GigaX1024i+

第二層智慧型交換器

使用手冊

T2698 / 2006年10月

版權資訊

T2698
2006 年 10 月
第一版

華碩連絡資訊

華碩電腦公司 ASUSTeK COMPUTER INC.
地址　台灣臺北市北投區 112 立德路 15 號
電話　+886-2-2894-3447
傳真　+886-2-2894-7798
電子郵件　info@asus.com.tw
全球資訊網　www.asus.com.tw

技術支援
電話　0800-093-456

ASUS COMPUTER INTERNATIONAL **(美國)**
地址　44370 Nobel Drive, Fremont, CA 94538, USA
傳真　+1-510-608-4555
全球資訊網　usa.asus.com

技術支援
電話
+1-502-995-0883(主機板 / 其他產品)
+1-510-739-3777 x5110 (筆記型電腦)
傳真　+1-502-933-8713
線上支援　support.asus.com

ASUS COMPUTER GmbH **(德國 / 奧地利)**
地址　Harkort Str. 25, D-40880 Ratingen, Germany
電話　+49-2102-95990
傳真　+49-2102-959911
全球資訊網　www.asuscom.de
線上連絡　www.asuscom.de/sales

技術支援
電話
+49-2102-95990 (主機板 / 其他產品)
+49-2102-959910 (筆記型電腦)
傳真　+49-2102-959911
線上支援　support.asus.com

目錄內容

圖片目錄

表格目錄

1 產品簡介

感謝您購買華碩 GigaX 第二層智慧型交換器！

從現在開始， 您可以透過友善且功能強大的使用者介面來管理您的區域網路。 本使用手冊將為您介紹如何安裝 GigaX 第二層智慧型交換器，以及如何設定 GigaX 第二層智慧型交換器以更好地利用其優異的功能。

1.1 關於本使用手冊

1.1.1 注意事項

- 本手冊將在縮寫詞第一次出現時解釋其含義，並將其含義解釋收入術語表中。
- 為了方便起見，在本手冊中，GigaX 第二層智慧型交換器將簡稱為「本交換器」。
- 術語「LAN（區域網路）」和「網路」在本手冊中將交替使用，表示某個區域內由乙太網路連接的一組電腦。

1.1.2 印刷提示

粗體字 表示該文字是您從選單或下拉選單中選擇的項目，或是需要您輸入的內容。

1.1.3 提示符號

在本使用手冊中會出現以下的圖示及說明文字，請您特別注意這些重點事項，這些圖示所代表的含義如下：

注意：提供對當前所述內容的說明或額外資訊。

定義：解釋使用者可能不瞭解或不熟悉的術語或縮寫。這些術語均可在術語表中查到。

警告：高重要性的資訊，包括涉及人身安全和系統完整性的資訊。

1.2 產品包裝內容

華碩 GigaX 1024i+ 交換器的產品包裝中包含以下物品：

- ☑ GigaX 1024i+（28 埠）第二層智慧型交換器
- ☑ AC 電源線
- ☑ 機架安裝套件（包括兩個托架與六顆 #6–32 螺絲）
- ☑ 使用手冊

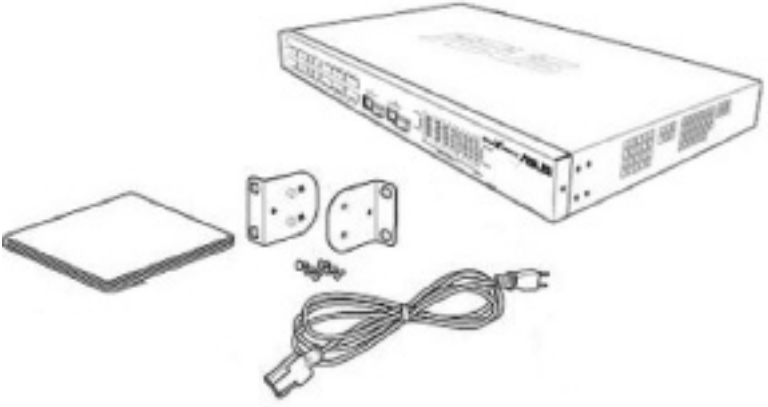


圖 1. GigaX 第二層智慧型交換器包裝內容

1.3 特性

- 24 個 10/100 BASE-TX 自動偵測高速乙太網路連接埠
- 2 個 10/100/1000BASE-T 自動偵測 Gigabit 乙太網路交換埠
- 2 個小型 (SFP) Gigabit 介面轉換插槽 (GBIC)
- 802.1D/802.1w 透明橋接 (transparent bridge)/ 生成樹協定 (spanning tree protocol)/ 快速生成樹協定 (rapid spanning tree protocol)
- 8K MAC 位址快取及硬體控制的老化時間
- 802.3x 流量控制
- 基於 802.1Q 標記 (tagged) 之虛擬區域網路 (VLAN)，最多支援 256 組 VLAN
- 以連接埠為基礎的 VLAN
- 私有 VLAN
- 802.1p 服務等級，每個連接埠支援 4 個佇列
- 支援 IGMP 偵聽 (v1/v2)
- 支援靜態多重播送群組
- 802.3ad 連結匯聚 (手動與 LACP)，最多可支援 15 個幹線群組
- 連接埠鏡像 (Port Mirroring) 功能
- 802.1X 以連接埠為基礎的網路存取控制
- RADIUS 遠端認證撥入使用者服務
- 傳入與傳出頻寬控制
- 連接埠安全 (Port Security) 功能
- 乙太網路纜線診斷
- DHCP 用戶端
- 服務品質等級：目的地 / 來源 MAC 優先權，VLAN 優先權，IPv4 ToS/ DiffServ， IPv6 流量等級 (Traffic Class)
- RMON：支援 4 個群組 (1, 2, 3, 9)
- SNMP v1, v2, v3 簡易網路管理通訊協定
- 支援 MIB-II 管理資料庫
- 企業級系統韌體版本資料庫 (MIB)
- FTP 用於韌體升級與設定備份
- 系統記錄 (Syslog.)
- 網頁圖形使用者介面 (GUI)
- LED 指示燈用於顯示連接埠連線狀態
- LED 指示燈用於顯示系統狀態

1.4 前面板特性

前面板的 LED 指示燈號可顯示系統及連接埠狀態。

圖 2. 前面板

表 1: 前面板標示與 LED 指示燈號

標示	顏色	狀態	說明
SYSTEM	綠色	恆亮	裝置電源開啓
		閃爍	自我檢測，初始化或下載中
	琥珀色	恆亮	溫度或電壓不正常
	熄滅		無電源供應
10/100/1000 port status	綠色	恆亮	已建立 RJ-45 或 SFP 連線；連接埠已啓用
		閃爍	正在傳送或接收資料
	熄滅		無乙太網路連線
10/100/1000 port speed	綠色	恆亮	Gigabit 連接埠的連線速率為 1000Mbps，或 10/100 連接埠的連線速率為 100Mbps
	琥珀色	恆亮	Gigabit 連接埠的連線速率為 100Mbps
	熄滅		連線速率為 10Mbps 或未連線

1.5 後面板特性

本交換器的後面板包含有一個電源線插孔。

圖 3. 後面板

表 2: 後面板標示

標示	說明
Power connector	連接電源線

1.6 技術規格

表 3: 技術規格

實體尺寸	43.5mm(H) X 444 mm(W) X 180mm(D)		
電源	輸入：100–240V AC/2A 50–60Hz		
	耗電量：<50 watts		
環境需求		運作	存放
	溫度	0 – 40°C (32 – 104°C)	-25 – 70°C (-13 – 158°C)
	濕度	5 – 90%	0 – 95%
	高度	最高 10,000ft (3,000m)	最高 40,000ft (12,000m)

2 快速安裝指南

本章節將介紹如何設定交換器的工作環境。

第一部分介紹如何將 GigaX1024i+ 交換器安裝在水平表面或機架上。

第二部分介紹硬體設定的步驟。

第三部分介紹 GigaX1024i+ 交換器的基本設定。

在您開始安裝和設定之前，請先向網路系統管理員取得以下相關資訊：

交換器的 IP 位址

預設的網路閘道器位址

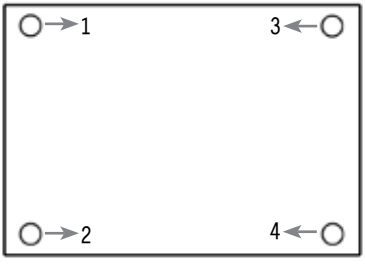
您所處網路的網路遮罩

2.1 第一部分 — 硬體安裝

您可以將本交換器安裝至水平表面或機架上。

2.1.1 將交換器安裝於水平表面

本交換器必須安裝在水平的，且能承受交換器及其附件重量的表面上。請將四個塑膠墊粘貼於交換器底部所標示的位置。參見下面的說明。



請將四個塑膠墊粘貼於交換器底部所標示的位置

2.1.2 將交換器安裝於機架

1. 將固定托架鎖在本機兩側，並將交換器置入機架。
2. 用螺絲將托架鎖在機架上。

2.2 第二部分 — 安裝交換器

將本交換器連上電源，並連接至電腦與網路。圖 4 為本交換器的硬體連接示意圖。

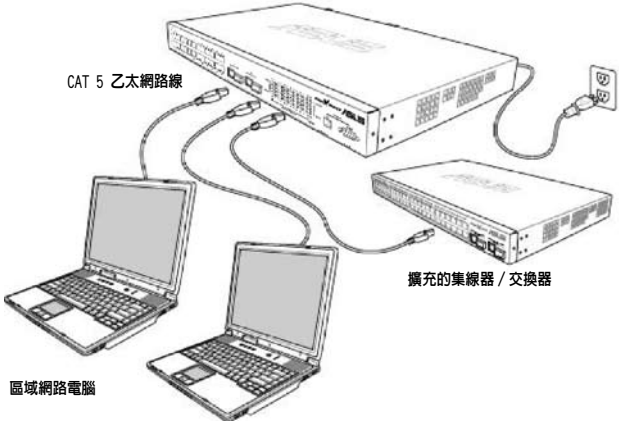


圖 4. 硬體連接示意圖

2.2.1 連接到電腦或區域網路

您可以使用乙太網路線將電腦、集線器(hub)或其他交換器連接到本交換器的連接埠。您可以使用直通型或交叉型乙太網路線來連接這些裝置。

請使用第 5 類乙太網雙絞線來連接 1000BASE-T 連接埠。否則，傳輸速率無法達到 1Gbps。

2.2.2 連接電源線

1. 將 AC 電源線的一端連接到交換器後面板的電源插孔，然後將電源線的另一端連接到電源插座。
2. 依照表 4 的描述檢查前面板的 LED 指示燈狀態。若 LED 指示燈亮起，如表中所述，則代表交換器的硬體已正常運作。

表 4: LED 指示燈

No	LED	說明
1	System	穩定的綠色代表交換器已經開啓。如果 LED 熄滅，請檢查交換器電源線是否正確連接並已連接到電源插座。
2	Switch ports [1] to [28]	穩定的綠色代表交換器和其他裝置的連接已經建立。閃爍代表交換器正在傳送或接收資料。

2.3 第三部分 — 交換器基本設定

當您完成硬體的安裝和連接後，還需要對交換器進行基本管理設定。您可以用下面的方法進行設定：

- **設定管理器：** 本交換器提供網頁管理介面，您可以使用帶 Java® 功能的 IE5.0 或更高版本的瀏覽器進行設定。 詳細說明請參考第 3 章與第 4 章。

2.3.1 透過設定管理器 (Configuration Manager) 進行設定

本交換器提供了一個預先安裝的網頁介面軟體應用程式，稱為設定管理器 (Configuration Manager) 。

您可以透過與本交換器 LAN 埠相連的任意一台電腦上的網頁瀏覽器（如 Microsoft Internet Explorer® 5.0 或更高版本，不支援 Netscape）來存取設定管理器。

1. 在預設情況下，交換器的網頁認證是關閉的。您必須開啓它以保證系統的安全設定。您可以在 **System --> Administration** 頁面開啓交換器的網頁認證功能。

2. 在網頁瀏覽器(IE 5.0 或更高版本)中，輸入以下IP位址：**http://192.168.1.1** 並按下 <Enter>。這是交換器的預設 IP 位址。

   此時將出現登入畫面，如圖 5 所示。

圖 5. 登入畫面

3. 輸入您的使用者名稱與密碼，然後按下**<OK>**。當登入畫面首次出現時，請使用下面的預設值：

   使用者名稱: admin
   密碼：（無密碼）

您可以隨時更改密碼。

4. 要設定一個新的 IP 位址，請點選 **System —> IP Setup**。填入新的 IP 位址，網路遮罩與預設閘道，然後點選 **<OK>**。

圖 6. IP 設定

5. 若新的位址與預設的不同，瀏覽器不會更新交換器的狀態視窗或重新取得任何頁面，這是正常情況。請在網址欄內輸入新的 IP 位址，然後按下 **<Enter>**，即可更新您的網頁顯示。

6. 要開啓網路存取認證功能，請在選單中點選 **Administration** 項，然後選擇 **Enabled** 以開啓密碼保護功能。

3 使用設定管理器（Configuration Manager）

本交換器提供了一個預先安裝的網頁介面軟體應用程式，稱為設定管理器（Configuration Manager）。它可讓您依據網路需要對裝置進行設定。您可以透過與交換器 LAN 埠相連的任意一台電腦上的網頁瀏覽器來存取設定管理器。

3.1 登入到 Configuration Manager

設定管理器（Configuration Manager）已預先安裝到了交換器。要存取這個應用程式，您需要以下條件：

- 一台連接到交換器 LAN 埠的電腦，如快速安裝指南章節所述。
- 您的電腦必須安裝了網頁瀏覽器。建議您使用 Microsoft Internet Explorer® 5.0 或更高版本，這樣可以達到最佳效果。不支援 Netscape。

您可以從任何一台連接到本交換器 LAN 埠的電腦上存取這個應用程式。

3.1.1 設定 Configuration Manager

1. 在預設情況下，交換器的網頁認證是關閉的。您必須開啓它以保證系統的安全設定。您可以在 **System --> Administration** 頁面開啓交換器的網頁認證功能。
2. 在網頁瀏覽器（IE5.0或更高版本）中，輸入以下IP位址：**http://192.168.1.1** 並按下 **<Enter>**。這是交換器的預設 IP 位址。此時將出現如下的登入畫面。

*圖 7. Config manager **登入畫面***

3. 輸入您的使用者名稱與密碼，然後按下<OK>。當登入畫面首次出現時，請使用下面的預設值：

使用者名稱：admin
密碼：（無密碼）

每次登入系統後您都會看到主頁。

圖 8. 主頁

3.1.2 設定一個新的 IP 位址

1. 要設定一個新的 IP 位址，請點選 System —> IP Setup。填入新的 IP 位址，網路遮罩與預設閘道，然後點選 <OK>。
2. 若新的位址與預設的不同，瀏覽器不會更新交換器的狀態視窗或重新取得任何頁面，這是正常情況。請在網址欄內輸入新的 IP 位址，然後按下 <Enter>，即可更新您的網頁顯示。
3. 要開啓網路存取認證功能，請在選單中點選 Administration 項，然後選擇 Enabled 以開啓密碼保護功能。

圖 9. IP 設定

3.2 功能結構

網頁設定頁面包含三個獨立的欄位：頂部欄、左側選單欄與右側欄位。

圖 10. 功能結構

頂部欄包含了交換器圖示和前面板圖，如圖 10 所示。這個欄位將一直位於瀏覽器視窗上方，同步顯示交換器前面板的 LED 燈號。以下是關於各燈號顏色的含義。

- 表 4 為各燈號的代表含義（見第 8 頁）。
- 表 5 為連接埠顏色說明。

表 5. 連接埠顏色說明

連接埠顏色	說明
綠色	乙太網路連線已建立
黑色	無乙太網路連線
琥珀色	連線已存在但連接埠被手動或被生成樹禁用

點選連接埠圖示即可在畫面右下方顯示連接埠的設定狀況。

左側框位為選單欄，包含了本交換器的所有可用功能設定選項。這些功能已經進行了分類，如 System, Bridge 等。您可以點選任何項目以顯示對應的設定頁面。

右側欄位用來顯示設定頁面或統計資料圖。詳細說明請參考第 4.8 章節的說明。

圖 11. 完整選單

3.2.1 瀏覽選單的技巧

- 要展開一組相關的功能選單，請雙按選單項目前的 圖示。
- 要關閉一組相關的功能選單，請雙按選單項目前的 圖示。

3.2.2 常用按鈕與圖示

下表介紹了本管理介面中所有按鈕與圖示的功能。

表 6: 常用按鈕與圖示

按鈕 / 圖示	功能
OK	儲存您對當前頁面做的任何變更。
Add	在系統中新增一個既有的設定，如靜態 MAC 位址或過濾的 ACL 規則。
Modify	修改一個既有項目。
Remove	刪除已選擇的項目，如靜態路由或過濾的 ACL 規則。
Reload	重新顯示當前頁面，且已加載新的統計資料或設定。

4 設定管理

本章節介紹了您可在設定管理器(Configuration Manager)中使用的功能。此設定管理器軟體應用程式已預先安裝至交換器。這些功能包括：

- 系統（System）
- 實體介面（Physical Interface）
- 橋接（Bridge）
- 簡易網路管理通訊協定（SNMP）
- 安全（Security）
- 纜線診斷（Cable Diagnosis）
- 統計圖表（Statistical Chart）
- 儲存設定值（Save Configuration）

要永久儲存對交換器功能（或設定）的變更或新的設定值，您必須至 Save Configuration 頁面，然後點選 <Save>。

4.1 系統頁面（System）

本章節介紹您在設定管理器（Configuration Manager）中的 System 頁面功能可執行的操作：

- 設定系統名稱、連絡資訊、系統位置及其他系統資訊；
- 指定 IP 位址；
- 開啓 / 關閉網頁認證功能；
- 重新啓動交換器；
- 韌體升級

4.1.1 管理（Management）

- Model Name: 產品名稱。
- MAC Address: 交換器的 MAC 位址。
- System Name: 使用者指定的用來辨識系統的名稱(可編輯)。
- System Contact:系統連絡資訊(可編輯）。
- System Location:系統位置（可編輯）

圖 12. 管理

System Name, System Contact 及 System Location 欄位不能包含符號 '/' 。

要儲存您所做的變更，請點選 <OK>。請點選 <Reload> 按鈕來更新設定。

4.1.2 IP 設定（IP Setup）

本交換器可支援動態 IP 與靜態 IP 位址。動態 IP 位址可從同一 VLAN 內的 DHCP 伺服器獲取。IP 設定（IP Setup）頁面包含以下可設定的參數：

- VLAN ID: 為系統管理介面指定 VLAN ID。若要用於管理，VLAN ID 必須位於同一個 VLAN 內。
- DHCP Client: 開啓 DHCP 以獲取動態 IP 位址，或關閉 DHCP 來指定靜態 IP 位址。DHCP 伺服器必須位於所管理的 VLAN 內，且可以存取。
- IP Address: 為交換器的管理介面指定一個靜態 IP 位址。
- Network Mask: 網路遮罩。
- Default Gateway: 預設閘道。

要儲存所做的變更，請點選 <OK>。點選 <Reload> 更新設定。

4.1.3 管理權限（Administration）

管理權限（Administration）頁面可讓您開啓或關閉網頁使用者認證，以及在使用者資料庫中新增 / 移除使用者。您可以設定最多 8 個使用者。預設的網頁存取設定不需要任何認證。

圖 13. 管理權限

- Password Protection is: 開啓或關閉網頁認證功能。
- User Name: 新的使用者名稱。
- Password: 新使用者的密碼。
- Confirm Password: 再次輸入密碼。

點選 <Add> 來新增新的使用者。當您完成修改後請點選 <Modify>。若您想要移除選定的使用者，請點選 <Remove>。

要儲存所做的變更，請點選 <OK>。點選 <Reload> 更新設定。若您開啓了密碼保護功能，您必須立即重新登入。

4.1.4 重新啓動（Reboot）

請依照以下步驟來重新啓動交換器：

1. 點選 System --> Reboot。此時將顯示 Reboot 頁面。
2. 點選 <Reboot> 按鈕。

圖 14. 重新啓動

重新啓動交換器將停止網路流量並中斷網際網路連線。

4.1.5 韌體升級（Firmware Upgrade）

華碩將經常推出更新的韌體，以供您的 GigaX 第二層網路管理交換器升級。所有的系統軟體都包含在一個單一的檔案內，稱為韌體映像(image)。設定管理器 (Configuration Manager) 提供了一種簡單的方法來載入新的韌體映像。

圖 15. 韌體升級

請依照以下步驟來升級韌體：

1. 點選 System --> Firmware Upgrade 來開啓韌體升級頁面。

   韌體升級頁面包含下列資訊：

   - Hardware Version: 顯示硬體版本號。
   - Boot ROM Version: 顯示啓動代碼的版本。
   - Firmware Version: 顯示當前執行的韌體版本。這個號碼會隨著韌體升級而更新。

2. 在 Firmware or Auto-config file 框中，輸入韌體映像檔案的位置與名稱。您也可以點選 <Browse> 按鈕在您的電腦上搜尋韌體映像。
3. 點選 <Upload> 升級韌體，升級完成後自動重新啓動交換器。

*若沒有自動重新啓動交換器，請參考 4.1.4 **重新啓動**（Reboot）中的描述步驟來重新啓動交換器。*

自動設定檔的檔名必須為“config.bat”，且檔案的第一行必須為“#autoconfig”。

4.2 實體介面（Physical Interface）

實體介面（Physical Interface）顯示了乙太網路連接埠的即時狀態。

圖 16. 實體介面

您可以設定連接埠的以下欄位：

- **Port**：選擇需要設定的連接埠
- **Admin**：禁用 / 啓用連接埠
- **Mode**：設定速率和雙工模式
- **Flow Control**：開啓 / 關閉 802.3x 流量控制機制
- **Port Status Window**：顯示每個連接埠的下列資訊：

Link Status	既有連線的速率和雙工模式，否則此連線為關閉的
State	顯示 STP（生成樹協定）狀態
Admin	顯示該連接埠是開啓還是關閉
Mode	顯示由使用者設定的連線速率和雙工模式
Flow Control	顯示 802.3x 流量控制機制是開啓或是關閉

要更改這個頁面，請選擇相應的連接埠號碼，並重新對連接埠進行設定，然後點選 **<Modify>** 按鈕。您更改的欄位將更新至顯示視窗中。然而，您必須執行 **Save Configuration** 操作後，才能使這些設定生效。參見 **4.9 儲存設定值（Save Configuration）** 部分的說明。

4.3 橋接（Bridge）

橋接（Bridge）頁面群組中包含了交換器的第二層設定，如連結匯聚（Link Aggreration），STP 等項目。

4.3.1 生成樹 (Spanning Tree)

生成樹協定（STP）設定頁面可在運作中開啓或關閉生成樹協定功能。本頁面包含三個部分：

a) 根資訊（Root Information）

b) STP 設定（STP Setting）

c) 連接埠設定（Port Setting）

圖 17. 生成樹

根資訊（Root Information）

第一部分顯示了根資訊。我們可以從中瞭解到根交換器的 STP 設定。

STP 設定（STP Setting）

第二部分是 STP 設定。您可以設定以下項目：

- **Disable/STP Enable/RSTP Enabled**: 開啓 / 關閉 STP/RSTP 功能。當您開啓了 STP/RSTP 功能，若本交換器為根交換器，則 STP/RSTP 將使用以下設定。
- **Hello Time**: BPDU 生成設定的間隔。
- **Max Age**: 接收到的協定資訊存在的最大時間，超過這個時間後，將會被丟棄。
- **Forward Delay**: 轉發延遲。
- **Bridge Priority**: 交換器在區域網路中的優先順序

連接埠設定（Port Setting）

第三部分是連接埠設定。它包含了一個顯示視窗，顯示每個連接埠的當前設定。點選 <**Modify**> 更改 STP/RSTP 的連接埠設定。您可以設定以下欄位：

- **Port**: 選擇需要設定的連接埠
- **Priority**: 交換器連接埠的優先順序。越小的數字代表越高的優先順序。當偵測到網路迴路的狀況下，擁有較低優先順序的連接埠較可能被 STP 封鎖。有效的設定值為 0 至 240。

- **Path Cost**: 有效的設定值為 1 至 200000000，或設定為 Auto。使用者設定的路徑耗費（Path Cost）將被顯示在 AdminCost 中，而運作路徑耗費（Path Cost）將被顯示在 OperCost 中。當偵測到網路迴路的狀況下，具有較高耗費（Cost）的連接埠較可能被 STP 封鎖。
- **Edge Port**: 預設情況下，所有的連接埠都被設定為邊緣連接埠（Edge port）。邊緣連接埠接收到 BPDU 後變為 STP 連接埠。邊緣連接埠只需要很短的時間就可進入轉發狀態。
- **Point to Point: Auto/Yes/No**: 全雙工模式的連接埠被判定為點對點連線；其他模式的連接埠被判定為共享連線。點對點連線具有較少的匯聚時間。在大多數情況下，建議設定為 **Auto**。

點選 <**OK**> 儲存您所做的更改。點選 <**Reload**> 更新設定。

4.3.2 連結匯聚（Link Aggregation）

本頁面用來設定連結匯聚群組。本交換器最多可提供15個連結匯聚群組。您可以設定以下參數：

圖 18. 連結匯聚

- **Show Trunk**: 選擇 **Add a new Trunk** 來新增一個群組。或選擇一個既有群組以顯示以下設定欄位與連接埠圖示。
- **Name**: 群組名稱。
- **Trunk ID**: 除了群組名稱外，用來區分不同匯聚群組的號碼。
- **LACP**: 開啓 / 關閉選定幹線群組的 LCAP 功能。LACP 模式固定為 Active。
- **Remove Trunk**: 移除選定的幹線群組。
- **Port Icons**: 這些連接埠的圖示按照交換器前面板上的位置列出。點選圖示可以選擇群組成員。再次點選選中的圖示可將這個連接埠從群組中移除。

點選 <**OK**> 可藉由 HTTP 伺服器將設定傳送至交換器。點選 <**Reload**> 可更新設定。要永久儲存新設定，請至 **Save Configuration** 頁面，然後點選 <**Save**>。

連結匯聚群組中所有的連接埠必須全部在全雙工模式下運作且具有相同的速度。

連結匯聚群組中所有的連接埠必須設定為自動協商（auto-negotiation）模式或全雙工模式。這樣設定才可能使用全雙工模式連線。若您將連接埠設定為強制全雙工模式，則其他連接埠也必須具有相同的設定，否則連結匯聚可能發生運作異常的狀況出現。

連結匯聚群組中所有的連接埠必須具有相同的 VLAN 設定。

連結匯聚群組中所有的連接埠都被視為一個邏輯連線，也就是說，如果任何一個群組成員屬性改變，其他成員的屬性也隨之改變。例如，某連結匯聚群組包括連接埠 1 和連接埠 2。若連接埠 1 的 VLAN 改變，則連接埠 2 的 VLAN 也隨之改變。

您必須檢查連線速率和雙工模式，以確保幹線群組實體處於活動狀態。請至 **實體介面（Physical Interface）**的 runtime status 視窗檢查幹線連接埠的連線模式。若所有的幹線成員都具有相同的速率與全雙工模式，則這個幹線群組已成功建立。若有一個成員不具備相同的速率或全雙工模式，則幹線群組沒有正確建立。請將幹線群組中的所有成員都設定為相同的速率與全雙工模式。

4.3.3 鏡像（Mirroring）

鏡像，配合網路流量分析，可以幫助您監控網路流量。您可以監控所選定之連接埠的傳出與傳入封包。

- Mirror Mode：啓用或禁用選定群組的鏡像功能。
- Monitor Port：接收選定的鏡像連接埠的所有流量的備份資料。

圖 19. 鏡像頁面

監控連接埠不能屬於任何連結匯聚群組。監控連接埠不能像一般交換器連接埠一樣運作。它不能進行封包交換或位址學習。本交換器最多可對 8 個傳出連接埠進行鏡像，被鏡像的連接埠都是未標記(untag)的。

點選 <OK> 可藉由 HTTP 伺服器將設定傳送至交換器。點選 <Reload> 可更新設定。

4.3.4 靜態多重播送（Static Multicast）

在這個頁面中，您可以將多重播送位址添加至多重播送列表。本交換器可以容納 127 個多重播送位址。群組中所有連接埠將把特定的多重播送封包轉發至這個群組的其他連接埠。

圖 20. 靜態多重播送

- Show Group: 選擇 Add a new Group 來建立一個新項目，或選擇一個既有的群組位址以顯示。
- MAC Address: 選擇多重播送位址。
- VLAN: 選擇 VLAN 群組。

點選 <OK> 儲存所做的變更。點選 <Reload> 更新設定。

4.3.5 IGMP 偵聽（IGMP Snooping）

藉由開啓或關閉 IGMP 偵聽功能，可以幫助減少網路中的多重播送流量。當本功能開啓時，交換器將會偵聽 IGMP 封包，並將新群組添加到多重播送列表。但是，一旦靜態位址項目占用了全部 256 個位址空間，IGMP 偵聽功能將無法正常運作。本交換器只允許 256 個第二層多重播送群組。

圖 21. IGMP 偵聽

4.3.6 頻寬控制（Bandwidth Control）

頻寬控制（bandwidth control）可限制所選定的訊框的傳輸速率。本交換器以每個連接埠為基礎支援此功能，您需要設定以下欄位：

圖 22. 頻寬控制

傳入頻寬控制 (Ingress bandwidth control)

- Port: 選擇需要設定的連接埠。
- Control: 關閉 / 開啓傳入頻寬控制功能。
- Mode:
  - Bcast: 限制廣播封包。
  - Bcast, Mcast: 限制廣播封包與多重播送封包。
  - Bcast, Mcast, Dlf: 限制廣播封包、多重播送封包與目的地位址搜尋失敗的單一播送封包。
  - All: 限制所有類型的封包。
- Limit Rate: 所有選定類型封包的總數限制值。例如，若開啓了廣播 / 多重播送封包限制功能，則每種類型封包的流量不能超過所設定的限制值。有效的設定值範圍為 70 至 250000(Kbps)。

傳出頻寬控制 (Egress bandwidth control)

- Port: 選擇需要設定的連接埠。
- Control: 關閉 / 開啓傳出頻寬控制功能。
- Limit Rate: 最大傳出速率。有效的設定值範圍為 70 至 250000(Kbps)。

點選 <OK> 可藉由 HTTP 伺服器將設定傳送至交換器。點選 <Reload> 可更新設定。要永久儲存新設定，請至 Save Configuration 頁面，然後點選 <Save>。

4.3.7 動態位址（Dynamic Addresses）

圖 23. 動態位址

本頁面用來顯示藉由連接埠、VLAN ID 或 MAC 位址來查找動態 MAC 位址的結果。在查找中指定的 MAC 位址稱為動態位址，它的存在時間由您設定的 **Aging Time** 所決定。您可以輸入一個 15 至 3825 (單位為秒)之間的值來設置其存在時間（或稱老化時間）。點選 <**OK**> 可儲存您在本頁面所做的所有變更。要永久儲存新設定，請至 **Save Configuration** 頁面，然後點選 <**Save**>。

要查找 MAC 位址，您可以勾選 port、VLAN ID 或 MAC address，並輸入相應的值，然後點選 <**Query**>。位址視窗將顯示查找結果。

4.3.8 靜態位址（Static Addresses）

圖 24. 靜態位址

本頁面的 MAC 位址項目不會過期老化。它將一直存在於位址表中，直到您將其從位址表中移除。

靜態位址（Static Addresses）頁面可設定以下參數：

- **MAC Address**: 輸入 MAC 位址。
- **VLAN ID**: 輸入 MAC 位址所屬的 VLAN ID。
- **Port Selection**: 選擇 MAC 位址所屬的連接埠。
- **Discard on**: 當 MAC 位址作為目的地位址出現在封包時，您可以執行封包過濾。

建立一個新的靜態 MAC 位址

點選 <**Add**>。新的項目將出現在位址視窗中。第一個位址視窗最多可以顯示 15 個項目，其他項目將在接下來的頁面顯示。點選 **First**, **Previous**, **Next** 或 **Last** 可瀏覽列表的各個頁面。

更改一個 MAC 位址

選擇您需要更改的 MAC 位址，然後點選 <**Modify**>。

移除一個 MAC 位址

選擇您需要移除的 MAC 位址，然後點選 <Remove>。

查找一個 MAC 位址

輸入 MAC 位址與 VLAN ID，然後點選 <Query>。查找結果將被顯示在位址視窗中。

點選 <OK> 可儲存您在本頁面所做的所有變更。 點選 <Reload> 可更新設定。要永久儲存新設定，請至 Save Configuration 頁面，然後點選 <Save>。

4.3.9 VLAN

4.3.9.1 VLAN 模式（VLAN Mode）

本交換器有兩種 VLAN 模式：(1) 以連接埠為基礎的 VLAN（Port-Based VLAN），(2) 802.1Q 標記 VLAN (802.1Q Tagged VLAN)。本交換器以每個連接埠為基礎支援這個功能，您需要設定以下欄位：

圖 25. VLAN 模式

a) **Port**: 選擇需要設定的連接埠。

b) **VLAN Mode（VLAN 模式）**

- **802.1Q Tagged VLAN**: 依照 802.1Q Tagged VLAN 的規則來做出轉發決定。
- **Port-Based VLAN**: 若連接埠是以連接埠為基礎的 VLAN 模式，則 1) 當該連接埠接收到標記（Tagged）封包時，將依照 802.1Q Tagged VLAN 的規則來做出轉發決定； 2) 當該連接埠接收到未標記（Untagged）封包時，將依照 Port-Based VLAN 的規則來做出轉發決定。

限制

- 若一個連接埠為以連接埠為基礎的 VLAN 模式，它將不能成為一個混雜連接埠（promiscuous port），也不能執行 802.1x 與 IGMP 偵聽。
- 幹線（Trunk）成員必須具備相同的 VLAN 模式。

點選 <OK> 可儲存您在本頁面所做的所有變更。點選 <Reload> 可更新設定。要永久儲存新設定，請至 Save Configuration 頁面，然後點選 <Save>。

4.3.9.2 標記 VLAN (Tagged VLAN)

圖 26. 標記 VLAN

您可以設定最多 227 個 VLAN 群組，並在這個頁面顯示。交換器有一個預設的 VLAN。這一功能可避免交換器的不正常運作。除了預設的 VLAN1 以外，您可以移除其他任何一組既有的 VLAN。

您可以按下連接埠按鈕來指定該連接埠為已標記(tagged)或未標記(untagged)連接埠。在連接埠選擇面板上有三種類型的按鈕：

- **“U” type**: 未標記的連接埠，從該連接埠傳送出去的封包會被移除 VLAN 標記（tag）。
- **“T” type**: 自本連接埠傳送的封包都會被標記。
- **“blank” type**: 本連接埠並非 VLAN 群組的成員。

其他可設定的欄位有：

- **Show VLAN**: 顯示選定的既有 VLAN。
- **Name**: VLAN 名稱。
- **VLAN ID**: 當建立一個新的 VLAN 時，使用者需要在這裡輸入 VLAN ID。
- **Remove VLAN**: 移除一個既有的 VLAN。這個欄位在建立新 VLAN 時不會出現。
- **Private VLAN**: 將這個 VLAN 設為私有 VLAN(PVLAN)。PVLAN 透過簡易的 VLAN 設定，實現 VLAN 安全。系統管理員可以減少 VLAN 和 IP 資源消耗，卻可獲得相同的 VLAN 安全。我們不能使用預設的 VLAN (VLAN 1) 作為私有 VLAN(PVLAN)。在我們的系統中，最多可有 4 個 PVLAN。鏡像功能中的監控連接埠不能成為 PVLAN 成員。靜態多重播送群組不能應用於 PVLAN。一個 PVLAN 共有兩種連接埠類型： 1) 混雜連接埠(Promiscuous Port) 2) 隔離連接埠（Isolated Port）。
  a) **Promiscuous Port**: 一個 PVLAN 必須且僅可擁有一個混雜連接埠。它與 PVLAN 內的所有介面通訊。對於混雜連接埠，有如下限制：
     - 混雜連接埠必須為未標記連接埠
     - 幹線（Trunked）連接埠不能作為混雜連接埠（promiscuous）。
     - 混雜連接埠不能運作於以連接埠為基礎的VLAN（Port-Based VLAN）模式。

b) **Isolated Port**: PVLAN 中的非混雜（non-promiscuous）連接埠。它與同一 VLAN 內的其他連接埠在第二層是完全隔離的，僅能與該 PVLAN 內的混雜連接埠通訊。PVLAN 將封鎖除了混雜連接埠流量之外的所有傳送至隔離連接埠的流量。從隔離連接埠傳出的流量僅可轉發至混雜連接埠。流量控制對隔離連接埠無效。對於隔離連接埠，有如下限制：

- 隔離連接埠僅處理未標記的封包。若隔離連接埠接收到標記封包，會將其丟棄。
- 隔離連接埠僅能屬於一個 VLAN，且此 VLAN 必須為私有 VLAN (PVLAN) 。
- 隔離連接埠不能進行 IGMP 偵聽。

- **Priority Override**: 當選擇了 priority override(優先權重寫)，基於 VLAN ID 的優先權重寫（priority override）功能僅適用於本 VLAN 成員。當應用此功能時，帶有此 VLAN ID 的任何封包的優先權（priority）欄位將被重寫為所設定的新的優先權數值。VLAN priority override 的優先權比連接埠預設的優先權及 IP 優先權更高。

- **Priority**: 若優先權重寫（priority override）功能開啓，這個值用來重寫與此 VLAN ID 相關的任何訊框的優先權。

若您想讓 VLAN 成員依照 802.1Q Tagged VLAN 的規則來做出轉發決定，您必須進入 **VLAN Mode** 頁面並選擇 **802.1Q Tagged VLAN** 模式作為這些連接埠成員的 VLAN Mode。

點選 <**OK**> 可藉由 HTTP 伺服器將設定傳送至交換器。點選 <**Reload**> 可更新設定。要永久儲存新設定，請至 **Save Configuration** 頁面，然後點選 <**Save**>。

4.3.9.3 以連接埠為基礎的 VLAN（Port-Based VLAN）

以連接埠為基礎的 VLAN（Port-Based VLAN）是依照目的地 MAC 位址及與其相關聯的連接埠來做出封包轉發決定的 VLAN。這是最簡單和最常見的 VLAN 形式。在一個以連接埠為基礎的 VLAN 中，系統管理員可指定交換器的連接埠至特定的 VLAN 群組。在這個頁面中，您可以設定最多 28 個以連接埠為基礎的 VLAN 群組，並將它們顯示出來。

圖 27. 以連接埠為基礎的 VLAN

- **Show Port-Based VLAN**: 選擇 **Add a new VLAN** 來建立一個新的群組，或選擇一個既有的群組以顯示下列欄位和連接埠圖示：

- Name: 群組名稱。
- Group ID: 當您建立一個新的以連接埠為基礎的 VLAN 時，這個欄位需要您輸入群組 ID（Group ID）。有效的群組 ID 值從 1 至 28。
- Remove Group: 移除一個既有的以連接埠為基礎的 VLAN 群組。本欄位在建立新的以連接埠為基礎的 VLAN 頁面不會出現。

若您想讓新建的以連接埠為基礎的 VLAN 生效，您必須到 **VLAN Mode** 頁面選擇 **Port-Based VLAN** 模式作為這些連接埠成員的 VLAN Mode 。

點選 <OK> 可藉由 HTTP 伺服器將設定傳送至交換器。點選 <Reload> 可更新設定。要永久儲存新設定，請至 **Save Configuration** 頁面，然後點選 <Save>。

4.3.10 預設連接埠 VLAN 與 CoS(Default Port VLAN and CoS)

本頁面包含了每個連接埠與 VLAN 標記相關的欄位設定。這些設定項目如下：

圖 28. 預設連接埠 VLAN 與 CoS

- Port: 選擇需要設定的連接埠
- PVID: 以連接埠為基礎的VLAN ID。從這個連接埠接收到的每一個未標記的封包都會標記為這個 VLAN 群組 ID。
- CoS (Class of Service) value: 從這個連接埠接收到的每一個未標記的封包都會被指定此 CoS 值到標記的 VLAN 中。

點選 <Modify> 將更改連接埠列表視窗中顯示的內容。點選 <OK> 可藉由 HTTP 伺服器將設定傳送至交換器。點選 <Reload> 可更新設定。要永久儲存新設定，請至 **Save Configuration** 頁面，然後點選 <Save>。

4.4 簡易網路管理通訊協定（SNMP）

簡易網路管理通訊協定（SNMP）可用來管理網路。您可以使用 SNMP 設定頁面來開啓或關閉 SNMP 功能。

SNMPv3 可提供更多的安全管理和存取控制。SNMP 具有下列可設定的參數：

4.4.1 團體列表（Community Table）

您可以輸入不同的團體名稱並可勾選後面的框來為團體指定寫入權限。點選 <OK> 儲存設定或點選 <Reload> 更新頁面。

圖 29. 團體列表

4.4.2 主機列表（Host Table）

本頁面將主機IP位址與團體列表（Community Table）頁面中填入的團體名稱連結在一起。輸入一個 IP 位址並從下拉選單中選擇團體名稱。點選 <OK> 儲存設定或點選 <Reload> 更新頁面。

圖 30. 主機列表

4.4.3 Trap 設定（Trap Setting）

藉由設定 trap 目的地 IP 位址與群組名稱，您可以開啓 SNMP trap 功能，傳送不同版本（ v1 或 v2c）的 trap 封包。點選 <OK> 儲存設定或點選 <Reload> 更新頁面。

圖 31. Trap 設定

4.4.4 VACM 群組（VACM Group）

圖 32. VACM 群組

VACM（View-based Access Control Model，基於檢視的存取控制模型）群組可用來設定 SNMPv3 VACM 群組資訊。

VACM Group 頁面有下列可設定的參數：

- **Group Name**: 輸入安全群組名稱。
- **Read View Name**: 輸入群組所屬的讀取檢視名稱（Read View Name）。相關的 SNMP 訊息為 Get, GetNext, GetBulk。
- **Write View Name**: 輸入群組所屬的寫入檢視名稱（Write View Name）。相關的 SNMP 訊息為 Set。
- **Notify View Name**: 輸入群組所屬的通知檢視名稱（Notify View Name）。相關的 SNMP 訊息為 Trap, Report。
- **Security Model**: 輸入群組所屬的安全模型（Security Model）。Any 適用於 v1,v2,v3。USM 則與 SNMPv3 相關。
- **Security level**: 輸入群組所屬的安全等級（Security level）。可選的項目有 NoAuth、AuthNopriv 與 AuthPriv。

點選 <**Add**> 以建立一個新的 VACM 群組。要移除一個既有的 VACM 群組，請選擇需要移除的群組並按下 <**Remove**>。要更新一個項目，請選擇需要更新的項目並按下<**Modify**>。點選<**OK**>可儲存對頁面所做的更改。點選<**Reload**>可更新設定。要永久儲存新設定，請至 **Save Configuration** 頁面，然後點選 <**Save**>。

4.4.5 VACM 檢視（VACM View）

圖 33. VACM 檢視

VACM 檢視用來查看 SNMPV3 VACM 群組訊息。

VACM 檢視（VACM View）頁面包含下列參數：

- **View Name**: 輸入安全群組名稱。
- **View Type**: 輸入檢視所屬的檢視類型（View Type）。當檢視子樹（View Subtree）與 SNMPv3 訊息中的 OID 相符合時，選擇包含（Included）或排除（Excluded）。

- **View Subtree**: 輸入檢視（View）所屬的檢視子樹（View Subtree）名稱。子樹(Subtree)是一個 Oid，它與 SNMPv3 訊息中的 Oid 相符合。當子樹短於 SNMPv3 訊息中的 Oid 時，為良好的符合狀態。
- **View Mask**: 輸入檢視（View）所屬的檢視遮罩（View Mask）。遮罩的每個位元代表了檢視子樹（View Subtree）中左側看過來點與點之間的數字，而位元‘0’表示無所謂。

點選 <Add> 可建立一個新的VACM 檢視（View）項目。要移除一個既有項目，選擇需要移除的檢視並按下 <Remove>。要更新一個既有的項目，選擇需要更新的檢視並按下 <Modify>。點選 <OK> 可儲存對頁面所做的更改。點選 <Reload> 可更新設定。 要永久儲存新設定，請至 Save Configuration 頁面，然後點選 <Save>。

4.4.6 USM 使用者（USM User）

USM 使用者（USM User）功能用來設定 SNMPv3 USM 使用者資訊。

USM 使用者（USM User）頁面包含下列參數：

圖 34. USM 使用者

- **Engine Id**: 輸入符合管理員中 ID 的 Engine ID。
- **Name**: 在管理員中輸入符合 Engine ID 名稱與 Engine ID 的一個合併名稱。
- **Auth Protocol**: 輸入 Engine ID 與名稱所屬的 Auth Protocol。在這當中只能選擇 NoAuth, MD5, SHA1 。若您選擇了 NoAuth，則無須輸入密碼。
- **Auth Password**: 輸入 Auth Protocol 所屬的密碼。在這裡密碼必須是至少八位的數字或字母。
- **Priv Protocol**: 輸入 Engine ID 與名稱所屬的 Priv Protocol。 在這當中只能選擇 NoPriv ,DES。若您選擇了 NoPriv ，則無須輸入密碼。
- **Priv Password**: 輸入 Priv Protocol 所屬的密碼。在這裡密碼必須是至少八位的數字或字母。

點選 <Add> 以建立一個新的 USM 使用者項目。要移除一個既有項目，選擇需要移除的檢視並按下 <Remove>。要更新一個既有的項目，選擇需要更新的檢視並按下 <Modify>。點選 <OK> 可儲存對頁面所做的更改。點選 <Reload> 可更新設定。 要永久儲存新設定，請至 Save Configuration 頁面，然後點選 <Save>。

4.5 安全（Security）

本交換器支援 802.1x 以連接埠為基礎的安全功能。只有經認證的主機才可以存取本交換器的連接埠。來自未經認證之主機的流量將被封鎖。認證服務可由 RADIUS 伺服器或交換器的本地資料庫提供。

本交換器亦支援透過 802.1x 認證的動態 VLAN 分配。關於使用者 / 連接埠的資訊必須在開啓本功能之前，在認證伺服器上進行設定。

4.5.1 連接埠存取控制（Port Access Control）

連接埠存取控制（Port Access Control）可用來設定 802.1x 參數。802.1x 使用 RADIUS/TACACS+ 伺服器或本地資料庫來認證連接埠的使用者。

連接埠存取控制有兩個設定：橋接設定（Bridge Setting）與連接埠設定（Port Setting）。

圖 35. 連接埠存取控制

橋接設定（Bridge Setting）

橋接設定頁面包含下列設定參數：

- **Reauthentication**: 開啓本項目後，交換器會在重新認證時間（ReAuthentication Time）到時，試圖重新認證連接埠的使用者。
- **Reauthentication Time**: 若 “Reauthentication” 項目已開啓，ReAuthentication Time（重新認證時間）指的是交換器重新發送認證請求到連接埠使用者的時間間隔。
- **Authentication Method**: 可以使用 RADIUS 或 本地資料庫認證連接埠的使用者。
- **Quiet Period**: 若從 RADIUS 或本地資料庫認證失敗，交換器再次發送認證請求到連接埠使用者前需要等待的時間。
- **Retransmission Time**: 若連接埠使用者未能回應交換器發出的認證請求，交換器再次發送認證請求到該連接埠使用者前需要等待的時間。
- **Max Reauthentication Attempts**: 若連接埠使用者未能回應交換器發出的認證請求，交換器重新發送認證請求的次數。

連接埠設定（Port setting）

連接埠設定頁面包含下列設定參數：

- **Port**：指定需要設定的連接埠。
- **AuthMode(Authentication Mode)**：若選擇了 **Port_based**，則每個連接埠只要有一台主機（host）通過遠端 RADIUS 伺服器、遠端 TACACS+ 伺服器或本地使用者資料庫的認證。**Port_based** 支援多主機（Multi-host）及 GuestVID。若選擇了 **MAC_based**，每個主機在存取網路之前都必須通過認證。 **MAC_based** 不支援多主機（Multi-host）及 GuestVID。系統最多可支援 256 個嘗試用 MAC_based 方式通過認證的主機。若選擇了 MAC_based，建議您開啓橋接設定中的 Reauthentication 項目。
- **AuthCtrl (Authentication Control)**：若選擇了 **Force_authorized**，選定的連接埠被認為已強制通過認證。因此，來自所有主機的流量都被允許通過。否則，若選擇了 **Force_unauthorized**，選定的連接埠是封鎖的，不允許任何流量通過。若選擇了 **Auto**，選定連接埠的動作由 802.1x 協定來控制。
- **Multi-host**:開啓本項目後，只要連接到選定連接埠的所有主機中，有一台通過了認證，則所有連接到該連上接埠的主機都可以使用這個連接埠。若關閉本項目，則僅有通過認證的那部主機可以使用這個連接埠。若您在 **Auth Mode** 中選擇了 **MAC_based**，則不支援 Multi-host。
- **GuestVID**：訪客 VLAN（Guest VLAN）可允許非 802.1x 用戶端訪客使用者擁有受限的網路存取權限。

點選 <**OK**> 可儲存更改。點選 <**Reload**> 可更新設定。要永久儲存新設定，請至 **Save Configuration** 頁面，然後點選 <**Save**>。

4.5.2 撥入使用者（Dial-In User）

撥入使用者（Dial-in User）選項用來定義交換器本地資料庫中的使用者。本項目包含下列設定參數：

- **User Name**：新的使用者名稱。
- **Password**：新使用者的密碼。
- **Confirm Password**：再次輸入密碼以確認。
- **Dynamic VLAN**：指定一個分配給 802.1x 認證之用戶端的 VLAN ID。

圖 36. 撥入使用者

點選 <Add> 建立新的使用者。若您想要做更改，請點選 <Modify>。若您想要移除一個選定的使用者，請點選 <Remove>。點選 <OK> 儲存設定，點選 <Reload> 更新設定。

4.5.3 RADIUS

若要使用外部 RADIUS 伺服器，您需要設定以下參數：

圖 37. RADIUS

- **Authentication Server IP**: RADIUS 伺服器的 IP 位址。
- **Authentication Server Port**: RADIUS 伺服器所偵聽的連接埠號碼。
- **Authentication Server Key**: 這個金鑰用來在 GigaX 交換器與 RADIUS 伺服器之間進行通訊。
- **Confirm Authentication Key**: 再次輸入金鑰以確認。

點選 <OK> 儲存設定，點選 <Reload> 更新設定。要永久儲存設定，請至 **Save Configuration** 頁面，然後點選 <Save>。

連接到交換器的 RADIUS 伺服器必須與系統管理介面位於同一個 VLAN 內。

4.5.4 連接埠安全（Port Security）

連接埠安全（Port security）頁面包含了連接埠設定（port configuration），連接埠狀態（port status）以及安全 MAC 位址（secure MAC addresses）功能。

4.5.4.1 連接埠設定（Port Configuration）

本頁面用來設定連接埠安全（Port Security）功能的多個參數。本交換器最多可支援 1024 個安全 MAC 位址。使用者可以設定連接埠的以下欄位：

圖 38. 連接埠設定

- **Port**: 選擇需要設定的連接埠。
- **Admin**: 關閉 / 開啓某連接埠的安全功能。

- **Violation Mode**: 本項用來設定當違反安全設定時連接埠的動作。下列狀況均為違反安全設定：

  1) 位址表中已經添加了最大數量的安全 MAC 位址，而此時有一個 MAC 位址並不存在於位址表中的設備想要存取介面。

  2) 在一個安全介面內學習所得或設定的位址在同一 VLAN 內的另一個安全介面出現。您可以設定介面在違反安全設定時的三種模式：

     a) **Protect**: 在這個模式下，當有違反安全設定的事件發生時，您將不會被通知。

     b) **Restrict**: 在這個模式下，當有違反安全設定的事件發生時，您將會被通知。此時，系統將會記錄訊息，Violation 計數器的數值會增加。

     c) **Shutdown**: 在這個模式下，連接埠將立即變成封鎖狀態，系統將發送一個 SNMP trap 並記錄訊息，Violation 計數器的數值會增加。

- **Max MAC Addresses**: 設定安全 MAC 位址的最大數量。有效值範圍從 1 至 132。所有連接埠這個值的總和必須小於或等於交換器允許的安全 MAC 位址的最大數量。

- **Aging Time**: 設定老化時間（aging time）。有效值範圍從 0 至 1440(分鐘)。老化機制僅對動態 MAC 位址有效。若時間設定為 0，則沒有開啓此連接埠的老化機制。

- **Aging Type**: 老化類型決定了當安全 MAC 位址老化後的動作。每個連接埠支援兩種類型的老化類型：

  a) **Absolute**: 連接埠的安全位址在老化時間到後會被移除。

  b) **Inactivity**: 若在指定的時間內沒有來自該安全 MAC 位址的流量，則該位址才會被移除。

選擇相應的連接埠號碼並進行設定，然後點選 <**Modify**>。顯示視窗的內容將會自動更新為您的新設定。點選 <**Reload**> 可更新設定。要永久儲存新設定，請至 **Save Configuration** 頁面，然後點選 <**Save**>。

4.5.4.2 連接埠狀態 (Port Status)

本頁面顯示了所有連接埠的連接埠安全資訊，包括以下項目：

圖 39. 連接埠狀態

- Port: 連接埠號碼。
- Status:
  a) NoOper: 表示連接埠的安全功能沒有開啓。
  b) SecureUp: 表示連接埠安全功能運作中。
  c) SecureDown: 表示連接埠的安全功能無法運作。這種狀況一般為開啓了連接埠安全功能，但由於某些原因（如與其他功能衝突）而無法正常運作。
  d) Restrict: 表示在 Violation mode 設定為"restrict" 時，連接埠出現了違反安全設定的狀況。
  e) Shutdown: 表示在 Violation mode 設定為"Shutdown" 時，連接埠出現了違反安全設定的狀況。
- Restart: 是否重新開啓處於 shutdown 狀態下的連接埠(Yes/No)。
- TotalMacAddrCount: 當前靜態與動態安全 MAC 位址的總和。
- StaticMacAddrCount: 當前靜態安全 MAC 位址的總數。
- ViolationCount: 違反安全設定事件的總數。

當下列情況發生時，連接埠的安全狀態為 SecureDown：

- 連接埠未連線。
- 管理員橋接連接埠被關閉
- 該連接埠為幹線連接埠。
- 該連接埠為連接埠鏡像功能中的監控連接埠。
- 該連接埠正在執行 802.1x，且運作於單主機模式下。

若連接埠的狀態為 Shutdown，使用者可以選擇相應的連接埠號碼並將 Restart 設定為 Yes，然後點選 <Modify>。顯示視窗的內容將會自動更新為您的新設定。點選 <Reload> 可更新設定。要永久儲存新設定，請至 Save Configuration 頁面，然後點選 <Save>。

4.5.4.3 安全 MAC 位址 (Secure MAC Addresses)

使用者可以新增 MAC 位址至連接埠的安全 MAC 位址表。通過這種方式新增的 MAC 位址不會從安全 MAC 位址表中老化。我們稱其為靜態安全 MAC 位址。

圖 40. 安全 MAC 位址

- **MAC Address**: 輸入 MAC 位址。
- **Port Selection**: 選擇 MAC 位址歸屬的連接埠。

在您新增了一個靜態 MAC 位址後，請點選 <**Add**>。這個新項目將會顯示在位址視窗中。

使用者可以從 Port Selection 中選擇一個連接埠，然後點選 <**Query**>。這個連接埠當前的所有安全 MAC 位址將顯示在位址視窗中。

使用者可以從列表中選擇一個連接埠，並按下 <**Remove**>，即可移除這個既有的位址。若您想要選中多個項目，請按住鍵盤上的 **Shift** 鍵，並用滑鼠選擇多個項目。

點選 <**Add**> 或 <**Remove**> 可使設定立即生效。要永久儲存這些靜態安全 MAC 位址，請至 **Save Configuration** 頁面，然後點選 <**Save**>。

4.6 QoS

QoS 頁面包含信任狀態（trust state），映射（mapping），優先權重寫（priority override），以及 CoS 功能（CoS function）。

4.6.1 信任狀態（Trust State）

傳入策略 (Ingress Policy) 的任務是，為佇列控制器 (Queue Controller) 決定每個訊框的優先權。本交換器以每個連接埠為基礎支援這一功能，您只需設定以下欄位：

圖 41. 信任狀態

- **Port**: 選擇需要設定的連接埠。
- **Trust State**: Trust DSCP 或 CoS。

a) **Trust CoS**: 使用 IEEE 標記 (Tags)。若訊框為 IEEE 802.3ac 標記訊框，則使用 IEEE 802.1p Traffic Class 欄位的數值作為訊框的優先權。否則，使用預設的優先權數值。

b) **Trust DSCP**: 使用 IP 作為優先權。若訊框的 IP 為 IPv4 模式，則使用 IPv4 TOS 與 / 或 Diffserv 欄位的數值作為訊框的優先權；若訊框的 IP 為 IPv6 模式，則使用 IPv6 Traffic Class 欄位的數值作為訊框的優先權。否則，使用預設的優先權數值。關於 Trust DSCP，相關的設定位於 **Mapping** 與 **CoS** 頁面。

點選 <**OK**> 可藉由 HTTP 伺服器將設定傳送至交換器。點選 <**Reload**> 可更新設定。要永久儲存新設定，請至 **Save Configuration** 頁面，然後點選 <**Save**>。

4.6.2 映射 (Mapping)

本頁面用來將 DSCP（差分服務代碼點）值映射至 CoS（服務等級）優先權。有效的 DSCP 值範圍為 0 至 63。對於 IPv6，DSCP 值乘以 4 得到的是流量等級（Traffic Class）的值。例如，DSCP 值 4 代表 IPv6 流量等級（Traffic Class）的值為 16。您只需設定以下欄位，即可開啓交換器的這個功能：

圖 42. 映射

- **DSCP**: 選擇 DSCP 值。
- **CoS**: 選擇 CoS 優先權。

點選 <**OK**> 可藉由 HTTP 伺服器將設定傳送至交換器。點選 <**Reload**> 可更新設定。要永久儲存新設定，請至 **Save Configuration** 頁面，然後點選 <**Save**>。

4.6.3 優先權重寫（Priority Override）

圖 43. 優先權重寫

優先權重寫（Priority Override）頁面可讓您開啓或關閉 QoS 來源 MAC 位址優先權重寫和目的地 MAC 位址優先權重寫。

若開啓了來源 MAC 位址重寫（priority override）功能，基於來源 MAC 位址的優先權重寫功能對所有連接埠都有效。當一個封包的來源 MAC 位址與已添加至靜態 MAC 位址表中並已指定了優先權的 MAC 位址項目相同時，即會執行來源 MAC 位址優先權重寫。當發生這種狀況時，指定給靜態 ARL 表的優先權數值將替代封包先前的優先權數值。來源 MAC 位址優先權重寫功能的優先權要高於連接埠的預設優先權、IP 優先權，及 VLAN 優先權重寫功能。

若開啓了目的地 MAC 位址優先權重寫功能，基於目的地 MAC 位址的優先權重寫功能對所有連接埠都有效。當一個封包的目的地 MAC 位址與已添加至靜態 MAC 位址表中並已指定了優先權的 MAC 位址項目相同時，即會執行目的地 MAC 位址優先權重寫。當發生這種狀況時，指定給靜態 ARL 表的優先權數值將替代封包先前的優先權數值。目的地 MAC 位址優先權重寫功能的優先權是最高的，它要高於連接埠的預設優先權、IP 優先權、 VLAN 優先權重寫，以及來源 MAC 位址優先權重寫功能。

若您想要新增一個靜態 MAC 項目並具有 CoS 優先權，請至 **Static Addresses** 頁面。

點選 <**OK**> 可藉由 HTTP 伺服器將設定傳送至交換器。點選 <**Reload**> 可更新設定。要永久儲存新設定，請至 **Save Configuration** 頁面，然後點選 <**Save**>。

4.6.4 CoS

本交換器每個連接埠支援 4 個傳出佇列。您可以指定以下的排序方式：

圖 44. CoS

- **Strict priority scheduling**: 每個 CoS 值可映射到四個佇列之一。佇列 4 具有最高的優先權來傳輸封包。較低優先權佇列中的封包只有在高優先權佇列為空時才能被傳送。在 Strict priority scheduling 方式下，權重 (weight) 設定為零。

- **Weighted round-robin (WRR) scheduling**: WRR（權重循環排序）需要您指定一個數字作為該佇列相對於其他 CoS 佇列的重要程度（權重）。WRR 可防止在傳送高優先權佇列中的流量時，低優先權佇列被完全忽略的狀況。WRR 排序將輪流從每個佇列中傳送一些封包。傳送的封包數量取決於相應佇列的重要程度。例如， 若佇列一的權重（weight）為 1， 佇列二的權重（weight）為 2，則每次從佇列一傳送一個封包，從佇列二傳送兩個封包。藉由這種排序方式，即使高優先權佇列不為空，低優先權佇列也有機會來傳送封包。權重的設定可以為 1, 2, 4, 8。

點選 <**OK**> 可藉由 HTTP 伺服器將設定傳送至交換器。點選 <**Reload**> 可更新設定。要永久儲存新設定，請至 **Save Configuration** 頁面，然後點選 <**Save**>。

4.7 纜線診斷（Cable Diagnosis）

纜線診斷（Cable Diagnosis）的主要功能是檢測纜線錯誤（開路或短路）並報告預測的錯誤位置。此外，纜線診斷功能還可以檢測 PHY 類型（10M, 100M 或 1000M）以及估測一般纜線的長度。纜線長度估測功能僅支援 Gigabit 速度模式。

只需選擇連接埠號碼，並按下 **<Go>**，即可顯示檢測結果。

圖 45. 纜線診斷

當您開啓連接埠的纜線診斷功能，則在診斷過程中，連接埠的網路連線將會中斷。

4.8 統計圖表（Statistics Chart）

統計圖表（Traffic Chart）頁面可以在不同的圖表中顯示網路流量。您可以指定更新統計圖表的時間間隔。在這些頁面中，您可以利用不同圖表來監控網路流量。大多數 MIB-II 計數器都被顯示在這些圖表中。

點選 **<Auto Refresh>** 或 **<Refresh Rate>** 來設定從交換器獲取新資料的時間間隔。您可以選擇不同的顏色（Color）來區分不同的連接埠或統計值。最後，點選 **Draw** 使瀏覽器產生統計圖表。每次點選 **Draw** 都會重置統計結果的顯示。

4.8.1 流量比較（Traffic Comparison）

本頁面可將所有連接埠的某一個統計值顯示在同一張圖表中。指定一個統計項目，並按下 **Draw**，瀏覽器將顯示更新的資料，並每隔一段時間更新一次。

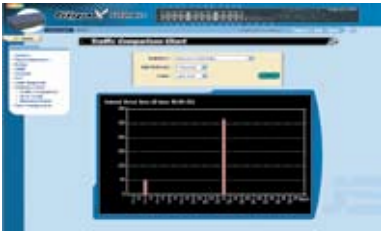


圖 46. 流量比較

4.8.2 錯誤群組（Error Group）

選擇連接埠（Port）和顯示顏色（Color），然後點選 Draw，統計視窗將顯示指定連接埠所有丟棄或錯誤的數量。這個資料每隔一段時間會自動更新。

圖 47. 錯誤群組

4.8.3 歷史狀態（Historical Status）

您可以在這個圖表中顯示不同的連接埠和統計項目。由於這裡顯示的是統計資訊的歷史狀態，因此，即使資料已更新，統計線條圖仍然會保留舊的統計資料。

圖 48. 歷史狀態

4.9 儲存設定值（Save Configuration）

要永久儲存設定，您需要點選 <Save> 按鈕。點選 <Restore> 可將設定回復至出廠預設值。回復出廠預設值後，您做的所有設定都將丟失。

圖 49. 儲存設定值

5. IP 位址、網路遮罩與子網路

5.1 IP 位址

本章節講述關於 IPv4 (version 4 of the Internet Protocol) 的內容，而不涉及 IPv6 位址的情況。

本章節設定您已經瞭解了二進位，比特，位元組等基礎知識。

IP 位址就好像 Internet 版本的電話號碼, 用於區分 Internet 上的單個節點(電腦或網路裝置)。每個 IP 位址包含4組號碼，每個號碼的範圍都是 0 到 255，之間用點區分，如 20.56.0.211。這些數字自左向右地被稱做 field1， field2，field3，和 field4。

書寫 IP 位址的習慣一般用十進位數字，之間用點區分，這稱為十進位表示。IP 位址 20.56.0.211 讀作:“ 二零點五六點零點二一一”。

5.1.1 IP 位址的結構

IP 位址的層次設計與電話號碼很相像。舉例說明，一個 7 位的電話號碼的前 3 位表示的是一個電話群組，其中包含上千路電話，後面的 4 位表示的是該電話的身份號碼。

類似地，IP 位址包含兩種資訊。

網路 ID
在Internet 或 Intranet 確認網路身份。

主機 ID
在網路中確認電腦或裝置身份。

每個 IP 位址的第一部分包含網路 ID，其餘部分則是主機 ID。網路 ID 的長度取決於網路的級別(見下面的章節)。表 7 顯示的是 IP 位址的結構。

表 7: IP 位址結構

	Field1	Field2	Field3	Field4
A 類	網路 ID	主機 ID		
B 類	網路 ID		主機 ID	
C 類	網路 ID			主機 ID

下列是有效的 IP 位址範例：

A類: 10.30.6.125 (網路 = 10, 主機 = 30.6.125)

B類: 129.88.16.49 (網路 = 129.88, 主機 = 16.49)

C類: 192.60.201.11 (網路 = 192.60.201, 主機 = 11)

5.1.2 網路類型

三種常用的網路類型為 A 類、B 類和 C 類。(事實上還有一種 D 類位址，但是它的特殊用途與我們這裡討論的主題無關。)這些分類有它們各自的作用和特性。

A 類網路是 Internet 上規模最大的網路，每個都可以容納 160 萬個主機。這樣的超級網路最多只有 126 個，總共支援 20 億個主機。由於它們的容量龐大，這些網路用於廣域網路或某些處於網路架構的組織，如您的 ISP。

B 類網路比 A 類小，但是其容量仍然很大，每個 B 類網路可以容納超過 65,000 個主機。這樣的網路一共有 16,384 個。B 類網路適合大型組織，如大型公司或政府機構。

C 類網路是最小的，一個 C 類網路最多只能容納 254 個主機，但是網路的總數卻超過了 200 萬(2,097,152 個)。連接到 Internet 的區域網路通常是 C 類網路。

從field1可以輕鬆識別位址類型:
field1 = 1–126: A 類
field1 = 128–191: B 類
field1 = 192–223: C 類
(field1 值中缺少的部分留作特殊用途)

主機 ID 可以是範圍內除 0 和 255 的任何值，這些值已留作專用。

5.2 子網路遮罩

網路遮罩看起來像普通的 IP 位址，但實際上它包含了一系列的位元表示 IP 位址的哪個部分是網路 ID，哪些是主機 ID：位元為1 表示“這是網路 ID”，0 表示“這是主機 ID”。

子網路遮罩是用來定義子網路的(用來將網路分為更小的部分)。一個子網路的網路 ID 是從主機 ID“借位”實現的。 子網路遮罩用於識別這些主機 ID 位元。

舉例說明，設想將一個 C 網位址 192.168.1.分為兩個子網路，您就需要用到下面的子網路遮罩:

255.255.255.128

將其轉換為二進位更容易看出它的真實面目：

11111111.11111111.11111111.10000000

就像 C 類位址一樣，field1 到 field 3都是網路 ID，但是請注意 field 4 中第一個位元同樣也被包括到了網路 ID 中。由於額外的位元只有兩種值(0 和 1)，就表示網路有兩個子網路，每個子網路使用剩餘的 7 位元作為其主機 ID，範圍是 0 到 127(而不是原來的 0 到 255 的 C 類位址)。

相似的，要將一個 C 類網路分為 4 個子網路，遮罩就是:

255.255.255.192 **或** 11111111. 11111111. 11111111.11000000

Field 4 中額外的兩個位元組可以有 4 個值(00，01，10，11)，因此產生了 4 個子網路。每個子網路使用剩餘的 6 位元作為其主機 ID，範圍是 0 到 63。

一些子網路遮罩並不表示額外的網路ID位元，因此也沒有子網路產生。這樣的遮罩稱為預設子網路遮罩，這些遮罩是:

A類: 255.0.0.0
B類: 255.255.0.0
C類: 255.255.255.0

這些稱做預設遮罩是因為網路在沒有子網路存在的時候已經設定完畢。

6 疑難排解

本章節列舉出幾種可用於診斷問題的 IP 工具。同時還列出一些可能出現的問題並附上建議解決方案。

所有已知的 bug 已經列在出貨說明中。請在設定交換器前仔細閱讀該說明。如果本手冊中的解決方式仍無法解決問題，請與我們的客服部門連絡。

6.1 使用 IP 工具診斷問題

6.1.1 ping

Ping 是用於檢測您的電腦是否能夠識別網路上其他電腦的指令。ping 指令向您指定的電腦送出一條訊息，如果該電腦收到這條訊息，它就會發送回應。要使用ping 指令，您需要知道進行連絡的電腦的IP 位址。

在 Windows® 作業系統的電腦上，您可以打開 **開始** 功能表，然後點選「**執行**」，在提示符下鍵入指令如下:

```
ping 192.168.1.1
```

點選 「**確定**」。您可以用已知區域網路的私有位址或公共網路上的IP 位址來替換。

如果目標電腦收到了這個訊息，就會出現如圖 50 所示的提示。

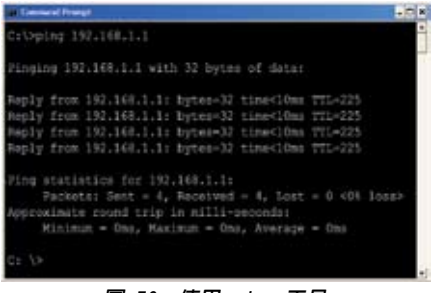


圖 50. 使用 ping 工具

如果無法定位目標電腦，就會顯示資訊“Request timed out”。

Ping 指令還可用於測試連接交換器的路徑是否通行無阻(使用預設的區域網路 IP 位址 192.168.1.1) 或其他為交換器指定的位址。

您也可以通過輸入一個外部位址，如 www.yahoo.com (216.115.108.243) 來檢測通往網際網路的路徑是否暢通。如果您不知道某個網際網路位置的IP位址，您可以使用 nslookup 指令，這個指令將在下節進行描述。

對於其他使用 IP 協定的作業系統，您可以在提示符下使用同樣的指令，或通過系統管理工具來實現這個指令。

6.1.2 nslookup

您可以使用 nslookup 指令來決定與網際網路站點相對應的 IP 位址。您可以指定一個普通名稱，nslookup 將在您的 DNS 伺服器中尋找 IP 位址(DNS 伺服器一般位於您的 ISP)。如果該名稱不在您的 ISP 的 DNS 伺服器的記錄中，位址請求就會傳送到上級伺服器，以此類推，直到找到位址為止。此時伺服器就會將相對應的 IP 位址傳送到您的電腦。

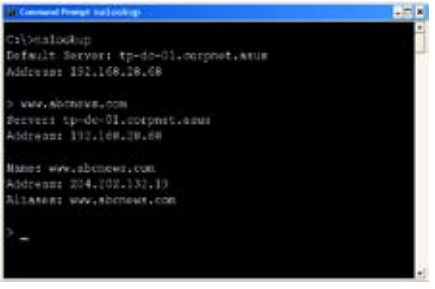


圖 51. 使用 nslookup 工具

對於使用 Windows® 作業系統的電腦，您可以打開 **開始** 功能表，點選「**執行**」，然後在文本視窗輸入以下內容:

nslookup

點選「**確定**」。提示符後就會出現一個括弧提示符 (>)。在這個括弧提示符後鍵入

網際網路位址，如 www.absnews.com。

視窗就會顯示相對應的 IP 位址, 如圖 51 所示。

事實上，一個網際網路名稱可能對應很多個IP位址，尤其對網路流量大的站點。這些站點可能使用多個備用伺服器來儲存相同的資訊。

要退出 nslookup，在提示符處鍵入 exit 並按 <Enter>。

6.2 簡易維修

表 8. 疑難排解

問題	建議方案
LED燈號	
系統打開後，SYSTEM LED 不亮	確認電源線是否連接到交換器或電源插座。
當連接網路線時，Gigabit 乙太網路 Link LED 不亮	1. 確認乙太網線是否正確地將交換器連接到您的區域網路交換器/集線器/電腦。確認電腦/集線器交換器已經打開。 2.確認纜線長度是否符合您的網路的要求。1000 Mbps 網路(1000BaseTx)須使用標有 Cat 5 的纜線。10Mbit/sec 纜線可能支持較低品質的纜線。
網路存取	
電腦不能存取同一網路中的另一個主機	1.檢查乙太網路線是否完好，LED 燈號是否呈綠色。 2.如果連接埠的LED燈號呈琥珀色，檢查該埠是否被禁用。 如果剛剛啓用STP, 可能會出現短時間的網路中斷。
電腦無法顯示網頁設定介面	1.交換器已打開並且連接埠也已經啓用。交換器的出廠預設 IP 為 192.168.1.1. 2.在您的電腦上確認您的網路設定。如果您的電腦沒有設定一個有效的路由來連接到交換器，請將交換器IP改成您的電腦可以存取的 IP 位址。 3.從電腦 Ping 您的交換器 IP，如果失敗，請重複第二步。

表 8. 疑難排解

問題	建議方案
網頁設定介面	
丟失/忘記網頁設定介面的使用者名稱或密碼	1.如果您還沒有修改使用者名稱和密碼，請嘗試使用者名稱“admin”，密碼為空。
某些頁面無法完全顯示	1.確認您使用的是 Internet Explorer® v5.5 或以後版本的瀏覽器。不支援 Netscape。您的瀏覽器必須啓用 Javascript®，也必須支持 Java®。 2.Ping 交換器的 IP 位址檢查連接是否穩定。如果一些ping 封包丟失，檢查您的網路設定，確認設定有效。
對設定的修改無法儲存	確認點選了 Save Configuration 頁面的 Save 按鈕。

6.3 上傳與下載檔案的程序

6.3.1 透過 FTP 上傳韌體

在您使用 ftp 功能及其他遠端管理工具時，請確認您的 PC 與交換器位於同一 VLAN 下。交換器的 VLAN 顯示於網頁管理介面的 System—>IP setup 頁面，或您可使用 CLI 指令“net interface show”來顯示 VID。

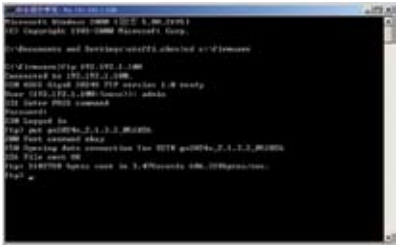


圖 52. 透過 FTP 上傳韌體

1. 開啓指令列介面視窗。
2. 將目錄更改為韌體所在的位置。
3. 用指令“ftp <IP Address>”來連線至交換器內部的FTP伺服器，所以此 IP 位址為交換器的 IP 位址，如“ftp 192.192.1.100”。
4. 輸入系統的使用者名稱。
5. 輸入系統密碼。
6. 用指令“put <File Name>”來上傳韌體。檔案名為韌體的名稱，如“put gx1024i+_2.1.3.2_051026”。

6.3.2 透過 FTP 上傳自動設定檔（auto-config file）

在您使用 ftp 功能及其他遠端管理工具時，請確認您的 PC 與交換器位於同一 VLAN 下。交換器的 VLAN 顯示於網頁管理介面的 System—>IP setup 頁面，或您可使用 CLI 指令“net interface show”來顯示 VID。

自動設定檔（auto-config file）是一個由 CLI 指令構成的文字檔，當這個檔案載入交換器後，交換器將執行這些指令。

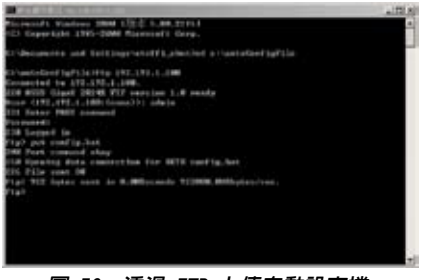


圖 53. 透過 FTP 上傳自動設定檔

1. 開啓指令列介面視窗。
2. 將目錄更改為自動設定檔所在的位置。

3. 用指令“ftp <IP Address>”來連線至交換器內部的FTP伺服器，所以此 IP 位址為交換器的 IP 位址，如“ftp 192.192.1.100”。
4. 輸入系統的使用者名稱。
5. 輸入系統密碼。
6. 用指令“put <File Name>”來上傳自動設定檔。檔案內容的開頭必須包含“#autoconfig”字樣，且自動設定檔的名稱必須為“config.bat”，如：“put config.bat”。

6.3.3 透過 FTP 備份系統設定

在您使用 ftp 功能及其他遠端管理工具時，請確認您的 PC 與交換器位於同一 VLAN 下。交換器的 VLAN 顯示於網頁管理介面的 System—>IP setup 頁面，或您可使用 CLI 指令“net interface show”來顯示 VID。

圖 54. 透過 FTP 備份系統設定

1. 開啓指令列介面視窗。
2. 將目錄更改為系統設定檔案所在的位置。
3. 用指令“ftp <IP Address>”來連線至交換器內部的FTP伺服器，所以此 IP 位址為交換器的 IP 位址，如“ftp 192.192.1.100”。
4. 輸入系統的使用者名稱。
5. 輸入系統密碼。
6. 系統設定檔案的預設名稱為“backup”。使用者必須使用這一名稱來備份系統設定。您可以在下載檔案後重新命名檔案。

6.3.4 透過 FTP 回復系統設定

在您使用 ftp 功能及其他遠端管理工具時，請確認您的 PC 與交換器位於同一 VLAN 下。交換器的 VLAN 顯示於網頁管理介面的 System—>IP setup 頁面，或您可使用 CLI 指令“net interface show”來顯示 VID。

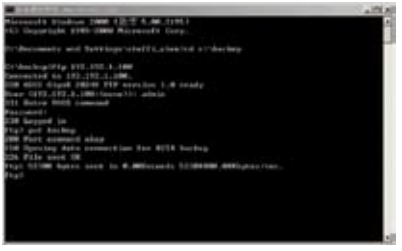


圖 55. 透過 FTP 回復系統設定

1. 開啓指令列介面視窗。
2. 將目錄更改為自動設定檔所在的位置。
3. 用指令“ftp <IP Address>”來連線至交換器內部的FTP伺服器，所以此 IP 位址為交換器的 IP 位址，如“ftp 192.192.1.100”。
4. 輸入系統的使用者名稱。
5. 輸入系統密碼。
6. 用指令 “put <File Name>” 來回復系統設定。此檔案必須是同一交換器機種的備份檔案如：“put backup”。

7. 術語表

10BASE-T 用於乙太網路的有線線纜，資料傳輸率為 10Mbps。亦稱 3 類線(CAT 3)。參見 Ethernet。

100BASE-T 用於乙太網路的有線線纜，資料傳輸率為 100Mbps。亦稱 5 類線 (CAT 5)。參見 Ethernet。

1000BASE-T 用於乙太網路的有線線纜，資料傳輸率為 1000Mbps。

binary 二進位。“基於 2”的數位系統，只使用 0 和 1 兩個數位來表示所有的數字。在二進位中，十進位數字 1 寫作 1，十進位數字 2 寫作 10，十進位數字 3 寫作 11，十進位數字 4 寫作 100，依次類推。雖然 IP 位址為方便起見表示為十進位數字， 實際上它使用的是二進位數字。比如 IP 位址 209.191.4.240 轉換為二進位是 11010001.10111111.00000100.11110000。比特，IP 位址，網路遮罩同樣也是二進位。

bit 比特。“二進位數字”的縮寫，一個比特就是一個只有0, 1兩種數值的數位。參見 binary。

bps 比特每秒

CoS 服務級別。在 802.1Q 中規定，值的範圍為 0 到 7。

DSCP 差分服務代碼點

IP 報頭中差分服務部分最重要的六位被稱為DSCP。GigaX 系列中可用的DSCP 值有 0, 8, 10, 16, 18, 24, 26, 32, 34, 40, 46,48 和 56。

broadcast 廣播。將資料發送到網路上所有的電腦。

Ethernet 乙太網路。最常見的電腦網路技術，通常使用雙絞線。乙太網路的資料傳輸速率為 10Mbps 和 100Mbps。參見 10BASE-T, 100BASE-T, twisted pair。

FTP 檔案傳輸協定

用於連接到 Internet 的電腦之間的檔案互傳。常見的用途包括上傳或更新網頁伺服器上的檔案，從網路伺服器下載檔案。

host 主機。連接到網路的裝置(通常指電腦)。

ICMP 網際網路控制訊息協定

一種網際網路協定，用於報告錯誤與其他網路相關資訊。ping 指令就是基於這種協定。

IGMP 網際網路群組管理協定

	一種網際網路協定，允許電腦與其網路成員通過多重播送群組共用訊息。一個電腦多重播送群組就是群組的成員都設定成從成員處接收特定的內容資訊。向 IGMP 群組傳送多重播送的應用可隨時更新群組的位址簿或將公司的通告傳送到收信人列表。
IGMP Snooping	在每個連接埠偵聽 IGMP 封包並將連接埠與二層多重播送群組相關聯。
mask	遮罩。參見 network mask。
Multicast	多重播送。將資料傳送到一組網路裝置上。
Mbps	百萬比特每秒的縮寫。網路資料傳輸率常表示為 Mbps。
Monitor	監視。亦稱“Roving Analysis”，允許將一個網路分析器連接至連接埠上並使之監測交換器的其他埠。
network	網路。指連接在一起，允許相互通信和共用資源（如軟體、檔案等）的一組電腦。網路可以是小型的，例如區域網路 (LAN)，也可以是大型的，例如網際網路。
network mask	網路遮罩。網路遮罩就是一系列的比特字串用於IP位址，以決定網路 ID 和主機 ID 的位元數。1 表示此位元有效，0 表示忽略此位元。舉例說明，如果網路遮罩 255.255.255.0 用到IP位址100.10.50.1，網路 ID 為 100.10.50，主機 ID 為 1。參見 binary, subnet 部分。
NIC	網路介面卡 插入電腦，提供網路線纜的物理介面 RJ-45 的介面卡。參見 Ethernet，RJ-45。
packet	封包，在網路上傳輸資料的單位。每個封包都包含資料、添加的資訊，如它從哪裡來（來源位址）及將到哪裡去（目的地位址）。
ping	封包探測 用於確認 IP 位址對應的主機是否能夠到達。它亦可用於尋找與功能變數名稱相對應的IP 位址。
port	埠。實體的網路設備接入點，如電腦，路由器，資料透過該接入點流入流出。
protocol	協定。一系列用於控制資料傳輸的規則。為了使資料能夠成功傳輸，資料傳輸來源和目標都必須遵守相同協定的規則。
PVLAN	私有虛擬區域網路
remote	遠端。即實體上處於不同地點。比如說，一名職員出差在

	外時登入公司的 intranet，他就是遠端使用者。
RJ-45	註冊介面標準45
	這種 8-pin 的插頭是用於在電話線上傳輸資料的。乙太網路線通常也會使用這種插頭。
RMON	遠端監控
	SNMP 的延伸，提供綜合性的網路監視功能。
routing	路由。在您的網路和網際網路之間，根據來源IP位址和網路情況，選擇最有效的路徑轉發封包。執行路由選擇的裝置稱為路由器。
SNMP	簡易網路管理通訊協定
	用於管理網路的 TCP/IP 協定。
STP	生成樹協定
	防止封包在複雜網路中造成迴路的橋接協定。
subnet	子網路。子網路是網路的一部分，子網路藉由將網路中的電腦歸分為小組而使這些電腦與其他網路上的電腦分隔開來。子網路中的電腦仍然在實體上與其他上層網路相連，但是他們被認為是一個獨立的網路。參見network mask。
subnet mask	子網路遮罩。將子網路之間加以區分的遮罩。參見 network mask。
TCP	參見 TCP/IP。
TCP/IP	傳輸控制協定/網際網路協定
	這是網際網路上基本的協定組。TCP 負責將資料分為可以在網際網路上傳輸的封包，IP負責將這些封包傳送到目的地址。當 TCP 和 IP 與一些上層應用進行捆綁如 HTTP, FTP, Telnet 等，TCP/IP 指的確是整套協定組。
Telnet/SSH	一種互動的，以字元為基礎的，用於存取遠端電腦的程式。HTTP (網路協定)和 FTP 只允許從遠端電腦下載檔案，而 Telnet/ SSH 允許從遠端登入並使用電腦。
TFTP	小型檔案傳輸協定
	一種傳輸檔案的協定。TFTP 比 FTP 更加容易使用，但是效能和安全性不如 FTP。
Trunk	兩個或兩個以上的埠合而為一成為一個虛擬埠，也稱為連結匯聚。
TTL	存活時間

	IP封包的一個欄位，決定了該封包的壽命。TTL原本表示的是持續時間，現在則通常用於表示最大計跳數，每經過一跳都消耗一個計跳數，當TTL為零時，該封包就被丟棄。
twisted pair	雙絞線。即普通的銅制電話線。它包含一對或多對互相纏繞的電線，以消除干擾和雜音。每根電話線使用一對線，在家用情況下，通常都安裝兩對。對於乙太網路區域網路，使用的是一種高端的，用於 10BASE-T 網路的三類線 (CAT 3)，以及更高端的 100BASE-T 網路的五類線 (CAT 5)。參見 10BASE-T，100BASE-T，Ethernet。
upstream	上行。資料從使用者流向網際網路的方向。
VLAN	虛擬區域網路
WAN	廣域網路
	所有的分佈于廣大的地理位置的網路統稱廣域網路，如一個國家或一個洲。對於交換器來說，廣域網路指的就是網際網路。
Web browser	網頁瀏覽器。一種使用超文本傳輸協定(HTTP) 的，用於從網站下載/上傳資訊的軟體。這些資訊包括文本，圖像，聲音或視訊。網頁瀏覽器使用了超文本傳輸協定(HTTP)。常用的網頁瀏覽器包括 Netscape Navigator 和 Microsoft Internet Explorer。參見 web site。
Web page	網頁。一個網站的檔案通常包括文本，圖像，和連接到其他頁面的超連結。當使用者存取一個網站時，顯示的第一頁成為主頁。參見 web site。
Web site	網站。網際網路上透過網頁瀏覽器為遠端使用者的提供資訊的電腦。網站常由包含文本，圖像，超連結的網頁構成。參見 web page。