 從與遠端系統關聯的表中刪除MSAP發佈的完整資訊集到的次數 |
| Drops | 由於資源不足無法將MSAP發佈的完整資訊集輸入到與遠端系統關聯的表中的次數 |
| Age Outs | 由於資訊及時性間隔已過期，從與遠端系統關聯的表中刪除MSAP發佈的完整資訊集到的次數 |

*點擊 "Clear" 清除頁面或 "Refresh" 重新整理頁面。*

### Statistics Table

| 欄位 | 描述 |
|---|---|
| Port | 介面或連接埠編號 |
| Transmit Frame Total | 對應連接埠傳送的LLDP訊框數 |
| Receive Frame | ● **Total :** LLDP 代理啟用時，該 LLDP 代理在對應連接埠接收到的 LLDP 訊框數<br>● **Discarded :** 對應連接埠上的 LLDP 代理因各種原因丟棄的 LLDP 訊框數<br>● **Errors :** LLDP 代理啟用時，LLDP 代理在對應連接埠接收到的無效 LLDP 訊框數 |
| Receive TLV | ● **Discarded :** 對應連接埠上的 LLDP 代理因各種原因丟棄的 LLDP 訊框的 TLV 數量<br>● **Unrecognized :** LLDP 代理啟用時，未識別 LLDP 訊框的 TLV 數量 |
| Neighbor Timeout | 超時的LLDP訊框數 |

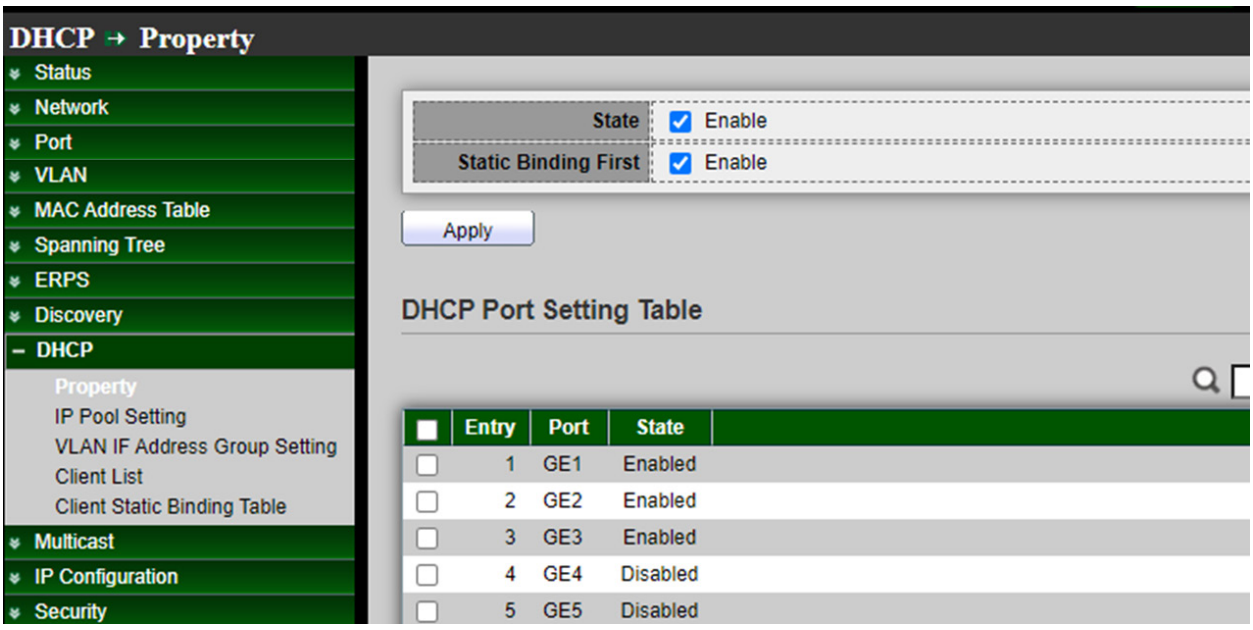
# 11. DHCP

該協定在用戶端-伺服器模型上運行。當 DHCP 用戶端連接到網路時，它們會發送廣播查詢，從 DHCP 伺服器請求必要的資訊。DHCP 伺服器管理 IP 位址範圍和網路設定資訊。如果它們收到來自 DHCP 用戶端的查詢，就會自動為它們分配一個 IP 位址和網路參數。

動態主機設定協定(DHCP)是一種標準化網路協定。它在互聯網協定(IP)網路中用於動態分配網路設定參數。例如，設備可以向 DHCP 伺服器請求介面的 IP 位址。使用 DHCP 還可以減少網路使用者管理員或使用者手動設定的需要。

## 11.1 屬性(Property)

使用者管理員可以設定“DHCP port Setting Table”來啟用/停用 DHCP 伺服器功能。



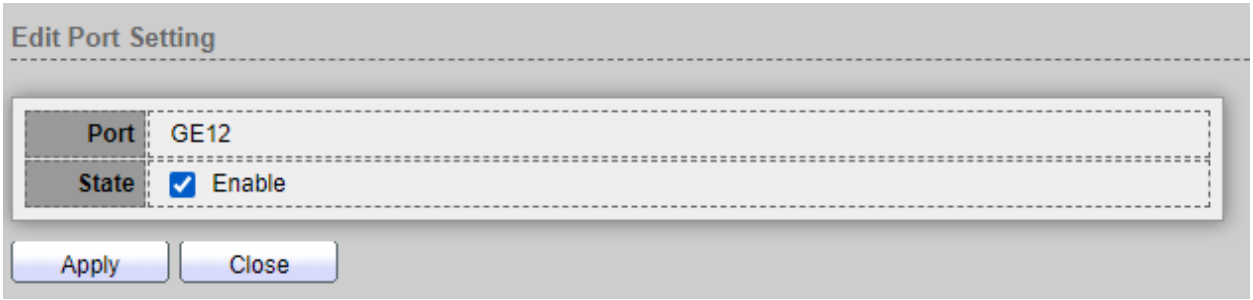

使用此部分啟用交換器上的功能。還可以選擇"Static Binding First"功能，勾選 “enable” 進行設定。

*點擊"Apply"儲存您的變更設定。*

| 欄位 | 描述 |
|---|---|
| Port | 顯示 DHCP 的連接埠清單 |
| State | 顯示 DHCP 啟用或 DHCP 停用狀態 |

### Edit Port Setting :

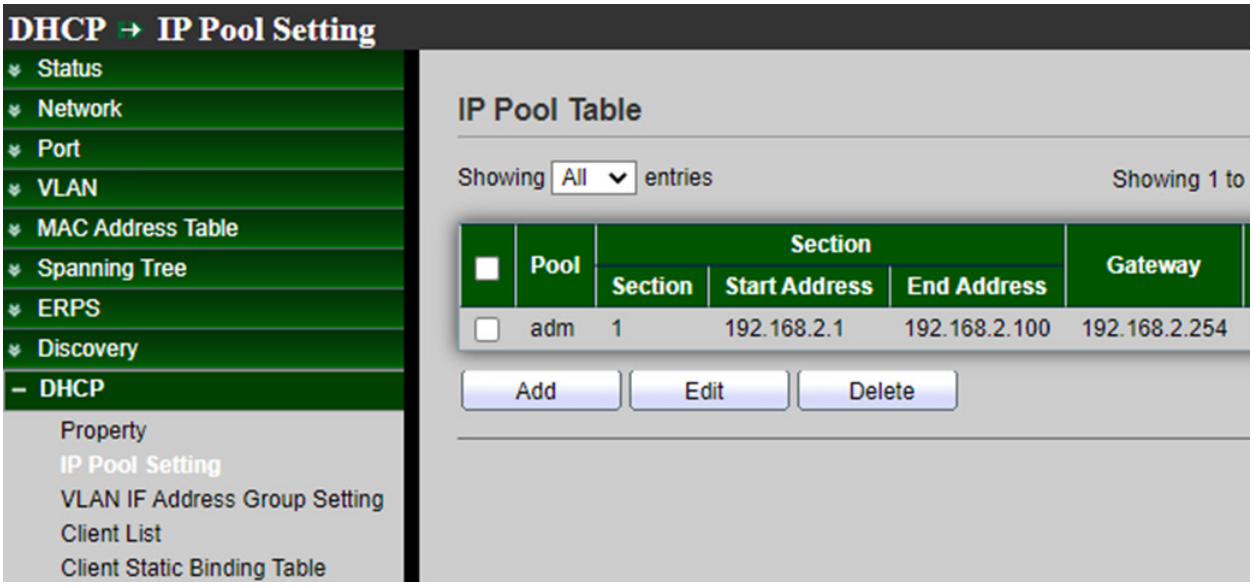
可以選擇要設定的連接埠形式 GE1 - GE28 (連接埠)和 LAG1~LAG8 (群組)，然後點擊"Edit"編輯 DHCP 連接埠，勾選 “enable” 進行設定。

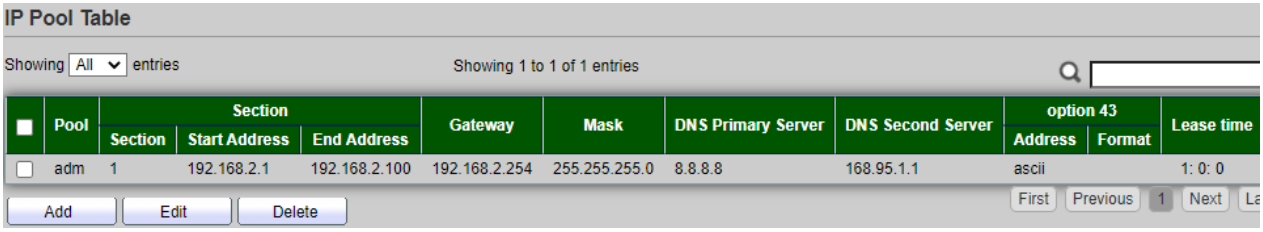



*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

## 11.2 IP 範圍設定(IP Pool Setting)

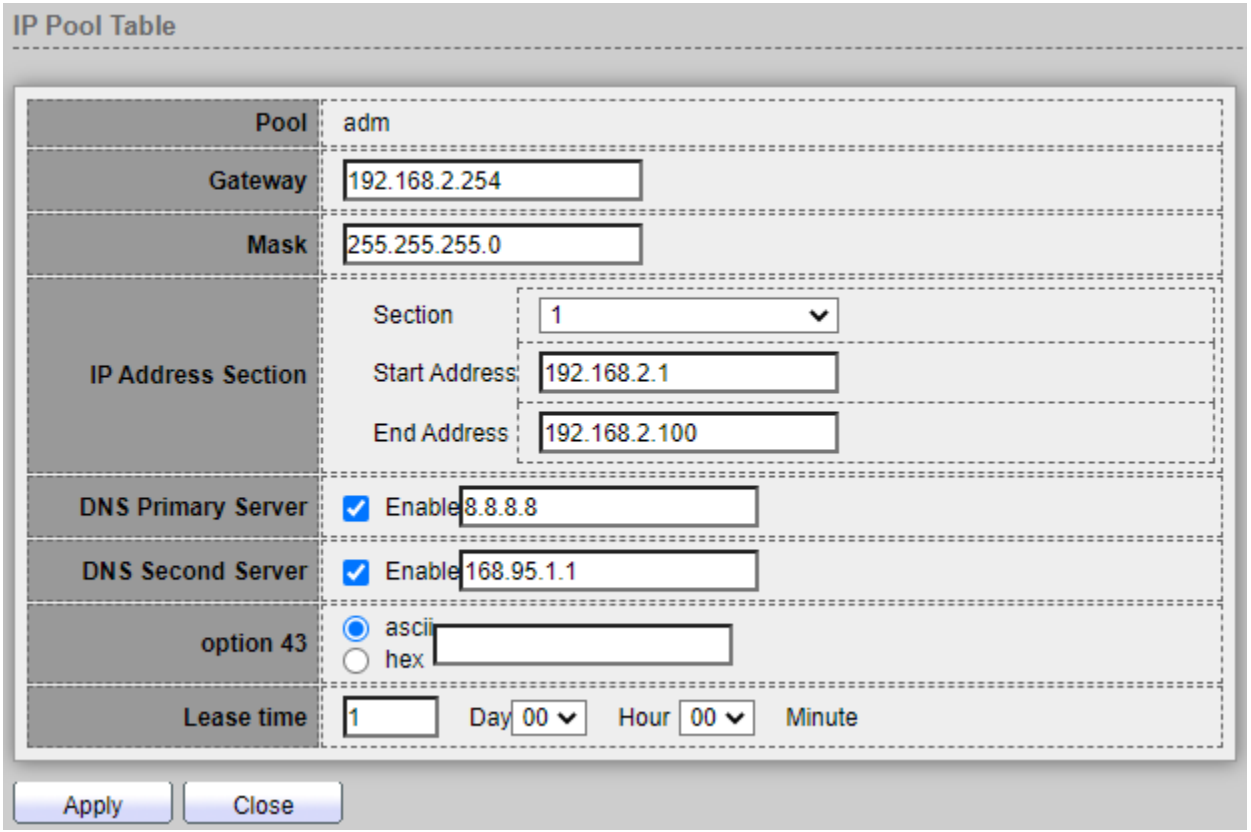
使用者管理員可以設定 IP Pool Table Setting，並設定"**add**"、"**Edit**"和"**Delete**"功能進行管理。




| 欄位 | 描述 |
|---|---|
| Pool | 顯示範圍名稱 |
| Section | • **Section :** 欄位清單<br>• **Start Address :** 顯示該DHCP伺服器實例設定的IP位址範圍的起始IP位址<br>• **End Address :** 顯示該DHCP伺服器實例設定的IP位址範圍的最後IP位址 |
| Gateway | 顯示從該 DHCP 伺服器實例發送給用戶端的預設閘道值 |
| Mask | 顯示從該 DHCP 伺服器實例發送到用戶端的子網絡遮罩值 |

| | |
|---|---|
| DNS Primary Server | 顯示從該 DHCP 伺服器實例發送到用戶端的主要 DNS 伺服器值 |
| DNS Second Server | 顯示從該 DHCP 伺服器實例發送到用戶端的次要 DNS 伺服器值 |
| Option43 | • **Address :** 顯示option 43位址<br>• **Format :** 顯示option 43格式類型 |
| Lease time | 該欄位顯示 IP 位址有效時間 |




- **Pool :** 選擇新增範圍並輸入 DHCP 範圍名稱。
- **Gateway :** 輸入閘道 IP 位址，閘道位置是在 LAN 上作為中繼所有進出 LAN 流量的主機(通常為主機上所指定的一台可將主機的子網路連結到其他網路(例如 WAN)的路由器。
- **Mask :** 分配 IP 位址的子網路遮罩。
- **IP Address Section :**
  - **Section :** 選擇欄位編號。
  - **Start Address :** 輸入 DHCP 伺服器為連接的設備分配 IP 位址的起始點 IP。

- **End Address :** 輸入 DHCP 伺服器為連接的設備分配 IP 位址的終點 IP。

➢ **DNS Primary Server :** 選擇 “enable” 並填寫主要 DNS IP 位址。

➢ **DNS Second Server :** 選擇 “enable” 並填寫次要 DNS IP 位址。

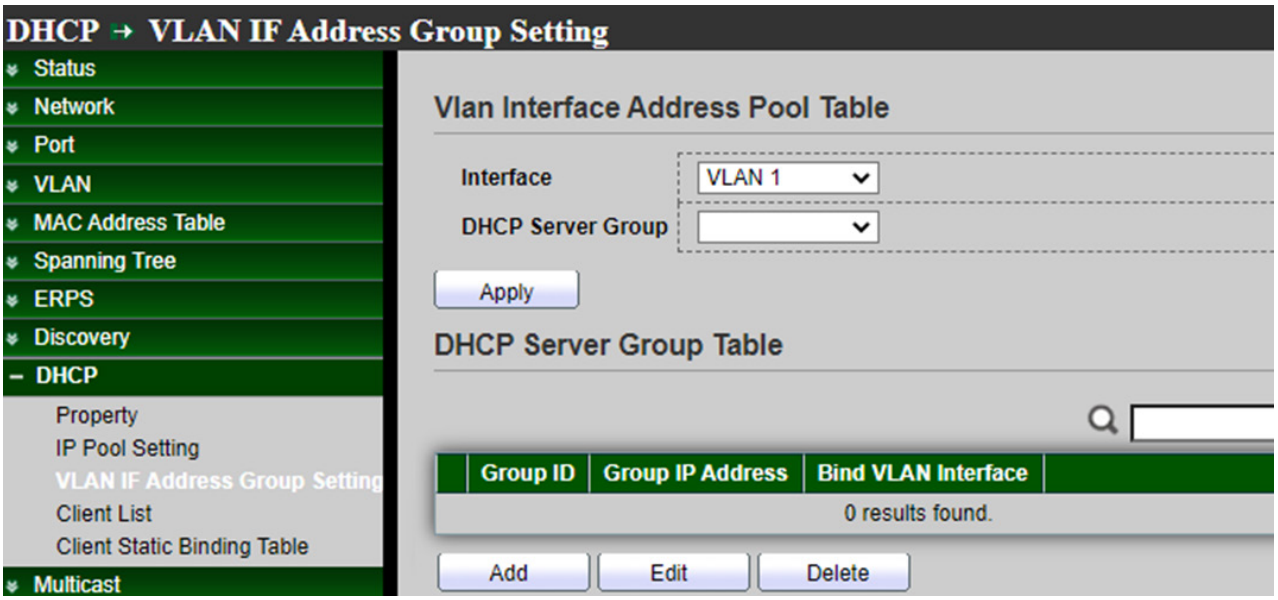
➢ **Option 43 :** 在 IP DHCP 範圍模式下，以 “ASCII” 格式設定 Option 43 字串，以 “HEX” 格式設定 Option 43 字串。

➢ **Lease time :** DHCP 伺服器回收 IP 位址的可控制時間段，選擇設定日/小時/分鐘，來設定時間值。

*點擊"Apply"儲存您的變更，或"Close"關閉設定。.*

## 11.3 VLAN IF Address Group Setting

使用者管理員可以在"VLAN Interface Address Pool Table"中設定選擇"VLAN Interface"和"DHCP server group"的下拉選單。



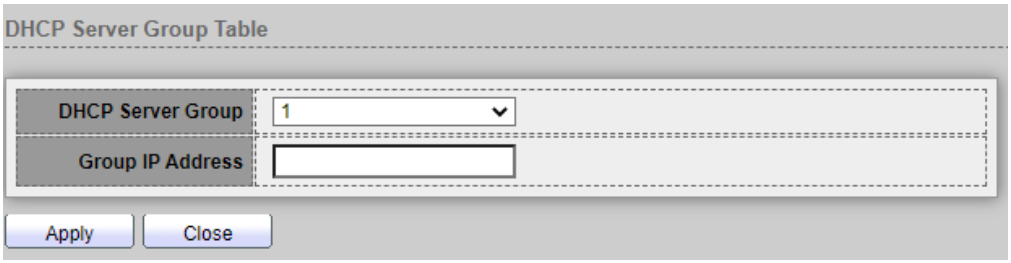

➢ **Interface :** 選擇一個 VLAN 介面。

➢ **DHCP Sever Group :** 選擇一個 DHCP 伺服器群組。

*點擊"Apply"儲存您的變更設定。*

使用者管理員可以設定"DHCP Server Group Table"頁面，設定**"add"**、**"Edit"**和**"Delete"**功能進行管理。

| 欄位 | 描述 |
|---|---|
| Group ID | 顯示 DHCP 伺服器群組 ID |
| Group IP Address | 顯示 DHCP 伺服器群組 IP 位址 |
| Bind VLAN Interface | DHCP 伺服器綁定 VLAN 介面 |

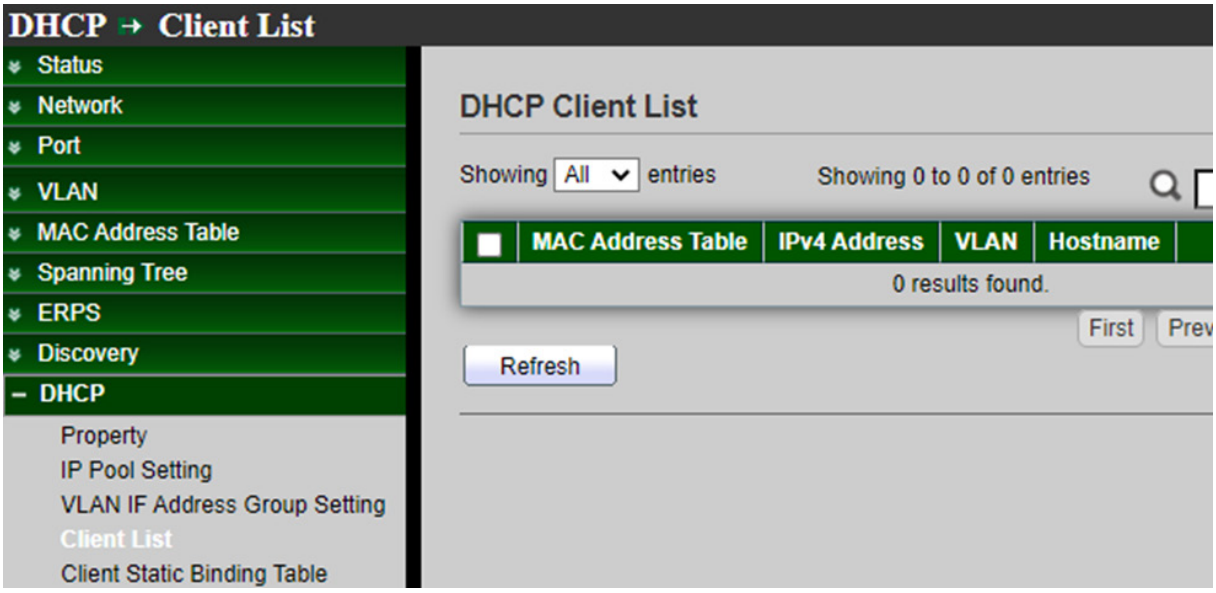



- **DHCP Server Group :** 使用者管理員可以在下拉選單中選擇“DHCP Server Group”，然後確定要設定的分組功能。
- **Group IP Address :** 使用者管理員填寫群組 IP 位址。

*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

## 11.4 用戶端列表(Client List)

該頁面“DHCP Client List”，顯示“MAC Address Table”、“IPv4 Address”、“VLAN”和“Hostname”資訊。

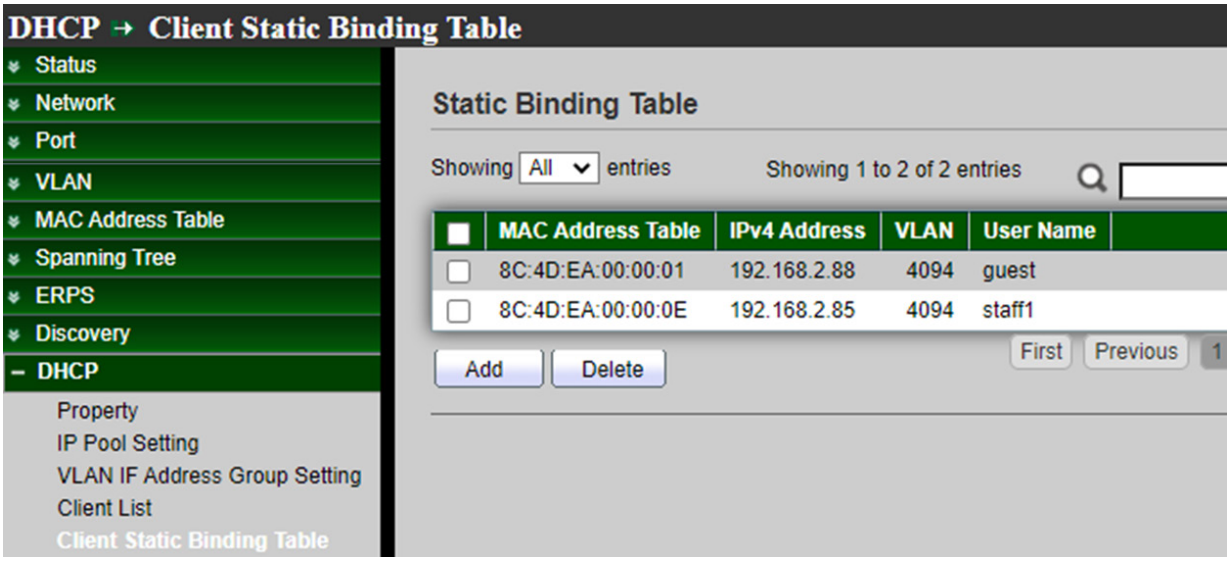


| 欄位 | 描述 |
|---|---|
| MAC Address Table | 顯示用戶端設備的 MAC 位址 |
| IPv4 Address | 顯示發送到用戶端設備的 IP 位址 |
| VLAN | 顯示 DHCP 用戶端的 VLAN ID |
| Hostname | 顯示 DHCP 用戶端的主機名稱 |

*點擊 "Refresh" 重新整理 "Client List" 的統計數據。*

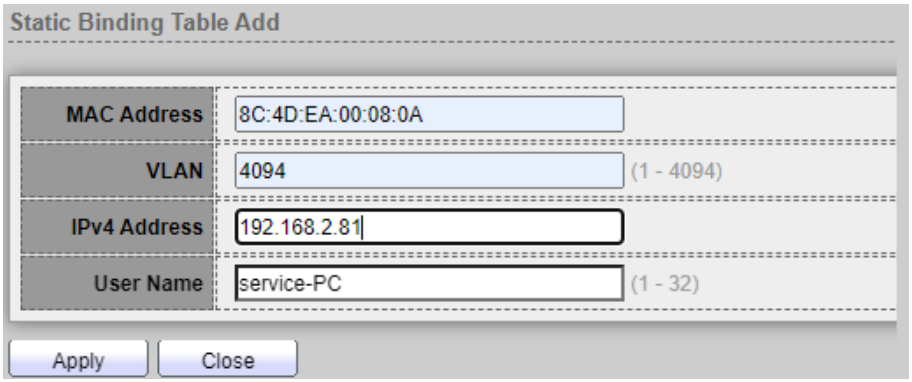
## 11.5 用戶端靜態綁定表(Client Static Binding Table)

使用者管理員可以在 "Static Binding Table" 設定**"add"**、**"Edit"**和**"Delete"**功能進行管理。該頁面 "Static Binding Table" ，顯示 "MAC Address Table"，"IPv4 Address"， "VLAN" 和 "User Name" 資訊。




| 欄位 | 描述 |
|---|---|
| MAC Address Table | 顯示用戶端設備的 MAC 位址 |
| IPv4 Address | 顯示發送到用戶端設備的 IP 位址 |

| | |
|---|---|
| VLAN | 顯示 DHCP 用戶端的 VLAN ID |
| Users Name | 顯示 DHCP 用戶端的使用者名稱 |




- **MAC Address :** 期望綁定的設備的 MAC 位址。
- **VLAN :** 使用者管理員可以設定 DHCP VLAN ID。
- **IPv4 Address :** 分配 IP 位址，給具有綁定 MAC 位址的設備。
- **User Name :** 為該綁定規則生成使用者名稱。

*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

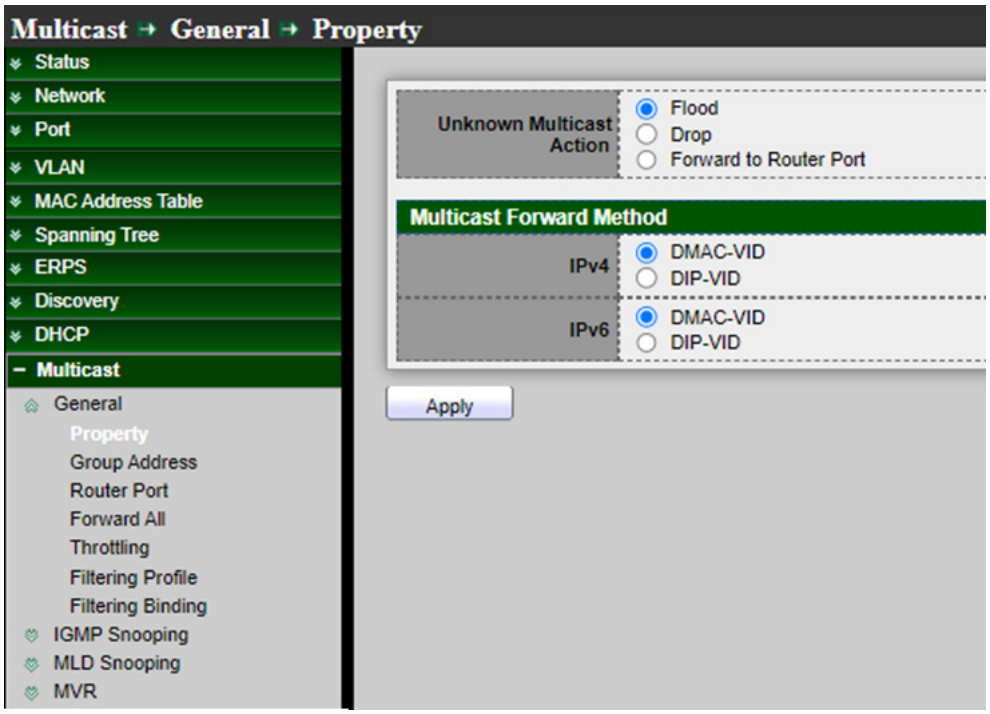
# 12. Multicast

多播是乙太網路閘道(Gateway)支援的唯一 IPV4 多播類型。

## 12.1 通用(General)

### 12.1.1 屬性(Property)

該頁面可以設定未知多播操作，使用者管理員可基於 DMAC 或 DIP 設定轉發方式，該功能可在網路中實現點到多點的高效能資料傳輸，從而降低網路負載。

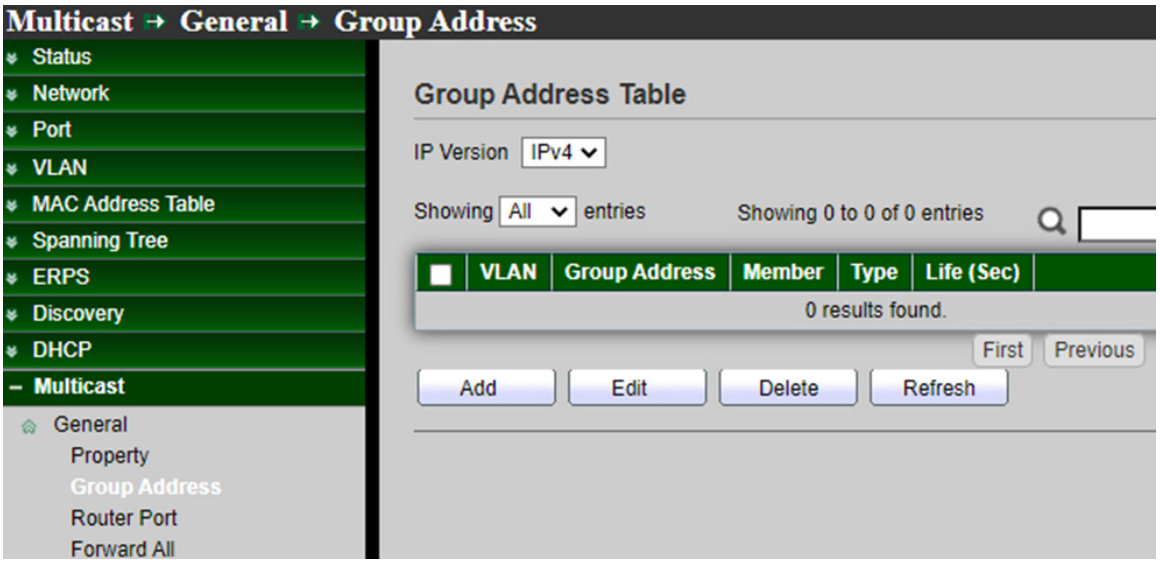



- **Unknown Multicast Action :** 設定未知多播操作。
  - **Drop :** 丟棄未知多播資料。
  - **Flood :** 氾濫未知多播資料。
  - **Router port :** 將未知多播資料轉發到路由器連接埠。
- **Multicast Forward Method :** 分配 IP 位址的子網路遮罩。
- **IPV4 :** 設定 IPv4 多播轉發方式。
  - **MAC-VID :** 轉發方式 dmac+vid。
  - **DIP-VID :** 轉發方式 dip+vid。
- **IPV6 :** 設定 IPv6 多播轉發方式。
  - **MAC-VID :** 轉發方式 dmac+vid。
  - **DIP-VID :** 轉發方式 dip+vid(dip 為 ipv6 低 32 位)。

*點擊"Apply"儲存您的變更設定。.*

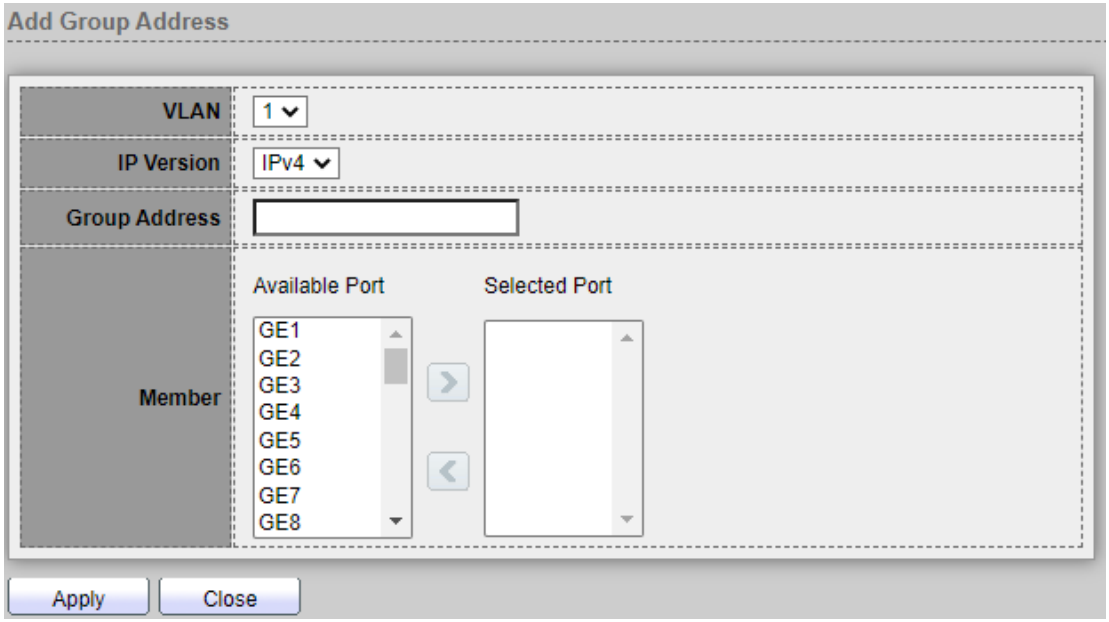
### 12.1.2 群組位址(Group Address)

多播位址範圍為 224.0.0.0 至 239.255.255.255，形成 D 類範圍，該範圍由高位 1110 跟 28 位元多播群組 ID 組成。這些 D 類位址不存在轉租行為。多播群組可以有一個永久分配的位址，也可以是瞬時位址。設定 **“Add”** 、 **“Edit”** 、 **“Delete”** 和 **“Refresh”** 功能進行管理。




- **IP Version :** 選擇 IP 版本。
  - **IPv4 :** ipv4 多播群組。
  - **IPv6 :** ipv6 多播群組。

| 欄位 | 描述 |
|---|---|
| VLAN | 群組VLAN ID |
| Group Address | 群組IP位址 |
| Member | 群組的成員埠 |
| Type | 群組類型：Static或Dynamic |
| Life(Sec) | 動態群組的生存時間 |

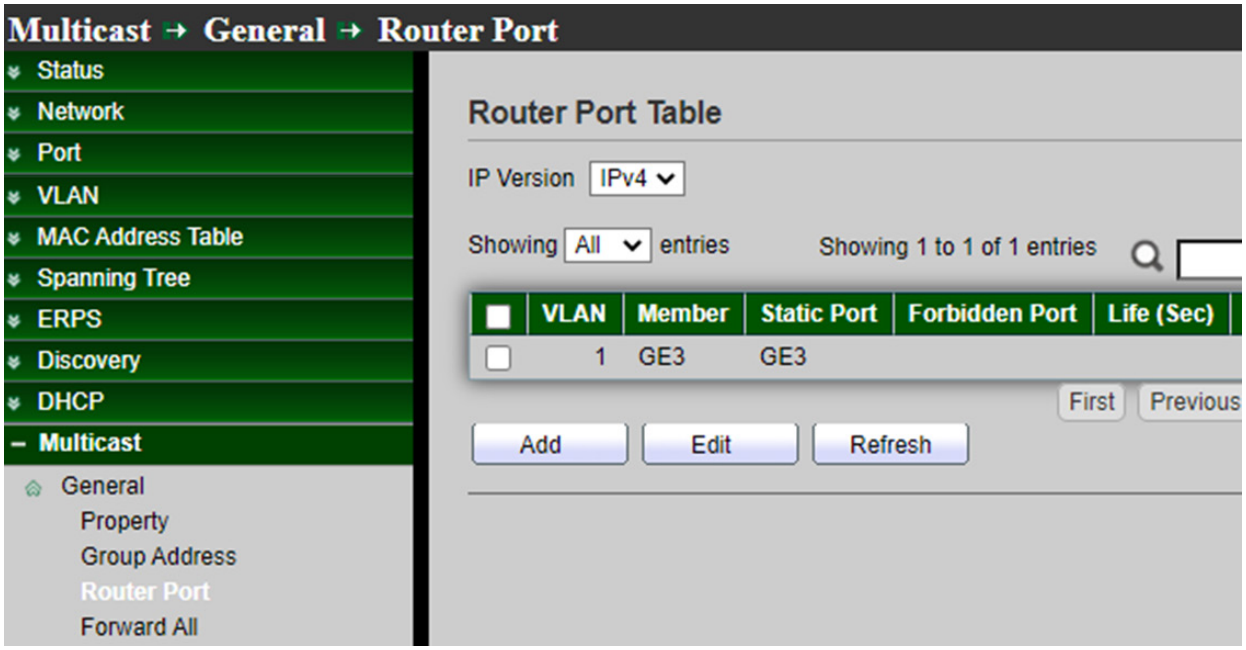



- **VLAN :** 群組 VLAN ID
- **IP Version :**
  - **IPv4 :** ipv4 多播群組。
  - **IPv6 :** ipv6 多播群組。
- **Group Address :** 群組 IP 位址。
- **Member :** 群組的成員埠。
  - **Available Port :** 可選連接埠成員。
  - **Selected Port :** 已選連接埠成員。

*點擊"Apply"儲存您的變更，或"Close"關閉設定。.*

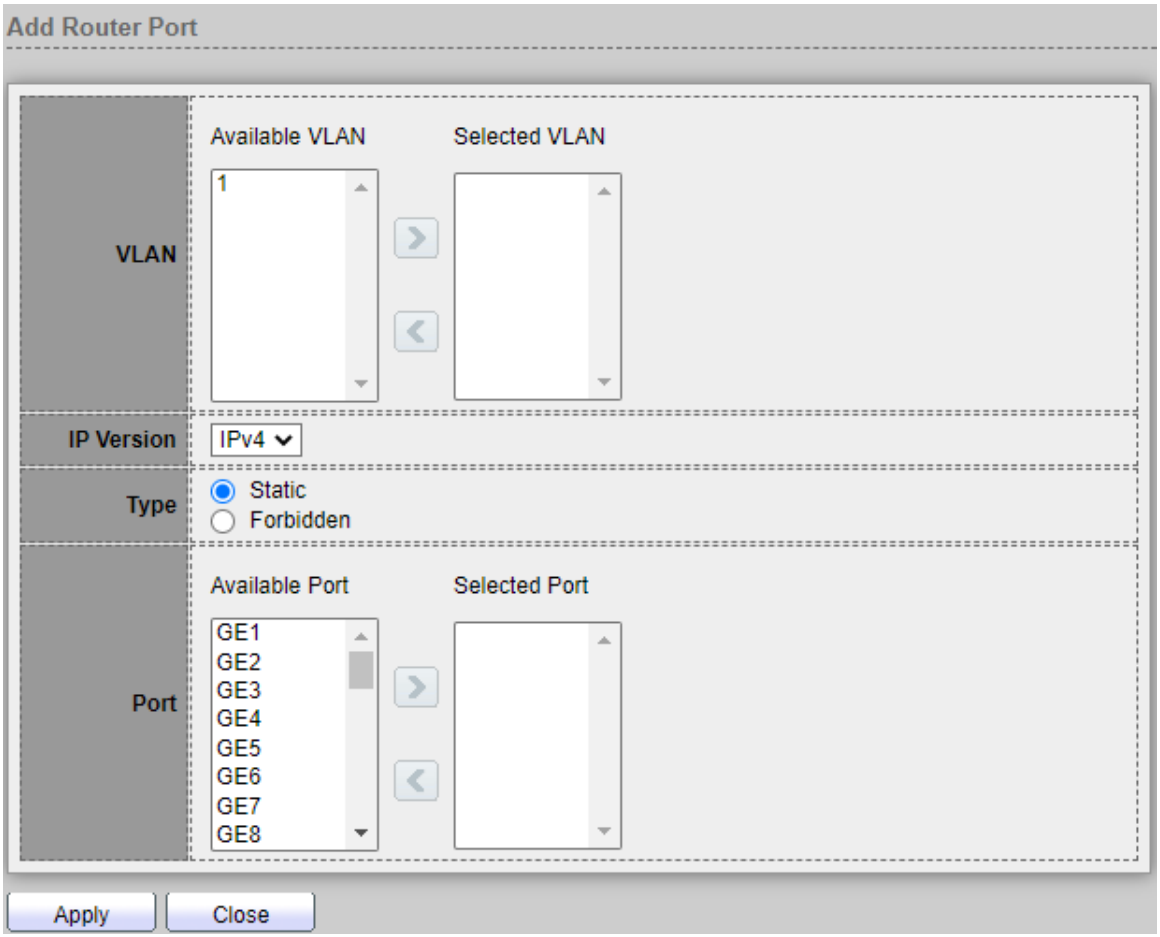
### 12.1.3 路由器連接埠(Router Port)

多播路由器(MRouter)連接埠是連接到多播路由器的連接埠。交換器在轉發多播流和 IGMP / MLD 註冊訊息時會包括 MRouter 連接埠。這是為了讓所有路由器轉發多播流並將註冊訊息傳播到其他子網路，設定 **“add”** 、 **“Edit”** 和 **“Delete”** 功能進行管理。




- **IP Version :** 選擇 IP 版本。
  - **IPv4 :** ipv4 多播路由器。
  - **IPv6 :** ipv6 多播路由器。

| 欄位 | 描述 |
|---|---|
| VLAN | 路由器清單VLAN ID |
| Member | 路由器連接埠成員(包括靜態和學習的連接埠成員) |
| Static Port | 靜態路由器連接埠成員 |
| Forbidden Port | 禁止的路由器連接埠成員 |
| Life(Sec) | 路由器清單的到期時間 |




- **VLAN :** 群組的 VLAN ID。
  - **Available VLAN :** 可選的 VLAN 成員。
  - **Selected VLAN**：已選的 VLAN 成員。
- **IP Version :**
  - **IPv4 :** ipv4 多播路由器。
  - **IPv6 :** ipv6 多播路由器。

**Type :** 路由器連接埠類型：

- **Static :** 靜態路由器連接埠。
- **Forbidden :** 禁止的路由器連接埠，無法學習動態路由器連接埠成員。

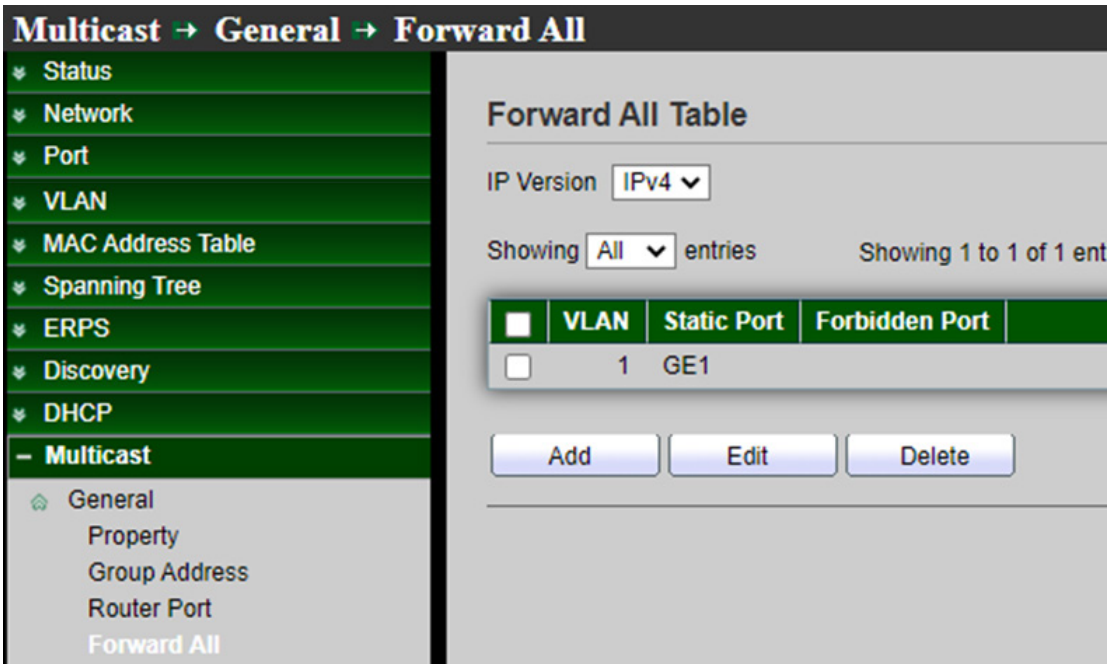
- **Port :** 路由器清單的成員埠。
  - **Available Port :** 可選的路由器連接埠成員。
  - **Selected Port**：已選的路由器連接埠成員。

*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

### 12.1.4 轉發全部(Forward All)

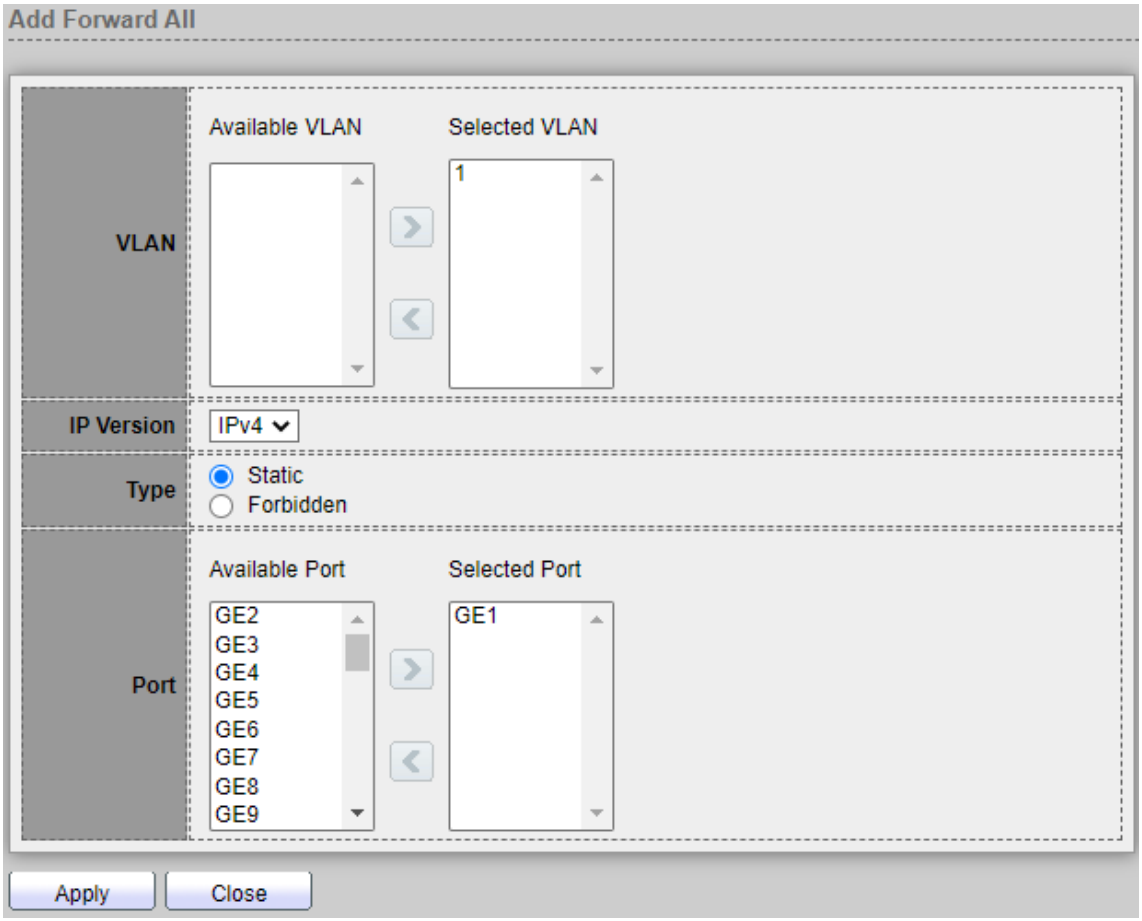
設定連接埠或 LAG 以接收來自特定 VLAN 的多播流。如果連接到該連接埠的設備不支援 IGMP 或 MLD，使用者管理員可以將連接埠靜態設定為 “Forward All” ，並設定**"add"**、**"Edit"**和**"Delete"**功能進行管理。

| Note | 設定只影響所選 VLAN 的成員連接埠。 |
|---|---|




- **IP Version :** 選擇 IP 版本。
  - **IPv4 :** IPv4 多播轉發全部。
  - **IPv6 :** IPv6 多播轉發全部。

| 欄位 | 描述 |
|---|---|
| VLAN | 轉發全部清單的VLAN ID |
| Static Port | 已知的多播群組始終為轉發連接埠成員 |
| Forbidden Port | 已知的多播群組始終不是轉發連接埠成員 |

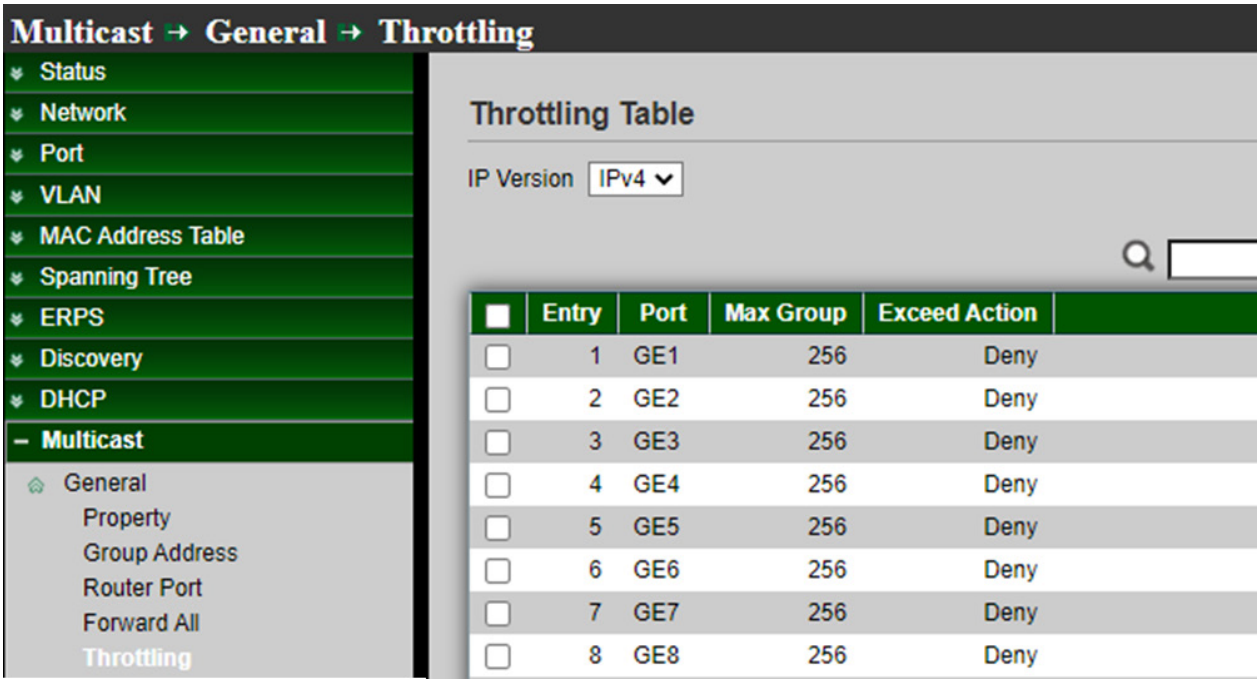



- **VLAN :** 轉發全部清單的 VLAN ID。
  - **Available VLAN :** 可選的 VLAN 成員。
  - **Selected VLAN :** 已選的 VLAN 成員。
- **IP Version :**
  - **IPv4 :** IPv4 多播轉發全部。
  - **IPv6 :** IPv6 多播轉發全部。
- **Type :** 轉發全部連接埠類型。
  - **Static :** 靜態的轉發全部的連接埠。此連接埠靜態設定為多播路由器連接埠。
  - **Forbidden :** 禁止的轉送全部的連接埠。即使此連接埠接收 IGMP 或 MLD 查詢，也不會將此連接埠設定為多播路由器連接埠。
- **Port :** 轉發全部的成員埠。
  - **Available Port :** 可選的路由器連接埠成員。
  - **Selected Port :** 已選的路由器連接埠成員。

*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

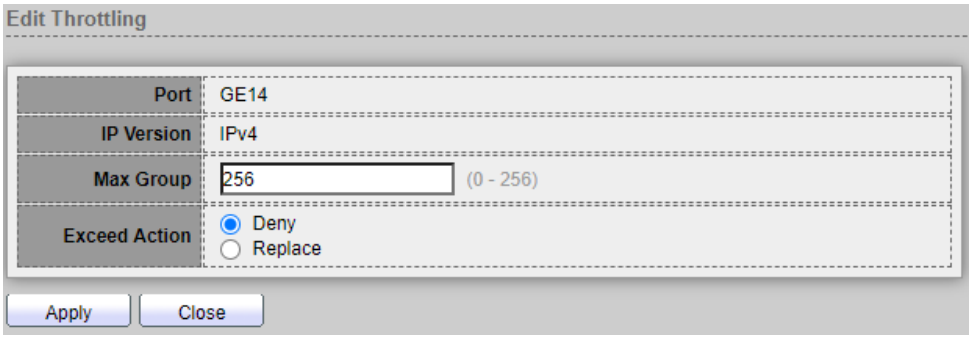
## 12.1.5 節流(Throttling)

該頁面允許使用者設定連接埠可學習的最大群組數，以及到達連接埠最大群組數的操作。




- **IP Version :** 選擇 IP 版本。
  - **IPv4 :** IPv4 用於 IGMP 監聽節流。
  - **IPv6 :** IPv6 用於 MLD 監聽節流。

| 欄位 | 描述 |
|---|---|
| Port | 顯示連接埠編號 |
| Max Group | 顯示連接埠的最大群組數 |
| Exceed Action | 顯示連接埠學習群組超過最大群組數的操作 |

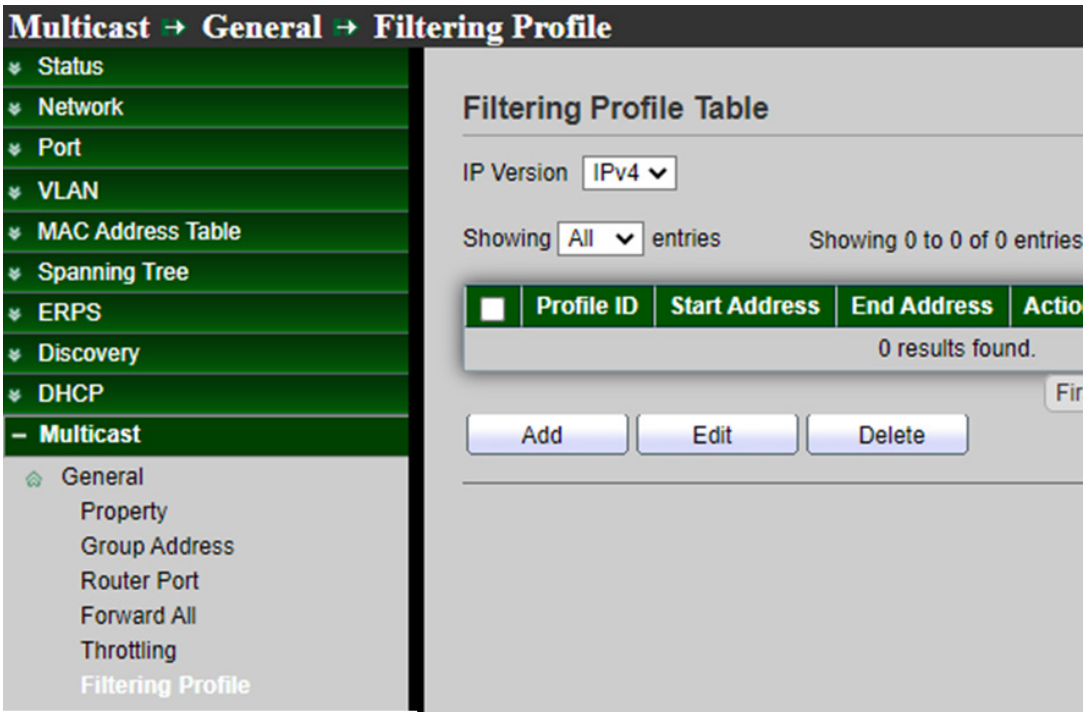


- **Port :** 顯示所選連接埠列表。
- **IP Version :** 顯示所選 IP 版本。
- **Max Group :** 連接埠的最大群組數。
- **Exceed Action :** 連接埠學習群組超過最大群組數的操作。
  - **Deny :** 停止學習群組。
  - **Replace :** 隨機替換一個存在群組。

*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

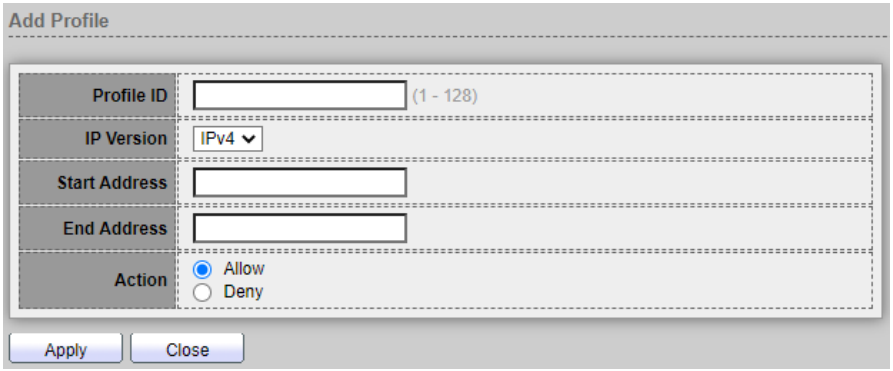
### 12.1.6 過濾設定檔(Filtering Profile)

當加入群組與過濾設定檔 IP 群組範圍相匹配時，過濾設定檔允許或拒絕一系列多播群組的學習，設定"add"、"Edit"和"Delete"功能進行管理。




- **IPV4 Version :** 選擇 IP 版本。
  - **IPv4 :** IPv4 用於 IGMP 監聽設定檔。
  - **IPv6 :** IPv6 用於 MLD 監聽設定檔。

| 欄位 | 描述 |
|---|---|
| Profile ID | 顯示設定檔 ID |
| Start Address | 設定檔起始群組位址 |
| End Address | 設定檔最終群組位址 |
| Action | 顯示設定檔操作 |

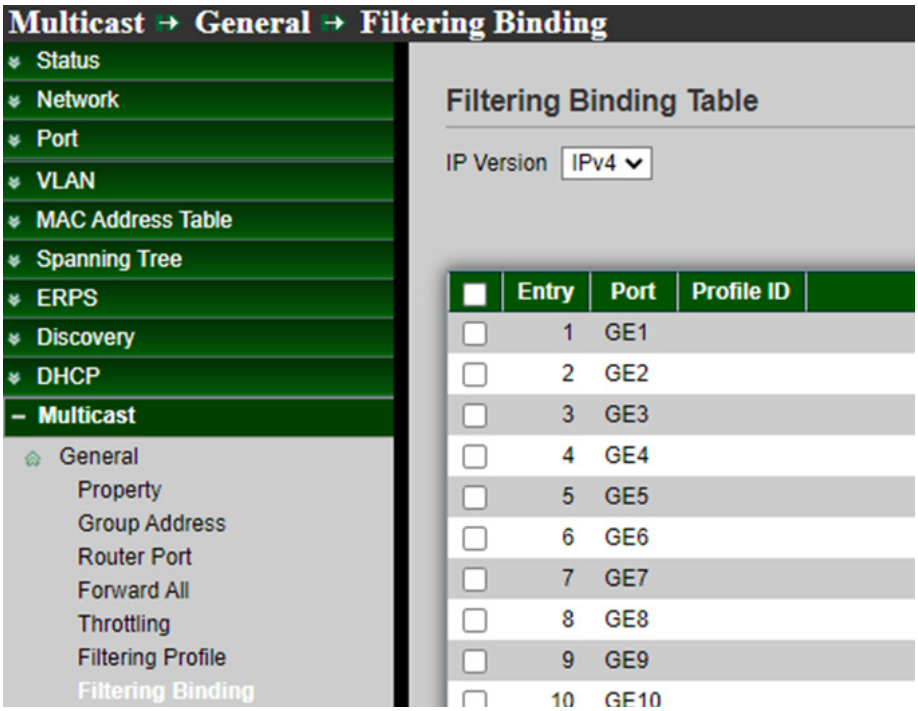



- **Profile ID : 設定檔 ID**。
- **IP Version :** 顯示所選 IP 版本。
  - **IPv4 :** IGMP 監聽設定檔。
  - **IPv6 :** MLD 監聽設定檔。
- **Start Address :** 設定檔起始群組位址
- **End Address :** 設定檔最終群組位址
- **Action :** 設定檔的操作：
  - **Allow :** 允許所有匹配設定檔的封包。
  - **Deny :** 拒絕所有匹配設定檔的封包。

*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

### 12.1.7 過濾綁定(Filtering Binding)

完成過濾設定檔設定後，使用者管理員可以選擇連接埠來設定過濾綁定。




- **IPV4 Version :** 選擇 IP 版本。
  - **IPv4 :** IPv4 用於 IGMP 監聽節流。
  - **IPv6 :** IPv6 用於 MLD 監聽節流。

| 欄位 | 描述 |
|---|---|
| Entry | 編號清單 |
| Port | 連接埠編號 |
| Profile ID | 連接埠綁定設定檔 ID |


- **Port :** 所選的連接埠列表。
- **IP Version :** 顯示所選連接埠過濾的 IP 版本。
- **Profile ID :** 如果選中 “Enable”,可以選擇或變更設定檔 ID,否則將刪除連接埠過濾設定檔綁定。

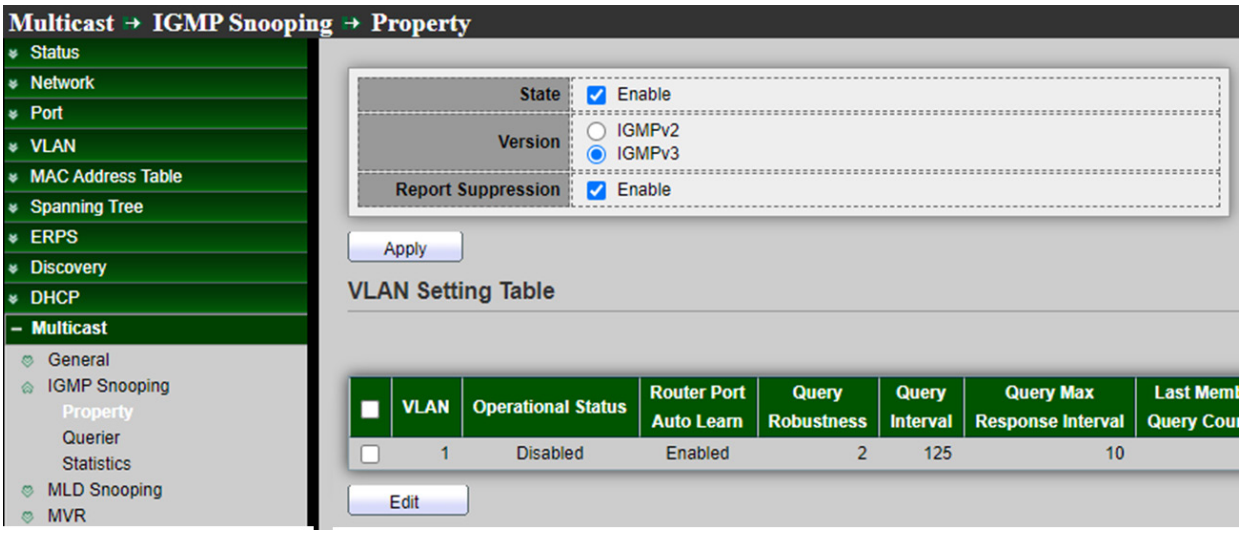
*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

## 12.2 IGMP 監聽(IGMP Snooping)

IGMP 監聽是監看網際網路組管理協定(IGMP)網路流量的過程。該功能允許網路交換器監看主機和路由器之間的 IGMP 對話。透過監看這些對話，交換器可以維護映射，顯示哪些鏈接需要哪些 IP 多播流量。可以過濾掉不需要多播的鏈路，從而控制哪些連接埠接收特定多播流量。IGMP 監聽支援 v2 和 v3，使用者管理者可以轉送或丟棄未知多播流量。

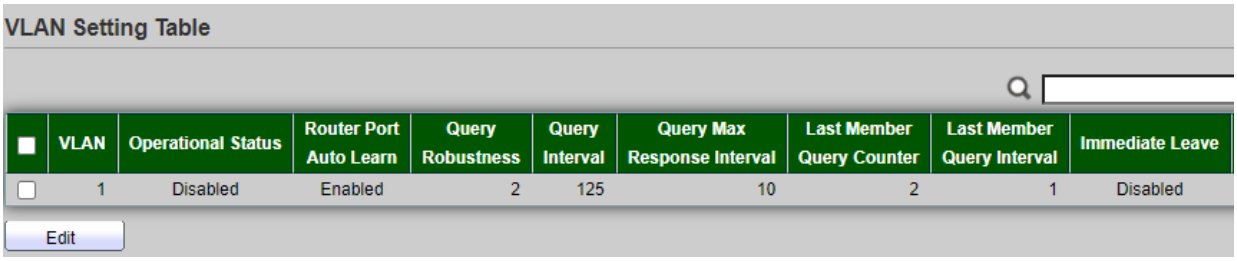
### 12.2.1 屬性(Property)

在全域或 VLAN 上啟用 IGMP 監聽時，所有 IGMP 封包都會轉送到 CPU。CPU 分析所選取的連接埠是否要求加入 VLAN 上的多播群組或產生 IGMP 查詢的路由器，或接收 PIM/OSFP/DVMRP/IGMP 查詢協定傳入的封包。

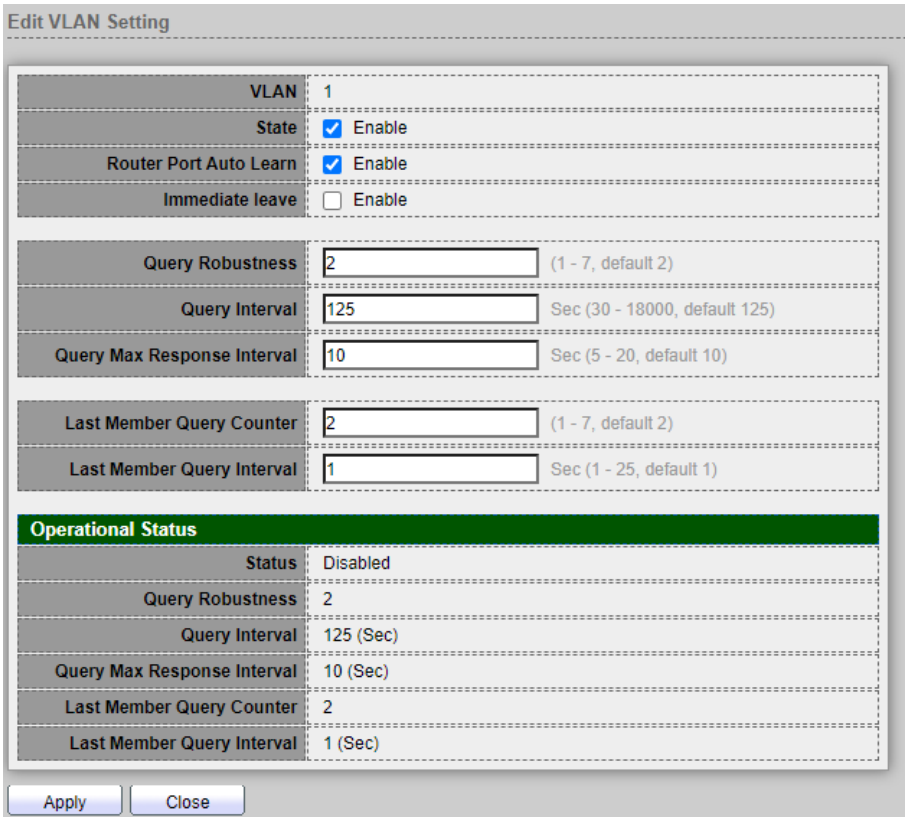



- **State :** 使用者管理員可以選擇或取消 Enable，來設定 IGMP Snooping 功能的啟用狀態。
  - **Enable :** 如果選中則啟用 IGMP 監聽，否則為停用 IGMP 監聽。
- **Version :** 選擇 IGMPv2 或 IGMPv3，設定 IGMP 監聽版本。
  - **IGMPv2 :** 僅支援處理 IGMP v2 封包。
  - **IGMPv3 :** 支援 v3 版本和 v2。
- **Report Suppression :** 啟用或停用 IGMP 報告抑制。如果使用者管理員選擇停用此功能，IGMP 會將所有報告轉送到多播路由器，設定 IGMP v2 報告抑制的啟用狀態。
  - **Enable :** 如果選中則啟用 IGMP 監聽 v2 報告抑制，否則停用報告抑制功能。

*點擊"Apply"儲存您的變更設定。*




| 欄位 | 描述 |
|---|---|
| VLAN | IGMP清單的VLAN ID |
| Operation Status | IGMP監聽VLAN功能的啟用狀態 |
| Router Port Auto Learn | IGMP監聽路由器連接埠自動學習的啟用狀態 |
| Query Robustness | 查詢穩健性允許調整子網路的預期封包遺失 |
| Query Interval | 查詢器發送通用查詢的時間間隔 |
| Query Max Response Interval | 在成員關係查詢訊息中，指定以1/10秒為單位發送回應報告前的最大允許時間 |
| Last Member Query count | Querier-交換器收到群組的離開群組訊息時發送特定群組查詢的計數 |
| Last Member Query Interval | Querier-交換器收到群組的離開群組訊息時發送特定群組查詢的時間間隔 |
| Immediate leave | 在立即離開狀態下，當連接埠接收IGMP離開訊息時，立即從轉發清單刪除該連接埠 |



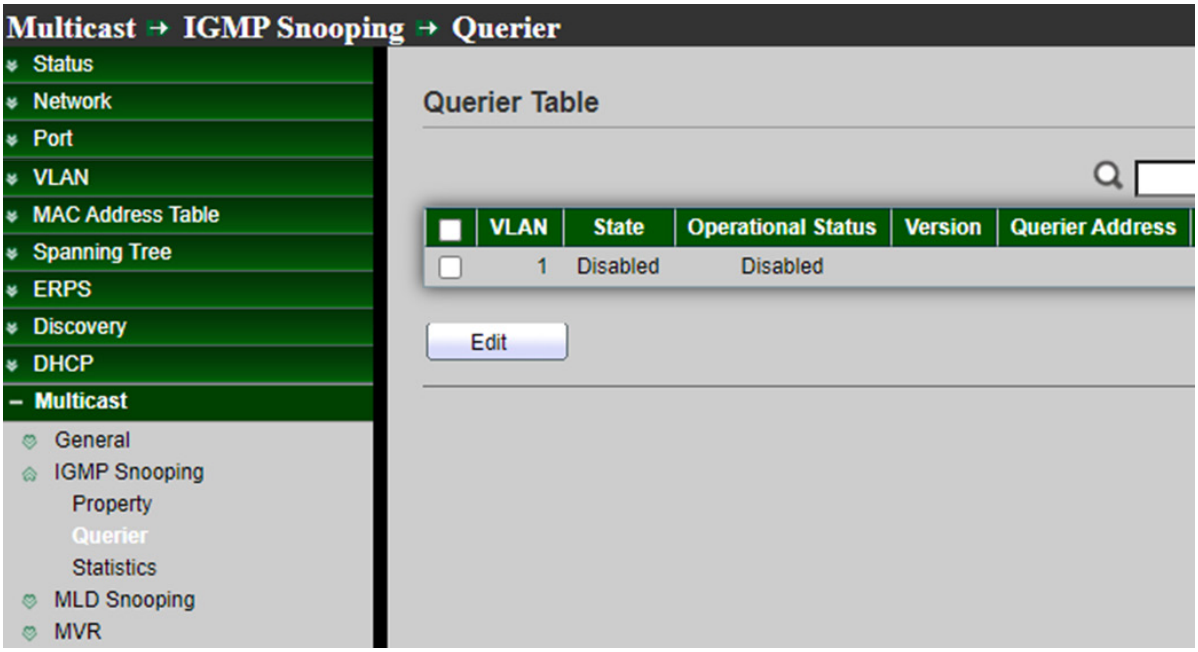

- **VLAN :** IGMP 監聽的 VLAN ID。
- **State :** 設定 IGMP 監聽 VLAN 功能的啟用狀態。
  - **Enable :** 如果選中則啟用 IGMP 監聽 VLAN，否則將停用 IGMP 監聽 VLAN。
- **Router Port Auto Learn :** 設定 IGMP 監聽路由器連接埠自動學習的啟用狀態。
  - **Enable :** 如果選中則啟用通過查詢、PIM 和 DVRMP 學習路由器連接埠，否則將停用學習路由器連接埠。
- **Immediate leave :** 當連接埠接收 IGMP 離開訊息時，立即從轉發清單刪除該連接埠。
  - **Enable :** 如果選中則啟用立即離開，否則停用立即離開。
- **Query Robustness :** 管理查詢穩健性允許對子網路的預期封包遺失進行調整。
- **Query Interval :** 管理查詢器發送通用查詢的時間間隔。
- **Query Max Response Interval :** 管理查詢最大回應間隔，在成員關係查詢訊息中，指定以 1/10 秒為單位發送回應報告前的最大允許時間。
- **Last Member Query Counter :** 管理 Querier-交換器收到群組的離開群組訊息時發送特定群組查詢的最後成員查詢計數。
- **Last Member Query Interval :** 管理 Querier-交換器收到群組的離開群組訊息時發送特定群組查詢的最後成員查詢時間間隔。
- **Opertional Status :** 設定 IGMP 監聽路由器連接埠學習的啟用狀態。

- **Status :** 運行 IGMP 監聽狀態，必須同時啟用 IGMP 監聽全域和 IGMP 監聽，狀態才會是 Enable。
- **Query Robustness :** 運行查詢穩健性。
- **Query Interval :** 運行查詢時間間隔。
- **Query Max Response Interval :** 運行查詢最大回應時間間隔。
- **Last Member Query Counter :** 運行最後成員查詢計數。
- **Last Member Query Interval :** 運行最後成員查詢時間間隔。

*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

### 12.2.2 查詢器(Querier)

使用者管理員可以選擇創建的VLAN來啟用或禁用IGMP監聽查詢功能。當選擇複選框並點擊"**Edit**"，將轉到設定 IGMP 監聽版本，此功能可以讓 IGMP 監聽查詢設備定期向本地網段的所有主機和路由器發送 IGMP 監聽通用查詢封包，來查詢網段中的多播群組成員。




| 欄位 | 描述 |
|---|---|
| VLAN | IGMP監聽查詢器清單的VLAN ID |
| State | IGMP監聽查詢器管理狀態 |

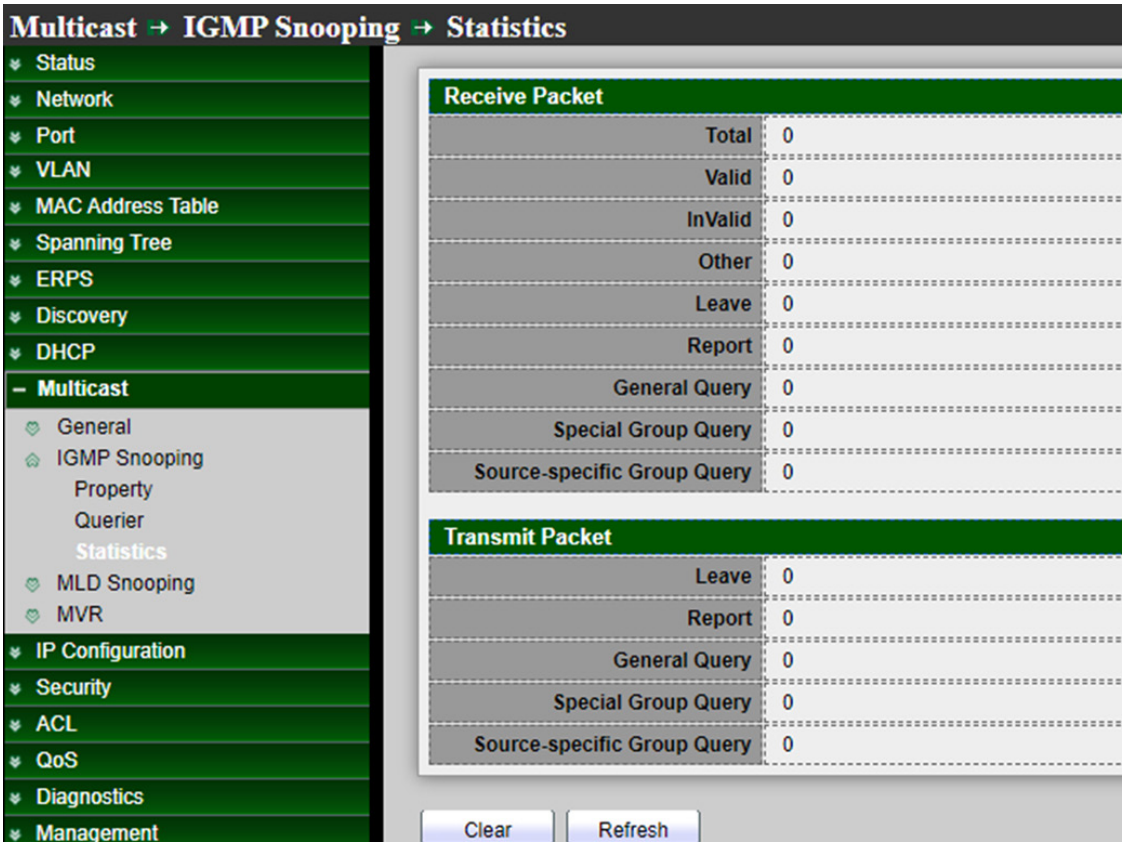
| | |
|---|---|
| Operational Status | IGMP監聽查詢器運行狀態 |
| Querier Version | IGMP監聽查詢器運行版本 |
| Querier IP | VLAN上運行的查詢器IP位址 |


- **VLAN :** 所選要編輯的 IGMP 監聽查詢器 VLAN 列表。
- **State :** 設定所選 VLAN 上 IGMP 查詢器的啟用狀態。
  - **Enabled :** 如果選中則啟用 IGMP 查詢器，否則禁用 IGMP 查詢器。
- **Version :** 設定所選 VLAN 上 IGMP 查詢器的查詢版本。
  - **IGMPv2 :** 查詢器版本 v2。
  - **IGMPv3 :** 查詢器版本 v3 (IGMP 監聽版本應為 IGMPv3)。

*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

### 12.2.3 統計數據(Statistics)

如果使用者管理員啟用 IGMP 監聽，頁面會顯示 IGMP 監聽的 Receive Packet/Transmit Packet 資訊。




| 欄位 | 描述 |
|---|---|
| Receive Packet | • **Total :** 接收 IGMP 封包總數，包括發送到 CPU 的 ipv4 多播數據<br>• **Valid :** 有效 IGMP 監聽進程封包<br>• **InValid :** 無效 IGMP 監聽進程封包<br>• **Other :** ICMP 封包類型不是 2，也不是 ipv4 多播數據封包<br>• **Leave :** IGMP 離開封包<br>• **Report :** IGMP 加入和報告封包<br>• **General Query :** IGMP 通用查詢封包<br>• **Special Group Query :** IGMP 特定群組通用查詢封包<br>• **Source-specific Group Query :** IGMP 特定來源和群組通用查詢封包 |
| Transmit Packet | • **Leave :** IGMP 離開封包<br>• **Report :** IGMP 加入和報告封包<br>• **General Query :** IGMP 通用查詢封包，包括查詢器傳送通 |

用查詢封包

- **Special Group Query :** IGMP 特定群組查詢封包，包括查詢器傳送特殊群組查詢封包
- **Source-specific Group Query :** IGMP 特定來源和群組通用查詢封包

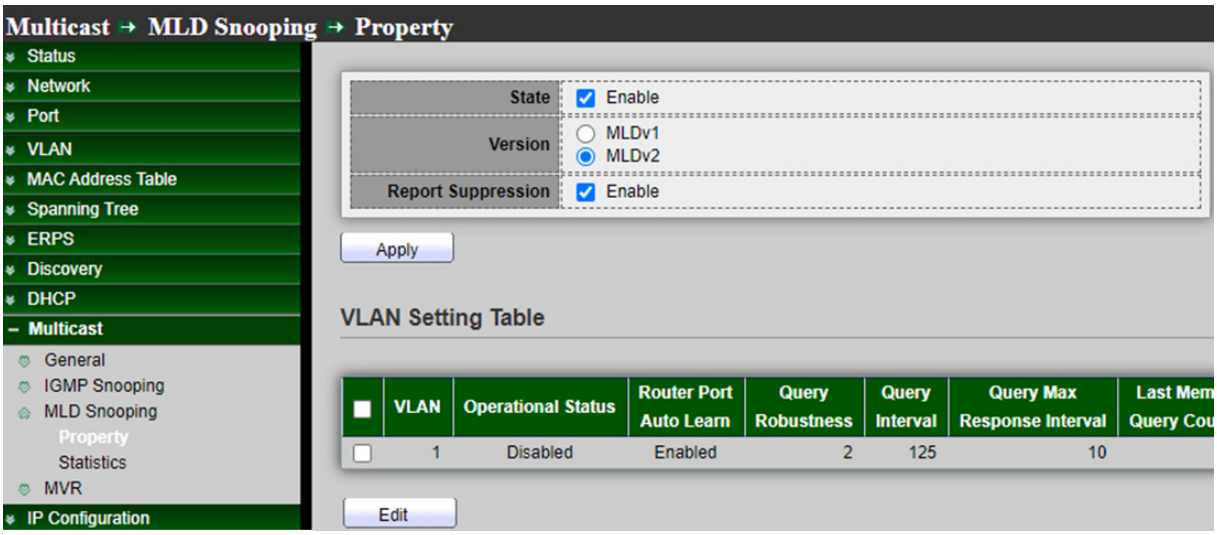
*點擊"Clear"清除該頁面，或"Refresh"重新整理頁面。*

## 12.3 MLD 監聽(MLD Snooping)

此功能支援選擇性多播轉發(IPv6)，MLD(Multicast Listener Discovery，多播監聽程式發現) Snooping 啟用必須在全域和每個相關 VLAN 中。此交換器支援靜態和動態 VLAN 上的 MLD 監聽。主機使用 MLD 協議報告其參與多播會話的情況，交換器使用 MLD 監聽來創建多播成員清單。使用這些清單，將多播封包只轉發到屬於多播群組成員主機節點的交換器連接埠。交換器不支援 MLD 查詢器。

### 12.3.1 屬性(Property)

使用者管理員啟用 MLD 監聽時並沒有手動設定多播群組，會導致源於手動設定和 MLD 監聽動態發現的多播群組和連接埠成員資格的聯合。但是，當交換器重新啟動時，僅保留靜態設定。




➢ **State :** 使用者管理員可以選擇啟用或取消啟用，來設定 MLD 監聽功能的啟用狀態。

- **Enable :** 如果選中則啟用 MLD 監聽，否則禁用 MLD 監聽。

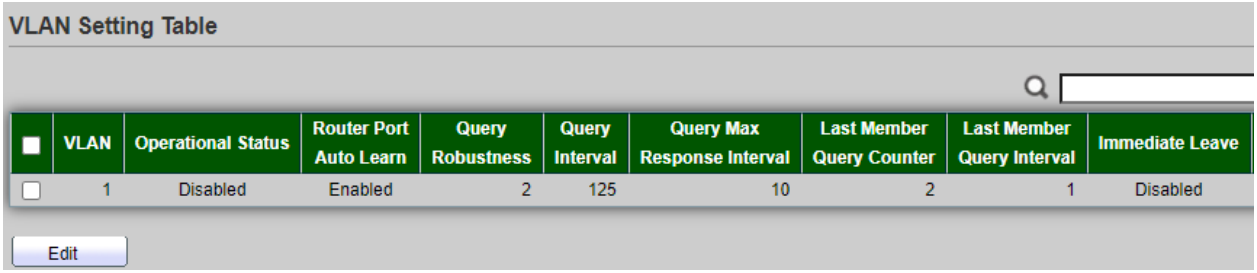
➢ **Version :** 選擇 MLDv1 或 MLDv2，設定 MLD 監聽版本。

- **MLDv1 :** 僅支援處理 MLDv1 封包。
- **MLDv2 :** 支援 v2 版本和 v1。

➢ **Report Suppression :** 設定 MLDv1 報告抑制的啟用狀態。

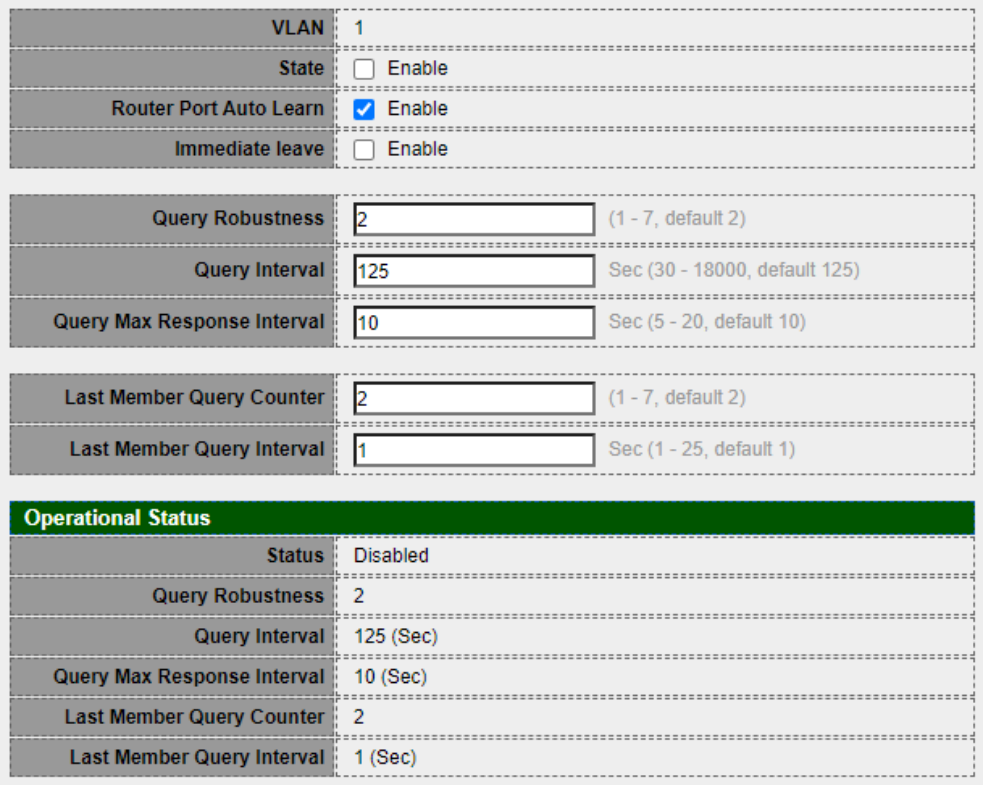
- **Enable :** 如果選中則啟用 MLD 監聽 v1 報告抑制，否則禁用報告抑制功能。

*點擊"Apply"儲存您的變更設定。*




| 欄位 | 描述 |
|---|---|
| VLAN | MLD清單的VLAN ID |
| Operation Status | MLD監聽VLAN功能的啟用狀態 |
| Router Port Auto Learn | MLD監聽路由器連接埠自動學習的啟用狀態 |
| Query Robustness | 查詢穩健性允許調整子網路的預期封包遺失 |
| Query Interval | 查詢器發送通用查詢的時間間隔 |
| Query Max Response Interval | 在成員關係查詢訊息中，指定以1/10秒為單位發送回應報告前的最大允許時間 |
| Query Max Response Interval | Querier-交換器收到群組的離開群組訊息時發送特定群組查詢的計數 |
| Last Member Query Interval | Querier-交換器收到群組的離開群組訊息時發送特定群組查詢的時間間隔 |
| Immediate leave | 在立即離開狀態下，當連接埠接收MLD離開訊息時，立即從轉發清單刪除該連接埠 |

使用者管理員可以在復選框中選擇 VLAN，並點擊 “Edit” 設定 MLD 監聽。

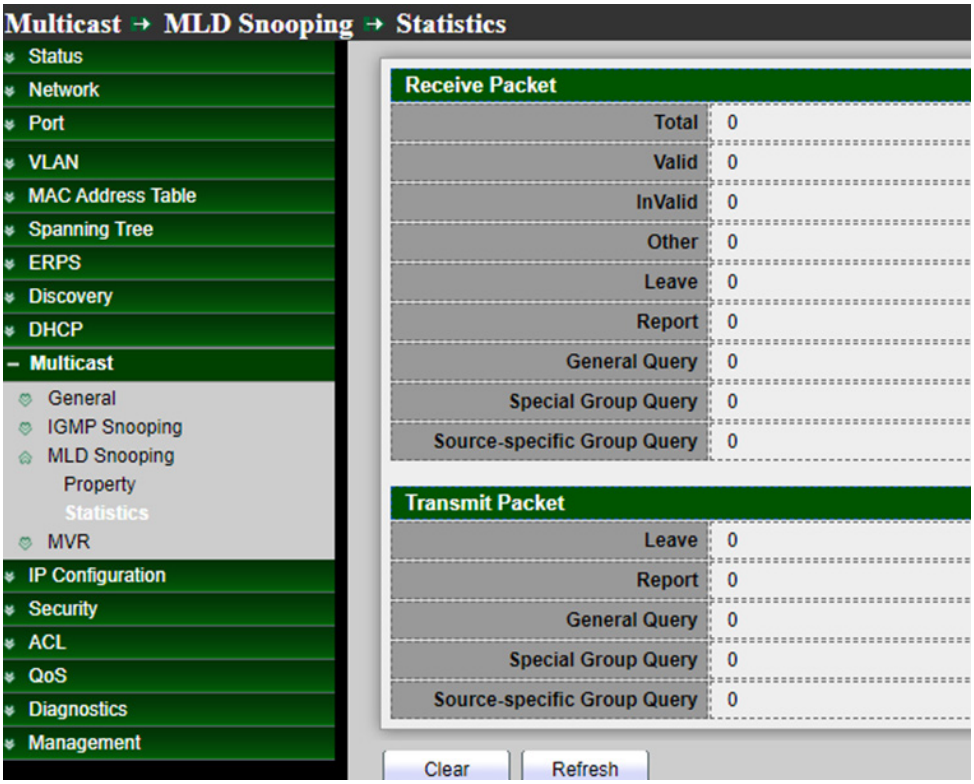



- **VLAN :** MLD 監聽的 VLAN ID。
- **State :** 設定 MLD 監聽 VLAN 功能的啟用狀態。
  - **Enable :** 如果選中則啟用 MLD 監聽 VLAN，否則禁用 MLD 監聽 VLAN。
- **Router Port Auto Learn :** 設定 MLD 監聽路由器連接埠自動學習的啟用狀態
  - **Enable :** 如果選中則啟用通過查詢、PIM 和 DVRMP 學習路由器連接埠，否則將停用學習路由器連接埠。
- **Immediate leave :** 當連接埠接收 MLD 離開訊息時，立即從轉發清單刪除該連接埠。
  - **Enable :** 如果選中則啟用立即離開，否則停用立即離開。
- **Query Robustness :** 管理查詢穩健性允許對子網路的預期封包遺失進行調整。
- **Query Interval :** 管理查詢器發送通用查詢的時間間隔。
- **Query Max Response Interval :** 管理查詢最大回應間隔，在成員關係查詢訊息中，指定以 1/10 秒為單位發送回應報告前的最大允許時間。
- **Last Member Query Counter :** 管理 Querier-交換器收到群組的離開群組訊息時發送特定群組查詢的最後成員查詢計數。
- **Last Member Query Interval :** 管理 Querier-交換器收到群組的離開群組訊息時發送特定群組查詢的最後成員查詢時間間隔。
- **Operational Status :** 設定 MLD 監聽路由連接埠學習的啟用狀態。

- **Status :** 運行 MLD 監聽狀態，必須同時啟用 IGMP 監聽全域和 IGMP 監聽，狀態才會是 Enable。
- **Query Robustness :** 運行查詢穩健性。
- **Query Interval :** 運行查詢時間間隔。
- **Query Max Response Interval :** 運行查詢最大回應時間間隔。
- **Last Member Query Counter :** 運行最後成員查詢計數。
- **Last Member Query Interval :** 運行最後成員查詢時間間隔。

### 12.3.2 統計數據(Statistics)

如果使用者管理員啟用 MLD 監聽，頁面會顯示 MLD 監聽的 Receive Packet/Transmit Packet 資訊。




| 欄位 | 描述 |
|---|---|
| Receive Packet | • **Total :** 接收 MLD 封包總數，包括發送到 CPU 的 ipv4 多播數據<br>• **Valid :** 有效 MLD 監聽進程封包<br>• **InValid :** 無效 MLD 監聽進程封包 |

| | |
|---|---|
| | ● **Other :** ICMP 封包類型不是 MLD，也不是 ipv6 多播數據封包，也不是 ipv6 路由器協定<br>● **Leave :** MLD 離開封包<br>● **Report :** MLD 加入和報告封包<br>● **General Query :** MLD 通用查詢封包<br>● **Special Group Query :** MLD 特定群組通用查詢封包<br>● **Source-specific Group Query :** MLD 特定來源和群組通用查詢封包 |
| **Transmit Packet** | ● **Leave :** MLD 離開封包<br>● **Report :** MLD 加入和報告封包<br>● **General Query :** MLD 通用查詢封包<br>● **Special Group Query :** MLD 特定群組通用查詢封包<br>● **Source-specific Group Query :** MLD 特定來源和群組通用查詢封包 |

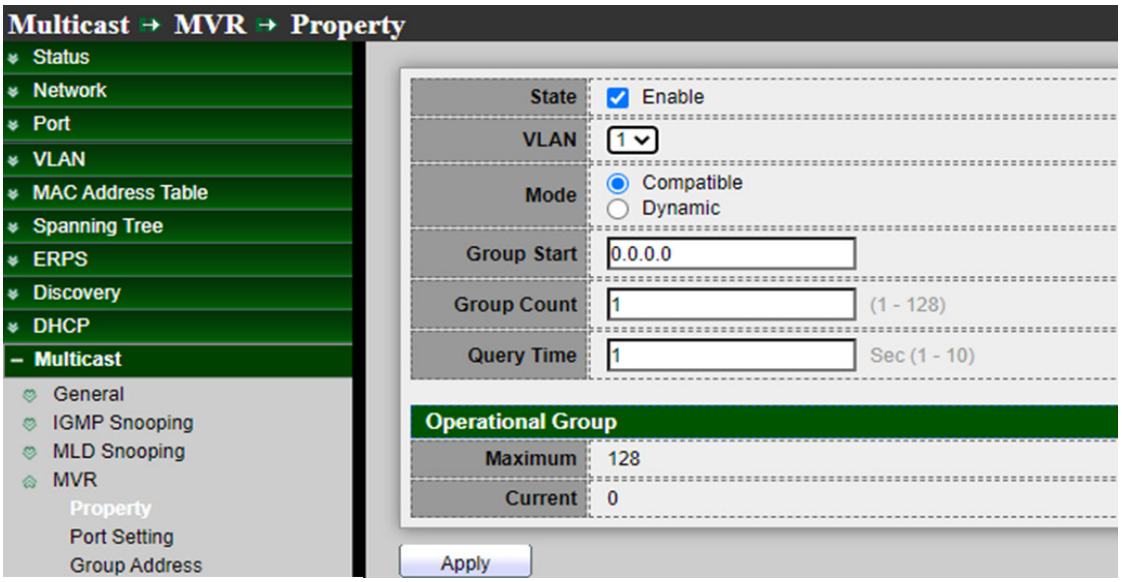
*點擊"**Clear**"清除該頁面，或"**Refresh**"重新整理頁面。*

## 12.4 多播 VLAN 註冊(MVR)

MVR(多播 VLAN 註冊)專為在基於乙太網路環的服務供應商網路上大規模部署多播放流量的應用而設計(例如，在服務供應商網路上廣播多個串流電視頻道)。MVR 允許連接埠上的使用者訂閱和取消訂閱全網多播 VLAN 上的多播流。

它允許在網路中共用單一多播 VLAN，而使用者則保留在單獨的 VLAN 中。MVR 提供了在多播 VLAN 中持續發送多播流的能力，但出於頻寬和安全原因將流量與使用者 VLAN 隔離。

### 12.4.1 屬性(Property)

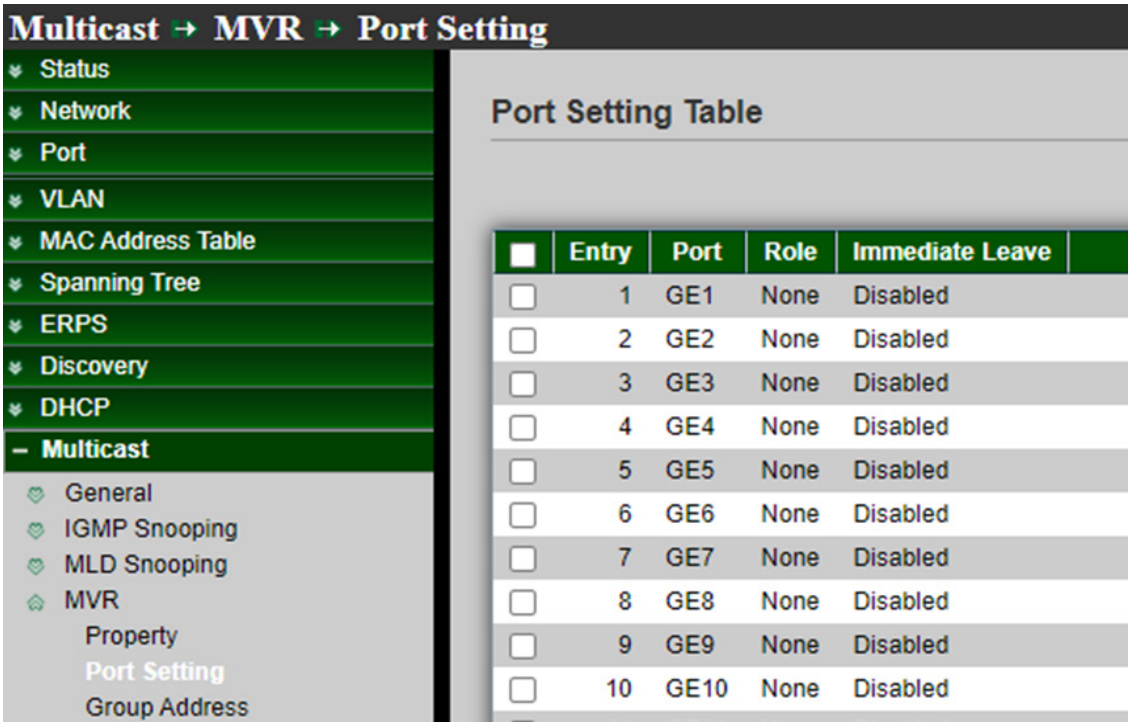



- **State :** 使用者管理員可以選擇啟用或取消啟用，來設定 MVR 功能的啟用狀態。
  - **Enable :** 如果選中則 MVR 為啟用狀態，否則 MVR 為禁用狀態。
- **VLAN :** 選擇 MVR 的 VLAN ID。
- **Mode :** 設定 MVR 模式。
  - **Compatible :** 相容模式。
  - **Dynamic :** 動態模式，將學習來源連接埠上的群組成員。
- **Group Start :** 使用者管理員可以設定 MVR 群組範圍起始點，範圍為 224.0.0.0 至 239.255.255.255。
- **Group Count :** MVR 群組持續計數，使用計數參數設定連續一系列的 MVR 群組位址(計數範圍為 1 至 128;預設值為 1)。
- **Query Time :** MVR 查詢時間為接收到 MVR 離開 MVR 群組封包時，使用者管理員可以決定從多播群組成員資格移除連接埠前，接收連接埠等待 IGMP 報告成員資格的最長時間。該值以秒為單位。範圍為 1 至 10，預設值為 1 秒。
- **Operational Group :**
  - **Maximum :** MVR 群組資料庫的最大數量。
  - **Current :** 當前已學習的 MVR 群組數。

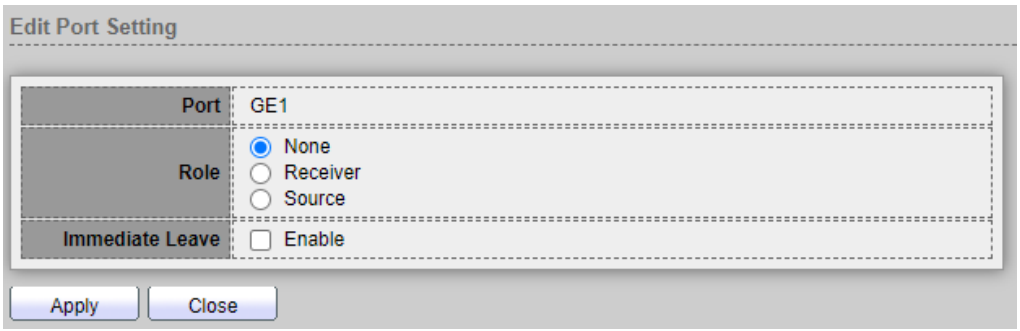
*點擊"Apply"儲存您的變更設定。*

## 12.4.2 連接埠設定(Port Setting)

使用者管理員可以選擇連接埠來設定 MVR 的角色和立即離開。




| 欄位 | 描述 |
|---|---|
| Port | 連接埠編號 |
| Role | MVR的連接埠角色，類型有None(無)/Receiver(接受埠)/Source(來源埠) |
| Immediate Leave | 立即離開的狀態 |




- **Port :** 顯示選擇的連接埠列表。
- **Role :** MVR 連接埠角色。

- **None :** 連接埠角色為無。
- **Receiver :** 如果連接埠是使用者連接埠並且只能接收多播數據，則設定連接埠為接收者連接埠。除非通過靜態或使用 IGMP 離開和加入訊息成為多播群組的成員，否則不會接收數據。接收連接埠不能屬於組播 VLAN。
- **Source :** 將接收和發送多播數據的上行連接埠設定為來源埠。使用者不能直接連接來源埠。交換器上的所有來源埠同屬一個多播 VLAN。

| Note | 如果使用者管理員設定具有 MVR 特性的非 MVR 連接埠，則操作會失敗。預設設定為非 MVR 連接埠。 |
|---|---|

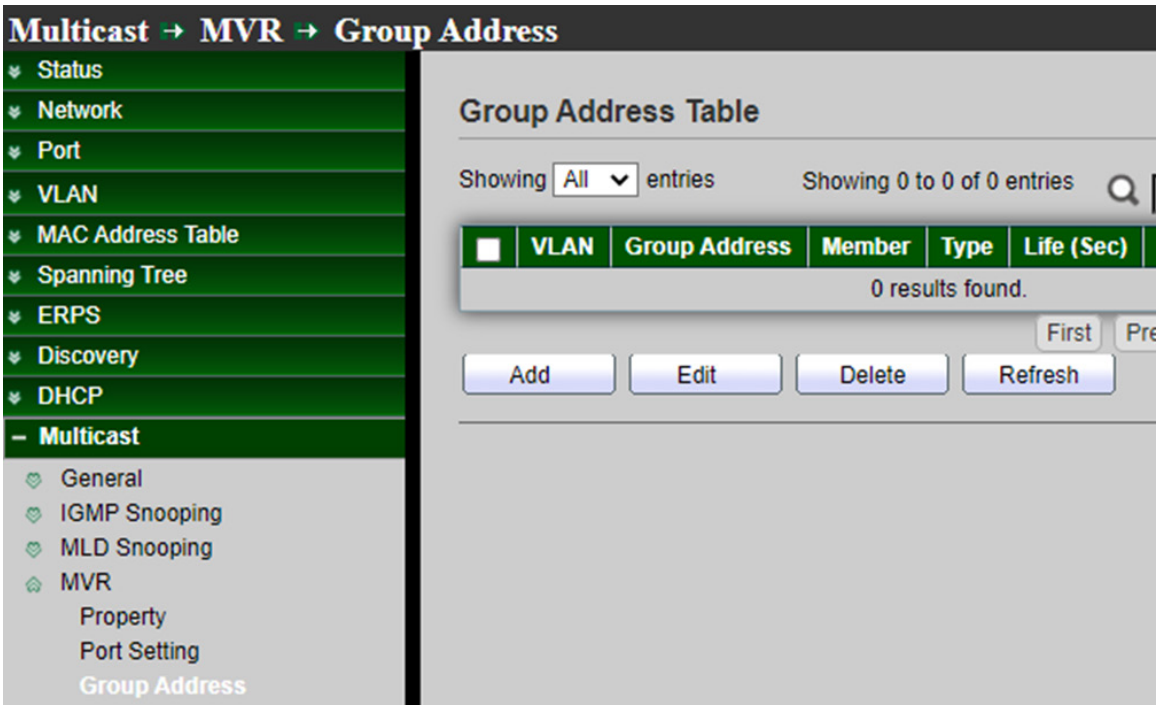
➢ **Immediate Leave :** MVR 連接埠立即離開。

- **Enable :** 如果選取則啟用立即離開，否則停用立即離開，此功能僅在連接單一接收設備的接收連接埠上啟用。預設情況下禁用 Immediate Leave 功能。

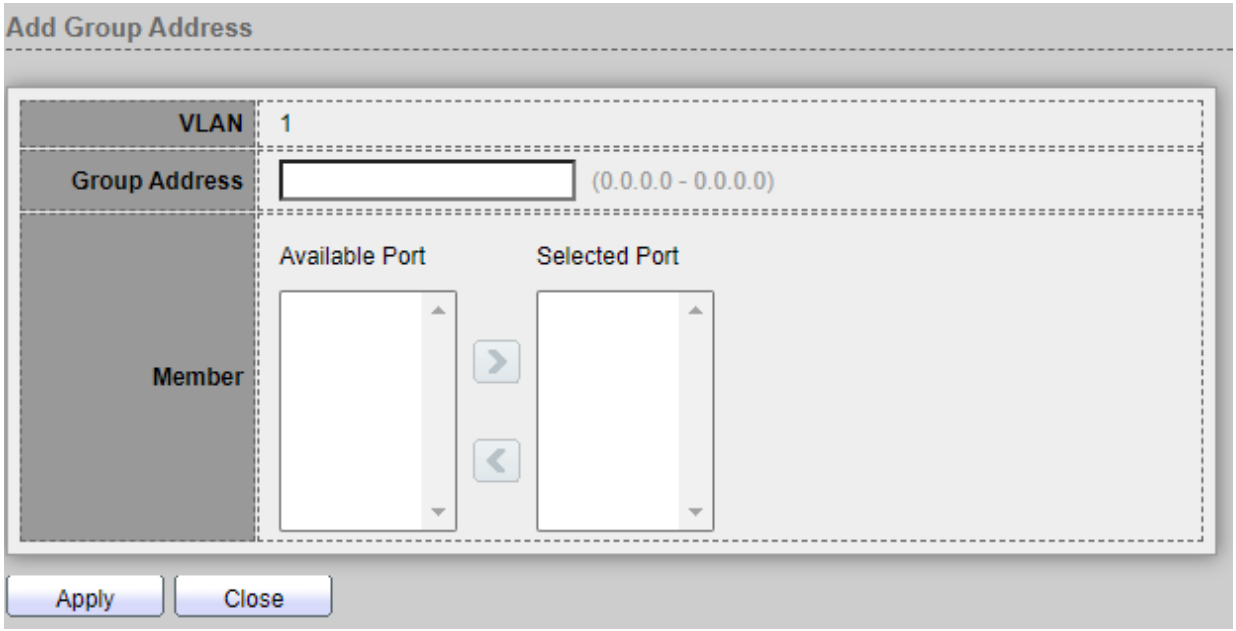
*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

## 12.4.3 群組位址(Group Address)

設定"add"、"Edit"、"Delete"和"Refresh"功能進行管理。



| 欄位 | 描述 |
|---|---|
| VLAN | MVR群組的VLAN ID |
| Group Address | MVR群組IP位址 |
| Member | MVR群組的成員連接埠 |
| Type | MVR群組類型：靜態或動態 |
| Life(Sec) | 動態MVR群組的存在時間 |




- **VLAN :** MVR 群組的 VLAN ID。
- **Group Address :** MVR 群組 IP 位址，使用者管理員可以在交換器上設定 MVR 多播群組位址(位址範圍為 224.0.0.0 至 239.255.255.255)。
- **Member :** 選擇 MVR 群組的連接埠。
  - **Available Port :** 可選的連接埠成員，當 MVR 模式為相容時僅有接收連接埠，當模式為動態時包括來源埠。
  - **Selected Port :** 已選的連接埠成員。

*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

# 13. IP Configuration

預設情況下，所有連接埠都屬於同一個 VLAN，交換器僅提供第 2 層功能。若要對連接的網路進行分段，首先為每個獨立的網路使用者群組或應用流量創建 VLAN，將屬於同一群組的所有連接埠分配給這些 VLAN，並為每個 VLAN 分配一個 IP 介面。透過將網路劃分為不同的 VLAN，可以將其劃分出在第 2 層斷開的子網路。同一子網路內的網路流量仍使用第 2 層進行交換。VLAN 現在可以(根據需求)與第 3 層交換互聯。

每個 VLAN 代表一個第 3 層虛擬介面。只需為每個虛擬介面提供網路位址，不同介面子網路之間的流量將透過第 3 層交換進行路由。

## 13.1 IPv4 管理和介面(IPv4 Management and Interfaces)

本章介紹如何設定 IP 介面以便通過網路管理訪問交換器。交換器支援 IPv4 和 IPv6，可以同時管理其中任一種位址類型。您可以手動設定特定的 IPv4 或 IPv6，也可以指示交換器從 BOOTP 或 DHCP 伺服器獲取 IPv4 位址。IPv6 位址只能手動設定。

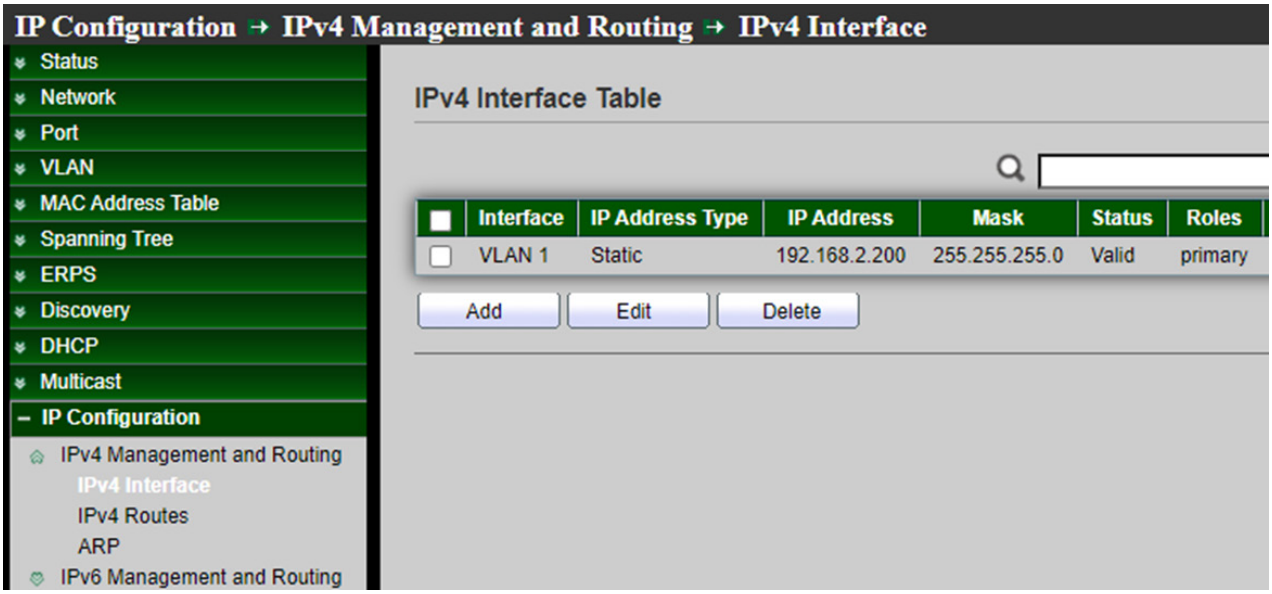
### IPv4 設定– 設定用於管理訪問的 IPv4 位址

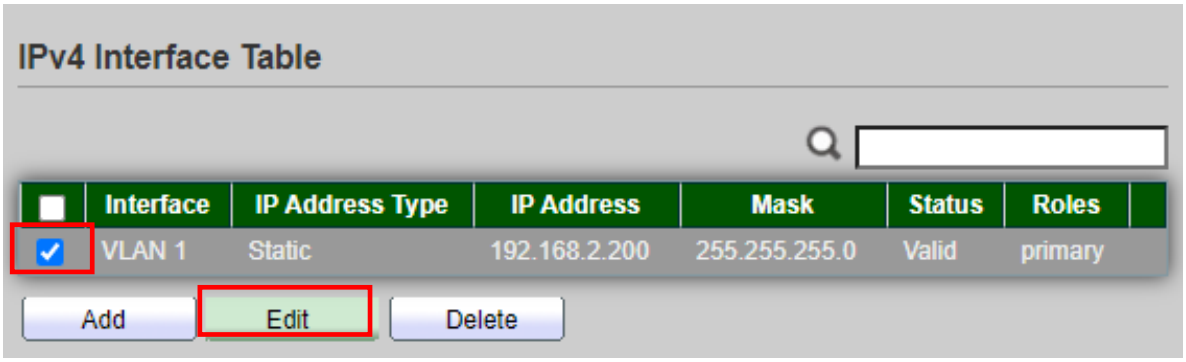
IPv4 位址預設 IP 為 **'192.168.2.200'** .若要設定靜態位元址，您需要將交換器的預設設定變更為與您的網路相容的值。**您可能還需要在交換器和另一個網段上的管理工作站之間建立預設閘道(如果未啟用路由協定)。**

您可以指示設備從 BOOTP 或 DHCP 伺服器獲取位址，也可以手動設定靜態 IP 位址。有效的 IP 位址由四個十進制數字(0 至 255)組成，並以句點分隔。不接受除此格式之外的任何格式。

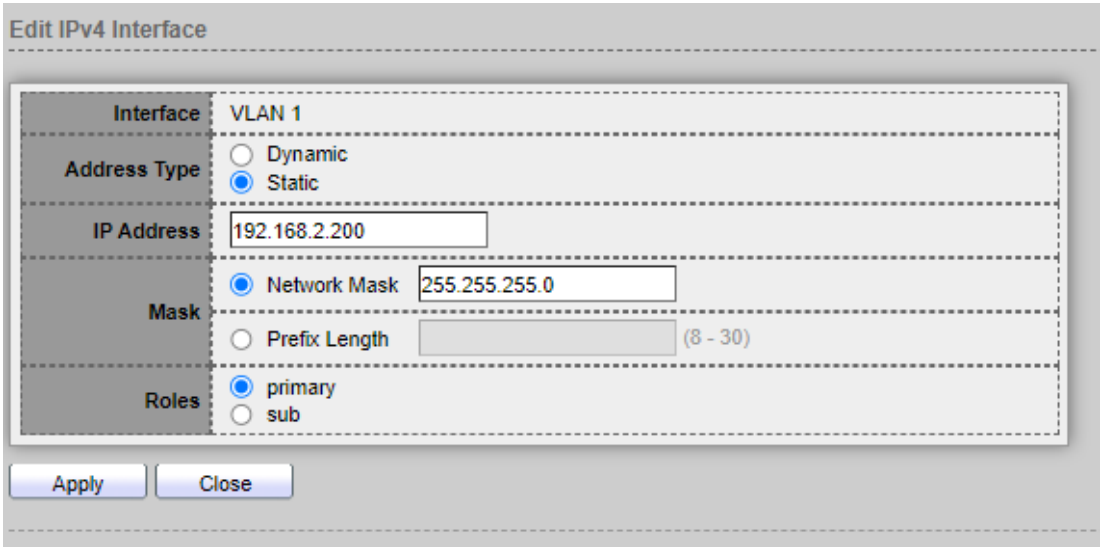
### 13.1.1 IPv4 介面&預設 IP 設定(IPv4 Interface & Default IP Configure)

使用者管理員可以設定該下拉清單來指定轉發 IPv4 封包通過的 IPv4 介面的 VLAN ID 編號，交換器支援 VLAN 介面類型和 Loopback 介面類型，設定**"add"**、**"Edit"**和**"Delete"**功能進行管理。




為您的 POE 交換器設定 VLAN1 (預設 VLAN ) IP 位址和 **'將運行設定儲存到啟動設定'**



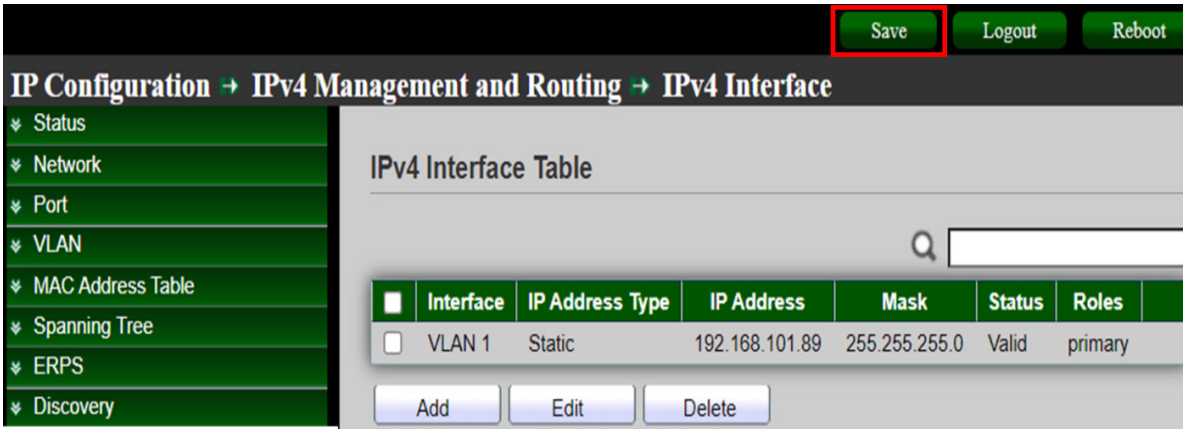
- Address Type :
  - Dynamic : 選擇設定為"Dynamic"類型。
  - Static : 選擇設定為"Static"類型。

| Note | 如果設定 “Dynamic” 類型，IP 設定會從 DHCP 伺服器分配獲取。 |
|---|---|

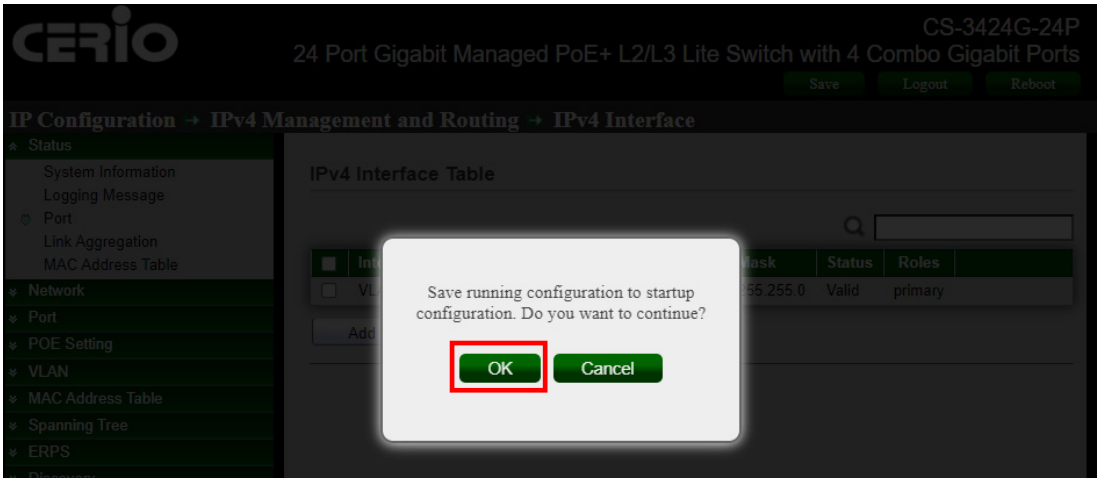
- IP Address : VLAN 的 IP 位址。有效的 IP 位址由四個數字(0 至 255)組成，並以句點分隔。 **(預設 IP 為 : 192.168.2.200)**
- Mask :
  - Network Mask : 該遮罩確定了用於路由到特定子網路的主機位址位元。**(預設網路遮罩為 : 255.255.255.0)**
  - Prefix Length : 在前綴長度欄位, 確定路由 IPv4 介面的前綴長度。
- Roles :
  - Primary : 在主要欄位,選擇確定為主要角色設定。
  - Sub : 在次要欄位, 選擇確定為次要角色設定。

*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

## ‘將運行設定儲存到啟動設定’

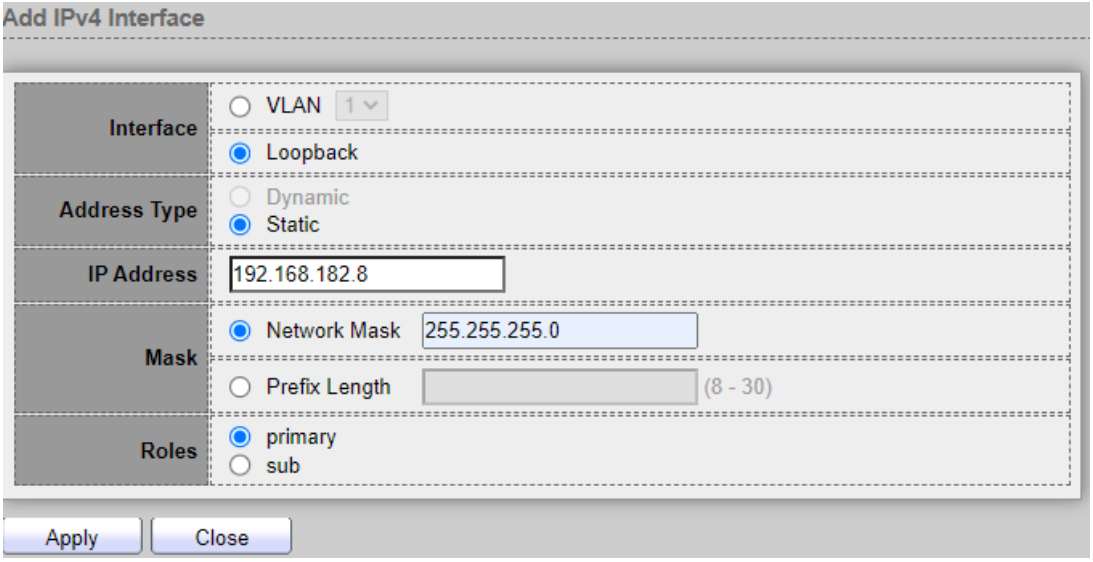



成功更改新 IP 後，執行"Save running configuration to startup configuration";使 POE 交換器新的 IP 設定在每次啟動時生效。




*點擊“ok”以保存‘Save running configuration to startup configuration’設定。*

## 在‘Loopback’新增 VLAN IP 位址設定

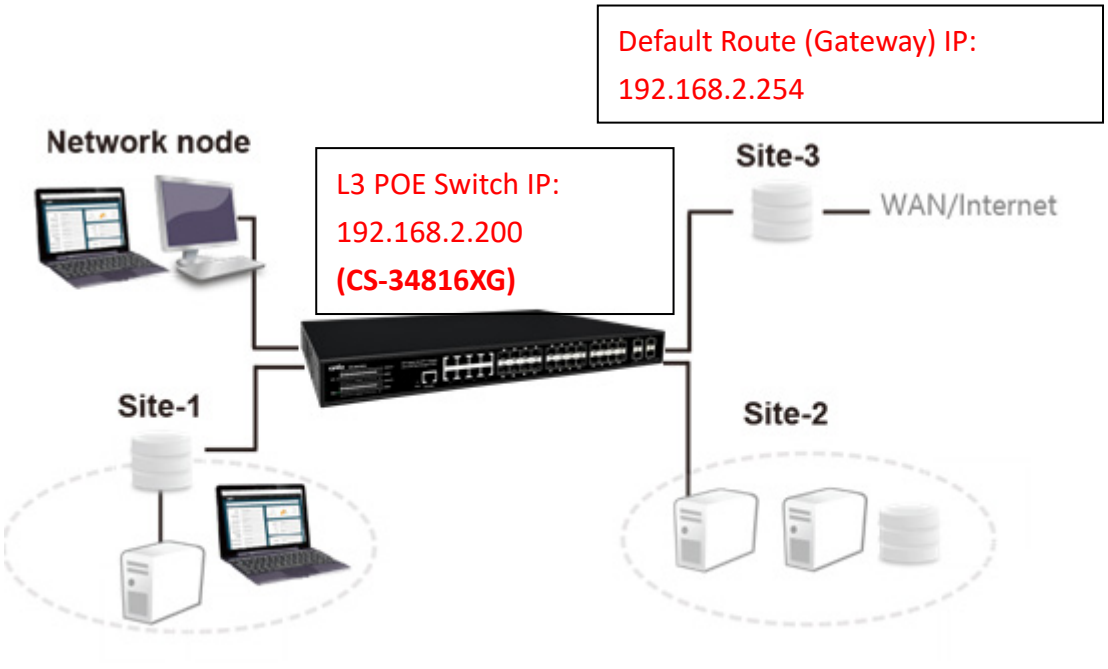



- **Address Type :** Loopback 介面只提供設定"static"類型。
- **IP Address :** 在 IP 位址欄位，確定路由 IPv4 介面的 IP 位址。
- **Mask :**
  - **Network Mask :** 在網路遮罩欄位，確定路由 IPv4 介面的子網路遮罩。
- **Prefix Length :** 在前綴長度欄位，確定路由 IPv4 介面的前綴長度。
- **Roles :**
  - **Primary :** 在主要欄位，選擇確定為主要角色設定。
  - **Sub :** 在次要欄位，選擇確定為次要角色設定。

*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

## 13.1.2 IPv4 路由&預設路由設定(IPv4 Routes & Default Route Configure)

您可以使用 IP > Static Routes (Add)頁面在路由表中輸入靜態路由。可能需要使用靜態路由來強制連接子網路的特定路由。靜態路由不會隨著網路拓撲結構的變化而自動變化，因此只需設定少量穩定路由即可確保網路的穩定。

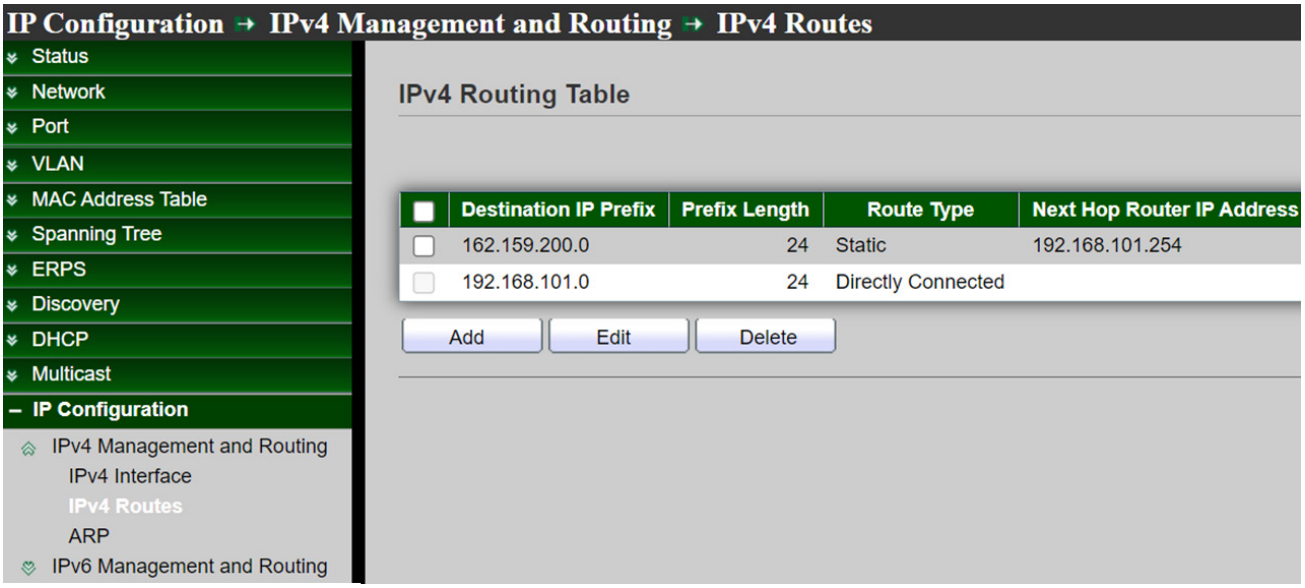



交換器通常使用預設閘道將 LAN 上的電腦的出站流量路由到網際網路。在網路中，路由器根據接收到資料的目的位元址選擇適當的路徑，並將資料轉送給下一個路由器。路徑中的最後一個路由器負責將封包轉送到目的主機。

例如，從“Network node”透過交換器的預設路由(預設閘道) (Site-3)到網際網路的流量。你可以創建一條靜態路由來連接到路由器(Site-2)後方 ISP 提供的服務。

創建另一條靜態路由來與連接到交換器的路由器(Site-1)後方的獨立網路進行通信。

使用者管理員可以設定“IPv4 Routing Table”頁面，並設定**"add"**、**"Edit"**和**"Delete"**功能進行管理。




## 在"Default Route"中設定閘道 IP 轉發封包的下一個目的路由，以便 LAN 設備訪問網際網路。和 ‘將運行設定儲存到啟動設定’

主機中的**預設路由**在通常稱為預設閘道。**預設閘道**通常是一個過濾設備。例如 NAT 閘道路由器、防火牆或代理伺服器。

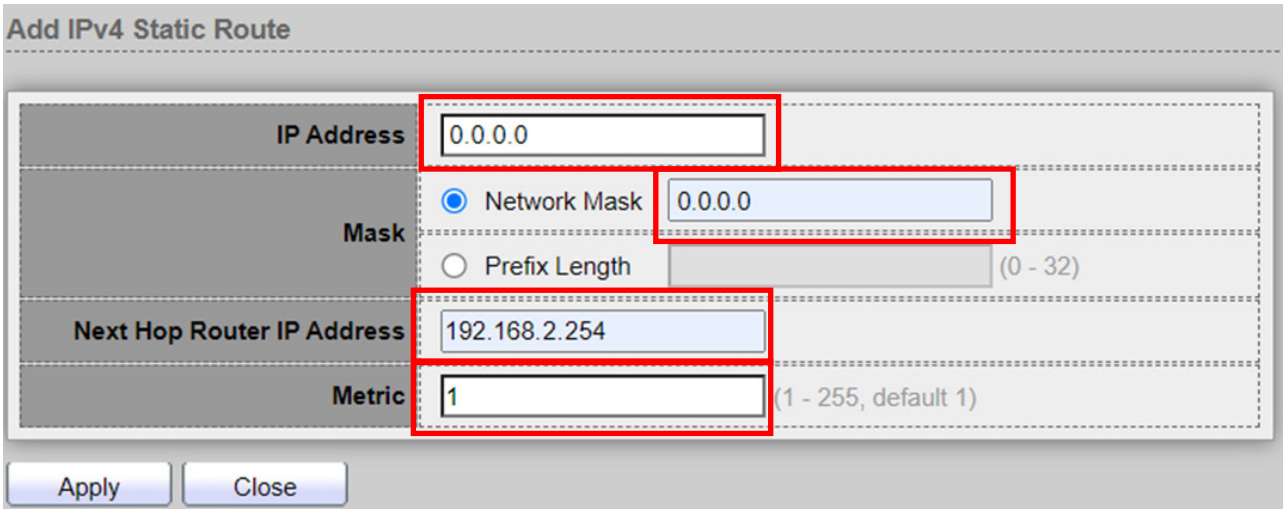
**"預設路由"**是當 IP 封包中的目的位元址找不到其他現有路由時，路由器選擇的路由。目的地不在路由器路由表中的所有封包都將使用預設路由。該路由通常指向另一個也處理封包的路由器：如果路由器知道如何路由封包，它就會將封包轉發到已知的路由；否則，封包將轉到預設路由。路由到另一個路由器。每次轉發，路由都會增加一跳的距離。

| Note | CS-34816XG 是一款具有路由功能的交換器。在第 2 層交換器環境運行時，“預設路由”該功能通常稱為"預設閘道設定"。L2 和 L3 的這些設定有相同目的，為未知 IP 資料設定的預設傳輸目的地。 |
|---|---|

TCP/ IP 網路中的預設路由設定是告知設備，在封包的目的 IP 與設備不在同一子網路時，如何轉發封包，以實現順利訪問網路。使用靜態路由設定來確定要指定為下一跳的閘道 IP 位址。

**設定 POE 交換器的"預設路由" (閘道 IP )。請參考以下內容。**

# 預設路由(閘道 IP)設定示例:



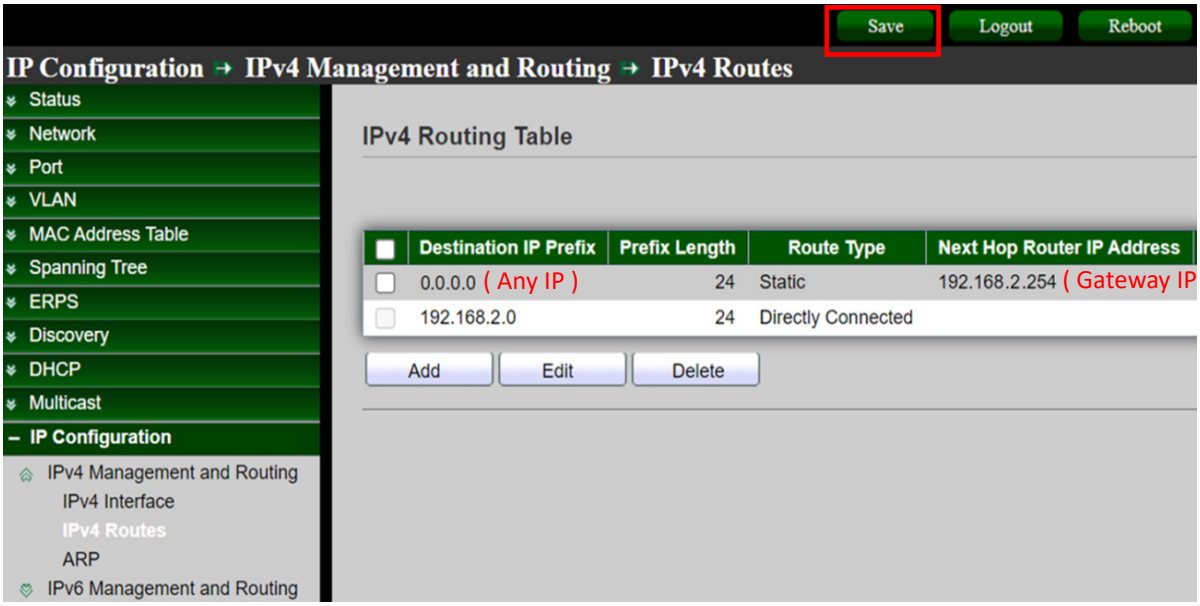

**預設路由器設定示例目的 IP 位元址和遮罩 IP 位址為 “0.0.0.0” (指任意 IP)，閘道路由器 IP 位址為 “192.168.2.254” ，度量為 “1” 。**

| Note | 目的 IP 和網路遮罩 0.0.0.0(指任意 IP)表示與其他路由清單不匹配的任意目的 IP 位元址。根據該預設的路由，所有上網流量都會被轉發到閘道路由器(192.168.2.254)。這樣就可以成功訪問網路(距離是一個可選參數，在這種情況下我們可以將其保留為預設值或將其設為 1)。 |
|---|---|

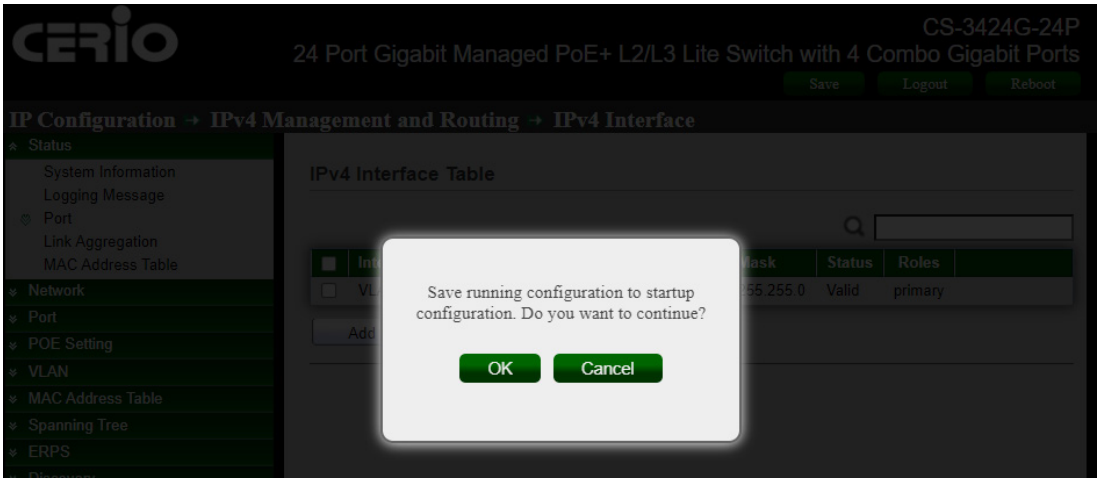
- **IP Address / Destination IP :** 在目的 IP 欄位元, 指定目的 IP 位元址。
- **Mask :**
  - **Network Mask :** 指定連接網路的子網路遮罩。
  - **Prefix Length :** 在 IPv4 前綴長度欄位元, 指定目的 IPv4 前綴長度。
- **Next Hop Router IP Address :** 在下一跳路由器 IP 位址欄位，指定將流量轉發至目的地路徑上的下一個路由器(如果有)時所使用的傳出路由器 IP 位址。
- **Metric :** 請填寫您想要用於路由目的的傳輸成本(跳數)。

*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

## ‘將運行設定儲存到啟動設定’

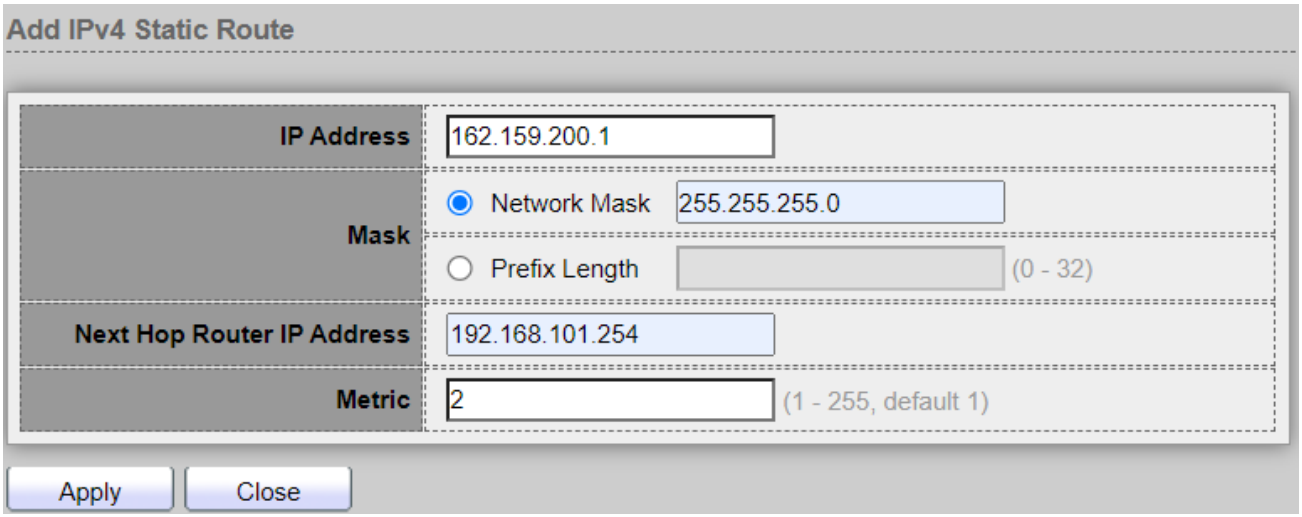



成功更改新 IP 後，執行"Save running configuration to startup configuration";使 POE 交換器新的 IP 設定在每次啟動時生效。




*點擊“ok”以保存‘Save running configuration to startup configuration’設定。*

# 靜態路由設定示例:




**靜態路由預設 IP 位址為 162.159.200.1**

**閘道路由器 IP 位址為 192.168.101.254**

- **IP Address / Destination IP :** 在目的 IP 欄位元,指定目的地 IP 位址。

| | |
|---|---|
| Note | 該參數指定最終目的地 IP 網路位址。路由選擇始終基於網路編號。<br>如果需要指定到單一主機的路由，請在 Subnet Mask 欄位中使用子網路遮罩 255.255.255.255，以強制網路編號與主機 ID 相同。 |

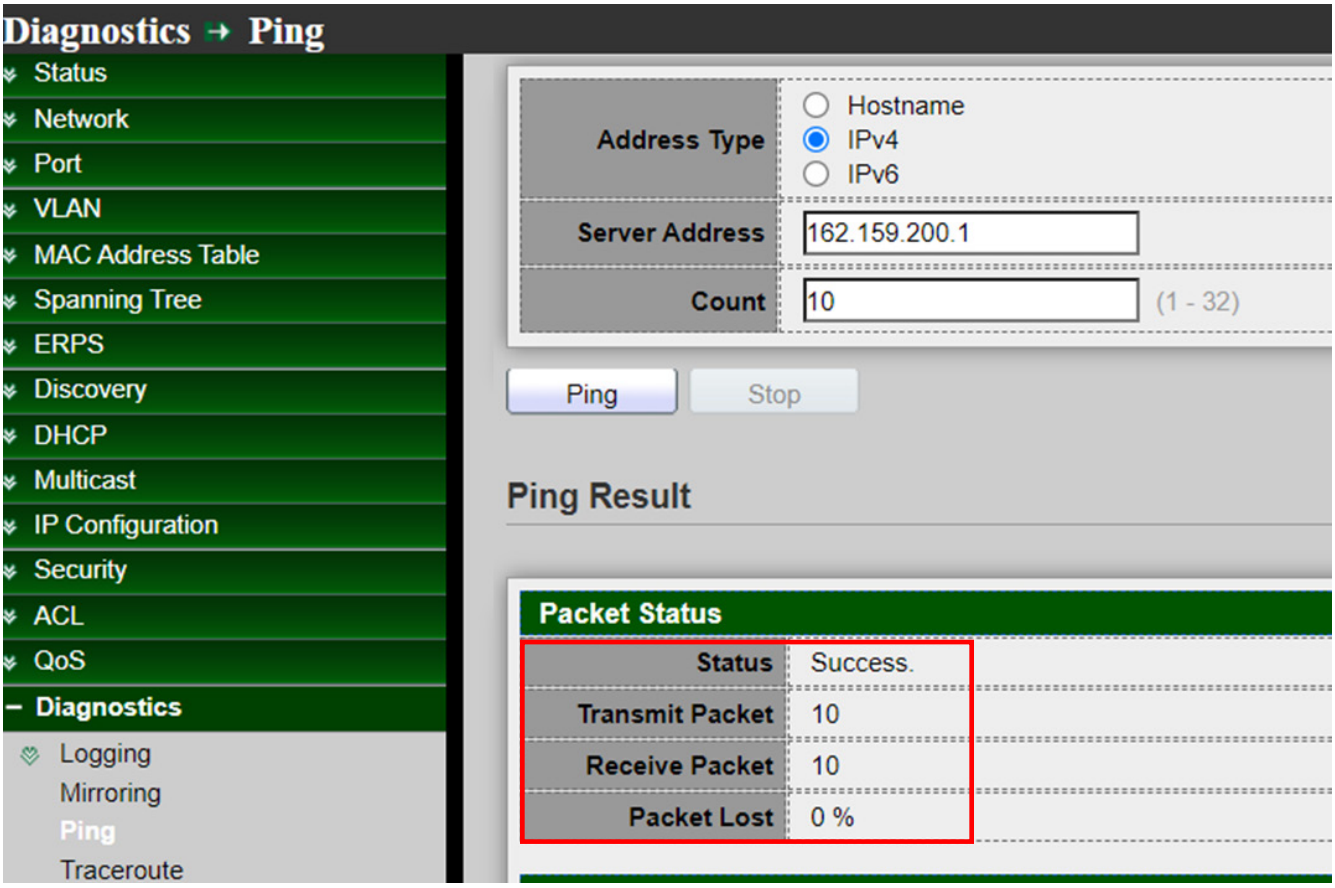
- **Mask :**
  - **Network Mask:** 指定連接網路的子網路遮罩。
  - **Prefix Length :** 在 IPv4 前綴長度欄位, 指定目的地 IPv4 前綴長度。
- **Next Hop Router IP Address :** 在下一跳路由器 IP 位址欄位,指定將流量轉發至目的地路徑上的下一個路由器(如果有)時所使用的傳出路由器 IP 位址。

| | |
|---|---|
| Note | 下一個路由器總是相鄰鄰近設備之一或直接連接網路的本地介面 IP 位址。 |

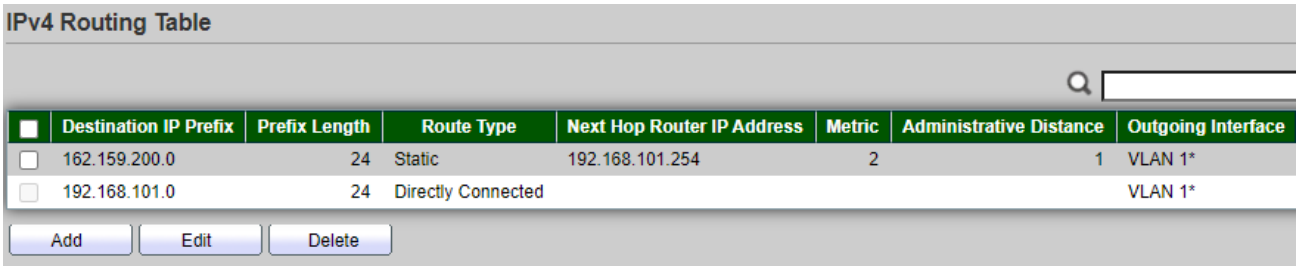
➢ **Metric :** 請填寫您想要用於路由目的的傳輸成本(跳數)。

| Note | 該度量表示用於路由目的的傳輸 “成本” 。IP 路由使用 “跳數” 來衡量成本，對於直接連接的網絡最小值為 1。輸入一個近似於該鏈路成本的數字。數字不必精確，但必須介於 1 和 255 之間。事實上，這裡通常建議填寫 1 或 2 或 3 來填寫常用的數字。 |
|---|---|

*點擊"Apply"儲存您的變更，或"Close"關閉設定。.*




**靜態路由示例 IP 位址輸入 “ 162.159.200.1”,如果設定成功，則可以透過 “Diagnostics> Ping tool” 進行測試驗證。**




| 欄位 | 描述 |
|---|---|
| Destination IP Prefix | 目的地IP前綴 |
| Prefix Length | 路由的前綴長度 |
| Router Type | 路由類型：靜態或動態，取決於路由的添加方式 |
| Next Hop Router IP Address | 將流量轉發至目的地路徑上的下一個路由器(如果有)時所使用的傳出路由器IP位址。下一個路由器**(例如，您的閘道站點IP位址)**總是相鄰鄰近設備之一或直接連接網路的本地介面IP位址 |
| Metric | 設定的下一跳的度量值<br>指定度量(有時稱為管理距離)，是一個從1至255的整數值 |
| Administrative Distance | 已設定路由的路由管理距離 |
| Outgoing Interface | 路由的輸出介面處於設定啟用的或非設定啟用的狀態 |

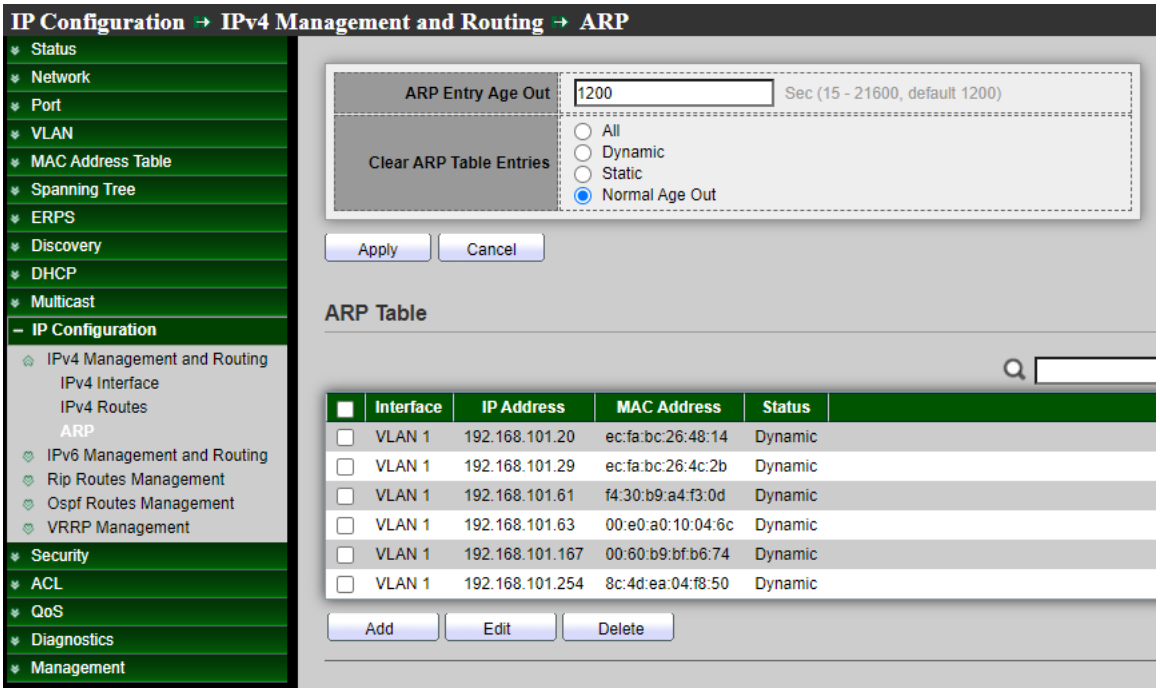
## 13.1.3 位址解析協定(ARP)

ARP(Address Resolution Protocol，位址解析協定)是將 IP 位址解析為乙太網路 MAC 位址(或實體位址)的協定。在區域網路中，當一台主機或其他網路設備有資料要傳送給另一台主機或設備時，它必須知道對方的網路層和 IP 位址。但僅有 IP 位址還不夠，因為 IP 資料必須封裝成訊框透過實體網路發送，所以發送站還必須有接收站的實體位址，所以位元址需要從 IP 映射到實體位址。ARP 就是實現這個功能的協定。

**ARP table** (ARP 緩存頁面)

設備透過 ARP 解析出目的 MAC 位元址後，會在自己的 ARP 表中新增一個 IP 位址到 MAC 位址的映射清單，以便後續資料轉送至相同目的地。ARP 表分為 “動態 ARP 表” 和 “靜態 ARP 表” 。

使用 **ARP table** (ARP 緩存頁面)查看表中的清單，這是該交換器最近記錄到的遠端連線的表。




- **ARP Entry Age Out :** ARP 延遲時間可以設定從 15 秒至 21600 秒，預設為 1200 秒。
- **Clear ARP Table Entries :** 使用者管理員可以透過 “All(全部)” 、 “Dynamic(動態)” 、 “Static(靜態)” 以及 “Normal Age Out(正常延遲)” (ARP 延遲設定時間)管理設定 ARP 表的 “Clean ARP Table Entries” 。

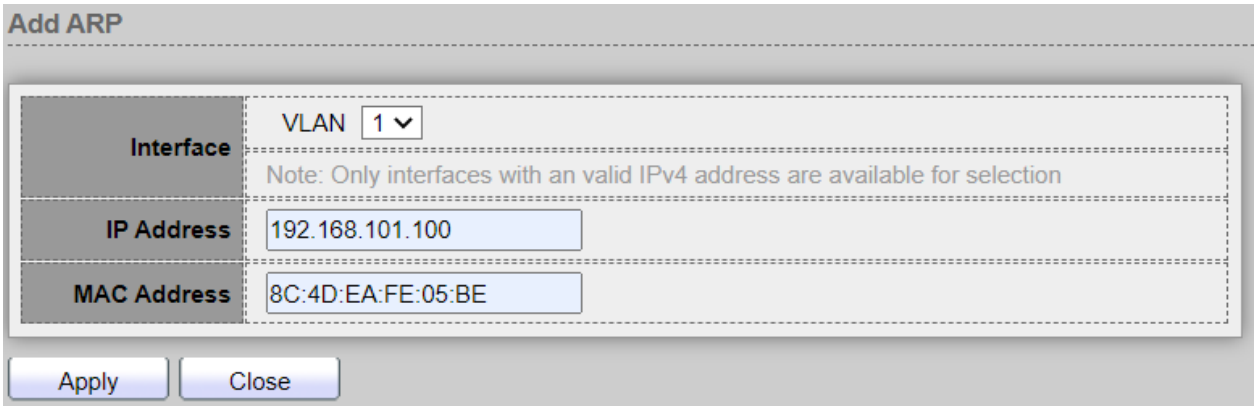
| Note | 1. 動態 ARP 表：<br>動態 ARP 表由 ARP 協定透過 ARP 延遲時間自動生成和維護，可以過期和無效，被新的 ARP 表更新或被被靜態 ARP 表覆蓋。當失效時間到期且介面被禁用時，對應的動態 ARP 表將自動刪除。<br>2. 靜態 ARP 表：<br>靜態 ARP 表是手動設定和維護的，不會失效被或被動態 ARP 表覆蓋。 |
|---|---|

*點擊"Apply"儲存您的變更，或 "Cancel" 取消設定。*

## ARP Table

使用者管理員可以設定 "ARP" 頁面，並設定**"add"**、**"Edit"**和**"Delete"**功能進行管理。

| 欄位 | 描述 |
|---|---|
| Interface | 與ARP清單關聯的路由介面 |
| IP Address | 顯示連接到交換器現有路由介面的設備(在子網路上)的IP位址 |
| MAC Address | 顯示連接設備的單播MAC位址。位址是用冒號分隔的六個兩位十六進制數，例如，40:bo:34:54:97:82 |
| Status | ARP清單類型，可能值如下：<br>• **Local :** 與交換器路由介面的一個MAC位址相關聯的ARP清單<br>• **Gateway :** 一個動態ARP清單，其IP位址是路由器的IP位址<br>• **Static :** ARP清單是手動設定的<br>• **Dynamic :** 路由器學習的ARP清單 |




- **Interface :** 使用者管理員可以選擇 VLAN 介面。
- **IP Address :** 輸入新增 ARP 表的 IPv4 位址。
- **MAC Address :** 輸入新增 ARP 表的 MAC 位址。

| | |
|---|---|
| Note | 設定靜態 ARP 表可以提高通訊安全性。靜態 ARP 表在與具有指定 IP 位址的設備通訊時限制使用指定的 MAC 位址。此時，有害網路傳輸無法修改清單的 IP 位址與 MAC 位址的映射關係，從而保護設備與指定設備之間的正常通訊。 |

*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

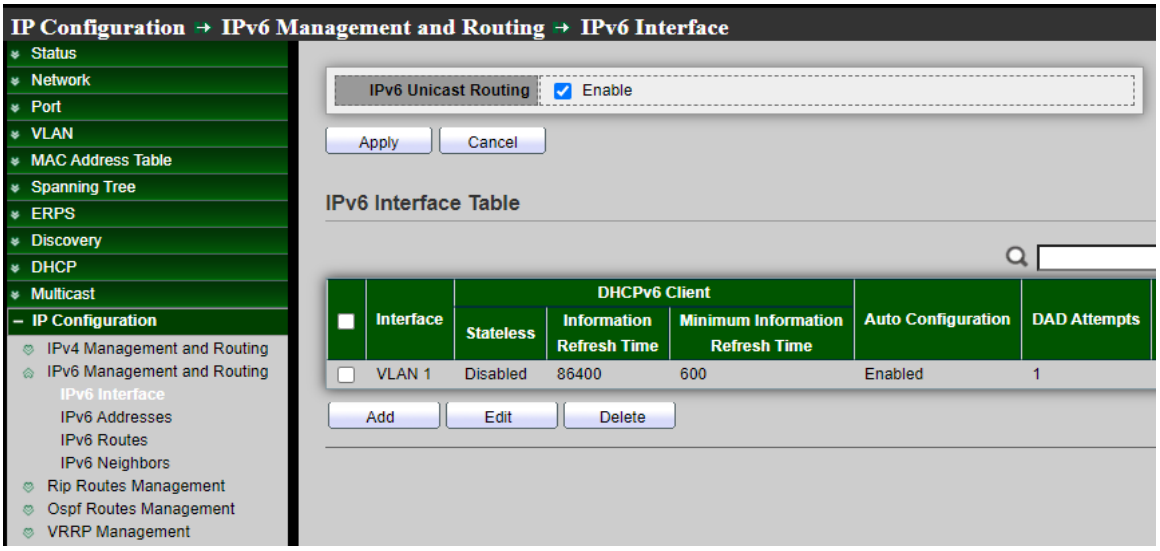
## 13.2 IPv6 管理和介面(IPv6 Management and Interfaces)

本章介紹如何設定 IP 介面以便通過網路管理訪問交換器。交換器支援 IPv4 和 IPv6，可以同時管理其中任一種位址類型。您可以手動設定特定的 IPv4 或 IPv6，也可以指示交換器從 BOOTP 或 DHCP 伺服器獲取 IPv4 位址。IPv6 位址只能手動設定。

### IPv6 設定– 設定用於管理訪問的 IPv6 位址

#### 13.2.1 IPv6 介面(IPv6 Interface)

使用者管理員可以設定 “IPv6 Interface Table” 頁面，並設定**"add"**、**"Edit"**和**"Delete"**功能進行管理。




**IPv6 Unicast Routing :** 使用者管理員可以設定“Enable”該 IPv6 單播路由功能。

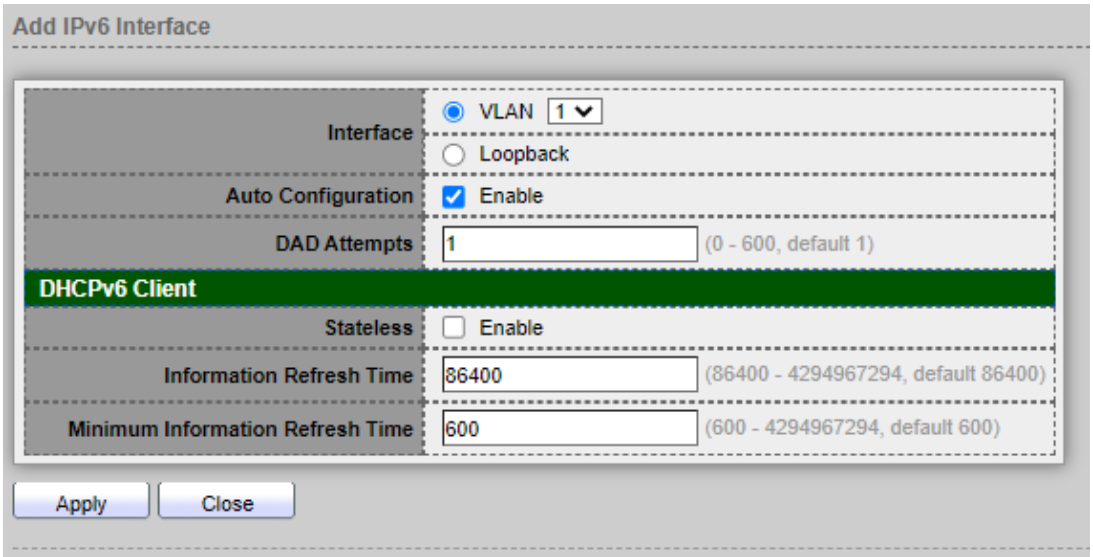
| Note | 在“IPv6 Unicast Routing”旁邊，透過選擇“啟用”或“禁用”，來指定是否全域啟用 IPv6 單播路由。 |
|---|---|

*點擊"Apply"儲存您的變更，或"Cancel"取消設定。*

選擇轉發 IPv6 封包通過的 IPv6 介面類型。

交換器支援 VLAN 介面類型和 Loopback 介面類型。

*在“VLAN“上設定“Interface”：*



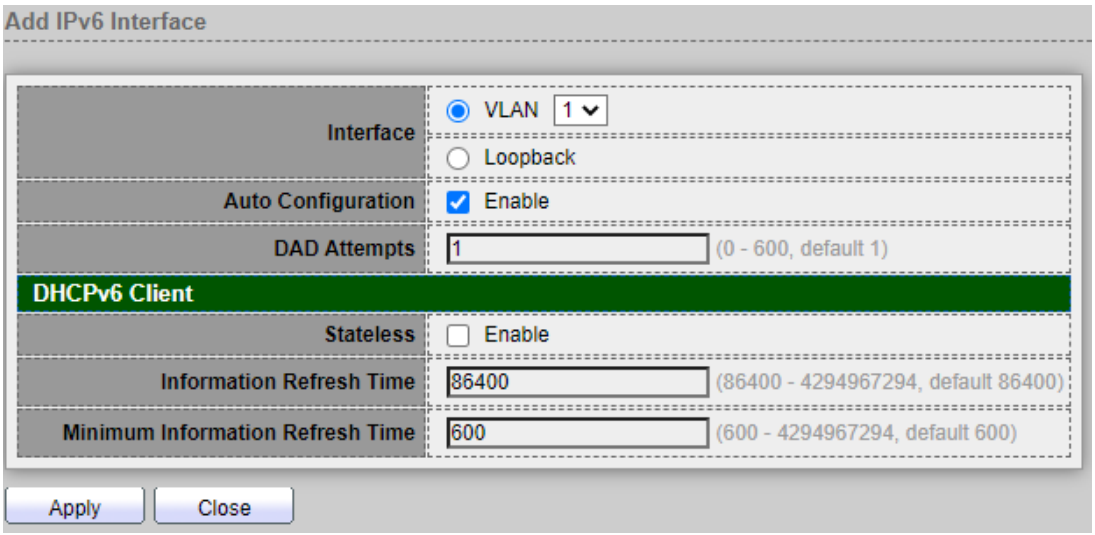
- **Auto Configuration :** IPv6 位址自動設定會自動為給定的線路描述創建新的 IPv6 介面，並為介面分配 IPv6 位址。
- **DAD Attempts :** 設定對介面上的單播位址執行重複位址探測(Duplicate Address Detect, DAD)時要傳送的鄰近設備請求的次數。此指令的 no 形式將嘗試次數設定為預設值。

**DHCP6 Client :**

- **Stateless :** IPv6 無狀態位址自動設定(StateLess Address Auto Configuration,SLAAC)功能。
- **Information Refresh Time :** 設定無狀態 DHCPv6 方式分配給客戶端的設定訊息的刷新時間。預設為 86400s。
- **Minimum Information Refresh Time :** 預設為 600s。

*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

*在 "Loopback "上設定 "Interface" :*

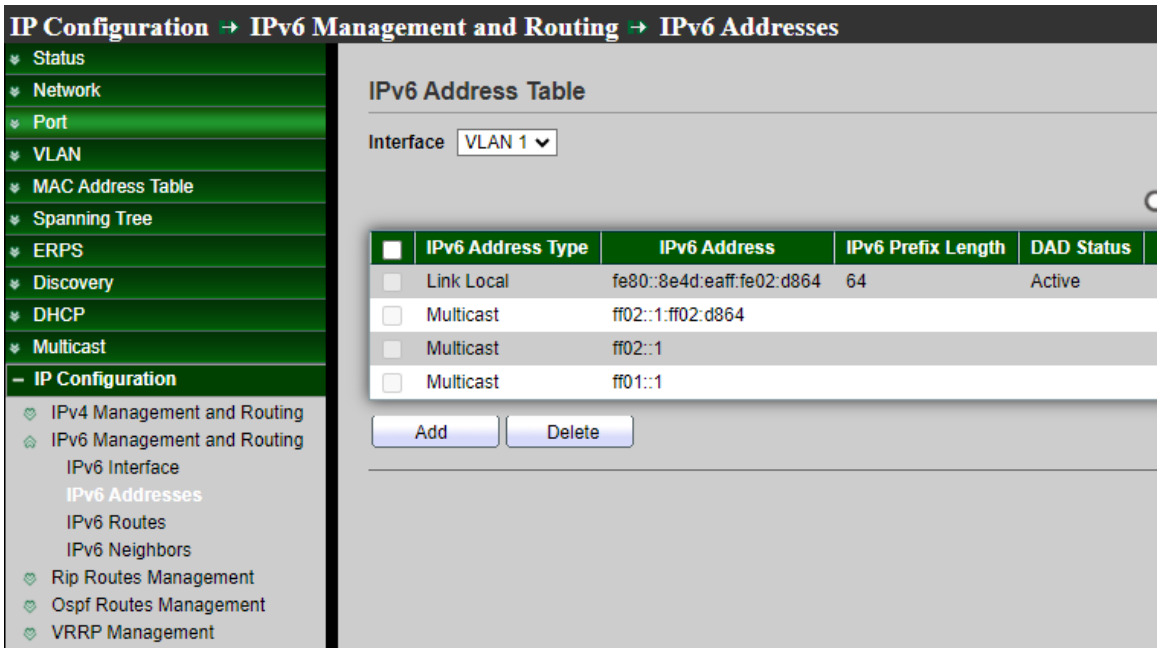



Loopback : 節點可使用 loopback 位址向其自身發送 IPv6 封包。
loopback 位址不得分配給實體或虛擬介面。

*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

### 13.2.2 IPv6 位址(IPv6 Addresses)

使用者管理員可以設定 “IPv6 Address Table” 頁面，並設定**"add"**和**"Delete"**功能進行管理。




#### IPv6 Address Table

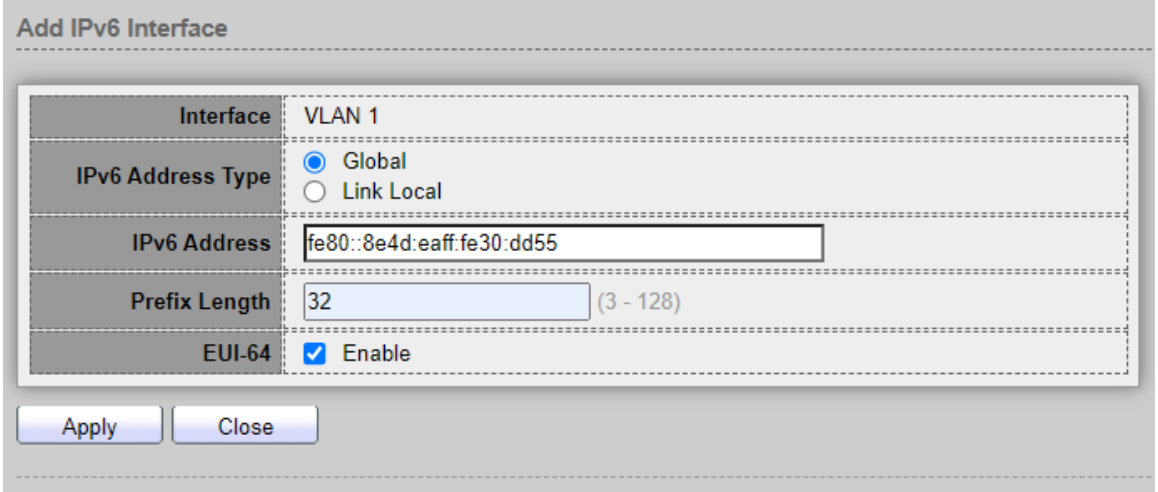
- **Interface :** 使用者管理員可以從介面選單選擇用於顯示 “IPv6 介面選擇” 頁面的 VLAN。該頁面也顯示 IPv6 介面設定表。

| 欄位 | 描述 |
|---|---|
| IPv6 Address Type | IPv6位址類型如：Multicast(多播)、Anycast(任播)或Unicast(單播) |
| IPv6 Address | 目的地的IPv6位址 |
| IPv6 Prefix Length | 設定啟用的路由的前綴長度 |
| DAD status | 顯示IPv6位址的狀態。可以是如下狀態：<br>• **Tent :** 由於 “重複位址探測” (DAD)狀態，路由被停用或位址不起作用<br>• **Active :** IPv6位址有效和設定啟用的狀態<br>• **Preferred :** 已驗證IPv6位址是唯一、有效和設定啟用的的 |

選擇使用 IPv6 格式的 IPv6 位址類型。

交換器支援 Global(全域)類型和 Link Local(鏈路本地)類型。

*在 "Global" 上設定 "IPv6 Address Type" :*

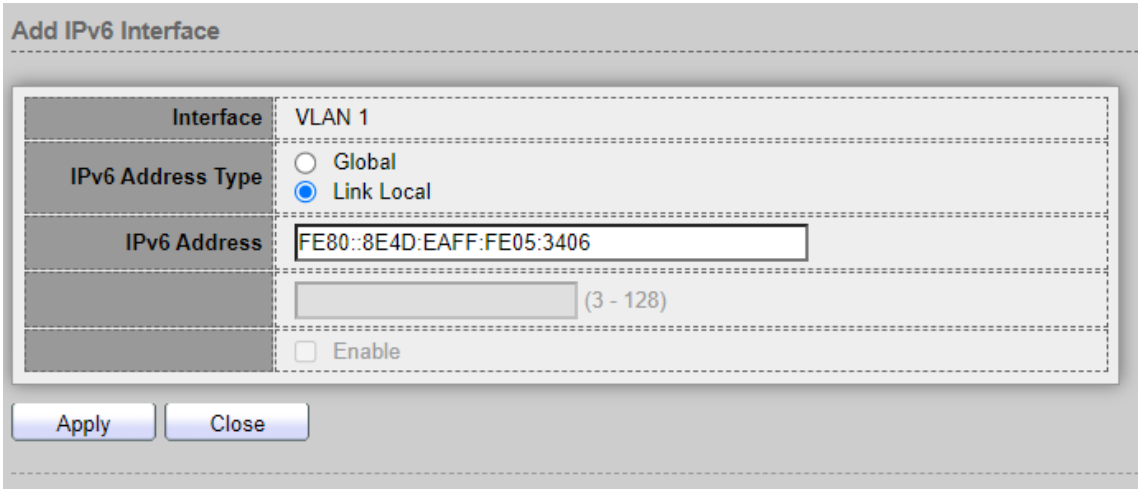



- **IPv6 Address Type :**
  - **Global :** 設定 IPv6 全域單播位址，用完整的 IPv6 位址，包括網路前綴和主機位址位元，後面跟一個正斜杠，以及十進位值，十進位值表示位址區塊中組成前綴的連續位元數。
  - **Link Local :** 設定 IPv6 鏈路本地位址。位址前綴範圍必須在 FE80 至 FEBF 之間，並且每個介面只能設定一個鏈路本地位址(指定的位址將取代介面自動生成的鏈路本地位址)。
- **IPv6 Address :** 輸入完整的 IPv6 位址。 IPv6 輸入網路範圍示例 : 2001 : 8E4D : EAFF : FE01 : 0000 : 0000 : 0000 : 0002 ~ FFFF : FFFF : FFFF : FFFE (如需獲取 IPv6 IP，請聯繫您的 ISP 供應商)。
- **Prefix Length :** 交換器 IPv6 位址的前綴長度。
- **EUI-64 :** 勾選此部分則啟用 EUI-64 格式 IP6v 設定，使用低 64 位元的 EUI-64 介面 ID 為介面設定 IPv6 位址。

| Note | 交換器必須設定鏈路本地位址。因此，任何啟用 IPv6 功能的設定程式，包括位元址自動設定、明確啟用 IPv6 或手動分配全域單播位址，都會自生成生鏈路本地單播位址。鏈路本地位址的前綴長度固定為 64 位，預設位元址的主機部分基於介面標識符的修改後 EUI-64(擴展通用識別碼)形式。 |
|---|---|

*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

*在“Link Local”上設定“IPv6 Address Type”：*




- **IPv6 Addrress :** 本節使用基於 IPv6 模式位元址操作規範所要求的本地識別碼介面的本地鏈路位址，例如 “FE80::8E4D:EAFF:FE05:3406” 。

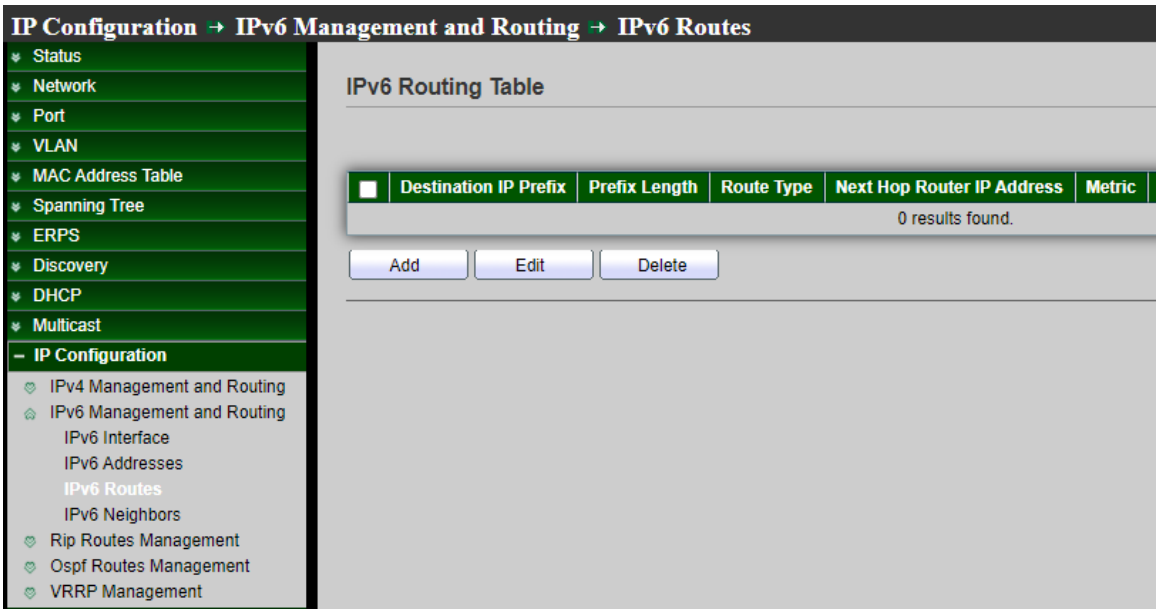
*點擊**"Apply"**儲存您的變更，或**"Close"**關閉設定。*

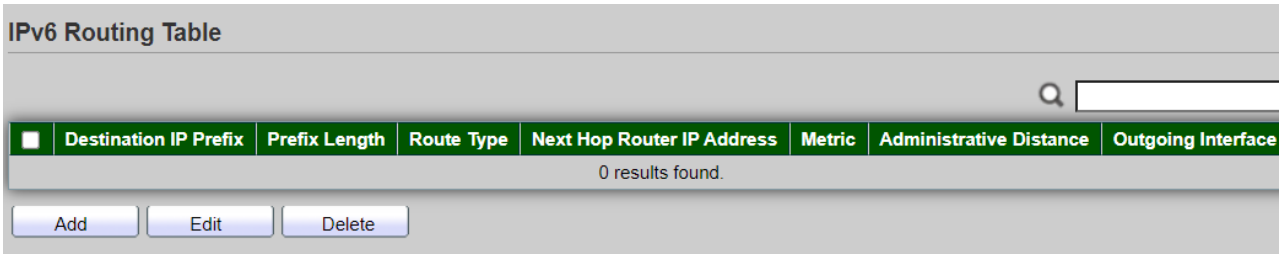
### 13.2.3 IPv6 路由(IPv6 Routes)

您可以使用 IP > Static Routes (Add)頁面在路由表中輸入靜態路由。可能需要使用靜態路由來強制連接子網路的特定路由。靜態路由不會隨著網路拓撲結構的變化而自動變化，因此只需設定少量穩定路由即可確保網路的穩定。

該頁面系統可以顯示 IPv6 路由表的 Destination IP Prefix(目的 IP 前綴) / Prefix Length(前綴長度) / Route Type(路由類型) / Next Hop Router IP Address(下一跳路由器 IP 位址) / Metric (度量) / Administrative Distance(管理距離) / Outgoing Interface(傳出介面)等資訊。

使用者管理員可以設定 “IPv6 Routing Table” 頁面，對**"add"**、**"Edit"**和**"Delete"**功能進行管理。




| 欄位 | 描述 |
|---|---|
| Destination IP Prefix | 目的地IP前綴 |
| Prefix Length | 設定啟用的路由的前綴長度 |
| Route Type | 設定啟用的路由的協定類型:<br>• Static(靜態).路由是手動確定的<br>• ND (鄰近設備發現).路由通過ND協定發現<br>• Connected(已連接).路由源自於手動設定的IPv6位址 |
| Next Hop Router IP Address | 設定啟用的路由的下一跳IPv6位址 |
| Metric | 設定的下一跳的度量值<br>指定度量(有時稱為管理距離)，是一個從1至255的整數值 |

| | |
|---|---|
| Administrative Distance | 已設定路由的路由管理距離 |
| Outgoing Interface | 路由的輸出介面處於設定啟用的或非設定啟用的狀態 |


- **IPv6 Prefix :** 在 IPv6 前綴欄位,指定目的地 IPv6 網路前綴。
- **IPv6 Prefix Length :** 在 IPv6 前綴長度欄位, 指定目的地 IPv6 前綴長度。
- **Next Hop Router IP Address :** 在下一跳 IPv6 位址欄位,指定將流量轉發至目的地路徑上的下一個路由器(如果有)時所使用的傳出路由器 IP 位址。

| | |
|---|---|
| **Note** | 下一個路由器總是相鄰鄰近設備之一或直接連接網路的本地介面 IP 位址。 |

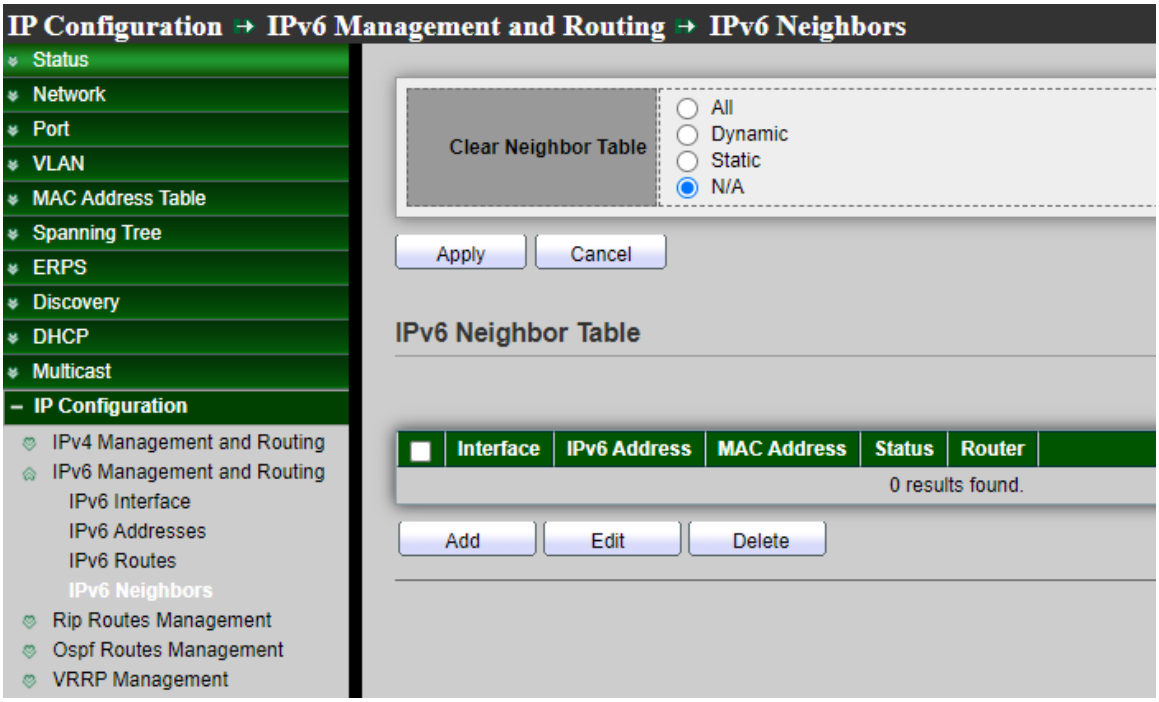
- **Metric :** 請填寫您想要用於路由目的的傳輸成本(跳數)。

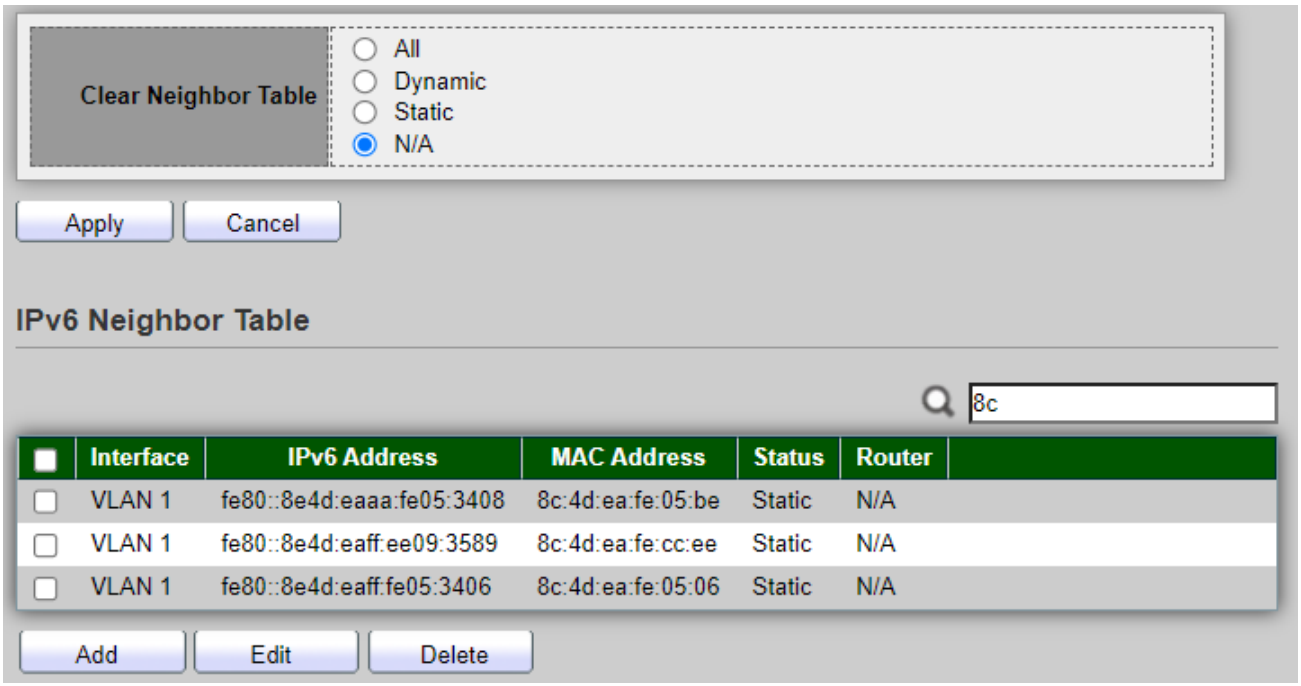
| | |
|---|---|
| **Note** | 該度量表示用於路由目的的傳輸“成本”。IP 路由使用“跳數”來衡量成本，對於直接連接的網絡最小值為 1。輸入一個近似於該鏈路成本的數字。數字不必精確，但必須介於 1 和 255 之間。事實上，這裡通常建議填寫 1 或 2 或 3 來填寫常用的數字。 |

*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

### 13.2.4 IPv6 鄰近設備(IPv6 Neighbors)

使用者管理員可以設定“IPv6 Neighbor Table”頁面，設定**"add"**、**"Edit"**和**"Delete"**功能進行管理。



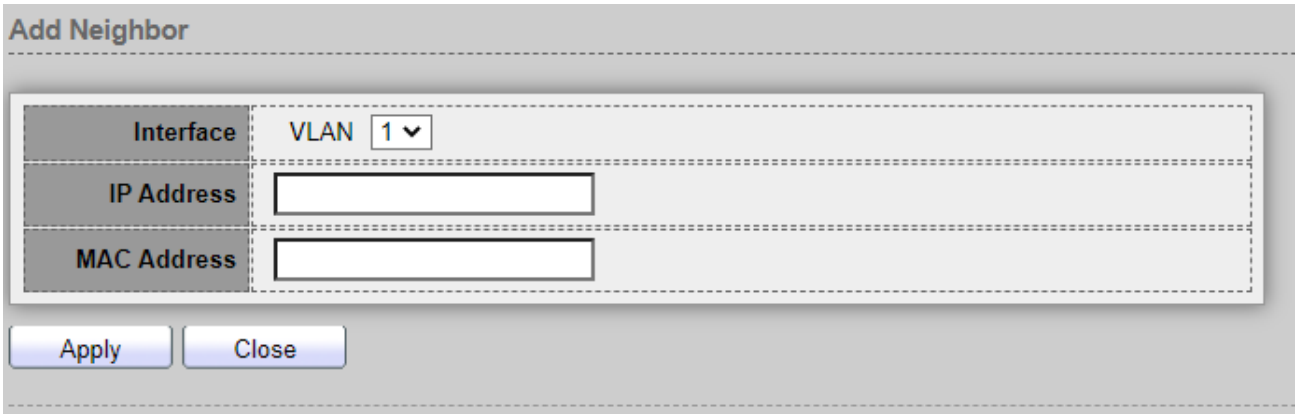

## Clear Neighbor Table

使用者管理員可以選擇過濾狀態類型，包括“All(全部)”、“Dynamic(動態)”、“Static(靜態)”或“N/A(不適用)”以快速選擇批量清除"IPv6 Neighbor Table"。

## Use the "Search" menu to consult the list

使用搜尋選單和欄位按 “關鍵字” 進行搜尋。例如，'8c'。然後點擊 “搜尋” 圖標。如果該位址存在，則顯示該清單。

| 欄位 | 描述 |
|---|---|
| Interface | 當前表格行中顯示其設定的介面<br>此欄位顯示創建了IPv6位址，或可以到達鄰近設備的IPv6介面ID編號 |
| IPv6 Address | 鄰近設備或介面的IPv6位址 |
| MAC Address | 該欄位顯示設定IPv6位址的IPv6介面的MAC位址或鄰近設備的MAC位址 |
| Status | 鄰近設備緩存清單的狀態。IPv6鄰近設備發現緩存中狀態為"Dynamic"或"Static" |
| Router | 為設定啟用的路由的鄰近設備 |




- **Interface :** 選擇用於 VLAN ID 設定的 IPv6 介面類型。
- **IP Addrress :** 指定可透過該介面到達的鄰近設備的 IPv6 位址。
- **MAC Addrerss :** 指定可透過該介面到達的鄰近設備的 MAC 位址。

*點擊**"Apply"**儲存您的變更，或**"Close"**關閉設定。*

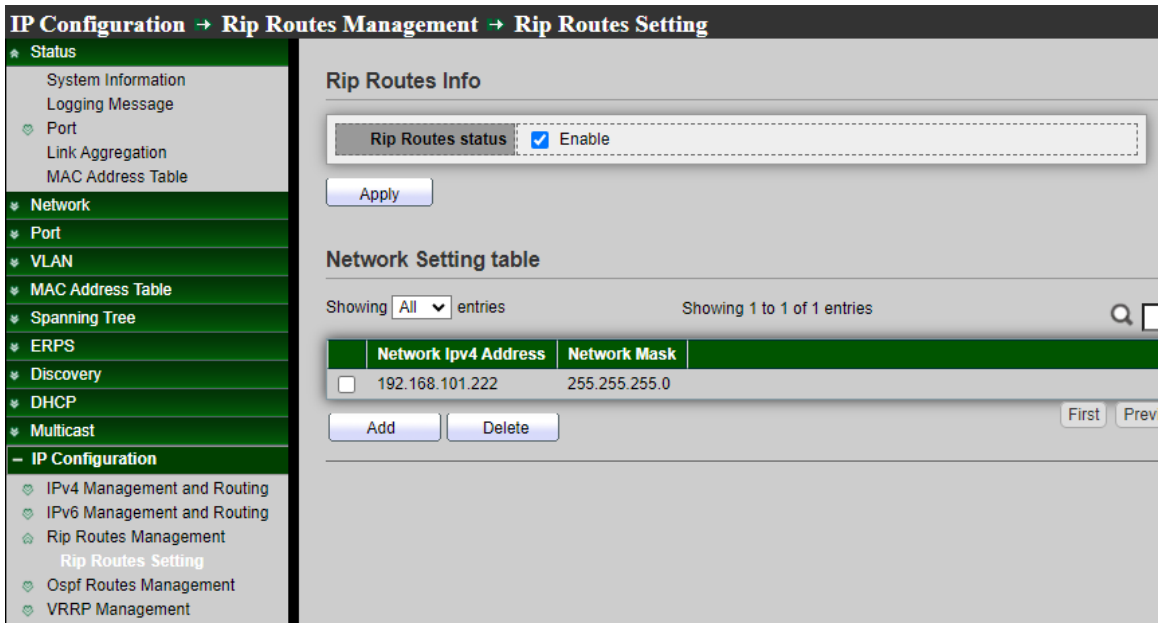
# 13.3 RIP 路由管理(RIP Routes Management)

此交換器 IPv4 路由支援 RIPv2 版本，RIPv2 能以多播方式傳送報文更新路由表。路由資訊協定(RIP)用於管理獨立網路(如企業區域網路或專用廣域網路)中的路由器資訊。使用 RIP，閘道主機每 30 秒傳送一次路由表給最近的路由器。然後該路由器將其路由表的內容傳送到相鄰路由器。

RIP 最適用小型網路。這是因為每 30 秒傳輸一次完整路由表會為網路帶來很大的流量負載，而且 RIP 表的跳數限制為 15 跳。因此，對於大型網路來說 OSPF 是更好的替代方案。

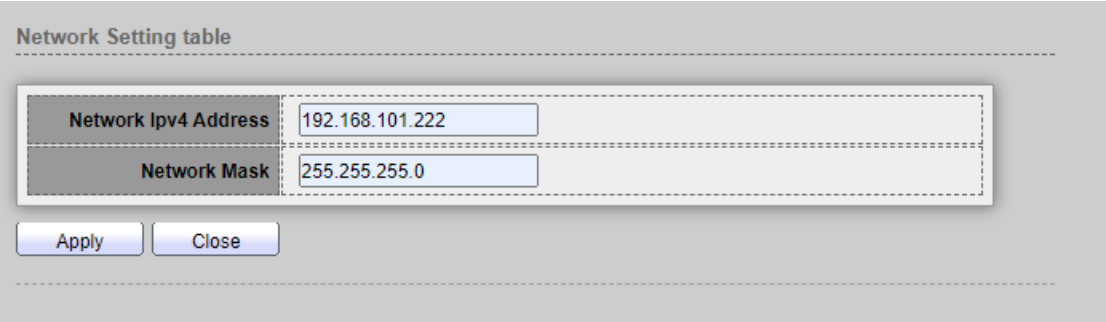
## 13.3.1 Rip 路由設定(Rip Routes Setting)

使用者管理員可以選擇啟用或停用，對 “Rip Routes status” 進行管理。




使用者管理員可以設定 “Rip Routes Info” 頁面，並設定**"add"**和**"Delete"**功能進行管理。

| 欄位 | 描述 |
|---|---|
| Network IPv4 Address | 顯示新增至要通告RIP路由協定中的IPv4 IP位址 |
| Network Mask | 顯示新增至要通告RIP路由協定中的路由遮罩 |




- **Network IPv4 Address :** 宣告要通告存取 RIPv2 路由協定的 IPv4 IP 位址。
- **Network Mask :** 宣告要通告存取 RIPv2 路由協定的路由遮罩。

*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

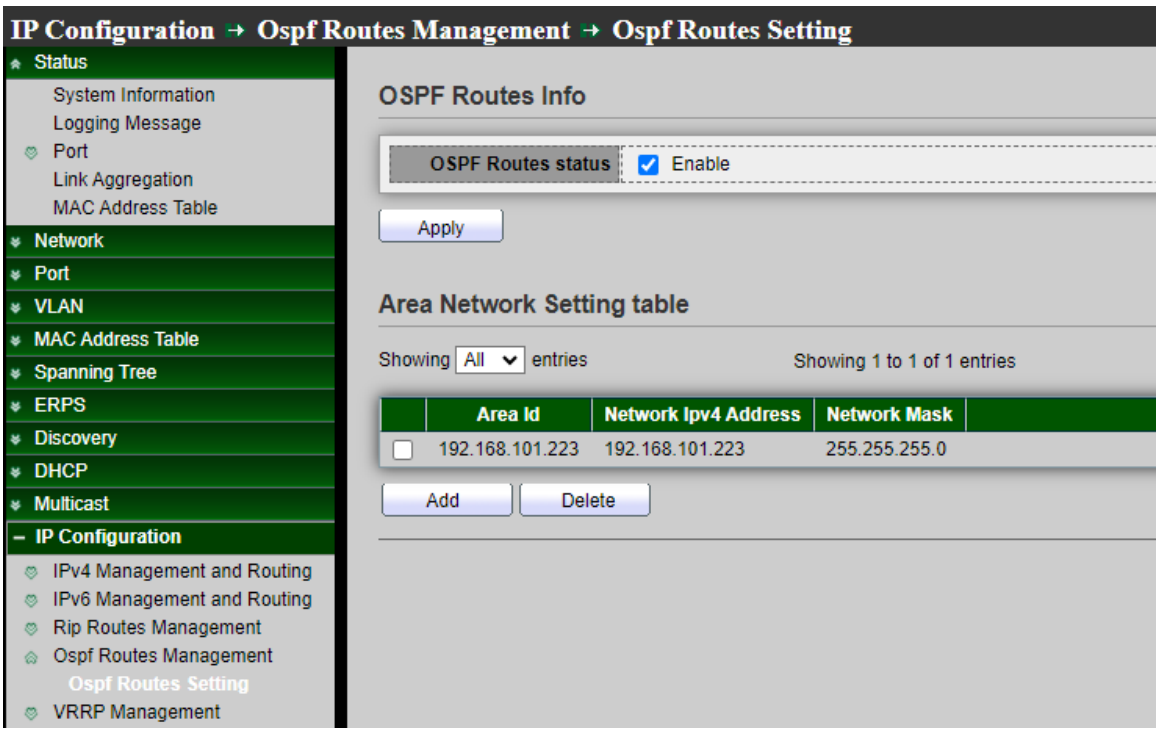
## 13.4 OSPF 路由管理(OSPF Routes Management)

在區域標籤上，以 x.x.x.x 為格式新增區域編號。要成為同一區域的一部分，這是每個鄰近設備必須接受的標識符。OSPF 透過從其他路由器取得資訊，並透過鏈路狀態通告(LSA)向其他路由器發佈路由通告來動態決定路由。路由器保留有關其與目的地之間的鏈路的訊息，並可以做出高效的路由決策。為每個路由器介面分配一個開銷，當對所有遇到的出站路由器介面和接收 LSA 的介面進行求和時，確定開銷最低的路徑為最佳路由。

分層技術用於限制必須通告的路由數量以及關聯的 LSA。由於 OSPF 動態處理大量路由訊息，因此對处理器和記憶體的要求比 RIP 更高。

### 13.4.1 Ospf 路由設定(Ospf Routes Setting)

使用者管理員可以選擇啟用或停用，對“OSPF Routes status “進行管理。




使用者管理員可以設定 “OSPF Routes Info” 頁面，並設定**"add"**和**"Delete"**功能進行管理。

| 欄位 | 描述 |
|---|---|
| Area Id | 顯示新增至要通告OSPFv2路由協定的A,B,C,D區域編號，在區域標籤上，以 x.x.x.x為格式新增區域編號。這是同一區域內每個鄰近設備必須接受的標識符 |
| Network IPv4 Address | 顯示新增至要通告OSPFv2路由協定的IPv4 IP地址 |
| Network Mask | 顯示新增至要通告OSPFv2路由協定的路由遮罩 |


- **Ared Id :** 宣告要通告存取 OSPFv2 路由協定的 A,B,C,D 區域編號。
- **Network IPv4 Address :** 宣告要通告存取 OSPFv2 路由協定的 IPv4 IP 地址。
- **Network Mask :** 宣告要通告存取 OSPFv2 路由協定的路由遮罩。

*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

## 13.5 VRRP 管理(VRRP Management)

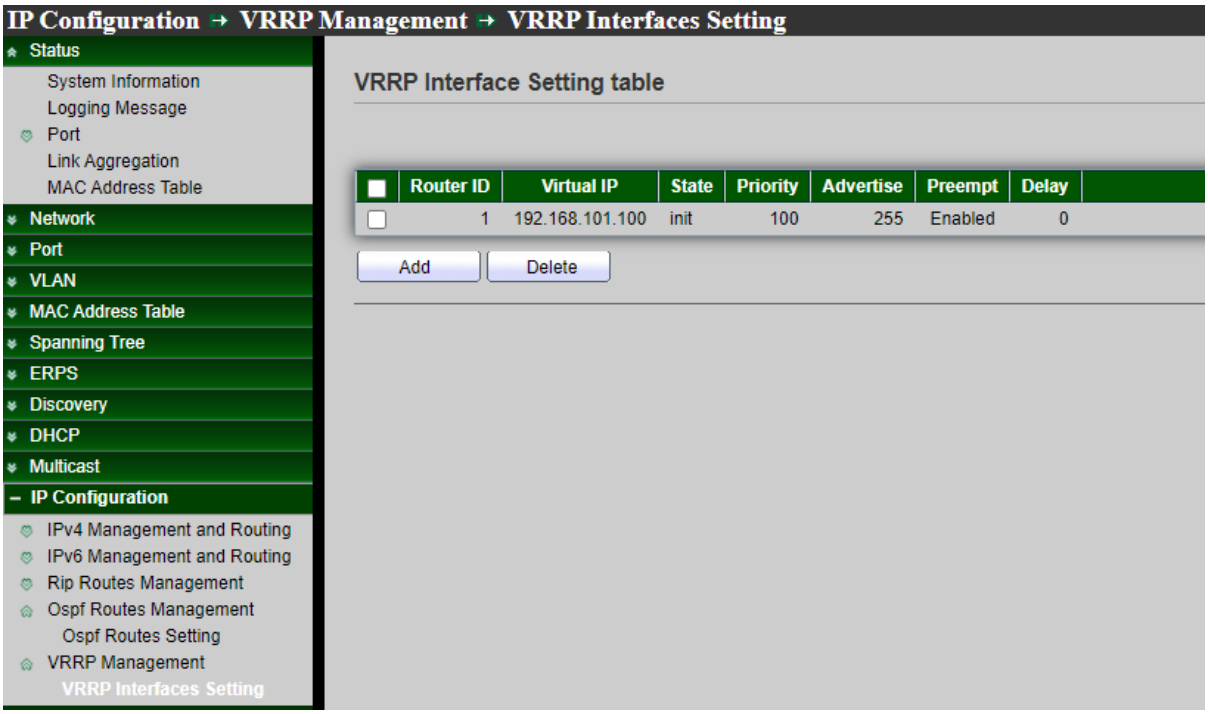
VRRP 會建立一個虛擬路由器，組態為預設閘道，在主路由器發生故障時充當備援路由器。主路由器定期發送通告。備援路由器監視這些通告以確定主路由器的狀態。如果主路由器發生故障，則優先級最高的備援路由器成為新的主路由器。

虛擬路由器備援協定 VRRPv2(Virtual Router Redundancy Protocol v2) 是一種網路協定，這個協定通過在子網路中自動選取預設閘道器，來增加路由的可用性和可靠性。該協定透過建立虛擬路由器來運行，虛擬路由器是對多個路由器作為一個群組的抽象表示。該群組在子網中向主機顯示自己為單一預設閘道。

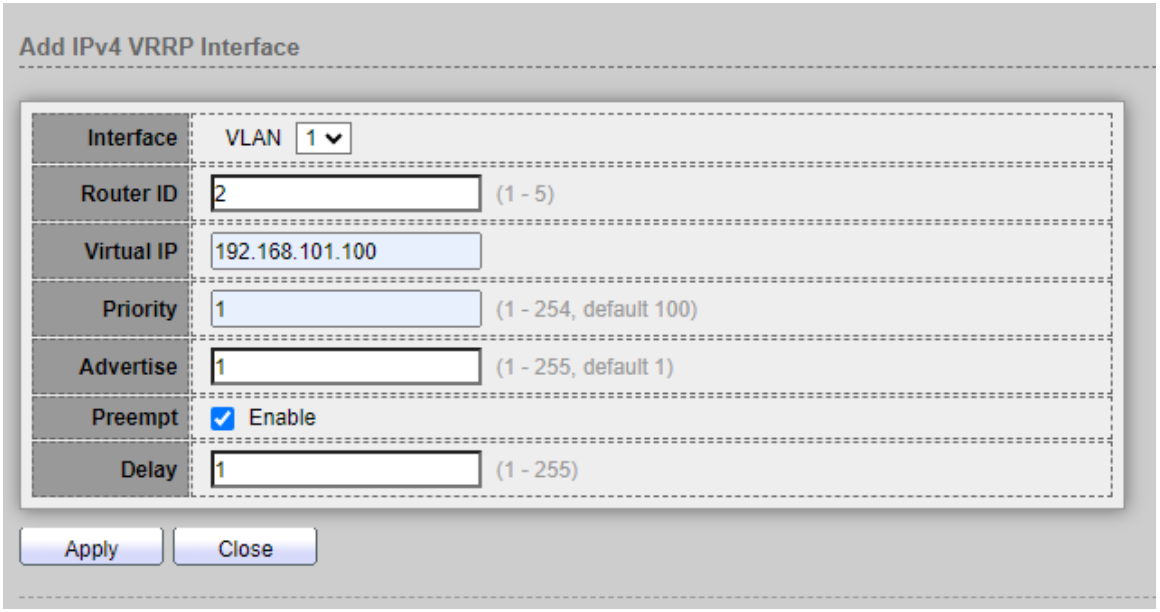
具有最高優先級的虛擬路由器成員成為主設備，並轉發發送到虛擬路由器 IP 位址的封包。其餘成員處於備援狀態，在主路由器故障時代替它。因此，虛擬路由器備援協定透過路由器冗餘來增強網路可靠性。

### 13.5.1 VRRP 介面設定(VRRP Interfaces Setting)

使用者管理員可以設定 “VRRP Interface Setting” 頁面，並設定**"add"**和**"Delete"**功能進行管理。




| 欄位 | 描述 |
|---|---|
| Router Id | 顯示虛擬路由器的ID編號 |
| Virtual IP | 顯示與虛擬路由器關聯的IP位址和IP路由域 |
| State | 顯示虛擬路由器的狀態<br>● Master : 該交換器充當主路由器<br>● Backup : 該交換器充當備援路由器<br>● Init : 該交換器正在啟動 VRRP 協定或上行鏈路狀態顯示故障 |
| Priority | 顯示清單的交換器VRRP優先級(1-255) |
| Advertise | 顯示交換器VRRP的通告間隔 |
| Preempt | 顯示交換器VRRP搶佔模式的啟用或停用狀態 |
| Delay | 顯示交換器VRRP搶佔模式的搶佔延遲時間 |




- **Interface :** 選擇 VLAN 介面。
- **Router ID :** 為建立的 VRRP 清單選擇虛擬路由器編號(1-5)。
  一個網路最多可以設定 5 個虛擬路由器。
- **Virtual IP :** 輸入虛擬路由器的 IP 位址。
- **Priority :** 輸入數字(1-254)來設定優先級。數字越大，優先級越高。預設值為 100。

| Note | 設定優先級 ( 1 - 254 ) 來決定在主路由器發生故障時由哪個備援路由器代替。主路由將由具有最高優先級的備份路由器接管。 |
|---|---|

- **Advertise :** 指定通告報文傳輸之間的間隔秒數。預設值為 1。參與虛擬路由器的所有路由器必須使用相同的通告間隔。

| Note | 主路由器發送通告報文，讓其他備援路由器知道它仍在正常運作。發送通告報文的時間間隔就是通告間隔。 |
|---|---|

- **Preempt :** 選中該選項可啟用搶佔模式。
- **Delay :** 輸入延遲時間(1-255)。

| Note | 如果主路由器不可用，則備援路由器將扮演主路由器的角色。然而，如果備援路由器的優先級比當前主路由器的優先級高，則主動將自己切換成主路由器。停用搶佔模式以防止這種情況發生。<br>無論搶佔模式如何，將虛擬路由器 IP 位址作為真實接口地址的第三層設備都將成為主路由器。 |
|---|---|

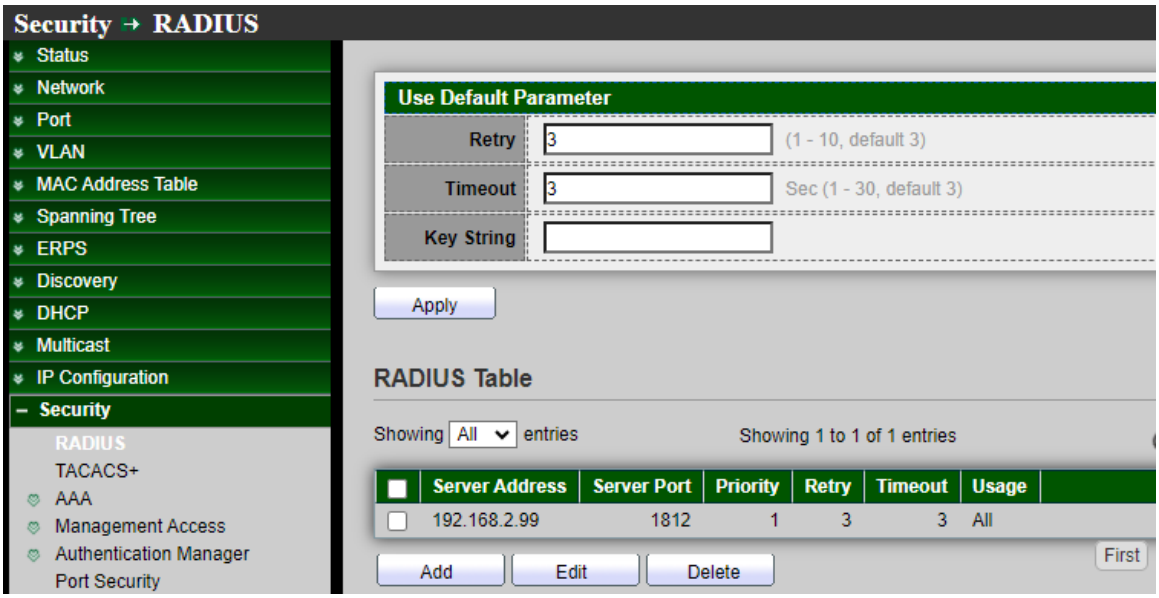
*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

# 14. Security

## 14.1 遠端使用者撥入驗證服務(RADIUS)

網路架構可以建立遠端使用者撥入驗證服務(RADIUS,Remote Authentication Dial In User Service)伺服器，為其所有設備提供集中式 802.1X 或基於 MAC 的網路訪問控制。此交換器可以充當 RADIUS 客戶端，使用 RADIUS 伺服器來提供集中式安全性、授權以及使用者身份驗證。

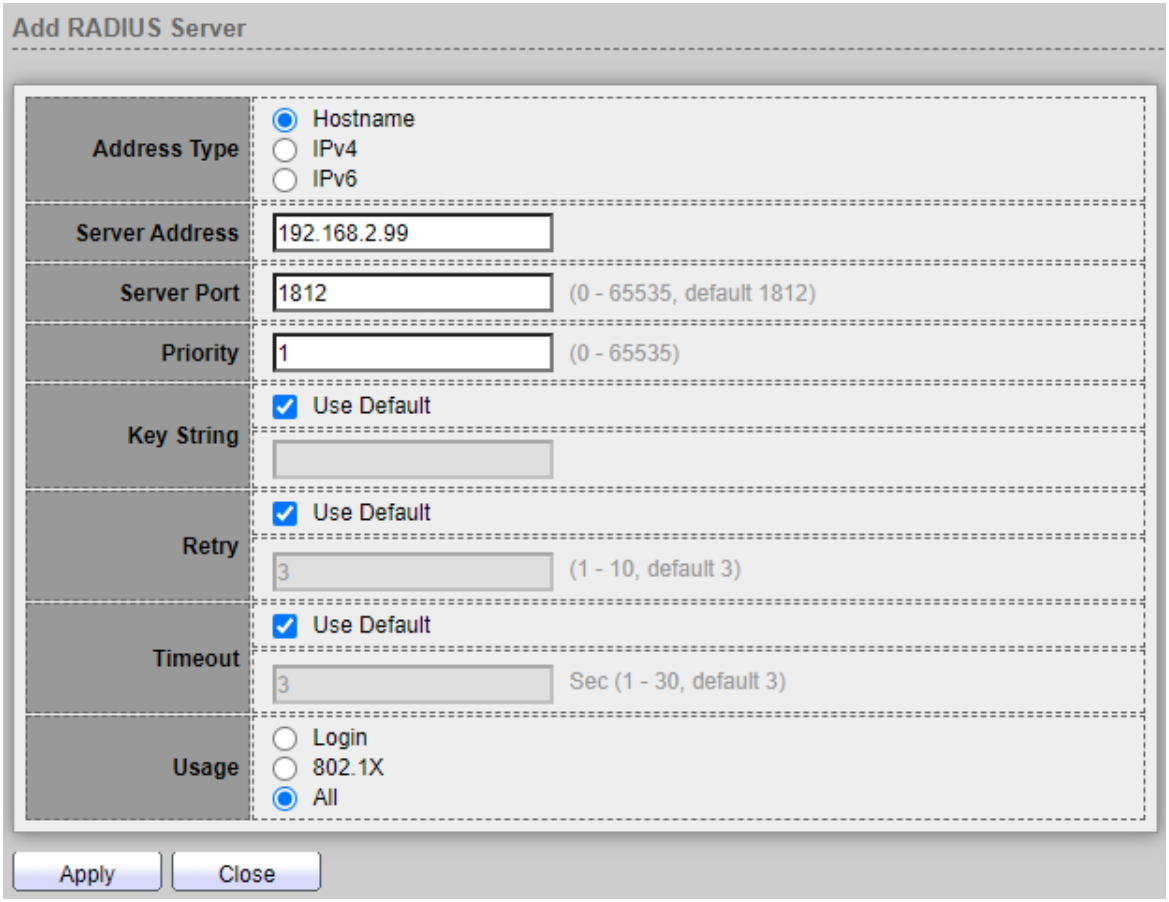
使用者管理員可以在 RADIUS 伺服器設定交換器的帳戶，並在 RADIUS 頁面設定 RADIUS 伺服器以及其它參數。




- **Use Default Parameters :**
  - **Retry :** 設定預設重試次數，輸入在認為發生故障之前，可向 RADIUS 伺服器發送的傳送請求次數。預設值為 3。
  - **Timeout :** 設定預設超時值，輸入交換器在重試查詢或切換到下一個伺服器之前，等待 RADIUS 伺服器應答的秒數。預設值為 3。
  - **Key String :** 設定預設的 RADIUS 密鑰字串，該密鑰字串用於交換器與 RADIUS 伺服器之間透過 MD5 進行安全通訊。該密鑰必須與 RADIUS 伺服器上設定的密鑰一致，如果沒有加密的密鑰字串（來自其他裝置），請以輸入明文形式的密鑰字串。

*點擊"Apply"儲存您的變更設定。*

| 欄位 | 描述 |
|---|---|
| Server Address | RADIUS伺服器位址 |
| Server Port | RADIUS伺服器連接埠 |
| Priority | RADIUS伺服器優先級別(值越小優先級別越高)。RADIUS會話將嘗試與具有最高優先級別的伺服器建立連接。如果失敗，它將嘗試連接到下一個更高優先值的伺服器 |
| Retry | RADIUS伺服器重試值。如果連接伺服器失敗，它將繼續嘗試，直到重試次數超過為止 |
| Timeout | RADIUS伺服器超時值。重傳或切換到下一個伺服器之前等待RADIUS伺服器回應的秒數 |
| Usage | RADIUS伺服器使用類型<br>• **Login :** 用於登錄驗證<br>• **802.1x :** 用於802.1x身份驗證<br>• **All :** 用於所有類型 |

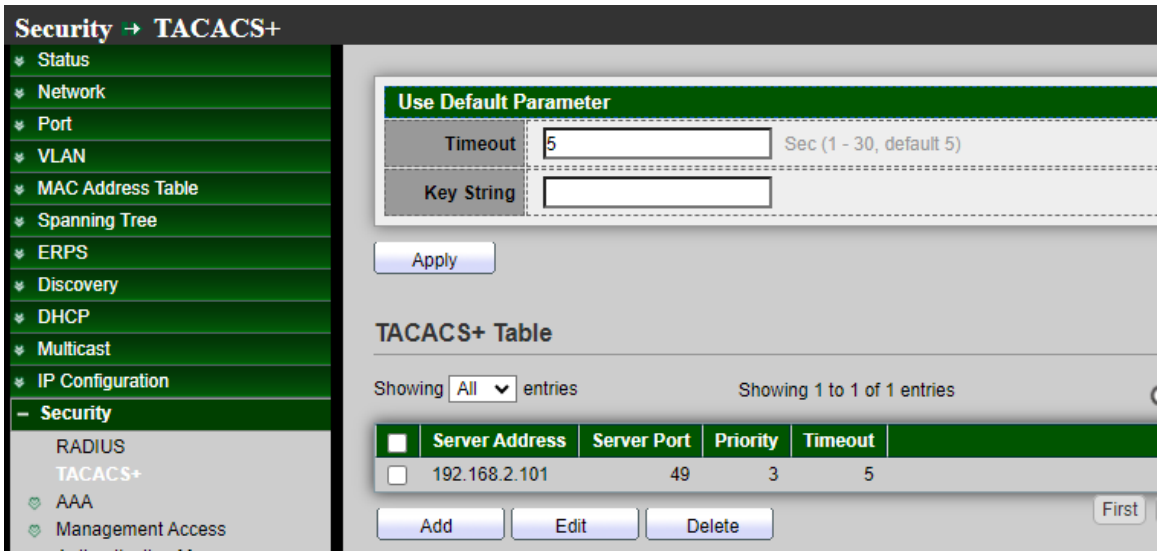


- **Address Type :** 可選擇 IPv4/IPv6 或主機名稱，在 “Add” 對話框中，使用者需要指定伺服器位元址類型：
  - **Hostname :** 使用網域名稱作為伺服器位址。
  - **IPv4 :** 使用 IPv4 作為伺服器位址。
  - **IPv6 :** 使用 IPv6 作為伺服器位址。
- **Server Address :** 請輸入 RADIUS 伺服器的 IP 位址或主機名稱。在 “Add” 對話框中，使用者需要根據位元址類型輸入伺服器位址。在 “Edit” 對話框中，顯示目前編輯伺服器位址。
- **Server Port :** 設定 RADIUS 伺服器的連接埠。
- **Priority :** 使用者管理員可以輸入伺服器的優先級別。優先級別決定交換器嘗試聯繫伺服器以驗證使用者身份的順序。交換器首先從優先級別最高的伺服器開始。0 為最高優先級，設定 RADIUS 伺服器優先級別(值越小優先權越高)。RADIUS 會話將嘗試與具有最高優先級別的伺服器設定建立。如果失敗，它將嘗試連接到下一個更高優先值的伺服器。
- **Key String :** 使用者管理員可以選擇 User Defined 的輸入加密或明文密鑰字串形式，用於對交換器和 RADIUS 伺服器之間的通訊進行身份驗證和加密。此密鑰必須與 RADIUS 伺服器上設定的密鑰相符。如果使用者管理員選擇 Use Default (選中複選框)將使用預設密鑰字串。
- **Retry :** 選擇 User Defined 以輸入在認為發生故障之前，可向 RADIUS 伺服器發送的請求次數，或選擇 Use Default 以使用預設值。
- **Timeout :** 選擇 User Defined 以輸入交換器在重試查詢或切換到下一個伺服器之前，等待 RADIUS 伺服器應答的秒數，或選擇 Use Default 以使用預設值。
- **Usage :** 選擇 RADIUS 伺服器身份驗證類型。
  - **Login :** RADIUS 伺服器用於對想要管理交換器的使用者進行身份驗證。
  - **802.1X :** RADIUS 伺服器用於 802.1X 訪問控制中的認證。
  - **All :** RADIUS 伺服器用於對想要管理交換器的使用者進行身份驗證，並用於 802.1X 訪問控制中的身份驗證。

*點擊**"Apply"**儲存您的變更，或**"Close"**關閉設定。*

## 14.2 終端訪問控制器訪問控制系統加(TACACS+)

使用者管理員可以設定 TACACS+來連接 TACACS+伺服器，為組織中的所有設備提供身份驗證和授權。此頁面允許使用者新增、編輯或刪除 TACACS+伺服器設定，以及修改 TACACS+伺服器的預設參數。



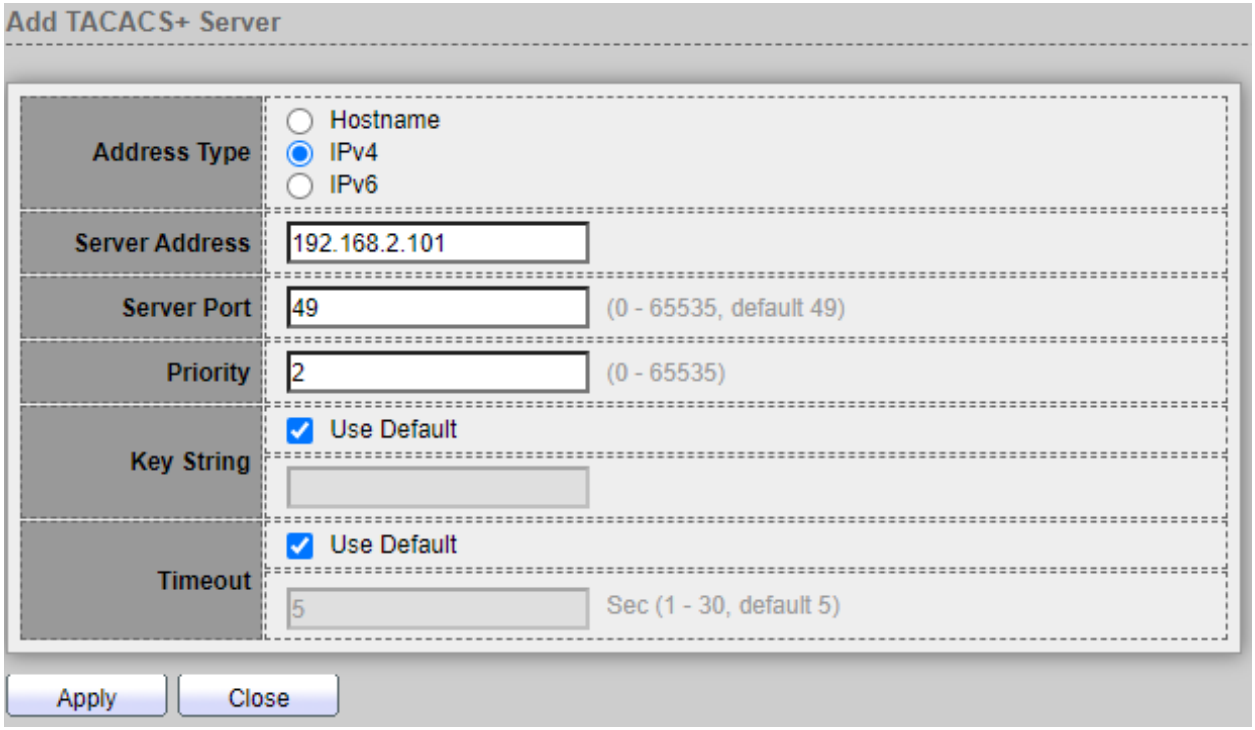

- **Use Default Parameters :**
  - **Timeout :** 輸入交換器與 TACACS+伺服器之間的連接超時前經過的時間(以秒為單位)。如果沒有為單一伺服器輸入值，則從該欄位中取值，預設值為 5。
  - **Key String :** 輸入加密或明文形式的預設密鑰字串，用於與所有 TACACS+伺服器通訊。

| Note | 如果使用者管理員未在此輸入預設密鑰字串，則在 Add 頁面上輸入的密鑰必須與 TACACS+伺服器使用的密鑰相符，或在此處輸入預設密鑰字串和為單一 TACACS+伺服器的密鑰字串，則為單一 TACACS+伺服器設定的密鑰字串優先。 |
|---|---|

*點擊"Apply"儲存您的變更設定。.*

| 欄位 | 描述 |
|---|---|
| Server Address | TACACS+伺服器位址 |
| Server Port | TACACS+伺服器連接埠 |

| | |
|---|---|
| Priority | TACACS+伺服器優先級別(值越小優先級別越高)。TACACS+會話將嘗試與具有最高優先級別的伺服器建立連接。如果失敗，它將嘗試連接到下一個更高優先值的伺服器 |
| Timeout | TACACS+伺服器超時值。如果連接伺服器失敗，它將等待，直到超時時間結束 |




- **Address Type :** 可選擇 IPv4/IPv6 或主機名稱，在 “Add” 對話框中，使用者需要指定伺服器位元址類型：
  - **Hostname :** 使用網域名稱作為伺服器位址。
  - **IPv4 :** 使用 IPv4 作為伺服器位址。
  - **IPv6 :** 使用 IPv6 作為伺服器位址。
- **Server Address :** 在 “Add” 對話框中，使用者需要根據位元址類型輸入伺服器位址。在 “Edit” 對話框中，顯示目前編輯伺服器位址。
- **Server Port :** 設定 TACACS+伺服器的連接埠。
- **Priority :** 使用者管理員可以輸入伺服器的優先級別。優先級別決定交換器嘗試聯繫伺服器以驗證使用者身份的順序。交換器首先從優先級別最高的伺服器開始。0 為最高優先級別，設定 TACACS+伺服器優先級別(值越小優先權越高)。TACACS+會話將嘗試與具有最高優先級別的伺服器設定建

立。如果失敗，它將嘗試連接到下一個更高優先值的伺服器。

- **Key String :** 使用者管理員可以選擇使用者定義的輸入加密或明文密鑰字串形式，用於對交換器和TACACS+伺服器之間的通訊進行身份驗證和加密。此密鑰必須與 TACACS+伺服器上設定的密鑰相符。如果使用者管理員選擇 Use Default(選中複選框)將使用預設密鑰字串。
- **Timeout :** 設定 TACACS+伺服器超時值。如果連接伺服器失敗，它將繼續嘗試，直到超時時間結束。

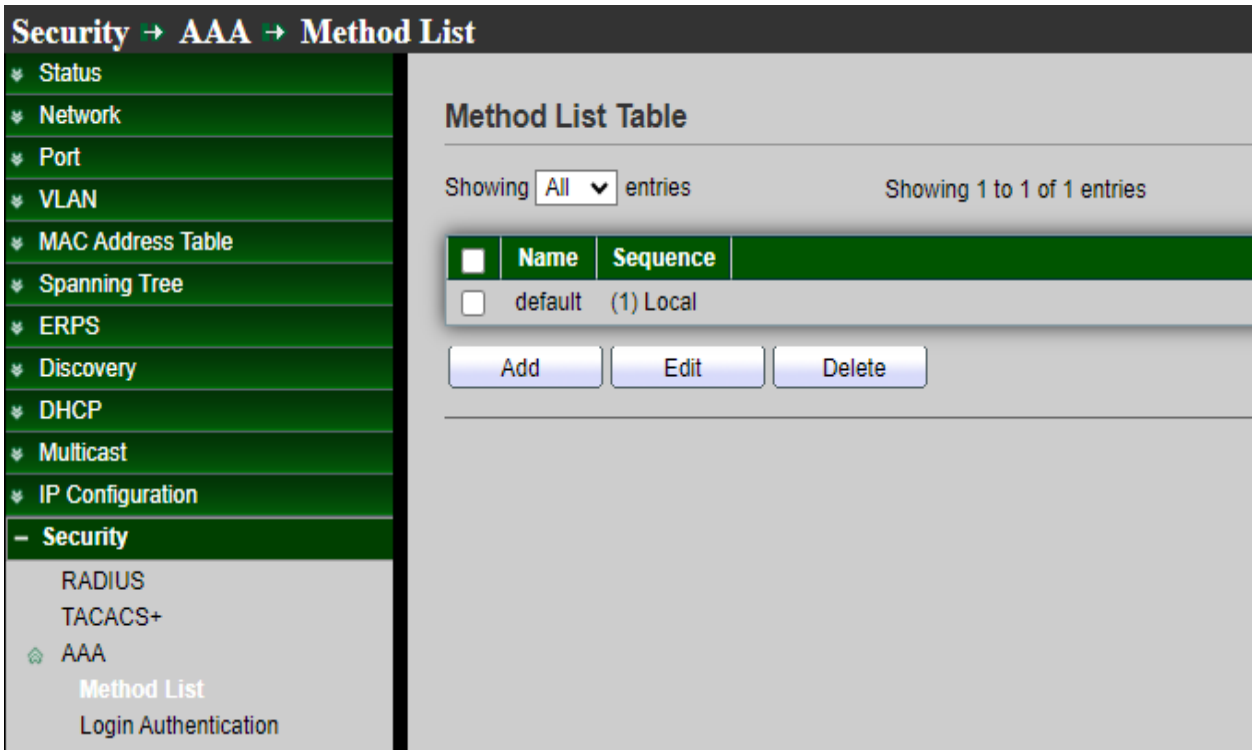
*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

# 14.3 AAA

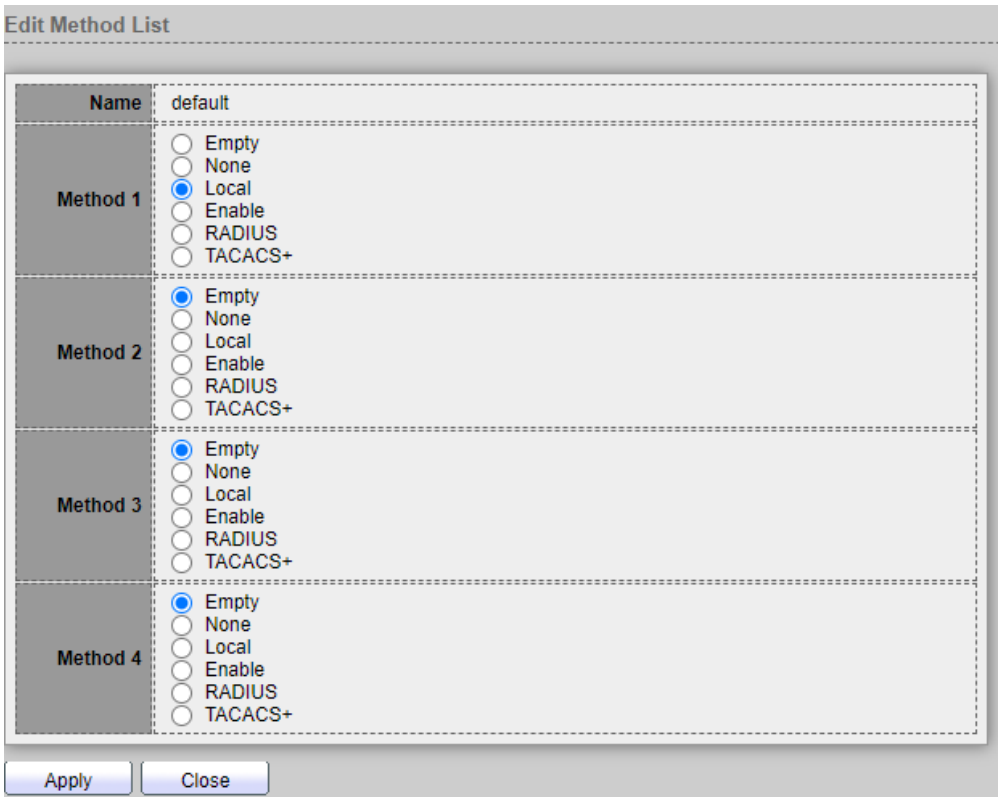
## 14.3.1 方法列表(Method List)

使用者管理員可以設定 AAA 安全群組，每組有 4 個方法表，每個方法可以從 6 種類型中選擇一種，其中包含 Empty / None /Local/ Enable/ RADIUS/TACACS+。

此頁面允許使用者新增、編輯或刪除登錄驗證列表設定(“default”列表無法刪除)。組合到此行的列表將透過列表中的方法對登錄使用者進行身份驗證。如果第一種方法失敗，它將嘗試使用下一個優先方法來驗證是否存在。對於 RADIUS 和 TACACS+方法，失敗表示連接伺服器失敗。對於 Local 方法，失敗表示在本地資料庫中找不到該使用者。




| 欄位 | 描述 |
|---|---|
| Name | 登錄驗證列表名稱。該名稱應與其他現有列表名稱不能重復 |
| Sequence | 登錄驗證方法的優先級別<br>• None：任何情況下都經過驗證<br>• Local：使用本地帳戶資料庫進行身份驗證<br>• TACACS+：使用遠程TACACS+伺服器進行身份認證<br>• RADIUS：使用遠程RADIUS伺服器進行身份認證<br>• Enable：使用本地啟用密碼進行身份驗證 |

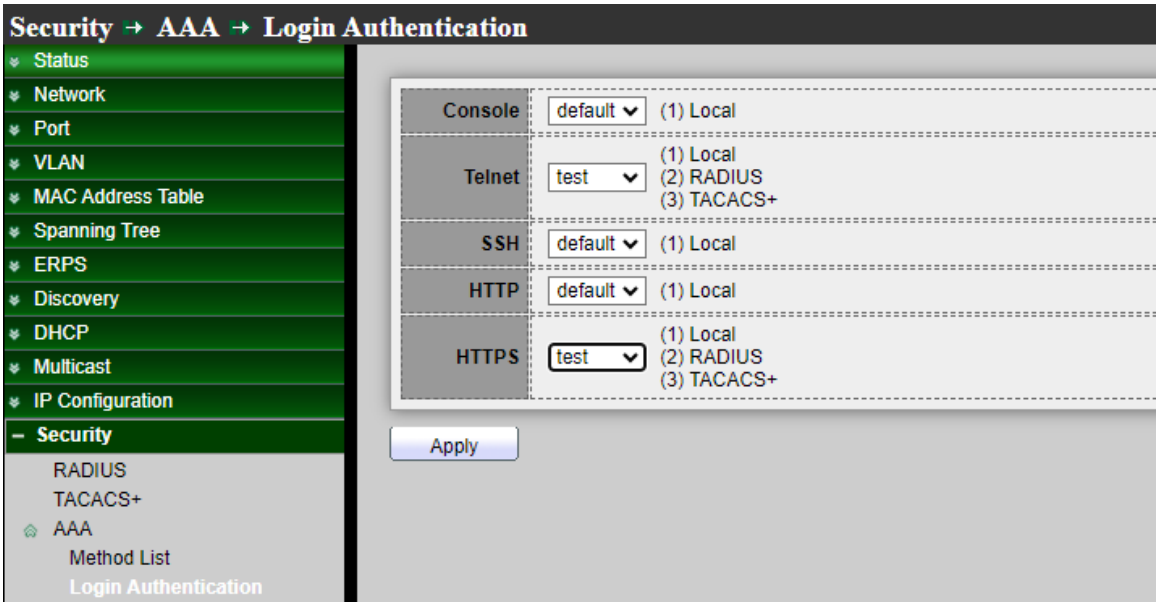



- **Name :** 登錄驗證列表名稱。該名稱應與其他現有列表名稱不能重復。
- **Method 1/2/3/4 :** 選擇登錄認證方法的優先級別。
  - **None :** 任何情況下都經過驗證。
  - **Local :** 使用本地帳戶資料庫進行身份驗證。
  - **TACACS+ :**使用遠程 TACACS+伺服器進行身份認證。
  - **RADIUS :** 使用遠程 RADIUS 伺服器進行身份認證。
  - **Enable :** 使用本地啟用密碼進行身份驗證。

*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

### 14.3.2 登錄認證(Login Authentication)

當使用者管理員在"AAA➔Method List"建立了安全群組後，使用者管理員可以在服務連接埠中選擇不同的安全群組。



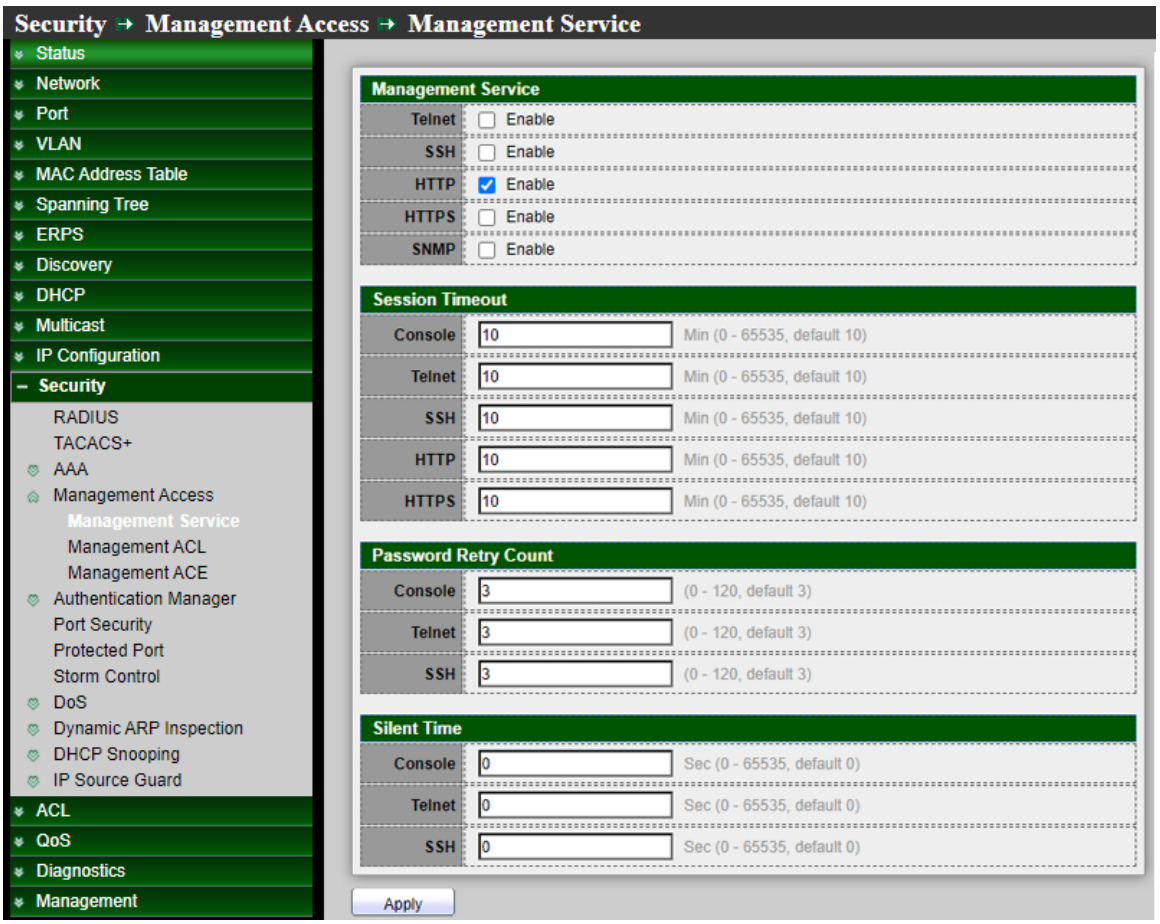

| 欄位 | 描述 |
|---|---|
| Console | 指定控制台的登錄認證列表組合 |
| Telnet | 指定Telnet的登錄認證列表組合 |
| SSH | 指定SSH的登錄認證列表組合 |
| HTTPS | 指定HTTPS的登錄認證列表組合 |

*點擊"Apply"儲存您的變更設定。*

# 14.4 管理訪問(Management Access)

## 14.4.1 管理服務(Management Service)

使用者管理員可以選擇啟用 Telnet / SSH / HTTP / HTTPS / SNMP 等不同協定的登錄服務，並設定登錄超時限制和密碼錯誤重試次數限制。




- **Management Service :** 管理服務的管理狀態。
  - **Telnet :** 透過 telnet 服務訪問 CLI。
  - **SSH :** 透過 SSH 服務訪問 CLI。
  - **HTTP :** 透過 HTTP 服務訪問 WEBUI。
  - **HTTPS :** 透過 HTTPS 服務訪問 WEBUI。
  - **SNMP :** 透過 SNMP 服務管理交換器。
- **Session Timeout :** 設定使用者訪問使用者介面的會話超時分鐘數。0 分鐘表示永不超時。登錄管理頁面後，在設定的時間內如果沒有會話，則系統將自動超時，使用者管理員需要重新登錄。
  - **Console :** 設定控制台會話超時 0~65535 分鐘。
  - **Telnet :** 設定 Telnet 會話超時 0~65535 分鐘。
  - **SSH :** 設定 SSH 會話超時 0~65535 分鐘。
  - **HTTP :** 設定 HTTP 會話超時 0~65535 分鐘。
  - **HTTPS :** 設定 HTTPS 會話超時 0~65535 分鐘。
- **Password Retry Count :** 重試次數是 CLI 密碼輸入容錯次數。輸入錯誤密碼超過此次數後，CLI

將在靜默時間後凍結，如果登錄錯誤次數達到設定值，登錄頁面將被踢出，使用者管理員需要重新打開登錄頁面。

- **Console :** 設定控制台密碼重試次數 0~120 次。
- **Telnet :** 設定 Telnet 密碼重試次數 0~120 次。
- **SSH :** 設定 SSH 密碼重試次數 0~120 次。

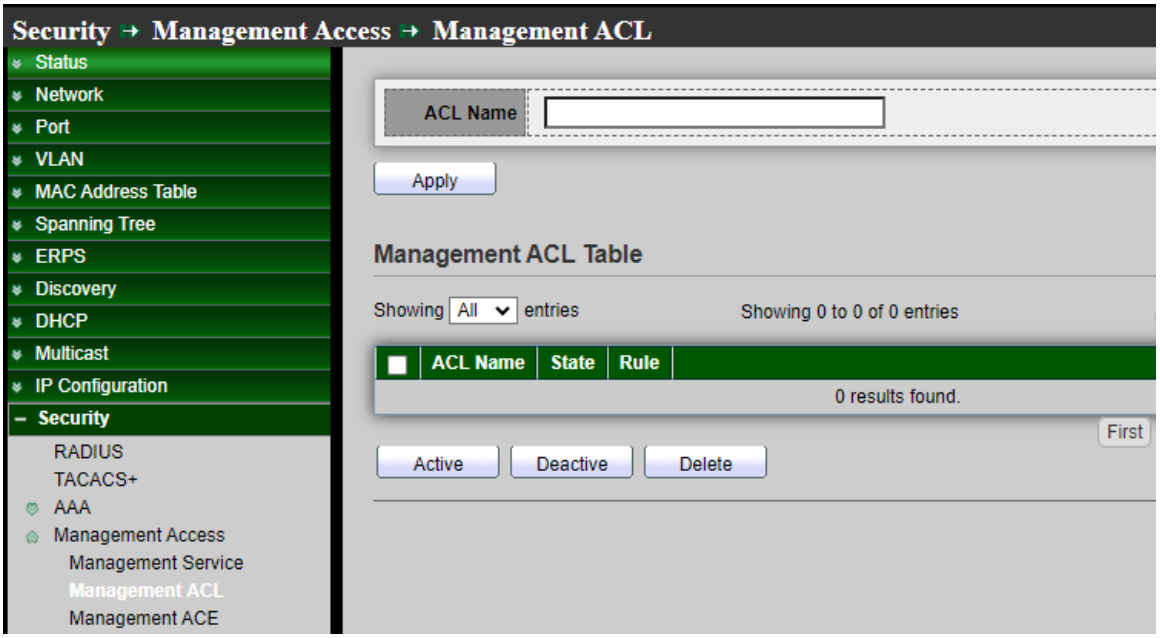
➢ **Silent Time :** 功能需配合"Password Retry Count"功能，如果登錄錯誤次數到達設定值，則在設定的靜默時間內將無法重新打開登錄頁面，直到設定時間結束。輸入錯誤密碼超過密碼重試次數後，CLI 將在靜默時間後凍結。

- **Console :** 設定控制台靜默時間 0~65535 分鐘。
- **Telnet :** 設定 Telnet 靜默時間 0~65535 分鐘。
- **SSH :** 設定 SSH 靜默時間 0~65535 分鐘。

### 14.4.2 管理訪問控制表(Management ACL)

使用者管理員可以創建訪問控制表(Access Control List，ACL)並設定規則的啟用或禁用。
如果使用者管理員設定"Active"，則會應用"Management ACE"規則。ACL 可以設定哪些連接埠允許或拒絕連接交換器管理介面的哪些服務。

| | |
|---|---|
| Note | 如果創建 ACL 設定檔並點擊"Active"，則所有連接埠和服務都將被拒絕。 |




➢ **ACL Name :** 輸入 MAC ACL 名稱。

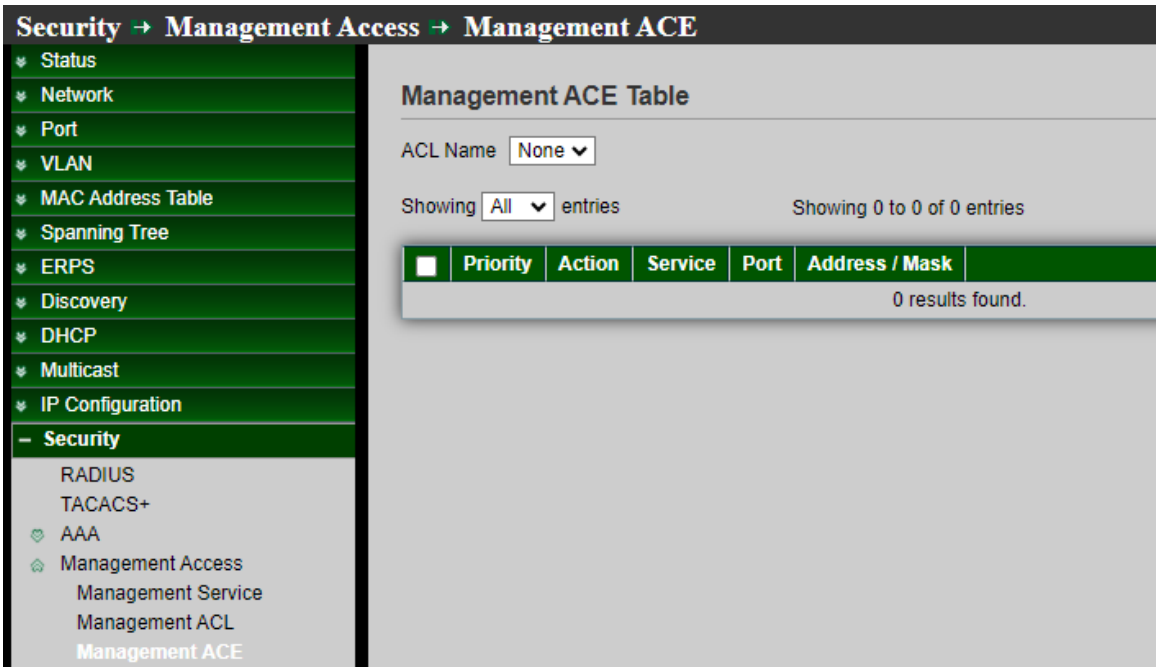
*點擊"Apply"儲存您的變更設定。*

| 欄位 | 描述 |
|---|---|
| ACL Name | 顯示管理ACL名稱 |
| State | 顯示管理ACL是否啟用 |
| Rule | 顯示ACL的管理ACE規則編號 |

*設定"Active"、"Deactive"和"Delete"對此表進行管理。*

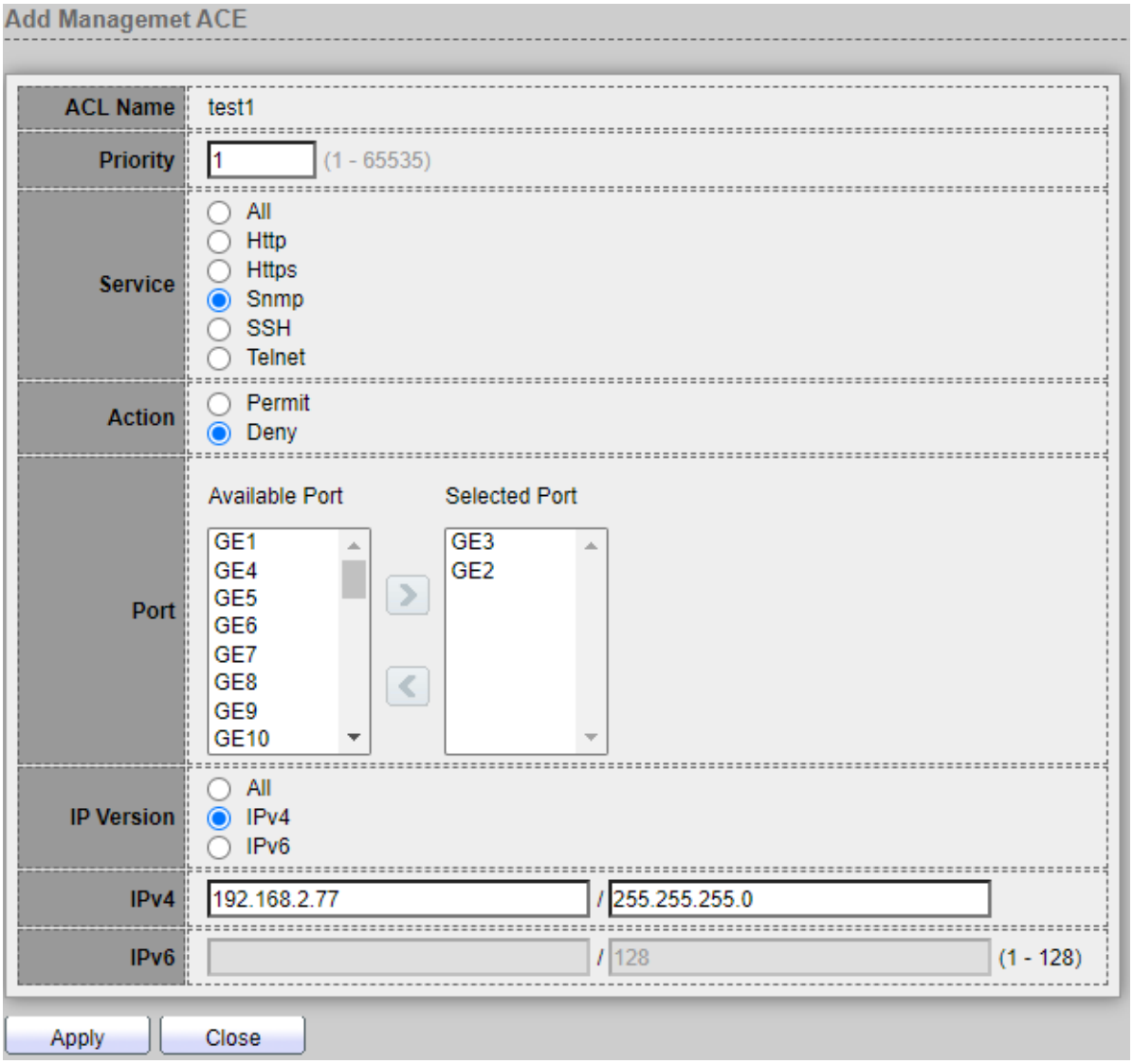
### 14.4.3 管理訪問控制清單(Management ACE)

此管理 ACE 頁面用於創建 ACL 設定檔規則。使用者管理員可以選擇已創建的 ACL 設定檔來設定安全規則。如果設定 ACE 只能使用 Telnet 單一規則。確認後，該規則將應用於 ACL 設定檔。
使用者管理員可以進入“management ACL”頁面並點擊“Active”來啟用規則。啟用規則後，此管理頁面將無法操作，只能使用 Telnet 協定進行管理，設定“**add**”、“**Edit**”和“**Delete**”功能進行管理。




➢ **ACL Name :** 選擇要要新增 ACE 的 ACL 名稱。

| 欄位 | 描述 |
|---|---|
| Priority | 顯示ACE優先級比別 |
| Action | 顯示ACE操作 |
| Service | 顯示ACE服務 |
| Port | 顯示ACE連接埠列表 |
| Address / Mask | 顯示ACE的來源IP位址和遮罩 |




- **ACL Name**：顯示要新增 ACE 的 ACL 名稱。
- **Priority**：設定此規則優先級別，指定 ACE 的優先級別。順序較高的 ACE 優先處理( 1 是最高優先級別)。僅適用於 “Add” 對話框。
- **Service**：選擇規則的服務類型。
  - **All**：所有服務。
  - **HTTP**：僅 HTTP 服務。
  - **HTTPs**：僅 HTTPS 服務。
  - **SNMP**：僅 SNMP 服務。
  - **SSH**：僅 SSH 服務。
  - **Telnet**：僅 Telnet 服務。
- **Action**：選擇 ACE 匹配封包後的操作。

- **Permit**：轉發符合 ACE 標準的封包。
- **Deny**：丟棄符合 ACE 標準的封包。

➢ **Port**：選擇要匹配的連接埠。

➢ **IP Version**：選擇來源 IP 位址類型。

- **All**：所有 IP 位址均可訪問。
- **IPv4**：指定 IPv4 位址可訪問。
- **IPv6**：指定 IPv4 位址可訪問。

➢ **IPv4**：輸入要匹配的來源 IPv4 位址值和遮罩。

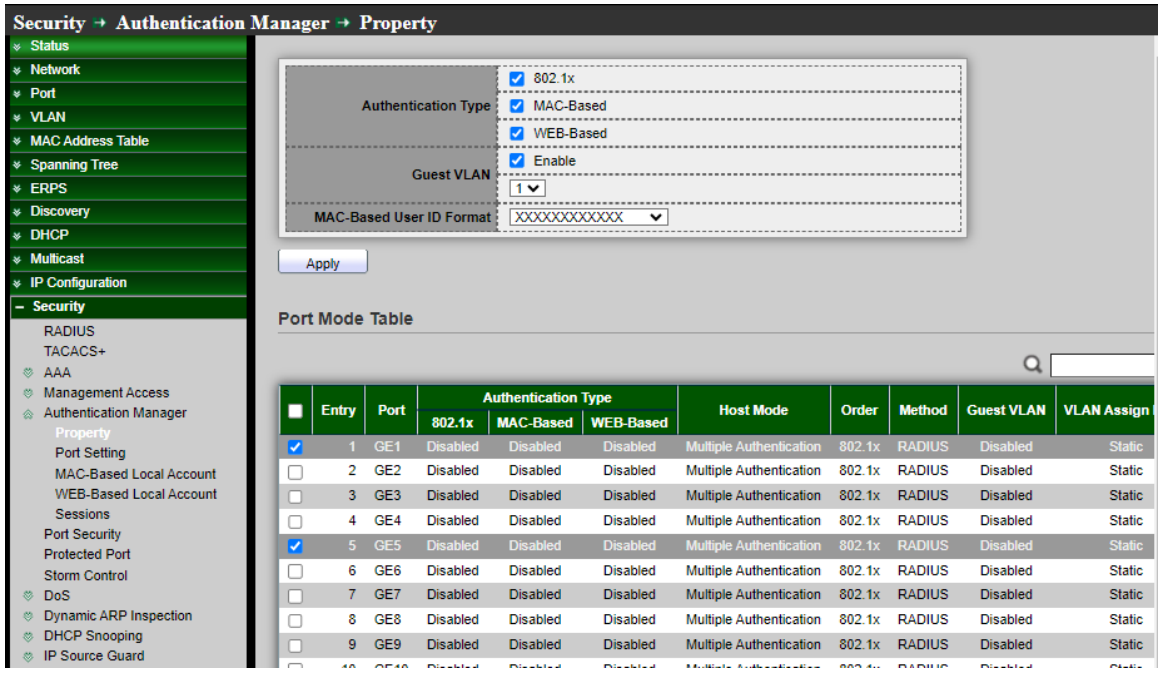
➢ **IPv6**：輸入要匹配的來源 IPv6 位址值和遮罩。

*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

# 14.5 身份認證管理器(Authentication Manager)

## 14.5.1 屬性(Property)

此頁面允許使用者管理員編輯身份驗證全域設定和一些連接埠模式的設定。




➢ **Authentication Type**：點選複選框以啟用/停用以下身份驗證類型：

- 802.1x：使用 IEEE 802.1x 進行身份驗證。
- MAC-Based：使用 MAC 位址進行身份驗證。

- WEB-Based : 提示認證網頁，供使用者進行驗證。

➢ **Guest VLAN :** 設定複選框以啟用/停用訪客 VLAN，如果啟用訪客 VLAN，則需要選擇一個可用的 VLAN ID 作為訪客 VID。

➢ **MAC-Based User ID Format :** 選擇基於 mac 的身份驗證 RADIUS 使用者名稱/密碼 ID 格式。

- XXXXXXXXXXXX
- xxxxxxxxxxxx
- XX : XX : XX : XX : XX : XX
- xx : xx : xx : xx : xx : xx
- XX-XX-XX-XX-XX-XX
- xx-xx-xx-xx-xx-xx
- XX.XX.XX.XX.XX.XX
- xx.xx.xx.xx.xx.xx
- XXXX : XXXX : XXXX
- xxxx : xxxx : xxxx
- XXXX-XXXX-XXXX
- xxxx-xxxx-xxxx
- XXXX.XXXX.XXXX
- xxxx.xxxx.xxxx
- XXXXXX : XXXXXX
- xxxxxx : xxxxxx
- XXXXXX-XXXXX
- xxxxxx-xxxxxx

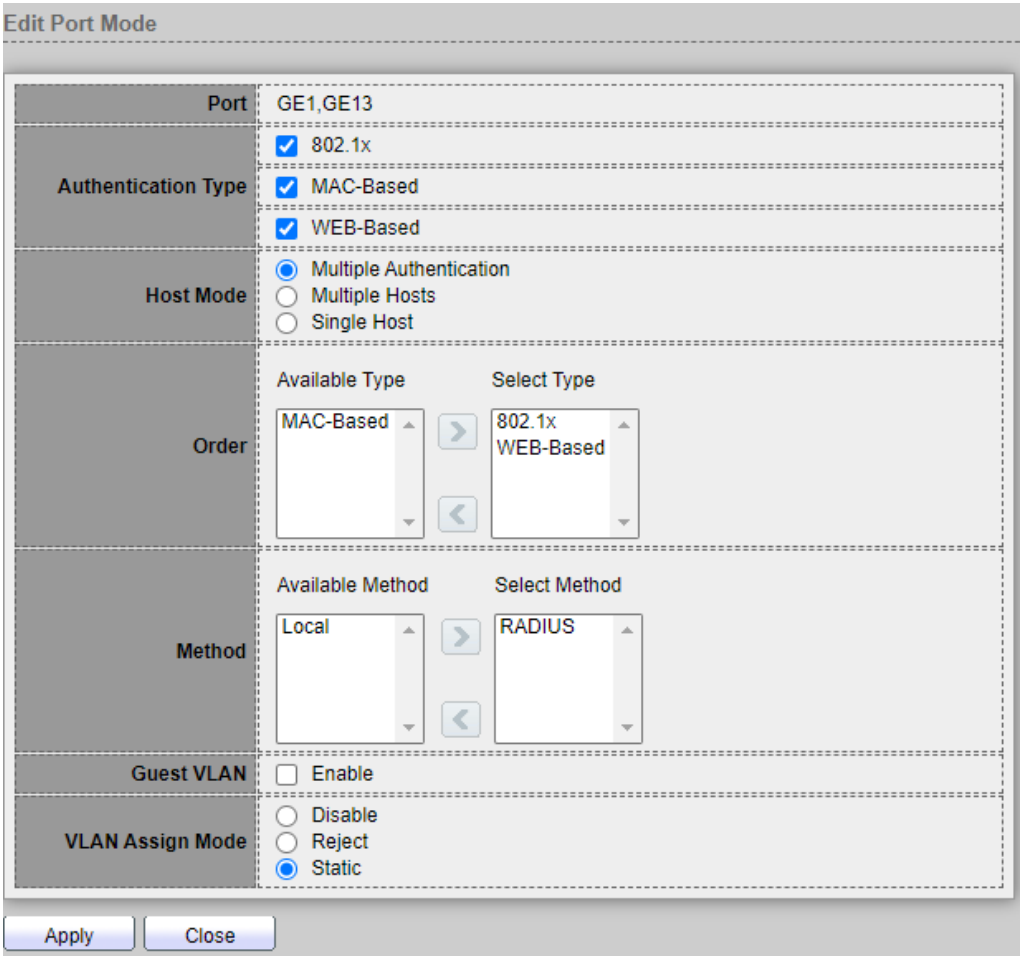
*點擊"Apply"儲存您的變更設定。*

Port Mode Table

| Entry | Port | Authentication Type | | | Host Mode | Order | Method | Guest VLAN | VLAN Assign Mode |
|---|---|---|---|---|---|---|---|---|---|
| | | 802.1x | MAC-Based | WEB-Based | | | | | |
| 1 | GE1 | Enabled | Enabled | Enabled | Multiple Authentication | 802.1x , WEB-Based | RADIUS , Local | Enabled | Disable |
| 2 | GE2 | Enabled | Enabled | Enabled | Multiple Authentication | 802.1x , WEB-Based | RADIUS , Local | Enabled | Disable |
| 3 | GE3 | Enabled | Enabled | Enabled | Multiple Authentication | 802.1x , WEB-Based | RADIUS , Local | Enabled | Disable |
| 4 | GE4 | Enabled | Enabled | Enabled | Multiple Authentication | 802.1x , WEB-Based | RADIUS , Local | Enabled | Disable |
| 5 | GE5 | Disabled | Disabled | Disabled | Multiple Authentication | 802.1x | RADIUS | Disabled | Static |
| 6 | GE6 | Disabled | Disabled | Disabled | Multiple Authentication | 802.1x | RADIUS | Disabled | Static |
| 7 | GE7 | Disabled | Disabled | Disabled | Multiple Authentication | 802.1x | RADIUS | Disabled | Static |
| 8 | GE8 | Disabled | Disabled | Disabled | Multiple Authentication | 802.1x | RADIUS | Disabled | Static |
| 9 | GE9 | Disabled | Disabled | Disabled | Multiple Authentication | 802.1x | RADIUS | Disabled | Static |

| 欄位 | 描述 |
|---|---|
| Port | 連接埠名稱 |
| Authentication Type (802.1X) | 802.1X認證類型狀態<br>• **Enabled** : 802.1X已啟用<br>• **Disabled** : 802.1X已禁用 |
| Authentication Type (MAC-Based) | 基於MAC身份驗證類型狀態<br>• **Enabled** : 基於MAC身份驗證已啟用<br>• **Disabled** : 基於MAC身份驗證已禁用 |
| Authentication Type (WEB-Based) | 基於網頁身份驗證類型狀態<br>• **Enabled** : 基於網頁身份驗證已啟用<br>• **Disabled** : 基於網頁身份驗證已禁用 |
| Host Mode | 驗證主機模式<br>• **Multiple Authentication** : 在這種模式下，每個客戶端都需要單獨通過身份驗證程式<br>• **Multiple Hosts** : 在這種模式下，只有一個客戶端需要進行身份驗證，其他用戶端將獲得相同的訪問權限。在此模式下無法啟用Web驗證<br>• **Single Host** : 在這種模式下，只允許一台主機進行認證。它與多重身份驗證模式相同，最大主機數設定為1 |

| | |
|---|---|
| Order | 支援以下認證類型順序組合。網路身份驗證應始終是最後一種類型<br>如果目前類型未啟用或驗證失敗，驗證管理器將轉到下一個類型<br>• 802.1x<br>• MAC-Based<br>• WEB-Based<br>• 802.1x MAC-Based<br>• 802.1x WEB-Based<br>• MAC-Based 802.1x<br>• WEB-Based 802.1x<br>• 802.1x MAC-Based WEB-Based<br>• 802.1x WEB-Based MAC-Based |
| Method | 支援以下認證方法順序組合。這些命令僅適用於基於MAC的身份驗證和基於WEB的身份驗證。 802.1x僅支援RADIUS方法<br>• **Local :** 使用DUT的本地資料庫進行認證<br>• **Radius :** 使用遠端RADIUS伺服器進行身份驗證 |
| Guest VLAN | 連接埠訪客VLAN啟用狀態<br>• **Enabled :** 連接埠的訪客VLAN已啟用<br>• **Disabled :** 連接埠的訪客VLAN已停用 |
| VLAN Assign Mode | 支援以下VLAN分配模式，僅當來源為RADIUS時適用<br>• **Disable :** 忽略VLAN授權結果，保留主機原始VLAN<br>• **Reject :** 如果取得VLAN授權訊息，則直接使用。但如果沒有VLAN授權訊息，則拒絕該主機，使其成為未授權的主機<br>• **Static :** 如果取得VLAN授權訊息，則直接使用。如果沒有VLAN授權訊息，則保留主機原始的VLAN |




- **Port :** 顯示選擇的連接埠編號。
- **Authentication Type :** 點選復選框來啟用/禁用認證類型。
  - **802.1x :** 使用 IEEE 802.1x 進行身份驗證。
  - **MAC-Based :** 使用 MAC 位址進行身份驗證。
  - **WEB-Based :** 提示認證網頁，供使用者進行驗證。
- **Host Mode :** 選擇驗證主機模式。
  - **Multiple Authentication :** 在這種模式下，每個客戶端都需要單獨通過身份驗證過程。
  - **Multiple Hosts :** 在這種模式下，只有一個客戶端需要進行身份驗證，其他用戶端將獲得相同的訪問權限。在此模式下無法啟用 Web 驗證。
  - **Single Host :** 在這種模式下，只允許一台主機進行認證。它與多重身份驗證模式相同，最大主機數設定為 1。
- **Order :** 支援以下認證類型順序組合。網路身份驗證應始終是最後一種類型。如果目前類型未啟用或驗證失敗，驗證管理器將轉到下一個類型。
  - 802.1x

- MAC-Based
- WEB-Based
- 802.1x MAC-Based
- 802.1x WEB-Based
- MAC-Based 802.1x
- WEB-Based 802.1x
- 802.1x MAC-Based WEB-Based
- 802.1x WEB-Based MAC-Based

➢ **Method :** 支援以下認證方法順序組合。這些命令僅適用於基於 MAC 的身份驗證和基於 WEB 的身份驗證。802.1x 僅支援 RADIUS 方法。

- **Local :** 用 DUT 的本地資料庫進行認證。
- **Radius :** 使用遠端 RADIUS 伺服器進行身份驗證。

➢ **Guest VLAN :** 點選復選框來啟用/禁用訪客 VLAN。

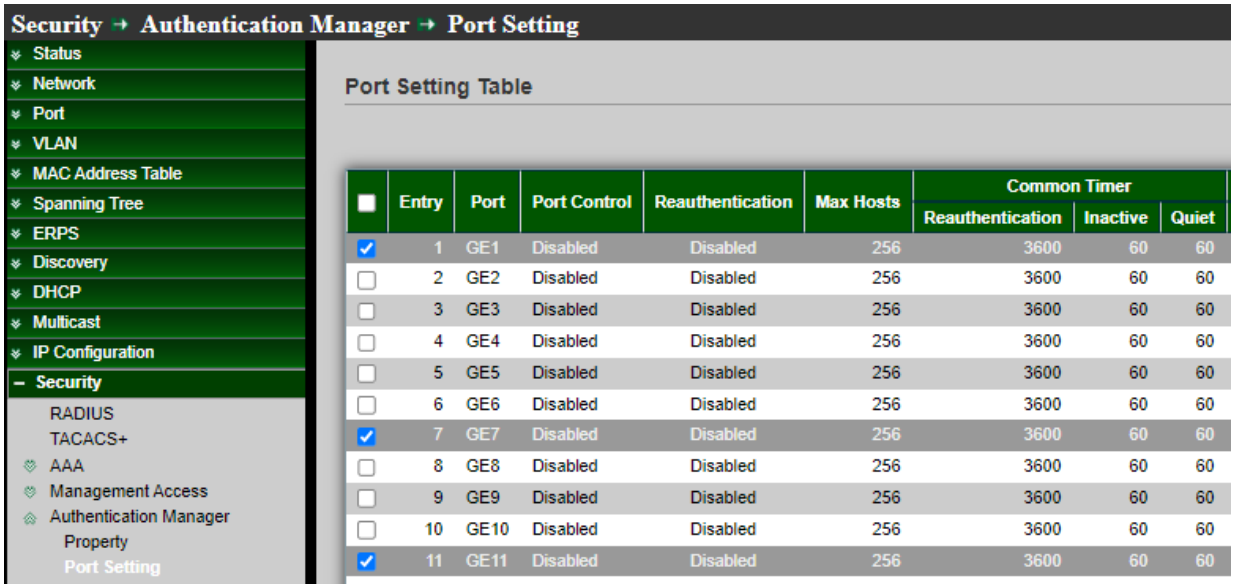
➢ **VLAN Assign Mode :** 支援以下 VLAN 分配模式，僅當來源為 RADIUS 時適用。

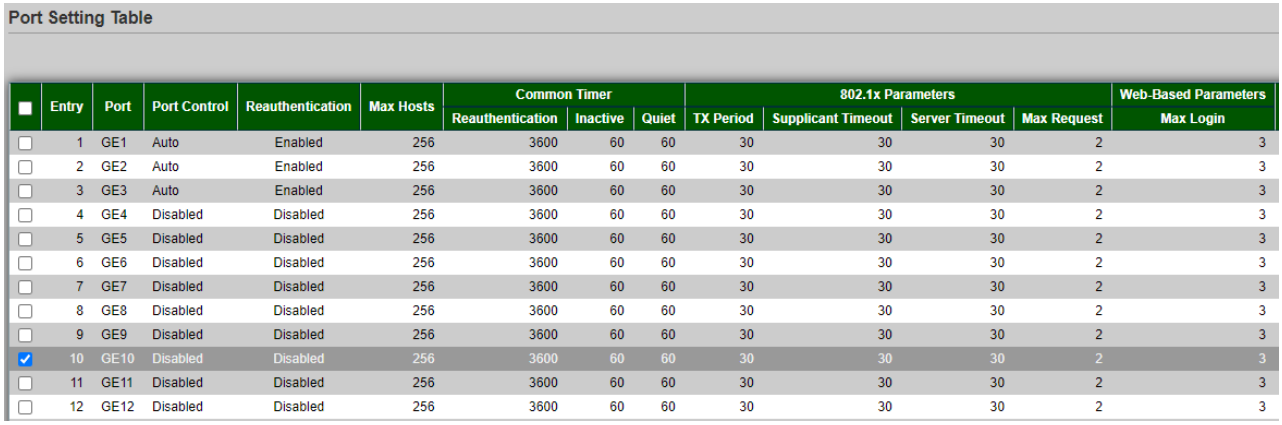
- **Disable**：忽略 VLAN 授權結果，保留主機原始 VLAN。
- **Reject**：如果取得 VLAN 授權訊息，則直接使用。但如果沒有 VLAN 授權訊息，則拒絕該主機，使其成為未授權的主機。
- **Static**：如果取得 VLAN 授權訊息，則直接使用。如果沒有 VLAN 授權訊息，則保留原始的 VLAN。

*點擊"**Apply**"儲存您的變更，或"**Close**"關閉設定。*

### 14.5.2 連接埠設定(Port Setting)

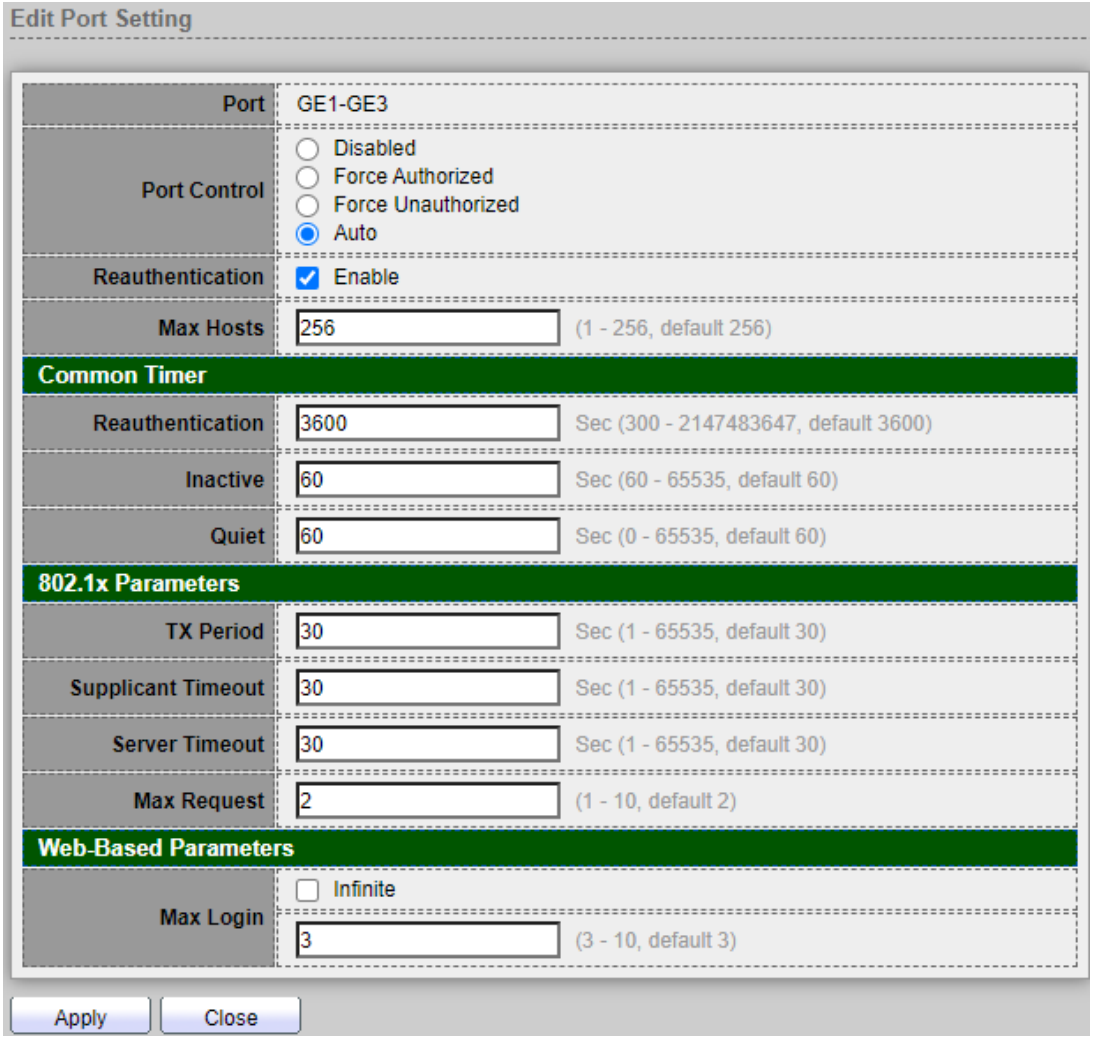
使用者管理員可以對認證管理器連接埠設定，此頁面允許使用者管理員對認證管理器連接埠設定。




| 欄位 | 描述 |
|---|---|
| Port | 連接埠名稱 |
| Port Control | 支援以下認證連接埠控制類型<br>• **Disable :** 停用認證功能並且所有用戶端都可以訪問網路<br>• **Force Authorized :** 連接埠強制授權並且所有用戶端都可做訪問網路<br>• **Force Unauthorized :** 連接埠強制未授權並且所有用戶端不能訪問網路<br>• **Auto :** 需要通過身份驗證過程和授權，用戶端才能訪問網路 |

| | |
|---|---|
| Reauthentication | 重新認證狀態<br>• **Enabled :** 重新驗證期限過後，主機需要重新進行驗證<br>• **Disabled :** 重新驗證期限過後，主機不需要重新進行驗證 |
| Max Hosts | 在多重認證模式下，主機總數不能超過最大主機數 |
| Common Timer | • **Reauthentication :** 重新認證期限過後，主機將恢復到初始狀態，需要再次通過認證過程<br>• **Inactive :** 如果沒有來自經過驗證的主機的封包，則非設定啟用的計時器將會增加。非設定啟用的超時後，主機將被視為未授權，相應的會話將被刪除。在多主機模式下，封包只計算授權主機，而不計入連接埠上的所有封包<br>• **Quiet :** 當連接埠多次認證失敗後處於Locked狀態時，主機將被封鎖在靜默期。靜默期過後，允許主機再次進行身份驗證 |
| 802.1X Params | • **TX Period :** 設備在重新發送請求前等待請求者(用戶端)回應可延伸身份驗證通訊協定(EAP)請求/身份訊框的秒數<br>• **Supplicant Timeout :** 向請求者重新發送EAP請求前經過的秒數<br>• **Server Timeout :** 交換器向身份認證伺服器重新發送請求前經過的秒數<br>• **Max Request :** 輸入可以傳送的最大EAP請求數。如果交換器在規定的時間(supplicant timeout)後沒有接收到回應，則重新啟動身份驗證過程 |
| Web-Based Param (Max Login) | 允許使用者登錄失敗的次數。登錄失敗次數超過後，主機將進入鎖定狀態，直到超過靜默期後才能進行身份驗證 |




- **Port :** 顯示選擇的連接埠編號。
- **Port Control :** 支援以下認證連接埠控制類型。
  - **Disable :** 停用認證功能並且所有用戶端都可以訪問網路。
  - **Force Authorized :** 連接埠強制授權並且所有用戶端都可做訪問網路。
  - **Force Unauthorized :** 連接埠強制未授權並且所有用戶端不能訪問網路。
  - **Auto :** 需要通過身份驗證過程和授權，用戶端才能訪問網路。
- **Reauthentication :** 設定復選框來啟用/停用重新認證狀態。
- **Max Hosts :** 在多重認證模式下，主機總數不能超過最大主機數。
- **Common Timer :**
  - **Reauthentication :** 重新認證期限過後，主機將恢復到初始狀態，需要再次通過認證過程。
  - **Inactive :** 如果沒有來自經過驗證的主機的封包，則非設定啟用的計時器將會增加。非設定啟用的超時後，主機將被視為未授權，相應的會話將被刪除。在多主機模式下，封包只

計算授權主機，而不計入連接埠上的所有封包。

- **Quiet :** 當連接埠多次認證失敗後處於 Locked 狀態時，主機將被封鎖在靜默期。靜默期過後，允許主機再次進行身份驗證。

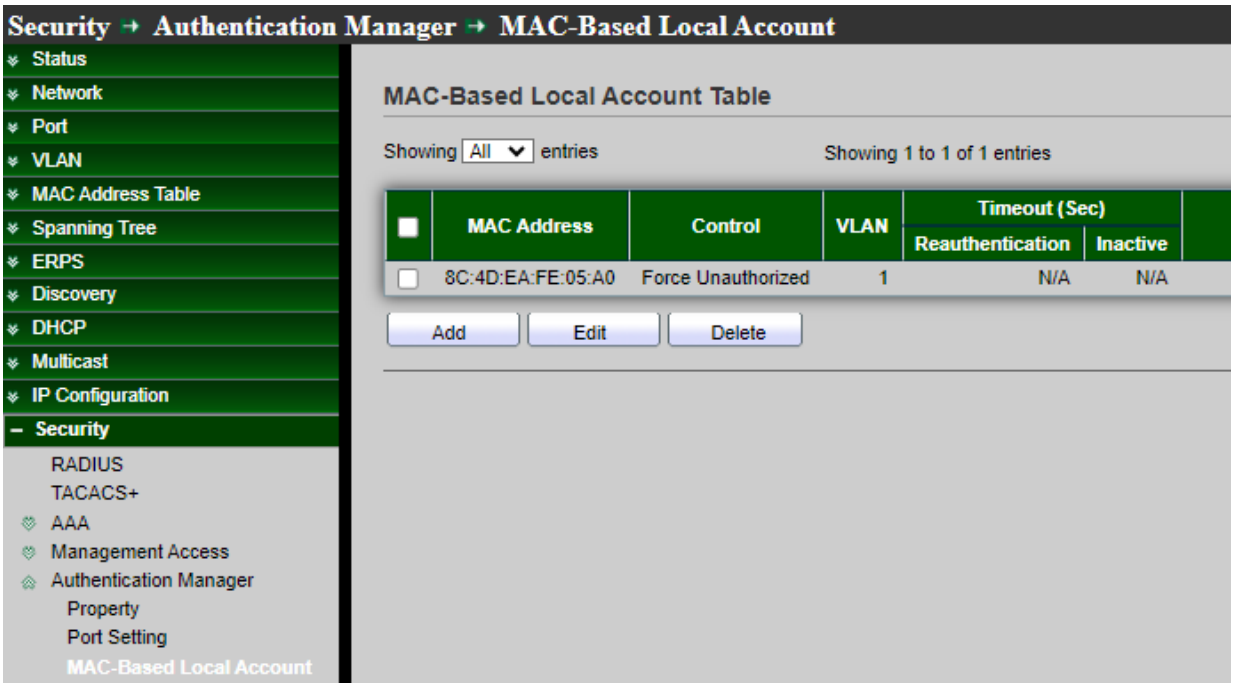
➢ **802.1X Params :**

- **TX Period :** 設備在重新發送請求前等待請求者(用戶端)回應可延伸身份驗證通訊協定(EAP)請求/身份訊框的秒數。
- **Supplicant Timeout :** 向請求者重新發送 EAP 請求前經過的秒數。
- **Server Timeout :** 交換器向身份認證伺服器重新發送請求前經過的秒數。
- **Max Request :** 輸入可以傳送的最大 EAP 請求數。如果交換器在規定的時間(supplicant timeout)後沒有接收到回應，則重新啟動身份驗證過程。
- **Max Login :** 設定復選框可將最大登錄次數設為無限次或指定最大登錄次數。

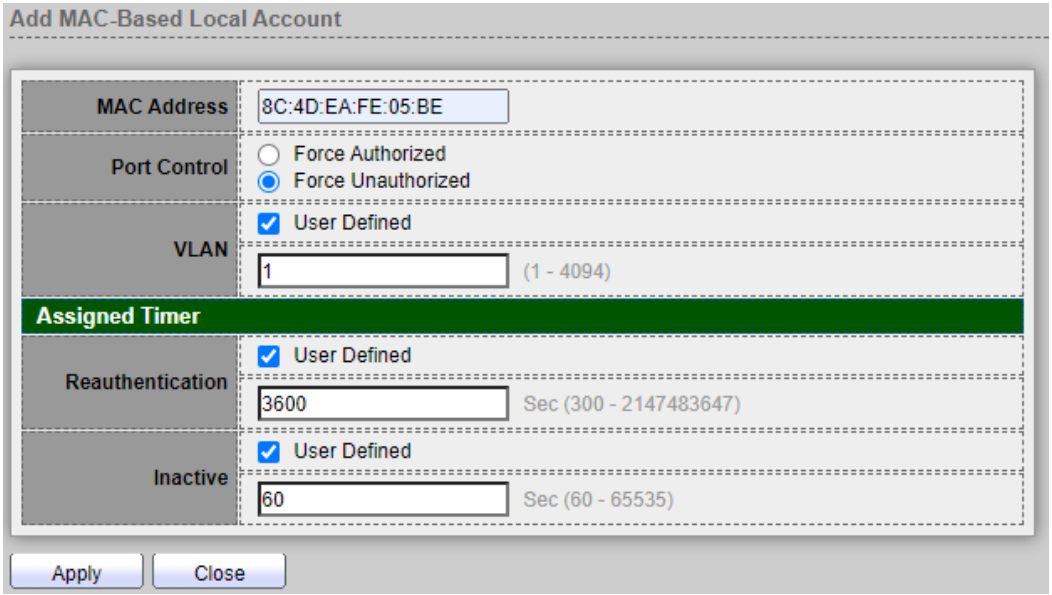
*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

### 14.5.3 基於 MAC 的本地帳戶(MAC-Based Local Account)

使用者管理員管理員可以允許新增/編輯/刪除基於 MAC 的身份驗證本地帳戶，並設定"add"、"Edit"和"Delete"功能進行管理。



| 欄位 | 描述 |
|---|---|
| MAC Address | 已驗證的主機MAC位址，每個MAC在本機資料庫中只能有一個清單 |
| Control | 控制類型<br>• **Force Authorized :** 主機將被強制授權<br>• **Force Unauthorized :** 主機將被強制未授權 |
| VLAN | 為已驗證的主機分配的VLAN ID |
| Timeout | • **Reauthentication :** 為已驗證的主機指定的重新驗證期限。<br>• **Inactive :** 為已驗證的主機指定非設定啟用的超時 |

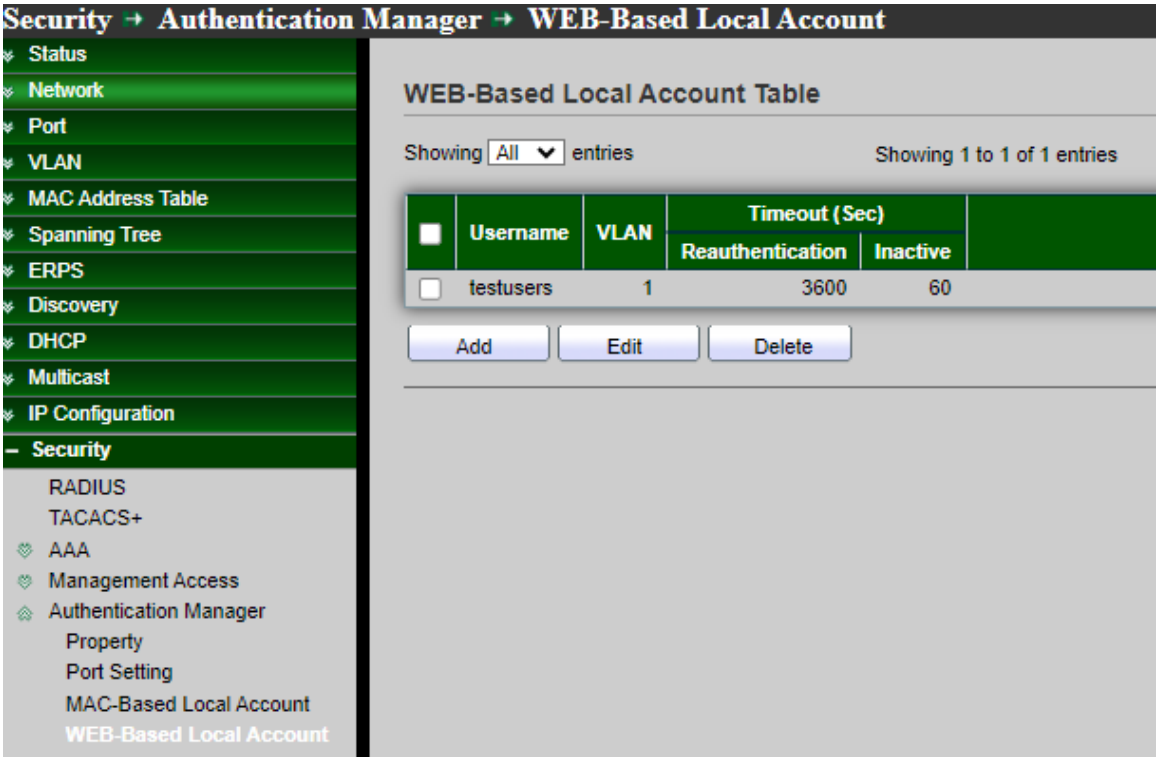



- **MAC Address :** 已驗證的主機 MAC 位址，每個 MAC 在本機資料庫中只能有一個清單。
- **Port Control :** 支援以下認證連接埠控制類型。
  - **Force Authorized :** 主機將被強制授權。
  - **Force Authorized :** 主機將被強制未授權。
- **VLAN :** 為已驗證的主機分配的 VLAN ID。
- **Assigned Timer :**
  - **Timeout (Reauthentication) :** 為已驗證的主機指定的重新驗證期限。
  - **Timeout (Inactive) :** 為已驗證的主機指定非設定啟用的超時。

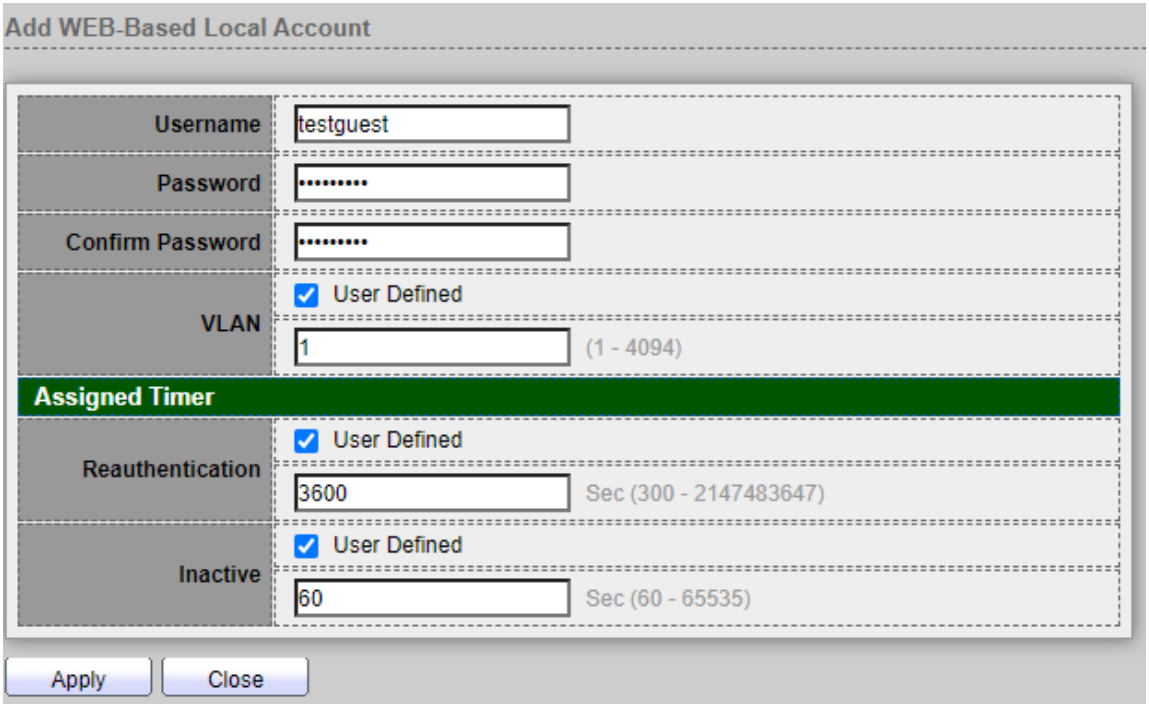
*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

### 14.5.4 基於 WEB 的本地帳戶(WEB-Based Local Account)

使用者管理員管理員可以允許新增/編輯/刪除基於 WEB 的身份驗證本地帳戶，並設定"add"、"Edit"和"Delete"功能進行管理。




| 欄位 | 描述 |
|---|---|
| Username | 驗證帳戶的使用者名稱 |
| VLAN | 為已驗證的主機分配的VLAN ID |
| Timeout(Sec) | • **Reauthentication :** 為已驗證的主機指定的重新驗證期限<br>• **Inactive :** 為已驗證的主機指定非設定啟用的超時 |

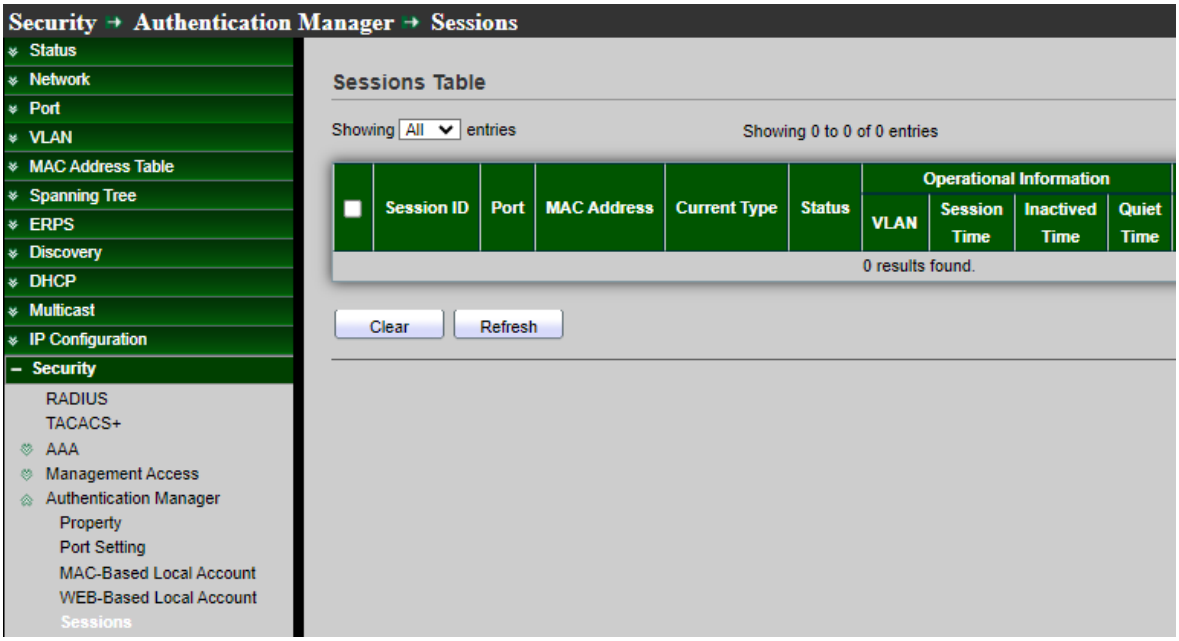


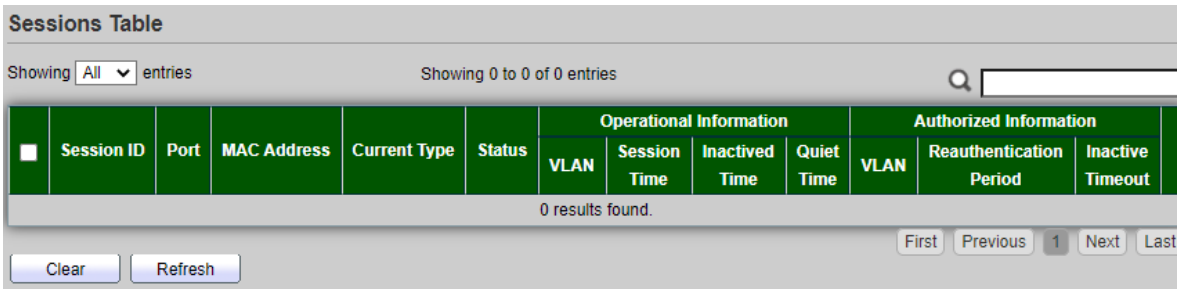

- **Username :** 驗證帳戶的使用者名稱。
- **Password :** 驗證帳戶的密碼。
- **Confirm Password :** 確認驗證帳戶的密碼。
- **VLAN :** 為已驗證的主機分配的 VLAN ID
- **Assigned Timer :**
  - **Timeout (Reauthentication) :** 為已驗證的主機指定的重新驗證期限
  - **Timeout (Inactive) :** 為已驗證的主機指定非設定啟用的超時

*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

### 14.5.5 會話(Sessions)

使用者管理員可以檢查身份驗證會話的所有詳細資訊，並允許使用者透過點擊 “Clear” 清除選擇的特定會話。




| 欄位 | 描述 |
|---|---|
| Session ID | 每個會話的Session ID唯一 |
| Port | 主機所在連接埠名稱 |
| MAC Address | 主機MAC位址 |
| Current Type | 顯示當前身份驗證類型<br>• **802.1x :** 使用IEEE 802.1X進行身份驗證<br>• **MAC-Based :** 使用MAC進行身份驗證<br>• **WEB-Based :** 使用網頁進行身份驗證 |

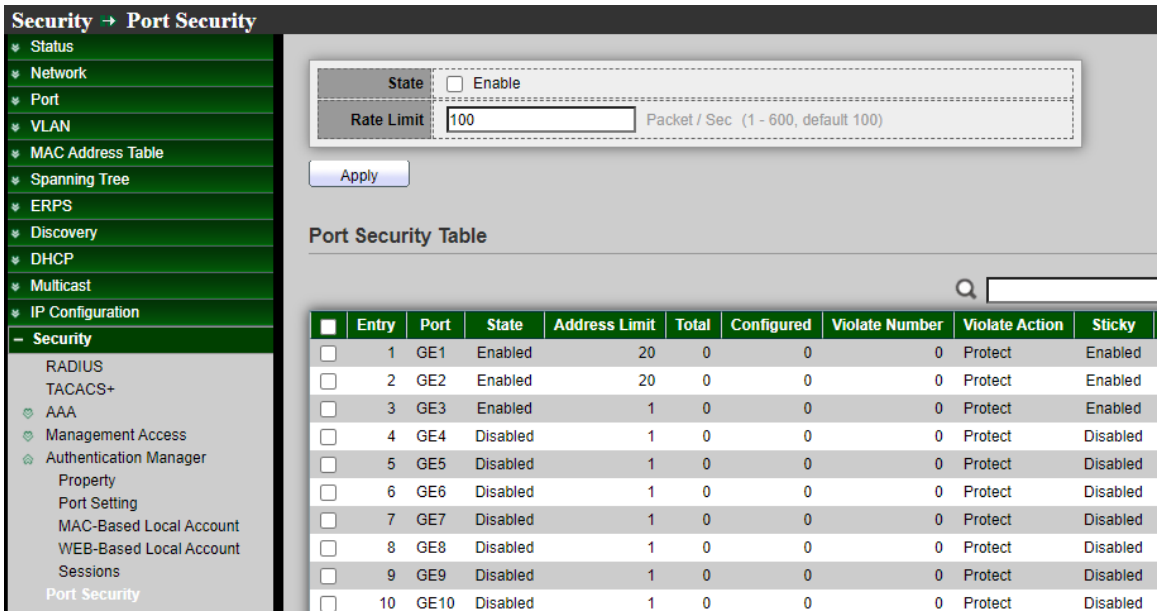
| | |
|---|---|
| Status | 顯示主機認證會話狀態<br>• **Disable :** 該會話已准備好刪除<br>• **Running :** 身份驗證過程正在運行<br>• **Authorized :** 身份驗證已通過且可以訪問網路<br>• **UnAuthorized :** 身份驗證未通過且無法訪問網路<br>• **Locked :** 主機被封鎖，直到靜默結束才能進行身份驗證<br>• **Guest :** 主機處於訪客VLAN中. |
| Operationl | • **VLAN :** 顯示主機運行VLAN ID<br>• **Session Time :** 處於“Authorized”狀態，則顯示授權後的總時間<br>• **Inactived :** 處於“Authorized”狀態, 顯示主機多長時間沒有發送封包<br>• **Quiet Time :** 處於“Locked”狀態,顯示封鎖後的總時間<br>• **Locked :** 主機被封鎖，直到靜默期結束才能進行身份驗證 |
| Authorized | • **VLAN :** 顯示授權程式提供的VLAN ID<br>• **Reauthentication Period :** 顯示授權程式給出的重新認證期限<br>• **Inactive Timeouts :** 顯示授權程式給出的非設定啟用的超時 |

*點擊"Clear"清除該頁面，或"Refresh"重新整理頁面。*

## 14.6 連接埠安全(Port Security)

連接埠安全會檢查安全埠接收的所有流量，以檢測違規或識別和保護新的 MAC 位址。設定關閉違規模式後，在檢測到違規行為後流量將無法進入安全埠，從而消除了違規可能導致 CPU 負載過高的可能性。

連接埠安全會監控接收到的封包。只有具有特定 MAC 位址的使用者才能訪問鎖定的連接埠，該頁面允許使用者為每個介面設定連接埠安全設定。在介面上啟用連接埠安全後，一旦 MAC 位址數超過就會執行操作。



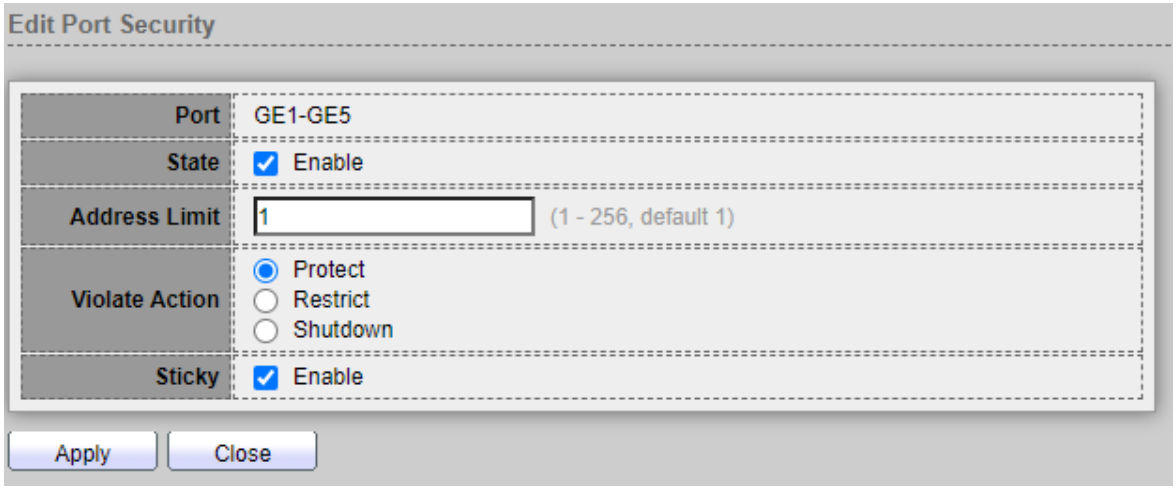

- **State :** 選擇連接埠安全的啟用狀態。
  - **Disable :** 停用連接埠安全功能。
  - **Enable :** 啟用連接埠安全功能。
- **Rate Limit :** 設定速率限制為每秒 1-600 封包。

| Note | 設定保護或限制違規模式後，連接埠安全會在違規發生後繼續處理流量，這可能會導致 CPU 負載過高。設定連接埠安全限速器，在設定保護或限制違規模式時，防止 CPU 負載過高。 |
|---|---|

*點擊"Apply"儲存您的變更設定。*

| 欄位 | 描述 |
|---|---|
| Port | 連接埠安全的連接埠名稱 |
| State | 顯示連接埠安全的啟用或停用狀態 |
| Addres Limie | 顯示連接埠上可設定的最大連接埠安全MAC位址數 |
| Total | 顯示連接埠上所有連接埠安全MAC位址總數 |

| | |
|---|---|
| Configured | 顯示連接埠上設定的所有連接埠安全MAC位址數量 |
| Violate Action | 顯示介面應用於到達鎖定介面的封包的操作<br>• **Protect(保護)**<br>• **Restrict(限制)**<br>• **Shutdown(關閉)** |
| Sticky | 顯示連接埠安全粘滯啟用或停用 |



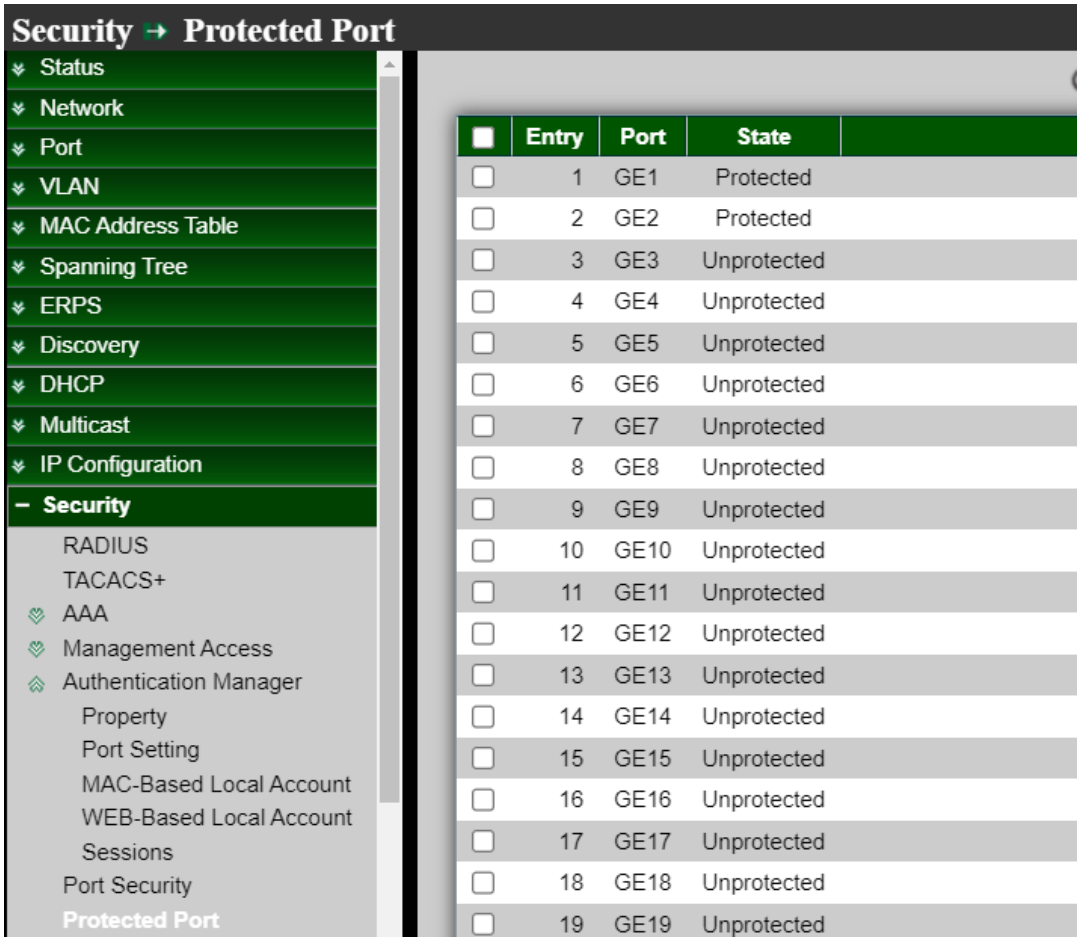

- **Port :** 顯示選擇的連接埠編號。
- **State :** 啟用或停用連接埠安全。
- **Address Limit :** 設定連接埠安全時，交換器可以設定的安全 MAC 位址的最大數量，安全埠預設為 1 個 MAC 位址。預設值可以更改為 1 到 256 之間的任何值。256 的上限可保證每個連接埠都有一個 MAC 位址。
- **Violate Action :** 當學習到 mac 位址，如果介面狀態為鎖定，請選擇應用於到達鎖定介面的封包的操作。
  - **Protect :** 丟棄具有無效 MAC 位址的封包。
  - **Restrict :** 丟棄具有無效 MAC 位址的封包並記錄事件日誌。
  - **Shutdown :** 丟棄具有無效 MAC 位址的封包，關閉連接埠介面，並記錄事件日誌。

*點擊"**Apply**"儲存您的變更，或"**Close**"關閉設定。*

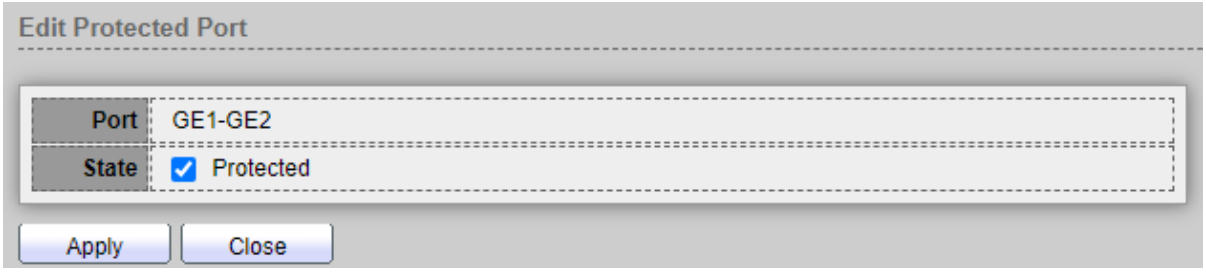
# 14.7 保護連接埠(Protected Port)

此頁面允許使用者設定保護連接埠的設定，以防止所選連接埠相互通訊。保護連接埠只允許與非保護連接埠通訊。換句話說，保護連接埠不允許與另一個保護連接埠通訊。

如果使用者管理員選中啟用，則此連接埠將成為保護連接埠。保護連接埠也稱為專用 VLAN 邊際。它在共用同一廣播域(VLAN)的介面(乙太網路連接埠和鏈路聚合群組)之間提供第 2 層隔離。啟用保護連接埠後，從保護連接埠接收的封包只能轉發給非保護出口連接埠，且不受 VLAN 成員的限制。




| 欄位 | 描述 |
|---|---|
| Port | 連接埠名稱 |
| State | 連接埠保護管理狀態<br>• **Protected :** 連接埠為保護<br>• **Unprotected :** 連接埠為非保護 |

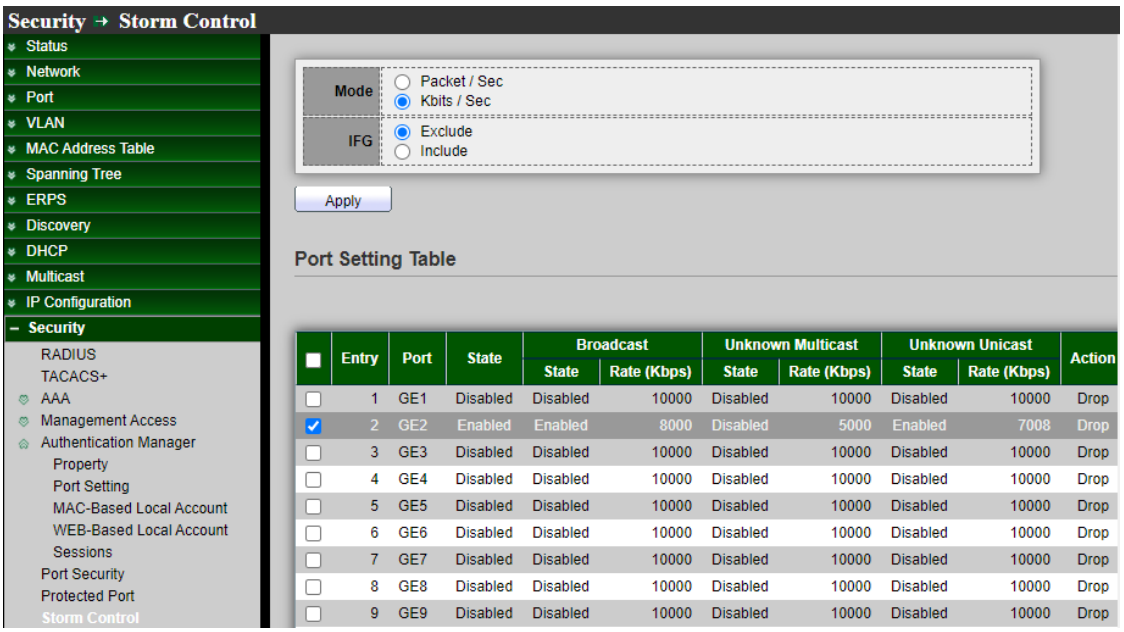



- Port : 顯示所選的連接埠編號。
- State : 連接埠保護管理狀態。
  - Protected : 啟用保護功能。
  - Unprotected (deselect) : 停用保護功能。

*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

## 14.8 風暴控制(Storm Control)

當廣播/未知多播或未知單播的訊框的速率高於使用者定義的限制值時，此功能可以限制進入交換器的訊框數量並定義計入此限制的訊框類型。接收到的超出限制值的訊框將被丟棄或介面關閉。

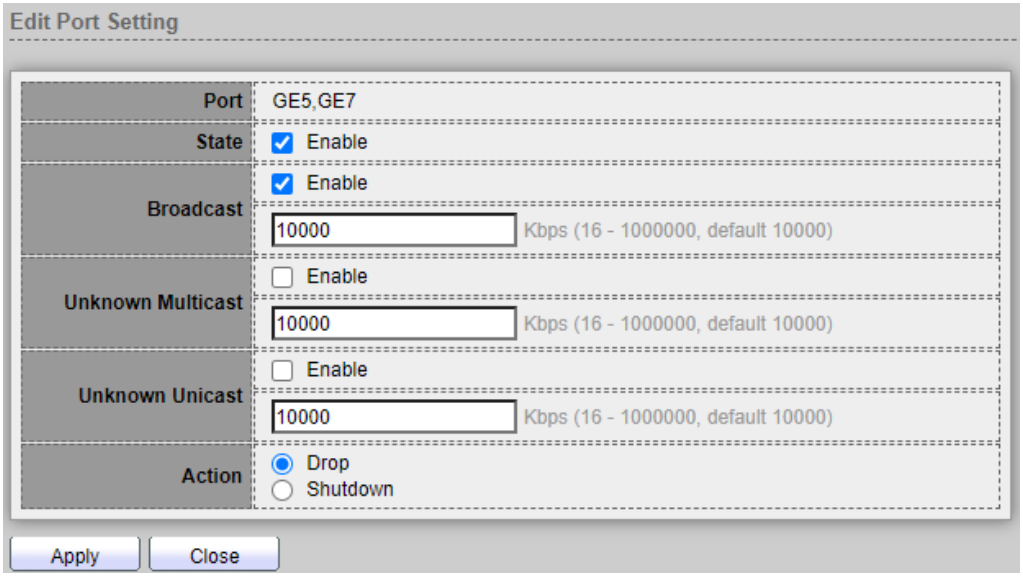



- Mode : 選擇風暴控制報文模式。
  - Packets/sec : 選擇速率限制值封包/秒。
  - Kbits/sec : 選擇速率限制值千位元/秒。

- **IFG :** 選擇有/沒有前導碼和 IFG(20 位元組)的速率計算。
  - **Excluded :** 計算入口風暴控制率時不包括前導碼和 IFG(20 位元組)。
  - **Include :** 計算入口風暴控制率時包括前導碼和 IFG(20 位元組)。

*點擊"Apply"儲存您的變更設定。*

| 欄位 | 描述 |
|---|---|
| Port | 主機所在的連接埠名稱 |
| State | 顯示啟用或停用風暴控制功能 |
| Broadcast | 顯示廣播封包的風暴控制<br>• **State :** 顯示啟用或停用廣播封包的風暴控制<br>• **Rate(Kpps) :** 顯示廣播封包的頻寬限制值速率 |
| Unknown Multicast | 顯示未知多播封包的風暴控制<br>• **State :** 顯示啟用或停用未知多播封包的風暴控制<br>• **Rate(Kpps) :** 顯示未知多播封包的頻寬限制值速率 |
| Unknown Unicast | 顯示未知單播封包的風暴控制<br>• **State :** 顯示啟用或停用未知單播封包的風暴控制<br>• **Rate(Kpps) :** 顯示未知單播封包的頻寬限制值速率 |
| Action | • **Drop :** 接收到的超出限制值的封包將被丟棄，封包超過風暴控制速率將被丟棄<br>• **Shutdown :** 接收到的超出限制值的封包將關閉連接埠，封包超過風暴控制速率時連接埠將關閉 |




- **Port :** 顯示所選連接埠編號。
- **State :** 選擇設定狀態。
  - **Enable :** 啟用風暴控制功能。
- **Broadcast :** 如果對廣播流量啟用風暴控制，則會將廣播流量計入頻寬限制值。
  - **Enable :** 啟用廣播封包的風暴控制功能。風暴控制的速率值，單位元：Kbps (千位元每秒，範圍 16 - 1000000)取決於全域模式設定。
- **Unknown Multicast :** 如果對未知多播啟用風暴控制，則會將未知多播流量計入頻寬限制值。
  - **Enable :** 啟用未知多播封包的風暴控制功能。風暴控制的速率值，單位元：Kbps (千位元每秒，範圍 16 - 1000000)取決於全域模式設定。
- **Unknown Unicast :** 如果對未知單播啟用風暴控制，則會將未知單播流量計入頻寬限制值。
  - **Enable :** 啟用未知多播單包的風暴控制功能。風暴控制的速率值，單位元：Kbps (千位元每秒，範圍 16 - 1000000)取決於全域模式設定。
- **Action :** 當廣播/未知多播或未知單播訊框高於使用者定義的限制值，使用者管理員可以選擇丟棄或關閉。
  - **Drop :** 接收到的超出限制值的封包將被丟棄，封包超過風暴控制速率將被丟棄。
  - **Shutdown :** 接收到的超出限制值的封包將關閉連接埠，封包超過風暴控制速率時連接埠將關閉。

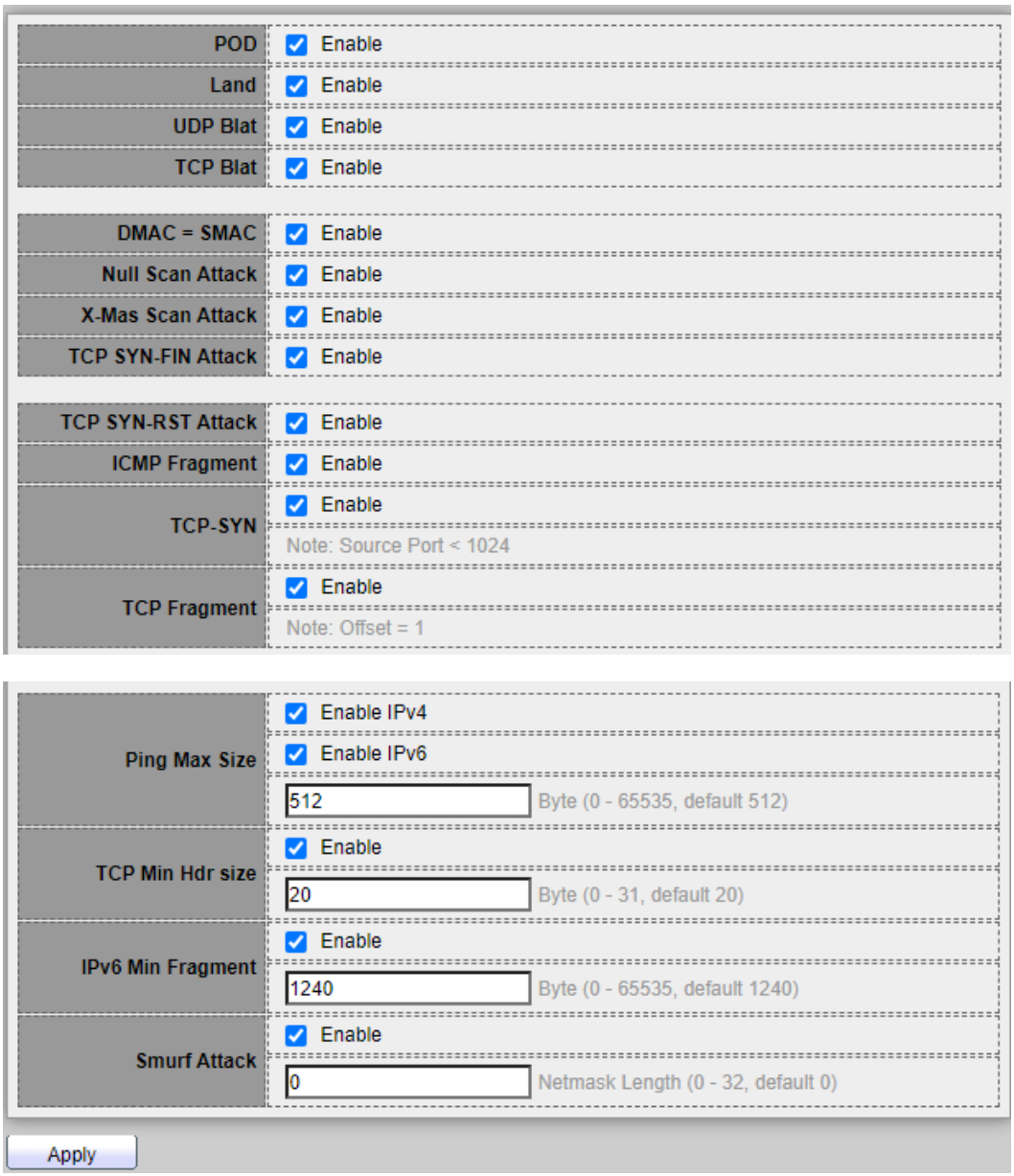
*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

# 14.9 DoS

DoS 攻擊(阻斷服務)是一種網路攻擊，攻擊者試圖透過暫時或無限期中斷連接到網路的主機的服務，使其目標使用者無法使用機器或網路資源。阻斷服務通常是透過向目標機器或資源發送大量多餘請求來實現的，目的是使服務暫時中斷或停止，導致其正常使用者無法訪問。

## 14.9.1 屬性(Property)

此預設啟用所有 DoS 保護功能和 SYN-FIN/SYN-RST 保護。預設限制值是每秒 60 個 SYN 封包。連接埠恢復時間預設為 60 秒。



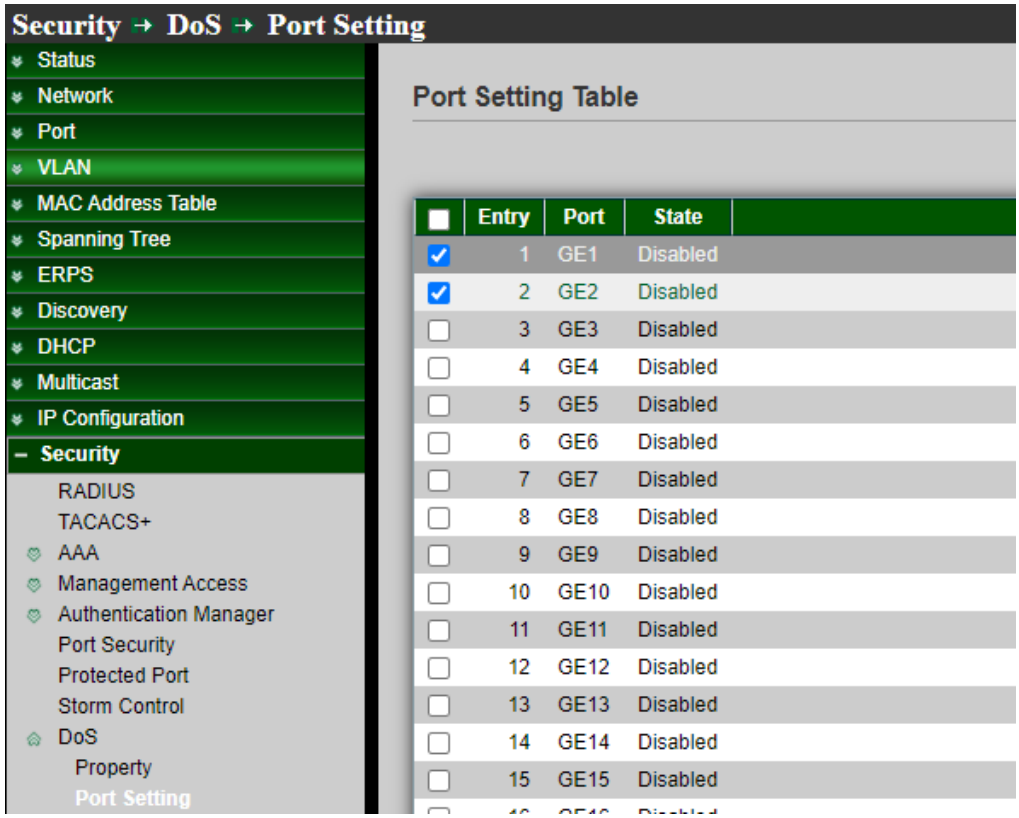
- **POD :**
  - **Enable :** 啟用功能，避免死亡之 ping 的 Dos 攻擊。
- **Land :**
  - **Enable :** 啟用功能，如果受到來源 IP 位址等於目標 IP 位址的封包的 Dos 攻擊，就丟棄封包。
- **UDP Blat :**
  - **Enable :** 啟用功能，如果受到 UDP 來源連接埠等於 UDP 目標連接埠的 Dos 攻擊，就丟棄封包。
- **TCP Blat :**
  - **Enable :** 啟用功能，如果受到 TCP 來源接埠等於 TCP 目標連接埠的 Dos 攻擊，就丟棄封包。
- **DMAC = SMAC :**
  - **Enable :** 啟用功能，如果受到目標 MAC 位址等於來源 MAC 位址的 Dos 攻擊，就丟棄封包。
- **Null Scan Attach :**
  - **Enable :** 啟用功能，受到 NULL 掃描的 Dos 攻擊就丟棄封包。
- **X-Mas Scan Attack :**
  - **Enable :** 啟用功能，如果受到序列號為 0，且 FIN、URG 和 PSH 位元同時設定的 Dos 攻擊，就丟棄封包。
- **TCP SYN-FIN Attack :**
  - **Enable :** 啟用功能，如果受到 SYN 和 FIN 位元設定的 Dos 攻擊，就丟棄封包。
- **TCP SYN-RST Attack :**
  - **Enable :** 啟用功能，如果受到 SYN 和 RST 位元設定的 Dos 攻擊，就丟棄封包。
- **ICMP Fragment :**
  - **Enable :** 啟用功能，受到 Dos 攻擊就丟棄 ICMP 分段封包。
- **TCP- SYN (SPORT<1024) :**
  - **Enable :** 啟用功能，受到 Dos 攻擊就丟棄 sport 小於 1024 的 SYN 封包。
- **TCP Fragment (Offset = 1) :**
  - **Enable :** 啟用功能，受到 Dos 攻擊就丟棄 offset 等於 1 的 TCP 分段封包。
- **Ping Max Size :**
  - **Enable :** 啟用功能，指定 ICMPv4/v6 ping 封包的最大大小的 Dos 攻擊。有效範圍為 0 至 65535 位元，預設值為 512 位元。
- **IPv4 Ping Max Size :**
  - **Enable :** 啟用功能，受到 Dos 攻擊檢查最大 ICMP ping 封包大小，並丟棄大於最大封包大小的封包。

- **IPv6 Ping Max Size :**
  - **Enable :** 啟用功能，受到 Dos 攻擊檢查最大 ICMPv6 ping 封包大小，並丟棄大於最大封包大小的封包。
- **TCP Min Hdr Size :**
  - **Enable :** 啟用功能，受到 Dos 攻擊檢查最小 TCP 表頭，並丟棄小於最小表頭大小的 TCP 封包。長度範圍是 0 至 31 位元，預設長度 20 位元。
- **IPv6 Min Flagment :**
  - **Enable :** 啟用功能，受到 Dos 攻擊檢查最小 IPv6 分段大小，並丟棄小於最小大小的封包。有效範圍為 0 至 65535 位元。預設值為 1240 位元。
- **Smurf Attack :**
  - **Enable :** 啟用功能，避免受到 smurf 攻擊的 Dos 攻擊。子網遮罩長度範圍為 0 至 323 位元，預設長度為 0 位元。

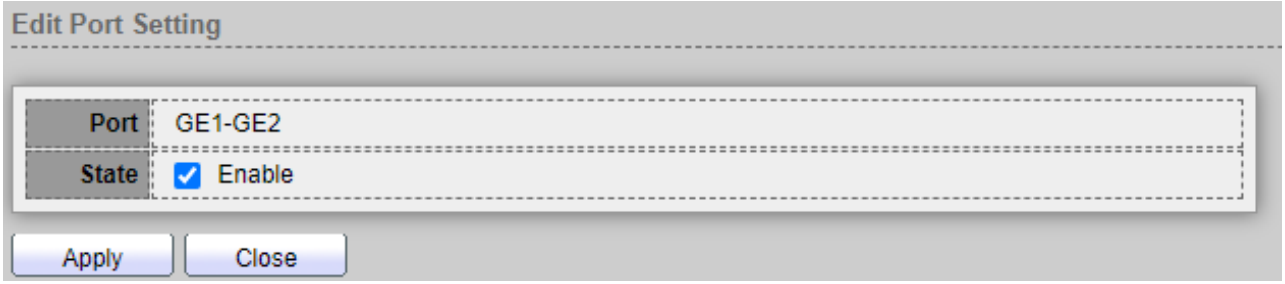
*點擊"Apply"儲存您的變更設定。*

### 14.9.2 連接埠設定(Port Setting)

使用者管理員可以選擇保護連接埠。



| 欄位 | 描述 |
|---|---|
| Port | 連接埠編號介面 |
| State | 顯示Enable/Disable介面上的Dos保護 |




- **Port :** 顯示選擇的連接埠編號。
- **State :** 選擇設定的狀態。
  - **Enable :** 啟用 Dos 保護功能。

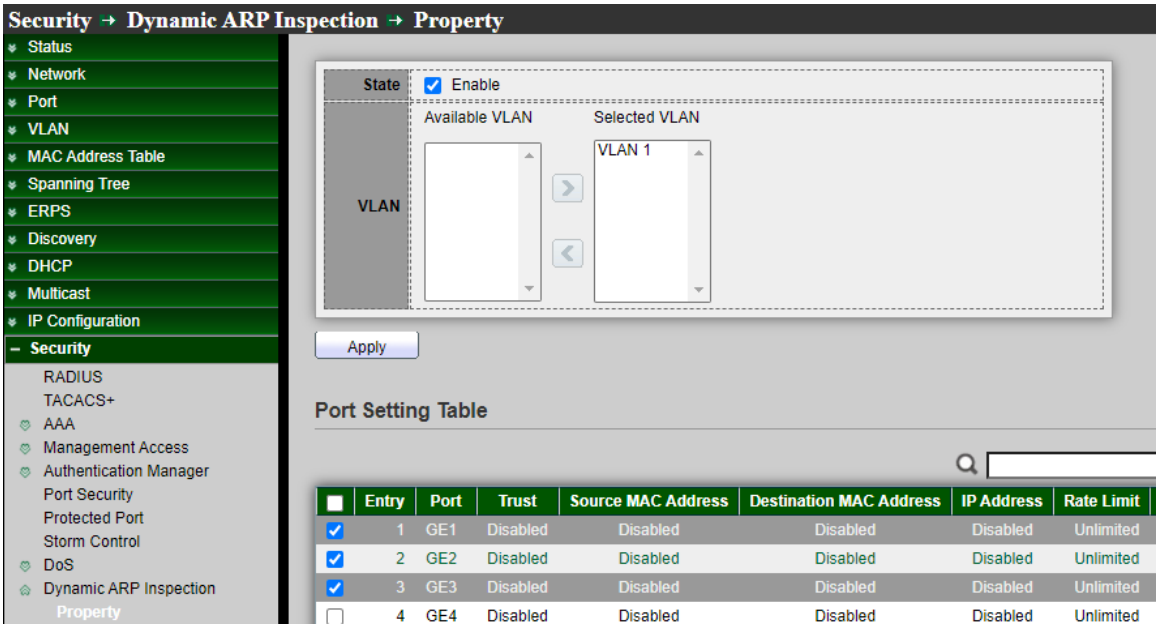
*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

# 14.10 動態 ARP 檢測(Dynamic ARP Inspection)

動態位址解析協定 (ARP) 是一種 TCP/ IP 協議，用於將 IP 位址轉換為 MAC 位址。使用動態 ARP 檢測頁面對動態 ARP 檢測設定。

## 14.10.1 屬性(Property)

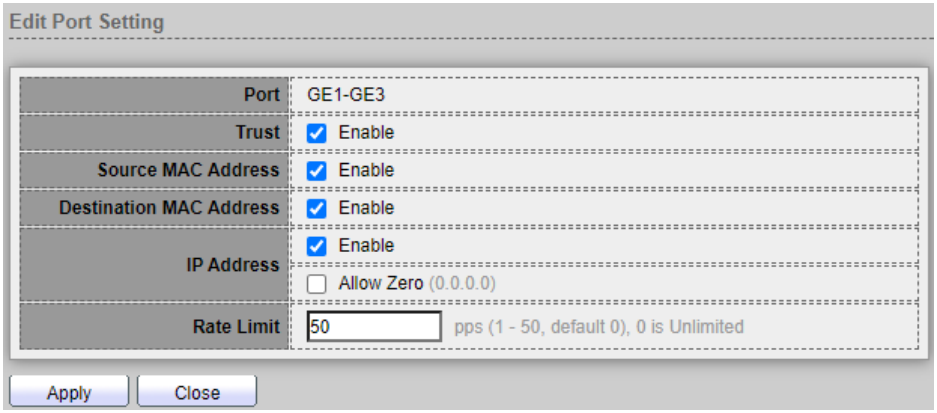
該頁面允許使用者設定全域和每個介面的動態 ARP 檢測設定。




- **State :** 使用者管理員可以啟用或禁用動態 ARP 檢測。選中復選框來啟用/禁用動態 ARP 檢測功能。
- **VLAN :** 在啟用 VLAN 表中，使用者將為啟用的 VLAN 分配靜態 ARP 檢測列表。當封包通過啟用了 ARP 檢測的未信任介面時，交換器將執行檢查。在左側框中選擇 VLAN，然後移至右側以啟用動態 ARP 檢測；或在右側框中選擇 VLAN，然後移至左側以停用動態 ARP 檢測。

*點擊"Apply"儲存您的變更設定。*

| 欄位 | 描述 |
|---|---|
| Port | 連接埠ID |
| Trust | 顯示啟用/禁用介面的信任屬性 |
| Source MAC Address | 顯示啟用/禁用介面來源mac位址驗證屬性 |
| Destination MAC Address | 顯示啟用/禁用介面目的mac位元址驗證屬性 |
| IP Address | 顯示啟用/禁用介面的IP位址驗證屬性，0表示0.0.0.0IP位址 |
| Rate Limit | 顯示介面的速率限制值 |

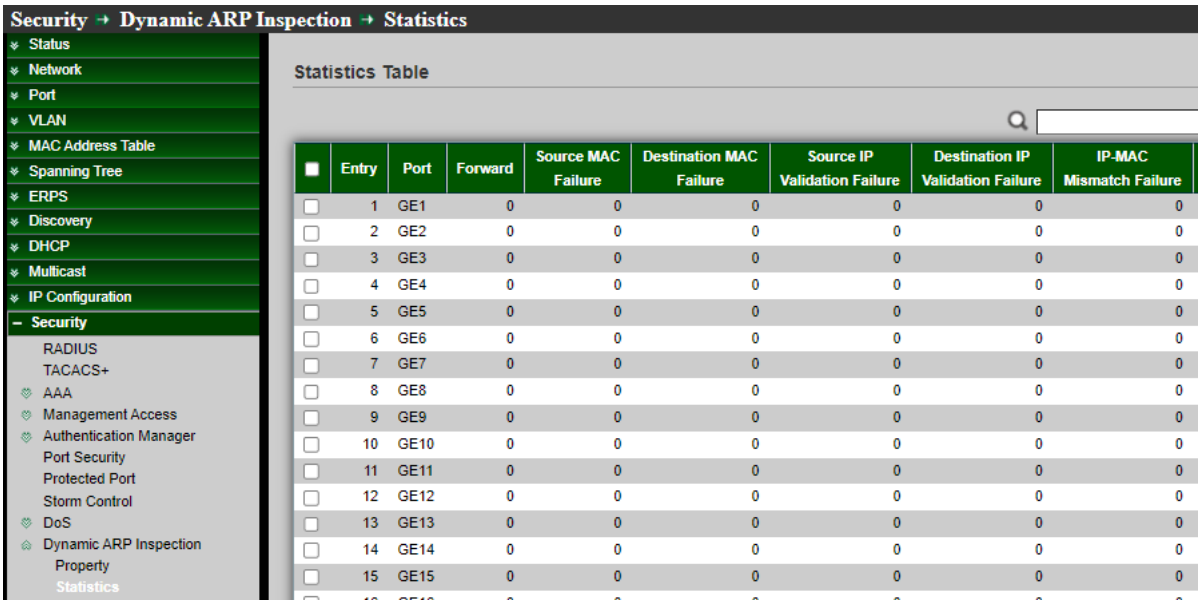



- **Port :** 顯示所選的連接埠編號。
- **Trust :** 如果啟用，則該連接埠或 LAG 是可信任介面，並且不會對發送到該介面或從該介面發送的 ARP 請求或回復執行 ARP 檢測。如果取消啟用，則該連接埠或 LAG 不是受信任的介面，並且將對發送到該介面或從該介面發送的 ARP 請求或回復執行 ARP 檢測。預設情況下禁用。
- **Source MAC Address :** 選取啟用以驗證 ARP 請求和回覆中的來源 MAC 位址，選中複選框以啟用或停用介面的來源 MAC 位址驗證。如果啟用來源 MAC 位址驗證，將檢查所有 ARP 封包的發送方 mac 是否與乙太網路表頭中的來源 mac 相同。預設為禁用。
- **Destination MAC Address :** 選取啟用以驗證 ARP 回覆，選中複選框以啟用或停用介面的目的 MAC 位元址驗證。如果啟用目的 MAC 位元址驗證，將檢查所有 ARP 封包的目標 mac 是否與乙太網路表頭中的目的 mac 相同。預設為禁用。
- **IP Address :** 選中複選框以啟用或停用介面的 IP 位址驗證。啟用後檢查所有 ARP 封包的 IP 位址是否為 0.0.0.0、255.255.255.255 或多播位址。
  - **Allow all-zeros IP :** 如果 IP 位址驗證已啟用，選中則允許 0.0.0.0 的 IP 位址。
- **Rate Limit :** 輸入介面允許的最大速率。範圍為 1 至 50pps，預設值為 0(無限制)。

*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

## 14.10.2 統計數據(Statistics)

統計頁面會顯示 ARP 檢測的統計數據。




| Entry | Port | Forward | Source MAC Failure | Destination MAC Failure | Source IP Validation Failure | Destination IP Validation Failure | IP-MAC Mismatch Failure |
|---|---|---|---|---|---|---|---|
| 1 | GE1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | GE2 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | GE3 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | GE4 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | GE5 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | GE6 | 0 | 0 | 0 | 0 | 0 | 0 |
| 7 | GE7 | 0 | 0 | 0 | 0 | 0 | 0 |
| 8 | GE8 | 0 | 0 | 0 | 0 | 0 | 0 |
| 9 | GE9 | 0 | 0 | 0 | 0 | 0 | 0 |
| 10 | GE10 | 0 | 0 | 0 | 0 | 0 | 0 |
| 11 | GE11 | 0 | 0 | 0 | 0 | 0 | 0 |
| 12 | GE12 | 0 | 0 | 0 | 0 | 0 | 0 |
| 13 | GE13 | 0 | 0 | 0 | 0 | 0 | 0 |
| 14 | GE14 | 0 | 0 | 0 | 0 | 0 | 0 |
| 15 | GE15 | 0 | 0 | 0 | 0 | 0 | 0 |

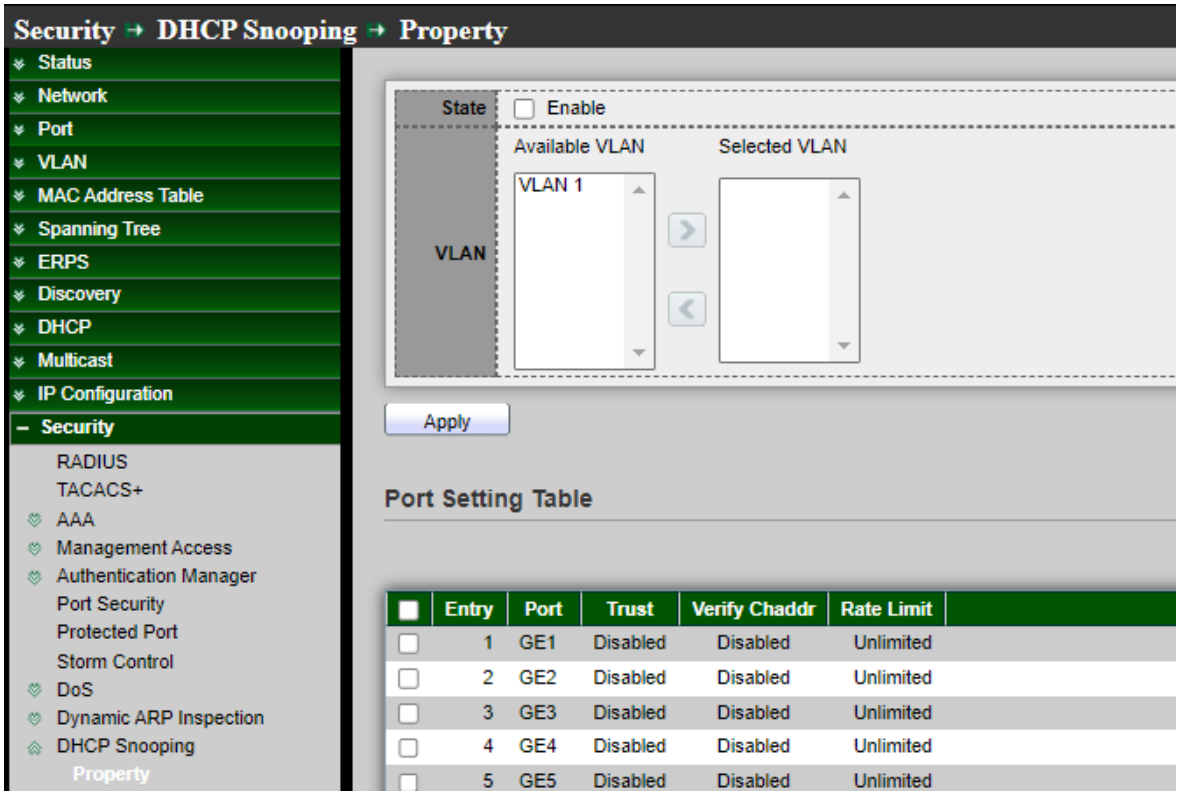
| 欄位 | 描述 |
|---|---|
| Port | 連接埠編號介面 |
| Forward | 顯示正常轉發的封包數量 |
| Source MAC Failure | 顯示來源MAC驗證丟棄的封包數量 |
| Destination MAC Failure | 顯示目的MAC驗證丟棄的封包數量 |
| Source IP Address Validation Failures | 顯示來源IP驗證丟棄的封包數量 |
| Destination IP Address Validation Failures | 顯示目的IP驗證丟棄的封包數量 |
| IP-MAC Mismatch Failures | 顯示IP-MAC與IP源保護綁定表不匹配而丟棄的封包數量 |

# 14.11 DHCP 監聽(DHCP Snooping)

使用者管理員可以使用 DHCP 監聽來協助避免阻斷服務攻擊，這種攻擊是由未經授權的使用者將 DHCP 伺服器新增至網路中，然後向網路上的其他 DHCP 用戶端提供無效的設定資料而導致的。啟用後從其他交換器連接埠上收到的 DHCP 封包轉送之前會先進行檢查。來自不受信任來源的封包將被丟棄。

## 14.11.1 屬性(Property)

該頁面允許使用者設定 DHCP 監聽全域和每個介面的設定。




- **State :** 使用者管理員可以啟用或取消啟用 DHCP 監聽，選中復選框以啟用/停用 DHCP 監聽功能。
- **VLAN :** 使用者管理員可以在 VLAN 上啟用 DHCP 監聽，確保 DHCP 監聽在交換器上已全域啟用，在左側框中選擇 VLAN，然後移至右側以啟用 DHCP 監聽。或在右側框中選擇 VLAN，然後移至左側以停用 DHCP 監聽。

*點擊"Apply"儲存您的變更設定。*

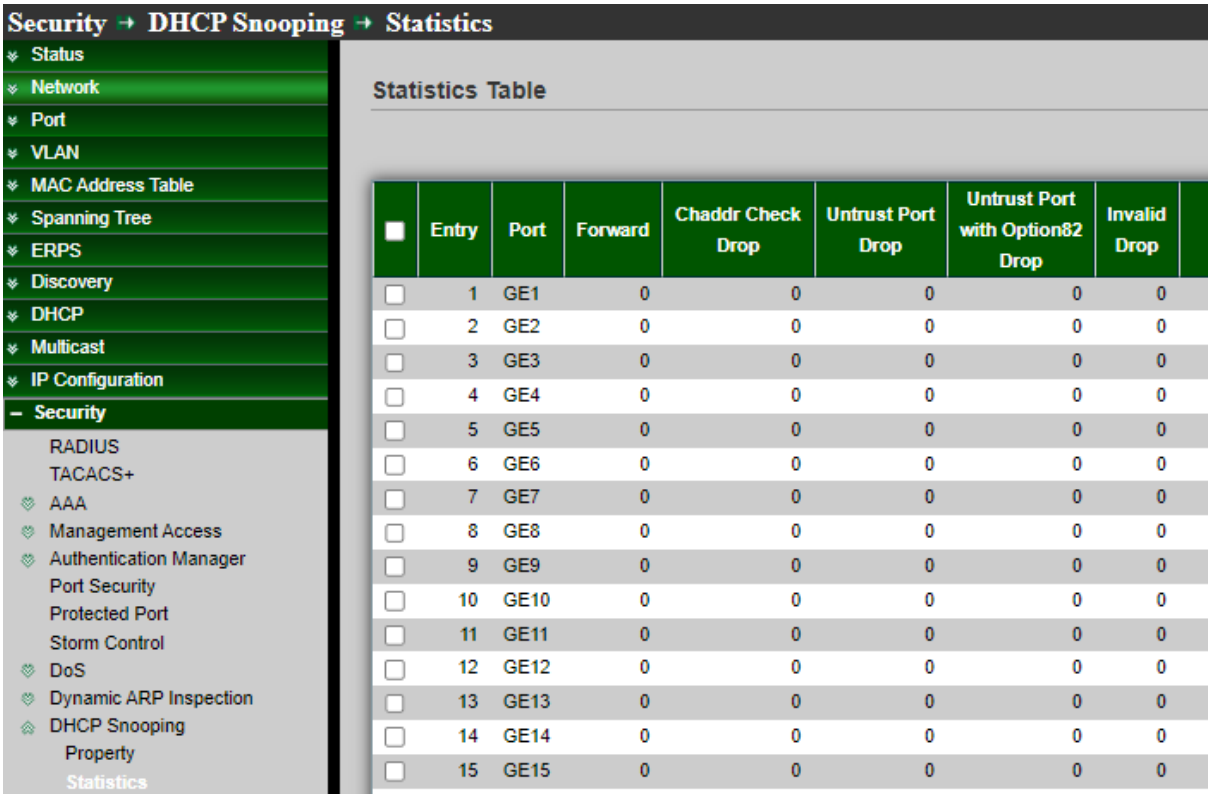
| 欄位 | 描述 |
|---|---|
| Port | 連接埠編號介面 |
| Trust | 顯示啟用/停用介面的信任屬性 |
| Verify Chaddr | 顯示啟用/停用介面的chaddr驗證屬性 |
| Rate Limit | 顯示介面的速率限制值 |


- **Port :** 顯示所選的連接埠編號。
- **Trust :** 如果選中啟用，會將連接到的 DHCP 伺服器或其他交換器或路由器作為可信任埠，選中複選框以啟用/停用介面的信任。如果啟用信任，所有 DHCP 封包將直接轉送。預設為禁用。
- **Verify Chaddr :** 選中復選框來啟用或停用介面的 chaddr 驗證。如果啟用 chaddr 驗證，將檢查所有 DHCP 封包用戶端硬體 mac 位元址是否與乙太網表頭的來源 mac 相同。預設為禁用。
- **Rate Limit :** 輸入介面允許的最大速率。範圍為 1 至 300pps，預設值為 0(無限制)。

*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

### 14.11.2 統計數據(Statistics)

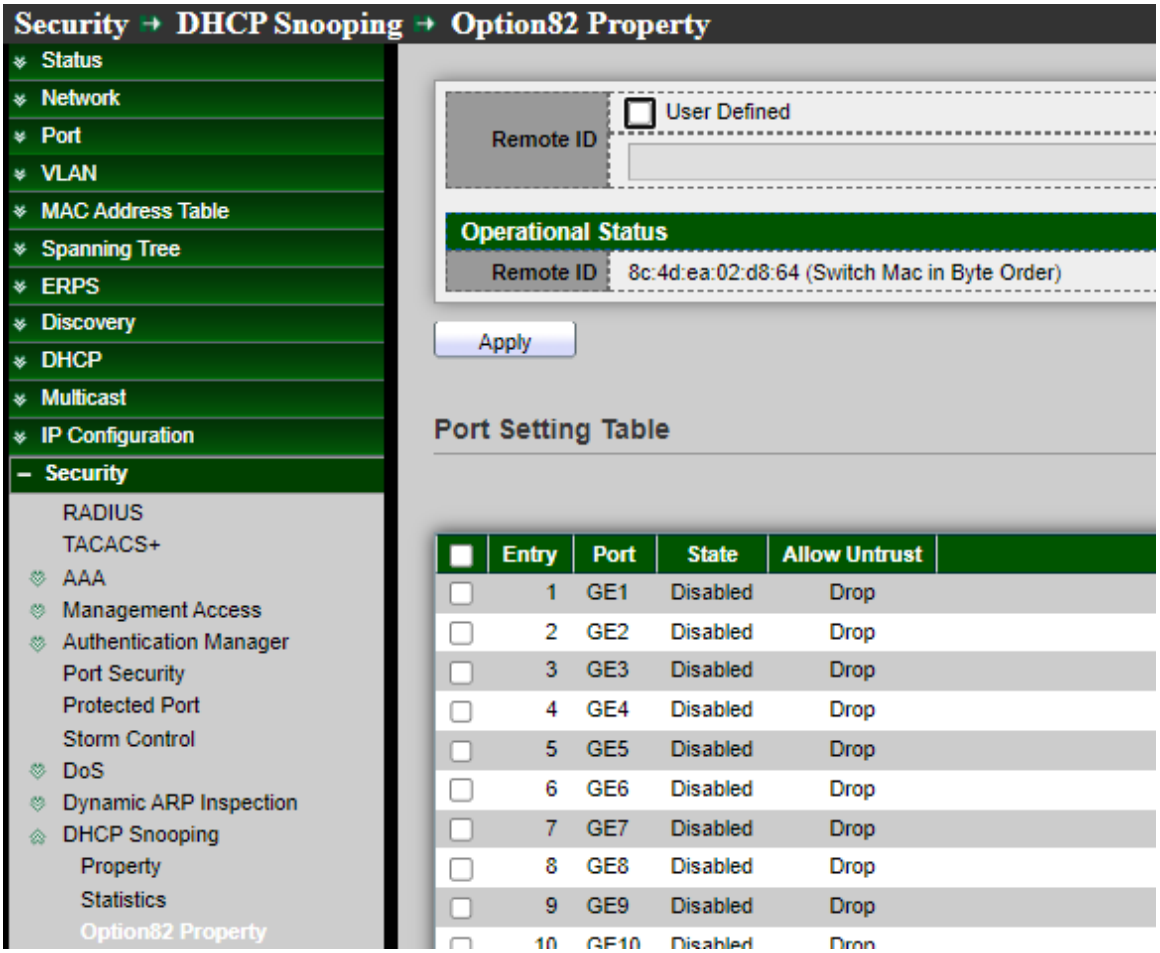
該頁面允許使用者瀏覽 DHCP 監聽功能記錄的所有統計數據。




| 欄位 | 描述 |
|---|---|
| Port | 連接埠編號介面 |
| Forward | 顯示正常轉發的封包數量 |
| Chaddr Check Drop | 顯示chaddr驗證丟棄的封包數量 |
| Untrusted Port Drop | 顯示不信任埠丟棄的DHCP伺服器封包數量 |
| Untrusted Port with Option82 Drop | 顯示透過option82選項檢查不信任埠丟棄的封包數量 |
| Invalid Drop | 顯示因無效檢查而丟棄的封包數量 |

### 14.11.3 Option82 選項屬性(Option82 Property)

此頁面允許使用者設定 DHCP option82 選項遠端 ID 的字串。如果插入選項，則該字串將附加在 option82 選項中。




- **Remote ID :** 如果啟用了 Option82 選項，選中 “User Defined” 以手動輸入遠端 ID 格式，選中複選框以啟用使用者定義的遠端 ID。預設情況下，遠端 ID 為按位元組順序排列的交換器 mac。

  輸入使用者定義的遠端 ID。僅在啟用使用者定義遠端 ID 時可用。

| 欄位 | 描述 |
|---|---|
| Operational Status | 顯示遠端ID資訊 |

*點擊"Apply"儲存您的變更設定。*

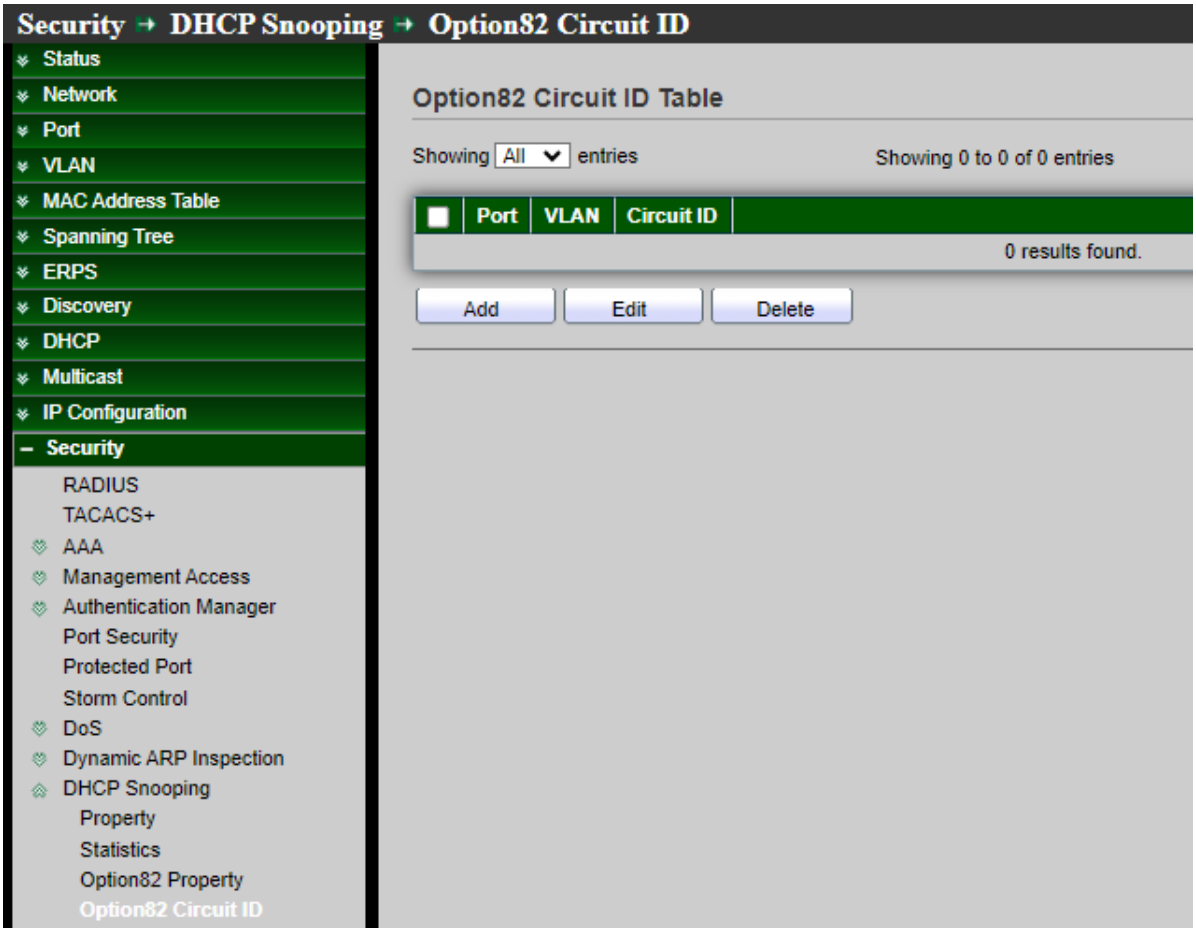
| 欄位 | 描述 |
|---|---|
| Port | 連接埠編號介面 |
| State | 選中復選框以啟用/停用介面的option82選項功能 |
| Allow untrusted | 顯示允許不信任介面的操作 |


- **Port :** 顯示選擇的連接埠編號。
- **State :** 選中啟用或取消啟用，顯示介面 option82 選項的啟用/停用狀態。
- **Allow untrusted :** 選擇當不信任連接埠收到帶有 option82 選項欄位的 DHCP 封包時執行的操作。預設為丟棄。
  - **Keep :** 保持原始 option82 選項內容。
  - **Drop :** 丟棄帶有 option82 選項的封包。
  - **Replace :** 用交換器設定替換 option82 選項內容。

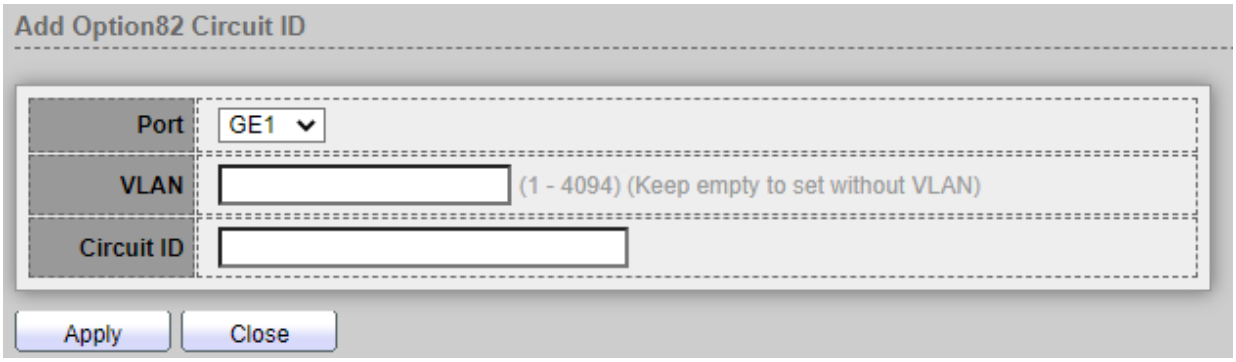
*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

## 14.11.4 Option82 選項代理電路 ID(Option82 Circuit ID)

使用者管理員可以使用 Option82 埠 CID 頁面來設定 Option 82 代理電路 ID，並設定**"add"**、**"Edit"**和**"Delete"**功能進行管理。此頁面允許使用者設定 DHCP option82 代理電路 ID 的字串。如果插入選項，則該字串將附加在 option82 選項中。




| 欄位 | 描述 |
|---|---|
| Port | 顯示連接埠ID清單 |
| VLAN | 顯示清單關聯VLAN |
| Circuit ID | 顯示清單的代理電路ID字串 |




- **Port :** 從列表選擇要與 CID 清單關聯的連接埠。僅適用於 “Add” 對話框。
- **VLAN :** 輸入與 CID 清單關聯的 VLAN ID。VLAN ID 不是必填項。僅適用於 “Add” 對話框。
- **Dircuit ID :** 輸入字串作為 CID。符合連接埠和 VLAN 的封包將插入 CID。

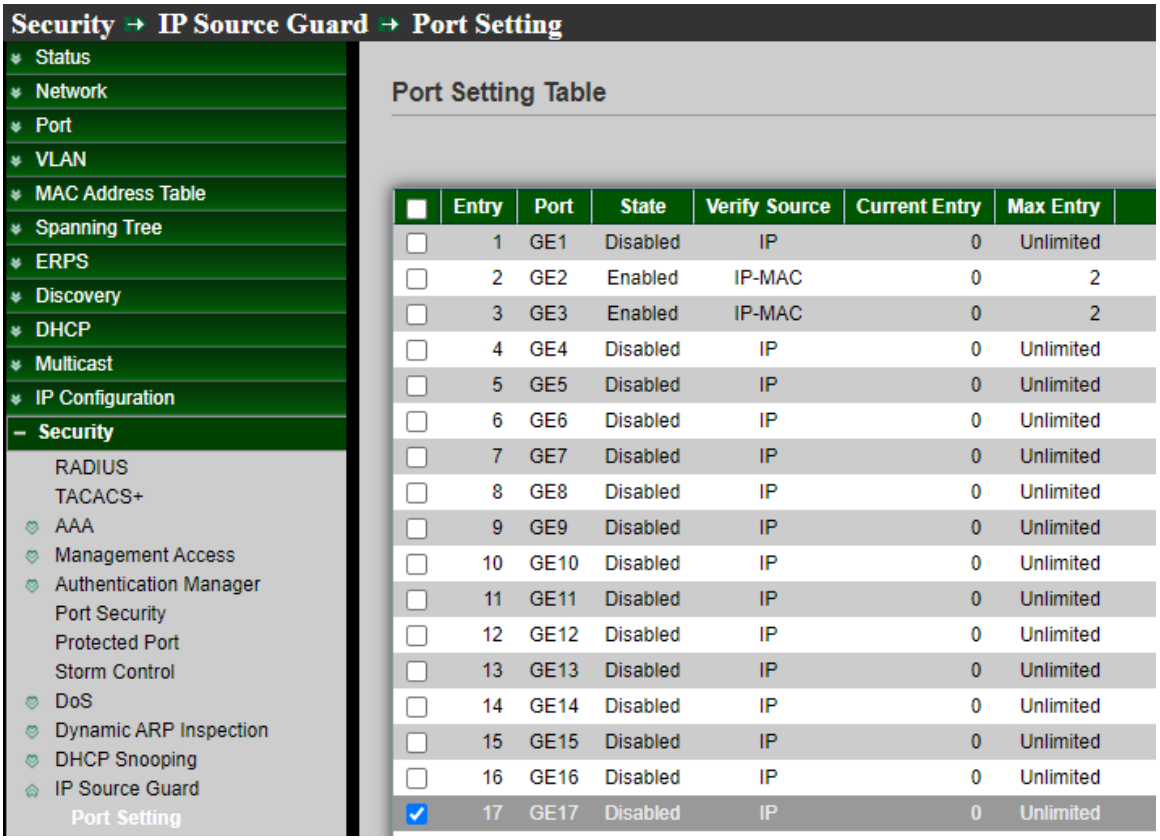
*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

## 14.12 IP 來源防護(IP Source Guard)

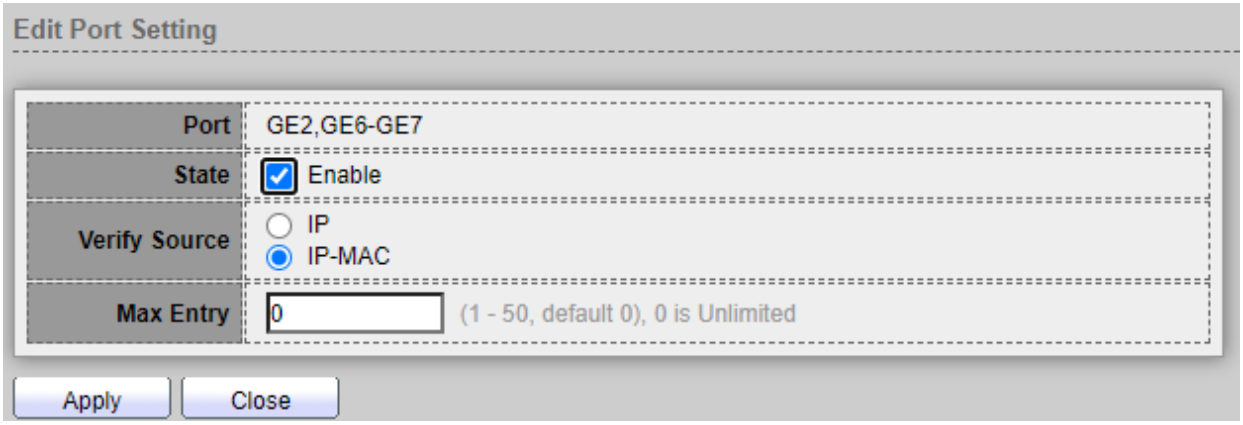
IP 來源防護(IPSG)可將用戶端 IP 流量限制在 IP 來源綁定資料庫中設定的來源 IP 位址，主要用於防止使用者主機嘗試私自手動設定 IP 或使用其鄰近設備 IP 位址時限制其使用。

### 14.12.1 連接埠設定(Port Setting)

此頁面允許使用者對每個連接埠的 IP 來源防護進行設定。




| 欄位 | 描述 |
|---|---|
| Port | 連接埠編號介面 |
| State | 顯示介面的IP來源防護的enable/disable狀態 |
| Verify Source | 顯示IP來源防護驗證的模式 |
| Current Binding Entry | 顯示介面目前的綁定清單 |
| Max Binding Entry | 顯示介面的最大綁定清單數量 |

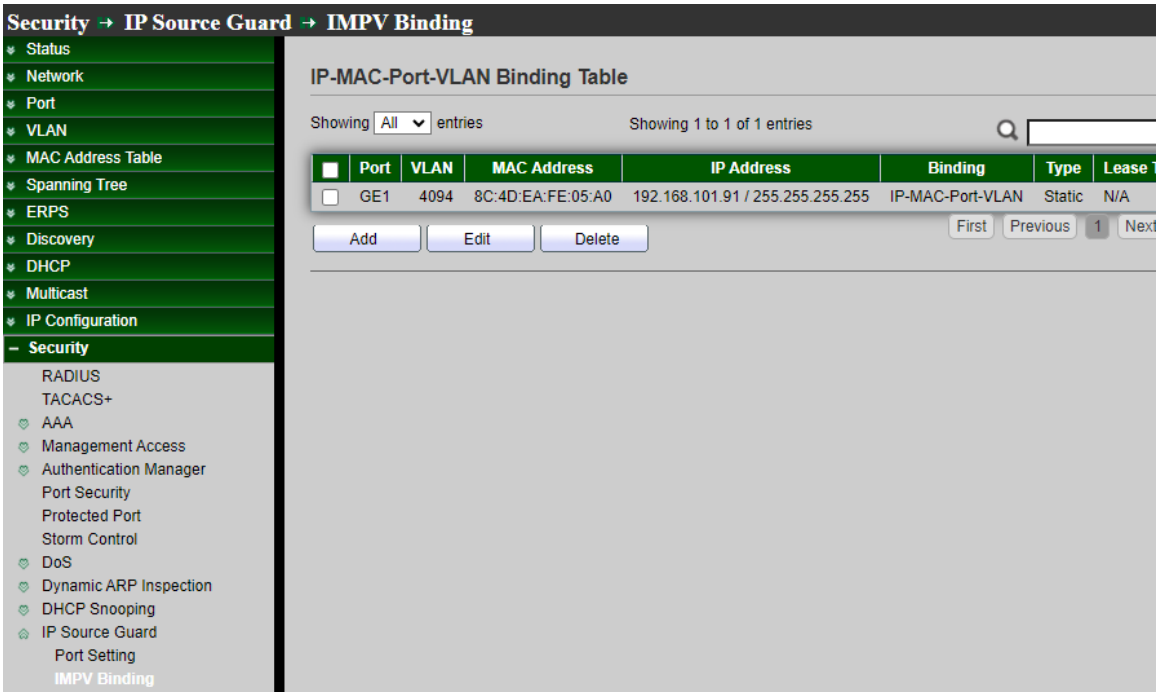



- **Port :** 顯示選擇的連接埠編號。
- **State :** 選中啟用或取消啟用該 IP 來源防護。主要將用戶端 IP 流量限制在已設定的來源 IP 位址。選中 “Enable” 可在介面啟用 IP 來源防護。使用者管理員可以停用此功能，預設為停用。
- **Verify Source :** 使用者管理員可以選擇要僅 IP 或 MAC-IP 類型的源流量進行驗證。
  - **IP :** 僅驗證封包的來源 IP 位址。
  - **IP-MAC :** 驗證封包的來源 IP 位址和來源 MAC 位址。
- **Max Entry :** 使用者管理員需要輸入 IP 來源綁定規則最大數量。範圍為 0 至 50(0 表示無限制)。

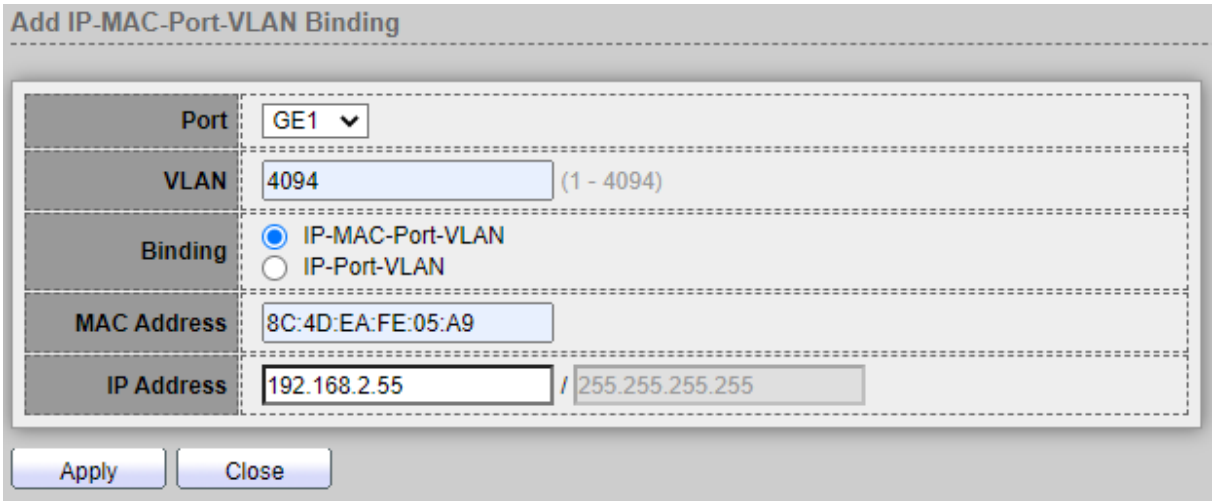
*點擊**"Apply"**儲存您的變更，或**"Close"**關閉設定。*

## 14.12.2 IMPV Binding

使用 IMPV Binding 可查詢和查看 IP 來源防護資料庫中記錄的非設定啟用的位址訊息，此頁面允許使用者新增靜態 IP 來源防護清單，並瀏覽透過 DHCP 監聽學習到的或使用者靜態建立的所有 IP 來源防護清單，設定**"add"**、**"Edit"**和**"Delete"**功能進行管理。




| 欄位 | 描述 |
|---|---|
| Port | 顯示清單的連接埠ID |
| VLAN | 顯示清單的VLAN ID |
| MAC Address | 顯示清單的MAC位址。僅適用於IP-MAC綁定清單 |
| IP Address | 顯示清單的IP位址。IP-MAC綁定清單的遮罩始終為255.255.255.255。IP綁定清單顯示為使用者輸入 |
| Binding | 顯示清單的綁定類型 |
| Status | 現有綁定清單類型:<br>• **Static :** 清單由使用者手動設定添加<br>• **Dynamic :** 清單通過DHCP監聽學習獲取 |
| Lease Time | DHCP監聽學習到的清單的租用時間。租用時間過後清單會被刪除。僅適用於動態清單 |

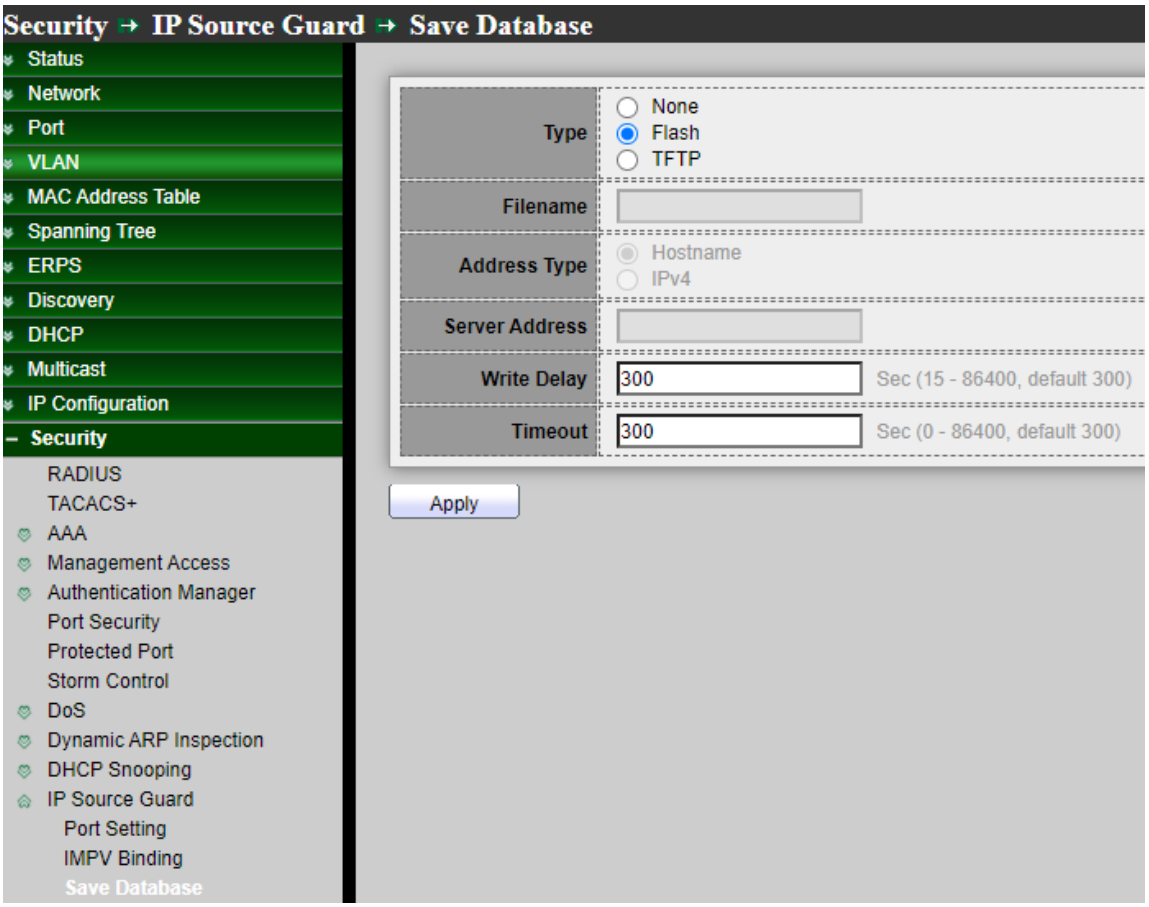



- **Port :** 使用者管理員可以從綁定清單列表中選擇連接埠。
- **VLAN :** 指定綁定清單的 VLAN ID。
- **Binding :** 使用者管理員可以選擇綁定清單的匹配模式。
  - **IP-MAC-Port-VLAN :** 封包必須匹配 IP 位址、MAC 位址、連接埠和 VLAN ID。
  - **IP-Port-VLAN :** 封包必須匹配 IP 位址或子網遮罩、連接埠和 VLAN ID。
- **MAC Address :** 輸入 MAC 位址。僅適用於 IP-MAC-Port-VLAN 模式。
- **IP Address :** 輸入 IP 位址和遮罩。遮罩僅適用於 IP-MAC-Port 模式。

*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

### 14.12.3 保存資料庫(Save Databases)

此頁面允許使用者設定 DHCP 監聽資料庫，該資料庫可以備份和復原動態 DHCP 監聽清單。




- **Type :** 使用者管理員可以選擇資料庫代理類型。
  - **None :** 禁用資料庫代理服務。
  - **Flash :** 將 DHCP 動態綁定清單儲存到快閃記憶體。
  - **TFTP :** 將 DHCP 動態綁定清單儲存到遠端 TFTP 伺服器。
- **Filename :** 設定 TFTP 伺服器的檔案名，輸入備份檔案的檔案名稱。僅當選擇 “Flash” 和 “TFTP” 類型時可用。
- **Address Type :** 選擇使用主機名稱或 IP 位址來連接 TFTP 伺服器。
  - **Hostname :** TFTP 伺服器位址為主機名稱。
  - **IPv4 :** TFTP 伺服器位址為 IPv4 位址。
- **Server Address :** 輸入遠端 TFTP 伺服器主機名稱或 IP 位址。僅當選擇 “TFTP” 類型時可用。
- **Write Delay :** 輸入延遲計時器，用於在發生變更後進行備份。預設值為 300 秒。
- **Timeout :** 輸入因備份失敗而逾時中止。預設值為 300 秒。

*點擊"Apply"儲存您的變更設定。*

# 15. 訪問控制表(ACL)

ACL(訪問控制表)是過濾分類和操作的規則列表。每個分類及其操作規則稱為訪問控制清單(ACE)。每個 ACE 由區分流量群組和關聯操作的過濾器組成。單一 ACL 可能包含一個或多個 ACE，這些 ACE 與傳入訊框的內容進行匹配，對於內容與過濾器匹配的訊框，會應用允許或拒絕的操作。

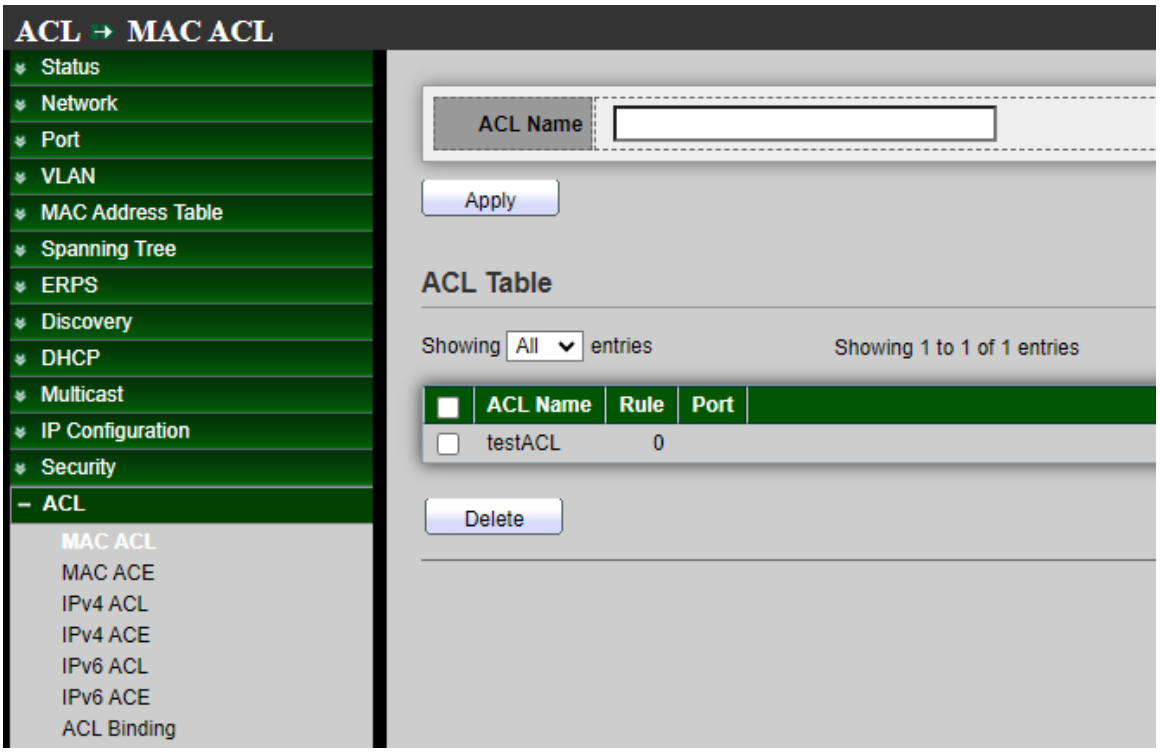
| | |
|---|---|
| Note | 當封包與 ACE 過濾器匹配時，將停止 ACL 處理並採取 ACE 操作。如果封包與 ACE 過濾器不匹配，則處理下一個 ACE。如果一個 ACL 的所有 ACE 都已處理完畢但未找到匹配項，且存在另一個 ACL，則以類似的方式處理。<br>如果在所有相關 ACL 中未找到任何匹配的 ACE，則 ACL 預設操作將丟棄該封包。 |

## 15.1 MAC ACL

此頁面主要創建 MAC ACL 設定檔。 MAC ACL 基於在 MAC ACE 頁面上定義的 Layer 2 欄位過濾流量。

此頁面允許使用者新增或刪除 ACL 規則。如果規則處於綁定狀態則無法刪除。

| | |
|---|---|
| Note | 連接埠既可以使用 ACL 保護，也可以設定進階 Qos 策略，但不能同時使用。 |



➢ **ACL Name :** 創建 ACL 名稱。

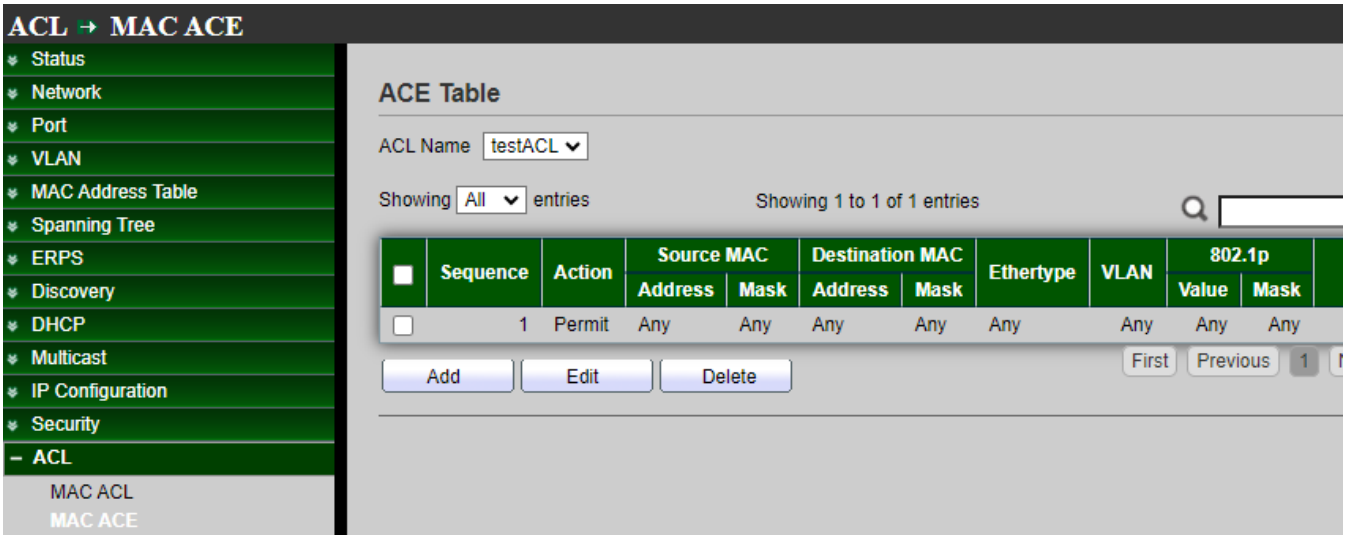
*點擊"Apply"儲存您的變更設定。*

| 欄位 | 描述 |
|---|---|
| ACL Name | 顯示MAC ACL名稱 |
| Rule | 顯示ACL的ACE規則數量 |
| Port | 顯示綁定該ACL的連接埠 |

*點擊 "Delete" 刪除 ACL 列表。*

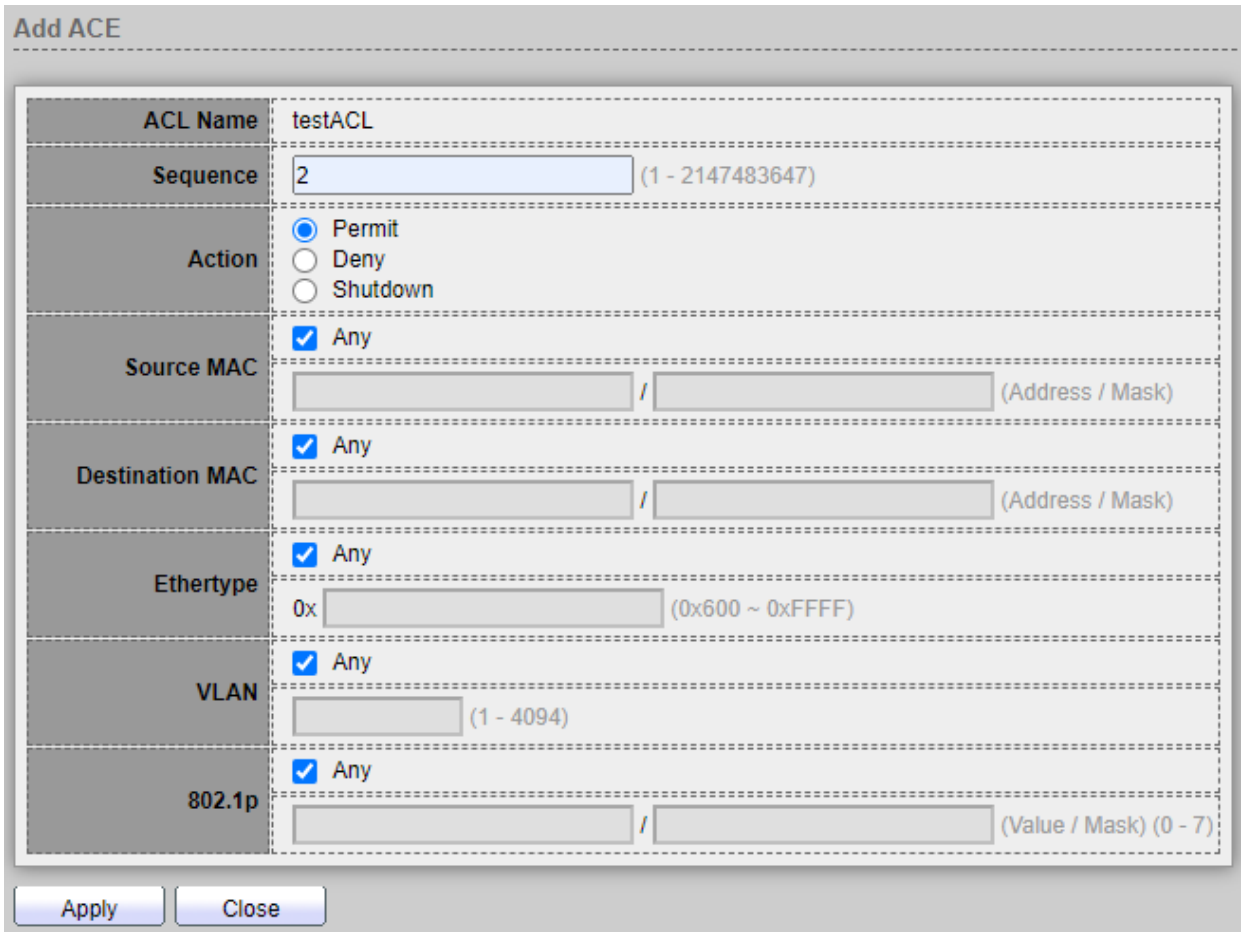
## 15.2 MAC ACE

MAC ACE 將檢查所有訊框是否匹配。設定"**add**"、"**Edit**"和"**Delete**"功能進行管理。此頁面允許使用者新增、編輯或刪除 ACE 規則。如果 ACL 處於綁定狀態，則無法新增、編輯或刪除 ACE 規則。




➢ **ACL Name :** 選擇要新增 ACE 的 ACL 名稱。

| 欄位 | 描述 |
|---|---|
| Sequence | 顯示ACE序列 |
| Action | 顯示ACE的操作 |
| Source MAC | 顯示ACE的來源MAC位址和遮罩 |
| Destination MAC | 顯示ACE的目的MAC位址和遮罩 |
| Ethertype | 顯示ACE的乙太網路訊框類型 |
| VLAN ID | 顯示ACE的VLAN ID |
| 802.1p Value | 顯示ACE的802.1p值 |
| 802.1p Mask | 顯示ACE的802.1p遮罩 |




- **ACL Name :** 顯示要新增 ACE 的 ACL 名稱。

- **Sequence :** 優先處理序列較高的 ACE(1 為最高優先級)。僅適用於 “Add” 對話框。
- **Action :** 使用者管理員可以選擇 ACE 匹配封包後的操作。
  - **Permit :** 轉發匹配 ACE 規則的封包。
  - **Deny :** 丟棄匹配 ACE 規則的封包。
  - **Shutdown :** 丟棄匹配 ACE 規則的封包，並停用接收封包的連接埠。可以從 “Port Settings” 頁面重新啟動此類連接埠。
- **Source MAC :** 選擇來源 MAC 位址的類型。
  - **Any :** 所有來源位址均可接受。
  - **User Defined :** 僅接受使用者定義的來源位址或來源位址範圍。輸入要匹配的來源 MAC 位址和遮罩。
- **Destination MAC :** 選擇目的 MAC 位元址的類型。
  - **Any :** 所有目的位元址均可接受。
  - **User Defined :** 僅接受使用者定義的目的位元址或目的位元址範圍。輸入要匹配的目的 MAC 位元址和遮罩。

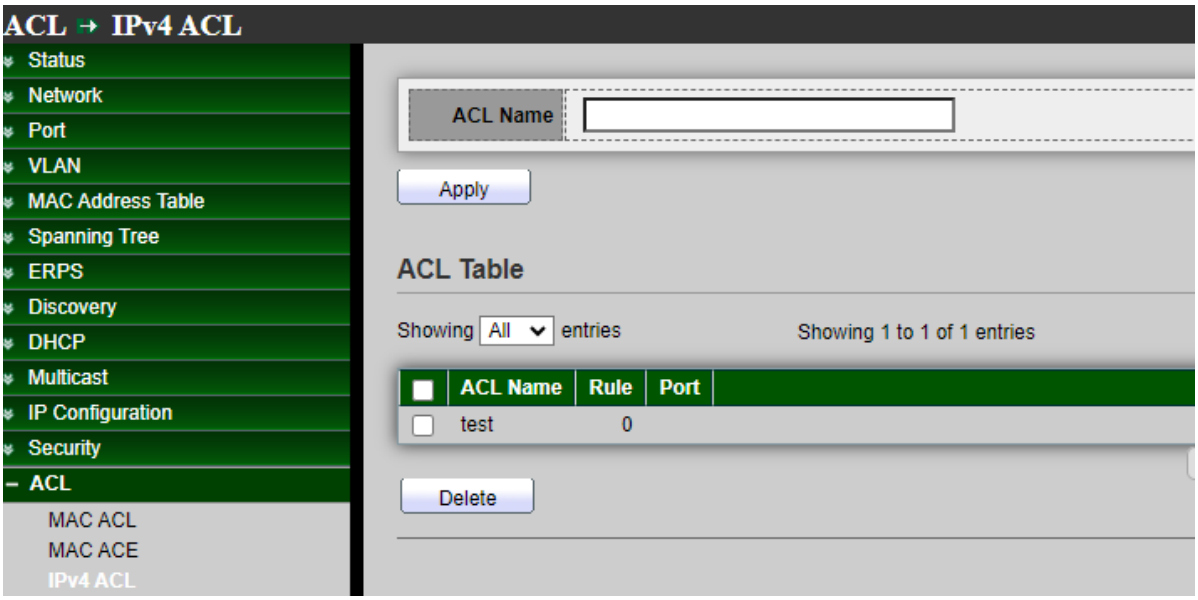
| Note | 設定 F 為顯示值，0 為遮罩值，例如，如果 MAC 為 8C : 4D : EA : 11 : 22 : 33，則遮罩值 FF : FF : FF : 00 : 00 : 00 表示僅使用目標 MAC 位址的前三個位元組(8C : 4D : EA)。 |
|---|---|

- **Ethertype :** 選擇乙太網路訊框類型。
  - **Any :** 所有乙太網路訊框類型均可接受。
  - **User Defined :** 僅接受使用者定義的乙太網路訊框。輸入要匹配的乙太網路訊框。
- **VLAN ID :** 選擇 VLAN ID 類型。
  - **Any :** 所有 VLAN ID 均可接受。
  - **User Defined :** 僅接受使用者定義的 VLAN ID。輸入要匹配的 VLAN ID。
- **802.1p :** 選擇 802.1p 值類型。
  - **Any :** 所有 802.1p 值均可接受。
  - **User Defined :** 僅接受使用者定義的 802.1p 值或 802.1p 值範圍。輸入要匹配的 802.1p 值。

*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

## 15.3 IPv4 ACL

主要創建 IPv4 ACL 設定檔。IPv4 ACL 用於檢查 IPv4 封包，此頁面允許使用者新增或刪除 IPv4 ACL 規則。如果規則處於綁定狀態，則無法刪除。




- ACL Name : 創建 ACL 名稱。

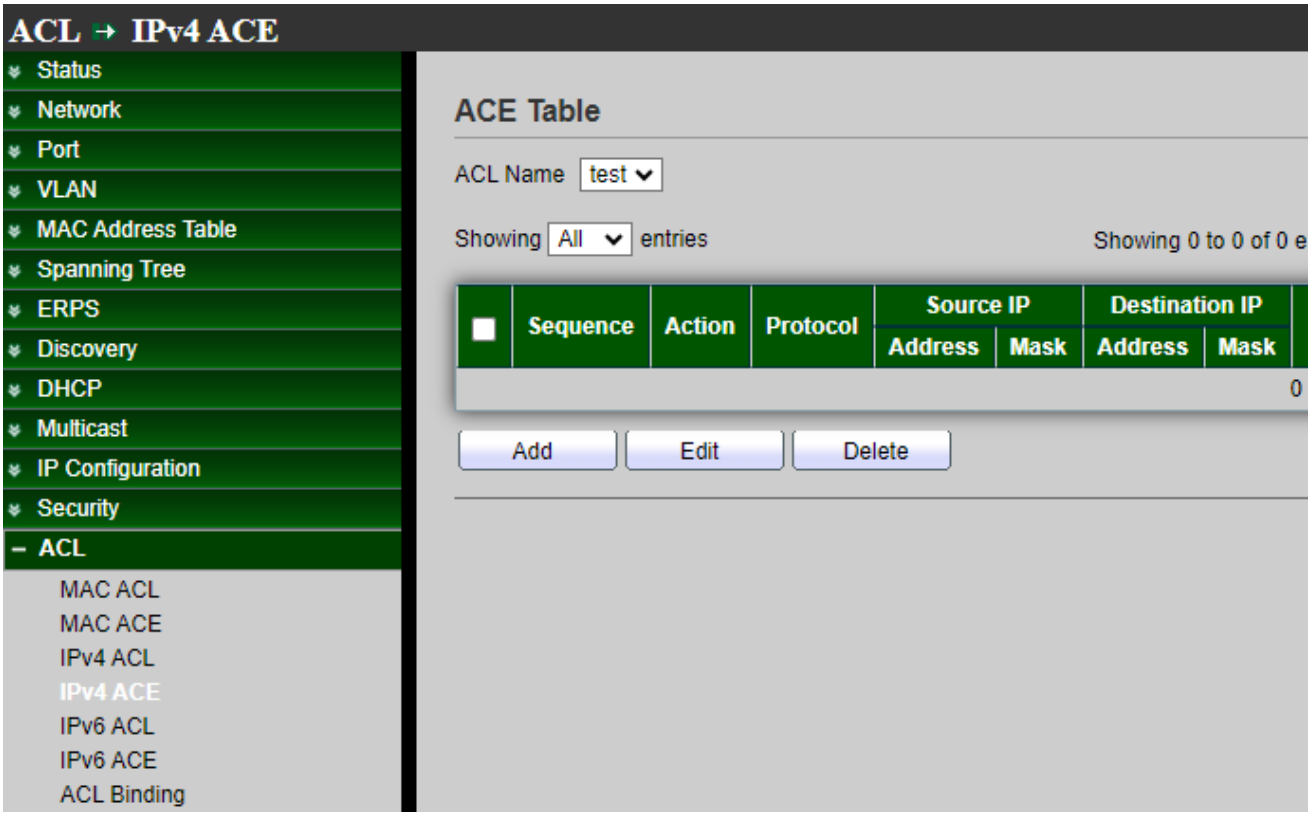
*點擊"Apply"儲存您的變更設定。*

| 欄位 | 描述 |
|---|---|
| ACL Name | 顯示IPv4 ACL名稱 |
| Rule | 顯示ACL的ACE規則數量 |
| Port | 顯示與此ACL綁定的連接埠列表 |

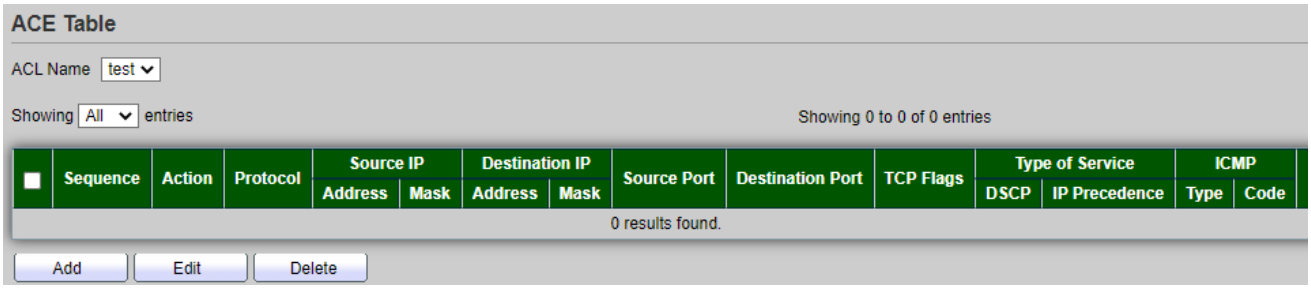
*點擊 "Delete" 選中的刪除列表。*

## 15.4 IPv4 ACE

此頁面允許使用者新增、編輯或刪除 ACE 規則。如果 ACL 處於綁定狀態，則無法新增、編輯或刪除 ACE 規則。設定"add"、"Edit"和"Delete"功能進行管理。

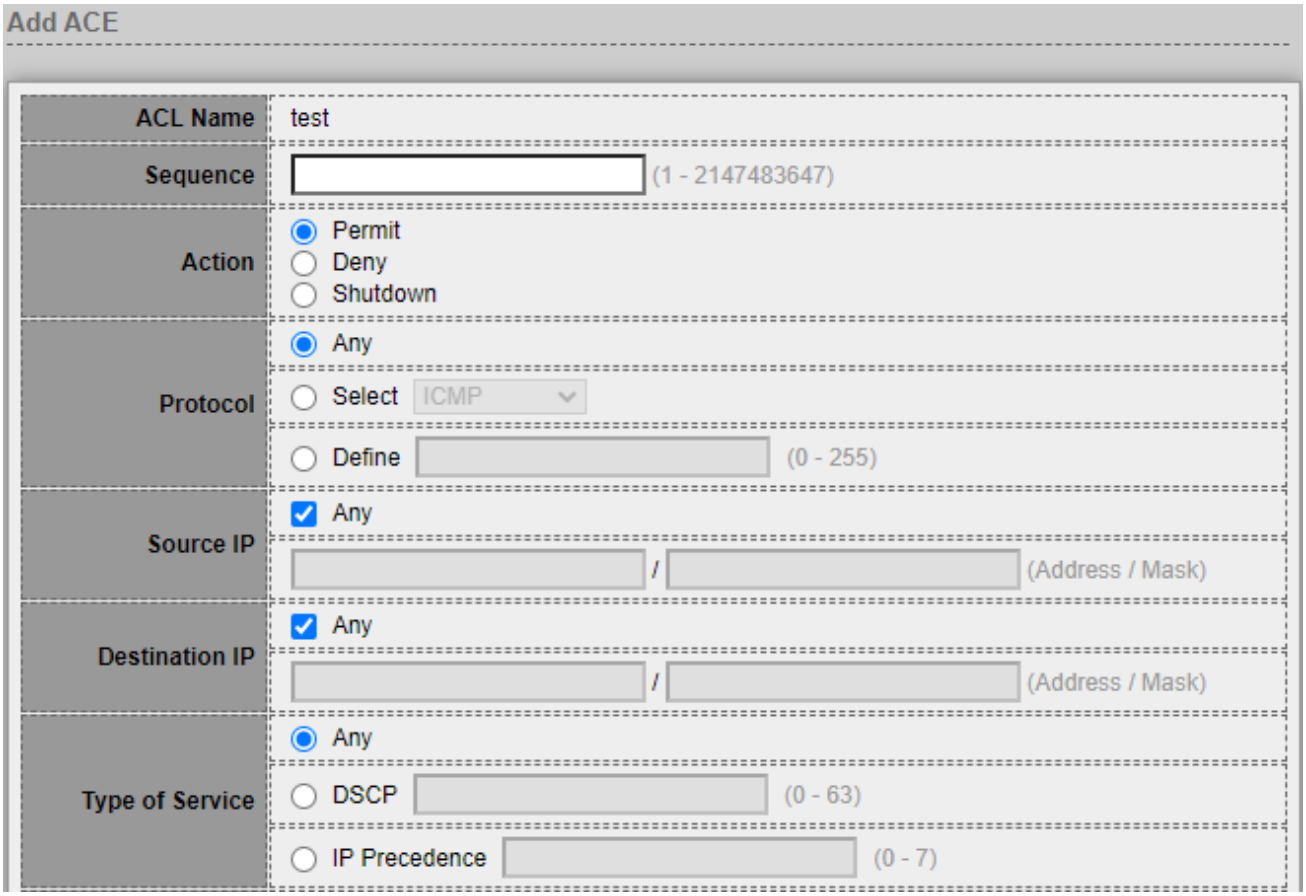



➢ **ACL Name :** 選擇要要新增 ACE 的 ACL 名稱。

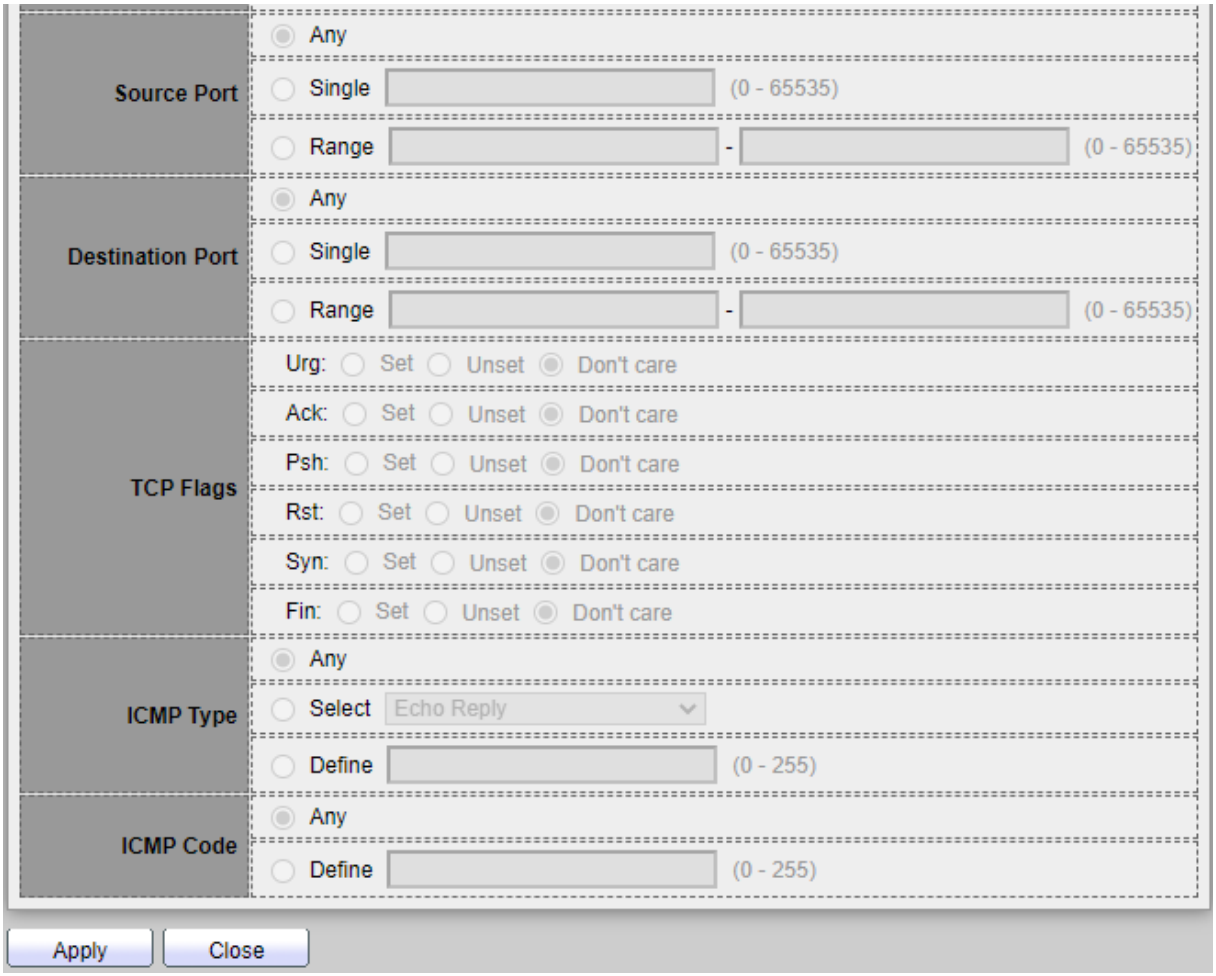



| 欄位 | 描述 |
|---|---|
| Sequence | 顯示ACE序列 |
| Action | 顯示ACE的操作 |
| Protocol | 顯示ACE的協議值 |

| | |
|---|---|
| Source IP | 顯示ACE的來源MAC位址和遮罩:<br>• **Address :** 顯示IPv4 IP位址<br>• **Mask :** 顯示遮罩位址 |
| Destination IP | 顯示ACE的目的MAC位元址和遮罩:<br>• **Address :** 顯示IPv4 IP位址<br>• **Mask :** 顯示遮罩位址 |
| Source Port | 顯示ACE的單一來源連接埠或一系列來源連接埠。僅當協定為TCP或UDP時可用 |
| Destination Port | 顯示ACE的單一目的連接埠或一系列目的連接埠。僅當協定為TCP或UDP時可用 |
| TCP Flags | 顯示ACE的TCP指標值。僅當協定為TCP時可用 |
| Type of Service | 顯示ACE的Tos值，可以是DSCP或IP優先級 |
| ICMP | 顯示ACE的ICMP類型和代碼。僅當協定為ICMP時可用 |



- **ACL Name :** 顯示要新增 ACE 的 ACL 名稱。
- **Sequence :** 指定 ACE 的序列，優先處理序列較高的 ACE(1 為最高優先級)。僅適用於 “Add” 對話框。
- **Action :** 使用者管理員可以選擇匹配封包後的操作。
  - **Permit :** 轉發匹配 ACE 規則的封包。
  - **Deny :** 丟棄匹配 ACE 規則的封包。
  - **Shutdown :** 丟棄符合 ACE 規則的封包，並停用接收封包的連接埠。可以從 “Port Settings” 頁面重新啟動此類連接埠。
- **Protocol :** 使用者管理員可以選擇匹配的協定類型。
  - **Any (IP) :** 所有 IP 協定均可接受。
  - **Select from list :** 從下拉選單中選擇以下協定之一。
    (ICMP/IPinIP/TCP/EGP/IGP/UDP/HMP/RDP/IPV6/IPV6 : ROUT/IPV6 : FRAG/ RSVP/IPV6 : ICMP/OSPF/PIM/L2TP)
  - **Protocol ID to match :** 輸入協定 ID。
- **Source IP :** 選擇來源 IP 位址的類型。
  - **Any :** 所有來源位址均可接受。
  - **User Defined :** 僅接受使用者定義的來源位址或來源位址範圍。輸入要匹配的來源 IP 位址值和遮罩。
- **Destination IP :** 選擇目的 IP 位元址的類型。
  - **Any :** 所有目的位元址均可接受。
  - **User Defined :** 僅接受使用者定義的目的位元址或目的位元址範圍。輸入要匹配的目的 IP 位元址值和遮罩。
- **Type of Service :** 選擇要匹配的服務類型。
  - **Any :** 所有服務類型均可接受。
  - **DSCP to match :** 輸入要匹配的差分服務代碼點(DSCP)。
  - **IP Precedence to match :** 輸入要匹配的 IP 優先級別。




- **Source Port :** 選擇匹配的協定類型。僅當協定為 TCP 或 UDP 時可用。
  - **Any :** 所有來源連接埠均可接受。
  - **Single :** 輸入匹配封包的單個 TCP/UDP 來源埠。
  - **Range :** 選擇匹配封包的 TCP/UDP 來源埠範圍。可以設定八個不同的連接埠範圍(在來源連接埠和目的連接埠之間共用)。TCP 和 UDP 協定各有八個連接埠範圍。
- **Destination Port :** 選擇匹配的協定類型。僅當協定為 TCP 或 UDP 時可用。
  - **Any :** 所有目的連接埠均可接受。
  - **Single :** 輸入匹配封包的單個 TCP/UDP 目的埠。
  - **Range :** 選擇匹配封包的 TCP/UDP 目的埠範圍。可以設定八個不同的連接埠範圍(在來源連接埠和目的連接埠之間共用)。TCP 和 UDP 協定各有八個連接埠範圍。
- **TCP Flags :** 選擇一個或多個用於過濾封包的 TCP 指標。過濾後的封包要則被轉發，要則被丟棄。透過 TCP 指標過濾封包可增強封包控制，進而提高網路安全性。僅當協定為 TCP 時可用。
  - **Set :** 如果 TCP 指標為 SET，則匹配。
  - **Unset :** 如果 TCP 指標為 NOT SET，則匹配。

- Don’ t care : 忽略 TCP 指標。

➢ ICMP Type : 按名稱選擇訊息類型或輸入訊息類型編號。僅當協定為 ICMP 時可用。

- Any : 所有訊息類型均可接受。
- Select from list : 通過名稱選擇訊息類型。
- Protocol ID to match : 輸入訊息類型編號。

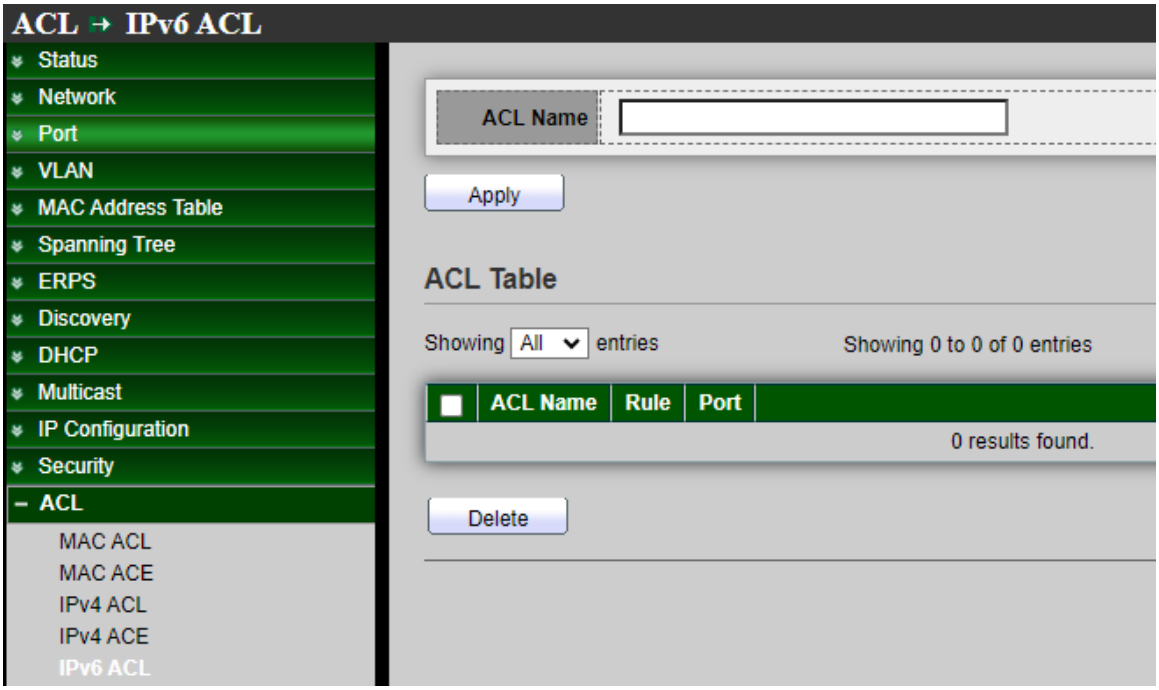
➢ ICMP Code : 選擇 ICMP 代碼類型。僅當協定為 ICMP 時可用。

- Any : 所有代碼均可接受。
- User Defined : 輸入要匹配的 ICMP 代碼。

*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

## 15.5 IPv6 ACL

主要創建 IPv6 ACL 設定檔。IPv6 ACL 用於檢查 IPv6 封包，此頁面允許使用者新增或刪除 IPv6 ACL 規則。如果規則處於綁定狀態，則無法刪除。




➢ ACL Name : 創建 ACL 名稱。

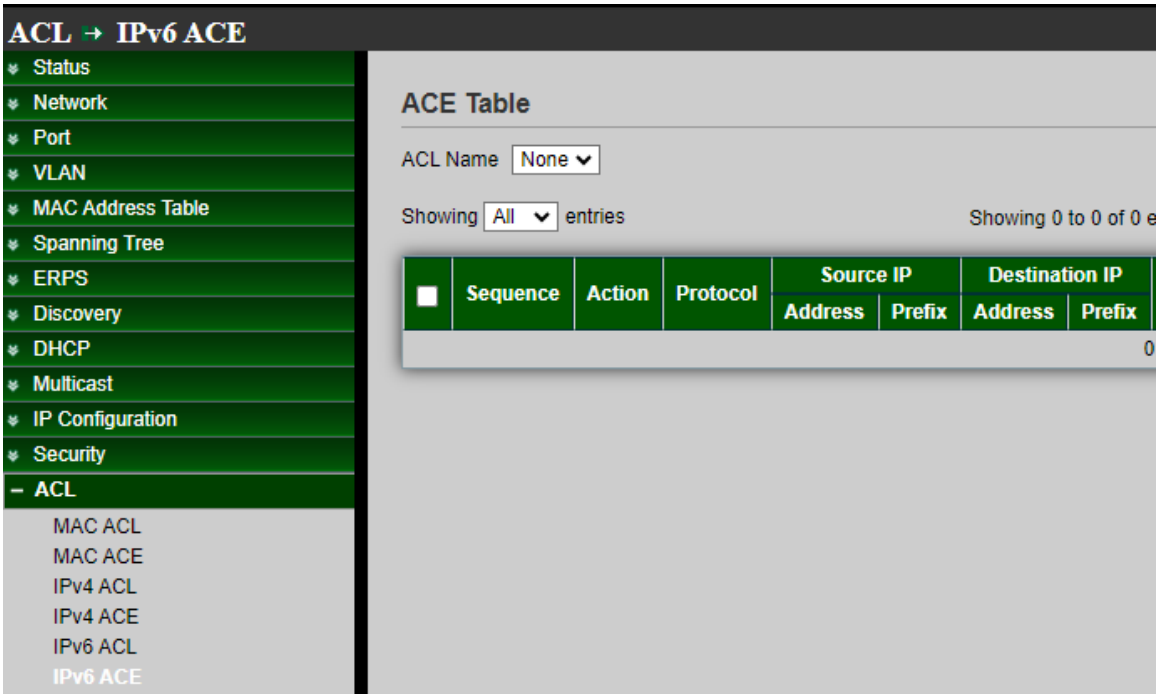
*點擊"Apply"儲存您的變更設定。*

| 欄位 | 描述 |
|---|---|
| ACL Name | 顯示IPv6 ACL名稱 |
| Rule | 顯示ACL的ACE規則數量 |
| Port | 顯示與該ACL綁定的連接埠列表 |

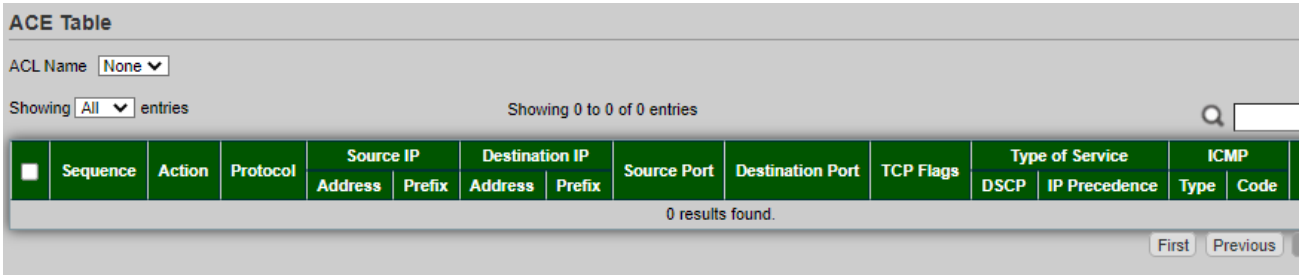
*點擊 "Delete" 刪除選中的列表。*

## 15.6 IPv6 ACE

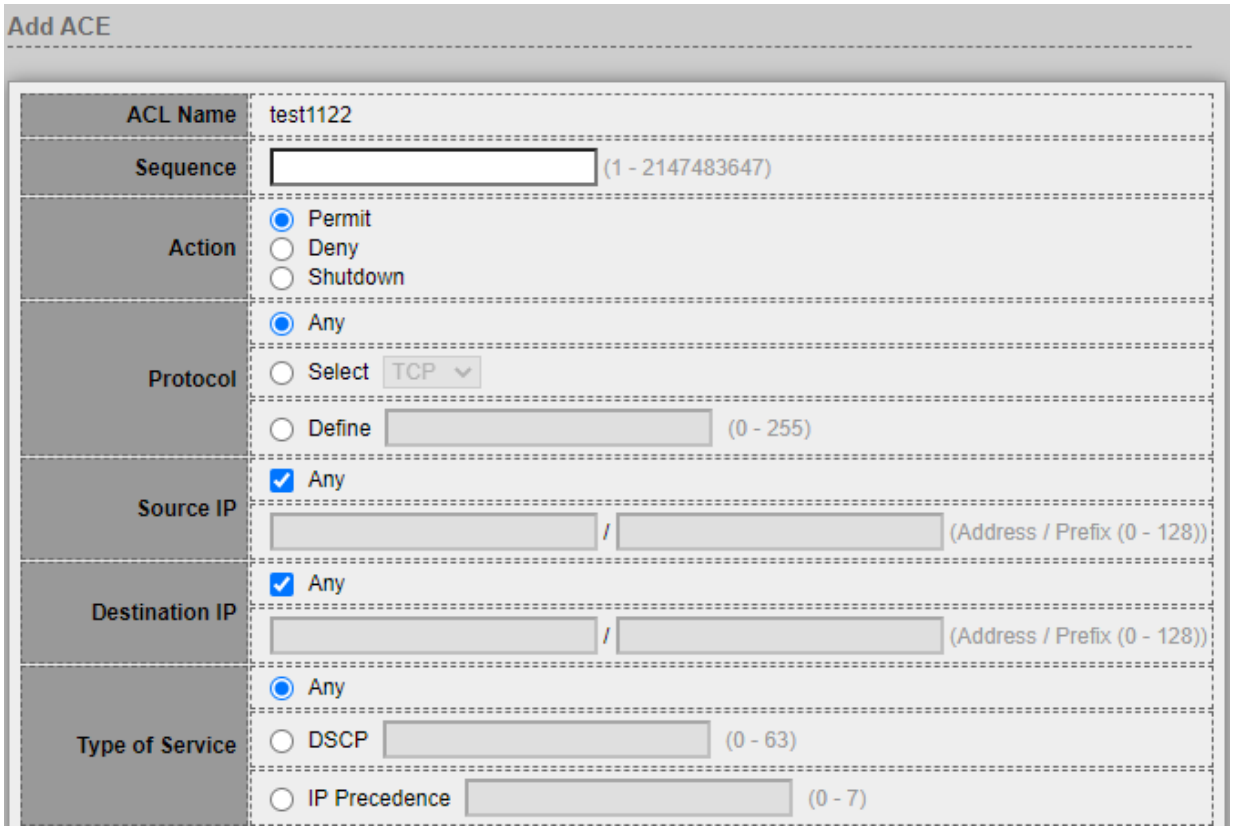
此頁面允許使用者新增、編輯或刪除 ACE 規則。如果 ACL 處於綁定狀態，則無法新增、編輯或刪除 ACE 規則。設定"add"、"Edit"和"Delete"功能進行管理。




- **ACL Name :** 選擇要新增 ACE 的 ACL 名稱。




| 欄位 | 描述 |
|---|---|
| Sequence | 顯示ACE序列 |
| Action | 顯示ACE的操作 |
| Protocol | 顯示ACE的協議值 |
| Source IP | 顯示ACE的來源MAC位址和遮罩:<br>• **Address :** 顯示IPv6 IP位址<br>• **Mask :** 顯示遮罩位址 |
| Destination IP | 顯示ACE的目的MAC位元址和遮罩 :<br>• **Address :** 顯示IPv6 IP位址<br>• **Mask :** 顯示遮罩位址 |
| Source Port | 顯示ACE的單一來源連接埠或一系列來源連接埠。僅當協定為TCP或UDP時可用 |
| Destination Port | 顯示ACE的單一目的連接埠或一系列目的連接埠。僅當協定為TCP或UDP時可用 |
| TCP Flags | 顯示ACE 的TCP指標值。僅當協定為TCP時可用 |
| Type of Service | 顯示ACE的Tos值，可以是DSCP或IP優先級 |
| ICMP | 顯示ACE的ICMP類型和代碼。僅當協定為ICMP時可用 |




- **ACL Name :** 顯示要新增 ACE 的 ACL 名稱。
- **Sequence :** 指定 ACE 的序列，優先處理序列較高的 ACE(1 為最高優先級)。僅適用於 “Add” 對話框。
- **Action :** 使用者管理員可以選擇匹配封包後的操作。
  - **Permit :** 轉發匹配 ACE 規則的封包。
  - **Deny :** 丟棄匹配 ACE 規則的封包。
  - **Shutdown :** 丟棄符合 ACE 規則的封包，並停用接收封包的連接埠。可以從 “Port Settings” 頁面重新啟動此類連接埠。
- **Protocol :** 使用者管理員可以選擇匹配的協定類型。
  - **Any (IP) :** 所有 IP 協定均可接受。
  - **Select from list :** 從下拉選單中選擇以下協定之一。(ICMP/IPinIP/TCP/EGP/IGP/UDP/HMP/RDP/IPV6/IPV6 : ROUT/IPV6 : FRAG/ RSVP/IPV6 : ICMP/OSPF/PIM/L2TP)
  - **Protocol ID to match :** 輸入協定 ID。
- **Source IP :** 選擇來源 IP 位址的類型。
  - **Any :** 所有來源位址均可接受。

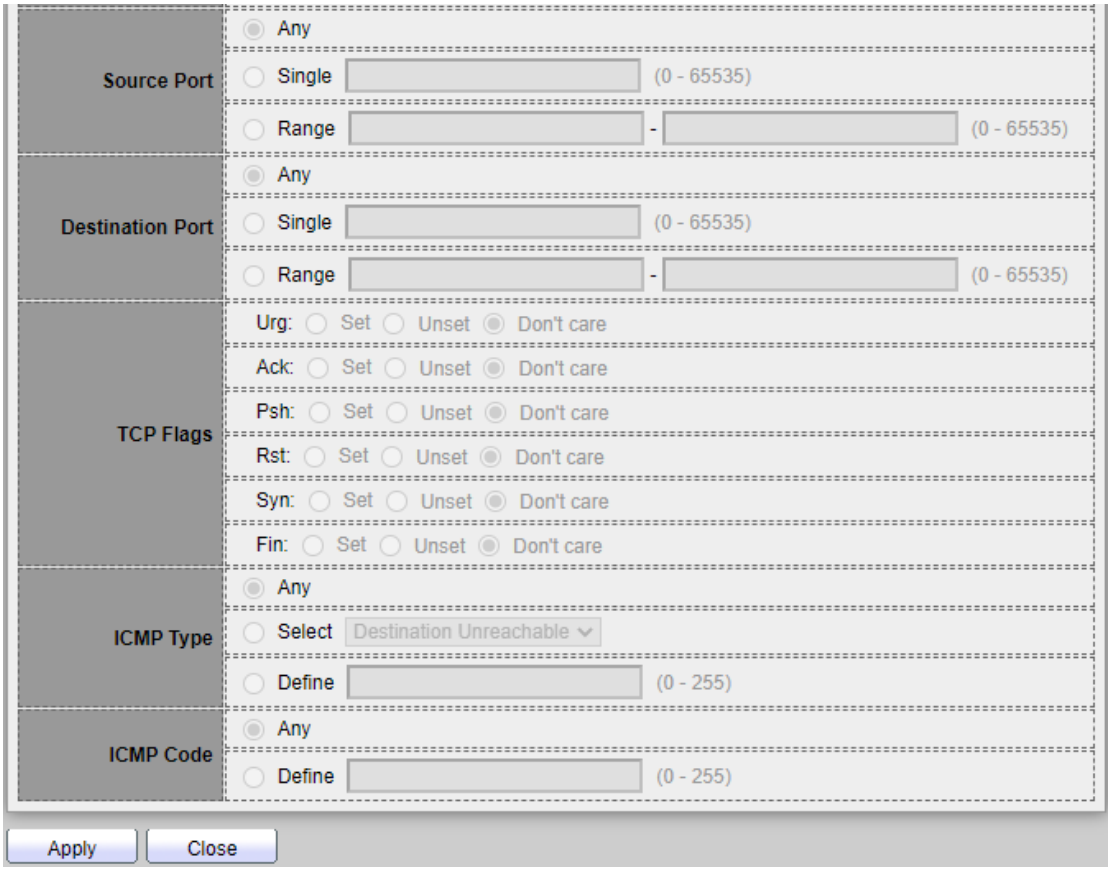
- **User Defined :** 僅接受使用者定義的來源位址或來源位址範圍。輸入要匹配的來源 IP 位址值和遮罩。

➢ **Destination IP :** 選擇目的 IP 位元址的類型。

- **Any :** 所有目的位元址均可接受。
- **User Defined :** 僅接受使用者定義的目的位元址或目的位元址範圍。輸入要匹配的目的 IP 位元址值和遮罩。

➢ **Type of Service :** 選擇要匹配的服務類型。

- **Any :** 所有服務類型均可接受。
- **DSCP to match :** 輸入要匹配的差分服務代碼點(DSCP)。
- **IP Precedence to match :** 輸入要匹配的 IP 優先級別。




➢ **Source Port :** 選擇匹配的協定類型。僅當協定為 TCP 或 UDP 時可用。

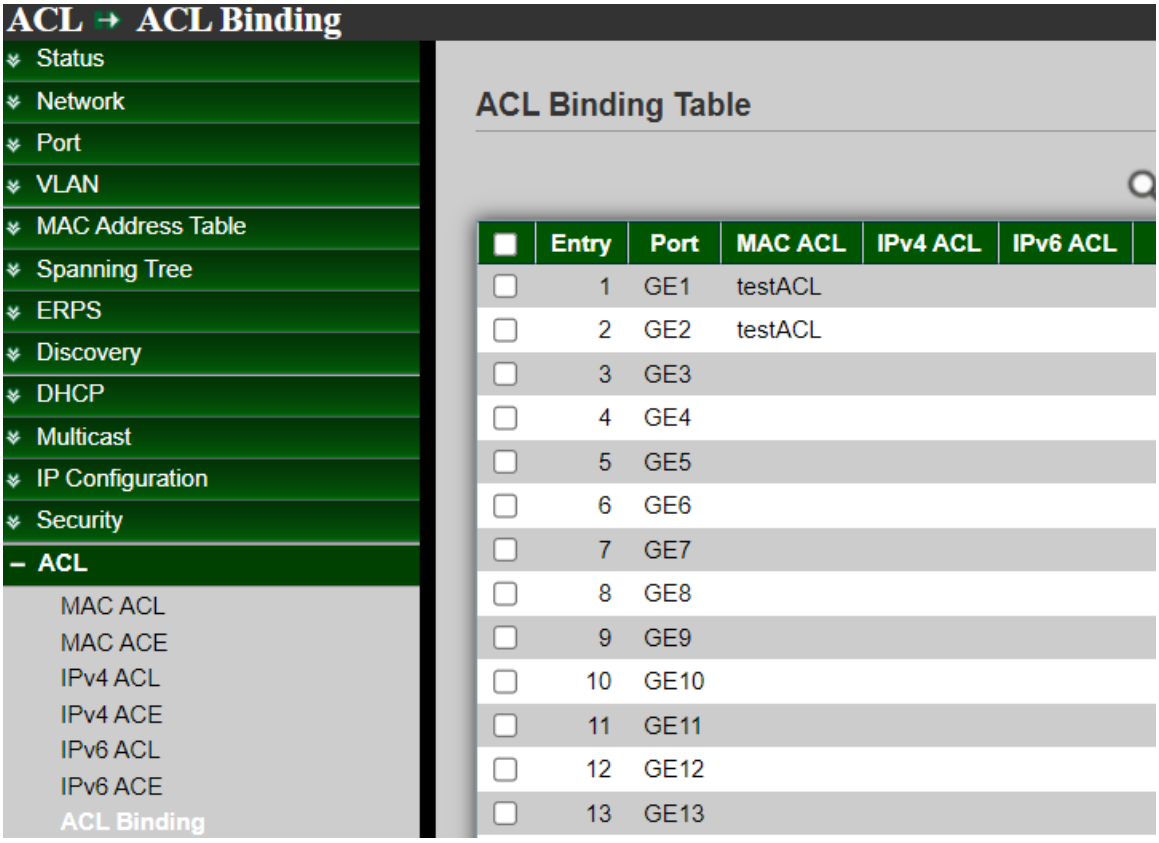
- **Any :** 所有來源連接埠均可接受。
- **Single :** 輸入匹配封包的單個 TCP/UDP 來源埠。
- **Range :** 選擇匹配封包的 TCP/UDP 來源埠範圍。可以設定八個不同的連接埠範圍(在來源連接埠和目的連接埠之間共用)。TCP 和 UDP 協定各有八個連接埠範圍。

- **Destination Port :** 選擇匹配的協定類型。僅當協定為 TCP 或 UDP 時可用。
  - **Any :** 所有目的連接埠均可接受。
  - **Single :** 輸入匹配封包的單個 TCP/UDP 目的埠。
  - **Range :** 選擇匹配封包的 TCP/UDP 目的埠範圍。可以設定八個不同的連接埠範圍(在來源連接埠和目的連接埠之間共用)。TCP 和 UDP 協定各有八個連接埠範圍。
- **TCP Flags :** 選擇一個或多個用於過濾封包的 TCP 指標。過濾後的封包要則被轉發，要則被丟棄。透過 TCP 指標過濾封包可增強封包控制，進而提高網路安全性。僅當協定為 TCP 時可用。
  - **Set :** 如果 TCP 指標為 SET，則匹配。
  - **Unset :** 如果 TCP 指標為 NOT SET，則匹配。
  - **Don’ t care :** 忽略 TCP 指標。
- **ICMP Type :** 按名稱選擇訊息類型或輸入訊息類型編號。僅當協定為 ICMP 時可用。
  - **Any :** 所有訊息類型均可接受。
  - **Select from list :** 通過名稱選擇訊息類型。
  - **Protocol ID to match :** 輸入訊息類型編號。
- **ICMP Code :** 選擇 ICMP 代碼類型。僅當協定為 ICMP 時可用。
  - **Any :** 所有代碼均可接受。
  - **User Defined :** 輸入要匹配的 ICMP 代碼。

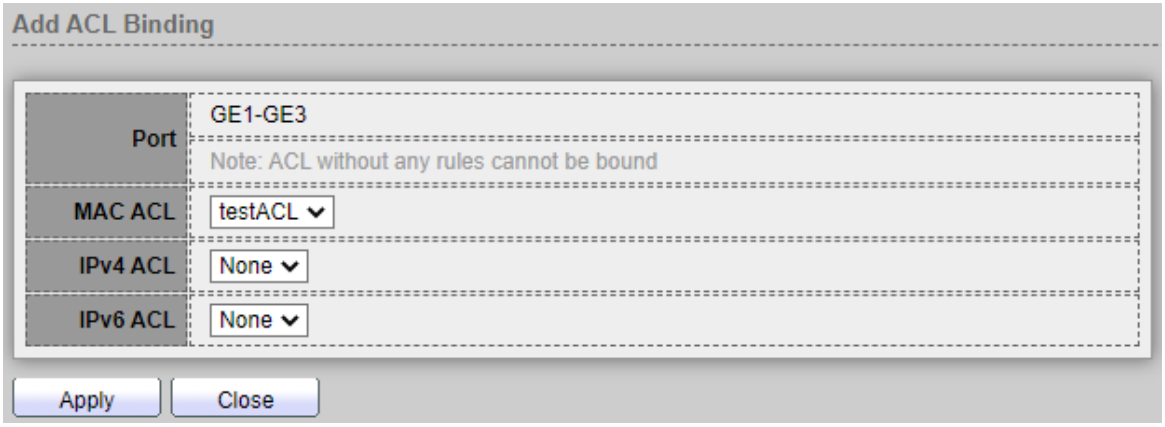
*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

## 15.7 ACL 綁定(ACL Binding)

此頁面允許使用者將 ACL 規則綁定到介面或從介面取消綁定。 IPv4 ACL 和 Ipv6 ACL 不能同時綁定到同一個連接埠，使用者管理員可以從 ACL 綁定表中選擇連接埠。當 ACL 綁定到介面時，其 ACE 規則將應用於到達該介面的封包。與 ACL 中任何 ACE 都不匹配的封包將匹配預設規則，預設操作是丟棄不匹配的封包。




| 欄位 | 描述 |
|---|---|
| Port | 顯示連接埠清單ID |
| MAC ACL | 顯示介面綁定的MAC ACL名稱。空表示沒有規則綁定 |
| IPv4 ACL | 顯示介面綁定的IPv4 ACL名稱。空表示沒有規則綁定 |
| IPv6 ACL | 顯示介面綁定的IPv6 ACL名稱。空表示沒有規則綁定 |




- **Port :** 顯示所選的連接埠編號。
- **MAC ACL :** 綁定到介面的 MAC ACL。從列表中選擇要綁定的 MAC ACL 名稱。
- **IPv4 ACL :** 綁定到介面的 IPv4 ACL。從列表中選擇要綁定的 IPv4 ACL 名稱。
- **IPv6 ACL :** 綁定到介面的 IPv6 ACL。從列表中選擇要綁定的 IPv6 ACL 名稱。.

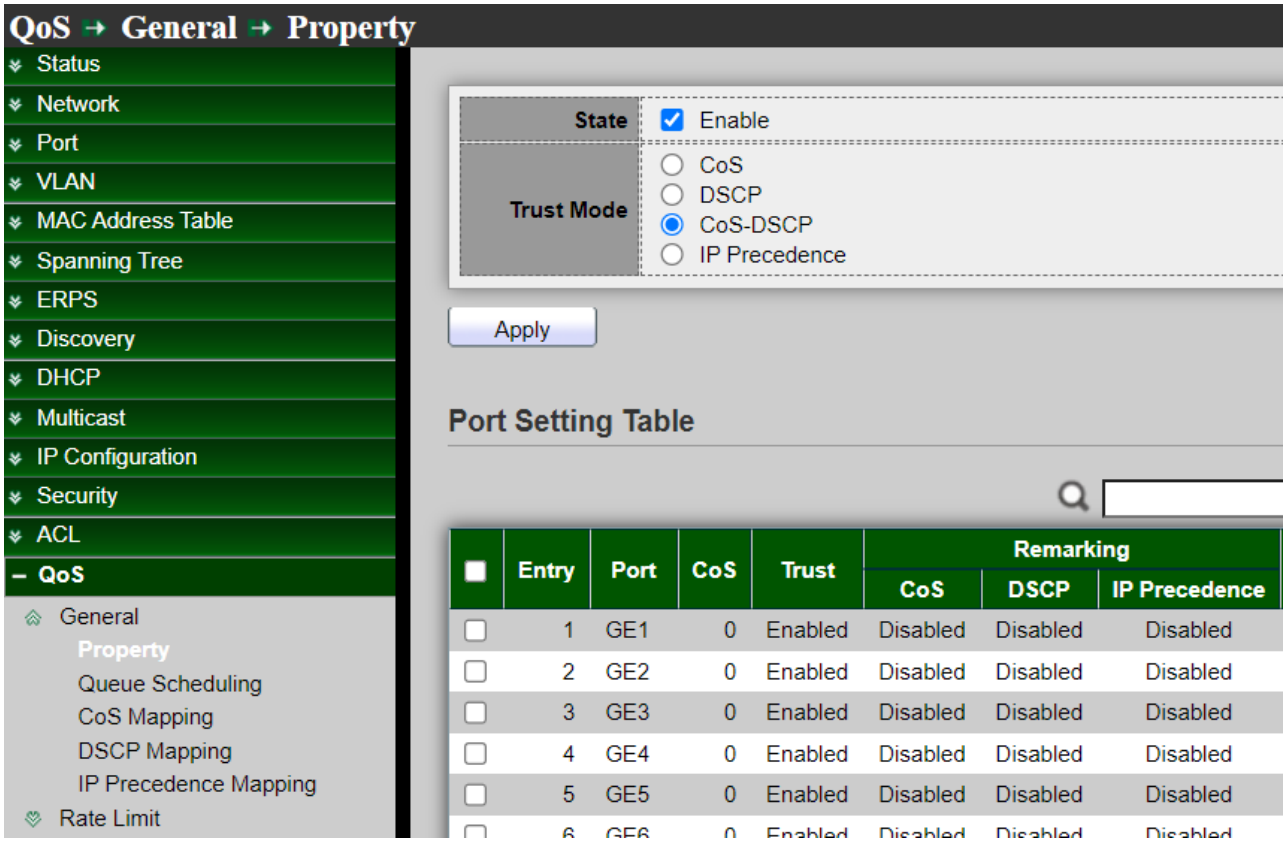
*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

# 16. QoS

服務品質 (QoS) 功能應用於整個網絡，以確保網路流量根據所需標準進行優先排序，並且優先處理所需流量。

## 16.1 屬性(Property)

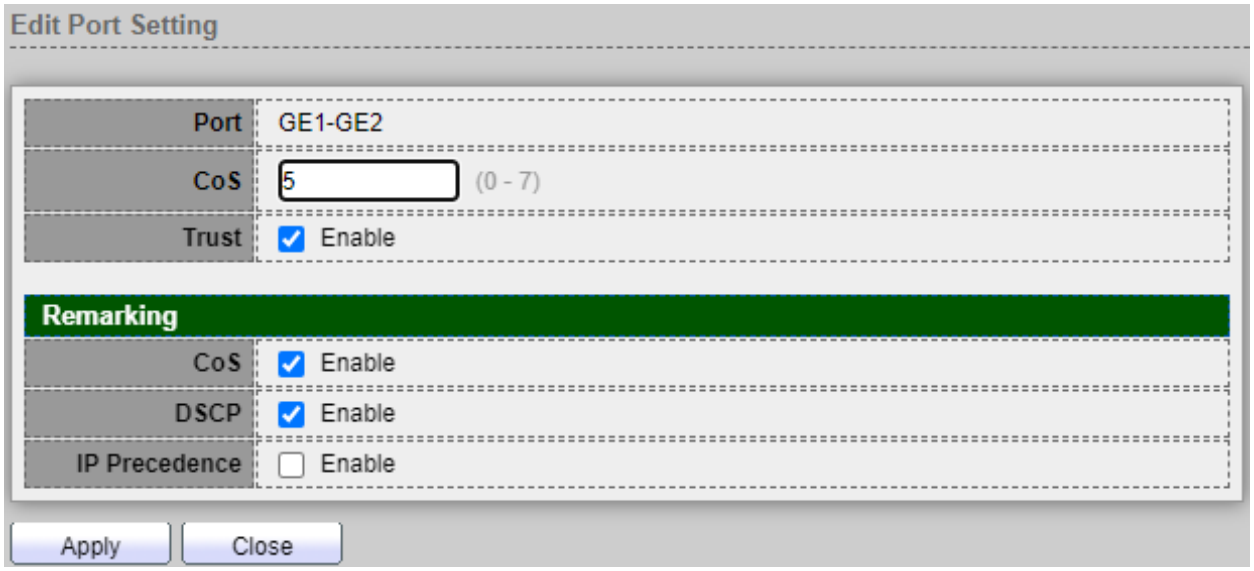
QoS 功能用於優化網路效能，使用 QoS 常規頁面進行通用設定




- **State :** 使用者管理員啟用或取消啟用 Qos 功能。
- **Trust Mode :** 使用者管理員可以選擇 CoS / DSCP / CoS-DSCP / IP Precedence 模式。
  - **CoS :** 流量會根據 VLAN 標記中的 CoS 欄位或每個連接埠的預設 Cos 值(如果傳入封包沒有 VLAN 標記)映射到佇列，CoS 到佇列的實際映射可在連接埠對話框中設定。
  - **DSCP :** 所有 IP 流量都根據 IP 表頭中的 DSCP 欄位映射到佇列。DSCP 到佇列的實際映射可以在 DSCP 對映頁面上設定。如果流量不是 IP 流量，則將其映射到最佳佇列。
  - **CoS-DSCP :** 選擇對非 IP 流量使用信任 CoS 模式，對 IP 流量使用信任 DSCP 模式。
  - **IP Precedence :** 流量根據 IP 優先級別映射到佇列。IP 優先級別到佇列的實際對應映射可以在 IP 優先級別映射頁面上設定。

*點擊"Apply"儲存您的變更設定。*

| 欄位 | 描述 |
|---|---|
| Port | 連接埠名稱 |
| CoS | 所選連接埠的預設CoS優先級別值 |
| Trust | 連接埠的可信模式:<br>• **Enabled :** 流量將按照全域設定中的可信模式<br>• **Disabled :** 流量將始終按照最佳的服務等級 |
| Remarking (CoS) | 連接埠CoS重新標記管理狀態:<br>• **Enabled :** CoS重新標記已啓用<br>• **Disabled :** CoS重新標記已停用 |
| Remarking (DSCP) | 連接埠DSCP重新標記管理狀態 :<br>• **Enabled :** DSCP重新標記已啓用<br>• **Disabled :** DSCP重新標記已停用 |




- **Port :** 顯示所選連接埠編號。
- **CoS :** 設定所選連接埠的預設 CoS/802.1p 優先級別值，設定為傳入封包(沒有 VLAN 標記)分配的預設 CoS 值。範圍是 0 到 7。
- **Trust :** 選中復選框以啟用/停用連接埠的可信狀態。
- **Remarking :**
  - **CoS :** 選中複選框以啟用/停用連接埠 CoS 重新標記，流量根據 VLAN 標記中的 VPT 欄位或根據每個連接埠預設 CoS 值(如果傳入封包上沒有 VLAN 標記)映射到佇列，VPT 到佇列的實際映射可以在 “CoS to Queue” 頁面上設定。

- **DSCP :** 設定複選框以啟用/停用連接埠 DSCP 重新標記，所有 IP 流量都根據 IP 表頭中的 DSCP 欄位映射到佇列。DSCP 到佇列的實際映射可以在 “DSCP to Queue” 頁面上設定。如果流量不是 IP 流量，則將其映射到最佳佇列。
- **IP Precedence :** 選中復選框以啟用/停用連接埠 IP 優先級別重新標記，流量根據 IP 優先級別映射到佇列。IP 優先級別到佇列的實際映射可以在 “IP Precedence to Queue” 頁面上設定。

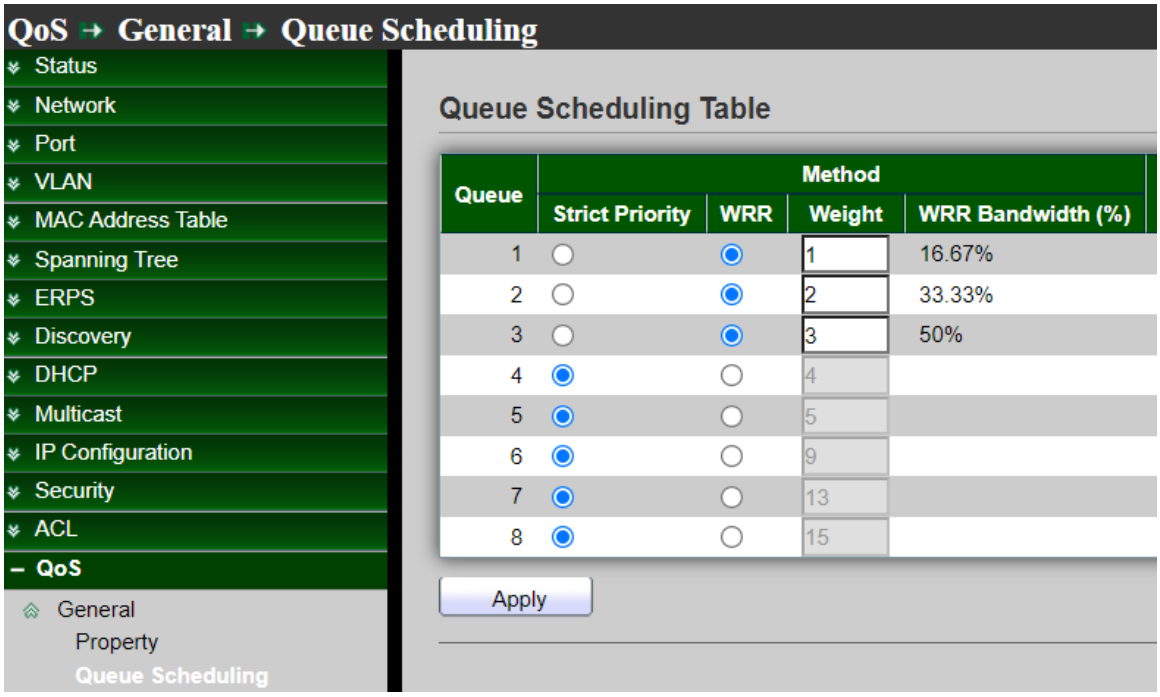
*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

## 16.2 佇列調度(Queue Scheduling)

交換器每個介面支援 8 個佇列。佇列 8 是最高優先級別佇列。佇列 1 是最低優先級別佇列。決定佇列流量處理方式的方法有兩種：嚴格優先級別 (SP) 和加權輪詢 (WRR)。

- 嚴格優先級別 (SP)—首先傳輸來自最高優先級別佇列的出口流量。來自較低佇列的流量僅在最高佇列傳輸完畢後才被處理，這為編號最高的佇列提供了最高優先級別的流量。
- 加權輪詢 (WRR)—在 WRR 模式下，從佇列發送的封包數量與佇列的權重成正比(權重越高，發送的訊框越多)。

佇列模式可以在Queue頁面上選擇。當佇列模式為嚴格優先級別時，優先級別會設定佇列的服務順序，從 queue 8 (最高優先級別)開始，每個佇列服務後轉到下一個級別較低的佇列。
當佇列模式為加權輪詢時，佇列將服務直到其配額用完，然後再服務另一個佇列。也可以將一些級別較低的佇列分配給 WRR，同時將一些級別較高的佇列保留為嚴格優先級別。在這種情況下，SP 佇列的流量始終在 WRR 佇列的流量之前發送。 SP 佇列清空後，將轉送 WRR 佇列中的流量。(每個 WRR 佇列的比例部分取決於其權重)。

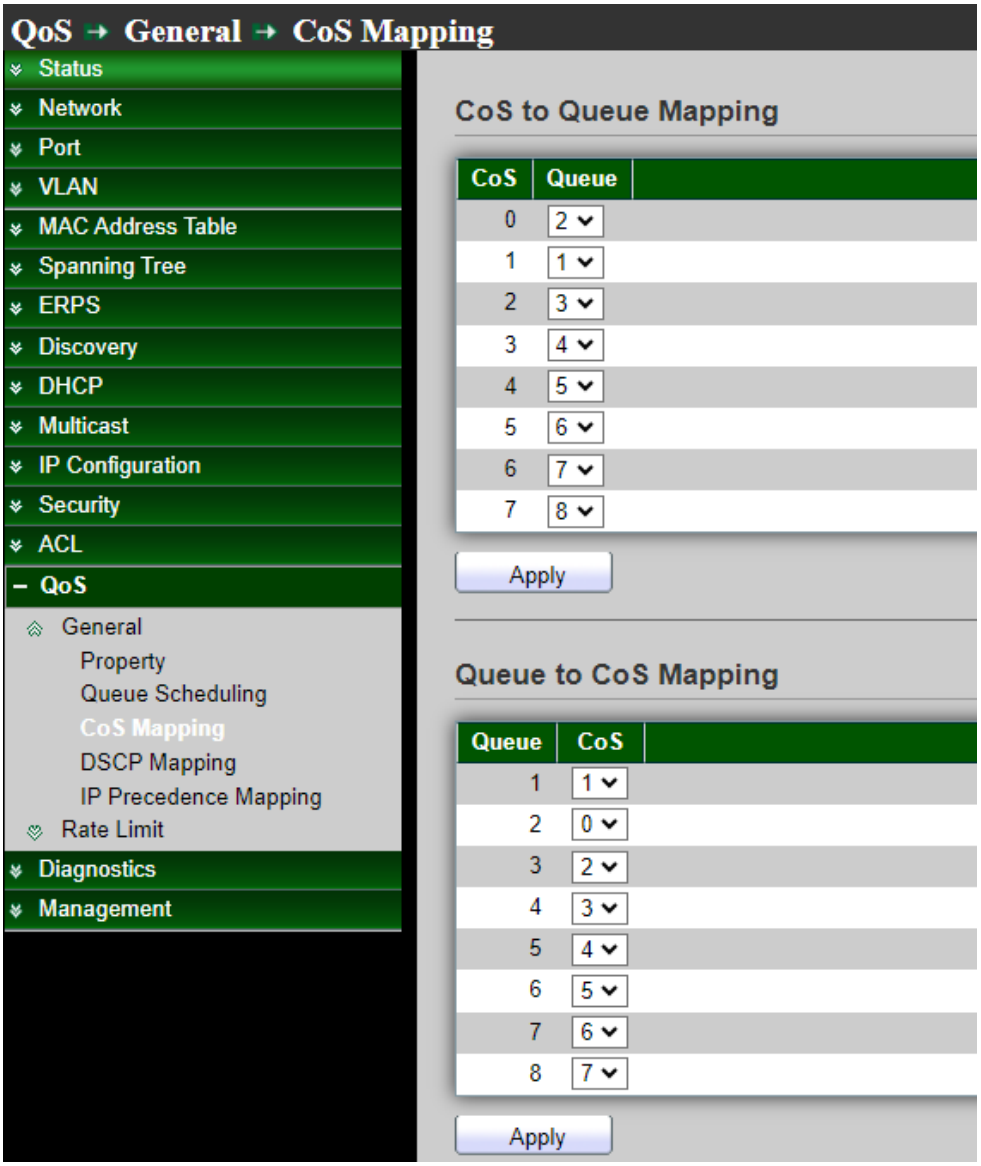



| 欄位 | 描述 |
|---|---|
| Queue | 要設定的佇列ID |
| Strict Priority | 設定佇列為嚴格優先級別類型 |
| WRR | 設定佇列為加權輪詢類型 |
| Weight | 如果佇列類型是WRR，則設定佇列的佇列權重 |
| WRR Bandwidth | WRR佇列頻寬百分比 |

*點擊"Apply"儲存您的變更設定。*

## 16.3 Cos 映射(CoS Mapping)

“CoS to Queue” 表根據 VLAN 標記中的 802.1p 優先級別決定傳入封包的出口佇列。對於傳入的 untagged 封包，802.1p 優先級別是分配給入口埠的預設 CoS/802.1p 優先級別。使用 “Queues to CoS” 表為每個佇列中的出口流量標記 CoS/802.1p 優先級別。




## CoS to Queue Mapping

- **CoS :** CoS 值。
- **Queue :** 選擇 Cos 值的佇列 ID。

*點擊"Apply"儲存您的變更設定。*

## Queue to CoS Mapping

- **Queue :** 佇列 ID。
- **Cos :** 選擇佇列 ID 的 Cos 值。

*點擊"Apply"儲存您的變更設定。*

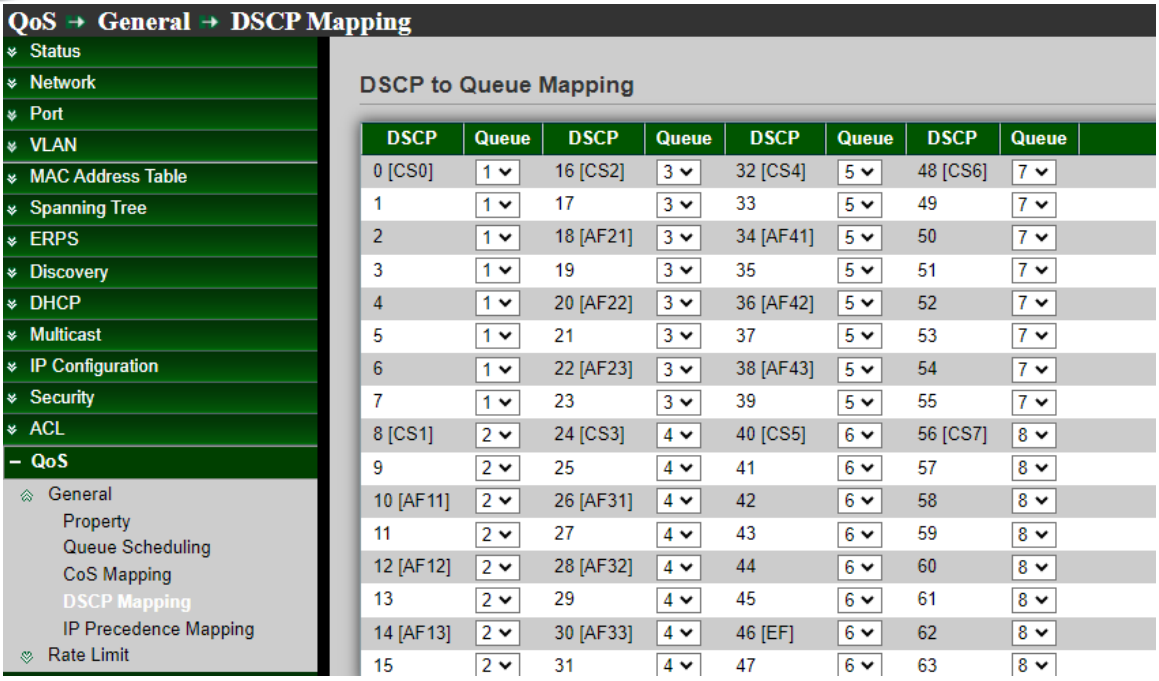
| CoS (0 to 7)<br>7 為最大值 | Queue(1 to 8)<br>8 為最高優先級別 | 描述 |
|---|---|---|
| 0 | 2 | 背景 |
| 1 | 1 | 最佳 |
| 2 | 3 | 出色的工作 |
| 3 | 4 | 關鍵應用 LSV 電話 SIP |
| 4 | 5 | 視頻 |
| 5 | 6 | 語音 Cisco IP 電話預設值 |
| 6 | 7 | 互通控制 LSV 電話 RTP |
| 7 | 8 | 網路控制 |

## 16.4 DSCP 映射(DSCP Mapping)

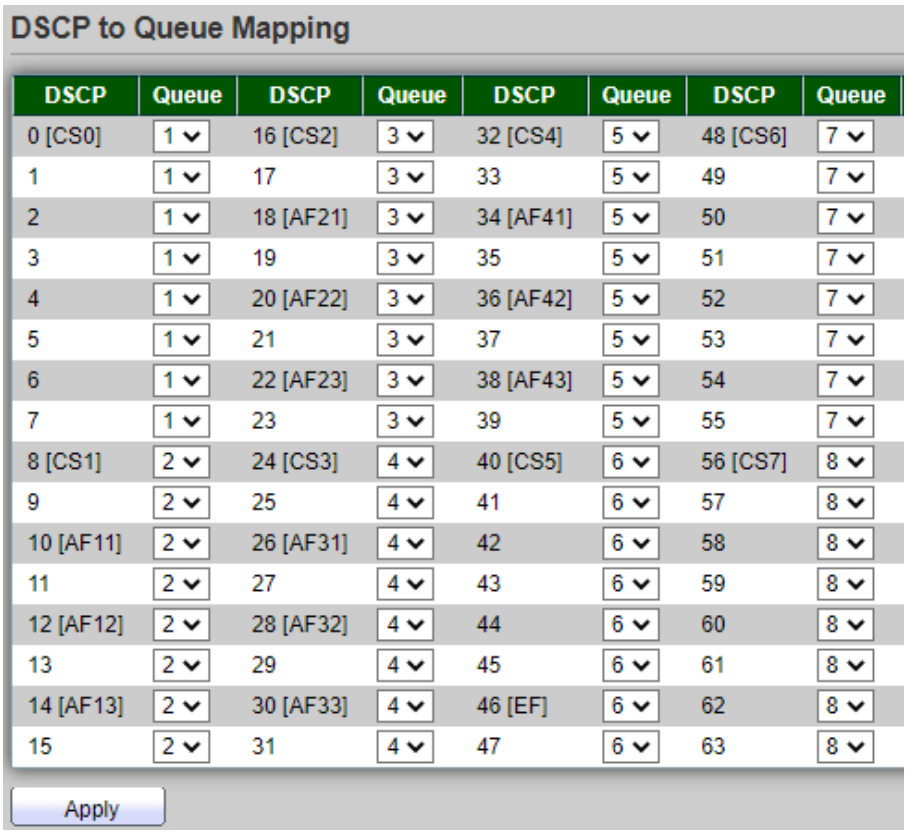
“DSCP to Queue”表根據傳入 IP 封包的 DSCP 值決定其出口佇列。封包的原始 VLAN 優先級別標記(VPT)保持不變。

DSCP 值的範圍為 0 至 63，而內部轉發優先級別範圍為 1 至 8。給定範圍內的任何 DSCP 值都會映射到相應的內部轉發優先級別值。其中包括 CS(類選擇器)、AF(確保轉發)和 EF(加急轉發)。例如，DSCP 標記值為 1 的封包可分配到高優先佇列。

使用“Queues to CoS”頁面為每個佇列中的出口流量標記 DSCP 值。



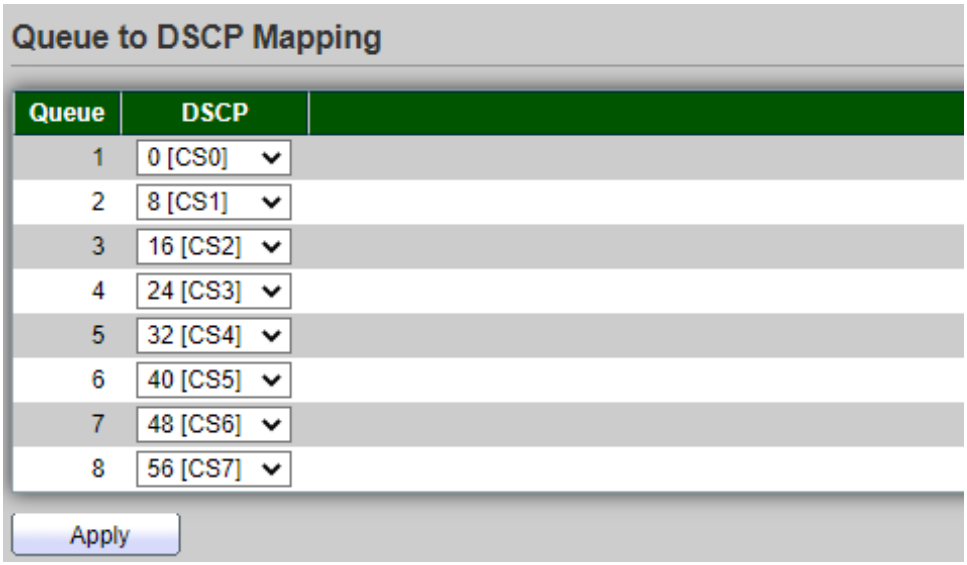

## DSCP to Queue Mapping




- **DSCP** : DSCP 值。
- **Queue** : 選擇 DSCP 值的佇列 ID。

*點擊"Apply"儲存您的變更設定。*

### Queue to DSCP Mapping

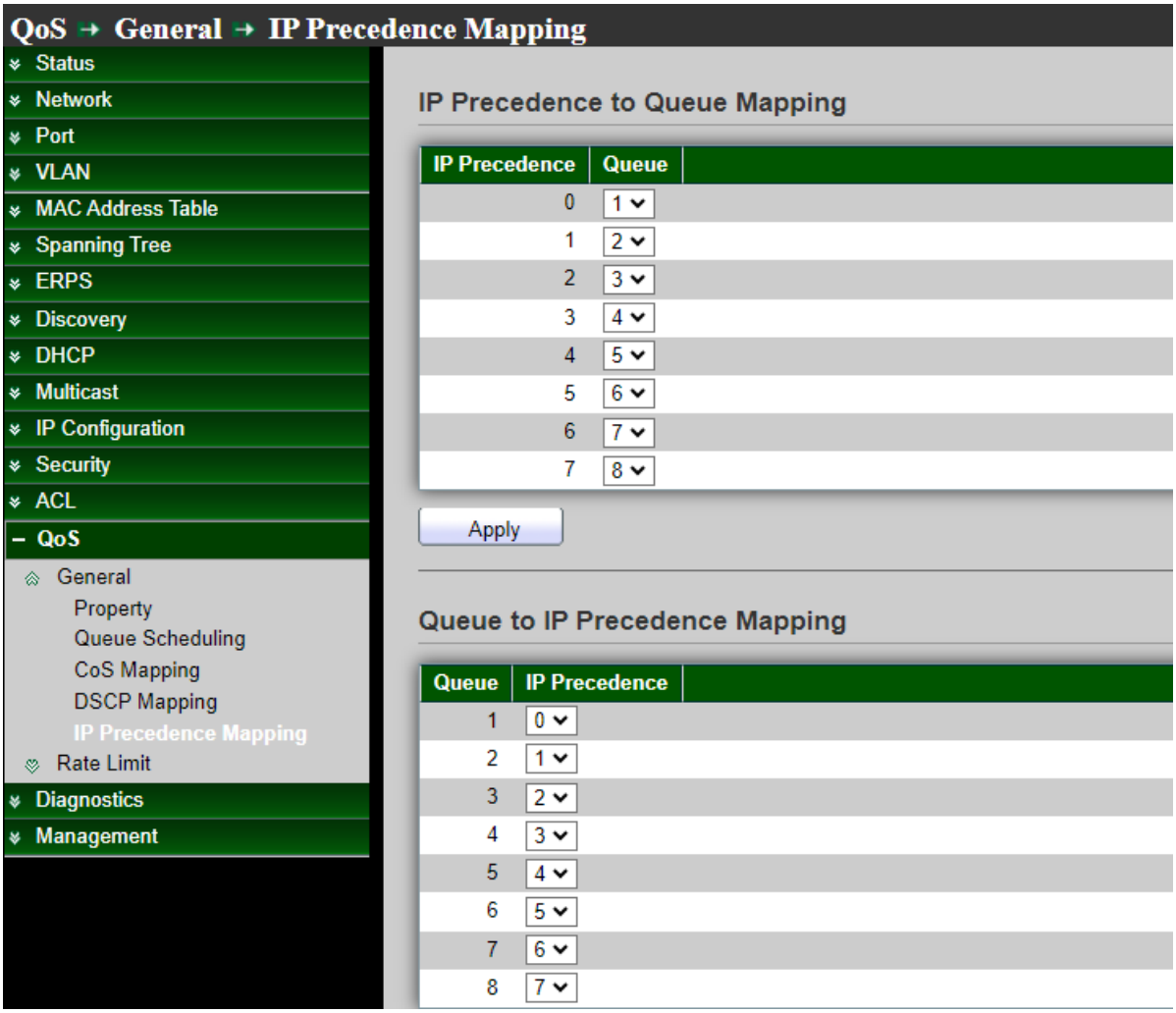



- **Queue :** 佇列 ID。
- **DSCP :** 選擇佇列 ID 的 DSCP 值。

*點擊"Apply"儲存您的變更設定。*

## 16.5 IP 優先級別到佇列映射(IP Precedence to Queue Mapping)

此頁面允許使用者設定 IP 優先級別到佇列映射以及佇列到 IP 優先級別映射，IP 優先級別標準使用 ToS 位元組的前 3 位來標記封包的 8 個優先級別，編號為 0-7，其中 0 為最低優先級別，7 為最高優先級別。由於 IP 優先級別和 ToS 使用 ToS 位元組中不同的位元來標記封包的優先級別，因此它們可以共存於同一封包頭中，且互不幹擾。




## IP Precedence to Queue mapping

- **IP Precedence :** IP 優先級別值。
- **Queue :** IP 優先級別映射的佇列值。

*點擊"Apply"儲存您的變更設定。*

## Queue to IP Precedence mapping

- **Queue :** 佇列值。
- **IP Precedence :** 佇列映射的 IP 優先級別值。

*點擊"Apply"儲存您的變更設定。*

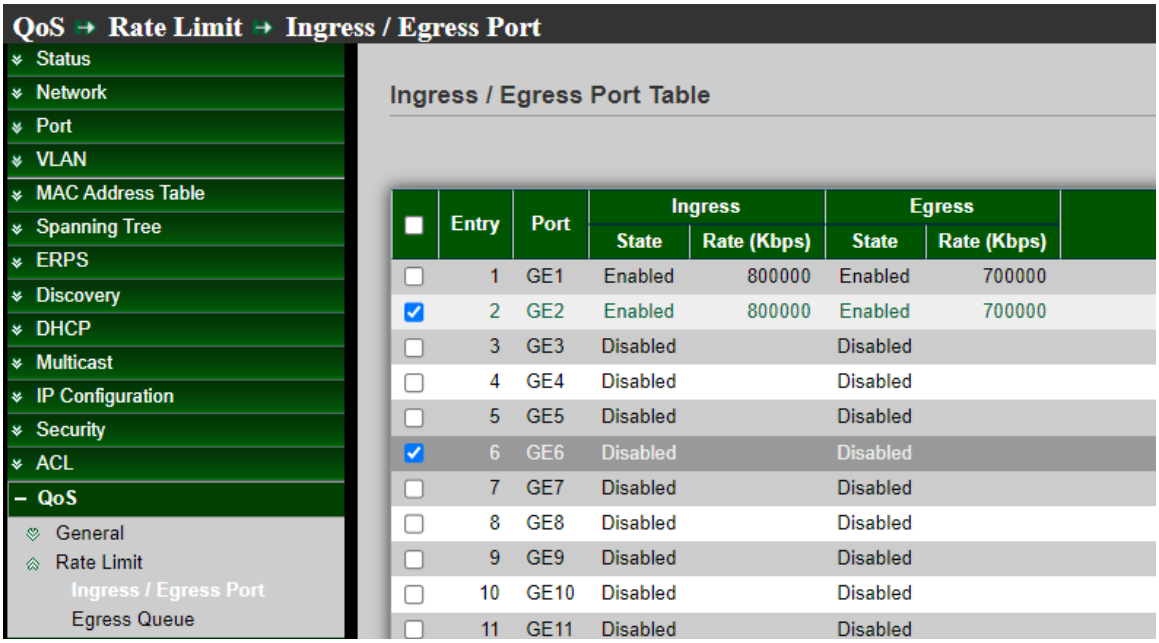
# 16.6 速率限制(Rate Limit)

此頁面允許使用者設定入口埠速率限制和出口埠速率限制。入口速率限制是每秒可以從入口介面接收的位元數。超過此限制的多餘頻寬將被丟棄。

## 16.6.1 入口/出口埠(Ingress / Egress Port)

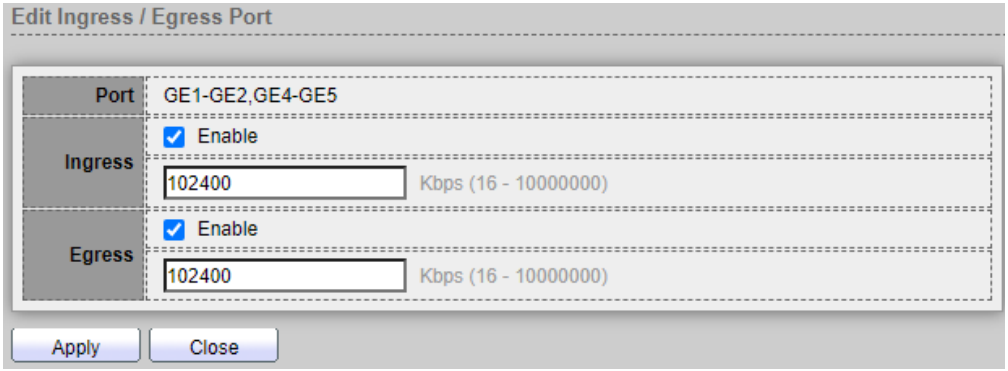
速率限制功能可以設定特定介面上的輸入/輸出流量限制。

使用者管理員可以設定連接埠的入口/出口速率限制。使用速率為 16 至 10000000Kbps。




| 欄位 | 描述 |
|---|---|
| Port | 連接埠名稱 |
| Trust | 連接埠入口速率限制狀態 ：<br>• **Enabled :** 啓用入口速率限制功能<br>• **Disabled :** 停用入口速率限制功能 |
| Ingress (Rate) | 顯示連接埠入口速率限制值 |
| Trust | 連接埠出口速率限制狀態 ：<br>• **Enabled :** 啟用出口速率限制狀態 |

| | |
|---|---|
| | • **Disabled :** 停用出口速率限制狀態 |
| **Egress (Rate)** | 顯示連接埠出口速率限制值 |

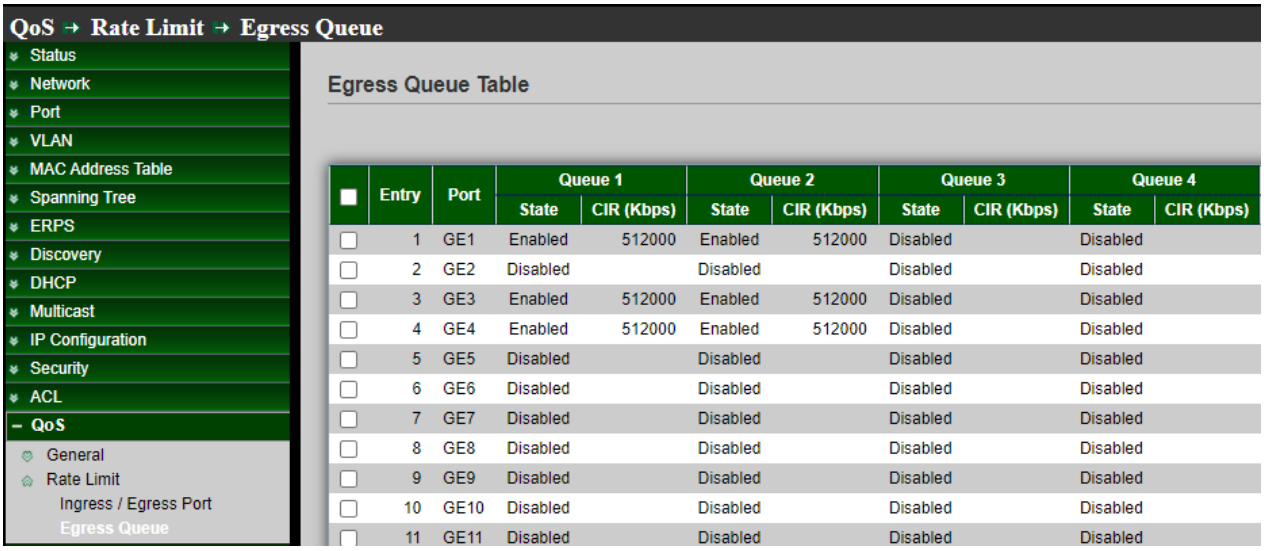



- **Port :** 在連接埠列表選中的復選框。
- **Ingress :** 選中複選框以啟用/停用入口速率限制。如果啟用了入口速率限制，則需要指定速率限制值，控制範圍為 “16-10000000 Kbps” 。
- **Egress :** 選中複選框以啟用/停用出口速率限制。如果啟用了出口速率限制，則需要指定速率限制值，控制範圍為 “16-10000000 Kbps” 。

*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

### 16.6.2 出口佇列(Egress Queue)

出口佇列功能可以通過 QoS 設定優先級別佇列。出口速率限制是通過調整輸出負載來實現的。使用者管理員可以通過限制 Qos 設定入口佇列。使用速率為 16 至 1000000 Kbps，請點擊"Edit"編輯設定出口佇列連接埠選單。



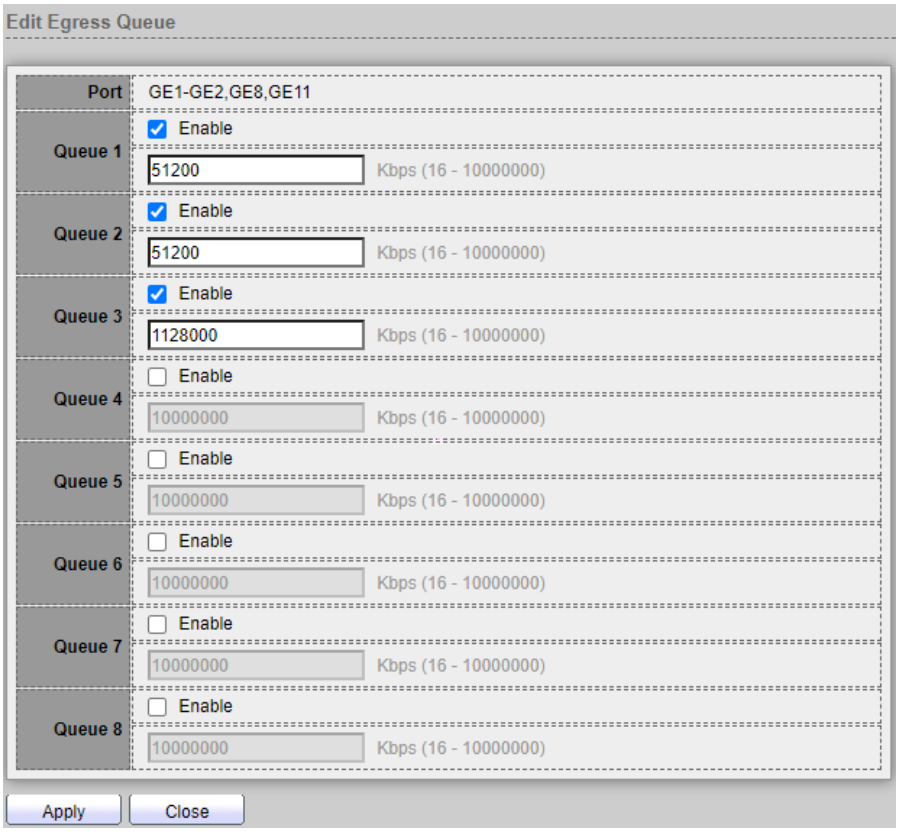

| Entry | Port | Queue 1 | | Queue 2 | | Queue 3 | | Queue 4 | |
|---|---|---|---|---|---|---|---|---|---|
| | | State | CIR (Kbps) | State | CIR (Kbps) | State | CIR (Kbps) | State | CIR (Kbps) |
| 1 | GE1 | Enabled | 512000 | Enabled | 512000 | Disabled | | Disabled | |
| 2 | GE2 | Disabled | | Disabled | | Disabled | | Disabled | |
| 3 | GE3 | Enabled | 512000 | Enabled | 512000 | Disabled | | Disabled | |
| 4 | GE4 | Enabled | 512000 | Enabled | 512000 | Disabled | | Disabled | |
| 5 | GE5 | Disabled | | Disabled | | Disabled | | Disabled | |
| 6 | GE6 | Disabled | | Disabled | | Disabled | | Disabled | |
| 7 | GE7 | Disabled | | Disabled | | Disabled | | Disabled | |
| 8 | GE8 | Disabled | | Disabled | | Disabled | | Disabled | |
| 9 | GE9 | Disabled | | Disabled | | Disabled | | Disabled | |
| 10 | GE10 | Disabled | | Disabled | | Disabled | | Disabled | |
| 11 | GE11 | Disabled | | Disabled | | Disabled | | Disabled | |

Egress Queue Table

| Entry | Port | Queue 1 | | Queue 2 | | Queue 3 | | Queue 4 | | Queue 5 | | Queue 6 | | Queue 7 | | Queue 8 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | State | CIR (Kbps) | State | CIR (Kbps) | State | CIR (Kbps) | State | CIR (Kbps) | State | CIR (Kbps) | State | CIR (Kbps) | State | CIR (Kbps) | State | CIR (Kbps) |
| 1 | GE1 | Enabled | 51200 | Enabled | 51200 | Enabled | 62496 | Disabled | | Disabled | | Disabled | | Disabled | | Disabled | |
| 2 | GE2 | Enabled | 51200 | Enabled | 51200 | Enabled | 62496 | Disabled | | Disabled | | Disabled | | Disabled | | Disabled | |
| 3 | GE3 | Disabled | | Disabled | | Disabled | | Disabled | | Disabled | | Disabled | | Disabled | | Disabled | |
| 4 | GE4 | Disabled | | Disabled | | Disabled | | Disabled | | Disabled | | Disabled | | Disabled | | Disabled | |
| 5 | GE5 | Disabled | | Disabled | | Disabled | | Disabled | | Disabled | | Disabled | | Disabled | | Disabled | |
| 6 | GE6 | Disabled | | Disabled | | Disabled | | Disabled | | Disabled | | Disabled | | Disabled | | Disabled | |
| 7 | GE7 | Disabled | | Disabled | | Disabled | | Disabled | | Disabled | | Disabled | | Disabled | | Disabled | |
| 8 | GE8 | Enabled | 51200 | Enabled | 51200 | Enabled | 62496 | Disabled | | Disabled | | Disabled | | Disabled | | Disabled | |
| 9 | GE9 | Disabled | | Disabled | | Disabled | | Disabled | | Disabled | | Disabled | | Disabled | | Disabled | |

| 欄位 | 描述 |
|---|---|
| Port | 連接埠編號介面 |
| Queue 1 (State) | 連接埠出口佇列1速率限制狀態<br>• **Enabled**：啟用出口佇列速率限制<br>• **Disabled**：停用出口佇列速率限制 |
| Queue 1 (CIR) | 佇列1出口調配速率訊息 |
| Queue 2 (State) | 連接埠出口佇列2速率限制狀態<br>• **Enabled**：啟用出口佇列速率限制<br>• **Disabled**：停用出口佇列速率限制 |
| Queue 2 (CIR) | 佇列2出口調配速率訊息 |
| Queue 3 (State) | 連接埠出口佇列3速率限制狀態<br>• **Enabled**：啟用出口佇列速率限制<br>• **Disabled**：停用出口佇列速率限制 |

| | |
|---|---|
| **Queue 3 (CIR)** | 佇列3出口調配速率訊息 |
| **Queue 4 (State)** | 連接埠出口佇列4速率限制狀態<br>• **Enabled :** 啟用出口佇列速率限制<br>• **Disabled :** 停用出口佇列速率限制 |
| **Queue 4 (CIR)** | 佇列4出口調配速率訊息 |
| **Queue 5 (State)** | 連接埠出口佇列5速率限制狀態<br>• **Enabled :** 啟用出口佇列速率限制<br>• **Disabled :** 停用出口佇列速率限制 |
| **Queue 5 (CIR)** | 佇列5出口調配速率訊息 |
| **Queue 6 (State)** | 連接埠出口佇列6速率限制狀態<br>• **Enabled :** 啟用出口佇列速率限制<br>• **Disabled :** 停用出口佇列速率限制 |
| **Queue 6 (CIR)** | 佇列6出口調配速率訊息 |
| **Queue 7 (State)** | 連接埠出口佇列7速率限制狀態<br>• **Enabled :** 啟用出口佇列速率限制<br>• **Disabled :** 停用出口佇列速率限制 |
| **Queue 7 (CIR)** | 佇列7出口調配速率訊息 |
| **Queue 8 (State)** | 連接埠出口佇列8速率限制狀態<br>• **Enabled :** 啟用出口佇列速率限制<br>• **Disabled :** 停用出口佇列速率限制 |
| **Queue 8 (CIR)** | 佇列8出口調配速率訊息 |




選中復選框以啟用/停用出口優先級別佇列 1 –佇列 8 等級，控製範圍為“16-1000000 Kbps”。

- **Port :** 選擇一個或多個連接埠進行設定。
- **Queue 1 :** 選中復選框以啟用/停用出口佇列 1 速率限制。
  - **Enable :** 如果啟用出口速率限制，則需分配速率限制值。
- **Queue 2 :** 選中復選框以啟用/停用出口佇列 2 速率限制。
  - **Enable :** 如果啟用出口速率限制，則需分配速率限制值。
- **Queue 3 :** 選中復選框以啟用/停用出口佇列 3 速率限制。
  - **Enable :** 如果啟用出口速率限制，則需分配速率限制值。
- **Queue 4 :** 選中復選框以啟用/停用出口佇列 4 速率限制。
  - **Enable :** 如果啟用出口速率限制，則需分配速率限制值。
- **Queue 5 :** 選中復選框以啟用/停用出口佇列 5 速率限制。
  - **Enable :** 如果啟用出口速率限制，則需分配速率限制值。
- **Queue 6 :** 選中復選框以啟用/停用出口佇列 6 速率限制。
  - **Enable :** 如果啟用出口速率限制，則需分配速率限制值。
- **Queue 7 :** 選中復選框以啟用/停用出口佇列 7 速率限制。
  - **Enable :** 如果啟用出口速率限制，則需分配速率限制值。

- **Queue 8 :** 選中復選框以啟用/停用出口佇列 8 速率限制。
  - **Enable :** 如果啟用出口速率限制，則需分配速率限制值。

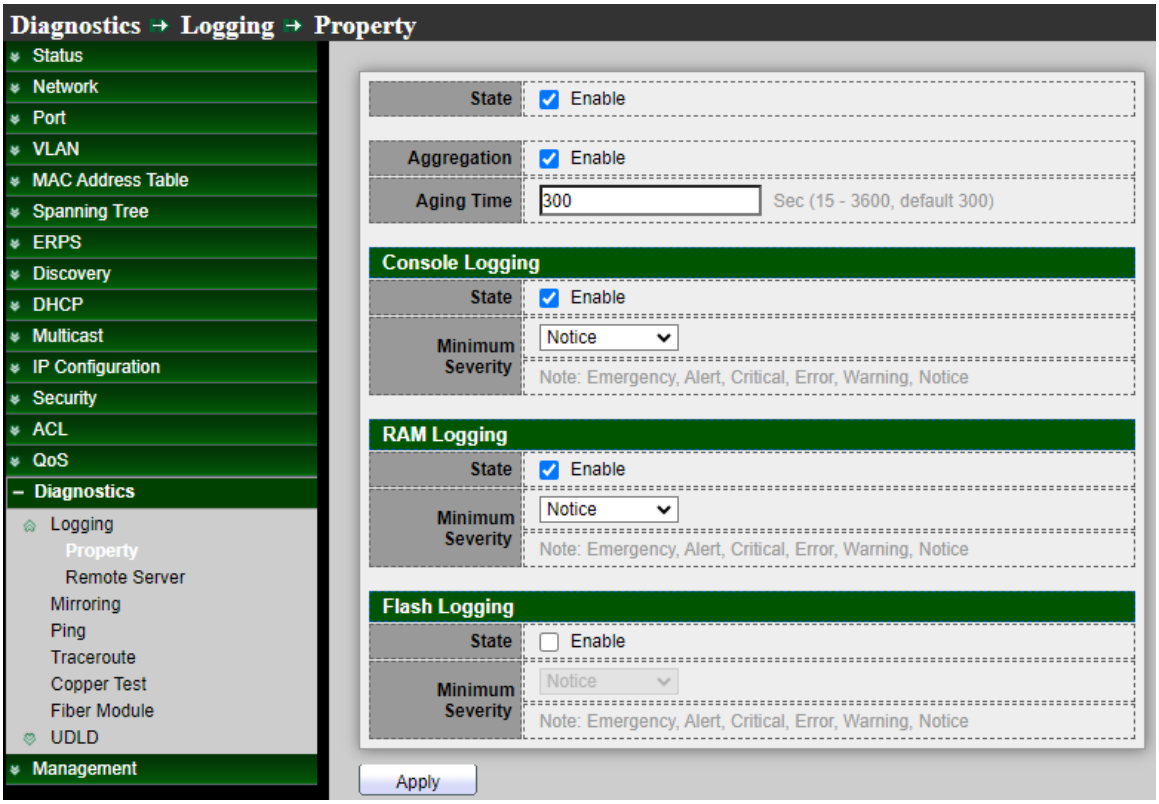
*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

# 17. Diagnostics

## 17.1 日誌(Logging)

### 17.1.1 屬性(Property)

此功能支援將日誌訊息包括 Console / RAM / Flash 訊息發送到遠端日誌伺服器。使用者管理員可以啟用或停用此功能。使用診斷頁面設定交換器診斷功能或操作診斷實用程式。




- **State :** 啟用日誌服務後，可以單獨設定每個目標規則的日誌配置。如果停用日誌服務，則不會向這些目的地傳送任何訊息。
  - **Enable :** 啟用/停用全域日誌服務。

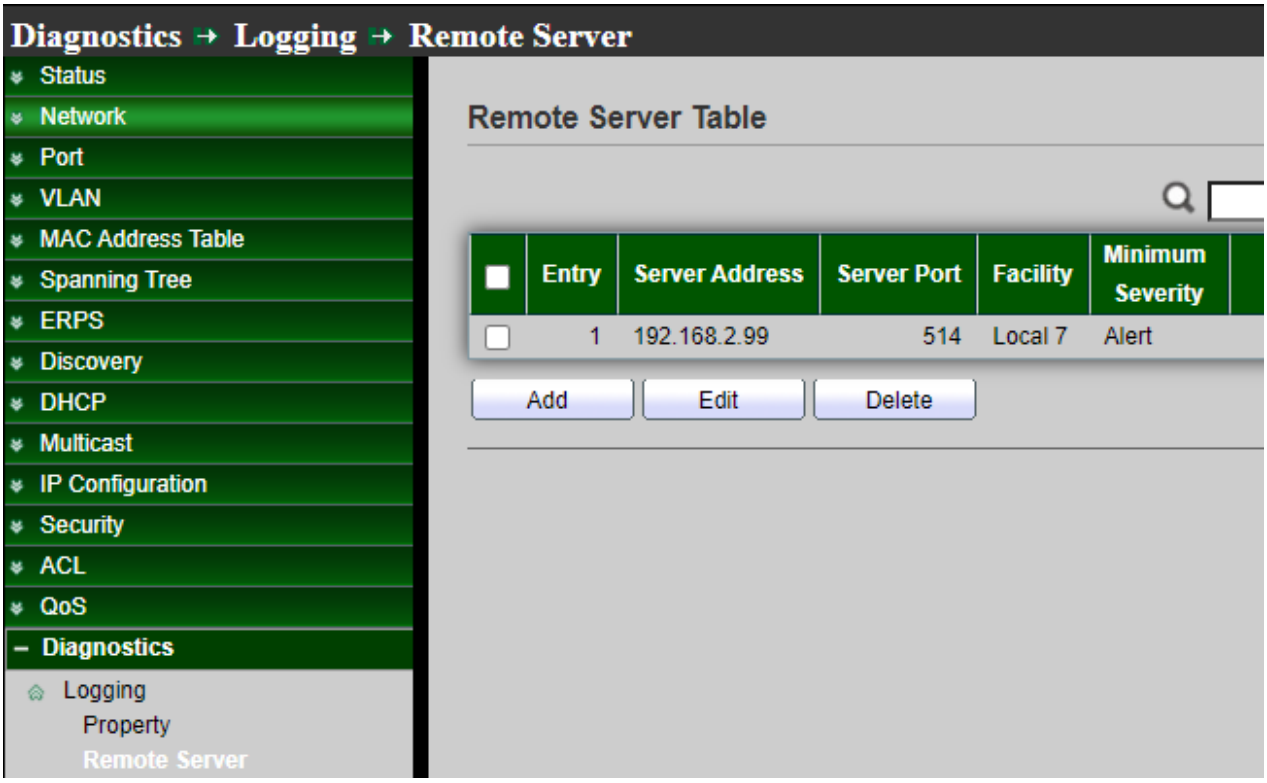
- **Aggregation :**
  - **Enable :** 啟用/停用聚合服務。
  - **Aging :** 延遲時間有效範圍 15~3600 秒。預設為 300 秒。
- **Console Logging :**
  - **State :** 啟用/停用控制台日誌服務。
  - **Minimum Severity :** 發送控制台日誌的最低嚴重級別。包括 Emergency(緊急), Alert(警報), Critical(嚴重), Error(錯誤), Warning(警告), Notice(通知), Information(資訊), Debug(調試)等事件的選擇。
- **RAM Loggong :**
  - **State :** 啟用/停用 RAM 日誌服務。
  - **Minimum Severity :** 發送 RAM 日誌的最低嚴重級別。包括 Emergency(緊急), Alert(警報), Critical(嚴重), Error(錯誤), Warning(警告), Notice(通知), Information(資訊), Debug(調試)等事件的選擇。
- **Flash Loggong :**
  - **State :** 啟用/停用閃存日誌服務。
  - **Minimum Severity :** 發送閃存日誌的最低嚴重級別。包括 Emergency(緊急), Alert(警報), Critical(嚴重), Error(錯誤), Warning(警告), Notice(通知), Information(資訊), Debug(調試)等事件的選擇。

| | |
|---|---|
| Note | •Emergency(緊急)—系統無法使用。<br>•Alert(警報)—需要採取行動。<br>•Critical(嚴重)—系統處於嚴重狀態。<br>•Error(錯誤)—系統處於錯誤狀態。<br>•Warning(警告)—發出系統警告。<br>•Notice(通知)—系統運行正常，但出現系統通知。<br>•Informational(資訊)—設備資訊。<br>•Debug(調試)—事件的詳細訊息。 |

*點擊"Apply"儲存您的變更設定。*

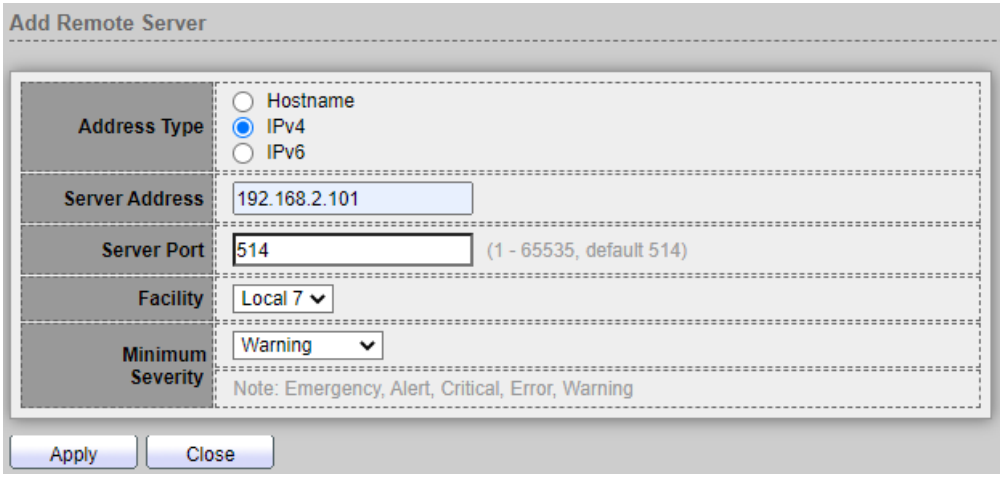
### 17.1.2 遠端伺服器(Remote Server)

使用 “Remote Log Servers” 頁面可定義發送日誌訊息的遠端 SYSLOG 伺服器(使用 SYSLOG 協定)。對於每台伺服器，您可以設定其接收的訊息的嚴重級別，並設定**"add"**、**"Edit"**和**"Delete"**功能進行管理。




| 欄位 | 描述 |
|---|---|
| Server Address | 遠端日誌伺服器的IP位址 |
| Server Ports | 遠端日誌伺服器的連接埠編號 |
| Facility | 記錄日誌訊息的記錄工具。可以是以下值之一：local 0 ~ local 7 |
| Minimum Severity | 最低嚴重級別<br>• **Emergency(緊急)**：系統無法使用<br>• **Alert(警報)**：需要採取行動<br>• **Critical(嚴重)**：系統處於嚴重狀態<br>• **Error(錯誤)**：系統處於錯誤狀態 |

- **Warning(警告)：** 發出系統警告
- **Notice(通知)：** 系統運行正常，但出現系統通知
- **Informational(資訊)：** 設備資訊
- **Debug(調試)：** 提供事件的詳細訊息

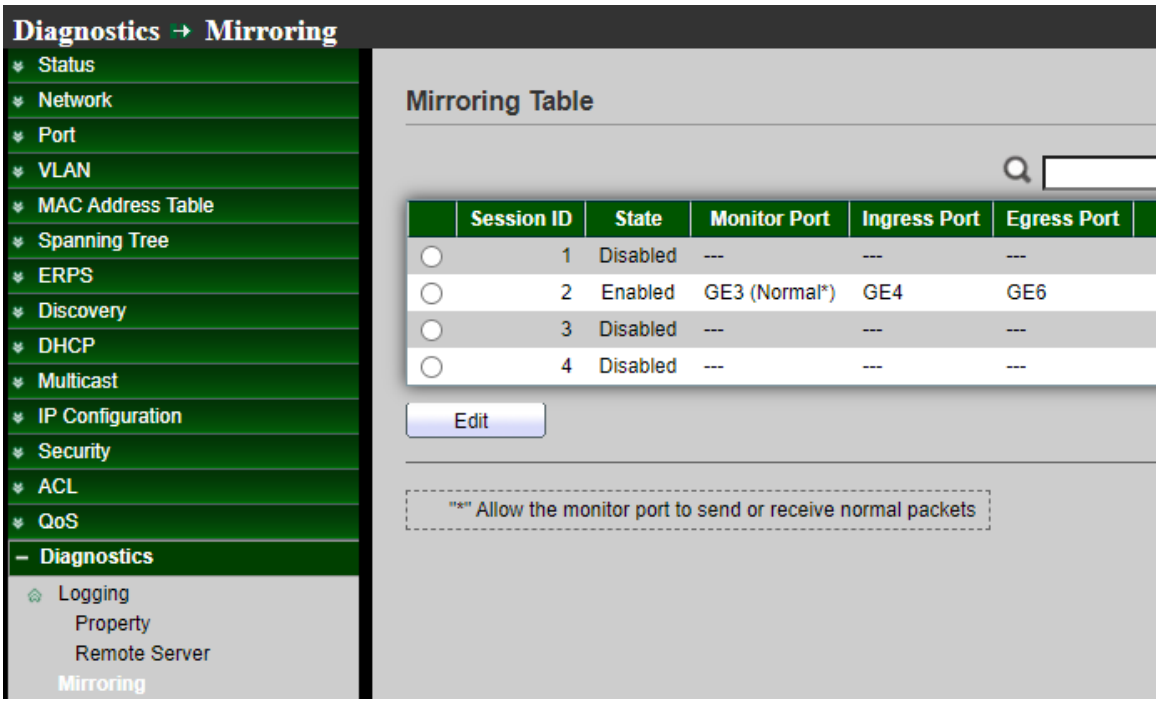



- **Address Type：** 使用者管理員可以選擇主機名稱或 IPv4/6 連接遠端日誌伺服器。
- **Server Address：** 輸入伺服器的 IP 位址。
- **Server Port：** 輸入發送日誌訊息的伺服器埠。
- **Facility：** 選擇向遠端伺服器發送系統日誌的工具。一台伺服器只能分配一個工具。
- **Minimum Severity：** 選擇向伺服器發送系統日誌訊息的最低嚴重級別。
  - **Emergency：** 系統無法使用。
  - **Alert：** 需要立即採取行動。
  - **Critical：** 系統處於嚴重狀態。
  - **Error：** 系統處於錯誤狀態。
  - **Warning：** 發出系統警告。
  - **Notice：** 系統運行正常，但出現系統通知。
  - **Informational：** 設備資訊。
  - **Debug：** 提供事件的詳細訊息。

*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

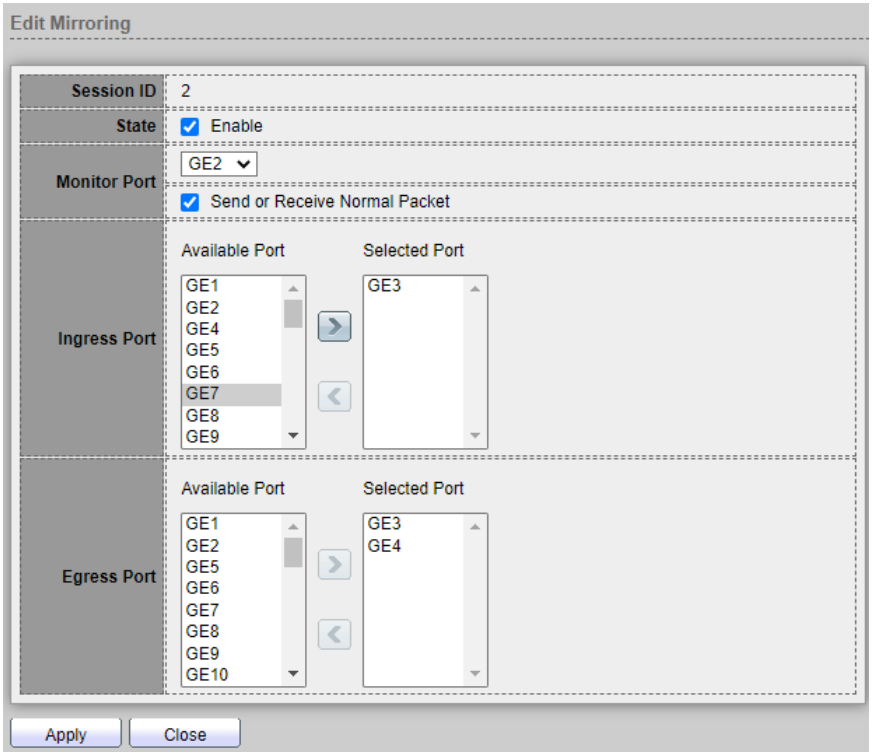
## 17.2 鏡像(Mirroring)

鏡像功能可以鏡像 Rx(輸入)/Tx(輸出)流量，鏡像封包到目的連接埠並進行分析。




| 欄位 | 描述 |
|---|---|
| Session ID | 選擇鏡像會話ID |
| State | 選擇鏡像會話狀態 ： 連接埠鏡像啟用或禁用<br>• **Enabled :** 啟用連接埠鏡像<br>• **Disabled :** 禁用鏡像 |
| Monitor Port | 選擇鏡像會話的監控連接埠，並選擇監控連接埠是否可以發送或接收正常封包 |
| Ingress port | 選擇鏡像會話的輸入(rx)來源埠 |
| Egress ports | 選擇鏡像會話的輸出(tx)來源埠 |

*點擊 "**Edit**" 編輯您的設定。*

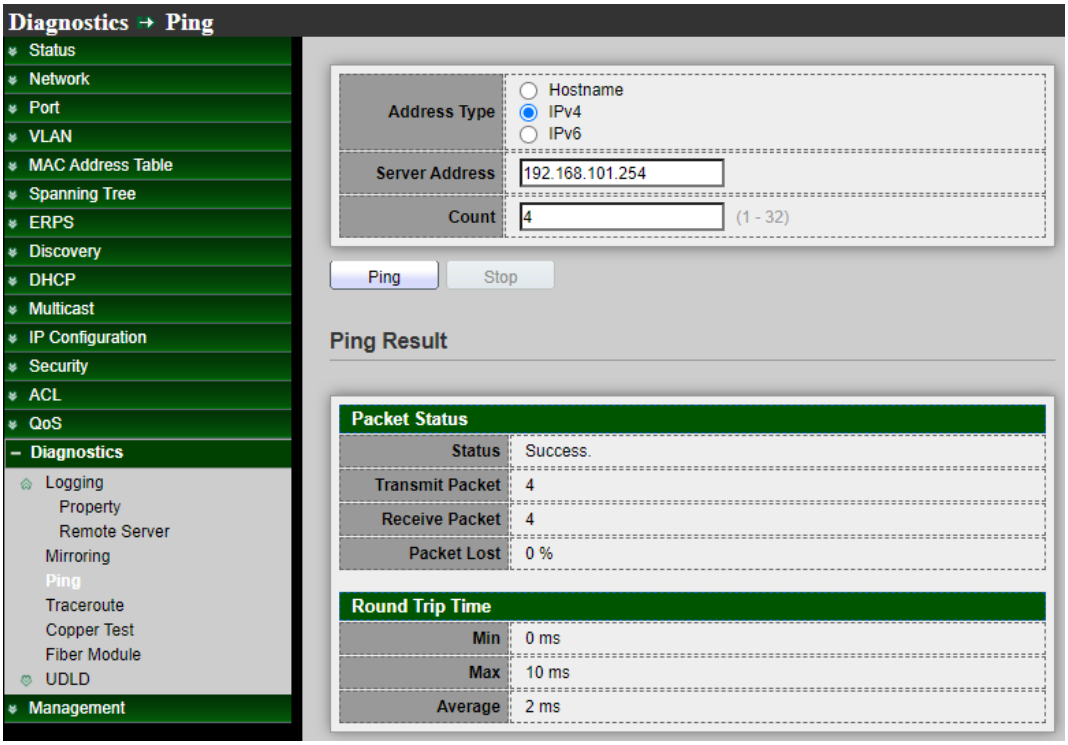



- **Session ID :** 顯示所選的鏡像會話 ID。
- **State :**
  - **Enable :** 啟用/停用鏡像功能。
- **Mirroring Port :** 使用者管理員可選擇一個鏡像連接埠(目的埠)。
- **Ingress Port :** 使用者管理員可選擇被鏡像的輸入連接埠。
- **Egress Port :** 使用者管理員可選擇被鏡像的輸出連接埠。

*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

## 17.3 Ping

Ping 指令測試遠端主機是否可以被訪問，並測量從設備發送到目標設備的封包的往返時間。
Ping 的運作原理為向目標主機發送一個網際網路控制訊息協定(ICMP)的回應請求封包，並等待 ICMP 回應。有時稱為 pong。它測量往返時間並記錄任何封包遺失，使用者管理員可以使用 ping 功能檢查連接的設備是否處於設定啟用的狀態。該 ping 功能支援 IPv4 和 IPv6 協定。



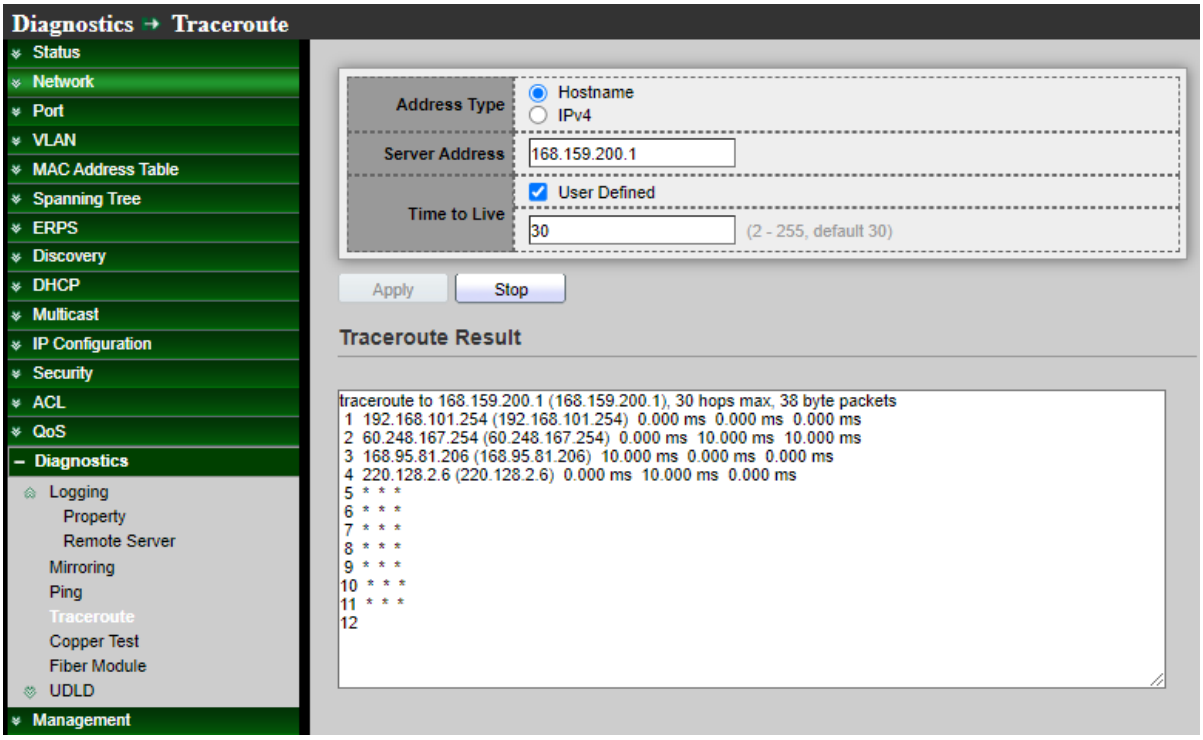

- **Address Type :** 將位址類型指定為 “Hostname” 、 “IPv6” 或 “IPv4” 。
- **Server Address :** 指定遠端日誌伺服器的主機名稱/IPv4/IPv6 位址。
- **Count :** 指定每個 ping 的 ICMP 請求數量。

*點擊 **“Ping”** 顯示 ping 的結果。*

| 欄位 | 描述 |
|---|---|
| Packet Status | 顯示ping成功或ping失敗<br>• **Status :** 顯示ping的結果 “ Success” 或 “Ping failed (timeout)”<br>• **Transmit Packet :** ping發送的封包數量<br>• **Receive Packet :** ping接收的封包數量<br>• **Packet Lost :** ping過程中遺失封包百分比(丟包率) |
| Round Trip Time | 顯示ping的往返時間<br>• **Min :** 封包返回的最短時間<br>• **Max :** 封包返回的最長時間<br>• **Average :** 封包返回的平均時間 |

# 17.4 Traceroute

Traceroute 透過將 IP 封包發送到目標主機並返回交換器，來發現封包經過的路由器的 IP 位址。Traceroute 頁面顯示交換器到目標主機之間的每一跳以及到每一跳的往返時間。

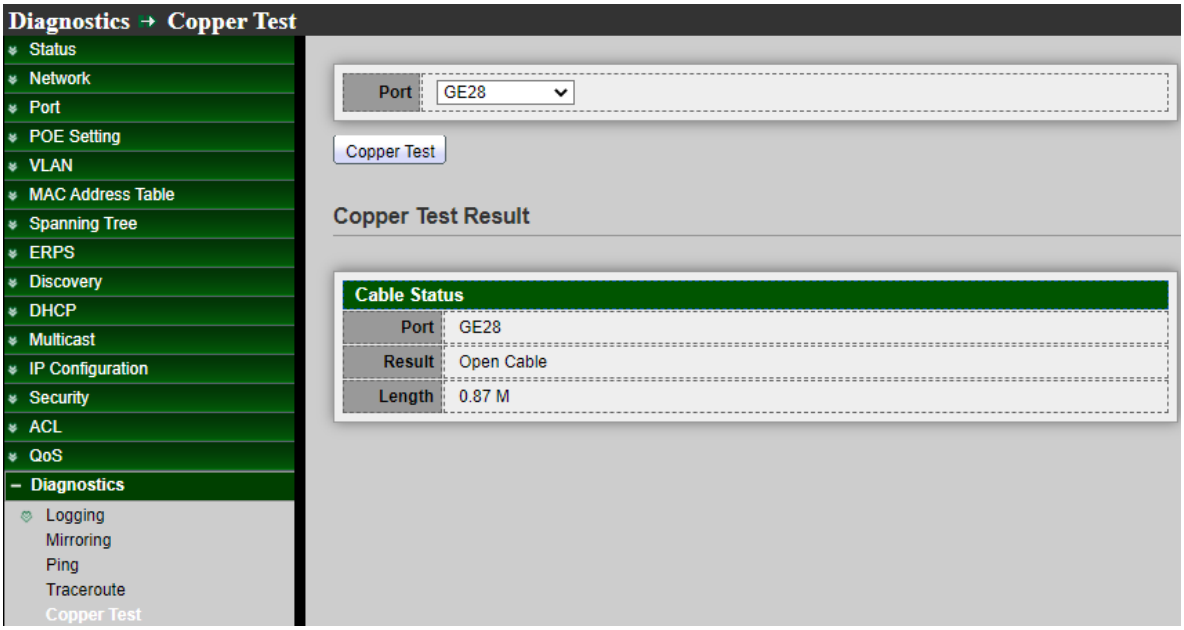



- **Address Type :** 將位址類型指定為 “Hostname” 或 “IPv4” 。
- **Server Address :** 指定遠端日誌伺服器的主機名稱/IPv4 位址。
- **Time to Live :** 輸入 Traceroute 允許的最大躍點數。用於防止發送的訊框陷入無限循環。當到達目的地或達到該值時，Traceroute 指令終止。若要使用預設值(30)，請選擇 “Use Default” 。

*點擊"**Apply**"即可顯示 Traceroute 結果。*

# 17.5 銅纜測試(Copper Test)

使用者管理員可以使用該功能檢查連接埠結果是否正常，如果正常則顯示。




| 欄位 | 描述 |
|---|---|
| Port | 指定銅纜測試的介面 |

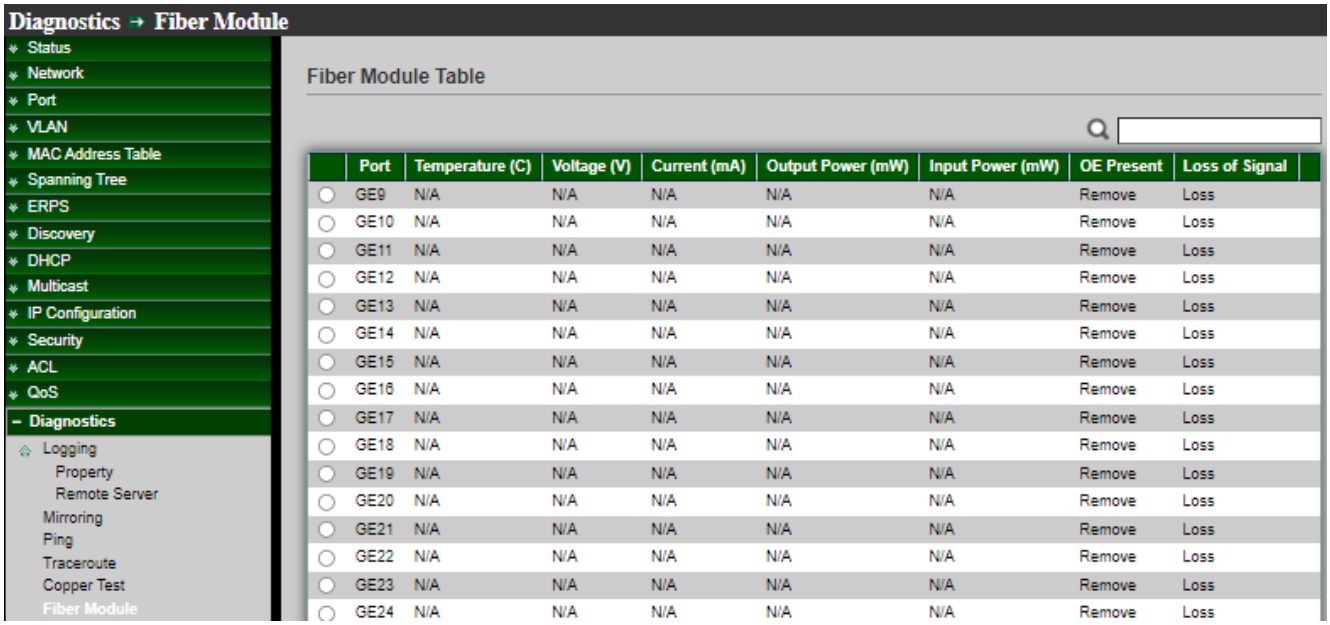
*點擊 "Copper Test" 顯示銅測試結果。*

## Cable Status

| 欄位 | 描述 |
|---|---|
| Port | 銅纜測試的介面 |
| Result | 銅纜測試的狀態，包括:<br>• OK：正確端接線對<br>• Short Cable：電纜發生短路<br>• Open Cable：開放鏈路，無連接端<br>• Impedance Mismatch：終端阻抗不在參考範圍內<br>• Line Drive：線路驅動 |
| Length | 從埠到發現故障的電纜上的位置的距離 |

## 17.6 光纖模組(Fiber Module)

顯示光纖模組信使。光模組狀態頁面顯示小封裝熱插拔收發器 (SFP) 報告的運行資訊。注意到: 不支援數字診斷監控標準 SFF-8472 的 SFP 可能無法取得某些資訊。




| 欄位 | 描述 |
|---|---|
| Port | 連接埠編號介面 |
| Temperature | 內部測量的收發器溫度 |
| Voltage | 內部測量的電源電壓 |
| Current | 測量的TX偏置電流 |
| Output Power | 測量的TX輸出功率(毫瓦) |
| Input Power | 測量的RX接收功率(毫瓦) |
| Transmitter Fault | TX故障狀態 |
| OE Present | 表示收發器已接通電源且資料準備就緒 |
| Loss of Signal | 訊號丟失 |

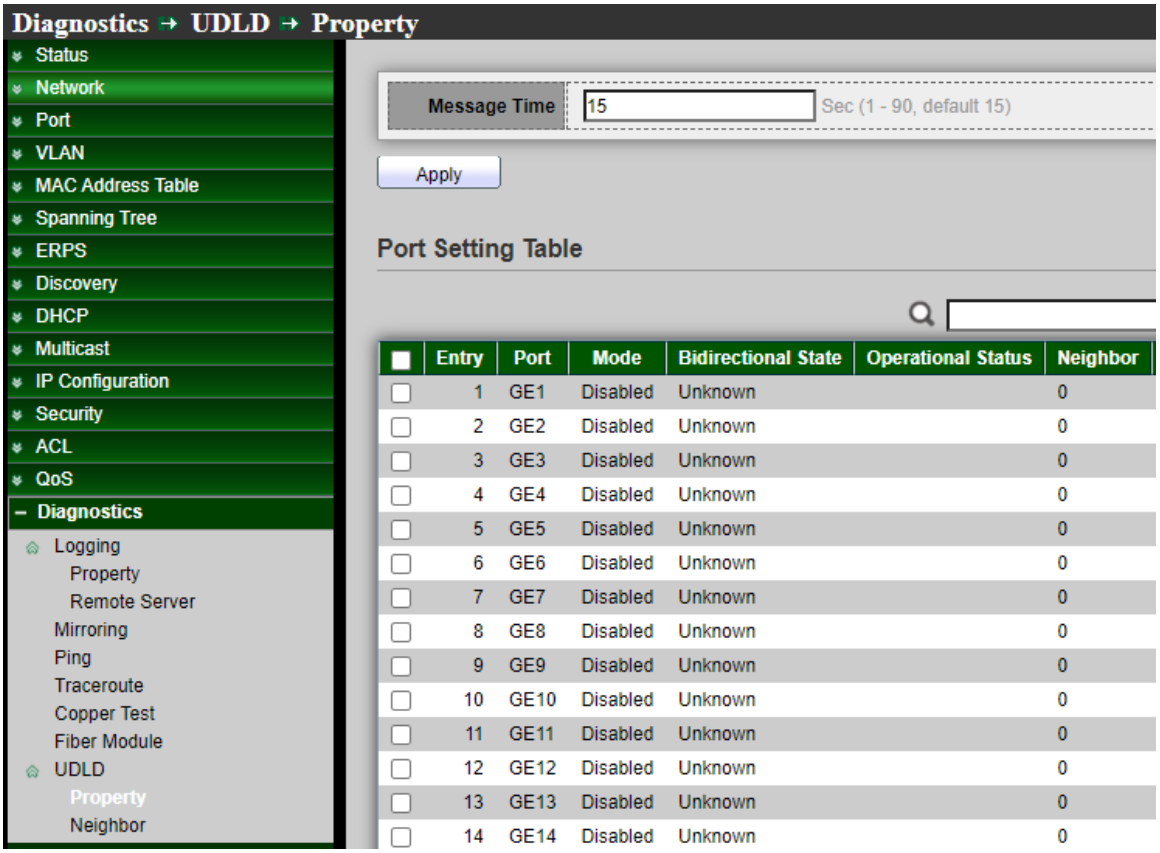
*點擊 "Refresh" 重新整理頁面，或點擊 "Detail" 查看詳細資料。*

# 17.7 單向鏈路檢測(UDLD)

單向鏈路檢測 (UDLD) 監視兩個設備之間的鏈路，如果兩個設備之間的任意點鏈路斷開，則將使鏈路兩端的連接埠癱瘓。使用 UDLD 頁面進行 UDLD 功能設定。

## 17.7.1 屬性(Property)

該頁面允許使用者設定 UDLD 的全域和每個介面的設定。




- **Message Time :** 若要使用 UDLD 協議，必須對所有連接的交換器和介面進行設定。設定了 UDLD 的交換器會向其鄰近設備發送 “hello” 封包(UDLD 通告)，並預期在指定的保持時間內收到一個 “hello” 封包(預設保持時間為 15 分鐘)。如果沒有收到，UDLD 將禁用無回應的介面。

*點擊"Apply"儲存您的變更設定。*

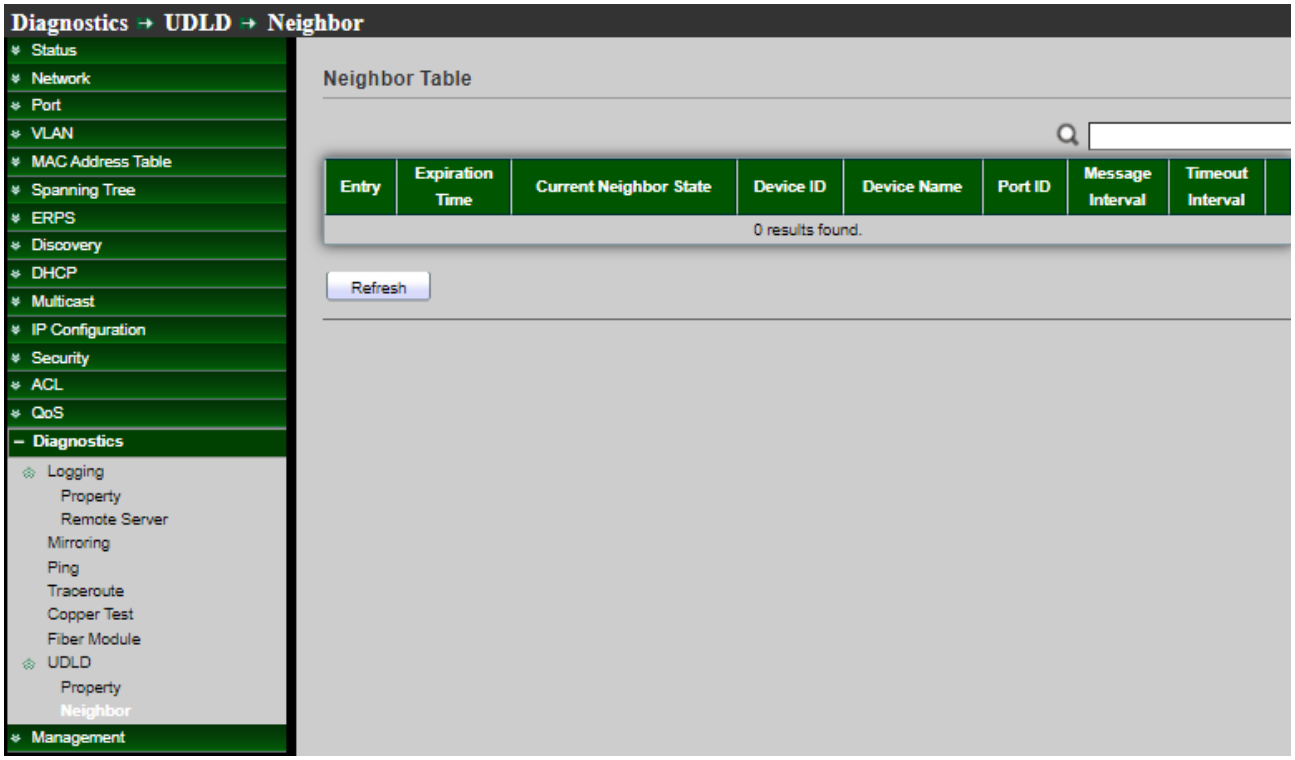
| 欄位 | 描述 |
|---|---|
| Port | 顯示清單的連接埠ID |
| Mode | 顯示介面的UDLD運行模式 |
| Bidirectional State | 顯示介面的雙向狀態 |
| Operational Status | 顯示介面的運行狀態 |
| Neighbor | 顯示介面的鄰近設備的數量 |


- **Port :** 選擇一個或多個要設定的連接埠。
- **Mode :** 選擇介面的 UDLD 運行模式。
  - **Disabled :** 停用 UDLD 功能。
  - **Normal :** 以正常模式運行時，連接埠在最後一個鄰近設備超時後進入單向連接狀態。
  - **Aggressive :** 以激進模式下運行時，連接埠在最後一個鄰近設備超時後進入重新建立階段。

*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

### 17.7.2 鄰近設備(Neighbor)

每個設定為 UDLD 的交換器連接埠都會交換 UDLD 協定封包，其中包括有關連接埠的設備和連接埠 ID 資訊，並且連接埠也會發送所知的有關與其連接的鄰近設備的設備和連接埠 ID 資訊。
因此，如果鏈路是雙向的，連接埠應該從其鄰近設備接收自己的設備和連接埠 ID 資訊。如果連接埠沒有從鄰近設備收到有關自己設備和連接埠 ID 的資訊，則認為該鏈路是單向的。
當鏈路兩端都已啟動，但一端未接收封包時，或出現佈線錯誤導致發送線和接收線未連接到鏈路兩端的連接埠時，就會發生這種情況。

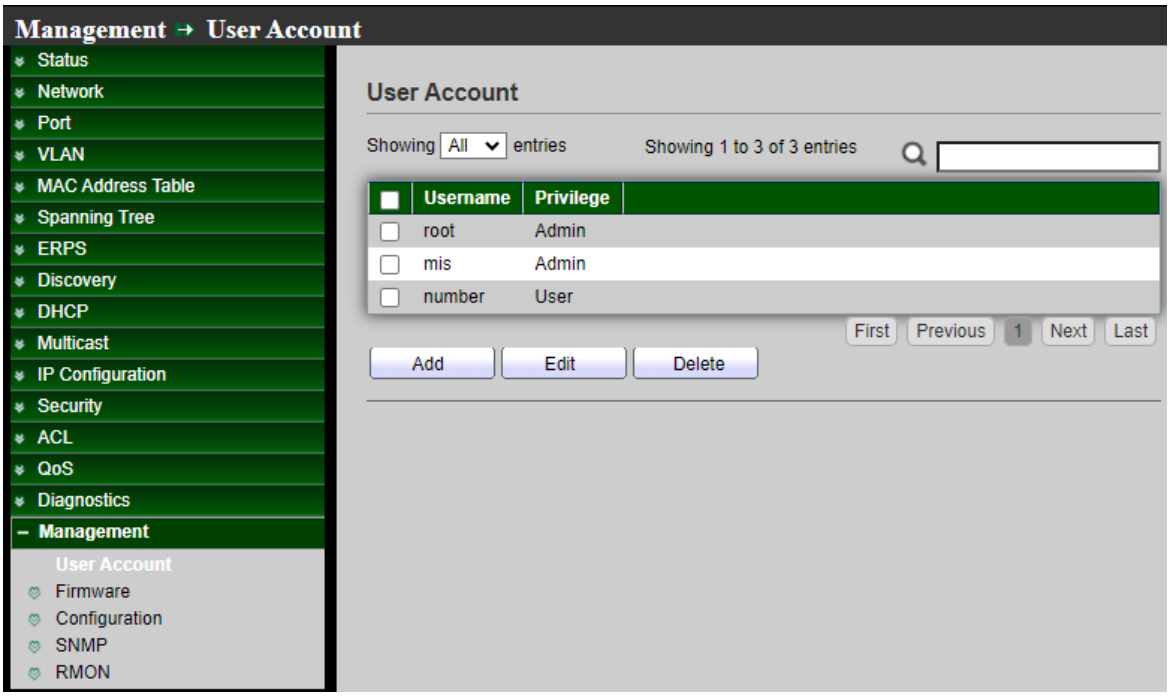



| 欄位 | 描述 |
|---|---|
| Entry | 顯示清單索引 |
| Expiration Time | 顯示超時前的保持時間 |
| Current Neighbor State | 顯示鄰近設備當前狀態 |
| Device ID | 顯示鄰近設備ID |
| Device Name | 顯示鄰近設備名稱 |
| Port ID | 顯示連接的鄰近設備連接埠ID |
| Message Interval | 顯示鄰近設備訊息時間間隔 |
| Timeout Interval | 顯示鄰近設備超時間隔 |

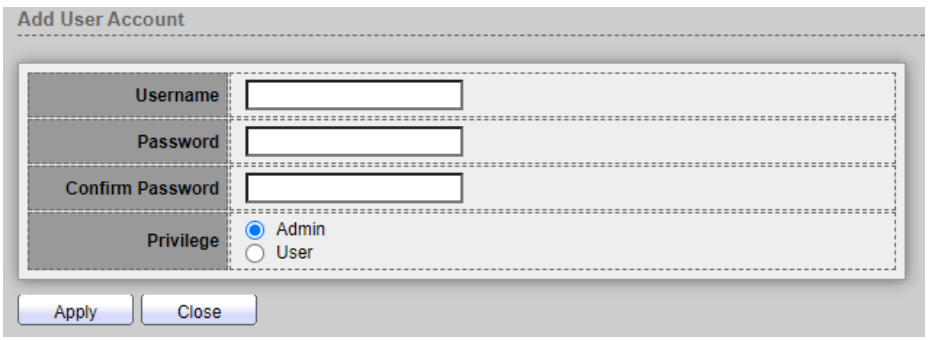
# 18. 管理(Management)

## 18.1 使用者帳戶(User Account)

預設使用者名稱/密碼是 root/default。使用者管理員可以修改登入密碼或建立新的使用者名稱/密碼並定義權限，並設定"**add**"、"**Edit**"和"**Delete**"功能進行管理。




| 欄位 | 描述 |
|---|---|
| Username | 帳戶的使用者名稱 |
| Privilege | 顯示新帳戶的權限級別<br>• **Admin :** 允許變更交換器設定。權限值等於15<br>• **User :** 只讀交換器設定。不允許變更，權限級別等於1 |



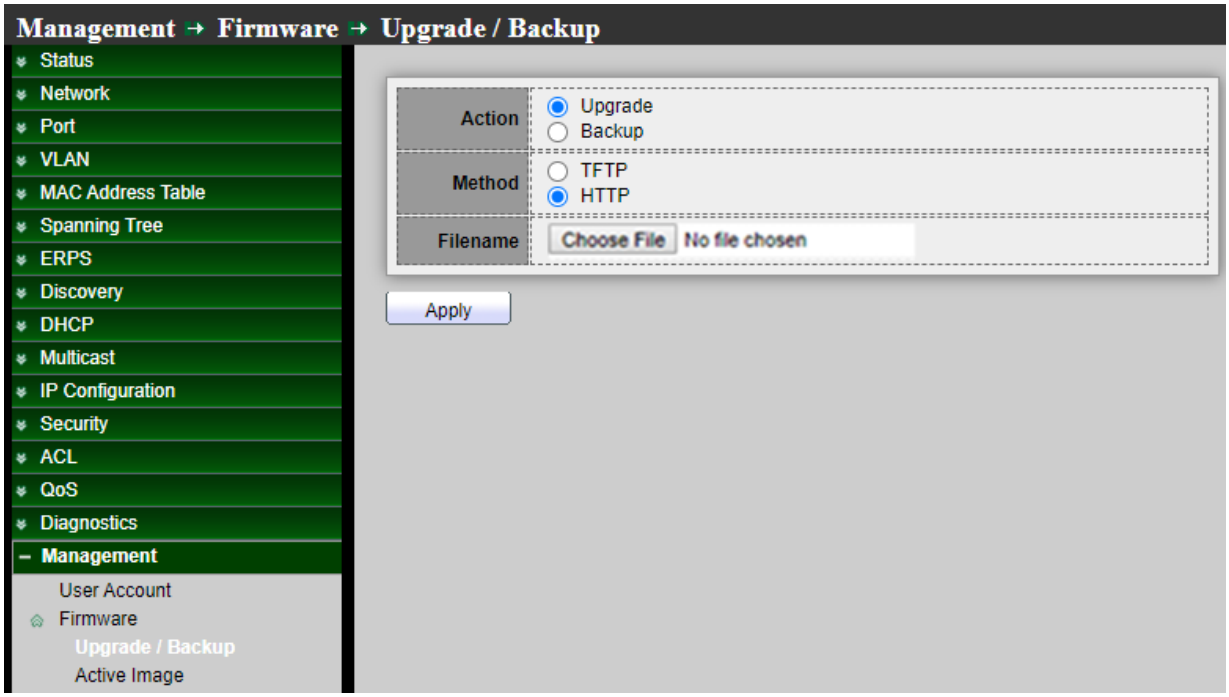
- **Username :** 帳戶的使用者名稱。
- **Password :** 設定帳戶的密碼。
- **Confirm Password :** 設定與 “Password” 欄位相同的帳戶密碼。.
- **Privilege :** 選擇新帳戶的權限等級。
  - **Admin :** 允許變更交換器設定。權限值等於 15。
  - **User :** 只讀交換器設定。不允許變更，權限級別等於 1。

*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

# 18.2 韌體(Firmware)

## 18.2.1 升級/備份(Upgrade / Backup)

使用者管理員可以升級或備份韌體，方法可以選擇使用 TFTP 或 HTTP 協定。如果選擇備份，則使用者管理員可以選擇要備份的韌體映像檔。



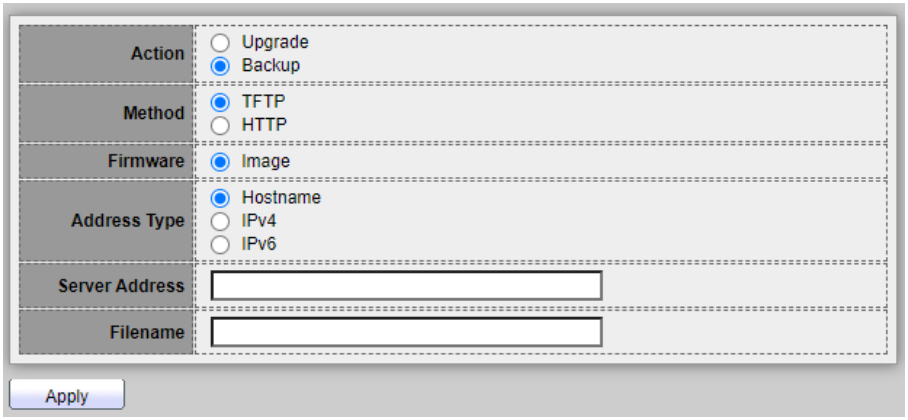

- **Action :** 韌體操作。
  - **Upgrade :** 從遠端主機向 DUT 升級韌體。
  - **Backup :** 從 DUT 向遠端主機備份韌體映射。
- **Method :** 韌體升級/備份方法。

- **TFTP :** 使用 TFTP 來升級/備份韌體。
- **HTTP :** 使用 WEB 瀏覽器來升級/備份韌體。

➢ **Filename :** 使用瀏覽器升級韌體，您應選擇主機上的韌體映像檔案。

| **Note** | 系統更新時，預設值始終升級為映像檔 1。 |
|---|---|

*點擊"Apply"儲存您的變更設定。*




➢ **Action :** 韌體操作。
- **Upgrade :** 從遠端主機向 DUT 升級韌體。
- **Backup :** 從 DUT 向遠端主機備份韌體映像檔。

➢ **Method :** 韌體升級/備份方法。
- **TFTP :** 使用 TFTP 來升級/備份韌體。
- **HTTP :** 使用 WEB 瀏覽器來升級/備份韌體。

➢ **Firmware :** 預設閃存中的韌體映像檔。

➢ **Address Type :** 指定 TFTP 伺服器位址類型。
- **Hostname :** 使用網域名稱作為伺服器位址。
- **IPv4 :** 使用 IPv4 作為伺服器位址。
- **IPv6 :** 使用 IPv6 作為伺服器位址。

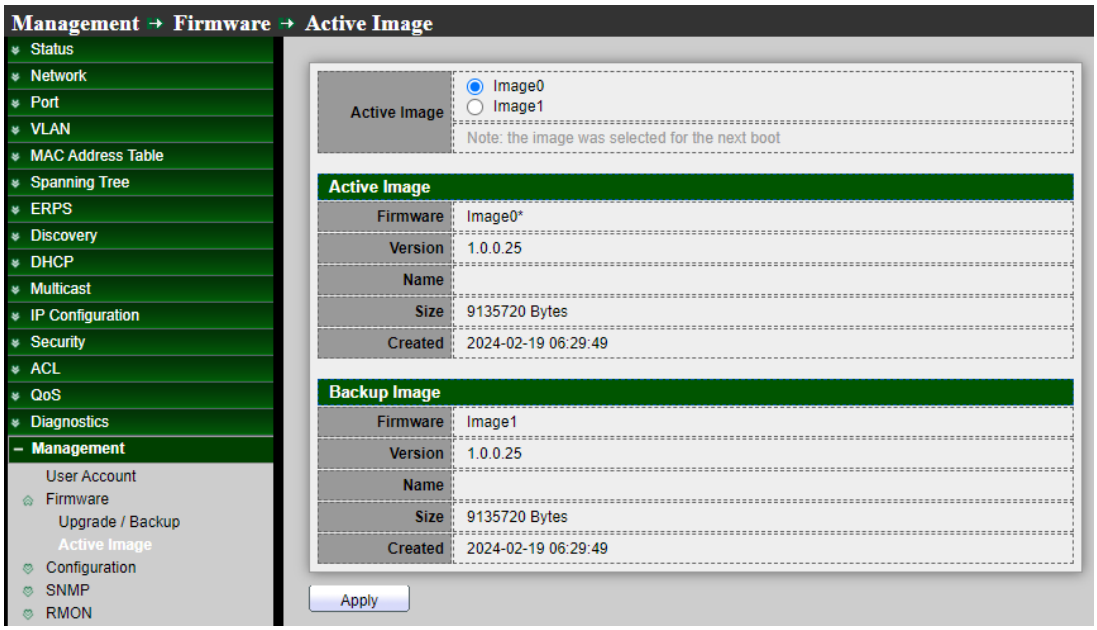
➢ **Server Address :** 指定 TFTP 伺服器位址。

➢ **Filename :** 遠端 TFTP 伺服器上的韌體映射檔案名。

*點擊"Apply"儲存您的變更設定。*

## 18.2.2 設定啟用的映像檔(Active Image)

此頁面允許使用者在下次啟動時選擇韌體映像檔，並顯示兩個閃存分區的韌體訊息，如果交換器在系統中上傳了多個韌體，使用者管理員可以選擇一個韌體進行系統預設啟動。




- Active Image : 選擇下次啟動時使用的韌體映像檔。
  - Image0 : 選擇閃存分區 0 啟用韌體設定檔 0。
  - Image1 : 選擇閃存分區 1 啟用韌體設定檔 1。

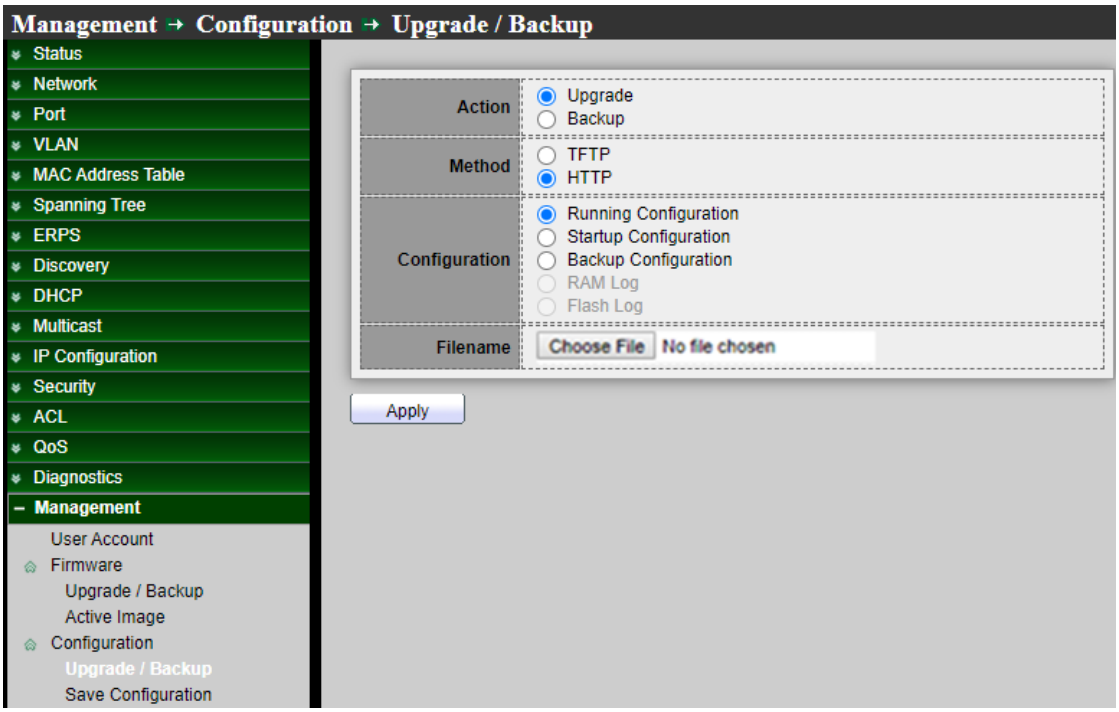
| 欄位 | 描述 |
|---|---|
| Active Image | • Firmware : 韌體映像檔<br>• Version : 韌體版本<br>• Name : 韌體名稱<br>• Size : 韌體映像檔大小<br>• Created : 韌體映像檔創建日期 |
| Backup Image | • Firmware : 韌體映像檔<br>• Version : 韌體映像檔<br>• Name : 韌體名稱<br>• Size : 韌體映像檔大小<br>• Created : 韌體映像檔創建日期 |

*點擊"Apply"儲存您的變更設定。*

# 18.3 配置(Configuration)

## 18.3.1 升級/備份(Upgrade / Backup)

使用者管理員可以將系統設定檔備份到 PC 或將設定檔上傳到交換器系統，此頁面允許使用者透過 HTTP 或 TFTP 伺服器升級或備份韌體映像檔。



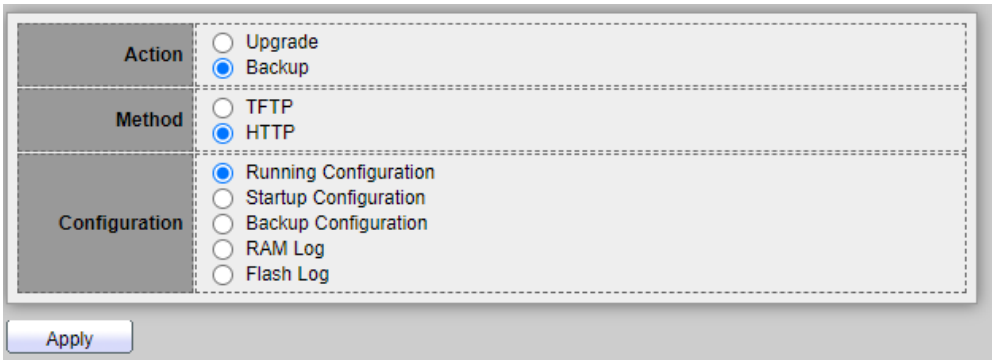

### Upgrade Configuration

- Action : 設定操作。
  - Upgrade : 從遠端主機向 DUT 升級韌體。
  - Backup : 從 DUT 向遠端主機備份韌體映像檔。
- Method : 設定升級方法。
  - TFTP : 使用 TFTP 來升級韌體。
  - HTTP : 使用 WEB 瀏覽器來升級韌體。
- Configuration : 設定類型。
  - Running Configuration : 合並到目前運行的設定檔。
  - Startup Configuration : 替換啟動設定檔。
  - Backup Configuration : 替換備份設定檔。

- **Address Type :** 指定 TFTP 伺服器位址類型。
  - **Hostname :** 使用網域名稱作為伺服器位址。
  - **IPv4 :** 使用 IPv4 作為伺服器位址。
  - **IPv6 :** 使用 IPv6 作為伺服器位址。
- **Server Address :** 指定 TFTP 伺服器位址。
- **Filename :** 遠端 TFTP 伺服器上的設定檔案名。

*點擊"Apply"儲存您的變更設定。*

## Backup Configuration

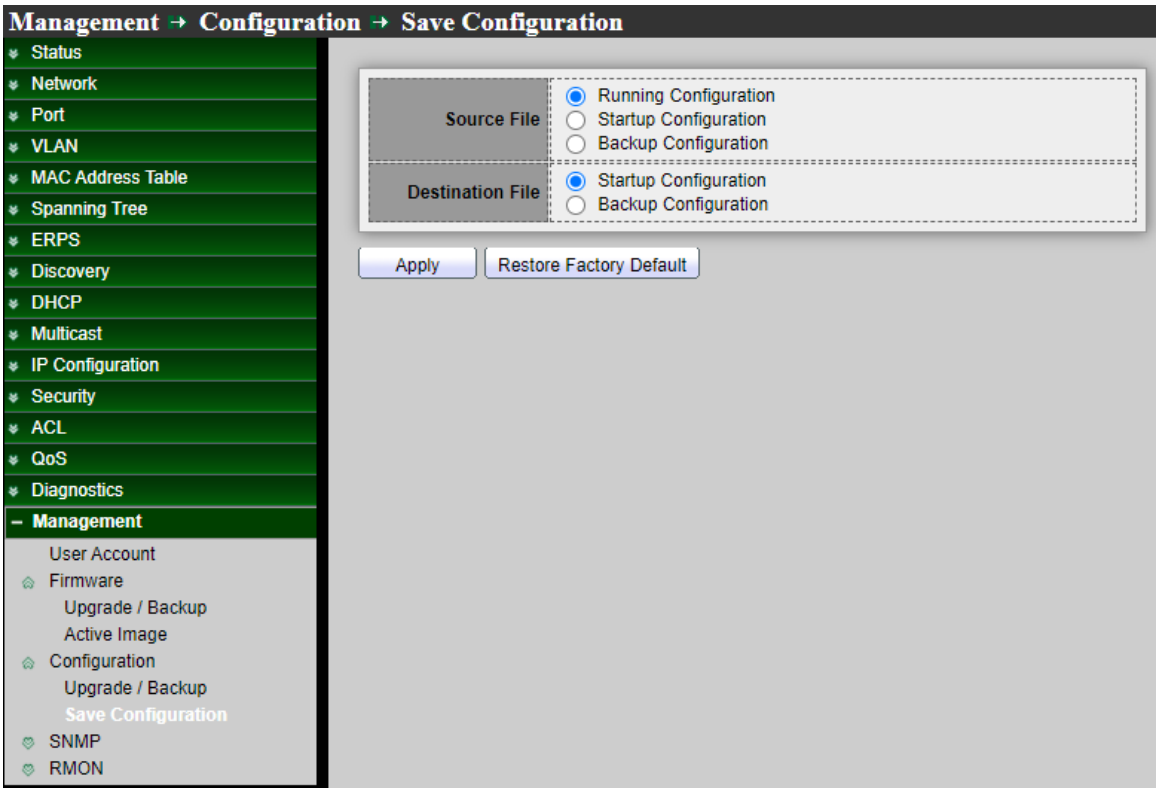



- **Action :** 設定操作。
  - **Upgrade :** 從遠端主機向 DUT 升級韌體。
  - **Backup :** 從 DUT 向遠端主機備份韌體映像檔。
- **Method :** 設定備份方法。
  - **TFTP :** 使用 TFTP 來備份韌體。
  - **HTTP :** 使用 WEB 瀏覽器來備份韌體。
- **Configuration :** 設定類型。
  - **Running Configuration :** 備份運行的設定檔。
  - **Startup Configuration :** 備份啟動設定檔。
  - **Backup Configuration :** 備份備份設定檔。
  - **RAM Log :** 備份儲存在 RAM 中的日誌。
  - **Flash Log :** 備份儲存在閃存的日誌。

*擊"Apply"儲存您的變更設定。*

## 18.3.2 保存設定(Save Configuration)

當使用者管理員在任何視窗上點擊 “Apply” 應用時，您對交換器設定所做的變更僅儲存在運行設定中。要保留運行設定中的參數，必須將運行設定複製到另一個設定類型或保存為其它設備上的文件，此頁面允許使用者管理保存在 DUT 上的設定檔，以及點擊 “Restore Factory Default” 恢復出廠預設值。




- Source File : 來源檔案類型。
  - Running Configuration : 複製運行設定檔案到目的地。
  - Startup Configuration : 複製啟動設定檔案到目的地。
  - Backup Configuration : 複製備份設定檔案到目的地。
- Destination File : 目的檔案類型。
  - Startup Configuration : 將檔案儲存為啟動設定。
  - Backup Configuration : 將檔案儲存為備份設定。

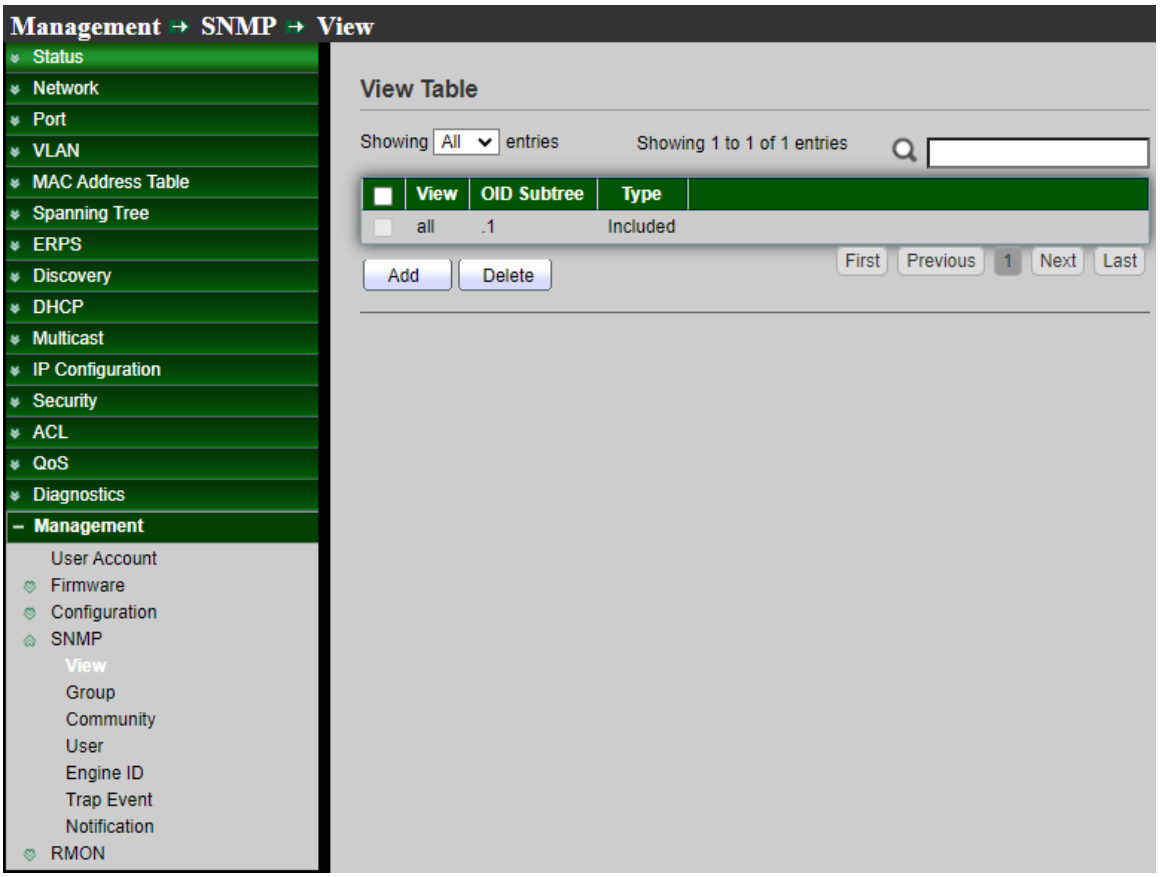
*點擊"Apply"儲存您的變更設定或點擊"Restore Factory Default"返回出廠預設值。*

# 18.4 簡易網路管理協定(SNMP)

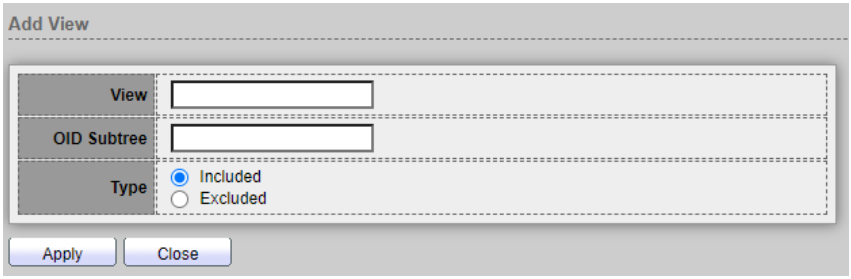
SNMP 支援 SNMP v1、v2 和 v3。它還能使用它支援的管理資料庫 (MIB) 中定義的陷阱，向陷阱接收器報告系統事件。

## 18.4.1 顯示(View)

顯示是使用者定義的 MIB 樹或子樹集合的標籤。每個子樹 ID 由相關子樹根的 OID 定義。您可以使用定義的名稱來指定所需子樹的根，也可以輸入 OID。設定"**add**"和"**Delete**"功能進行管理。




| 欄位 | 描述 |
|---|---|
| View | SNMP的view名稱。其最大長度為30個字元 |
| Subtree OID | 指定要從SNMP顯示中包含或排除的 ASN.1子樹物件識別碼(OID) |
| View Type | 在顯示中包含或排除選定的MIB |



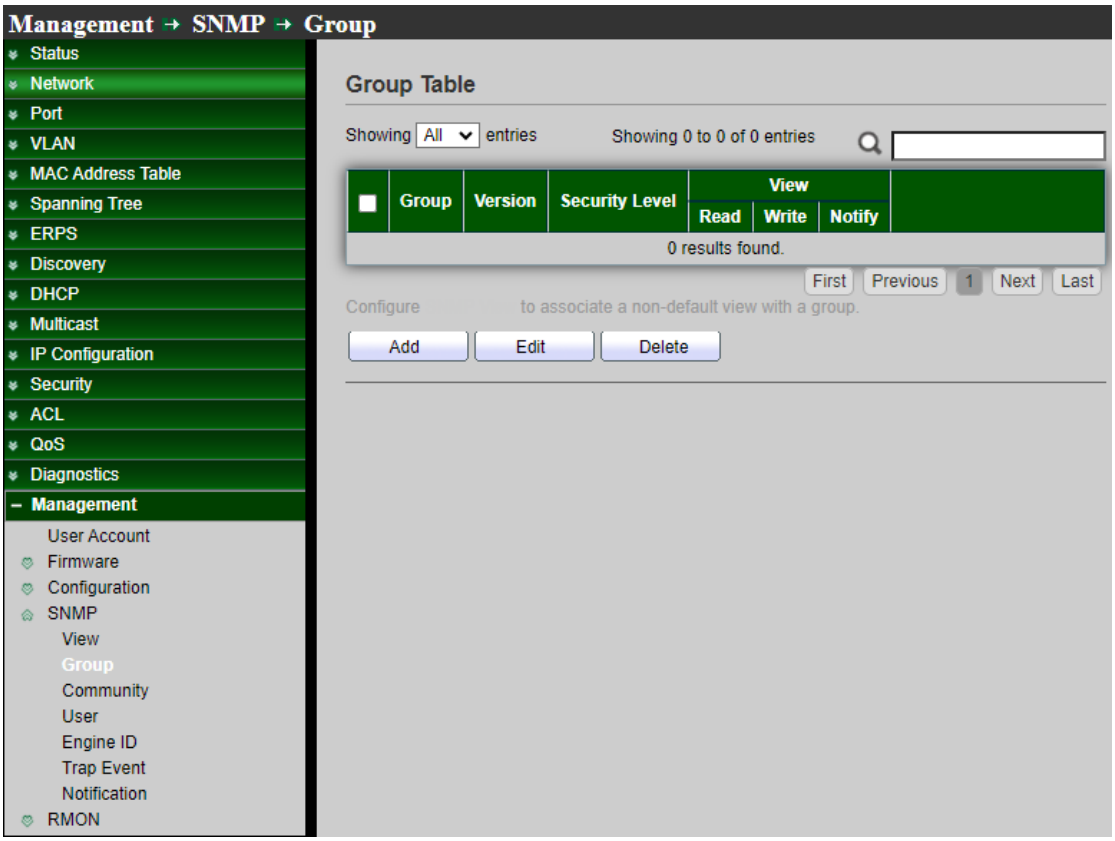

- **View :** 輸入一個獨特的顯示名稱。
- **Object Subtree :** 選擇“使用者定義”手動定義 OID，或從列表中選擇現有 OID。顯示中將包含或排除該節點的所有子節點。
- **Type :**

  Include : 選中以將所選 MIB 包含在顯示中。

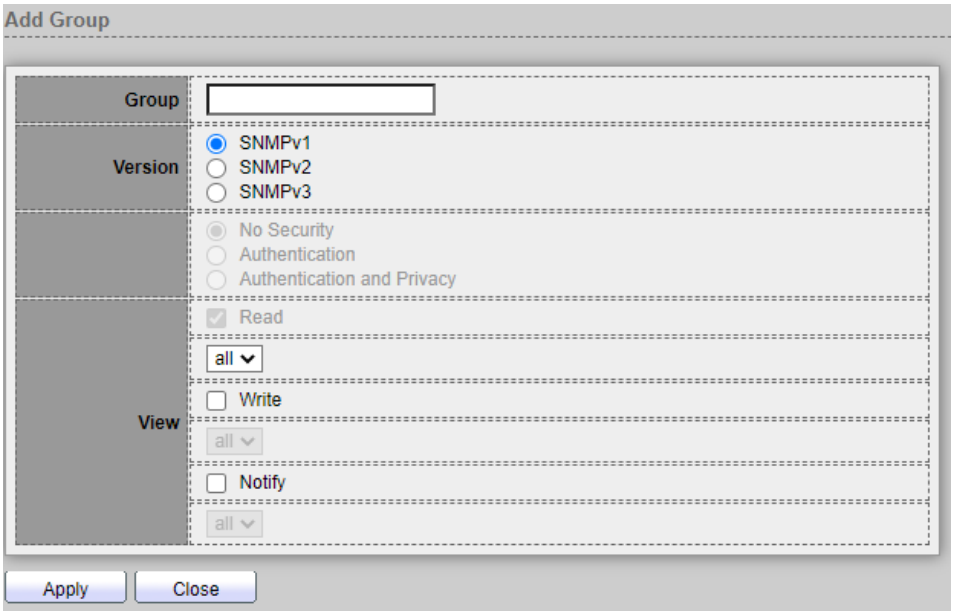
  Excluded : 選中以將所選 MIB 排除在顯示中。

## 18.4.2 群組(Group)

在 SNMPv1 和 SNMPv2 中，社群字串與 SNMP 訊框一起發送。社群字串是存取 SNMP 代理的密碼。然而，訊框和社群字串都沒有加密。因此 SNMPv1 和 SNMPv2 並不安全。在 SNMPv3 中可以設定“Authentication and Privacy”更加安全。設定**"add"**、**"Edit"**和**"Delete"**功能進行管理。



| 欄位 | 描述 |
|---|---|
| Group | 指定SNMP群組名稱，其最大長度為30個字元 |
| Version | 指定SNMP版本<br>• **SNMPv1**：SNMP版本1<br>• **SNMPv2**：基於社群認證-SNMP版本2c<br>• **SNMPv3**：使用者安全模型(USM)-SNMP版本3 |
| Security Level | 指定SNMP安全級別<br>• **No Security**：指定不執行封包認證<br>• **Authentication**：指定執行未加密的封包身份認證<br>• **Authentication and Privacy**：指定執行帶加密的封包身份認證 |
| View | 指定SNMP檢視的管理存取<br>• **Read**：所選檢視的管理存取為只讀<br>• **Write**：所選檢視的管理存取為寫入<br>• **Notify**：當所選檢視上發生事件時，會向SNMP使用者傳送通知訊息 |




- **Group**：指定 SNMP 群組名稱，其最大長度為 30 個字元。
- **Version**：指定 SNMP 版本。
  - **SNMPv1**：SNMP 版本 1。
  - **SNMPv2**：基於社群認證的 SNMP 版本 2c。
  - **SNMPv3**：使用者安全模型(USM)的 SNMP 版本 3。
- **Security Level**：指定 SNMP 安全級別。

- **No Security :** 指定不執行封包認證。
- **Authentication :** 指定執行未加密的封包身份認證
- **Authentication and Privacy :** 指定執行帶加密的封包身份認證。

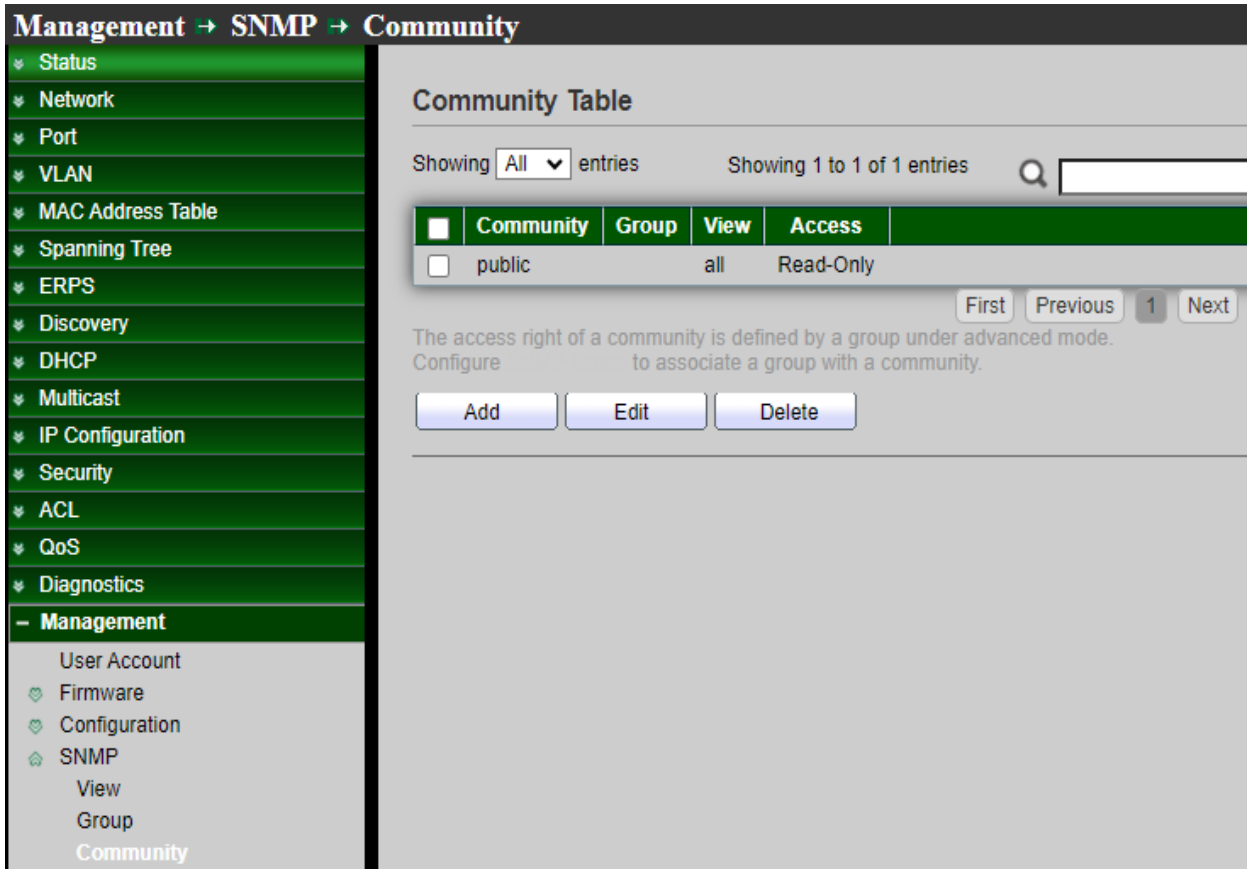
➢ **View :**

- **Read :** 如果選中 “Read” ,則選擇檢視的管理存取為只讀。
- **Write :** 如果選中 “Write” ,則選擇檢視的管理存取為寫入。
- **Notify :** 如果選中 “Notify” ,則所選檢視上發生事件時，會向 SNMP 使用者傳送通知訊息。

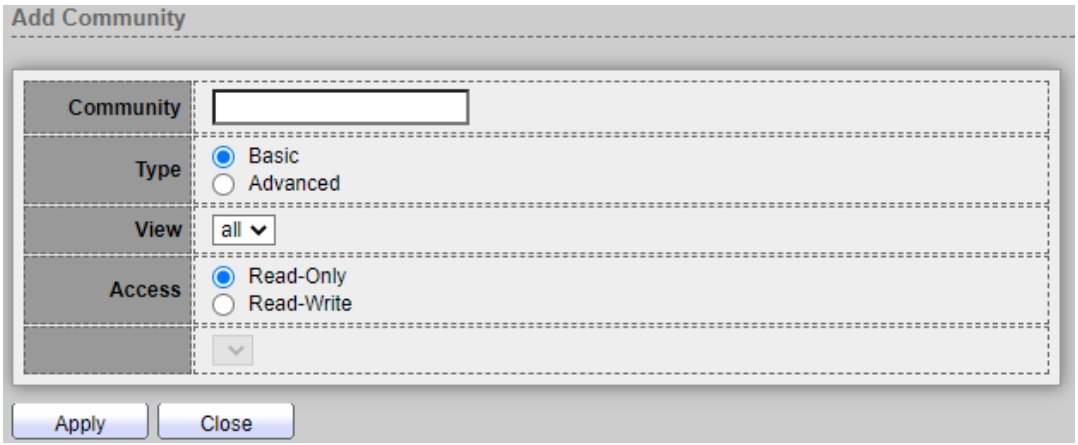
*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

## 18.4.3 社群(Community)

社群僅在 SNMPv1 和 v2 中定義，因為 SNMPv3 基於使用者安全性而非社群。使用者屬於為其分配了存取權限的群組，並設定"**add**"、"**Edit**"和"**Delete**"功能進行管理。



| 欄位 | 描述 |
|---|---|
| Community | SNMP社群名稱，其最大長度為20個字元 |
| Community | SNMP社群模式<br>• **Basic :** snmp社群指定顯示和存取權限<br>• **Advanced :** snmp社群指定群組 |
| Group | 指定透過**SNMP group**指令設定的SNMP群組，以定義社群可用的物件 |
| View | 指定SNMP顯示，以定義社群可用的物件 |
| Access | SNMP存取模式<br>• **Read-Only :** 只讀<br>• **Read-Write :** 讀寫 |



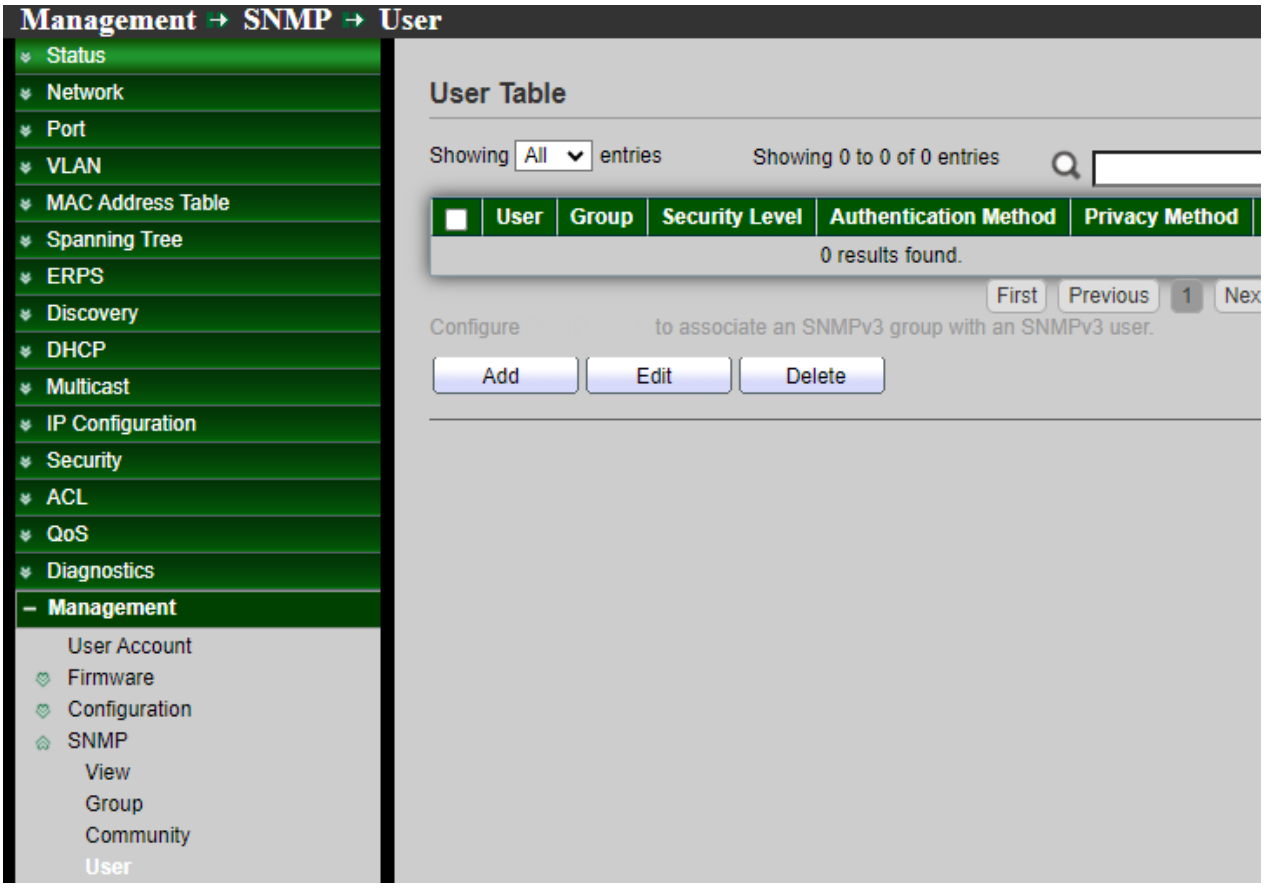

- **Community :** SNMP 社群名稱，其最大長度為 20 個字元。
- **Type :** 指定 SNMP 版本類型。
  - **Basic :** SNMP 社群指定檢視和存取權限，社群的存取權限可以設定為只讀或讀寫。此外，使用者管理員可以透過選擇顯示，限制社群只能存取某些 MIB 物件。
  - **Advanced :** SNMP 社群指定群組，社群的存取權限由群組定義。你可以使用特定的安全模型設定群組，群組的存取權限包括讀取、寫入和通知。
- **View :** 指定 SNMP 顯示，以定義社群可用的物件。
- **Access :** SNMP 存取模式。
  - **Read Only :** 只讀，管理存取權限僅限於只讀。無法對社區進行更改。
  - **Read Write :** 讀寫，管理存取權限為讀寫。可以對交換器設定進行更改，但不能更改社群。

- Group：如果設定則指定 SNMP 版本類型設定為 “Advanced” 類型，必須設置指定使用者設定的 SNMP 群組，以定義社群可用的物件。

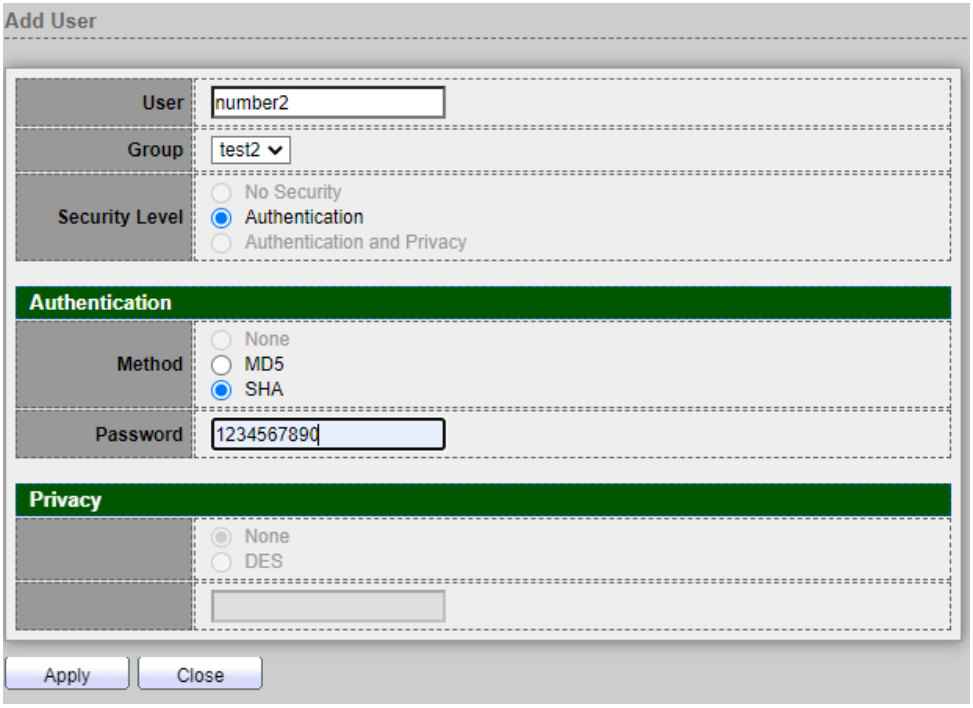
*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

### 18.4.4 使用者(User)

SNMP 使用者由登入憑證(使用者名稱、密碼和驗證方法)以及與群組和引擎 ID 相關聯的操作上下文和範圍來定義。設定的使用者具有其群組的屬性，並擁有在相關顯示中設定的存取權限。
通過群組，網絡管理員能夠為一組用戶而非單一用戶分配存取權限。一個使用者只能是單一群組的成員。
使用者管理員需要創建一個 SNMPv3 使用者，必須有一個 SNMPv3 群組，並設定**"add"**、**"Edit"**和**"Delete"**功能進行管理。



| 欄位 | 描述 |
|---|---|
| User | 指定連接到 SNMP 代理的主機上的 SNMP 使用者名稱。最大字元數為30個字元。對於 SNMP v1 或 v2c，使用者名稱必須與社群名稱匹配 |
| Group | 指定SNMP使用者所屬的SNMP群組 |
| Security Level | SNMP權限模式<br>• **No Security :** 指定不執行封包認證<br>• **Authentication :** 指定執行未加密的封包身份認證<br>• **Authentication and Privacy :** 指定執行帶加密的封包身份認證 |
| Authentication Method | 權限模式為" **Authentication** "或" **Authentication and Privacy** "時可用的認證協定<br>• **None :** 無需身份認證<br>• **MD5 :** 指定HMAC-MD5-96身份認證協定<br>• **SHA :** 指定HMAC-SHA-96身份認證協定 |
| Privacy Method | 加密協定<br>• **None :** 無需隱私保護<br>• **DES :** 資料加密標準(DES)演算法 |



- **User :** 指定連接到 SNMP 代理的主機上的 SNMP 使用者名稱。最大字元數為 30 個字元。
- **Security Level :** SNMP 權限模式。
  - **No Security :** 指定不執行封包認證。
  - **Authentication :** 指定執行未加密的封包身份認證。
  - **Authentication and Privacy :** 指定執行帶加密的封包身份認證。

### Authentication

- **Method :** 權限模式為" Authentication "或" Authentication and Privacy "時可用的認證協定。
  - **None :** 無需身份認證。
  - **MD5 :** 指定 HMAC-MD5-96 身份認證協定。
  - **SHA :** 指定 HMAC-SHA-96 身份認證協定。
- **Password :** 身份認證密碼，字元長度範圍為 8 至 32 字元。

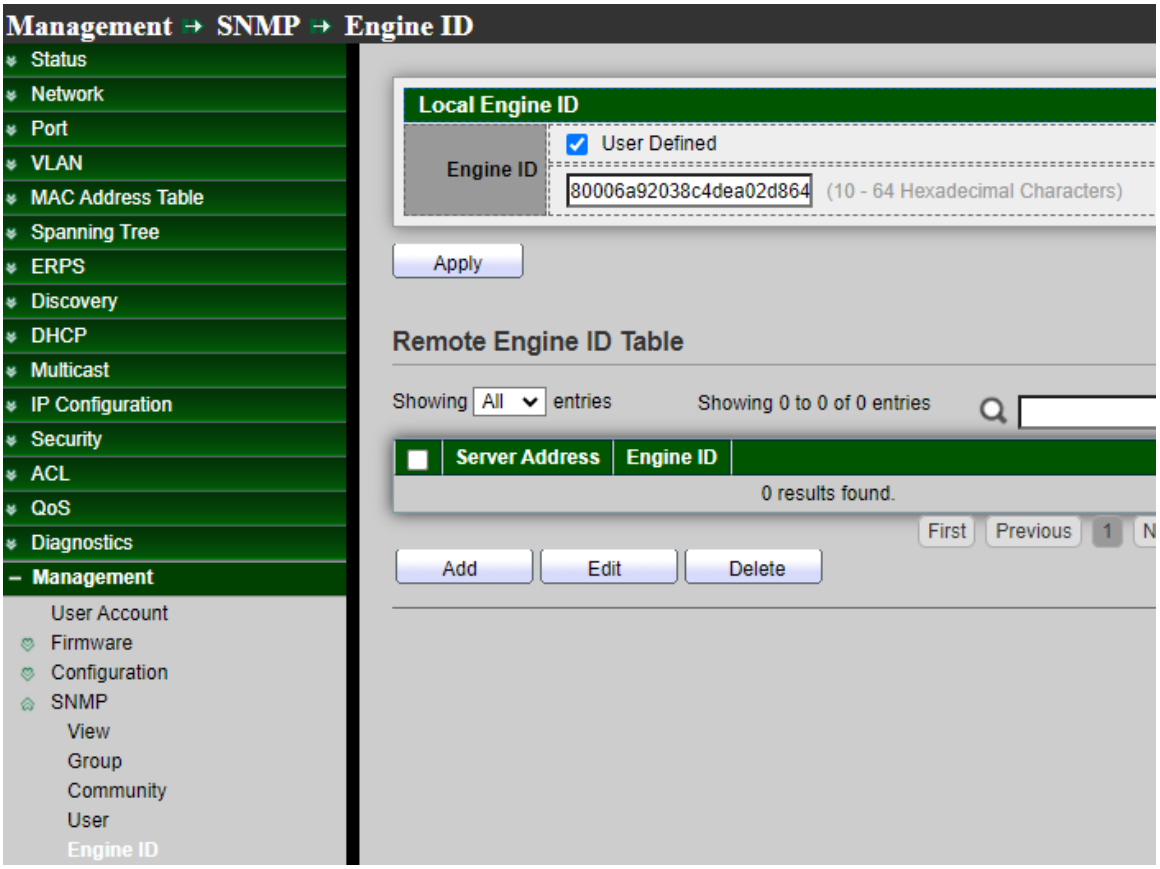
### Privacy

- **Method :** 加密協定。
  - **None :** 無需隱私保護。
  - **DES :** 資料加密標準(DES)演算法。
- **Password :** 隱私保護密碼，字元長度範圍為 8 至 64 字元。

*點擊**"Apply"**儲存您的變更，或**"Close"**關閉設定。*

## 18.4.5 引擎 ID(Engine ID)

引擎 ID 為僅用在管理 SNMPv3 實體的唯一標識。SNMP 代理被認為是權威的 SNMP 引擎。這表示代理會回應傳入訊息(Get、GetNext、GetBulk、Set)，並向管理器傳送陷阱訊息。
每個 SNMP 代理維護用於 SNMPv3 訊息交換的本地資料。預設的 SNMP 引擎 ID 由企業號和預設 MAC 位址組成。SNMP 引擎 ID 在管理域必須是唯一的，因此一個網絡中不會有兩個設備有相同的引擎 ID。設定**"add"**、**"Edit"**和**"Delete"**功能進行管理。



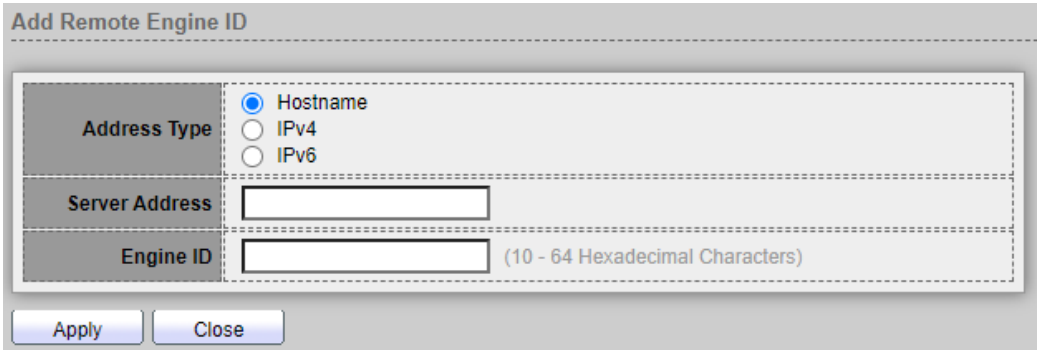

## Local Engine ID

- **Engine ID :** 如果選中 “User Defined”，則本地引擎 ID 由使用者設定，否則使用由 MAC 和企業號組成的預設引擎，使用者定義的引擎 ID 範圍為 10 至 64 十六進制字元，且十六進制數字必須能除 2。

*點擊"Apply"儲存您的變更設定。*

## Remote Engine ID Table

| 欄位 | 描述 |
|---|---|
| Server Address | 遠端主機位址 |
| Engine ID | 指定遠端SNMP引擎ID。引擎ID範圍為10至64十六進制字元，且十六進制數字必須能除2 |



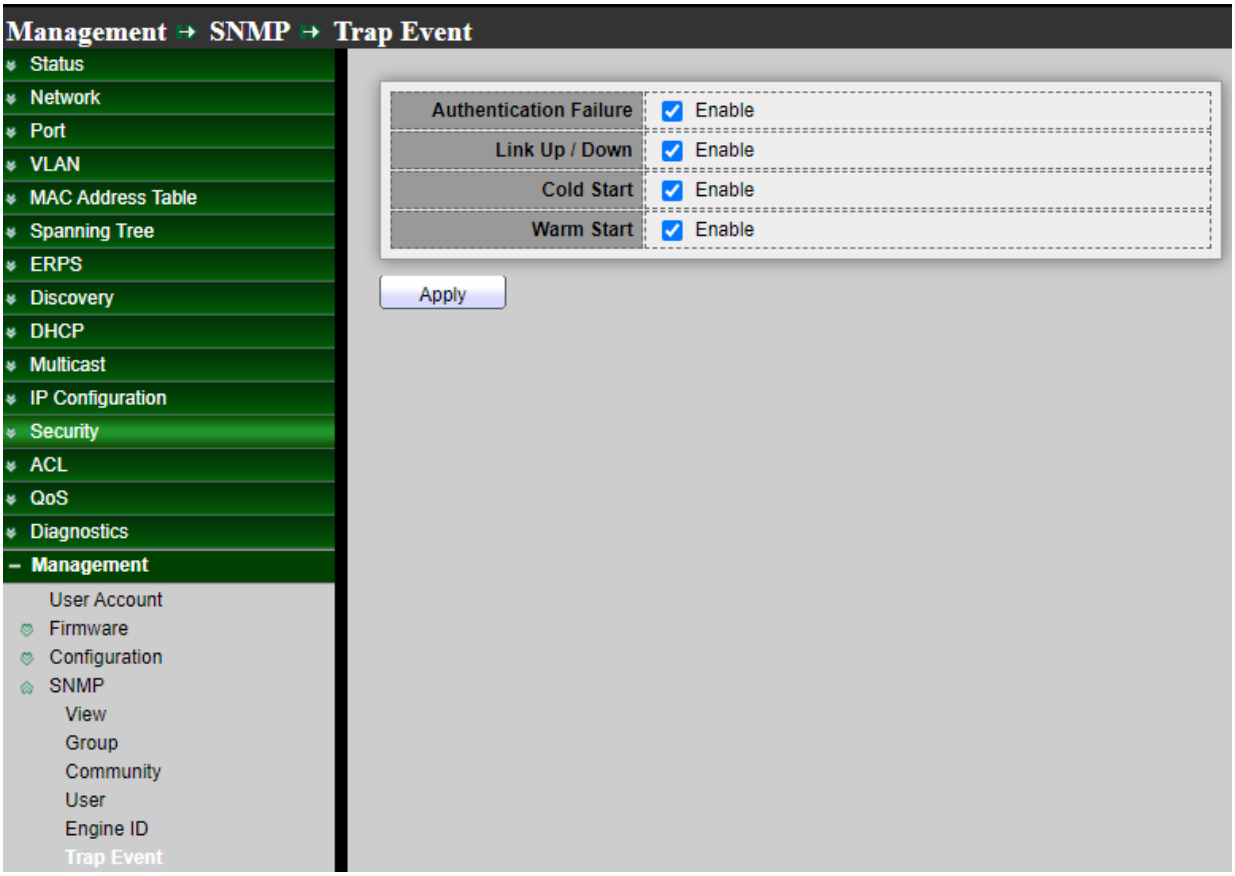

- **Address Type :** 遠端主機位址類型為主機名稱/IPv4/IPv6。
- **Server Address :** 遠端主機位址。
- **Engine ID :** 指定遠端 SNMP 引擎 ID。引擎 ID 範圍為 10 至 64 十六進制字元，且十六進制數字必須能除 2。

*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

### 18.4.6 事件採集(Trap Event)

使用者管理員可以選擇要監控的 SNMP 採集事件類型。

產生此採集 SNMP 訊息是為了報告系統事件，如網路標準 RFC 1215 中所定義的內容。

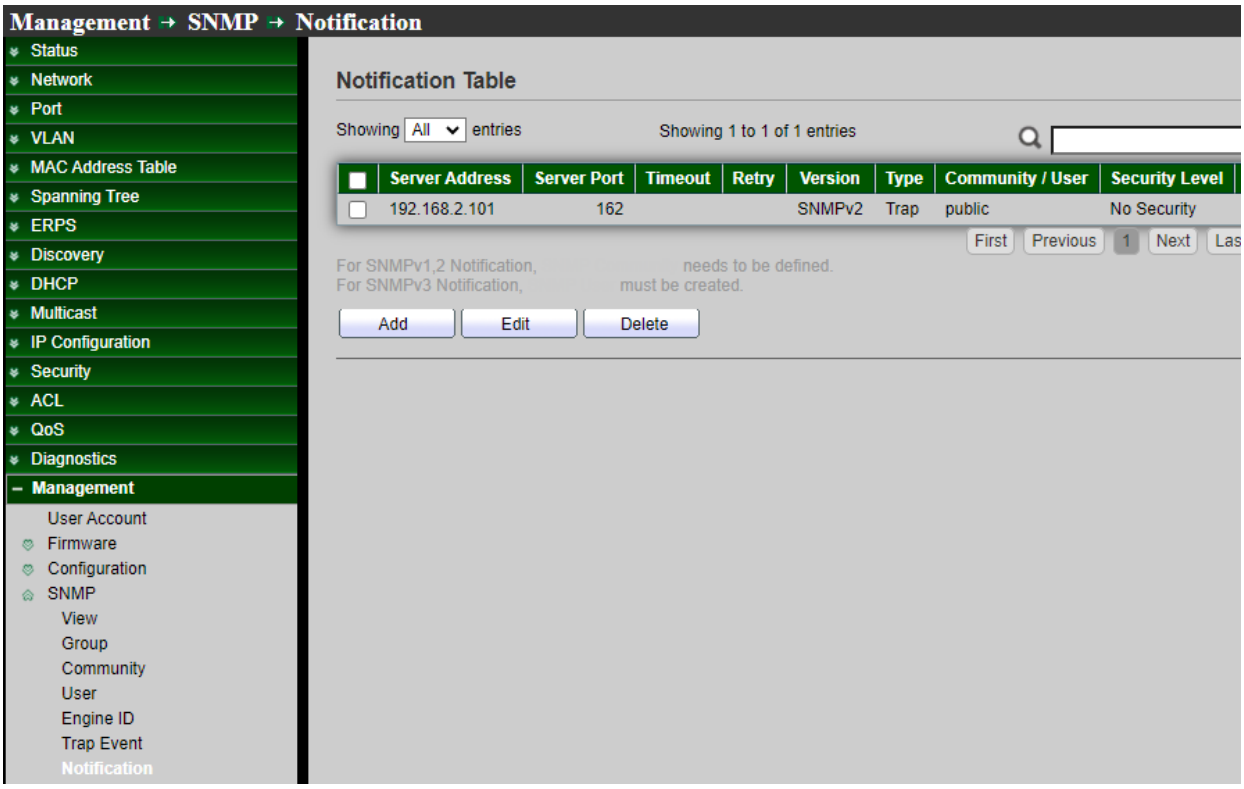



| 欄位 | 描述 |
|---|---|
| Authentication Failure | 驗證錯誤；SNMP的採集擷取驗證失敗，當社群Community字串設定不符或使用者身份驗證密碼不符時進而觸發的採集擷取。 |
| Link Up/Down | 連接埠鏈路上行或下行進而觸發的採集擷取。 |
| Cold Start | 冷啟動；當設備通過使用者設定重啟後進而觸發的採集擷取。 |
| Warm Start | 熱啟動；當設備斷電重啟後進而觸發的採集擷取。 |

*點擊"Apply"儲存您的變更設定。*

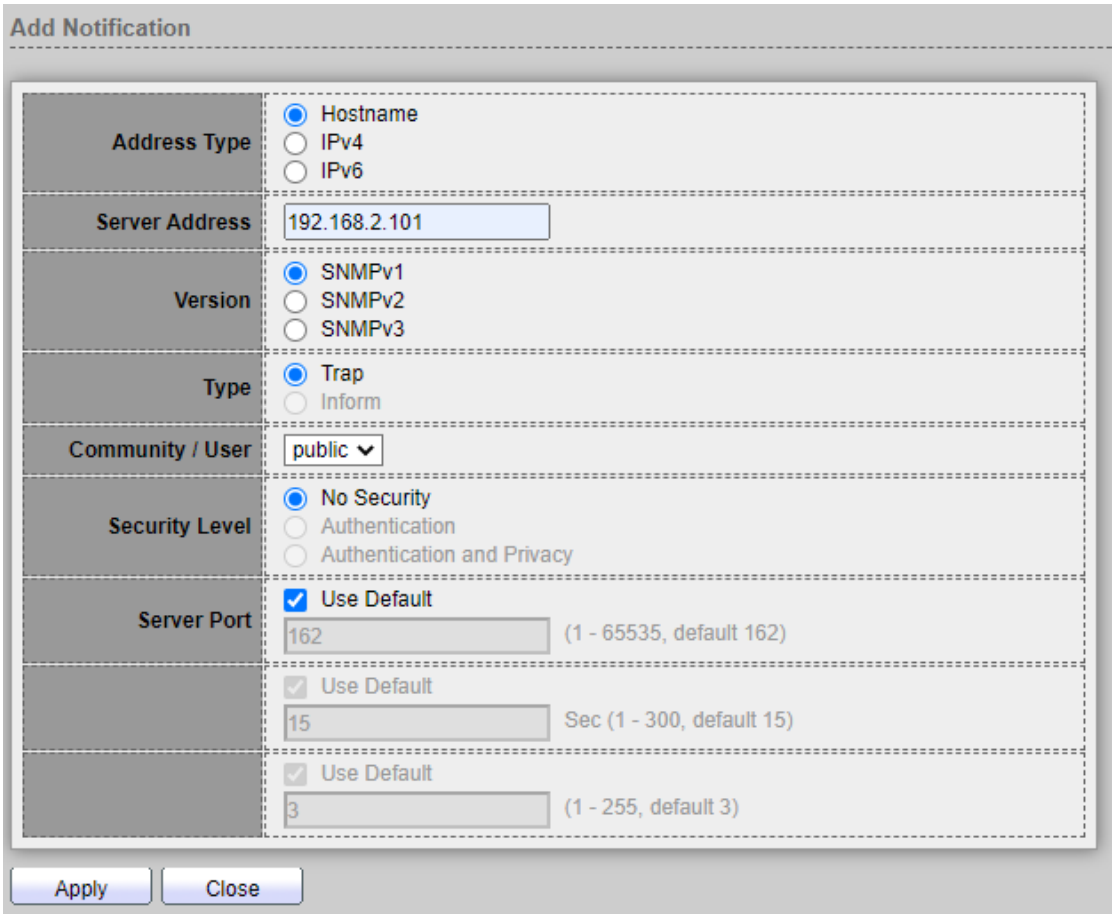
## 18.4.7 通知(Notification)

通知是交換器發送陷阱訊息的網路節點。通知接受者列表被定義為陷阱訊息的目標。陷阱接收器清單包含節點的 IP 位址以及在陷阱訊息理對應版本的 SNMP 憑證。當發生需要發送陷阱訊息的事件時，將向通知接收者表中列出的每個節點發送訊息，設定"**add**"、"**Edit**"和"**Delete**"功能進行管理。




| 欄位 | 描述 |
|---|---|
| Server Address | SNMP陷阱接收者的IP位址或主機名稱 |
| Server Port | 接受者伺服器 UDP 連接埠編號 |
| Timeout | 指定 SNMP 通知逾時 |
| Retry | 指定 SNMP 通知的重試計數器 |
| Version | 指定SNMP通知版本<br>• **SNMPv1** : SNMP版本1通知<br>• **SNMPv2** : SNMP版本2通知<br>• **SNMPv3** : SNMP版本3通知 |

| | |
|---|---|
| Type | 通知類型<br>• **Trap :** 發送SNMP陷阱到主機<br>• **Inform :** 發送SNMP通知到主機 |
| Community/User | 用於通知的SNMP社群/使用者名稱。如果版本是SNMPv3，則名稱為使用者名，否則為社群名稱 |
| Security Level | SNMP通知封包安全級別<br>• **No Security :** 指定不執行封包身份認證<br>• **Authentication :** 指定執行未加密封包的身份認證<br>• **Authentication and Privacy :** 指定執行帶加密封包的身份認證 |



- **Address Type :** 遠端主機位址類型為主機名稱/IPv4/IPv6。
- **Server Address :** SNMP 陷阱接收者的 IP 位址或主機名稱。
- **Version :** 指定 SNMP 通知版本。
  - **SNMPv1 :** SNMP 版本 1 通知。
  - **SNMPv2 :** SNMP 版本 2 通知。
  - **SNMPv3 :** SNMP 版本 3 通知。
- **Type :** 通知類型。
  - **Trap :** 發送 SNMP 陷阱(設陷)到主機。
  - **Inform :** 發送 SNMP 通知到主機(v1 沒有通知)。
- **Community/User :** 用於通知的 SNMP 社群/使用者名稱。如果版本是 SNMPv3，則名稱為使用者名，否則為社群名稱。
- **Security Level :** SNMP 通知封包安全級別，安全級別必須低於或等於社群/使用者名稱。
  - **No Security :** 指定不執行封包身份認證。
  - **Authentication :** 指定執行未加密封包的身份認證。
  - **Authentication and Privacy :** 指定執行帶加密封包的身份認證。
- **Server Port :** 接收者伺服器 UDP 連接埠編號，如果選中“use default”則值為 162，否則為使用者設定。
- **Timeout :** 指定 SNMP 通知超時，如果選中“use default”則值為 15，否則為使用者設定。
- **Retry :** 指定 SNMP 通知重新計數器，如果選中“use default”則值為 3，否則為使用者設定。

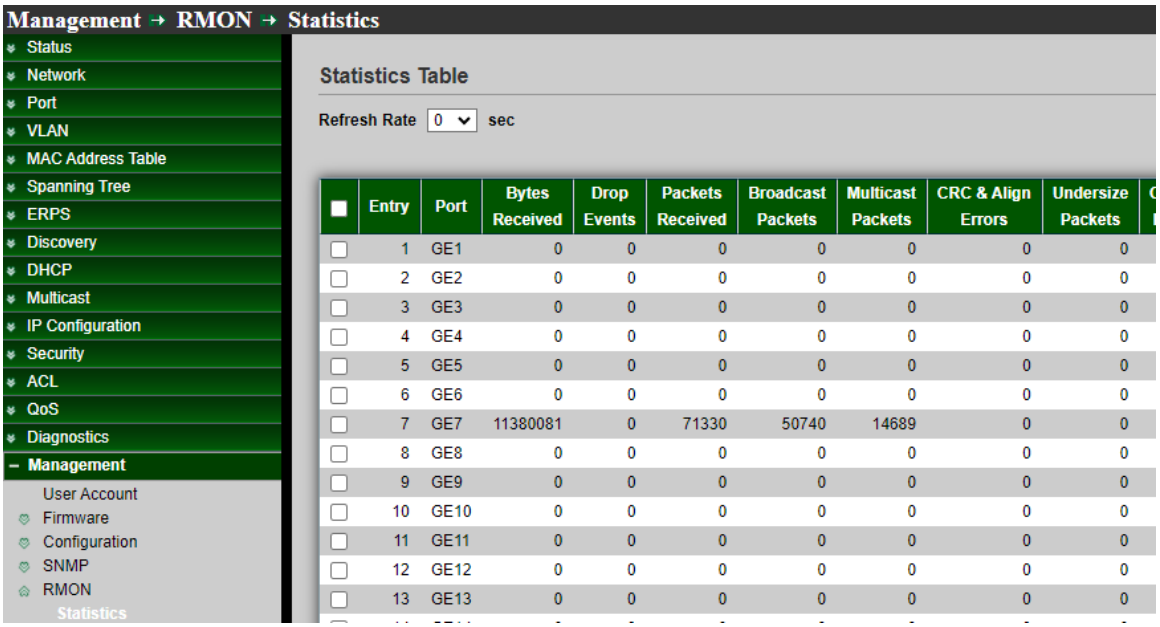
*點擊**"Apply"**儲存您的變更，或**"Close"**關閉設定。*

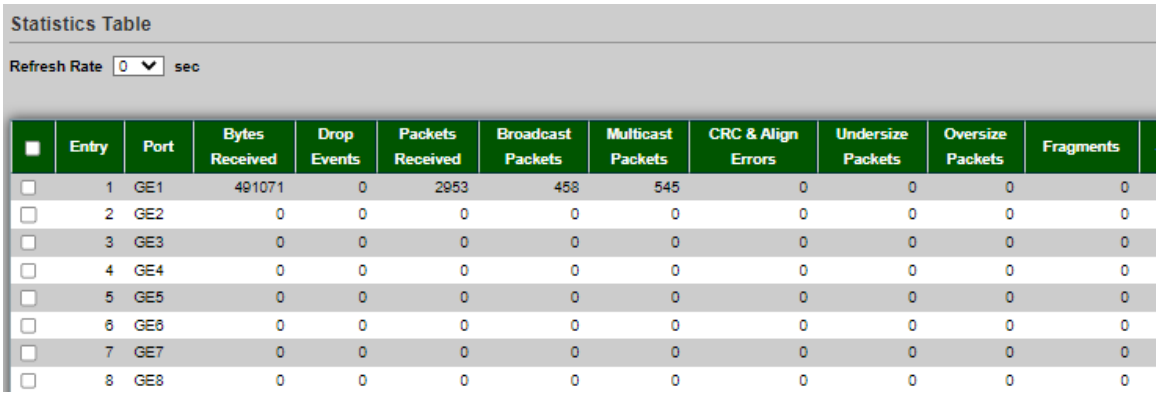
# 18.5 RMON

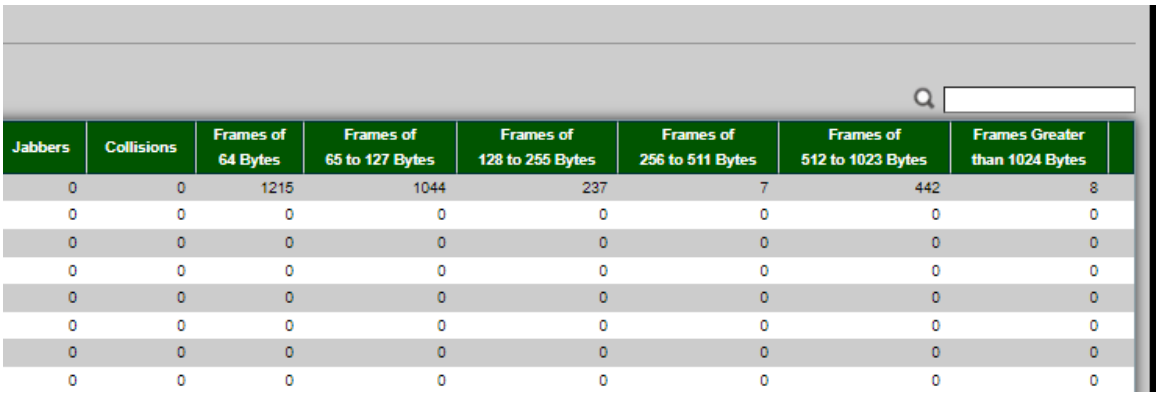
## 18.5.1 統計數據(Statistics)

此頁面顯示每個介面的流量統計資料。可以選擇資訊的刷新速率。此頁面可用於分析發送和接收的流量及其分佈情況(單播、多播和廣播)。

*點擊 "Clear" 清除此頁面，或點擊 "Refresh" 重新整理頁面，或點擊 "View" 檢視頁面。*





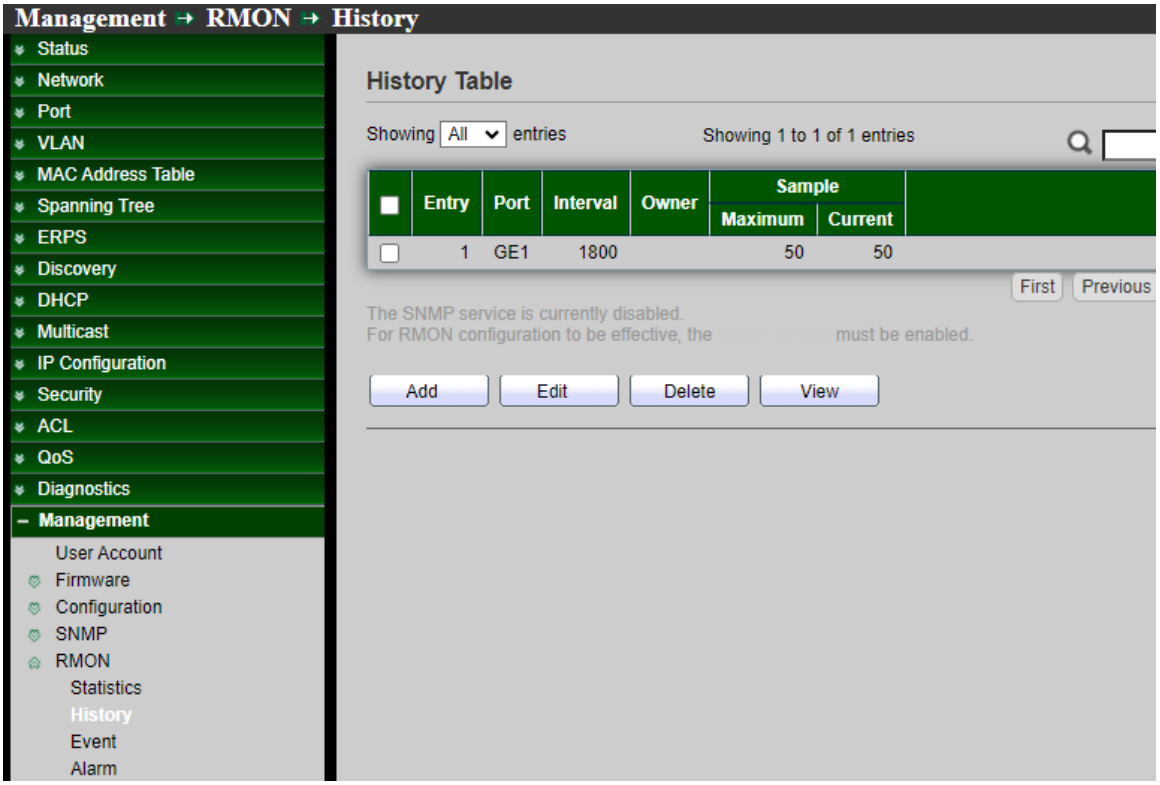
| Jabbers | Collisions | Frames of 64 Bytes | Frames of 65 to 127 Bytes | Frames of 128 to 255 Bytes | Frames of 256 to 511 Bytes | Frames of 512 to 1023 Bytes | Frames Greater than 1024 Bytes |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 1215 | 1044 | 237 | 7 | 442 | 8 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

| 欄位 | 描述 |
|---|---|
| Port | RMON統計數據的連接埠 |
| Bytes Received | 收到的八位元組數，包括錯誤封包和 FCS 八位元組，但不包括幀位元 |
| Drop Events | 丟棄的封包數量 |
| Packets Received | 接收的封包數量，包括錯誤封包、多播封包和廣播封包 |
| Broadcast Packets | 接收的良好廣播封包數量。該數量不包括多播封包 |
| Multicast Packets | 接收的良好多播封包數量 |
| CRC & Align Errors | 發生的循環多餘校驗(CRC)錯誤和對齊錯誤數 |
| Undersize Packages | 接收的過小封包(小於64個八位元組)的數量 |
| Oversize Packages | 接收的過大封包(超過1518個八位元組)的數量 |
| Fragments | 接收的片段(少於64個八位元組的封包，不包括幀位元，但包括FCS八位元組)的數量 |

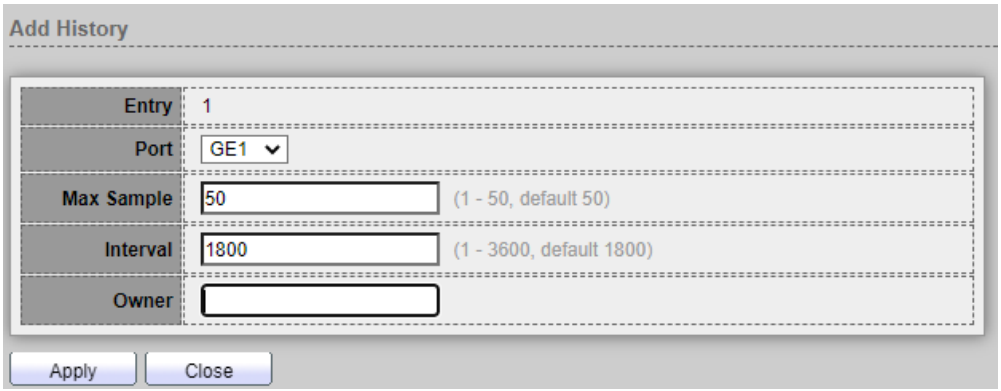
| | |
|---|---|
| Jabbers | 接收的超過1632個八位元組的封包數量。該數字不包括訊框位元，但包括的不良FCS(訊框檢查序列)的FCS八位元組具有整數的八位元組數(FCS錯誤)，或具有非整數八位元組數(對齊錯誤)。Jabber封包被定義為滿足以下標準的乙太網路訊框 ：<br>• 封包資料長度超過MRU(最大接收位元)<br>• 封包具有無效CRC<br>• 未檢測到RX錯誤事件 |
| Collision | 接收的衝突數。如果啟動巨大封包，則將Jabber訊框的限制值提高到巨大封包的最大大小 |
| Frames of 64 Bytes | 接收的包含64位元組的訊框數量 |
| Frames of 65 to 127 Bytes | 接收的包含65至127位元組的訊框數量 |
| Frames of 128 to 255 Bytes | 接收的包含128至255位元組的訊框數量 |
| Frames of 256 to 511 Bytes | 接收的包含256至511位元組的訊框數量 |
| Frames of 512 to 1023 Bytes | 接收的包含512至1023位元組的訊框數量 |
| FramesGreater than 1024 Bytes | 接收的包含1024至1518位元組的訊框數量 |

### 18.5.2 歷史記錄(History)

使用“History Table”頁面定義取樣頻率，要存儲的樣本量以及從收集數據的埠。對數據進行取樣和存儲後，它會出現在歷史記錄表頁面上，可以通過單擊歷史記錄表查看，設定**"add"**、**"Edit"**、**"Delete"**和**"view"**功能進行管理。




| 欄位 | 描述 |
|---|---|
| Port | RMON歷史記錄的連接埠 |
| Interval | 每次取樣的時間間隔 |
| Owner | 事件的使用者名稱 (0~31個字元) |
| Sample | 保存樣本的最大數量<br>• **Maximum :** 樣本的最大數量<br>• **Current :** 樣本的當前數量 |

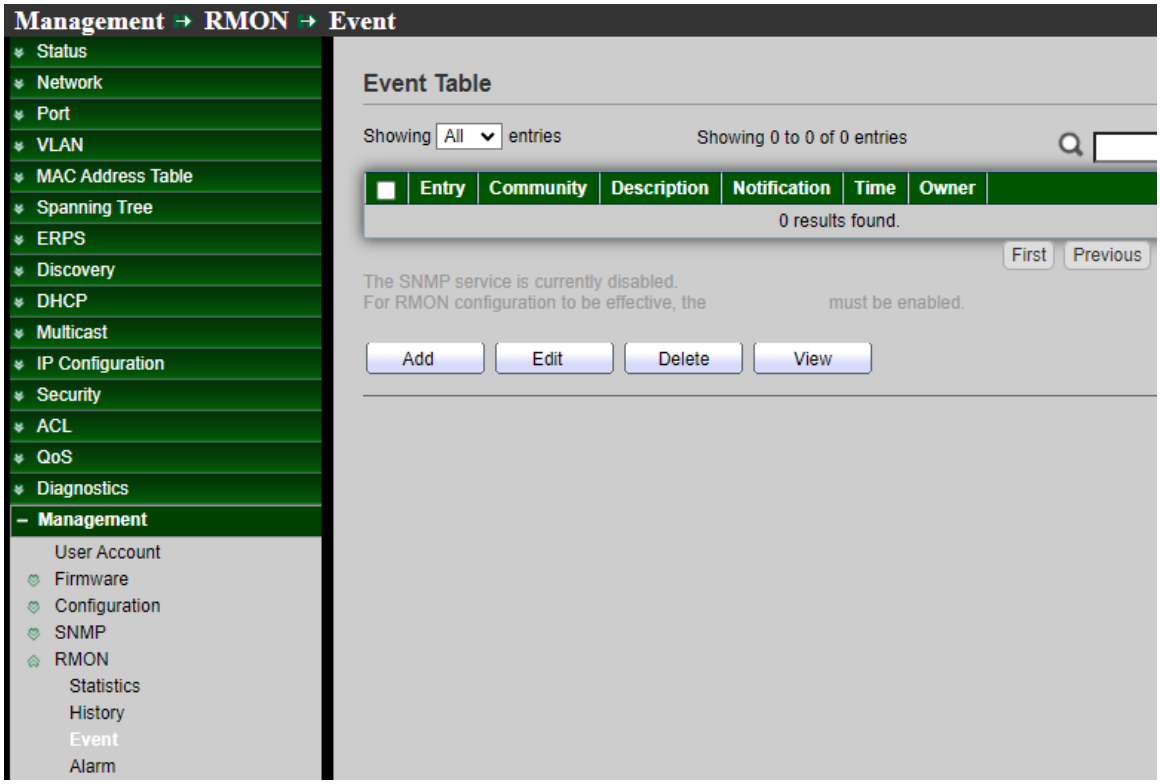



- **Port :** 選擇連接埠進行設定。
- **Max Sample :** 指定保存樣本的最大數量。
- **Interval :** 輸入從介面收取樣本的時間(以秒為單位)，指定每個樣本的秒數。
- **Owner :** 輸入請求 RMON 資料的 RMON 工作站或使用者，指定事件的擁有者名稱(0~31 個字元)。

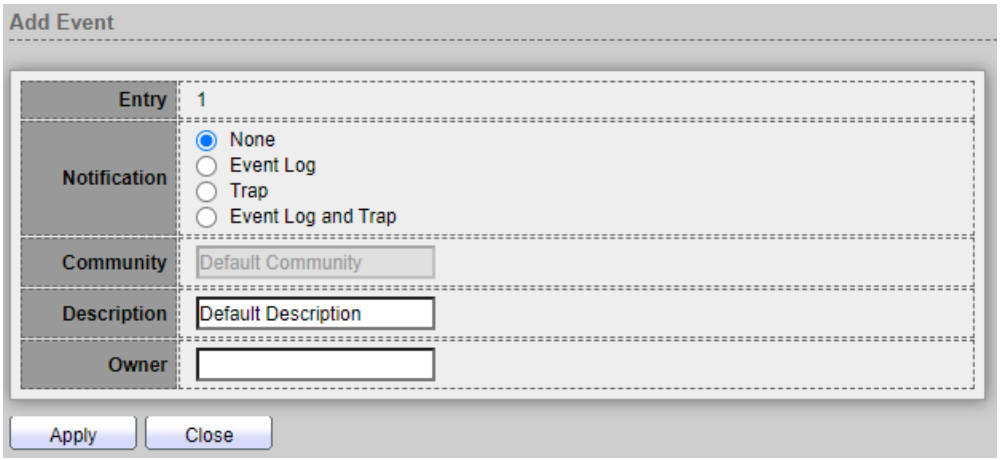
*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

### 18.5.3 事件(Event)

事件頁面用於設定事件，這些事件是產生警報時執行的操作(警報在 “Alarms” 頁面上定義)。事件可以是日誌和陷阱的任意組合。如果操作包含記錄事件，它們將顯示在 “Event Log Table” 頁面上，並設定**"Add"**、**"Edit"**、**"Delete"**和**"view"**功能進行管理。




| 欄位 | 描述 |
|---|---|
| Entry | 顯示事件對應的清單 |
| Community | 顯示指定的社群 |
| Description | 顯示事件的描述 |
| Notification | 事件的通知類型，可能的值有：None/Event Log/Trap/Event Log and Trap |
| Time | 每個樣本的秒數 |
| Owner | 事件的所有者名稱(0~31個字元) |

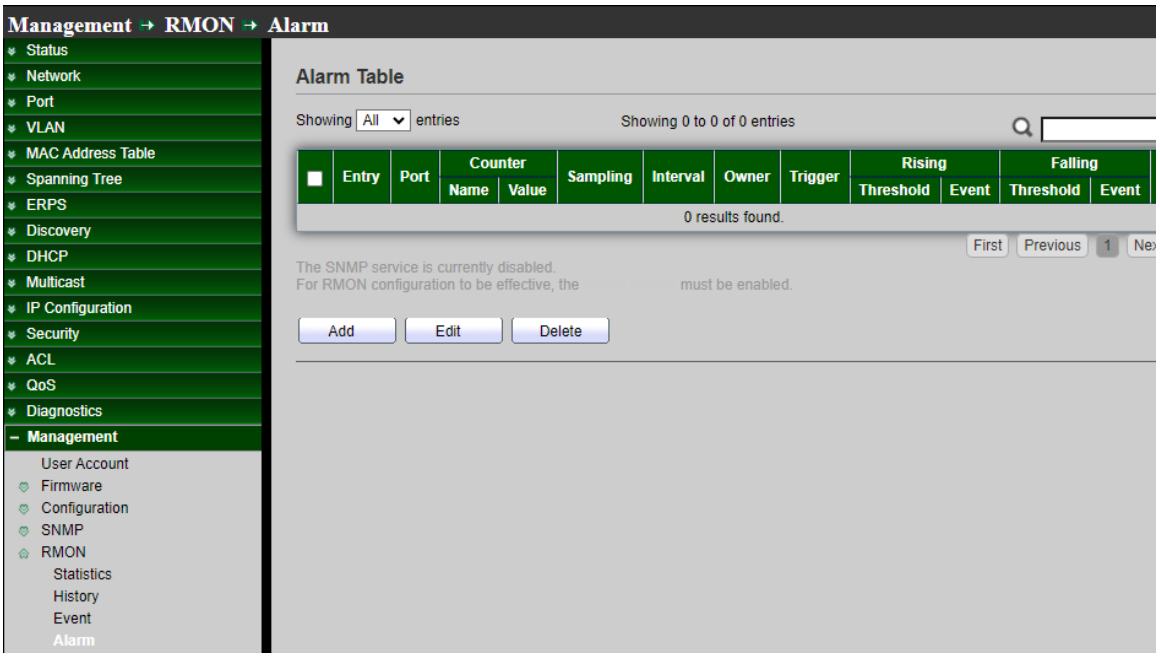



- **Entry :** 事件對應的清單編號。
- **Notification :** 指定事件的通知類型，可選如下值：
  - **None :** 沒有任何通知。
  - **Event Log :** 在 RMON 的 “Event Log table” 中記錄事件日誌。
  - **Trap :** 向網管站發送 trap 訊息。
  - **Event Log and Trap :** 記錄事件日誌並發送 SNMP trap 訊息。
- **Community :** 當通知類型指定為 “Trap” 和 “Event Log and Trap” 時，指定 SNMP 社群名稱，其最大長度為 20 個字元。
- **Description :** 指定事件的描述。
- **Owner :** 指定事件的所有者。

*點擊"Apply"儲存您的變更，或"Close"關閉設定。*

### 18.5.4 警報(Alarm)

RMON 警報提供了一種機制，用於設定限制值和採樣間隔，以防在代理維護的計數器或其他 SNMP 物件計數器上生成異常事件。必須在警報中配置上升限制值和下降限制值。超過上升限制值後，不會生成上升事件，直到越過相應的下降限制值。發出下降警報後，只有當越過上升限制值時才會發出下一個警報。設定"Add"、"Edit"和"Delete"功能進行管理。




| 欄位 | 描述 |
|---|---|
| Port | RMON警報的連接埠設定 |
| Counter | 取樣計數器<br>• **DropEvents (Drop Event)**：接收的丟棄封包的事件總數<br>• **Octes (Received Bytes)**：接收的八位元組數<br>• **Pkts (Received Packets)**：接收的封包數量<br>• **BroadcastPkts (Broadcast Packets Received)**：接收的廣播封包數<br>• **MulticastPkts (Multicast Packets Received)**：接收的多播封包數<br>• **CRCAlignError (CRC and Align Error)**：發生的CRC錯誤和對齊錯誤數<br>• **UndersizePkts (Undersize Packets)**：接收的過小封包的數量<br>• **OversizePkts (Oversize Packets)**：接收的過大封包的數量<br>• **Fragments (Fragments)**：接收的片段的總數量<br>• **Jabbers (Jabbers)**：jabber 封包的總數量<br>• **Collisions (Collisions)**：接收的衝突數<br>• **Pkts64Octetes (Frames of 64 Bytes)**：接收 64 位元組的封包數量<br>• **Pkts65to127Octetes (Frames of 65 to 127 Bytes)**：接收的 65 至 |

| | |
|---|---|
| | 127 位元組的封包數量<br>• **Pkts128to255Octetes (Frames of 128 to 255 Bytes)**：接收的 128 至 255 位元組的封包數量<br>• **Pkts256to511Octetes (Frames of 256 to 511 Bytes)**：接收的 256 至 511 位元組的封包數量<br>• **Pkts512to1023Octetes (Frames of 512 to 1023 Bytes)**：接收的 512 至 1023 位元組的封包數量<br>• **Pkts1024to1518Octets (Frames Greater than 1024 Bytes)**：接收的 1024至1518位元組的封包數量 |
| **Version** | 采樣類型包括:<br>• **Absolute :** 所選變量值在採樣間隔結束時直接與限制值進行比較<br>• **Delta :** 所選變量在採樣間隔內的變化值與限制值進行比較 |
| **Interval** | 每個樣本的時間間隔 |
| **Owner** | 警報清單的所有者名稱 |
| **Trigger** | 事件觸發的類型 |
| **Rising Threshold** | 觸發上升事件的限制值 |
| **Rising Event** | 警報觸發的上升事件 |
| **Falling Threshold** | 觸發下降事件的限制值 |
| **Falling Event** | 警報觸發的下降事件 |