GigaX2124

第二層網路管理交換器

使用手册

C3394
2007 年 9 月
第一版

華碩連絡資訊

華碩電腦公司 ASUSTeK COMPUTER INC.

位址	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	+886-2-2894-3447

ASUS COMPUTER INTERNATIONAL (美國)

位址	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	
	+1-812-282-2787 (主機板／其他產品)
	+1-510-739-3777 x5110 (筆記型電腦)
傳真	+1-812-284-0883
線上支援	support.asus.com

ASUS COMPUTER GmbH (德國／奧地利)

位址	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

第一章　產品簡介

感謝您購買華碩 GigaX2124 第二層網路管理交換器！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。

本手冊將為您提供安裝和設定　GigaX2124 第二層交換器所需的相關資訊，以發揮本產品的最佳效能。

1.1　GigaX2124 第二層交換器特性

- 24 個 10/100/1000BASE-T 自動偵測 Gigabit 乙太網路交換埠
- 4 組 SFP GBIC 插槽
- 所有連接埠支援自動 MDI/MDIX 功能
- 相容於 802.3z 和 802.3ab 規格
- 802.1D 透明橋接 (transparent bridge)
- 16K 組硬體計時汰換 (aging) 之 MAC 位址
- 迴路（Loop Back）檢測
- STP/RSTP/MSTP
- 第二層至第四層的存取控制列表
- 支援 IGMP 偵聽
- 支援 DHCP 使用者端
- 支援 DHCP 偵聽
- 802.3ad 連結匯聚（幹線），最多可支援 8 個幹線群組
- 連接埠鏡像（Port Mirroring）功能
- 基於 802.1Q 標記之虛擬區域網路（VLAN），最多支援 4096 組
- LACP
- GVRP
- 802.1p (CoS) 標記
- 802.3x 流量控制
- 以連接埠為基礎的優先順序，每個連接埠支援 8 個佇列
- 頻寬控制
- WRR（權重循環排序）
- QoS 策略圖表設定
- 802.1x 認證

- 連接埠安全（Port Security）功能
- RADIUS 使用者端
- 802.1x 動態 VLAN 指定
- DoS
- SNMP v1, v2, v3 簡易網路管理通訊協定
- 支援 MIB-II 管理資料庫
- RMON：支援四個群組（1，2，3，9）
- NTP
- 企業級電源供應器、風扇和系統溫度、電壓管理資料庫（MIB）
- Telnet/SSH 遠端登入
- TFTP/FTP 韌體更新和備份設定
- 如 Cisco 操作的 CLI 指令介面
- 網頁圖形使用者介面（GUI）
- 每個連接埠具有 LED 指示燈表示連線狀態
- 系統、備用電源 (RPS) 與風扇狀態 LED 指示燈

1.2 關於本手冊

1.2.1 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，GigaX2124 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。

1.2.2 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。

1.2.3 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。

第二章　瞭解 GigaX2124 交換器

2.1　產品包裝內容

GigaX2124 交換器的產品包裝中包含以下物品：

- GigaX2124 第二層網路管理交換器
- AC 電源線
- 終端管理介面連接線 (DB9)
- 機架安裝套件 (包括兩個托架與六顆 #6-32 螺絲)
- 連接終端管理介面的 USB 纜線
- 安裝光碟
- 快速安裝指南

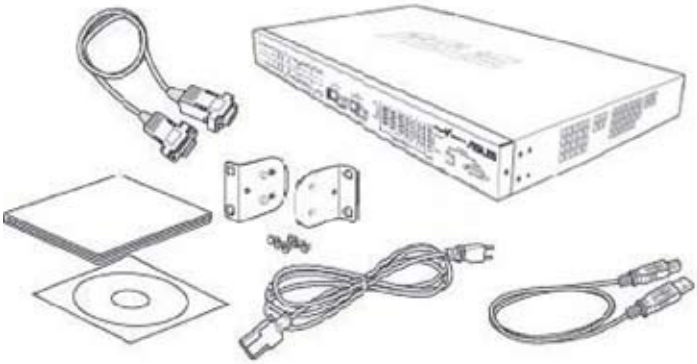

圖 1. GigaX2124 第二層網路管理交換器產品包裝內容

2.2 前面板

前面板包括了 24 個 RJ-45 10/100/1000Base-T 連接埠，4 個 SPF GBIC 連接埠，24 組連接埠連線狀態 LED 指示燈，和一組 LED 指示燈，用於顯示系統、備用電源 (RPS)、風扇的狀態。

圖 2. 前面板

表 1. 前面板標示和 LED 指示燈

標示	顏色	狀態	描述
SYSTEM	綠色	恆亮	裝置電源開啟
		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
RPS	綠色	恆亮	裝置的電源供應器 (PSU) 工作正常，且交換器的備用電源正常
	琥珀色	恆亮	裝置的電源供應器 (PSU) 工作異常，交換器正由備用電源供電
	熄滅		無電源供應 (system LED 亦熄滅); 備用電源異常或尚未安裝 (system LED 亮起)
FAN	綠色	恆亮	兩個風扇均工作正常
	琥珀色	恆亮	兩個風扇全部或有一個停止運轉
10/100/1000 port status	綠色	恆亮	已建立 RJ-45 或 SFP 連線；連接埠已開啟
		閃爍	正在傳送或接收資料
	琥珀色	恆亮	已建立連線，但連接埠已被手動或 STP 關閉
		閃爍	連接埠處於 STP 阻斷、偵聽和學習狀態 連接埠安全設定為 Shutdown-Violatin 狀態 連接埠因產生環路而被線路協定（Line Protocol）關閉
	熄滅		無乙太網路連線
10/100/1000 port speed	綠色	恆亮	1000Mbps
	琥珀色	恆亮	100Mbps
	熄滅		10Mbps
10/100/1000 port duplex	綠色	恆亮	全雙工模式
	琥珀色	恆亮	半雙工模式
		閃爍	衝突

2.3 後面板

本交換器的後面板包含有風扇、電源線插孔與一個備用電源供應器 (RPS) 連接插座。

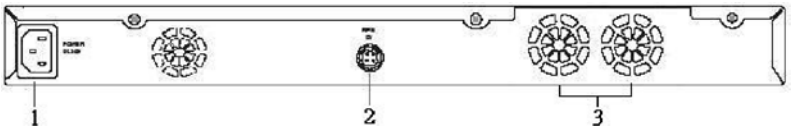

圖 3. 後面板

表 2. 後面板標示

序號	標示	描述
1	Power	連接電源線
2	RPS	備用電源供應器
3	FAN1-FAN2	系統風扇

2.4 技術規格

表 3. 技術規格

實體尺寸	43.5mm(H) x 444 mm(W) x 322mm(D)		
電源	輸入	耗電量	
	100-240V AC/ 2.5A 50-60Hz	< 82 瓦	
備用電源供應器 (RPS)	輸入	輸出	
	100-240V AC/ 1.8A 50-60Hz	12V DC/12.5A	
環境需求		操作	存放
	溫度	0 ~ 40° C (32 ~ 104° F)	-25 ~ 70° C (-13 ~ 158° F)
	濕度	15 ~ 90%	0 ~ 95%
	高度	最高 10,000ft (3,000m)	最高 40,000 ft (12,000m)
風扇	尺寸	電壓和電流	轉速
	40 x 40 x 20 mm	12VDC, 0.13A	8200RPM

第三章　快速安裝指南

本章節將介紹如何設定交換器的工作環境。您也可以參考 GigaX2124 的安裝指南。

第一部分介紹如何將 GigaX2124 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 GigaX2124 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

3.1　第一部分 — 硬體安裝

3.1.1　將交換器安裝於平坦表面

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。

3.1.2　將交換器安裝於機架

1. 用螺絲將銷售包裝中附帶的掛鉤固定在交換器的兩側。
2. 將交換器上的掛鉤固定在機架的兩側，並用螺絲加固。

3.2　第二部分 — 設定交換器

3.2.1　連接控制終端連接埠（Console port）

在使用控制終端對交換器進行管理之前，請使用 RS232 (DB9) 或 USB 纜線來連接交換器。若您想使用網頁介面進行設定，請用乙太網路線連接您的 PC 和交換器。

3.2.2 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。您可以使用一般或跳接過（crossover）的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。

3.2.3 連接備用電源模組（RPS）

將備用電源模組（選購）連接到交換器後面板的RPS插孔，並確認RPS的另一端連接了電源線。將電源線插到具備接地迴路的電源插座上。

3.2.4 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。

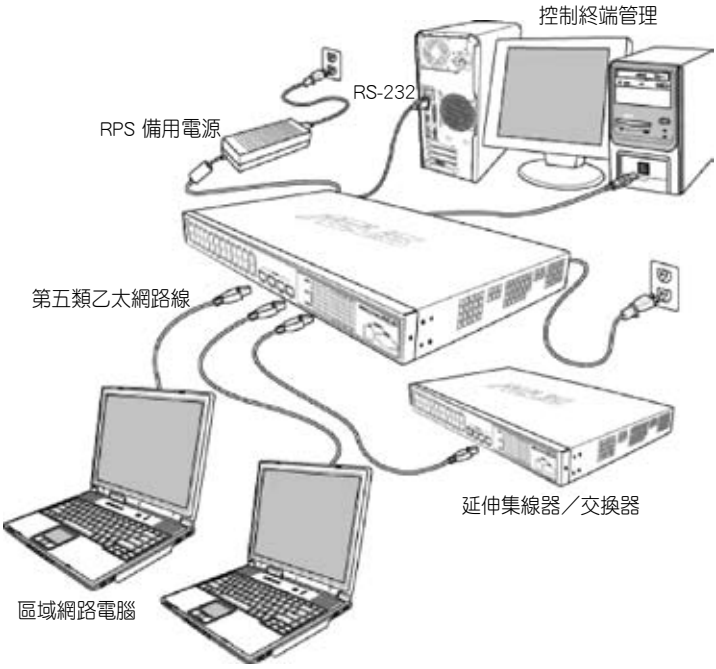

圖 4. 硬體連接示意圖

表 4. LED 指示燈

No.	LED	描述
1	System	穩定的綠色代表交換器已經開啟。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 [24]	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。
3	RPS	穩定的綠色代表備用電源（RPS）模組已成功安裝。
4	Fan	穩定的綠色代表所有的風扇都運作正常。

3.3 第三部分 — 交換器基本管理設定

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：

- **網頁介面：**本交換器提供網頁管理介面，您可以使用帶 Java® 功能的 IE 6.0 或更高版本的瀏覽器進行設定。
- **指令列介面：**透過控制終端連接埠來設定交換器。

3.3.1 透過控制終端連接埠進行設定

1. 請使用產品包裝中附帶的交叉型 RS-232 纜線來連接交換器前面右側的控制終端連接埠。此連接埠為 DB-9 公接頭，專門用於資料終端裝置 (DTE) 的連接。將纜線接頭上的緊固螺絲固定在控制終端接頭上，將纜線的另一頭連接到具有終端模擬軟體，如 Hyper Terminal 的電腦上。
2. 用產品包裝中附帶的 USB 纜線將交換器連接到電腦。在連接前您必須首先安裝隨機光碟中的 USB 驅動程式。USB 驅動可以在 Windows Me/2000/XP 作業系統中模擬一個額外的 COM 連接埠。
3. 請確認控制終端的模擬軟體的設定如下：
   a) 選擇合適的序列埠號
   b) 將資料傳輸速率設定為每秒 9600 位元
   c) 設定資料格式為無同位檢查（no parity），8 個資料位元（Data bit）及一個停止位元 (Stop bit)。
   d) 無流量控制
   e) 模擬模式設為 VT100
4. 控制終端設定完畢後，您可以在終端畫面上看到“ASUS login:”。
5. 預設的使用者名稱為“admin”，且無需輸入密碼，直接按下 <Enter> 即可。

您可以隨時藉由 CLI 指令列介面來修改密碼 (請參考使用手冊 5.3.1 節)。為避免您的交換器被未經許可的人士使用，建議您盡快修改預設密碼。

6. 請依照以下步驟來指定交換器的 IP 位址：

   a) 輸入“enable”。

   b) 輸入“configure terminal”，新的提示為“ASUS(config)#”。

   c) 輸入“interface vlan 1”，新的提示為“ASUS (config-if)#”。

   d) 輸入“ip address < 您的 IP 位址 > < 您的網路遮罩 >”。例如，若您的交換器 IP 為 192.168.1.1，網路遮罩為 255.255.255.0，則您需要鍵入“ip address 192.168.1.1/24”。

   e) 輸入“end”，此時將回到先前的提示“ASUS#”層級。

   f) 輸入“write”，將會套用變更並將變更寫入設定檔中。

   g) 輸入“reboot”。

7. 如果交換器必須跨網路進行管理，則需要一個預設的閘道器或靜態路由，請按照以下的步驟來指定一個預設的閘道器或靜態路由：

   a) 輸入“ASUS#”。

   b) 鍵入“show running-configuration”來檢視當前設定。若有不正確的路由，您需要鍵入“no ip route 0.0.0.0/0 192.168.1.254”來移除它。

   c) 輸入“configure terminal”，新的提示為“ASUS(config)#”。

   d) 輸入“no ip route 0.0.0.0/0 192.168.1.254”來清除預設路由。

   e) 輸入“ip route 0.0.0.0/0 192.168.1.2” 來設定您的預設路由。

   f) 輸入“end”。

   g) 輸入“write”。

```
ASUS login: admin
Password:

ASUSTek GigaX 2124 4.1.05.00.01 Copyright (c) 2007


ASUS> enable
ASUS# configure terminal
ASUS(config)# interface vlan 1
ASUS(config-if)# ip address 192.168.1.1/24
[admin] Install IP address 192.168.1.1/24 succeeded!
ASUS(config-if)# end
ASUS# configure terminal
ASUS(config)# no ip route 0.0.0.0/0 192.168.1.254
ASUS(config)# ip route 0.0.0.0/0 192.168.1.2
ASUS(config)# end
ASUS# write
Building Configuration ...
Integrated configuration saved as 'startup_config' ok!
ASUS# _
```

圖 5. 登入與 IP 設定畫面

3.3.2 透過網頁介面進行設定

若想將您的個人電腦連接到交換器，您的個人電腦必須在網路中取得合法的 IP 位址。請連絡您的網路管理人員來取得交換器的合法 IP 位址。若您想要更改交換器的預設 IP 位址，請參考 3.3.1 節的說明。

1. 若您的電腦中沒有安裝 Java 環境，您的電腦將會自動進行下載與安裝。這時 您的個人電腦需要能連上網際網路。若您的個人電腦不能連接到網際網路，您必須從光碟或磁片中安裝這個軟體。
2. 在交換器可以存取的網路中任何一臺電腦上，開啟您的網頁瀏覽器 (Internet Explorer)，在網址欄內鍵入以下 URL，並按下 <Enter>：

   http://192.168.1.1

   這是交換器出廠的預設 IP 位址值。

此時會出現登入畫面，如圖 6 所示。

圖 6. 預設網頁介面

點選 “ASUS GigaX-Switch Manager”，將出現如下的登入畫面。

圖 7. 登入畫面

輸入您的使用者名稱和密碼，並按下 OK 以進入設定管理介面。當您第一次登入此畫面時，請輸入如下所示的預設值：

預設的使用者名稱: admin

預設的密碼: (無密碼)

您可以隨時透過 CLI 指令列介面來更改密碼。

瀏覽器將會透過交換器來下載 java 應用程式，這可能需要花費幾秒鐘的時間。

3. 要設定新的 IP 位址，請點選 System，並選擇 IP Setup。 然後請填寫 IP 位址、子網路路遮罩與預設閘道器，完成後點選 OK 鈕。

4. 當交換器套用了新的 IP 位址後，瀏覽器不會自動更新交換器的狀態視窗或是退回之前的設定頁面。您需要在網址欄內重新輸入新的 IP 位址，並按下 <Enter>，重新進入網頁設定介面。

圖 8. IP 設定

第四章　用網頁介面進行管理

本交換器提供網頁管理介面，您可以透過網頁瀏覽器進行交換器的管理。本功能推薦使用支援 Java® 的微軟 Internet Explorer® 6.0 或更高版本。

4.1　登入網頁管理介面

1. 在電腦上開啟網頁瀏覽器 (IE)，在位址欄內輸入以下內容，並按下 <Enter>：

   http://192.168.1.1

這是本交換器出廠時預設的 IP 位址。輸入完成後將會出現預設網頁，如圖 6 所示。點選“ASUS GigaX-Switch Manager”，將出現登入畫面，如圖 9 所示。

圖 9. 設定管理介面登入畫面

2. 輸入您的使用者名稱和密碼，並按下 OK 鈕。

   在首次登入時，請使用下面的預設值。 您可以透過指令列介面隨時更改密碼 (參考 5.3.1 節的說明)。

   預設的使用者名稱 : admin

   預設的密碼 : < 無 >

每次當您登入網頁管理介面時，您都會看到如圖 10 所示的主畫面。

圖 10. 主畫面

4.2 功能結構

典型的網頁設定頁面包含兩個獨立的欄位。頂部欄包含了交換器圖示和前面板圖，如圖 11 所示。這個欄位將一直位於瀏覽器視窗上方，可自動或手動更新交換器前面板的 LED 燈狀態，您可以透過按下右邊的“Auto”或“Manual”按鈕來選擇。請參考表 4 以認識各指示燈的含義。關於各指示燈顏色的含義，請參考表 5 。

圖 11. 頂部欄

表 5. 連接埠顏色描述

連接埠顏色	描述
綠色	乙太網路連線已建立
琥珀色	連接埠被管理員、生成樹、連接埠安全設定或線路協定關閉
熄滅	無乙太網路連線

選單項目，如圖 12 所示，包含了交換器所有的功能設定選項。這些功能會按照群組劃分，例如系統 (System)、橋接 (Bridge) 等功能。您可以點選任何一個項目來開啟對應的功能。

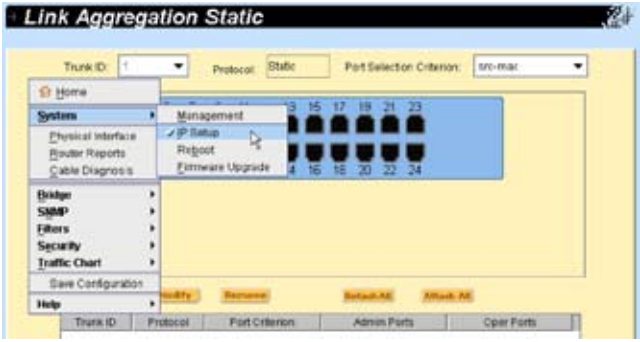

圖 12. 點選選單項目

4.2.1 瀏覽選單的技巧

若要開啟特定的設定頁面，請在選單中點選您所要開啟的選項。

4.2.2 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	描述
OK	儲存您對當前頁面做的任何變更。
Reload	重新顯示當前頁面，更新狀態和設定。
Edit	在系統中修改既有設定，如靜態路由或過濾的 ACL 規則。
New	清除所有輸入欄位，建立一個新設定。
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	修改選定的項目。
Remove	移除選定的項目，如靜態路由或過濾的 ACL 規則。
Query	查詢一個指定項目的狀態。
Detach All	從所有連接埠移除此設定值。
Attach All	新增此設定值至所有連接埠。

4.3 系統 (System)

圖 13. 系統選單

系統頁面包含有 Management（管理），IP setup（IP 設定），Reboot（重新啟動）和 Firmware update（韌體更新）等功能。

4.3.1 管理（Management）

管理（Management）頁面包含下列資訊：

Model Name：產品名稱。

MAC Address：交換器的 MAC 位址。

System Name：使用者設定的系統辨識名稱（可編輯）。

System Contact（可編輯）。

System Location（可編輯）。

點選 OK 鈕可儲存變更並使其立即生效。點選 Reload 鈕，頁面將會重新載入，更新成目前的設定。

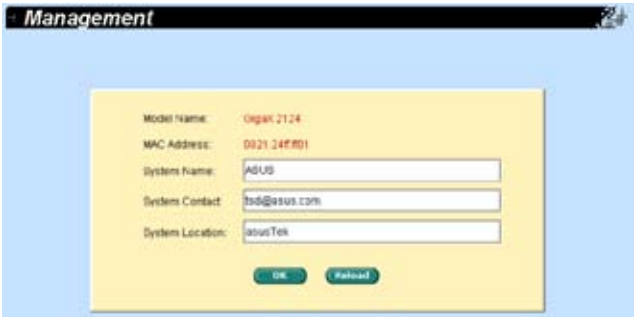

圖 14. 管理頁面

4.3.2 IP 設定（IP setup）

IP 設定（IP Setup）頁面包含以下可編輯的資訊：

DHCP Client：開啟／關閉交換器的自動取得 IP 功能。

IP Address：為交換器指定一個靜態 IP 位址。

Network Mask：設定網路遮罩。

Default Gateway：設定預設閘道。

點選 OK 鈕可儲存變更並使其立即生效。點選 Reload 鈕，頁面將會重新載入，更新成目前的設定，如圖 15 所示。

圖 15. IP 設定頁面

4.3.3 重新啟動（Reboot）

Reboot 頁面包含了一個 Reboot 按鈕。點選此按鈕可以重新啟動系統。

重新啟動系統將暫時中斷網路連線及網頁管理介面的連線。

4.3.4 韌體更新（Firmware Upgrade）

Firmware Upgrade and Auto-config 頁面包含下列資訊：

Hardware Version：顯示硬體版本。

Boot ROM Version：顯示 boot code 版本。

Firmware Version：顯示當前所執行的韌體版本。本編號會隨著韌體的更新而改變。

輸入 TFTP 伺服器的 IP 位址與韌體名稱。點選 Upgrade 來更新交換器的韌體。

例如：

TFTP 伺服器：192.168.1.155

檔案名稱：Gx2124-4.1.05.00.img

點選 Upload 按鈕將指定的韌體載入到交換器中。更新完成後請重新啟動交換器。您需要重新登入網頁設定介面。

我們強烈建議您在更新韌體之前先備份“startup-config”檔。

利用 FTP 方式的韌體更新只能透過 CLI 指令來執行。

圖 16. 韌體更新頁面

4.4 實體介面 (Physical Interface)

圖 17. 實體介面項目

實體介面 (Physical Interface) 頁面會顯示乙太網路埠的目前狀態。您可以在 Interface Configuration 視窗設定以下項目：

Port：選擇需要設定的連接埠

Admin：開啟／關閉連接埠

Mode：設定速度與雙工模式

Flow Control：開啟／關閉 802.3x 流量控制機制。

Switchport Mode：設定此連接埠為幹線（trunk）模式或存取（access）模式

Admin port VLAN：將選擇的連接埠指定到特定的 PVID

DHCP-Snoop： 開啟／關閉 DHCP 偵聽功能

DHCP-Snooping：將選定的連接埠設定為信任或不信任。

選擇對應的連接埠號並對其進行設定，然後點選 Modify 鈕。完成設定後，點選 OK 鈕可儲存變更並使其立即生效。點選 Reload 鈕，頁面將會重新載入，更新成目前的設定。

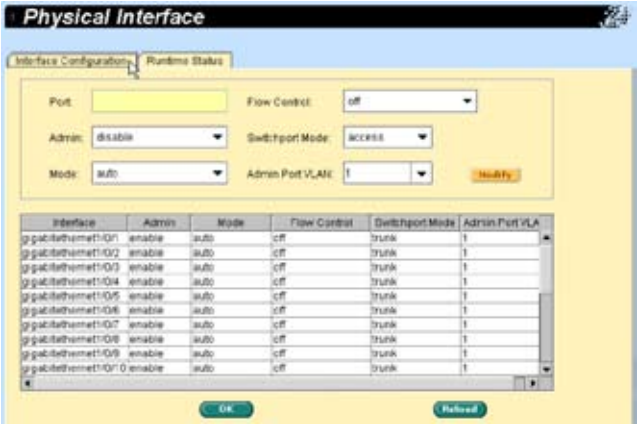

圖 18. 實體介面 -1

Runtime Status 畫面顯示每個連接埠的下列相關資訊。

Ethernet Link：已連線或未連線狀態。

STP Status：STP（生成樹）狀態。

Duplex：雙工模式。

Speed：連線速度。

Flow Control：開啟或關閉 802.3x 流量控制機制。

Oper Port VLAN：連接埠的 PVID。

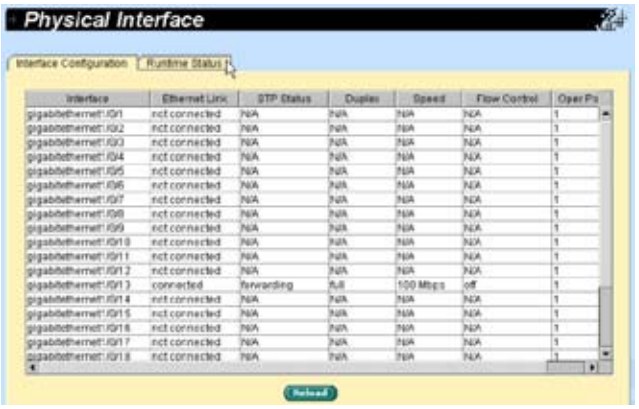

圖 19. 實體介面 -2

4.5 路由報告 (Router Reports)

圖 20. 路由報告項目

本頁面顯示了所有的路由資訊。

點選 Reload 鈕可更新狀態。

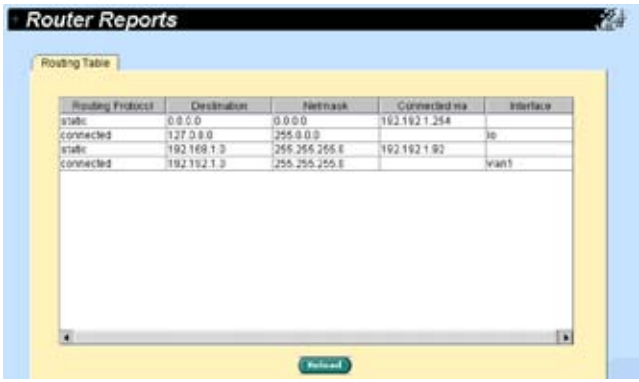

圖 21. 路由報告

4.6 纜線診斷 (Cable Diagnosis)

圖 22. 纜線診斷項目

可對常見的纜線問題作分析，如開路、短路或阻抗不匹配。

Interface：選擇您想要檢測的連接埠。

點選 Query 鈕開始診斷。

纜線診斷可用來檢測纜線開路或短路的長度。若纜線過短，檢測結果的誤差會較大。

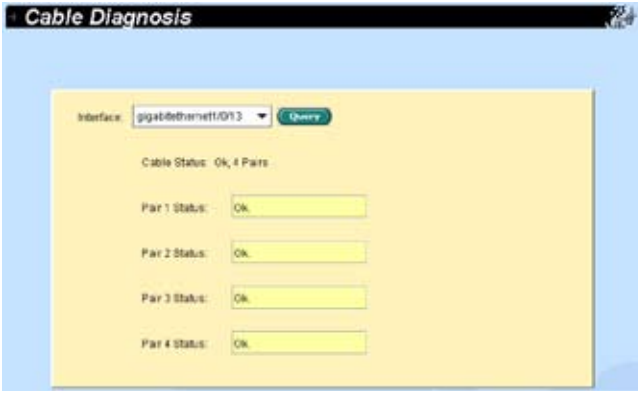

圖 23. 纜線診斷

4.7 儲存設定 (Save Configuration)

圖 24. 儲存設定項目

要永久儲存設定，點選 Save 鈕。

有時候您可能想要重置交換器的設定，您可以點選 Reload 將設定檔回復為出廠預設值。當然，在執行這個回復動作後，系統將會重新啟動。

若選擇了回復出廠預設設定，您所做的所有設定將全部消失。

圖 25. 儲存設定

4.8 橋接（Bridge）

圖 26. 橋接選單

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

4.8.1 生成樹（Spanning tree）

本頁面可設定三種不同類型的生成樹協定。

4.8.1.1 STP 狀態（STP Status）

“STP Status”可開啟或關閉 STP。您可以開啟 STP、RSTP 與 MSTP 三種模式。若開啟了 MSTP，則以下的四種設定也同時開啟：

Region Name：由字母和數字組成的名稱。

Revision：設定版本編號。

Instance ID：STP 實例（instance），您可以在交換器上設定 MSTP 來將多個 VLAN 映射到一個單一的 STP 實例（instance）。

VLAN Group：對應到實例（instanace）的 VLAN 群組。

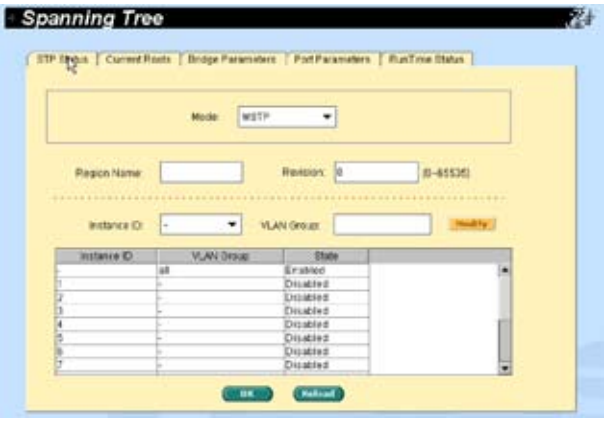

圖 27. 生成樹 - STP 狀態

4.8.1.2 生成樹的目前狀態（Current roots）

本頁顯示了目前生成樹的運作狀態，包括：

- 實例（Instance）ID
- VLAN 群組屬於哪個實例（Instance）ID
- 根橋接器的 MAC 位址
- 根橋接器的優先權大小
- 每次接收訊息後，根橋接器有效的最長時間
- 傳送 Hello packet 的間隔時間
- 連接埠轉變為 Forward 狀態所需的時間
- 連接到根橋接器的路徑成本（Cost）
- 連接到根橋接器的連接埠

圖 28. 生成樹 - 生成樹的目前狀態

4.8.1.3 橋接器參數（Bridge parameters）

這個頁面中可以設定此交換器生成樹運作的參數（Spanning-tree parameters）：

Priority：交換器在區域網路中的優先權。

Max Age：每次接收訊息後，根橋接器有效的最長時間。

Hello Time：傳送 Hello packet 的間隔時間。

Forward Delay：連接埠轉變為 Forward 狀態所需的時間。

Transmission Limit: 傳送 BPDU 的最小時間間隔。

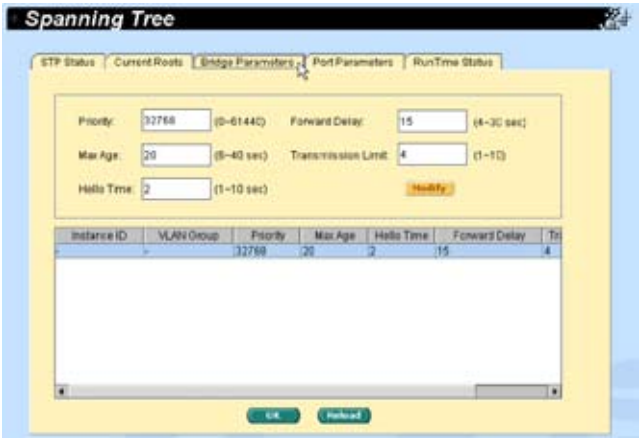

圖 29. 生成樹 - 橋接器參數

4.8.1.4 連接埠參數（Port parameters）

本頁面包含了一個顯示視窗，用來顯示每個連接埠的目前設定。您可以選擇一個連接埠然後對其進行編輯。點選 Modify 鈕將更改連接埠的生成樹設定。您可以設定以下欄位：

Instance ID（僅 MSTP）：您可以在交換器上設定 MSTP 來將多個 VLAN 映射到一個單一的 STP 實例（instance）。

Path Cost: 有效的設定值為 1 到 200000000。當偵測到網路迴路的狀況下，具有較高成本（Cost）的連接埠較可能被 STP 封鎖。

Priority：設定交換器連接埠的優先權。越小的數字代表越高的優先權。當偵測到網路迴路的狀況下，擁有較低優先權的連接埠較可能被 STP 封鎖。有效的設定值為 0 至 240。

Link Type：預設情況下，連線類型（Link Type）由連接埠的雙工模式決定：全雙工模式的連接埠被判定為點對點連線；半雙工模式的連接埠被判定為共享連線。

Edge Port：功能與 Port Fast-enabled 相同，只有在連接了一個單獨的終端裝置時您才可以開啟它。

點選 OK 鈕使設定生效。點選 Reload 鈕，頁面將會重新載入，更新成目前的設定。

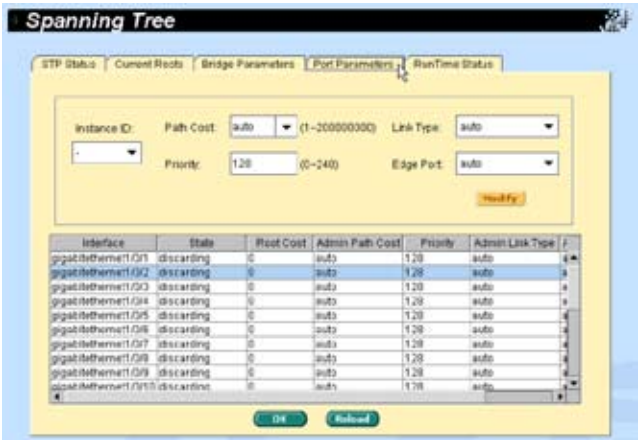

圖 30. 生成樹 - 連接埠參數

4.8.1.5 運作狀態（Runtime Status）

本頁面包含了一個顯示視窗，用來顯示每個連接埠的目前狀態。

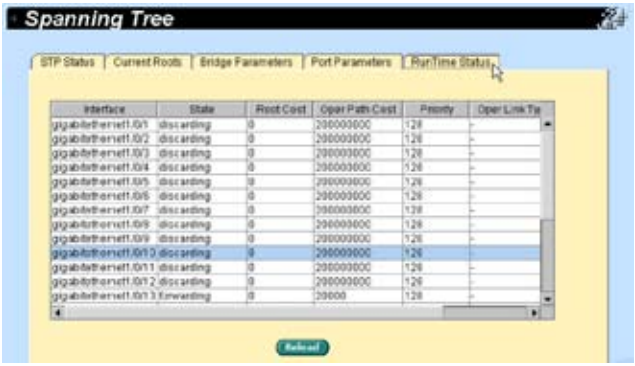

圖 31. 生成樹 - 運作狀態

4.8.2 連結匯聚（Link Aggregation Static）

本頁面用來設定連結匯聚靜態群組（連接埠幹線）。GigaX2124 最多可支援 8 個連結匯聚群組，而每個連結匯聚群組可設定 8 個連接埠。

Trunk ID：用來區分不同匯聚群組的號碼。

Protocol：顯示連結匯聚群組的狀態。對於本頁面來說是靜態（Static）。

Port Selection Criterion：可依照來源 MAC 位址、目的地 MAC 位址、來源與目的地 MAC 位址、來源 IP 位址、目的地 IP 位址或來源與目的地 IP 位址這些演算法，選定一種來決定匯聚群組中封包由哪個連接埠來傳遞。

Port：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刪除。

點選 OK 鈕使設定生效。點選 Reload 鈕，頁面將會重新載入，更新成目前的設定。

您需要檢查連線速度和雙工模式來確認連結匯聚群組是否真的正常運作。請至 Physical Interface 頁面的 Runtime Status 視窗檢查匯聚群組中所有連接埠的連線模式。如果所有的匯聚群組成員都具有相同的速度和全雙工模式，則匯聚群組已正確建立。如果有一個連接埠具有不一致的速度和雙工模式，則匯聚群組的設定不正確。 請檢查您的設定，使匯聚群組中的所有成員都具有相同的速度和全雙工模式。

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，則與其對接的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。

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。

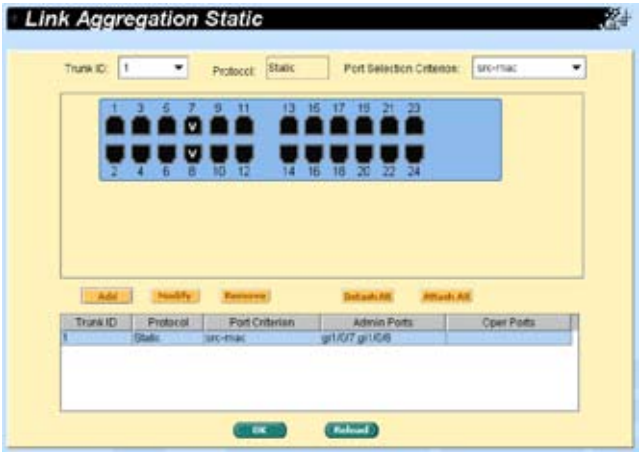

圖 32. 連結匯聚

4.8.3 動態連結匯聚 (LACP)

本頁面用來設定 LACP 群組 (連接埠匯聚) 並顯示 LACP 運作資訊。GigaX2124 最多可支援 8 個連結匯聚群組，而每個連結匯聚群組最多可設定 8 個連接埠。

Trunk ID：用來區分不同匯聚群組的號碼。

Protocol：顯示連結匯聚群組的狀態。對於本頁面來說是 LACP。

Port Selection Criterion：可依照來源 MAC 位址、目的地 MAC 位址、來源與目的地 MAC 位址、來源 IP 位址、目的地 IP 位址或來源與目的地 IP 位址這些演算法，選定一種來決定匯聚群組中封包由哪個連接埠來傳遞。

Port: 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刪除。

Admin Ports：顯示使用者設定的連接埠成員。

Oper Ports：顯示實際運作的連接埠。

點選 OK 鈕使設定生效。點選 Reload 鈕，頁面將會重新載入，更新成目前的設定。

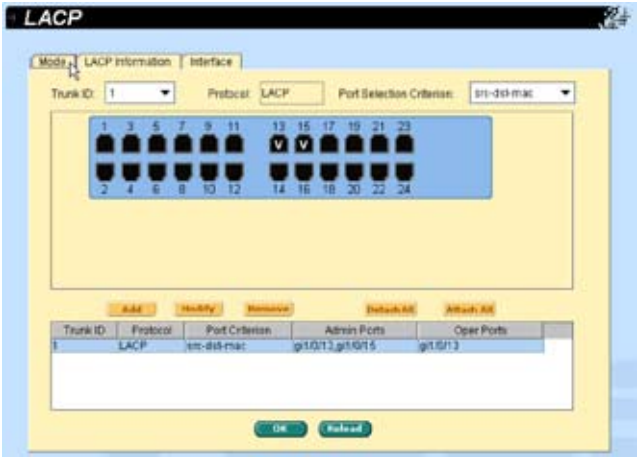

圖 33. LACP - 模式

第二部分顯示每個 Trunk ID 的 LACP 運作資訊。

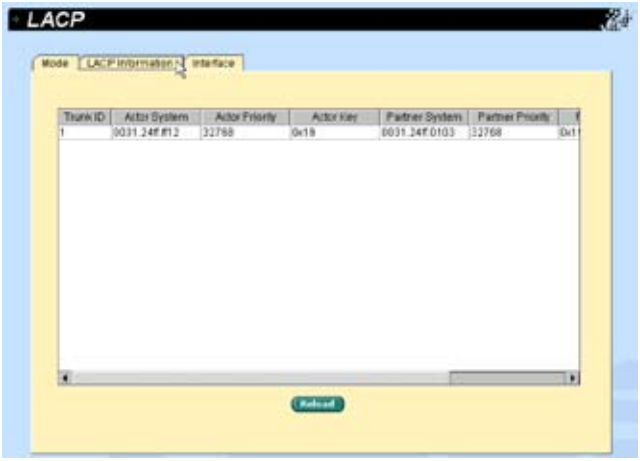

圖 34. LACP - LACP 資訊

最後一部分顯示了有運作的連接埠之 LACP 資訊。

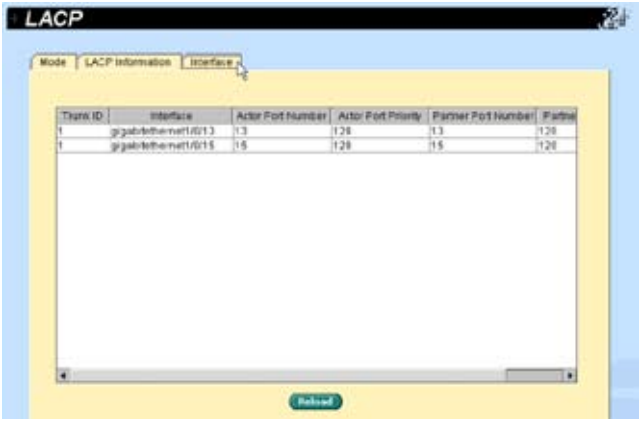

圖 35. LACP - 介面

4.8.4 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：開啟或關閉選定群組的鏡像功能。

Stack ID：選擇 stack ID。在單部交換器模式下，這個值保持為 1。

Session：有兩個選項可供選擇。Session 1 用於連接埠 1~12；Session 2 用於連接埠 13~24。

Monitor Port：接收來源連接埠之封包副本的連接埠。

Port：從選擇面板中選取來源連接埠，可被監控傳入 (Ingress)、傳出 (Egress) 或傳出傳入的封包。

監控埠不能屬於任何連結匯聚群組。

監控埠不會像一般交換器連接埠一樣地運作，不會進行封包交換或位址學習。

點選 OK 鈕使設定生效。點選 Reload 鈕，頁面將會重新載入，更新成目前的設定。

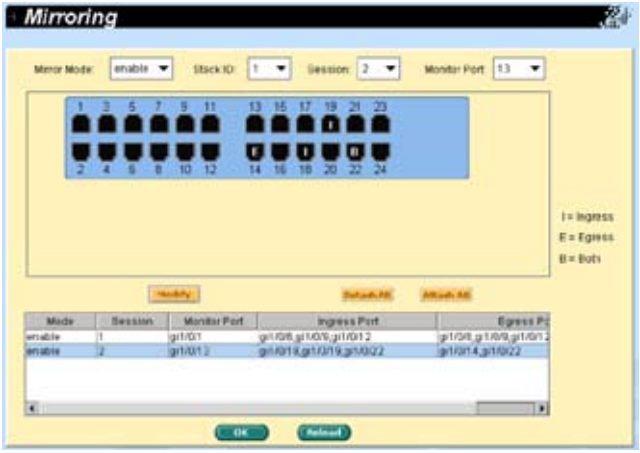

圖 36. 鏡像

4.8.5 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 256 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。

VLAN：選擇 VLAN 群組，這是一個基於 VLAN 的功能。

MAC Address：指定多重播送位址。

Port：從選擇面板上選擇連接埠，或者從顯示列表中選擇一個既有的群組位址。

點選 OK 鈕使設定生效。點選 Reload 鈕，頁面將會重新載入，更新成目前的設定。

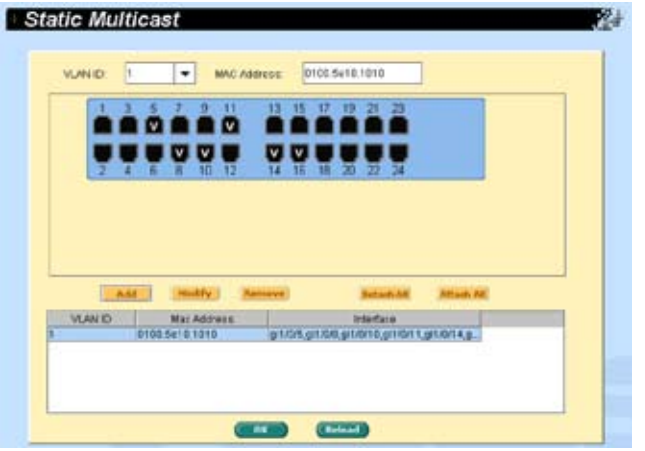

圖 37. 靜態多重播送

4.8.6 IGMP 偵聽（IGMP snooping）

透過開啟或關閉 IGMP 偵聽功能，可以幫助減少網路中的多重播送流量。

第一部分提供以下功能設定：

Enable IGMP Snooping：開啟系統的 IGMP 偵聽功能，預設是關閉的。一旦開啟後，現有的 VLAN 群組將會全部被偵聽。

若系統偵聽功能沒有開啟，您無法開啟 VLAN 偵聽功能。若系統偵聽功能開啟，您可以開啟或關閉 VLAN 偵聽功能。

Last Member Query Interval：如果沒有啟用即時離線（Immediate-Leave）功能，當交換器從某個連接埠收到使用者的 IGMP Leave 封包時，不會立即離線。它會傳送一個 IGMP Query 到該連接埠，並等待此 IGMP 群組成員回覆。如果在設定的時間內，沒有收到回覆，該接收埠將從這個多重播送的群組成員中刪除。

第二部分提供以下功能設定：

Status：如果系統偵聽功能已開啟，您可以開啟或關閉 VLAN 偵聽功能。

Immediate leave：開啟後，當交換器在某連接埠接收到某個多重播送群組的 IGMP V2 Leave 封包時，會立即將該埠從群組中刪除。只有當選定的 VLAN

在每個連接埠只有一台主機的情況下，此功能才應該被啟用。僅支援 IGMP V2 的主機才可搭配使用。

然而 ,如果靜態群組設定占滿了全部 256 個位址空間 ,IGMP 偵聽將無法正常運作。本交換器只允許 256 個第二層多重播送群組。

點選 OK 鈕使設定生效。點選 Reload 鈕，頁面將會重新載入，更新成目前的設定。

圖 38. IGMP 偵聽 - 設定

Multicast Group 頁面顯示了所有的多重播送群組資訊，包括靜態設定的與動態偵聽到的。

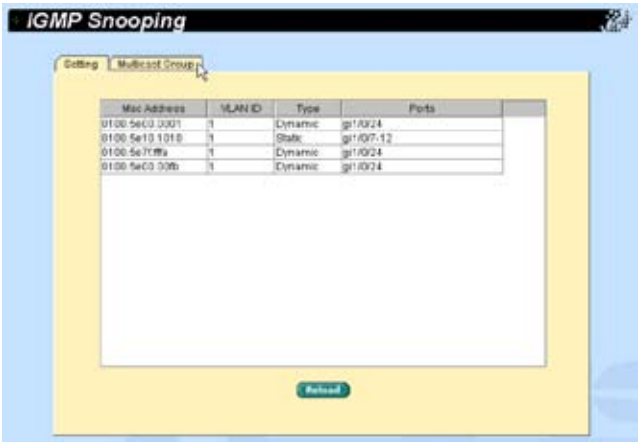

圖 39. IGMP 偵聽 - 多重播送群組

4.8.7 流量控制（Traffic control）

流量控制（Traffic control）可防止湧入過多的泛流（flooding）封包，如廣播封包、多重播送封包與目的地位址尋找失敗的單一播送封包等，避免系統頻寬異常負荷。本頁面中所設定的數量為該類型之封包每秒收到的上限。例如，若開啟了廣播與多重播送，則這兩種封包每秒收到的量均不會超過分別設定的值。

Broadcast：選擇關閉該功能或輸入一個數作為廣播封包的速度限制值。

Multicast：選擇關閉該功能或輸入一個數作為多重播送封包的速度限制值。

Destination Lookup Failure：選擇關閉該功能或輸入一個數作為目的地位址尋找失敗封包的速度限制值。

選擇一個連接埠並進行需要的設定，然後點選 Modify 鈕。

點選 OK 鈕使設定生效。點選 Reload 鈕，頁面將會重新載入，更新成目前的設定。

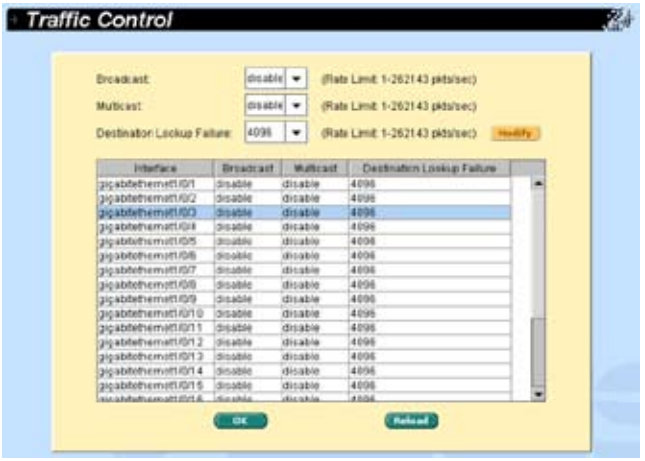

圖 40. 流量控制頁面

4.8.8 動態位址（Dynamic addresses）

本頁面顯示了依據連接埠、VLAN ID 或指定的 MAC 位址來搜尋動態 MAC 位址的結果。動態 MAC 位址是交換器自動學習的 MAC 位址，若該位址在其存在時間內，沒有被交換器再次學習，該位址就會從位址表中刪除（age out）。使用者可以輸入一個 10-1,000,000 範圍內的值（單位為秒），即可設定位址的汰換時間。點選 OK 鈕使設定生效。點選 Reload 鈕，頁面將會重新載入，更新成目前的設定。

您可以透過連接埠 VLAN ID 與／或 MAC 位址來搜尋 MAC 位址 然後點選 Query 鈕。位址視窗將顯示搜尋結果。

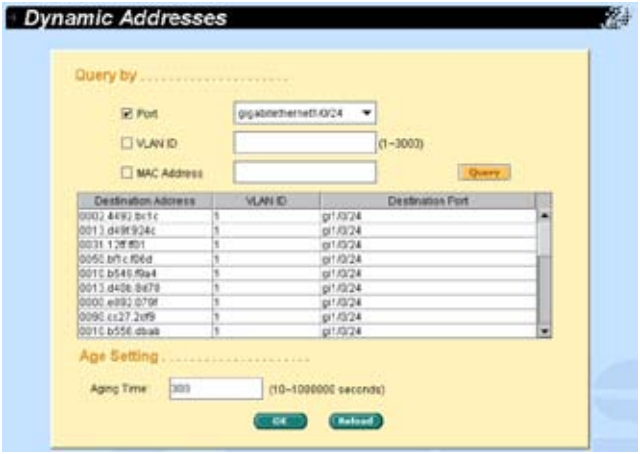

圖 41. 動態位址

4.8.9 靜態位址（Static addresses）

您可以將 MAC 位址添加到交換器的位址表中。透過這種方式添加的 MAC 位址將不會被汰換(age out) 我們稱其為靜態位址 。本交換器允許使用 1024 個靜態位址。

MAC Address：輸入 MAC 位址。

VLAN ID：輸入此 MAC 位址所處的 VLAN 群組。

Stack ID：選擇 stack ID。在單部交換器模式下，這個值保持為 1。

Port Selection：選擇此 MAC 位址所處的連接埠。

當您依據上述資訊建立了一個新的靜態 MAC 位址時，請點選 Add 鈕。然後您將在位址視窗中看到這個新增的位址。

您可以用滑鼠選定一個既有的位址，然後點選 Remove 鈕，即可刪除這個位址。Modify 鈕可更新既有的 MAC 位址。點選 OK 鈕使設定生效。點選 Reload 鈕，頁面將會重新載入，更新成目前的設定。

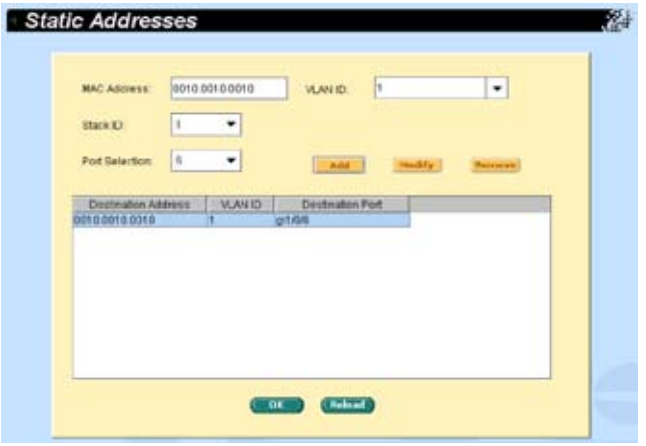

圖 42. 靜態位址

4.8.10 VLAN 設定（VLAN configuration）

您可以設定最多 3000 個 VLAN 群組，並顯示於本頁面中。VLAN1 是預設的 VLAN，是由系統建立的，無法被刪除，這可避免交換器運作不正常。除了預設的 VLAN1 以外，您可以刪除其他任何一組既有的 VLAN。

您可以透過按連接埠按鈕來指定該埠為已標記（tagged）或未標記（Untagged）。在連接埠選擇面板上有三種類型的按鈕：

"P" type：設定連接埠的預設 VLAN ID。如果連接埠接收到未標記的封包，這些封包將被視為屬於預設 VLAN 群組。

"U" type：未標記的連接埠，從該連接埠傳送出去的封包會被刪除 VLAN 標記（tag）。

"T" type：自本連接埠傳送出去的封包都會被標記。

"blank" type：本連接埠並不屬於此 VLAN 群組。

如果一個未標記的連接埠同時屬於兩個或更多的 VLAN 群組，將有可能造成交換器的混亂並導致流量擁塞。要避免這類狀況，交換器只允許某個未標記的連接埠在同一時間內只屬於一個 VLAN。

若您想要將一個未標記的連接埠從一個 VLAN 設定到另一個 VLAN，您必須先將其從原有的 VLAN 中刪除，或在原有 VLAN 中將其設為已標記狀態。

VLAN ID：建立新群組時，必須填入 VLAN ID。

Name：設定此 VLAN 的名稱。

點選 OK 鈕使設定生效。點選 Reload 鈕，頁面將會重新載入，更新成目前的設定。

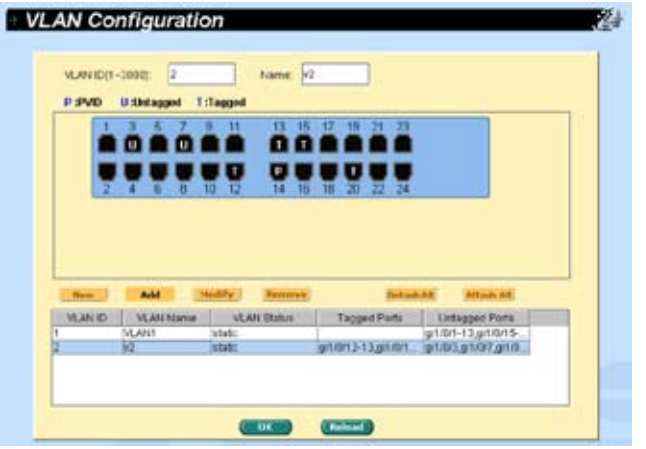

圖 43. VLAN 設定

4.8.11 GVRP

GARP (Generic Attribute Registration Protocol) VLAN Registration Protocol (GVRP) 是 IEEE 802.1Q 標準定義的應用程式，提供 VLAN 相關控制。

GVRP 僅能在 802.1Q 幹線連接埠上運作，主要是用來去除一些不需要在幹線交換器之間傳遞的 VLAN 封包。以下是 GVRP 的設定參數：

GVRP Enable：交換器的 GVRP 預設是沒有開啟的。您必須先開啟此功能，這樣對 802.1Q 連接埠設定的 GVRP 參數才會生效。

Port Mode：對個別的 802.1Q 幹線連接埠開啟／關閉 GVRP。GVRP 必須在幹線的兩端都進行設定，才能使幹線正常運作。

Registration：在預設狀況下，GVRP 連接埠為正常（Normal）註冊模式。這些連接埠透過從鄰近交換器上得到的 GVRP Join 資訊，來增加或刪除在 802.1Q 幹線連線上運作的 VLAN。若裝置的另一端無法傳送 GVRP 資訊，或者您不想讓交換器整合 VLAN 群組，請使用固定（Fixed）模式。在 Fixed 模式中，連接埠只會將目前存在於交換器中的 VLAN 群組傳遞出去。而在禁止（Forbidden）模式下的連接埠只轉發 VLAN 1。

點選 OK 鈕使設定生效。點選 Reload 鈕，頁面將會重新載入，更新成目前的設定。

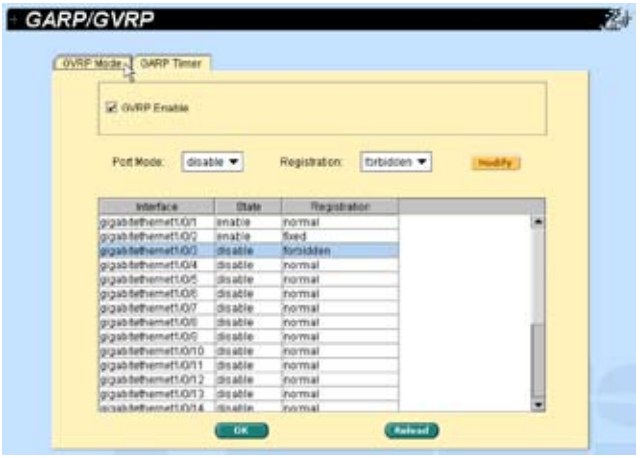

圖 44. GVRP 模式

如果需要，您可以編輯以下內容：

Joint Timer：以百分之一秒為單位設定數值。

Leave Timer：以百分之一秒為單位設定數值。

LeaveAll Timer：以百分之一秒為單位設定數值。

點選 OK 鈕使設定生效。點選 Reload 鈕，頁面將會重新載入，更新成目前的設定。

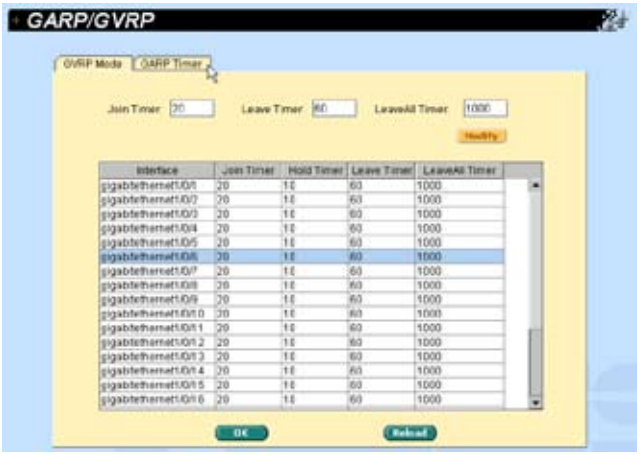

圖 45. GARP 計時器

4.8.12 QoS 與 CoS

4.8.12.1 802.1p 優先權

本交換器的每個連接埠支援 8 個傳出佇列。這些佇列可以設定為全部採用權重循環排序（Weight Round Robin，WRR），或其中一個佇列為絕對優先佇列（strict priority queue），其他佇列採用權重循環排序 (WRR)。絕對優先佇列的封包被傳送完之後，才輪到其他佇列的封包被傳送。您可以使用絕對優先佇列來傳送那些重要的或是有時效性的流量。以下有三個選項：

First Come First Service：先到的封包具有最高的優先權。

High Priority First：封包的優先權取決於其 CoS 數值。

Weighted Round Robin (WRR)：若開啟了 WRR 演算法，權重比率即為每個佇列中 WRR 演算法的封包被傳送頻率的比率。

點選 OK 鈕使設定生效。點選 Reload 鈕，頁面將會重新載入，更新成目前的設定。

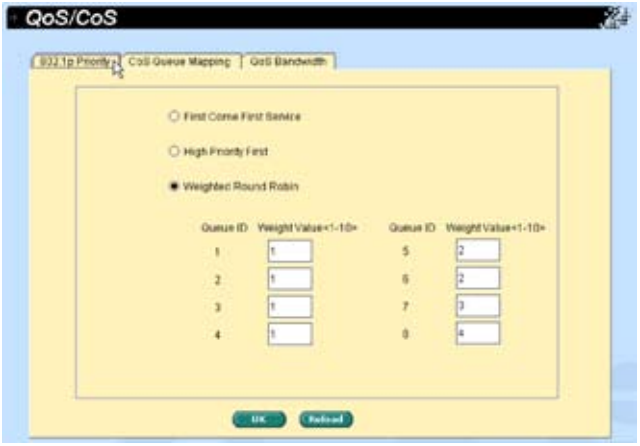

圖 45. 802.1p 優先權

4.8.12.2 CoS 佇列映像

採用絕對優先權排序時，GigaX2124 每個連接埠支援 8 個傳出佇列。也就是說，每一個 CoS 數值都可以映射至這 8 個佇列之一。佇列 8 具有最高的優先權來傳送封包。點選 OK 鈕使設定生效。點選 Reload 鈕，頁面將會重新載入，更新成目前的設定。

CoS 數值範圍從 1 至 8，其中，1 代表最低優先權，8 代表最高優先權。

圖 46. CoS 佇列映射

4.8.12.3 QoS 頻寬（QoS bandwidth）

本頁面可對連接埠進行一些與 VLAN 標記相關的設定，包括：

Port：從列表視窗中選擇一個連接埠進行設定。

Ingress Bandwidth：選定連接埠的最大傳入頻寬。

Egress Bandwidth：選定連接埠的最大傳出頻寬。

Default CoS：從這個連接埠接收到的未標記封包在 VLAN 標記中都會被指定為此 CoS 數值。

點選 Modify 鈕更改連接埠列表視窗中的內容。點選 OK 鈕使設定生效。點選 Reload 鈕，頁面將會重新載入，更新成目前的設定。

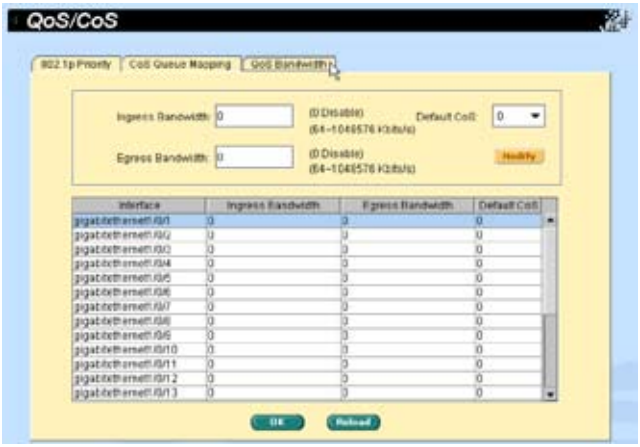

圖 47 QoS 頻寬

4.8.13 策略圖表 (Policy Map)

在 Policy Map 頁面，使用者可以更改傳入或傳出封包的優先權，也可在超過負荷時丟棄封包。

4.8.13.1 策略圖表設定

為策略圖表設定一個名稱然後點選 Add 鈕。點選 OK 鈕永久儲存設定，或點選 Reload 鈕，頁面將會重新載入，更新成目前的設定。在編輯策略組合規則之前請點選 OK 鈕。

點選您想要編輯或刪除的策略圖表組合。然後，點選 Edit 鈕進入規則設定頁面，或點選 Remove 鈕刪除圖表組合。請依照前面敘述的操作方法來設定策略圖表。

圖 48. 策略圖表組合

在規則設定時，提供四個標準 (Criterion) 選擇和三種動作 (Action) 設定：

Match Criterion：您可以選擇 IP DSCP 並輸入範圍，也可選擇 IP Precedence 並輸入範圍，或者，選擇 ACL name 並輸入一個既有的過濾存取列表，或選擇 None。

Profile Action：您可以選擇 Police Drop、Police High-Drop 或 None。

In-Profile Action：選擇 CoS Override 並輸入 COS 值、Mark IP SCP、Mark IP Precedence 或 None 來對傳入封包進行處理。

Out-Profile Action：選擇 Drop、IP DSCP 或 None 來處理傳出封包，並可設定 Rate 和 Burst Size。

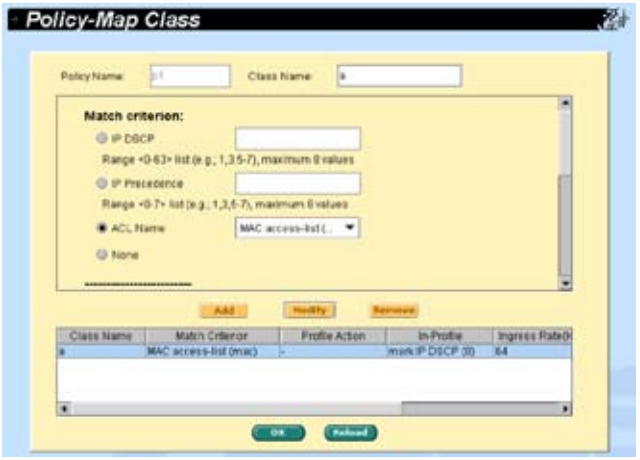

圖 49. 策略圖表類型

4.8.13.2 附加策略 (Policy Attach)

若您沒有將策略圖表組合附加到任何一個連接埠，則這個策略圖表組合是不會有作用的。使用 Policy Attach 頁面來將策略圖表組合附加到連接埠。

選擇一個既有的策略圖表組合，然後點選需要套用此策略圖表組合的連接埠。

點選 OK 鈕使設定生效。點選 Reload 鈕，頁面將會重新載入，更新成目前的設定。

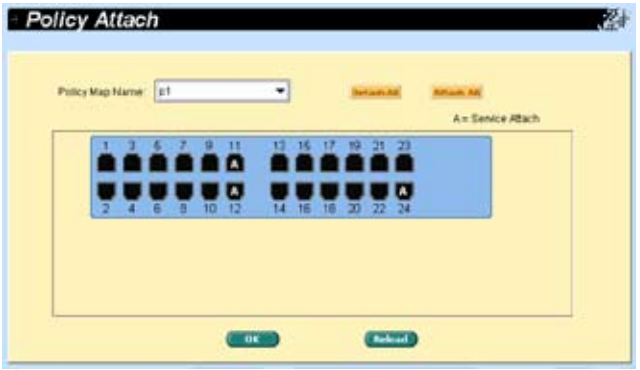

圖 50. 策略附加

4.9 簡單網路管理協定（SNMP）

圖 51. SNMP 選單

本群組提供包括群組列表（Community Table）、主機列表（Host Table）與 Trap 設定（Trap Setting）在內的 SNMP 設定。

4.9.1 群組列表（Community Host Table）

本頁面將主機 IP 位址與群組名稱聯繫起來。輸入一個 IP 位址，輸入群組名稱並從下拉選單中選擇群組類型。“ro” 代表只讀，“rw” 代表讀／寫。點選 OK 鈕使設定生效。點選 Reload 鈕，頁面將會重新載入，更新成目前的設定。

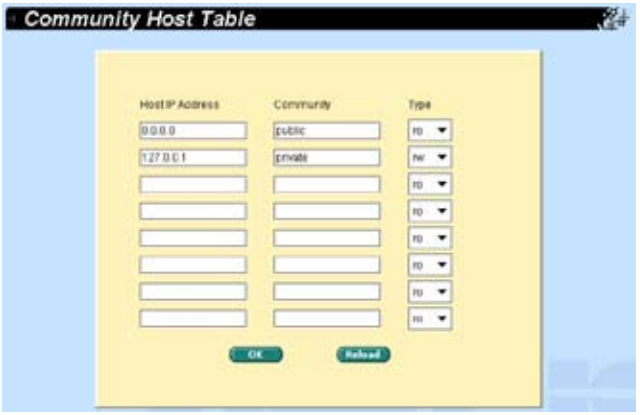

圖 52. 群組主機列表頁面

4.9.2 Trap 設定（Trap setting）

透過設定 Trap 目的地 IP 位址與群組名稱，您可以開啟 SNMP Trap 功能來傳送不同版本的 Trap 封包 (v1 或 v2c)。

點選 OK 鈕永久儲存設定，或點選 Reload 鈕，頁面將會重新載入，更新成目前的設定。

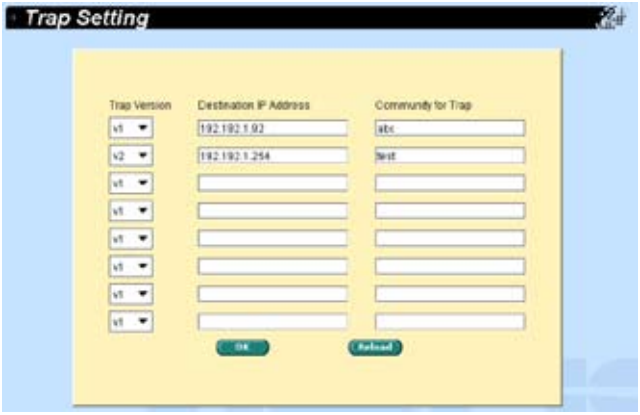

圖 53. Trap 設定頁面

4.9.3 SNMPv3 VGU 列表

這裡有兩項 SNMPv3 定義的新安全功能。一為 USM（User-based Security Model，以使用者為基礎的模型），可提供 SNMPv3 封包的認證、加密與解密。二為 VACM（View-based Access Control Model，以檢視為基礎的存取控制模型），可提供存取控制。以下為相關的三個頁面。點選 OK 鈕使設定生效。點選 Reload 鈕，頁面將會重新載入，更新成目前的設定。

4.9.3.1 檢視（View）

VACM 檢視用來查看 SNMPV3 VACM 群組資訊。

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 資訊中的 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 資訊中的 Oid 相符合。當子樹短於 SNMPv3 資訊中的 Oid 時，就算是符合。

當您透過上述資訊建立一組新的 VACM 檢視項目後，點選 Add。然後您將看到新增的項目顯示在檢視視窗中。您可以用滑鼠選定一個既有項目，並點選 Remove 鈕將其刪除。點選 Modify 鈕可將修改過的設定顯示在 VACM 檢視項目。點選 OK 鈕使設定生效。點選 Reload 鈕，頁面將會重新載入，更新成目前的設定。

圖 54. SNMPv3 VGU 列表 - 檢視

4.9.3.2 群組（Group）

VACM 群組用來設定 SNMPv3 VACM 群組。

Group Name：輸入安全群組名稱。

Security Model：輸入群組所屬的安全模型名稱（Security Model Name）。 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名稱（Security level Name）。可選的項目有 NoAuth，AuthNopriv 與 AuthPriv。

Read View Name：輸入群組所屬的讀取檢視名稱。相關的 SNMP 資訊有：Get，GetNext，GetBulk。

Write View Name：輸入群組所屬的寫入檢視名稱。相關的 SNMP 資訊為 Set。

Notify View Name：輸入群組所屬的通知檢視名稱（Notify View Name）。相關的 SNMP 資訊為 Trap，Report。

當您透過上述資訊建立一個新的 VACM 群組後，請點選 Add 鈕。然後您將看到新增的項目顯示在檢視視窗中。您可以用滑鼠選定一個既有群組，並點選 Remove 鈕將其刪除 點選 Modify 鈕可更新既有 VACM 群組項目 點選 OK 鈕使設定生效。點選 Reload 鈕，頁面將會重新載入，更新成目前的設定。

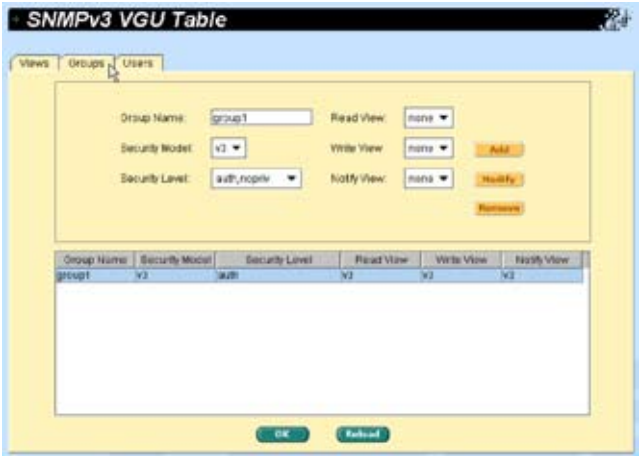

圖 55. SNMPv3 VGU 列表 - 群組

4.9.3.3 使用者（User）

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

User Name：指定安全群組的使用者名稱。

Group Name：輸入安全群組的名稱

Security level：輸入群組所屬的安全性等級名稱（Security level Name）。 可選的項目有 NoAuth，AuthNopriv 與 AuthPriv。

Auth Algorithm：輸入 SNMP 使用者和安全群組所屬的認證協定（Auth Protocol），可選的項目有 NoAuth，MD5 與 SHA1。若選擇了 NoAuth，則不需要輸入密碼。

Auth Password：輸入認證演算法（Auth Algorithm）的密碼。此密碼至少為 8 位數的數字或字符。

Priv Algorithm：輸入 SNMP 使用者和安全群組所屬的 Priv Protocol。可選的項目有 NoPriv 與 DES。若選擇了 NoPriv，則不需要輸入密碼。

Priv Password：輸入 Priv Protocol 的密碼。此密碼至少為 8 位數的數字或字符。

當您透過上述資訊建立一組新的 VACM 群組項目後，點選 Add 鈕。然後您將看到新增的項目顯示在群組視窗中。您可以用滑鼠選定一個既有群組，並點選 Remove 鈕將其刪除。點選 Modify 鈕可更新既有 VACM 群組項目。點選 OK 鈕使設定生效。點選 Reload 鈕，頁面將會重新載入，更新成目前的設定。

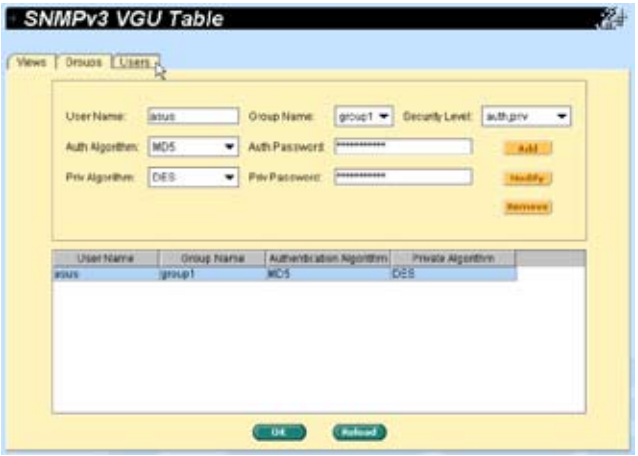

圖 56. SNMPv3 VGU 列表 - 使用者

4.10 過濾（Filter）

圖 57. 過濾選單

本交換器可根據第二層至第四層封包的頭資訊來過濾某些封包類型。每個過濾設定都包含多個規則。您需要將過濾設定套用至某些連接埠才能使過濾功能生效。

4.10.1 過濾組合（Filter set）

本交換器定義了兩種規則模式，一種為 MAC 模式，另一種為 IP 模式。只有相同的規則模式可以相互組合形成一組過濾設定。 每種模式具有不同的過濾選項。例如，您可以使用 IP 模式來過濾 FTP 封包。

您可以選擇 MAC Filter 並命名，然後點選 Add 來新增一組 MAC 過濾規則。 您也可以勾選 IP Filter 並指定其 ID/ 名稱。IP Filter Standard 與 IP Filter Extended 的區別在於，Extended 模式可以設定更多複雜的規則。設定過濾模式和名稱後，點選 Add 鈕。點選 OK 鈕永久儲存設定，點選 Reload 鈕，頁面將會重新載入，更新成目前的設定。在編輯前請點選 OK 鈕。

點選您需要編輯或刪除的過濾設定。然後點選 Edit 鈕進入規則頁面。或點選 Remove 鈕刪除該過濾設定。您必須遵照以下規則來建立一組有效的過濾設定。

一個過濾設定組合由一種類型的規則構成。在相同範圍內過濾封包的規則屬於同一類型。例如，兩個規則都是用目的地 IP 位址過濾封包，則它們屬於同一類型。但是用來源 IP 位址過濾封包的規則就不屬於同一類型。

規則類型的數量是有限制的。開啟交換器的一些特殊功能可能會減少這一數量。若已沒有可用的類型，系統會出現警告資訊，而規則也將無法設定。

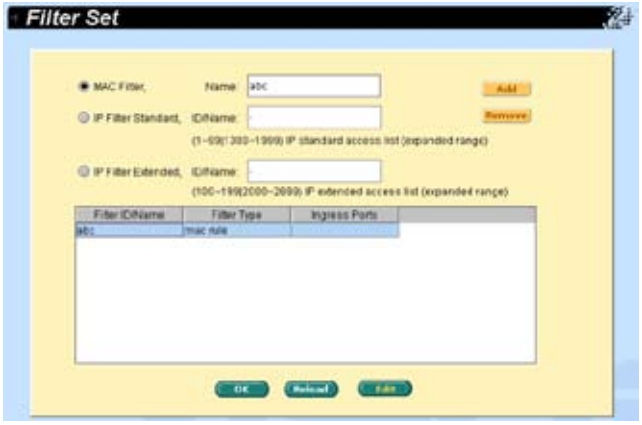

圖 58. 過濾組合

過濾規則（Filter Rule）頁面提供了規則模式的選項，一種為 MAC 規則，另一種為 IP 規則。 使用者可以設定 MAC 位址，VLAN ID 與 CoS 值。若您沒有在空白欄位輸入 MAC 位址，則代表此規則對所有的 MAC 位址有效。在 IP 規則設定中，您可以輸入以下五種類型中的任一種：source IP（來源 IP 位址），destination IP（目的地 IP 位址），protocol（協定），source application port（來源應用連接埠）與 destination application port（目的地應用連接埠）。在 Action 欄位，您可以選擇要轉發或丟棄符合規則的封包。若一個封包符合兩種規則，且這兩種規則對應不同的動作，封包將依據規則列表中顯示的第一個規則來運作。

圖 59. MAC 模式下的過濾規則

圖 60. IP 模式下的過濾規則

以下兩種方式告訴您如何提供 IP：

1. 指定一個專用 IP， Type = subnet，IP = 10.10.1.2，Wildcard = 0.0.0.0
2. 指定一個子網路（一組 IP），Type = subnet，IP = 10.10.1.0，Wildcard = 0.0.0.255

4.10.2 附加過濾規則（Filter attach）

一組過濾規則若是沒有套用到任何連接埠，那麼這組規則並不會運作。請使用 Filter Attach 頁面來將過濾規則附加到交換器的傳入連接埠。

點選 OK 鈕使設定生效。點選 Reload 鈕，頁面將會重新載入，更新成目前的設定。

您可以用下列方法將過濾規則附加到連接埠：

Filter ID/Name：選擇一個過濾規則的 ID 或名稱。

Attach to all ports：套用過濾規則至系統中所有的連接埠。

Attach to certain ports：套用過濾規則至指定的連接埠。

Detach from all ports：將原有已套用過濾規則的連接埠取消套用規則。

使用 "Attach All" 指令過後， 您將無法刪除指定的連接埠的過濾規則。若您需要刪除規則，請使用 "Detach All" 指令。

當過濾規則套用到傳入連接埠，則會根據套用的規則來過濾連接埠所收到的封包。例如，某過濾規則附加於傳入連接埠 3，僅過濾目的地 MAC 位址為 00:10:20:30:40:50 的封包。則來自連接埠 3 且目的地 MAC 位址為 00:10:20:30:40:50 的封包將不會被傳送。

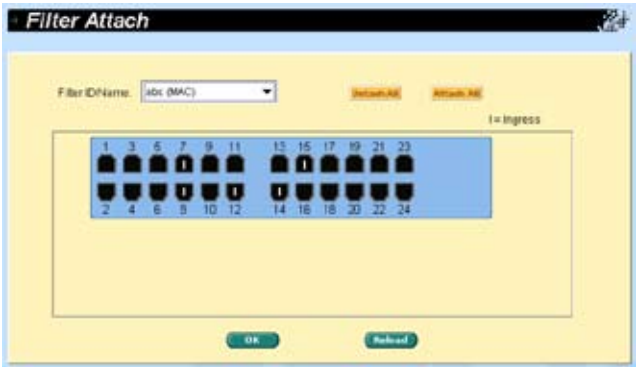

圖 61. 過濾規則附加

4.11 安全（Security）

圖 62. 安全選單

本交換器支援 802.1x 以連接埠為基礎的安全功能。只有認證過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 指定。關於使用者／連接埠的資訊必須要先在認證伺服器上設定。

4.11.1 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 伺服器或本地資料庫來認證連接埠的使用者。

第一部分是橋接 (Global) 設定：

Sys-Auth-Control：選擇本項目開啟認證。

Authentication Method：RADIUS 或本地資料庫可用來認證連接埠的使用者。

第二部分為連接埠設定。當您完成修改後，請點選 Modify 鈕：

Port：從連接埠列表視窗中選擇需要設定的連接埠。

Host Mode：若選擇了“multi-host”，則連接到選定連接埠的所有主機中，只要有一部主機透過了認證，則所有主機都允許使用這個連接埠。若選擇了“single-host”，則只有通過認證的那部主機可以使用這個連接埠。

Authentication Control：若選擇了“force-authorized”，選定的連接埠會被視為已經通過認證。因此，所有主機的流量都被允許通過。否則，若選擇了“force-unauthorized”，選定的連接埠是被封鎖的，不允許任何流量通過。若選擇了“Auto”，該連接埠的動作由 802.1x 協定來控制。在正常情況下，所有的連接埠都應該設定為“Auto”。

Reauthentication:開啟本項目後， 交換器會在重新認證時間（ReAuthentication Time）到時，嘗試重新認證連接埠的使用者。

ReAuthentication Time：若“Reauthentication”項目已開啟，ReAuthentication Time（重新認證時間）指的是交換器重新傳送認證請求到連接埠使用者的時間間隔。

Quiet Period：若認證失敗，交換器再次傳送認證請求到連接埠使用者前需要等待的時間。

Guest Vlan：指定一個訪客（Guest）VLAN 給不相容於 802.1x 的用戶端。

點選 OK 鈕使設定生效。點選 Reload 鈕，頁面將會重新載入，更新成目前的設定。

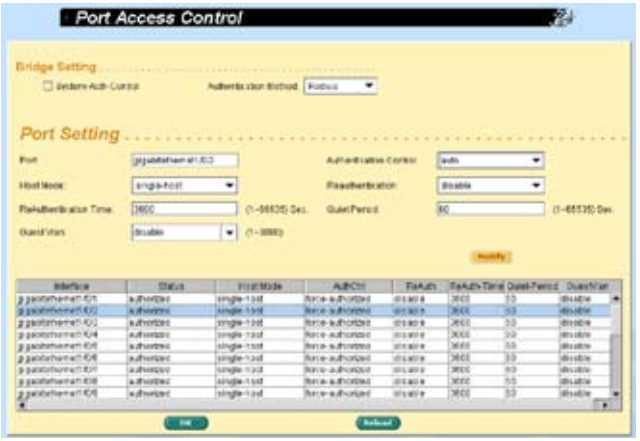

圖 63. 連接埠存取控制

4.11.2 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。

User Name：新的使用者名稱稱。

Password：新使用者的密碼。

Confirm Password：再次輸入密碼。

VIan ID：指定 VLAN ID 給 802.1x 認證的使用者。

請點選 Add 鈕來添加使用者。當您完成修改後，點選 Modify 鈕。若您想要刪除選定的使用者，請點選 Remove 鈕。

點選 OK 鈕使設定生效。點選 Reload 鈕，頁面將會重新載入，更新成目前的設定。

圖 64. 撥入使用者

4.11.3 RADIUS

若要使用外部 RADIUS 伺服器，您需要設定以下參數：

Authentication Primary/Secondary Server IP：主要／次要 RADIUS 伺服器的 IP 位址。

Authentication Primary/Secoondary Server Port：主要／次要 RADIUS 伺服器偵聽的連接埠埠號。

Authentication Primary/Secondary Server Key：用於在 GigaX2124 與主要／次要 RADIUS 伺服器之間進行通訊的密鑰。

Confirm Authentication Key：再次輸入上述密碼。

連接至交換器之 RADIUS 伺服器必須與系統管理埠位於同一個 VLAN 內。

點選 OK 鈕使設定生效。點選 Reload 鈕，頁面將會重新載入，更新成目前的設定。

圖 65. RADIUS

4.11.4 連接埠安全（Port security）

本交換器也支援連接埠安全（Port security）功能。它允許系統管理員來控制哪些使用者可以連線到他們的網路。您可以使用連接埠安全功能來指定可存取該連接埠主機的 MAC 位址，並設定允許通過的位址數量。當您指定了一個安全連接埠的安全 MAC 位址後，該連接埠將不會轉發除了已定義的來源位址群組之外的任何封包。這樣就降低了未經認證的裝置使用我們的網路進行惡意行為的可能性。

4.11.4.1 連接埠設定（Port configuration）

本頁面用來進行連接埠安全設定。

首先，您必須從顯示列表中點選一個連接埠。然後，開始進行連接埠設定。修改完成後點選 Modify 鈕：

Admin：開啟或關閉連接埠安全功能。

Violation Mode：本項用來設定當違反安全設定時連接埠的動作。若選擇“Shutdown”，連接埠將變成封鎖狀態，系統將記錄資訊，Violation 計數器的數值會增加。若選擇“Restrict”，系統將會記錄資訊，Violation 計數器的數值會增加。若選擇“Protect，當有違反安全設定的事件發生時，您將不會被通知。

Max MAC Address：在這個連接埠上安全 MAC 位址的最大數量。有效設定數值是由 1 至 256，系統中的總數為 1024。

Aging Time：連接埠上安全 MAC 位址的汰換時間。超過了這段時間後，該埠的動態安全 MAC 位址就會從安全 MAC 位址表中刪除。有效的設定範圍是由 0 至 1440(mins)。若設定的時間為 0，則該連接埠的汰換時間機制沒有開啟。

Aging Type：此選項決定了安全 MAC 位址的汰換方式。若選擇“Absolute”，連接埠的安全位址在汰換時間到後會被刪除。若選擇“Inactivity”，當指定的時間內沒有來自該安全 MAC 位址的流量，才會被刪除。

點選 OK 鈕使設定生效。點選 Reload 鈕，頁面將會重新載入，更新成目前的設定。

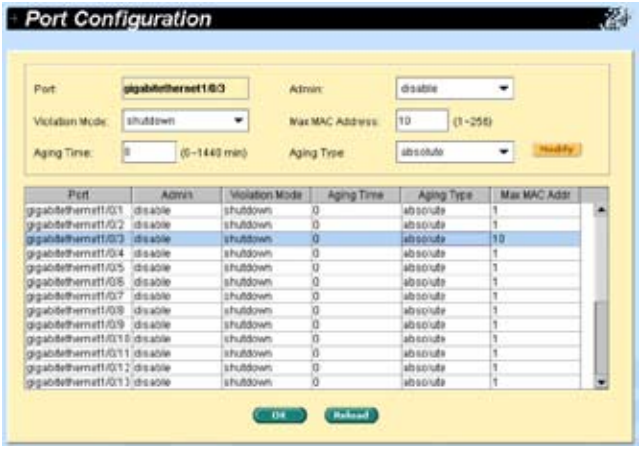

圖 66. 連接埠設定

4.11.4.2 連接埠狀態（Port status）

本頁面顯示了目前的連接埠狀態，MAC 位址數量，靜態 MAC 位址數量，以及違反安全設定的事件數量。

連接埠有五種狀態：

NoOper：表示連接埠的安全功能沒有開啟。

SecureUp：表示連接埠安全功能運作中。

SecureDown：表示連接埠的安全功能無法運作。這種狀況一般為開啟了連接埠安全功能，但由於某些原因（如與其他功能衝突）而無法正常運作。

Restrict：當 Violatioon mode 設定為 "restrict" 時，連接埠出現了違反安全設定的狀況。

Shutdown：當 Violatioon mode 設定為 "Shutdown" 時，連接埠出現了違反安全設定的狀況。

若某些連接埠狀態為 “Shutdown”，您可以點選它並選擇 “Re-Start” 為 “Yes”。這將重新開啟連接埠並將其狀態改為 “SecureUp”。當您修改完成後，請點選 Modify 鈕。

點選 OK 鈕使設定生效。點選 Reload 鈕，頁面將會重新載入，更新成目前的設定。

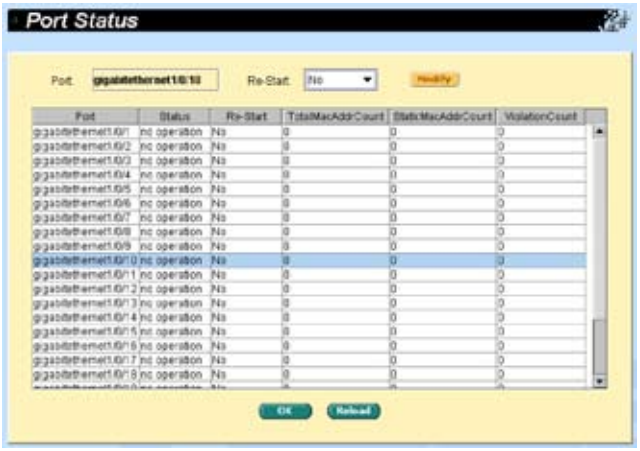

圖 67. 連接埠狀態

4.11.4.3 安全 MAC 位址（Secure MAC address）

安全 MAC 位址（Secure MAC Address）提供了三種管理功能：

Query：您可以在“Port Selection”欄位選擇一個連接埠。點選 Query 鈕後，將顯示該連接埠的所有 MAC 位址。

Add：使用者可以在“Port Selection”欄位選擇一個連接埠，然後在“MAC Address”欄位輸入一個 MAC 位址，並點選 Add 鈕，即可將該位址添加至連接埠。新增的位址為靜態 MAC 位址。

Remove：您可以使用“Query”功能來顯示某連接埠上的所有 MAC 位址。從列表中選擇一個 MAC 位址並按下 Remove 鈕，即可立刻刪除該位址。

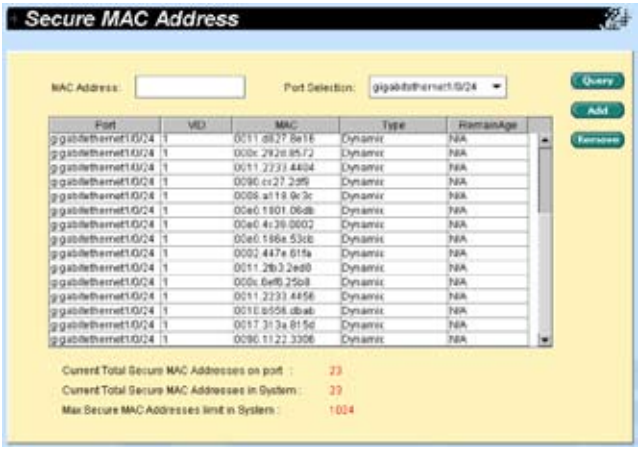

圖 68. 安全 MAC 位址

4.12 流量統計圖表（Traffic chart）

圖 69 流量統計圖表選單

流量統計圖表（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 來設定從交換器更新資料的時間間隔。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 鈕使瀏覽器產生統計圖表。每次點選 Draw 鈕都會重置統計結果的顯示。

4.12.1 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。

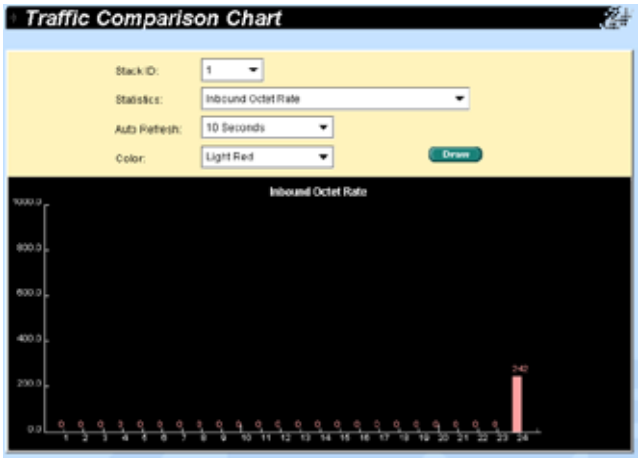

圖 70. 流量比較

4.12.2 錯誤群組（Error group chart）

選擇連接埠和顯示顏色（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 71. 錯誤群組

4.12.3 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。

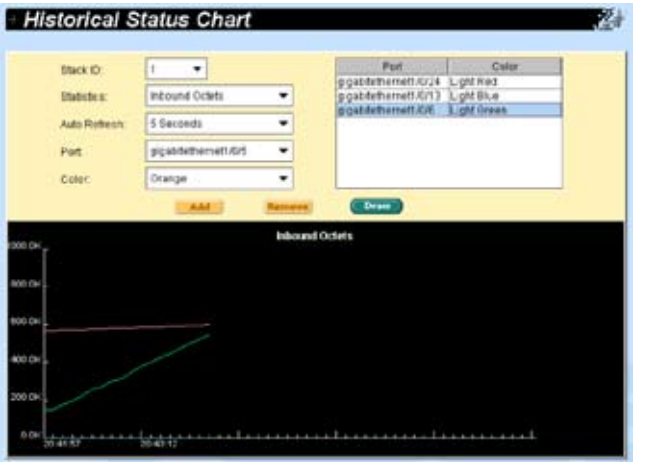

圖 72. 歷史狀態

第五章　控制終端介面（Console interface）

本章節將會介紹如何使用控制終端介面來設定交換器。本交換器提供 RS232 與 USB 連接埠來與您的 PC 相連接。您的 PC 需要執行終端模擬軟件，如 HyperTerminal，以及指令翻譯器來對交換器進行設定。您必須將傳輸速率設為 9600，8 個資料位，無同位檢查，1 個停止位，無流量控制。

當您進入 CLI 模式後，輸入“?”將顯示所有可用的指令說明資訊。若您對於 CLI 指令不熟悉，這將是非常有用的資訊。所有的 CLI 指令都區分大小寫。

5.1　開機自我檢測（Power-on self test）

POST（開機自我檢測）是在系統啟動時進行的。它測試系統內存、LED 指示燈與交換器主機板上的硬體晶片。系統測試和初始化完成之後會顯示系統資訊。您可以忽略這些資訊直到出現“ASUS>:”提示符。

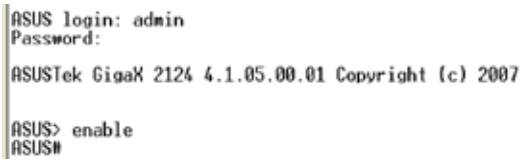

圖 73. CLI 介面

5.1.1　Boot ROM 指令模式

在 POST 過程中， 您可以按下 <ENTER> 鍵來進入“Boot ROM Command”模式。輸入“?”可顯示所有可用指令的說明資訊。

盡管這些指令在有些情況下相當有用，但如果您不了解這些指令的功能，我們強烈建議您不要使用它們。

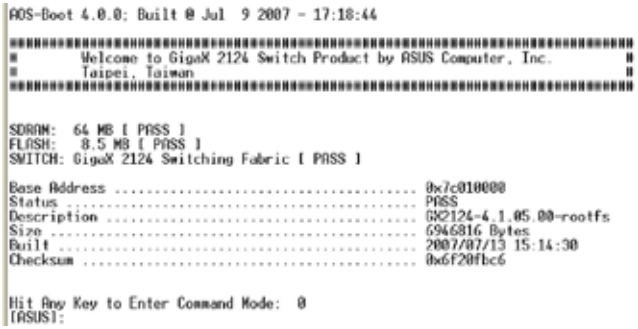

圖 74. Boot ROM 指令模式

5.1.2 Boot ROM 指令

以下為 Boot ROM 指令的兩種類型：

- “command”：顯示當前設定。
- “command” + 新設定：用指定的新設定代替當前設定。

表 7. Boot ROM 指令

指令	參數	參數舉例	說明
baudrate	Baud rate	9600, 19200, 38400, 57600, 115200	您需要將終端模擬軟件設為相同的鮑率。
ethaddr	none	none	取得 MAC 位址
gatewayip	IP address	xxx.xxx.xxx.xxx	設定閘道的 IP 位址
go	none	none	啟動韌體映像
? or help	none	none	顯示線上說明
ipaddr	IP address	xxx.xxx.xxx.xxx	設定 TFTP 用戶端的 IP 位址
xload	none	none	載入二進位文件 load binary file over serial line (X modem)
ping	host	xxx.xxx.xxx.xxx	傳送 ICMP echo_request 至主機
pwd	none	none	重置交換器密碼
serverip	IP address	xxx.xxx.xxx.xxx	設定 TFTP 伺服器 IP 位址
slot	slot	1, 2, auto	選擇啟動槽區
tftpboot	filename	如：firmware.img	搭配 TFTP 透過網路載入韌體映像
version	none	none	顯示 Boot ROM 版本

5.2 登入與登出

要進入 CLI 模式，您需要輸入一個有效的使用者名稱與密碼。首次登入時，您可以輸入“admin”作為使用者名稱（無需輸入密碼）。為了安全考慮，請在登入後修改使用者名稱與密碼。若您忘記了使用者名稱和密碼，您可以連絡華碩技術支援部門，或使用 Boot ROM 指令模式中的“pwd”指令來將使用者帳號回復至預設值。若您選擇第二種方法，使用者名稱將回復為“admin”。

輸入“exit”可安全地離開 CLI 模式。這個動作可在您離開的同時確保系統的安全。下一個使用者需要輸入經認證的使用者名稱與密碼才能登入。

5.3 CLI 指令

本交換器提供了一系列 CLI 指令，用於所有的管理功能。這樣，您可以根據提示，如同使用網頁介面一樣方便正確地進行交換器的設定。

使用“?”或“list”來取得可用的指令與說明。
使用“end”可返回根目錄（enable 模式）。

5.3.1 使用者帳號（User account）

5.3.1.1 新增使用者（add user）

新增使用者或修改既有使用者的密碼。

CLI 指令：add user user-name password

舉例：ASUS# configure terminal

ASUS(configure)#user add *admin 123*

5.3.1.2 刪除使用者（delete user）

刪除一個既有的使用者。

CLI 指令：delete user user-name

舉例：ASUS# configure terminal

ASUS(configure)# user delete *admin*

5.3.2 備份與回復（Backup and Restore）

5.3.2.1 備份啟動設定檔（Backup start-up configuration file）

備份交換器的啟動設定檔“startup_config”至 TFTP/FTP 伺服器。

CLI 指令：copy startup-config tftp: *URL*

舉例：ASUS# copy startup-config tftp: *192.168.8.56/backup.cfg*

CLI 指令：copy startup-config ftp: *[Username:Password@]URL*

舉例：ASUS# copy ftp: *asus:1234@192.168.1.2/backup.cfg startup-config*

5.3.3 系統管理設定（System management configuration）

5.3.3.1 開啟（enable）

進入開啟（enable）模式並開啟優先模式指令。

CLI 指令：enable

舉例：ASUS> enable

5.3.3.2 關閉（disable）

關閉優先模式並返回使用者模式。

CLI 指令：disable

舉例：ASUS# disable

5.3.3.3 韌體更新（Firmware upgrade）

更新新的韌體至交換器。

CLI 指令：archive download-sw /overwrite tftp: *URL*

舉例：ASUS# archive download-sw /overwrite *tftp:192.168.1.3/firmware.img*

CLI 指令：archive download-sw /overwrite ftp: *[Username:Password@]URL*

舉　例：ASUS# archive download-sw /overwrite *ftp:asus@1234:192.168.1.3 /firmware.img*

5.3.3.4 設定終端（configure terminal）

進入設定模式來設定終端。

CLI 指令 : configure terminal

舉例 : ASUS# configure terminal

5.3.3.5 結束（end）

本指令可讓使用者結束當前模式並進入開啟（enable）模式。

CLI **指令：**end

舉例：ASUS# end

5.3.3.6 離開（exit）

本指令可讓使用者離開當前模式而進入前入一個模式。

CLI **指令：**exit

舉例：ASUS# exit

5.3.3.7 說明（Help）

本指令列出了操作模式下所有的指令。

CLI **指令：**list

舉例：ASUS# list

舉例：ASUS# ?

5.3.3.8 主機名稱（host name）

顯示交換器的名稱。這是 RFC-1213 定義的系統群組（System Group）中的 MIB 項目，在管理節點上提供管理資訊。

CLI **指令：**hostname *HOSTNAME*

舉例：(config)# hostname *Switch*

若您在名稱描述欄位內輸入了名稱，則交換器系統名稱將改為新設的名稱。

5.3.3.9 系統連絡資訊（System contact）

顯示交換器的詳細連絡資訊。這是 RFC-1213 定義的系統群組（System Group）中的 MIB 項目，在管理節點上提供連絡資訊。

CLI **指令：**snmp-server contact *string*

舉例：(config)# snmp-server *contact fae@loop.com.tw*

若您在若連絡資訊描述欄位內輸入了連絡資訊，則交換器的連絡資訊將改為新設的內容。

5.3.3.10 系統位置（System Location）

顯示交換器的實體位置。這是 RFC-1213 定義的系統群組（System Group）中的 MIB 項目，在管理節點上提供位置資訊。

CLI 指令：snmp-server location *string*

舉例：(config)# snmp-server location *Loop-Taipei*

在位置描述欄位內輸入位置描述資訊即可修改位置資訊。

```
Switch# configure terminal
Switch(config)# hostname Switch
Switch(config)# snmp-server contact my_contact_information
Switch(config)# snmp-server location enterprise_building_B1
Switch(config)#
```

圖 75. 系統指令

5.3.3.11 IP 位址與網路遮罩（IP address and network mask）

顯示交換器的 IP 位址。這個位址用於管理用途，如交換器的 http 伺服器、SNMP 伺服器、TFTP 伺服器、SSH 與 Telnet 伺服器等網路套用在 VLAN1 介面中都使用這個 IP 位址。

CLI 指令：ip address *A.B.C.D/M*

舉例：(config)# interface vlan *1*

(config-if)# ip address *192.168.20.121/24*

5.3.3.12 預設閘道（Default gateway）

顯示預設閘道的 IP 位址。若交換器所在的網路包含一個或多個路由器，則本項目必須設定。

CLI 指令：ip route *A.B.C.D/M (A.B.C.D|INTERFACE)*

舉例：(config)# ip route *0.0.0.0/0 192.168.1.2*

5.3.3.13 重新啟動（reboot）

使用本指令來重新啟動系統。

CLI 指令：reboot

舉例：ASUS# reboot

5.3.3.14 載入預設檔（reload default-config file）

這個指令用預設的設定檔來取代當前設定檔。要使預設的設定檔運作，交換器必須執行重新啟動指令。

CLI 指令：reload default-config file

舉例： ASUS# reload default-config file

5.3.3.15 顯示運作設定（show running-config）

顯示運作設定。

CLI 指令：show running-config

舉例： ASUS# show running-config

5.3.3.16 寫入（write）

用這個指令來將設定寫入到交換器設定檔。

CLI 指令：write

舉例： ASUS# write

5.3.3.17 指定一個新的使用者帳號（Assign a new user account）

如：新增一個使用者，名稱為 tony，密碼為 *tony123456*。

CLI 指令：user add *USERNAME PASSWORD*

舉例： user add *tony tony123456*

5.3.3.18 刪除一個使用者帳號（Delete a new user account）

如：刪除一個名稱為 *tony* 的帳號。

CLI 指令：user delete *USERNAME*

舉例： (config)#user delete *tony*

5.3.4 實體介面指令（Physical interface commands）

5.3.4.1 介面模式（Interface mode）

在交換器上使用自動協商（auto-negotiation）設定指令來設定連接埠的自動協商狀態。

CLI 指令 : auto-negotiation

舉例 : (config)# interface *gi1/0/2*

(config-if)# auto-negotiation

這個例子說明了如何使用交換器的自動協商設定指令來開啟自動協商模式。

5.3.4.2 介面雙工模式 (Interface duplex)

使用交換器的雙工設定指令來設定連接埠的雙工狀態。

CLI 指令 : duplex *(full | half)*

舉例 : (config)# interface fa1/0/2

(config-if)# duplex *full*

這個例子說明了如何使用交換器的雙工設定指令來設定連接埠的全雙工模式。

5.3.4.3 介面流量控制 (Interface flow control)

使用交換器的流量控制設定指令來設定連接埠的流量控制狀態。

CLI 指令 : flowcontrol (*rx| tx | both*)

舉例 : (config)# interface *gi1/0/2*

(config-if)# flowcontrol *both*

這個例子說明了如何使用交換器的流量控制設定指令來設定連接埠的流量控制。

5.3.4.4 顯示二層介面 (Show L2 interface)

使用交換器的顯示連接埠指令來顯示介面狀態。

CLI 指令 : show interfaces *IFNAME*

舉例 : ASUS# show interface *gi1/0/2*

5.3.5 IP 介面（IP interface）

5.3.5.1 顯示 VLAN 名稱列表（show vlan name string）

用顯示 VLAN 使用者 EXEC 指令來顯示交換器上已設定的所有 VLAN 或一個 VLAN（若 VLAN ID 或名稱已指定）的參數。

CLI 指令：show vlan name *VLANNAME*

舉例： ASUS# show vlan name *VLAN1*

VLAN 1 是用於系統用途，例如，用於韌體更新，管理，等等。

5.3.5.2 建立一個 VLAN 項目（Create a vlan entry）

使用 vlan vid 指令在交換器上建立 VLAN 項目。使用名稱字符串（name string）指令來建立一個帶名稱的 VLAN 項目。

CLI 指令：vlan *ID*

舉例： (config)# vlan *3*

(config-vlan)# name vlan*3*

5.3.5.3 介面 VLAN 指令模式（interface vlan VLAN-ID）

本指令用來將操作更改為 VLAN 介面指令模式。

CLI 指令：interface vlan *VLAN-ID*

舉例： interface vlan *1*

5.3.5.4 IP 位址（ip address）

本指令用來設定指定連接埠的 IP 位址。

CLI 指令：ip address A.B.C.D/M

舉例： (config-if)# ip address 192.168.20.121/24

連接埠的名稱在設定過程中不會被顯示。請在設定過程中記住您要設定的連接埠。

5.3.5.5 ip dhcp client

本指令用於設定系統介面透過 DHCP 伺服器取得 IP 位址。

CLI 指令：ip dhcp client

舉例： (config-if)# ip dhcp client

介面名稱在設定過程中不會被顯示。請在設定過程中記住您要設定的介面。

5.3.6 生成樹（Spanning Tree）

5.3.6.1 show spanning-tree summary

顯示目前的生成樹。

CLI 指令 : show spanning-tree summary

舉例 : ASUS# show spanning-tree summary

5.3.6.2 spanning-tree enable and disable

開啟／關閉生成樹。

CLI 指令 : spanning-tree (enableldisable)

舉例 : (config)# spanning-tree disable

5.3.7 連結匯聚（Link aggregation）

5.3.7.1 trunk aggregation group

使用交換器的連結匯聚幹線群組設定指令來設定幹線匯聚群組。

CLI 指令 : aggregation-link group *<1-8> IFLIST*

舉例 : (config)# aggregation-link group *1 gi1/0/1-3*

5.3.7.2 trunk load balancing

使用交換器的連結匯聚幹線群組指令，以來源位址或目的地位址為基礎的轉發方式來設定幹線負載均衡。

CLI 指令: aggregation-link group <1-8> load-balance (*src-mac* / *dst-mac* / *src-dst-mac* / *src-ip* / *dst-ip* / *src-dst-ip*)

舉例: ASUS#aggregation-link group 1 load-balance *src-mac*

5.3.7.3 show aggregation-link trunk

顯示連結匯聚幹線狀態。

CLI 指令: show aggregation-link group *GROUPID*

舉例: ASUS# show aggregation-link group *1*

5.3.8 LACP

5.3.8.1 lacp aggregation-link trunk

本指令用來新增／設定交換器幹線群組連接埠的連結匯聚控制協定(LACP)。

CLI 指令: lacp aggregation-link group *<1-8> (addlset) IFLIST*

舉例: ASUS(config)# lacp aggregation-link group*1 add gi1/0/1-3*

5.3.8.2 no lacp aggregation-link trunk

本指令用來將交換器幹線群組連接埠的連結匯聚控制協定(LACP)關閉。

CLI 指令: no lacp aggregation-link group *<1-8>*

舉例: ASUS(config)# no lacp aggregation-link group *1*

5.3.8.3 lacp system-priority

本指令為交換器上的連結匯聚控制協定(LACP)設定系統優先權。

CLI 指令: lacp system-priority *<1-65535>*

舉例: (config)# lacp system-priority *20000*

5.3.9 鏡像（Mirroring）

5.3.9.1 Mirror

本指令用來將來源介面列表中的流量鏡像至目的介面。鏡像類型支援接收流量、傳送流量或兩者兼有。

CLI 指令：mirror session *<1-2>* source *IFLIST (both | rx | tx)*
mirror session *<1-2>* destination *IFNAME*

舉例： (config)# mirror session *1* source *gi1/0/1-4 both*
(config)# mirror session *1* destination *gi1/0/5*

5.3.9.2 show mirror

顯示當前的鏡像功能。

CLI 指令 : Show mirror session

舉例 : ASUS# show mirror session

5.3.9.3 no mirror

本指令用來關閉鏡像功能。

CLI 指令 : no mirror session *<1-2>*

舉例 : (config)# no mirror session *1*

5.3.9.4 no mirror source IFLIST

本指令用來重置來源介面接收或傳送的流量。

CLI 指令 : no mirror session *<1-2>* source *IFLIST*

舉例 : (config)# no mirror session *1* source *gi1/0/1-2*

5.3.10 靜態多重播送（Static Multicast）

5.3.13.1 mac-address-table multicast

使用交換器的 mac-address-table multicast 設定指令來將多重播送位址新增至 MAC 位址表。

CLI 指令：mac-address-table multicast *MACADDR VLANID IFLIST*

舉例：(config)# mac-address-table multicast *0100.5e11.1111 2 gi1/01-3*

5.3.10.2 no mac-address-table multicast

使用 no mac-address-table multicast 設定指令來刪除 MAC 位址表中的多重播送靜態位址。

CLI 指令：no mac-address-table multicast *MACADDR VLANID IFLIST*

舉例：(config)# no mac-address-table multicast *0100.5e11.1111 2 gi1/0/1-3*

5.3.10.3 show mac-address-table multicast

使用顯示 MAC 位址表多重播送（show mac-address-table multicast）使用者 EXEC 指令來顯示所有 VLAN 的二層多重播送項目。在特權 EXEC 模式下用這個指令可顯示指定的多重播送項目。

CLI 指令：show mac-address-table multicast

舉例：ASUS# show mac-address-table multicast

5.3.11 IGMP 偵聽（IGMP Snooping）

5.3.11.1 ip igmp snooping

本指令用來完整開啟 IGMP 偵聽功能。

CLI 指令：ip igmp snooping

舉例：(config)# ip igmp snooping

5.3.11.2 間隔時間（interval time）

本指令用來設定交換器傳送 IGMP 詢問的間隔時間。

CLI 指令：ip igmp snooping last-member-query-interval *TIMEVALUE*

舉例：(config)# ip igmp snooping last-member-query-interval *100*

5.3.12 DHCP 偵聽（DHCP Snooping）

5.3.12.1 ip dhcp snooping

本指令用來完整開啟 DHCP 偵聽功能。

CLI **指令：** ip dhcp snooping

舉例： (config)# ip dhcp snooping

5.3.12.2 ip dhcp snooping vlan VLANLIST

本指令用來設定開啟的用於 DHCP 偵聽的 VLAN 群組。

CLI **指令：** ip dhcp snooping vlan VLANLIST

舉例： (config)# ip dhcp snooping vlan 1, 4, 5-100

5.3.12.3 ip dhcp snooping trust

本指令用來設定作為 DHCP 偵聽的可信任連接埠的介面。

CLI **指令：** ip dhcp snooping trust

舉例： (config-if)# ip dhcp snooping trust

5.3.12.4 show ip dhcp snooping binding

本指令用來顯示 DHCP 偵聽須遵守的資訊。

CLI **指令：** show ip dhcp snooping binding

舉例： (config)# show ip dhcp snooping binding

5.3.13 流量控制（Traffic control）

5.3.13.1 storm-control

在使用交換器的 storm 控制設定指令來限制連接埠用於廣播／ dlf ／多重播送的總頻寬的傳輸速率。

CLI **指令：** storm-control (*broadcast* | *dlf* | *multicast*) *LIMIT_RATE*

舉例： (config)# interface *gi1/0/1*

(config-if)# storm-control *broadcast 25*

5.3.13.2 no storm-control

使用交換器的 no storm-control 設定指令來關閉對連接埠用於廣播／ dlf ／多重播送的總頻寬的速率限制。

CLI **指令：**no storm-control (*broadcast* | *dlf* | *multicast*)

舉例：(config)# interface *gi1/0/1*

(config-if)# no storm-control *broadcast*

5.3.13.3 show storm-control

使用交換器的顯示 storm 控制設定指令來顯示對連接埠用於廣播／ dlf ／多重播送的總頻寬的速率限制。

CLI **指令：**show storm-control (*broadcast* | *dlf* | *multicast*)

舉例： ASUS# show storm-control *broadcast*

5.3.14 動態位址（Dynamic addresses）

5.3.14.1 clear dynamic mac-address

使用交換器的以下指令在資料庫中清除動態第二層 MAC 位址。

CLI **指令：**clear mac-address-table dynamic mac *MACADDR*

舉例： (config)# clear mac-address-table dynamic mac *0000.1111.2222*

5.3.14.2 aging time

在一組堆疊或單獨的交換器上使用 mac-address-table aging-time 指令可設定動態位址在使用或更新後仍然存在於 MAC 位址表中的時間。

CLI **指令：**mac-address-table aging-time *<10-1000000>*

舉例： (config)# mac-address-table aging-time *100*

這個例子說明了如何將 MAC 位址表的汰換時間設定為 300 秒。

5.3.14.3 no aging time

重置 MAC 位址表的汰換功能計時器。

CLI **指令：**no mac-address-table aging-time

舉例： (config)# no mac-address-table aging-time

5.3.14.4 show mac-address-table aging-time

CLI 指令：show mac-address-table aging-time

舉例：ASUS# show mac-address-table aging-time

5.3.15 靜態位址（Static addresses）

5.3.15.1 新增靜態 MAC 位址（add static mac-address）

您可以新增 MAC 位址到交換器的 MAC 位址表中。透過這種方式新增的 MAC 位址將不會從位址表中汰換。我們稱之為靜態位址。

CLI 指令：mac-address-table static *MACADDR VLANID IFNAME*

舉例：(config)# mac-address-table static *0000.1111.2222 1 gi1/0/2*

5.3.15.2 顯示 MAC 位址表（show mac-address-table）

顯示靜態與動態 MAC 位址。

CLI 指令：show mac-address-table

舉例：ASUS# show mac-address-table

5.3.16 VLAN

5.3.16.1 show vlan name string

使用交換器的顯示 VLAN 使用者 EXEC 指令來顯示所有設定的 VLAN 或單一 VLAN（若指定 VLAN ID 或名稱）的參數。

CLI 指令：show vlan name *VLANNAME*

舉例：ASUS# show vlan name *VLAN1*

5.3.16.2 vlan vid

使用 vlan vid 指令在交換器上建立 VLAN 項目。

CLI 指令：vlan *vid*

舉例：(config)# vlan 2

5.3.16.3 name VLANNAME

使用 name VLANNAME 指令在交換器上建立 VLAN 項目。

CLI 指令 : name *VLANNAME*

舉例 : (config)# vlan 2

(config-vlan)# name VLAN2

5.3.16.4 access vlan

設定所有介面的存取模式特徵及設定虛擬區域網路。

CLI 指令 : switchport access vlan <1-3000>

舉例 : (config)# interface gi1/0/2

(config-if)# switchport access vlan 1

5.3.16.5 allowed VLAN

使用交換器連接埠的幹線許可 VLAN（allowed vlan）設定指令來新增或刪除許可 VLAN，許可 VLAN 在幹線模式下可在此連接埠以標記形式接收和傳送流量。

CLI 指令 : switchport trunk allowed vlan *(add | remove) VLANLIST*

舉例 : (config)# interface gi1/0/2

(config-if)# switchport access vlan 1

5.3.17 GVRP

5.3.17.1 clear gvrp statistics

使用交換器的清除 GVRP 統計資料（clear gvrp statistics）設定指令來清除一個或多個連接埠的所有 GVRP 統計資料。

CLI 指令 : clear gvrp statistics *[IFNAME]*

舉例 : ASUS# clear gvrp statistics *gi1/0/2*

5.3.17.2 GVRP 模式（gvrp mode）

本指令可完整開啟或關閉交換器的 GVRP 功能。

CLI 指令 : gvrp (*enable | disable)*

舉例 : ASUS# gvrp *enable*

5.3.17.3 顯示 GVRP 設定（show gvrp configuration）

顯示 GVRP 設定狀態。

CLI 指令：show gvrp interface *[IFNAME]*

舉例：ASUS# show gvrp interface *gi1/0/1*

5.3.17.4 顯示 GVRP 統計資料（show gvrp statistics）

顯示 GVRP 統計資料的狀態。

CLI 指令：show gvrp statistics *[IFNAME]*

舉例：ASUS# show gvrp statistics *gi1/0/1*

5.3.18 CoS/QoS

5.3.18.1 排列 CoS 映像（queue cos-map）

使用交換器的排列 CoS 映像（queue cos-map）設定指令來設定 CoS 佇列的優先權順序。

CLI 指令：cos cos-map *PRIORITY QUEUE*

舉例：ASUS# cos cos-map 3 3

5.3.18.2 show queue cos-map

本指令用來顯示 CoS 佇列與優先權資訊。。

CLI 指令：show cos cos-map

舉例：(config)# show cos cos-map

5.3.18.3 CoS 策略(cos policy)

本指令用來設定處理傳入封包的 CoS 策略。

CLI 指令：cos policy (fifo/ strict/ wrr-queue)

舉例：(config)# cos policy fifo

5.3.18.4 顯示 CoS 策略（show cos policy）

本指令顯示 CoS 策略。

CLI 指令：show cos policy

舉例：(config)# show cos policy

5.3.18.5 QoS 傳入頻寬（qos ingress bandwidth）

本指令用來設定傳入封包的 QoS 頻寬資訊參數。

CLI 指令 : qos ingress bandwidth *LIMITRATE*

舉例 : (config)# interface *gi1/0/2*

(config-if)# qos ingress bandwidth *64*

5.3.18.6 QoS 傳出頻寬（qos egress bandwidth）

本指令用來設定傳出封包的 QoS 頻寬資訊參數。

CLI 指令 : qos egress bandwidth *LIMITRATE*

舉例 : (config)# interface *gi1/0/2*

(config-if)# qos egress bandwidth *64*

5.3.19 策略圖表 (Policy Map)

策略圖表 (Policy Map) 可讓使用者更改傳入封包的優先權，當超過負荷時，可選擇傳送封包或丟棄封包。

5.3.19.1 policy-map

本指令可定義一個策略組合名稱。

CLI 指令：policy-map *POLICYMAP*

舉例： (config)# policy-map *policy1*

5.3.19.2 class

本指令可定義一個策略組合類別。

CLI 指令：class *CLASSMAP*

舉例： (config-pmap)# class *a*

5.3.19.3 match

本指令設定匹配標準。

CLI 指令：match (access-group ACLNAME | ip dscp *DSCPLIST* / *ip precedence IPPRECEDENCES*)

舉例：(config-pmap-class)# match access-group *ipacl1*

(config-pmap-class)# match ip dscp 4-6

(config-pmap-class)# match ip precedence *1,3,5*

5.3.19.4 police

本指令用來設定對於與標準符合的傳入封包的動作。

CLI 指令：police (*RATE BURSTSIZE* | drop | high-drop)

舉例：(config-pmap-class)# police 64 128

(config-pmap-class)# police drop

(config-pmap-class)# police high-drop

5.3.19.5 set

本指令用來設定對於與標準符合的傳入封包的 CoS 與 IP 優先權。

CLI 指令：set (cos override VALUE | ip dscp VALUE | ip precedence VALUE)

舉例：(config-pmap-class)# set cos 3

(config-pmap-class)# set ip dscp 20

(config-pmap-class)# set ip precedence 5

5.3.19.6 service-policy input

本指令用來添加策略圖表到一個介面。

CLI 指令：policy map input POLICYMAP

舉例：(config-if)# policy map input policy1

5.3.20 SNMP

5.3.20.1 show rmon statistics

顯示 RMON 統計資料狀態。

CLI 指令：show rmon statistics *[IFNAME]*

舉例： ASUS# show rmon statistics *gi1/0/1*

5.3.20.2 show snmp-server community

顯示 SNMP 伺服器群組。

CLI 指令：show snmp-server community

舉例： ASUS# show snmp-server community

5.3.20.3 snmp-server host

本指令用來設定 SNMP 主機資訊。

CLI 指令：snmp-server host *A.B.C.D*

舉例：(config)# snmp-server host *192.168.8.31*

5.3.21 過濾（Filter）

5.3.21.1 MAC 過濾組合 (MAC filter set)

本指令用來定義一個延伸 MAC 位址存取列表，並進入存取列表設定模式。

CLI 指令：mac access-list extended *ACLNAME*

舉例：(config)# mac access-list extended *mac_acl_1*

5.3.21.2 IP 過濾組合 (IP filter set)

本指令用來定義延伸／標準 ip 存取列表，並進入存取列表設定模式。

CLI 指令：ip access-list (standard | extended) *ACLNAME*

舉例：(config)# ip access-list extended *ip_acl_1*

5.3.21.3 拒絕任何主機（deny any host）

使用交換器的拒絕 MAC 存取列表（deny MAC access list）設定指令來防止符合條件的非 IP 流量被傳送。使用此指令的否定 (no) 形式來從命名的 MAC 存取列表中刪除一個拒絕的條件。

CLI 指令：deny any host MACADDR *[IFNAME]*

舉例：(config-mac-acl)# deny any host c2f3.220a.12f4 gi1/0/2

5.3.21.4 過濾條件 (filter conditions)

本指令用來指定一種或多種拒絕或允許的條件，來決定封包是轉發或是丟棄。

CLI 指令：(permitldeny) any any

舉例：(config-mac-acl)# permit any any

5.3.21.5 附加過濾規則 (filter attach)

本指令用來將 MAC 或 IP 存取列表附加到一個介面。

CLI 指令：mac access-group ACLNAME in

舉例：ASUS# interface gi1/0/1

(config-if)# mac access-group mac_acl_1 in

5.3.22 連接埠存取控制（Port access control）

5.3.22.1 dot1x guest-vlan

使用交換器的 dot1x guest-vlan 介面設定指令來指定一組活動的 VLAN 為 802.1x 訪客 VLAN。用本指令的否定（no）形式來將設定回復為預設值。

CLI 指令：dot1x guest-vlan *<1-3000>*

舉例：(config)# interface *gi1/0/1*

(config-if)# dot1x guest-vlan *3*

5.3.22.2 dot1x port-control

使用交換器的 dot1x 連接埠控制（dot1x port-control）介面設定指令來開啟連接埠認證狀態的手動控制。用本指令的否定（no）形式將設定回復為預設值。

CLI 指令：dot1x port-control (auto|force-authorized| force-unauthorized)

舉例：(config)# interface *gi1/0/1*

(config-if)# dot1x port-control *force-authorized*

5.3.23 撥入使用者（Dial-in user）

5.3.23.1 dot1x username password

新增使用者至本地 RADIUS 資料庫。

CLI 指令：dot1x user *USERNAME PASSWORD VLANID*

舉例：(config)# dot1x *user test 12345 3*

5.3.23.2 show dot1x user

顯示 dot1x 撥入使用者。

CLI 指令：show dot1x user

舉例：ASUS# show dot1x user

5.3.24 RADIUS

5.3.24.1 RADIUS 設定（RADIUS settings）

本指令用來設定 802.1x 的 RADIUS 伺服器 IP、RADIUS 密鑰及 RADIUS 連接埠。

CLI **指令：**dot1x radius server *A.B.C.D RADIUS_KEY [PORT]*

舉例：(config)# dot1x radius server *192.168.1.38 123456 1812*

5.3.24.2 show dot1x radius

顯示 802.1x 設定的 dot1x RADIUS 伺服器 IP、RADIUS 密鑰及 RADIUS 連接埠。

CLI **指令：**show dot1x radius

舉例：ASUS# show dot1x radius

5.3.25 連接埠安全（Port security）

5.3.25.1 show port security

本指令用來顯示連接埠的安全設定、狀態與 MAC 位址資訊。

CLI **指令：**show port-security [address] *[interface IFNAME]*

舉例：ASUS# show port-security

ASUS# show port-security interface *gi1/0/24*

ASUS# show port-security address

ASUS# show port-security address *gi1/0/24*

5.3.25.2 clear port security

本指令用來清除連接埠安全動態 MAC 位址。

CLI **指令：**clear port-security dynamic [address *MAC*] | [interface *IFNAME*]

舉例：ASUS# clear port-security dynamic

ASUS# clear port-security dynamic *0023.1313.2313*

ASUS# clear port-security dynamic interface *gi1/0/24*

5.3.25.3 switchport port-security

本指令用來設定連接埠的安全設定及 MAC 位址。

CLI 指 令：switchport port-security [mac-address *MACADDR*] | [maximum *VALUE*] | [violation {protect | restrict | shutdown}] | [reup]

舉例： (config)# interface gi1/0/24

(config-if)# switchport port-security

(config-if)# switchport port-security mac-address *0023.1313.2313*

(config-if)# switchport port-security maximum *20*

(config-if)# switchport port-security violation protect

(config-if)# switchport port-security reup

5.3.25.4 switchport port-security aging

本指令用來進行連接埠安全的汰換設定。

CLI **指令：**switchport port-security aging {time *TIME* | type {absolute | inactivity}}

舉例: (config)# interface gi1/0/1

(config-if)# switchport port-security aging-time *20*

(config-if)# switchport port-security aging-type absolute

5.3.26 NTP

本功能可讓交換器自動將時間與 NTP 伺服器同步。

5.3.26.1 ntp server

本指令用來設定用於 NTP 同步的伺服器 IP 位址。

CLI **指令**：ntp server IPADDR

舉例： (config)# ntp server 220.130.158.52

5.3.26.2 ntp sync

本指令用來使交換器時鐘時間與 NTP 伺服器同步。

CLI **指令**：ntp sync IPADDR

舉例： ASUS# ntp sync 220.130.158.52

5.3.26.3 show ntp server

本指令用來顯示 NTP 伺服器資訊。

CLI 指令：show ntp server

舉例： ASUS# show ntp server

5.3.26.4 show clock

本指令用來顯示交換器的時鐘時間。

CLI 指令：show clock

舉例： ASUS# show clock

5.4 其他指令（Miscellaneous commands）

show private health: 顯示環境變量，如溫度、風扇轉速與電壓。

show private led : 顯示三個系統 LED 指示燈 - SYSTEM，RPS 與 FAN。

show private model : 顯示交換器的型號名稱。

show version : 顯示硬體、Boot ROM 及韌體版本號。

ping : ping 遠程主機。

show ip route : 顯示路由表中的項目。

第六章　IP 位址，網路遮罩和子網路

6.1　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。您可以在第八章中尋找到這些內容的詳細資訊。

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”。

6.1.1　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 8 顯示的是IP 位址的結構。

表 8.　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)

6.1.2 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。

一些與 IP 位址相關的重要資訊 :

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。

6.2 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 類地址）。

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。

第七章　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。

7.1　使用 IP 工具診斷問題

7.1.1　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，它就會傳送回應。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，就會出現如下圖所示的提示。

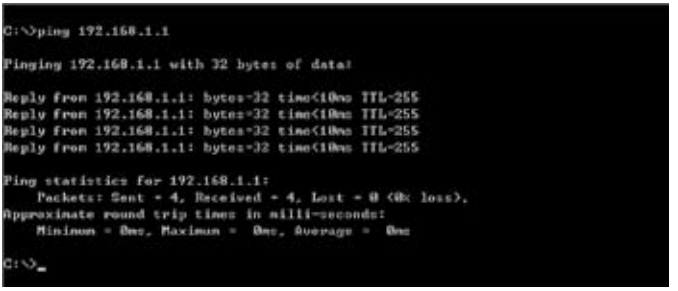

圖 76. 使用 ping 工具

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 Internet 的路徑是否暢通。如果您不知道某個 Internet 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。

7.1.2 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 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。

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 , 如下圖所示。

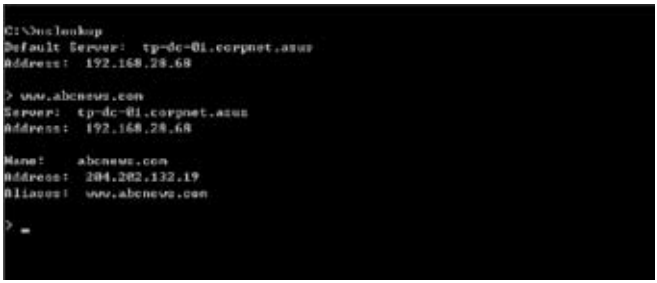

圖 77. 使用 nslookup 工具

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>。

7.2 簡易維修

下表內列出了一些交換器的常見問題，您可能在安裝或使用交換器的過程中遇到這樣的問題，同時該表也列出了一些建議的解決方案。

表 9. 疑難排解

問題	建議方案
LED 指示燈	
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。
連接後備電源後，RPS LED 不亮	1. 確認 RPS 電源線是否連接到電源插座。 2. 確認安裝的 RPS 模組是否符合 RPS 標準。
FAN LED 呈琥珀色閃爍	檢查交換器背部的風扇。如果其中任一個風扇有故障，您可以替換風扇。
當連接網路線時，千兆乙太網路 Link LED 不亮	1. 確認乙太網路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 / 集線器交換器已經開啟。 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 纜線可能支援較低品質的纜線。
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 指示燈是否呈綠色。 2. 如果連接埠的 LED 指示燈呈琥珀色，檢查該連接埠是否被關閉。 如果剛剛開啟 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開啟。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。 4. 如果 ping 成功，但是網頁設定介面仍不能使用，請透過 RS232 或 USB 連接控制終端。檢查是否有過濾規則或靜態 MAC 位址將 WEB 流量堵塞。

問題	建議方案
網頁設定介面	
丟失 / 忘記網頁設定連接埠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。 2. 透過 RS232 或 USB 登入控制終端，在 Boot ROM 模式下用“psw”指令重置密碼。
某些頁面無法完全顯示	1. 確認您使用的是 Internet Explorer® v6.0 或以後版本的瀏覽器。不支援 Netscape。您的瀏覽器必須開啟 Javascript®，也必須支援 Java®。 2.Ping 交換器的 IP 位址檢查連線是否穩定。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。
控制終端介面	
不能顯示終端模擬器上的文字	1. 出廠設定的鮑率為 9600，無流量控制，8 位資料，無同位檢查，1 位停止位。 2. 將您的終端模擬器設定如上，如果您使用的是 USB 連接埠，請先安裝 USB 驅動程式。 3. 檢查連接線是否良好。

第八章　術語表

10BASE-T	用於乙太網路的有線纜線，資料傳輸率為 10Mbps。亦稱 3 類線(CAT 3)。參見data rate, Ethernet。
100BASE-T	用於乙太網路的有線纜線，資料傳輸率為 100Mbps。亦稱 5 類線 (CAT 5)。參見data rate, Ethernet。
1000BASE-T	用於乙太網路的有線纜線，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。將資料傳送到網路上所有的電腦。
download	以下行的方向傳輸資料，例如，從網際網路到使用者。
Ethernet	乙太網。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。
filtering	根據過濾規則，篩選出符合條件的資料類型。過濾可以是單向（傳入或傳出），也可以是雙向的。
filtering rule	判斷路由裝置應該接受還是拒絕某種類型資料的規則。過濾規則是用於單個（或多個）介面操作的， 並且有特定的方向性（上行、下行或雙向）。
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)。
HTTP	超文本傳輸協定 HTTP 是用來進行網路資料傳輸的最主要的協定，可以通過網頁瀏覽器顯示。參見web browser, web site。
ICMP	網際網路控制訊息協定 一種互聯網協定，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。
Internet	網際網路，用於私人或商業通信。
intranet	私有的公司內部網路，看起來像網際網路(Internet) 的一部分(使用者使用網頁瀏覽器來存取資訊)，但是只能被本公司員工所使用。
IP	參見 TCP/IP。
IP address	網際網路協定位址 主機（電腦）在網際網路上的位址，它包含四個數字，每個數字的範圍是 0 ~ 255，用小數點分隔。如，209.191.4.240。一個IP 位址包含了網路ID和主機ID，網路ID表示主機屬於哪個特定的網路，主機ID則是網路中確定該主機的唯一標誌。網路遮罩用來定義網路ID和主機ID。由於IP 位址比較難記，它們通常都對應一個功能變數名稱（domain name）。參見domain name, network mask。
ISP	網路服務提供商 向顧客提供網際網路存取服務的公司，通常是收費的。
LAN	區域網路 存在於一個較小地理範圍內的網路，例如家裡，辦公室或大樓。
LED	發光二極體 一種電子發光裝置。交換器前面的指示燈號就是LED。

MAC address	媒體存取控制位址，簡稱MAC 位址 由製造商分配的裝置的永久性硬體位址。MAC 位址由六對字元組成。
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, IP address, subnet,“IP Addresses Explained” 部分。
NIC	網路介面卡 插入電腦, 提供網路纜線的物理介面　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。實體的網路裝置接入點，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
QoS	服務品質（Quality of Service） 在802.1Q 中定義。對於資料通信網路性能，QoS特性有頻寬、延遲和可靠性。
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HTTP, web site, WWW。
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 hyperlink, 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hyperlink, web page。
WWW	全球資訊網 也稱 Web。 全球範圍內可透過網際網路存取的所有網站的總和。