



GigaX2024B/M

第二層網路管理交換器

使用手冊

T2635

2006 年 9 月

第一版

版權所有・不得翻印 © 2006 華碩電腦

在未獲得華碩電腦公司（以下稱華碩）書面許可的情況下，本手冊中的任何部分，包括所述產品和軟體，均不得通過任何手段以任何形式進行複製，轉換格式，轉譯，翻譯以及儲存於公共資源系統中。本手冊僅作為使用者購買時附帶的說明文檔。

若出現以下情況，恕不再提供產品的保固或服務：(1) 產品已由未經華碩書面授權的維修商進行維修，改裝；或 (2) 產品序列號無法辨識或已丟失。

華碩提供本手冊不代表華碩作出任何隱含或直接的保證，這些保證包括但不限於隱含的保固承諾，產品的暢銷性，或針對某種需求的必然適應性。在任何情況下，華碩電腦公司，其領導層，其各級官員和職員，以及其代理商對於本產品造成的任何間接的，特殊的，意外的或後續的損害（包括利潤損失，業務損失，資料丟失，業務中斷等類似損失）均不承擔責任，即使華碩已經事先接到通知提醒，本產品或手冊中的錯誤或缺陷可能導致上述損失。

本手冊中的規格和資訊僅供參考，並以華碩最新修訂版本為準，並且華碩毋需對本手冊內容的修改進行通知。華碩對本手冊中任何錯誤或不精確的資料均不承擔責任，其中包括產品以及所述軟體。

本手冊中出現的產品和公司名可能是其各自公司的註冊商標或版權，華碩在手冊中的引用僅作為方便使用者進行識別或解釋的一種手段，並非對相關公司的侵權行為。

華碩連絡資訊

華碩電腦公司 ASUSTeK COMPUTER INC.

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

技術支援

電話 +886-2-2894-3447

ASUS COMPUTER INTERNATIONAL (美國)

地址 44370 Nobel Drive, Fremont, CA 94538, USA
傳真 +1-510-608-4555
全球資訊網 usa.asus.com

技術支援

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

ASUS COMPUTER GmbH (德國 / 奧地利)

地址 Harkort Str. 25, D-40880 Ratingen, Germany
電話 +49-2102-95990
傳真 +49-2102-959911
全球資訊網 www.asuscom.de
線上連絡 www.asuscom.de/sales

技術支援

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

目錄內容

1	產品簡介	1
1.1	GigaX2024B/M 特性	1
1.2	關於本使用手冊	2
1.2.1	注意事項	2
1.2.2	印刷提示	2
1.2.3	提示符號	2
2	瞭解 GigaX2024B/M 交換器	3
2.1	產品包裝內容	3
2.2	前面板	4
2.3	後面板	5
2.4	技術規格	5
3	快速安裝指南	6
3.1	第一部分 — 硬體安裝	6
3.1.1	將交換器安裝於平坦表面	6
3.1.2	將交換器安裝於機架	6
3.2	第二部分 — 設定交換器	6
3.2.1	連接控制終端連接埠 (Console port)	6
3.2.2	連接到電腦或區域網路	7
3.2.3	連接備用電源模組 (RPS)	7
3.2.4	連接電源線	7
3.3	第三部分 — 交換器的基本管理設定	8
3.3.1	透過控制終端連接埠進行設定	8
3.3.2	透過 WEB 介面進行設定	10
4	用網頁介面進行管理	11
4.1	登入網頁管理使用者介面	11
4.2	功能結構	12
4.2.1	瀏覽選單的技巧	14

4.2.2	常用按鈕與圖示	14
4.3	系統頁面	15
4.3.1	管理 (Management) 頁面	15
4.3.2	IP 設定 (IP setup 設定) 頁面	15
4.3.3	重新啟動 (Reboot) 頁面	16
4.3.4	韌體升級 (Firmware upgrade)	16
4.4	實體介面	17
4.5	橋接 (Bridge) 頁面	19
4.5.1	生成樹 (Spanning tree)	19
4.5.1.1	STP 狀態 (STP status)	19
4.5.1.2	當前根 (Current roots)	20
4.5.1.3	橋接器參數 (Bridge parameters)	21
4.5.1.4	連接埠參數 (Port parameters)	22
4.5.1.5	運行狀態 (Runtime status)	23
4.5.2	連結匯聚 (Link aggregation static)	23
4.5.3	LACP	25
4.5.4	鏡像 (Mirroring)	26
4.5.5	靜態多重播送 (Static multicast)	27
4.5.6	IGMP 偵聽 (IGMP snooping)	28
4.5.7	流量控制 (Traffic control)	29
4.5.8	動態位址 (Dynamic addresses)	30
4.5.9	靜態位址 (Static addresses)	30
4.5.10	VLAN 設定 (VLAN configuration)	31
4.5.11	GVRP	33
4.5.12	QoS 與 CoS	34
4.5.12.1	802.1p 優先權	34
4.5.12.2	CoS 佇列映射	36
4.5.12.3	QoS 頻寬	37
4.6	簡易網路管理協定 (SNMP)	38

4.6.1	群組列表 (Community Host Table)	38
4.6.2	Trap 設定 (Trap setting)	39
4.6.3	SNMPv3 VGU 列表	40
4.6.4.1	VACM 檢視 (VACM view)	40
4.6.4.2	VACM 群組 (VACM group)	41
4.6.4.3	USM 使用者 (USM user)	42
4.7	過濾功能頁面 (Filter pages)	43
4.7.1	過濾組合 (Filter set)	43
4.7.2	附加過濾規則 (Filter attach)	45
4.8	安全 (Security)	46
4.8.1	連接埠存取控制 (Port access control)	46
4.8.2	撥入使用者 (Dial-in user)	48
4.8.3	RADIUS	49
4.8.4	連接埠安全 (Port security)	50
4.8.4.1	連接埠設定 (Port configuration)	50
4.8.4.2	連接埠狀態 (Port status)	51
4.8.4.3	安全 MAC 位址 (Secure MAC address)	52
4.9	流量統計圖表 (Traffic chart)	53
4.9.1	流量比較 (Traffic comparison)	53
4.9.2	錯誤群組 (Error group chart)	54
4.9.3	歷史狀態 (Historical status)	54
4.10	纜線診斷 (Cable diagnosis)	55
4.11	管理交換器的堆疊	55
4.12	儲存設定值 (Save configuration)	57
5	控制終端介面 (Console interface)	58
5.1	開機自我測試 (Power-on self test)	58
5.1.1	Boot ROM 指令模式	58
5.1.2	Boot ROM 指令	59
5.2	登入與登出	60

5.3	CLI 指令	60
5.3.1	使用者帳號 (User account)	60
5.3.2	備份與回復 (Backup and Restore)	60
5.3.3	系統管理設定 (System management configuration)	61
5.3.4	實體介面指令 (Physical interface commands)	64
5.3.5	IP 介面 (IP interface)	66
5.3.6	生成樹 (Spanning Tree)	67
5.3.7	連結匯聚 (Link aggregation)	67
5.3.8	LACP	68
5.3.9	鏡像 (Mirroring)	70
5.3.10	靜態多重播送 (Static Multicast)	70
5.3.11	IGMP 偵聽 (IGMP snooping)	71
5.3.12	流量控制 (Traffic control)	71
5.3.13	動態位址 (Dynamic addresses)	72
5.3.14	靜態位址 (Static addresses)	73
5.3.15	VLAN	73
5.3.16	GVRP	74
5.3.17	CoS/QoS	75
5.3.18	SNMP	76
5.3.19	過濾 (Filter)	76
5.3.20	連接埠存取控制 (Port access control)	77
5.3.21	撥入使用者 (Dial-in user)	78
5.3.22	RADIUS	78
5.3.23	連接埠安全 (Port security)	78
5.4	其他指令 (Miscellaneous commands)	79
6	IP 位址，網路遮罩和子網路	81
6.1	IP 位址	81
6.1.1	IP 位址的結構	81
6.1.2	網路類型	82
6.2	子網路遮罩	82

- 7 疑難排解84
 - 7.1 使用 IP 工具診斷問題 84
 - 7.1.1 ping 84
 - 7.1.2 nslookup 85
 - 7.2 更換損壞的風扇..... 86
 - 7.3 簡易維修..... 88
- 8 術語表90

1 產品簡介

感謝您購買華碩 GigaX2024B/M 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。

本使用手冊將為您提供安裝和設定 GigaX2024B/M 交換器所需的相關資訊。

1.1 GigaX2024B/M 特性

- 24 個 10/100BSAE-T 以及 2 個 10/100/1000BASE-T 自動偵測 gigabit 乙太網路交換埠。若使用 all-in-one 模組，GigaX2024M 還可獲得兩個額外的 10/100/1000BASE-T 自動偵測 gigabit 乙太網路交換埠。
- 兩個小型 (SFP) Gigabit 介面轉換插槽 (GBIC)
- 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)
- STP/RSTP/MSTP
- GigaX2024M 支援 16K (GigaX2024B 支援 8K) MAC 位址快取及硬體控制的存在時間
- 802.3x 流量控制
- 基於 802.1Q 標記之虛擬區域網路 (VLAN)，GigaX2024B 最多支援 255 組虛擬區域網路，GigaX2024M 最多支援 3000 組虛擬區域網路
- 802.1p 服務等級，GigaX2024B 每個連接埠支援 4 個佇列，GigaX2024M 每個連接埠支援 8 個佇列。
- 支援 IGMP 偵聽
- 802.3ad 連結匯聚 (幹線)，GigaX2024B 最多可支援 6 個幹線群組，GigaX2024M 最多可支援 8 個幹線群組
- LACP
- GVRP
- 存取控制列表
- 速率限制，GigaX2024B 以 1Mbps 為間隔，GigaX2024M 以 64Kbps 為間隔
- 連接埠鏡像 (Port Mirroring) 功能
- 802.1x 認證
- 連接埠安全 (Port Security) 功能
- 支援 DHCP 偵聽

- SNMP v1, v2, v3 簡易網路管理通訊協定
- 支援 MIB-II 管理資料庫
- 企業級電源供應器、風扇和系統溫度、電壓管理資料庫 (MIB)
- Telnet/SSH 遠端登入
- TFTP 韌體升級和備份設定
- 如 Cisco 操作的 CLI 指令介面
- 網頁圖形使用者介面 (GUI)
- LED 指示燈，用於顯示連接埠連線狀態

1.2 關於本使用手冊

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，GigaX2024B/M 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。

2 瞭解 GigaX2024B/M 交換器

2.1 產品包裝內容

GigaX2024B/M 交換器的產品包裝中包含以下物品：

- GigaX 2024B/M 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

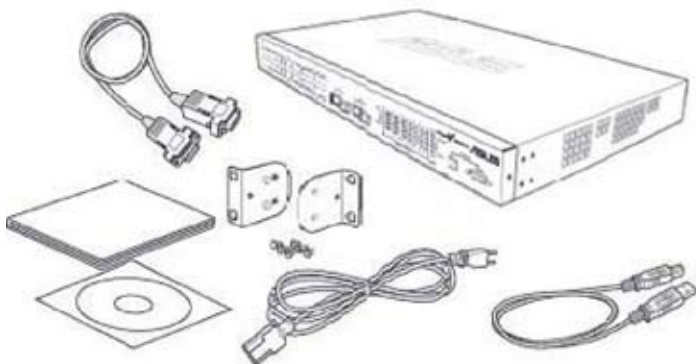


圖 1. GigaX 第二層網路管理交換器產品包裝內容

2.2 前面板

前面板包括了 24 個 RJ-45 10/100Base-T 連接埠，2 個 10/100/1000Base-T 連接埠，2 個 SPF GBIC 連接埠和一組 LED 指示燈，用於顯示系統、備用電源 (RPS)、風扇與連接埠的狀態。

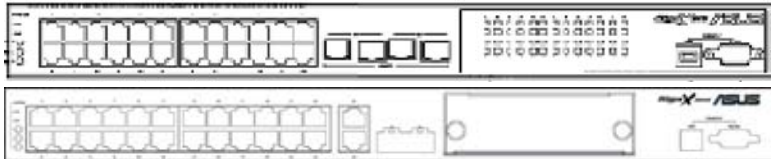


圖 2. 前面板 (上：GigaX2024B 下：GigaX2024M)

表 1. 前面板標示和 LED 指示燈

標示	顏色	描述
SYSTEM	綠色	裝置電源開啓
		自我檢測，初始化或下載中
	琥珀色	溫度或電壓不正常
	熄滅	無電源供應
RPS	綠色	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	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	兩個風扇均工作正常
	琥珀色	兩個風扇全部或有一個停止運轉
10/100 ports	綠色	乙太網路連線已建立
		正在傳送或接收資料
	熄滅	無乙太網路連線
10/100/1000 port status	綠色	已建立 RJ-45 或 SFP 連線；連接埠已啓用
		正在傳送或接收資料
	琥珀色	已建立連線，但連接埠已被手動或生成樹關閉
		連接埠處於生成樹協定阻斷、偵聽和學習狀態
	熄滅	無乙太網路連線
10/100/1000 port speed	綠色	1000Mbps
	琥珀色	100Mbps
	熄滅	10Mbps

2.3 後面板

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

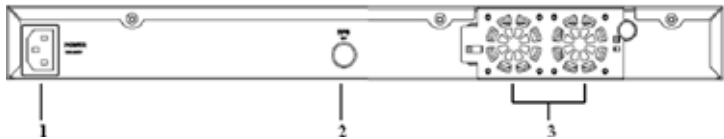


圖 3. 後面板

表 2. 後面板標示

序號	標示	描述
1	Power Connector	連接電源線
2	RPS	備用電源供應器
3	FAN1-FAN2	可抽換式風扇

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	< 50 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)
可抽換式風扇	尺寸	電壓和電流	轉速
	40 x 40 x 20 mm	12VDC, 0.13A	8200RPM

3 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 GigaX2024B/M 的安裝指南。

第一部分介紹如何將 GigaX2024B/M 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 GigaX2024B/M 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. 請將托架分別對準交換器兩側的對應螺絲孔。
2. 用三個螺絲來將托架固定到交換器的一側。
3. 重複上述步驟，固定交換器另一側的托架。
4. 用四個機架螺絲將交換器固定於機架上（本產品包裝中不含機架螺絲）。

3.2 第二部分 — 安裝交換器

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（需要安裝隨機光碟中的 USB 驅動程式）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。您可以使用直通型或交叉型乙太網路線來連接這些裝置。



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

3.2.3 連接備用電源模組 (RPS)

將備用電源 (RPS) 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。

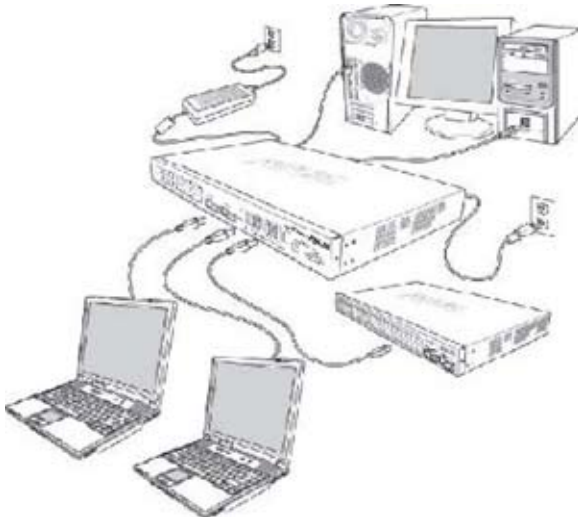


圖 4. 硬體連接示意圖

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啓。如果 LED 熄滅，請檢查交換器電源線是否正確連接並已連接到電源插座。
2	Switch ports [1] to [26]	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 IE5.0 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，專門用於資料終端設備 (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) 及一個停止位元 (Stop bit)。
 - d) 無流量控制
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案中。
- g) 輸入 “reboot”。

如果交換器必須透過網路進行管理，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。若您輸入了不正確的路由，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:
ASUS GigaX 2024B 3.2.02.00 Copyright (c) 2005

ASUS> enable
ASUS# configure terminal
ASUS(config)# interface vlan 1
ASUS(config-if)# ip address 192.168.1.1/24
Install IP address 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. 控制終端設定

3.3.2 透過 WEB 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 Runtime Environment，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。



Java Runtime Environment 安裝到您的電腦後，您才可以透過網頁進行交換器的管理與設定。您可以從公用程式光碟中找到安裝程式。

2. 在交換器可以存取的網路中任何一臺電腦上，開啓您的網頁瀏覽器 (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. 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)



您可以隨時更改密碼 (參考 6.3.1 節系統指令部分的說明)。

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、子網路遮罩與預設閘道器，完成後點選 **OK**。
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 7. IP 設定

4 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工作。本功能推薦使用支援 Java® 的微軟 Internet Explorer® 6.0 或更高版本。

4.1 登入網頁管理使用者介面

1. 在您的電腦上開啓網頁瀏覽器 (IE)，在網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登入視窗，如圖 8 所示。



圖 8. 設定管理界面登入畫面

2. 輸入您的使用者名稱和密碼，並按下 **OK**。

在首次登入時，請使用下面的預設值。您可以藉由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： <無密碼>

每次當您登入網頁管理介面時，您都會看到如圖 9 所示的主畫面。



圖 9. 網頁管理介面主畫面

4.2 功能結構

網頁設定頁面包含三個獨立的欄位。頂部欄包含了交換器圖示和前面板圖，如圖 10 所示。這個欄位將一直位於瀏覽器視窗上方，同步顯示交換器前面板的 LED 燈號。請參考表 4 以認識各燈號的含義。關於各燈號顏色的含義，請參考表 5。



GigaX2024B



GigaX2024M 無 module 卡

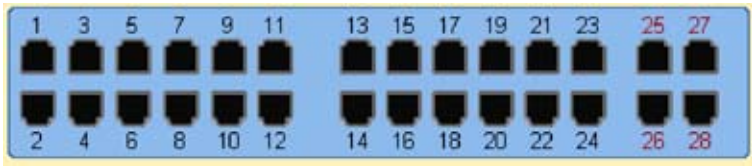


GigaX2024M 帶 all-in-one 卡



GigaX2024M 帶 stack 卡

圖 10. 頂部欄



GigaX2024M 帶 all-in-one 卡



GigaX2024B, GigaX2024M 無 module 或 stack 卡

圖 11. 連接埠選擇面板

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	連線已存在但連接埠被手動或被生成樹禁用
熄滅	無乙太網路連線

點選交換器連接埠圖標即可在畫面右下方欄位中顯示該連接埠的設定。

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啓對應的功能。

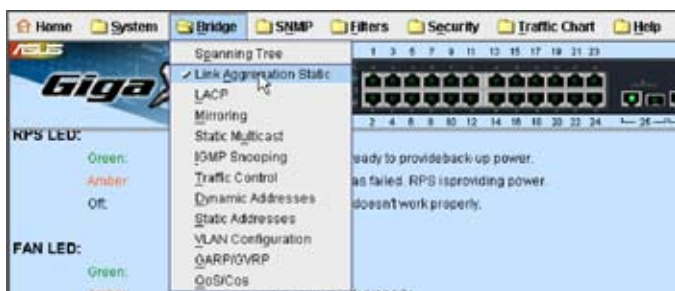


圖 12. 選單項目

4.2.1 瀏覽選單的技巧

若要開啓特定的設定頁面，請在選單中點選您所要開啓的選項。

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 / 圖標	描述
	儲存您對當前頁面做的任何變更。
	重新顯示當前頁面，更新狀態和設定。
	在系統中修改既有設定，如靜態路由或過濾的 ACL 規則。
	在系統中創建一個新的設定。
	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。
	修改一個既有項目。
	刪除已選擇的項目，如靜態路由或過濾的 ACL 規則。
	查找一個指定項目的狀態。
	從所有連接埠移除此設定值。
	新增此設定值至所有連接埠。

4.3 系統頁面

系統頁面包含有 管理 (Management)，IP 設定 (IP setup)，管理權限 (Administration)，重新啟動 (Reboot) 和 韌體升級 (firmware update) 功能。

4.3.1 管理 (Management) 頁面

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: 使用者指定的用來辨識系統的名稱 (可編輯)。

System Contact (可編輯)。

System Location (可編輯)。

點選 OK 可儲存變更並使其立即生效。點選 Reload 將更新設定到當前值。如圖 13 所示。



圖 13. 管理頁面

4.3.2 IP setup (IP 設定) 頁面

IP Setup 頁面包含以下可編輯的資訊：

DHCP Client: 啟用或禁用 DHCP。

IP Address: 為交換器指定一個靜態 IP 位址。

Network Mask (網路遮罩)

Default Gateway (預設閘道器)

點選 OK 可儲存變更並使其立即生效。點選 Reload 將更新設定到當前值。



圖 14. IP 設定頁面

4.3.3 重新啟動 (Reboot) 頁面

重新啟動 (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 韌體升級 (Firmware Upgrade)

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

- Hardware Version: 顯示硬體版本號。
- 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 來升級交換器的韌體。請參考圖 15。

例如：TFTP 伺服器：192.168.1.155 檔案名稱：gx2024b-3.2.02.0a.img



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



圖 15. 韌體升級頁面

4.4 實體介面

實體介面會即時顯示乙太網連接埠的狀態。您可以設定以下項目：

Port: 選擇需要設定的連接埠

Admin: 啟用 / 禁用連接埠

Mode: 設定速度與雙工模式

Flow Control: 啟用 / 禁用 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: 完整啟用 / 禁用 DHCP 偵聽功能。要將此功能套用至指定的 VLAN，您需要在 VLAN 設定 (VLAN Configuration) 中為不同的 VLAN 開啟 VLAN-Snooping 功能。

DHCP-Snooping: 指定所選擇的連接埠為不可信任或可信任的埠。

選擇對應的連接埠號並對其進行設定，然後點選 **Modify** 按鈕。您所更改的項目將會在視窗中更新。然而，只有執行了 **Save Configuration** 之後，您所做的更新才會生效。

Runtime Status Window: 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: 啟用或禁用 802.3x 流量控制機制。

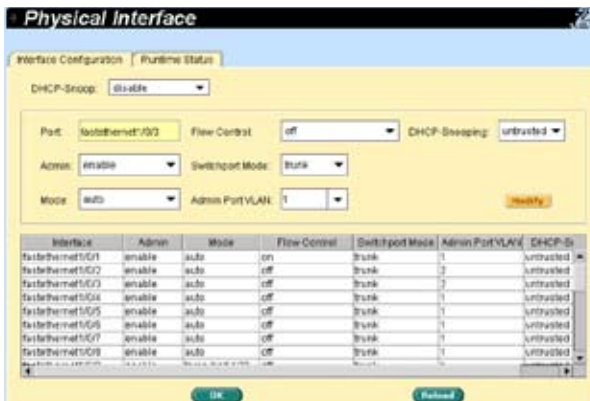


圖 16. 實體介面 - 設定頁面

Physical Interface

Interface Configuration

Runtime Status

Interface	Ethernet Link	STP Status	Duplex	Speed	Flow Control	Oper Prio
FastEthernet0/01	not connected	N/A	N/A	N/A	N/A	1
FastEthernet0/02	not connected	N/A	N/A	N/A	N/A	2
FastEthernet0/03	not connected	N/A	N/A	N/A	N/A	2
FastEthernet0/04	not connected	N/A	N/A	N/A	N/A	1
FastEthernet0/05	not connected	N/A	N/A	N/A	N/A	1
FastEthernet0/06	not connected	N/A	N/A	N/A	N/A	1
FastEthernet0/07	not connected	N/A	N/A	N/A	N/A	1
FastEthernet0/08	not connected	N/A	N/A	N/A	N/A	1
FastEthernet0/09	not connected	N/A	N/A	N/A	N/A	1
FastEthernet0/10	not connected	N/A	N/A	N/A	N/A	1
FastEthernet0/11	not connected	N/A	N/A	N/A	N/A	1
FastEthernet0/12	not connected	N/A	N/A	N/A	N/A	1
FastEthernet0/13	not connected	N/A	N/A	N/A	N/A	1
FastEthernet0/14	not connected	N/A	N/A	N/A	N/A	1
FastEthernet0/15	not connected	N/A	N/A	N/A	N/A	1
FastEthernet0/16	not connected	N/A	N/A	N/A	N/A	1
FastEthernet0/17	not connected	N/A	N/A	N/A	N/A	1
FastEthernet0/18	not connected	N/A	N/A	N/A	N/A	1

Refresh

圖 17. 實體介面 - runtime status 頁面

4.5 橋接 (Bridge) 頁面

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

4.5.1 生成樹 (Spanning tree)

本頁面可設定三種不同類型的生成樹協定。

4.5.1.1 STP 狀態 (STP Status)

第一頁 “STP Status” 可以啟用或禁用 STP。您可以啟用 STP、RSTP 與 MSTP 三種模式。若啟用了 MSTP，則以下的四種屬性也同時啟用：

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: 此群組能聯結可被建立的 3000 個 VLAN 裡的每一個 VLAN 到給定的實例 (instance)。

Instance ID	VLAN Group	State
1	all	Enabled
2		Disabled
3		Disabled
4		Disabled
5		Disabled
6		Disabled
7		Disabled

圖 18. 生成樹 - status 頁面

4.5.1.2 當前根 (Current roots)

本頁顯示了當前根的相關資訊，包括：

- 實例 (Instance) ID
- VLAN 群組屬於哪個實例 (Instance) ID
- 根橋的 MAC 位址
- 根橋的優先順序
- 根橋的最長存在時間
- 根橋的 Hello timer
- 根橋的轉發延遲計時器
- 根橋的路徑耗費 (Cost)
- 橋接器的根埠

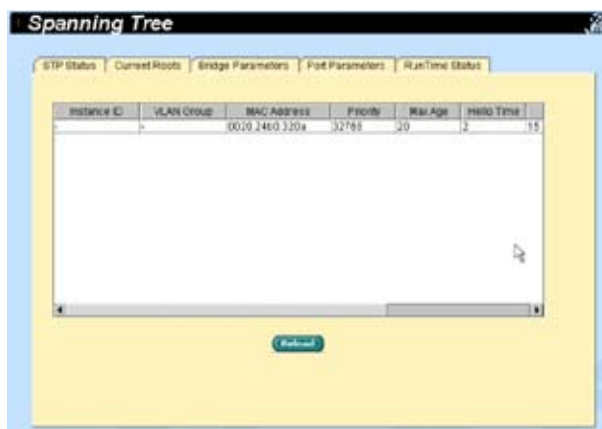


圖 19. 生成樹 - current roots 頁面

4.5.1.3 橋接器參數 (Bridge parameters)

在這個頁面中可以設定 BPDU 傳輸的生成樹參數 (Spanning-tree parameters)：

Hello Time: BPDU 生成設定的間隔。

Max Age: 區域網路中所有橋接裝置使用的超時設定值。

Forward Delay: 轉發延遲。

Bridge Priority: 交換器在區域網路中的優先順序。

Transmission Limit: 根交換器總是傳送一個 BPDU (或 M-record) 訊息，耗費 (Cost) 為 0，transmission limit 設定為最大值。

Instance ID	VLAN Group	Priority	Max Age	Hello Time	Forward Delay	Trans
1	22768	20	2	15	3	

Buttons: OK, Refresh

圖 20. 生成樹 - bridge parameters 頁面

4.5.1.4 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當前設定。您可以選擇一個連接埠然後對其進行編輯。點選 **Modify** 按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)：一個生成樹實例 (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)。

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

Path Cost：有效的設定值為 1 至 65535 (RSTP:200000000)。當偵測到網路迴路的狀況下，具有較高耗費 (Cost) 的連接埠較可能被 STP 封鎖。

Link Type：預設情況下，連線類型 (Link Type) 由介面的雙工模式決定：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：邊緣連接埠與 Port Fast-enabled 連接埠相同，只有在連接了一個單獨的終端裝置時您才可以啓用它。

點選 **OK** 使設定生效。點選 **Reload** 更新設定到當前值。

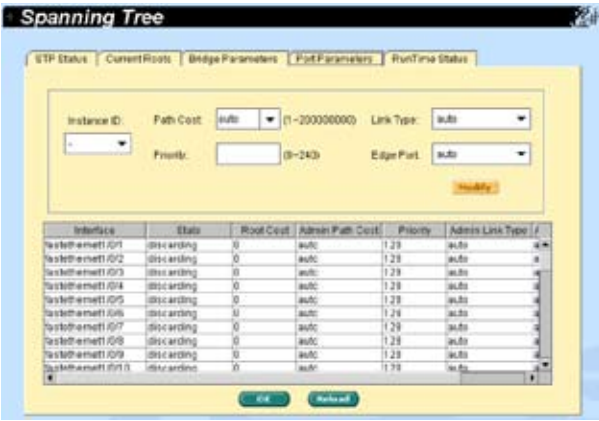


圖 21. 生成樹 - port parameters 頁面

4.5.1.5 運行狀態 (Runtime status)

本頁面包含了一個顯示視窗，用來顯示每個連接埠的當前狀態。

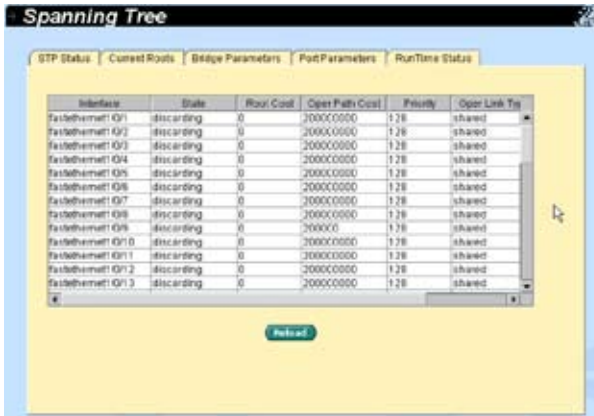


圖 22. 生成樹 - runtime status 頁面

4.5.2 連結匯聚 (Link aggregation static)

本頁面用來設定連結匯聚群組。GigaX2024B 最多可提供 6 個連結匯聚群組，而 GX2024M 最多可提供 8 個連結匯聚群組。

Port Selection Criterion: 依照封包的來源 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、來源與目的地 IP 位址在連結匯聚群組的各連接埠之間分配封包的一種演算法。

Trunk ID: 除了群組名稱外，用來區分不同匯聚群組的號碼。

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移除。

點選 **OK** 來將設定傳送到交換器。點選 **Reload** 來更新設定到當前值。要使設定生效，請至 **Save Configuration** 頁面並點選 **Save**。

您需要檢查連線速度和雙工模式來確認連結匯聚群組實體處於正常運作狀態。請至 **Physical Interface** 頁面的 **Runtime status** 視窗檢查匯聚連接埠的連線模式。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，則其他連接埠也必須具有相同的設定，否則連結匯聚可能發生運作異常的狀況出現。

連結匯聚群組中所有的連接埠必須具有相同的 VLAN 設定。

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

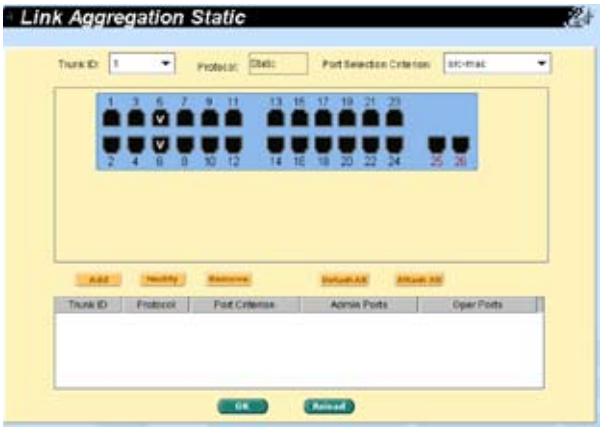


圖 23. 連結匯聚頁面

4.5.3 LACP

本頁面用來設定 LACP 群組（連接埠匯聚）。GX2024B 提供了最多 6 組（GX2024M 提供最多 32 組）連結匯聚群組，每個群組最多可支援 8 個連接埠。

Port Selection Criterion: 依照封包的來源 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、來源與目的地 IP 位址在連結匯聚群組的各連接埠之間分配封包的一種演算法。

Trunk ID: 除了群組名稱外，用來區分不同匯聚群組的號碼。

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移除。



圖 24. LACP 頁面

4.5.4 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: 從選擇面板上選擇鏡像群組。您可以對選定連接埠的傳入、傳出流量或同時對這兩種流量進行鏡像。

Mirror Mode: 啟用或禁用選定群組的鏡像功能。

Monitor Port: 接收選定的鏡像連接埠的所有流量的備份資料。

- 監控連接埠不能屬於任何連結匯聚群組。
- 監控連接埠不能屬於任何私有 VLAN。
- 監控連接埠不能像一般交換器連接埠一樣運作。它不能進行封包交換或位址學習。

點選 **OK** 將設定傳送至交換器 (HTTP 伺服器)。點選 **Reload** 更新設定至當前值。

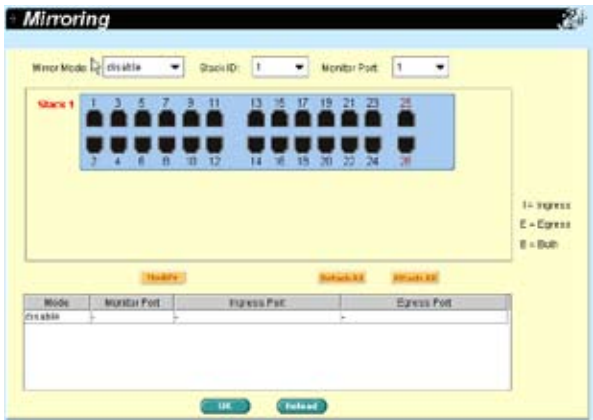


圖 25. 鏡像頁面

4.5.5 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。

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。

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。

CoS: 指定服務等級 (CoS) 的優先順序。

點選 **OK** 來使設定生效。點選 **Reload** 將設定更新至當前值。



圖 26. 靜態多重播送頁面

4.5.6 IGMP 偵聽 (IGMP snooping)

藉由開啓或關閉 IGMP 偵聽功能，可以幫助減少網路中的多重播送流量。

第一部分提供以下功能設定：

Enable IGMP Snooping: 完整開啓所有 VLAN 介面的 IGMP 偵聽功能。在預設值中，交換器的 IGMP 偵聽功能已經開啓。當完整開啓後，所有 VLAN 介面的 IGMP 偵聽都被開啓。

若完整偵聽功能沒有開啓，您無法開啓 VLAN 偵聽功能。若完整偵聽功能開啓，您可以開啓或關閉 VLAN 偵聽功能。

Last Member Query Interval: 沒有即時離線 (Immediate-Leave) 功能的情況下，當交換器的接收埠從一個使用者處收到一個 IGMP 離線訊息時，不會立即離線。它會傳送一個 IGMP 詢問到該連接埠，並等待 IGMP 群組所有成員回覆。如果在設定的時間內，沒有收到回覆，該接收埠將從多重組播的群組成員中移除。

第二部分提供以下功能設定：

Status: 如果完整的偵聽功能已開啓，您可以開啓或關閉 VLAN 偵聽功能。

Immediate leave: 當您開啓 IGMP 即時離線 (Immediate-Leave) 功能後，當交換器在某連接埠檢測到一個 IGMP 版本 2 離線訊息時，交換器會立即將該連接埠移除。只有當 VLAN 中每個連接埠只有一個主機的情況下才可以使用即時離線 (Immediate Leave) 功能。僅 IGMP 版本 2 的主機才可支援即時離線 (Immediate Leave) 功能。

然而，如果靜態位址占用了全部的 256 個位址空間，IGMP 偵聽將無法正常運作。本交換器只允許 256 個二層多重播送群組。



圖 27. IGMP 偵聽頁面

4.5.7 流量控制 (Traffic control)

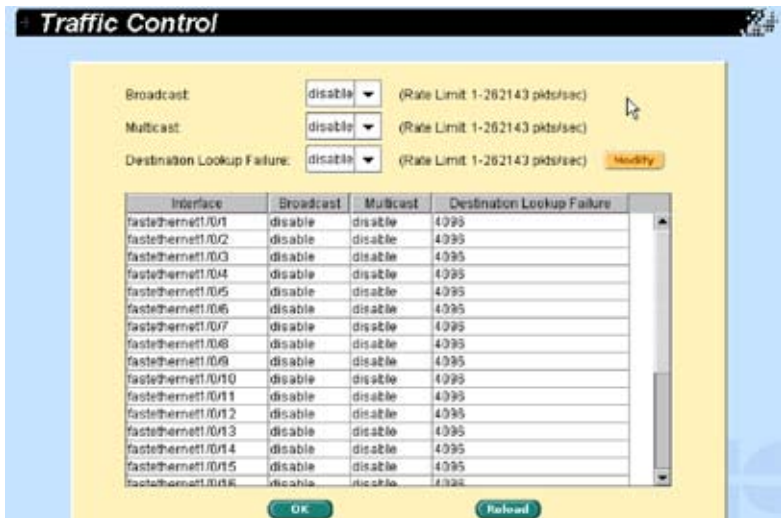
流量控制 (Traffic control) 可防止湧入過多的泛洪 (flooding) 封包，如廣播封包、多重播送封包與目的地地址搜尋失敗的單一播送封包等，避免系統頻寬異常負荷。本頁面中所輸入的限制數字為所有已開啟類型之封包的數目總和。例如，若開啟了廣播與多重播送，則這兩種封包的總和不能超過已設定的限制數值。

選擇一個介面並進行需要的設定，然後點選 **Modify**。

點選 **OK** 來儲存新設定。要使設定生效，請至 **Save Configuration** 頁面，然後點選 **Reload**。



GigaX2024B 流量控制



GigaX2024M 流量控制

圖 28. 流量控制頁面

4.5.8 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老化 (age out)。使用者可以輸入一個 10~1,000,000 範圍內的值 (單位為秒)，即可設定位址的老化時間。點選 **OK** 可儲存新的老化時間值。要使設定生效，請至 “Save Configuration” 頁面，然後點選 **Reload**。

您可以藉由連接埠、VLAN ID 與 / 或 MAC 位址來搜尋 MAC 位址，然後點選 **Query**。位址視窗將顯示搜尋結果。

Dynamic Addresses

Query by

☐ Port

☐ VLAN ID (1-3000)

☐ MAC Address **Query**

Destination Address	VLAN ID	Destination Port
0002.4492.b01c	1	fastEthernet1/0/1
0031.124f.001	1	fastEthernet1/0/1
0013.d452.40a8	1	fastEthernet1/0/1
0011.d89c.49e9	1	fastEthernet1/0/1
000c.2917.52d9	1	fastEthernet1/0/1
0050.846c.7c6f	1	fastEthernet1/0/1
0010.2030.4002	1	fastEthernet1/0/1
0004.759a.a05e	1	fastEthernet1/0/1
00e0.4c39.3002	1	fastEthernet1/0/1

Age Setting

Aging Time: (10-1000000 seconds)

OK **Reload**

圖 29. 動態位址頁面

4.5.9 靜態位址 (Static addresses)

您可以將 MAC 位址添加到交換器的位址表中。通過這種方式添加的 MAC 位址將不會老化 (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 位址所歸屬的 VLAN ID

Port Selection: 選擇此 MAC 位址所歸屬的連接埠

當您依據上述資訊創建了一個新的靜態 MAC 位址時，請點選 **Add**。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**，即可移除這個位址。**Modify** 按鈕可更新既有的 MAC 位址。您也可以輸入 MAC 位址與 VLAN ID，然後按下 **Query** 來搜尋某個靜態位址。點選 **OK** 將設定傳送至交換器 (HTTP 伺服器)。點選 **Reload** 更新設定至當前值。要使設定生效，請至 **Save Configuration** 頁面，然後點選 **Save**。



圖 30. 靜態位址頁面

4.5.10 VLAN 設定 (VLAN configuration)

在這個頁面中，您可以設定並顯示最多 254 個 (2024M 為 3000 個) VLAN 群組。VLAN1 是預設的 VLAN，是由系統建立的，無法被移除。本功能可避免交換器的不正常運作。除了預設的 VLAN1 以外，您可以移除其他任何一組既有的 VLAN。

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

“U” type: 未標記的連接埠，從該連接埠傳送出去的封包會被移除 VLAN 標記 (tag)。

“T” type: 自本連接埠傳送的封包都會被標記。

“blank” type: 本連接埠並非 VLAN 群組的成員。

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壅塞狀況。要避免這類狀況，交換器只能允許某個未標記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 配置到另一個 VLAN，您需要首先將其從原有的 VLAN 中移除，或在原有 VLAN 中將其設為已標記狀態。

VLAN ID: 當建立一組新的 VLAN 時，這個欄位要求使用者輸入 VLAN ID。

Name: 本欄位要求使用者輸入 VIAN 的名稱。

DHCP-Snooping: 開啟 / 關閉 VLAN 的 DHCP 偵聽功能。

點選 **OK** 儲存設定。要使設定生效，請至 **Save Configuration** 頁面，然後點選 **Save**。

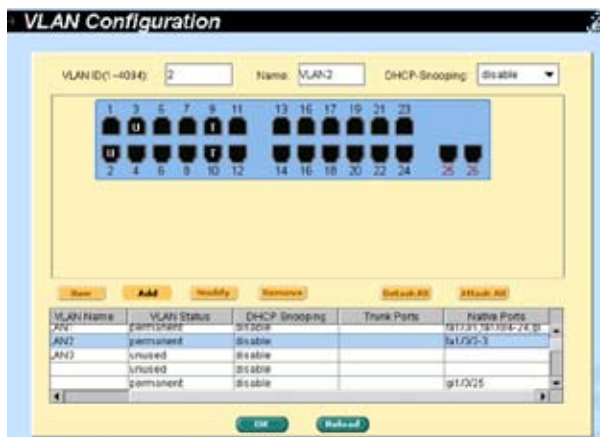


圖 31. 標記 VLAN 頁面



建立 60 組 VLAN (包括介面 fa1/0/1~fa8/0/26)，大約需要 3 分鐘。

建立 256 組 VLAN (包括介面 fa1/0/1~fa8/0/26)，大約需要 5 分鐘。

建立 1024 組 VLAN (包括介面 fa1/0/1~fa8/0/26)，大約需要 14 分鐘。

建立 2000 組 VLAN (包括介面 fa1/0/1~fa8/0/26)，大約需要 26 分鐘。

建立 3000 組 VLAN (包括介面 fa1/0/1~fa8/0/26)，需要超過 30 分鐘。

4.5.11 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 幹線埠下執行，主要用來在 VLAN 中去除那些不需要在幹線交換器之間傳遞的流量。以下是 GVRP 設定參數：

GVRP Enable: 在預設狀況下，交換器的 GVRP 沒有開啓。您必須首先在交換器上開啓 GVRP 功能，才能設定 802.1Q 連接埠進行 GVRP 操作。

Port Mode: 在單獨的 802.1Q 幹線埠上開啓 / 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 埠為正常 (Normal) 註冊模式。這些連接埠使用從鄰近的交換器上獲得的 GVRP 加入訊息修整在 802.1Q 幹線連接上運作的 VLAN。若裝置的另一端無法傳送 GVRP 訊息，或者您不想讓交換器修整任何 VLAN，請使用固定 (Fixed) 模式。Fixed 模式連接埠將轉發所有存在於交換器資料庫中的 VLAN。而禁止 (Forbidden) 模式下的連接埠只轉發 VLAN 1。



圖 32. GVRP 頁面

如果需要，您可以編輯以下屬性：

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。

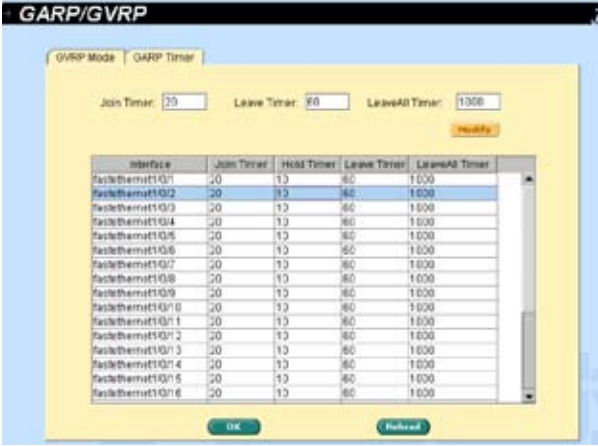


圖 33. GARP timer 頁面

4.5.12 QoS 與 CoS

4.5.12.1 802.1p 優先權

本交換器的每個連接埠支援四個 (GigaX2024B) / 八個 (GigaX2024M) 傳出行列。這些行列可以設定為先到先服務 (First Come First Service)，最高優先權排序 (High Priority First) 或權重循環排序 (Weight Round Robin, WRR)。絕對優先行列 (strict priority queue) 在其他行列得到服務之前必須為空。您可以使用絕對優先行列來傳送那些關鍵的或是有很強時效性的流量。以下有三個選項：

First Come First Service: 第一個來到的訊框具有最高的優先權。

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

Weighted Round Robin (WRR): 若啓用了 WRR 演算法，權重比率即為每個行列中 WRR 演算法的封包被傳送頻率的比率。

點選 OK 儲存設定。要使設定生效，請至 Save Configuration 頁面，然後點選 Save。

QoS/CoS

802.1p Priority CoS Queue Mapping **QoS Bandwidth**

☐ First Come First Service
☐ High Priority First
☒ Weighted Round Robin

Queue ID	Weight Value<1-10>
1	<input type="text" value="1"/>
2	<input type="text" value="2"/>
3	<input type="text" value="3"/>
4	<input type="text" value="4"/>

OK Reload

GigX2024B QoS/CoS

QoS/CoS

802.1p Priority CoS Queue Mapping **QoS Bandwidth**

☐ First Come First Service
☒ High Priority First
☐ Weighted Round Robin

Queue ID	Weight Value<1-10>	Queue ID	Weight Value<1-10>
1	<input type="text"/>	5	<input type="text"/>
2	<input type="text"/>	6	<input type="text"/>
3	<input type="text"/>	7	<input type="text"/>
4	<input type="text"/>	8	<input type="text"/>

OK Reload

GigaX2024M QoS/CoS

圖 34. QoS/CoS 頁面

4.5.12.2 CoS 佇列映射

GigaX2024B 每個連接埠支援四個傳出佇列 (GigaX2024M 支援八個傳出佇列)，這些佇列都可以採用絕對優先權排序。也就是說，每一個 CoS 數值都可以映射至這四 / 八個佇列之一。對於絕對優先權，佇列四 / 八具有最高的優先權來傳送封包。點選 **OK** 儲存設定。要使設定生效，請至“Save Configuration”頁面，然後點選 **Save**。

對於 GigaX2024B，CoS 數值範圍從 1 至 4，其中，1 代表最低優先權，4 代表最高優先權。對於 GigaX2024M，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。

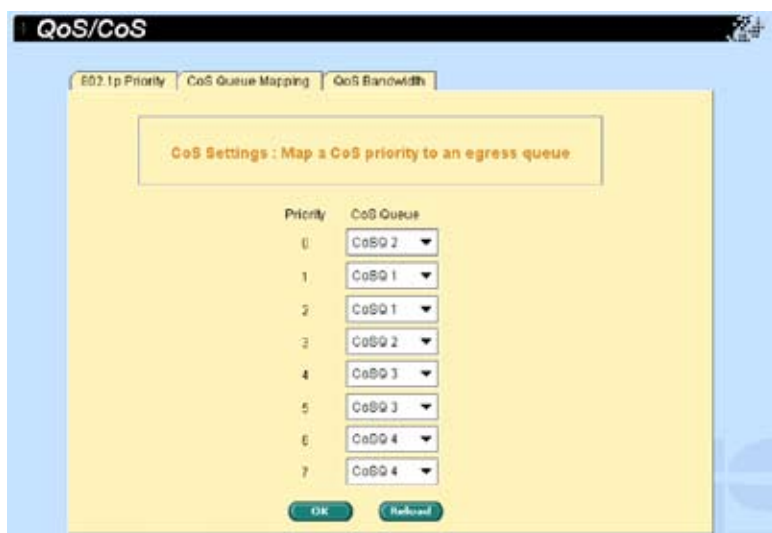


圖 35. CoS 佇列映射

4.5.12.3 QoS 頻寬 (QoS bandwidth)

本頁面為每個連接埠提供一些與 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。

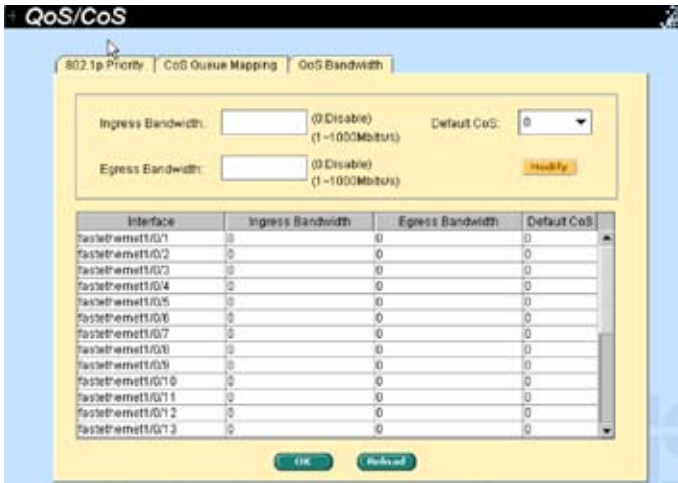
Egress Bandwidth: 選定連接埠的最大傳出頻寬 (僅 GigaX2024M 適用)

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

點選 **Modify** 更改連接埠列表視窗中的內容。點選 **OK** 儲存設定。要使設定生效，請至 **Save Configuration** 頁面，然後點選 **Save**。

Interface	Ingress Bandwidth	Egress Bandwidth	Default CoS
FastEthernet1/0/1	0	0	0
FastEthernet1/0/2	10	0	0
FastEthernet1/0/3	0	0	0
FastEthernet1/0/4	0	0	0
FastEthernet1/0/5	0	0	0
FastEthernet1/0/6	0	0	0
FastEthernet1/0/7	0	0	0
FastEthernet1/0/8	0	0	0
FastEthernet1/0/9	0	0	0
FastEthernet1/0/10	0	0	0
FastEthernet1/0/11	0	0	0
FastEthernet1/0/12	0	0	0
FastEthernet1/0/13	0	0	0

GigaX2024B QoS 頻寬



GX2024M QoS 頻寬

圖 36 QoS 頻寬頁面

4.6 簡易網路管理協定（SNMP）

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。

4.6.1 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 永久儲存設定，或點選 Reload 更新頁面。



Community Host Table

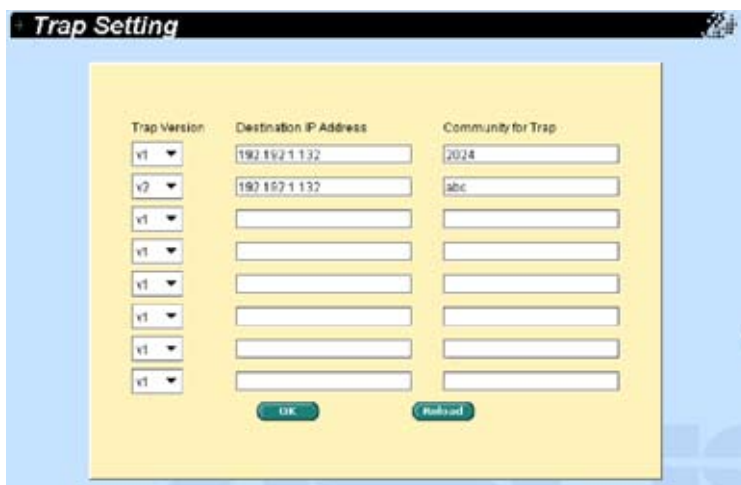
Host IP Address	Community	Type
0.0.0.0	public	ro
127.0.0.1	private	rw
		ro
		ro
		ro
		ro
		ro
		ro

OK Reload

圖 37. 群組主機列表頁面

4.6.2 Trap 設定 (Trap setting)

藉由設定 Trap 目的地 IP 位址與群組名稱，您可以開啓 SNMP Trap 功能來傳送不同版本的 Trap 封包 (v1 或 v2c)。點選 OK 永久儲存設定，或點選 Reload 更新頁面。



Trap Setting

Trap Version	Destination IP Address	Community for Trap
v1	192.162.1.132	2024
v2	192.162.1.132	abc
v1		
v1		
v1		
v1		
v1		
v1		

OK Reload

圖 38. Trap 設定頁面

4.6.3 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, 基於使用者的模型), 可提供 SNMPv3 封包的認證、加密與解密。二為 VACM (View-based Access Control Model, 基於檢視的存取控制模型), 可提供存取控制。以下為相關的三個頁面。點選 **OK** 永久儲存設定, 點選 **Reload** 更新頁面。

4.6.3.1 VACM 檢視 (VACM view)

VACM 檢視用來查看 SNMPv3 VACM 群組訊息。

View Name: 輸入安全群組名稱。

View Type: 輸入檢視所屬的檢視類型 (View Type)。當檢視子樹 (View Subtree) 與 SNMPv3 訊息中的 Oid 相符合時, 選擇包含 (Included) 或排除 (Excluded)。

View Subtree: 輸入檢視 (View) 所屬的檢視子樹 (View Subtree) 名稱。子樹 (Subtree) 是一個 Oid, 它與 SNMPv3 訊息中的 Oid 相符合。當子樹短於 SNMPv3 訊息中的 Oid 時, 為良好的符合狀態。

當您藉由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** 將其移除。點選 **Modify** 按鈕可更新既有 VACM 檢視項目。點選 **OK** 儲存設定。點選 **Reload** 更新設定到當前值。要使設定生效, 請至 **Save Configuration** 頁面, 然後點選 **Save**。



圖 39. SNMPv3 VGU 列表 1

4.6.3.2 VACM 群組 (VACM group)

VACM 群組用來設定 SNMPv3 VACM 群組。

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。相關的 SNMP 訊息有：Get, GetNext, GetBulk。

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 (Notify View Name)。相關的 SNMP 訊息為 Trap, Report。

Security Model: 輸入群組所屬的安全模型名稱 (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。

當您藉由上述資訊建立一個新的 VACM 群組後，請點選 **Add**。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** 將其移除。點選 **Modify** 按鈕可更新既有 VACM 群組項目。點選 **OK** 儲存設定。點選 **Reload** 更新設定到當前值。要使設定生效，請至 **Save Configuration** 頁面，然後點選 **Save**。



圖 40. SNMPv3 VGU 列表 2

4.6.3.3 USM 使用者 (USM User)

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

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

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。

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。

當您藉由上述資訊建立一組新的 VACM 群組項目後，點選 **Add**。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** 將其移除。點選 **Modify** 按鈕可更新既有 VACM 群組項目。點選 **OK** 儲存設定。點選 **Reload** 更新設定到當前值。要使設定生效，請至 **Save Configuration** 頁面，然後點選 **Save**。



圖 41. SNMPv3 VGU 列表 3

4.7 過濾功能頁面 (Filter pages)

本交換器可根據第二層至第四層封包的標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。

4.7.1 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。您也可以選擇 IP Filter Standard 並指定其 ID/ 名稱，然後點選 **Add** 來新增一組 IP 過濾規則。點選 **OK** 永久儲存設定，點選 **Reload** 更新頁面。在編輯前請點選 **OK** 按鈕。

點選您需要編輯或移除的過濾設定。然後點選 **Edit** 進入規則頁面。或點選 **Remove** 移除該過濾設定。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。

一個連接埠可以同時套用四種類型的規則。若超過了四種，系統會自動禁用這些規則。



圖 42. 過濾組合頁面

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。若您沒有在空白欄位輸入 MAC 位址，則代表此規則對所有的 IP 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執行。

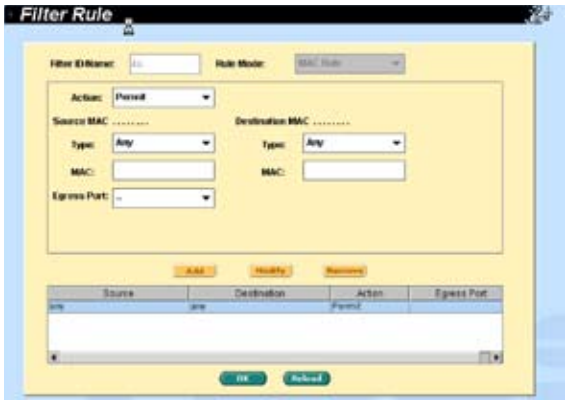


圖 43. MAC 模式下的過濾規則



圖 44. 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

4.7.2 附加過濾規則 (Filter attach)

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

點選 **OK** 儲存設定。要使設定生效，請至 **Save Configuration** 頁面，然後點選 **Save**，或者點選 **Reload** 更新頁面。

您可以用下列方法將過濾規則附加到連接埠：

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，您將無法移除指定的連接埠的過濾規則。若您需要移除規則，請使用 “Detach All” 指令。

當過濾規則套用到傳入連接埠，該規則會根據傳入連接埠和規則中的封包範圍來過濾封包。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。

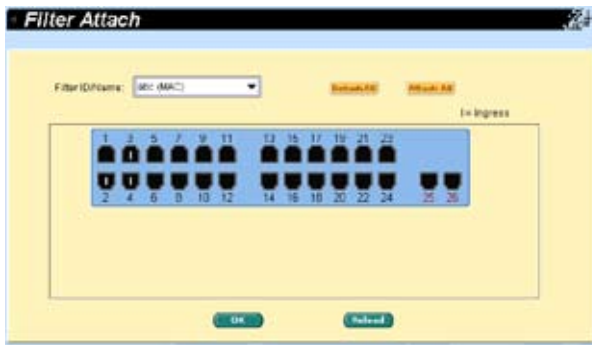


圖 45. 附加過濾規則

4.8 安全 (Security)

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

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

4.8.1 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: 選擇本項目開啓認證

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**：

Port: 從連接埠列表視窗中選擇需要設定的連接埠。

Host Mode (Single-host/Multi-host): 若開啓了本項目，連接到選定連接埠的所有主機中，只要有一部主機通過了認證，則所有主機都允許使用這個連接埠。若關閉本項目，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“ForceAuthorized”，選定的連接埠被認為已強制通過認證。因此，來自所有主機的流量都被允許通過。否則，若選擇了“ForceUnauthorized”，選定的連接埠是封鎖的，不允許任何流量通過。若選擇了“Auto”，選定連接埠的動作由 802.1x 協定來控制。在正常情況下，所有的連接埠都應該設定為“Auto”。

Reauthentication: 開啓本項目後，交換器會在重新認證時間 (ReAuthentication Time) 到時，試圖重新認證連接埠的使用者。

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

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

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

點選 **OK** 永久儲存設定。點選 **Reload** 更新設定至當前值。

Port Access Control

Bridge Setting

☐ System-Auth-Control Authentication Method: **Radius**

Port Setting

Port: Authentication Control: **auto**

Host Mode: **single-host** Reauthentication: **disable**

ReAuthentication Time: (1-65535) Sec Quiet Period: (1-65535) Sec

Guest Vlan: **disable** (1-3999) **Apply**

Interface	Status	Host Mode	AuthCtrl	ReAuth	ReAuth-Time	Quiet Period	GuestVlan
FastEthernet1/0/1	authorized	single-host	force-authorized	disable	3600	60	disable
FastEthernet1/0/2	authorized	single-host	force-authorized	disable	3600	60	disable
FastEthernet1/0/3	authorized	single-host	force-authorized	disable	3600	60	disable
FastEthernet1/0/4	authorized	single-host	force-authorized	disable	3600	60	disable
FastEthernet1/0/5	authorized	single-host	force-authorized	disable	3600	60	disable
FastEthernet1/0/6	authorized	single-host	force-authorized	disable	3600	60	disable
FastEthernet1/0/7	authorized	single-host	force-authorized	disable	3600	60	disable
FastEthernet1/0/8	authorized	single-host	force-authorized	disable	3600	60	disable
FastEthernet1/0/9	authorized	single-host	force-authorized	disable	3600	60	disable

OK **Cancel**

圖 46. 連接埠存取控制

4.8.2 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。

Password: 新使用者的密碼。

Confirm Password: 再次輸入密碼。

Vlan ID: 為 802.1x 認證的用戶端指定 VLAN ID。

請點選 **Add** 來新增使用者。當您完成修改後，點選 **Modify**。若您想要移除選定的使用者，請點選 **Remove**。點選 **OK** 永久儲存設定。點選 **Reload** 更新設定至當前值。



User Name	Password	Vlan ID
-----------	----------	---------

圖 47. 撥入使用者

4.8.3 RADIUS

若要使用外部 RADIUS 伺服器，您需要設定以下參數：

Authentication Primary-Server IP: RADIUS 伺服器的 IP 位址。

Authentication Primary-Server Port: RADIUS 伺服器偵聽的連接埠號碼。

Authentication Primary-Server Key: 用於在 GigaX 與 RADIUS 伺服器之間進行通訊的金鑰。

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介面位於同一個 VLAN 內。

點選 OK 永久儲存設定。點選 Reload 更新設定至當前值。

RADIUS	
Authentication Primary-Server IP:	192.192.1.132
Authentication Primary-Server Port:	1812
Authentication Primary-Server Key:	*****
Confirm Authentication Key:	*****
Authentication Secondary-Server IP:	192.192.1.131
Authentication Secondary-Server Port:	1812
Authentication Secondary-Server Key:	*****
Confirm Authentication Key:	*****
<input type="button" value="OK"/> <input type="button" value="Reload"/>	

圖 48. RADIUS

4.8.4 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接到他們的網路。您可以使用連接埠安全功能來限制和指定可存取該連接埠之站台的 MAC 位址，從而限制介面的輸入量。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。

4.8.4.1 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**：

- a) **Admin**: 開啟或關閉連接埠安全功能。
- b) **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，系統將記錄訊息，Violation 計數器的數值會增加。若選擇 “Restrict”，系統將會記錄訊息，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。
- c) **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 132，系統中的總數為 1024。
- d) **Aging Time**: 連接埠上安全 MAC 位址的老化時間。超過了這段時間後，相應的動態安全 MAC 位址就從安全 MAC 位址表中移除。有效的設定範圍是由 0 至 1440 (mins)。若設定的時間為 0，則該連接埠的老化時間機制沒有開啓。
- e) **Aging Type**: 老化類型決定了當安全 MAC 位址老化後的動作。若選擇 “Absolute”，連接埠的安全位址在老化時間到後會被移除。若選擇 “Inactivity”，若在指定的時間內沒有來自該安全 MAC 位址的流量，則該位址才會被移除。

點選 **OK** 永久儲存設定。點選 **Reload** 更新設定至當前值。

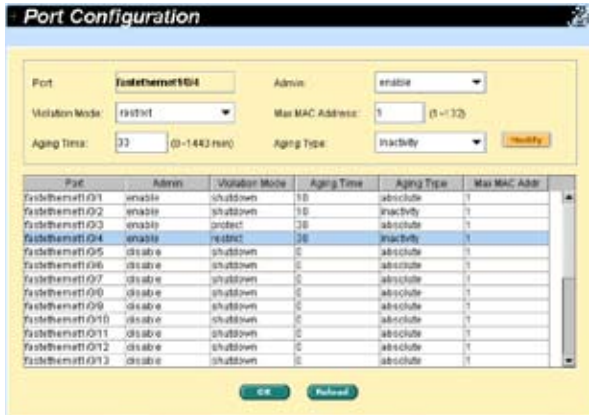


圖 49. 連接埠安全設定

4.8.4.2 連接埠狀態 (Port status)

本頁面顯示了當前的連接埠狀態，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：

- a) NoOper: 表示連接埠的安全功能沒有開啓。
- b) SecureUp: 表示連接埠安全功能運作中。
- c) SecureDown: 表示連接埠的安全功能無法運作。這種狀況一般為開啓了連接埠安全功能，但由於某些原因（如與其他功能衝突）而無法正常運作。
- d) Restrict: 表示在 Violation mode 設定為“restrict”時，連接埠出現了違反安全設定的狀況。
- e) Shutdown: 表示在 Violation mode 設定為“Shutdown”時，連接埠出現了違反安全設定的狀況。

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

點選 OK 永久儲存設定。點選 Reload 更新設定至當前值。

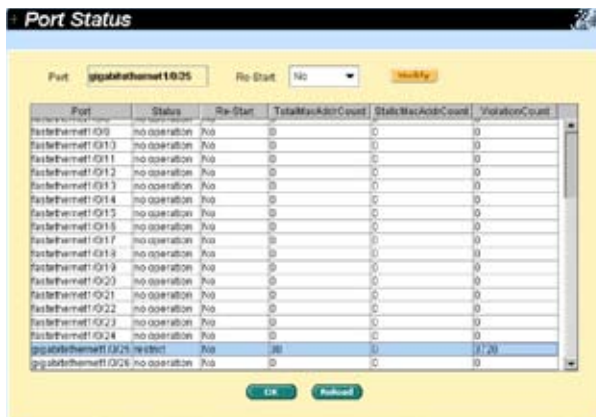


圖 50. 連接埠狀態

4.8.4.3 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** 按鈕後，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** 按鈕，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** 按鈕，即可立刻移除該位址。

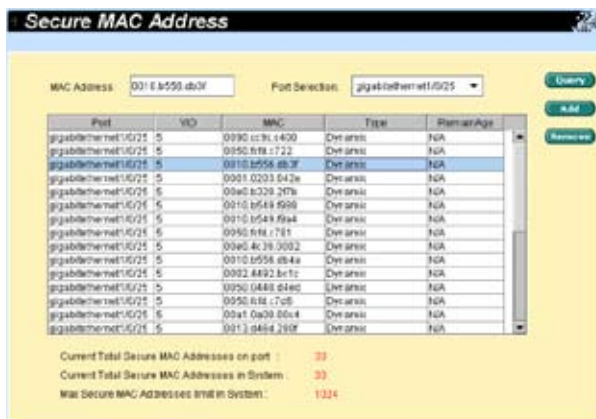


圖 51. 安全 MAC 位址

4.9 流量統計圖表 (Traffic chart)

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 使瀏覽器產生統計圖表。每次點選 Draw 都會重置統計結果的顯示。

4.9.1 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。

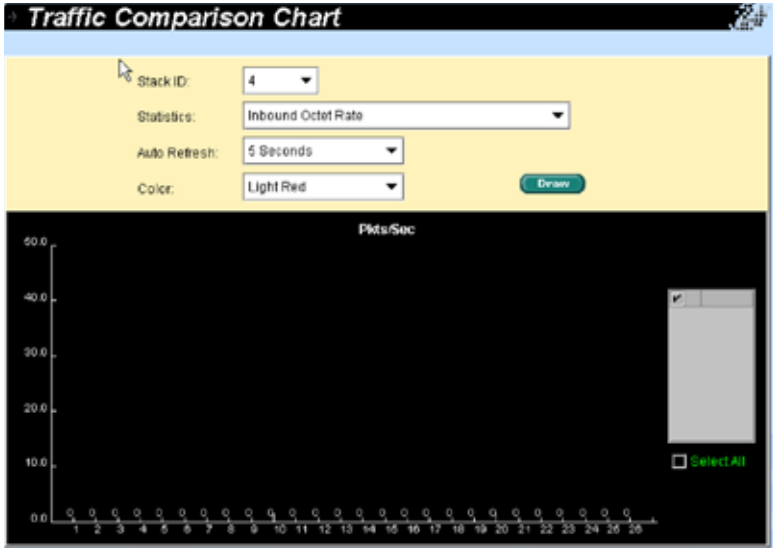


圖 52. 流量比較

4.9.2 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 53. 錯誤群組

4.9.3 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。

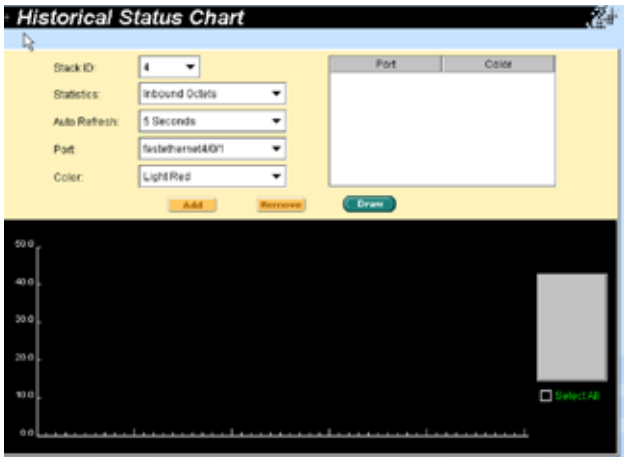


圖 54. 歷史狀態

4.10 纜線診斷 (Cable diagnosis)

本功能可以用來分析一般的纜線問題，如開路、短路和阻抗不匹配。

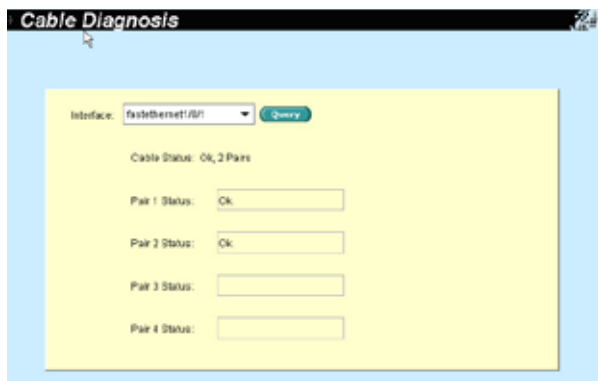


圖 55. 纜線診斷

4.11 管理交換器的堆疊

本章節僅適用於帶有 Stack 卡的 GigaX2024M 交換器。

交換器堆疊指的是一組（最多 8 部）GigaX2024M 交換器藉由它們的堆疊（Stacking）連接埠連接到一起。其中一部交換器控制這組堆疊交換器的運作，稱為主機（Master）。卡上的 LED 面板將顯示“A.x”，這裡的 x 代表堆疊（Stack）ID。堆疊中其他的交換器被稱為從機（Slave），卡上的 LED 面板將顯示“P.x”。堆疊的成員協同運作，組成一個統一的系統。

所有的堆疊成員都可以成為主機（Master）。若堆疊主機變為不可用，其他的堆疊成員會從它們中間選出一個新的堆疊主機。擁有最高優先權（1為最高優先權）的交換器將成為新的主機。若優先權相同，則具有較低橋接 ID 的交換器將成為主機。要建立一個堆疊系統，請先將它們連接起來並一起開啓電源。

點選 Reload 更新堆疊系統。

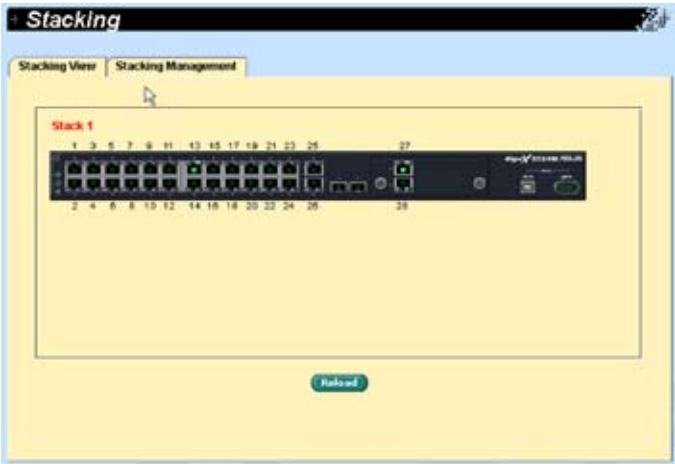


圖 60. 堆疊管理

您可以透過堆疊管理（Stacking Management）頁面設定堆疊（Stack）ID 與優先權。但您不可以在堆疊系統建立後再設定堆疊（Stack）ID 與優先權。您必須在建立系統前進行這些設定。



圖 61. 堆疊



1. 若您沒有指定交換器的堆疊 ID，那此交換器必須最後一個加入堆疊系統。
2. 當系統自動選擇主機失敗或無法執行，請重新啟動所有交換器。
3. 我們強烈建議您為交換器指定堆疊 ID。雖然系統將自動指定一個堆疊 ID 給交換器，但仍然會存在一些潛在的問題。
4. 當您移除然後又增加一個堆疊成員（非主機）時，若新加入的交換器與移除的那部具有相同的堆疊 ID，堆疊系統將自動按照舊的那部交換器的設定來設定新交換器。

4.12 儲存設定值 (Save configuration)

要永久儲存設定，您需要點選 **Save** 按鈕。在成功地儲存設定後，此設定即開始生效。

若您希望重置交換器的設定，可以點選 **Restore** 將設定回復至出廠預設值。當然，重置設定後，系統將會重新啟動。



回復出廠預設值後，您做的所有設定都將丟失。



圖 56. 儲存設定值

5 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 需要運行終端模擬軟體，如 HyperTerminal，以及指令翻譯器來對交換器進行設定。您必須將終端模擬軟體的鮑率設為 9600，8 個資料位元，無同位檢查，1 個停止位元，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幫助訊息。若您對於 CLI 指令不熟悉，這將是非常有用的訊息。所有的 CLI 指令都區分大小寫。

5.1 開機自我測試 (Power-on self test)

POST（開機自我測試）是在系統啟動時進行的。它測試系統記憶體、LED 指示燈號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。

```
ASUS login: admin
Password:
ASUS GigaX 2024B 3.2.02.00 Copyright (c) 2005

ASUS> enable
ASUS# _
```

圖 57. 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幫助訊息。



儘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。

```

R05-Boot 3.0.1; Built 0 Sep 8 2005 - 13:29:43

Welcome to GigaX 2024B Switch Product by R05 Computer, Inc.
Taipei, Taiwan

On board SDRAM: 32 MB ( P855 )
FLASH ROM: 16.5 MB ( P855 )

Firmware Slot 1 ..... Active
Base Address ..... 0x00100000
Status ..... P855
Description ..... GX2024B-R05-3.2.02.0b
Size ..... 561612 Bytes
Built ..... 2005/10/26 20:26:29
Checksum ..... 0x10956963

Firmware Slot 2 ..... Obsolete
Base Address ..... 0x00100000
Status ..... P855
Description ..... GX2024B-R05-3.2.02.0b
Size ..... 561612 Bytes
Built ..... 2005/10/26 17:54:45
Checksum ..... 0x10956963

Hit any Key to Enter Command Mode: 0
(R05B) _
    
```

圖 58. 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 with new setting：用指定的新設定代替當前設定。

指令	參數	參數舉例	說明
baudrate	Baud rate	9600, 38400, 57600, 115200	您需要將終端模擬軟體設為相同的鮑率。
ethaddr	none	none	取得 MAC 位址
gatewayip	IP address	xxx.xxx.xxx.xxx	設定閘道器的 IP 位址
go	none	none	啟動韌體映像
? or help	none	none	顯示線上幫助
ipaddr	IP address	xxx.xxx.xxx.xxx	設定 TFTP 用戶端的 IP 位址
xload	none	none	載入二進位檔案 load binary file over serial line (X modem)
netmask	mask	xxx.xxx.xxx.xxx	設定網路遮罩
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	xxx.img	搭配 TFTP 經由網路載入韌體映像
version	none	none	顯示版本號

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幫助。

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# 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：user delete user-name

舉例：ASUS# 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 伺服器。

CLI 指令：copy startup-config tftp: URL

舉例：ASUS# copy startup-config tftp: 192.168.8.56/gx2024b.cfg

5.3.2.2 回復啟動設定檔 (Restore start-up configuration file)

從 TFTP 伺服器上回復交換器的啟動設定檔 “ startup_config”。

CLI 指令：copy tftp: URL startup-config

舉例：ASUS# copy tftp: 192.168.1.2/gx2024b.cfg startup-config

5.3.3 系統管理設定 (System management configuration)

5.3.3.1 韌體升級 (Firmware upgrade)

升級新的韌體至交換器。

CLI 指令：archive download-sw/overwrite tftp: ImageFile

舉例：ASUS# archive download-sw/overwrite tftp: 192.168.1.3/GX2024B-3.2.02.00-release.img

5.3.3.2 設定終端機 (configure terminal)

進入設定模式來設定終端機。

CLI 指令：configure terminal

舉例：ASUS# configure terminal

5.3.3.3 啟用 (enable)

進入啟用 (enable) 模式並開啓特權模式指令。

CLI 指令：enable

舉例：ASUS# enable

5.3.3.4 禁用 (disable)

關閉特權模式並返回使用者模式。

CLI 指令：disable

舉例：ASUS# disable

5.3.3.5 結束 (end)

本指令可讓使用者結束當前模式並進入啓用 (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一個模式。

CLI 指令： exit

舉例： ASUS# exit

5.3.3.7 列出 (list)

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 WORD

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 DWORD

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。

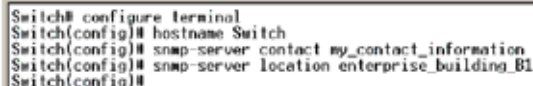
5.3.3.10 系統位置 (System Location)

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 DWORD

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 59. 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 伺服器等網路應用在 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)

顯示預設閘道器的 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：reboot

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

這個命令用預設檔來取代當前設定檔。

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)

在這疊或單一的交換器上用寫入檔案設定指令來將設定寫入到交換器設定檔案。

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 WORD WORD

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 WORD

舉例： 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 fa1/0/2

(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啓自動協商模式。

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介面的全雙工模式。

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 fa1/0/2

(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介面的流量控制。

5.3.4.4 顯示二層介面 (Show L2 interface)

使用交換器的顯示介面指令來顯示介面狀態。

CLI 指令： show interfaces IFNAME

舉例： ASUS# show interface fa1/0/2

5.3.5 IP 介面 (IP interface)

5.3.5.1 顯示 VLAN 名稱字串 (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 string

舉例： ASUS# show vlan name VLAN1



VLAN 1 是用於系統用途，例如，用於韌體升級，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 vlan3

5.3.5.3 VLAN 介面命令模式 (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介面的 IP 位址。

CLI 指令： ip address A.B.C.D/M

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



介面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內容。

5.3.5.5 DHCP 用戶端模式 (ip dhcp client)

本指令用來設定系統介面通過 DHCP 伺服器取得 IP 位址。

CLI 指令： ip dhcp client

舉例： (config-if)#ip dhcp client

5.3.5.6 IP 路由 (ip route)

本指令用來在系統中設定 IP 路由。

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

舉例： (config)# ip route 192.168.20.0 255.255.255.0 192.168.20.1

5.3.6 生成樹 (Spanning Tree)

5.3.6.1 顯示生成樹摘要 (show spanning-tree summary)

顯示目前的生成樹。

GigaX2024B:

CLI 指令： aggregation-link group <1-6> IFLIST

舉例： ASUS(config)#aggregation-link group 1 fa1/0/1-3

GigaX2024M:

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

舉例： ASUS(config)#aggregation-link group 1 fa1/0/1-3

5.3.6.2 生成樹的啟用與禁用 (spanning-tree enable and disable)

啟用 / 禁用生成樹。

CLI 指令： spanning-tree (enable|disable)

舉例： ASUS# spanning-tree disable

5.3.7 連結匯聚 (Link aggregation)

5.3.7.1 幹線匯聚群組 (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 <1-6> IFLIST

舉例： ASUS(config)#aggregation-link group 1 fa1/0/1-3

5.3.7.2 幹線負載均衡 (trunk load balancing)

使用交換器的連結匯聚幹線群組指令，用基於來源位址或基於目的地位址的轉發方式來設定幹線負載均衡。

GigaX2024B:

CLI 指令： aggregation-link group <1-6> load-balance (src-mac |dst-mac |src-dst-mac |src-ip |dst-ip |src-dst-ip)

舉例： ASUS(config)#aggregation-link group 1 load-balance src-mac

GigaX2024M:

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(config)#aggregation-link group 1 load-balance src-mac

5.3.7.3 顯示連結匯聚幹線 (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 連結匯聚幹線 (lACP aggregation-link trunk)

本指令用來進行連結匯聚控制協定 (LACP) 新增 / 設定交換器上的幹線群組連接埠的操作。

GigaX2024B:

CLI 指令： lACP aggregation-link group <1-6> (add|set) IFLIST

舉例： ASUS(config)# lACP aggregation-link group1 add fa1/0/1-3

GigaX2024M:

CLI 指令： lACP aggregation-link group <1-8> (add|set) IFLIST

舉例： ASUS(config)# lACP aggregation-link group1 add fa1/0/1-3

5.3.8.2 禁用 LACP 連結匯聚幹線 (disable lacp aggregation-link trunk)

本指令用來進行連結匯聚控制協定 (LACP) 新增 / 設定或禁用交換器上的幹線群組連接埠的操作。

GigaX2024B:

CLI 指令：no lacp aggregation-link group <1-6>

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

GigaX2024M:

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 系統優先權 (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 鏡像設定 (Mirror setting)

使用 "Mirror Session" 指令，您可以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 source IFLIST (both/ rx/ tx)
mirror session 1 destination IFNAME

舉例：(config)# mirror session 1 source fa1/0/1-4 both
(config)# mirror session 1 destination fa1/0/5

5.3.9.2 顯示鏡像 (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 無鏡像 (no mirror)

本指令用來關閉鏡像功能。

CLI 指令：no mirror session 1
舉例：(config)# no mirror session 1

5.3.9.4 無鏡像 (no mirror)

本指令用來重置來源介面接收或傳送的流量或兩者至目的介面。

CLI 指令：no mirror session 1 source IFLIST
舉例：(config)# no mirror session 1 source fa1/0/1-2

5.3.10 靜態多重播送 (Static Multicast)

5.3.10.1 MAC 位址表多重播送 (mac-address-table multicast)

使用交換器的 MAC 位址表多重播送 (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
fa1/0/1-3

5.3.10.2 無 MAC 位址表多重播送 (no mac-address-table multicast)

使用無 MAC 位址表多重播送 (no mac-address-table multicast) 設定指令來移除 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 fa1/0/1-3

5.3.10.3 顯示 MAC 位址表多重播送 (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 的第二層多重播送項目。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 偵聽 (ip igmp snooping)

本指令用來完整開啓 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 流量控制 (Traffic control)

5.3.12.1 風暴控制 (storm-control)

在使用交換器的風暴控制 (storm-control) 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。GX2024B 風暴控制功能位於 Configure Terminal 模式。它是一個全局的功能，應用於整部交換器。GX2024M 的風暴控制功能位於 Interface 模式。其功能設定是針對每個連接埠的。以下是 GigaX2024B 的指令舉例：

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

舉例：(config)# storm-control broadcast 25

5.3.12.2 無風暴控制 (no storm-control)

使用交換器的無風暴控制 (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-if)# no storm-control broadcast

5.3.12.3 顯示風暴控制 (show storm-control)

使用交換器的顯示風暴控制 (show storm-control) 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

5.3.13 動態位址 (Dynamic addresses)

5.3.13.1 清除動態 MAC 位址 (clear dynamic mac-address)

使用交換器的以下指令在資料庫中清除動態二層 MAC 位址。

CLI 指令：clear mac-address-table dynamic mac MAC_ADDR

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

5.3.13.2 老化時間 (aging time)

在一組堆疊或單獨的交換器上使用 MAC 位址表老化時間 (mac-address-table aging-time) 設定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。真正老化時間是您設定數字的三倍。

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 位址表的老化時間設定為 300 秒。

5.3.13.3 無老化時間 (no aging time)

關閉 MAC 位址表的老化功能。

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

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

5.3.13.4 顯示 MAC 位址表老化時間 (show mac-address-table aging-time)

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

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

5.3.14 靜態位址 (Static addresses)

5.3.14.1 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老化。我們稱之為靜態位址。

CLI 指令：mac-address-table static MAC_ADDR VLANID IFNAME

舉例：(config)# mac-address-table static 0000.1111.2222 1 fa1/0/2

5.3.14.2 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

5.3.15 VLAN

5.3.15.1 顯示 VLAN 名稱字串 (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 string

舉例：ASUS# show vlan name VLAN1

5.3.15.2 建立 VLAN (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

5.3.15.3 名稱字串 (name string)

使用名稱字串 (name string) 指令在交換器上建立帶名稱的 VLAN 項目。

CLI 指令： name string

舉例： (config-vlan)# name VLAN2

5.3.15.4 存取 VLAN (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 fa1/0/2

(config-if)# switchport access vlan 1

5.3.15.5 許可的 VLAN (allowed VLANs)

使用交換器連接埠的幹線許可 VLAN (allowed vlan) 設定指令來新增或移除許可 VLAN，許可 VLAN 在幹線模式下可在此介面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 fa1/0/2

(config-if)# switchport trunk allowed vlan add 1-10

5.3.16 GVRP

5.3.16.1 清除 GVRP 統計資料 (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介面的所有 GVRP 統計資料。

CLI 指令： clear gvrp statistics [IFNAME]

舉例： ASUS# clear gvrp statistics fa1/0/2

5.3.16.2 GVRP 模式 (gvrp mode)

本指令可完整開啓或關閉交換器的 GVRP 功能。

CLI 指令： gvrp (enable|disable)

舉例： ASUS# gvrp enable

5.3.16.3 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 fa1/0/1

5.3.16.4 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 fa1/0/1

5.3.17 CoS/QoS

5.3.17.1 排列 CoS 映射 (queue cos-map)

使用交換器的排列 CoS 映射 (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

5.3.17.2 顯示排列 CoS 映射 (show queue cos-map)

本指令用來將 GVRP 設定回復為預設值。

CLI 指令：show cos cos-map

舉例：(config)# show cos cos-map

5.3.17.3 QoS 模式 (qos mode)

本指令用來設定 QoS 模式。

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

舉例：(config)# cos policy fifo

5.3.17.4 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

5.3.17.5 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 LIMIT_RATE BURST_RATE

舉例：(config)# interface fa1/0/2
(config-if)# qos ingress bandwidth 10

5.3.18 SNMP

5.3.18.1 顯示 RMON 統計資料 (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 fa1/0/1

5.3.18.2 顯示 SNMP 伺服器群組 (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

5.3.18.3 SNMP 伺服器主機 (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

5.3.19 過濾 (Filter)

5.3.19.1 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 存取列表中移除一個拒絕的條件。

CLI 指令：deny any host MACADDR [IFNAME]

舉例：(config-acl)# deny any host c2f3.220a.12f4 [fa1/0/2]

5.3.19.2 過濾組合 (filter set)

本指令用名稱定義了一個延伸的 MAC 存取列表，並進入存取列表設定模式。

CLI 指令： mac access-list extended WORD

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

5.3.19.3 過濾條件 (filter conditions)

本指令指定了一個或多個拒絕或允許條件來決定封包應被轉發或丟棄。

CLI 指令： (permit|deny) any any

舉例： (config-acl)# permit any any

5.3.19.4 附加過濾規則 (filter attach)

本指令用名稱定義了一個延伸的 MAC 存取列表，並進入存取列表設定模式。

CLI 指令： mac access-group WORD in

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

5.3.20 連接埠存取控制 (Port access control)

5.3.20.1 dot1x 訪客 VLAN (dot1x guest-vlan)

使用交換器的 dot1x guest-vlan 介面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 fa1/0/1
(config-if)# dot1x guest-vlan 3

5.3.20.2 dot1x 連接埠控制 (dot1x port-control)

使用交換器的 dot1x 連接埠控制 (dot1x port-control) 介面設定指令來開啓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 fa1/0/1
(config-if)# dot1x port-control force-authorized

5.3.21 撥入使用者 (Dial-in user)

5.3.21.1 dot1x 使用者名稱和密碼 (dot1x username password)

新增使用者至本地 RADIUS 資料庫。

CLI 指令：dot1x user WORD WORD VLAN-ID

舉例：(config)# dot1x user test 12345 3

5.3.21.2 顯示 dot1x 使用者 (show dot1x user)

顯示 dot1x 撥入使用者。

CLI 指令：show dot1x user

舉例：ASUS# show dot1x user

5.3.22 RADIUS

5.3.22.1 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

5.3.22.2 顯示 dot1x RADIUS (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

5.3.23 連接埠安全 (Port security)

5.3.23.1 顯示連接埠安全 (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 gi1/0/25
ASUS# show port-security address
ASUS# show port-security address gi1/0/25
```

5.3.23.2 清除連接埠安全設定 (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 gi1/0/25

5.3.23.3 交換埠的連接埠安全 (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 gi1/0/25
(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

5.3.23.4 交換埠的連接埠安全老化 (switchport port-security aging)

本指令用來進行連接埠安全的老化設定。

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

5.4 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 燈號 — 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 遠端主機。

show ip route: 顯示路由表中的項目。

6 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 8 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”。

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。

7 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

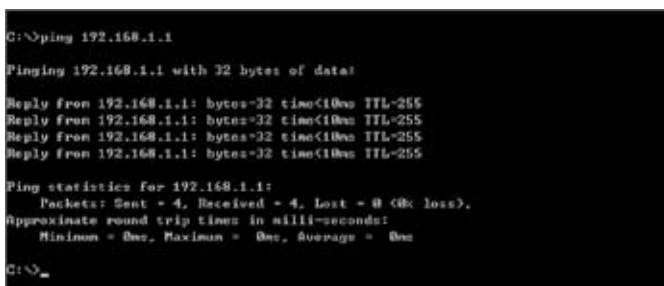
Ping 是用於檢測您的電腦是否能夠識別網路上其他電腦的指令。ping 指令向您指定的電腦送出一條訊息，如果該電腦收到這條訊息，它就會發送回應。要使用 ping 指令，您需要知道進行連絡的電腦的 IP 位址。

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

```
ping 192.168.1.1
```

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

如果目標電腦收到了這個訊息，就會出現如圖 62 所示的提示。



```
G:\>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

G:\>
```

圖 62. 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，這個指令將在下一節進行描述。

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

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

nslookup

點選「**確定**」。提示符後就會出現一個括弧提示符 (>)。在這個括弧提示符後鍵入網際網路位址，如 www.absnews.com。

視窗就會顯示相對應的 IP 位址，如圖 63 所示。

```
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 63. 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 更換損壞的風扇



在您卸下交換器背面的風扇模組前，請關閉交換器電源。

當交換器背面任何一個風扇出現故障時，您可以按照下列步驟進行替換。

1. 擰開將風扇固定在背部的螺絲。

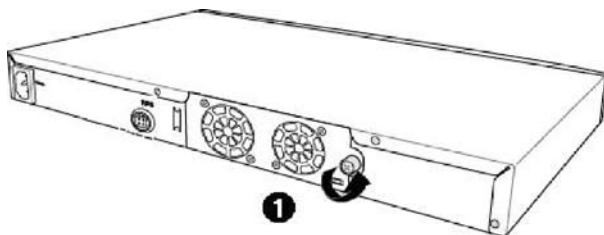


圖 64. 擰開螺絲

2. 如圖所示拉出風扇模組。

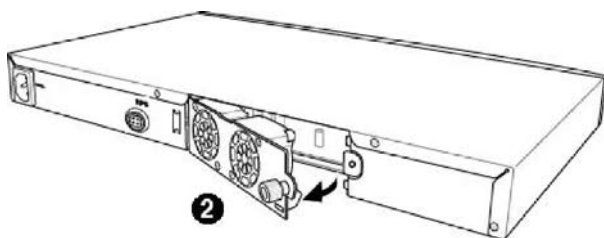


圖 65. 拉出風扇模組

3. 小心地將兩條電源線從風扇電源插座上移除。
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。

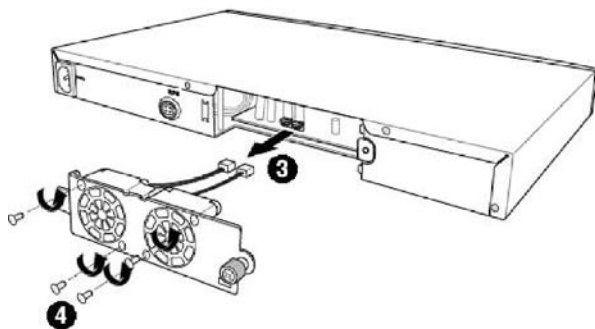


圖 66. 卸下損壞的風扇

5. 將新的風扇裝在原來風扇的位置，確保風扇電源線靠近模組底部。
按照同樣的步驟替換另一個風扇。
6. 將風扇電源線連接到電路板上，確認風扇電源線連接到正確的介面。當您面對交換器背部面板時，左邊的風扇是風扇 1
7. 將風扇模組置入交換器直至其卡入位置。確認風扇電源線沒有卡在風扇模組和機殼之間。
8. 用螺絲固定風扇模組。檢查風扇模組四周確認沒有電線卡在風扇模組和機殼之間。

風扇規格

尺寸：40 x 40 x 20 mm

電壓與電流：12VDC, 0.13A

轉速：8200RPM

7.3 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 燈號	
系統打開後，SYSTEM LED 不亮	確認電源線是否連接到交換器或電源插座。
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，參見 7.2 節的說明替換風扇。
當連接網路線時，乙太網 Link LED 不亮	1. 確認乙太網線是否正確地將交換器連接到您的區域網路交換器 / 集線器 / 電腦。確認電腦 / 集線器交換器已經打開。 2. 確認纜線長度是否符合您的網路的要求。1000 Mbps 網路 (1000BaseTx) 須使用標有 Cat 5 的纜線。10Mbit/sec 纜線可能支持較低品質的纜線。
網路存取	
電腦不能訪問同一網路中的另一個主機	1. 檢查乙太網路線是否完好，LED 燈號是否呈綠色。 2. 如果連接埠的 LED 燈號呈琥珀色，檢查該埠是否被禁用。 如果剛剛啓用 STP，可能會出現短時間的網路中斷。

問題	建議方案
電腦無法顯示網頁設定介面	<ol style="list-style-type: none"> 1. 交換器已打開並且連接埠也已經啟用。交換器的出廠預設 IP 為 192.168.1.1。 2. 在您的電腦上確認您的網路設定。如果您的電腦沒有設定一個有效的路由來連接到交換器，請將交換器 IP 改成您的電腦可以存取的 IP 位址。 3. 從電腦 Ping 您的交換器 IP，如果失敗，請重複第二步。 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。
網頁設定介面	
丟失 / 忘記網頁設定介面的使用者名稱或密碼	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 1. 確認您使用的是 Internet Explorer® v5.5 或以後版本的瀏覽器。不支持 Netscape。您的瀏覽器必須啟用 Javascript®，也必須支持 Java®。 2. Ping 交換器的 IP 位址檢查連接是否穩定。如果一些 ping 封包丟失，檢查您的網路設定，確認設定有效。
對設定的修改無法儲存	確認點選了 Save Configuration 頁面的 Save 按鈕。
控制終端介面	
不能顯示終端模擬器上的文字	<ol style="list-style-type: none"> 1. 出廠設置的速率為 9600，無流量控制，8 位元資料，無同位檢查，停止位為 1。 2. 將您的終端模擬器設定如上，如果您使用的是 USB 介面，請先安裝 USB 驅動程式。 3. 檢查連接線是否良好。

8 術語表

10BASE-T	用於乙太網路的有線線纜，資料傳輸率為 10Mbps。亦稱 3 類線 (CAT 3)。參見 data rate, Ethernet。
100BASE-T	用於乙太網路的有線線纜，資料傳輸率為 100Mbps。亦稱 5 類線 (CAT 5)。參見 data rate, Ethernet。
1000BASE-T	用於乙太網路的有線線纜，資料傳輸率為 1000Mbps。
binary	二進位。“基於 2”的數位系統，只使用 0 和 1 兩個數位來表示所有的數字。在二進位中，十進位數字 1 寫作 1，十進位數字 2 寫作 10，十進位數字 3 寫作 11，十進位數字 4 寫作 100，依次類推。雖然 IP 位址為方便起見表示為十進位數字，實際上它使用的是二進位數字。比如 IP 位址 209.191.4.240 轉換為二進位是 11010001.10111111.00000100.11110000。比特，IP 位址，網路遮罩同樣也是二進位。
bit	比特。“二進位數字”的縮寫，一個比特就是一個只有 0, 1 兩種數值的數位。參見 binary。
bps	比特每秒
CoS	服務級別。在 802.1Q 中規定，值的範圍為 0 到 7。
DSCP	差分服務代碼點 IP 報頭中差分服務部分最重要的六位被稱為 DSCP。GigaX 系列中可用的 DSCP 值有 0, 8, 10, 16, 18, 24, 26, 32, 34, 40, 46, 48 和 56。
broadcast	廣播。將資料發送到網路上所有的電腦。
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	<p>超文本傳輸協定</p> <p>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。</p>
ICMP	<p>網際網路控制訊息協定</p> <p>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。</p>
IGMP	<p>網際網路群組管理協定</p> <p>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。</p>
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	<p>網際網路協定位址</p> <p>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。</p>
ISP	<p>網路服務提供商</p> <p>向顧客提供網際網路存取服務的公司，通常是收費的。</p>
LAN	<p>區域網路</p> <p>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。</p>
LED	<p>發光二極體</p> <p>一種電子發光裝置。交換器前面的指示燈號就是 LED。</p>

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，提供網路線纜的物理介面 RJ-45 的介面卡。參見 Ethernet，RJ-45。
packet	封包，在網路上傳輸資料的單位。每個封包都包含資料、添加的資訊，如它從哪裡來（來源位址）及將到哪裡去（目的地位址）。
ping	封包探測 用於確認 IP 位址對應的主機是否能夠到達。它亦可用於尋找與功能變數名稱相對應的 IP 位址。
port	埠。實體的網路設備接入點，如電腦，路由器，資料透過該接入點流入流出。
protocol	協定。一系列用於控制資料傳輸的規則。為了使資料能夠成功傳輸，資料傳輸來源和目標都必須遵守相同協定的規則。
PVLAN	私有虛擬區域網路
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
	所有的分佈於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。