

# GigaX 系列

## 第二層網路管理交換器

繁體中文

使用手冊

## GigaX 系列

本產品的所有部分，包括配件與軟體等，其所有權都歸華碩電腦公司（以下簡稱華碩）所有，未經華碩公司許可，不得任意地仿製、拷貝、謄抄或轉譯。本產品使用手冊沒有任何型式的擔保、立場表達或其它暗示。若有任何因本快速安裝指南或其所提到之產品的所有資訊，所引起直接或間接的資料流失、利益損失或事業終止，華碩及其所屬員工恕不為其擔負任何責任。除此之外，本快速安裝指南所提到的產品規格及資訊僅供參考，內容亦會隨時更新，恕不另行通知。本快速安裝指南的所有部分，包括硬體及軟體，若有任何錯誤，華碩沒有義務為其擔負任何責任。

快速安裝指南中所談論到的產品名稱僅做識別之用，而這些名稱可能是屬於其他公司的註冊商標或是版權，在此聲明如下：

- Windows、MS-DOS 是 Microsoft 公司的註冊商標
- Adobe、Acrobat 是 Adobe System 公司的註冊商標

版權所有，不得翻印 ©2005華碩電腦

注意！倘若本產品上之產品序號有所破損或無法辨識者，則該項產品恕不保固！

產品名稱:	華碩 GigaX 2024/2048 第二層網路管理交換器
手冊版本:	T2211 V1
發表日期:	2005 年 11 月

## 第二層網路管理交換器

---

### 華碩電腦公司ASUSTeK COMPUTER INC.(亞太地區)

#### 市場訊息

地址 : 台灣臺北市北投區112立德路15號  
電話 : +886-2-2894-3447  
傳真 : +886-2-2890-7798  
電子郵件 : info@asus.com.tw

#### 技術支援

免費服務電話 : 0800-093-456  
服務時間 : 週一至週五 AM 9:00 ~ PM 6:00  
傳真 : +886-2-2890-7698  
全球資訊網 : <http://tw.asus.com>  
技術支援網址 : <http://support.asus.com>

### ASUS COMPUTER INTERNATIONAL (美國)

#### 市場訊息

地址 : 44370 Nobel Drive, Fremont, CA 94538, USA  
傳真 : +1-502-608-4555  
電子郵件 : tmdl@asus.com

#### 技術支援

傳真 : +1-502-933-8713  
電話 : +1-502-995-0883  
電子郵件 : <http://vip.asus.com/eservice/techserv.aspx>  
全球資訊網 : <http://www.asus.com>

### ASUS COMPUTER GmbH (德國/奧地利)

#### 市場訊息

地址 : Harkort str. 25, D-40880 Ratingen, Germany  
電話 : 49-2102-95990  
傳真 : 49-2102-959911  
電子郵件 : sales@asuscom.de  
線上連絡 : <http://www.asuscom.de/sales>

#### 技術支援

電話 : 49-2102-9599-0 .....主機板/其他產品  
          49-2102-9599-10 .. 筆記型電腦  
傳真 : 49-2102-9599-11  
線上支援 : <http://www.asuscom.de/support>

## GigaX 系列

# 使用手冊目錄

華碩連絡資訊 .....	3
1 產品簡介 .....	7
1.1 第二層管理功能 .....	7
1.2 關於閱讀本使用手冊 .....	8
2 瞭解 GigaX 2024/2048 第二層網路管理交換器 .....	9
2.1 產品包裝 .....	9
2.2 前面板 .....	10
2.3 後背板 .....	11
2.4 技術規格 .....	11
3 快速安裝指南 .....	12
3.1 Part 1 – 硬體安裝 .....	12
3.1.1 將交換器安裝於平坦表面 .....	12
3.1.2 將交換器安裝於機架 .....	12
3.2 Part 2 – 設定本交換器 .....	13
3.2.1 連接控制台連接埠 .....	13
3.2.2 連接到電腦或區域網路 (LAN) .....	13
3.2.3 連接備用電源模組 (RPS) .....	13
3.2.4 連接電源線 .....	13
3.3 Part 3 – 交換器基本管理設定 .....	15
3.3.1 透過控制台連接埠 (Console Port) 進行設定 .....	15
3.3.2 透過 WEB 介面進行設定 .....	17
4 網路介面進行管理 .....	19
4.1 登入網頁管理使用者介面 .....	19
4.2 網頁管理介面的功能結構 .....	21
4.2.1 瀏覽選單的技巧 .....	23
4.2.2 常用按鍵與圖示 .....	23
4.3 系統頁面 .....	23
4.3.1 Management 介面 .....	23
4.3.2 Reboot 頁面 .....	24
4.3.3 Administration 頁面 .....	25
4.3.4 IP Setup .....	26
4.3.5 韌體升級 .....	26
4.4 實體介面 .....	28
4.5 橋接 .....	29
4.5.1 連結彙聚 (Link Aggregation) .....	30
4.5.2 鏡像 (Mirroring) .....	33
4.5.3 靜態多重播送 (static Multicast) .....	35

## 第二層網路管理交換器

4.5.4 IGMP 偵聽 (IGMP Snooping)	37
4.5.5 流量控制 (Traffic Control)	38
4.5.6 動態位址 (dynamic address)	39
4.5.7 靜態位址 (Static address)	40
4.5.8 標示 VLAN (Tagged VLAN)	41
4.5.9 預設連接埠VLAN 與服務等級 (CoS)	43
4.5.10 DHCP 偵聽 (DHCP Snooping)	44
4.6 簡易網路管理通訊協定 (SNMP)	46
4.6.1 群組列表 (Community Table)	46
4.6.2 主機列表 (Host Table)	47
4.6.3 Trap 設定 (Trap Setting)	48
4.6.4 VACM 群組 (VACM Group)	49
4.6.5 VACM 檢視 (VACM View)	50
4.6.6 USM 使用者	51
4.7 過濾功能頁面	52
4.7.1 過濾設定	52
4.7.2 附加過濾規則	54
4.8 安全功能	56
4.8.1 連接埠存取控制	56
4.8.2 撥入使用者	58
4.8.3 RADIUS	59
4.8.4 連接埠安全性	60
4.9 QoS	65
4.9.1 Trust State	65
4.9.2 Mapping	67
4.9.3 等級設定	68
4.9.4 Policy Set	69
4.9.5 Policy Attach	71
4.9.6 CoS	72
4.10 統計圖表 (Static chart)	73
4.10.1 傳輸狀況比較	73
4.10.2 錯誤群組	74
4.10.3 歷程狀態	75
4.10.4 儲存設定值	76
<b>5. 控制台介面 (Console Interface)</b>	<b>77</b>
5.1 開機自我檢測	78
5.1.1 Boot ROM 指令模式	79
5.1.2 Boot ROM 指令	80
5.2 登入與登出	80
5.3 CLI 指令	81
5.3.1 系統指令	81
5.3.2 實體介面指令	84

## GigaX 系列

5.3.3 橋接指令 .....	85
5.3.4 簡易網路管理通訊協定 .....	93
5.3.5 過濾器指令 .....	98
5.3.6 安全指令 .....	102
5.3.7 QoS 指令 .....	107
5.4 其他指令 .....	111
<b>6. IP 位址、網路遮罩，與子網路 .....</b>	<b>111</b>
6.1 IP 位址 .....	111
6.1.1 IP 位址的結構 .....	111
6.1.2 網路等級 .....	112
6.2 子網路遮罩 .....	113
<b>7 疑難排解 .....</b>	<b>115</b>
7.1 使用 IP 公用程式診斷網路問題 .....	115
7.2 更換系統風扇 .....	118
7.3 簡易維修 .....	120
<b>8 術語表 .....</b>	<b>122</b>

### 1 產品簡介

首先，恭喜您成為華碩 GigaX 第二層網路管理交換器的使用者！您現在將可以透過友善且有效率的使用介面來管理您的區域網路環境。

本使用手冊除了將告訴您如何設定、管理您的 GigaX 第二層網路管理交換器外，也將指導您如何依自身使用環境需要來設定本產品，讓 GigaX 第二層網路管理交換器得以發揮最大的功效。

#### 1.1 第二層管理功能

- 24 個 10/100BASE-T 自動偵測高速乙太網路連接埠 (GigaX 2024)
- 2 個支援自動偵測的 10/100/1000BASE-T Gigabit 乙太網路連接埠
- 2 個小型可插拔 (SFP) Gigabit 介面轉換插槽 (GBIC)
- 支援 802.1D / 802.1w 透明橋接/生成樹協定 (Transparent bridge/Spanning tree protocol)
- 支援 8K MAC 地址快取與硬體控制存在時間
- 802.3x 流量控制
- 支援 802.1Q-based 之虛擬區域網路，最高可支援 256 組虛擬區域網路
- 支援 802.1p 服務等級，每個連接埠可支援 4 組
- 支援 IGMP 偵聽 (Snooping)
- 802.3ad 連結幹線 (Trunk)，最高每個群組可支援 15 組幹線
- 連接埠鏡像 (Port Mirroring) 功能
- 802.1X 連接埠網路存取控制
- RADIUS (撥入使用者遠端認證服務)
- 支援 4 組 (1,2,3,9) RMON 遠端網路監視
- SNMP V1,V2,V3 簡易網路管理通訊協議
- 支援 MIB II 管理資料庫
- 企業級電源供應器、風扇與系統溫度、電壓管理資料庫 (MIB)
- Telnet 或 SSH 遠端登入
- FTP 韌體更新與備份設定
- 支援 Syslog 系統記錄檔
- 支援透過控制埠與 Telnet 的指令列 (CLI) 介面

## GigaX 系列

---

- 支援網頁式 GUI
- 連接埠連線狀況 LED 顯示
- 系統、備援式電源供應、風扇狀態 LED 顯示

## 1.2 關於閱讀本使用手冊

### 1.2.1 注意事項

- 爲了方便起見，在本手冊中部份 GigaX 網管交換器簡稱為「本交換器」。
- 除非有特殊標明，本手冊中的圖示及 Web 介面圖示均適用於 GigaX2024/2048 交換器。

### 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，而這些圖示所代表的意義如下：



說明: 進一步的資訊說明。



重要: 重點提示說明。



警告: 禁止不當行為及操作，提醒您在進行某一項操作時要注意安全。

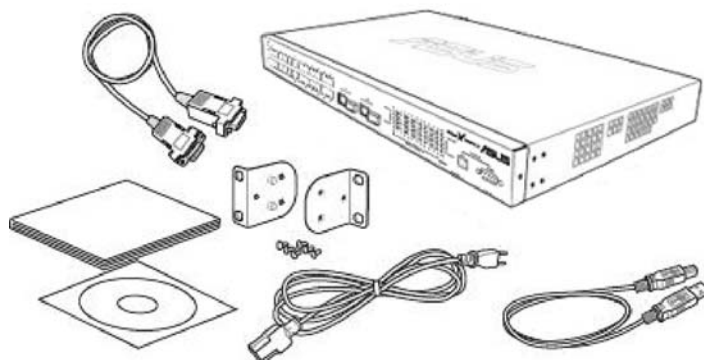


## 2 瞭解 GigaX 第二層網路管理交換器

### 2.1 產品包裝內容

GigaX 交換器的產品包裝中包含有以下物品：

- GigaX 2024X (26 埠) 第二層網路管理交換器
- AC 電源線
- 供終端管理介面使用的數據機連接線 (DB9)
- 機架安裝套件 (包括 2 個托架與 6 顆 #6-32 螺絲)
- 供終端管理介面使用的 USB 纜線
- 安裝光碟
- 使用手冊
- 快速安裝指南



圖一 華碩 GigaX 2024X 第二層網路管理交換器產品包裝

GigaX 系列

前面板

前面板包括有 LED 指示燈與終端連接埠。LED 指示燈可以顯示系統、備用電源 (RPS)、風扇與連接埠的狀態。



圖二 前面板燈號標示表

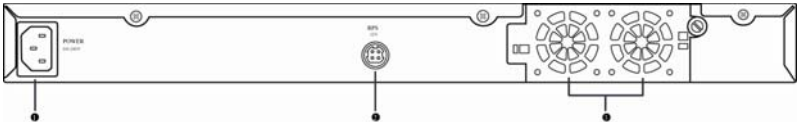
表1 前面板燈號標示表

No.	標示	顏色	狀態	說明
1	SYSTEM	綠色	恆亮	裝置電源開啓
			閃爍	自我測試、初始化、下載中
		橙色	恆亮	溫度或電壓異常
			熄滅	無電源供應
2	RPS	綠色	恆亮	裝置之電源供應器正常且處於良好供電狀態
		橙色	恆亮	裝置之電源供應器異常且由備用電源供電
		熄滅	熄滅	無電源供應 (system LED 燈號亦熄滅), 裝置備用電源異常或並未安裝 (system 燈號亦會亮起)
3	FAN	綠色	恆亮	風扇皆運作正常
		橙色	恆亮	兩個風扇或其中一個風扇停止運轉
4	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	資料正被傳送或接收
			熄滅	無乙太網路連線
		橙色	恆亮	有連線, 但連接埠已被手動或生成樹關閉
			閃爍	連接埠處於生成樹協議阻塞、偵聽與學習狀態
5	10/100/1000 port status	綠色	恆亮	Giga 連接埠已建立 1000Mbps 連線, 或 10/100 連接埠已建立 100Mbps 連線
		橙色	恆亮	Giga 連接埠已建立 100Mbps 連線
		熄滅	熄滅	未出現 10Mbps 的狀態

第二層網路管理交換器

2.3 後背板

本交換器的後背板包含有可抽換式風扇與電源線插孔。



圖三 後背板燈號標示表

No.	標示	說明
1	Power Connector	請將電源線連接於此
2	RPS	備用電源供應連接插座
3	FAN1 _ FAN2	可更換式系統風扇

2.4 技術規格

表3 技術規格

實體尺寸	43.5mm(H) X 444 mm(W) X 265mm(D)		
電源	輸入	耗電量	
	100-240V AC/2.5A 50-60Hz	< 90 watts	
備用電源供應 (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	-10 to 50C (14 to 122° F)	-40 to 70C (-40 to 158° F)
	溼度	15 to 90%	0 to 95%
	高度	up to 10,000 ft (3,000m)	40,000 ft (12,000m)
可更換式風扇	尺寸	電壓與電流	轉速 :
	40 x 40 x 20 mm	12VDC, 0.13A	8200RPM

## GigaX 系列

---

### 3 快速安裝指南

本交換器的後背板包含有可抽換式風扇與電源線插孔。您也可以參考 GigaX 系列安裝指南進行安裝。

Part1. 指導您如何將 GigaX 交換器安裝於平坦表面或機架上。

Part2. 提供硬體設定相關介紹。

part3. 指導您如何針對 GigaX 交換器進行基本設定。

在您進行安裝動作前，請先向您的網路系統管理員取得以下相關資訊：

提供交換器使用的 IP 位址

預設的網路閘道器位址

您所處網路環境下的網路遮罩

#### 3.1 Part1— 硬體的安裝

##### 3.1.1 將交換器安裝於平坦表面

本交換器與其附屬配件需安置於可承受其重量的表面上。請將四個塑膠軟點黏附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. 請將托架分別對準交換器兩側的對應螺絲孔。本交換器與其附屬配件需安置於可承受其重量的表面上，並將四個塑膠軟點黏附於交換器底部所標示的位置。

2. 接下來，用產品包裝中的螺絲以每邊兩顆的方式對準托架與交換器上的螺絲孔，並將交換器確實地鎖緊固定於機架上。

## 第二層網路管理交換器

### 3.2 Part2— 設定交換器

請依照圖四所示，分別將您的個人電腦與網路線連接到交換器上，並將交換器的電源線插到室內插座上。

#### 3.2.1 連接控制台連接埠

若您要使用控制台介面進行管理，則您可以使用 RS-232 (DB9) 或 USB 連接線來連接本交換器。而要是您想要以網頁管理介面進行管理，則請將您的個人電腦用乙太網路線連接到交換器上。

#### 3.2.2 連接到電腦或區域網路 (LAN)

您可以使用乙太網路線來直接連接電腦與交換器的連接埠。此外，您也可以使用乙太網路線來連接交換器與集線器 (Hub)。在乙太網路線的種類上，您可使用經過跳線或未經跳線的乙太網路線來連接上述裝置。



請使用雙絞 Category 5 乙太網路線來連接 1000BASE-T 連接埠。否則，您將無法達到 1Gbps 的傳輸速率。

#### 3.2.3 連接備用電源模組 (RPS)

請將您的備用電源模組一端連接到交換器上的 RPS 插孔，接著請確認 RPS 電源模組的另一端已連接電源線。最後將電源線插到具備接地迴路的家用電源插座上。

#### 3.2.3 連接電源線

1. 請將 AC 電源線的一端連接到交換器後背版上的電源插孔，然後將電源線的另一端連接到家用電源插座或是電源延長線上。
2. 請參考列表 4 來檢查交換器前面版的燈號顯示。若燈號顯示如同列表中的敘述，便代表交換器已正常運作。

## GigaX 系列

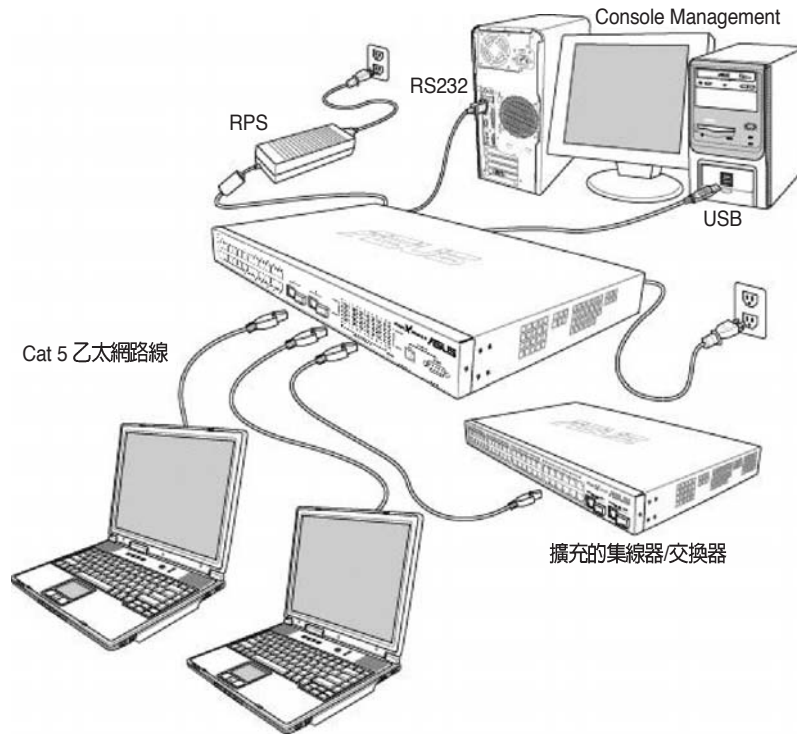


圖4 硬體連接示意圖

表3 LED 指示燈

No.	LED	說明
1	System	恆亮的綠色燈號代表裝置已啟動。若燈號是熄滅未亮起，請檢查交換器的電源線是否正確連接並已連接至電源插座。
2	Switch ports [1] to [12]	恆亮的綠色燈號代表本裝置已可連接區域網路，而若是綠燈閃爍代表交換器正從區域網路的電腦傳送或接收資料。
3	RPS	恆亮的綠色燈號代表本裝置已成功安裝 RPS 模組。
4	Fan	恆亮的綠色燈號代表所有的系統風扇皆運作正常。

## 第二層網路管理交換器

### 3.3 Part3— 交換器基本管理設定

當您完成交換器的硬體安裝與連接後，接下來便要開始對交換器進行基本管理設定。您可以使用下列兩種方式來管理本交換器。

- 網頁管理介面：本交換器內建網頁管理介面，可以讓您透過使用 Java、IE5.5（或更高版本）來進行交換器的功能設定。
- 指令列管理介面：本管理介面可讓您連接交換器前面板的控制台連接埠來進行交換器的功能管理。

#### 3.3.1 透過控制台連接埠（Console Port）進行設定

1. 使用支援跳線的 RS-232 纜線來連接交換器前面板上的控制台連接埠。此一連接埠為公端的 DB-9 接頭，可作為連接資料終端設備（DTE）的連接用途。當您將連接頭接到交換器上的連接埠後，請將接頭兩側的螺絲旋鈕轉緊，並將纜線的另一端連接到執行 Hyper Terminal 這類終端模擬軟體的個人電腦上。
2. 若要使用產品內附的 USB 纜線連接個人電腦，您需要從安裝光碟中安裝 USB 驅動程式讓 USB 連接可以正常運作。安裝 USB 驅動程式後在 Windows ME/2000/XP 作業系統中，會產生一組模擬 COM 連接埠。
3. 請確認您的終端模擬軟體設定如下所示：
  - a) 選擇適當的序列埠編號
  - b) 將資料速率設定為 9600.
  - c) 設定資料格式為無同位檢查 (No parity)、8個資料位元 (Data bit) 及 1 個停止位元 (Stop bit)。
  - d) 設定無流量控制
  - e) 將模擬模式 (Emulation mode) 設定為 VT100。
4. 待正確設定好終端機後，您將在終端機畫面上看到 “ (ASUS) ”
5. 請輸入 “login” 來進入指令行介面。在這邊預設的使用者名稱為 “Admin” 且無需輸入密碼，直接按下 <Enter> 即可。



您可隨時藉由使用 CLI 來變更密碼（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，建議變更預設密碼。

## GigaX 系列

6. 請依照下列步驟來指定 IP 給交換器使用：

- a) 輸入 “Net interface ip sw0 <your ip address> <your network mask>”，例如您的交換器 IP 位址是 192.168.10.1 且子網路遮罩是 255.255.255.0，則您應輸入 “Net interface ip sw0 192.168.10.1 255.255.255.0”。
- b) 如果交換器必須透過網路進行管理，則必須輸入一個預設的閘道器或靜態路由。請輸入 “Net route static add 0.0.0.0 <your network gateway IP> 0.0.0.01” 為您的預設路由，如下圖所示：

```
(Asus)% login
user name: admin
password: ****
user 'admin' logged in
(Asus)% net interface ip sw0 192.168.10.1 255.255.255.0
IP address set successfully
(Asus)% net route static add 0.0.0.0 192.168.10.254 0.0.0.0 1
Route added successfully
Specific route is added successfully
(Asus)% _
```

圖5 登入與 IP 設定畫面

### 3.3.2 透過 WEB 介面進行設定

如欲成功將您的個人電腦連接至交換器，您的個人電腦必須在您的網路環境中取得合法的 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。如果您想變更交換器預設的 IP 位址，請參考本產品的使用手冊中 3.3.1 節的介紹來變更 IP 位址。由於本交換器不支援 DHCP 用戶端功能，所以必須為交換器設定一個可用的固定 IP 位址。

1. 如果您是第一次登入到 Web 管理介面，則不需要輸入使用者名稱與密碼，因為網頁存取驗證的預設值是關閉的。而為了確保系統設定的安全性，請啟動 “System” 項目下的 “Administration” 選項的驗證功能。如果您的驗證功能是關閉的，請略過步驟 2。
2. 任何連接到本交換器的個人電腦皆可連線到 Web 管理介面。請打開網路瀏覽器（如微軟 Internet Explorer），並在網址列輸入 http://192.168.1.1，並按下 <Enter> 鍵。上述位址為本交換器的預設值，輸入後便會出現右圖所示的畫面。



## 第二層網路管理交換器



圖6 登入畫面

輸入您的使用者名稱與密碼後，按下 **OK** 鍵並進入 Web 設定介面“Configuration Manager”。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：(no password)



您可以隨時改變密碼。（請參閱使用手冊 5.3.1 節系統指令的說明）

3. 如欲設定一個新的 IP 位址，請點選“IP Interface”並選擇 SWO。接著請填寫 IP 位址、子網路遮罩與預設閘道器，然後點選 **OK**。
4. 如果您所設定的新位址與預設位址不同，則瀏覽器無法更新交換器狀態視窗或是重新取得任何頁面，這是正常的狀況。遇到這類狀況時，請在瀏覽器的位址列重新輸入新的 IP 位址並按一下<Enter>鍵，即可重新進入 Web 管理介面。
5. 如欲啟動 Web 連線認證功能，請點選選單列表中的“Administration”，然後選擇“Enabled”以啟動保護功能。  
在您點選 **OK** 後，會出現如下圖所示的登入畫面。



圖7 IP 設定 (GigaX 2024)

## GigaX 系列

### 4 網頁介面進行管理

本交換器提供網頁管理模式，讓您可以透過使用網際網路瀏覽器的方式進行交換器的管理工作。本網頁管理介面是專為在微軟 Internet Explorer 5.5（或更新版本）的瀏覽器執行所設計。請注意：本網頁管理介面不支援使用 Netscape 瀏覽器。

#### 4.1 登入網頁管理使用者介面

1. 首先，在個人電腦端請開啓您的網路瀏覽器，並在瀏覽器的網址列中輸入 `http://192.168.1.1` 並按下 <Enter> 鍵，這邊您所輸入的 IP 位址為交換器的出廠預設值。完成輸入後螢幕會顯示如圖 8 所示的登入視窗。

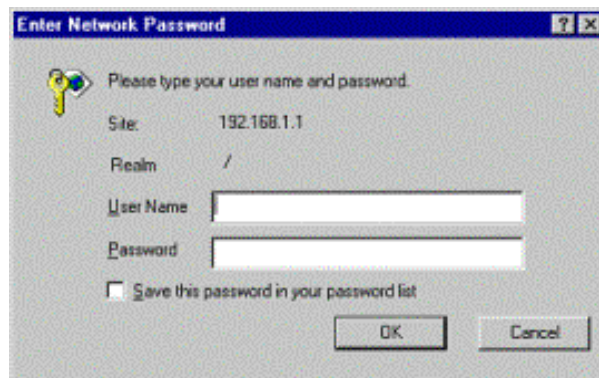


圖8 管理設定登入視窗

2. 在登入視窗中，請輸入您的使用者名稱與密碼，然後按下 **OK**。若您第一次登入此管理程式，請輸入下列帳號名稱與密碼登入。（請參考 90 頁 5.3.1 節）

預設使用者名稱（Default User Name）：admin

預設密碼（Default Password）：無須輸入密碼

每次您登入網頁管理介面後，您都會看到如圖 9 所示的網頁畫面。



若您未開啓網頁管理介面的認證功能，則便無須每次都要執行登入動作。

## 第二層網路管理交換器



圖9 網頁管理介面主畫面

### 4.2 網頁管理介面的功能結構

標準的網頁管理介面包含三個獨立的框架結構。在上方的框架中如圖 10 所示具有一交換器的圖示與交換器前面板圖，此一位於視窗上方的圖示可以同步顯示交換器前面板的 LED 燈號。請參考表 4 以了解各燈號顏色所代表的意義。關於燈號閃爍狀態所代表的意義，則請參考表 5 的燈號顏色狀態敘述。



圖10 上方框架畫面

表4 後背板標示表

連接埠顏色	狀況說明
綠色	乙太網路連線已建立
黑色	無乙太網路連線
橙色	顯示有連線，但連接埠被生成樹手動關閉

## GigaX 系列

在管理介面右下方框架中，您可以點選連接埠的圖示來顯示連接埠的相關設定狀況。

至於左側的框架中會顯示出一個如圖10 所示的選單框架，這個框架中包含所有交換器擁有的功能設定選項。這些功能都已被群組式劃分，例如系統（System）、橋接（Bridge）等功能。您可以點選框架中任何一個功能選項來開啓對應的設定頁面。



圖11 功能設定選單列表

至於右側的框架則會顯示設定頁面或以圖像顯示交換器的狀況。請參考 4.3 節的說明。

## 第二層網路管理交換器







### 4.2.1 瀏覽選單的技巧

- 如欲瀏覽同一群組中的延伸選單，請點選對應群組名稱。接下來群組名稱旁的 [ > ] 標示將會轉換為 [ V ] 並顯示其他的延伸設定選項。
- 如欲合併相關選單群組，則請點選對應的群組名稱，則 [ > ] 標示將會顯示在群組名稱旁。
- 若要開啓特定的設定頁面，則請選單中點選您所要開啓的選項。選擇的欲合併相關選單群組，則請點選對應的群組名稱，則 [ > ] 標示將會顯示在群組名稱旁。

### 4.2.2 常用按鍵與圖示

在以下列表中，將會描述在本管理介面中所有按鍵與圖示的功能。

表6 常用按鍵與圖示

按鍵 / 圖示	功能
	儲存任何您在目前頁面所作的變更。
	在系統中新增既有的設定，如固定 MAC 位址或是防火牆的 ACL 規則等設定。
	變更既有選項的設定值。
	在系統中新增既有的設定，如固定 MAC 位址或是防火牆的 ACL 規則等設定。
	清除已選載的選項，如靜態路由、ACL 規則過濾等設定。
	更新顯示目前的設定頁面與狀態。

## 4.3 系統頁面

系統頁面包含有 Management、Administration、Reboot 與 Firmware Update 功能。

### 4.3.1 Management 頁面

在 Management 頁面中包含有下列資訊：

Model Name：產品名稱

MAC Address：交換器的 MAC 位址

System Name：使用者所指定用來辨識系統的名稱（可編輯）

System Contact：（可編輯）

System Location：（可編輯）

## GigaX 系列

如欲儲存任何變更並使變更的設定立即生效，請點選 **OK**。接著請如圖 12 所示使用 **Reload** 按鍵來更新設定值。

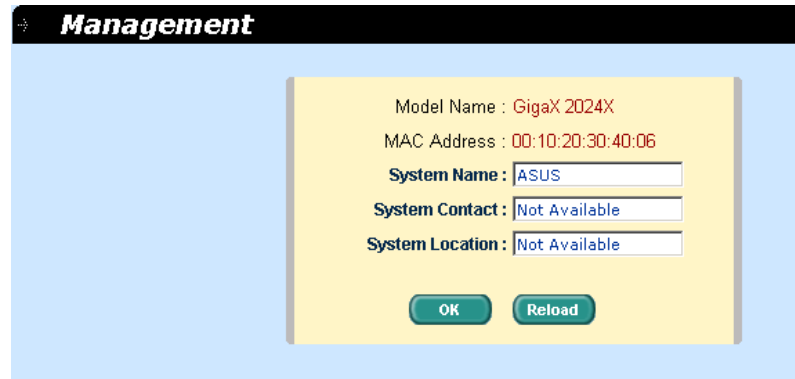


圖12 Management 頁面

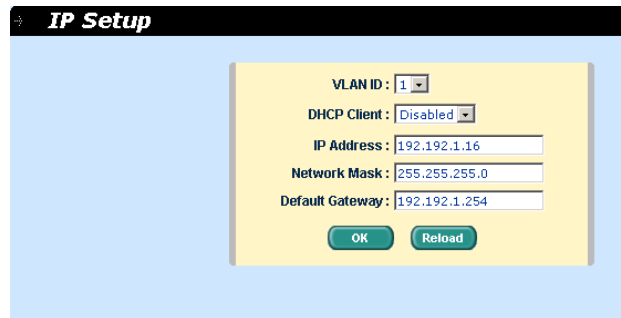
### 4.3.2 IP Setup

本交換器僅支援動態 IP 配發。在 IP Setup 頁面中包含有以下資訊：

- VLAN ID：在系統管理介面中指定一組 VLAN ID。若要使用管理介面，則必須處於相同的 VLAN 內。
- DHCP Client：開啓本項以取得一動態 IP 位址，或是關閉本項以指定一靜態 IP 位址。
- IP Address：配發一個靜態 IP 位址給交換器管理介面。
- Network Mask：網路遮罩。
- Default Gateway：預設閘道器。

如欲儲存任何變更並使其立即生效，請點選 **OK** 鍵，並如下圖所示使用 **Reload** 鍵來更新設定。

## 第二層網路管理交換器



The image shows a web interface titled "IP Setup". It contains a yellow box with the following fields: "VLAN ID" with a dropdown menu showing "1", "DHCP Client" with a dropdown menu showing "Disabled", "IP Address" with a text box containing "192.192.1.16", "Network Mask" with a text box containing "255.255.255.0", and "Default Gateway" with a text box containing "192.192.1.254". At the bottom of the yellow box are two buttons: "OK" and "Reload".

圖13 IP Setup 頁面

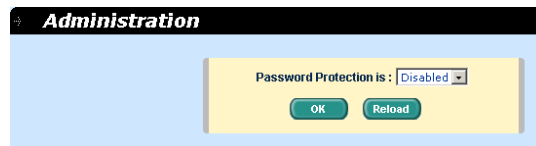
### 4.3.3 Administration 頁面

在 Administration 頁面中您可以開啓或關閉當使用者需要登入管理介面時輸入帳號與密碼的網路認證功能。在預設值中，網路連線認證功能是關閉的，無需經過任何認證。

若要儲存任何變更且讓設定立即生效，請如圖 13 所示點選 **OK** 後再選擇 **Reload** 來更新設定。當開啓密碼保護功能後，請立即重新登入。



**注意：**透過 CLI 介面，您可以隨時變更網頁管理介面的登入密碼。



The image shows a web interface titled "Administration". It contains a yellow box with the following field: "Password Protection is:" with a dropdown menu showing "Disabled". At the bottom of the yellow box are two buttons: "OK" and "Reload".

### 4.3.2 Reboot 頁面

在 Reboot 頁面中包含有一 [Reboot] 按鈕，點選本按鈕即可進行交換器的硬體重置動作。



**系統重置動作將會暫時中斷網路連線與網路管理介面的連線。**

圖17 Administration 頁面

## GigaX 系列

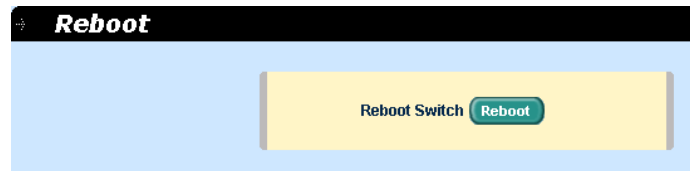


圖15 Fireware Upgrade 頁面

### 4.3.5 Firmware Upgrade

在 Fireware 頁面中包含有以下資訊：

- Hardware Version：顯示硬體版本編號。
- BootROM Version：顯示 boot code 的版本。
- Fireware Version：顯示目前所執行的韌體版本。本編號會隨著韌體的升級而改變。

請直接輸入韌體所存放的位置，或點選 **Browse...** 來選擇檔案所儲存的路徑與名稱。選擇完畢後請點選管理頁面中的 **Upload** 來升級交換器韌體。請參考圖 14。



請點選 **upload** 鍵來將指定的韌體載入到交換器中，並在韌體更新成功後進行系統重啟動作。系統重置後您必須進行重新登入才可以再次進入網頁管理介面。

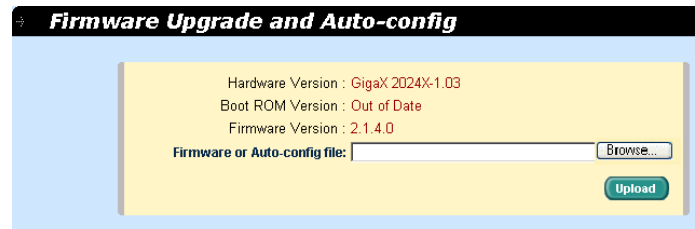


圖16 Fireware Upgrade 頁面



## 第二層網路管理交換器

### 4.4 實體介面

本交換器的實體介面會即時顯示乙太網路連接埠的狀態。你可以針對連接埠進行下列幾個項目的設定。

Port：選擇您所要進行設定的連接埠。

Admin：開啓或關閉連接埠。

Mode：設定速度與雙工模式。

Flow Control：開啓 / 關閉 802.3x 流量控制機制。

Port Status Window：顯示每個連接埠以下的相關資訊。

a) Link status：顯示既有連線的速度與雙工模式，若無顯示則代表無連線狀態

b) State：顯示 STP 狀態

c) Admin：開啓或關閉網路連接埠的設定

d) Mode：連線速度與雙工模式的設定

e) Flow Control：開啓或關閉 802.3x 流量控制機制的設定。

您可以選擇對應網路連接埠的埠號並對其進行設定，接著點選 **Modify** 鍵，而您所變更的項目將會在視窗顯示內容做出更新。然而，在您點選“Safe Configuration”之前，您所作的設定將不會生效。

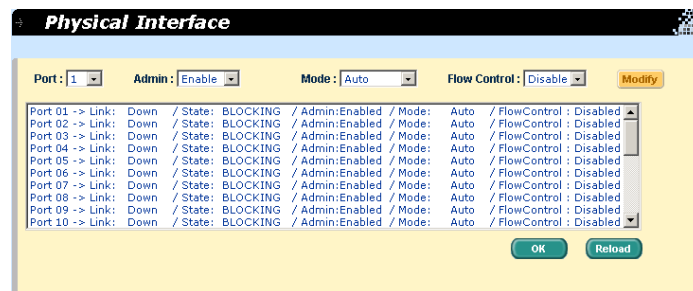


圖17 實體介面

## GigaX 系列

---

### 4.5 橋接 (Bridge)

在 Bridge 橋接頁面群組中，包含有兩層設定，像是 Link aggregation, STP 等設定項。

#### 4.5.1 生成樹 (Spanning Tree)

生成樹協定 (STP) 設定頁面可在執行時開啓或關閉該功能。本頁面總共包含三個部份。

第一部份將會顯示根交換器的相關資訊。這個頁面會告知使用者根交換器的 STP 設定。

至於第二部份則是 STP 設定，共有以下選項可供您設置：

**Disable / Enable**：開啓或關閉 STP，當您開啓 STP，若交換器為根交換器，則 STP 會採用如下設定值。

**Hello Time**：BPDU 生成設定的間隔

**MAX Age**：為區域網路所有橋接裝置所使用的中斷時間設定值

**Forward Delay**：本項目為區域網路所有橋接裝置所使用的中斷時間設定值

**Bridge Priority**：區域網路中交換器的優先順序

而第三部份則是網路連接埠的設定。本頁面包含一視窗顯示目前每一個網路連接埠的設定狀況。您可以點選 **Modify** 來變更每一個通訊連接埠的 STP 設定。本頁面共有以下選項可供您設置：

**Port**：選擇對應連接埠進行設定

**Priority**：設定交換器網路連接埠的優先順序，較低的數值代表較高的優先順序。在網路迴路被偵測到的狀況下，優先順序較低的網路連接埠較可能被 STP 所阻隔。

**Cost**：此一設定的有效數值從 1 至 65535。在網路迴路被偵測到的狀況下，較高的數值則較可能被 STP 所阻隔。

**Fast Link**：設定當連線建立時將連接埠設為傳送狀態，而連接埠接下來亦會加入 STP 中。

**Edge Port (邊緣連接埠)**：所有的連接埠在預設值中被設定為邊緣連接埠。當 BPDU 被接收時，則邊緣連接埠將會變成 STP 連接埠。邊緣連接埠可以在很短的時間內就進入轉發狀態。

**Point to Point: Auto/Yes/No**。全雙工的連線會被判斷為點對點連線。否則，便會被判斷為分享連線。點對點連線將會具有較短的聚合時間。所以在大多數狀態下，建議設定為 **Auto**。

## 第二層網路管理交換器

點選 **OK** 來讓設定生效。點選 **Reload** 來將更新目前的設定值。

**Spanning Tree**

**Root Information**

Root Port :	None	Bridge Hello Time :	2
Root Port Path Cost :	0	Bridge Max Age :	20
Root MAC Address :	00:10:20:30:40:06	Bridge Forward Delay :	15
Switch MAC Address :	00:10:20:30:40:06	Root Bridge Priority :	32768

**STP Setting**

Spanning Tree is : **Disabled**

Hello Time : **2** (1 - 10 seconds)      Max Age : **20** (6 - 40 seconds)

Forward Delay : **15** (4 - 30 seconds)      Bridge Priority : **32768** (0 - 61440)

**Port setting**

Port : **1**      Priority : **128**      Path Cost : **200000**

Edge Port : **True**      Point-to-point : **Auto**      **Modify**

Port 1 ->	priority:128 / Cost: 200000 / EdgePort: True / Point-to-point: Auto
Port 2 ->	priority:128 / Cost: 200000 / EdgePort: True / Point-to-point: Auto
Port 3 ->	priority:128 / Cost: 200000 / EdgePort: True / Point-to-point: Auto
Port 4 ->	priority:128 / Cost: 200000 / EdgePort: True / Point-to-point: Auto
Port 5 ->	priority:128 / Cost: 200000 / EdgePort: True / Point-to-point: Auto
Port 6 ->	priority:128 / Cost: 200000 / EdgePort: True / Point-to-point: Auto
Port 7 ->	priority:128 / Cost: 200000 / EdgePort: True / Point-to-point: Auto
Port 8 ->	priority:128 / Cost: 200000 / EdgePort: True / Point-to-point: Auto
Port 9 ->	priority:128 / Cost: 200000 / EdgePort: True / Point-to-point: Auto
Port 10 ->	priority:128 / Cost: 200000 / EdgePort: True / Point-to-point: Auto

**OK**      **Reload**

圖18 生成樹頁面

### 4.5.2 連結彙聚 (Link aggregation)

本頁面是用以設定連結彙聚群組（連接埠幹線）。本交換器可以設定 6 組 連結彙聚群組。

Show Trunk：選擇 “Add a new Trunk” 來建立一新群組。或是，您也可以選擇一組既有的群組，用來顯示其後的設定項與連接埠圖示。

## GigaX 系列

---

**Port Selection Criterion**：依據連結彙聚群組封包來源的 MAC 位址、封包目的地的 MAC 位址、封包來源與目的地的 MAC 位址、封包來源的 IP 位址、封包目的地的 IP 位址，或是封包來源與目的地的 IP 位址，利用演算方式來分配封包。

**Name**：群組名稱

**Trunk ID**：除了群組名稱之外，用來辨識幹線群組的號碼

**LACP**：在選定的幹線中開啓/關閉 LACP。LACP 功能被固定為主動（Active）模式。

**Remove Trunk**：移除已選定的幹線。

**Port Icon**：這些連接埠圖示的配置與交換器前面板的連接埠配置一致。您必須點選連接埠圖示來選擇群組號碼。利用再次點選該圖示的方式，則可以將連接埠自群組中移除。

點選 [OK] 來將設定傳送到交換器（HTTP 伺服器）。點選 [Reload] 來將設定值更新至目前的設定。如要讓設定值生效，請至“Save configuration”頁面接著點選 [Save] 來儲存設定。

您必須檢查連線速度與雙工模式來確定幹線實體正處於正確運作狀態。請至“Physical Interface”以便在連線運作狀態視窗中檢視幹線連接埠的連線模式。如果所有的幹線連接埠都處於一致的連線速度與雙工模式，則表示您的幹線設定正確。若是連線速度與雙工模式不一致則表示您的幹線設定錯誤。請檢查您的幹線設定以便讓群組成員可以具有相同的連線速度與雙工模式。

- 
- 所有連結彙聚群組的連接埠必須在全雙工模式下運作且具有相同的速率。
  - 所有連結彙聚群組的連接埠必須設定 auto-negotiation 或全雙工模式。本項設定將可讓連接埠在全雙工模式下運作。如果您設定強制全雙工模式，則其他的連接埠也必須使用相同的設定，否則連結彙聚將可能發生運作異常的狀況。
  - 所有連結彙聚群組的連接埠必須屬於相同的虛擬區域網路（VLAN）。
  - 所有在連結彙聚群組中的連接埠都被視為一邏輯連線，也就是說，任何群組成員變更設定則其他成員將會一同變更。舉例來說，一個包含有連接埠 1 與連接埠 2 的幹線群組，如果連接埠 1 的虛擬區域網路設定變更，則連接埠 2 的虛擬區域網路設定也會一同變更。
-

## 第二層網路管理交換器

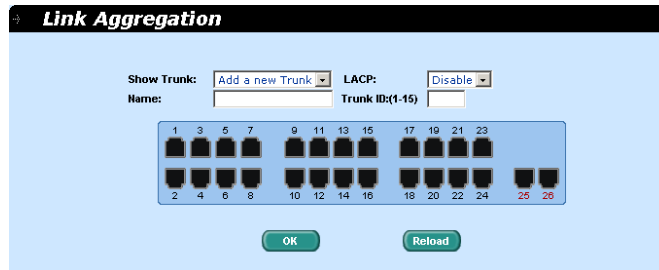


圖19 連結彙聚頁面

### 4.5.3 鏡像 (Mirroring)

以鏡像配合網路流量分析，可以協助您監控網路傳輸狀況。您可以監控所選定連接埠之傳出與傳入封包。

**Mirror：**選擇鏡像群組。每一個群組包含有 24 個 Fast Ethernet 網路連接埠與 1 個 Gigabit 網路連接埠。（僅適用於 GigaX 2048）

**Mirror Mode：**開啓或關閉所選定群組之鏡像功能。

**Monitor Port：**接收所有選定連接埠傳輸狀況的備份資料。

GigaX 2048 具有兩個監控埠，此一連接埠可以監測 24 個高速乙太網路連接埠與 2 個 Gigabit 連接埠。

GigaX 2024 只具有一個監控埠，此一連接埠可以監測 24 個高速乙太網路連接埠與 2 個 Gigabit 連接埠。

**鏡像連接埠不屬於任何連結彙聚群組。而鏡像連接埠也不能如一般交換器連接埠一樣進行運作，且不能交換封包或是進行位址記憶。**

點選 **OK** 來將設定傳送到交換器（HTTP 伺服器），而點選 **Reload** 則重新載入目前的設定。

## GigaX 系列

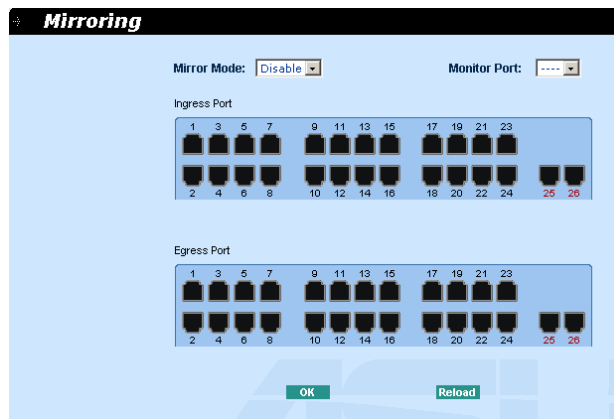


圖20 鏡像頁面

### 4.5.4 靜態多重播送 (Static Multicast)

在本頁面中，您可以在播送列表中新增播送位址。在交換器中共可以擁有 256 個多重播送位址。所有群組中的連接埠將換傳送特定的多重播送封包至群組中其他的連接埠。

**Show Group**：選擇 “Add a new group” 來輸入一個新的位址。或是選擇顯示一個既定群組的位址。

**MAC Address**：選擇多重播送位址。

**VLAN ID**：選擇虛擬網路群組。

**CoS**：指定服務等級的優先順序。

點選 [OK] 來將設定傳送到交換器（HTTP 伺服器），而點選 [Reload] 則重新載入目前的設定。

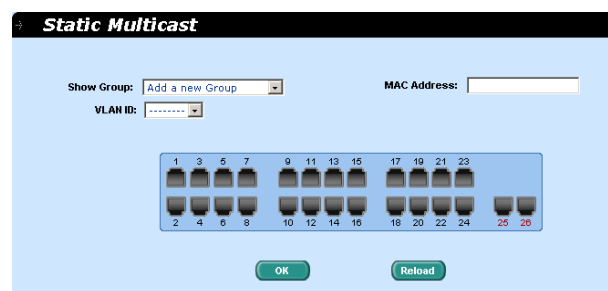


圖21 固定多重播送 (GigaX 2048)

## 第二層網路管理交換器

### 4.5.5 IGMP 偵聽 (IGMP Snooping)

藉由開啓或關閉 IGMP 偵聽功能，可以減少網路環境中多重播送的傳輸狀況。當本功能開啓時，交換器會偵聽 IGMP 封包並將新群組放置到多重播送列表中。然而，若是靜態位址已完全佔用 256 組的位址空間，IGMP 偵聽功能便無法正常運作。本交換器只允許擁有 256 組第二層多重播送群組。

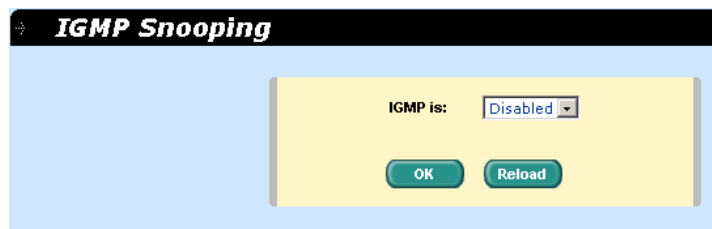
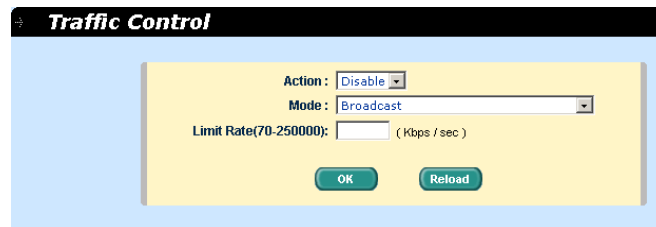


圖22 IGMP 偵聽

### 4.5.6 流量控制 (Traffic control)

流量控制功能可以避免交換器湧入過多包括廣播封包、多重播送封包與因為目標位址搜尋失敗的單一播送封包，以避免系統頻寬異常負荷。本頁面所輸入的限制數字為已知類型之所有封包的總和。舉例來說，若是啟動廣播與多重播送，則所有這兩種類型的封包傳輸量將不會超過您所輸入的限制數值。點選 **OK** 來將設定傳送到交換器（HTTP 伺服器）。如要讓設定值生效，請至“Save Configuration”頁面接著點選 **Save** 來儲存設定。

## GigaX 系列



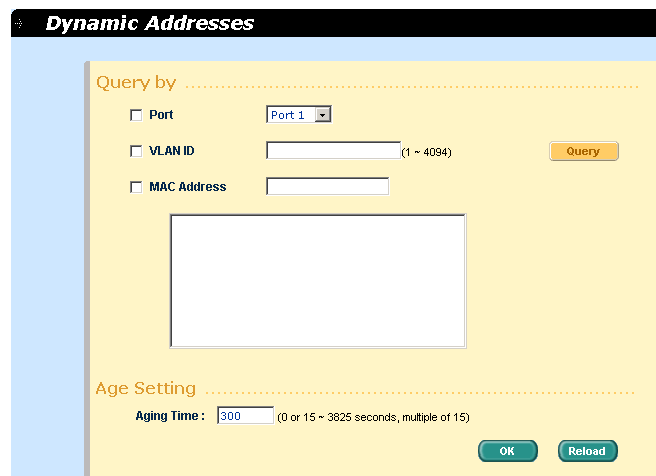
The screenshot shows the 'Traffic Control' configuration page. It features a yellow background with a black header bar containing the title 'Traffic Control'. Below the header, there are three main configuration fields: 'Action' set to 'Disable', 'Mode' set to 'Broadcast', and 'Limit Rate(70-250000)' with an empty input box and '( Kbps / sec )' label. At the bottom, there are two green buttons labeled 'OK' and 'Reload'.

圖23 傳輸控制

### 4.5.7 動態位址 (Dynamic address)

本頁面會顯示依連接埠、VLAN ID，或特定 MAC 位址進行動態 MAC 位址搜尋後的結果。動態位址為交換器所記憶的 MAC 位址，因此若是在位址存活期間內位址沒有再次進行記憶，則該位址便可能不正確。使用者在此可以從 10 至 1,000,000 秒，自行設定位址存活的時間。設定完畢後請接著點選 **OK** 來設定新的更新時間數值。如要讓設定值生效，請至“Save configuration”頁面接著點選 **Save** 來儲存設定。

此外，您也可以藉由點選 **Query** 檢查連接埠的VLAN ID 與 MAC 位址的方式來搜尋 MAC 位址。查詢完畢後的結果，視窗會已顯示位址的方式來表示。



The screenshot shows the 'Dynamic Addresses' configuration page. It features a yellow background with a black header bar containing the title 'Dynamic Addresses'. Below the header, there are three query options: 'Port' (selected), 'VLAN ID', and 'MAC Address'. The 'Port' option has a dropdown menu showing 'Port 1'. The 'VLAN ID' option has an input box with '(1 ~ 4094)' next to it. The 'MAC Address' option has an empty input box. A yellow 'Query' button is located to the right of the input boxes. Below the query options, there is a large empty rectangular box for results. At the bottom, there is an 'Age Setting' section with an 'Aging Time' input box set to '300' and a label '(0 or 15 ~ 3825 seconds, multiple of 15)'. At the bottom right, there are two green buttons labeled 'OK' and 'Reload'.

圖24 動態位址



## 第二層網路管理交換器

### 4.5.8 靜態位址 (Static addresses)

您可以將 MAC 位址新增進交換器的位址列表中。藉由這麼做，MAC 位址便不會發生因未更新而導致位址列表發生不正確的狀況。

MAC Address：輸入 MAC 位址。

VLAN ID：輸入 MAC 位址所歸屬的 VLAN ID。

Port Selection：選擇 MAC 位址所歸屬的連接埠。

當您依據上述資訊來建立一個新的靜態 MAC 位址時，請點選 **Add**，接著在位址視窗中您將會見到一個新的位址。您也可以使用滑鼠來選擇位址並點選 **Remove** 鍵的方式，您便可以刪除既有的位址。至於 **Modify** 鍵則可以更新既有的 MAC 位址。請點選 **OK** 來進行儲存，或是點選 **Reload** 鍵來重新載入目前的設定。如要讓設定值生效，請至“Save configuration”頁面接著點選 **Save** 來儲存設定。

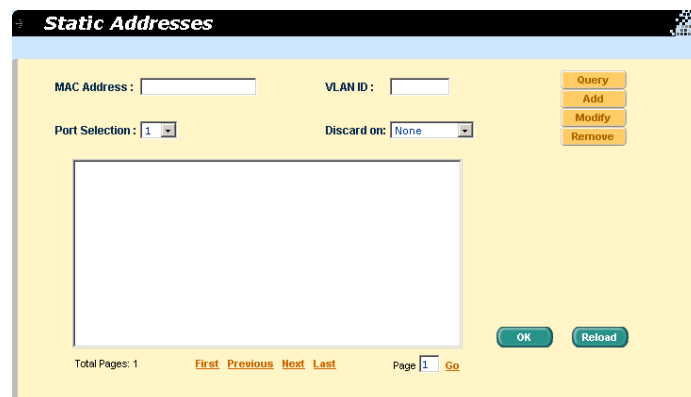


圖25 固定位址

## GigaX 系列

### 4.5.9 標示 VLAN (Tagged VLAN)

在本頁面中，您可以設定並顯示最多 4094 組 VLAN 群組。在交換器中已建立有一組預設的 VLAN，而這組 VLAN 是無法移除的。本功能是爲了避免交換器的不正確運作狀況。除了這組預設的 VLAN 之外，您可以移除任何既存的 VLAN。

您可以指定一個連接埠作爲已標示的連接埠，或是點選連接埠來解除標示連接埠。在本頁面中共會顯示三種類的按鍵：

“U”：從該連接埠傳送出去的封包會被移除 VLAN tag。

“T”：自本連接埠傳輸的所有的封包都將被標示。

空白：本連接埠並非 VLAN 群組的成員。



若是一未經標示的連接埠在同一時間內屬於兩個或更多的虛擬網路群組，將有可能造成交換器的混亂並導致流量壅塞狀況。因此如果要避免這類狀況，交換器只能允許某個未加標示之連接埠在同一時間只屬於一個 VLAN。此即稱爲“PVID”，並設定在“Default Port VLAN & CoS”頁面中。若您要將不加標示的連接埠從某一 VLAN 配置到另一個 VLAN，則您必須將其從原本的 VLAN 群組中移除，或是在原本的 VLAN 群組中，先將其設定爲已標示狀態。

**Show VLAN**：選擇既有的 VLAN 來顯示或選擇“Add a new VLAN”來建立一新的 VLAN 群組。

**Name**：VLAN 群組的名稱。

**VLAN ID**：當一組新的 VLAN 群組被建立時，本項中會要求使用者輸入 VLAN ID。

**Remove VLAN**：移除既有的 VLAN 群組。本項目在 VLAN 建立頁面中會消失。

請點選  來儲存設定。如要讓設定值生效，請至“Save Configuration”頁面接著點選  來儲存設定。

## 第二層網路管理交換器

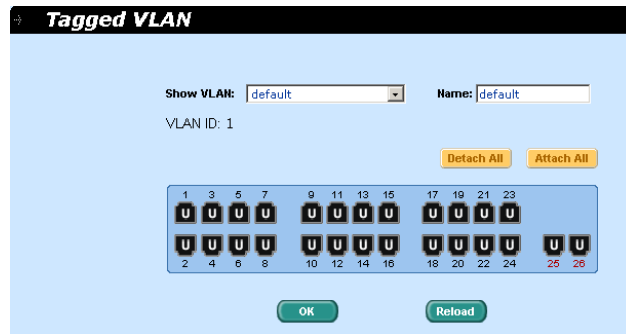


圖26 標示虛擬網路

### 4.5.10 預設連接埠VLAN 與服務等級（CoS）

本頁面中包含某些與虛擬網路標示相關的設定項目。這些選項包含有：

**Port：**選擇要進行設定的連接埠。

**PVID：**以連接埠為基礎的 VLAN ID。所有自本連接埠所接收未經標示的封包都會以這個 VLAN 群組 ID 進行標示。

**CoS（Class of Service）Value：**所有自本連接埠所接收未經標示的封包都會使用指定的 CoS 值（在 VLAN 標示中）。

請點選 **Modify** 來變更連接埠列表視窗的內容。點選 **OK** 來儲存設定值。如要讓設定值生效，請至“Save Configuration”頁面接著點選 **Save** 來儲存設定。

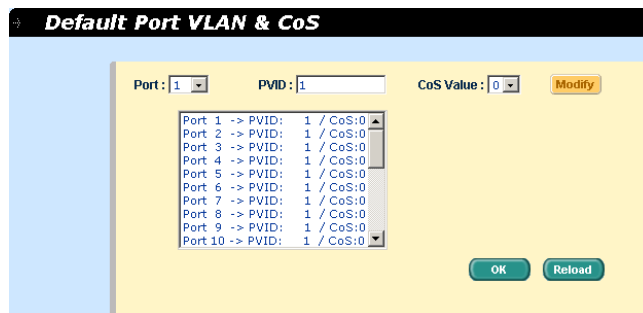


圖27 預設連接埠 VLAN 與服務等級 CoS

## GigaX 系列

### 4.5.11 CoS Queue Mapping (CoS Queue Mapping)

本交換器支援每個連接埠 4 組對外佇列。在每一個佇列，您可以指定如下列的排成類型：

- 強制優先排程：每個 CoS 數值可以導向 4 組佇列之一。其中佇列 4 具備最高的優先權來傳送封包。而在較低優先順序的佇列的封包便不會被傳送直到所有較高優先順序的佇列都已清空。在強制優先排程中，權重設定都會被設定為 0。
- Weightted round-robin (WRR) 排程：這項排成會需要您設定一數字來指明與 CoS 佇列相關之佇列的重要性（權重）。WRR 排程可以在高優先權佇列進行傳輸時，也避免低優先順序的佇列被完全忽略。WRR 排程會每個佇列中輪流進行傳輸。所傳送封包的數目與具有相同重要性的佇列相對應。舉例來說，當佇列 1 具備權重 1，則佇列 2 具備權重 2。從佇列 1 傳送 1 個封包等於每兩個從佇列 2 所傳送的封包。利用這種排程方式，則當較高優先權之佇列尚未清空前，具備較低優先權的佇列也還是能夠傳送封包。固定的權重為 1,2,4,8。

點選 **OK** 來將設定值傳送到交換器，或是點選 **Reload** 來將設定值更新到目前的設定。若要讓設定生效，請至“儲存設定”頁面接著點選 Save 鍵即可。

Priority	CoS Queue
0	Queue 2
1	Queue 1
2	Queue 1
3	Queue 2
4	Queue 3
5	Queue 3
6	Queue 4
7	Queue 4

圖28 CoS 佇列導向 頁面

### 4.6 簡易網路管理通訊協定 (SNMP)

本群組提供包含群組列表、主機列表與 Trap 設定在內的 SNMP 設定。

#### 4.6.1 群組列表 (Community Table)

您可以建立不同的群組並自訂存取，在這裡輸入群組名稱，並勾選其是否具有設定（寫入存取）的權力。點選 **OK** 來永久保存設定或點選 **Reload** 重新載入目前的設定。



The image shows the 'Community Table' configuration window. It has a title bar with a plus icon and the text 'Community Table'. The main area is a yellow box containing a table with two columns: 'Community Name' and 'Set'. The 'Community Name' column has input fields with 'private' and 'public' entered. The 'Set' column has checkboxes, with the first one checked. Below the table are 'OK' and 'Reload' buttons.

Community Name	Set
private	<input checked="" type="checkbox"/>
public	<input type="checkbox"/>
	<input type="checkbox"/>
	<input type="checkbox"/>
	<input type="checkbox"/>
	<input type="checkbox"/>
	<input type="checkbox"/>

圖29 群組列表

#### 4.6.2 主機列表 (Host table)

本頁面將主機的 IP 位址對照到在群組頁面所輸入的群組名稱。請輸入 IP 位址並從下拉式選單中選擇群組名稱。點選 **OK** 來立即儲存設定或是點選 **Reload** 來更新頁面。



The image shows the 'Host Table' configuration window. It has a title bar with a plus icon and the text 'Host Table'. The main area is a yellow box containing a table with two columns: 'Host IP Address' and 'Community'. The 'Host IP Address' column has input fields with '127.0.0.1' and '0.0.0.0' entered. The 'Community' column has dropdown menus with 'private' and 'public' selected. Below the table are 'OK' and 'Reload' buttons.

Host IP Address	Community
127.0.0.1	private
0.0.0.0	public
	private
	private
	private
	private
	private
	private
	private
	private

圖30 主機列表

## GigaX 系列

### 4.6.3 Trap 設定 (Trap Setting)

藉由設定 Trap 目的地 IP 位址與群組名稱，您可以啟動 SNMP Trap 功能在不同的版本中（v1 或 v2c）傳送 Trap 封包。點選 **OK** 來立即儲存設定或是點選 **Reload** 來更新頁面。

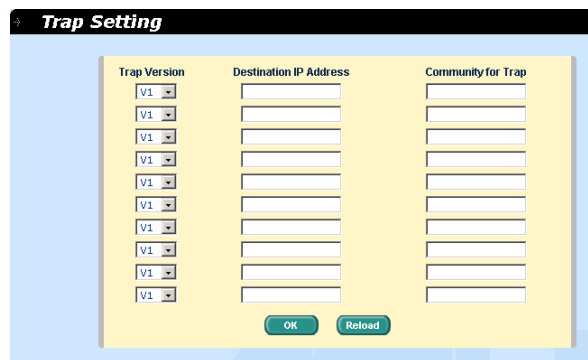


圖31 攔截設定

### 4.6.4 VACM 群組 (VACM Group)

VACM (View-based Access Control Model) 是以檢視為基礎的存取控制模型。

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。可以藉此取得像是 GetNext、GetBulg 這些相關的 SNMP 訊息。

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

Notify View Name：輸入群組所屬的通知檢視名稱。相關的 SNMP 訊息為 Trap、Report。

Security Model：輸入群組所屬的安全模型名稱。Any 適用於 v1, v2, v3。USM 則與 SNMPv3 相關。

Security Level：輸入群組所屬的安全層級名稱。只有 NoAuth, AuthNopriv, AuthPriv 可加以選擇。

當您要想要藉由上述資訊建立一組新的 VACM 群組項目，請點選 **Add**。接著您便可以在群組視窗中看見新增的項目。此外，您也可以藉由選定視窗中的項目並點選 **Remove** 來移除既有的群組。至於按下 **Modify** 鍵則可更新既有的 VACM 群組項目。點選 **OK** 來儲存設定值並使其生效。點選 **Reload** 來更新設定到目前的設定值。若要讓設定值生效，請至 "Save Configuration" 頁面接著點選 **Save** 來儲存設定。

## 第二層網路管理交換器

View Name	Security Model	Security Level	Security View
initial	-->PV: all	/WV: all	/NV: none
ro_auth	-->PV: all	/WV: none	/NV: none
rw_auth	-->PV: all	/WV: all	/NV: none
rw_noauth	-->PV: all	/WV: none	/NV: none

圖32 VACM 群組

### 4.6.5 VACM 檢視 (VACM View)

VACM (View-based Access Control Model, 以檢視為基礎的存取控制模型)。

**View Name**：輸入安全群組名稱。

**View Type**：選擇檢視所屬的檢視型式，當 View Subtree 符合 SNMP v3 訊息的 Oid 時，可選擇包含 (Include) 或排除 (Exclude)。

**View Subtree**：輸入檢視所屬的 View Subtree 名稱。此一 Subtree 需為符合 SNMPv3 訊息中的 Oid。當 Subtree 短於 SNMPv3 訊息中之 Oid 即為良好的符合狀態。

**View Mask**：輸入檢視所屬的 View Mask。遮罩中的每一位元代表 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。

當您想要藉由上述資訊建立一組新的 VACM 檢視項目，請點選 **Add**。接著您便可以在檢視視窗中看見新增的項目。此外，您也可以藉由選定視窗中的項目並點選 **Remove** 來移除既有的檢視。至於按下 **Modify** 鍵則可更新既有的 VACM 檢視項目。點選 **OK** 來儲存設定值並使其生效。點選 **Reload** 來更新設定到目前的設定值。若要讓設定值生效，請至 "Save Configuration" 頁面接著點選 **Save** 來儲存設定。

## GigaX 系列



圖33 VACM 檢視

### 4.6.6 USM 使用者

USM (User-based Security Model, 以使用者為基礎的安全模型) 本功能可用來作為設定 SNMPv3 USM User 資訊的用途。

**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。若選擇 NoAuth，則無須輸入密碼。

**Auth Password**：輸入 Auth Protocaol 所屬的密碼。在這裡密碼必需是至少八位數的數字或號碼。

**Priv Protocol**：輸入 Engine Id 與名稱所屬的 Priv Protocol。在這當中只能選擇 NoPriv, DES。若選擇 NoPriv，則無須輸入密碼。

**Priv Password**：輸入 Priv Protocol 所屬的密碼。在這裡密碼必需是至少八位數的數字或號碼。

當您要想要藉由上述資訊建立一組新的 USM 使用者項目，請點選 **Add**。接著您便可以在使用者視窗中看見新增的項目。此外，您也可以藉由選定視窗中的項目並點選 **Remove** 來移除既有的使用者。至於按下 **Modify** 鍵則可更新既有的 USM 使用者項目。點選 **OK** 來儲存設定值並使其生效。點選 **Reload** 來更新設定到目前的設定值。若要讓設定值生效，請至“Save Configuration”頁面接著點選 **Save** 來儲存設定。



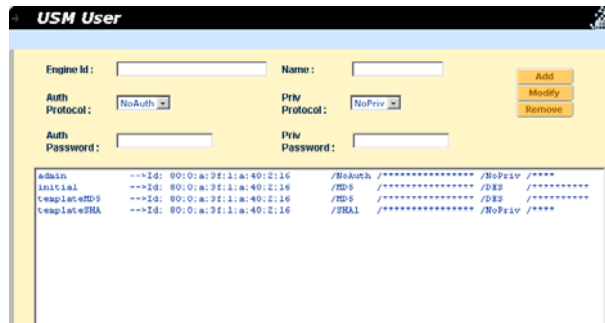


圖34 USM 使用者

### 4.7 安全功能 (Security)

本交換器具有 802.1x port-based 的安全功能。只有通過認證的主機可以透過交換器的連接埠進行存取，至於未經認證的存取行為則會被阻擋。認證服務是由一組 RADIUS 伺服器或是交換器本地端的資料庫（只支援 MD5 認證）所提供。

此外，本交換器亦支援透過 802.1x 認證作業進行動態 VLAN 配發。提供使用者/連接埠的 VLAN 資訊應該在開啓本功能前，先行在認證伺服器進行正確的設定。

#### 4.7.1 連接埠存取控制 (Port Access Control)

連接埠存取控制可用以設定多項 802.1x 參數。而 802.1x 可使用 RADIUS 伺服器或是連接於通過認證之連接埠之使用者以本地端資料庫進行設定。

## GigaX 系列

第一部份為橋接（Bridge）設定：

**Reauthentication**：當開啓本項目，交換器將會在重新認證時間到時，試圖再次認證連接於該連接埠的使用者輸入目的地 IP 位址。


**Reauthentication Time**：若本項目設定開啓，則表示連接到該連接埠之使用者需要再次進行認證的時間。

**Authentication Method**：RADIUS 或本地端資料庫可以用來供使用連接埠的使用者進行認證之用。

**Quiet Period**：無論從 RADIUS 伺服器或是本地端資料庫認證失敗，交換器會再次發出重新認證訊息給使用者的這段間隔時間。

**Retransmission Time**：若使用者無法回應來自交換器的認證要求，則交換器再次發出重新認證訊息給使用者的這段等待間隔時間。

**MAX Reauthentication Attempts**：若使用者無法從交換器回應認證要求的重新嘗試次數。

第二部份為連接埠（Port）設定，若您要調整設定則請點選 。

**Port**：指定所要進行設定的連接埠。

**Multi-host**：若本項目設定開啓，則所有連接到被選定之連接埠的主機中，只要有一部主機通過認證，則視為所有的主機都已通過認證。若設定關閉，則只有通過認證的主機可以透過該連接埠進行存取。

**Authentication Control**：若選擇“force\_authorized”，則被選定的連接埠會被視為已強制通過認證。因此，來自所有主機的流量是被允許通過的。反過來說，當選擇“force\_unauthorized”，則被選定的連接埠會被阻擋無法進行傳輸行為。若是選擇“Auto”，則被選擇之連接埠的傳輸動作是由 802.1x 通訊協定所控制。在一般使用狀態下，建議將所有連接埠設定為“Auto”。

**Guest VLAN**：指定一訪客 VLAN 給不相容於 802.1x 的用戶端。

點選  來儲存設定。或是點選  來將設定更新至目前的設定值。

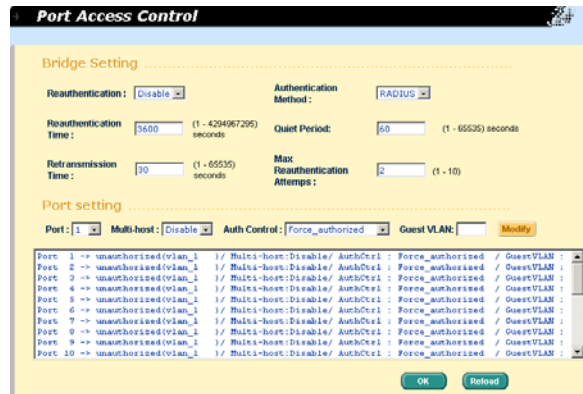


圖35 連接埠存取控制

### 4.7.2 撥入使用者（Dial-In User）

撥入使用者選項是用來定義交換器資料庫中的使用者。

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。

Dynamic VLAN：指定 VLAN ID 給通過 802.1x 認證的用戶端。

MAX Reauthentication Attempts：若使用者無法從交換器回應認證要求的重新嘗試次數。

請點選 **Add** 來新增使用者。當您設定完畢則請點選 **Modify**。而要是您想要移除選定的使用者，則請點選 **Remove**。若要套用設定請點選 **OK**。若想將設定值更新到目前的設定，請點選 **Reload**。

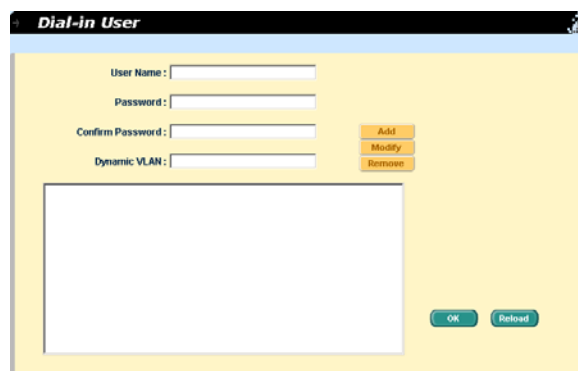


圖36 撥入使用者

## GigaX 系列

### 4.9.3 RADIUS

若要使用外部 RADIUS 伺服器，則需要進行以下的參數設定：

Authentication Server IP：RADIUS 伺服器的 IP 位址。

Authentication Server Port：聆聽 RADIUS 伺服器的連接埠號。

Authentication Server Key：用以連接 GigaX 交換器與 RADIUS 伺服器間的金鑰。

Confirm Authentication Key：再次輸入上述的金鑰。

**連接至交換器之 RADIUS 伺服器的 VLAN 必需與系統管理介面的 VLAN 相同。**

請點選  來讓設定值生效。若想將設定值更新到目前的設定，請點選 。

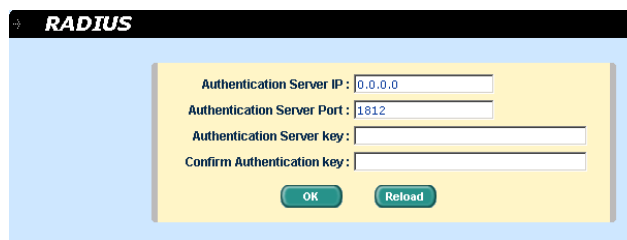


圖37 RADIUS

## 4.8 統計圖表 (Statistic chart)

在統計圖表頁面中，可以利用不同類型的圖表來標示網路流量。您可指定一段特定時間作為更新圖表的頻率設定。藉由使用這些頁面中的不同圖表，您也可以隨時監控網路傳輸狀況。大多數的 MIB-II 計數器將會在這些圖表中顯示出來。

您可以藉由點選 Refresh Rate 來設定自交換器接收更新資料的間隔時間。您也可以利用選用不同 Color 標示的方式來區隔不同的統計值或連接埠。最後，請點選 Draw 來讓瀏覽器開始繪製統計圖表。每一個新的圖表 Draw 也會重置統計值的顯示。

#### 4.8.1 傳輸狀況比較 (Traffic comparison)

本頁面將會在同一圖表中顯示所有連接埠單一項目的統計圖表。您可以選擇特定的統計項目並點選 **Draw**，接下來瀏覽器便會顯示出更新的資料與更新這段期間的統計圖表。

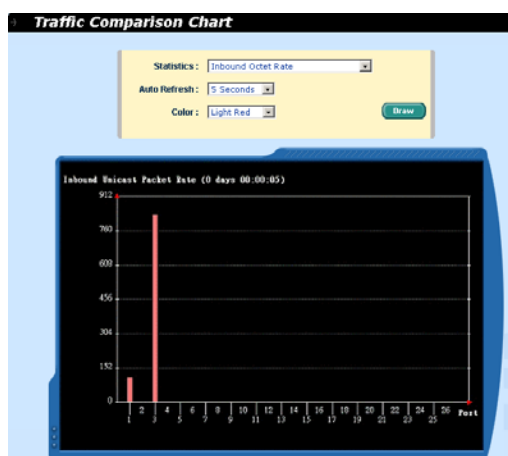


圖38 傳輸狀況比較

### 4.8.2 錯誤群組 (Error Group)

選擇 **Port** 與指定顯示 **Color**，接著點選 **Draw**後，統計視窗便會顯示出特定連接埠中，所有遺失與錯誤的統計。本資料會在一定的時間間隔內進行更新。

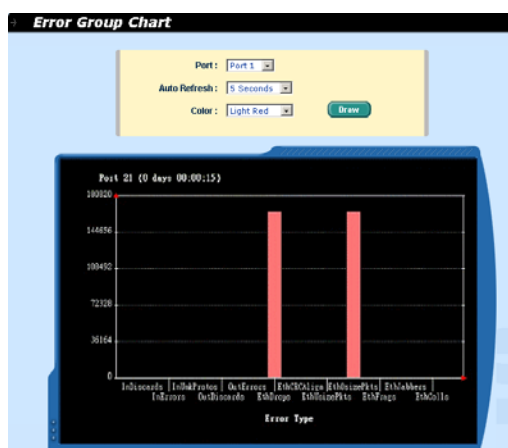


圖39 錯誤群組

## GigaX 系列

### 4.8.3 歷程狀態 (Historical Status)

在本圖表中，您可以選擇顯示不同連接埠與統計選項的資訊。從本圖表中，顯示出統計資訊的歷程。即使資料以更新，線條圖仍舊會保留舊的統計資料。

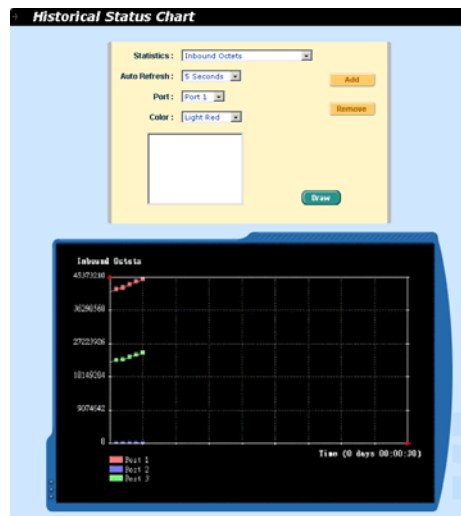


圖40 歷程狀態

### 4.9 儲存設定值 (Save configuration)

如果要永久儲存所變更的設定值，您必須點選 **Save** 加以儲存。在設定值成功儲存後，設定值也會同時生效。

有時您可能會進行交換器的設定重置，此時您可以點選 **Restore** 來將設定值重置回出廠預設值。而重置設定值後，交換器硬體亦會進行重新啟動。

當您選擇回復出廠預設值時，您將會失去所有先前進行設定時所輸入的設定值。

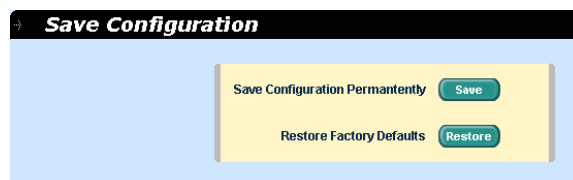


圖41 儲存設定值

### 5 控制台介面 (Console interface)

本章節將會敘述如何使用控制台介面來設定交換器。本交換器提供有 RS232 與 USB 纜線讓您可用來連接您的 PC。而藉由使用您 PC 上像是 HyperTerminal 與 command line interpreter 這類終端模擬軟體，對交換器進行設定。在開始進行設定前，您必須將終端模擬軟體的鮑率設定為 9600、8 bit 資料位元、no parity、1 停止位元，與無流量控制。

當您進入 CLI 模式，輸入“？”將會所有可用的指令協助訊息。若您對於 CLI 指令不甚熟悉時，這將是非常有用的訊息。當您沒有使用 CLI 模式 10 分鐘後，CLI 模式會自動暫停，此時您必須再次進行登入才可進入 CLI 模式。

為了讓使用者更容易操作，所有的 CLI 指令設計得非常靈敏，您可以輸入不同類型指令的全名，則此一類型會成為您的工作類型指令。之後，您就不需要在次指令之前輸入“sys”。例如，“sys”是一個包含許多次指令的指令類型，當您更改您的工作指令到“sys”，您不需要在次指令前輸入“sys”。當您的工作類型指令為“sys”時，命令列的提示會變為“(system name)sys%”。

## GigaX 系列

### 5.1 開機自我測試 (Power On Self Test)

POST 開機自我測試是在系統開機階段執行。這項測試會測試交換器的記憶體、LED 燈號，與交換器機板上的晶片。在系統測試與初始化之後，將會顯示相關的系統資訊。您可以不必理會此一訊息直到“(ASUS)%”的提示符號出現。(如圖 41)

```
Step 4
>>>>> ASUS OS Initialization Start(Phase 2)

System Parameters Reloading ..... [ DONE ]
Layer 2 Functions Initialization ..... [ DONE ]
CLI Command Tree Initialization ..... [ DONE ]
In-ROM File System Initialization ..... [ DONE ]
RADIUSd Initialization ..... [ DONE ]
SNMPd Initialization ..... [ DONE ]
Telnetd Initialization ..... [ DONE ]
HTTPd Initialization ..... [ DONE ]
FTPD Initialization ..... [ DONE ]
SSHd Initialization..... [ DONE ]

ASUS OS Initialization Success.

Step 5
>>>>> Entering CCM(CLI Command Mode) ...

Login is required!
(ASUS)%
```

圖42 CLI 介面



## 第二層網路管理交換器

### 5.1.1 Boot ROM 指令模式

在開機自我檢測的過程中，您可以藉由按下 <Enter> 鍵進入“Boot ROM Command”模式。（如圖 50 所示）

圖 42 顯示交換器中的兩個韌體，一個位於 Slot 0，而另一個則位於 Slot 1。較新的版本將會被自動選擇作為系統開機的用途。

請輸入“？”來顯示所有可用的指令說明訊息。



若您不確定了解指令的功能所在，即使在某些狀況下輸入指令可以帶來幫助，我們仍強烈建議您不要去使用這些指令。

```
>>>>> Switch Software Information
Switch Type ..... GigaK 2024
Boot ROM Version ..... Rev 1.1
Boot ROM Build Date ..... Jun  8 2005 19:53:06

>>>>> Firmware slot 0 Information
Firmware Address ..... 0xff900000
Firmware Age ..... 0x00
Firmware Status ..... PASS
Firmware Version ..... 2.1.3
Firmware Creation Date ..... 6/20/2005 18:52:30
Firmware Size ..... 2090256 bytes
Firmware Checksum ..... 0xfcfc0
Firmware Starting Address ..... 0x100000
Firmware Web Files Size ..... 275610 bytes

>>>>> Firmware slot 1 Information
Firmware Address ..... 0xffc00000
Firmware Age ..... 0x00
Firmware Status ..... PASS
Firmware Version ..... 2.1.3
Firmware Creation Date ..... 6/20/2005 18:27:0
Firmware Size ..... 2090256 bytes
Firmware Checksum ..... 0x1c13
Firmware Starting Address ..... 0x100000
Firmware Web Files Size ..... 275610 bytes

Hit Any Key to Enter Command Mode in 2 Second(s)
[Asus OS Boot]:
```

圖43 Boot ROM 指令模式

## GigaX 系列

### 5.1.2 Boot ROM 指令

請輸入 “？” 來顯示所有有效的指令列表。

表6 Boot ROM 指令

指令	參數	用途
c	IP address	設定 TFTP 用戶端的 IP 位址
g	NONE	執行韌體，進入 CLI 模式
h	NONE	顯示線上說明
m	mask	設定網路遮罩
p	NONE	顯示目前開機參數
r	NONE	系統重置
s	IP address	設定 TFTP 伺服器端的 IP 位址
t	NONE	進入安全模式
b	0 or 1 or a	支援雙重映像。您可藉由給予 Slot ID 或使用自動執行來執行韌體，選擇自動執行會執行最近更新的韌體，這是系統的預設值。
u	File name	透過使用 TFTP 協定的網路上傳開機模組韌體至交換器
v	NONE	顯示開機 rom 版本
W	NONE	使用系統管理者密碼進行重置

### 5.2 登入與登出

藉由輸入“login”來進入 CLI 模式，在登入過程中您必須輸入一個有效的使用者名稱與密碼。當您第一次進行登入，您可輸入“admin”作為使用者名稱並略過密碼。但基於安全的理由，在第一次登入後，請變更您的使用者名稱與密碼。若是您忘記您的使用者名稱與密碼，您可與華碩的技術支援部門連絡，或是在 Boot ROM Command 模式下將設定檔案清除。若您選擇後者，則您所有先前的設定資料都將被清除，這也代表您必須重新進行交換器的系統設定。

若要登入控制台介面，您可以輸入“logout”來退出介面。這個指令動作可以在您退出的同時確保系統的安全。也就是說，當下一次使用者想要登入系統時，他便得要重新輸入使用者名稱與密碼進行認證方可再次登入控制台介面。

### 5.3 CLI 指令 (CLI commands)

本交換器針對所有的管理功能都提供有對應的 CLI 指令。至於指令的分類方式則與網頁管理介面大致相同。因此，您可以如同使用網頁管理介面一般輕易地完成交換器的管理設定。

- 
- 請使用 “?” 來取得可用的指令列表與說明。
  - 請使用 “..” 來回到上一層目錄。
  - 請使用 “/” 來回到根目錄。
  - 只有在需要取得指令說明時才輸入完整的指令。
- 

#### 5.3.1 系統指令 (System commands)

##### [System Name]

顯示交換器既有的名稱。在系統群組中，本交換器是一個 RFC-1213 定義的 MIB 裝置，並且在管理節點上，提供系統管理資訊。

**CLI command :** sys name <system name description>

若您將一組名稱置於名稱敘述欄位，則交換器的系統名稱將會變更為新設定的那一組名稱。

##### [System Contact]

顯示詳細的交換器連絡資訊。在系統群組中，本交換器是一個 RFC-1213 定義的 MIB 裝置，並且在管理節點上，提供系統管理資訊。

**CLI command :** sys contact <system contact description>

若您將接點資訊置於聯繫敘述欄位，則交換器的接點資訊將會變更為新設定的那一組。

## GigaX 系列

### [System Location]

顯示交換器的實體位置。在系統群組中，本交換器是一個 RFC-1213 規範的系統群組的 MIB 裝置，並提供系統端的位置資訊。

**CLI 指令：**sys location <system location description>

在系統位置描述欄中輸入位置描述，以更新交換器的實體位置。

```
(ASUS)%  
(ASUS)%  
(ASUS)%  
(ASUS)%  
(ASUS)%  
(ASUS)%  
(ASUS)%  
(ASUS)%  
(ASUS)%  
(ASUS)%  
(ASUS)%  
(ASUS)%  
(ASUS)%  
(ASUS)%  
(ASUS)%  
(ASUS)%  
(ASUS)% sys  
(ASUS)sys% info  
(ASUS)sys/info% name  
Current system name is ASUS  
  
(ASUS)sys/info% name GX2024X  
System name is set to GX2024X  
  
(GX2024X)sys/info%
```

圖44 系統指令

### [VLAN ID]

顯示交換器的 VLAN ID。當用於管理用途時，此 ID 需要在相同的 VLAN 內。

**CLI 指令：**I3 interface vlan sw0 <VLAN ID>

### [DHCP Client]

開啓 DHCP 已取得一個動態 IP 位址，或是關閉 DHCP 以指定一個固定的 IP 位址。若您開啓 DHCP，則可以更新或釋放交換器的 IP 位址，此外也可以指令來顯示動態 IP 位址。

**CLI 指令：**net interface ip sw0 <enabled/disabled/renew/release/show>[IP Address]

顯示交換器上的 IP 位址。本 IP 位址是作為管理的用途。舉例來說，像交換器中的 http server、SNMP server、ftp server、telnet 與 SSH server 等網路應用皆使用此一 IP 位址。

**CLI 指令：**net interface ip sw0 <IP address><netmask>

## 第二層網路管理交換器

---

### [Network Mask]

顯示交換器子網路遮罩的 IP 位址。

**CLI 指令：**net interface ip sw0 <ip adress> <netmask>

### [Default Gateway]

顯示交換器預設閘道器的 IP 位址。若此交換器網路包含一個或多個路由器，則此項目必須設定。

**CLI 指令：**net interface ip sw0 <ip adress> <netmask>

### [Password Protection is] [Enabled/Disabled]

若啟動密碼保護功能，當使用者要透過網路瀏覽器來連接交換器時，會要求輸入使用者的名稱與密碼。

**CLI 指令：**sys weblogin set <enabled/disabled>

### [New Password]

### [Verify Password]

預設的使用者名稱爲 **admin**。沒有密碼，您必須在這裡設定密碼。

**CLI 指令：**sys users modify<user name, 'admin' by default>

**user name** : (old user name 'admin' by default);<new user name>

**password** (old password, 'asus' by default); <new password>

### [Reboot]

使用這個指令來重新啟動交換器。

**CLI 指令：**sys reboot

## GigaX 系列

---

### [Upload]

此功能沒有任何 CLI 指令。請參考 Boot ROM 指令來操作本功能。

### 5.3.2 實體介面指令 (Physical interface commands)

#### [Admin] [Enabled/Disabled]

顯示連接埠的狀態，使用者可以開啓或關閉此一連接埠功能。

**CLI 指令：** `l2 port admin <port number> <enabled/disabled>`

#### [Mode] [Auto/10M-Half/10M-Full/100M-Half/100M-Full/1G-Full]

顯示連接埠目前的速率與雙工模式。當您開啓連接埠的 auto-negotiation 功能時，則會自動偵測速率與雙工模式。

**CLI 指令：** `l2 port autoneg <port number> <enable/disable>`

**CLI 指令：** `l2 port speed <port number> <10/100/1000>`

**CLI 指令：** `l2 port duplex <port number> <full/half>`

#### [Flow Control] [Enabled/Disabled]

顯示連接埠的 IEEE802.3x 的流量控制設定，此一流量控制只能在全雙工模式下運作。

**CLI 指令：** `l2 port flow <port number> <enable/disable>`

### [Reload]

從設定檔案中恢復此一連接埠先前的設定值。

**CLI 指令：** `l2 port retrieve`

### 5.3.3 橋接指令 (Bridge commands)

#### [Spanning Tree is] [STP Enabled/RSTP Enabled/Disabled]

可讓使用者確認交換器是否加入生成樹協定 (STP/RSTP)。

**CLI 指令：** `l2 stp start <stp/rstp>`

## 第二層網路管理交換器

---

**CLI 指令：** `l2 stp stop`

**[Hello Time]**

**[Forward Delay]**

**[Max Age]**

**[Bridge Priority]**

顯示目前的STP 橋接參數設定。

**CLI 指令：** `l2 stp bridge set`

Hello Time (1..10 seconds):*[old Hello Time]* *<new Hello Time>*

Max Age (6..40 seconds):*[ old Max Age]* *<new Max Age>*

Forward Delay (4..30 seconds):*[ old Forward Delay]* *<new Forward Delay>*

Bridge Priority (0..61440):*[ old Bridge Priority]* *<new Bridge Priority>*

**[Priority]**

**[Path Cost]**

**[Edge Port]**

**[Point-to-point]**

顯示目前的 STP/ RSTP 快速生成樹協定連接埠參數設定。

**CLI 指令：** `l2 stp port set`

Port Settings (all,...):*[all]* *<select a port number, or just type 'all' to iteratively config>*

Port *<port number>* Priority (0..240):*[old port Priority]* *<new port Priority>*

Port *<port number>* Path Cost (1..200000000):*[old port Path Cost]* *<new port Path Cost>*

Port *<port number>* Edge Port (Yes/No):*[old port Edge Port]* *<new port Edge Port>*

Port *<port number>* Point-to-poin (Yes/No/Auto):*[old port Point-to-Point]* *<new port Point-to-Point>*

**[Reload]**

從設定檔案中，恢復先前的設定值。

## GigaX 系列

---

CLI 指令 : `l2 stp retrieve`

CLI 指令 : `l2 stp bridge retrieve`

CLI 指令 : `l2 stp port retrieve`

### [Show Trunk]

顯示一特定的幹線群組設定。使用者可以藉由給予一特定的幹線 ID、幹線群組的名稱敘述、連接埠選擇標準，與其幹線群組的成員連接埠，來建立一新的幹線群組。

CLI command : `l2 trunk show <trunk id>`

### [Create Trunk]

藉由給予幹線 ID、rtag、名稱與連接埠號碼來建立一組新的幹線群組。而 rtag 所指的是幹線群組的封包分配計算法則。

CLI 指令 : `l2 trunk create <trunk id> <rtag (1-6)> <trunk name> <port list>`

### [Add/Remove Trunk]

幹線群組的連接埠成員，可以從一既有的幹線群組被新增或是移除。

CLI 指令 : `l2 trunk add <trunk id> <port list>`

CLI 指令 : `l2 trunk remove <trunk id> <port list>`

### [LACP Action]

使用者可以在一特定的幹線群組開啓或關閉 LACP。

CLI 指令 : `l2 trunk lacp action <trunk id> <enable/disable>`

### [LACP System Priority]

使用者可以指定系統執行 LACP 的優先順序。

CLI 指令 : `l2 trunk lacp syspri <priority (1-65535)>`

### [LACP Port Priority]

使用者可以指定執行 LACP 連接埠的優先順序。

CLI 指令 : `l2 port lacppri <priority> <port list / * for all ports>`



## 第二層網路管理交換器

---

### [Reload]

從設定檔案中回復先前儲存的幹線設定。

**CLI 指令 :** `l2 trunk retrieve`

### [Mirror Mode] [*Enable/Disable*]

### [Monitor Port] [*port number*]

顯示交換器的鏡像設定。使用者可以從交換器的兩個鏡像埠中建立一組最大值。

**CLI 指令 :** `l2 mirror create <monitor port no> <enable/disable>`

**CLI 指令 :** `l2 mirror ingress <port list>`

**CLI 指令 :** `l2 mirror egress <port list>`

**CLI 指令 :** `l2 mirror remove <ingress/egress> <port list>`

### [Reload]

從設定檔案中回復先前儲存的設定值。

**CLI 指令 :** `l2 mirror retrieve`

### [Show Multicast Group]

顯示在多重播送列表中的靜態多重播送群組。

**CLI 指令 :** `l2 mcast show`

### [Set Multicast Group]

本項目可讓使用者藉由指定 MAC 位址、VLAN ID、服務等級、VLAN 連接埠參數與未標示的連接埠來新增或變更一個靜態的多重播送群組。請注意！MAC 位址與 VLAN ID 的組合會在多重播送群組列表中形成一組特定的項目。

**CLI 指令 :** `l2 mcast set`

`mac address` [format : xx:xx:xx:xx:xx:xx] : <multicast mac address>

`vlan id` [1 by default] <vlan id>

`cos` [0-7, 0 by default] <class of service>

`port list` [format : 1 2 3 4-50/\* for all ports] <vlan port list>

`untagged port list` [format : 1 2 3 4-50/\* for all ports] <untagged port list>

## GigaX 系列

---

### [Remove Multicast Group]

本項目可讓使用者從多重播送群組列表中，藉由給予一個 MAC 位址與 VLAN ID 來刪除一個靜態多重播送群組項目。

**CLI 指令：** l2 mcast delete mac address [format: xx:xx:xx:xx:xx:xx]: <multicast mac address> vlan id: <vlan id>

[Reload]

從設定檔案中回復先前儲存的設定。

### **CLI 指令：** l2 mcast retrieve

[IGMP is] [Enabled/Disabled]

Layer 2 IGMP snooping can be started or terminated by user if necessary.

### **CLI 指令：** l2 igmp <start/stop>

[Reload]

從設定檔案中回復先前儲存的設定。

### **CLI 指令：** l2 igmp retrieve

[Action] [Enabled/Disabled]

[Mode] [Broadcast] or [Broadcast/Multicast] or [Broadcast/Multicast/Unknown unicast]

[Limit Rate]

藉由開啓傳輸控制，將可以顯示目前交換器的廣播、多重播送與泛流（由於 Destination Lookup Failed）傳輸率。

**CLI 指令：** l2 rate set <enabled / disabled> [<mode(1: broadcast only, 2:broadcast and multicast, 3:broadcast, multicast and unknown unicast)> <limit rate(70~250000 Kbps/sec)>]

[Reload]

從設定檔案中回復先前儲存的設定。

### **CLI 指令：** l2 rate retrieve

[Aging Time]

使用者可以藉由點選持續時間設定值來設定 ARL(Address Resolution Logic) 項目。

**CLI 指令：** l2 arl age [aging time value]

## 第二層網路管理交換器

---

### [Query by Port]

ARL 項目存在於 ARL 列表，可以依照連接埠號進行查詢。

**CLI 指令 :** `l2 arl port <port number>`

### [Query by VLAN ID]

ARL 項目存在於 ARL 列表並可依照 VLAN ID 進行查詢。

**CLI 指令 :** `l2 arl vlan <vlan id>`

### [Query by MAC Address]

ARL 項目存在於 ARL 列表並可依照 MAC address 進行查詢。

**CLI 指令 :** `l2 arl mac <mac address> [vlan id]`

### [MAC Address]

### [VLAN ID]

### [Port Selection]

### [Discard] [none/source/destination/source & destination]

使用者可以藉由指定一個 MAC address、VLAN ID、連接埠號、幹線 ID 來新增或變更一個靜態 ARL 登錄。

**CLI 指令 :** `l2 arl static <mac> <vlan id> <port no> <trunk id>  
<discard: 0-3>`

### [Remove]

靜態 ARL 登錄可藉由指定 MAC address 與其 VLAN ID 來加以刪除。這邊的兩個組合欄位會形成一組 ARL 列表中的特定登錄。

**CLI 指令 :** `l2 arl delete <mac address> <vlan id>`

### [Retrieve]

從設定檔案中回復先前的設定值。

**CLI 指令 :** `l2 arl retrieve`

### [Show VLAN]

顯示交換器中既有的 VLAN 資訊。

**CLI 指令 :** `l2 vlan show <vlan id>`

## GigaX 系列

---

[Name]

[VLAN ID]

可讓使用者進行 VLAN 的設定。使用者可以藉由給予一組特定的 VLAN ID、一組 VLAN 敘述名稱與其連接埠號列表來建立一組新的 VLAN。請注意，在這裡連接埠號是藉由標示連接埠號來指出。如欲指出一組未標示的連接埠群組，使用 CLI 指令可以達到此一目的。使用者可以使用 CLI 指令來新增或移除以進一步新應一些連接埠群組成員給一組 VLAN 或從 VLAN 中排除一些既有的連接埠成員。

**CLI 指令 : l2 vlan create <vlan id> <vlan name> <port list>**

**CLI 指令 : l2 vlan add <vlan id> <port list>**

**CLI 指令 : l2 vlan remove <vlan id> <port list>**

**CLI 指令 : l2 vlan utportadd <vlan id> <untagged port list>**

[Remove VLAN]

讓使用者可以完全清除一組既有的 VLAN。

**CLI 指令 : l2 vlan delete <vlan id>**

[Reload]

從設定檔案中回復先前儲存的設定。

**CLI 指令 : l2 vlan retrieve**

[Show Port]

顯示連接埠設定。

**CLI 指令 : l2 port show <port id or \* for all ports>**

[PVID]

藉由給予一組 VLAN ID 與其相關的群組成員列表來指定預設的 VLAN 給一組連接埠。

**CLI command : l2 port vlan <vlan id, 4095 to disable the port-based vlan> <port list>**

[CoS Value]

## 第二層網路管理交換器

---

Sets the Class of Service for a port by assigning it a priority (with range of 0-7) criteria value.

**CLI 指令 :** `l2 port priority <CoS> <port list>`

[Reload]

從設定檔案裝回復先前的預設值。

**CLI 指令 :** `l2 port retrieve`

[CoS Map]

可讓使用者指定 CoS 優先順序 (範圍 0-7) 作為緩衝佇列 (總共 4 組, 使用 1-4 的佇列 ID)。

**CLI 指令 :** `l2 cos map <queue id (1-4)> <cos (0-7)>`

[Scheduling Algorithm] [Strict/WRF]

可讓使用者使用基於權重優先方式的強制優先順序來設定排程表。

**CLI 指令 :** `l2 cos sched <mode (1:strict 2:weighted round robin)>`

[Reload]

從設定檔案中回復先前儲存的設定值。

**CLI 指令 :** `l2 cos retrieve`

### 5.3.4 簡易網路管理通訊協定 (SNMP)

[Community Name] [Set]

您可以建立不同的團體並自訂存取，在這裡輸入團體名稱，並勾選是否具有設定（寫入存取）的權力。

**CLI 指令 :** `snmp community add`

**New community string:** *<new community string>*

**Get privileges:** [y, always turn on by default]

## GigaX 系列

---

Set privileges? (y/n):[n] <set privilege, y for 'yes' ; n for 'no' >

**CLI 指令:** snmp community set

使用者可以修改團體表內容及其權力。

**CLI 指令:** snmp community set:

**Community entry (table index):** <entry id to config>

**Community string (old community string):** <new community string>

這個動作會修改所有主機的團體名稱，從 'old community' 改為 'new community'。

Are you sure? (y/n):[y] <y for 'yes' n for 'no' >

**Get privileges:** [y, always turn on by default]

Set privileges? (y/n):[n] <set privilege, y for 'yes' n for 'no' >

使用者可以刪除團體表中的項目。

**CLI 指令:** snmp community delete

**Community entry (table index):** <entry id to delete>

這個動作會刪除所有主機的某一團體。

Are you sure? (y/n):[y] <y for 'yes' n for 'no' >

### [Reload]

從設定檔案裝恢復先前儲存的設定值。

**CLI 指令:** snmp community retrieve

### [Host IP Address] [Community]

主機內容包含了主機 IP 位址、網路遮罩及其所屬團體。

**CLI 指令:** snmp host add

**Host IP/Subnet:** <IP address>

**Netmask:** <netmask>

**Community:** <community string>

**CLI 指令:** snmp host set

使用者可以藉由重新輸入 IP 位址、網路遮罩，及其所屬團體，在此表中修改主機內容。

**Host table entry (table index):** <entry id to config>

## 第二層網路管理交換器

---

**Host IP/Subnet (old IP address):** <new IP address>

**Netmask (old netmask):** <new netmask>

**Community (old community string):** <new community string>

使用者可以從主機表中刪除主機內容。

**CLI 指令:** snmp host delete

**Entry id (table index):** <entry id to delete>

**[Reload]**

從設定檔案中恢復先前儲存的設定值。

**CLI 指令:** snmp host retrieve

**[Trap Version]** [v1/v2c]

**[Destination]**

**[Community for Trap]**

Trap 項目中包含 SNMP 版本（目前支援 V1 與 V2c）、目的 IP 位址及遠端團體名稱。

**CLI 指令:** snmp trap add

**SNMP version?** (1/2c):[1, by default] <snmp version>

**Destination IP:** <IP address>

**Community:** <community string>

使用者可以藉由修改 SNMP 版本、目的 IP 位置及團體名稱，來修改 Trap 表。

**CLI 指令:** snmp trap set

**Trap table entry (table index):** <entry id to config>

**SNMP version?** (1/2c):[old snmp version] <new snmp version>

**Destination IP (old IP address):** <new IP address>

使用者可以從 Trap 表中刪除某一項目。

**CLI 指令:** snmp trap delete

**Trap table entry (table index):** <entry id to delete>

## GigaX 系列

---

### [Reload]

從設定檔案中恢復先前儲存的設定值。

**CLI 指令 :** snmp trap retrieve

[Group Name]

[Read View Name]

[Write View Name]

[Notify View Name]

[Security Model]

[Security level]

一個 VACM(View-based Access Control Model) 群組登錄包含有群組名稱、讀取檢視名稱、寫入檢視名稱、提示檢視名稱、安全性模具，安全性等級與背景比較。

**CLI 指令 :** snmp snmpv3 access add

Group Name: <group name string>

Security Model [0/1/2/3](any/v1/v2c/usm): <security model>

Security Level [1/2/3](noauth/authnopriv/authpriv): <security level>

Context Match [0/1](inexact/exact): <context match>

Read View Name: <read view name string>

Write View Name: <write view name string>

Notify View Name: <notify view name string>

使用者可藉由在群組中重新指定允許的群組名稱、讀取檢視名稱、寫入檢視名稱、提示檢視名稱、安全性模具，安全性等級與背景比較來變更群組登錄。

**CLI 指令 :** snmp snmpv3 access set

Group Name: (old group name string) <new group name string>

Security Model [0/1/2/3](any/v1/v2c/usm): (old security model) <new security model>

Security Level [1/2/3](noauth/authnopriv/authpriv): (old security level) <new security level>



## 第二層網路管理交換器

---

Context Match [0/1](inexact/exact): (old context match) <new context match>

Read View Name: (old read view name string) <new read view name string>

Write View Name: (old write view name string) <new write view name string>

Notify View Name: (old notify view name string) <new notify view name string>

使用者可由 VACM 群組中刪除一組 VACM 登錄。

**CLI 指令 : snmp snmpv3 access delete**

Access entry: <entry id to delete>

[Reload]

從設定檔案中回復先前儲存的設定值。

**CLI 指令 : snmp snmpv3 access retrieve**

[View Name]

[View Type]

[View Subtree]

[View Mask]

VACM(View-based Access Control Model) 檢視是用於檢視 VACM 群組的 SNMPV3 的相關資訊。一組 VACM 檢視登錄包含有一檢視名稱、檢視類型、檢視子目錄與檢視遮罩。

**CLI 指令 : snmp snmpv3 view add**

View Name: <view name string>

View Subtree [oid]: <view subtree>

View Mask: <view mask>

View Type[1/2](included/excluded): <view type>

使用者可以藉由在列表中重新指定 VACM 檢視登錄來允許檢視名稱、類型、子目錄與遮罩。

**CLI 指令 : snmp snmpv3 view set**

## GigaX 系列

---

View Name: (old view name string)<new view name string>

View Subtree [oid]: (old view subtree)<new view subtree>

View Mask:: (old view mask)<new view mask>

View Type[1/2](included/excluded):(old view type) <new view type>

可讓使用者刪除一組 VACM 檢視登錄。

**CLI 指令 : snmp snmpv3 view delete**

**View entry:<entry id to delete>**

[Reload]

從設定檔案中回復先前儲存的設定值。

**CLI 指令 : snmp snmpv3 view retrieve**

EngineId: <engine id string >

Name: <user name string >

AuthProtocol [oid]: <auth protocol oid string >

AuthPassword: <auth password string>

Priv Protocol [oid]: <priv protocol oid string >

Priv Password: <priv password string >

USM(User-based Security Model) 使用者是用於設定 SNMPV3 USM 的使用者資訊，這項資訊包含有引擎 Id、名稱、認證協定、認證密碼、隱私協定與隱私密碼。

**CLI 指令 : snmp snmpv3 usmuser add**

EngineId: <engine id string >

Name: <user name string >

AuthProtocol [oid]: <auth protocol oid string >

AuthPassword: <auth password string>

Priv Protocol [oid]: <priv protocol oid string >

Priv Password: <priv password string >

## 第二層網路管理交換器

使用者可以藉由重新指定允許的引擎 Id、名稱、認證協定、認證密碼、隱私協定與陰私密碼來變更 USM 列表中的使用者登錄。

### CLI 指令 : snmp snmpv3 usmuser set

EngineId: (old engine id string ) <new engine id string >

Name: (old user name string ) < new user name string >

AuthProtocol [oid]: (old auth protocol oid string) < new auth protocol oid string >

AuthPassword: (old auth password string) < new auth password string>

Priv Protocol [oid]: (old priv protocol oid string) < new priv protocol oid string >

Priv Password: (old priv password string) < new priv password string >

使用者可刪除一組 USM 使用者登錄。

### CLI 指令 : snmp snmpv3 view delete

USM user entry: <entry id to delete>

[Reload]

從設定檔案中回復先前儲存的設定值。

### CLI 指令 : snmp snmpv3 usmuser retrieve

## 5.3.6 安全指令 (Security Commands)

[Reauthentication]

使用者可開啓或關閉每隔一段時間的重新認證功能。

### CLI 指令 : security dot1x bridge reauth <enable / disable>

[Reauthentication Time]

使用者可以設定重新認證的時間。

### CLI 指令 : security dot1x bridge reauthtime <reauthentication time(1-4294967295 sec)>

## GigaX 系列

---

### [Authentication Method]

使用者可以設定認證方式。(RADIUS 或本地端資料庫).

**CLI 指令 : security dot1x bridge authmeth <type (1:local 2:radius)>**

### [Quiet Period]

使用者可設定待機時間。

**CLI 指令 : security dot1x bridge quietperiod <quiet period (1-65535 sec)>**

### [Retransmission Time]

使用者可設定重新傳輸時間。

**CLI 指令 : security dot1x bridge retxtime <retransmission time (1-65535 sec)>**

### [Max Reauthentication Attempts]

使用者可設定重新認證的最多次數。

**CLI 指令 : security dot1x bridge reauthmax <max reauthentication attempts (1-10)>**

### [Multi-host]

使用者在某些特定連接埠可開啓或關閉多重主機功能。

**CLI 指令 : security dot1x port multihost <enable/disable><port list/\*>**

### [Authentication Control]

使用者在某些特定連接埠可設定認證控制功能。

**CLI 指令 : security dot1x port authctrl <type (1: force\_authorized 2:force\_unauthorized 3: auto)><port list/\*>**

### [Guest VLAN]

使用者可由部份特定的連接埠設定來賓 VLAN ID。

**CLI 指令 : security dot1x bridge port guestvlan <vlan id (0:no guest vlan)> <port list/\*>**

## 第二層網路管理交換器

---

[Reload]

從設定檔案中回復先前儲存的設定值。

**CLI 指令 : security dot1x retrieve**

[User Name]

[Password]

[Confirm Password]

[Dynamic VLAN]

在交換器的本地端資料庫建立使用者作為 802.1x 認證之用。一個使用者登錄包含使用者名稱、密碼與動態 VLAN。

**CLI 指令 : security dialinuser create**

User Name: <user name string>

Password: <password string>

Confirm Password: <confirm password string>

Dynamic VLAN: <dynamic VLAN>

**CLI 指令 : security dialinuser remove <user name/\*>**

使用者可由本地端資料庫刪除一個使用者登錄。

**CLI 指令 : security dialinuser modify <user name/\*>**

使用者可由本地端資料庫變更一個使用者登錄。這組登錄包含使用者名稱、密碼與動態 VLAN。

User Name: <new user name string>

Password: <new password string>

Confirm Password: <new confirm password string>

Dynamic VLAN: <new dynamic VLAN>

[Reload]

從設定檔案中回復先前儲存的設定值。

**CLI 指令 : security dialinuser retrieve**

## GigaX 系列

---

[Authentication Server IP]

[Authentication Server Port]

[Authentication Server Key]

[Confirm Authentication Key]

使用者可以設定 RADIUS 伺服器 IP、伺服器連接埠與伺服器金鑰。

### CLI 指令 : security radius set

authentication server ip <ip/none>: (old server ip)<new server ip >

authentication server port <port/default>: (old server port)<new server port>

authentication server key <key/none>: <server key>

confirm authentication key <key/none>: <confirm server key>

[Reload]

從設定檔案中回復先前儲存的設定值。

### CLI 指令 : security radius retrieve

[Generate SSH key]

使用者可以產生 SSH 金鑰。SSH (Secure SHell) 為一種透過 shell 遠端登入至一台機器的通訊協定。這項協定與 telnet 的功能相當類似，然而卻又不同於 telnet，所有在用戶端與伺服器端的資料都是經過加密的。經由加密可以保護資料避免許多來自網路的安全性風險。目前來說，我們的交換器支援 SSH protocol version 2 並可在同一時間中登入一使用者。兩對 SSH 金鑰將會被建立並儲存於交換器的快閃記憶體中。這兩個金鑰分別為 RSA 與 DSA 公開/私人金鑰。

### CLI 指令 : security sshkey start

[Reset SSH key]

重置 SSH 金鑰到預設值。

### CLI 指令 : security radius default

[Show Generating Status]

顯示 SSH 金鑰的產生狀態。此指令將會顯示 “success” 或 “SSH keys generated fail” 或 “system is generating keys ...”。

### CLI 指令 : security sshkey show

## 5.4 其他指令 (Miscellaneous commands)

**sys time uptime:** 顯示系統啟動時間。

**sys time date:** 顯示目前的日期及時間。

**sys time settime:** 設定目前時間。

**sys files config backup:** 備份設定檔案。

**sys files config default:** 恢復工廠預設的設定檔案。

**sys monitor auto:** 開啓或關閉風扇自動偵測。

**sys monitor set:** 設定風扇轉速指令（1~255）。

**sys monitor show:** 顯示系統環境狀況。

**net ping:** ping 遠端的主機。

**net route show:** 顯示路由表內容。

## 6 IP 位址、網路遮罩與子網路 (IP Address, network mask, & subnet)

### 6.1 IP 位址 (IP Address)



Note

- 本節所涵蓋的內容僅關於 IPv4 中之 IP 位址 (Version 4 of Internet Protocol)，至於 IPv6 位址則不在本節所介紹的範圍。
- 本節將讓使用者對於 binary number、bits 與 bytes 能有基本的認識。

IP 位址，如同網際網路領域的電話號碼，可用以辨識網際網路中獨立的節點（電腦或其他裝置）。每一個 IP 位址具有四組號碼，而每一組號碼可以是 0 至 255 間的任一數字，至於四組數字間則以英文字母中的句點加以分隔，如 20.56.0.211。這幾組數字是由左而右來讀出，分別是欄位 1. 欄位 2. 欄位 3. 欄位 4。

書寫 IP 位址的方式是以句點分隔四組十進位號碼進行，又稱作句點十進位標記法。在這裡若 IP 位置為 20.56.0.211，則可讀作“二十點五十六點零點二一一”。

#### 6.1.1 IP 位址的結構 (Structure of IP Address)

IP 位址如同電話號碼一般採用一種分等設計。舉例來說，一個七位數的電話號碼，起始於三個用以從數千條電話線中進行辨識的號碼，而後四位數則是則用以辨識該線路是位於哪個群組中。

同樣地，一個 IP 位址中包含有兩種資訊。

網路 ID (Network ID)

在網際網路與內部網路中標示一特定的網路環境。

主機 ID (Host ID)

標示在網路環境中一台特定的電腦或裝置。

每一個 IP 位址的第一部份包含有網路 ID，至於其餘的位址則包含主機 ID。網路 ID 的長度取決於網路的“等級”（請參閱下一節中的介紹）。下面的列表 8 顯示一個 IP 的結構。



## 第二層網路管理交換器

表7 IP 位址結構

	欄位 1	欄位 2	欄位 3	欄位 4
Class A	網路 ID	主機 ID		
Class B	網路 ID		主機 ID	
Class C	網路 ID			主機 ID

以下為有效 IP 位址的範例：

Class A：10.36.6.125（網路 = 10，主機 = 30.6.125）

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

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

### 6.1.2 網路等級（Network classes）

在網路等級中最常備用到的三種等級為 A、B 與 C。（在此之外尚有 Class C，但是其特殊的使用環境不在本章節的討論範疇中）而上述三種網路等級，各有其不同的使用範圍與特性。

Class A 的網路環境是指網際網路中最大範圍的網路環境，每一個屬於此等級的網路環境皆可容納超過 1 千 6 百萬台的主機。而這類等級的網路環境最多可存在 126 個，也就是說總共可以容納 2 億的主機。由於它們巨大的容量，所以這類網路環境多用於 WAN 廣域網路或是具有組織的網際網路環境，像是網際網路服務提供廠商（ISP）。

相較於 Class A，Class B 的網路環境雖然較小，但是仍屬大範圍的網路環境。每一個屬於此等級的網路環境可容納超過 6 萬 5000 台的主機。而共可有高達 16,384 的 Class B 網路環境存在，一個 Class B 等級的網路可以歸屬於一個較大的組織，像是商業或政府機關。

在三個等級中，最小的便是 Class C，此一等級只能夠擁有最多 254 台主機，但是這類網路可能的總數可以超過 2 百萬（正確的數量為 2,097,152）。連接到網際網路的區域網路便是屬於此一等級的網路環境。

上述等級可由 IP 位置的第一欄位做簡單的辨識：

網路等級可依照 IP 位址的第一欄位進行辨識：

field 1 = 1 - 125： Class A

field 1 = 128 - 191： Class B

field 1 = 192 - 223： Class C

（欄位 1 的數值若不在上述範圍者則是用於特殊用途）

一個主機 ID 可以是 0 或 255 以外的任何數值，上述這兩個數值是作為特殊用途的設定值。

## GigaX 系列

### 6.2 子網路遮罩 (Subnet masks)

網路遮罩就如同一般的 IP 位址，但其包含有之位元樣式，可以告知一個 IP 位址的哪些部份是網路 ID，而又有哪些部份是屬於主機 ID：位元數設定為 1 者代表此一位元屬於網路 ID，至於設定為 0 者，則意指此一位元屬於主機 ID。

子網路遮罩是讓您用來定義子網路（如您所知，便是將現有網路切割成更小的區塊）。一組子網路的網路 ID 是藉由從主機 ID 的位址中“借”一個或更多的位元數來加以建立的。所以子網路遮罩可以確認這些主機 ID 的位元。

舉例來說，當 Class C 的網路位址 192.168.1，若要將其分為兩個子網路，您則會使用下列的子網路遮罩設定：

255.255.255.128

若用二進位數字來看便更容易理解其中的意義：

11111111.11111111.11111111.10000000

就像任何 Class C 的位址一樣，所有欄位 1 至欄位 3 的位元都是網路 ID 的一部份，但請注意遮罩是如何指定第四欄位中的第一位元也包含在網路 ID 中。因為額外的位元只有兩個數值（0 與 1），這表示有兩個子網路。而每一個子網路在欄位 4 中使用剩下的七個位元作為主機 ID，可設定的範圍由 0 至 127（而不是如同 Class C 的數值範圍，由 0 至 255）。

同樣地，若將 Class C 的網路分為四個子網路，則遮罩便是：

255.255.255.192 或 11111111.11111111.11111111.11000000

在欄位 4 多出的兩個位元可以是四個數值（00, 01, 10, 11），所以有四組子網路。每一個子網路在第四欄位中使用剩下從 0 至 63 間的 6 個位元作為其主機 ID。

- 在某些狀況下，一組子網路遮罩並不特指任何多出的網路 ID 位元，也因此便沒有子網路，而該遮罩便稱做預設的子網路遮罩。這些遮罩在三個網路等級中分別是：

**Class A：** 255.0.0.0

**Class B：** 255.255.0.0

**Class C：** 255.255.255.0

- 上面所列出的預設子網路遮罩之所以會被這樣稱呼，原因在於它們是在網路進行初始設定時被使用，而在當時的狀況是沒有子網路的。

## 7 疑難排解 (Troubleshooting)


本節中將會介紹幾個使用 IP 公用程式進行問題診斷的方式。此外也會提供相關可能發生的問題與解決建議列表供使用者參考。

在注意事項中，會列出所有已知問題的列表，在您設定交換器前，請先詳閱這些注意事項。而若是這些疑難排除建議仍舊無法解決您的問題，請儘速與客戶支援部門聯繫。

### 7.1 使用 IP 公用程式來診斷問題

#### 7.1.1 封包探測 (Ping)

封包探測是您可用來檢查您的 PC 是否可正確辨識您網路環境或是網際網路中其他電腦的常用指令。當您下達封包探測 (Ping) 指令時，您的電腦會送出一個訊息到您所指定的電腦，若指定的電腦接收到這個訊息，便會回傳一個訊息作為回復。若要使用此一指令，您必須知道所想要進行連接電腦的 IP 位址。

在安裝視窗作業系統的電腦中，您可由“開始”選單執行 ping 指令。請點選作業系統的“開始”按鍵，並點選“執行”選項。接著請在文字輸入視窗中如右所示輸入：ping 192.168.1.1 (IP 位址請輸入您要進行測試電腦的 IP 位址)，輸入完畢後點選  即可。

若您知道您區域網路或是網際網路可供測試的 IP 位址，您也可於視窗中變更輸入這些 IP 位址。

若是目標電腦接收到訊息，則在視窗中會顯示如圖 52 所示的指令列。

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<10ms TTL=255
Reply from 192.168.1.1: bytes=32 time<10ms TTL=255
Reply from 192.168.1.1: bytes=32 time<10ms TTL=255
Reply from 192.168.1.1: bytes=32 time<10ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

圖45 使用封包探測公用程式

## GigaX 系列

若無法得到目標電腦的回應，您將會收到“Request timed out”的訊息。

藉由使用封包探測指令，您可以檢查交換器對外連線路徑（使用預設的區域網路 IP 位址進行 192.168.1.1 進行探測）或是其他您所指定的位址是否正常運作。

您也可以藉由輸入外部的 IP 位址例如輸入：`www.yahoo.com`（或 `216.115.108.243`）來測試交換器對外連線是否正常。若您不知道特定網際網路的 IP 位址，您則可以使用將在下一節中介紹的網路資訊查詢指令（`nslookup command`）。

從其他開啓 IP 的作業系統，您可以透過系統管理工具來執行上述的指令進行測試。

### 7.1.2 網路資訊查詢（nslookup）

您可以使用網路資訊查詢指令來辨認與網際網路之網站名稱相關連的 IP 位址。您可以指明一般的網站名稱，接著網路資訊查詢指令就會在您的 DNS 伺服器（通常位於您的 ISP）中查詢該名稱。若該名稱不是您 ISP 中 DNS 列表的一個登錄名稱，則該搜尋請求會被指向另一更高層級的伺服器，以此類推，直到該名稱被搜尋到為止。查詢完畢後，伺服器會回覆與您輸入名稱相關連的 IP 位址。

在安裝視窗作業系統的電腦中，您可由“開始”選單執行 `nslookup` 指令。請點選作業系統的“開始”按鍵，並點選“執行”選項。接著請在文字輸入視窗中如右所示輸入：`nslookup`，輸入完畢後點選“確定”。

點選  後，畫面便會出現一個提示視窗，顯示一含括弧的提示（>）。在此一提示訊息後方，請輸入您想要查詢的網際網路位址的名稱，像是 `www.absnews.com`。

輸入完畢後，畫面會顯示如下圖 46 顯示的相關連 IP 位址。



```
C:\>nslookup
Default Server: tp-dc-01.corpnet.asus
Address: 192.168.28.68

> www.absnews.com
Server: tp-dc-01.corpnet.asus
Address: 192.168.28.68

Name:      absnews.com
Address: 204.202.132.19
Aliases:   www.absnews.com

> _
```

圖46 使用網路資訊查詢公用程式

## 第二層網路管理交換器

進行查詢後，您可以會得到數個與該網際網路名稱相關連的 IP 位址。這在網站處於重度傳輸狀態下是正常的狀況，這是因為網站使用多重、備用的伺服器來傳輸相同的資訊。

若要從網路查詢公用程式中退出，請在指令提示右方輸入 `exit` 並按下 `<Enter>` 鍵。

### 7.2 更換損壞的風扇

當您要移除位於交換器後背板的風扇模組前，請先將交換器的電源關閉。

當任何一個交換器風扇（位於交換器後背板）發生運作不正常狀況時，請依照下列步驟來進行快速更換動作。

1. 藉由轉開固定交換器後背板的手旋式螺絲來將風扇模組鬆開。

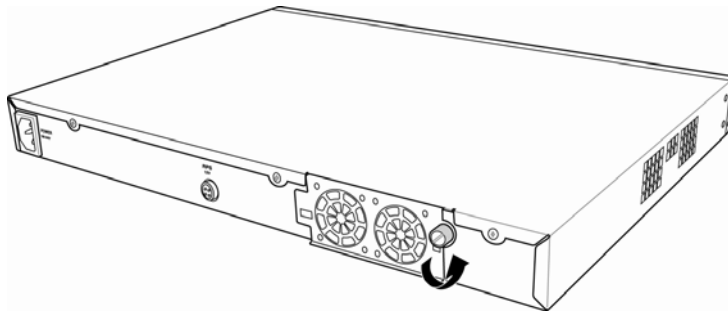


圖47 轉開手旋式螺絲

2. 如下圖所示小心地將風扇模組由交換器中拉出。

## GigaX 系列

---

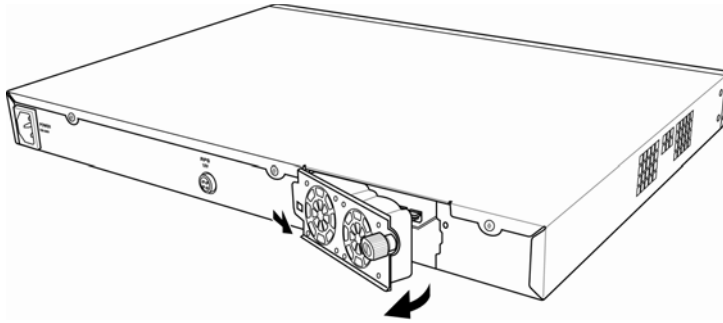


圖48 移除風扇模組

3. 從交換器機身的風扇電源插座上小心地將兩條風扇電源線移除。
4. 鬆開將風扇固定於風扇模組上的螺絲，並移除損壞的風扇。
5. 替換新的風扇後，用固定舊風扇的螺絲重新將新風扇鎖緊固定於風扇模組，並確認風扇的電源線靠近風扇模組的底部。之後，請採用相同的步驟來更換其他風扇。

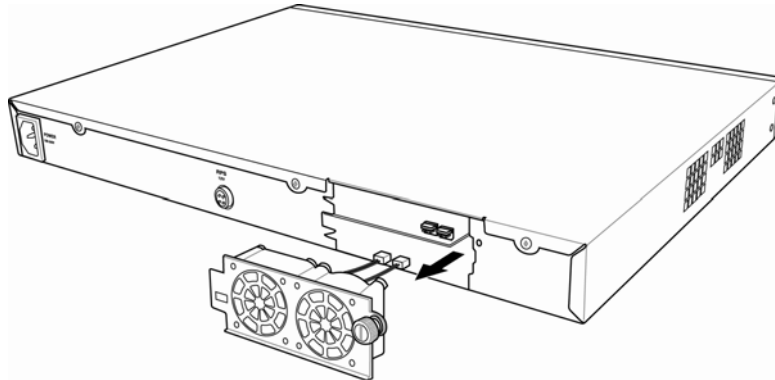


圖49 將風扇自風扇模組拆除

6. 連接風扇的電源線到交換器電路板上的插座，並確認風扇的電源接頭連接到正確的電源插座上。當您面對交換器的後背板時，FAN 1 是位於模組的左側。
7. 將風扇模組插回交換器的機身中，直到模組的外緣與機身切齊。在將風扇模組裝回機身時，請確認風扇的電源線沒有卡在模組與機身間。
8. 使用手旋式螺絲將風扇模組固定於交換器的機身上，並確認風扇的電源線沒有夾在風扇模組與機身間。

## 第二層網路管理交換器

### 風扇規格

尺寸：40 x 40 x 20 mm

電壓與電流：12VDC，0.13A


風扇轉速：8200 RPM

### 7.3 簡易修護

以下的列表將列出一些當您使用本交換器時所可能遭遇到的問題，並提出該問題的解決建議。

問題	建議採取措施
LED 燈號	
在開啓交換器後，SYSTEM 燈號並未亮起	請確認電源線兩端已分別緊密地連接到交換器的電源插座與牆壁 / 電源延長線上的插頭。
在連接備用電源後，RPS 燈號並未亮起	1. 請確認 RPS 電源纜線已分別緊密地連接到 RPS 插座與牆壁 / 電源延長線上的插頭。 2. 確認備用電源符合備用電源一節中所提到的規格標準。
FAN 燈號閃爍橘色燈號	請檢查位在交換氣後背板的風扇。若有任何風扇損壞，請依照 7.2 節中的介紹更換風扇。
在連接乙太網路線後，Gigabit 乙太網路連線燈號並未亮起	1. 請確認您所使用的乙太網路線一端已緊密地連接到區域網路端的交換器 / 集線器 / 個人電腦，至於另一端也正確地連接到 GigaX 交換器。此外請確認交換器 / 集線器 / 個人電腦電源開啓的。 2. 請確認網路纜線符合您網路環境的需求。舉例來說，若網路環境傳輸速率為 1000 Mbps (1000Base Tx)，則您必須使用標示 Cat 5 或 Cat 6 的乙太網路線。若使用較低規格的纜線，便會得到較低的傳輸速率。
網路連線	
在相同網路環境下，個人電腦無法連接到其他主機	1. 請確認乙太網路線是正常的並且燈號顯示為綠色。 2. 若連接埠的燈號為橘色，請檢查此一連接埠是否設定為關閉。若您開啓 STP，則將會有一小段時間您會無法連線到網路。

## GigaX 系列

問題	建議採取措施
個人電腦端無法顯示網頁設定管理頁面	<ol style="list-style-type: none"> <li>1. 請確認交換器的電源已開啓且連接埠也是設定為開啓的。本交換器的出廠預設 IP 位址為 192.168.1.1。</li> <li>2. 請檢查您個人電腦端的網路設定。若您的個人電腦並未設定有效的路由來與交換器連線，請試著變更交換器的預設 IP 位址以便讓您的交換器可連接到交換器。</li> <li>3. 在個人電腦端下達封包探測指令 (ping) 若是仍無得到交換器的回應，請再重複步驟 2。</li> <li>4. 若經過封包探測有得到交換器回應，卻仍無法開啓網頁設定管理介面，則請使用 RS-232 或 USB 纜線來連接交換器的控制台介面，並檢查過濾規則或靜態 MAC 位址設定是否阻礙 WEB 資料的傳遞。</li> </ol>
網頁設定管理介面	
您忘記或遺失網頁設定管理介面的使用者名稱或密碼。	<ol style="list-style-type: none"> <li>1. 若您並未變更預設的使用者名稱與密碼，請試著輸入 admin 作為使用者名稱並透過密碼輸入項目直接選擇確認。</li> <li>2. 利用 RS-232 或 USB 纜線來登入交換器的控制台介面，使用 “sys user show” 指令來顯示您所遺失的使用者資訊。</li> <li>3. 進入 BootROM 模式，使用 “w” 來開啓系統管理員密碼重置功能（使用者名稱也會進行重置），接著請輸入 “g” 並按下 Enter 來執行韌體。請注意！使用者名稱與密碼只會重啓一次。</li> </ol>
部份頁面並未完全顯示。	<ol style="list-style-type: none"> <li>1. 請確認您所使用的是 Internet Explorer 5.5 或更新版本的瀏覽器，請注意 Netscape 瀏覽器並不支援本功能。此外您必須開啓瀏覽器支援 Javascript 的功能，本功能需要支援 Java 語言。</li> <li>2. 利用封包探測 (ping) 功能測試交換器的 IP 位址來確認連線品質是否穩定。若封包探測失敗，則請檢查您的網路連線設定是正確的。</li> </ol>
進行變更的設定值並未被保存。	當您進行設定值的變更後，請確認已按下  鍵儲存變更的設定值。
控制台介面	
在終端模擬軟體中無法顯示輸入的文字。	<ol style="list-style-type: none"> <li>1. 請檢查相關設定值，出廠預設值為波特率 9600，無流量控制、8 位元資料、無同位檢查與停止位元為 1。</li> <li>2. 將您的終端模擬軟體設定值變更為上述設定值。若您使用 USB 纜線連接控制台，請先安裝 USB 驅動程式。</li> <li>3. 請檢查您所用來連接控制台介面的纜線是可以正常運作的。</li> </ol>



## 8 術語表 (Glossary)

10BASE-T	乙太網路使用的配線的名稱，資料傳輸率為10 Mbps。又被稱為 Category 3 (CAT 3) 配線。又見資料傳輸率，Ethernet。
100BASE-T	乙太網路使用的配線的名稱，資料傳輸率為 100 Mbps。又被稱為 Category 5 (CAT 5) 配線。又見資料傳輸率，Ethernet。
1000BASE-T	乙太網路使用的配線的名稱，資料傳輸率為1000 Mbps。
binary	二進位，兩個最基礎的數位系統之一，僅使用兩個數位（0 和 1）來代表所有的數位。在二進位裏，數位1寫成1，2寫成10，3寫成11，4寫成100，如此類推。儘管為方便起見，IP 位址常常用十進位的數位來表達，但實際上，IP位址是二進位數字；例如，209.191.4.240 在二進位內是11010001.10111111.00000100.11110000。又見bit, IP address, network mask。
bit	比特，“binary digit，二進位數字”的簡寫，一個 bit 其實是有 0 或 1 兩個值的數位。又見 binary。
bps	每秒位元數。
CoS	服務等級，由 802.1Q 加以定義，數值範圍由 1 至 7。
broadcast	廣播，把資料傳送到網路中所有的電腦上。
download	下載，從網際網路傳遞資料給用戶。
Ethernet	乙太網路，最普遍應用的電腦網路技術，常使用雙絞線電纜。乙太網資料傳輸率為10 Mbps 與 100 Mbps。又見10BASE-T, 100BASE-T, twisted pair。
filtering	過濾，以過濾規則為基礎篩選出資料的類型。過濾可被應用在一個方向（上載或下載），或雙向。
filtering rule	過濾規則，一個指定路由設備將接收和 / 或拒絕何種類型的資料的規則。過濾規則被定義為，在某一介面（或多個介面）操作且朝著特定方向（如下載、上載，或雙向）。
FTP	File Transfer Protocol，檔案傳輸協定。一程式用於在連線至網際網路的電腦間傳輸檔案。最常見的使用方式便是上傳新聞或檔案至 Web 伺服器，或是自 Web 伺服器下載資料。
host	主機，連接到網路的設備（通常是指電腦）。

## GigaX 系列

HTTP	Hyper-Text Transfer Protocol，超文本傳輸協定，HTTP是 用在Web瀏覽器與Web伺服器之間傳輸文件（如文字或 圖片文件）的協定。又見web browser, web site。
ICMP	Internet Control Message Protocol，網際網路控制消息協 定，網路層面的網際網路協定，負責錯誤報告及提供I P 封包處理相關的資訊。Ping 命令就使用了ICMP。
IGMP	Internet Group Management Protocol，網際網路群組管理協 定，一個使電腦能在多點廣播內與相鄰路由器與分享成 員資訊的網際網路協定。多點廣播群組是指成員已經被 認定為願意從其他電腦那裏接收特定內容的資訊感興趣 的群組。對IGMP群組的多點廣播可同時被用來更新移動 用戶群組位址簿，或將公司的時事通訊傳送到名單上的 用戶。
IGMP Snooping	在與第二層多重播送群組相關聯的每個連接埠進 行封包偵聽的動作。
Internet	網際網路，最大的全球性網路，連接全世界上萬個網 路，為私人和商業用戶使用。
intranet	內部網路，一個私人的，或企業內部的網路，看起來像 網際網路的一部分（用戶使用網頁瀏覽器訪問資訊）， 但是僅為內部成員使用。
IP	見TCP/IP。
IP address	Internet Protocol address，網際網路協定位址，網際網路上 主機（電腦）的位址，由四個數位組成，每個都是從0 到 255，以點號隔開，例如，209.191.4.240。IP位址由確 認主機所屬的特殊網路的network ID與確認主機自身處於 網路的獨一無二的host ID 構成。網路遮罩被用來定義 network ID與 host ID。因為每個成員的IP位址均不相同， 所以他們常常擁有相關聯可被指定的功能變數名稱。 又見 domain name, network mask。
ISP	Internet Service Provider，網路服務供應商，提供顧客訪問 網際網路收費服務的公司。
LAN	Local Area Network，區域網路，局限於一個小的地理區 域的網路，例如，家庭、辦公室，或小型建築。
LED	Light Emitting Diode，發光二極體，透過轉換電子能量的 方式來發射光線的半導體設備。一般硬體設備上的狀態 燈都是典型的LED。

## 第二層網路管理交換器

MAC address	Media Access Control address，媒體訪問控制位址，由製造商指定的設備的永久硬體位址。MAC位址用六對字元來表示。
mask	見network mask。
Multicast	將資料傳輸到一個群組的網路裝置。
Mbps	每秒百萬位元，Megabits per second的簡寫。網路資料傳輸率通常用Mbps來表示。
Monitor	又被稱作“游移分析”，可讓您附加一分析器於一網路連接埠，並使用其監控分析交換器上其他連接埠的傳輸狀況。
network	網路，一群可透過傳輸媒體互相通信的電腦、印表機、交換器及其它的設備。網路可以很小，如區域網路LAN，也可以非常大，如網際網路Internet。
network mask	網路遮罩，指一系列當忽略掉host ID時被應用於IP位址選擇的一系列bit。Bit設定為1意味著“選擇此位”，而當bit設定為0則意味著“忽略此位”。例如，如果網路遮罩255.255.255.0應用到IP位址100.10.50.1，那network ID為100.10.50，host ID為1。又見binary, IP address, subnet。
NIC	Network Interface Card，網路介面卡，插入您的電腦中，並能為網路線纜提供物理介面的介面卡，典型的乙太網NIC是RJ-45連接器。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、添加的資訊例如它從那裏來（來源位址）以及將到哪里去（目標位址）。
ping	Packet Internet (or Inter-Network) Groper，資訊及其回應，用來檢驗與IP位址相關聯的主機是否在線的程式。它亦能被用來顯示給定功能變數名稱的IP位址。
port	埠，電腦、路由器等設備的物理接入點，資料透過埠來流入和流出此設備。
protocol	協定，管理設備如何在網路上交換資訊的一套規則和規範的正式稱呼。
remote	遠端，物理上分離的位置。例如，員工在出差的途中登入公司內部網路為遠端用戶。

## GigaX 系列

RJ-45	8-pin 的插頭用來代替電話線傳輸資料。乙太網線纜通常使用此種類型的連接器。
RMON	遠端監控 - 延伸至 SNMP，提供廣泛的網路監控能力。
routing	路由，找到一條到達目的地主機路徑的程式。在大型網路裏，路由是非常複雜的，因為封包在抵達目的地之前，可經過的中間節點非常多。履行路由職責的設備被稱為路由器。
SNMP	Simple Network Management Protocol，簡單網路管理協定，用於網路管理的指TCP/IP 協定。
STP	生成樹協定 - 為一橋接協定，用以避免封包在複雜的網路環境下發生不斷循環無法傳遞的狀況。
subnet mask	子網路遮罩，定義子網的遮罩。又見network mask。TCP 見TCP/IP。
TCP	見TCP/IP。
TCP/IP	Transmission Control Protocol/Internet Protocol，傳輸控制協定/網際網路協定，網際網路所使用的基本協定。TCP 負責分割需傳遞資料至封包並在目的地將它們重新組裝起來，而IP 負責將封包從來源地傳輸至目的地。當TCP 和 IP與高級應用程式如HTTP, FTP, Telnet等捆綁在一起時，TCP/IP指的是整套協定。
Telnet	互動式的、通常用在使得用戶能登入遠端的系統就如同在本地般使用其資源的遠端終端機聯機。HTTP（網路協定）與FTP僅允許您從遠端電腦下載文件，而Telnet可允許您從遠端登入及使用電腦。
TFTP	Trivial File Transfer Protocol，一般文件傳輸協定，FTP的簡化版，允許在網路上傳送和接收文件的協定，但是沒有FTP的功能強大，安全性也較差。
Trunk	兩個或更多的連接埠相連成一虛擬的網路連接埠，又被稱作連結彙聚。
TTL	Time To Live，存活時間，IP表頭中的專案，用來指出一個封包被認為有效的時間有多長。TTL 為零時，封包將被丟棄。

## 第二層網路管理交換器

---

twisted pair	雙絞線，包含兩條被絞成螺旋狀絕緣線的低速傳輸媒體。此絕緣線可以是遮蔽或無遮蔽。雙絞線是語音通訊應用中常見的媒體，且日漸在資料網路上逐漸普遍。對於乙太網LAN，一個更高等級的 Category 3 (CAT 3) 正在為 10BASE-T 網路所應用，一個更高等級的 Category 5 (CAT 5)正在為 100BASE-T 網路所應用。又見 10BASE-T, 100BASE-T, Ethernet。
upstream	向上游，資料傳輸的方向是從用戶到網際網路。
VLAN	虛擬區域網路。
WAN	Wide Area Network，廣域網路，由電信公司所提供，服務於廣大區域使用者的資料通訊網路。對於交換器來說，WAN指整個網際網路。
Web browser	使用超文件傳輸協定HTTP來從網路站點下載資訊，並為用戶顯示由文件、圖形、音頻或視頻組成的資訊的用戶端的應用軟體。例如，Internet Explorer、Mosaic和Netscape Navigator。又見 HTTP, web site, WWW。
Web page	網頁，網路站點文件，一般包括文本、圖形以及鏈結到本站點及其它站點的網頁的超鏈結（前後對照）。當用戶訪問網路站點時，顯示的第一個頁面稱為主頁 home page。又見hyperlink, web site。
Web site	網路站點，指網際網路上透過網頁瀏覽器分配資訊給遠端用戶、以及從遠端用戶獲得資訊的電腦。網路站點一般由包含文本、圖形以及超鏈結的網頁組成。又見hyperlink, web page。
WWW	World Wide Web，全球資訊網。提供超鏈結及其它服務給執行像瀏覽器等用戶端軟體的網際網路伺服器的大型網路。











