



# Sun Fire™ B1600 Blade 系統機箱交換器管理指南

---

Sun Microsystems, Inc.  
4150 Network Circle  
Santa Clara, CA 95054 U.S.A.  
650-960-1300

文件號碼：817-1896-10  
2003 年 4 月，修訂版 A

如果您對本文件有任何建議，請寄到：[docfeedback@sun.com](mailto:docfeedback@sun.com)

Copyright 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. 版權所有。

Sun Microsystems, Inc. 對於本文件提及產品所採用的技術擁有其相關智慧財產權。這些智慧財產權包括 <http://www.sun.com/patents> 所列之一項或多項美國專利，以及在美國與其他國家已經申請到或正在申請的一項或多項專利，但並不以此為限。

本文件以及其所屬的產品均按照限制其使用、複製、分發和反解譯的授權進行分發。未經 Sun 及其授權公司的書面授權，不得以任何方式、任何形式複製本產品或本文件的任何部分。

協力廠商軟體，包括字型技術，由 Sun 供應商提供許可和版權。

此產品或許有部份是從 Berkeley BSD 系統衍伸而來，此部份已向加州大學取得授權許可。UNIX 是在美國和其他國家的註冊商標，經 X/Open Company, Ltd. 獨家許可授權。

Sun、Sun Microsystems、Sun 標誌、AnswerBook2、docs.sun.com、Sun Fire 與 Solaris 為 Sun Microsystems, Inc. 在美國及其他國家之商標或註冊商標。

所有的 SPARC 商標都按授權許可使用，是 SPARC International, Inc. 在美國和其他國家的商標或註冊商標。具有 SPARC 商標的產品都是採用 Sun Microsystems, Inc. 開發的架構。

OPEN LOOK 和 Sun™ 圖形使用者介面是 Sun Microsystems, Inc. 為其用戶和授權許可持有人開發的。Sun 承認 Xerox 在為電腦行業研究和開發視覺或圖形使用者介面方面所做出的先行努力。Sun 以非獨占方式從 Xerox 獲得 Xerox 圖形使用者介面的授權許可，該授權許可涵蓋實施 OPEN LOOK GUI 且遵守 Sun 的書面許可協議的授權許可持有人。

本資料按「現有形式」提供，不承擔明確或隱含的條件、陳述和保證，包括對特定目的或非侵害性的商業活動和適用性的任何隱含保證，除非這種不承擔責任的聲明是不合法的。

---

Copyright (c) 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. 版權所有。此產品受一項或多項美國專利保護。許多專利仍在申請中。

本套件內可能含有其他廠商開發的物品。

Sun、Sun Microsystems、Sun 標誌、Java、Solaris、Sun Fire 以及 100% Pure Java 標誌都是 Sun Microsystems, Inc. 在美國與其他國家的商標或註冊商標。

所有 SPARC 商標都是授權使用的，而且是 SPARC International, Inc. 在美國及其他國家的商標或註冊商標。具有 SPARC 商標的產品都是採用 Sun Microsystems, Inc. 開發的架構。

本產品為美國出口物品控制法之管轄控制範圍，同時亦可能受其它國家之進出口法律條文管制。凡是與核能、飛彈、生化武器或核能航海相關的用途，無論直接或間接均嚴格禁止。本設備嚴格禁止出口或轉售至美國禁運國家或美國出口排外名單中所列地區，包括但不限於不歡迎人士與特別指定國家名單。

任何庫存或更換所需的 CPU，均只限用在符合美國出口法規的出口產品上，用來作 CPU 的修復或一對一替換的用途。除非得到美國政府授權，否則嚴禁將 CPU 用在產品升級上。



# 目錄

---

前言	xv
<b>1. 簡介</b>	<b>1-1</b>
1.1 簡介	1-1
1.1.1 交換器架構	1-2
1.1.2 連接交換器管理軟體的方式	1-2
1.2 硬體描述	1-3
1.2.1 乙太網路連接埠	1-3
1.2.1.1 上連連接埠	1-3
1.2.1.2 內部連接埠	1-3
1.2.2 狀態 LED	1-4
1.3 交換器特色	1-5
1.4 預設值	1-7
<b>2. 初始組態設定</b>	<b>2-1</b>
2.1 連上交換器介面	2-2
2.1.1 組態選項	2-2
2.1.1.1 透過內建的交換器介面設定交換器	2-3

- 2.2 啓用 SNMP 管理功能 2-4
  - 2.2.1 群體字串 2-4
  - 2.2.2 Trap 接收者 2-5
- 3. **管理概述** 3-1
  - 3.1 使用 Web 介面 3-2
    - 3.1.1 網路瀏覽器介面導覽 3-3
      - 3.1.1.1 首頁 3-3
      - 3.1.1.2 組態選項 3-4
    - 3.1.2 顯示面板 3-4
    - 3.1.3 主功能表 3-5
  - 3.2 基本組態 3-7
    - 3.2.1 顯示系統資訊 3-7
    - 3.2.2 設定 IP 位址 3-10
      - 3.2.2.1 手動設定 3-12
      - 3.2.2.2 使用 DHCP/BOOTP 3-14
    - 3.2.3 顯示交換器軟體版本 3-16
    - 3.2.4 管理韌體 3-18
      - 3.2.4.1 從伺服器下載系統軟體 3-18
    - 3.2.5 組態設定的儲存與復原 3-21
      - 3.2.5.1 從伺服器下載組態設定 3-21
    - 3.2.6 設定使用者認證機制 3-23
    - 3.2.7 設定 SNMP 3-27
      - 3.2.7.1 設定 SNMP 通訊協定的存取權限 3-28
      - 3.2.7.2 指定 Trap 管理員與 Trap 類別 3-29

- 3.3 設定全區網路通訊協定 3-32
  - 3.3.1 VLAN 組態 3-32
    - 3.3.1.1 顯示基本 VLAN 資訊 3-35
    - 3.3.1.2 GVRP 的啓用與停用 (全區設定) 3-37
    - 3.3.1.3 設定 VLAN 3-38
    - 3.3.1.4 在 VLAN 內加入固定成員 3-40
  - 3.3.2 群組廣播組態 3-43
    - 3.3.2.1 設定 IGMP Snooping 參數 3-44
    - 3.3.2.2 設定與群組廣播路由器連接的介面 3-47
    - 3.3.2.3 設定群組廣播服務 3-50
  - 3.3.3 廣播風暴控制 (全區設定) 3-53
  - 3.3.4 設定 Spanning Tree 演算法 3-55
    - 3.3.4.1 設定基本 STA 組態 3-55
    - 3.3.4.2 設定進階 STA 組態 3-61
  - 3.3.5 服務類別組態 3-63
    - 3.3.5.1 設定介面預設優先等級 3-63
    - 3.3.5.2 將 CoS 設定值對應到輸出佇列 3-65
    - 3.3.5.3 設定流量類別的服務權重 3-68
    - 3.3.5.4 將第 3/4 層的優先等級對應到 CoS 設定值 3-69
    - 3.3.5.5 對應 IP 優先權 3-71
    - 3.3.5.6 對應 DSCP 優先等級 3-73
  - 3.3.6 位址表設定 3-75
    - 3.3.6.1 顯示位址表 3-75
    - 3.3.6.2 更改保留期限 3-77
- 3.4 連接埠組態 3-78
  - 3.4.1 顯示連線狀態 3-78
  - 3.4.2 設定介面連線 3-82

- 3.4.3 連接埠寬道組態設定 3-86
  - 3.4.3.1 使用 LACP 動態設定寬道 3-87
  - 3.4.3.2 設定固定寬道 3-89
- 3.4.4 設定介面的 VLAN 行爲 3-91
- 3.4.5 設定靜態位址 3-97
- 3.4.6 管理 Spanning Tree 演算法介面 3-100
  - 3.4.6.1 顯示 STA 目前的介面設定 3-100
  - 3.4.6.2 設定介面的 STA 組態 3-104
  - 3.4.6.3 檢查介面的 STA 通訊協定狀態 3-107
- 3.4.7 阻擋流量進入管理連接埠 3-108
- 3.5 監視通訊埠與管理流量 3-112
  - 3.5.1 設定通訊埠鏡射 3-112
  - 3.5.2 顯示通訊埠統計數據 3-113
  - 3.5.3 顯示 SNMP 統計數據 3-122
  - 3.5.4 設定訊息日誌 3-125

## 4. 指令行參考資料 4-1

- 4.1 使用指令行介面 4-1
  - 4.1.1 連上 CLI 4-1
    - 4.1.1.1 主控台連線 4-1
    - 4.1.1.2 Telnet 連線 4-2
  - 4.1.2 輸入指令 4-3
    - 4.1.2.1 關鍵字與引數 4-3
    - 4.1.2.2 最短縮寫 4-4
    - 4.1.2.3 指令補齊 4-4
    - 4.1.2.4 取得指令的說明 4-4
    - 4.1.2.5 顯示指令 4-5
    - 4.1.2.6 不完整關鍵字查詢 4-6
    - 4.1.2.7 反轉指令的效果 4-6

- 4.1.2.8 使用指令歷程 4-6
- 4.1.2.9 了解指令模式 4-6
- 4.1.2.10 Exec 指令 4-7
- 4.1.2.11 組態設定指令 4-8
- 4.1.2.12 指令行的處理方式 4-9
- 4.2 指令群組 4-10
- 4.3 指令詳細說明 4-11
  - 4.3.1 一般指令 4-11
    - 4.3.1.1 enable 4-12
    - 4.3.1.2 disable 4-13
    - 4.3.1.3 configure 4-13
    - 4.3.1.4 show history 4-14
    - 4.3.1.5 reload 4-15
    - 4.3.1.6 end 4-15
    - 4.3.1.7 exit 4-16
    - 4.3.1.8 quit 4-16
  - 4.3.2 Flash/檔案指令 4-17
    - 4.3.2.1 copy 4-17
    - 4.3.2.2 delete 4-20
    - 4.3.2.3 dir 4-21
    - 4.3.2.4 whichboot 4-22
    - 4.3.2.5 boot system 4-23
  - 4.3.3 系統管理指令 4-24
    - 4.3.3.1 hostname 4-24
    - 4.3.3.2 username 4-25
    - 4.3.3.3 enable password 4-27
    - 4.3.3.4 ip http port 4-28
    - 4.3.3.5 ip http server 4-28

- 4.3.3.6 jumbo-frame 4-29
- 4.3.3.7 logging on 4-30
- 4.3.3.8 logging history 4-31
- 4.3.3.9 clear logging 4-32
- 4.3.3.10 show logging 4-33
- 4.3.3.11 show startup-config 4-34
- 4.3.3.12 show running-config 4-36
- 4.3.3.13 show system 4-38
- 4.3.3.14 show users 4-39
- 4.3.3.15 show version 4-40
- 4.3.4 認證指令 4-41
  - 4.3.4.1 authentication login 4-42
  - 4.3.4.2 radius-server host 4-43
  - 4.3.4.3 radius-server port 4-43
  - 4.3.4.4 radius-server key 4-44
  - 4.3.4.5 radius-server retransmit 4-44
  - 4.3.4.6 radius-server timeout 4-45
  - 4.3.4.7 show radius-server 4-45
  - 4.3.4.8 tacacs-server host 4-46
  - 4.3.4.9 tacacs-server port 4-46
  - 4.3.4.10 tacacs-server key 4-47
  - 4.3.4.11 show tacacs-server 4-47
- 4.3.5 SNMP 指令 4-48
  - 4.3.5.1 snmp-server community 4-48
  - 4.3.5.2 snmp-server contact 4-49
  - 4.3.5.3 snmp-server location 4-50
  - 4.3.5.4 snmp-server host 4-50



- 4.3.5.5 snmp-server enable traps 4-51
- 4.3.5.6 show snmp 4-52
- 4.3.6 線路指令 4-54
  - 4.3.6.1 line 4-55
  - 4.3.6.2 login 4-56
  - 4.3.6.3 password 4-57
  - 4.3.6.4 exec-timeout 4-58
  - 4.3.6.5 password-thresh 4-59
  - 4.3.6.6 silent-time 4-60
  - 4.3.6.7 show line 4-61
- 4.3.7 IP 指令 4-62
  - 4.3.7.1 ip address 4-62
  - 4.3.7.2 ip dhcp restart 4-64
  - 4.3.7.3 ip dhcp client-identifier 4-65
  - 4.3.7.4 ip default-gateway 4-66
  - 4.3.7.5 show ip interface 4-67
  - 4.3.7.6 show ip redirects 4-67
  - 4.3.7.7 ping 4-68
  - 4.3.7.8 ip filter 4-69
  - 4.3.7.9 show ip filter 4-72
- 4.3.8 介面指令 4-73
  - 4.3.8.1 interface 4-74
  - 4.3.8.2 description 4-74
  - 4.3.8.3 speed-duplex 4-75
  - 4.3.8.4 negotiation 4-76
  - 4.3.8.5 capabilities 4-77
  - 4.3.8.6 flowcontrol 4-78
  - 4.3.8.7 shutdown 4-79

- 4.3.8.8 switchport broadcast packet-rate 4-80
- 4.3.8.9 clear counters 4-81
- 4.3.8.10 show interfaces status 4-81
- 4.3.8.11 show interfaces counters 4-82
- 4.3.8.12 show interfaces switchport 4-84
- 4.3.9 位址表指令 4-85
  - 4.3.9.1 mac-address-table static 4-86
  - 4.3.9.2 clear mac-address-table dynamic 4-87
  - 4.3.9.3 show mac-address-table 4-87
  - 4.3.9.4 mac-address-table aging-time 4-88
  - 4.3.9.5 show mac-address-table aging-time 4-89
- 4.3.10 連接埠安全功能指令 4-89
  - 4.3.10.1 port security 4-90
- 4.3.11 Spanning Tree 指令 4-91
  - 4.3.11.1 spanning-tree 4-92
  - 4.3.11.2 spanning-tree mode 4-93
  - 4.3.11.3 spanning-tree forward-time 4-94
  - 4.3.11.4 spanning-tree hello-time 4-95
  - 4.3.11.5 spanning-tree max-age 4-95
  - 4.3.11.6 spanning-tree priority 4-96
  - 4.3.11.7 spanning-tree pathcost method 4-97
  - 4.3.11.8 spanning-tree transmission-limit 4-97
  - 4.3.11.9 spanning-tree cost 4-98
  - 4.3.11.10 spanning-tree port-priority 4-99
  - 4.3.11.11 spanning-tree edge-port 4-100
  - 4.3.11.12 spanning-tree protocol-migration 4-101
  - 4.3.11.13 spanning-tree link-type 4-101
  - 4.3.11.14 show spanning-tree 4-102

- 4.3.12 VLAN 指令 4-104
  - 4.3.12.1 vlan database 4-105
  - 4.3.12.2 vlan 4-105
  - 4.3.12.3 interface vlan 4-106
  - 4.3.12.4 switchport mode 4-107
  - 4.3.12.5 switchport acceptable-frame-types 4-108
  - 4.3.12.6 switchport ingress-filtering 4-109
  - 4.3.12.7 switchport native vlan 4-110
  - 4.3.12.8 switchport allowed vlan 4-111
  - 4.3.12.9 switchport forbidden vlan 4-112
  - 4.3.12.10 show vlan 4-113
- 4.3.13 GVRP 與橋接擴充功能指令 4-114
  - 4.3.13.1 switchport gvrp 4-114
  - 4.3.13.2 show gvrp configuration 4-115
  - 4.3.13.3 garp timer 4-116
  - 4.3.13.4 show garp timer 4-117
  - 4.3.13.5 bridge-ext gvrp 4-118
  - 4.3.13.6 show bridge-ext 4-119
- 4.3.14 IGMP Snooping 指令 4-120
  - 4.3.14.1 ip igmp snooping 4-121
  - 4.3.14.2 ip igmp snooping vlan static 4-122
  - 4.3.14.3 ip igmp snooping version 4-122
  - 4.3.14.4 show ip igmp snooping 4-123
  - 4.3.14.5 show mac-address-table multicast 4-124
  - 4.3.14.6 ip igmp snooping querier 4-124
  - 4.3.14.7 ip igmp snooping query-count 4-125
  - 4.3.14.8 ip igmp snooping query-interval 4-126
  - 4.3.14.9 ip igmp snooping query-max-response-time 4-127

- 4.3.14.10 ip igmp snooping router-port-expire-time 4-128
- 4.3.14.11 ip igmp snooping vlan mrouter 4-129
- 4.3.14.12 show ip igmp snooping mrouter 4-130
- 4.3.15 優先等級指令 4-131
  - 4.3.15.1 switchport priority default 4-132
  - 4.3.15.2 queue bandwidth 4-133
  - 4.3.15.3 queue cos-map 4-134
  - 4.3.15.4 show queue bandwidth 4-135
  - 4.3.15.5 show queue cos-map 4-136
  - 4.3.15.6 map ip precedence (Global Configuration) 4-136
  - 4.3.15.7 map ip precedence (Interface Configuration) 4-137
  - 4.3.15.8 map ip dscp (Global Configuration) 4-138
  - 4.3.15.9 map ip dscp (Interface Configuration) 4-139
  - 4.3.15.10 show map ip precedence 4-140
  - 4.3.15.11 show map ip dscp 4-141
- 4.3.16 鏡射連接埠指令 4-142
  - 4.3.16.1 port monitor 4-142
  - 4.3.16.2 show port monitor 4-143
- 4.3.17 連接埠寬道指令 4-144
  - 4.3.17.1 channel-group 4-145
  - 4.3.17.2 lacp 4-146

<b>A. 管理資訊庫</b>	<b>A-1</b>
A.1 支援的 MIB	A-1
A.2 支援的 Trap	A-3
<b>B. 疑難排解</b>	<b>B-1</b>
B.1 診斷交換器指示燈	B-1
B.2 診斷連接埠線路	B-2
B.3 存取管理介面	B-2
B.4 使用系統日誌	B-3
B.4.1 日誌訊息	B-4
B.5 錯誤訊息	B-5
B.5.1 指令行錯誤偵測	B-5
B.5.2 系統錯誤	B-5
B.5.3 指令行錯誤	B-6
B.5.4 Web 介面錯誤	B-8
<b>C. 規格</b>	<b>C-1</b>
C.1 交換器架構	C-1
C.2 管理功能	C-2
C.3 實體	C-2
C.4 電力	C-3
C.5 週遭環境	C-3
C.6 標準	C-4
<b>辭彙表</b>	<b>辭彙表 -1</b>
<b>索引</b>	<b>索引 -1</b>



# 前言

---

本手冊《*Sun Fire™ B1600 Blade 系統機箱交換器管理指南*》說明系統機箱 SSC (Switch and System Controller, 交換器與系統控制器) 模組內的交換器，讓讀者深入了解並能熟悉使用。交換器有兩種介面：指令行介面與 Web 介面，本手冊將詳細解釋這兩種介面。

本手冊是為負責管理系統機箱的網路管理者所撰寫的，並假設讀者對於區域網路有實際操作經驗，且相當熟悉各種網路通訊協定。

---

## 閱讀本書之前

開始設定交換器組態之前：

依照《*Sun Fire™ B1600 Blade 系統機箱硬體安裝手冊*》與《*Sun Fire™ B1600 Blade 系統機箱軟體設定手冊*》中的操作程序將系統機箱安裝起來。

---

# 本書組織結構

第一章會先對整個交換器作個概略介紹，包括管理選項、硬體特性、軟體特性以及預設值等等。

第二章說明如何連上交換器主控台以及 Web 介面。

第三章敘述交換器的所有主要功能，示範如何透過 Web 介面與主控台介面對這些功能進行設定。並列出所有 MIB 變數供 SNMP 管理軟體使用。

第四章詳細列出主控台可使用的所有指令與相關參數。

附錄 A 列出此交換器提供的管理資訊庫 (Management Information Bases，簡稱 MIB) 與 trap。

附錄 B 提供基本的疑難排解資訊。包括各個系統與連接埠 LED 的意義、如何解決各種導致您無法連上管理介面的問題以及系統日誌的使用方式。

附錄 C 詳列交換器各項功能的規格。

詞彙解釋列出許多專業術語的定義。

索引列出本書討論各項主題在書中的頁數。



---

## 排版慣例

字體	含義	範例
AaBbCc123	指令與檔案的名稱；電腦輸出畫面	顯示系統檔案。 請用 <code>dir</code> 列出所有檔案。
<b>AaBbCc123</b>	您所鍵入的內容（與電腦的螢幕輸出對照時）	<b>&gt;enable</b> Password:
<i>AaBbCc123</i>	書名、新字或專有名詞，以及要強調的字。請用實際的名稱或數值取代指令行變數。	請閱讀《 <i>Sun Fire™ B1600 安裝維護指南</i> 》第六章中的說明。 它們稱為 <i>class</i> 選項。 您必須以管理員的身分來做這件事。 若要刪除檔案，請鍵入 <code>del filename</code> 。

---

## 相關文件

應用	書名	文件號碼
安裝	<i>Sun Fire™ B1600 Blade 系統機箱硬體安裝手冊</i>	817-1902
機箱軟體設定	<i>Sun Fire™ B1600 Blade 系統機箱軟體設定手冊</i>	817-1891
機箱管理	<i>Sun Fire™ B1600 Blade 系統機箱管理指南</i>	817-1901

---

## 線上存取 Sun 文件

以下網站提供種類繁多的 Sun 系統文件：

<http://www.sun.com/products-n-solutions/hardware/docs>

完整的 Solaris 文件集和其它主題則位於：

<http://docs.sun.com>

---

## 訂購 Sun 文件

Fatbrain.com 是一家 Internet 上的專業書店，備有來自 Sun Microsystems, Inc. 的各種產品文件。

要取得文件清單及其訂購方法，請到以下 Fatbrain.com 網站的 Sun 文件中心網址：

<http://www.fatbrain.com/documentation/sun>

---

## Sun 歡迎您提出寶貴意見

Sun 非常樂於提高文件品質，誠心歡迎您的建議與意見。您可以將意見用電子郵件傳送給 Sun，收件地址為：

[docfeedback@sun.com](mailto:docfeedback@sun.com)

請將文件的文件號碼 (817-1896-10) 寫在電子郵件的主旨行中。

## 第 I 部分 入門

---

本節將對 Sun Fire™ B1600 Blade 系統機箱作概略性的說明，並介紹網路交換器的一些基本概念，同時也會敘述存取管理介面所需的基本設定。

簡介

初始組態設定



# 簡介

---

Sun Fire™ B1600 Blade 系統機箱含有兩個 SSC (Switch and System Controller，交換器與系統控制器) 模組。每個 SSC 內都有一台高速的 Gigabit 乙太網路交換器，其中內部含有 16 個全雙工 Gigabit 連接埠，為機箱中的各個組件提供高速連線，另外還有 8 個對外的全雙工 Gigabit 連接埠，用以與外界網路連接。

---

## 1.1 簡介

此交換器提供 Gigabit 乙太網路連線給 Sun Fire™ B1600 Blade 系統機箱使用。萬一其中一台交換器故障，另一台交換器上的動作仍然照常進行，完全不受影響。機箱內所有組件 – 伺服器葉片、SSC 與 PSU 都接在同一個中板上，並透過這個中板相互連接。

16 台伺服器葉片每一台都透過一條 Gigabit 乙太網路線路連到交換器上的一個連接埠，這是伺服器葉片最主要的 I/O 通道。每個 SSC 內交換器除了有八個對外連接埠連到外界之外，內部都有 Gigabit 乙太網路結構將所有伺服器葉片連接起來。每個伺服器葉片也都透過一條簡單的序列線路連到每個 SSC 內的系統控制器 (System Controller，(SC))。SC 可讓您管理監控機箱的各個組件，亦可連上交換器的命令行介面，以及機箱內所安裝之每台伺服器葉片的主控台。

## 1.1.1 交換器架構

此交換器採用高速結構，可讓所有交換器同時傳輸許多封包，所需的傳輸時間非常短。此外，此交換器也採用「先儲存後轉送」技術，盡可能確保資料完整。在這種模式中，每個封包都必須完整接收到連接埠緩衝區內並檢查確認無任何問題後，才會轉送到目的地去，以防止有問題的封包在整個網路內四處流竄。

## 1.1.2 連接交換器管理軟體的方式

系統上有一個序列式 RJ-45 插槽的主控台連接埠，透過此連接埠可連上系統控制器進行管理。當系統機箱電源打開時，系統控制器的介面便會顯示出來。連上交換器命令行介面的方式，請參閱第 2-2 頁的「組態選項」或《*Sun Fire B1600 Blade 系統機箱軟體設定手冊*》。

用 telnet 透過 SSC 上的 100BASE-TX RJ-45 管理連接埠 (NETMGT)，亦可直接連上這個命令行介面。

用網路瀏覽器或 SNMP/RMON 軟體透過網路連上這個連接埠，亦可對交換器進行管理。

透過網路瀏覽器連接時，交換器會提供圖形使用者介面讓您透過 HTTP 進行管理。

SNMP 提供的資訊，可透過適當設定且能使用 SNMP 的管理軟體加以顯示。

---

## 1.2 硬體描述

交換器與系統控制器 (Switch and System Controller, SSC) 內含有交換器電路板、系統控制器 (SC)、冷卻風扇、中板與背板接頭。SC 除了可讓您連上伺服器葉片與交換器電路板進行管理之外，還負責驅動兩套一模一樣的系統指示燈，分別位於 Sun Fire™ B1600 Blade 系統機箱的前後兩面。

### 1.2.1 乙太網路連接埠

#### 1.2.1.1 上連連接埠

八個外部 RJ-45 連接埠均支援 IEEE 802.3x 速度、全雙工模式與流量控制的自動協商。每個連接埠均能以 10 Mbps、100 Mbps 與 1000 Mbps 以及全雙工和半雙工的模式運作，並能控制資料流量避免塞爆緩衝區。上連連接埠可連接其它符合 IEEE 802.3ab 1000BASE-T 的裝置，若使用 Category 5 雙絞線，則線路最長可達 100 公尺 (32.8 呎)。這些連接埠也都有自動 MDI/MDI-X 功能，因此任何未彎曲的線都可以拿來使用。上連連接埠在組態介面中的名稱分別為 NETP0 - NETP7。

---

**注意：**請注意，使用自動協商功能時，若連上此交換埠的裝置也支援同樣的功能，雙方便可自動設定適當的速度、傳輸模式與流量控制；否則就必須手動調整這些設定。

---

---

**注意：**必須啓動自動協商功能，自動 MDI/MDI-X pin-out 組態才會有效。

---

#### 1.2.1.2 內部連接埠

此交換器共有 16 個內部 1000BASE-X Gigabit 乙太網路連接埠，連接到機箱內的伺服器葉片。這些連接埠都是固定在 1000 Mbps 全雙工模式，在組態設定介面中的名稱分別為 SNP0 - SNP15。

此交換器也含有一個內部 10/100BASE-TX 的連接埠，稱為 NETMGT，透過內部集線器連上 SC 的網路埠以及 SSC 前面板上的外部管理連接埠。

## 1.2.2 狀態 LED

交換器層級指示燈位於 SSC 模組上。SSC 背板上的 1000BASE-T 上連連接埠與 10/100BASE-TX 管理連接埠，也含有連線與否以及速度的指示燈。

■ 1-1 SSC 外部面板

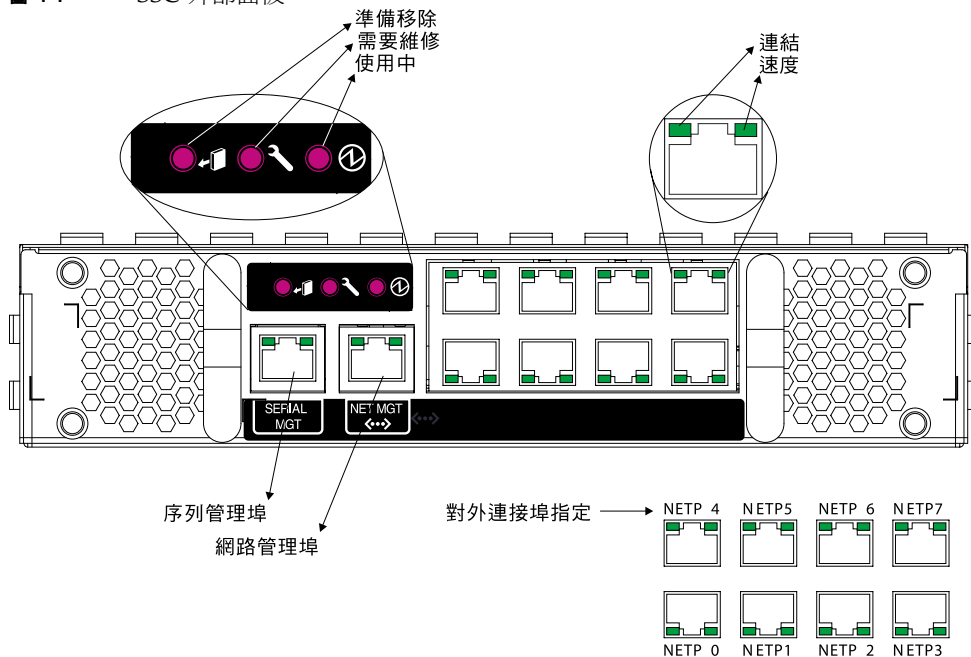


表 1-1 連接埠 LED

LED 指示燈	狀況	狀態
SSC		
使用中	亮起 (綠色)	SSC 正常運作。
需要維修	亮起 (琥珀色)	SSC 需要維修。
可以放心拆除	亮起 (藍色)	現在可以拆卸這台 SSC。
RJ-45 連接埠		
連線	亮起 (綠色)	此連接埠已與對方建立正常網路連線。
速度	亮起 (琥珀色)	線路以 1 Gbps 速度運作。
	熄滅	線路以低於 1 Gbps 的速度運作。



## 1.3 交換器特色

此交換器具有許多高等的效能提昇特性。例如群組廣播過濾功能支援即時網路通訊的軟體；可根據連接埠或標記分辨 VLAN 以及支援自動 GVRP VLAN 註冊的功能，除了提高資料傳輸安全，同時也能讓網路頻寬的使用更有效率；QoS 優先排序功能可將即時性的多媒體資料透過網路傳遞的延遲時間降到最低；流量控制功能可確保不會因為連接埠飽和而出現瓶頸，進而導致封包遺失的狀況發生；廣播風暴抑制功能可防止廣播流量風暴在網路上發生。以下簡短介紹其中部分管理功能。

**IEEE 802.1D 橋接** – 此交換器支援 IEEE 802.1D 通透性橋接功能，其位址表會自動學習位址，據以過濾或轉送流量，讓資料的交換更為順暢。此位址表最多可容納 8000 個位址。

**先儲存後轉送交換** – 此交換器會將完整的封包複製到其記憶體之後，才轉送到另一個連接埠上，不僅確保所有封包的大小均符合標準乙太網路的規範，而且也可以用 CRC (cyclic redundancy check, 週期循環檢查) 檢查封包的內容正確與否，另外還可以防止不良封包進入網路內浪費頻寬。

為了避免連接埠過於壅塞而開始丟棄封包，此交換器的每個連接埠都有 128KB 的封包緩衝空間，當網路出現壅塞狀況時，封包便可暫時存放在緩衝區內等待傳送。

**Spanning Tree 通訊協定** – 此交換器支援以下幾種 spanning tree 通訊協定：

**Spanning Tree Protocol (STP, IEEE 802.1D)** – 可讓兩個 LAN 網段之間建立兩條或多條連線，以提供多一層的故障容忍能力。當兩個網段之間有多條路徑相通時，此通訊協定會選擇其中一條，並將其所有路徑關閉，確保網路上任何兩個裝置之間只有一條路由，以免造成網路中出現迴圈的情形。萬一所選取的路徑故障時，此通訊協定會啟用另一條路徑，讓兩個網段之間仍然保持暢通。

**快速 Spanning Tree Protocol (RSTP, IEEE 802.1w)** – 此通訊協定能將網路拓模改變時的收斂速度大幅降低，約只需要舊版 IEEE 802.1D STP 標準的 10% 時間就夠了。這套通訊協定雖然是為了完全取代 STP 而設計的，但若偵測到所連接設備發出舊版的 STP 通訊協定訊息，便會自動將連接埠設定成符合 STP 的模式，因此還是可以與使用舊版 STP 的交換器共用。

**虛擬 LAN** – 此交換器最多可支援 256 個 VLAN。VLAN 由一群網路節點組成，無論這些節點在網路中的實際位置與連接點為何，均同屬一個碰撞領域。此交換器支援 IEEE 802.1Q 標準定義的標籤式 VLAN。此交換器會透過 GVRP 動態得知 VLAN 群組中的成員，亦可經由人工方式設定各 VLAN 所含節點，以後交換器便會將流量限制在使用者所屬的 VLAN 群組內。將網路切割成許多 VLAN 具有以下優點：

- 消除可能導致一般網路效能大幅下降的廣播風暴。
- 當任何節點有變動或移動位置時，不需要更改實際接線，只要從遠端設定各連接埠隸屬的 VLAN 即可，使網管工作簡化許多。
- 將流量限制在其出發的 VLAN 內，各 VLAN 之間若要進行連線，必須利用路由器或第三層交換器才能達成，讓資料得到更安全的保障。

**連接埠鏡射** – 此交換器可將任何一個連接埠上流量複製一份到監視連接埠，而且完全不會有任何影響。您只要將一台通訊協定分析器或 RMON 偵測器接到這個連接埠，就可以進行流量分析以及檢驗連線的完整性。

**連接埠集束** – 數個連接埠可以合併成一個聚合連線，稱為寬道 (trunk)。管理者可以手動設定寬道，也可以用 IEEE 802.3ad LACP (Link Aggregation Control Protocol，線路聚合控制通訊協定) 進行動態設定。額外增加的連接埠不僅能大幅提高連線的資料吞吐量，萬一寬道中的某個連接埠故障時，還可以立刻取代達到備援的效果。此交換器最多可設定六條寬道，每條寬道最多可含四個上連連接埠或最多兩個下連連接埠。

**連接埠安全** – 防止未經授權的使用者連上您的網路。此功能讓每個連接埠能夠學習或手動設定有權透過該連接埠連上此網路之裝置的 MAC 位址，以後該連接埠所接收到的封包，其來源位址若不在允許連線的範圍內，該封包便會被丟棄。所有連接埠預設都是將連接埠安全功能關閉，必要時可分別予以啟動。

**廣播抑制** – 廣播抑制功能可防止網路上出現大量廣播流量。當您在某個連接埠上啟動這項功能後，交換器便會限制通過此連接埠的廣播流量。當廣播流量攀升到預定的流量時，交換器便會將其阻絕，直到流量下降到預定流量以下。

**流量控制** – 流量控制功能可降低網路壅塞時的流量，以免封包因連接埠緩衝區滿載而被丟棄。此交換器支援 IEEE 802.3x 標準所規範的流量控制功能。所有連接埠的流量控制功能預設都是關閉的。

**流量優先等級** – 此交換器提供 QoS 功能，可根據所需服務等級，利用四個權重式循環 (Weighted Round Robin) 佇列設定每個封包的優先順序。此交換器利用 IEEE 802.1p 與 802.1Q 標籤以及終端節點的輸入資料設定流量的優先順序。管理者可以利用這些功能為需要較低延遲時間以及盡量遞送到目的地的不同資料設定不同的優先順序。

為了符合多項用途的需要，此交換器另外還支援好幾種常見用來設定第三/四層流量優先順序的方法。流量可以依據 IP 封包的 ToS (Type of Service，服務類別) 位元組中的優先順序位元劃分其等級。當這些服務啟動時，交換器便會將各優先順序對應到服務類別設定值，將流量分別送往對應的輸出佇列。

**位址過濾** – 此交換器具有封包過濾功能，可篩選進入 CPU 連接埠的所有流量，藉以控制哪些流量可以轉送到管理網路內。此封包過濾器採用規則/樣式運作，由兩組樣式組成，符合第一組內任何一個樣式的封包均會被丟棄，符合另一組內任何一個樣式的封包則可通過。

**群組廣播轉送** – 您可以將特定的群組廣播流量設定自己的 VLAN，以免與一般網路流量相互干擾，另外還可以設定該 VLAN 的優先等級，以保證即時性資料的傳輸。此交換器使用 IGMP Snooping 與 IGMP 管理群組廣播成員的註冊。

## 1.4 預設值

表 1-2 預設值

功能	預設值
系統設定	
Web 管理	啟用
安全 Web 管理	停用
BOOTP	啟用
DHCP	啟用
SNMP 群體	public：唯讀 private：可讀寫
SNMP Trap	認證 trap：啟用 線路中斷與連通事件：啟用
使用者名稱	admin (主控台、Telnet、Web) guest (主控台、Telnet、Web)
密碼	登入 - 使用者 admin 的密碼為 admin 使用者 guest 的密碼為 guest 從 Normal Exec 模式切換到 Privileged Exec 模式：super
序列埠	鮑率：9600，資料位元：8，停止位元：1，同位檢查：無
IP 設定	位址：0.0.0.0，子網路遮罩：255.0.0.0
連接埠狀態	
連接埠速度	連接埠 SNP0-15：1000 Mbps 連接埠 NETP0-7：10/100/1000 Mbps，自動協商 連接埠 NETMGT：10/100 Mbps，自動協商
雙工模式	連接埠 SNP0-15：全雙工 連接埠 NETP0-7、NETMGT：半雙工全雙工均可，自動協商
流量控制	停用
連接埠優先等級	進入優先等級：0
連接埠安全性	停用
Spanning Tree 通訊協定	啟用，預設使用 RSTP (預設值：所有參數均根據 IEEE 802.1w 設定)
邊緣連接埠 (快速轉送)	SNP0-15 預設啟用，NETP0-7 預設停用

**表 1-2**      預設值

<b>功能</b>	<b>預設值</b>
位址保留期間	300 秒
虛擬 LAN	
GVRP	停用
預設 VLAN	PVID 1 ( 未加註標籤的封包 )
管理 VLAN	VLAN 2 ( 管理連接埠 )
標籤	RX : 所有封包 , TX : 未加註標籤的封包
接收過濾	停用
群組廣播過濾	
IGMP Snooping	啓用
ARP	啓用
快取逾時	20 分鐘

## 初始組態設定

---

關於對交換器進行初始組態設定的詳細相關資訊，請參閱 《*Sun Fire B1600 Blade 系統機箱軟體設定手冊*》。

本章所含各小節如下：

- 第 2-2 頁的「連上交換器介面」
- 第 2-4 頁的「啓用 SNMP 管理功能」

---

## 2.1 連上交換器介面

### 2.1.1 組態選項

交換器模組提供指令行組態設定介面 (CLI) 進行管理用途。要連上此管理介面，首先先連上交換器上的 RJ-45 序列主控台連接埠，接著從系統控制器 (SC) 的指令提示登入交換器的 CLI 即可，如以下所示 (其中  $SSC_n$  可為  $SSC_0$  或  $SSC_1$ )。

```
sc>: console sscn/swt
Username: admin
Password:

      CLI session with the Sun Fire B1600 is opened.
      To end the CLI session, enter [Exit].

Console#
```

---

**注意：**若管理網路上已有架設 DHCP 伺服器，則您還可以用 telnet 或 web 連上交換器。為了確保交換器每次開機 (發出 DHCP 要求) 時都得到相同的位址，請將以下用戶端識別碼寫入 DHCP 伺服器的組態內：SUNW,SWITCH\_ID= 機箱序號, 0 (SSC0 中的交換器) 或 SUNW,SWITCH\_ID= 機箱序號, 1 (SSC1 中的交換器)。關於如何將網路準備好以便順利接收此型系統機箱，以及交換器初次設定組態時所有程序的相關資訊，請參閱 《Sun Fire B1600 Blade 系統機箱軟體設定手冊》。

---

### 2.1.1.1 透過內建的交換器介面設定交換器

主控台連線 – 在系統控制器指令提示符號後輸入 `console sscn/swt` 指令 (n 代表 SSC0 或 SSC1)，便可連上交換器的指令行介面 (CLI)。

Telnet 連線 – 用 `telnet` 可從遠端透過管理網路連上交換器的 CLI。

Web 介面 – 交換器內部亦含有一個 HTTP Web 軟體，管理網路中任何一台電腦均可使用標準網路瀏覽器連上此代理程式。

SNMP 軟體 – 交換器的管理軟體含有一個 SNMP (Simple Network Management Protocol，簡易網路管理通訊協定，支援版本 1 與 2c) 代理程式，管理網路中任何一個系統，只要透過 `SunNet Manager` 之類的管理軟體連上此 SNMP 代理程式，便可對交換器進行管理。

系統組態設定程式與 SNMP 代理程式支援以下管理功能：

- 啟用/停用任何連接埠
- 設定任何連接埠的速度/雙工模式
- 設定 SNMP 參數
- 將連接埠加入網路 VLAN 內
- 顯示系統資訊或統計資料
- 設定交換器加入 Spanning Tree
- 下載系統韌體

---

## 2.2 啓用 SNMP 管理功能

此交換器可設定成接受 SunNet Manager 之類簡易網路管理通訊協定 (SNMP v1 或 v2c) 軟體所發出的管理指令，並回應收到的 SNMP 要求以及產生 SNMP trap。

當 SNMP 管理主機發出要求給此交換器時 (可能是要求傳回某些資訊或設定某個參數)，此交換器便會提供對方所要求的資料或設定對方指定的參數。此交換器亦可設定成以 trap 訊息的格式將資訊發送給 SNMP 管理主機 (後者無須發出任何要求)，告知後者有特定事件發生。

### 2.2.1 群體字串

群體字串是用來控制哪些人有權連上 SNMP 設備進行管理，以及哪些 SNMP 管理主機有權接收 SSC 發出的 trap 訊息。因此您必須為特定使用者或群組設定群體字串，並設定其存取等級。

預設字串為：

- **public** – 唯讀權限，代表有權存取的管理主機只能讀取 MIB 物件。
- **private** – 讀寫權限，代表有權存取的管理主機可讀取與修改 MIB 物件。

---

**注意：**若您不打算使用 SNMP，建議您將這兩個預設的群體字串刪掉。只要沒有設定任何群體字串，交換器的 SNMP 管理功能便會關閉。

---

群體字串的設定步驟如下：

1. 在 Privileged Exec 層全區設定模式提示符號後，輸入 `snmp-server community string mode`，其中 `string` 為群體存取字串，而 `mode` 則可以是 **rw** (可讀寫) 或 **ro** (唯讀)。按下 <Enter>。
2. 要刪除原有的任何字串，只要輸入 `no snmp-server community string` 即可，其中 `string` 便是您要刪除的群體存取字串。按下 <Enter>。

```
Console(config)#snmp-server community sun rw
Console(config)#no snmp-server community private
Console(config)#
```



## 2.2.2 Trap 接收者

您也可以指定哪些 SNMP 會接收 SSC 發出的 trap。

trap 接收者的設定步驟如下：

1. 在全區設定模式提示符號後，輸入 `snmp-server host host-address community-string`，其中 `host-address` 為 trap 接收主機的 IP 位址，`community-string` 則是該主機的字串。

按下 <Enter>。

2. 至少要輸入一個 `snmp-server enable traps` 指令，SSC 才會發出 SNMP 通報。

輸入 `snmp-server enable traps [type]`，其中 `type` 可以是 `authentication` 或 `link-up-down`。按下 <Enter>。

```
Console(config)#snmp-server enable traps link-up-down
Console(config)#
```

3. 請依照 《Sun Fire B1600 Blade 系統機箱軟體設定手冊》中的程序，將組態設定儲存起來。



## 第 II 部分 設定交換器組態

---

本節說明交換器的基本功能，並示範如何透過網路瀏覽器與指令行介面對每一項功能進行設定。

管理概述

指令行參考資料



## 管理概述

---

本章說明如何進行基本的組態設定工作。

- 第 3-2 頁的 3.1 節「使用 Web 介面」
- 第 3-7 頁的 3.2 節「基本組態」
- 第 3-32 頁的 3.3 節「設定全區網路通訊協定」
- 第 3-78 頁的 3.4 節「連接埠組態」
- 第 3-112 頁的 3.5 節「監視通訊埠與管理流量」

---

## 3.1 使用 Web 介面

此交換器內附有一個 HTTP Web 代理程式，讓您可以透過網路瀏覽器設定交換器，以及觀看統計數據監視網路上的活動。網路上任何電腦只要使用標準的網路瀏覽器（例如 5.0 或更新版的 Internet Explorer，以及 6.2 或更新版的 Netscape Navigator），便可連上此 Web 代理程式。

---

**注意：**此外，透過序列線路連上主控台連接埠或透過 Telnet，亦可連上指令行介面 (CLI) 對交換器進行管理。關於使用 CLI 的詳細相關資訊，請參閱第 4 章。

---

透過網路瀏覽器連上交換器之前，請注意先做好以下事項：

1. 用外接序列線路、BOOTP 或 DHCP 通訊協定為交換器設定正確的 IP 位址、子網路遮罩以及預設閘道。（如需執行此動作的相關資訊，請參閱《Sun Fire B1600 Blade 系統機箱軟體設定手冊》。）
2. 用外接序列線路設定使用者名稱與密碼。Web 代理程式的存取控制，也是使用與內附組態設定程式同一套的使用者名稱與密碼。（如需執行此動作的相關資訊，請參閱《Sun Fire B1600 Blade 系統機箱軟體設定手冊》。）

---

**注意：**若管理主機與此交換器之間的路徑並未經過任何使用 Spanning Tree 演算法的裝置，則管理主機所連的交換器連接埠便可以設定成使用快速轉送，加快交換器對於 Web 介面所發出管理指令的反應時間。（請參閱第 3-105 頁的「Admin Edge Port」。）

---

3. 輸入使用者名稱與密碼之後，便可使用系統組態設定程式。

---

**注意：**您有三次機會輸入正確的密碼，若三次都錯誤，交換器便會將連線切斷。

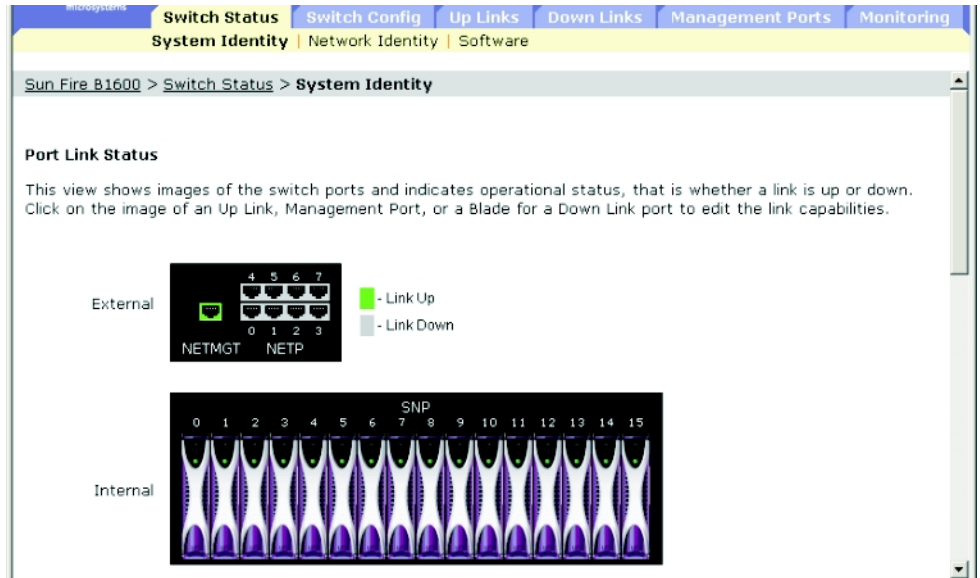
---

## 3.1.1 網路瀏覽器介面導覽

要使用網路瀏覽器介面，首先要輸入使用者名稱與密碼。管理員對所有組態參數與統計資料均有讀寫權限，其預設使用者名稱與密碼均為 **admin**。

### 3.1.1.1 首頁

當網路瀏覽器連上交換器的 Web 代理程式時，便會將其首頁顯示出來。選取左邊主功能表中的 **Switch**，組態選項便會顯示在功能表標籤上，相對應的功能表項目（橫列於功能表標籤下方）也會顯示在畫面最上方。功能表標籤與次功能表項目可用來存取組態設定功能表、顯示組態參數以及統計資料。



### 3.1.1.2 組態選項

組態參數有一個對話方塊或下拉式清單。每當您修改某一頁顯示的組態後，請務必記得按下「Save」按鈕確認新的設定。以下簡介網頁上的各個組態設定按鈕。

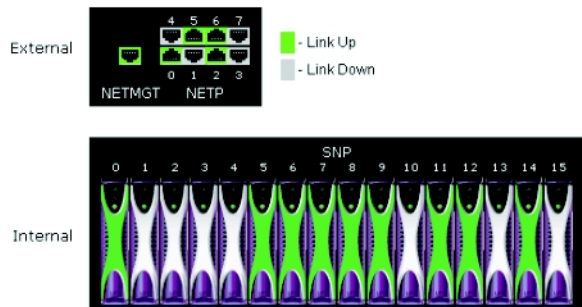
按鈕	動作
Cancel	取消新設定的值，恢復為原來的設定值。
Reset	取消新設定的值，恢復為原來的設定值。
Save	將新的設定值傳給系統。

**注意：**為了確保螢幕正常刷新顯示，請依照以下方式設定 Internet Explorer 5.x：在「工具」/「網際網路選項」/「一般」/「Temporary Internet Files」/「設定」中，將「檢查儲存的畫面是否有較新的版本」設定為「每次查閱畫面時」。

**注意：**若您使用的是 Internet Explorer 5.0，每次對組態有任何修改後，請按下瀏覽器的「重新整理」按鈕，手動讓螢幕重新顯示。

## 3.1.2 顯示面板

Web 代理程式會顯示交換器上連連接埠的圖案，且圖案中會顯示每個連接埠究竟是否有任何接線。按下任何一個連接埠的圖案，便會出現如第 3-78 頁所描述的「連接埠組態」頁面。





### 3.1.3 主功能表

透過內附的 Web 代理程式，您可以設定系統參數、管控交換器與所有連接埠、以及監視網路的狀態。下表簡單說明此軟體提供的功能。

功能表	說明	頁數
Switch Setup	基本組態設定	3-7
System Identity	提供基本系統描述，包括所在位置與聯絡人資料	3-7
Network Identity	透過 DHCP、BOOTP 或手動方式設定管理所用的 IP 位址	3-10
Software	顯示韌體版本、下載程式碼與組態設定值	3-16
Switch Config	全區組態設定通訊協定	3-32
Security	設定使用者名稱與密碼，以及是否要利用 RADIUS 或 TACACS+ 遠端存取認證服務	3-23
Communication	設定 SNMP 群體存取字串、trap 管理主機以及要發出的 trap 種類	3-28
VLANs	顯示基本 VLAN 資訊、啓動 GVRP 群組廣播通訊協定、設定 VLAN	3-32
Static VLAN Port Membership	將固定的成員加入 VLAN 內	3-40
Broadcast & Multicast	設定廣播風暴控制以及群組廣播通訊協定，包括 IGMP 窺探、靜態路由器連接埠資訊以及群組廣播服務	3-43
IGMP Parameters	啓動群組廣播過濾、設定群組廣播查詢參數	3-44
Multicast Router Ports	指派連接鄰近群組廣播路由器 / 交換器的連接埠	3-47
Multicast Services	在特定介面上指派群組廣播服務	3-50
Broadcast Parameters	設定廣播風暴流量上限	3-53
Spanning Tree	設定 Spanning Tree 通訊協定	3-55
Basic Configuration	設定全區 spanning tree 的設定值	3-55
Advanced Configuration	設定 RSTP 的進階設定值	3-61
Class of Service	設定服務類別	3-63
Basic Traffic Prioritisation	設定預設 CoS 優先順序、將 CoS 優先順序對應到輸出佇列，以及設定權重式巡迴佇列	3-63
Layer 3/4 Traffic Prioritisation	選取第 3/4 層的優先等級服務、將 IP 優先標籤對應到 CoS 設定值，以及將 DSCP 標籤對應到 CoS 設定值	3-69
Address Tables	設定位址保留期限，顯示指定介面、VLAN 或位址的項目，設定靜態位址	3-75

功能表	說明	頁數
Up Links	連接埠組態	3-78
Connection Status	顯示連接埠連線狀態	3-78
Connection Configuration	設定連接埠連線組態、啓動廣播風暴控制	3-82
Link Aggregation	將連接埠設定成透過 LVAP 動態加入寬道，或設定將哪些連接埠組成一個固定的寬道	3-86
VLANs	設定連接埠屬性（包括預設 PVID、switchport 模式、接收過濾器、GVRP、GARP 計時器）以及固定的 VLAN 成員	3-91
Static Addresses	顯示或編輯位址表中的靜態項目、啓用或停用固定項目的學習功能	3-97
Spanning Tree	設定全區 spanning tree 的連接埠設定	3-100
Spanning Tree Protocol	設定全區 spanning tree 上各介面的 STA 連接埠層級組態	3-100
Down Links	連接埠組態	3-78
Connection Status	顯示連接埠連線狀態	3-78
Connection Configuration	設定連接埠連線組態、啓動廣播風暴控制	3-82
Link Aggregation	將連接埠設定成透過 LVAP 動態加入寬道，或設定將哪些連接埠組成一個固定的寬道	3-86
VLANs	設定連接埠屬性（包括預設 PVID、switchport 模式、接收過濾器、GVRP、GARP 計時器）以及固定的 VLAN 成員	3-91
Static Addresses	顯示或編輯位址表中的靜態項目、啓用或停用固定項目的學習功能	3-97
Spanning Tree	設定全區 spanning tree 的連接埠設定	3-100
Spanning Tree Protocol	設定全區 spanning tree 上各介面的 STA 連接埠層級組態	3-100
Management Port	連接埠組態	3-78
Connection Status	顯示連接埠連線狀態	3-78
VLANs	設定連接埠屬性（包括預設 PVID、switchport 模式、接收過濾器、GVRP、GARP 計時器）以及固定的 VLAN 成員	3-91
Packet Filtering	過濾從上連連接埠進入管理連接埠的流量	3-108
Monitoring	交換器監視功能	3-112
Port Mirroring	設定鏡射功能的來源與目的地連接埠	3-112
Port Statistics	顯示連接埠流量統計數據，包括 Interfaces 群組、Ethernetlike MIB 以及 RMON MIB	3-113
SNMP Statistics	顯示 SNMP 訊息統計數據	3-122
Logs	設定日誌訊息參數，顯示交換器記憶體內存放的訊息	3-122

---

## 3.2 基本組態

### 3.2.1 顯示系統資訊

為系統設定一個有意義的名稱，並輸入其所在位置與聯絡人資訊，以後就可以很容易辨認出這個系統。

#### 指令屬性

- **Host Name** – 設定給此交換器的名稱。
- **Location** – 指定系統機箱所在位置。
- **Contact** – 負責此系統的管理員。
- **System Up Time** – 此管理代理程式自從上次啓動之後至今歷時多久。
- **System Description** – 製造商指派的系統硬體說明。
- **Serial Number**<sup>1</sup> – 主機板的序號。
- **System OID string**<sup>2</sup> – 交換器網路管理子系統的 MIB II 物件 ID。
- **MAC Address**<sup>3</sup> – 此交換器的硬體層位址。
- **Web server**<sup>2</sup> – 顯示透過 HTTP 進行管理的功能是否啓用或停用。
- **Web server port**<sup>2</sup> – 顯示 Web 介面使用的 TCP 通訊埠編號。
- **POST result**<sup>2</sup> – 顯示開機自我測試結果。

1: CLI: 請參閱第 4-40 頁的「show version」

2: 僅適用於 CLI

3: Web: 請參閱第 3-10 頁的「設定 IP 位址」

**Web** – 打開 Switch Setup=>System Identity。設定主機名稱、所在位置以及系統管理員的聯絡資訊，然後按下「Save Changes」。

The screenshot shows the 'System Identity' configuration page in a web browser. The page has a navigation bar with tabs for 'Switch Status', 'Switch Config', 'Up Links', 'Down Links', 'Management Ports', and 'Monitoring'. Under 'Switch Config', there are sub-tabs for 'System Identity', 'Network Identity', and 'Software'. The main content area is titled 'System Configuration' and contains a text block explaining the purpose of the page. Below this are several input fields: 'Host Name' with the value 'R&D 5', 'Location' with 'WC 9', and 'Contact' with 'Charles'. There are also read-only fields for 'System Uptime', 'System Description', and 'Serial Number'.

**CLI** – 設定主機名稱、所在位置以及聯絡資訊。

```
Console(config)#hostname R&D 5                                4-24
Console(config)#snmp-server location WC 9                    4-50
Console(config)#snmp-server contact Bill                     4-49
Console#show system                                          4-38
System description: Sun Fire B1600
System OID string: 1.3.6.1.4.1.674.10895.4
System information
  System Up time: 0 days, 0 hours, 55 minutes, and 54.91 seconds
  System Name      : [NONE]
  System Location  : [NONE]
  System Contact   : [NONE]
  MAC address      : 00-00-e8-00-00-01
  Web server       : enable
  Web server port  : 80
  Web secure server : enable
  Web secure server port : 443
  POST result

--- Performing Power-On Self Tests (POST) ---
UART Loopback Test ..... PASS
Timer Test ..... PASS
DRAM Test ..... PASS
I2C Initialization ..... PASS
Runtime Image Check ..... PASS
PCI Device Check ..... PASS
Switch Driver Initialization ..... PASS
----- DONE -----
Console#
```

## SNMP – 對等 MIB 變數。

欄位名稱	MIB 變數	權限	設定值範圍	預設值
System Name (Host Name)	MIB-II. system. sysName	可讀寫	字串 (長度 0-255)	
System Location	MIB-II. system. sysLocation	可讀寫	字串 (長度 0-255)	
System Contact	MIB-II. system. sysContact	可讀寫	字串 (長度 0-255)	
System Up Time	MIB-II. system. sysUpTime	唯讀	時間 (以百分之一秒 為單位)	
System Description	MIB-II. system. sysDescr	唯讀	字串 (長度 0-255)	
System Object Identification	MIB-II. system. sysObjectID	唯讀	物件識別碼	
MAC Address	MIB-II. interfaces. ifTable.ifEntry. ifPhysAddress	唯讀	實體位址	
HTTP State (Web Server)	sun... ipMgt. ipHttpState	可讀寫	enabled (1), disabled (2)	enabled
HTTP Port (Web Server Port)	sun... ipMgt. ipHttpPort	可讀寫	整數 (1-65535)	80
HTTPS State (Secure Server)	sun... ipMgt. ipHttpsState	可讀寫	enabled (1), disabled (2)	enabled
HTTPS Port (Secure Server Port)	sun... ipMgt. ipHttpsPort	可讀寫	整數 (1-65535)	443

## 3.2.2 設定 IP 位址

交換器預設會用 DHCP 搜尋其 IP 位址、預設閘道以及網路遮罩。

您可以手動為其設定 IP 位址，或引導該裝置從 BOOTP 或 DHCP 伺服器取得位址。正確的 IP 位址由四個 0 到 255 的十進位數字組成，各數字以小數點隔開。不符合此格式的設定值，都不會為交換器軟體所接受。

---

**注意：**交換器的 IP 位址事實上是包含管理連接埠 (NETMGT) 之 VLAN 的 IP 位址。此管理連接埠預設隸屬於 VLAN 2，因此您必須指定 IP 位址給 VLAN 2，才能設好交換器透過網路連接的功能。只有管理連接埠所屬的 VLAN，才應該設定 IP 位址。設定 IP 位址給任何 VLAN 時，原來 IP 位址會立刻停止使用，新的位址也會立刻生效。

---

### 指令屬性

- **Current IP Address** – 允許連線進行管理之 VLAN 介面目前的位址。
- **MAC Address**<sup>1</sup> – 此交換器的硬體層位址。
- **Management VLAN** – 這是管理交換器時必經的唯一 VLAN。管理連接埠 (NETMGT) 預設為此 VLAN (即 VLAN 2) 的成員。但如果您更改了管理 VLAN，而且 NETMGT 連接埠還未設定成隸屬於這個新的 VLAN，便無法連上交換器進行管理，此時必須透過主控台介面將 NETMGT 連接埠加入新設定的管理 VLAN 才行。(請參閱第 4-111 頁的 4.3.12.8 節「switchport allowed vlan」。)

1: CLI: 請參閱第 3-7 頁的「顯示系統資訊」。

- **IP Address Mode** – 設定 IP 功能要透過手動設定 (靜態)、DHCP 或 BOOTP 啓動。若使用 DHCP/BOOTP，則在還沒收到伺服器的回應之前，IP 功能都不會運作。交換器會定期以廣播方式發出要求，請伺服器回應 IP 組態設定。(DHCP/BOOTP 設定值可含 IP 位址、子網路遮罩以及預設閘道。)
- **DHCP** – Dynamic Host Configuration Protocol (動態主機組態設定通訊協定)
  - **Enable Client ID** – 將用戶端識別碼放入與 DHCP 來往的所有通訊資料內。
    - **Text / Hex** – 設定用戶端 ID 是以文字字串 (1-15 個字元) 或十六進位值輸入。要使用哪一種資料型態，視 DHCP 伺服器的需求而定。

---

**注意：**此功能表內設定的 Client ID 在下次系統或交換器重新開機時，便會被 SC 蓋掉。下一版的韌體將不再有 Client ID 這個欄位。

---

- **BOOTP** – Boot Protocol (開機通訊協定)
- **Manual** – 將管理介面設定成指定值。
  - **IP Address** – 允許連入進行管理之 VLAN 介面的位址。正確的 IP 位址由四個 0 到 255 的十進位數字組成，各數字以小數點隔開。(預設值：0.0.0.0)
  - **Subnet Mask** – 此遮罩定出通往特定子網路之路由所使用的是哪幾個主機位址位元。(預設值：255.0.0.0)
  - **Broadcast Address<sup>2</sup>** – 在指定 IP 位址之介面上發送封包時所使用的 IP 廣播位址，適用於交換器所使用之子網路與網路廣播位址。(預設值：0.0.0.1)
  - **Gateway IP Address** – 此裝置與位於其它網段之管理主機之間的閘道路由器的 IP 位址。(預設值：0.0.0.0)

2: 僅適用於 Web

### 3.2.2.1 手動設定

**Web** – 打開 Switch Setup=>Network Identity。選取管理介面，按下「Manual」圓形按鈕，設定 IP 位址、子網路遮罩以及預設閘道，然後按下「Save」。

microsystems

Switch Status | Switch Config | Up Links | Down Links | Management Ports | Monitoring

System Identity | Network Identity | Software

Sun Fire B1600 > Switch Status > Network Identity

To change the VLAN used for managing the switch, you will need to change the Management VLAN. Note: To prevent loss of connection to the switch, ensure that the Management Port is configured as a member of the new VLAN.

**Current IP Address:** 10.1.0.2

**MAC Address:** 00-00-E8-66-66-72

**Management VLAN:** 2 MgtVlan

Use the radio buttons to select whether the switch IP address is manually configured or dynamically configured by a DHCP or BOOTP Server on your network. The switch will broadcast a request for IP configuration settings on the next power Cancel. Otherwise, you can click the Request Address button to immediately request a new address.

**Select IP Address Mode:**

DHCP Client

Enable Client ID :

Text      Hex

BOOTP

Restart DHCP/BOOTP for changes to take effect: **Save and Restart**

Manual

IP Address:

Subnet Mask:

Broadcast Address:

Gateway IP Address:

**Save**   **Cancel**

**注意：**若出現的錯誤訊息表示您輸入的資料不正確，請檢查您設定的每個 IP 位址是否正確。



CLI – 設定管理介面、IP 位址以及預設閘道。

```

Console#config
Console(config)#interface vlan 2                                4-74
Console(config-if)#ip address 10.1.0.2 255.255.255.0          4-62
Console(config-if)#exit
Console(config)#ip default-gateway 10.1.0.254                4-66
Console(config)#
    
```

SNMP – 對等 MIB 變數。

欄位名稱	MIB 變數	權限	設定值範圍	預設值
Management VLAN	sun... switchMgt. switchManagementVlan	可讀寫	整數 (1-4094)	1
IP Address Mode	sun... vlanMgt. vlanTable.vlanEntry. vlanAddressMethod	可讀寫	user (1), bootp (2), dhcp (3)	user
IP Address Configuration	MIB-II. ip.ipAddrTable. ipAddrEntry. ipAdEntAddr	可讀寫	IP 位址	
Subnet Mask Configuration	MIB-II. ip.ipAddrTable. ipAddrEntry. ipAdEntNetMask	可讀寫	IP 位址	
Broadcast Address	MIB-II. ip.ipAddrTable. ipAddrEntry. ipAdEntBcastAddr	唯讀	整數 (0-1)	1
Default Gateway Configuration	sun... ipMgt. netDefaultGateway	可讀寫	IP 位址	

### 3.2.2.2 使用 DHCP/BOOTP

交換器預設使用 DHCP/BOOTP 服務尋找自己的 IP 組態資訊。

**Web** – 打開 Switch Setup=>Network Identity。設定管理介面，按下 DHCP 或 BOOTP 圓形按鈕。

機箱內的系統控制器預設會提供一組用戶端識別碼給交換器，分別為 SUNW, SWITCH\_ID= 機箱序號,0 或 SUNW,SWITCH\_ID= 機箱序號,1，視交換器在 SSC0 或 SSC1 內而定。您可以在「Enable Client ID」核取方塊內設定用戶端識別碼，但下次系統控制器重置或重新開機後，此設定值便會失效。建議您不要以這種方法設定。未來新版韌體將取消這個「Enable Client ID」欄位。

The screenshot shows the 'Network Identity' configuration page. At the top, there are tabs for 'Switch Status', 'Switch Config', 'Up Links', 'Down Links', 'Management Ports', and 'Monitoring'. Below these are sub-tabs for 'System Identity', 'Network Identity', and 'Software'. The 'Network Identity' sub-tab is active. The page displays the following information:

- Current IP Address: 10.1.0.1
- MAC Address: 00-00-E8-66-66-72
- Management VLAN: 2 MgtVlan (selected from a dropdown menu)

Below this information, there is a text block: "Use the radio buttons to select whether the switch IP address is manually configured or dynamically configured by a DHCP or BOOTP Server on your network. The switch will broadcast a request for IP configuration settings on the next power Cancel. Otherwise, you can click the Request Address button to immediately request a new address."

The 'Select IP Address Mode:' section contains:

- DHCP Client
- BOOTP
- Enable Client ID :
  - Text:
  - Hex:  0010b55169f7

At the bottom, there is a text field: "Restart DHCP/BOOTP for changes to take effect:" followed by a **Save and Restart** button.

**注意：**若管理連線斷掉，請使用主控台連線，輸入 show ip interface 找出交換器的新位址。

**注意：**在此功能表內設定的 Client ID，下次系統控制器或交換器本身重新開機後，便會被 SC 蓋掉。下一版的韌體將不再有 Client ID 這個欄位。

**CLI** – 指定管理介面，將 IP 位址模式設定為 DHCP 或 BOOTP，然後輸入 ip dhcp restart 指令。

```

Console#config
Console(config)#interface vlan 2                                4-74
Console(config-if)#ip address dhcp                             4-62
Console(config-if)#ip dhcp client-id hex 00-00-e8-66-65-72    4-65
Console(config-if)#end
Console#ip dhcp restart                                       4-64
Console#show ip interface                                     4-67
IP address and netmask: 10.1.0.54 255.255.255.0 on VLAN 2,
  and address mode: DHCP.
Console#

```

**更新 DHCP** – DHCP 可能會將位址發放給用戶端無限期使用，也可能只讓用戶端使用一段時間。若位址的租用時間到期，或交換器移到另一個網段內，會導致交換器暫時無法連線。此時請讓交換器重新開機或再發出一筆用戶端要求，重新啟動 DHCP 服務。

**Web** – 若 DHCP 發放的位址無法繼續使用，就無法透過 web 介面更新 IP 的設定值。只有當目前的位址還能正常運作時，才能透過 Web 介面重新啟動 DHCP 服務。

**CLI** – 請輸入以下指令重新啟動 DHCP 服務。

```

Console#ip dhcp restart                                       4-64

```

**SNMP** – 對等 MIB 變數。

欄位名稱	MIB 變數	權限	設定值範圍	預設值
Management VLAN	sun... switchMgt. switchManagementVlan	可讀寫	整數 (1-4094)	1
IP Address Mode	sun... vlanMgt. vlanTable.vlanEntry. vlanAddressMethod	可讀寫	user (1), bootp (2), dhcp (3)	dchp
DHCP Client ID	sun... ipMgt. dhcpClientIfClientId	可讀寫	二進位字串 (MAC 位址)	
DHCP Restart	sun... ipMgt. ipDhcpRestart	可讀寫	restart (1), noRestart (2)	noRestart

### 3.2.3

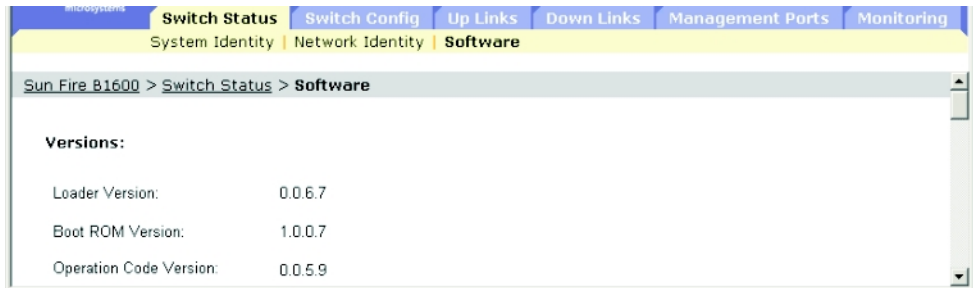
## 顯示交換器軟體版本

### 指令屬性

- **Loader Version** – 載入程式的版本號碼。
- **Boot-ROM Version** – 開機程式的版本。
- **Operation Code Version** – 執行時期程式碼的版本。
- **Unit ID\*** – 主交換器的 Id。(此設定值永遠為 1。)

\* 僅適用於 CLI。Unit Id 的設定值在 Stiletto B1600 Blade 系統機箱現在這個版本的交換器中沒有任何作用。

Web – 打開 Switch Setup=>Software。



CLI – 請輸入以下指令即可顯示版本號碼資訊。

```
Console#show version
Unit1
Serial number      : 1
Service tag       :
Hardware version   : R0B
Number of ports    : 25
Main power status  : up
Redundant power status : not present
Agent(master)
Unit id            : 1
Loader version     : 0.0.6.5
Boot rom version   : 0.0.7.3
Operation code version : 1.0.0.1
Console#
```

4-40

SNMP – 對等 MIB 變數。

欄位名稱	MIB 變數	權限	設定值範圍	預設值
Switch Serial Number	SUN. switchMgt. switchInfoTable. switchInfoEntry. swSerialNumber	唯讀	顯示字串 (0 到 80 個字元)	
Switch Hardware Version	SUN. switchMgt. switchInfoTable. switchInfoEntry. swHardwareVer	唯讀	顯示字串 (0 到 20 個字元)	
Switch Port Number	SUN. switchMgt. switchInfoTable. switchInfoEntry. swPortNumber	唯讀	整數	25
Switch Unit Index	SUN. switchMgt. switchInfoTable. switchInfoEntry. swUnitIndex	不可讀取	整數	1
Switch Loader Version	sun... switchMgt. switchInfoTable. switchInfoEntry. swLoaderVer	唯讀	字串 (0 到 20 個字元)	
Switch Boot Rom Version	sun... switchMgt. switchInfoTable. switchInfoEntry. swBootRomVer	唯讀	字串 (0 到 20 個字元)	
Switch Operation Code Version	sun... switchMgt. switchInfoTable. switchInfoEntry. swOpCodeVer	唯讀	字串 (0 到 20 個字元)	

## 3.2.4 管理韌體

您可以將韌體上傳到 TFTP 伺服器上，也可以從 TFTP 伺服器下載韌體。將執行時期程式碼放到 TFTP 伺服器上存成檔案，以後這個檔案就可以下載到交換器上，使交換器恢復運作。交換器也可以設定成使用新的韌體，而且不會將舊版的韌體蓋掉。

### 指令屬性

- 目的檔案名稱不可以含有斜線（包括 \ 與 /），檔案名稱開頭不可以是小數點（.），且 TFTP 伺服器上檔案名稱的長度不可超過 127 個字元，交換器上的檔案名稱長度不可超過 32 個字元。（可用字元：A-Z、a-z、0-9、.、-、\_）
- 交換器檔案目錄內只能存放兩份系統軟體檔案（其中含有執行時期韌體），而且目前設定開機時拿來使用的那個檔案無法刪除。若交換器內存有兩份系統軟體檔案，您便可以將其中未被指定在開機時使用的那個檔案刪除，以新的檔案取代，或用現有檔案名稱之一將另一個新的檔案複製到該目錄內。或者，您也可以取消目前指定用來開機的檔案，然後將它刪除，再把新版的系統軟體檔案複製到該目錄內，最後用這個新的檔案當作開機時使用的檔案。

### 3.2.4.1 從伺服器下載系統軟體

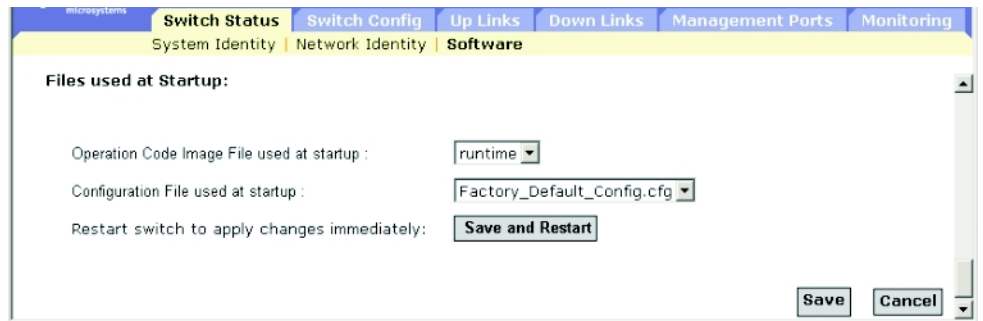
下載執行時期程式碼時，可以指定目的檔案名稱將現有的檔案蓋掉，或者存成與目前執行時期程式碼檔案名稱不同的檔案，然後將這個新的檔案設定成開機檔案。

**Web** – 打開 Switch Status=>Software。輸入 TFTP 伺服器的 IP 位址，輸入要下載的軟體檔案名稱，選取要替代交換器上的哪個檔案或設定新的檔名，接著按下「Download」。

The screenshot displays the 'Switch Software Deployment' web page. At the top, there are navigation tabs: 'Switch Status', 'Switch Config', 'Up Links', 'Down Links', 'Management Ports', and 'Monitoring'. Below these is a sub-menu: 'System Identity', 'Network Identity', and 'Software'. The main content area is titled 'Switch Software Deployment' and includes a note: 'If you would like to upgrade your firmware with a file other than the ones in the lists below, please include it to the list using the Add Button. Note: Space is limited and each list can only hold 2 user-defined files at a time. To add additional files please delete one first.' There are two main sections: 'TFTP Server' and 'Switch Operation Code Image Files'. The 'TFTP Server' section has input fields for 'IP Address' (containing '10.1.0.19') and 'File Name' (containing 'V1.0'), along with 'Download' and 'Upload' buttons. The 'Switch Operation Code Image Files' section shows a list of files with 'runtime' selected, and a 'Remove' button.

**注意：**若出現錯誤訊息說您輸入的資料不正確，可能是您輸入了錯誤的 IP 位址或檔案名稱，或者您沒有適當的權限可進行 TFTP 傳輸。此外，交換器上的記憶體不足也可能是原因之一。

若您下載成新的檔案，請從下拉式方塊中選取該檔案，當作開機時所使用的程式碼，然後按下「Save」。若要立刻開始使用新版的韌體，請按下「Save and Restart」讓系統重新開機。



**CLI** – 輸入 TFTP 伺服器的 IP 位址，選取 config 或 opcode 檔案類型，接著輸入來源檔案名稱與目的檔案名稱，設定用這個新的檔案啟動系統，最後重新啟動交換器。

```
Console#copy tftp file 4-17
TFTP server ip address: 10.1.0.99
Choose file type:
  1. config: 2. opcode: <1-2>: 2
Source file name: v10.bix
Destination file name: V10000
\Write to FLASH Programming.
-Write to FLASH finish.
Success.

Console#config
Console(config)#boot system opcode: V10000 4-23
Console(config)#exit
Console#reload 4-15
```

若要啟動新版的韌體，必須輸入 reload 指令讓系統重新開機才行。

SNMP – 對等 MIB 變數。

欄位名稱	MIB 變數	權限	設定值範圍
Switch Operation Code Image Files	未定義		
TFTP Server IP Address	sun... tftpMgt. tftpServer	可讀寫	IP 位址
TFTP File Type	sun... tftpMgt. tftpFileType	可讀寫	opcode (1), config (2)
TFTP Source File Name	sun... tftpMgt. tftpSrcFile	可讀寫	字串 (0 到 127 個字元)
TFTP Destination File Name	sun... tftpMgt. tftpDestFile	可讀寫	字串 (0 到 127 個字元)
TFTP Action	sun... tftpMgt. tftpAction	可讀寫	notDownloading (1), downloadToPROM (2), downloadToRAM (3) ( <i>not supported</i> ) upload (4)
TFTP Status	sun... tftpMgt. tftpStatus	可讀寫	tftpSuccess (1), tftpStatusUnknown (2), tftpGeneralError (3), tftpNoResponseFromServer (4), tftpDownloadChecksumError (5), tftpDownloadIncompatible Image (6), tftpTftpFileNotFound (7), tftpTftpAccessViolation (8)
Restart Operation Code File	sun... restartMgt. restartOpCodeFile	可讀寫	顯示字串 (0 到 127 個字元)
Restart Action	sun... restartMgt. restartControl	可讀寫	running (1), warmBoot (2), coldBoot (3)



## 3.2.5 組態設定的儲存與復原

您可以從 TFTP 伺服器下載組態設定，也可以將組態設定上傳到 TFTP 伺服器上以後就可以將組態檔案下載到交換器上，讓交換器的設定恢復成以前的樣子。

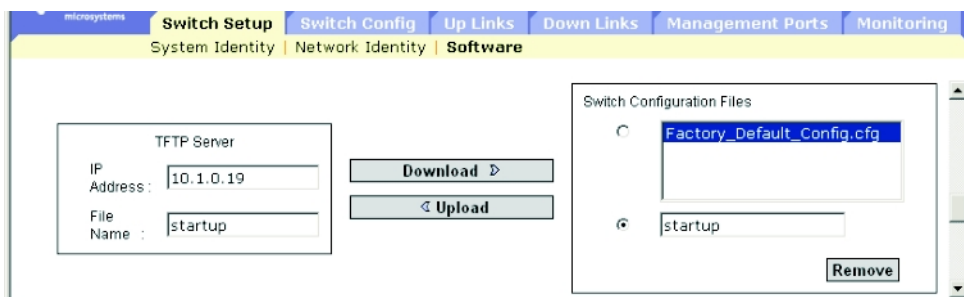
### 指令屬性

- 目的檔案名稱不可以含有斜線 (包括 \ 與 /)，檔案名稱開頭不可以是小數點 (.)，且 TFTP 伺服器上檔案名稱的長度不可超過 127 個字元，交換器上的檔案名稱長度不可超過 32 個字元。(可用字元：A-Z、a-z、0-9、.、-、\_)
- 使用者定義的組態檔案個數不得超過記憶體容量。

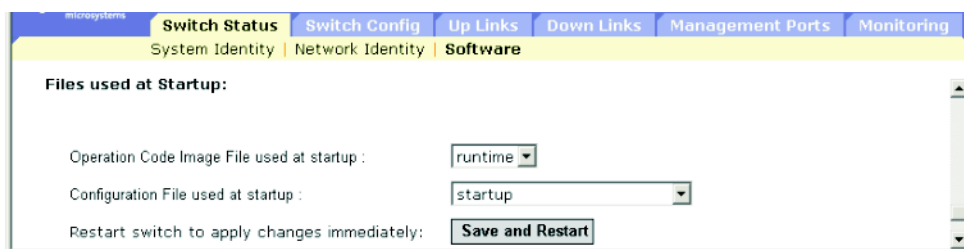
### 3.2.5.1 從伺服器下載組態設定

您可以將組態檔案下載下來存成新的檔案名稱，然後再將它設定為開機檔案，或者也可以將其存成目前的開機組態檔案，直接將舊的開機組態檔案蓋掉。請注意，Factory\_Default\_Config.cfg 可以複製到 TFTP 伺服器上，但是將檔案下載到交換器上時，不可以存成這個檔案名稱。

**Web** – 打開 Switch Setup=>Software。輸入 TFTP 伺服器的 IP 位址，輸入要下載的檔案名稱，選取要替代交換器上的哪個檔案或設定新的檔名，接著按下「Download」。



若要下載存成新的檔案名稱，請從下拉式方塊中選出此新檔名，然後按下「Save」。若要使用新的設定值，請按下「Save and Restart」讓系統重新開機。



**CLI** – 輸入 TFTP 伺服器的 IP 位址，指定要下載伺服器上的哪個來源檔案，設定交換器上的開機檔案名稱，最後重新啟動交換器。

```

Console#copy tftp startup-config                               4-17
TFTP server ip address: 192.168.1.19
Source configuration file name: startup2.0
Startup configuration file name [startup] : startup2.0
\Write to FLASH Programming.
-Write to FLASH finish.
Success.

Console#reload
System will be restarted, continue <y/n>?y

```

若您將開機組態檔案下載成新的檔案名稱，以後還可將這個檔案設定成開機檔案，然後再重新啟動交換器。

```

Console#config
Console(config)#boot system config: startup-new              4-23
Console(config)#exit
Console#reload                                               4-15
System will be restarted, continue <y/n>?y

```

**SNMP** – 對等 MIB 變數。

欄位名稱	MIB 變數	權限	設定值範圍
TFTP Server IP Address	sun... tftpMgt. tftpServer	可讀寫	IP 位址
TFTP File Type	sun... tftpMgt. tftpFileType	可讀寫	opcode (1), config (2)
TFTP Source File Name	sun... tftpMgt. tftpSrcFile	可讀寫	顯示字串 (長度 0-127)
TFTP Action	sun... tftpMgt. tftpAction	可讀寫	notDownloading (1), downloadToPROM (2), downloadToRAM (3), upload (4)
TFTP Status	sun... tftpMgt. tftpStatus	可讀寫	tftpSuccess (1), tftpStatusUnknown (2), tftpGeneralError (3), tftpNoResponseFromServer (4), tftpDownloadChecksumError (5), tftpDownloadIncompatibleImage (6),

欄位名稱	MIB 變數	權限	設定值範圍
			tftpTftpFileNotFound (7), tftpTftpAccessViolation (8)
Restart Configuration File	sun... restartMgt. restartConfigFile	可讀寫	顯示字串 (長度 0-127)
Restart Action	sun... restart.Mgt. restartControl	可讀寫	running (1), warmBoot (2), coldBoot (3)

## 3.2.6 設定使用者認證機制

「Security」功能表可依據使用者名稱與密碼設定其管理權限，您可以在交換器上手動設定存取權限，也可以透過使用 RADIUS 或 TACACS+ 通訊協定的遠端存取認證伺服器進行認證。

存取權限分為 Normal (一般權限) 與 Privileged (特權) 兩種：Normal 層級只有權使用部分指令，而 Privileged 層則能夠使用到所有指令。由於預設管理員帳號有權寫入交換器內附軟體的所有參數，因此建議您應盡快為此帳號設定密碼，並將密碼放置在安全的地方。

**注意：**預設管理員的名稱與密碼均為 admin。

### 指令使用方式

- 所有管理權限的檢查，預設都會採用交換器本身所儲存認證資料庫內的資料。若要使用遠端的認證伺服器，就必須針對每種遠端認證通訊協定設定其認證序列以及相關參數。
- Remote Authentication Dial-in User Service (遠端認證撥入使用者服務，簡稱 RADIUS) 與 Terminal Access Controller Access Control System (終端機存取控制存取控制系統，簡稱 TACACS) 兩種登入認證通訊協定，都是使用中央伺服器上執行的軟體控制網路上能夠使用 RADIUS 或 TACACS 之裝置的存取權限。認證伺服器上的資料庫內含有許多組使用者名稱/密碼，以及要連上交換器進行管理工作的每個使用者或群組的權限等級。

**注意：**設定 RADIUS 或 TACACS 伺服器上的權限等級時，請記得等級 0 代表以來賓 (即 Normal Exec) 權限連上交換器，而且只有等級 15 才是管理員 (即 Privileged Exec) 權限。

- RADIUS 採用 UDP，而 TACACS 則使用 TCP。UDP 只會盡全力將資料送達，但 TCP 卻提供連線式的傳輸功能。此外，請注意 RADIUS 只會將用戶端傳送給伺服器之存取要求封包內的密碼加密，而 TACACS 則會將整個封包的內容全部加密。
- RADIUS 與 TACACS 登入認證功能可控制透過主控台連接埠、網路瀏覽器與 telnet 進行的管理權限，但這些存取權限的設定必須事先在認證伺服器上設定好才行。
- RADIUS 與 TACACS 的登入認證功能會設定每組使用者名稱/密碼的權限等級，因此使用者名稱、密碼以及權限等級都必須在認證伺服器上事先設定好。
- 每個使用者都可以採用一到三種認證方式，並依照您設定的認證順序進行。例如選取 (1) RADIUS 與 (2) Local，則交換器便會先利用 RADIUS 檢查這組使用者名稱與密碼，若沒有 RADIUS 伺服器可用，便改用交換器上存放的使用者名稱與密碼資料進行認證。

## 指令屬性

### ■ Authentication Mechanisms

- **Require User Authentication** – 代表是否要進行認證。
- **Preference** – 交換器會依照指定的順序對使用者進行認證。

### ■ Authentication Server Settings

- **Server IP Address** – 認證伺服器的位址。(預設值：10.1.0.1)
- **Server Port Number** – 認證伺服器上用來接收認證訊息的網路 (UDP) 通訊埠。(範圍：1-65535，預設值：1812)
- **Encryption Key** – 對用戶端登入動作進行認證時所使用的加密金鑰，請勿在此字串內放入空格字元。(最大長度：20 個字元)
- **No. of Retries\*** – 交換器透過認證伺服器對登入動作進行認證時，最多會嘗試幾次。(範圍：1-30，預設值：2)
- **Timeout for reply\*** – 交換器等待回應時應該等待幾秒鐘才重送要求。(範圍：1-65535，預設值：5)

### ■ Local Access Authentication

- **User Account** – 使用者的名稱。(最大長度：8 個字元，使用者人數上限：5)
- **Access Level** – 使用者的層級。(選項：Normal 與 Privileged。)
- **Password** – 使用者的密碼。(最大長度：8 個名碼字元，大小寫有別)

\* 僅適用於 RADIUS 伺服器認證。

Web – 打開 Switch Config=>Security。若要設定採用交換器本身或遠端的認證機制，請設定認證順序(即一到三種方法)，輸入各種認證方法的參數，然後按下「Save」。

The screenshot shows the 'Authentication Mechanisms' configuration page. At the top, there are tabs for 'Switch Status', 'Switch Config', 'Up Links', 'Down Links', 'Management Ports', and 'Monitoring'. Under 'Switch Config', there are sub-tabs for 'Security', 'Communication', 'VLANs', 'Broadcast & Multicast', 'Spanning Tree', 'Class of Service', and 'Address'. The 'Security' sub-tab is active.

**Authentication Mechanisms**

Require User Authentication

First-preference: TACACS+    Second-preference: RADIUS    Third-preference: Local

**Authentication Server Settings**

**RADIUS Setting**

Server IP Address: 10.11.12.13    No. of Retries: 2  
Server Port Number: 1812    Timeout for reply: 5  
Encryption Key: \*\*\*\*\*

**TACACS Setting**

Server IP Address: 192.160.1.25  
Server Port Number: 88  
Encryption Key: \*\*\*\*\*

Buttons: Save, Cancel

設定採用交換器本身認證機制的參數時，需輸入使用者名稱、密碼與存取層級，然後按下「Add」。

The screenshot shows the 'Local Access Authentication' configuration page. At the top, there are tabs for 'Switch Status', 'Switch Config', 'Up Links', 'Down Links', 'Management Ports', and 'Monitoring'. Under 'Switch Config', there are sub-tabs for 'Security', 'Communication', 'VLANs', 'Broadcast & Multicast', 'Spanning Tree', 'Class of Service', and 'Address'. The 'Security' sub-tab is active.

**Local Access Authentication**

User Accounts    Access Level

admin	Privileged
guest	Normal

Buttons: Change Password..., Remove

User: bot    Access Level: Privileged

password: \*\*\*\*\*    Add

CLI – 設定使用者名稱與存取層級 (0 代表 Normal，15 代表 Privileged)，接著再設定密碼。最後設定 RADIUS 與 TACACS 遠端用戶認證機制所需的各項參數。

```

Console(config)#username bob access-level 15                4-25
Console(config)#username bob password smith
Console(config)#authentication login local tacacs radius    4-42
Console(config)#tacacs-server host 192.168.1.24            4-46
Console(config)#tacacs-server port 181                     4-46
Console(config)#tacacs-server key green                    4-47
Console(config)#radius-server host 192.168.1.25            4-43
Console(config)#radius-server port 181                    4-43
Console(config)#radius-server key white                    4-44
Console(config)#radius-server retransmit 5                 4-44
Console(config)#radius-server timeout 10                   4-45
Console(config)#

```

SNMP – 對等 MIB 變數。

欄位名稱	MIB 變數	權限	設定值範圍	預設值
User Name	未定義			
Password	未定義			
Access Level	未定義			
Authentication Sequence	未定義			
RADIUS Server Address	sun... securityMgt.radiusMgt. radiusServerAddress	可讀寫	IP 位址	10.11.12.13
RADIUS Server Port Number	sun... securityMgt.radiusMgt. radiusServerPortNumber	可讀寫	整數 (1-65535)	1812
RADIUS Server Encryption Key	sun... securityMgt.radiusMgt. radiusServerKey	可讀寫	字串 (讀取所得的 值永遠為 0)	(0 到 20 個字元)
RADIUS Server Retransmit	sun... securityMgt.radiusMgt. radiusServerRetransmit	可讀寫	整數 (1-65535)	2
RADIUS Server Timeout	sun... securityMgt.radiusMgt. radiusServerTimeout	可讀寫	整數 (1-65535) 秒	5
TACACS Server Address	sun... securityMgt.tacacsMgt. tacacsServerAddress	可讀寫	IP 位址	

欄位名稱	MIB 變數	權限	設定值範圍	預設值
TACACS Server Port Number	sun... securityMgt.tacacsMgt. tacacsServerPortNumber	可讀寫	整數 (1-65535)	
TACACS Server Encryption Key	sun... securityMgt.tacacsMgt. tacacsServerKey	可讀寫 (讀取所得的 值永遠為 0)	字串 (0 到 20 個字元)	

### 3.2.7 設定 SNMP

SNMP (Simple Network Management Protocol, 簡易網路管理通訊協定) 是一種專門針對控管網路上各種裝置或其他元件而設計的通訊協定, 交換器、路由器以及主機電腦都是常見可以透過 SNMP 進行管理的設備。除了用來監視網路環境中各項裝置的效能以及偵測潛在的問題之外, SNMP 一般還可以用來對這些裝置進行適當的設定, 使其正常運作。

本交換器內附一個 SNMP 代理程式, 會持續不斷監視硬體的狀態以及流過各連接埠的流量。網路管理主機只要使用 SunNet Manager 之類的軟體, 便可取得這些資訊。此內附軟體的存取權限由群體字串控制。要連上此交換器, 管理主機必須先傳送正確的群體字串通過認證才行。以下各節會說明群體字串與相關 trap 功能的設定方式。

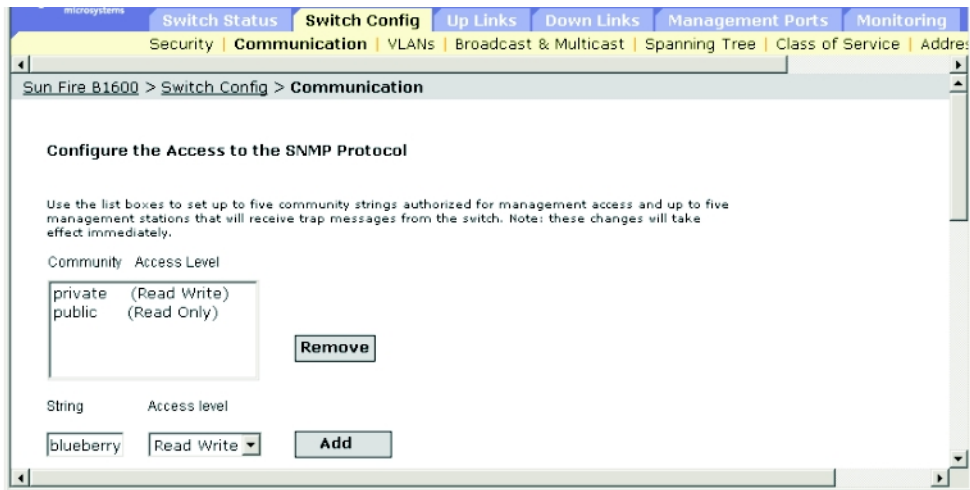
### 3.2.7.1 設定 SNMP 通訊協定的存取權限

用來檢查是否具有管理權限的群體字串，最多可以設定五組。為了安全上的考量，請務必將預設字串刪除。

#### 指令屬性

- **Community** – 群體字串與密碼的作用類似，提出此字串的人有權使用 SNMP 通訊協定。  
預設字串：public (唯讀權限)、private (讀寫權限)
  - 範圍：1–32 個字元，大小寫有別
  - 預設值：public (唯讀權限)、private (讀寫權限)
- **Access Level**
  - **Read Only** – 指定唯讀權限。代表有權存取的管理主機只能讀取 MIB 物件。
  - **Read/Write** – 指定讀寫權限。代表有權存取的管理主機可讀取與修改 MIB 物件。

**Web** – 打開 Switch Config=>Communication。視需要加入新的群體字串，從「Access Level」下拉式清單中選取存取權限，然後按下「Add」。



**CLI** – 以下示範加入具有讀寫權限的字串 blueberry。

```
Console(config)#snmp-server community blueberry rw
Console(config)#
```

4-48

**SNMP** – 對等 MIB 變數。

這些功能沒有相對應的 MIB 變數。



### 3.2.7.2 指定 Trap 管理員與 Trap 類別

交換器會發送代表狀態改變的 trap 給指定的 trap 管理員。請務必指定 trap 管理員，以後交換器才能將重大事件回報給管理主機（使用 SunNet Manager 之類的網路管理平台）。此交換器上最多可以設定五個接收交換器 trap 訊息的管理主機。第 A-3 頁的「支援的 Trap」所列便是此交換器支援的 trap。

#### 指令屬性

- **IP Address** – 該主機（接收 trap）的 IP 位址。  
（主機位址個數上限：5 個 trap 目的地位址項目）
- **Community** – 隨著通報訊息發送的群體字串，其作用與密碼類似。雖然您可以在 Trap Managers 表中設定此字串，但建議您最好也在 SNMP Protocol 表中予以定義。（最大長度：32 個字元）
- **Version** – 此主機使用的是第 1 版或 2c 版的 SNMP。
- **Generate SNMP notification for**
  - **Port link up and down events** – 任何連接埠斷線或建立連線時，均發出 trap 訊息。
  - **Authentication traps** – 任何 SNMP 存取認證過程中，每遇到一次輸入錯誤的群體字串，便發送一個 trap 訊息。

**Web** – 打開 Switch Setup=>Communications。填入所有會接收這些訊息之 Trap Manager 的 IP 位址與群體字串，然後按下「Add」。視需要挑選「Port link up and link down events」與「Authentication traps」核取方塊，然後按下「Save」。

**Specify TrapManagers**

IP Address	Community	Version
192.168.2.6	private	1
192.168.2.7	private	1

Remove

IP Address: 192.168.2.8    String: private    Version: 1    Add

**Specify Trap Types**

To disable the switch from sending link-up, link-down or authentication traps, you should uncheck these check boxes and press the save button to store the changes on the switch.

Generate SNMP notification for :

link up and down events

Authentication traps

Save    Cancel

**CLI** – 以下示範加入一個 trap 管理員，並啓動 link-up-down 與 authentication trap。

```
Console(config)#snmp-server host 10.1.0.19 private version 1 4-50
Console(config)#snmp-server enable traps link-up-down 4-51
Console(config)#snmp-server enable traps authentication
```

SNMP – 對等 MIB 變數。

欄位名稱	MIB 變數	權限	設定值範圍	預設值
Trap Destination Address	sun... trapDestMgt. trapDestTable. trapDestEntry. trapDestAddress	不提供外界存取	IP 位址	
Trap Destination Community	sun... trapDestMgt. trapDestTable. trapDestEntry. trapDestCommunity	讀取/建立	字串 (長度 0-127)	
Trap Destination Version	sun... trapDestMgt. trapDestTable. trapDestEntry. trapDestStatus	讀取/建立	version 1 (1), version 2 (2)	
Trap Destination Status	sun... trapDestMgt. trapDestTable. trapDestEntry. trapDestStatus	讀取/建立	valid (1), invalid (2)	
Enable Link-up-down Traps	MIB-II ifMIB.ifMIBObjects. ifXTable.ifXEntry. ifLinkUpDownTrapEnable	可讀寫	enabled (1), disabled (2)	enabled

---

## 3.3 設定全區網路通訊協定

本節說明各項交換器全區設定，包括虛擬 LAN、群組廣播服務、Spanning Tree 演算碼、根據特定服務類別要求處理資料、顯示位址表以及設定靜態位址。

### 3.3.1 VLAN 組態

在含有路由器的傳統網路中，廣播流量會被切分成好幾個領域，但交換器基本上並不支援廣播領域這項功能，因此會導致處理 IPX 或 NetBeui 流量的大型網路內出現廣播風暴的情形。若改用符合 IEEE 802.1Q 的 VLAN，便可將任意群組的網路節點隔離成不同的廣播領域，從而將廣播流量限制只能在其原來的群組內傳送，而且還能使網路環境更加安全整齊。

IEEE 802.1Q VLAN 由一群位於網路中任何位置的連接埠構成，但這些連接埠彼此之間以特殊方式聯繫，使他們看起來有如位於同一個實體網段內。

由於 VLAN 可在不更動任何實體接線的狀況下，將裝置改成隸屬於另一個新的 VLAN，因此能協助簡化網路的管理工作。VLAN 的劃分方式很有彈性，可根據部門（例如行銷部門或研發部門）、使用群組（例如電子郵件）或廣播群組（例如視訊會議之類的多媒體用途）等條件進行劃分。

VLAN 除了可降低廣播流量讓網路的使用更有效率之外，還可以在不需要更新 IP 位址或 IP 子網路的狀況下更動網路。由於每個 VLAN 的流量都必須經過事先設定好的第三層線路才能到達另一個 VLAN，因此 VLAN 基本上就具有較高階的網路安全功能。

此交換器支援的 VLAN 功能如下：

- 最多 255 個符合 IEEE 802.1Q 標準的 VLAN
- 利用明確或隱含的標籤以及 GVRP 通訊協定，可跨越多個交換器作到分散式 VLAN 學習
- 連接埠重疊，讓連接埠可以同時參與好幾個 VLAN
- 末端設備可隸屬於好幾個 VLAN
- 在具有 VLAN 功能以及不具有 VLAN 功能的裝置之間傳遞流量
- 加註優先等級標籤

## 設定連接埠所屬的 VLAN

啓動交換器的 VLAN 功能之前，必須先將每個連接埠設定給其欲加入的 VLAN 群組。所有連接埠一開始均預設隸屬於 VLAN 1，而且是不會加註標籤的連接埠。若您希望傳送多個 VLAN 的流量，而且所有中介網路裝置以及連線另一端的主機都支援 VLAN，請將連接埠設定成會加註標籤後再加入 VLAN，然後以手動方式或 GVRP 動態方式，將流量沿途流經路線上具有 VLAN 功能的網路裝置連接埠加入同一個 VLAN 內。不過如果要讓交換器上的連接埠加入一個以上的 VLAN，但沿途網路裝置以及連線另一端的主機都不具有 VLAN 功能，就應將此連接埠設定成不會加註標籤的連接埠，然後才加入 VLAN。

---

**注意：**加註 VLAN 標籤的封包可流過具有 VLAN 以及不具有 VLAN 的網路互連裝置，但不可以傳給沒有 VLAN 標籤加註功能的末端節點。

---

**VLAN 分類** – 交換器收到任何封包時，都會根據以下兩種方式其中任何一種為封包進行分類。若封包並未加註標籤，則交換器便會將此封包指定給相關的 VLAN (根據收到此封包之連接埠的 PVID)。但如果封包上有加註標籤，交換器就會利用所加註的 VLAN ID 找出該封包的連接埠廣播領域。

**連接埠重疊** – 此項功能可讓檔案伺服器或印表機之類經常共用的網路資源同時隸屬於好幾個 VLAN 群組。請注意，如果所有的 VLAN 都設定成不互相重疊，但彼此之間又需要互傳資料，請用第三層路由器或交換器將它們連接起來。

**根據連接埠劃分 VLAN** – 此種 VLAN 亦稱靜態 VLAN，經由手動方式設定所含連接埠。此時交換器會根據目的地 MAC 位址與相對應連接埠進行流量轉送，因此交換器在運作過程中必須得知 MAC 位址與相關連接埠的關係 (據此可推斷出與 VLAN 的關係)，才能作出正確的轉送或廣播決定。不過如果啓動 GVRP，整個過程就可以全部自動化。

**自動 VLAN 註冊** – 在 GARP VLAN Registration Protocol (GARP VLAN 註冊通訊協定，簡稱 GVRP) 定義的系統中，交換器會自動學習到每個末端裝置應指定給哪個 VLAN。若末端裝置 (或其網路卡) 支援 IEEE 802.1Q VLAN 通訊協定，便可設定成向網路發出廣播訊息，宣告其欲加入的 VLAN 群組。當交換器收到這些訊息時，便會自動將接收到訊息的連接埠放入指定的 VLAN 內，並將訊息轉送到其它所有的連接埠。當這些訊息傳到另一個支援 GVRP 的交換器時，該交換器也會將收到此訊息的連接埠放入指定的 VLAN 內，接著也會將這些訊息繼續轉送到其它所有連接埠。VLAN 的需求就是用這種方式散播到整個網路的每個角落，讓具有 GVRP 功能的裝置只要根據末端主機的要求，便能自動設定好 VLAN 群組。

要在網路內實施 GVRP，首先請將主機裝置加入所需的 VLAN 內（使用作業系統或其它應用軟體），讓其 VLAN 設定傳遞到網路上。在這些主機直接連接的邊緣交換器以及位於網路核心位置的交換上，啟動兩者互連之連接埠的 GVRP 功能。（請參閱第 3-91 頁的「設定介面的 VLAN 行爲」。）此外，您還必須定出網路中的安全邊界，在您不希望宣告訊息繼續往外傳遞的末端連接埠上關閉其 GVRP 功能，或是禁止某些連接埠加入限定成員的 VLAN 內。

---

**注意：**對於不支援 GVRP 的網路裝置，就必須在這些裝置所連之交換器連接埠上設定靜態 VLAN（如第 3-40 頁的「在 VLAN 內加入固定成員」所示）。不過這些邊緣交換器以及位於網路核心位置的交換器上還是必須啟動 GVRP 功能。

---

## 轉送加註標籤與未加註標籤的封包

如果您想為直接連接在同一個交換器上的裝置建立一個根據連接埠設定的小 VLAN，只要將這些連接埠加入同一個未加註標籤的 VLAN 即可。但如果要加入一個橫跨好幾個交換器的 VLAN 群組，除了必須為該群組建立一個 VLAN 之外，所有連接埠上也必須啟動加註標籤的功能才行。

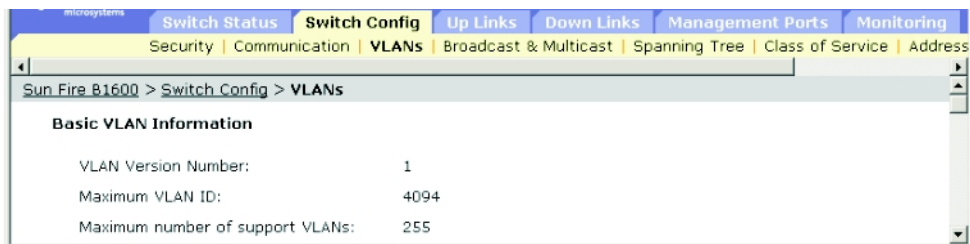
由於每個連接埠都可以隸屬於多個有加註標籤或未加註標籤的 VLAN，因此交換器上的每個連接埠都有能力傳送加註標籤或未加註標籤的封包。將交換器收到的封包轉送到沿路有部分裝置支援 VLAN 的路線上時，交換器便會將 VLAN 標籤加上去。但如果交換器收到的封包要轉送到沿路裝置（包括目的地主機）都不支援 VLAN 的路線，交換器就應該先將 VLAN 標籤拿掉，才可以將封包轉送出去。當交換器收到有加註標籤的封包時，會將此封包傳到標籤所指定的 VLAN 上。但如果交換器從不具有 VLAN 功能的裝置收到未加註標籤的封包，首先交換器會決定應該將此封包轉送到哪裡去，然後在此封包內加上 VLAN 標籤，註明接收此封包之連接埠的預設 VID。

### 3.3.1.1 顯示基本 VLAN 資訊

#### 指令屬性

- **VLAN Version Number** – 此交換器使用之 IEEE 802.1Q 標準中的 VLAN 版本。
- **Maximum VLAN ID** – 此交換器認得之最大 VLAN ID。
- **Maximum Number of Supported VLANs** – 此交換器上可設定之 VLAN 個數上限。

Web – 打開 Switch Config=>VLAN。



CLI – 輸入以下指令。

```
Console#show bridge-ext 4-119
Max support vlan numbers: 32
Max support vlan ID: 4094
Extended multicast filtering services: No
Static entry individual port: Yes
VLAN learning: IVL
Configurable PVID tagging: Yes
Local VLAN capable: Yes
Traffic classes: Enabled
Global GVRP status: Disabled
GMRP: Disabled
Console#
```

SNMP – 對等 MIB 變數。

欄位名稱	MIB 變數	權限	設定值範圍	預設值
VLAN Version Number	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qBase. dot1qVlanVersion- Number	唯讀	version1 (1)	version1

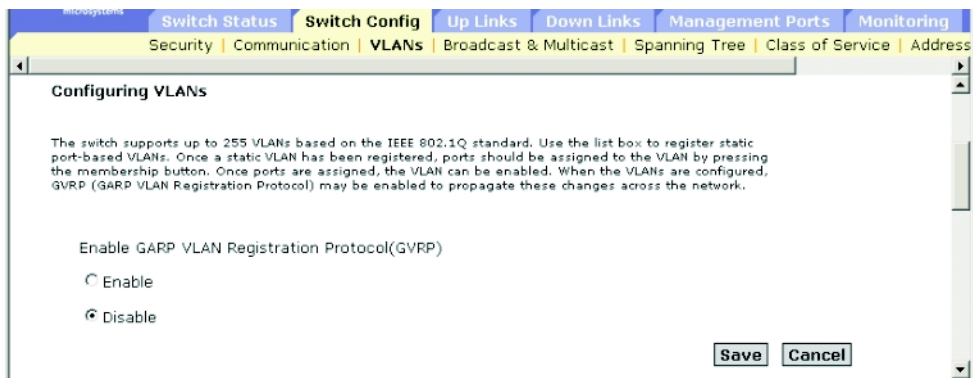
欄位名稱	MIB 變數	權限	設定值範圍	預設值
Maximum VLAN ID	MIB-II. dot1dBridge. BridgeMIB. BridgeMIBObjects. dot1qBase. dot1qMaxVlanId	唯讀	整數	4094
Maximum Number of Supported VLANs	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qBase. dot1qMaxSupportedVlans	唯讀	整數	255
Device Capabilities	MIB-II. dot1dBridge. pBridgeMIB. pBridgeMIBObjects. dot1dExtBase. dot1dDeviceCapabilities	唯讀	位元字串 – ExtendedFiltering dot1dServices (0), dot1dTrafficClasses (1), StaticEntry dot1dIndividualPort (2), dot1dIVLCapable (3), dot1dSVLCapable (4), dot1dHybridCapable (5), dot1dConfigurablePvid dot1dTagging (6), dot1dLocalVlanCapable (7)	2, 3, 6, 7
Traffic Classes Enabled	MIB-II. dot1dBridge. pBridgeMIB. pBridgeMIBObjects. dot1dExtBase. dot1dTrafficClasses- Enabled	可讀寫	true (1), false (2)	true
GMRP Status	MIB-II. dot1dBridge. pBridgeMIB. pBridgeMIBObjects. dot1dExtBase. dot1dGmrpStatus	可讀寫	enabled (1), disabled (2)	disabled
GVRP Status	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qBase. dot1qGvrpStatus	可讀寫	enabled (1), disabled (2)	disabled



### 3.3.1.2 GVRP 的啓用與停用（全區設定）

GVRP (GARP VLAN Registration Protocol, GARP VLAN 註冊通訊協定) 爲交換器定義了一種彼此交換 VLAN 資訊的方式, 以便在網路其它地方的連接埠上註冊 VLAN 成員。VLAN 是根據主機裝置所發出並在網路上傳遞的參加訊息動態設定的。您必須先啓動 GVRP, 自動 VLAN 註冊功能才會運作, 而且也才能支援交換器本身以外的 VLAN。

**Web** – 打開 Switch Config=>VLAN。啓用或停用 GVRP, 按下「Save」。



**CLI** – 以下示範啓用交換器 GVRP 的方式。

```
Console(config)#bridge-ext gvrp
Console(config)#
```

4-118

**SNMP** – 對等 MIB 變數。

欄位名稱	MIB 變數	權限	設定值範圍	預設值
GVRP Status	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qBase. dot1qGvrpStatus	可讀寫	enabled (1), disabled (2)	disabled

### 3.3.1.3

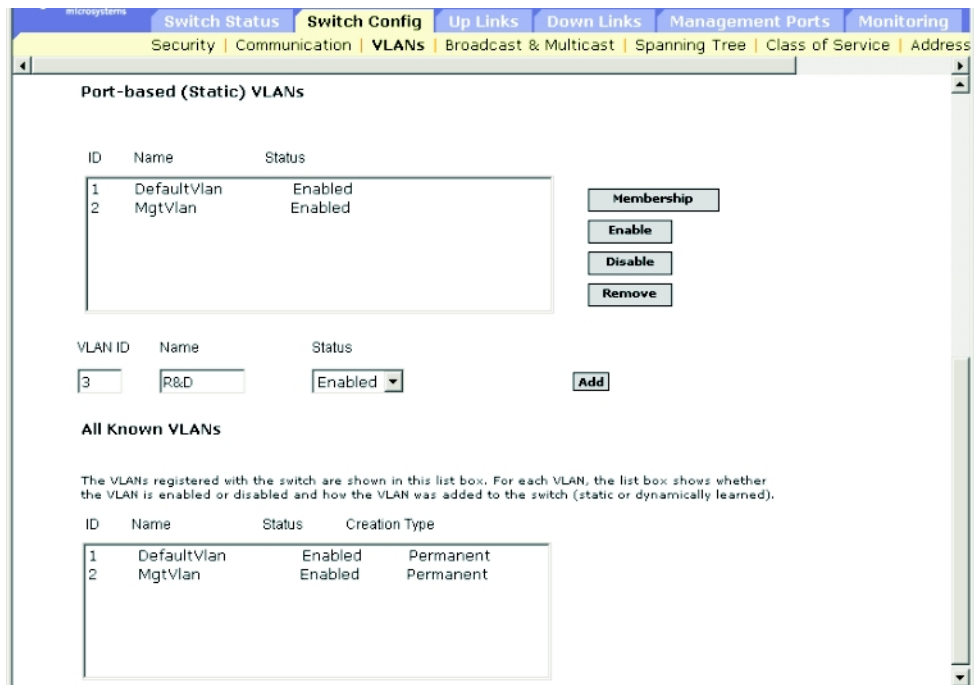
## 設定 VLAN

### 指令屬性

- **ID** – 欲設定之 VLAN 的 ID (1-4094)。
- **Name** – VLAN 的名稱 (可包含 1 到 15 個字元)。
- **Status** – 顯示此 VLAN 已啟用或停用。
  - **Enable** (使用中 \*) – 表示 VLAN 正在運作中。
  - **Disable** (暫停 \*) – 表示 VLAN 暫停運作，也就是不會傳送封包。
- **Creation Type** – 顯示此 VLAN 以何種方式加入此交換器內。
  - **Dynamic GVRP** (動態 \*)：經由 GVRP 自動得知。
  - **Permanent** (靜態 \*)：由管理員手動加入靜態項目。
- **Ports/Channel groups\*** – 顯示此 VLAN 介面所屬成員。

\* 這些項目會顯示在 CLI 上。

**Web** – 打開 Switch Config=>VLAN。新 VLAN 的建立方式如下：先輸入 VLAN 的 ID 與名稱，將狀態設定為 Enabled (啟用) 或 Disabled (停用)，然後按下「Add」即可。若要修改原有的 VLAN，請先選取一或多個項目，接著按下「Enable」、「Disable」或「Remove」。若要將介面接入 VLAN 內，請選取所需項目，然後按下「Membership」。(請參閱第 3-40 頁的「在 VLAN 內加入固定成員」。)



CLI – 以下示範如何建立一個新的 VLAN，並顯示 VLAN 的所有資訊。

```

Console(config)#vlan database 4-105
Console(config-vlan)#vlan 3 name R&D media ethernet state active 4-105
Console(config-vlan)#
Console#show vlan 4-113
VLAN Type Name Status Ports/Channel groups
-----
1 Static DefaultVlan Active SNP0 SNP1 SNP2 SNP3 SNP4
SNP5 SNP6 SNP7 SNP8 SNP9
SNP10 SNP11 SNP12 SNP13 SNP14
SNP15 NETP0 NETP1 NETP2 NETP3
NETP4 NETP5 NETP6 NETP7
2 Static MgtVlan Active NETMGT
3 Static R&D Active
Console#

```

SNMP – 對等 MIB 變數。

欄位名稱	MIB 變數	權限	設定值範圍	預設值
VLAN ID	MIB-II.dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanCurrentTable. dot1qVlanCurrentEntry. dot1qVlanIndex	不提供外界 存取	整數	1
VLAN Name	MIB-II.dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanStaticName	讀取/建立	二進位字串 (長度 0-32)	
VLAN Status	MIB-II.dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanStatic. RowStatus	讀取/建立	enable (1), disable (2)	
VLAN Type	MIB-II.dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanCurrentTable. dot1qVlanCurrentEntry. dot1qVlanStatus	唯讀	other (1), permanent (2), dynamicGvrp (3)	

欄位名稱	MIB 變數	權限	設定值範圍	預設值
VLAN Ports	MIB-II.dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanCurrentTable. dot1qVlanCurrentEntry. dot1qVlanCurrent- EgressPorts	唯讀	二進位字串 (連接埠清單)	

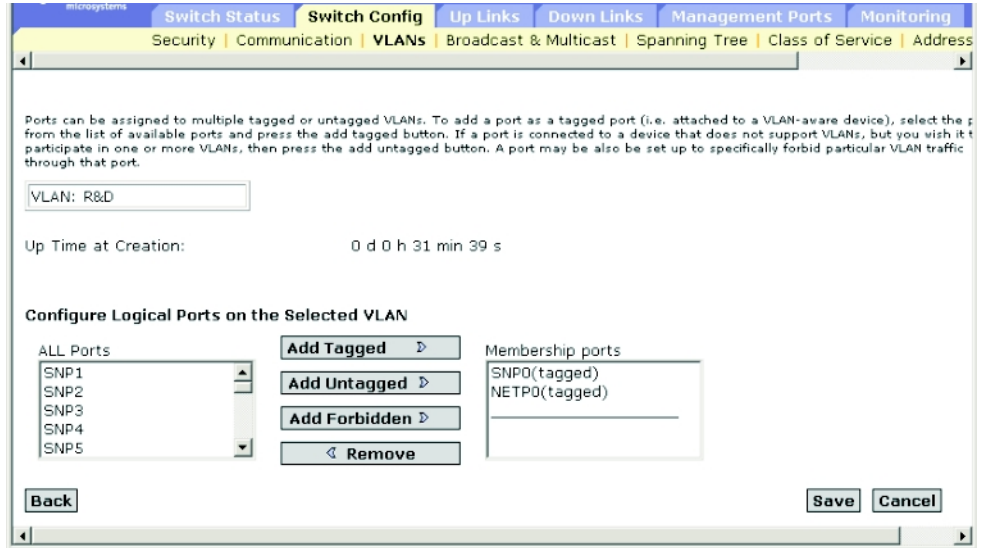
### 3.3.1.4 在 VLAN 內加入固定成員

#### 指令屬性

- **Name** – 此 VLAN 的名稱。
- **Up Time at Creation** – 此 VLAN 的建立時間。
- **Status\*** – 顯示此 VLAN 以何種方式加入此交換器內。
  - **Dynamic**：經由 GVRP 自動得知。
  - **Static**：由管理員手動加入靜態項目。
- **All Ports** – 連接埠或寬道識別碼。
- **Membership Ports** – 加入選定 VLAN 的介面，可能會加註標籤，也可能不會，或限制介面不得自動透過 GVRP 加入。
- **Membership Type** – 設定 VLAN 所屬成員，請選取所需介面，然後按下適當的「Add」按鈕：
  - **Add Tagged**：介面是 VLAN 的成員之一，凡是此 VLAN 上的連接埠傳送的封包都會被加上標籤，使其帶有 VLAN 或 CoS 資訊。
  - **Add Untagged**：介面是 VLAN 的成員之一，凡是此 VLAN 上的連接埠傳送的封包都不會加上標籤，因此不帶有 VLAN 或 CoS 資訊。
  - **Add Forbidden**：介面禁止自動透過 GVRP 加入此 VLAN 內。請參閱第 3-33 頁中關於自動 VLAN 註冊的說明。
  - **Remove**：將選定介面從此 VLAN 中移除。

\* 僅適用於 CLI。

**Web** – 打開 Switch Config=>VLAN。從固定清單中選取一個 VLAN，接著按下「Membership」。在連接埠隸屬關係網頁上，從「All Ports」清單（包括連接埠與寬道）中選出一個介面，接著按下「Add Tagged」、「Add Untagged」或「Add Forbidden」（禁止此介面透過 GVRP 加入）。若要刪除某個介面，請從「Membership Ports」清單中選出該介面，然後按下「Remove」即可。



**CLI** – 以下示範如何加入數個介面，並顯示此 VLAN 所含的成員。

```

Console(config)#interface ethernet NETP1                                4-74
Console(config-if)#switchport allowed vlan add 3 tagged                4-111
Console(config-if)#exit
Console(config)#interface ethernet NETP2
Console(config-if)#switchport allowed vlan add 3 untagged
Console(config-if)#exit
Console(config)#interface ethernet SNP13
Console(config-if)#switchport forbidden vlan add 3
Console(config-if)#end
Console#show vlan id 3
VLAN Type      Name                Status        Ports/Channel groups
-----
      3 Static                R&D           Active        NETP1  NETP2
Console#

```

## SNMP – 對等 MIB 變數。

欄位名稱	MIB 變數	權限	設定值範圍	預設值
VLAN ID	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanIndex	索引	列	
VLAN Name	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanStaticName	讀取/建立	二進位字串 (長度 0-32)	
Up Time at Creation	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanCurrentTable. dot1qVlanCurrentEntry. dot1qVlanCreationTime	唯讀	時間 (以百分之一秒 為單位)	
VLAN Status	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanCurrentTable. dot1qVlanCurrentEntry. dot1qVlanStatus	唯讀	other (1), permanent (2), dynamicGvrp (3)	
Tagged Ports, Untagged Ports (Allowed VLAN)	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanTable. dot1qVlanEntry. dot1qVlanStatic- UntaggedPorts	讀取/建立	二進位字串 (連接埠清單)	

欄位名稱	MIB 變數	權限	設定值範圍	預設值
VLAN Forbidden Ports	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qPortVlanTable. dot1qPortVlanEntry. dot1qVlanForbidden- EgressPorts	讀取/建立	二進位字串 (連接埠清單)	
Port Trunk Index (Channel Groups)	sun... portMgt. portTable portEntry. portTrunkIndex	唯讀	整數	
VLAN Static Row Status	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanStatic- RowStatus	讀取/建立	enable(1), disable(2)	

### 3.3.2 群組廣播組態

群組廣播是用來支援視訊會議以及串流音訊之類的即時應用。群組廣播伺服器不需要與每個用戶端分別建立連線，只要將其服務廣播到網路上，而想要接收此群組廣播服務的主機則必須向其群組廣播交換器/路由器註冊。雖然這種方法可以降低群組廣播伺服器網路負荷量，但群組廣播流量流經的每一台群組廣播交換器/路由器卻必須謹慎處理這些資料，確保只將這些流量傳給有登記需此服務的主機。

本交換器使用 IGMP (Internet Group Management Protocol, 網際網路群組管理通訊協定) 詢問其所連接且要接收特定群組廣播服務的所有主機。交換器會找出要求加入此服務之主機所連的連接埠，然後只會將相關資料傳到這些連接埠而已。此外，交換器還會將服務要求傳送給相連的群組廣播交換器/路由器，確保本身也會繼續收到群組廣播服務。此程序稱為群組廣播過濾。

IP 群組廣播過濾的目的在於讓交換網路的效能達到最佳狀態，因此群組廣播封包並不會傳給子網路 (VLAN) 中的所有連接埠，只會傳給含有群組廣播主機或路由器/交換器的連接埠而已。

### 3.3.2.1 設定 IGMP Snooping 參數

此交換器可以設定成用比較聰明的方法轉送群組廣播流量，讓交換器根據 IGMP 查詢與回報訊息，只將相關流量轉送給要求群組廣播流量的連接埠，避免交換器將流量發送到所有連接埠上，導致網路效能大幅下降。

#### 指令使用方式

- **IGMP Snooping** – 此交換器能被動窺探 IP 群組廣播路由器/交換器與 IP 群組廣播主機群組之間傳遞的 IGMP 查詢與回報封包，並據此找出 IP 群組廣播中各群組的成員。方法很簡單，交換器只要監視流過的 IGMP 封包，將其中的群組註冊資訊取出，然後據以設定群組廣播過濾器即可。
- **IGMP Querier** – 指的是會定期詢問其所連接各台主機是否要接收群組廣播流量的路由器或具有群組廣播能力的交換器。若 LAN 中負責 IP 群組廣播的路由器/交換器不只一台，則這些裝置會合力選出其中一台當作「查詢者」，負責詢問 LAN 中各主機要加入哪些群組，並將服務要求轉送到任何上連的群組廣播交換器/路由器，確保本身會繼續收到群組廣播服務。

---

**注意：**群組廣播路由器利用這些資訊，再加上 DVMRP 之類的群組廣播路由協定，便可提供跨越網際網路的 IP 群組廣播功能。

---

#### 指令屬性

- **IGMP Snooping** — 此功能啓用後，交換器便會監視網路流量，以找出哪些主機想要接收群組廣播流量。(預設值：停用)
- **IGMP Protocol Version** — 設定通訊協定版本，以便與網路上其他裝置相容。(預設值：2，可用範圍：1-2)
- **IGMP Querier** — 此功能啓用後，交換器便會擔任查詢者的角色，負責詢問所有主機是否要接收群組廣播流量。(預設值：停用)
  - **Query Count** — 設定查詢者應該連續發出多少個查詢，且該用戶端都沒有回應的狀況下，才可決定將該用戶端從廣播群組中去除。(預設值：2，可用範圍：2-10)
  - **Query Interval** — 設定交換器發出 IGMP 主機詢問訊息的頻率。(預設值：125 秒，可用範圍：60-125)
  - **Query Report Delay** — 設定交換器從連接埠收到某個 IP 群組廣播位址的 IGMP 回報訊息後，應該等待多久時間，才可以從同一個連接埠發出 IGMP 詢問訊息，並將該項目從清單中除去。(預設值：10 秒，可用範圍：5-25)
  - **Router Port Expire Time** — 自從最近一次查詢者停止發送詢問訊息之後，交換器應該等待多少時間，才可以判定先前都持續收到查詢者發出之詢問封包的介面已經失去與查詢者的連線了。(預設值：300 秒，可用範圍：300-500)

---

**注意：**子網路上的所有系統都必須採用相同的版本。某些屬性只有 IGMPv2 才支援，包括 IGMP Report Delay 與 Router Port Expire Time。

---



Web – 按下 Switch Config=>Broadcast & Multicast=>IGMP Parameters。視需要調整 IGMP 設定，然後按下「Save」。

The screenshot shows the Mikrotik web interface for configuring IGMP parameters. The breadcrumb navigation is: Sun Fire B1600 > Switch Config > Broadcast & Multicast. The 'View' dropdown is set to 'IGMP Parameters'. The main heading is 'Configuring IGMP Parameters'. Below this, there is a note: 'To configure the switch to use IGMP (Internet Group Management Protocol) for multicast filtering, you will need to enable IGMP Snooping. You can also configure the switch to act as an IGMP Querier, which will make it responsible for propagating multicast traffic to other switches or routers on the network.' The configuration options are: 'IGMP Snooping Enabled' (checked), 'IGMP Protocol Version' (radio buttons for 'Version 2' and 'Version 1', with 'Version 2' selected), 'IGMP Querier Enabled' (checked), and four input fields: 'Query Count (1-2):' (10), 'Query Interval(60-125)secs:' (100), 'Query Report Delay (5-30)secs:' (20), and 'Router Port Expire Time (300-500)secs:' (300). At the bottom right, there are 'Save' and 'Cancel' buttons.

View : IGMP Parameters

### Configuring IGMP Parameters

To configure the switch to use IGMP (Internet Group Management Protocol) for multicast filtering, you will need to enable IGMP Snooping. You can also configure the switch to act as an IGMP Querier, which will make it responsible for propagating multicast traffic to other switches or routers on the network.

IGMP Snooping Enabled

IGMP Protocol Version

Version 2

Version 1

IGMP Querier Enabled

Query Count (1-2):

Query Interval(60-125)secs:

Query Report Delay (5-30)secs:

Router Port Expire Time (300-500)secs:

CLI – 以下示範如何修改群組廣播過濾功能的設定值，並顯示出目前的狀態。

```

Console(config)#ip igmp snooping 4-121
Console(config)#ip igmp snooping querier 4-124
Console(config)#ip igmp snooping query-count 10 4-125
Console(config)#ip igmp snooping query-interval 100 4-126
Console(config)#ip igmp snooping query-max-response-time 20 4-127
Console(config)#ip igmp router-port-expire-time 300 4-128
Console(config)#ip igmp snooping version 2 4-122
Console(config)#exit
Console#show ip igmp snooping 4-123
  Igmp Snooping Configuration
-----
Service status          : Enabled
Querier status          : Enabled
Query count              : 10
Query interval          : 100 sec
Query max response time : 20 sec
Query time-out          : 300 sec
IGMP snooping version   : Version 2
Console#

```

SNMP – 對等 MIB 變數。

欄位名稱	MIB 變數	權限	設定值範圍	預設值
Snooping Status	sun... igmpSnoopMgt. igmpSnoopStatus	可讀寫	enabled (1), disabled (2)	enabled
Snooping Querier	sun... igmpSnoopMgt. igmpSnoopQuerier	可讀寫	enabled (1), disabled (2)	enabled
Snooping Query Count	sun... igmpSnoopMgt. igmpSnoopQueryCount	可讀寫	整數 (2-10)	2
Snooping Query Interval	sun... igmpSnoopMgt. igmpSnoop- QueryInterval	可讀寫	整數 (60-125) 秒	125
Snooping Query Max Response Time	sun... igmpSnoopMgt. igmpSnoopQuery- MaxResponseTime	可讀寫	整數 (5-25) 秒	10

欄位名稱	MIB 變數	權限	設定值範圍	預設值
Snooping Router Port Expire Time	sun... igmpSnoopMgt. igmpSnoopRouterPort- ExpireTime	可讀寫	整數 (300-500) 秒	300
Snooping Version	sun... igmpSnoopMgt. igmpSnoopVersion	可讀寫	整數 (1-2)	2

### 3.3.2.2 設定與群組廣播路由器連接的介面

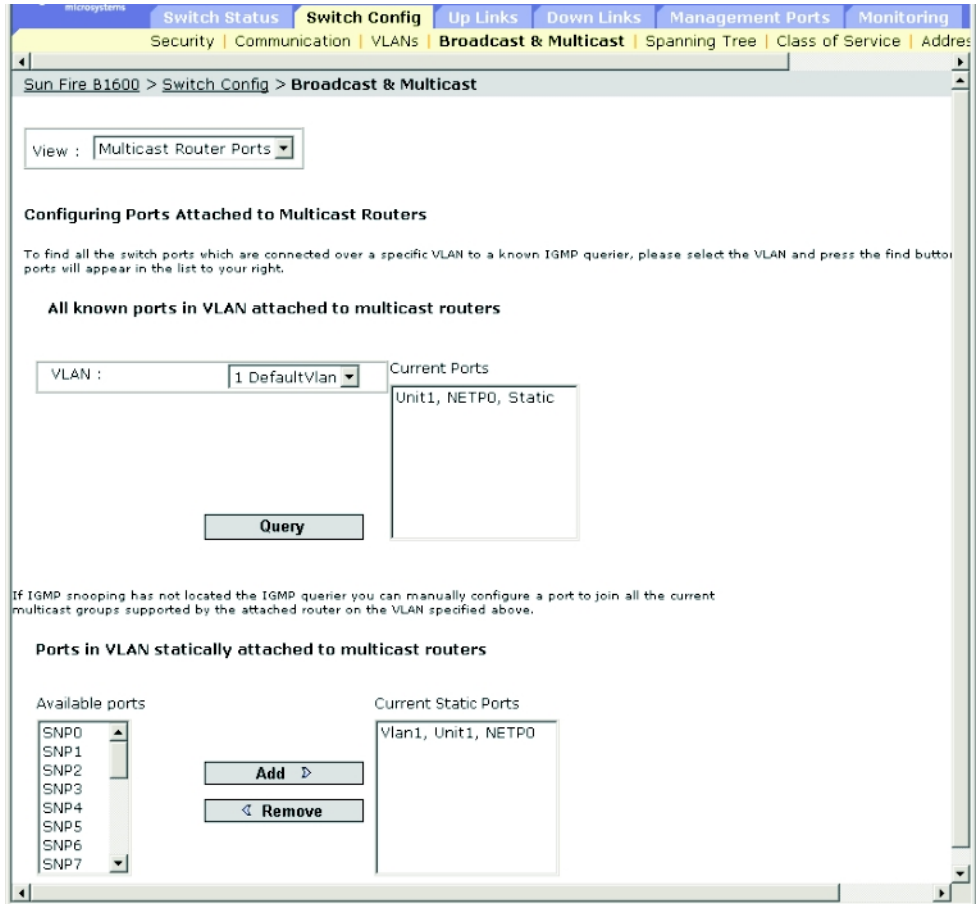
群組廣播使用從 IGMP 獲得的資訊，以及 DVMRP 之類的群組廣播路由協定，提供跨越網際網路的 IP 群組廣播功能。交換器可用動態的方式逐漸得知這些路由器的存在，亦可經由人為方式設定交換器的哪些介面連接這些路由器。

由於網路連線的變化很大，因此 IGMP 窺探方式不見得能夠找出 IGMP 查詢者。因此若事先就知道 IGMP 查詢者是網路上哪一台群組廣播路由器/交換器，而且知道連在交換器的哪個介面（連接埠或寬道）上，就可以手動將此介面（以及指定的 VLAN）設定成加入該路由器目前支援的所有廣播群組，確保其群組廣播流量一定會傳到交換器中所有適當的介面上。

#### 指令屬性

- VLAN 中所有已知與群組廣播路由器相連的連接埠 –
  - **VLAN** – 選取此交換器上的一個 VLAN。（下拉式清單中含有 VLAN 的 ID 與名稱。）
  - **Interface** – 顯示與群組廣播路由器相連的介面，以及此設定是經由手動方式 (Static) 或動態方式 (IGMP) 達成。
- VLAN 中固定與群組廣播路由器相連的連接埠 –
  - **Available Ports** – 顯示尚未加入選定 VLAN 中當作群組廣播路由器連接埠的介面。
  - **Current Static Ports** – 顯示已加入選定 VLAN 中當作群組廣播路由器連接埠的介面。

**Web** – 按下 Switch Config=>Broadcast & Multicast=>Multicast Router Ports。選取一個 VLAN，接著按「Query」顯示 VLAN 中與群組廣播路由器相連的所有介面，或用「Add」與「Remove」按鈕直接設定與群組廣播路由器相連的介面。



**CLI** – 以下示範如何將 NETP0 連接埠設定成 VLAN 1 中的群組廣播路由器連接埠。

```

Console(config)#ip igmp snooping vlan 1 mrouter ethernet NETP0 4-129
Console(config)#exit
Console#show ip igmp snooping mrouter vlan 1 4-130
VLAN M'cast Router Port Type
-----
1 NETP0 Static
    
```

## SNMP – 對等 MIB 變數。

欄位名稱	MIB 變數	權限	設定值範圍
Snooping Multicast Router Current VLAN	sun... igmpSnoopMgt. igmpSnoopRouterCurrentTable. igmpSnoopRouterCurrentEntry. dot1qVlanIndex	索引	整數
VLAN Name	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanStaticName	讀取/建立	二進位字串 (長度 0-32)
Snooping Multicast Router Current Ports	sun... igmpSnoopMgt. igmpSnoopRouterCurrentTable. igmpSnoopRouterCurrentEntry. igmpSnoopRouterCurrentPorts	唯讀	二進位字串 (連接埠清單)
Snooping Multicast Router Static Vlan Index	sun... igmpSnoopMgt. igmpSnoopRouterStaticTable. igmpSnoopRouterStaticEntry. dot1qVlanIndex	索引	整數
Snooping Multicast Router Static Ports	sun... igmpSnoopMgt. igmpSnoopRouterStaticTable. igmpSnoopRouterStaticEntry. igmpSnoopRouterStaticPorts	讀取/建立	二進位字串 (連接埠清單)
Snooping Multicast Router Static Status	sun... igmpSnoopMgt. igmpSnoopRouterStaticTable. igmpSnoopRouterStaticEntry. igmpSnoopRouterStaticStatus	讀取/建立	valid (1), invalid (2)

### 3.3.2.3 設定群組廣播服務

群組廣播過濾功能可以用 IGMP 窺探與 IGMP 詢問訊息動態設定，如第 3-44 頁的「設定 IGMP Snooping 參數」所述。對於需要更細緻控制的用途，就必須手動設定特定介面的群組廣播服務。首先需將欲加入廣播群組之主機所連的全部連接埠加入同一個 VLAN 內，然後將群組廣播服務指定給此 VLAN 群組即可。

#### 指令使用方式

- 靜態群組廣播位址永遠不會過期。
- 當某個群組廣播位址以靜態方式加入某個 VLAN 中的某個介面時，相對應的流量就只能轉送給該 VLAN 中的連接埠。

#### 指令屬性

- VLAN 上所有已知連接埠以及所支援的群組廣播服務 –
  - **VLAN** – 選取此交換器上的一個 VLAN。  
(下拉式清單中含有 VLAN 的 ID 與名稱。)
  - **IP Address** – 特定群組廣播服務的 IP 位址。
  - **Interface** – 顯示與群組廣播路由器相連的介面，以及此項設定是以靜態 (User) 或動態 (IGMP) 的方式達成。
- VLAN 上靜態設定的連接埠與群組廣播服務 –
  - **IP Address** – 特定群組廣播服務的 IP 位址。
  - **Available Ports** – 顯示尚未指定給選定 VLAN 支援特定群組廣播服務的介面。
  - **Current Static Ports (IP Addresses)** – 顯示已指定給選定 VLAN 負責傳遞特定群組廣播服務的介面，同時還會顯示指定給此介面的 IP 位址。

**Web** – 按下 Switch Config=>Broadcast & Multicast=>Multicast Support。若要顯示負責傳遞特定群組廣播服務的交換器介面，請先從下拉式清單中選出該群組廣播服務的 VLAN ID 與 IP 位址，然後按下「Query」即可。若要手動將群組廣播服務設定到某個介面上，請從下拉式清單中選出一個 VLAN，接著在文字方塊內輸入該群組廣播服務的 IP 位址，然後按下「Add」即可。

The screenshot shows the 'Multicast Services' configuration page in a web browser. The breadcrumb trail is: Security | Communication | VLANs | Broadcast & Multicast | Spanning Tree | Class of Service | Addressing. The 'View' dropdown is set to 'Multicast Services'. The page title is 'Configuring Multicast Services'. A sub-header reads: 'All known ports and muticast Services supported on VLAN'. Below this, there are two input fields: 'VLAN :' with a dropdown menu showing '1 DefaultVlan', and 'IP Address:' with a dropdown menu showing '224.0.1.3'. To the right of these fields is a 'Ports Creation Type' dropdown menu with the value 'Unit1,NETP0, User'. A 'Query' button is located below the input fields. Below the 'Query' button, there is a section titled 'Ports and multicast services statically configured on VLAN'. This section contains three main components: 'Available Ports' (a list box with items SNP0 through SNP7), 'IP Address:' (a text input field containing '0.0.0.0'), and 'Current Static Ports (IP Addresses)' (a text area containing 'VLAN 1, 224.0.1.3, Unit 1, NETP0'). There are 'Add' and 'Remove' buttons between the 'Available Ports' and 'IP Address' fields.

**注意：**若出現的錯誤訊息表示您輸入的資料不正確，請檢查您設定的每個 IP 位址是否正確。

**CLI** – 以下示範如何將一個群組廣播位址設定給 NETP0 連接埠，並將 VLAN 1 上支援的所有已知群組廣播服務顯示出來。

```

Console(config)#ip igmp snooping vlan 1 static 224.0.0.12 ethernet NETP0 4-122
Console(config)#exit
Console#show mac-address-table multicast vlan 1 4-124
  VLAN M'cast IP addr. Member ports Type
  ----
    1      224.0.0.12      NETP1    IGMP
    1      224.1.2.3       NETP0    USER
Console#

```

**SNMP** – 對等 MIB 變數。

欄位名稱	MIB 變數	權限	設定值範圍
Snooping Multicast Router Static Vlan Index	sun... igmpSnoopMgt. igmpSnoopMulticastStaticTable. igmpSnoopMulticastStaticEntry. dot1qVlanIndex	索引	整數
Snooping Multicast Static IP Address	sun... igmpSnoopMgt. igmpSnoopMulticastStaticTable. igmpSnoopMulticastStaticEntry. igmpSnoopMulticastStaticIPAddress	索引	IP 位址
Snooping Multicast Static Port List	sun... igmpSnoopMgt. igmpSnoopMulticastStaticTable. igmpSnoopMulticastStaticEntry. igmpSnoopMulticastStaticPorts	讀取/建立	二進位字串 ( 連接埠清單 )
Snooping Multicast Router Static Status	sun... igmpSnoopMgt. igmpSnoopRouterStaticTable. igmpSnoopRouterStaticEntry. igmpSnoopRouterStaticStatus	讀取/建立	valid (1), invalid (2)



### 3.3.3 廣播風暴控制 (全區設定)

當網路上有裝置故障、軟體設計不當或組態設定錯誤時，就有可能發生廣播風暴。萬一網路上的廣播流量過多，效能便有可能嚴重下降，導致所有設備都無法透過網路傳送資料。

爲了保護網路不受廣播風暴影響，請在每個連接埠上都設定廣播流量的上限，然後在必要的連接埠上啓動廣播風暴控制功能。

只要超過預先設定的流量上限，所有廣播封包都會被丟棄。

#### 指令使用方式

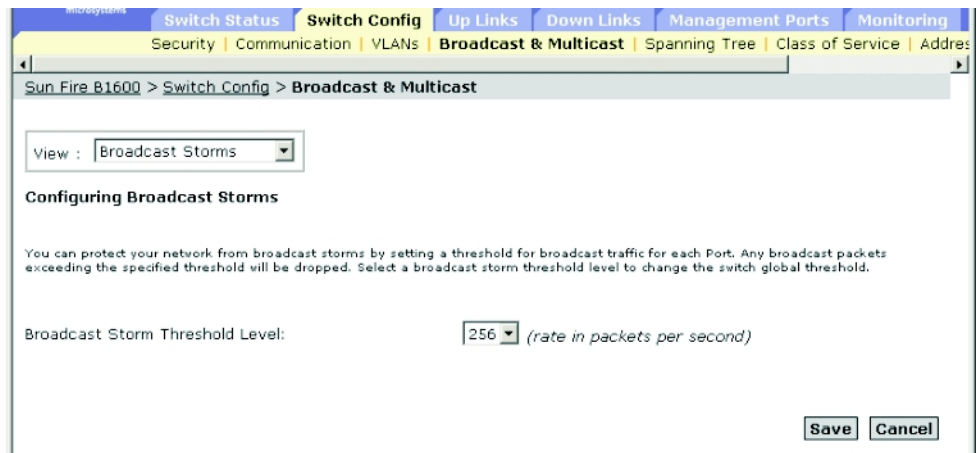
- 廣播風暴控制功能預設已經啓用。
- 廣播控制功能對 IP 群組廣播流量無任何影響。

#### 指令屬性

- **Broadcast Storm Threshold Level\*** – 流量上限，以每秒鐘的封包個數爲單位。(範圍：16、64、128、256，預設值：256)

\* CLI 顯示的是 Broadcast Storm Limit。

**Web** – 打開 Switch Config=>Broadcast & Multicast=>Broadcast Parameters。設定流量上限，然後按下「Save」。



CLI – 以下示範如何將廣播流量上限設定為每秒鐘 64 個封包。

**注意：**請注意 **switchport broadcast** 指令會啓動指定介面上的廣播風暴控制功能，並為交換器上的每個介面設定其廣播流量上限。

```

Console(config)#interface ethernet NETP7                                4-74
Console(config-if)#switchport broadcast packet-rate 64                 4-80
Console(config-if)#end
Console#show interfaces status ethernet NETP7                          4-81
Information of NETP7
  Basic information:
    Port type: 1000T
    Mac address: 00-00-E8-66-66-83
  Configuration:
    Name:External RJ-45 connector NET7
    Port admin: Up
    Speed-duplex: Auto
    Capabilities: 10half, 10full, 100half, 100full, 1000full,
    Broadcast storm: Enabled
    Broadcast storm limit: 256 packets/second
    Flow control: Disabled
    LACP: Disabled
  Current status:
    Link status: Up
    Port operation status: Up
    Operation speed-duplex: 1000full
    Flow control type: None
Console#

```

SNMP – 對等 MIB 變數。

欄位名稱	MIB 變數	權限	設定值範圍	預設值
Broadcast Storm Packet Rate	sun... bcastStormMgt. bcastStormTable. bcastStormEntry. bcastStormPktRate	可讀寫	整數 (16、64、128、256)	256
Broadcast Storm Status	sun... bcastStormMgt. bcastStormTable. bcastStormEntry. bcastStormStatus	可讀寫	enabled (1), disabled (2)	enabled

### 3.3.4 設定 Spanning Tree 演算法

Spanning Tree 演算法 (STA) 可用來偵測與切斷網路中行程的迴路，並為交換器、橋接器與路由器之間提供備援線路，讓交換器得以與網路上的其它橋接裝置 (即具有 STA 功能的交換器、橋接器或路由器) 協調搭配，確保網路中任何兩點之間只有一條路由存在，而且萬一這條主要路由斷掉時，還會自動接起一條備援路由予以取代。

本交換器支援以下幾個版本的 spanning tree 演算法：

- STP – Spanning Tree 通訊協定 (IEEE 802.1D)
- RSTP – 快速 Spanning Tree 通訊協定 (IEEE 802.1w)

RSTP 是爲了全面取代速度較慢且已經不符現況的 STP 而設計的。由於 RSTP 會在使用中連接埠開始學習之前便將狀態變動次數降低，預先定出節點或連接埠故障時可使用的備用路由，並爲組態重新調整時對樹狀結構變動不敏感的連接埠保留轉送資料庫，因此其組態重新調整的速度比 STP 快上許多，約只需要 STP 所花的十分之一時間而已。

#### 3.3.4.1 設定基本 STA 組態

全區設定對整個交換器都有作用。

##### 指令使用方式

- 快速 Spanning Tree 通訊協定

RSTP 會監視收到的通訊協定訊息，並動態調整 RSTP 節點傳送的通訊協定訊息類別，因此無論連接的節點支援 STP 或 RSTP 都能支援，詳細運作狀況如下所述：

- STP Mode – 若連接埠的移轉延遲計時器終止後，交換器收到 802.1D 的 BPDU (即 STP BPDU)，交換器便會假設自己是連到 802.1D 的橋接器，以後就只會使用 802.1D 的 BPDU。
- RSTP Mode – 若 RSTP 原本在某個連接埠上使用的是 802.1D BPDU，但在移轉延遲時間到期之後，卻收到 RSTP BPDU，則 RSTP 就會重新啓動移轉延遲計時器，並開始在此連接埠上使用 RSTP BPDU。

## 指令屬性

### 全區設定的基本組態

以下列出可設定的全區屬性：

- **Enable Spanning Tree** – 啓用/停用此交換器上的 STA 功能。
- **Spanning Tree 通訊協定** – 設定此交換器上使用哪一種 spanning tree：
  - **STP**：Spanning Tree 通訊協定 (IEEE 802.1D，換句話說，選取這個選項後，交換器便會使用設定成 STP 強迫相容模式的 RSTP)
  - **RSTP**：快速 Spanning Tree (IEEE 802.1w)

以下全區屬性均已固定且無法更改：

- **Bridge ID** – 此裝置的優先等級與 MAC 位址。
- **Designated Root** – Spanning Tree 中被交換器接受作為根裝置的優先等級與 MAC 位址。
  - **Root Port** – 此交換器上與根最接近之連接埠的編號。交換器透過這個連接埠與根裝置互傳資料。若沒有根連接埠，代表此交換器已經被當作整個 spanning tree 網路的根裝置。
  - **Root Path Cost** – 從交換器根連接埠到根裝置的路徑成本。
  - **Root Hello Time** – 此裝置每隔多久 (以秒為單位) 會傳送一個組態訊息。
  - **Root Maximum Age** – 此裝置應該等待多久時間 (以秒為單位) 沒收到組態訊息之後，才開始重新設定組態。所有裝置連接埠 (除了指定的連接埠之外) 都應該定時收到組態訊息。萬一原來的根連接埠上次發出之組態訊息中的 STA 訊息超過時限，則此網路中的所有裝置連接埠便會重新選出一個新的根連接埠。(本小節中所提「連接埠」指的是「介面」，連接埠與寬道均包含在內。)
  - **Root Forward Delay** – 此裝置應等待多久時間 (以秒為單位) 後，才可以開始改變狀態 (即丟棄原有資料，開始學習轉送所需的資訊)。由於每個裝置都必須先接收網路拓樸的變化資訊，才能開始轉送封包，因此這項延遲時間是有必要的。此外，每個連接埠也都需要時間觀察可能會導致其回到丟棄狀態的衝突資訊，否則網路中便有可能出現暫時性的資料迴路。
  - **Root Hold Time** – 節點在此處設定的這段時間 (以秒為單位) 內，不得發送兩個以上的橋接器組態通訊協定資料單元。

## 根裝置組態

以下列出可設定的全區屬性：

- **Priority** – 橋接器優先等級是用來選取根裝置、根連接埠與指定連接埠的。擁有最高優先等級的裝置，便成為 STA 的根裝置。如果所有裝置的優先等級都相同，則以 MAC 位址最低的裝置當作根裝置。
  - 預設值：32768
  - 範圍：0-61440，以 4096 遞增
  - 選項：0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440
- **Hello Time** – 此裝置每隔多久（以秒為單位）會傳送一個組態訊息。
  - 預設值：2
  - 最小值：1
  - 最大值：10 與  $[(\text{Max. Message Age} / 2) - 1]$  兩者取較低值
- **Maximum Age** – 此裝置應該等待多久時間（以秒為單位）沒收到組態訊息之後，才開始重新設定組態。所有裝置連接埠（除了指定的連接埠之外）都應該定時收到組態訊息。在任何連接埠上，只要最近一次收到之組態訊息中的 STA 資訊過期，便會成為其所連接 LAN 的指定連接埠。如果該連接埠本身又正好是根連接埠，則此網路中所連的裝置連接埠便會再選出一個新的根連接埠。（本小節中所提「連接埠」指的是「介面」，連接埠與寬道均包含在內。）
  - 預設值：20
  - 最小值：6 與  $[2 \times (\text{Hello Time} + 1)]$  兩者取較大值
  - 最大值：40 與  $[2 \times (\text{Forward Delay} - 1)]$  取較低值
- **Forward Delay** – 此裝置應等待多久時間（以秒為單位）後，才可以開始改變狀態（即丟棄原有資料，開始學習轉送所需的資訊）。由於每個裝置都必須先接收網路拓樸的變化資訊，才能開始轉送封包，因此這項延遲時間是有必要的。此外，每個連接埠也都需要時間觀察可能會導致其回到丟棄狀態的衝突資訊，否則網路中便有可能出現暫時性的資料迴路。
  - 預設值：15
  - 最小值：4 與  $[(\text{Max. Message Age} / 2) + 1]$  取較大值
  - 最大值：30

## Spanning Tree 統計數據

以下全區屬性會顯示統計數據（無法更改）：

- **Number of Topology Changes** – 此 spanning tree 重新設定組態的次數。
- **Last Topology Change** – 自從最近一次 spanning tree 重新設定組態之後迄今經過多少時間。

Web – 打開 Switch Config=>Spanning Tree=>Basic Configuration。修改所需的屬性，然後按「Save」。

microsystems

Switch Status | **Switch Config** | Up Links | Down Links | Management Ports | Monitoring

Security | Communication | VLANs | Broadcast & Multicast | **Spanning Tree** | Class of Service | Address

### Spanning Tree

Basic Configuration | [Advanced Configuration](#) | [MST Instance Configuration](#) | [MSTI VLAN Configuration](#)

Enable Spanning Tree

Select Spanning Tree Protocol:

The Spanning Tree root device is selected using the bridge priority and MAC address. If there is no root port, then it has been accepted as the root device.

Bridge ID:	32768.0000E8666672
Designated Root:	32768.0000E8666672
Root Port:	0
Root Path Cost:	0
Root Hello Time (secs):	2
Root Maximum Age (secs):	20
Root Forward Delay (secs):	15
Root Hold Time (secs):	1

#### Root Device Configuration

Priority (0-61440):	<input type="text" value="32768"/>
Hello Time (1-10) secs:	<input type="text" value="2"/>
Maximum Age (6-40) secs:	<input type="text" value="20"/>
Forward Delay (4-30) secs:	<input type="text" value="15"/>

#### Spanning Tree Statistics

Number of Topology Changes:	0
Last Topology Change:	0 d 1 h 12 min 59 s

**注意：**若畫面上出現訊息說您輸入的資料不正確，請檢查您在 Priority、Hello Time、Maximum Age 以及 Forward Delay 中輸入的值是否都在這些參數可接受的範圍內。

CLI – 以下示範如何顯示全區 STA 設定以及每個連接埠的設定。

```
Console#show spanning-tree 4-102
Spanning-tree information
-----
Spanning tree mode           : RSTP
Spanning tree enable/disable : enable
Priority                     : 32768
Bridge Hello Time (sec.)    : 2
Bridge Max Age (sec.)       : 20
Bridge Forward Delay (sec.) : 15
Root Hello Time (sec.)      : 2
Root Max Age (sec.)         : 20
Root Forward Delay (sec.)   : 15
Designated Root             : 32768.0000E8666672
Current root port           : 0
Current root cost           : 0
Number of topology changes  : 0
Last topology changes time (sec.): 9142
Transmission limit         : 3
Path Cost Method            : 4308020
.
.
.
```

**注意：**當此裝置未接上網路時，其目前的根連接埠與根成本都會顯示 0。

以下範例將 `spanning tree` 模式設定為 RSTP，啟動 `spanning tree` 功能，並設定相關屬性。

```
Console(config)#spanning-tree mode rst 4-93
Console(config)#spanning-tree 4-92
Console(config)#spanning-tree priority 40000 4-96
Console(config)#spanning-tree hello-time 5 4-95
Console(config)#spanning-tree max-age 40 4-95
Console(config)#spanning-tree forward-time 20 4-94
Console(config)#
```

SNMP – 對等 MIB 變數。

欄位名稱	MIB 變數	權限	設定值範圍	預設值
STA System Status	sun...staMgt. staSystemStatus	可讀寫	enabled (1), disabled (2)	enabled
STA Protocol Type	sun...staMgt. staProtocolType	可讀寫	stp (1), rstp (2),	rstp
Bridge ID	由橋接器優先等級與 MAC 位址共同組成。			
Designated Root	sun...xstMgt. mstInstanceCfgTable. mstInstanceCfgEntry. mstInstanceCfg- DesignatedRoot	唯讀	八進位字串	
Root Port	sun...xstMgt. mstInstanceCfgTable. mstInstanceCfgEntry. mstInstanceCfgRootPort	唯讀	整數	
Root Cost	sun...xstMgt. mstInstanceCfgTable. mstInstanceCfgEntry. mstInstanceCfgRootCost	唯讀	整數	
Hello Time	sun...staMgt.xstMgt. mstInstanceCfgTable. mstInstanceCfgEntry. mstInstanceCfg- HelloTime	唯讀	整數	200 百分之一秒
Maximum Age	sun...staMgt.xstMgt. mstInstanceCfgTable. mstInstanceCfgEntry. mstInstanceCfgMaxAge	唯讀	整數	2000 百分之一秒
Forward Delay	sun...staMgt.xstMgt. mstInstanceCfgTable. mstInstanceCfgEntry. mstInstanceCfg- ForwardDelay	唯讀	整數	1500 百分之一秒
Priority	sun...staMgt.xstMgt. mstInstanceCfgTable. mstInstanceCfgEntry. mstInstanceCfgPriority	可讀寫	整數 (0-61440)	32768
Bridge Hello Time	MIB-II. dot1dStp. dot1dStp- BridgeHelloTime	可讀寫	整數 (100 到 1000) 百分之一秒	200 百分之一秒



欄位名稱	MIB 變數	權限	設定值範圍	預設值
Bridge Maximum Age	MIB-II. dot1dStp. dot1dStpBridgeMaxAge	可讀寫	整數 (600 到 4000) 百分之一秒	2000 秒
Bridge Forward Delay	MIB-II. dot1dStp. dot1dStp- BridgeForwardDelay	可讀寫	整數 (400 到 3000) 百分之一秒	1500 百分之一秒
STA Configuration Changes	MIB-II. dot1dBridge.dot1dStp. dot1dStpTopChanges	唯讀	計數器	
STA Last Topology Change	MIB-II. dot1dBridge.dot1dStp. dot1dStpTimeSince- TopologyChange	唯讀	整數	

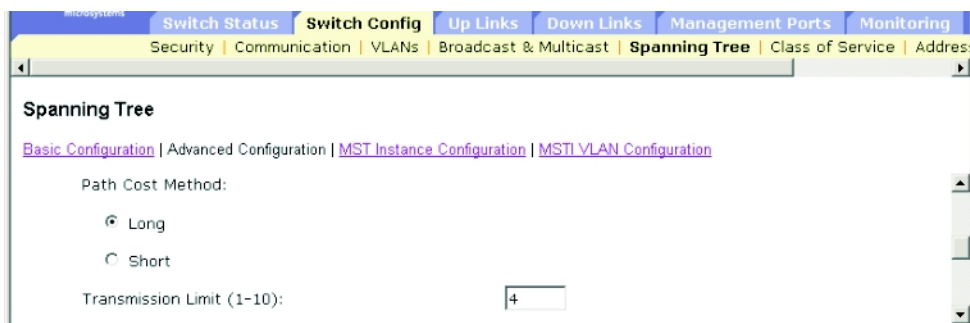
### 3.3.4.2 設定進階 STA 組態

本節說明 RSTP 的進階組態設定。

#### 指令屬性

- **Path Cost Method** – 裝置之間的最佳路徑是根據路徑成本算出來的。每個介面可以設定的成本值範圍，則是根據路徑成本法決定。
  - Long：使用 32 位元的值，範圍從 1 到 200,000,000。
  - Short：使用 16 位元的值，範圍從 1 到 65535。
- **Transmission Limit** – BPDU 的最大傳輸率，可經由設定兩個連續通訊協定訊息之間的最小間隔時間得出。(範圍：1-10，預設值：3)

**Web** – 打開 Switch Config=>Spanning Tree=>Advanced Configuration。修改所需的屬性，然後按「Save」。



---

**注意：**若出現錯誤訊息說您輸入的資料不正確，請檢查您設定的傳輸限制是否在限定範圍內。

---

**CLI** – 以下示範如何設定 **spanning tree** 的路徑成本法以及傳輸限制。

Console(config)#spanning-tree pathcost method long	4-97
Console(config)#spanning-tree transmission-limit 4	4-97
Console(config)#	

**SNMP** – 對等 MIB 變數。

欄位名稱	MIB 變數	權限	設定值範圍	預設值
RSTP Path Cost Method	sun... staMgt. staPathCostMethod	可讀寫	short (1), long (2)	long
RSTP Transmission Hold Count	sun.. staMgt. staTxHoldCount	可讀寫	整數 (1-10)	3

## 3.3.5 服務類別組態

當流量由於網路壅塞而堵在交換器上時，服務類別 (Class of Service，簡稱 CoS) 可用來設定哪些資料封包擁有較高的優先權。本交換器的每個連接埠都有四個優先等級佇列，提供 CoS 功能。位於連接埠較高優先等級佇列中的資料封包會先傳送，然後才輪到較低優先等級佇列中的封包傳送。您可以設定每個介面的預設優先等級，然後將封包優先等級標籤對應到交換器的優先等級佇列。

### 3.3.5.1 設定介面預設優先等級

您可以設定交換器上每個介面的預設連接埠優先等級。以後所有進入此交換器且未加註標籤的封包，都會加上此預設連接埠優先等級的標籤，然後才放入輸出連接埠的適當等級佇列內。

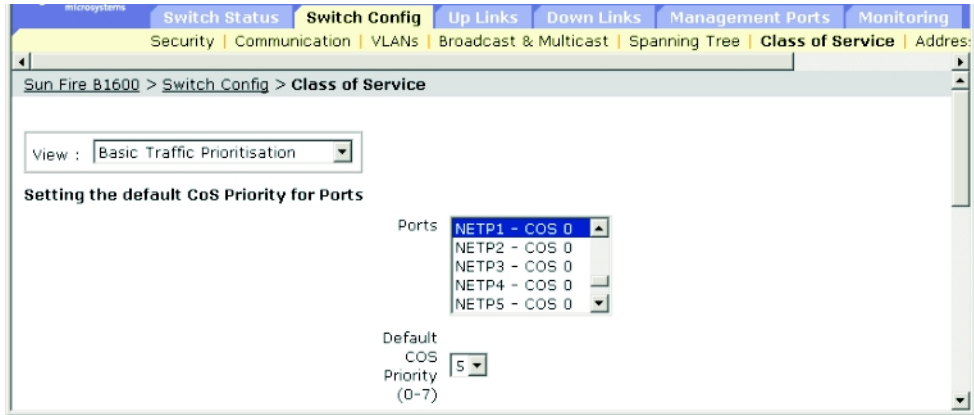
#### 指令使用方式

- 本交換器的每個連接埠都有四個優先等級佇列，並採用權重式巡迴方式避免佇列開頭卡住。
- 當設定成接收所有類型封包（無論封包有無加註標籤均會接收進來）的連接埠收到未加註任何標籤的封包時，便會將此預設優先等級加註在此封包上。不過這項等級設定並不會加在 IEEE 802.1Q VLAN 已加註標籤的封包上。若收到的是 IEEE 802.1Q VLAN 已加註標籤的封包，則會使用 IEEE 802.1p 使用者優先等級 (User Priority) 位元。
- 若輸出連接埠設定成其所屬 VLAN 中不會加註標籤的成員，則這些封包上的 VLAN 標籤便會先全部刪掉，然後才會傳送出去。

#### 指令屬性

- **Ports** – 指已經設定預設服務類別優先等級的介面（包括連接埠與寬道）。
  - **Default COS Priority\*** – 指定介面上所接收之未加註任何標籤封包所使用的優先等級。（範圍：0-7，預設值：0）
- \* CLI 會將此資訊顯示為「Priority for untagged traffic」。

**Web** – 打開 Switch Config=>Class of Service=>Basic Traffic Prioritisation。往下捲動到「Scroll to Setting the Default CoS Priority for Ports」，從「Ports」清單中選出一個介面，修改其預設優先等級，然後按下「Save」。



**CLI** – 以下示範如何將 NETP1 連接埠的預設優先等級設定為 5。

```
Console(config)#interface ethernet NETP1                                4-74
Console(config-if)#switchport priority default 5                       4-132
Console#show interfaces switchport ethernet NETP1                      4-84
Information of NETP1
Broadcast threshold: Enabled, 256 packets/second
Lacp status: Disabled
VLAN membership mode: Hybrid
Ingress rule: Disabled
Acceptable frame type: All frames
Native VLAN: 1
Priority for untagged traffic: 5
Gvrp status: Enabled
Allowed Vlan: 1(u),
Forbidden Vlan:
Console#
```

## SNMP – 對等 MIB 變數。

欄位名稱	MIB 變數	權限	設定值範圍	預設值
Port Default User Priority	MIB-II. dot1dBridge. pBridgeMIB. pBridgeMIBObjects. dot1dPriority. dot1dPortPriorityTable. dot1dPortPriorityEntry. dot1dPortDefault- UserPriority	可讀寫	整數 (0-7)	0

### 3.3.5.2 將 CoS 設定值對應到輸出佇列

此交換器使用每個連接埠的四個優先等級佇列處理加註 CoS 標籤的流量，並採用權重式循環法排定服務先後順序 (參閱第 3-68 頁)。IEEE 802.1p 中定義最多 8 個流量優先等級。預設優先等級是根據 IEEE 802.1p 標準所建議的方式設定，如下表所示。

		佇列			
		0	1	2	3
優先等級	0	0			
	1				
	2				
	3	3			
	4			4	
	5			5	
	6				6
	7				7

下表列出 IEEE 802.1p 標準中建議為各種網路應用設定的優先等級。但是您也可以根據最適合網路流量的方式，將這些優先等級對應到交換器的輸出佇列。

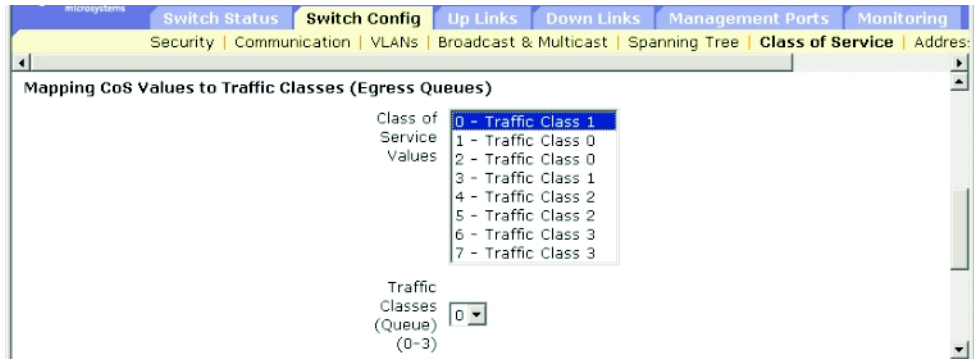
優先等級	流量類別
1	背景流量
2	( 備用 )
0 ( 預設 )	盡力傳送
3	盡全力傳送
4	受控制的負荷量
5	視訊資料，要求延遲與偏移時間不得超過 100 毫秒
6	音訊資料，要求延遲與偏移時間不得超過 10 毫秒
7	網路控制

### 指令屬性

- **Class of Service Values** – CoS 設定值。( 範圍：0-7，以 7 為最高等級 )
- **Traffic Classes (Queue)\*** – 輸出佇列緩衝區。( 範圍：0-3)

\* CLI 會顯示成 Queue ID。

**Web** – 打開 Switch Config=>Class of Service=>Basic Traffic Prioritisation。往下捲動到「Mapping CoS Values to Traffic Classes (Egress Queues)」，從「Class of Service Values」清單中選出一種等級，再從「Traffic Classes」捲動清單中選出一個輸出佇列，然後按下「Save」。



**CLI** – 以下示範如何將 CoS 的值 0、1 與 2 對應到 CoS 優先等級佇列 0，將 3 對應到 CoS 優先等級佇列 1，將 4 和 5 對應到 CoS 優先等級佇列 2，以及將 6 和 7 對應到 CoS 優先等級佇列 3。

```

Console(config)#interface ethernet NETP0                                4-74
Console(config)#queue cos-map 0 0 1 2                                  4-134
Console(config)#queue cos-map 1 3
Console(config)#queue cos-map 2 4 5
Console(config)#queue cos-map 3 6 7
Console(config)#exit
Console#show queue cos-map ethernet NETP0                               4-136
Information of NETP0
Queue ID   Class of service
-----
0         0 1 2
1         3
2         4 5
3         6 7
Console#

```

**SNMP** – 對等 MIB 變數。

欄位名稱	MIB 變數	權限	設定值範圍	預設值
Traffic Class Priority	MIB-II. dot1dBridge. pBridgeMIB. pBridgeMIBObjects. dot1dPriority. dot1dTrafficClassTable. dot1dTrafficClassEntry. dot1dTrafficClassPriority	不可讀取	整數 (0-7)	
Traffic Class	MIB-II. dot1dBridge. pBridgeMIB. pBridgeMIBObjects. dot1dPriority. dot1dTrafficClassTable. dot1dTrafficClassEntry. dot1dTrafficClass	可讀寫	整數 (0-7)	第 3-65 頁

### 3.3.5.3

## 設定流量類別的服務權重

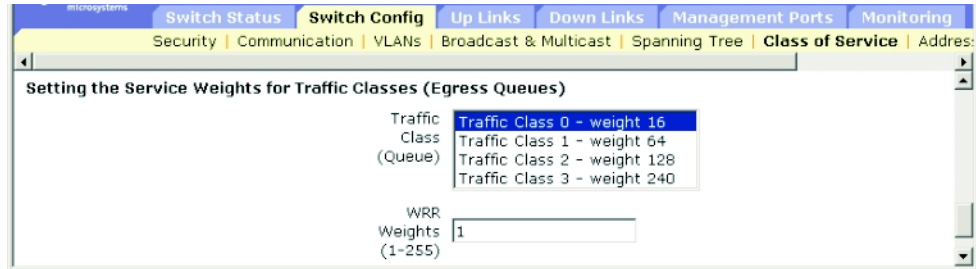
本交換器採用權重式循環 (Weighted Round Robin, 簡稱 WRR) 演算法決定服務每個優先等級佇列的頻率。如第 3-65 頁的「將 CoS 設定值對應到輸出佇列」所述, 各種類別的流量會對應到每個連接埠上四個輸出佇列中的一個。每個佇列都可以設定權重, 如此一來, 其相對的流量也就設定了優先等級。此權重代表了每個佇列輪到被服務的頻率, 從而影響被設定優先等級之軟體應用程式的反應時間。

### 指令屬性

- **Traffic Class (Queue)\*** – 顯示各流量類別的權重。
- **WRR Weights** – 為選定的流量類別設定新的權重。(範圍: 1-255)

\* CLI 會顯示成 Queue ID。

**Web** – 打開 Switch Config=>Class of Service=>Basic Traffic Prioritisation。往下捲到「Setting the Service Weights for Traffic Classes (Egress Queues)」, 選取其中一種流量類別 (即輸出佇列), 輸入權重, 然後按下「Save」。



**CLI** – 以下示範如何將 WRR 權重 1、4、16 與 64 設定給 CoS 優先等級佇列 0、1、2 與 3。

```
Console(config)#queue bandwidth 1 4 16 64          4-133
Console(config)#exit
Console#show queue bandwidth                        4-135
  Queue ID Weight
  -----
      0         1
      1         4
      2        16
      3        64
Console#
```



## SNMP – 對等 MIB 變數。

欄位名稱	MIB 變數	權限	設定值範圍	預設值
WRR Traffic Class (Queue ID)	sun... priorityMgt. prioWrrTable. prioWrrEntry. prioWrrTrafficClass	索引	整數 (0-7)	
WRR Weight	sun... priorityMgt. prioWrrTable. prioWrrEntry. prioWrrWeight	可讀寫	整數 (1-255)	佇列 0 : 16 佇列 1 : 64 佇列 2 : 128 佇列 3 : 240

### 3.3.5.4 將第 3/4 層的優先等級對應到 CoS 設定值

此交換器支援好幾種劃分第 3/4 層流量的常見方法，以符合各種用途的需求。流量優先等級可以用封包 IP 表頭中 ToS (Type of Service, 服務類別) 內的優先等級位元設定。使用這些優先等級位元時，ToS 位元組可能含有 3 個代表 IP 等級的位元，或 6 個代表 DSCP (Differentiated Services Code Point, 差異式服務代碼點) 服務。當這些服務啟動時，交換器便會將各優先順序對應到服務類別設定值，將流量分別送往對應的輸出佇列。

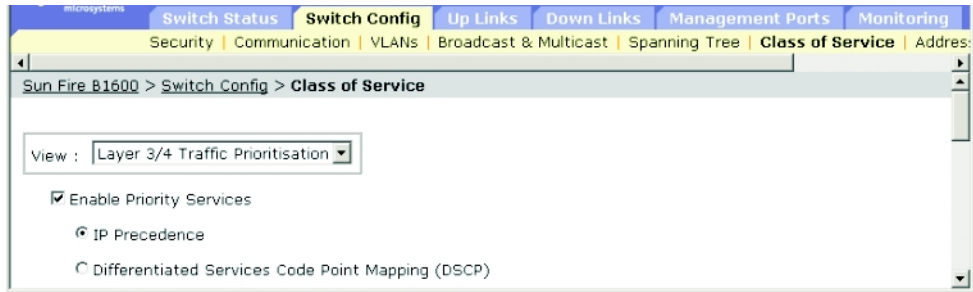
由於網路流量中可能含有不同的優先等級資訊，因此交換器根據以下方式將優先等級設定值對應到輸出佇列：

- 優先等級對應以 IP 優先權或 DSCP 優先等級當作優先權，接著才是預設連接埠優先等級。
- IP 優先權與 DSCP 優先等級兩者不可同時啟用，啟用其中一個之後，另一個就會自動停用。

#### 指令屬性

- **Enable Priority Services** – 您可以啟用或停用將第 3/4 層優先等級對應到 CoS 值的功能。(預設值：停用)
- **IP Precedence** – 使用 IP 優先權對應第 3/4 層優先等級。
- **Differentiated Services Code Point Mapping (DSCP)** – 使用 DSCP 對應第 3/4 層優先等級。

**Web** – 打開 Switch Config=>Class of Service=>Layer 3/4 Traffic Prioritisation。選取「Enable Priority Services」，接著選取 IP Precedence 或 DSCP，最後按下「Save」。



**CLI** – 以下示範如何啟動交換器上的 IP 優先權服務。

```
Console(config)#map ip precedence 4-136
Console(config)#
```

若要將第 3/4 層流量優先等級分配功能全部停用，請使用以下指令。

```
Console(config)#no map ip precedence 4-136
Console(config)#no map ip dscp 4-138
```

**SNMP** – 對等 MIB 變數。

欄位名稱	MIB 變數	權限	設定值範圍	預設值
IP Precedence/ DSCP Status	sun... priorityMgt. prioIpPrecDscpStatus	可讀寫	disabled (1), precedence (2), dscp (3)	disabled

### 3.3.5.5 對應 IP 優先權

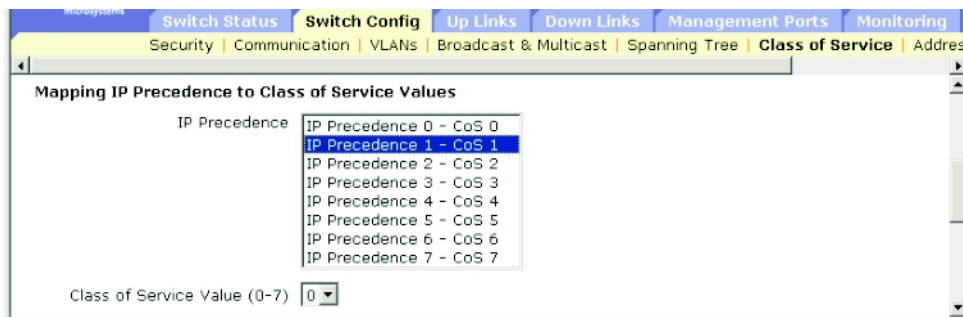
IPv4 表頭中的 ToS (Type of Service, 服務類別) 位元組含有三個優先權位元, 定義了從網路控制用途的最高等級到給一般流量使用的最低等級共 8 個。預設的 IP 優先權設定值是以一對一的方式對應到 CoS 值 (換句話說, 優先權 0 對應到 CoS 0 等等)。第 6 和第 7 位元用於網路控制, 其它位元則用在其他用途。ToS 位元的定義如下表。

優先等級	流量類別
7	網路控制
6	互連網路控制
5	重要
4	Flash Override
3	Flash
2	中等
1	優先等級
0	一般

#### 指令屬性

- **IP Precedence** – 顯示 IP 優先權與 CoS 的對應狀況。
- **Class of Service Value** – 將 CoS 值對應到選定的 IP 優先權設定值。請注意 0 代表最低等級, 7 代表最高等級。

**Web** – 打開 Switch Config=>Class of Service=>Layer 3/4 Traffic Prioritisation。捲動到「Mapping IP Precedence to Class of Service Values」, 從「IP Precedence」表中選出一個項目, 在「Class of Service Value」欄位中輸入設當的值, 然後按下「Save」。



**CLI** – 以下示範如何將 SNP5\* 連接埠上的 IP 優先值 1 對應到 CoS 值，並將該連接埠的所有 IP 優先值設定顯示出來。

```

Console(config)#interface ethernet SNP5                                4-74
Console(config-if)#map ip precedence 1 cos 0                          4-137
Console(config-if)#end
Console#show map ip precedence ethernet SNP5                          4-140
Precedence mapping status: disabled

  Port          Precedence  COS
  -----
      SNP5             0      0
      SNP5             1      0
      SNP5             2      2
      SNP5             3      3
      SNP5             4      4
      SNP5             5      5
      SNP5             6      6
      SNP5             7      7
Console#

```

\* IP 優先權特定值的對應雖然是作成一個介面組態設定指令，但任何更動對於交換器上的所有介面都有效。

### SNMP – 對等 MIB 變數。

欄位名稱	MIB 變數	權限	設定值範圍	預設值
IP Precedence Value	sun... priorityMgt. prioIpPrecTable. prioIpPrecEntry. prioIpPrecValue	不可讀取	整數 (0-7)	
IP Precedence CoS	sun... priorityMgt. prioIpPrecTable. prioIpPrecEntry. prioIpPrecCos	可讀寫	整數 (0-7)	一對一對應

### 3.3.5.6 對應 DSCP 優先等級

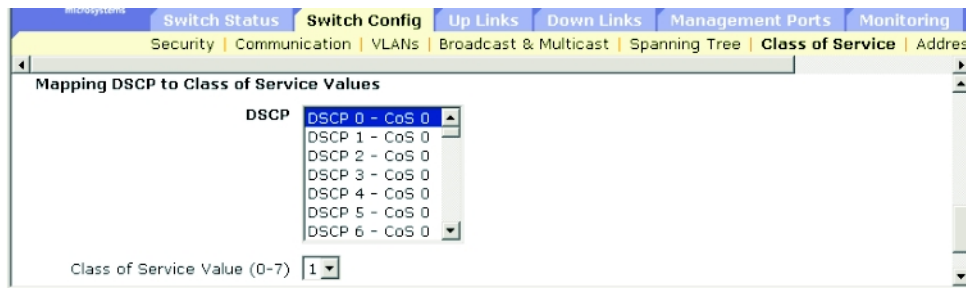
DSCP 有 6 個位元，共可容納 64 種不同的行為。DSCP 雖然取代了 ToS 位元，但仍然保持了 ToS 的三個優先權位元以便與 ToS 相容，讓只看得懂 ToS 但不懂 DSCP 的裝置不會與 DSCP 的對應衝突。不同種類的網路流量可以根據網路政策標示成採用不同的轉送方式。DSCP 的預設值定義如下表所示。請注意，未於下表內定義的所有 DSCP 設定值都會對應成 CoS 值 0。

IP DSCP 值	CoS 值
0	0
8	1
10, 12, 14, 16	2
18, 20, 22, 24	3
26, 28, 30, 32, 34, 36	4
38, 40, 42	5
48	6
46, 56	7

#### 指令屬性

- **DSCP** – 顯示 DSCP 優先等級與 CoS 的對應。
- **Class of Service Value** – 將 CoS 值對應到選定的 DSCP 優先權值。請注意 0 代表最低等級，7 代表最高等級。

**Web** – 打開 Switch Config=>Class of Service=>Layer 3/4 Traffic Prioritisation。捲動到「Mapping DSCP to Class of Service Values」，從「DSCP」表中選取一個項目，在「Class of Service Value」欄位輸入適當的值，然後按下「Save」。



**CLI** – 以下示範如何將 SNP5\* 連接埠上的 DSCP 值 0 對應到 CoS 值 1，並將該連接埠的所有 DSCP 優先等級設定全部顯示出來。

```

Console(config)#interface ethernet SNP5                                4-74
Console(config-if)#map ip dscp 0 cos 1                                4-139
Console(config-if)#end
Console#show map ip dscp ethernet SNP5                                4-141
DSCP mapping status: disabled

  Port          DSCP  COS
  -----
          SNP1    0    1
          SNP1    1    0
          SNP1    2    0
          SNP1    3    0
.
.
.
          SNP1   61    0
          SNP1   62    0
          SNP1   63    0
Console#

```

\* IP DSCP 的對應雖然是作成一個介面組態設定指令，但任何更動對於交換器上的所有介面都有效。

### SNMP – 對等 MIB 變數。

欄位名稱	MIB 變數	權限	設定值範圍	預設值
IP DSCP Value	sun... priorityMgt. prioIpDscpTable. prioIpDscpEntry. prioIpDscpValue	不可讀取	整數 (0-63)	
IP DSCP CoS	sun... priorityMgt. prioIpDscpTable. prioIpDscpEntry. prioIpDscpCos	可讀寫	整數 (0-7)	第 3-73 頁

## 3.3.6 位址表設定

交換器會將所有已知裝置的位址儲存起來，以便利用這些資訊將流量直接轉到各個進出的連接埠上。交換器透過監視網路流量所得知的所有位址，都存放在動態位址表內。您也可以手動將某個靜態位址固定在特定的連接埠上。

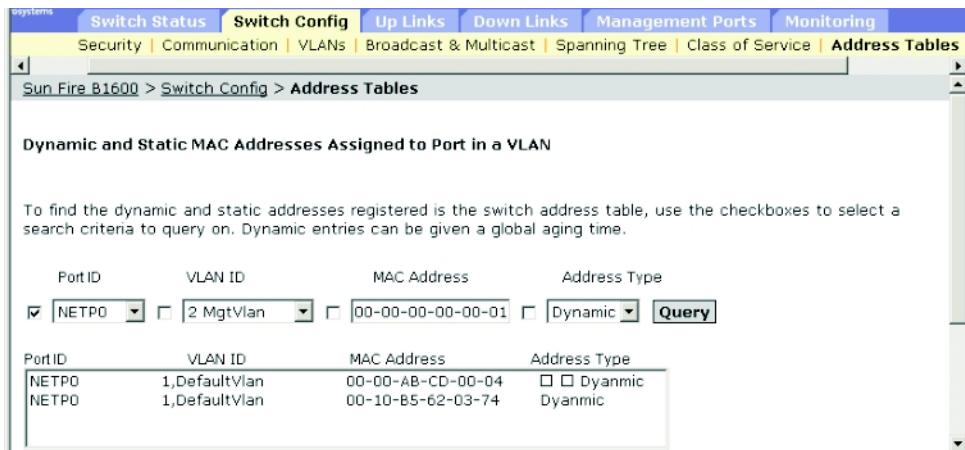
### 3.3.6.1 顯示位址表

位址表內含有交換器動態學習到的 MAC 位址，這些都是資料流進交換器時，交換器監視其中的來源位址而得到的。當交換器收到之流量的目的地位址在資料庫中找到相同的項目時，此封包便會直接轉送到相關的連接埠上，否則該封包便會傳送給所有連接埠。位址表也含有固定在特定連接埠上的靜態 MAC 位址。（請參閱第 3-97 頁的「設定靜態位址」。）

#### 指令屬性

- **Port ID** (介面 \*) – 連接埠或寬道 (上連連接埠：NETP0-7，下連連接埠：SNP0-15；NETMGT 的 MAC 位址表無法顯示)。
- **VLAN ID** – VLAN 識別碼 (1-4094)。  
(此欄位含有 VLAN 的 ID 與名稱。)
- **MAC Address** – 固定在此介面上的 MAC 位址。
- **Address Type** – 顯示此位址是動態學習得到或靜態設定的。

**Web** – 打開 Switch Config=>Address Tables。指定一個介面、VLAN、MAC 位址或位址類別 (混合亦可) 當作搜尋條件，然後按下「Query」。



PortID	VLAN ID	MAC Address	Address Type
NETP0	1,DefaultVlan	00-00-AB-CD-00-04	<input type="checkbox"/> Dyanmic
NETP0	1,DefaultVlan	00-10-B5-62-03-74	Dyanmic

CLI – 以下示範如何顯示 NETP1 連接埠的位址表。

```

Console#show mac-address-table interface ethernet NETP1
Interface   Mac Address      Vlan Type
-----
          NETP0 00-20-9c-23-cd-61 1   Dynamic
Console#
    
```

SNMP – 對等 MIB 變數。

欄位名稱	MIB 變數	權限	設定值範圍
Interface	MIB-II. dot1dBridge.dot1dTp. dot1dTpFdbTable.dot1dTpFdbEntry. dot1dTpFdbPort	唯讀	not learned (0), Port List (1-24)
MAC Address	MIB-II. dot1dBridge.dot1dTp. dot1dTpFdbTable.dot1dTpFdbEntry. dot1dTpFdbAddress	唯讀	MAC 位址
VLAN	MIB-II. dot1dBridge.qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanIndex	不可讀取	整數
Type	MIB-II. dot1dBridge.dot1dTp. dot1dTpFdbTable.dot1dTpFdbEntry. dot1dTpFdbStatus	唯讀	other (1), invalid (2), learned (3), self (4), mgmt (5)



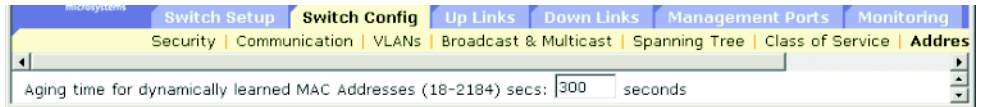
### 3.3.6.2 更改保留期限

您可以設定動態位址表內各項目的保留期限。

#### 指令屬性

- **Aging Time** – 學習得到的項目多久之後會被丟棄。  
(範圍：18-2184 秒，預設值：300 秒)

**Web** – 按下 Switch Config=>Address Tables。指定新的保留期限，然後按下「Save」。



**CLI** – 以下示範如何將保留期限改為 400 秒。

```
Console(config)#mac-address-table aging-time 400           4-88
Console(config)#
```

**SNMP** – 對等 MIB 變數。

欄位名稱	MIB 變數	權限	設定值範圍	預設值
Aging Time	MIB-II dot1dBridge.dot1dTp. dot1dTpAgingTime	可讀寫	整數 (18-2184) 秒	300 秒

## 3.4 連接埠組態

本節包含下連連接埠、上連連接埠與管理連接埠的組態設定功能表，其中大部分功能表對於所有種類的連接埠都是相同的，但管理連接埠只支援一些基本的功能表，而且封包過濾功能（參閱第 3-108 頁）也只有管理連接埠才提供。

---

**注意：**以下功能表中使用的連接埠設定包含上連連接埠 NETP0-7，下連連接埠 SNP0-15，以及管理連接埠 NETMGT。

---

### 3.4.1 顯示連線狀態

連接埠狀態頁會顯示目前的連線狀態，包括線路狀態、速度/雙工模式、流量控制、自動協商與廣播風暴控制。

#### 指令屬性

- **Port Type** – 此連接埠的種類 (1000Base-SX、1000Base-T 或 10/100Base-TX)。
- **Port** – 代表連接埠或寬道 (上連連接埠：NETP0-7，下連連接埠：SNP0-15，管理連接埠：NETMGT)。
- **Description** – 介面標籤。
- **Admin Status** – 顯示此介面已啟用或停用。
  - Web – 顯示 Enabled 或 Disabled。
  - CLI – 顯示 Port Admin (啟用或停用)。
- **Link Status** – 顯示線路是否有連上。
- **Port Operation Status** – 提供連接埠狀態的詳細資訊。
  - 僅 CLI 才有，只有在線路連通時才顯示這個項目。
- **Speed/Duplex** – 顯示目前的速度與雙工模式。
- **Flow Control** – 顯示流量控制功能啟用或停用。
  - Web – IEEE 802.3x、Back-Pressure 或 None。
  - CLI – Enabled 或 Disabled。Flow Type 會顯示 IEEE 802.3x、Back-Pressure 或 None。
- **Auto-negotiation** – 顯示自動協商功能啟用或停用。
- **Protect Status** – 顯示此介面上的廣播風暴控制功能啟用或停用。關於流量上限的設定方式，請參閱第 3-53 頁的「廣播風暴控制 (全區設定)」。
- **MAC Address** – 此連接埠的實體層位址。
  - 僅 CLI 顯示，若要在 Web 上看到此項目，請參閱第 3-10 頁的「設定 IP 位址」。

- **Port Capabilities\*** – 設定連接埠進行自動協商時應向對方表明具有的能力。此交換器的連接埠具有以下的能力。
  - **10half** – 支援 10 Mbps 半雙工運作模式
  - **10full** – 支援 10 Mbps 全雙工運作模式
  - **100half** – 支援 100 Mbps 半雙工運作模式
  - **100full** – 支援 100 Mbps 全雙工運作模式
  - **1000full** – 支援 1000 Mbps 全雙工運作模式
  - **Sym** – 能收發流量控制需要用到的暫停封包
  - **FC** – 支援流量控制功能
- **LACP Status** – 顯示此連接埠上的 LACP (Link Aggregation Control Protocol，線路集束控制通訊協定) 功能啓用或停用。(僅適用於 CLI)

\* 若要透過 Web 看到這個項目，請參閱第 3-82 頁的「設定介面連線」。

**Web** – 按下 Up Links / Down Links / Management Port=>Status。若要設定某一個或多個介面的連線，請按下選定項目旁邊的核取方塊，然後按下「Configure」。(請參閱第 3-82 頁的「設定介面連線」。)

Sun\_Fire\_B1600 > Up\_Links > Connection Status

Port Type: 1000Base-TX

The Up Links are the external 1000-BASE-T ports from the switch into the data network. The Up Links table displays the current link status, including link state, speed/duplex mode, flow control, auto-negotiation and port security. The link capabilities can be configured either by marking the checkbox next to the selected entries and clicking configure, or by clicking directly on the port.

**Configure...**

Port	Description	Admin Status	Link Status	Speed Duplex	Flow Control	AutoNeg	Protect Status
<input type="checkbox"/> NETP0	External RJ-45 connector NET0	Enabled	Up	100full	None	Enabled	Enabled
<input type="checkbox"/> NETP1	External RJ-45 connector NET1	Enabled	Down	1000full	None	Enabled	Enabled
<input type="checkbox"/> NETP2	External RJ-45 connector NET2	Enabled	Down	1000full	None	Enabled	Enabled
<input type="checkbox"/> NETP3	External RJ-45 connector NET3	Enabled	Down	1000full	None	Enabled	Enabled
<input type="checkbox"/> NETP4	External RJ-45 connector NET4	Enabled	Down	1000full	None	Enabled	Enabled
<input type="checkbox"/> NETP5	External RJ-45 connector NET5	Enabled	Down	1000full	None	Enabled	Enabled
<input type="checkbox"/> NETP6	External RJ-45 connector NET6	Enabled	Down	1000full	None	Enabled	Enabled
<input type="checkbox"/> NETP7	External RJ-45 connector NET7	Enabled	Down	1000full	None	Enabled	Enabled

CLI – 以下示範如何顯示 NETP7 連接埠的連線狀態。

```

Console#show interfaces status ethernet NETP7
Information of NETP7
Basic information:
  Port type: 1000T
  Mac address: 00-00-E8-66-66-83
Configuration:
  Name:External RJ-45 connector NET7
  Port admin: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full, 1000full,
  Broadcast storm: Enabled
  Broadcast storm limit: 256 packets/second
  Flow control: Disabled
  LACP:Disabled
Current status:
  Link status: Up
  Port operation status: Up
  Operation speed-duplex: 1000full
  Flow control type: None
Console#
    
```

SNMP – 對等 MIB 變數。

欄位名稱	MIB 變數	權限	設定值範圍	預設值
Port Type	sun... portMgt. portTable. portEntry. portType	唯讀	other (1), hundredBaseTX (2), hundredBaseFX (3), thousandBaseSX (4), thousandBaseLX (5), thousandBaseT (6), thousandBaseMiniGBIC (7) thousandBaseSFP (8)	
MAC Address	MIB-II. interfaces. ifTable.ifEntry. ifPhysAddress	唯讀	實體位址	
Port	sun... portMgt. portTable. portEntry	索引	整數 (1-25)	
Port Name	sun... portMgt. portTable. portEntry. portName	可讀寫	顯示字串 (長度 0-64)	

欄位名稱	MIB 變數	權限	設定值範圍	預設值
Administrative Status	MIB-II. interfaces. ifTable.ifEntry. ifAdminStatus	可讀寫	up (1), down (2), testing (3)	up
Link Status	MIB-II. interfaces. ifTable.ifEntry. ifOperStatus	唯讀	up (1), down (2-7),	
Operational Status	MIB-II. interfaces. ifTable.ifEntry. ifOperStatus	唯讀	up (1), down (2), testing (3), unknown (4), dormant (5), notPresent (6), lowerLayerDown (7)	
Port Speed Duplex Status	sun... portMgt. portTable.portEntry. portSpeedDpxStatus	唯讀	error (1), halfDuplex10 (2), fullDuplex10 (3), halfDuplex100 (4), fullDuplex100 (5), halfDuplex1000 (6), fullDuplex1000 (7)	
Port Capabilities	sun... portMgt. portTable.portEntry. portCapabilities	可讀寫	Bits{ portCap10half (0), portCap10full (1), portCap100half (2), portCap100full (3), portCap1000half (4), portCap1000full (5), reserved6-13 (6-13), portCapSym (14), portCapFlowCtrl (15)}	
Port Flow Control Status	sun... portMgt. portTable.portEntry. portFlowCtrlStatus	唯讀	error (1), backPressure (2), dot3xFlowControl (3), none (4)	none
LACP Port Status	sun... lacpMgt. lacpPortTable. lacpPortEntry. lacpPortStatus	可讀寫	enabled (1), disabled (2)	disabled

欄位名稱	MIB 變數	權限	設定值範圍	預設值
Port Auto-negotiation	sun... portMgt. portTable.portEntry. portAutonegotiation	可讀寫	enabled (1), disabled (2)	enabled
Broadcast Storm Status	sun... bcastStormMgt. bcastStormTable. bcastStormEntry. bcastStormStatus	可讀寫	enabled (1), disabled (2)	enabled

## 3.4.2 設定介面連線

您可以用「Port Setup」頁啓用或停用介面、設定自動協商功能、該介面應該對外宣告的能力，或手動設定速度、雙工模式與流量控制。

### 指令屬性

- **Port/s** – 代表連接埠或寬道 (上連連接埠：NETP0-7，下連連接埠：SNP0-15)。
- **Port Description** – 讓您設定介面的標籤。(範圍：1-64 個字元；預設值 – 上連連接埠：External RJ-45 connector NETn，下連連接埠：Blade Slot n，管理連接埠：External RJ-45 connector NETMGT)
- **Administrative Status** – 讓您手動關閉介面。您可以停用行為不正常的介面 (例如碰撞次數過多)，然後等問題解決之後再重新啓用該介面。或者爲了某些安全上的顧慮，亦可停用介面。
- **Negotiate Link Capabilities<sup>1</sup>** – 讓您啓用或停用自動協商功能。自動協商功能啓用後，您就必須設定要對外宣告的能力。等自動協商功能停用，則可強迫設定速度、模式與流量控制。此交換器的連接埠具有以下的能力。
  - **10half** – 支援 10 Mbps 半雙工運作模式
  - **10full** – 支援 10 Mbps 全雙工運作模式
  - **100half** – 支援 100 Mbps 半雙工運作模式
  - **100full** – 支援 100 Mbps 全雙工運作模式
  - **100half** – 支援 1000 Mbps 半雙工運作模式
  - **1000full** – 支援 1000 Mbps 全雙工運作模式
  - **symmetric** (僅適用於 Gigabit) – 勾選此項目，連接埠便會開始接收與傳送暫停封包；若將此項目清除，則收送兩端便會自動協商要使用的非對稱暫停封包。(此交換器僅支援對稱式暫停封包。)
  - **flowcontrol** – 支援流量控制  
當交換器緩衝區滿載時，流量控制功能會阻擋交換器直接連接之末端主機或網段所傳來的流量，以免發生封包遺棄的狀況。此功能啓用後，半雙工運作模式會採用 back pressure，全雙工運作模式則使用 IEEE 802.3x。

---

**注意：**Sun Fire B1600 Blade 系統機箱內整合的交換器，每一個都含有一對相互連接的交換器晶片。兩個連接埠必須位於同一顆交換器晶片上，彼此之間才可以使用流量控制功能。連接埠 NETP0 到 NETP3 以及 SNP0 到 SNP7 位於同一顆交換器晶片上，連接埠 NETP4 到 NETP7 以及 SNP8 到 SNP15 則位於另一顆上。

---

- **Speed/Duplex<sup>2</sup>** – 當自動協商功能停用時，您就可以手動設定連接埠的速度與雙工模式。

---

**注意：**當自動協商功能停用時，您只能將上連連接埠設定成 10 Mbps 或 100 Mbps。若要強迫連接埠以 1 Gbps 全雙工模式運作，請啟用自動協商功能，並將連接埠的能力設定為只有 1000full 這一項。

---

- **Flow Control<sup>2</sup>** – 當自動協商功能停用時，您必須啟用或停用流量控制功能。(除非為了解決問題的需要，否則請盡量避免在與集線器連接的連接埠上使用流量控制功能，因為 back pressure 干擾訊號可能會導致該集線器連接的網段整體效能下降。)
  - **Broadcast storm suppression** – 針對選定連接埠啟用廣播風暴抑制功能。關於廣播風暴控制或廣播流量上限設定的詳細相關資訊，請參閱第 3-53 頁的「廣播風暴控制 (全區設定)」。
1. 下連連接埠上的自動協商功能無法停用的，這些連接埠均固定以 1000 Mbps 全雙工模式運作。
  2. 上連連接埠的自動協商功能必須先停用，才可以設定或強迫該介面使用特定速度、雙工模式或流量控制功能。

**Web** – 打開 Up Links / Down Links=>Status screen。選取您想要設定之介面的核取方塊，然後按下「Configure」，修改所需介面設定值，然後按下「Save」。

Switch Setup | Switch Config | **Up Links** | Down Links | Management Ports | Monitoring

Status | Link Aggregation | VLANs | Address Filtering | Spanning Tree

Port/s:NETP0

Port Description: External RJ-45 connect

**Set Port Administrative Status:**

Enable  
 Disable

**Enable port auto-negotiation capabilities:**

Auto-negotiation enabled  
 Select link parameter capabilities to advertise

1000full     1000half  
 100full     100half  
 10full     10half  
 flowcontrol     symmetric

Auto-negotiation disable  
 Select link parameters to use

1000full     1000half  
 100full     100half  
 10full     10half

Flow control enabled

**Set Broadcast storm Suppression:**

Enable  
 Disable

**CLI** – 選取要設定的介面，然後輸入所需的設定值。

```

Console#Console(config)#interface ethernet NETP1           4-74
Console(config-if)#description RD SW#17                   4-74
Console(config-if)#shutdown                                4-79
.
.
.
Console(config-if)#no shutdown
Console(config-if)#negotiation
Console(config-if)#capabilities 1000full                   4-77
Console(config-if)#capabilities 1000full                   4-77
Console(config-if)#capabilities flowcontrol
.
.
.
Console(config-if)#no negotiation                          4-76
Console(config-if)#speed-duplex 100half                    4-75
Console(config-if)#flowcontrol                              4-78
Console(config-if)#

```



## SNMP – 對等 MIB 變數。

欄位名稱	MIB 變數	權限	設定值範圍	預設值
Port Name	sun... portMgt. portTable.portEntry. portName	可讀寫	顯示字串 (長度 0-64)	第 3-82 頁
Administrative Status	MIB-II. interfaces. ifTable.ifEntry. ifAdminStatus	可讀寫	up (1), down (2), testing (3)	up
Port Auto-negotiation	sun... portMgt. portTable.portEntry. portAutonegotiation	可讀寫	enabled(1), disabled(2)	enabled
Port Capabilities	sun... portMgt. portTable.portEntry. portCapabilities	可讀寫	Bits{ portCap10half (0), portCap10full (1), portCap100half (2), portCap100full (3), portCap1000half (4), portCap1000full (5), reserved6-13 (6-13), portCapSym (14), portCapFlowCtrl (15)}	
Port Speed Duplex Configuration	sun... portMgt. portTable.portEntry. portSpeedDpxCfg	可讀寫	reserved (1), halfDuplex10 (2), fullDuplex10 (3), halfDuplex100 (4), fullDuplex100 (5), halfDuplex1000 (6), fullDuplex1000 (7)	
Port Flow Control Configuration	sun... portMgt. portTable.portEntry. portFlowCtrlCfg	可讀寫	enabled (1), disabled (2), backPressure (3), dot3xFlowControl (4)	

### 3.4.3 連接埠寬道組態設定

裝置之間的多條線路可以合併成一個虛擬的集束線路。一條連接埠寬道除了讓兩個裝置之間擁有容錯的連線之外，還可以為網段提昇原本已經到達瓶頸的頻寬。同一個時間最多可以建立 6 條寬道。

本交換器支援靜態寬道與動態 LACP (Link Aggregation Control Protocol, 線路集束控制協定)。利用 LACP 設定組態的連接埠，會自動與另一個裝置上啟動 LACP 功能之連接埠協商出一條集束寬道線路。交換器上任何連接埠只要尚未設定屬於任何靜態寬道，都可以設定成使用 LACP。若另一個裝置上的連接埠也設定成 LACP，則此交換器與其他裝置便會協商出兩者之間要用的寬道線路。如果 LACP 寬道由超過四個以上的連接埠組成，則其它所有連接埠都會被設定成備用模式，萬一寬道中的任何一條線路故障，則其中一個備用連接埠便會自動啟動取代。

#### 指令使用方式

除了讓寬道中的所有連接埠附載均衡之外，這些額外的連接埠還可以在寬道中任何一個連接埠當掉時取代之，提供備援的能力。不過在將兩個裝置實際接起來之前，請先用 Web 介面或 CLI 將兩端裝置的寬道設定好。使用連接埠寬道時，請注意以下幾點：

- 先將連接埠寬道設定好，然後才用網路線將交換器連接起來，以免造成網路中出現迴路。
- 此交換器上最多可以建立 6 條寬道，每條寬道最多可以含有 4 個連接埠。
- 線路兩端的連接埠都必須設定成寬道連接埠。
- 同一寬道兩端的連接埠都必須以相同方式設定，包括通訊模式 (即速度、雙工模式與流量控制)、VLAN 隸屬關係與 CoS 設定等等。
- 若目的交換器在互連的連接埠上也啟用 LACP，則寬道便會自動啟動。
- 用 LACP 與另一個交換器合組成的寬道，會自動使用下一個可用的寬道 id。
- 若同一個目的交換器所連接的連接埠有四個以上啟用 LACP，則多餘的連接埠便會被設定成備用模式，只有在任何一條使用中線路故障時才會啟用。
- 從 VLAN 中移出、移入 VLAN、加入 VLAN 內、從 VLAN 內刪除時，寬道中所有連接埠都必須視為一體一起設定。
- STP、VLAN 與 IGMP 都只能在整個寬道上進行設定。

### 3.4.3.1 使用 LACP 動態設定寬道

**Web** – 按下 Up Links / Down Links=>Link Aggregation。在「Link Aggregation」表中找出需要的連接埠，然後按下「Enable LACP」或「Disable LACP」按鈕。

**注意：**由於這些動作按鈕都會立刻生效，為了避免在網路中建立迴路，請先啟用 LACP，再將連接埠連起來，此外，先拔掉連接埠之間的網路線，然後才停用 LACP。請參閱第 3-86 頁上的指令使用方式。



**CLI** – 以下示範如何啟動 NETP0 與 NETP1 兩個連接埠的 LACP 功能。只要將這兩個連接埠連到另一個交換器上同樣具有 LACP 功能的連接埠，就可以組成一條寬道。

```
Console(config)#interface ethernet NETP0                                4-74
Console(config-if)#lACP                                                4-146
Console(config-if)#exit
Console(config)#interface ethernet NETP1
Console(config-if)#lACP
Console(config-if)#end
Console#show interfaces status port-channel 1                            4-81
Information of Trunk 1
Basic information:
  Port type: 1000T
  Mac address: 00-00-E8-66-66-83
Configuration:
  Name:
  Port admin: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full, 1000full,
  Flow control status: Disabled
```

```

Current status:
  Created by: LACP
  Link status: Up
  Port operation status: Up
  Operation speed-duplex: 1000full
  Flow control type: None
  Member Ports: NETP0, NETP1,
  Console#

```

### SNMP – 對等 MIB 變數。

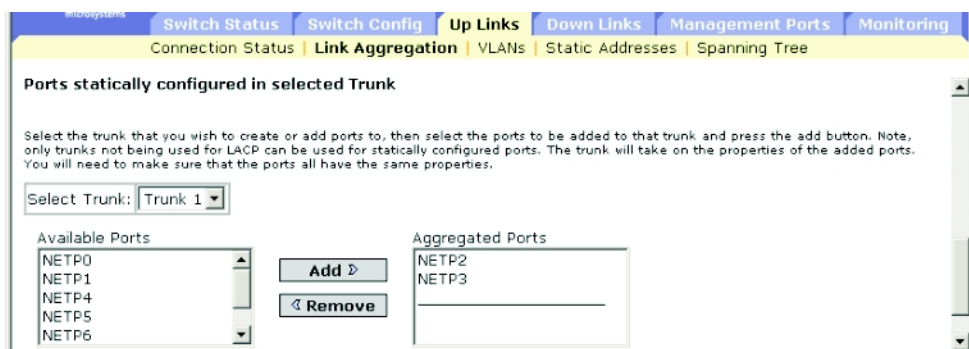
欄位名稱	MIB 變數	權限	設定值範圍	預設值
Trunk Maximum ID	sun... trunkMgt. trunkMaxId	唯讀	整數	6
Trunk Valid Number	sun... trunkMgt. trunkValidNumber	唯讀	整數 (1-6)	
Trunk Index	sun... trunkMgt. trunkTable.trunkEntry. trunkIndex	索引	整數	
Trunk Ports	sun... trunkMgt. trunkTable.trunkEntry. trunkPorts	讀取/建立	二進位字串 (連接埠清單)	
Trunk Creation	sun... trunkMgt. trunkTable.trunkEntry. trunkCreation	唯讀	static (1), lACP (2)	
Trunk Status	sun... trunkMgt. trunkTable.trunkEntry. trunkStatus	讀取/建立	valid (1), invalid (2)	
LACP Port Status	sun... lACP Mgt. lACP PortTable. lACP PortEntry. lACP PortStatus	可讀寫	enabled (1) disabled (2)	

關於其他 CLI 變數的說明，請參閱第 3-78 頁的「顯示連線狀態」

### 3.4.3.2 設定固定寬道

**Web** – 按下 Up Links / Down Links=>Link Aggregation。從下拉式清單中選出寬道索引，接著選取所需的連接埠，最後按下「Add」或「Remove」。

**注意：**由於這些動作按鈕都會立刻生效，為了避免網路中出現迴路，請務必先透過組態設定介面增加一條固定寬道，然後才用網路線將連接埠連起來；最後也應先將網路線拔掉，然後才透過組態設定介面刪除此固定通道。請參閱第 3-86 頁上的指令使用方式。



**CLI** – 以下示範如何用 NETP2 與 NETP3 兩個連接埠建立寬道 2。只要將這兩個連接埠連到另一個交換器上同樣用固定方式設定寬道的連接埠，就可以組成一條寬道。

```
Console(config)#interface port-channel 2 4-74
Console(config-if)#exit
Console(config)#interface ethernet NETP2 4-74
Console(config-if)#channel-group 2 4-145
Console(config-if)#exit
Console(config)#interface ethernet NETP3
Console(config-if)#channel-group 2
Console(config-if)#end
Console#show interfaces status port-channel 2 4-81
Information of Trunk 2
Basic information:
  Port type: 1000t
  Mac address: 00-00-E8-66-66-83
Configuration:
Port admin status: Up
Speed-duplex: Auto
Capabilities: 10half, 10full, 100half, 100full, 1000full,
Flow control status: Disabled
```

```

Current status:
Created by: User
Link status: Up
Port operation status: Up
Operation speed-duplex: 1000full
Flow control type: None
Member Ports: NETP2, NETP3,
Console#

```

### SNMP – 對等 MIB 變數。

欄位名稱	MIB 變數	權限	設定值範圍	預設值
Trunk Maximum ID	sun... trunkMgt.trunkMaxId	唯讀	整數	6
Trunk Valid Number	sun... trunkMgt. trunkValidNumber	唯讀	整數 (1-6)	
Trunk Index	sun... trunkMgt.trunkTable. trunkEntry.trunkIndex	索引	整數	
Trunk Ports	sun... trunkMgt.trunkTable. trunkEntry.trunkPorts	讀取/建立	二進位字串 (連接埠清單)	
Trunk Creation	sun... trunkMgt. trunkTable.trunkEntry. trunkCreation	唯讀	static (1), lacp (2)	
Trunk Status	sun... trunkMgt.trunkTable. trunkEntry.trunkStatus	讀取/建立	valid (1), invalid (2)	

關於其他 CLI 變數的說明，請參閱第 3-78 頁的「顯示連線狀態」

## 3.4.4 設定介面的 VLAN 行爲

您可以設定特定介面的 VLAN 行爲，包括預設 VLAN 識別碼 (PVID)、可接受的封包種類、輸入過濾方式、GVRP 狀態以及 GARP 計時器。

### 指令使用方式

- **GVRP – GARP VLAN Registration Protocol (GARP VLAN 註冊通訊協定)** 為交換器定義了一種彼此交換 VLAN 資訊的方式，以便在網路其它地方的介面上自動註冊 VLAN 成員。
- **GARP – GVRP 使用 GARP (Group Address Registration Protocol, 群組位址註冊通訊協定)** 為橋接 LAN 中的用戶端服務註冊或取消用戶端屬性。GARP 計時器的預設值與傳輸媒介的存取方法以及資料速路都沒有關係。除非 GVRP 註冊/取消功能無法正常使用，否則請勿修改這些設定值。

### 指令屬性

- **Port** – 代表連接埠或寬道 (上連連接埠：NETP0-7，下連連接埠：SNP0-15，管理連接埠：NETMGT)。
- **Default VLAN for Port (PVID)** – 介面收到未加註任何標籤的封包時，便以此設定值指定當作該封包的 VLAN ID。(預設值 – 上連/下連線路：1，NETMGT：2)

---

**注意：**設定 RADIUS 或 TACACS 伺服器上的權限等級時，請記得等級 0 代表以 來賓 (即 Normal Exec) 權限連上交換器，至於其他所有 VLAN，所有介面都必須先設定成不會加註標籤的成員，才可以將其 PVID 設為該群組。

---

- **Acceptable Frame Types** – 設定此介面接收所有封包類別，包括有加註標籤的封包與未加註標籤的封包，或是只接收有加註標籤的封包。設定成接收所有類別的封包時，所收到未加註任何標籤的封包都會被分給預設 VLAN。(選項：all 和 tagged，預設值：all)
- **Switch Port Mode** – 顯示連接埠的 VLAN 隸屬模式。(預設值：Trunk)
  - **Trunk** – 將連接埠作為 VLAN 寬道的一個端點。由於寬道是兩個交換器之間的直接連線，因此這個連接埠會傳輸標籤標示該來源 VLAN 的封包。
  - **Hybrid** – 設定混合式 VLAN 介面，表示連接埠可以傳送有加註標籤與沒加註標籤的封包。

---

**注意：**若交換器模式設定程 **Trunk**，則屬於該連接埠預設 VLAN (即其 PVID 所指的 VLAN) 的封包不加註標籤就會傳送出去，但所有其他封包都會加註指定的 VLAN ID。

---

- **Ingress Filtering** – 啓用輸入過濾功能後，未含有此輸入連接埠的 VLAN 收到封包時，在該輸入連接埠就會被丟棄。(預設值：Disabled)

---

**注意：**

- 輸入過濾功能只對加註標籤的封包有影響。
  - 若停用輸入過濾功能，則當此介面收到有加註 VLAN 標籤的封包時，只要封包的標籤符合交換器已知的任何一個 VLAN，此介面就會將該封包收進來 (除非封包的標籤剛好是此連接埠明確禁止 VLAN)。
  - 若啓用輸入過濾功能，且此介面收到的封包其標籤指的 VLAN 並未含有這個輸入連接埠，則此介面就會將此封包丟棄。
  - 輸入過濾功能對沒用到 VLAN 的 BPDU 封包，例如 GVRP 與 STP 等等，並無任何影響。但是對於 GMRP 之類會用到 VLAN 的 BPDU 封包就絕對有影響。
- 
- **GVRP** – 啓用/停用此介面的 GVRP。整個交換器的 GVRP 必須先啓用，這項設定才會有效 (請參閱第 3-37 頁)。停用連接埠的 GVRP 後，此連接埠所收到的任何 GVRP 封包都會被丟棄，而且也不會將其它連接埠傳來的 GVRP 註冊訊息傳遞出去。(預設值：Disabled)
  - **GARP Join Timer** – 連續發出兩個要加入 VLAN 群組的要求/詢問訊息之間的時間。  
(範圍：0.2 秒到 10 秒，預設值：0.2 秒)
  - **GARP Leave Timer** – 連接埠應該等待多久時間之後才離開 VLAN 群組。這個時間應該設定成加入時間 (join time) 的兩倍以上，以確保 Leave 或 LeaveAll 訊息發出後，連接埠還可以在離開此群組之前重新加入。  
(範圍：0.6 到 30 秒，預設值：0.6 秒)
  - **GARP LeaveAll Timer** – 從發出 LeaveAll 詢問訊息給 VLAN 群組成員開始，到此連接埠離開群組所經過的時間。此設定值應該遠大於離開時間 (Leave Time)，使要重新加入此群組的節點所發出的流量降到最低。  
(範圍：5 到 180 秒，預設值：10 秒)
  - **VLANs on Selected Port** – 固定將連接埠加入指定的 VLAN 內。
  - **Membership Type** – 設定連接埠的靜態 VLAN 隸屬關係。
    - **Tagged**：介面爲此 VLAN 的成員之一。這個連接埠在此 VLAN 上傳送的所有封包都會加註標籤，換句話說，就是會帶著一個標籤，其中標明了 VLAN 或 CoS 資訊。
    - **Untagged**：介面爲此 VLAN 的成員之一。這個連接埠在此 VLAN 上傳送的所有封包都不會加註標籤，換句話說，並沒有帶著一個標籤標明 VLAN 或 CoS 資訊。
    - **Forbidden**：禁止介面透過 GVRP 自動加入 VLAN 內。請參閱第 3-33 頁的「自動 VLAN 註冊」。
    - **Remove**：將選定介面從此 VLAN 中移除。



Web – 打開 Up Links / Down Links / Management Port=>VLANs。填入每個介面所需的設定值，按下「Save」。

microsystems | Switch Status | Switch Config | **Up Links** | Down Links | Management Ports | Monitoring

Connection Status | Link Aggregation | **VLANs** | Static Addresses | Spanning Tree

Sun Fire 81600 > Up Links > VLANs

Select Port: NETP4

You can configure VLAN behavior for specific interfaces, including the default VLAN identifier (PVID), accepted frame types, ingress filtering, GVRP status and GARP timers.

Default VLAN for Port (PVID): 4, Finance

Acceptable Frame Types:

- All Frame Types
- Tagged Only

Switch Port Mode:

- Trunk
- Hybrid

Ingress Filtering Enabled

Enable GARP VLAN Registration Protocol (GVRP):

- Enable
- Disable

Configure Group Address Registration Protocol(GARP) Parameters:

GARP Join Timer: 20

GARP Leave Timer: 60

GARP LeaveAll Timer: 1000

Save Cancel

往下捲到 VLAN 隸屬成員表，針對選定介面設定所需的 VLAN。

microsystems | Switch Status | Switch Config | **Up Links** | Down Links | Management Ports | Monitoring

Connection Status | Link Aggregation | **VLANs** | Static Addresses | Spanning Tree

Sun Fire 81600 > Up Links > VLANs

Configure VLANs on Selected Port:

You can use these list boxes to statically assign VLANs to the selected port.

**All VLANs**

- 3, R&D
- 5, Marketing

**Membership VLANs**

- 1, DefaultVlan, Allow(untagged)
- 2, MgtVlan, Forbidden
- 4, Finance, Allow(tagged)

Add Tagged Add Untagged Add Forbidden Remove

Save Cancel

CLI – 以下示範如何將 NETP4 連接埠設定成只接收有加註標籤的封包、將 PVID 4 設定為固有 VLAN ID、啟動 GVRP、設定 GARP 計時器，然後將 switchport 模式設定為 hybrid (混合)。

```

Console(config)#interface ethernet NETP4                                4-74
Console(config-if)#switchport acceptable-frame-types tagged          4-108
Console(config-if)#no switchport ingress-filtering                   4-109
Console(config-if)#switchport allowed vlan add 4 tagged              4-111
Console(config-if)#switchport native vlan 4                          4-110
Console(config-if)#switchport gvrp                                    4-114
Console(config-if)#garp timer join 10                                4-116
Console(config-if)#garp timer leave 90                               4-116
Console(config-if)#garp timer leaveall 2000                          4-116
Console(config-if)#switchport mode hybrid                             4-107
Console(config-if)#switchport forbidden vlan add 3                   4-112
Console(config-if)#

```

SNMP – 對等 MIB 變數。

欄位名稱	MIB 變數	權限	設定值範圍	預設值
Port PVID	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qPortVlanTable. dot1qPortVlanEntry. dot1qPvid	可讀寫	整數 (1-4094)	1
Port Acceptable Frame Type	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qPortVlanTable. dot1qPortVlanEntry. dot1qPortAcceptable-FrameTypes	可讀寫	admitAll (1), admitOnlyVlan-Tagged (2)	admitAll
Port Mode	sun... vlanMgt. vlanPortTable. vlanPortEntry. vlanPortMode	可讀寫	hybrid (1), dot1qTrunk (2)	hybrid

欄位名稱	MIB 變數	權限	設定值範圍	預設值
Port Ingress Filtering	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qPortVlanTable. dot1qPortVlanEntry. dot1qPortIngressFiltering	可讀寫	true (1), false (2)	false
Port GVRP Status	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qPortVlanTable. dot1qPortVlanEntry. dot1qPortGVRPStatus	可讀寫	enabled (1), disabled (2)	disabled
GARP Join Time	MIB-II. dot1dBridge. pBridgeMIB. pBridgeMIBObjects. dot1dGarp. dot1dPortGarpTable. dot1dPortGarpEntry. dot1dPortGarpJoinTime	可讀寫	整數 (20-100)0 百分之一秒	20 百分之一秒
GARP Leave Time	MIB-II. dot1dBridge. pBridgeMIB. pBridgeMIBObjects. dot1dGarp. dot1dPortGarpTable. dot1dPortGarpEntry. dot1dPortGarpLeaveTime	可讀寫	整數 (60 到 3000) 百分之一秒	60 百分之一秒
GARP Leave All Time	MIB-II. dot1dBridge. pBridgeMIB. pBridgeMIBObjects. dot1dGarp. dot1dPortGarpTable. dot1dPortGarpEntry. dot1dPortGarp- LeaveAllTime	可讀寫	整數 (500-18000) 百分之一秒	1000 百分之一秒

欄位名稱	MIB 變數	權限	設定值範圍	預設值
VLAN Static Name	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanStaticName	讀取/建立	二進位字串 (長度 0-32)	
VLAN Static Row Status	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanStaticRowStatus	讀取/建立	enable (1), disable (2)	
Tagged Ports, Untagged Ports (Allowed VLAN)	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanTable. dot1qVlanEntry. dot1qVlanStatic- UntaggedPorts	讀取/建立	二進位字串 (連接埠清單)	
VLAN Forbidden Ports	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qPortVlanTable. dot1qPortVlanEntry. dot1qVlanForbidden- EgressPorts	讀取/建立	二進位字串 (連接埠清單)	

## 3.4.5 設定靜態位址

您可以用位址過濾功能設定固定在某個連接埠與 VLAN 的靜態位址，或者啓用連接埠的安全功能，限制只接收傳給位址表中所列之項目（包括動態與靜態位址）的流量。

### 指令使用方式

- **Setting Static Addresses** – 交換器的每個介面都可以設定靜態位址。當固定綁在某個介面的靜態位址出現在另一個介面上時，後者便不會接受與傳輸從該位址發出或傳給該位址的資料，同時也不會將這個位址放在它的位址表內。
- **Configuring Port Security** – 啓用連接埠安全功能後，交換器就會停止在指定連接埠上動態學習新的位址，並且只會接收來源位址已列在動態位址表內的流量。若要用連接埠安全功能，首先給交換器一段時間動態學習該介面所接收之封包的 < 來源 MAC 位址與 VLAN > 資訊，然後再啓用連接埠安全功能使位址學習行為停止。交換器的學習時間一定要夠長，才能確保所有 VLAN 成員都已經在選定介面上註冊過了。

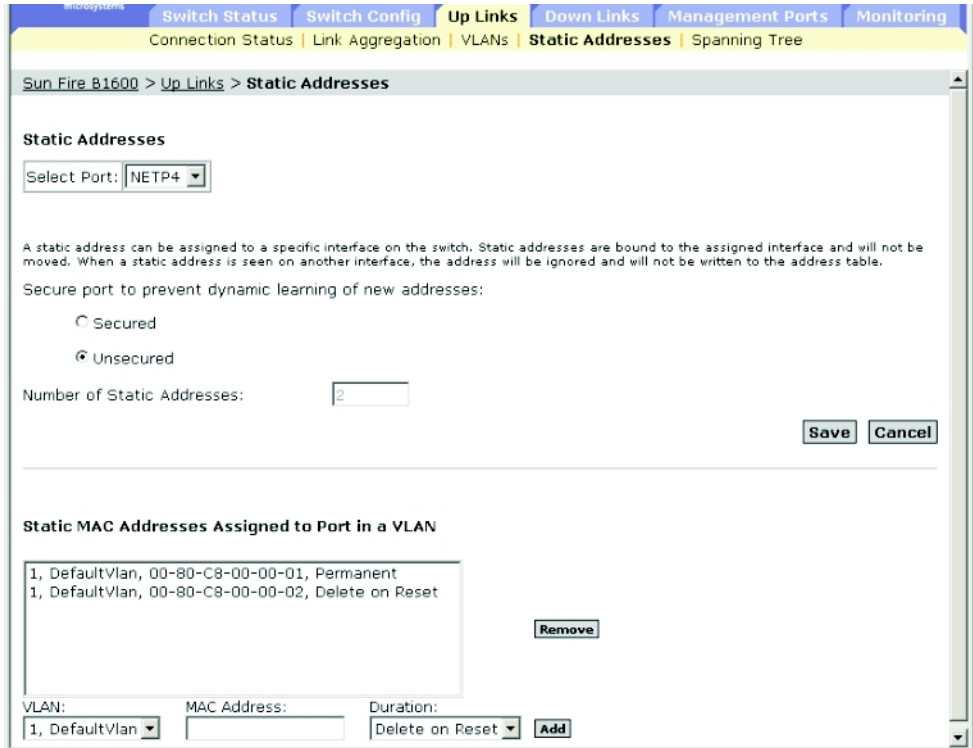
以後要增加新的 VLAN 成員時，可手動加入靜態位址，或暫時關閉連接埠安全功能，使學習功能重新啓動一段時間，讓此新 VLAN 成員有時間註冊，然後再視情況需要停用學習功能。

### 指令屬性

- **Port** – 介面（包含連接埠與寬道）。  
（上連連接埠：NETP0-7，下連連接埠：SNP0-15）
- **Secure Port** – 啓用或停用連接埠安全功能。（預設值：Disabled）  
安全連接埠有以下限制：
  - 不可使用連接埠監視功能。
  - 不可成爲多 VLAN 介面。
  - 不可連上網路互連裝置。
  - 不可加入寬道。
- **Number of Static Addresses\*** – 手動設定位址個數。
- **VLAN** – 已設定好之 VLAN 的 ID (1-4094) 與名稱。
- **MAC Address** – 固定在此介面上的 MAC 位址。
- **Duration** – 此位址可設定爲以下幾種類別：
  - **Permanent** – 永久有效，交換器重新開機後還是會恢復回來。
  - **Delete on Reset** – 設定只持續到交換器重設爲止。

\* 僅適用於 Web

Web – 打開 Up Links / Down Links=>Address Filtering。指定介面，選取「Secure Port」核取方塊啓用連接埠安全功能，接著再輸入 VLAN、MAC 位址與時間長短，最後按下「Add」。



CLI – 以下示範如何將同樣的項目加入靜態位址表內。

```

Console(config)#interface ethernet NETP4
Console(config-if)#port security                                4-90
Console(config-if)exit
Console(config)#mac-address-table static 00-80-c8-00-00-01
    interface ethernet NETP4 vlan 1 permanent                    4-86
Console(config)#mac-address-table static 00-80-c8-00-00-02
    interface ethernet NETP4 vlan 1 delete-on-reset
Console(config)#exit
Console#show mac-address-table ethernet NETP4                    4-87
Interface   Mac Address           Vlan Type
-----
          NETP4 00-80-C8-00-00-01    1 Permanent
          NETP4 00-80-C8-00-00-02    1 Delete-on-reset
Console#

```

SNMP – 對等 MIB 變數。

欄位名稱	MIB 變數	權限	設定值範圍	預設值
Static Receive Port	MIB-II. dot1dBridge. dot1dStatic. dot1dStaticTable. dot1dStaticEntry. dot1dStaticReceivePort	可讀寫	整數	
Port Security Status	sun... securityMgt. portSecurityMgt portSecPortTable. portSecPortEntry. portSecPortStatus	可讀寫	enabled (1), disabled (2)	disabled
Number of Static Addresses	未定義			
VLAN Index	MIB-II. dot1dBridge. qBridgeMIB. qBridgeMIBObjects. dot1qVlan. dot1qVlanStaticTable. dot1qVlanStaticEntry. dot1qVlanIndex	索引	整數	
Static Address	MIB-II. dot1dBridge. dot1dStatic. dot1dStaticTable. dot1dStaticEntry. dot1dStaticAddress	可讀寫	MAC 位址	
Static Status	MIB-II. dot1dBridge. dot1dStatic. dot1dStaticTable. dot1dStaticEntry. dot1dStaticStatus	可讀寫	other (1), invalid (2), permanent (3), deleteOnReset (4), deleteOnTimeout (5)	permanent

## 3.4.6 管理 Spanning Tree 演算法介面

您可以設定所需介面的 RSTP 屬性，包括連接埠優先等級、路徑成本、線路類別與邊緣連接埠。同一種媒體類型的連接埠可以使用不同的優先等級或路徑成本，標示出喜好路徑、線路種類（點對點連線或共用媒體連線）以及邊緣連接埠（顯示出所連裝置是否支援快速轉送）。

### 3.4.6.1 顯示 STA 目前的介面設定

#### 指令屬性

- **Port** – 只可使用連接埠，不可使用寬道以及隸屬寬道的連接埠。  
（上連連接埠：NETP0-7，下連連接埠：SNP0-15）
- **STA Status** – 顯示此連接埠在 Spanning Tree 內目前的狀態：
  - **Discarding** – 連接埠會接收 STA 組態訊息，但不會轉送封包。
  - **Learning** – 連接埠已經發出組態訊息，而且經過 Forward Delay 參數設定的時間之後，並未收到任何矛盾的資訊，於是此連接埠便將位址表清除，並開始學習位址。
  - **Forwarding** – 連接埠會轉送封包，而且會繼續學習位址。
- **Priority** – 定義此連接埠在 Spanning Tree 演算法中使用的優先等級。若交換器上所有連接埠的路徑成本都一樣，則優先等級最高（數值最低）的連接埠便會被設定成 Spanning Tree 中的主線路。如此一來，當 Spanning Tree 演算法偵測到網路中有迴路出現時，優先等級較高的連接埠就比較不可能被擋掉。若被設定為最高優先等級的連接埠個數不只一個，則啟用其中識別碼數字最低的連接埠。
- **Path Cost** – STA 利用此參數決定裝置之間的最佳路徑。因此較低的數值應該設定給連接速度較快媒體的連接埠，較高的數值應該設定給連接速度較慢媒體的連接埠。（路徑成本的效用排在連接埠優先等級之前。）
- **Designated Cost** – 在目前的 Spanning Tree 演算法下，封包從連接埠傳到根所需的成本。傳輸媒體速度愈慢，成本就愈高。
- **Designated Bridge** – 此連接埠要通往 Spanning Tree 的根時，一定要聯繫的裝置的優先等級與 MAC 位址。
- **Designated Port** – 此交換器要與 Spanning Tree 根通訊時，必經的標定橋接裝置的優先等級與連接埠編號。



- **Link Type (Admin Link type\*)** – 此介面所連接的線路種類。
  - 點對點 – 只連接另一個橋接器的線路。
  - 共用 – 連接兩個或多個橋接器的線路。
  - 自動 – 交換器會自動檢查此介面所連接的是點對點線路或共用的傳輸媒介。
- **Edge Port (Admin Edge Port\*)** – 若介面所連 LAN 網段位於橋接 LAN 的末端或通往末端節點，便可啓用此選項。由於末端節點**不可能**導致轉送迴路，因此可以直接跳過到達 Spanning Tree 的轉送狀態。設定成 Edge Port 可以讓工作站或伺服器之類的裝置收斂速度加快，保留現有的轉送資料庫以減少重新設定組態時因重建位址表而發出的廣播封包數量，此介面更改狀態時，Spanning Tree 不會啓動重新設定組態程序，而且還能克服其它 STA 相關的逾時問題。雖然有這麼多好處，但請務必記得 Edge Port 只能在連接末端節點裝置的連接埠上啓用。

\* CLI 會顯示這些文字。

以下多餘的參數只會顯示在 CLI 上：

- **Admin status** – 顯示此介面的 STA 是否有啓用。
- **Role** – 角色的設定是根據此連接埠是否為使用中拓樸的一部份，使用中拓樸可能是將橋接器連到根橋接器（即**根**連接埠）、將 LAN 透過橋接器連上根橋接器（即**標定**連接埠）或是其它橋接器、橋接器連接埠或 LAN 故障或被移除時可提供連線的**替代**或**備援**連接埠。如果連接埠在 Spanning Tree 內未擔任任何角色，便會被設定為取消（即 **disabled** 連接埠）。
- **Designated root** – 此 Spanning Tree 中已被交換器接受當作根裝置的裝置的優先等級與 MAC 位址。
- **Forward transitions** – 此連接埠從 Learning 狀態轉換成 Forwarding 狀態的次數。
- **Oper edge port** – 此參數一開始會設定成與 Admin Edge Port 一樣（即 true 或 false），但收到 BPDU 後就會變成 false。
- **Oper Link type** – 與此介面相連之 LAN 網段的點對點運作狀態。此參數可由手動設定控制，也可以由自動偵測控制，如「Admin Link Type」中所述。

Web – 按下 Up Links / Down Links=>Spanning Tree=>Spanning Tree Protocol 。

Port	STA Status	Priority	Path Cost	Designated Cost	Designated Bridge	Designated Port	Link Type	Edge Port Status
<input type="checkbox"/> NETP0	Forwarding	128	100000	0	32768.0.0000E8666672	128.17	Point-to-Point	Disabled
<input type="checkbox"/> NETP1	Broken	128	10000	0	32768.0.0000E8666672	128.18	Point-to-Point	Disabled
<input type="checkbox"/> NETP2	Broken	128	10000	0	32768.0.0000E8666672	128.19	Point-to-Point	Disabled
<input type="checkbox"/> NETP3	Broken	128	10000	0	32768.0.0000E8666672	128.20	Point-to-Point	Disabled

CLI – 以下示範如何顯示 NETP4 的 STA 屬性。

```

Console#show spanning-tree ethernet NETP4                                     4-102
SNP0 information
-----
Admin status           : enable
Role                   : designate
State                  : forwarding
Path cost              : 10000
Priority                : 128
Designated cost       : 10000
Designated port       : 128.1
Designated root       : 32768.00209C23C267
Designated bridge     : 32768.0000E8666672
Forward transitions   : 0
Admin edge port       : disable
Oper edge port        : disable
Admin Link type       : point-to-point
Oper Link type        : point-to-point
Console#

```

## SNMP – 對等 MIB 變數。

欄位名稱	MIB 變數	權限	設定值範圍	預設值
Port	sun...xstMgt. mstInstancePortTable. mstInstancePortEntry	索引	整數 (1-25)	
STA Port State	sun...xstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePortState	唯讀	discarding (1), learning (2), forwarding (3)	
STA Port Priority	sun...xstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePortPriority	可讀寫	整數 (0-240)	128
STA Port Path Cost	sun...xstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePortPathCost	可讀寫	整數 (長：1-200,000,000， 短：1-65,535)	第 3-104 頁
STA Port Designated Cost	sun...xstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePort- DesignatedCost	唯讀	整數	
STA Port Designated Bridge	sun...xstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePort- DesignatedBridge	唯讀	八進位字串	
STA Port Designated Port	sun...xstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePort- DesignatedPort	唯讀	八進位字串	
STA Port Admin Point to Point	sun...staMgt. staPortTable. staPortEntry. staPortAdminPointTo- Point	可讀寫	forceTrue (0) forceFalse (1) auto (2),	auto
STA Port Admin Edge Port	sun...staMgt. staPortTable. staPortEntry. staPortAdminEdgePort	可讀寫	true (1), false (2)	false

欄位名稱	MIB 變數	權限	設定值範圍	預設值
STA Port Enable (Admin status)	sun...mstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePortEnable	可讀寫	enabled (1), disabled (2)	enabled
STA Port Role	sun...mstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePortPortRole	唯讀	disabled (1), root (2), designated (3), alternate (4), backup (5)	
STA Port Designated Root	sun...mstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePort- DesignatedRoot	唯讀	八進位字串	
STA Port Forward Transitions	sun...mstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePort- ForwardTransitions	唯讀	計數器	

### 3.4.6.2 設定介面的 STA 組態

當交換器設定為 STP 強制相容模式 (參閱第 3-55 頁) 與 RSTP 時，這些設定便會套用到選定介面上。

#### 指令屬性

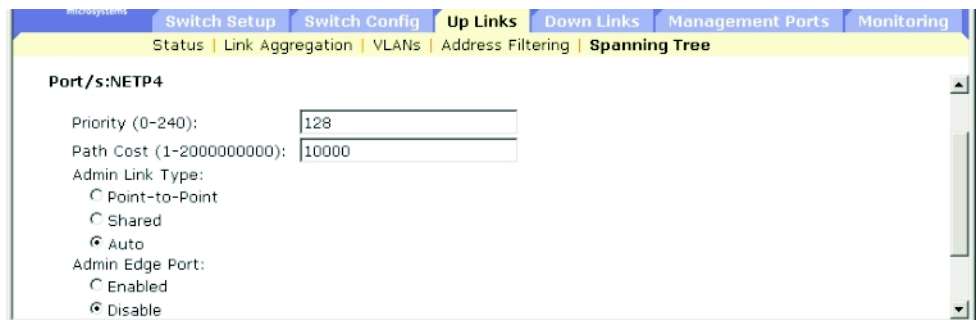
- **Priority** – 定義此連接埠在 Spanning Tree Algorithm (Spanning Tree 演算法，簡稱 STA) 中使用的優先等級。若交換器上所有連接埠的路徑成本都一樣，則優先等級最高 (數值最低) 的連接埠便會被設定成 Spanning Tree 中的主線路。如此一來，當 STA 偵測到網路中有迴路出現時，優先等級較高的連接埠就比較不可能被擋掉。若被設定為最高優先等級的連接埠個數不只一個，則啓用其中識別碼數字最低的連接埠。
  - 預設值：128
  - 範圍：0-240，以 16 遞增
- **Path Cost** – STA 利用此參數決定裝置之間的最佳路徑。因此較低的數值應該設定給連接速度較快媒體的連接埠，較高的數值應該設定給連接速度較慢媒體的連接埠。(路徑成本的效用排在連接埠優先等級之前。)
  - 範圍 –
    - 乙太網路：200,000-20,000,000
    - 快速乙太網路：20,000-2,000,000
    - Gigabit 乙太網路：2,000-200,000

- 預設值 –
  - 乙太網路 – 半雙工：2,000,000，全雙工：1,000,000，寬道：500,000
  - 快速乙太網路 – 半雙工：200,000，全雙工：100,000，寬道：50,000
  - Gigabit 乙太網路 – 全雙工：10,000，寬道：5,000

**注意：**當 Path Cost Method 設定為 short 時 ( 參閱第 3-61 頁 )，最大路徑成本為 65,535。

- **Admin Link Type** – 此介面所連接的線路種類。( 預設值：Auto)
  - 點對點 – 只連接另一個橋接器的線路。
  - 共用 – 連接兩個或多個橋接器的線路。
  - 自動 – 交換器會自動檢查此介面所連接的是點對點線路或共用的傳輸媒介。
- **Admin Edge Port** – 若介面所連 LAN 網段位於橋接 LAN 的末端或通往末端節點，便可啓用此選項。由於末端節點**不可能**導致轉送迴路，因此可以直接跳過到達 Spanning Tree 的轉送狀態。設定成 Edge Port 可以讓工作站或伺服器之類的裝置收斂速度加快，保留現有的轉送資料庫以減少重新設定組態時因重建位址表而發出的廣播封包數量，此介面更改狀態時，Spanning Tree 不會啓動重新設定組態程序，而且還能克服其它 STA 相關的逾時問題。雖然有這麼多好處，但請務必記得 Edge Port 只能在連接末端節點裝置的連接埠上啓用。( 預設值：NETP0-7：停用，SNP0-15：啓用且固定為此設定值 )

**Web** – 按下 Up Links / Down Links=>Spanning Tree=>Spanning Tree Protocol。若要設定介面的 STP (IEEE 802.1D) 組態，請按下所需介面的核取方塊，然後按下「Configure」，接著只修改必要的屬性，最後按下「Save」。



CLI – 以下示範如何顯示 NETP5 連接埠的 STP 屬性。

Console(config)# interface ethernet NETP5	4-74
Console(config-if)#spanning-tree port-priority 128	4-99
Console(config-if)#spanning-tree cost 19	4-98
Console(config-if)#spanning-tree link-type auto	4-101
Console(config-if)#no spanning-tree edge-port	4-100

SNMP – 對等 MIB 變數。

欄位名稱	MIB 變數	權限	設定值範圍	預設值
STA Port Priority	sun...mstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePortPriority	可讀寫	整數 (0-240)	128
STA Port Path Cost	sun...mstMgt. mstInstancePortTable. mstInstancePortEntry. mstInstancePortPathCost	可讀寫	整數 (長：1-200,000,000， 短：1-65,535)	第 3-104 頁
STA Port Admin Link Type	sun...staMgt. staPortTable. staPortEntry. staPortAdmin- PointToPoint	可讀寫	forceTrue (0), forceFalse (1), auto (2)	auto
STA Port Admin Edge Port	sun...staMgt. staPortTable. staPortEntry. staPortAdminEdgePort	可讀寫	true (1), false (2)	false

### 3.4.6.3 檢查介面的 STA 通訊協定狀態

任何時候只要交換器偵測到 STP BPDU，包括 Configuration（組態設定）或 Topology Change Notification（拓樸改變通知）BPDU，都會自動將選定介面設定為強制 STP 相容模式。不過您也可以使用「Protocol Migration」按鈕手動重新勾選適合在選定介面上發送的 BPDU 格式（RSTP 或 STP 相容）。

**Web** – 按下 Up Links / Down Links=>Spanning Tree=>Spanning Tree Protocol。選取所需介面，然後按下「Protocol Migration」按鈕。

Port	STA Status	Priority	Path Cost	Designated Cost	Designated Bridge	Designated Port	Link Type	Edge Port Status
<input checked="" type="checkbox"/> NETP4	Broken	128	10000	0	32768.0.0000E8666672	128.21	Point-to-Point	Disabled

**CLI** – 以下示範如何使用通訊協定遷移指令檢驗要在此介面上發送出去的 spanning tree 訊息類別（即 RSTP 或 STP 相容）。

```

Console(config)interface ethernet NETP4
Console(config-if)#spanning-tree protocol-migration           4-101
Console(config-if)#
  
```

**SNMP** – 對等 MIB 變數。

欄位名稱	MIB 變數	權限	設定值範圍	預設值
STA Port Protocol Migration	sun...staMgt. staPortTable. staPortEntry. staPortProtocolMigration	可讀寫	true (1), false (2)	true

## 3.4.7 阻擋流量進入管理連接埠

封包過濾功能可以設定成阻擋從下連連接埠進來的特定 IP 流量流入內埠管理管理連接埠 (NETMGT)。(請注意，從上連連接埠傳來的流量絕對不會允許轉給管理連接埠。)

### 指令使用方式

- 系統預設會將內部管理連接埠與下連連接埠之間的所有 IP 封包阻擋下來，如果您想透果管理連接埠連上伺服器葉片，就必須另外設定一組過濾器，允許封包在管理連接埠和下連連接埠之間流通。
- 系統預設會將下連連接埠流往管理連接埠 (NETMGT) 的所有 IP 封包阻擋下來，如果您希望伺服器葉片能透過管理連接埠 (NETMGT) 接觸到管理網路，就必須另外設定一組過濾器，允許封包從下連連接埠流到管理連接埠。

---

**注意：**上連連接埠和管理連接埠之間不得相互傳遞流量。

---

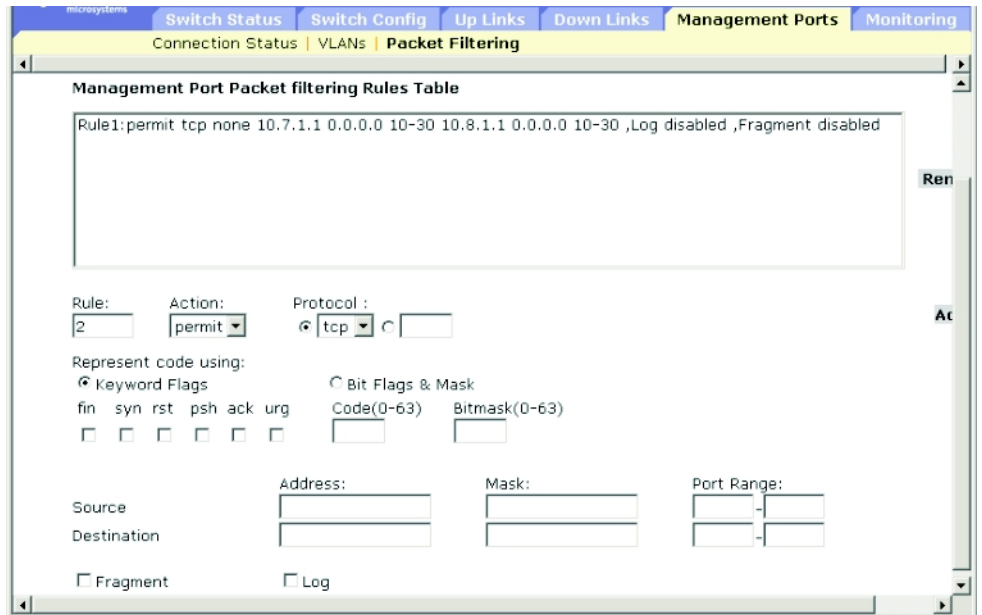
### 指令屬性

- **Rule** – 在表格內指定位置插入一條過濾規則，將表格中原來在此位置或此位置底下的所有樣式全部往下推。規則編號不得超過表格中下一個可使用的編號。若未指定規則編號，則新的樣式就會被放到規則表的結尾。(範圍：1-128)
- **Action** – 阻擋或允許下連連接埠傳往管理連接埠的封包。(選項：permit、deny)
- **Protocol** – 選取一種通訊協定 (TCP、UDP、Any) 或通訊協定編號 (0-255)。
- **Keyword Flags** (代碼順序) – 表示 TCP 表頭第 14 個位元組中的旗標。您可以指定一連串代碼 (ON 代表選定，OFF 代表未選定)。這些符號名稱與相對應的位元包括以下項目：
  - **fin** (1) – 完成
  - **syn** (2) – 同步
  - **rst** (4) – 重設
  - **psh** (8) – 推送
  - **ack** (16) – 確認
  - **urg** (32) – 緊急指標
- **Code** – 代表 TCP 表頭第 14 個位元組內各旗標位元的十進位數字 (表示一個位元字串)。(範圍：0-63)
- **Bitmask** – 套用到代碼上的十進位數字 (代表位元遮罩)。輸入一個十進位數字，其中相對位置 1 的位元代表要與該位置的位元符合，0 則代表忽略該位元。可使用的位元包括：  
32 (urg)、16 (ack)、8 (psh)、4 (rst)、2 (syn)、1 (fin)
- **Source** – 封包的 TCP/UDP 來源位址、網路遮罩與連接埠範圍。(連接埠範圍：0-65535)
- **Destination** – 封包的 TCP/UDP 目的位址、網路遮罩與連接埠範圍。(連接埠範圍：0-65535)



- **Fragment** – 表示此規則只會作用在已經設定了 MF (More Fragments)，還有其他片段位元或片段位置大於 0 的封包上。若未設定這個屬性，則不論是不是片段封包，都會受到此規則的控制。
- **Log** – 將符合規則的封包記錄到日誌緩衝區內，其中最多可以存放 64 筆資料。當日誌緩衝區存滿資料後，便會從頭開始覆寫最舊的資料。請注意，這份日誌是放在 RAM 裡面，交換器重設後其中的資料便會消失。

**Web** – 按下 Management Port=>Packet Filtering。輸入所需規則，接著按下「Add」。此範例中的規則會允許使用 TCP 通訊埠 10-30 的封包從來源位址 107.1.1 流到目的地位址 10.8.1.1。



**CLI** – 以下示範如何讓所有封包通過過濾器：允許任何通訊協定，並在來源位址與目的地位址輸入都是 0 的位址與網路遮罩。至於完整的設定範例，請參閱第 4-69 頁的 4.3.7.8 節「ip filter」。

```
Console(config)#ip filter permit any 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 4-69
Console(config)#
```

## SNMP – 對等 MIB 變數。

欄位名稱	MIB 變數	權限	設定值範圍	預設值
索引	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleIndex	不提供外界 存取	整數 (1-128)	
動作	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleAction	讀取/建立	permit (1), deny (2)	
Protocol	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleProtocol	讀取/建立	整數 (0-256, 其中 256 代表任何通訊協定)	
Source IP Address & Bitmask	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleSrcIpAddr & pfuRuleSrcIpBitmask	讀取/建立	IP 位址	
Source IP Port Range	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleSrcPortRange1 & pfuRuleSrcPortRange2	讀取/建立	整數 (1-65536)	
Destination IP Address & Bitmask	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleDstIpAddr & pfuRuleDstIpBitmask	讀取/建立	IP 位址	

欄位名稱	MIB 變數	權限	設定值範圍	預設值
Destination IP Port Range	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleDstPortRange1 & pfuRuleDstPortRange2	讀取/建立	整數 (1-65536)	
TCP Code	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleTcpCode	讀取/建立	整數 (0-63)	
TCP Code Bitmask	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleTcpCodeBitmask	讀取/建立	整數 (0-63)	
Fragments	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleFragments	讀取/建立	enabled (1), disabled (2)	disabled
Log	sun... securityMgt. packetFilterUnitMgt. pfuRuleTable. pfuRuleEntry. pfuRuleLog	讀取/建立	enabled (1), disabled (2)	disabled

## 3.5 監視通訊埠與管理流量

本節將說明交換器的監視功能，例如將流量複製到監視通訊埠以便進行分析，顯示任何通訊埠的詳盡網路統計數據，以及顯示通過管理連接埠的 SNMP 流量重要統計數據。

**注意：**Sun Fire B1600 Blade 系統機箱內整合的交換器，每一個都含有一對相互連接的交換器晶片。任何一個通訊埠上的流量，只能複製到位於同一交換器晶片上的其它通訊埠。連接埠 NETP0 到 NETP3 以及 SNP0 到 SNP7 位於同一顆交換器晶片上，連接埠 NETP4 到 NETP7 以及 SNP8 到 SNP15 則位於另一顆上。

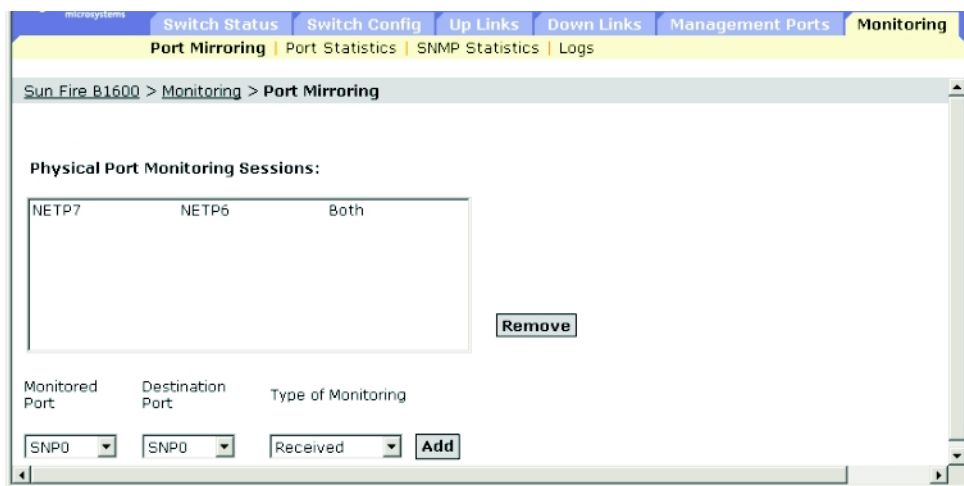
### 3.5.1 設定通訊埠鏡射

為了進行即時分析，您可以將任何通訊埠的流量鏡射複製一份到另一個通訊埠上，然後在後者接上一台邏輯分析儀或 RMON 探測器，在完全不妨礙原來的流量狀況下，仔細觀察流過此通訊埠的資料。

#### 指令使用方式

- 監視通訊埠的速度不應低於被監視通訊埠的速度，否則前者可能會丟棄部分流量。
- 監視通訊埠的流量時，原來的通訊埠以及用來監視的通訊埠兩者必須放在同一個 VLAN 內才行。

**Web** – 打開 Monitoring=>Port Mirror。指定要監視哪個通訊埠、要鏡射複製的流量種類、以及用哪個通訊埠進行監視，最後按下「Add」。



CLI – 先用 `interface` 指令選取用來監視的通訊埠，然後用 `port monitor` 指令挑選要監視的通訊埠。請注意，CLI 的預設監視功能對於接收進來與發送出去的封包都會進行監視。

```

Console(config)#interface ethernet NETP7                               4-74
Console(config-if)#port monitor ethernet NETP6                         4-142
Console(config-if)#

```

SNMP – 對等 MIB 變數。

欄位名稱	MIB 變數	權限	設定值範圍	預設值
Mirror Source Port	sun... mirrorMgt. mirrorTable.mirrorEntry. mirrorSourcePort	不可讀取	整數	
Mirror Destination Port	sun... mirrorMgt. mirrorTable.mirrorEntry. mirrorDestinationPort	不可讀取	整數	
Mirror Type	sun... mirrorMgt. mirrorTable.mirrorEntry. mirrorType	讀取/建立	rx (1), tx (2), both (3)	both
Mirror Status	sun... mirrorMgt. mirrorTable.mirrorEntry. mirrorStatus	讀取/建立	valid (1), invalid (2)	

### 3.5.2 顯示通訊埠統計數據

您可以將 `Interfaces Group` (介面群組) 與 `Ethernet-like` (類乙太網路) MIB 中的網路流量標準統計數據顯示出來，也可以根據 `RMON` MIB 將流量作進一步的分類。`Interfaces` 與 `Ethernet-like` 統計數據會顯示流過每個通訊埠流量中的錯誤，利用這些資訊便可找出交換器內可能潛在的問題 (例如有問題的連接埠或不正常的超高負荷量)。`RMON` 統計數據則可讓您看到非常廣泛的統計數據，包括流經每個連接埠的各種封包的數量與總資料量統計。所有的顯示數據都是從最近一次系統重新開機後就一直累計，以每秒鐘的個數為單位，且預設每 20 秒鐘重新顯示一次。

**注意：**RMON 群組 2、3 與 9 只能透過 SNMP 存取。

## 指令屬性

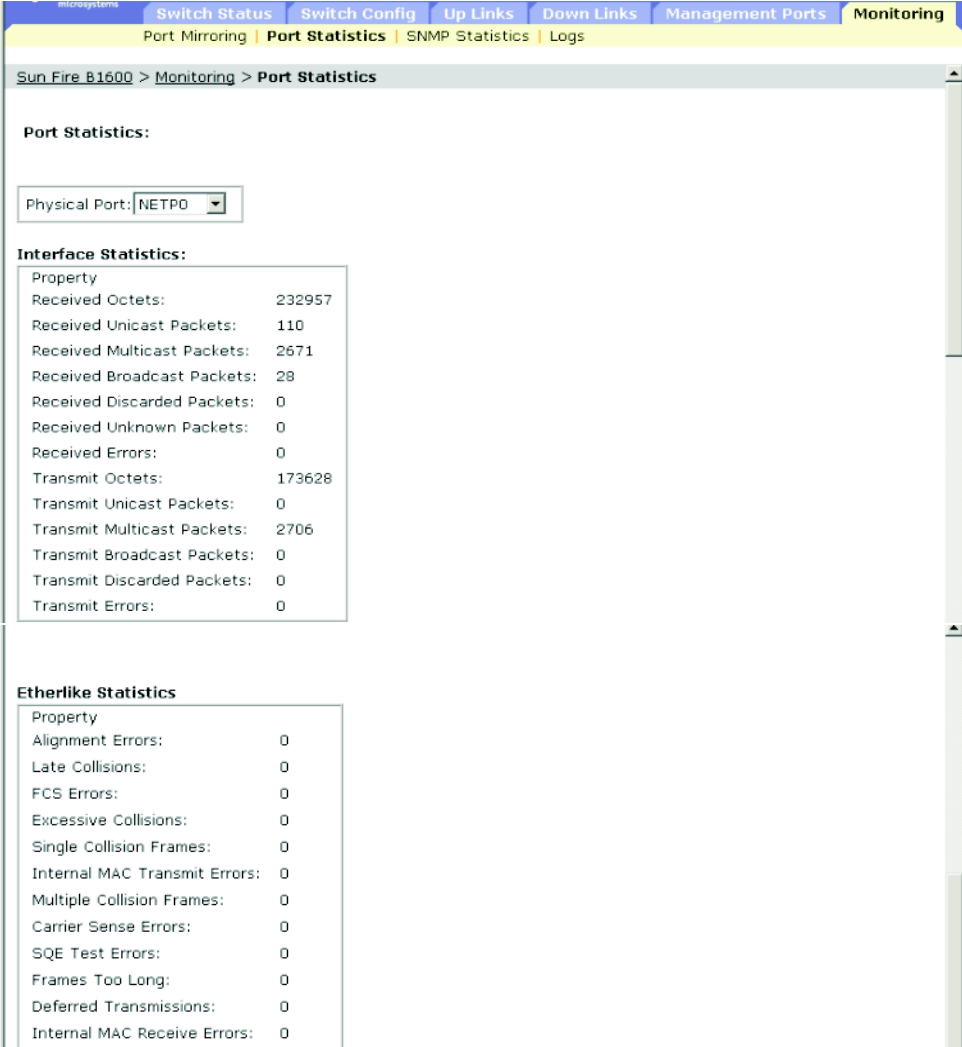
參數	說明
<i>Interface Statistics</i>	
Received Octets	此介面總共收到的位元組個數，包括用來分隔各封包的字元。
Received Unicast Packets	傳給更高層通訊協定處理的子網路單一目的地封包個數。
Received Multicast Packets	傳給更高層處理且其在這一層的目的地位址為群組廣播位址的封包個數。
Received Broadcast Packets	傳給更高層處理且其在這一層的目的地位址為廣播位址的封包個數。
Received Discarded Packets	即使未偵測到任何錯誤也必須將之丟棄的往內封包個數，以免它們被轉送給更高層的通訊協定。例如為了空出更多緩衝區空間，便是丟棄這類封包的其中一項原因。
Received Unknown Packets	經由此介面接收進來，但卻因為所含通訊協定不明或不支援而被丟棄的封包個數。
Received Errors	因含有錯誤而無法轉送到更高層通訊協定的流入封包個數。
Transmit Octets	經由此介面發送出去的位元組個數，包括用來分隔各封包的字元。
Transmit Unicast Packets	更高層通訊協定要求傳送給子網路單一目的位址的封包個數，包括被丟棄或未傳送出去的均涵蓋在內。
Transmit Multicast Packets	更高層通訊協定要求傳送出去、且以此層的群組廣播位址當作目的地位址的封包個數，包括被丟棄或未傳送出去的均涵蓋在內。
Transmit Broadcast Packets	更高層通訊協定要求傳送出去、且以此層的廣播位址當作目的地位址的封包個數，包括被丟棄或未傳送出去的均涵蓋在內。
Transmit Discarded Packets	即使未偵測到任何錯誤也必須將之丟棄的往外封包個數，以免它們被傳送出去。例如為了空出更多緩衝區空間，便是丟棄這類封包的其中一項原因。
Transmit Errors	由於發生錯誤而無法傳送出去的往外封包個數。

參數	說明
<i>Etherlike Statistics</i>	
Alignment Errors	對位錯誤（未同步的資料封包）次數。
Late Collisions	從封包開始發送後超過 512 個位元時間才發現有碰撞發生的次數。
FCS Errors	某個介面上所收到長度為整數個位元組但卻未通過 FCS 檢查的封包個數。此數字不包括有 <b>frame-too-long</b> （封包長度過長）以及 <b>frame-too-short</b> （封包長度過短）錯誤的封包。
Excessive Collisions	介面上由於碰撞情形過於頻繁而無法順利傳送出去的封包個數。當介面以全雙工模式運作時，此數字就不會增加。
Single Collision Frames	發送時只遇到一次碰撞後就順利傳送出去的封包個數。
Internal MAC Transmit Errors	介面上因為內部 MAC 次層級發生傳輸錯誤而無法順利發送出去的封包個數。
Multiple Collision Frames	發送時遇到一次以上碰撞但最後仍然順利傳送出去的封包個數。
Carrier Sense Errors	發送封包時，傳輸媒介感測條件被破壞甚至一直未曾恢復回來的次數。
SQE Test Errors	PLS 次層級為某個介面產生 SQE TEST ERROR 訊息的次數。
Frames Too Long	某個介面所收到超過最大允許長度的封包個數。
Deferred Transmissions	在介面上第一次發送時因為傳輸媒介繁忙而被迫延後的封包個數。
Internal MAC Receive Errors	介面上因為內部 MAC 次層級發生接收錯誤而無法順利收進來的封包個數。
<i>RMON Statistics</i>	
Drop Events	由於缺乏資源而導致封包被丟棄的事件個數。
Jabbers	收到長度超過 1518 位元組（扣掉分隔各封包的位元，但 FCS 位元組則計算在內）且有 FCS 或對位錯誤的封包個數。

參數	說明
Received Bytes	從這個網路上收到的資料位元組個數。此統計數據可用來合理推測出乙太網路的使用率。
Collisions	對此乙太網路網段上所發生碰撞總次數的最接近估計值。
Received Frames	接收到的封包總個數（包括有問題、廣播與群組廣播均計算在內）。
Broadcast Frames	所接收直接發給此廣播位址且毫無錯誤的封包個數。請注意，這並不包括群組廣播封包。
Multicast Frames	所接收直接發給此群組廣播位址且毫無錯誤的封包個數。
CRC/Alignment Errors	CRC/對位錯誤 (FCS 或對位錯誤) 個數。
Undersize Frames	所收到長度小於 64 個位元組（不含分隔封包的位元，但 FCS 位元組則計算在內），但除此之外無任何錯誤的封包個數。
Oversize Frames	所收到長度超過 1518 個位元組（不含分隔封包的位元，但 FCS 位元組則計算在內），但除此之外無任何錯誤的封包個數。
Fragments	所收到長度小於 64 位元組（扣掉分隔各封包的位元，但 FCS 位元組則計算在內）且有 FCS 或對位錯誤的片段封包個數。
64 Bytes Frames	所收到以及發送之長度正好為 64 個位元組（扣掉分隔各封包的位元，但 FCS 位元組則計算在內）的封包個數（包括有錯誤的封包）。
65-127 Byte Frames	所收到以及發送之封包長度落在指定範圍（扣掉分隔各封包的位元，但 FCS 位元組則計算在內）內的封包個數（包括有錯誤的封包）。
128-255 Byte Frames	
256-511 Byte Frames	
512-1023 Byte Frames	
1024-1518 Byte Frames	
1519-1536 Byte Frames	



Web – 按下 Monitoring=>Statistics。選取所需介面，接著按下「Select」。您也可以用網頁最下面的「Refresh」按鈕重新更新畫面。



Sun Fire B1600 > Monitoring > Port Statistics

Port Statistics:

Physical Port: NETPO

**Interface Statistics:**

Property	
Received Octets:	232957
Received Unicast Packets:	110
Received Multicast Packets:	2671
Received Broadcast Packets:	28
Received Discarded Packets:	0
Received Unknown Packets:	0
Received Errors:	0
Transmit Octets:	173628
Transmit Unicast Packets:	0
Transmit Multicast Packets:	2706
Transmit Broadcast Packets:	0
Transmit Discarded Packets:	0
Transmit Errors:	0

**Etherlike Statistics**

Property	
Alignment Errors:	0
Late Collisions:	0
FCS Errors:	0
Excessive Collisions:	0
Single Collision Frames:	0
Internal MAC Transmit Errors:	0
Multiple Collision Frames:	0
Carrier Sense Errors:	0
SQE Test Errors:	0
Frames Too Long:	0
Deferred Transmissions:	0
Internal MAC Receive Errors:	0

#### RMON Statistics

Property	
Drop Events:	0
Jabbers:	0
Received Bytes:	438662
Collisions:	0
Received Frames:	0
64 Bytes Frames:	5859
Broadcast Frames:	29
65-127 Bytes Frames:	97
Multicast Frames:	5869
128-255 Bytes Frames:	14
CRC/Alignment Errors:	0
256-511 Bytes Frames:	0
Undersize Frames:	0
512-1023 Bytes Frames:	2
Oversize Frames:	0
1024-1518 Bytes Frames:	40
Fragments:	0

CLI – 以下示範如何顯示 SNP13 連接埠的統計數據。

```
Console#show interfaces counters ethernet SNP13
Ethernet 13
Iftable stats:
  Octets input: 868453, Octets output: 3492122
  Unicast input: 7315, Unicast output: 6658
  Discard input: 0, Discard output: 0
  Error input: 0, Error output: 0
  Unknown protos input: 0, QLen output: 0
Extended iftable stats:
  Multi-cast input: 0, Multi-cast output: 17027
  Broadcast input: 231, Broadcast output: 7
Ether-like stats:
  Alignment errors: 0, FCS errors: 0
  Single Collision frames: 0, Multiple collision frames: 0
  SQE Test errors: 0, Deferred transmissions: 0
  Late collisions: 0, Excessive collisions: 0
  Internal mac transmit errors: 0, Internal mac receive errors: 0
  Frame too longs: 0, Carrier sense errors: 0
RMON stats:
  Drop events: 0, Octets:4422579, Packets: 31552
  Broadcast pkts: 238, Multi-cast pkts: 17033
  Undersize pkts: 0, Oversize pkts: 0
  Fragments: 0, Jabbers: 0
  CRC align errors: 0, Collisions: 0
  Packet size <= 64 octets:25568, Packet size 65 to 127 octets: 1616
  Packet size 128 to 255 octets:1249, Packet size 256 to 511 octets: 1449
  Packet size 512 to 1023 octets:802, Packet size 1024 to 1518 octets: 871
Console#
```

4-82

## SNMP – 對等 MIB 變數。

欄位名稱	MIB 變數	權限	範圍
<i>Interface Statistics</i>			
In Octets	MIB-II. interfaces.ifNumber.ifTable.ifEntry.ifInOctets	唯讀	整數
In Unicast Packets	MIB-II. interfaces.ifNumber.ifTable.ifEntry. ifInUcastPkts	唯讀	整數
In Multicast Packets	MIB-II. ifMIB.ifMIBObjects.ifXTable.ifXEntry. ifInMulticastPkts	唯讀	整數
In Broadcast Packets	MIB-II. ifMIB.ifMIBObjects.ifXTable.ifXEntry. ifInBroadcastPkts	唯讀	整數
In Discards	MIB-II. interfaces.ifTable.ifEntry.ifInDiscards	唯讀	整數
In Unknown Protocols	MIB-II. interfaces.ifTable.ifEntry.ifInUnknownProtos	唯讀	整數
In Errors	MIB-II. interfaces.ifTable.ifEntry.ifInErrors	唯讀	整數
Out Octets	MIB-II. interfaces.ifTable.ifEntry.ifOutOctets	唯讀	整數
Out Unicast Packets	MIB-II. interfaces.ifTable.ifEntry.ifOutUcastPkts	唯讀	整數
Out Multicast Packets	MIB-II. ifMIB.ifMIBObjects.ifXTable.ifXEntry. ifOutMulticastPkts	唯讀	整數
Out Broadcast Packets	MIB-II. ifMIB.ifMIBObjects.ifXTable.ifXEntry. ifOutBroadcastPkts	唯讀	整數
Out Discards	MIB-II. interfaces.ifTable.ifEntry.ifOutDiscards	唯讀	整數
Out Errors	MIB-II. interfaces.ifTable.ifEntry.ifOutErrors	唯讀	整數

欄位名稱	MIB 變數	權限	範圍
<i>Etherlike Statistics</i>			
Alignment Errors	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsAlignmentErrors	唯讀	整數
Late Collisions	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsLateCollisions	唯讀	整數
FCS Errors	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsFCSErrors	唯讀	整數
Excessive Collisions	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3Stats-ExcessiveCollisions	唯讀	整數
Single Collision Frames	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsSingleCollisionFrames	唯讀	整數
Internal Mac Transmit Errors	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsInternalMacTransmitErrors	唯讀	整數
Multiple Collision Frames	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsMultipleCollisionFrames	唯讀	整數
Carrier Sense Errors	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsCarrierSenseErrors	唯讀	整數
SQE Test Errors	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsSQETestErrors	唯讀	整數
Frames Too Long	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsFrameTooLongs	唯讀	整數
Deferred Transmissions	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsDeferredTransmissions	唯讀	整數
Internal MAC Receive Errors	MIB-II. transmission.dot3StatsTable.dot3StatsEntry. dot3StatsInternalMacReceiveErrors	唯讀	整數

欄位名稱	MIB 變數	權限	範圍
<i>RMON Statistics</i>			
Drop Events	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry. etherStatsDropEvents	唯讀	整數
Jabbers	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry. etherStatsJabbers	唯讀	整數
Received Octets	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry. etherStatsOctets	唯讀	整數
Collisions	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry. etherStatsCollisions	唯讀	整數
Received Packets	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry. etherStatsPkts	唯讀	整數
Broadcast Packets	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry. etherStatsBroadcastPkts	唯讀	整數
Multicast Packets	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry. etherStatsMulticastPkts	唯讀	整數
CRC/Alignment Errors	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry. etherStatsCRCAlignErrors	唯讀	整數
Undersize Packets	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry. etherStatsUndersizePkts	唯讀	整數
Oversize Packets	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry. etherStatsOversizePkts	唯讀	整數
Fragments	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry. etherStatsFragments	唯讀	整數
64 Bytes Frames	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry. etherStatsPkts64Octets	唯讀	整數
X-Y Byte Frames	MIB-II. rmon.statistics.etherStatsTable.etherStatsEntry. etherStatsPktsXtoYOctets	唯讀	整數

### 3.5.3 顯示 SNMP 統計數據

您可以顯示通過管理連接埠的 SNMP 流量主要統計數據。此資訊可用來檢查 SNMP 錯誤，或顯示交換器所處理的 SNMP 總流量，以及任何想透過 SNMP 連上此交換器的不良企圖。

#### 指令屬性

參數	說明
<i>SNMP packets input</i>	
SNMP packets input	從傳輸服務轉給 SNMP 功能的訊息個數。
Bad SNMP version errors	轉送給 SNMP 通訊協定功能但其版本不被支援的 SNMP 訊息個數。
Unknown community name	SNMP 通訊協定功能收到但卻不認得其中之 SNMP 群體名稱的 SNMP 訊息個數。
Illegal operation for community name supplied	轉送給 SNMP 通訊協定功能，但其 SNMP 群體名稱不允許其指定之 SNMP 動作的 SNMP 訊息個數。
Encoding errors	SNMP 通訊協定對所收到的 SNMP 訊息進行解碼時所碰到的 ASN.1 或 BER 錯誤個數。
Number of requested variables	SNMP 通訊協定功能收到正確的 SNMP Get-Request 與 Get-Next PDU 之後，成功取得的 MIB 物件個數。
Number of altered variables	SNMP 通訊協定功能收到正確的 SNMP Set-Request PDU 之後，成功更改的 MIB 物件個數。
Get-request PDUs	SNMP 通訊協定功能收到並處理完畢的 SNMP Get-Request PDU 個數。
Get-next PDUs	SNMP 通訊協定功能收到並處理完畢的 SNMP Get-Next PDU 個數。
Set-request PDUs	SNMP 通訊協定功能收到並處理完畢的 SNMP Set-Request PDU 個數。

參數	說明
<i>SNMP packets output</i>	
SNMP packets output	從 SNMP 通訊協定功能傳給傳輸服務的 SNMP 訊息個數。
Too big errors	轉送給 SNMP 通訊協定功能且其 error-status 為 tooBig 的 SNMP PDU 個數。
No such name errors	轉送給 SNMP 通訊協定功能且其 error-status 為 noSuchName 的 SNMP PDU 個數。
Bad values errors	轉送給 SNMP 通訊協定功能且其 error-status 為 badValue 的 SNMP PDU 個數。
General errors	轉送給 SNMP 通訊協定功能且其 error-status 為 genErr 的 SNMP PDU 個數。
Response PDUs	SNMP 通訊協定功能所產生的 SNMP Get-Response PDU 個數。
Trap PDUs	SNMP 通訊協定功能所產生的 SNMP Trap PDU 個數。

**Web** – 按下 Monitoring=>SNMP Statistics。您也可以用網頁最下面的「Refresh」按鈕重新更新畫面。

SNMP packets input:	
SNMP packets input	0
Bad SNMP version errors:	0
Unknown community name:	0
Illegal operation for community name supplied	0
Encoding errors	0
Number of requested variables	0
Number of altered variables	0
Get-request PDUs	0
Get-next PDUs	0
Set-request PDUs	0

SNMP packets output	
SNMP packets output	18
Too big errors	0
No such name errors	0
Bad values errors	0
General errors:	0
Response PDUs	0
Trap PDUs	18

CLI – 以下示範如何顯示交換器的 SNMP 統計數據。

```
Console#show snmp 4-52

SNMP traps:
  Authentication: enable
  Link-up-down: enable

SNMP communities:
  1. private, and the privilege is read/write
  2. public, and the privilege is read-only

11 SNMP packets input
  0 Bad SNMP version errors
  0 Unknown community name
  8 Illegal operation for community name supplied
  0 Encoding errors
  0 Number of requested variables
  1 Number of altered variables
  0 Get-request PDUs
  0 Get-next PDUs
  3 Set-request PDUs
11 SNMP packets output
  0 Too big errors
  0 No such name errors
  0 Bad values errors
  2 General errors
  3 Response PDUs
  0 Trap PDUs

SNMP logging: disabled
Console#
```

SNMP – 對等 MIB 變數。

欄位名稱	MIB 變數	權限	範圍
<i>SNMP packets input</i>			
In Packets	MIB-II.snmp.snmpInPkts	唯讀	整數
In Bad Versions	MIB-II.snmp.snmpInBadVersions	唯讀	整數
In Bad Community Names	MIB-II.snmp.snmpInBadCommunityNames	唯讀	整數
In Bad Community Uses	MIB-II.snmp.snmpInBadCommunityUses	唯讀	整數
In ASN Parse Errors	MIB-II.snmp.snmpInASNParseErrs	唯讀	整數



欄位名稱	MIB 變數	權限	範圍
In Total Request Variables	MIB-II.snmp.snmpInTotalReqVars	唯讀	整數
In Total Set Variables	MIB-II.snmp.snmpInTotalSetVars	唯讀	整數
In Get Requests	MIB-II.snmp.snmpInGetRequests	唯讀	整數
In Get Nexts	MIB-II.snmp.snmpInGetNexts	唯讀	整數
In Set Requests	MIB-II.snmp.snmpInSetRequests	唯讀	整數
Silent Drops	MIB-II.snmp.snmpSilentDrops	唯讀	整數
Proxy Drops	MIB-II.snmp.snmpProxyDrops	唯讀	整數
<i>SNMP packets output</i>			
Out Packets	MIB-II.snmp.snmpOutPkts	唯讀	整數
Out Too Bigs	MIB-II.snmp.snmpOutTooBigs	唯讀	整數
Out No Such Names	MIB-II.snmp.snmpOutNoSuchNames	唯讀	整數
Out Bad Values	MIB-II.snmp.snmpOutBadValues	唯讀	整數
Out General Errors	MIB-II.snmp.snmpOutGenErrs	唯讀	整數
Out Get Responses	MIB-II.snmp.snmpOutGetResponses	唯讀	整數
Out Traps	MIB-II.snmp.snmpOutTraps	唯讀	整數

## 3.5.4 設定訊息日誌

您可以根據嚴重程度限制存入交換器記憶體的系统日誌訊息。

### 指令屬性

- **Enable Logging** – 將除錯或錯誤訊息記錄到交換器記憶體內。(預設值：Disabled)
- **Logging Level** – 根據嚴重程度限制存入交換器記憶體內的系統日誌訊息。請注意，從選定層級開始一直往下到 0 這個層級的訊息都會儲存起來。(範圍：7-0，預設值 – Flash：3-0，RAM：7-0)

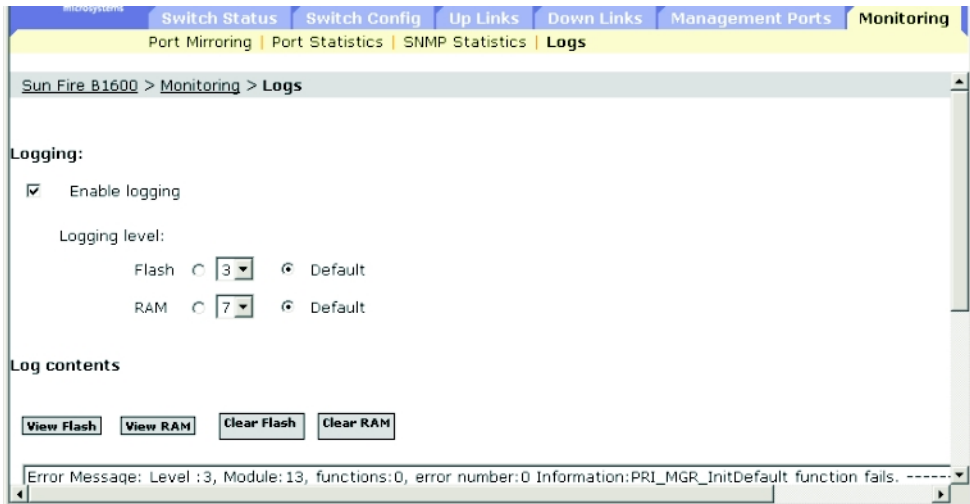
表 3-1 錯誤層級

層級參數	層級	說明
debugging	7	除錯訊息
informational	6	一般訊息 (例如所有 trap)
notifications	5	值得注意的一般訊息, 例如冷開機
warnings	4	警告狀態 (例如收到錯誤或預期以外的答案)
errors	3	錯誤狀況 (例如錯誤輸入, 此為預設值)
critical	2	重大狀況 (例如記憶體配置錯誤、記憶體釋放錯誤、資源耗進等等)
alerts	1*	需要立即處理
emergencies	0*	系統不堪使用

\* 目前此軟體版本不會發出層級 0 與層級 1 的錯誤訊息。

- **Log contents** – 有按鈕可以讓您列出 Flash 與 RAM 中存放的所有系統與事件訊息，亦可清除 Flash 記憶體 (系統重新開機後仍保有原來資料的記憶體) 或 RAM (系統開機後原來資料便全部消失的隨機存取記憶體) 內的日誌訊息。

**Web** – 按下 Monitoring=>Logs。啓用日誌功能，按下 flash 或 RAM，選取要記錄的訊息層級 (從此層級到 0 的訊息都會記錄下來)，最後按下「Save Changes」。按下「View Flash」或「View RAM」便可更新所顯示的訊息。



**CLI** – 以下示範如何啓動日誌功能、將 Flash 記憶體記錄的訊息設定爲層級 3 (即 errors 這個層級) 以及如何顯示 Flash 內存放的日誌訊息。

```

Console(config)#logging on                                4-30
Console(config)#logging history flash                    4-31
Console#show logging flash                              4-33
Syslog logging: Enable
History logging in FLASH: level errors
[0] 0:0:5 1/1/1
    "PRI_MGR_InitDefault function fails."
    level: 3, module: 13, function: 0, and event no.: 0
Console#

```

**SNMP** – 對等 MIB 變數。

欄位名稱	MIB 變數	權限	設定值範圍	預設值
Log Status	sun... sysLogMgt. sysLogStatus	可讀寫	enabled (1), disabled (2)	
History Flash Level	sun... sysLogMgt. sysLogStatus.sysLog.HistoryFlashLevel	可讀寫	整數 (0-7)	
History RAM Level	sun... sysLogMgt. sysLogStatus.sysLog.HistoryRAMLevel	可讀寫	整數 (0-7)	
Log Messages	未定義。			



# 指令行參考資料

---

本章說明指令行介面 (Command Line Interface，簡稱 CLI) 的使用方式。

## 4.1 使用指令行介面

### 4.1.1 連上 CLI

透過直接連線接上伺服器的主控台連接埠或用 Telnet 連上交換器的管理介面後，便可以在提示符號後輸入指令關鍵字與參數對交換器進行管理。此交換器的指令行介面 (CLI) 使用方式與在 UNIX 系統上輸入指令的方式很類似。

#### 4.1.1.1 主控台連線

若要透過主控台連接埠連上交換器，請依照以下步驟進行：

1. 在主控台提示符號後輸入使用者名稱與密碼。(預設使用者名稱有兩組，帳號與密碼分別都是 admin 與 guest) 若輸入的是管理員的使用者名稱與密碼，CLI 就會顯示 Console# 提示符號，並進入特權存取模式 (即 Privileged Exec)。但若輸入的是來賓 (guest) 使用者名稱與密碼，CLI 就會顯示 Console> 提示符號，並進入一般存取模式 (即 Normal Exec)。
2. 依照您的需要輸入適當指令完成工作。
3. 完成後，輸入 quit 或 exit 指令結束連線。

以下是透過主控台連接埠連上系統時的登入畫面：

```
User Access Verification

Username: admin
Password:

      CLI session with the Sun Fire B1600 is opened.
      To end the CLI session, enter [Exit].

Console#
```

### 4.1.1.2 Telnet 連線

由於 telnet 是利用 IP 傳輸通訊協定運作的，因此在這個環境中，管理主機與任何您想透過網路管理的網路裝置，都必須各有正確的 IP 位址。正確的 IP 位址由四個 0 到 255 的數字組成，各數字之間以小數點隔開。每個位址都由網路部分和主機部分組成，例如 IP 位址 10.1.0.1 的網路部分就是 10.1.0，主機部分則是 1。

---

**注意：**此交換器的 IP 位址預設並沒有設定，其管理連接埠 (NETMGT) 設定屬於 VLAN 2，而且無法設定給含有上連或下連連接埠的 VLAN。

---

若要透過 telnet 連上交換器，首先要先設定交換器的位址，如果要從另一個 IP 子網路連上交換器，則還必須為交換器設定預設閘道。例如：

```
Console(config)#interface vlan 2
Console(config-if)#ip address 10.1.0.1 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 10.1.0.254
```

如果您的公司網路要連到辦公室以外的網路甚至連上網際網路，則您必須另外申請一個註冊 IP 位址。但如果您連接的是一個與外界隔絕的網路，只要是符合您所在區域網路使用規範的 IP 位址都可以使用。

設定好交換器的 IP 位址之後，依照以下步驟便可用 telnet 連上交換器：

1. 在遠端主機上，輸入 telnet 指令以及您想連上之裝置的 IP 位址。
2. 在提示符號後輸入使用者名稱與系統密碼，CLI 便會顯示管理員專用的 Vty-0# 提示符號，提醒您現在使用的是特權存取模式 (Privileged Exec)，或顯示來賓專用的 Vty-0>，提醒您現在使用的是一般存取模式 (Normal Exec)。
3. 依照您的需要輸入適當指令完成工作。
4. 完成後，輸入 quit 或 exit 指令結束連線。

以下是輸入 telnet 指令後的登入畫面：

```
Username: admin
Password:

          CLI session with the Sun Fire B1600 is opened.
          To end the CLI session, enter [Exit].

Vty-0#
```

---

**注意：**交換器可讓外界同時以 telnet 建立 4 條連線。

---

## 4.1.2 輸入指令

本節說明如何輸入 CLI 指令。

### 4.1.2.1 關鍵字與引數

每一個 CLI 指令都是由一連串的關鍵字與引數組成，其中關鍵字代表指令本身，引數則是所需的組態設定值，例如 show interfaces status ethernet SNP5 這個指令中，**show interfaces** 與 **status** 為關鍵字，**ethernet** 則是指定介面種類的引數，而 **SNP5** 則指定連接埠。

指令的輸入方式有以下幾種：

- 如果是輸入一個簡單指令，只要輸入指令關鍵字即可。
- 若要輸入好幾個指令，請依照所需順序依序輸入每個指令。例如要啓動 Privileged Exec 指令模式，接著還要顯示開機組態，請輸入：

```
Console>enable  
Console#show startup-config
```

- 如果輸入的指令需要參數，請將所需參數放在指令關鍵字之後。例如要設定管理員的密碼，請輸入：

```
Console(config)#username admin password 0 smith
```

#### 4.1.2.2 最短縮寫

只要您輸入的字元個數已經足以分辨出來是哪個指令，CLI 都會接受，例如 `logging history` 這個指令就可以簡短輸入成 `logging h`。如果輸入的字還無法看出是哪一個指令，系統會出現提示要求您多輸入一點。

#### 4.1.2.3 指令補齊

輸入指令中途若按下 `Tab` 鍵，CLI 便會將關鍵字剩下的字元補齊到不會模稜兩可的地方。例如上述 `logging history` 範例中，輸入 `log` 之後馬上按下 `tab` 鍵，CLI 便會將此指令剩下的字元印出來，變成 `logging`。

#### 4.1.2.4 取得指令的說明

輸入 `help` 指令便可看到輔助說明系統的簡短描述。您也可以使用 `?` 字元顯示指令的語法，將關鍵字和參數全部列出來。



## 4.1.2.5 顯示指令

在提示符號後輸入？，系統便會顯示目前指令類別 (Normal Exec 或 Privileged Exec) 或組態類別 (Global、Interface、Line 或 VLAN Database) 的第一層關鍵字。您也可以顯示任何指令可以用的關鍵字，例如輸入 **show ?** 便會顯示出所有可以使用的 **show** 指令：

```
Console#show ?
  bridge-ext      Bridge extend information
  garp             Garp property
  gvrp            Show gvrp information of interface
  history         Information of history
  interfaces      Information of interfaces
  ip              Ip
  line            TTY line information
  logging         Show the contents of logging buffers
  mac-address-table Set configuration of the address table
  map             Map priority
  port            Characteristics of the port
  queue          Information of priority queue
  radius-server   Radius server information
  running-config The system configuration of running
  snmp           SNMP statistics
  spanning-tree   Specify spanning-tree
  startup-config  The system configuration of starting up
  system         Information of system
  tacacs-server   Login by tacacs server
  users           Display information about terminal lines
  version         System hardware and software status
  vlan           Switch VLAN Virtual Interface
Console#show
```

**show interfaces ?** 這個指令會顯示以下資訊：

```
Console>show interfaces ?
  counters      Information of interfaces counters
  status        Information of interfaces status
  switchport    Information of interfaces switchport
```

### 4.1.2.6 不完整關鍵字查詢

若只輸入關鍵字的一部份，後面緊跟著一個問號，便可看到所有以這些字元開頭的全部關鍵字。(請注意指令與問號之間不可以有空格。)例如 's?' 便會顯示所有以 s 開頭的關鍵字。

```
Console#show s?  
snmp          spanning-tree  startup-config  system
```

### 4.1.2.7 反轉指令的效果

許多組態設定指令前面都可以加上 **no** 這個關鍵字，取消該指令的作用或將組態重設回預設值。例如 **logging** 指令本來會將系統訊息傳到主機伺服器上，不過如果改成輸入 **no logging** 指令，此功能便會取消。本文會說明所有可用指令的反轉效果。

### 4.1.2.8 使用指令歷程

CLI 會記住您最近輸入過的指令，只要按往上鍵就可以往回翻閱。其中顯示的任何指令都可以拿來再度執行，也可以先經修改後再執行。

**show history** 指令則可顯示比較多最近執行過的指令。

### 4.1.2.9 了解指令模式

此交換器的指令集共分為 **Exec** (執行) 與 **Configuration** (組態設定) 兩種類別。**Exec** 指令一般用於顯示系統狀態資訊或清除統計數據的計數器；**Configuration** 指令則是用於修改介面參數或啟動某些交換功能。這兩種指令又可再細分為幾種不同的模式。任何狀況下有哪些指令可以使用，均取決於當時的指令模式。在提示符號後輸入問號 '?'，則可列出當時模式所提供的全部指令。以下列出所有的指令類別與相關模式：

類別	模式
Exec	Normal (一般)
	Privileged (特權)
Configuration*	Global (全區)
	Interface (介面)
	Line (線路)
	VLAN Database (VLAN 資料庫)

\* 必須先進入 Privileged Exec 模式，才可以使用任何一種組態設定模式。

## 4.1.2.10 Exec 指令

使用 `guest` 這個使用者名稱與密碼連上交換器開啓新的主控台連線時，系統便會進入 `Normal Exec` 指令模式 (又稱來賓模式)，並顯示 `Console>` 指令提示符號。此模式中只能使用部分指令。只有 `Privileged Exec` 指令模式 (亦稱管理員模式) 才能使用到所有的指令。要進入 `Privilege Exec` 模式，請用 `admin` 這組使用者名稱與密碼開啓新的主控台連線，系統便會顯示 `Console#` 提示符號。或者，在 `Normal Exec` 模式中輸入 `enable` 指令，然後再輸入特權層級密碼 `super`，亦可進入 `Privileged Exec` 模式 (參閱第 4-27 頁)。

輸入以下使用者名稱與密碼，便可進入 `Privileged Exec` 模式：

```
Username: admin
Password: [admin login password]

      CLI session with the Sun Fire B1600 is opened.
      To end the CLI session, enter [Exit].

Console#
```

```
Username: guest
Password: [guest login password]

      CLI session with the Sun Fire B1600 is opened.
      To end the CLI session, enter [Exit].

Console>enable
Password: [privileged level password]
Console#
```

## 4.1.2.11 組態設定指令

組態設定指令是用來修改交換器設定值的特權層級指令，但只會修改目前使用的組態而已，其修改的部分到下次交換器重新開機時便會消失。若要將使用中的組態存到失去電力時資料也不會遺失的儲存區域內，請使用 **copy running-config startup-config** 指令。

所有組態設定指令劃分成以下幾種模式：

- Global Configuration (全區組態) – 這些指令會修改系統層級的組態，包括 **hostname** 與 **snmp-server community** 之類的指令都屬於此模式。
- Interface Configuration (介面組態) – 修改連接埠組態的指令，例如 **speed-duplex** 與 **negotiation**。
- Line Configuration (線路組態) – 修改主控台連接埠與 telnet 組態，例如 **exec-timeout** 與 **silent-time** 等指令都包括在內。
- VLAN Configuration (VLAN 組態) – 建立 VLAN 群組的指令。

若要進入「Global Configuration」模式，請在「Privileged Exec」模式中輸入 **configure** 指令，系統提示符號便會改成 **Console(config)#**，讓您可以使用所有的 Global Configuration 指令。

```
Console#configure
Console(config)#
```

若要進入其它模式，請在組態設定提示符號後輸入以下任何一個指令。**exit** 指令可回到「Configuration」模式，**end** 指令則可回到「Privileged Exec」模式。

模式	指令	提示	參閱頁數
Interface	interface {ethernet <i>port</i>   port-channel <i>id</i>   vlan <i>id</i> }	Console(config-if)#	4-74
Line	line {console   vty}	Console(config-line)#	4-55
VLAN	vlan database	Console(config-vlan)	4-105

例如您可以先用以下指令進入介面組態設定模式，然後再回到「Privileged Exec」模式。

```
Console(config)#interface ethernet SNP5
.
.
.
Console(config-if)#exit
Console(config)
```

#### 4.1.2.12 指令行的處理方式

交換器接收指令時並不區分英文字母的大小寫，而且您也可以用縮寫的方式輸入指令和參數，只要輸入的字元夠多，足以與目前可用的任何其它指令或參數分辨即可。此外，您也可以用 **Tab** 鍵將沒有打完整的指令補齊，或者輸入指令的一部份，後面緊跟著？字元，便會看到所有開頭是這些字元的關鍵字。以下列出可以用來處理指令行的編輯按鍵：

按鍵	功能
Ctrl-A	將游標移到指令行開頭。
Ctrl-B	將游標往左移動一個字元。
Ctrl-E	將游標移到指令行尾端。
Ctrl-F	將游標往右移動一個字元。
Ctrl-P	顯示最後一個指令。
Ctrl-U	將整行刪除。
Ctrl-W	刪除最後輸入的字。
Delete 鍵或 backspace 鍵	消掉輸入指令時打錯的地方。

## 4.2 指令群組

系統指令可分類為好幾個功能群組，如下所示。

指令群組	說明	頁數
一般	進入特權存取模式、重新啓動系統與跳出 CLI 的基本指令	4-11
Flash/ 檔案	程式碼映像與交換器組態檔案管理	4-17
系統管理	控制系統日誌、系統密碼、使用者名稱、瀏覽器管理選項以及其他各式各樣的系統資訊	4-24
認證	設定使用交換器本身資料庫、RADIUS 或 TACACS 對登入者進行身分認證	4-41
SNMP	啓動認證失敗 trap、設定群體存取字串與 trap 管理員	4-48
線路	設定序列連接埠與 telnet 的連線選項，包括密碼檢查與主控台逾時時間	4-54
IP	設定連線進行管理所需的 IP 位址與閘道、顯示預設閘道以及 ping 指定裝置	4-62
介面	設定所有乙太網路連接埠、集束線路與 VLAN 的連線參數	4-73
位址表	設定過濾特定位址所需的位址表、顯示目前所含項目、清除此位址表以及設定保留期限	4-85
連接埠安全性	設定連接埠的安全位址	4-89
Spanning Tree	設定交換器的 Spanning Tree 組態	4-91
VLAN	設定 VLAN 組態以及定義 VLAN 群組含有哪些連接埠	4-104
GVRP 與 Bridge 擴充功能	設定進行自動 VLAN 學習所需的 GVRP 組態，以及顯示橋接擴充功能 MIB 的組態。	4-114
IGMP Snooping	設定 IGMP 群組廣播過濾功能，查詢者資格、查詢參數以及接上群組廣播的是哪些連接埠	4-120
優先等級	設定未加註任何標籤之封包的連接埠優先等級、各優先佇列的相對權重、最多啓動多少個佇列、以及 IP 優先權與 DSCP 的優先等級	4-131
鏡射連接埠	將資料鏡射複製到另一個連接埠進行分析，以免影響流經被監視連接埠的資料或效能	4-142
連接埠寬道與 LACP	將數個連接埠固定組成一條邏輯寬道，以及設定連接埠寬道的 Link Aggregation Control Protocol (線路及數控制通訊協定)	4-144

以下各表格提到各種存取模式時所使用的縮寫意義如下：

**NE** (Normal Exec，一般執行)      **LC** (Line Configuration，線路組態)  
**PE** (Privileged Exec，特權執行)    **VC** (VLAN Database Configuration，  
VLAN 資料庫組態)  
**GC** (Global Configuration，全區組態)  
**IE** (Interface Configuration，介面組態)

---

## 4.3 指令詳細說明

### 4.3.1 一般指令

指令	功能	模式	頁數
enable	啓動特權模式	NE	4-12
disable	從特權模式轉回一般模式	PE	4-13
configure	啓動全區組態模式	PE	4-13
show history	顯示指令歷程緩衝區	NE、 PE	4-14
reload	重新啓動系統	PE	4-15
end	回到「Privileged Exec」模式	GC, IC, LC, VC	4-15
exit	回到前一個組態模式，或離開 CLI	任意	4-16
quit	結束 CLI 連線	NE、 PE	4-16
help	顯示輔助說明的使用方式	任意	NA
?	顯示已輸入的部分字元有可能是哪些指令或參數的開頭 (視當時狀況而定)	任意	NA

### 4.3.1.1 enable

此指令可啓動「Privileged Exec」模式。在特權模式中，不僅多了一些指令可以使用，而且有些指令還會顯示較多的訊息。請參閱第 4-6 頁的「了解指令模式」。

#### 語法

**enable** [*level*]

*level* - 登入裝置的特權等級。

此裝置有兩種特權等級：0: Normal Exec、15: Privileged Exec。進入層級 15 即可進入「Privileged Exec」模式。

#### 預設設定

層級 15

#### 指令模式

Normal Exec

#### 指令使用方式

- 'super' 是指令模式從「Normal Exec」切換成「Privileged Exec」時所需的預設密碼。(此密碼的設定方式請參閱第 4-27 頁，關於 **enable password** 指令的說明。)
- 緊跟在提示字串後面的 # 字元，用意在於提醒使用者目前系統處在特權存取模式。

#### 範例

```
Console>enable
Password: [privileged level password]
Console#
```

#### 相關指令

disable (4-13)

enable password (4-27)



### 4.3.1.2 disable

使用此指令可從特權模式回到「Normal Exec」模式。在一般存取模式中，只能顯示交換器組態的基本資訊與乙太網路統計數據。若要能使用所有指令，必須使用特權模式才行。請參閱第 4-6 頁的「了解指令模式」。

#### 預設設定

無

#### 指令模式

Privileged Exec

#### 指令使用方式

提示字串後面會緊個著一個 '>' 字元，表示系統目前處於一般存取模式。

#### 範例

```
Console#disable  
Console>
```

#### 相關指令

enable (4-12)

### 4.3.1.3 configure

此指令可啟動「Global Configuration」模式，只有在這個模式中才能修改交換器的設定，而且啟動其它幾種組態設定模式之前，例如「Interface Configuration」、「Line Configuration」與「VLAN Database Configuration」等等，也都必須先進入「Global Configuration」模式。請參閱第 4-6 頁的「了解指令模式」。

#### 預設設定

無

#### 指令模式

Privileged Exec

#### 範例

```
Console#configure  
Console(config)#
```

## 相關指令

end (4-15)

### 4.3.1.4 show history

顯示指令歷程緩衝區的內容。

#### 預設設定

無

#### 指令模式

Normal Exec、Privileged Exec

#### 指令使用方式

歷程緩衝區的大小是固定的，只能存放 10 個 Execution (執行) 指令與 10 個 Configuration (組態設定) 指令。

#### 範例

以下示範如何用 show history 指令將指令歷程緩衝區中的內容顯示出來：

```
Console#show history
Execution command history:
 2 config
 1 show history

Configuration command history:
 4 interface vlan 1
 3 exit
 2 interface vlan 1
 1 end

Console#
```

驚嘆號！指令在「Normal Exec」或「Privileged Exec」模式中可重複 Execution 指令歷程緩衝區中的指令，在任何一個組態設定模式中則可重複 Configuration 指令歷程緩衝區中的指令。以下範例中的 !2 指令，便會重複 Execution 歷程緩衝區 (config) 中的第二個指令。

```
Console#!2
Console#config
Console(config)#
```

### 4.3.1.5 reload

此指令可重新啓動系統。

---

**注意：**系統重新啓動時，都會執行 Power-On Self-Test (開機自我測試)，同時也會保留 **copy running-config startup-config** 指令存放在非揮發記憶體中的所有組態資訊。

---

#### 預設設定

無

#### 指令模式

Privileged Exec

#### 指令使用方式

此指令會重設整個系統。

#### 範例

以下示範如何重設交換器：

```
Console#reload
System will be restarted, continue <y/n>? y
```

### 4.3.1.6 end

此指令可返回「Privileged Exec」模式。

#### 預設設定

無

#### 指令模式

Global Configuration, Interface Configuration, Line Configuration, VLAN Database Configuration, Router Configuration

#### 範例

以下示範如何從「Interface Configuration」模式回到「Privileged Exec」模式：

```
Console(config-if)#end
Console#
```

### 4.3.1.7 exit

此指令可回到前一個組態設定模式或結束組態設定程式。

#### 預設設定

無

#### 指令模式

任意

#### 範例

以下示範如何先從「Global Configuration」模式回到「Privileged Exec」模式，然後再結束 CLI 連線：

```
Console(config)#exit
Console#exit

Press ENTER to start session

User Access Verification

Username:
```

### 4.3.1.8 quit

此指令可結束 CLI 連線。

#### 預設設定

無

#### 指令模式

Normal Exec、Privileged Exec

#### 指令使用方式

**quit** 與 **exit** 兩個指令都可以結束組態設定程式。

## 範例

以下示範如何結束 CLI 連線：

```
Console#quit

Press ENTER to start session

User Access Verification

Username:
```

## 4.3.2 Flash/檔案指令

這些指令可用來管理系統程式碼與組態檔案。

指令	功能	模式	頁數
copy	將程式碼映像或交換器組態複製到 Flash 記憶體或 TFTP 伺服器上，或從 Flash 記憶體或 TFTP 伺服器上複製出來	PE	4-17
delete	刪除檔案或程式碼映像	PE	4-20
dir	將 Flash 記憶體中的檔案列出來	PE	4-21
whichboot	顯示用來開機的檔案	PE	4-22
boot system	設定系統啟動所使用的檔案或映像	GC	4-23

### 4.3.2.1 copy

此指令可將程式碼映像與組態檔案在交換器 Flash 記憶體與 TFTP 伺服器之間移動（就是上傳和下載）。將系統程式碼或組態設定存到 TFTP 伺服器上的檔案，以後就可以將這個檔案下載到交換器上讓系統恢復運作。檔案的傳輸是否能成功，TFTP 伺服器是否正常運作以及網路連線品質為最重要的兩個因素。

#### 語法

```
copy file {file | running-config | startup-config | tftp}
copy running-config {file | startup-config | tftp}
copy startup-config {file | running-config | tftp}
copy tftp {file | running-config | startup-config}
copy tftp https-certificate
```

- **file** – 關鍵字，表示要將檔案中的內容複製出來，或將資料複製到檔案中存放。
- **running-config** – 關鍵字，表示要將目前執行的組態複製一份，或將資料複製成目前執行的組態使用。
- **startup-config** – 系統啟動時所使用的組態。
- **tftp** – 關鍵字，表示要從 TFTP 伺服器複製檔案，或將檔案複製到 TFTP 伺服器上存放。
- **https-certificate** – 指定使用交換器認得的憑證核發單位所發出的憑證、私密鍵與密碼。

## 預設設定

無

## 指令模式

Privileged Exec

## 指令使用方式

- 系統會提示您輸入完成 **copy** 指令所需的資料。
- 目的組態檔案名稱不可以含有斜線 (包括 \ 與 /)，檔案名稱開頭不可以是小數點 (.)，且 TFTP 伺服器上檔案名稱的長度不可超過 127 個字元，交換器上的檔案名稱長度不可超過 32 個字元。(可用字元：A-Z、a-z、0-9、.、-、\_)
- 由於 **flash** 記憶體容量有限，交換器內只放得下兩份作業程式碼檔案。
- 使用者定義的組態檔案個數需視可用記憶體的容量而定。
- 複製檔案時，**Factory\_Default\_Config.cfg** 可以當作來源檔案使用，代表交換器的出廠預設組態檔案，但是不可以當作複製動作的目的地。
- 以 **startup-config** 當作目的地，便可取代開機組態。
- **Boot ROM** 與 **Loader** 程式碼不可以上傳到 TFTP 伺服器上，也不能從 TFTP 伺服器上下載回來。**Boot ROM** 與 **Loader** 程式碼的更換一定要由 Sun 維修工程師處理才行。

## 範例

以下示範如何將組態設定上傳到 TFTP 伺服器上存成檔案：

```
Console#copy file tftp
Choose file type:
 1. config: 2. opcode: <1-2>: 1
Source file name: startup
TFTP server ip address: 10.1.0.99
Destination file name: startup.01
TFTP completed.
Success.

Console#
```

以下示範如何將執行中的組態複製到檔案。

```
Console#copy running-config file
destination file name : startup
Write to FLASH Programming.
\Write to FLASH finish.
Success.

Console#
```

以下示範如何下載組態檔案：

```
Console#copy tftp startup-config
TFTP server ip address: 10.1.0.99
Source configuration file name: startup.01
Startup configuration file name [startup]:
Write to FLASH Programming.
\Write to FLASH finish.
Success.

Console#
```

以下示範如何將安全憑證存放到 TFTP 伺服器上，然後將交換器重新啓動，讓憑證開始生效。

```
Console#copy tftp https-certificate

      TFTP server ip address: 10.1.0.19
      Source certificate file name: SS-certificate

      Source private file name: SS-private
      Private password: *****

Success.
Console#reload
System will be restarted, continue <y/n>? y
```

### 4.3.2.2 delete

此指令可刪除檔案或映像。

#### 語法

**delete** *filename*

*filename* – 組態檔案或映像的名稱。

#### 預設設定

無

#### 指令模式

Privileged Exec

#### 指令使用方式

- boot-ROM 檔案與開機使用的檔案都是無法刪除的。
- 'Factory\_Default\_Config.cfg' 也是無法刪除的。

#### 範例

以下示範如何刪除 Flash 記憶體中的組態檔案 test2.cfg。

```
Console#delete test2.cfg
Console#
```

#### 相關指令

dir (4-21)



### 4.3.2.3 dir

此指令可將 Flash 記憶體中的檔案列出。

#### 語法

**dir [boot-rom | config | opcode [:filename]]**

可顯示的檔案與映像種類包括：

- **boot-rom** – Boot ROM
- **config** – 組態檔案
- **opcode** – 檔案或映像的名稱。若指定的檔案存在但是其中有問題，該檔案內的資訊就無法顯示出來。
- **filename** – 要顯示之檔案的名稱。

#### 預設設定

無

#### 指令模式

Privileged Exec

#### 指令使用方式

- 輸入 **dir** 指令時若不帶任何參數，系統便會將所有檔案全部顯示出來。
- 以下說明各項檔案資訊：

表 4-1 檔案資訊

欄位標題	說明
file name	檔案的名稱。
file type	檔案類型：Boot-Rom、Operation Code (作業程式碼) 或 Config (組態) 檔案。
startup	若系統開機時會用到這個檔案，則此欄位便會顯示出來。
size	檔案大小，以位元組為單位。

## 範例

以下示範如何將所有檔案資訊全部顯示出來：

```
Console#dir
```

file name	file type	startup	size (byte)
diag_0060	Boot-Rom image	Y	111360
run_01642	Operation Code	N	1074304
run_0200	Operation Code	Y	1083008
Factory_Default_Config.cfg	Config File	N	2574
startup	Config File	Y	2710

```
-----  
Total free space: 0  
Console#
```

### 4.3.2.4 whichboot

此指令會顯示系統電源開啓時用哪些檔案開機。

#### 預設設定

無

#### 指令模式

Privileged Exec

#### 指令使用方式

關於此指令顯示的檔案資訊，請參閱第 4-21 頁的表 4-1。

## 範例

以下範例顯示 **whichboot** 所列出的資訊

```
Console#whichboot
```

file name	file type	startup	size (byte)
diag_0060	Boot-Rom image	Y	111360
run_0200	Operation Code	Y	1083008
startup	Config File	Y	2710

```
Console#
```

## 4.3.2.5 boot system

此指令可設定系統開機啓動時所使用的檔案與映像。

### 語法

**boot system** {**boot-rom** | **config** | **opcode**}: *filename*

可當作預設值的檔案與映像種類包括：

- **boot-rom** – Boot ROM
- **config** – 組態檔案
- **opcode** – 執行時期作業程式碼

冒號 (:) 一定要輸入。

*filename* – 組態檔案或映像的名稱。

### 預設設定

無

### 指令模式

Global Configuration

### 指令使用方式

- 指定檔案類別後面一定要跟著一個冒號 (:)。
- 檔案內容如果有問題，就不可以當作預設檔案。

### 範例

```
Console(config)#boot system config: startup
Console(config)#
```

### 相關指令

dir (4-21)

whichboot (4-22)

## 4.3.3 系統管理指令

此指令可用來控制系統日誌、密碼、使用者名稱、瀏覽器組態選項以及顯示或設定系統其它各種資訊。

指令	功能	模式	頁數
<i>裝置描述指令</i>			
hostname	設定或修改裝置的主機名稱	GC	4-24
<i>使用者存取指令</i>			
username	建立根據使用者名稱進行認證的系統，以便登入時使用	GC	4-25
enable password	設定密碼控制「Privileged Exec」層級的存取權	GC	4-27
<i>網站伺服器指令</i>			
ip http port	設定網路瀏覽器介面使用的通訊埠	GC	4-28
ip http server	允許使用者用瀏覽器監視或設定交換器	GC	4-28
<i>特大封包指令</i>			
jumbo-frame	啓用特大封包支援功能	GC	4-29
<i>事件日誌指令</i>			
logging on	控制錯誤訊息的記錄方式	GC	4-30
logging history	根據重要性限制存放在交換器記憶體內的 syslog 訊息	GC	4-31
clear logging	清除日誌緩衝區中的訊息	PE	4-32
show logging	顯示日誌狀態	PE	4-33
<i>系統狀態指令</i>			
show startup-config	顯示用來啓動系統的組態檔案內容 ( 存放在 Flash 記憶體內 )	PE	4-34
show running-config	顯示目前使用的組態資料	PE	4-36
show system	顯示系統資訊	NE、 PE	4-38
show users	顯示使用中的主控台與 telnet 連線，包括使用者名稱、閒置時間與 telnet 用戶端的 IP 位址	NE、 PE	4-39
show version	顯示系統版本資訊	NE、 PE	4-40

### 4.3.3.1 hostname

此指令可設定或修改裝置的主機名稱，加上 **no** 則可恢復為預設的主機名稱。

## 語法

**hostname** *name*

**no hostname**

*name* - 此主機的名稱。(最大長度：255 個字元)

## 預設設定

無

## 指令模式

Global Configuration

## 範例

```
Console(config)#hostname Server_Chassis_35
Console(config)#
```

### 4.3.3.2

## username

此指令可新增指定名稱的使用者、強制登入時進行認證、設定或更改使用者的密碼 (或設定為不需要密碼) 以及設定或更改使用者的存取層級，加上 **no** 則可刪除使用者的名稱。

## 語法

**username** *name* {**access-level** *level* | **nopassword** | **password** {**0** | **7**} *password*}

**no username** *name*

- *name* – 使用者的名稱。  
(最大長度：8 個字元，使用者人數上限：5)
- **access-level** *level* – 設定使用者的等級。  
此裝置共有兩層預設權限：**0**：Normal Exec，**15**：Privileged Exec。(第 1 到第 14 層並未使用。)
- **nopassword** – 此使用者登入時不需要密碼。
- **{0 | 7}** - 0 代表所輸入的就是密碼本身，7 則代表輸入的是已經加密過的密碼。
- **password** *password* – 使用者的認證密碼。  
(最大長度：8 個名碼字元、32 位元加密、大小寫有別)

## 預設設定

- 預設存取層級為「Normal Exec」。
- 「Normal Exec」模式的預設密碼為 guest，「Privileged Exec」模式的預設密碼為 admin。

使用者名稱與密碼的出廠預設值為：

表 4-2 預設使用者名稱與密碼

使用者名稱	存取層級	密碼
guest	0	guest
admin	15	admin

## 指令模式

Global Configuration

## 指令使用方式

在指令行上不需要使用經過加密的密碼。如果輸入數字 7，則交換器在系統啟動時便會讀取存放在組態檔案中所有經過加密的密碼。

## 範例

以下示範如何設定使用者的存取層級與密碼。

```
Console(config)#username bob access-level 15
Console(config)#username bob password 0 smith
Console(config)#
```

### 4.3.3.3 enable password

第一次登入系統後，首先第一件事就是設定「Privileged Exec」密碼，並請將這份密碼記錄下來放在安全的地方。此指令可用來控制從「Normal Exec」層級進入「Privileged Exec」層級的存取權，加上 **no** 則可重設預設密碼。

#### 語法

**enable password** [level *level*] {0 | 7} *password*

**no enable password** [level *level*]

- *level level* – 層級 15 代表「Privileged Exec」。(第 0 到第 14 層並未使用。)
- {0 | 7} - 0 代表所輸入的就是密碼本身，7 則代表輸入的是已經加密過的密碼。
- *password* – 此特權層級的密碼。  
(最大長度：8 個名碼字元、32 位元加密、大小寫有別)

#### 預設設定

- 預設使用層級 15。
- 預設密碼為 super。

#### 指令模式

Global Configuration

#### 指令使用方式

- 密碼不可以是空的。使用 **enable** 指令將指令模式從「Normal Exec」轉到「Privileged Exec」時，一定要輸入密碼才行 (參閱第 4-12 頁)。
- 在指令行上不需要使用經過加密的密碼。如果輸入數字 7，則交換器在系統啟動時便會讀取存放在組態檔案中所有經過加密的密碼。

#### 範例

```
Console(config)#enable password level 15 0 admin
Console(config)#
```

#### 相關指令

enable (4-12)

### 4.3.3.4 ip http port

此指令可設定網路瀏覽器介面應使用的 TCP 通訊埠編號，加上 **no** 則表示使用預設通訊埠。

#### 語法

```
ip http port port-number  
no ip http port
```

*port-number* – 瀏覽器介面使用的 TCP 通訊埠。(範圍：1-65535)

#### 預設設定

80

#### 指令模式

Global Configuration

#### 範例

```
Console(config)#ip http port 769  
Console(config)#
```

#### 相關指令

ip http server (4-28)

### 4.3.3.5 ip http server

此指令可讓管理員透過瀏覽器監視與設定此裝置，加上 **no** 則可取消此項功能。

#### 語法

```
ip http server  
no ip http server
```

#### 預設設定

Enabled

#### 指令模式

Global Configuration



## 範例

```
Console(config)#ip http server
Console(config)#
```

## 相關指令

ip http port (4-28)

### 4.3.3.6 jumbo-frame

此指令可啟動支援巨大封包的功能，加上 **no** 則可停用此功能。

## 語法

```
jumbo-frame
no jumbo-frame
```

## 預設設定

disabled

## 指令模式

Global Configuration

## 指令使用方式

- 利用支援長達 9000 位元組巨大封包的功能，交換器可讓大量循序資料的交換速度有效提高。與最長只有 1.5 KB 的標準乙太網路封包比較起來，使用巨大封包可大幅減少每個封包中爲了處理通訊協定封裝欄位所耗掉的額外負擔。
- 若要使用巨大封包，必須來源與目的兩端節點（例如電腦或伺服器）均支援這項功能才行。若雙方連線以全雙工進行，則介於兩個節點之間的所有交換器也都必須能接受較大的封包長度；如果雙方之間是半雙工的連線，則處於同一個碰撞領域中的所有裝置都必須能支援巨大封包。
- 巨大封包功能啓用後，廣播風暴控制的流量上限值最多就只能設到每秒鐘 64 個封包。（請參閱第 4-80 頁的 **switchport broadcast** 指令說明。）

## 範例

```
Console(config)#jumbo-frame
Console(config)#
```

### 4.3.3.7 logging on

此指令可控制錯誤訊息的記錄方式，且會將除錯或錯誤訊息傳到交換器的記憶體內。加上 **no** 則可停止記錄訊息。

#### 語法

```
logging on  
no logging on
```

#### 預設設定

無

#### 指令模式

Global Configuration

#### 指令使用方式

訊息記錄程序控制了哪些錯誤訊息會儲存到交換器的記憶體內，您可以用 **logging history** 指令控制要儲存哪些種類的錯誤訊息。

#### 範例

```
Console(config)#logging on  
Console(config)#
```

#### 相關指令

```
logging history (4-31)  
clear logging (4-32)
```

### 4.3.3.8 logging history

此指令可根據重要性限制存放在交換器記憶體內的 syslog 訊息，加上 **no** 則可將 syslog 訊息的記錄方式恢復為預設層級。

#### 語法

**logging history** {flash | ram} level

**no logging history** {flash | ram}

- **flash** – 將事件歷程儲存到 flash 記憶體（即永久記憶體）內。
- **ram** – 將事件歷程存放到暫時性 RAM（電源重設其內容便消失不見）內。
- **level** – 0-7（從指定的層級開始到 0 的所有訊息都會儲存起來。）

表 4-3 錯誤層級

層級參數	層級	說明
debugging	7	除錯訊息
informational	6	一般資訊訊息
notifications	5	值得注意的一般訊息，例如冷開機
warnings	4	警告狀態（例如收到錯誤或預期以外的答案）
errors	3	錯誤狀況（例如錯誤輸入，此為預設值）
critical	2	重大狀況（例如記憶體配置錯誤、記憶體釋放錯誤、資源耗進等等）
alerts	1	需要立即處理
emergencies	0	系統不堪使用

\* 目前此韌體版本不會發出層級 0 與層級 1 的錯誤訊息。

#### 預設設定

Flash : errors (層級 3-0)

RAM : warnings (層級 7-0)

#### 指令模式

Global Configuration

#### 指令使用方式

設定給 flash 記憶體的訊息層級必須高於（也就是數字低於）設定給 RAM 的訊息層級。

#### 範例

```
Console(config)#logging history ram 0
Console(config)#
```

### 4.3.3.9 clear logging

此指令可將日誌緩衝區中的訊息清除。

#### 語法

**clear logging [flash | ram]**

- **flash** – 將事件歷程儲存到 flash 記憶體 (即永久記憶體) 內。
- **ram** – 將事件歷程存放到暫時性 RAM (電源重設其內容便消失不見) 內。

#### 預設設定

Flash 與 RAM

#### 指令模式

Privileged Exec

#### 範例

```
Console#clear logging
Console#
```

#### 相關指令

show logging (4-33)

### 4.3.3.10 show logging

此指令可顯示目前的訊息記錄設定，以及記憶體內存放的任何系統與事件訊息。

#### 語法

**show logging {flash | ram}**

- **flash** – 將事件歷程儲存到 flash 記憶體 (即永久記憶體) 內。
- **ram** – 將事件歷程存放到暫時性 RAM (電源重設其內容便消失不見) 內。

#### 預設設定

無

#### 指令模式

Privileged Exec

#### 指令使用方式

此指令會顯示以下資訊：

- Syslog logging – 系統日誌功能是否已經使用 **logging on** 指令啓用。
- History logging in FLASH/RAM – 根據 **logging history** 指令的設定所應回報的訊息層級。
- 記憶體內的任何系統與事件訊息。

#### 範例

在以下範例輸出畫面中，系統日誌功能已啓用，Flash 記憶體的訊息層級為 **errors** (即預設層級 3-0)，RAM 的訊息層級為 **debugging** (即預設層級 7-0)，並列出一個錯誤。

```
Console#show logging flash
Syslog logging: Enable
History logging in FLASH: level errors
[0] 0:0:5 1/1/1
    "PRI_MGR_InitDefault function fails."
    level: 3, module: 13, function: 0, and event no.: 0
Console#show logging ram
Syslog logging: Enable
History logging in RAM: level debugging
[0] 0:0:5 1/1/1
    "PRI_MGR_InitDefault function fails."
    level: 3, module: 13, function: 0, and event no.: 0
Console#
```

#### 相關指令

logging on (4-30)  
logging history (4-31)

### 4.3.3.11 show startup-config

此指令可顯示非揮發記憶體中所儲存用來啓動系統的組態檔案。

#### 預設設定

無

#### 指令模式

Privileged Exec

#### 指令使用方式

- 此指令與 **show running-config** 指令並用，可比較執行記憶體中的資訊與非揮發記憶體中儲存的資訊。
- 此指令會顯示主要指令模式的設定，每一種模式群組均以 ! 隔開，並包含組態模式指令與相對應的指令。此指令會顯示以下資訊：
  - 系統描述 (主機名稱、位置、聯絡資訊)
  - SNMP 群體字串
  - 使用者 (名稱、存取層級與經過加密的密碼)
  - VLAN 資料庫 (VLAN ID、名稱與狀態)
  - 每個介面的 VLAN 組態設定
  - 管理 VLAN 的 IP 位址
  - 使用者認證順序，以及遠端認證伺服器的位址與 UDP 通訊埠
  - 對主控台與 telnet 所作的任何組態設定

#### 範例

```
Console#show startup-config
building startup-config, please wait.....
!
hostname R&D 5
snmp-server location WC 9
snmp-server contact Charles
```

```

!
snmp-server community private rw
snmp-server community public ro
!
username admin access-level 15
username admin password 7 21232f297a57a5a743894a0e4a801fc3
username guest access-level 0
username guest password 7 084e0343a0486ff05530df6c705c8bb4
enable password level 15 7 1b3231655cebb7a1f783eddf27d254ca
!
vlan database
vlan 1 name DefaultVlan media ethernet state active
vlan 2 name MgtVlan media ethernet state active
!
!
spanning-tree mst-configuration
name XSTP REGION 0
!
interface ethernet SNP0
description Blade Slot 1
flowcontrol
switchport allowed vlan add 1 untagged
switchport native vlan 1
spanning-tree edge-port
spanning-tree link-type auto
.
.
interface vlan 2
ip address 0.0.0.0 255.0.0.0
!!
no bridge-ext gvrp!
!
authentication login local
tacacs-server host 0.0.0.0
tacacs-server port 0
!
line console
!
!
line vty
!
!
end
Console#

```

#### 相關指令

show running-config (4-36)

### 4.3.3.12 show running-config

此指令可顯示目前使用的組態資訊。

#### 預設設定

無

#### 指令模式

Privileged Exec

#### 指令使用方式

- 此指令與 **show startup-config** 指令並用，可比較執行記憶體中的資訊與非揮發記憶體中儲存的資訊。
- 此指令會顯示主要指令模式的設定，每一種模式群組均以 ! 隔開，並包含組態模式指令與相對應的指令。此指令會顯示以下資訊：
  - 系統描述 (主機名稱、位置、聯絡資訊)
  - SNMP 群體字串
  - 使用者 (名稱、存取層級與經過加密的密碼)
  - VLAN 資料庫 (VLAN ID、名稱與狀態)
  - 每個介面的 VLAN 組態設定
  - 管理 VLAN 的 IP 位址
  - 使用者認證順序，以及遠端認證伺服器的位址與 UDP 通訊埠
  - 對主控台與 telnet 所作的任何組態設定

#### 範例

```
Console#show running-config
building running-config, please wait.....
!
hostname R&D 5
snmp-server location WC 9
snmp-server contact Charles
!
snmp-server community private rw
snmp-server community public ro
```



```

!
username admin access-level 15
username admin password 7 21232f297a57a5a743894a0e4a801fc3
username guest access-level 0
username guest password 7 084e0343a0486ff05530df6c705c8bb4
enable password level 15 7 1b3231655cebb7a1f783eddf27d254ca
!
vlan database
vlan 1 name DefaultVlan media ethernet state active
vlan 2 name MgtVlan media ethernet state active
!
!
!
spanning-tree mst-configuration
!
interface ethernet SNP0
description Blade Slot 0
flowcontrol
switchport allowed vlan add 1 untagged
switchport native vlan 1
spanning-tree edge-port
spanning-tree link-type auto
.
.
interface vlan 2
ip address 0.0.0.0 255.0.0.0
!
!
no bridge-ext gvrp
!
!
authentication login local
tacacs-server host 0.0.0.0
tacacs-server port 0
!
line console
!
line vty
!
!
end
Console#

```

### 相關指令

show startup-config (4-34)

### 4.3.3.13 show system

此指令會顯示系統資訊。

#### 預設設定

無

#### 指令模式

Normal Exec、Privileged Exec

#### 指令使用方式

- 關於此指令所顯示各項目的說明，請參閱第 3-7 頁的「顯示系統資訊」。
- POST 的每項結果應該都要顯示 PASS 才正常。如果有任何一項 POST 測試結果為 FAIL，請與經銷商聯絡尋求協助。

#### 範例

```
Console#show system
System description: Sun Fire B1600
System OID string: 1.3.6.1.4.1.42.2.24.1
System information
  System Up time: 0 days, 0 hours, 55 minutes, and 54.91 seconds
  System Name      : [NONE]
  System Location  : [NONE]
  System Contact   : [NONE]
  MAC address      : 00-00-e8-00-00-01
  Web server       : enable
  Web server port  : 80
  Web secure server : enable
  Web secure server port : 443
  POST result

--- Performing Power-On Self Tests (POST) ---
UART Loopback Test ..... PASS
Timer Test ..... PASS
DRAM Test ..... PASS
I2C Initialization ..... PASS
Runtime Image Check ..... PASS
PCI Device Check ..... PASS
Switch Driver Initialization ..... PASS
----- DONE -----
Console#
```

### 4.3.3.14 show users

顯示使用中的主控台與 telnet 連線，包括使用者名稱、閒置時間與 telnet 用戶端的 IP 位址。

#### 預設設定

無

#### 指令模式

Normal Exec、Privileged Exec

#### 指令使用方式

用來執行此指令的連線會以 Line (連線) 編號旁邊的 \* 符號標示。

#### 範例

```
Console#show users
Username accounts:
  Username Privilege
  -----
    admin      15
    guest       0

Online users:
  Line      Username Idle time (h:m:s) Remote IP addr.
  -----
* 0  console  admin      0:00:00
  1  vty 0    admin      0:04:37      10.1.0.19

Console#
```

### 4.3.3.15 show version

此指令可顯示系統的硬體與軟體版本資訊。

#### 預設設定

無

#### 指令模式

Normal Exec、Privileged Exec

#### 指令使用方式

關於各軟體項目的詳細資訊，請參閱第 3-16 頁的「顯示交換器軟體版本」。以下為各硬體項目的意義：

- **Serial Number** – 主機板的序號。
- **Service Tag** – 此型交換器沒有這個欄位。
- **Hardware Version** – 主機板的硬體版本。
- **Number of Ports** – 此交換器上的連接埠數量。
- **Main Power Status** – 交換器的電力狀態。
- **Redundant Power Status** – 此型交換器沒有這個欄位。

#### 範例

```
Console#show version
Unit1
  Serial number       : 1
  Service tag         :
  Hardware version    : R0B
  Number of ports     : 25
  Main power status   : up
  Redundant power status : not present
Agent(master)
  Unit id             : 1
  Loader version      : 0.0.6.5
  Boot rom version    : 0.0.7.3
  Operation code version : 1.0.0.1
Console#
```

## 4.3.4 認證指令

此交換器可設定成使用本身資料、RADIUS 或 TACACS 等認證方法對登入系統進行管理的使用者進行認證。

RADIUS 與 TACACS 兩種登入認證通訊協定，都是使用中央伺服器上執行的軟體控制具有 RADIUS 或 TACACS 功能之裝置的存取權限。認證伺服器上的資料庫內含有許多組使用者名稱/密碼，以及要連上交換器進行管理工作的每個使用者或群組的權限等級。

指令	功能	模式	頁數
<i>認證方法</i>			
authentication login	定義登入認證方法與順序	GC	4-42
<i>RADIUS 用戶端</i>			
radius-server host	指定要使用的 RADIUS 伺服器	GC	4-43
radius-server port	設定 RADIUS 伺服器的網路通訊埠	GC	4-43
radius-server key	設定 RADIUS 的加密鍵	GC	4-44
radius-server retransmit	設定重傳次數	GC	4-44
radius-server timeout	設定重送認證要求的間隔時間	GC	4-45
show radius-server	顯示目前的 RADIUS 設定	PE	4-45
<i>TACACS 用戶端</i>			
tacacs-server host	指定要使用的 TACACS 伺服器	GC	4-46
tacacs-server port	設定 TACACS 伺服器的網路通訊埠	GC	4-46
tacacs-server key	設定 TACACS 的加密鍵	GC	4-47
show tacacs-server	顯示目前的 TACACS 設定	PE	4-47

### 4.3.4.1 authentication login

此指令可用來定義登入認證的方法與先後順序，加上 **no** 則可恢復為預設值。

#### 語法

**authentication login** {[local] [radius] [tacacs]}  
**no authentication login**

- **local** – 使用存放在交換器上的密碼。
- **radius** – 使用 RADIUS 伺服器密碼。
- **tacacs** – 使用 TACACS 伺服器密碼。

認證方式可以用任何順序輸入。

#### 預設設定

無

#### 指令模式

Global Configuration

#### 指令使用方式

- RADIUS 採用 UDP，而 TACACS 則使用 TCP。UDP 只會盡全力將資料送達，但 TCP 卻提供連線式的傳輸功能。此外，請注意 RADIUS 只會將用戶端傳送給伺服器之存取要求封包內的密碼加密，而 TACACS 則會將整個封包的內容全部加密。
- RADIUS 與 TACACS 登入認證功能可控制透過主控台連接埠、網路瀏覽器與 Telnet 進行的管理權限，但這些存取權限的設定必須事先在認證伺服器上設定好才行。
- RADIUS 與 TACACS 的登入認證功能會設定每組使用者名稱與密碼的權限等級，因此使用者名稱、密碼以及權限等級都必須在認證伺服器上事先設定好。
- 同一個指令可以設定用兩個或三個認證方法，並依指定順序進行。例如輸入 **authentication login radius local**，交換器便會優先採用 RADIUS 伺服器上的使用者與密碼進行認證，若沒有 RADIUS 伺服器可用，便改用交換器上存放的使用者名稱與密碼資料進行認證。

#### 範例

```
Console(config)#authentication login radius
Console(config)#
```

#### 相關指令

**username** – 設定交換器上存放的使用者名稱與密碼 (4-25)

### 4.3.4.2 radius-server host

此指令可指定要使用的 RADIUS 伺服器，加上 **no** 則可恢復為預設值。

#### 語法

```
radius-server host host_ip_address  
no radius-server host
```

*host\_ip\_address* – 伺服器的 IP 位址。

#### 預設設定

10.11.12.13

#### 指令模式

Global Configuration

#### 範例

```
Console(config)#radius-server host 192.168.1.25  
Console(config)#
```

### 4.3.4.3 radius-server port

此指令可設定 RADIUS 伺服器的網路通訊埠，加上 **no** 則可恢復為預設值。

#### 語法

```
radius-server port port_number  
no radius-server port
```

*port\_number* – RADIUS 伺服器上用來收發認證訊息的 UDP 通訊埠。(範圍：1-65535)

#### 預設設定

1812

#### 指令模式

Global Configuration

#### 範例

```
Console(config)#radius-server port 181  
Console(config)#
```

#### 4.3.4.4 radius-server key

此指令可設定要使用的 RADIUS 加密鍵，加上 **no** 則可恢復為預設值。

##### 語法

**radius-server key** *key\_string*  
**no radius-server key**

*key\_string* – 對用戶端登入動作進行認證時所使用的加密鍵，請勿在此字串內放入空格字元。(最大長度：20 個字元)

##### 預設設定

無

##### 指令模式

Global Configuration

##### 範例

```
Console(config)#radius-server key green  
Console(config)#
```

#### 4.3.4.5 radius-server retransmit

此指令可設定重試次數，加上 **no** 則可恢復為預設值。

##### 語法

**radius-server retransmit** *number\_of\_retries*  
**no radius-server retransmit**

*number\_of\_retries* – 交換器嘗試透過 RADIUS 伺服器對使用者登入進行認證的次數。(範圍：1-30)

##### 預設設定

2

##### 指令模式

Global Configuration

##### 範例

```
Console(config)#radius-server retransmit 5  
Console(config)#
```



### 4.3.4.6 radius-server timeout

此指令可設定每隔多久傳送認證要求給 RADIUS 伺服器，加上 **no** 則可恢復為預設值。

#### 語法

**radius-server timeout** *number\_of\_seconds*  
**no radius-server timeout**

*number\_of\_seconds* – 交換器等待多少秒後仍未收到回應，則重新發送一次要求。  
(範圍：1-65535)

#### 預設設定

5

#### 指令模式

Global Configuration

#### 範例

```
Console(config)#radius-server timeout 10  
Console(config)#
```

### 4.3.4.7 show radius-server

此指令可顯示 RADIUS 伺服器目前的設定。

#### 預設設定

無

#### 指令模式

Privileged Exec

#### 範例

```
Console#show radius-server  
Remote radius server configuration:  
Server IP address: 10.11.12.13  
Communication key with radius server: green  
Server port number: 1812  
Retransmit times: 2  
Request timeout: 5  
Console#
```

### 4.3.4.8 tacacs-server host

此指令可指定要使用的 TACACS 伺服器，加上 **no** 則可恢復為預設值。

#### 語法

```
tacacs-server host host_ip_address  
no tacacs-server host
```

*host\_ip\_address* – 伺服器的 IP 位址。

#### 預設設定

無

#### 指令模式

Global Configuration

#### 範例

```
Console(config)#tacacs-server host 192.168.1.25  
Console(config)#
```

### 4.3.4.9 tacacs-server port

此指令可設定 TACACS 伺服器的網路通訊埠，加上 **no** 則可恢復為預設值。

#### 語法

```
tacacs-server port port_number  
no tacacs-server port
```

*port\_number* – TACACS 伺服器上用來收發認證訊息的 UDP 通訊埠。(範圍：1-65535)

#### 預設設定

無

#### 指令模式

Global Configuration

#### 範例

```
Console(config)#tacacs-server port 181  
Console(config)#
```

### 4.3.4.10 tacacs-server key

此指令可設定要使用的 TACACS 加密鍵，加上 **no** 則可恢復為預設值。

#### 語法

```
tacacs-server key key_string  
no tacacs-server key
```

*key\_string* – 對用戶端登入動作進行認證時所使用的加密鍵，請勿在此字串內放入空格字元。(最大長度：20 個字元)

#### 預設設定

無

#### 指令模式

Global Configuration

#### 範例

```
Console(config)#tacacs-server key green  
Console(config)#
```

### 4.3.4.11 show tacacs-server

此指令可顯示 TACACS 伺服器目前的設定。

#### 預設設定

無

#### 指令模式

Privileged Exec

#### 範例

```
Console#show tacacs-server  
Remote TACACS server configuration:  
Server IP address: 10.11.12.13  
Communication key with tacacs server: green  
Server port number: 1824  
Console#
```

## 4.3.5 SNMP 指令

SNMP 指令可控制哪些 SNMP 管理主機有權存取此交換器，以及要發送哪些類別的錯誤訊息給 trap 管理員。

指令	功能	模式	頁數
snmp-server community	設定 SNMP 網管系統存取此交換器的 SNMP 指令時應提出的群體字串	GC	4-48
snmp-server contact	設定系統聯絡資訊字串	GC	4-49
snmp-server location	設定系統所在位置字串	GC	4-50
snmp-server host	指定 SNMP 通報作業的接收者	GC	4-50
snmp-server enable traps	啓用交換器發送 SNMP trap 或其它提醒要求 (例如 SNMP 通報) 的裝置	GC	4-51
show snmp	顯示 SNMP 通訊狀態	NE、 PE	4-52

### 4.3.5.1 snmp-server community

此指令可定義 SNMP (Simple Network Management Protocol, 簡易網路管理協定) 的群體存取字串，加上 **no** 則可將原來的群體字串刪除。

#### 語法

```
snmp-server community string [ro | rw]  
no snmp-server community string
```

- *string* – 作用與密碼類似的群體字串，提出此字串的人便有權使用 SNMP 通訊協定。(最大長度：32 個字元、大小寫有別、群體字串個數上限：5)
- **ro** – 表示只允許讀取的動作，代表有權存取的管理主機只能讀取 MIB 物件。
- **rw** – 表示可進行讀取與寫入的動作，代表有權存取的管理主機可讀取與修改 MIB 物件。

#### 預設設定

- public – 唯讀權限。
- private – 讀寫權限。

#### 指令模式

Global Configuration

#### 指令使用方式

只要輸入一個 **snmp-server community** 指令，便可啓動所有版本的 SNMP 功能 (SNMPv1 與 SNMPv2c)，輸入 **no snmp-server community** 指令則會將所有版本的 SNMP 功能全部停止。

## 範例

```
Console(config)#snmp-server community alpha rw
Console(config)#
```

### 4.3.5.2 snmp-server contact

此指令可設定系統聯絡資訊字串，加上 **no** 則可將原來的系統聯絡資訊刪除。

#### 語法

**snmp-server contact** *string*  
**no snmp-server contact**

*string* – 描述系統聯絡資訊的字串。  
(最大長度：255 個字元)

#### 預設設定

無

#### 指令模式

Global Configuration

#### 範例

```
Console(config)#snmp-server contact Paul
Console(config)#
```

#### 相關指令

snmp-server location (4-50)

### 4.3.5.3 snmp-server location

此指令可設定系統所在位置字串，加上 **no** 則可將原來的字串刪除。

#### 語法

```
snmp-server location text  
no snmp-server location
```

*text* – 描述系統所在位置的字串。  
(最大長度：255 個字元)

#### 預設設定

無

#### 指令模式

Global Configuration

#### 範例

```
Console(config)#snmp-server location WC-19  
Console(config)#
```

#### 相關指令

snmp-server contact (4-49)

### 4.3.5.4 snmp-server host

此指令可指定 SNMP 通報作業的接收主機，加上 **no** 則可將原來指定的主機刪除。

#### 語法

```
snmp-server host host-addr community-string version version-number  
no snmp-server host host-addr
```

- *host-addr* – 該主機 (接收 trap) 的名稱 IP 位址。(主機位址個數上限:5 個 trap 目的地位址項目)
- *community-string* – 與通報作業一起傳送的群體字串，作用類似密碼。雖然您可以使用 **snmp-server host** 指令自行設定此字串，但建議您在使用 **snmp-server host** 指令前，最好先用 **snmp-server community** 指令定義這個字串。(最大長度：32 個字元)
- *version-number* - {1 | 2c}  
此主機使用的是第 1 版或 2c 版的 SNMP。

## 預設設定

無

## 指令模式

Global Configuration

## 指令使用方式

若未輸入任何 **snmp-server host** 指令，交換器便不會發送任何通報訊息。因此爲了要讓交換器將 SNMP 通報訊息發送出去，至少要輸入一個 **snmp-server host** 指令。如果還要同時發給好幾台主機，每一台主機都要用 **snmp-server host** 指令設定一次。

**snmp-server host** 指令應與 **snmp-server enable traps** 指令合併使用。**snmp-server enable traps** 指令可設定要將哪些 SNMP 通報訊息發送出去。若要讓某台主機接收到通報訊息，至少要爲該主機輸入一個 **snmp-server enable traps** 指令與 **snmp-server host** 指令。

不過某些通報類別並無法用 **snmp-server enable traps** 指令控制，例如某些通報類別無論如何都是會啓用的。

## 範例

```
Console(config)#snmp-server host 10.1.19.23 batman version 1
Console(config)#
```

## 相關指令

snmp-server enable traps (4-51)

### 4.3.5.5 snmp-server enable traps

此指令可啓動交換器發送 SNMP trap 或 inform (SNMP 通報)，加上 **no** 則可將發送 SNMP 通報的功能取消。

## 語法

```
snmp-server enable traps [authentication | link-up-down]  
no snmp-server enable traps [authentication | link-up-down]
```

- **authentication** – 表示要交換器發送認證失敗的 trap。
- **link-up-down** – 表示要交換器發送斷線或連線的 trap。

## 預設設定

發送認證、斷線與連線的 trap。

## 指令模式

Global Configuration

## 指令使用方式

若未輸入任何 **snmp-server enable traps** 指令，交換器便不會發送此指令控制的任何通報訊息。至少要輸入一個 **snmp-server enable traps** 指令，交換器才會發出 SNMP 通報。輸入此指令時若未加上任何關鍵字，則認證、連線與斷線的通報都會發送出去。若輸入指令時只加上一個關鍵字，則只有該關鍵字指定的通報訊息才會發送出去。

**snmp-server enable traps** 指令應與 **snmp-server host** 指令合併使用。**snmp-server host** 指令可設定哪一台或哪些主機會接收 SNMP 通報。因此爲了要讓交換器將通報訊息發送出去，至少要輸入一個 **snmp-server host** 指令。

## 範例

```
Console(config)#snmp-server enable traps link-up-down
Console(config)#
```

## 相關指令

snmp-server host (4-50)

### 4.3.5.6 show snmp

此指令可檢查 SNMP 通訊的狀態。

## 預設設定

無

## 指令模式

Normal Exec、Privileged Exec

## 指令使用方式

此指令會顯示群體存取字串、SNMP 輸入與輸出的通訊協定資料單元數量以及 SNMP 記錄功能是否已經用 **snmp-server enable traps** 指令啓用。



## 範例

```
Console#show snmp

SNMP traps:
  Authentication: enable
  Link-up-down: enable

SNMP communities:
  1. private, and the privilege is read/write
  2. public, and the privilege is read-only

0 SNMP packets input
  0 Bad SNMP version errors
  0 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  0 Number of requested variables
  0 Number of altered variables
  0 Get-request PDUs
  0 Get-next PDUs
  0 Set-request PDUs
0 SNMP packets output
  0 Too big errors
  0 No such name errors
  0 Bad values errors
  0 General errors
  0 Response PDUs
  0 Trap PDUs

SNMP logging: disabled
Console#
```

## 4.3.6 線路指令

將一台與 VT100 相容的裝置連到伺服器的序列連接埠，便可使用交換器內附的組態設定程式。以下指令都是用來設定序列連接埠與 telnet (即虛擬終端機) 的通訊參數。

---

**注意：**序列介面的連線參數固定為 8 個資料位元、1 個停止位元、不使用同位檢查、9600 bps。

---

指令	功能	模式	頁數
line	挑選一條要設定組態的特定線路，並啟動線路組態設定模式	GC	4-55
login	啓用登入時的密碼檢查功能	LC	4-56
password	設定線路的密碼	LC	4-57
exec-timeout	設定指令解譯程式偵測到使用者有輸入資料之前應等待多久時間	LC	4-58
password-thresh	設定密碼重試次數，限制失敗登入的嚐試次數	LC	4-59
silent-time*	當失敗登入次數超過 <b>password-thresh</b> 指令設定的次數時，管理主控台應停止多久時間不讓外界存取	LC	4-60
show line	顯示終端機線路的參數	NE、 PE	4-61

\* 此指令僅適合序列埠使用。

## 4.3.6.1 line

此指令可挑選要設定組態的線路，並處理接下來的線路組態設定指令。

### 語法

**line** {**console** | **vty**}

- **console** – 主控台終端機線路。
- **vty** – 給遠端主控台存取 ( 即 telnet ) 所使用的虛擬終端機。

### 預設設定

沒有預設值。

### 指令模式

Global Configuration

### 指令使用方式

telnet 被視為虛擬終端機連線的一種，在 **show users** 之類指令所顯示的畫面中以 Vty 表示。

### 範例

輸入以下指令便可進入主控台線路模式：

```
Console(config)#line console
Console(config-line)#
```

### 相關指令

show line (4-61)  
show users (4-39)

## 4.3.6.2 login

此指令可啓用登入時的密碼檢查功能，加上 **no** 則可停用密碼檢查功能，允許外界不需輸入密碼便可連上交換器。

### 語法

**login [local]**  
**no login**

**local** – 使用交換機上的密碼進行檢查。認證程序將根據使用者在 **username** 指令指定的使用者名稱進行檢查。

### 預設設定

login local

### 指令模式

Line Configuration

### 指令使用方式

- 交換器本身提供給登入時使用的認證模式共有三種：
  - **login** 採用 **password** 線路組態指令所設定的單一組密碼進行認證。使用這個方法時，管理介面會以「Normal Exec (NE)」模式啓動。
  - **login local** 採用 **username** 指令所設定的使用者名稱與密碼進行認證 (預設值)。使用這個方法時，管理介面會以「Normal Exec (NE)」或「Privileged Exec (PE)」模式啓動，視使用者的權限等級而定 (即 0 或 15)。
  - **no login** 不進行認證程序。使用這個方法時，管理介面會以「Normal Exec (NE)」模式啓動。
- 此指令僅控制透過交換器本身進行的登入認證程序，若要設定給遠端認證伺服器認證的使用者名稱與密碼，請使用這些伺服器上所安裝的 RADIUS 或 TACACS 軟體。

### 範例

```
Console(config-line)#login local
Console(config-line)#
```

### 相關指令

username (4-25)  
password (4-57)

### 4.3.6.3 password

此指令可指定線路的密碼，加上 **no** 則可將密碼刪除。

#### 語法

```
password {0 | 7} password  
no password
```

- {0 | 7} - 0 代表所輸入的就是密碼本身，7 則代表輸入的是已經加密過的密碼。
- *password* - 設定線路密碼的字串。  
(最大長度：8 個名碼字元、32 位元加密、大小寫有別)

#### 預設設定

未設定任何密碼。

#### 指令模式

Line Configuration

#### 指令使用方式

- 當使用者連到有密碼保護的任何一條線路時，系統便會要求輸入密碼。此時只要輸入的密碼正確，系統便會顯示提示符號。您可以用 **password-thresh** 指令設定使用者輸入錯誤密碼多少次之後，系統便中斷該連線，並讓終端機回到閒置等待模式。
- 在指令行上不需要使用經過加密的密碼。如果輸入數字 7，則交換器在系統啟動時便會讀取存放在組態檔案中所有經過加密的密碼。

#### 範例

```
Console(config-line)#password 0 secret  
Console(config-line)#
```

#### 相關指令

login (4-56)  
password-thresh (4-59)

## 4.3.6.4 exec-timeout

此指令可設定系統等待多少時間使用者都未輸入資料後，系統即可逕自切斷其連線，加上 **no** 則可恢復為預設值。

### 語法

**exec-timeout** [*seconds*]

**no exec-timeout**

*seconds* – 指定應等待的整數秒數。  
(範圍：0 - 65535 秒；0 代表無時間限制)

### 預設設定

CLI：無時間限制

Telnet：10 分鐘

### 指令模式

Line Configuration

### 指令使用方式

- 在等待時間尚未到達之前，只要偵測到使用者有輸入資料，交換器便會繼續保持此連線不斷線，否則時間一到交換器便會將連線切斷。
- 此指令適用於序列主控台與 telnet 連線（但 telnet 連線的時間限制無法停用）。

### 範例

輸入以下指令便可將逾時時間設定為 2 分鐘：

```
Console(config-line)#exec-timeout 120
Console(config-line)#
```

## 4.3.6.5 password-thresh

此指令可設定密碼入侵上限，限制失敗登入的次數，加上 **no** 則可刪除此限制值。

### 語法

**password-thresh** *threshold*  
**no password-thresh**

*threshold* – 允許使用者最多輸入幾次錯誤的密碼。  
(範圍：1-120；0 代表不設任何限制)

### 預設設定

預設值為三次。

### 指令模式

Line Configuration

### 指令使用方式

- 當使用者在主控台連接埠輸入密碼的錯誤次數達到設定的上限時，系統介面便會暫時凍結一段時間，然後才會再接受下一次的登入。(凍結時間的長短可用 **silent-time** 指令加以設定。)當使用者透過 **telnet** 連線但輸入密碼的錯誤次數達到設定的上限時，交換器便會將 **telnet** 登入介面關閉。
- 此指令同時適用於交換器本身的主控台與 **telnet** 連線。

### 範例

輸入以下指令便可將密碼嘗試次數上限定為 5 次：

```
Console(config-line)#password-thresh 5
Console(config-line)#
```

### 相關指令

**silent-time** (4-60)

## 4.3.6.6 silent-time

此指令可設定登入錯誤次數超過 **password-thresh** 指令設定的上限時，管理主控台應該凍結多少時間，加上 **no** 則可將凍結時間設定值刪除。

### 語法

**silent-time** [*seconds*]

**no silent-time**

*seconds* – 主控台應該暫停回應的秒數。  
(範圍：0-65535 秒；0 代表不回凍結回應)

### 預設設定

主控台預設並不會凍結回應。

### 指令模式

Line Configuration

### 範例

以下指令可將凍結時間設定為 60 秒：

```
Console(config-line)#silent-time 60
Console(config-line)#
```

### 相關指令

password-thresh (4-59)



## 4.3.6.7 show line

此指令可顯示終端機線路的參數。

### 語法

**show line [console | vty]**

- **console** – 主控台終端機線路。
- **vty** – 給遠端主控台存取 ( 即 telnet ) 所使用的虛擬終端機。

### 預設設定

顯示所有線路

### 指令模式

Normal Exec、Privileged Exec

### 範例

以下指令可顯示所有線路的連線設定：

```
Console#show line
Console configuration:
  Password threshold: 3 times
  Interactive timeout: Disabled
  Silent time: Disabled
  Baudrate: 9600
  Databits: 8
  Parity: none
  Stopbits: 1

Vty configuration:
  Password threshold: 3 times
  Interactive timeout: 600
Console#
```

## 4.3.7 IP 指令

交換器預設會用 DHCP 搜尋其 IP 位址、預設閘道以及網路遮罩。

您可以手動為其設定 IP 位址，或引導該裝置從 BOOTP 或 DHCP 伺服器取得位址。正確的 IP 位址由四個 0 到 255 的十進位數字組成，各數字以小數點隔開。不符合此格式的設定值，都不會為交換器軟體所接受。

指令	功能	模式	頁數
<i>IP 組態</i>			
ip address	設定此裝置的 IP 位址	IC	4-62
ip dhcp restart	發出一個 BOOTP 或 DHCP 用戶端要求	PE	4-64
ip dhcp client-identifier	指定交換器的 DHCP 的用戶端識別碼。請注意，由於每次系統控制器或交換器開機時，系統控制器便會重新設定交換器的用戶端識別碼，因此建議您最好不要自行指定用戶端識別碼。	VC	4-65
ip default-gateway	定義預設閘道，以便 in-band 管理主機可透過此閘道連上此裝置	GC	4-66
show ip interface	顯示此裝置的 IP 設定	PE	4-67
show ip redirects	顯示設定給此裝置使用的預設閘道	PE	4-67
ping	發出 ICMP echo 要求封包給網路上的另一個節點	NE、PE	4-68
<i>IP 封包過濾</i>			
ip filter	阻擋特定 IP 封包從交換器其它連接埠進入內部的管理連接埠 (NETMGT)	GC	4-69
show ip filter	顯示過濾規則或擷取到的封包	PE	4-72

### 4.3.7.1 ip address

此指令可設定交換器的 IP 位址，加上 **no** 則可恢復為預設的 IP 位址。

#### 語法

**ip address** {*ip-address netmask* | **bootp** | **dhcp**}

**no ip address**

- *ip-address* – IP 位址
- *netmask* – 相關 IP 子網路的網路遮罩，用以指定轉送到特定子網路時所使用的主機位址位元個數。
- **bootp** – 從 BOOTP 取得 IP 位址。
- **dhcp** – 從 DHCP 取得 IP 位址。

## 預設設定

預設值為：dhcp

## 指令模式

Interface Configuration (VLAN)

## 指令使用方式

- 您可以手動為其設定 IP 位址，或引導該裝置從 BOOTP 或 DHCP 伺服器取得位址。交換器出廠時預設是使用 DHCP。正確的 IP 位址由四個 0 到 255 的數字組成，各數字之間以小數點隔開。不符合此格式的設定值，都不會為組態設定軟體所接受。
- 若選擇採用 **bootp** 或 **dhcp** 方式，IP 功能雖會啓用，但須等到收到 BOOTP 或 DHCP 的回應時才會開始運作。此裝置每隔一段固定時間就會以廣播的方式往外發送要求，以取得本身的 IP 位址。(BOOTP 與 DHCP 供應的設定值可以包括 IP 位址、預設閘道與子網路遮罩。)
- 輸入 **ip dhcp restart** 指令或重新啓動交換器，都會讓交換器開始往外發出廣播 BOOTP 或 DHCP 要求。

---

**注意：**交換器的 IP 位址事實上是包含管理連接埠 (NETMGT) 之 VLAN 的 IP 位址。此管理連接埠預設隸屬於 VLAN 2，因此您必須指定 IP 位址給 VLAN 2，才能設好交換器透過網路連接的功能。只有管理連接埠所屬的 VLAN，才應該設定 IP 位址。設定 IP 位址給任何 VLAN 時，原來 IP 位址會立刻停止使用，新的位址也會立刻生效。

---

## 範例

以下範例為裝置指派 VLAN2 中的位址。

```
Console(config)#interface vlan 2
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#
```

## 相關指令

ip dhcp restart (4-64)

## 4.3.7.2 ip dhcp restart

此指令可發出 BOOTP 或 DHCP 用戶端要求。

### 預設設定

無

### 指令模式

Privileged Exec

### 指令使用方式

- 根據 DHCP 的規定，只要先前發給用戶端的位址還沒有發給其他人使用，伺服器就應該核發同一個位址給用戶端。
- 若 BOOTP 或 DHCP 伺服器已經移到另一個領域，則其提供給用戶端之位址的網路部分將會依照伺服器所在的領域設定。

### 範例

在以下範例中，此裝置仍獲核發相同的位置。

```
Console(config)#interface vlan 2
Console(config-if)#ip address dhcp
Console(config-if)#exit
Console#ip dhcp restart
Console#show ip interface
IP interface vlan
  IP address and netmask: 10.1.0.54 255.255.255.0 on VLAN 2,
  and address mode: DHCP.
Console#
```

### 相關指令

ip address (4-62)

### 4.3.7.3 ip dhcp client-identifier

此指令可指定交換器的 DHCP 用戶端識別碼，加上 **no** 則可刪除此識別碼。

---

**注意：**下次系統或交換器本身重新開機時，原來的用戶端識別碼便會被 SC 新設定的值蓋掉。未來新版韌體將取消 **client-identifier** 這個指令。

---

#### 語法

```
ip dhcp client-identifier {text text | hex hex}
no ip dhcp client-identifier
```

- *text* – 文字字串。(範圍：1-15 個字元)
- *hex* – 十六進位值。

#### 預設設定

每次系統控制器重設交換器時，SSC 中的系統控制器便會設定新的 DHCP 用戶端識別碼，因此建議您最好不要用交換器的指令行介面更改這個值。關於交換器與系統機箱內其它組件的 DHCP 用戶端識別碼相關資訊，請參閱《*Sun Fire 1600 Blade 系統機箱軟體設定手冊*》。

#### 指令模式

Interface Configuration (VLAN)

#### 指令使用方式

- 此指令可將用戶端識別碼放入與 DHCP 互傳的所有資料中，要使用哪一種資料型態，視 DHCP 伺服器的需求而定。
- 下次系統控制器重新開機時，此指令設定的用戶端識別碼便會被系統控制器新設的值蓋掉。

#### 範例

```
Console(config)#interface vlan 2
Console(config-if)#ip dhcp client-identifier hex 00-00-e8-66-65-72
Console(config-if)#
```

#### 相關指令

ip dhcp restart (4-64)

## 4.3.7.4 ip default-gateway

此指令可在交換器與另一個網段上的管理主機之間建立一條靜態路由，加上 **no** 則可將此靜態路由刪除。

### 語法

```
ip default-gateway gateway  
no ip default-gateway
```

*gateway* – 預設閘道的 IP 位址

### 預設設定

沒有建立任何靜態路由。

### 指令模式

Global Configuration

### 指令使用方式

若管理主機位於另一個 IP 網段，就一定要定義閘道。

### 範例

以下範例爲此裝置定義一個預設閘道：

```
Console(config)#ip default-gateway 10.1.0.254  
Console(config)#
```

### 相關指令

show ip redirects (4-67)

### 4.3.7.5 show ip interface

此指令可顯示 IP 介面的設定值。

#### 預設設定

所有介面

#### 指令模式

Privileged Exec

#### 指令使用方式

此交換器只能被指派一個 IP 位址，以便用來管理交換器時使用。

#### 範例

```
Console#show ip interface
IP address and netmask: 10.1.0.54 255.255.255.0 on VLAN 2,
and address mode: User specified.
Console#
```

#### 相關指令

show ip redirects (4-67)

### 4.3.7.6 show ip redirects

此指令可顯示設定給此裝置使用的預設閘道。

#### 預設設定

無

#### 指令模式

Privileged Exec

#### 範例

```
Console#show ip redirects
ip default gateway 10.1.0.254
Console#
```

#### 相關指令

ip default-gateway (4-66)

## 4.3.7.7 ping

此指令可發送 ICMP echo 要求封包給網路上的另一個節點。

### 語法

**ping** *host* [**count** *count*][**size** *size*]

- *host* – 主機的 IP 位址。
- *count* – 發出的封包個數。(範圍：1-16，預設值：5)
- *size* – 每個封包所含位元組個數。(範圍：32-512，預設值：32)  
由於交換器還會在封包前面加上一些表頭資訊，因此實際封包大小會比此處的設定多出 8 個位元組。

### 預設設定

此指令不會預設任何主機。

### 指令模式

Normal Exec、Privileged Exec

### 指令使用方式

- ping 指令可以測試是否能到達網路上的另一個地方。
- 以下是執行 ping 指令後可能獲得的幾種結果：
  - 正常回應 – 約在 1 到 10 秒之內，視網路流量而定。
  - 目的地無任何回應 – 若對方主機無任何回應，交換器會顯示 **timeout**。
  - 無法到達目的地 – 目的地的閘道回報無法將封包送給目的地。
  - 無法到達網路或主機 – 閘道在路由表內找不到相對應的項目。
- 按 <Esc> 便可停止 ping。

### 範例

```
Console#ping 10.1.0.19
Type Ctrl-C to abort.
PING to 10.1.0.19, by 5 32-byte payload ICMP packets, timeout is 5
seconds
response time: 0 ms
response time: 0 ms
response time: 10 ms
response time: 10 ms
response time: 10 ms
Ping statistics for 10.1.0.19:
 5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)
Approximate round trip times:
  Minimum = 0 ms, Maximum = 10 ms, Average = 6 ms
Console#
```



## 4.3.7.8 ip filter

此指令可阻擋特定 IP 封包從下連連接埠進入內部管理連接埠，加上 **no** 則可將規則從過濾表中刪除。

### 語法

```
ip filter [rule-number] action protocol {source source-bitmask}  
{destination destination-bitmask} [fragments] [log]
```

不檢查通訊埠編號。可使用 **fragments** 選項。

```
ip filter [rule-number] action protocol {source source-bitmask} [source-port-range]  
{destination destination-bitmask} [destination-port-range] [log]
```

會檢查通訊埠編號，換句話說，只要指定了 *source-port-range* 或 *destination-port-range*，就不可以使用 **fragments** 選項。

```
ip filter [rule-number] action tcp {source source-bitmask} [source-port-range]  
{destination destination-bitmask} [destination-port-range]  
[code {{code code-bitmask} | code-keyword-seq}] [log]
```

檢查 **tcp** 關鍵字，如果有找到，便可使用 **code** 選項。

```
no ip filter {all | rule-number}
```

從過濾表中將址定的規則編號刪除。

- *rule-number* – 將過濾規則放入表格中指定的位置，並將該位置以及底下的所有樣式推向表格下方。**rule-number** 不可超過表格中下一個可用的編號。若未指定規則編號，則新的樣式就會被放到規則表的結尾。規則總數不得超過 128 條。
- *action* – {**deny** | **permit**}  
阻擋或允許封包在下連連接埠與管理連接埠 (NETMGT) 之間移動。
- *protocol* – {**any** | **tcp** | **udp** | *number*}  
指定任何通訊協定、TCP、UDP 或特定通訊協定編號 (0-255)。
- *source source-bitmask* – 封包的來源位址與網路遮罩。
- *source-port-range* – [*number* | *start\_number-end\_number*]  
指定一個或一段 TCP/UDP 來源連接埠。(範圍：0-65535)
- *destination destination-bitmask* – 封包的目的地位址與網路遮罩。
- *destination-port-range* – [*number* | *start\_number-end\_number*]  
指定一個或一段 TCP/UDP 目的連接埠。(範圍：0-65535)
- **code**
  - *code* – 表示 TCP 表頭第 14 個位元組中旗標位元的十進位數字 (代表一個位元字串)。(範圍：0-63)
  - *code-bitmask* – 套用到 *code* (代碼) 上的十進位數字 (代表位元遮罩)。輸入一個十進位數字，其中相對位置 1 的位元代表要與該位置的位元符合，0 則代表忽略該位元。可使用的位元包括：
    - 1 (fin) – Finish (完成)
    - 2 (syn) – Synchronize (同步)
    - 4 (rst) – Reset (重設)
    - 8 (psh) – Push (推送)

- 16 (ack) – Acknowledgement ( 確認 )
- 32 (urg) – Urgent pointer ( 緊急指標 )
- *code-keyword-seq* – 可設定的 code keywords ( 代碼關鍵字 ) 如下，但必須依照以下所列的順序設定：**fin | syn | rst | psh | ack | urg**  
( 此處有設定的代碼關鍵字表示封包中相對應的位元必須為 1 才算符合，沒有設定的代碼關鍵字則表示封包中相對應的位元必須為 0 才算符合。)
- **fragments** – 帶有 MF (More Fragments，還有其他封包片段) 位元或片段偏移量大於 0 的封包才算符合規則。若未設定 **fragment**，則完整封包與片段封包均算符合規則。
- **log** – 將符合規則的所有封包全部記錄到日誌緩衝區內，其中最多可以存放 64 筆資料。當日誌緩衝區存滿資料後，便會從頭開始覆寫最舊的資料。請注意，這份日誌是放在 RAM 裡面，交換器重設後其中的資料便會消失。

## 預設設定

無

## 指令模式

General Configuration

## 指令使用方式

- 系統預設會將下連連接埠流往管理連接埠 (NETMGT) 的所有 IP 封包阻擋下來，如果您希望單片伺服器能透過管理連接埠 (NETMGT) 接觸到管理網路，就必須另外設定一組過濾器，允許封包從下連連接埠流到管理連接埠。請注意，從上連連接埠傳來的流量絕對不會允許轉到管理連接埠上。
- 片段封包 (fragment) 指的是 MF (more fragments，還有其它片段封包) = 1 或 Fragment Offset ( 片段封包偏移量 ) > 0 的封包。若過濾規則中沒有 **fragments** 關鍵字，則完整封包與片段封包都會受到此規則檢查。
- 設定代碼的值與遮罩時，只要封包 < 表頭中的代碼值 > & < 遮罩 > == < 設定的代碼值 > & < 遮罩 >，就算符合此過濾規則。例如以下的代碼與遮罩便可抓到含有以下旗標的封包：
  - 含有 SYN 旗標，代碼為 2 2
  - 同時含有 SYN 與 ACK，代碼為 18 18
  - 含有 SYN 但不含有 ACK，代碼為 2 18

## 範例 – 位址過濾器

以下範例允許任何通訊協定類別，並以全部都是 0 的位址與網路遮罩作為來源位址與目的位址，其作用等於允許所有封包通過此過濾器。

```
Console(config)#ip filter permit any 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
Console(config)#
```

以下範例會接收來源位址在 10.7.1x 子網路中的封包。只要符合此規則，也就是 10.7.1.1 & 255.255.255.0 等於遮罩之後的位址 10.7.1.2 & 255.255.255.0，封包便可通過。

```
Console(config)#ip filter permit any 10.7.1.1 255.255.255.0 0.0.0.0
0.0.0.0
Console(config)#
```

### 範例 – 檢查片段封包

以下範例會阻擋所有片段封包，並將符合的封包記錄到日誌內。

```
Console(config)#ip filter deny any 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
fragment log
Console(config)#
```

### 範例 – 檢查代碼的值

以下範例會將來自類別 C 位址 192.168.1.0 且含有 SYN 旗標的所有 TCP 封包擋掉。

```
Console(config)#ip filter deny tcp 192.168.1.0 255.255.255.0 0.0.0.0
0.0.0.0 code syn
Console(config)#
```

以下範例同樣也可以阻擋來自類別 C 位址 192.168.1.0 且含有 SYN 旗標的所有 TCP 封包。

```
Console(config)#ip filter deny tcp 192.168.1.0 255.255.255.0 0.0.0.0
0.0.0.0 code 2 2
Console(config)#
```

### 範例 – 檢查通訊埠編號

此範例允許從類別 C 位址 192.168.1.0 發出前往任何地方且目的地通訊埠為 80 的 TCP 封包。

```
Console(config)#ip filter permit tcp 192.168.1.0 255.255.255.0 0.0.0.0
0.0.0.0 80
Console(config)#
```

以下範例會丟棄從來源位址 10.7.1.1 傳到目的位址 10.8.1.1、來源通訊埠在 30 - 46 之間，且目的通訊埠在 100 - 2000 之間的所有 TCP 封包。

```
Console(config)#ip filter deny tcp 10.7.1.1 255.255.255.255 30-46
10.8.1.1 255.255.255.255 100-2000
Console(config)#
```

## 4.3.7.9 show ip filter

此指令可將 IP 過濾表中的所有規則全部顯示出來。

### 語法

**show ip filter** [*rule-number* | **log**]

- *rule-number* – 將位於表格中指定位置的過濾規則顯示出來。範圍：1-128
- **log** – 將日誌緩衝區中儲存的所有封包全部顯示出來。請注意，此緩衝區中存放的封包一定會符合過濾表中的規則。日誌緩衝區內最多只能存放 64 個封包。

若未加上任何選項，則日誌緩衝區中的所有封包都會顯示出來。

### 預設設定

無

### 指令模式

Privileged Exec

### 範例

以下範例中只有一條規則，允許子網路 10.1.0.x 中的封包在管理連接埠與下連連接埠之間來回傳送。

```
Console#show ip filter
Ip filter:
Rule: 1, Action: permit, Protocol: any, Log: disable, Fragments: disable
Source: 10.1.0.0 255.255.255.0 any
Destination: 10.1.0.0 255.255.255.0 any
```

## 4.3.8 介面指令

這些指令可用來控制與設定乙太網路連接埠、集束線路與 VLAN 的通訊參數。

指令	功能	模式	頁數
interface	設定介面種類，並進入介面組態設定模式	GC	4-74
description	在介面組態中加入說明文字	IC	4-74
speed-duplex	設定指定介面在自動協商功能停用時，應該採用的速度與雙工模式	IC	4-75
negotiation	啓用指定介面的自動協商功能	IC	4-76
capabilities	對外公告指定介面在自動協商時可使用的能力	IC	4-77
flowcontrol	啓用指定介面的流量控制功能	IC	4-78
shutdown	停用介面	IC	4-79
switchport broadcast packet-rate	設定廣播風暴控制的流量上限	IC	4-80
clear counters	將介面的統計數據歸零	PE	4-81
show interfaces status	顯示指定介面的狀態	NE、PE	4-81
show interfaces counters	顯示指定介面的統計數據	NE、PE	4-82
show interfaces switchport	顯示介面的管理與運作狀態	NE、PE	4-84

### 4.3.8.1 interface

此指令可設定介面的類別，並進入介面組態設定模式。

#### 語法

**interface** *interface*  
**no interface port-channel** *channel-id*

*interface*

- **ethernet** *port-name*  
*port-name* – 下連連接埠：SNP0-15；上連連接埠：NETP0-7；管理連接埠：NETMGT
- **port-channel** *channel-id* (範圍：1-6)
- **vlan** *vlan-id* (範圍：1-4094)

#### 預設設定

無

#### 指令模式

Global Configuration

#### 範例

輸入以下指令便可指定第一個上連連接埠：

```
Console(config)#interface ethernet NETP0  
Console(config-if)#
```

### 4.3.8.2 description

此指令可加入說明介面的文字，加上 **no** 則可將說明文字刪除。

#### 語法

**description** *string*  
**no description**

*string* – 註解或說明文字，協助您記住此介面連接的對象。(範圍：1-64 個字元)

#### 預設設定

NETP0-7：外部 RJ-45 接頭 NET0-7

SNP0-15：葉片插槽 0-15

NETMGT：外部 RJ-45 接頭 NETMGT

#### 指令模式

Interface Configuration (Ethernet、Port Channel)

## 範例

以下示範如何設定下連連接埠 SNP5 的說明文字。

```
Console(config)#interface ethernet SNP5
Console(config-if)#description RD-SW#3
Console(config-if)#
```

### 4.3.8.3 speed-duplex

此指令可設定指定介面的自動協商功能停用時，應採用的速度與雙工模式，加上 **no** 則可恢復為預設值。

#### 語法

```
speed-duplex {1000full | 100full | 100half | 10full | 10half}
no speed-duplex
```

- **1000full** – 強迫 1000 Mbps 全雙工運作模式
- **100full** – 強迫 100 Mbps 全雙工運作模式
- **100half** – 強迫 100 Mbps 半雙工運作模式
- **10full** – 強迫 10 Mbps 全雙工運作模式
- **10half** – 強迫 10 Mbps 半雙工運作模式

#### 預設設定

- 預設啟用自動協商功能。
- 當自動協商功能停用時，快速乙太網路連接埠預設會使用 100full，Gigabit 乙太網路連接埠則預設使用 1000full。

---

**注意：**當自動協商功能停用時，您只能將上連連接埠設定成 10 Mbps 或 100 Mbps。若要強迫連接埠以 1 Gbps 全雙工模式運作，請啟用自動協商功能，並將連接埠的能力設定為只有 1000full 這一項。

---

#### 指令模式

Interface Configuration (Ethernet、Port Channel)

#### 指令使用方式

- 若要強迫某個介面以 **speed-duplex** 指令中設定的速度與雙工模式運作，請用 **no negotiation** 指令將該介面的自動協商功能停用。但有一點要特別注意，下連連接埠的自動協商功能是无法停用的，這些連接埠均固定以 1000 Mbps 全雙工模式運作。
- 使用 **negotiation** 指令啟用自動協商功能時，最佳的設定將由 **capabilities** 指令決定。若要設定自動協商功能啟用時所使用的速度與雙工模式，請在該介面的能力清單中指定。

## 範例

以下示範如何將連接埠 NETP5 設定成 100Mbps 半雙工的模式運作。

```
Console(config)#interface ethernet NETP5
Console(config-if)#no negotiation
Console(config-if)#speed-duplex 100half
Console(config-if)#
```

## 相關指令

negotiation (4-76)

capabilities (4-77)

### 4.3.8.4 negotiation

此指令可啓用指定介面的自動協商功能，加上 **no** 則可停用自動協商功能。

## 語法

**negotiation**  
**no negotiation**

## 預設設定

啓用

## 指令模式

Interface Configuration (Ethernet、Port Channel)

## 指令使用方式

- 下連連接埠 SNP0-15 的自動協商功能永遠都是停用的。
- 啓用自動協商功能後，交換器便會根據 **capabilities** 指令的設定與對方協調出最適合線路的運作模式。若停用自動協商功能，就必須用 **speed-duplex** 與 **flowcontrol** 指令手動指定線路的屬性。
- 自動協商功能停用後，上連連接埠的自動 MDI/MDI-X 腳位訊號組態也會一併停用。

## 範例

以下示範將連接埠 SNP11 設定為使用自動協商功能。

```
Console(config)#interface ethernet SNP11
Console(config-if)#negotiation
Console(config-if)#
```



## 相關指令

capabilities (4-77)  
speed-duplex (4-75)  
flowcontrol (4-78)

### 4.3.8.5 capabilities

此指令可設定連接埠的自動協商功能啟用時，對外宣告所具有的能力，加上 **no** 與適當參數，則可消除原先宣告的能力，或者用 **no** 但不加上任何參數，即可恢復成預設值。

#### 語法

```
capabilities {1000full | 100full | 100half | 10full | 10half | flowcontrol |  
symmetric}  
no port-capabilities [1000full | 100full | 100half | 10full | 10half | flowcontrol |  
symmetric]
```

- 1000full – 支援 1000 Mbps 全雙工運作模式
- 100full – 支援 100 Mbps 全雙工運作模式
- 100half – 支援 100 Mbps 半雙工運作模式
- 10full – 支援 10 Mbps 全雙工運作模式
- 10half – 支援 10 Mbps 半雙工運作模式
- flowcontrol – 支援流量控制
- symmetric (僅適用於 Gigabit) – 指定此參數後，連接埠便會收發暫停封包 (pause frame)，若未指定此參數，連接埠會以自動協商的方式決定非對稱暫停封包的發送者與接收者。(目前此交換器的 ASCII 僅支援對稱式暫停封包。)

#### 預設設定

NETMGT : 10half、10full、100half、100full  
NETP0-7 : 10half、10full、100half、100full、1000full、flow control  
SNP0-15 : 1000full

#### 指令模式

Interface Configuration (Ethernet、Port Channel)

#### 指令使用方式

- SNP0-15 下連連接埠的能力固定為 1000full。
- NETP0-7 上連連接埠的能力包括：10half、10full、100half、100full、1000full、flowcontrol 與 symmetric。使用 **negotiation** 指令啟用自動協商功能後，交換器便會根據 **capabilities** 指令的設定與對方協調出最適合線路的運作模式。若停用自動協商功能，就必須用 **speed-duplex** 與 **flowcontrol** 指令手動指定線路的屬性。
- NETMGT 連接埠的能力固定為 10half、10full、100half、100full。

## 範例

以下範例將連接埠 NETP5 的能力設定為 100half、100full 與 flow control。

```
Console(config)#interface ethernet NETP5
Console(config-if)#no capabilities 10half
Console(config-if)#no capabilities 10hfull
Console(config-if)#no capabilities 1000full
Console(config-if)#capabilities 100half
Console(config-if)#capabilities 100full
Console(config-if)#capabilities flowcontrol
Console(config-if)#
```

## 相關指令

negotiation (4-76)  
speed-duplex (4-75)  
flowcontrol (4-78)

### 4.3.8.6 flowcontrol

此指令可啟用流量控制功能，加上 **no** 則可停用此功能。

---

**注意：**Sun Fire B1600 Blade 系統機箱內整合的交換器，每一個都含有一對相互連接的交換器晶片。兩個連接埠必須位於同一顆交換器晶片上，彼此之間才可以使用流量控制功能。連接埠 NETP0、NETP1、NETP4、NETP5，以及 SNP8 到 SNP15 位於同一顆交換器晶片上，連接埠 NETP2、NETP3、NETP6、NETP7，以及 SNP0 到 SNP7 則位於另一顆上。

---

## 語法

**flowcontrol**  
**no flowcontrol**

## 預設設定

啟用流量控制功能

## 指令模式

Interface Configuration (Ethernet、Port Channel)

## 指令使用方式

- 當交換器緩衝區滿載時，流量控制功能會阻擋交換器直接連接之末端主機或網段所傳來的流量，以免發生封包遺棄的狀況。此功能啟用後，半雙工運作模式會採用 back pressure，全雙工運作模式則使用 IEEE 802.3x。

- 若要強迫啓動或關閉流量控制功能（使用 **flowcontrol** 或 **no flowcontrol** 指令），請用 **no negotiation** 指令將選定介面的自動協商功能停用。
- 使用 **negotiation** 指令啓用自動協商功能時，最佳的設定將由 **capabilities** 指令決定。若希望自動協商時能使用流量控制功能，請務必將 **flowcontrol** 放入任何連接埠的能力清單內。
- 除非爲了解決問題的需要，否則請盡量避免在與集線器連接的連接埠上使用流量控制功能，因爲 **back pressure** 干擾訊號可能會導致該集線器連接的網段整體效能下降。

### 範例

以下示範如何啓用連接埠 NETP7 上的流量控制功能。

```
Console(config)#interface ethernet NETP7
Console(config-if)#flowcontrol
Console(config-if)#no negotiation
Console(config-if)#
```

### 相關指令

negotiation (4-76)

capabilities (flowcontrol, symmetric) (4-77)

## 4.3.8.7 shutdown

此指令可停用指定介面，加上 **no** 則可將被停用的介面重新啓動。

### 語法

```
shutdown
no shutdown
```

### 預設設定

所有介面預設均會啓用。

### 指令模式

Interface Configuration (Ethernet、Port Channel)

### 指令使用方式

此指令可停用行爲不正常的介面（例如碰撞次數過多），等問題解決之後再重新啓用該介面。有時爲了安全方面的因素，也會需要暫時停用連接埠。

## 範例

以下示範如何停用乙太網路連接埠 SNP5。

```
Console(config)#interface ethernet SNP5
Console(config-if)#shutdown
Console(config-if)#
```

### 4.3.8.8 switchport broadcast packet-rate

此指令可設定廣播風暴控制的參數，加上 **no** 則可停用廣播風暴控制功能。

#### 語法

```
switchport broadcast packet-rate rate
no switchport broadcast
```

*rate* – 流量上限值，以每秒中通過的封包個數計算。(範圍：16, 64, 128, 256)

#### 預設設定

所有連接埠預設均會啟用廣播風暴控制功能  
每秒鐘 256 個封包

#### 指令模式

Interface Configuration (Ethernet)

#### 指令使用方式

- 當廣播流量超過指定的上限時，超過部分的封包便會被丟棄。
- 此指令雖可啟用與停用選定介面的廣播風暴控制功能，但指定的流量上限卻是整個交換器一體適用。
- 下連連接埠 SNP0-15 的廣播風暴控制功能永遠都會啟用。

## 範例

以下示範如何將廣播流量抑制在每秒鐘 64 個封包：

```
Console(config)#interface ethernet SNP5
Console(config-if)#switchport broadcast packet-rate 64
Console(config-if)#
```

---

**注意：**請注意，**switchport broadcast** 指令雖然可單獨啟用個別介面的廣播流量控制功能，但其設定的廣播流量上限值對整個交換器卻是一體適用的。

---

### 4.3.8.9 clear counters

此指令可將介面的統計數據歸零。

#### 語法

**clear counters** *interface*

*interface* – **ethernet** *port-name*

*port-name* – 下連連接埠：SNP0-15；上連連接埠：NETP0-7；管理連接埠：NETMGT

#### 預設設定

無

#### 指令模式

Privileged Exec

#### 指令使用方式

統計數據只有在電源重開的時候才會重新開始計算，此指令只是將顯示給目前管理連線觀看的統計數據設為 0，等您登出然後再重新登入管理介面時，所看到的統計數據還是從上次電源重開之後一直累計到目前的值。

#### 範例

以下示範如何將連接埠 SNP5 的統計數據歸零。

```
Console#clear counters ethernet SNP5
Console#
```

### 4.3.8.10 show interfaces status

此指令可顯示介面的狀態。

#### 語法

**show interfaces status** [*interface*]

*interface*

- **ethernet** *port-name*

*port-name* – 下連連接埠：SNP0-15；上連連接埠：NETP0-7；管理連接埠：NETMGT

- **port-channel** *channel-id* (範圍：1-6)

- **vlan** *vlan-id* (範圍：1-4094)

## 預設設定

顯示所有介面的狀態。

## 指令模式

Normal Exec、Privileged Exec

## 指令使用方式

若未指定任何介面，則所有介面的資訊都會顯示出來。關於此指令顯示各項目的說明，請參閱第 3-78 頁的「顯示連線狀態」。

## 範例

```
Console#show interfaces status ethernet SNP11
Information of SNP11
Basic information:
  Port type: 1000SX
  Mac address: 00-00-e8-00-00-0a
Configuration:
  Name: Blade Slot 11
  Port admin status: Up
Speed-duplex: Auto
  Capabilities: 1000full,
Broadcast storm status: Enabled
  Broadcast storm limit: 256 packets/second
  Flow control status: Enabled
  LACP status: Disabled
Current status:
  Link status: Down
  Operation speed-duplex: 1000full
  Flow control type: Dot3X
Console#
```

### 4.3.8.11 show interfaces counters

此指令可顯示指定介面的統計數據。

## 語法

**show interfaces counters** [*interface*]

*interface*

- **ethernet** *port-name*

*port-name* – 下連連接埠：SNP0-15；上連連接埠：NETP0-7；管理連接埠：NETMGT

- **port-channel** *channel-id* (範圍：1-6)

## 預設設定

顯示所有介面的計數器。

## 指令模式

Normal Exec、Privileged Exec

## 指令使用方式

若未指定任何介面，則所有介面的資訊都會顯示出來。關於此指令顯示各項目的說明，請參閱第 3-113 頁的「顯示通訊埠統計數據」。

## 範例

```
Console#show interfaces counters ethernet NETP7
NETP7:
  Iftable stats:
    Octets input: 19648, Octets output: 714944
    Unicast input: 0, Unicast output: 0
    Discard input: 0, Discard output: 0
    Error input: 0, Error output: 0
    Unknown protos input: 0, QLen output: 0
  Extended iftable stats:
    Multi-cast input: 0, Multi-cast output: 10524
    Broadcast input: 136, Broadcast output: 0
  Ether-like stats:
    Alignment errors: 0, FCS errors: 0
    Single Collision frames: 0, Multiple collision frames: 0
    SQE Test errors: 0, Deferred transmissions: 0
    Late collisions: 0, Excessive collisions: 0
    Internal mac transmit errors: 0, Internal mac receive errors: 0
    Frame too longs: 0, Carrier sense errors: 0
  RMON stats:
    Drop events: 0, Octets: 734720, Packets: 10661
    Broadcast pkts: 136, Multi-cast pkts: 10525
    Undersize pkts: 0, Oversize pkts: 0
    Fragments: 0, Jabbers: 0
    CRC align errors: 0, Collisions: 0
    Packet size <= 64 octets:9877, Packet size 65 to 127 octets: 93
    Packet size 128 to 255 octets: 691, Packet size 256 to 511 octets: 0
    Packet size 512 to 1023 octets: 0, Packet size 1024 to 1518 octets: 0
Console#
```

## 4.3.8.12 show interfaces switchport

此指令可顯示介面的進階組態設定。

### 語法

**show interfaces switchport** [*interface*]

*interface*

- **ethernet** *port-name*

*port-name* – 下連連接埠：SNP0-15；上連連接埠：NETP0-7；管理連接埠：NETMGT

- **port-channel** *channel-id* (範圍：1-6)

### 預設設定

顯示所有介面。

### 指令模式

Normal Exec、Privileged Exec

### 指令使用方式

若未指定任何介面，則所有介面的資訊都會顯示出來。此指令顯示的項目包括：

- **Broadcast threshold** – 顯示是否已啟用廣播風暴抑制功能，如果有啟用，一併顯示流量上限值 (參閱第 4-80 頁)。
- **Lacp status** – 顯示是否已啟用 Link Aggregation Control Protocol (線路集束控制通訊協定) 功能 (參閱第 4-146 頁)。
- **VLAN membership mode** – 顯示隸屬模式為 Trunk 或 Hybrid (參閱第 4-107 頁)。
- **Ingress rule** – 顯示是否已啟用輸入過濾功能 (參閱第 4-109 頁)。
- **Acceptable frame type** – 顯示可接受的 VLAN 封包是否包含所有種類，或只限有加註標籤的封包而已 (參閱第 4-108 頁)。
- **Native VLAN** – 顯示預設連接埠 VLAN ID (參閱第 4-110 頁)。
- **Priority for untagged traffic** – 顯示未加註任何標籤之封包的預設優先等級 (參閱第 4-132 頁)。
- **Gvrp status** – 顯示是否已啟用 GARP VLAN Registration Protocol (GARP VLAN 註冊通訊協定) (參閱第 4-114 頁)。
- **Allowed Vlan** – 顯示此介面加入的 VLAN，其中 (u) 代表未加註標記，(t) 代表會加註標記 (參閱第 4-111 頁)。
- **Forbidden Vlan** – 顯示此介面無法透過 GVRP 動態加入的 VLAN (參閱第 4-112 頁)。



## 範例

以下範例顯示乙太網路連接埠 NETP7 的組態設定。

```
Console#show interfaces switchport ethernet NETP7
Information of NETP7
Broadcast threshold: Enabled, 256 packets/second
Lacp status: Enabled
VLAN membership mode: Hybrid
Ingress rule: Disabled
Acceptable frame type: All frames
Native VLAN: 1
Priority for untagged traffic: 0
Gvrp status: Enabled
Allowed Vlan: 1(u),
Forbidden Vlan: 2,
Console#
```

## 4.3.9 位址表指令

這些指令可設定位址表過濾特定位址、顯示位址表所含項目、清除位址表內容以及設定保留期限。

指令	功能	模式	頁數
mac-address-table static	將靜態位址對應到 VLAN 中的某個連接埠	GC	4-86
clear mac-address-table dynamic	將轉送資料庫中所學得的項目刪除	PE	4-87
show mac-address-table	顯示橋接轉送資料庫中的資料	PE	4-87
mac-address-table aging-time	設定位址表的保留期限	GC	4-88
show mac-address-table aging-time	顯示位址表的保留期限	PE	4-89

### 4.3.9.1 mac-address-table static

此指令可將靜態位址對應到某個目的連接埠，加上 **no** 則可將此位址刪除。

#### 語法

```
mac-address-table static mac-address {interface interface} vlan vlan-id [action]  
no mac-address-table static mac-address vlan vlan-id
```

- *mac-address* – MAC 位址。
- *interface*
  - **ethernet** *port-name*  
*port-name* – 下連接埠：SNP0-15；上連接埠：NETP0-7；管理連接埠：NETMGT
  - **port-channel** *channel-id* (範圍：1-6)
- *vlan-id* – VLAN ID (範圍：1-4094)
- *action* –
  - **permanent** – 此設定永久有效。
  - **delete-on-reset** – 此設定有效期限僅到下次交換器重設為止。

#### 預設設定

預設並未定義任何靜態位址。預設模式為 **permanent**。

#### 指令模式

Global Configuration

#### 指令使用方式

- 主機裝置的靜態位址可設定在特定 VLAN 的某一個連接埠上。此指令可將靜態位址加入 MAC 位址表。靜態位址特性如下：
  - 當介面線路斷線時，位址表中的靜態位址並不會隨之消失。
  - 靜態位址會一直固定在所指定的介面上，不會移動到其他介面。出現在其他介面的靜態位址會被忽略，也不會寫入位址表內。
  - 靜態位址若未以這個指令加上 **no** 刪除，其它連接埠永遠都不會學到此靜態位址。

#### 範例

```
Console(config)#mac-address-table static 00-e0-29-94-34-de  
ethernet SNP1 vlan 1 delete-on-reset  
Console(config)#
```

### 4.3.9.2 clear mac-address-table dynamic

此指令可將轉送資料庫中學習到的項目全部刪除，並將靜態設定或系統設定之項目的收送統計數據歸零。

#### 預設設定

無

#### 指令模式

Privileged Exec

#### 範例

```
Console#clear mac-address-table dynamic
Console#
```

### 4.3.9.3 show mac-address-table

此指令可顯示橋接轉送資料庫中項目的類別。

#### 語法

```
show mac-address-table [address mac-address [mask]] [interface interface]
  [vlan vlan-id] [sort {address | vlan | interface}]
```

- *mac-address* – MAC 位址。
- *mask* – 表示應忽略位址中哪些位元。
- *interface*
  - **ethernet** *port-name*  
*port-name* – 下連連接埠：SNP0-15；上連連接埠：NETP0-7；管理連接埠：NETMGT
  - **port-channel** *channel-id* (範圍：1-6)
- *vlan-id* – VLAN ID (範圍：1-4094)
- **sort** – 根據位址、vlan 或介面排序。

#### 預設設定

無

#### 指令模式

Privileged Exec

## 指令使用方式

MAC 位址表含有每個介面所知的 MAC 位址，請注意 Type 欄位可能含有以下的類別：

- Learned – 動態位址項目
- Permanent – 靜態項目
- Delete-on-reset – 系統重設時便會刪除的靜態項目

## 範例

```
Console#show mac-address-table
Interface Mac Address      Vlan Type
-----
      SNP11 00-10-b5-62-03-74    1 Learned
Console#
```

### 4.3.9.4 mac-address-table aging-time

此指令可設定位址表中各項目的保留期限，加上 **no** 則可恢復為預設的保留期限。

#### 語法

```
mac-address-table aging-time seconds
no mac-address-table aging-time
```

*seconds* – 時間以秒數計算 (18-2184)。

#### 預設設定

300 秒

#### 指令模式

Global Configuration

#### 指令使用方式

保留期限可將動態得知但已使用時間過久的轉送資訊刪除。

## 範例

```
Console(config)#mac-address-table aging-time 300
Console(config)#
```

### 4.3.9.5 show mac-address-table aging-time

此指令可顯示位址表內各項目的保留期限。

#### 預設設定

無

#### 指令模式

Privileged Exec

#### 範例

```
Console#show mac-address-table aging-time
Aging time: 300 sec.
Console#
```

### 4.3.10 連接埠安全功能指令

這些指令可停用學習功能，或手動指定連接埠的安全位址。建議您可以先暫時將連接埠安全功能關閉一段時間（已啟用學習功能），讓目前 VLAN 所有成員都在此連接埠上註冊之後，再啟用連接埠安全功能，才能確保連接埠會將含有未知來源 MAC 位址或被其它連接埠學習得知的封包丟棄。

指令	功能	模式	頁數
port security	設定安全連接埠	IC	4-90
mac-address-table static	將靜態位址對應到 VLAN 中的某個連接埠	GC	4-86
show mac-address-table	顯示橋接轉送資料庫中的資料	PE	4-87

### 4.3.10.1 port security

此指令可設定安全的連接埠，加上 **no** 則可停用連接埠的安全功能。

#### 語法

```
port security
no port security
```

#### 預設設定

所有連接埠的安全功能預設都是停用的。

#### 指令模式

Interface Configuration (Ethernet)

#### 指令使用方式

- 連接埠的安全功能啟用後，交換器便會停止在指定連接埠上學習新的位址。流進來的封包中，只有來源位址在動態或靜態位址表中找得到的封包才會被接受。
- 若要使用連接埠安全功能，首先應讓交換器動態學習連接埠上接收到的封包的 < 來源 MAC 位址與 VLAN >，等學習一段時間之後，再啟用連接埠安全功能，並停止位址學習功能。請注意，學習功能打開的時間一定要夠長，才能讓 VLAN 的所有成員全部在選定連接埠上註冊。
- 以後若要增加新的 VLAN 成員，可以手動用 **mac-address-table static** 指令將安全位址加入，或關閉連接埠安全功能一段時間，讓學習功能重新啟用，以便新的 VLAN 成員進行註冊。然後再視情況需要停用學習功能。
- 安全連接埠有以下限制：
  - 不可使用連接埠監視功能。
  - 不可成爲多 VLAN 連接埠。
  - 不可連上網路互連裝置。
  - 不可加入寬道。

#### 範例

以下示範如何啟用 SNP5 連接埠的安全功能：

```
Console(config)#interface ethernet SNP5
Console(config-if)#port security
```

#### 相關指令

```
mac-address-table static (4-86)
show mac-address-table (4-87)
```

## 4.3.11 Spanning Tree 指令

本節所含指令可設定整台交換器的 Spanning Tree Algorithm (Spanning Tree 演算法，簡稱 STA)，亦可設定某個介面的 STA。

指令	功能	模式	頁數
spanning-tree	啓用 spanning tree 通訊協定	GC	4-92
spanning-tree mode	設定使用 STP 或 RSTP 模式	GC	4-93
spanning-tree forward-time	設定 spanning tree 的橋接轉送時間	GC	4-94
spanning-tree hello-time	設定 spanning tree 橋接 hello 時間	GC	4-95
spanning-tree max-age	設定 spanning tree 橋接保留期限	GC	4-95
spanning-tree priority	設定 spanning tree 橋接優先等級	GC	4-96
spanning-tree path-cost method	設定 RSTP 的路徑成本方法	GC	4-97
spanning-tree transmission-limit	設定 RSTP 的傳輸限制	GC	4-97
spanning-tree cost	設定介面的 spanning tree 路徑成本	IC	4-98
spanning-tree port-priority	設定介面的 spanning tree 優先等級	IC	4-99
spanning-tree edge-port	啓用邊緣連接埠的快速轉送功能	IC	4-100
spanning-tree protocol-migration	重新檢查適當的 BPDU 格式	PE	4-101
spanning-tree link-type	設定 RSTP 的線路類別	IC	4-101
show spanning-tree	設定 spanning tree 組態	PE	4-102

### 4.3.11.1 spanning-tree

此指令可啓動整台交換器的 spanning tree 演算法，加上 **no** 則可停用此功能。

#### 語法

```
spanning-tree  
no spanning-tree
```

#### 預設設定

spanning tree 功能預設會啓用。

#### 指令模式

Global Configuration

#### 指令使用方式

Spanning Tree 演算法可偵測網路中出現的迴路予以消除，同時還能為交換器、橋接器與路由器之間提供備援線路。讓交換器得以與網路上的其它橋接裝置（即具有 STA 功能的交換器、橋接器或路由器）協調搭配，確保網路中任何兩點之間只有一條路由存在，而且萬一這條主要路由斷掉時，還會自動接起一條備援路由予以取代。

#### 範例

以下示範如何啓用交換器的 spanning tree 演算法：

```
Console(config)#spanning-tree  
Console(config)#
```



## 4.3.11.2 spanning-tree mode

此指令可選取交換器的 spanning tree 模式，加上 **no** 則可恢復為預設值。

### 語法

```
spanning-tree mode {stp | rstp}
no spanning-tree mode
```

- **stp** – Spanning Tree Protocol (Spanning Tree 通訊協定，IEEE 802.1D)
- **rstp** – Rapid Spanning Tree (快速 Spanning Tree，IEEE 802.1w)

### 預設設定

stp

### 指令模式

Global Configuration

### 指令使用方式

- 快速 Spanning Tree 通訊協定  
RSTP 會監視收到的通訊協定訊息，並動態調整 RSTP 節點傳送的通訊協定訊息類別，因此無論連接的節點支援 STP 或 RSTP 都能支援，詳細運作狀況如下所述：
  - STP Mode – 若連接埠的移轉延遲計時器終止後，交換器收到 802.1D 的 BPDU，交換器便會假設自己是連到 802.1D 的橋接器，以後就只會使用 802.1D 的 BPDU。
  - RSTP Mode – 若 RSTP 原本在某個連接埠上使用的是 802.1D BPDU，但在移轉延遲時間到期之後，卻收到 RSTP BPDU，則 RSTP 就會重新啓動移轉延遲計時器，並開始在此連接埠上使用 RSTP BPDU。

### 範例

以下示範如何將交換器設定成使用快速 Spanning Tree：

```
Console(config)#spanning-tree mode rstp
Console(config)#
```

### 4.3.11.3 spanning-tree forward-time

此指令可設定整個交換器的 spanning tree 橋接轉送時間，加上 **no** 則可恢復為預設值。

#### 語法

**spanning-tree forward-time** *seconds*

**no spanning-tree forward-time**

*seconds* – 時間，以秒為單位。(範圍：4-30 秒)

最小值為 4 與 [(最長期限 / 2) + 1] 兩者取較大值。

#### 預設設定

15 秒

#### 指令模式

Global Configuration

#### 指令使用方式

此指令可設定根裝置應等待多久時間 (以秒為單位) 後，才可以開始改變狀態 (即丟棄原有資料，開始學習轉送所需的資訊)。由於每個裝置都必須先接收網路拓樸的變化資訊，才能開始轉送封包，因此這項延遲時間是有必要的。此外，每個連接埠也都需要時間觀察可能會導致其回到丟棄狀態的衝突資訊，否則網路中便有可能出現暫時性的資料迴路。

#### 範例

```
Console(config)#spanning-tree forward-time 20
Console(config)#
```

### 4.3.11.4 spanning-tree hello-time

此指令可設定整個交換器的 spanning tree 橋接 hello 時間，加上 **no** 則可恢復為預設值。

#### 語法

**spanning-tree hello-time** *time*  
**no spanning-tree hello-time**

*time* – 時間，以秒為單位。(範圍：1-10 秒)  
最大值為 10 與 [(最長期限 / 2) - 1] 兩者取較小值。

#### 預設設定

2 秒

#### 指令模式

Global Configuration

#### 指令使用方式

此指令會設定根裝置每隔多久 (以秒為單位) 回傳送一個組態訊息。

#### 範例

```
Console(config)#spanning-tree hello-time 5  
Console(config)#
```

### 4.3.11.5 spanning-tree max-age

此指令可設定整個交換器的 spanning tree 橋接保留期限，加上 **no** 則可恢復為預設值。

#### 語法

**spanning-tree max-age** *seconds*  
**no spanning-tree max-age**

*seconds* – 時間，以秒為單位。(範圍：6-40 秒)  
最小值為 6 與 [2 x (hello 時間) + 1] 兩者取較大值。  
最大值為 40 與 [2 x (hello 時間) - 1] 兩者取較小值。

#### 預設設定

20 秒

#### 指令模式

Global Configuration

## 指令使用方式

此指令可設定裝置應該等待多久時間 (以秒為單位) 沒收到組態訊息之後，才開始重新設定組態。所有裝置連接埠 (除了指定的連接埠之外) 都應該定時收到組態訊息。在任何連接埠上，只要最近一次收到之組態訊息中的 STA 資訊過期，便會成爲其所連接 LAN 的指定連接埠。如果該連接埠本身又正好是根連接埠，則此網路中所連的裝置連接埠便會再選出一個新的根連接埠。

## 範例

```
Console(config)#spanning-tree max-age 40
Console(config)#
```

### 4.3.11.6 spanning-tree priority

此指令可設定整台交換器的 spanning tree 優先等級，加上 **no** 則可恢復爲預設值。

## 語法

**spanning-tree priority *priority***  
**no spanning-tree priority**

*priority* – 橋接器的優先等級。  
(範圍 – 0-61440，以 4096 爲單位遞增；可使用的值；0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440)

## 預設設定

32768

## 指令模式

Global Configuration

## 指令使用方式

橋接器優先等級是用來選取根裝置、根連接埠與指定連接埠的。擁有最高優先等級的裝置，便成爲 STA 的根裝置。如果所有裝置的優先等級都相同，則以 MAC 位址最低的裝置當作根裝置。

## 範例

```
Console(config)#spanning-tree priority 40000
Console(config)#
```

### 4.3.11.7 spanning-tree pathcost method

此指令可設定快速 Spanning Tree 所使用的路徑成本方法，加上 **no** 則可恢復為預設值。

#### 語法

**spanning-tree pathcost method {long | short}**  
**no spanning-tree pathcost method**

- **long** – 使用 32 位元的值，範圍從 1 到 200,000,000。
- **short** – 使用 32 位元的值，範圍從 1 到 65535。

#### 預設設定

short 方法

#### 指令模式

Global Configuration

#### 指令使用方式

路徑成本方法的用途在於找出裝置之間的最佳路徑，因此較低的數值應該設定給連接速度較快媒體的連接埠，較高的數值應該設定給連接速度較慢媒體的連接埠。請注意，路徑成本（參閱第 4-98 頁）的效用排在連接埠優先等級之前。（參閱第 4-99 頁。）

#### 範例

```
Console(config)#spanning-tree pathcost method long
Console(config)#
```

### 4.3.11.8 spanning-tree transmission-limit

此指令可設定兩個連續傳送的 RSTP BPDU 之間應該至少間隔多少時間，加上 **no** 則可恢復為預設值。

#### 語法

**spanning-tree transmission-limit count**  
**no spanning-tree transmission-limit**

*count* – 傳輸時間限制，以秒為單位。（範圍：1-10）

#### 預設設定

3

#### 指令模式

Global Configuration

## 指令使用方式

此指令可限制 BPDU 的最大重傳速率。

## 範例

```
Console(config)#spanning-tree transmission-limit 4
Console(config)#
```

### 4.3.11.9 spanning-tree cost

此指令可設定指定介面的 `spanning tree` 路徑成本，加上 `no` 則可恢復為預設值。

## 語法

**spanning-tree cost** *cost*  
**no spanning-tree cost**

*cost* – 此介面的路徑成本。  
(範圍 – 1-200,000,000)  
建議範圍如下 –

- 乙太網路：200,000-20,000,000
- 快速乙太網路：20,000-2,000,000
- Gigabit 乙太網路：2,000-200,000

## 預設設定

- 乙太網路 – 半雙工：2,000,000，全雙工：1,000,000，寬道：500,000
- 快速乙太網路 – 半雙工：200,000，全雙工：100,000，寬道：50,000
- Gigabit 乙太網路 – 全雙工：10,000，寬道：5,000

## 指令模式

Interface Configuration (Ethernet、Port Channel)

## 指令使用方式

- `spanning-tree` 演算法利用此指令決定裝置之間的最佳路徑，因此較低的數值應該設定給連接速度較快媒體的介面，較高的數值應該設定給連接速度較慢媒體的介面。
- 路徑成本的效用排在連接埠優先等級之前。
- 當 `spanning-tree` 路徑成本方法設定為 `short` 時，路徑成本的最大值為 65,535。

## 範例

```
Console(config)#interface ethernet SNP5
Console(config-if)#spanning-tree cost 50
Console(config-if)#
```

## 相關指令

spanning-tree port-priority (4-99)

### 4.3.11.10 spanning-tree port-priority

此指令可設定指定介面的優先等級，加上 **no** 則可恢復為預設值。

#### 語法

**spanning-tree port-priority** *priority*

**no spanning-tree port-priority**

*priority* – 介面的優先等級。(範圍：0-240，以 16 為單位遞增)

#### 預設設定

128

#### 指令模式

Interface Configuration (Ethernet、Port Channel)

#### 指令使用方式

- 此指令可定義介面在 **spanning-tree** 演算法中使用的優先等級。若交換器上所有介面的路徑成本都一樣，則優先等級最高(數值最低)的介面便會被設定成 **spanning tree** 中的主線路。
- 若被設定為最高優先等級的介面個數不只一個，則啓動其中識別碼數字最低的介面。

#### 範例

```
Console(config)#interface ethernet SNP5
Console(config-if)#spanning-tree port-priority 0
Console(config-if)#
```

## 相關指令

spanning-tree cost (4-98)

### 4.3.11.11 spanning-tree edge-port

此指令可將某個介面設定為邊緣連接埠，加上 **no** 則可恢復為預設值。

#### 語法

```
spanning-tree edge-port  
no spanning-tree edge-port
```

#### 預設設定

NETP0-7、NETMGT：停用  
SNP0-15：啓用 ( 固定為此設定值 )

#### 指令模式

Interface Configuration (Ethernet、Port Channel)

#### 指令使用方式

若介面連上的是末端節點或位於橋接 LAN 末端的 LAN 網段，便可啓用此選項。由於末端節點不可能導致轉送迴路，因此可以直接跳過到達 **spanning tree** 的轉送狀態。設定成 **Edge Port** 可以讓工作站或伺服器之類的裝置收斂速度加快，保留現有的轉送資料庫以減少重新設定組態時因重建位址表而發出的廣播封包數量，此介面更改狀態時，**Spanning Tree** 不會啓動重新設定組態程序，而且還能克服其它 STA 相關的逾時問題。雖然有這麼多好處，但請務必記得 **Edge Port** 只能在連接末端節點裝置的連接埠上啓用。

#### 範例

```
Console(config)#interface ethernet SNP5  
Console(config-if)#spanning-tree edge-port  
Console(config-if)#
```



### 4.3.11.12 spanning-tree protocol-migration

此指令可重新檢查要在選定介面上發出的適當 BPDU 格式。

#### 語法

**spanning-tree protocol-migration** *interface*

*interface*

- **ethernet** *port-name*

*port-name* – 下連連接埠：SNP0-15；上連連接埠：NETP0-7；管理連接埠：NETMGT

- **port-channel** *channel-id* (範圍：1-6)

#### 指令模式

Privileged Exec

#### 指令使用方式

任何時候只要交換器偵測到 STP BPDU，包括 Configuration (組態設定) 或 Topology Change Notification (拓樸改變通知) BPDU，都會自動將選定介面設定為強制 STP 相容模式。不過，任何時候您都可以用 **spanning-tree protocol-migration** 指令，手動重新勾選適合在選定介面上發送出去的 BPDU 格式 (RSTP 或 STP 相容)。

#### 範例

```
Console(config)#interface ethernet SNP5
Console(config-if)#spanning-tree protocol-migration
Console(config-if)#
```

### 4.3.11.13 spanning-tree link-type

此指令可設定快速 Spanning Tree 使用的線路種類，加上 **no** 則可恢復為預設值。

#### 語法

**spanning-tree link-type** {**auto** | **point-to-point** | **shared**}

**no spanning-tree link-type**

- **auto** – 自動從雙工模式設定推測線路種類。
- **point-to-point** – 點對點線路。
- **shared** – 共用媒體。

#### 預設設定

auto

#### 指令模式

Interface Configuration (Ethernet、Port Channel)

## 指令使用方式

- 如果此介面只能連上一個橋接器，請選用 **point-to-point** 線路，若此介面只能連上兩個或多個橋接器，請選用 **shared** 線路。
- 選用自動偵測方式時，交換器會根據雙工模式推測出線路的種類：全雙工介面視為點對點線路，半雙工介面則視為共用線路。
- RSTP 僅適用於兩個橋接器之間的點對點線路，在設定為共用線路的連接埠上不能使用 RSTP 的。

## 範例

```
Console(config)#interface ethernet SNP5
Console(config-if)#spanning-tree link-type point-to-point
Console(config-if)#
```

### 4.3.11.14 show spanning-tree

此指令可顯示 **spanning tree** 的組態。

#### 語法

**show spanning-tree** [*interface*]

- *interface*
  - **ethernet** *port-name*  
*port-name* – 下連連接埠：SNP0-15；上連連接埠：NETP0-7；管理連接埠：NETMGT
  - **port-channel** *channel-id* (範圍：1-6)

#### 預設設定

無

#### 指令模式

Privileged Exec

#### 指令使用方式

- 使用 **show spanning-tree** 指令時若未加上任何參數，則除了顯示交換器的 **spanning tree** 組態之外，還會將 **spanning tree** 中每個介面的組態也顯示出來。
- 若要顯示某個介面的 **spanning tree** 組態，請使用 **show spanning-tree interface** 指令。
- 關於 **Bridge-group information** 下所顯示的各項目說明，請參閱第 3-55 頁的「設定基本 STA 組態」。關於各介面之顯示項目的說明，請參閱第 3-100 頁的「管理 Spanning Tree 演算法介面」。

## 範例

```
Console#show spanning-tree
Bridge-group information
-----
Spanning tree mode           : RSTP
Spanning tree enable/disable : enable
Priority                     : 32768
Bridge Hello Time (sec.)    : 2
Bridge Max Age (sec.)      : 20
Bridge Forward Delay (sec.) : 15
Root Hello Time (sec.)     : 2
Root Max Age (sec.)       : 20
Root Forward Delay (sec.)  : 15
Designated Root            : 8.0000E8666672
Current root port          : 0
Current root cost          : 0
Number of topology changes : 0
Last topology changes time (sec.): 1363
Transmission limit         : 3
Path Cost Method           : 21
-----
SNP0 information
-----
Admin status      : enable
Role              : designate
State             : forwarding
Path cost         : 10000
Priority          : 128
Designated cost   : 0
Designated port   : 8.1
Designated root   : 8.0000E8666672
Designated bridge : 8.0000E8666672
Forward transitions : 0
Admin edge port   : disable
Oper edge port    : disable
Admin Link type   : point-to-point
Oper Link type    : point-to-point
.
.
.
Console#
```

## 4.3.12 VLAN 指令

VLAN 由一群位於網路中任何位置的連接埠構成，但這些連接埠彼此之間以特殊方式聯繫，使他們看起來有如位於同一個實體網段內。本節所說明的指令，可用來建立 VLAN 群組、新增連接埠成員、指定 VLAN 標記如何使用以及啓用選定介面的自動 VLAN 註冊功能。

指令	功能	模式	頁數
<i>編輯 VLAN 群組</i>			
vlan database	進入 VLAN 資料庫模式，準備開始新增、更改或刪除 VLAN	GC	4-105
vlan	設定 VLAN，包括 VID、名稱與狀態	VC	4-105
<i>設定 VLAN 介面</i>			
interface vlan	進入指定 VLAN 的介面組態設定模式	GC	4-106
switchport mode	設定介面的 VLAN 成員模式	IC	4-107
switchport acceptable-frame-types	設定介面可接受的封包種類	IC	4-108
switchport ingress-filtering	啓用介面的輸入過濾功能	IC	4-109
switchport native vlan	設定介面的 PVID ( 固有 VLAN)	IC	4-110
switchport allowed vlan	設定介面相關的 VLAN	IC	4-111
switchport gvrp	啓用介面的 GVRP	IC	4-114
switchport forbidden vlan	設定介面拒絕的 VLAN	IC	4-112
<i>顯示 VLAN 資訊</i>			
show vlan	顯示 VLAN 資訊	NE、 PE	4-113
show interfaces status vlan	顯示指定 VLAN 介面的狀態	NE、 PE	4-81
show interfaces switchport	顯示介面的管理與運作狀態	NE、 PE	4-84

### 4.3.12.1 vlan database

此指令可進入 VLAN 資料庫模式，此模式中的所有指令均會立刻生效。

#### 預設設定

無

#### 指令模式

Global Configuration

#### 指令使用方式

- 此 VLAN 資料庫指令模式可用來新增、更改與刪除 VLAN，等組態修改完畢之後，可以輸入 **show vlan** 指令將 VLAN 設定值顯示出來。
- **interface vlan** 指令模式可以定義連接埠成員隸屬模式、將連接埠加入 VLAN 內以及刪除 VLAN 內的連接埠。這些指令的結果都會寫入執行組態檔案內，輸入 **show running-config** 指令便可顯示這個檔案。

#### 範例

```
Console(config)#vlan database
Console(config-vlan)#
```

#### 相關指令

show vlan (4-113)

### 4.3.12.2 vlan

此指令可用來設定 VLAN，加上 **no** 則可恢復為預設值或將 VLAN 刪除。

#### 語法

```
vlan vlan-id [name vlan-name] media ethernet [state {active | suspend}]
no vlan vlan-id [name | state]
```

- *vlan-id* – 欲設定之 VLAN 的 ID。(範圍：1-4094，數字前面請勿加上 0)
- **name** – VLAN 名稱之前的關鍵字。
  - *vlan-name* – ASCII 字串，長度從 1 到 15 個字元。
- **media ethernet** – 乙太網路媒介類別。
- **state** – 緊跟在 VLAN 狀態後的關鍵字。
  - **active** – VLAN 運作中。
  - **suspend** – VLAN 暫停運作。暫停運作的 VLAN 不會傳遞封包。

#### 預設設定

預設只有一個 VLAN (VLAN 1) 運作。

## 指令模式

VLAN Database Configuration

## 指令使用方式

- **no vlan *vlan-id*** 刪除 VLAN。
- **no vlan *vlan-id* name** 刪除 VLAN 名稱。
- **no vlan *vlan-id* state** 將 VLAN 恢復為預設狀態 ( 啟動 )。
- 除了 VLAN 1 之外，其它任何 VLAN 都可以暫停。
- 交換器上最多可以設定 255 個 VLAN。

## 範例

以下範例用 *vlan-id* 105 與名稱 RD5 新增一個 VLAN，此 VLAN 預設就會運作。

```
Console(config)#vlan database
Console(config-vlan)#vlan 105 name RD5 media ethernet
Console(config-vlan)#
```

## 相關指令

show vlan (4-113)

### 4.3.12.3 interface vlan

此指令可進入 VLAN 的介面組態模式與設定實體介面。

## 語法

**interface vlan *vlan-id***

*vlan-id* – 欲設定之 VLAN 的 ID。( 範圍：1-4094，數字前面請勿加上 0)

## 預設設定

無

## 指令模式

Global Configuration

## 範例

以下示範如何將介面組態模式設定為 VLAN 1，並設定 VLAN 的 IP 位址：

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.254 255.255.255.0
Console(config-if)#
```

## 相關指令

shutdown (4-79)

### 4.3.12.4 switchport mode

此指令可設定連接埠的 VLAN 隸屬模式，加上 **no** 則可恢復為預設值。

#### 語法

**switchport mode {trunk | hybrid}**

**no switchport mode**

- **trunk** – 將連接埠作為 VLAN 寬道的一個端點。由於寬道是兩個交換器之間的直接連線，因此這個連接埠會傳輸標籤標示該來源 VLAN 的封包。不過請注意一點，隸屬連接埠預設 VLAN (即 PVID 所指) 的封包，傳送時不會加上標籤。
- **hybrid** – 指定混合式 VLAN 介面，表示連接埠可以傳送有加註標籤與沒加註標籤的封包。

#### 預設設定

所有連接埠預設都是混合模式，且 PVID 均設定為 VLAN 1。

#### 指令模式

Interface Configuration (Ethernet、Port Channel)

#### 範例

以下示範如何將組態模式設定為 SNP1，接著將 switchport 模式設定為 hybrid：

```
Console(config)#interface ethernet SNP1
Console(config-if)#switchport mode hybrid
Console(config-if)#
```

## 4.3.12.5 switchport acceptable-frame-types

此指令可設定連接埠接收的封包類別，加上 **no** 則可恢復為預設值。

### 語法

```
switchport acceptable-frame-types {all | tagged}  
no switchport acceptable-frame-types
```

- **all** – 此連接埠可接收所有封包，無論有無加註標籤均可。
- **tagged** – 此連接埠只接收有加註標籤的封包。

### 預設設定

所有類別的封包均可接受

### 指令模式

Interface Configuration (Ethernet、Port Channel)

### 指令使用方式

設定成接收所有類別的封包時，所收到未加註任何標籤的封包都會被分給預設 VLAN。

### 範例

以下示範如何限制 SNP1 只接收有加註標籤的封包：

```
Console(config)#interface ethernet SNP1  
Console(config-if)#switchport acceptable-frame-types tagged  
Console(config-if)#
```



## 4.3.12.6 switchport ingress-filtering

此指令可啓用介面的輸入過濾功能，加上 **no** 則可恢復爲預設值。

### 語法

```
switchport ingress-filtering
no switchport ingress-filtering
```

### 預設設定

停用

### 指令模式

Interface Configuration (Ethernet、Port Channel)

### 指令使用方式

- 輸入過濾功能只對加註標籤的封包有影響。
- 若停用輸入過濾功能，則當此介面收到有加註 VLAN 標籤的封包時，只要封包的標籤符合交換器已知的任何一個 VLAN，此介面就會將該封包收進來（除非封包的標籤剛好是此連接埠明確禁止 VLAN）。
- 若啓用輸入過濾功能，且此介面收到的封包其標籤指的 VLAN 並未含有這個輸入連接埠，則此介面就會將此封包丟棄。
- 輸入過濾功能對沒用到 VLAN 的 BPDU 封包，例如 GVRP 與 STP 等等，並無任何影響。但是對於 GMRP 之類會用到 VLAN 的 BPDU 封包就絕對有影響。

### 範例

以下示範如何將介面設定爲 SNP1 連接埠，然後啓用其輸入過濾功能：

```
Console(config)#interface ethernet SNP1
Console(config-if)#switchport ingress-filtering
Console(config-if)#
```

### 4.3.12.7 switchport native vlan

此指令可設定介面的 PVID (即預設 VID)，加上 **no** 則可恢復為預設值。

#### 語法

```
switchport native vlan vlan-id  
no switchport native vlan
```

*vlan-id* – 介面的預設 VLAN ID。(範圍：1-4094，數字前面請勿加上 0)

#### 預設設定

VLAN 1

#### 指令模式

Interface Configuration (Ethernet、Port Channel)

#### 指令使用方式

- 若介面不屬於 VLAN 1，但您將其 PVID 指派為此 VLAN，該介面便會自動被加入 VLAN 1 內，視為不會加註標籤的成員。至於其他所有 VLAN，所有介面都必須先設定成不會加註標籤的成員，才可以將其 PVID 設為該群組。
- 若可接受封包類別設定為 **all** 或 **switchport** 模式設定為 **hybrid**，此 PVID 就會被放到進入此輸入連接埠且未加註任何標籤的封包內。

#### 範例

以下示範如何將 SNP1 連接埠的 PVID 設定為 VLAN 3：

```
Console(config)#interface ethernet SNP1  
Console(config-if)#switchport native vlan 3  
Console(config-if)#
```

## 4.3.12.8 switchport allowed vlan

此指令可設定選定介面上的 VLAN 群組，加上 **no** 則可恢復為預設值。

### 語法

**switchport allowed vlan** {**add** *vlan* [**tagged** | **untagged**] | **remove** *vlan*}

- **add** *vlan* – 欲加入的 VLAN 識別碼。
- **remove** *vlan* – 欲刪除的 VLAN 識別碼。

數字開頭不可以是 0。(範圍：1-4094)

**no switchport allowed vlan**

---

**注意：**您無法使用 NETMGT 連接埠的 **no switchport allowed vlan** 指令 (否則交換器會顯示錯誤訊息)。若要讓管理連接埠恢復到其出廠預設的 VLAN (即 VLAN 2)，並將它從其他 VLAN 中刪除，請輸入以下指令：

```
Console(config)#interface ethernet NETMGT
Console(config-if)#switchport allowed vlan add 2
Console(config-if)#switchport native vlan 2
Console(config-if)#switchport allowed vlan remove <vlan id>
```

其中 *<vlan id>* 指 NETMGT 曾加入的 VLAN (VLAN 2 除外) 編號。(除了 VLAN 2 之外，請對 NETMGT 所隸屬其它所有 VLAN 重複以上指令。)

---

### 預設設定

- 所有連接埠 (不含 NETMGT) 均預設隸屬於 VLAN 1。NETMGT 則預設隸屬於 VLAN 2。
- 預設封包類別是未加註任何標籤的封包。

### 指令模式

Interface Configuration (Ethernet、Port Channel)

### 指令使用方式

- 若 **switchport** 模式設定為 **trunk**，則將介面設定成屬於任何 VLAN 群組時，介面就只能當作會加註標籤的成員。
- 封包在交換器之內都有加上標籤。將 VLAN 加入介面時所使用的 **tagged** 與 **untagged** 參數，是告訴交換器發出封包時，應保留或移除封包上的標籤。
- 若中間經過的網路裝置以及連線另一端的主機都不支援 VLAN，此介面就應當作不會加註標籤的成員加入這些 VLAN 內，否則最多只要加入一個未加註標籤的 VLAN 即可，而且加入的應該就是介面原本所隸屬的 VLAN。
- 若介面拒絕清單上的某個 VLAN 被手動加入該介面，該 VLAN 便會自動從該介面的拒絕清單中移除。

## 範例

以下示範如何將 VLAN 1、2、5 與 6 加入 SNP1 的允許清單內當作有加註標籤的 VLAN：

```
Console(config)#interface ethernet SNP1
Console(config-if)#switchport allowed vlan add 1 tagged
Console(config-if)#switchport allowed vlan add 2 tagged
Console(config-if)#switchport allowed vlan add 5 tagged
Console(config-if)#switchport allowed vlan add 6 tagged
Console(config-if)#
```

### 4.3.12.9 switchport forbidden vlan

此指令可設定拒絕 VLAN，加上 **no** 則可刪除拒絕 VLAN 清單。

#### 語法

**switchport forbidden vlan {add *vlan* | remove *vlan*}**  
**no switchport forbidden vlan**

- **add *vlan*** – 欲加入的 VLAN ID。
  - **remove *vlan*** – 欲刪除的 VLAN ID。
- 數字開頭不可以是 0。(範圍：1-4094)

#### 預設設定

拒絕清單中預設不含任何 VLAN。

#### 指令模式

Interface Configuration (Ethernet、Port Channel)

#### 指令使用方式

- 此指令可禁止某個 VLAN 透過 GVRP 自動加入指定介面。
- 若某個 VLAN 已經加入介面的允許 VLAN 清單內，就不可以再加入同一介面的拒絕清單。

## 範例

以下示範如何禁止 SNP1 連接埠加入 VLAN 3：

```
Console(config)#interface ethernet SNP1
Console(config-if)#switchport forbidden vlan add 3
Console(config-if)#
```

## 4.3.12.10 show vlan

此指令可顯示 VLAN 資訊。

### 語法

**show vlan** [*id vlan-id* | **name** *vlan-name*]

- **id** – VLAN ID 前面的關鍵字。
  - *vlan-id* – 欲設定之 VLAN 的 ID。(範圍：1-4094，數字前面請勿加上 0)
- **name** – VLAN 名稱之前的關鍵字。
  - *vlan-name* – ASCII 字串，長度從 1 到 15 個字元。

### 預設設定

顯示所有 VLAN。

### 指令模式

Normal Exec、Privileged Exec

### 範例

以下示範如何顯示 VLAN 的資訊：

```
Console#show vlan id 1
VLAN Type      Name                Status  Ports/Channel groups
-----
  1  Static      DefaultVlan        Active  SNP0   SNP1   SNP2   SNP3   SNP4
                                           SNP5   SNP6   SNP7   SNP8   SNP9
                                           SNP10  SNP11  SNP12  SNP13  SNP14
                                           SNP15  NETP0  NETP1  NETP2  NETP3
                                           NETP4  NETP5  NETP6  NETP7
  2  Static      MgtVlan            Active  NETMGT
Console#
```

## 4.3.13 GVRP 與橋接擴充功能指令

GVRP (GARP VLAN Registration Protocol, GARP VLAN 註冊通訊協定) 為交換器定義了一種彼此交換 VLAN 資訊的方式, 以便自動在網路其它地方的介面上註冊 VLAN 成員。本節將說明如何啓用整個交換器與各個介面的 GVRP, 並示範如何顯示 Bridge Extension (橋接器擴充功能) MIB 的預設組態設定。

指令	功能	模式	頁數
<i>介面指令</i>			
switchport gvrp	啓用介面的 GVRP	IC	4-114
switchport forbidden vlan	設定介面拒絕的 VLAN	IC	4-112
show gvrp configuration	顯示選定介面的 GVRP 組態	NE、PE	4-115
garp timer	設定選定功能的 GARP 計時器	IC	4-116
show garp timer	顯示選定功能的 GARP 計時器	NE、PE	4-117
<i>全區指令</i>			
bridge-ext gvrp	啓用整個交換器的 GVRP 功能	GC	4-118
show bridge-ext	顯示橋接器擴充功能組態	PE	4-119

### 4.3.13.1 switchport gvrp

此指令可啓用連接埠的 GVRP, 加上 **no** 則可停用此功能。

#### 語法

```
switchport gvrp  
no switchport gvrp
```

#### 預設設定

Enabled

#### 指令模式

Interface Configuration (Ethernet, Port Channel)

## 範例

```
Console(config)#interface ethernet SNP1
Console(config-if)#switchport gvrp
Console(config-if)#
```

### 4.3.13.2 show gvrp configuration

此指令可顯示 GVRP 功能已啓用或關閉。

#### 語法

**show gvrp configuration** [*interface*]

*interface*

- **ethernet** *port-name*

*port-name* – 下連連接埠：SNP0-15；上連連接埠：NETP0-7；管理連接埠：NETMGT

- **port-channel** *channel-id* (範圍：1-6)

#### 預設設定

整個交換器與各介面的組態都會顯示出來。

#### 指令模式

Normal Exec、Privileged Exec

## 範例

```
Console#show gvrp configuration
Whole system:
GVRP configuration: Enabled
SNP0:
  Gvrp configuration: Enabled
SNP1:
  Gvrp configuration: Enabled
.
.
.
```

### 4.3.13.3 garp timer

此指令可設定參加、離開與全部離開計時器的值，加上 **no** 則可將計時器恢復為預設值。

#### 語法

```
garp timer {join | leave | leaveall} timer_value  
no garp timer {join | leave | leaveall}
```

- {join | leave | leaveall} – 要設定的計時器。
- timer\_value – 計時器的值。  
範圍：
  - 參加：0.2-10 秒
  - 離開：0.60-30 秒
  - 全部離開：5-180 秒

#### 預設設定

- 參加：0.2 秒
- 離開：0.6 秒
- 全部離開：10 秒

#### 指令模式

Interface Configuration (Ethernet、Port Channel)

#### 指令使用方式

- GVRP 與 GMRP 使用 Group Address Registration Protocol (GARP，群組位址註冊通訊協定) 橋接 LAN 中的用戶端服務註冊或取消用戶端屬性。GARP 計時器的預設值與傳輸媒介的存取方法以及資料速路都沒有關係。除非 GMRP 或 GVRP 註冊/取消功能無法正常使用，否則請勿修改這些設定值。
- 計時器的值對所有 VLAN 上所有連接埠的 GVRP 都有效。
- 計時器的值必須符合以下規定：
  - 離開  $\geq$  (2 x 參加)
  - 全部離開 > 離開

---

**注意：**接在同一個網路上的所有第二層裝置都必須設定相同的 GVRP 計時器，否則 GVRP 將無法正常運作。

---

#### 範例

```
Console(config)#interface ethernet SNP1  
Console(config-if)#garp timer join 100  
Console(config-if)#
```



## 相關指令

show garp timer (4-117)

### 4.3.13.4 show garp timer

此指令可設定選定介面的 GARP 計時器。

#### 語法

**show garp timer** [*interface*]

*interface*

- **ethernet** *port-name*

*port-name* – 下連連接埠：SNP0-15；上連連接埠：NETP0-7；管理連接埠：NETMGT

- **port-channel** *channel-id* (範圍：1-6)

#### 預設設定

顯示所有 GARP 計時器。

#### 指令模式

Normal Exec、Privileged Exec

#### 範例

```
Console#show garp timer ethernet SNP1
SNP1 GARP timer status:
  Join timer: 20 sec.
  Leave timer: 60 sec.
  Leaveall timer: 1000 sec.
Console#
```

## 相關指令

garp timer (4-116)

### 4.3.13.5 bridge-ext gvrp

此指令可啓用整個交換器的 GVRP 功能，加上 **no** 則可停用此功能。

#### 語法

```
bridge-ext gvrp
no bridge-ext gvrp
```

#### 預設設定

Enabled

#### 指令模式

Global Configuration

#### 指令使用方式

GVRP 爲交換器定義了一種彼此交換 VLAN 資訊的方式，以便在網路其它地方的連接埠上註冊 VLAN 成員。此功能必須先啓動，自動 VLAN 註冊功能才會運作，而且也才能支援交換器本身以外的 VLAN。

#### 範例

```
Console(config)#bridge-ext gvrp
Console(config)#
```

### 4.3.13.6 show bridge-ext

此指令可顯示橋接器擴充功能指令的組態。

#### 預設設定

無

#### 指令模式

Privileged Exec

#### 指令使用方式

此指令所顯示各項目的意義如下：

- **Max support vlan numbers** – 此交換器使用之 IEEE 802.1Q 標準中的 VLAN 版本。
- **Max support vlan ID** – 此交換器認得之最大 VLAN ID。
- **Extended multicast filtering services** – 此交換器沒有依據 GMRP (GARP Multicast Registration Protocol, GARP 群組廣播註冊通訊協定) 過濾個別群組位址的功能。
- **Static entry individual port** – 此交換器可過濾一對一連線與群組廣播的位址 (參閱第 4-86 頁與第 4-122 頁)。
- **VLAN learning** – 此交換器使用 IVL (Independent VLAN Learning, 獨立 VLAN 學習), 每個連接埠都有自己的過濾資料庫。
- **Configurable PVID tagging** – 此交換器可讓您修改每個連接埠的預設連接埠 VLAN ID (封包標記中使用的 PVID) 與輸出狀態 (有加註標記或未加註標記的 VLAN) (參閱第 4-110 頁)。
- **Local VLAN capable** – 指交換器提更的多重 Spanning Tree 功能, 目前此交換器尚未支援多重 Spanning Tree。
- **Traffic classes** – 此交換器提供將使用者優先等級對應到流量類別的功能 (參閱第 4-134 頁)。
- **Global GVRP status** – GARP VLAN Registration Protocol (GARP VLAN 註冊通訊協定, GVRP) 為交換器定義了一種彼此交換 VLAN 資訊的方式, 以便在網路其它地方的連接埠上註冊需要的 VLAN 成員。若要讓 VLAN 群組涵蓋範圍擴大到此交換器以外的地方, 就必須啓用這項功能 (參閱第 4-118 頁)。
- **GMRP** – GARP Multicast Registration Protocol (GARP 群組廣播註冊通訊協定, GMRP) 可讓網路裝置向廣播群組註冊終端站台。此交換器雖不支援 GMRP, 但可用 Internet Group Management Protocol (網際網路群組管理通訊協定, IGMP) 提供自動群組廣播過濾功能。

## 範例

```
Console#show bridge-ext
Max support vlan numbers: 255
Max support vlan ID: 4094
Extended multicast filtering services: No
Static entry individual port: Yes
VLAN learning: IVL
Configurable PVID tagging: Yes
Local VLAN capable: Yes
Traffic classes: Enabled
Global GVRP status: Enabled
GMRP: Disabled
Console#
```

### 4.3.14 IGMP Snooping 指令

本交換器使用 IGMP (Internet Group Management Protocol，網際網路群組管理通訊協定) 詢問其所連接且要接收特定群組廣播服務的所有主機。交換器會找出要求服務之主機所連的连接埠，然後就只會將相關資料傳到這些连接埠而已。此外，交換器還會將服務要求傳送給相連的群組廣播交換器/路由器，確保本身也會繼續收到群組廣播服務。

指令	功能	模式	頁數
<i>基本 IGMP 指令</i>			
ip igmp snooping	啓用 IGMP snooping	GC	4-121
ip igmp snooping vlan static	將介面加入廣播群組中成爲其成員之一	GC	4-122
ip igmp snooping version	設定 IGMP 版本以便進行窺探	GC	4-122
show ip igmp snooping	顯示 IGMP snooping 組態	PE	4-123
show bridge multicast	顯示 IGMP snooping MAC 群組廣播清單	PE	4-124
<i>IGMP 查詢者指令</i>			
ip igmp snooping querier	讓此裝置擔任 IGMP snooping 的查詢者角色	GC	4-124
ip igmp snooping query-count	設定查詢次數	GC	4-125
ip igmp snooping query-interval	設定查詢間隔時間	GC	4-126

指令	功能	模式	頁數
ip igmp snooping query-max-response-time	設定回報延遲時間	GC	4-127
ip igmp snooping router-port-expire-time	設定查詢逾時時間	GC	4-128
show ip igmp snooping <i>群組廣播路由器指令</i>	顯示 IGMP snooping 組態	PE	4-123
ip igmp snooping vlan mrouter	新增一個群組廣播路由器連接埠	GC	4-129
show ip igmp snooping mrouter	顯示群組廣播路由器連接埠	PE	4-130

### 4.3.14.1 ip igmp snooping

此指令可啓用交換器上的 IGMP snooping 功能，加上 **no** 則可停用此功能。

#### 語法

```
ip igmp snooping  
no ip igmp snooping
```

#### 預設設定

Disabled

#### 指令模式

Global Configuration

#### 範例

以下示範如何啓用 IGMP snooping 功能。

```
Console(config)#ip igmp snooping  
Console(config)#
```

## 4.3.14.2 ip igmp snooping vlan static

此指令可將連接埠加入廣播群組中，加上 **no** 則可將連接埠從廣播群組中刪除。

### 語法

```
ip igmp snooping vlan vlan-id static ip-address interface  
no ip igmp snooping vlan vlan-id static ip-address interface
```

- *vlan-id* – VLAN ID (範圍：1-4094)
- *ip-address* – 廣播群組的 IP 位址
- *interface*
  - **ethernet** *port-name*  
*port-name* – 下連接埠：SNP0-15；上連接埠：NETP0-7；管理連接埠：NETMGT
  - **port-channel** *channel-id* (範圍：1-6)

### 預設設定

無

### 指令模式

Global Configuration

### 範例

以下示範如何在連接埠上靜態設定廣播群組：

```
Console(config)#ip igmp snooping vlan 1 static 224.0.0.12  
ethernet SNP5  
Console(config)#
```

## 4.3.14.3 ip igmp snooping version

此指令可設定 IGMP snooping 版本，加上 **no** 則可恢復為預設值。

### 語法

```
ip igmp snooping version {1 | 2}  
no ip igmp snooping version
```

- 1 – IGMP 版本 1
- 2 – IGMP 版本 2

### 預設設定

IGMP 版本 2

### 指令模式

Global Configuration

### 指令使用方式

- 子網路上的所有系統都必須採用相同的版本。若網路上還有只支援版本 1 的老舊裝置，交換器就必須設定成使用版本 1。
- 某些指令只有在 IGMPv2 才能使用，包括 `ip igmp query-max-response-time` 與 `ip igmp query-timeout`。

### 範例

以下示範如何將交換器設定成使用 IGMP 版本 1：

```
Console(config)#ip igmp snooping version 1
Console(config)#
```

## 4.3.14.4 show ip igmp snooping

此指令可顯示 IGMP snooping 組態設定。

### 預設設定

無

### 指令模式

Privileged Exec

### 指令使用方式

關於此指令所顯示各項目的說明，請參閱第 3-44 頁的「設定 IGMP Snooping 參數」。

### 範例

以下示範如何顯示目前的 IGMP snooping 組態：

```
Console#show ip igmp snooping
Service status: Enabled
Querier status: Enabled
Query count: 2
Query interval: 125 sec
Query max response time: 10 sec
Query time-out: 300 sec
IGMP snooping version: Version 2
Console#
```

### 4.3.14.5 show mac-address-table multicast

此指令可將已知的群組廣播位置顯示出來。

#### 語法

**show mac-address-table multicast** [vlan *vlan-id*] [**user** | **igmp-snooping**]

- *vlan-id* – VLAN ID (1 到 4094)
- **user** – 只顯示使用者設定的群組廣播項目。
- **igmp-snooping** – 只顯示透過 IGMP snooping 學習到的項目。

#### 預設設定

無

#### 指令模式

Privileged Exec

#### 指令使用方式

此指令顯示的成員類別有 IGMP 和 USER 兩種，視選定何種選項而定。

#### 範例

以下示範橋接群組 1 VLAN 1 透過 IGMP snooping 所學習到的群組廣播項目：

```
Console#show mac-address-table multicast vlan 1 igmp-snooping
VLAN M'cast IP addr.Member ports Type
-----
      1      224.0.0.12      NETP0      USER
      1      224.1.1.2.3      NETP1      IGMP
Console#
```

### 4.3.14.6 ip igmp snooping querier

此指令可將交換器設定擔任 IGMP snooping 查詢者的角色，加上 **no** 則可停用此功能。

#### 語法

**ip igmp snooping querier**  
**no ip igmp snooping querier**

#### 預設設定

Disabled

#### 指令模式

Global Configuration



## 指令使用方式

此功能啟用後，交換器便可以被推舉出來擔任查詢者的角色。查詢者需負責詢問各主機是否想要接收群組廣播流量。

## 範例

```
Console(config)#ip igmp snooping querier
Console(config)#
```

### 4.3.14.7 ip igmp snooping query-count

此指令可設定查詢個數，加上 **no** 則可恢復為預設值。

## 語法

```
ip igmp snooping query-count count
no ip igmp snooping query-count
```

*count* – 查詢者應該連續發出多少個查詢，且該用戶端都沒有回應的狀況下，才決定將該用戶端從廣播群組中去除。(範圍：2-10)

## 預設設定

2 times

## 指令模式

Global Configuration

## 指令使用方式

查詢次數定義了查詢者應該等待群組廣播用戶端多久都沒有回應之後，才可以採取行動。當查詢者發出的查詢到達此指令規定的次數時，用戶端仍然一直沒有回應，查詢者便會從 **ip igmp snooping query-max-response-time** 定義的時間開始倒數。若數到零時用戶端仍然沒有任何回應，便將該用戶端視為已經離開此廣播群組。

## 範例

以下示範如何將查詢次數設定為 10：

```
Console(config)#ip igmp snooping query-count 10
Console(config)#
```

## 相關指令

ip igmp snooping query-max-response-time (4-127)

### 4.3.14.8 ip igmp snooping query-interval

此指令可設定窺探查詢間隔時間，加上 **no** 則可恢復為預設值。

#### 語法

**ip igmp snooping query-interval** *seconds*  
**no ip igmp snooping query-interval**

*seconds* – 交換器發出 IGMP 主機詢問訊息的頻率。(範圍：60-125)

#### 預設設定

125 秒

#### 指令模式

Global Configuration

#### 範例

以下示範如何將查詢間隔時間設定為 100 秒：

```
Console(config)#ip igmp snooping query-interval 100
Console(config)#
```

### 4.3.14.9 ip igmp snooping query-max-response-time

此指令可設定窺探回報延遲時間，加上 **no** 則可恢復為預設值。

#### 語法

```
ip igmp snooping query-max-response-time seconds  
no ip igmp snooping query-max-response-time
```

*seconds* – IGMP 查詢中宣告的回報延遲時間。(範圍：5-25)

#### 預設設定

10 秒

#### 指令模式

Global Configuration

#### 指令使用方式

- 交換器必須使用 IGMPv2，此指令才會有效。
- 當查詢者發出查詢後，會等待群組廣播用戶端傳回的回應，等待的時間便由此指令定義。當查詢者發出的查詢達到 **ip igmp snooping query-count** 設定的次數時，若用戶端沒有任何回應，查詢者便會從此指令設定的值開始往下倒數。若數到零時用戶端仍然沒有任何回應，便將該用戶端視為已經離開此廣播群組。

#### 範例

以下示範如何將最長回應時間設定為 20 秒：

```
Console(config)#ip igmp snooping query-max-response-time 20  
Console(config)#
```

#### 相關指令

```
ip igmp snooping version (4-122)  
ip igmp snooping query-max-response-time (4-127)
```

## 4.3.14.10 ip igmp snooping router-port-expire-time

此指令可設定窺探查詢逾時時間，加上 **no** 則可恢復為預設值。

### 語法

**ip igmp snooping router-port-expire-time** *seconds*  
**no ip igmp snooping router-port-expire-time**

*seconds* – 從最近一次查詢者停止發送詢問訊息之後，交換器應該等待多少時間，才可以判定先前都持續收到查詢者發出之詢問封包的介面已經失去與查詢者的連線了。(範圍：300-500)

### 預設設定

300 秒

### 指令模式

Global Configuration

### 指令使用方式

交換器必須使用 IGMPv2，此指令才會有效。

### 範例

以下示範如何將逾時時間設定為 500 秒：

```
Console(config)#ip igmp snooping router-port-expire-time 500
Console(config)#
```

### 相關指令

ip igmp snooping version (4-122)

## 4.3.14.11 ip igmp snooping vlan mrouter

此指令可靜態設定群組廣播路由器通訊埠，加上 **no** 則可將組態刪除。

### 語法

```
ip igmp snooping vlan vlan-id mrouter interface  
no ip igmp snooping vlan vlan-id mrouter interface
```

- *vlan-id* – VLAN ID (範圍：1-4094)
- *interface*
  - **ethernet** *port-name*  
*port-name* – 下連連接埠：SNP0-15；上連連接埠：NETP0-7；管理連接埠：NETMGT
  - **port-channel** *channel-id* (範圍：1-6)

### 預設設定

不設定任何靜態群組廣播路由器連接埠。

### 指令模式

Global Configuration

### 指令使用方式

由於網路連線的變化很大，因此 IGMP 窺探方式不見得能夠找出 IGMP 查詢者。因此若事先就知道 IGMP 查詢者是網路上哪一台群組廣播路由器/交換器，而且知道連在交換器的哪個介面 (連接埠或寬道) 上，就可以手動將此介面設定成加入目前所有廣播群組。

### 範例

以下示範如何將第 11 個連接埠設定為 VLAN 1 中的群組廣播路由器連接埠：

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet NETP0  
Console(config)#
```

## 4.3.14.12 show ip igmp snooping mrouter

此指令可顯示靜態設定與動態習得之群組廣播路由器連接埠的資訊。

### 語法

```
show ip igmp snooping mrouter [vlan vlan-id]
```

*vlan-id* – VLAN ID (範圍：1-4094)

### 預設設定

顯示所有已設定 VLAN 的群組廣播路由器連接埠。

### 指令模式

Privileged Exec

### 指令使用方式

此指令顯示的群組廣播路由器連接不種類包括 Static (靜態) 與 Dynamic (動態) 兩種。

### 範例

以下示範如何顯示與群組廣播路由器連接的連接埠：

```
Console#show ip igmp snooping mrouter
VLAN M'cast Router Ports Type
-----
    1                NETP5  Static
    2                NETP6  Dynamic
Console#
```

## 4.3.15 優先等級指令

本節說明的指令可用來指定流量由於網路壅塞而堵在交換器上時，哪些資料封包具有比較高的優先權。本交換器的每個連接埠都有四個優先等級佇列，提供 CoS 功能。位於連接埠較高優先等級佇列中的資料封包會先傳送，然後才輪到較低優先等級佇列中的封包傳送。您可以設定每個介面的預設優先等級、各佇列的相對權重以及將封包優先等級標籤對應到交換器的優先等級佇列。

指令	功能	模式	頁數
<i>第 2 層優先等級指令</i>			
switchport priority default	設定流入之未加註標籤封包的連接埠優先等級	IC	4-132
queue bandwidth	設定優先等級佇列的巡迴權重	GC	4-133
queue cos map	設定優先等級佇列的服務類別	IC	4-134
show queue bandwidth	顯示優先等級佇列所設定的巡迴權重	PE	4-135
show queue cos-map	顯示服務類別對應表	PE	4-136
show interfaces switchport	顯示介面的管理與運作狀態	PE	4-84
<i>第 3 層和第 4 層優先等級指令</i>			
map ip precedence	啓用 IP 優先權服務類別對應功能	GC	4-136
map ip precedence	將 IP 優先權值對應到服務類別	IC	4-137
map ip dscp	啓用 IP DSCP 服務類別對應功能	GC	4-138
map ip dscp	將 IP DSCP 值對應到服務類別	IC	4-139
show map ip precedence	顯示 IP 優先權對應	PE	4-140
show map ip dscp	顯示 IP DSCP 對應圖	PE	4-141

## 4.3.15.1 switchport priority default

此指令可設定流入且未加註標籤之封包的優先等級，或接在特定介面之裝置所接收之封包的優先等級，加上 **no** 則可恢復為預設值。

### 語法

**switchport priority default** *default-priority-id*  
**no switchport priority default**

*default-priority-id* – 未加註標籤之流入流量的優先等級編號。  
此優先等級由 0-7 的數字代表，7 為最高等級。

### 預設設定

未設定任何優先等級，且此介面所接收未加註標籤之封包的預設值為 0。

### 指令模式

Interface Configuration (Ethernet, Port Channel)

### 指令使用方式

- 優先等級對應以 IP 優先權或 IP DSCP 當作優先權，接著才是預設 switchport 優先等級。
- 當設定成接收所有類型封包（無論封包有無加註標籤均會接收進來）的連接埠收到未加註任何標籤的封包時，便會將此預設優先等級加註在此封包上。不過這項等級設定並不會加在 IEEE 802.1Q VLAN 已加註標籤的封包上。若收到的是 IEEE 802.1Q VLAN 已加註標籤的封包，則會使用 IEEE 802.1p 使用者優先等級 (User Priority) 位元。
- 本交換器的每個連接埠都有四個優先等級佇列，均設定成使用巡迴式權重法，可以 **queue bandwidth** 指令將其顯示出來。流入且未加註 VLAN 標籤的封包，會被加上輸入連接埠的預設輸入使用者優先等級，並放到輸出連接埠的適當優先等級佇列中。所有輸入連接埠的預設優先等級均為 0，因此任何沒有優先等級標籤的輸入封包都會被放在輸出連接埠編號 0 的佇列中。（請注意，若輸出連接埠設定成其所屬 VLAN 中不會加註標籤的成員，則這些封包上的 VLAN 標籤便會先全部刪掉，然後才會傳送出去。）

### 範例

以下示範如何設定 SNP3 到 SNP5 各連接埠的預設優先等級：

```
Console(config)#interface ethernet SNP3  
Console(config-if)#switchport priority default 5
```



## 4.3.15.2 queue bandwidth

此指令可設定四個服務類別 (CoS) 優先等級佇列的巡迴權重，加上 **no** 則可恢復為預設權重。

### 語法

```
queue bandwidth weight1...weight4  
no queue bandwidth
```

*weight1...weight4* – WRR 排程程式採用的權重取決於佇列 0 - 3 的權重比例。(範圍：1-255)

### 預設設定

佇列 0、1、2 與 3 的預設權重分別為 16、64、128 與 240。

### 指令模式

Global Configuration

### 指令使用方式

WRR 會定義排程權重，以便在輸出連接埠上共享頻寬。

### 範例

以下示範如何將 WRR 權重 1、3、5 與 7 設定給 CoS 優先等級佇列 0、1、2 與 3。

```
Console(config)#queue bandwidth 1 3 5 7  
Console(config)#
```

### 相關指令

show queue bandwidth (4-135)

### 4.3.15.3 queue cos-map

此指令可將服務類別 (CoS, class-of-service) 值指派給 CoS 優先等級佇列，加上 **no** 則可將 CoS 對應恢復為預設值。

#### 語法

**queue cos-map** *queue\_id* [*cos1* ... *cosn*]

**no queue cos-map**

- *queue\_id* – CoS 優先等級佇列的佇列 id。  
範圍從 0 到 3，其中 3 為最高等級的 CoS 佇列。
- *cos1* .. *cosn* – 對應到佇列 id 的 CoS 值，各數值之間以空格分開。CoS 值由 0-7 的數字代表，7 為最高等級。

#### 預設設定

此交換器的每個連接埠都有四個優先等級佇列，採用巡迴式權重方式運作，藉以提供服務類別 (Class of Service) 功能。IEEE 802.1p 定義了 8 個流量類別。預設優先等級是根據 IEEE 802.1p 標準所建議的方式設定，如下表所示。

	佇列			
	0	1	2	3
優先等級		0		
	1			
	2			
		3		
			4	
			5	
				6
				7

#### 指令模式

Interface Configuration (Ethernet, Port Channel)

#### 指令使用方式

交換器根據輸入連接埠設定的 CoS 值挑選輸出連接埠的 CoS 優先等級。

## 範例

以下示範如何將 CoS 的值 0、1 與 2 對應到 CoS 優先等級佇列 0，將 3 對應到 CoS 優先等級佇列 1，將 4 和 5 對應到 CoS 優先等級佇列 2，以及將 6 和 7 對應到 CoS 優先等級佇列 3：

```
Console(config)#interface ethernet SNP1
Console(config-if)#queue cos-map 0 0 1 2
Console(config-if)#queue cos-map 1 3
Console(config-if)#queue cos-map 2 4 5
Console(config-if)#queue cos-map 3 6 7
Console(config-if)#
```

## 相關指令

show queue cos-map (4-136)

### 4.3.15.4 show queue bandwidth

此指令可顯示四個服務類別 (CoS) 優先等級佇列的巡迴式權重頻寬分配情形。

## 預設設定

無

## 指令模式

Privileged Exec

## 範例

```
Console#show queue bandwidth
Queue ID Weight
-----
      0      16
      1      64
      2     128
      3     240
Console#
```

### 4.3.15.5 show queue cos-map

此指令可顯示服務類別優先等級對應表。

#### 語法

**show queue cos-map** [*interface*]

*interface*

- **ethernet** *port-name*

*port-name* – 下連連接埠：SNP0-15；上連連接埠：NETP0-7；管理連接埠：NETMGT

- **port-channel** *channel-id* (範圍：1-6)

#### 預設設定

無

#### 指令模式

Privileged Exec

#### 範例

```
Console#show queue cos-map ethernet SNP11
Information of SNP11
Queue ID Traffic class
-----
0      1 2
1      0 3
2      4 5
3      6 7
Console#
```

### 4.3.15.6 map ip precedence (Global Configuration)

此指令可啓用 IP 優先權對應 (即 IP Type of Service, IP 服務種類), 加上 **no** 則可停用 IP 優先權的對應功能。

#### 語法

**map ip precedence**

**no map ip precedence**

#### 預設設定

Enabled

#### 指令模式

Global Configuration

### 指令使用方式

- 優先等級對應以 IP 優先權或 IP DSCP 當作優先權，接著才是預設 switcport 優先等級。
- IP 優先權與 IP DSCP 兩者不可同時啓用，啓用其中一個之後，另一個就會自動停用。

### 範例

以下示範如何啓用整個交換器的 IP 優先權對應功能：

```
Console(config)#map ip precedence
Console(config)#
```

## 4.3.15.7 map ip precedence (Interface Configuration)

此指令可設定 IP 優先權等級（即 IP Type of Service，IP 服務種類優先等級），加上 **no** 則可恢復為預設表。

### 語法

```
map ip precedence ip-precedence-value cos cos-value  
no map ip precedence
```

- *precedence-value* – 3 個位元的優先權值。（範圍：0-7）
- *cos-value* – 服務類別值（範圍：0-7）

### 預設設定

一對一對應（即優先權值 0 對應到 CoS 值 0，依此類推）

### 指令模式

Interface Configuration (Ethernet, Port Channel)

### 指令使用方式

- 優先等級對應以 IP 優先權或 IP DSCP 當作優先權，接著才是預設 switcport 優先等級。
- IP 優先權值會根據 IEEE 802.1p 標準的建議，以一對一的方式對應到預設服務類別值，然後再對應到佇列的預設值。
- IP 優先權特定值的對應雖然是作成一個介面組態設定指令，但任何更動對於交換器上的所有介面都有效。

## 範例

以下示範如何將 IP 優先權值 1 對應到 CoS 值 0：

```
Console(config)#interface ethernet SNP5
Console(config-if)#map ip precedence 1 cos 0
Console(config-if)#
```

### 4.3.15.8 map ip dscp (Global Configuration)

此指令可啟用 IP DSCP 對應功能 (即 Differentiated Services Code Point 差異式服務代碼點對應)，加上 **no** 則可停用 IP DSCP 對應功能。

#### 語法

```
map ip dscp
no map ip dscp
```

#### 預設設定

Enabled

#### 指令模式

Global Configuration

#### 指令使用方式

- 優先等級對應以 IP 優先權或 IP DSCP 當作優先權，接著才是預設 switchport 優先等級。
- IP 優先權與 IP DSCP 兩者不可同時啟用，啟用其中一個之後，另一個就會自動停用。

## 範例

以下示範如何啟用整個交換器的 IP DSCP 對應功能：

```
Console(config)#map ip dscp
Console(config)#
```

### 4.3.15.9 map ip dscp (Interface Configuration)

此指令可設定 IP DSCP 優先等級 (即 Differentiated Services Code Point 差異式服務代碼點優先等級)，加上 **no** 則可恢復為預設表。

#### 語法

**map ip dscp** *dscp-value* **cos** *cos-value*

**no map ip dscp**

- *dscp-value* – 8 個位元的 DSCP 值 (範圍：0-255)
- *cos-value* – 服務類別值 (範圍：0-7)

#### 預設設定

DSCP 的預設值定義如下表所示。請注意，未定義的所有 DSCP 設定值都會對應成 CoS 值 0。

IP DSCP 值	CoS 值
0	0
8	1
10, 12, 14, 16	2
18, 20, 22, 24	3
26, 28, 30, 32, 34, 36	4
38, 40, 42	5
48	6
46, 56	7

#### 指令模式

Interface Configuration (Ethernet, Port Channel)

#### 指令使用方式

- 優先等級對應以 IP 優先權或 IP DSCP 當作優先權，接著才是預設 switcpport 優先等級。
- DSCP 優先等級值會根據 IEEE 802.1p 標準的建議對應到預設服務類別值，然後再對應到佇列的預設值。
- DSCP 特定值的對應雖然是作成一個介面組態設定指令，但任何更動對於交換器上的所有介面都有效。

## 範例

以下示範如何將 IP DSCP 值 1 對應到 CoS 值 0：

```
Console(config)#interface ethernet SNP5
Console(config-if)#map ip dscp 1 cos 0
Console(config-if)#
```

### 4.3.15.10 show map ip precedence

此指令可顯示 IP 優先權優先等級對應表。

#### 語法

**show map ip precedence** [*interface*]

*interface*

- **ethernet** *port-name*

*port-name* – 下連連接埠：SNP0-15；上連連接埠：NETP0-7；管理連接埠：NETMGT

- **port-channel** *channel-id* (範圍：1-6)

#### 預設設定

無

#### 指令模式

Privileged Exec

## 範例

```
Console#show map ip precedence ethernet SNP5
Precedence mapping status: disabled

Port          Precedence COS
-----
SNP5          0    0
SNP5          1    1
SNP5          2    2
SNP5          3    3
SNP5          4    4
SNP5          5    5
SNP5          6    6
SNP5          7    7
Console#
```



## 相關指令

- map ip precedence (Global Configuration) (4-136)
- map ip precedence (Interface Configuration) (4-137)

### 4.3.15.11 show map ip dscp

此指令可顯示 IP DSCP 優先等級對應表。

#### 語法

```
show map ip dscp [interface]
```

*interface*

- **ethernet** *port-name*

*port-name* – 下連連接埠：SNP0-15；上連連接埠：NETP0-7；管理連接埠：NETMGT

- **port-channel** *channel-id* (範圍：1-6)

#### 預設設定

無

#### 指令模式

Privileged Exec

#### 範例

```
Console#show map ip dscp ethernet SNP1
DSCP mapping status: disabled

Port          DSCP  COS
-----
              SNP1   0    0
              SNP1   1    0
              SNP1   2    0
              SNP1   3    0
              :
              :
              SNP1  61    0
              SNP1  62    0
              SNP1  63    0
Console#
```

## 相關指令

- map ip dscp (Global Configuration) (4-138)
- map ip dscp (Interface Configuration) (4-139)

## 4.3.16 鏡射連接埠指令

本節說明如何透過鏡射功能將一個連接埠（來源連接埠）的流量複製到另一個連接埠（目的連接埠）上。

指令	功能	模式	頁數
port monitor	設定鏡射作業	IC	4-142
show port monitor	顯示鏡射連接埠的組態	PE	4-143

### 4.3.16.1 port monitor

此指令可設定鏡射作業，加上 **no** 則可停止鏡射。

**注意：**Sun Fire B1600 Blade 系統機箱內整合的交換器，每一個都含有一對相互連接的交換器晶片。任何一個通訊埠上的流量，只能複製到位於同一交換器晶片上的其它通訊埠。連接埠 NETP0 到 NETP3 以及 SNP0 到 SNP7 位於同一顆交換器晶片上，連接埠 NETP4 到 NETP7 以及 SNP8 到 SNP15 則位於另一顆上。

#### 語法

```
port monitor interface [rx | tx | both]
no port monitor interface
```

- **interface** – ethernet *port-name*  
*port-name* – 下連接埠：SNP0-15；上連接埠：NETP0-7；管理連接埠：NETMGT  
（此介面定義的是來源連接埠。）
- **rx** – 複製收到的封包。
- **tx** – 複製發送出去的封包。
- **both** – 複製收到與發送出去的封包。

#### 預設設定

預設並未定義任何鏡射作業。啓用鏡射功能後，預設的鏡射方式會將收到與發送出去的封包兩種全部複製到目的連接埠上。

#### 指令模式

Interface Configuration (Ethernet, destination port)

#### 指令使用方式

- 您可以將一個通訊埠的流量鏡射複製一份到另一個通訊埠（目的通訊埠）上，以便進行即時分析。然後在後者接上一台邏輯分析儀或 RMON 探測器，在完全不妨礙原來的流量狀況下，仔細觀察流過此通訊埠的資料。
- 設定目的通訊埠時，應指定一個乙太網路介面當作目的通訊埠。

## 範例

以下示範如何將 SNMP 連接埠的所有封包複製到 NETP2 連接埠上：

```
Console(config)#interface ethernet NETP2
Console(config-if)#port monitor ethernet SNMP6 both
Console(config-if)#
```

## 相關指令

show port monitor (4-143)

### 4.3.16.2 show port monitor

此指令會顯示鏡射相關資訊。

#### 語法

**show port monitor** [*interface*]

*interface* – **ethernet** *port-name*

*port-name* – 下連連接埠：SNP0-15；上連連接埠：NETP0-7；管理連接埠：NETMGT

(此介面定義的是來源連接埠。)

#### 預設設定

顯示所有鏡射作業

#### 指令模式

Privileged Exec

#### 指令使用方式

此指令會顯示目前設定的來源連接埠、目的連接埠與鏡射模式 (即 RX、TX、RX/TX)。

## 範例

以下顯示將連接埠 SNP6 流量複製到連接埠 NETP2 的鏡射組態：

```
Console(config)#interface ethernet NETP2
Console(config-if)#port monitor ethernet SNP6
Console(config-if)#end
Console#show port monitor
Port Mirroring
-----
Destination port(listen port): NETP2
Source port(monitored port)  : SNP6
Mode                          : RX/TX
Console#
```

## 相關指令

port monitor (4-142)

## 4.3.17 連接埠寬道指令

連接埠可以靜態組成一個集束線路（也就是寬道），提昇網路連線頻寬與確保遇到故障時能迅速復原。或者也可以用 Link Aggregation Control Protocol (LACP，線路集束控制通訊協定)，讓此交換器與另一個網路裝置自動協商出一條寬道線路。採用靜態寬道時，雙方交換器必須屬於同一種類型。但如果使用動態寬道，交換器只要符合 LACP 的規定即可。此交換器最多可提供六條寬道。例如由兩個 1000 Mbps 連接埠組成的寬道，以全雙工模式運作時，就可以提供 4 Gbps 的總頻寬。

指令	功能	模式	頁數
<i>手動組態指令</i>			
interface port-channel	設定一條寬道，並進入此寬道的介面組態設定模式	GC	4-74
channel-group	將一個連接埠加入寬道內	IC	4-145
<i>動態組態指令</i>			
lACP	設定目前介面的 LACP	IC	4-146
<i>寬道狀態顯示指令</i>			
show interfaces status port-channel	顯示寬道資訊	NE, PE	4-81

## 建立寬道的建議方式

- 先將連接埠寬道設定好，然後才用網路線將交換器連接起來，以免造成網路中出現迴路。
- 一條寬道最多可以含有四個上連連接埠或最多兩個下連連接埠。
- 線路兩端的連接埠都必須設定成寬道連接埠。
- 寬道所含的全部連接埠都必須以相同方式設定，包括通訊模式（即速度、雙工模式與流量控制）、VLAN 隸屬關係與 CoS 設定等等。
- 透過指定 `port-channel` 從 VLAN 中移出、移入 VLAN、加入 VLAN 內、從 VLAN 內刪除時，寬道中所有連接埠都必須視為一體一起設定。
- STP、VLAN 與 IGMP 都只能透過指定 `port-channel` 在整個寬道上進行設定。

### 4.3.17.1 channel-group

此指令可將連接埠加入靜態寬道內，加上 `no` 則可將連接埠從寬道中刪除。

#### 語法

```
channel-group channel-id  
no channel-group
```

*channel-id* – 寬道索引（範圍：1-6）

#### 預設設定

目前通訊埠會加入此寬道內。

#### 指令模式

Interface Configuration (Ethernet)

#### 指令使用方式

- 設定靜態寬道時，只有相同類型的交換器才可以連起來。
- `no channel-group` 可將一個連接埠群組從寬道中刪除。
- `no interfaces port-channel` 可將寬道從交換器中刪除。

#### 範例

以下示範如何建立寬道 1，然後再將 NETP2 連接埠加進這個寬道內：

```
Console(config)#interface port-channel 1  
Console(config-if)#exit  
Console(config)#interface ethernet NETP2  
Console(config-if)#channel-group 1  
Console(config-if)#
```

## 4.3.17.2 lacp

此指令可啓用目前介面的 802.3ad Link Aggregation Control Protocol (LACP，線路集束控制通訊協定) 功能，加上 **no** 則可停用此功能。

### 語法

```
lacp
no lacp
```

### 預設設定

啓用

### 指令模式

Interface Configuration (Ethernet)

### 指令使用方式

- LACP 通道兩端的連接埠無論用強迫設定或自動協商的方式，都必須都設定成全雙工模式。
- 用 LACP 與另一個交換器建立的寬道，會自動被設定為下一個可用的 port-channel id。
- 若目的交換器在互連的連接埠上也啓用 LACP，則寬道便會自動啓動。
- 若同一個目的交換器所連接的連接埠有四個以上啓用 LACP，則多餘的連接埠便會被設定成備用模式，只有在任何一條使用中線路故障時才會啓用。

## 範例

以下顯示 NETP0-2 連接埠都啓用了 LACP 功能。由於線路另一端的連接埠上也啓用了 LACP，**show interfaces status port-channel 1** 指令便顯示寬道 1 已經建立起來了。

```
Console(config)#interface ethernet NETP0
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#interface ethernet NETP1
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#interface ethernet NETP2
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#exit
Console#show interfaces status port-channel 1
Information of Trunk 1
Basic information:
  Port type: 1000t
  Mac address: 00-00-e8-00-00-0b
Configuration:
  Name:
  Port admin status: Up
  Speed-duplex: Auto
  Capabilities: 10half, 10full, 100half, 100full, 1000full
  Flow control status: Disabled
Current status:
  Created by: lacp
  Link status: Up
  Operation speed-duplex: 1000full
  Flow control type: None
  Member Ports: NETP0, NETP1, NETP2,
Console#
```





## 第 III 部分 附錄

---

本節將更詳細說明以下主題。

管理資訊庫

疑難排解

規格



# 管理資訊庫

---

透過設定或讀取 MIB (Management Information Base, 管理資訊庫) 規定的裝置變數, SNMP 管理主機便能設定與監視網路裝置。本附錄列出此型交換器支援的主要 MIB 群組, 此外, 各項組態設定程序所使用的特殊 MIB 變數則列在第 3 章的「管理概述」中。

---

## A.1 支援的 MIB

下表列出幾個標準的 MIB。

RFC 編號	書名	支援的群組
1213	MIB-II	<ul style="list-style-type: none"><li>• system 群組</li><li>• interfaces 群組</li><li>• ip 群組</li><li>• icmp 群組</li><li>• tcp 群組</li><li>• udp 群組</li><li>• snmp 群組</li></ul>
1493	Bridge MIB	<ul style="list-style-type: none"><li>• dot1dBase 群組</li><li>• dot1dStp 群組</li><li>• dot1dTp 群組</li><li>• dot1dStatic 群組</li></ul>
2863	Interfaces Evolution MIB	<ul style="list-style-type: none"><li>• ifXTable 群組</li><li>• ifStackTable 群組</li></ul>

RFC 編號	書名	支援的群組
2819	RMON MIB	<ul style="list-style-type: none"> <li>• statistics 群組</li> <li>• history 群組</li> <li>• alarm 群組</li> <li>• event 群組</li> </ul>
2618	RADIUS MIB	<ul style="list-style-type: none"> <li>• radiusAuthClientMIB</li> </ul>
2665	Etherlike MIB	<ul style="list-style-type: none"> <li>• dot3StatsTable 群組</li> </ul>
2737	Entity 群組	<ul style="list-style-type: none"> <li>• entityPhysical 群組</li> </ul>
2674	P-bridge	<ul style="list-style-type: none"> <li>• dot1dExtBase 群組</li> <li>• dot1dPriority 群組</li> <li>• dot1dGarp 群組</li> </ul>
2674	Q-bridge	<ul style="list-style-type: none"> <li>• dot1qBase 群組</li> <li>• dot1qTp 群組</li> <li>• dot1qStatic 群組</li> <li>• dot1qVlan</li> </ul>

以下則是 Sun 本身的企業 MIB。

書名	版本
CSSP.MIB	01.00.00

---

## A.2 支援的 Trap

此型交換器支援的各種 SNMP trap 如下：

---

RFC 編號	書名
RFC 1215 (SNMPv1),	<ul style="list-style-type: none"><li>• coldStart</li><li>• linkDown</li></ul>
RFC 1907 (SNMPv2c)	<ul style="list-style-type: none"><li>• linkUp</li><li>• authenticationFailure</li></ul>
RFC 1493	<ul style="list-style-type: none"><li>• newRoot</li><li>• topologyChange</li></ul>
RFC 2819	<ul style="list-style-type: none"><li>• risingAlarm</li><li>• fallingAlarm</li></ul>

---

以下則是此型交換器支援的 Sun 企業 trap：

---

RFC 編號	書名
CSSP.MIB	<ul style="list-style-type: none"><li>• swPowerStatusChangeTrap</li></ul>

---



## 疑難排解

---

如果您無法正常連上網路，請先檢查網路線看看裝置是否已經正確接上網路，接著請參閱第 B-1 頁的「診斷交換器指示燈」檢查交換器上相對應連接埠的運作是否正常。

如果您無法正常連上管理介面，請參閱第 B-2 頁的「存取管理介面」中的疑難排解圖。

---

### B.1 診斷交換器指示燈

如果裝置連上交換器的連接埠後，Link LED 燈還是沒有亮起來，請檢查以下項目：

- 網路線兩端是否緊緊插入交換器與相對應的裝置上。
- 使用的網路線種類是否正確，其長度是否在規定的範圍內。
- 裝置的網路卡與網路線本身是否有任何問題，必要時請將故障的網路卡換掉。

檢查所有系統組件的安裝是否正確。如果發現任何網路接線似乎有問題，請將它拿到另一個全部組件都正常運作的環境中進行測試。

---

## B.2 診斷連接埠線路

遇到連接埠故障時，請檢查以下項目：

- 網路線是否牢固，且兩端是否接在正確的连接埠上。
- 連接埠狀態 (Admin) 已啟動，且自動協商功能也有啟動，否則線路兩端的連接埠就必須設定成同樣的速度與雙工模式。相關資訊，請參閱第 3-78 頁的「連接埠組態」。

---

## B.3 存取管理介面

從交換器所連網路中的任何一個地方，都可以透過 telnet、網路瀏覽器與具有 SNMP 功能的網管軟體連上交換器的管理介面。如果無法正常連上其管理介面，請參閱以下所示疑難排解資訊。

無法用 telnet、網路瀏覽器或 SNMP 軟體連上交換器時，請作以下檢查：

- 確認伺服器機箱電源是否有打開。
- 檢查管理主機與交換器之間的網路線。
- 檢查通往交換器的網路連線是否正常，以及您使用的連接埠是否被關掉。請參閱第 3-78 頁的「連接埠組態」。
- 若管理主機與伺服器機箱之間只有第二層交換器，請注意以下事項：
  - 交換器的管理 VLAN 必須設定正確的 IP 位址與子網路遮罩。
  - 管理主機在管理 VLAN 所屬的子網路中也必須有一個 IP 位址。
  - 管理主機所連接的交換器連接埠必須是管理 VLAN 的成員之一。
  - 負責連接網路內各中介交換器的所有連接埠，都必須是會加註標籤的連接埠，而且也必須隸屬於管理 VLAN。
- 如果管理主機與伺服器機箱之間有一台或多台第三層交換器，請注意以下事項：
  - 交換器的管理 VLAN 必須設定正確的 IP 位址、子網路遮罩與預設閘道。
  - 管理主機必須設定正確的 IP 位址、子網路遮罩與預設閘道。
  - 管理主機所連接的交換器連接埠必須是管理 VLAN 的成員之一。
  - 負責連接網路內各中介交換器與第三層交換器的所有連接埠，都必須是會加註標籤的連接埠，而且也必須隸屬於管理 VLAN。
- 如果是無法用 telnet 連上交換器，可能是目前同時連上交換器的 telnet 連線個數已經達到上限，請稍後再試。



若無法透過序列式連接埠線路連上內附的組態設定軟體，請作以下檢查：

- 使用 Sun Fire B1600 Blade 機箱所附的 DB-9 轉 RJ-45 線，將終端機或電腦連上 SSC 模組的序列埠。
- 確認已經將終端機模擬軟體設定為 VT100 相容、8 個資料位元、1 個停止位元、無同位檢查以及 9600 bps。
- 檢查 null-modem (空接數據機) 序列接線是否符合附錄 B 所述的腳位。

---

## B.4 使用系統日誌

萬一真的出現故障，請參閱伺服器機箱的其它手冊，先確認遇到的問題是不是真的由交換器造成的。如果問題看起來確實是由交換器引起的，請依照以下步驟進行。

1. 啟動記錄功能。
2. 將系統回報錯誤訊息範圍設定成涵蓋所有種類。
3. 指定負責接收錯誤訊息的 SNMP 主機。
4. 將當初造成錯誤的一連串指令或動作重複一遍。
5. 將導致問題的所有指令或狀況記錄下來。此外，系統顯示的任何錯誤訊息也請全部記錄下來。
6. 與客戶服務部門聯絡。

### 範例

```
Console(config)#logging on
Console(config)#logging history flash 7
Console(config)#snmp-server host 10.1.0.23
.
.
.
```

## B.4.1 日誌訊息

下表列出此交換器所產生的日誌訊息：

**表 B-1** 日誌訊息

訊息	說明	層級*
System coldStart notification	系統冷開機。	5
System warmStart notification	系統暖開機。	5
Unit 1 Port YY link-up notification	連接埠連線成功。	6
Unit 1 Port YY link-down notification	連接埠斷線。	6
Trunk 1 link-up notification	寬道連線成功。	6
Trunk 1 link-down notification	寬道斷線。	6
VLAN XX link-up notification	VLAN 連線成功。	6
VLAN XX link-down notification	VLAN 斷線。	6
Authentication failure notification	SNMP 存取認證失敗。	6
STA root change notification	STA root 變更。	6
STA topology change notification	STA 拓樸變更。	6
RMON rising alarm notification	RMON 偵測到的數值攀升到指定數值之上。	6
RMON falling alarm notification	RMON 偵測到的數值落到指定數值以下。	6

**Unit 1 Port YY** 代表單元 1，連接埠 YY (YY: 1 到 25)。

**VLAN XX** 代表某些 VLAN ID 值 (XX: 1 到 4094)。

\* syslog 訊息層級 (參閱第 4-31 頁的「logging history」)。

## B.5 錯誤訊息

### B.5.1 指令行錯誤偵測

交換器偵測到指令行輸入的資料不正確時，會在偵測到的錯誤位置底下顯示一個 ^ 符號，例如：

```
Console#show interfaces status s e 1/1
                                     ^
% Invalid input detected at '^' marker.
```

### B.5.2 系統錯誤

下表列出此交換器所產生的主要錯誤訊息。若要控制交換器發出的訊息層級，請參閱第 4-31 頁的「logging history」。

表 B-2 系統錯誤訊息

訊息	說明	層級*
<module> create task fail.	該軟體模組無法建立工作。	2
<module> task idle too long.	該軟體模組閒置時間過長。	2
Allocate <string> memory fail.	為 <字串> 配置記憶體時失敗。	2
Free <string> memory fail.	釋放 <字串> 的記憶體時失敗。	2
<string> switch to default.	指定的設定值不正確或不支援，因此改用預設值。(關於可使用哪些設定值，請參閱線上說明或本手冊。)	3

**module** 指的是交換器的軟體模組 (即 STA、VLAN、XFER、TRAP 或 RMON)。

**string** 指的是您輸入的組態設定值。

\* syslog 訊息層級 (參閱第 4-31 頁的「logging history」)。

## B.5.3 指令行錯誤

下表列出此交換器針對指令行介面所產生的錯誤訊息，請注意這些訊息都不會寫入日誌檔案內。

**表 B-3** 指令行錯誤訊息

訊息	說明
Ambiguous command: <string>	指令模稜兩可。
Clear dynamic address error.	無法清除動態位址。
CLI internal error - contact your local service provider.	CLI 指令內部錯誤。
Copy error.	複製失敗。
Exec-timeout could not be disabled for vty session.	透過 telnet 連線時不允許關閉 exec-timeout。
Factory default configuration file cannot be deleted.	不允許刪除出廠預設檔案。
Factory default configuration file cannot be replaced.	不允許取代出廠組態檔案。
Failed to allocate resource.	資源不足。
Failed to get <string>	show 指令失敗。
Failed to set <string>	組態設定指令失敗。
Failed to write certificate file to flash.	憑證檔案有問題、私密鍵檔案有問題（例如 pass phrase 不對）或私密鍵與憑證檔案的公用鍵不符。
Incomplete command.	指令不完整。
Insufficient memory.	記憶體不足。
Insufficient memory to display or save running config.	空間不足，無法收集所有資訊。
Invalid file name.	輸入的檔案名稱無效。
Invalid input.	從鍵盤輸入的資料錯誤。
Invalid input detected at '^' marker.	指令無效。
Invalid parameter.	ping 參數錯誤。
Invalid parameter value/range.Type '?' to get more detail information.	輸入的設定值或字串不適合。
Invalid TFTP server IP address.	TFTP IP 位址錯誤。
Not enough resources; please try later.	ping 函數資源不足。

**表 B-3** 指令行錯誤訊息

訊息	說明
No such file.	系統沒有這個檔案。
No such VLAN.	VLAN 不存在。
Port <port name> does not exist.	連接埠名稱不存在。
Port <port name> is an ethernet port.	指定的連接埠是乙太網路連接埠。
Port <port name> is not present.	進入介面模式時，此連接埠不存在。
Port <port name> unknown.	未知連接埠。
Session terminated.	CLI 將目前的連線結束。
Session timed out.	連線逾時。
Startup file cannot be deleted.	不允許刪除開機檔案。
This command for console only.	連線模式 (vty) 不可使用主控台參數指令。
This command is only valid for adding a single port to a trunk.	此指令只能將一個連接埠加入寬道內。
This command is only valid for the name of a single port.	設定連接埠說明時，不可同時挑選多個連接埠。
This command is not supported for management port in current release.	不能針對管理連接埠使用 no switchport allow vlan 指令。
Trunk ID:<trunk> is out of range.	輸入的寬道 id 不合適。
Trunk <trunk> does not exist.	寬道不存在。
Trunk <trunk> is a normal trunk.	此為一般寬道。
Trunk with no members cannot be displayed.	無法設定或顯示寬道成員。
Type 'show ?' for a list of subcommands.	此時只能輸入 show 指令。
Unknown error.	不明錯誤。
Unrecognized command.	無法辨認的指令。

<string> 指的是輸入給指令使用的設定值。

## B.5.4 Web 介面錯誤

下表列出此交換器 Web 介面所產生的錯誤訊息，請注意這些訊息都不會寫入日誌檔案內。

**表 B-4** Web 介面錯誤訊息

功能表	訊息	說明
Switch Setup		
System Identity	User privileges are not enough to perform this operation.	權限不足。
Network Identity	Current IP Address Mode is not DHCP or BOOTP.	重新啟動 DHCP 時，交換器必須是在 DHCP 或 BOOTP 模式才行。
	Data is invalid.	一般錯誤。
	Set DHCP Client-ID error.	DHCP 用戶端 ID 設定失敗。
	User privileges are not enough to perform this operation.	權限不足。
Software	Data is invalid.	一般錯誤。
	Please input a destination file.	請輸入要下載或上傳的目的檔案名稱。
	Please input a source file.	請輸入要下載或上傳的來源檔案名稱。
	Please input or select a destination file.	請輸入或選取要下載或上傳的檔案名稱。
	Please select a file.	請選取要下載或上傳的檔案。
	System will be restarted...	系統即將重新啟動。
	User privileges are not enough to perform this operation.	權限不足。
Switch Config		
Security	Cannot add user.	使用者名稱無效，或使用者人數已達上限。
	Cannot set password for user.	密碼無效。
	Cannot set user privilege.	使用者表格有問題。
	Cannot set user status.	使用者表格有問題。
	User does not exist.	使用者表格有問題。
Communication	Community String cannot contain spaces.	群體字串中不可以含有空格。
	Community table is full or data is invalid.	群組表已滿或資料無效。

表 B-4 Web 介面錯誤訊息

功能表	訊息	說明
	Data is invalid.	一般錯誤。
	Illegal SNMP trap IP address.	IP 位址格式不正確。
	Please select a Community String.	請選取要移除的群體字串。
	Please type a Community String.	請輸入要加入的群體字串。
	Trap Manager table is full or data is invalid.	trap 管理員表已滿或資料無效。
	User privileges are not enough to perform this operation.	權限不足。
	You must specify an IP trap community string.	請輸入要加入的 IP trap 群體字串。
Security	Authentication type doesn't exist.	不支援 Local、TACACS 或 RADIUS 其中一種認證方式。
	Data is invalid	一般錯誤。
	Illegal IP address.	IP 位址格式不正確。
	Number of Server Transmits is out of range.	RADIUS 重傳次數超過範圍。
	Password too long.	密碼超過最大長度。
	Please input username.	請輸入使用者名稱以便增加一個新的使用者。
	Please select an user	請選取要移除或更改密碼的使用者。
	RADUIS KEY is invalid	RADIUS 加密金鑰無效。
	Server Port Number is out of range.	RADIUS 通訊埠編號超出範圍。
	Select a privilege level.	請選取新使用者的權限等級。
	TACACS PORT is invalid	TACACS 通訊埠無效。
	TACACS KEY is invalid	TACACS 鍵無效。
	Timeout is out of range.	RADIUS 逾時設定值超出範圍。
	User privileges are not enough to perform this operation.	權限不足。
VLAN	Cannot create VLAN.	VLAN ID 無效，或超過可支援的 VLAN 個數上限。
	Cannot set VLAN name.	VLAN 名稱無效。
	Cannot set VLAN status.	無法取消 VLAN 1 或定義給管理連接埠使用的固有 VLAN (PVID)。
	Cannot delete VLAN.	還含有成員的 VLAN 以及定義成介面的固有 VLAN (PVID) 都是不可以刪除的。

表 B-4 Web 介面錯誤訊息

功能表	訊息	說明
	Data is invalid	一般錯誤。
	User privileges are not enough to perform this operation.	權限不足。
Membership	Data is invalid.	一般錯誤。
	User privileges are not enough to perform this operation.	權限不足。
Broadcast & Multicast		
Broadcast Parameters	Threshold is out of range.	超過最大廣播風暴上限值。
	User privileges are not enough to perform this operation.	權限不足。
IGMP Parameters	Please enter a valid version.	請輸入正確的版本。
	Query count is out of range.	查詢次數超過範圍。
	Query interval is out of range.	查詢間隔時間超過範圍。
	Query timeout is out of range.	查詢逾時時間超過範圍。
	Report delay is out of range.	回報延遲時間超過範圍。
	User privileges are not enough to perform this operation.	權限不足。
Multicast Router Ports	Data is invalid.	一般錯誤。
	Please select a port	請選取要加入群組廣播路由器或從其中刪除的連接埠。
	User privileges are not enough to perform this operation.	權限不足。
Multicast Services	Data is invalid.	一般錯誤。
	Igmp group member is null.	請從清單中選出 IGMP 群組成員。
	Illegal IP address.	IP 位址格式不正確。
	Select a port or trunk	請選取要加入 VLAN 成爲靜態連接埠或從其中移除的連接埠。
	User privileges are not enough to perform this operation.	權限不足。
Spanning Tree		
Basic Configuration	Data is invalid.	一般錯誤。
	Priority is out of range.	權限等級超出範圍。
	User privileges are not enough to perform this operation.	權限不足。



表 B-4 Web 介面錯誤訊息

功能表	訊息	說明
Advanced Configuration	Data is invalid.	一般錯誤。
	User privileges are not enough to perform this operation.	權限不足。
Class of Service		
Basic Traffic Prioritisation	Cos Value is out of range.	CoS 設定值超出範圍。
	Data is invalid.	一般錯誤。
	Priority is out of range.	權限等級超出範圍。
	Queue weight must be in a order of $Q0 \leq Q1 \leq Q2 \leq Q3$	佇列權重不合適。
	Traffic Class is out of range.	流量等級超出範圍。
Layer 3/4 Traffic Prioritisation	User privileges are not enough to perform this operation.	權限不足。
	Cos Value is out of range.	CoS 設定值超出範圍。
	Please select IP Precedence or DSCP mode	啓動優先等級服務時，請選取其中一種選項。
	Traffic Class is out of range.	流量等級超出範圍。
Address Tables	User privileges are not enough to perform this operation.	權限不足。
	Aging time is out of range.	超過最長位址保存期限。
Up Links, Down Links		
Status	Cannot set port capabilities.	指定連接埠的速度/雙工模式不正確。
	Data is invalid.	一般錯誤。
	User privileges are not enough to perform this operation.	權限不足。
Link Aggregation	Cannot add trunk.The specified trunk is full or data is invalid.	指定寬道已滿或資料無效。
	Cannot create trunk.	超過寬道個數上限。
	Cannot remove trunk.	寬道表有問題。
	Cannot remove trunk member.Data is invalid.	寬道表有問題。
	Cannot set trunk status.	無法啓動此靜態寬道成員的 LACP。
	Data is invalid.	一般錯誤。

表 B-4 Web 介面錯誤訊息

功能表	訊息	說明
	User privileges are not enough to perform this operation.	權限不足。
VLANs	Data is invalid.	一般錯誤。
	Please enter a valid PVID.	PVID 無效，請選取正確的 PVID。
	Please enter a valid timer.	計時器無效，請選取正確的計時器。
	Table is full or data is invalid.	表格已滿或資料無效。
	User privileges are not enough to perform this operation.	權限不足。
Address Filtering	Data is invalid.	一般錯誤。
	Please enter a valid MAC address.	MAC 位址無效。
	Please enter a valid VLAN ID.	VLAN ID 無效。
	Table is full or data is invalid.	表格已滿或資料無效。
	User privileges are not enough to perform this operation.	權限不足。
Spanning Tree	Data is invalid.	一般錯誤。
	User privileges are not enough to perform this operation.	權限不足。
Config	Path cost is out of range.	路徑成本超過範圍。
	Priority is out of range.	優先等級超出範圍。
Port	Path cost is out of range.	路徑成本超過範圍。
	Priority is out of range.	優先等級超出範圍。
	User privileges are not enough to perform this operation.	權限不足。
Management Ports		
VLANs	Data is invalid.	一般錯誤。
	Please enter a valid PVID.	PVID 無效，請選取正確的 PVID。
	Please enter a valid timer.	計時器無效，請選取正確的計時器。
	Table is full or data is invalid.	表格已滿或資料無效。
	User privileges are not enough to perform this operation.	權限不足。
Packet Filtering	User privileges are not enough to perform this operation.	權限不足。
Monitoring		

表 B-4 Web 介面錯誤訊息

功能表	訊息	說明
Port Mirroring	Data is invalid.	一般錯誤。
	User privileges are not enough to perform this operation.	權限不足。
Logs	Data is invalid.	一般錯誤。
	User privileges are not enough to perform this operation.	權限不足。



# 規格

---

## C.1 交換器架構

### 連接埠

上連線路 – 8 個 1000BASE-T

Midplane – 16 個連續的 Gigabit 下連線路 ( 連接各伺服器葉片 )

管理通道 – 1 個 10/100BASE-TX、1 個主控台連接埠 ( 序列式 RJ-45)

### 網路介面

10/100/1000Base-T 連接埠 NETP0-7 :

RJ-45 接頭、自動協商、自動 MDI/MDI-X

線路：10BASE-T：100 歐姆，UTP 線，第 3、4、5 類

100BASE-TX：100 歐姆，UTP 線，第 5 類

1000BASE-T：100 歐姆，UTP 線，第 5 或 5e 類

### 緩衝區架構

上連與下連連接埠：共用 1 Mbyte

### 總頻寬

48 Gbps

### 交換資料庫

可容納 32K 個 MAC 位址

### LED

SSC：Active ( 正常運作 )、Service Required ( 需維修 )、Ready to Remove ( 可以拆除 )

乙太網路連接埠：Link/Active ( 連線/運作 )、Speed ( 速度 )

---

## C.2 管理功能

### 透過網路進行管理

Telnet、HTTP (透過瀏覽器)、SNMP

### 透過網路以外的方式進行管理

使用 RS-232 訊號連上 RJ-45 主控台連接埠

### 軟體載入

透過 TFTP 網路傳輸，或用 XModem 接線傳送

### 支援的 MIB

SNMP v1/v2 (RFC 1215、1907)、MIB II (RFC 2863)、Bridge MIB (RFC 1493)、Etherlike MIB (RFC 1643/2665)、RMON (RFC 2819 groups 1、2、3、9)、IEEE 802.1Q VLAN (RFC 2674)、IEEE 802.3ad LACP、private MIB

### 支援的 RMON

群組 1、2、3、9 (Statistics (統計)、History (歷程資料)、Alarm (警告)、Event (事件))

### 其它功能

連接埠集束寬道 (靜態與 LACP 皆可)

連接埠鏡射

連接埠安全性

RADIUS 認證用戶端

---

## C.3 實體

### 重量

2.08 公斤 (4.59 磅)

### 大小

27.5 x 20.3 x 4.3 公分 (10.8 x 8.0 x 1.7 英吋)

---

## C.4 電力

### 運轉電壓

+12 VDC

### 最大電流

5.2 安培

### 消耗功率

最高 62 瓦

### 熱放射

最高 211 BTU/小時

---

## C.5 週遭環境

### 溫度

適合運轉溫度範圍：5 到 45 °C (41 到 113 °F)

適合放置溫度範圍：-40 到 70 °C (-40 到 158 °F)

### 濕度

適合運轉溼度範圍：10% 到 90% (未凝結)

---

## C.6 標準

IEEE 802.3 Ethernet (乙太網路)、IEEE 802.3u Fast Ethernet (快速乙太網路)、  
IEEE 802.3ab Gigabit Ethernet (Gigabit 乙太網路)  
IEEE 802.1D Spanning Tree Protocol and traffic priorities (Spanning Tree 通訊協定與  
流量優先等級)、  
IEEE 802.1w Rapid Reconfiguration (快速重設組態, STP)  
IEEE 802.1p priority tags (優先等級標籤)、IEEE 802.1Q VLAN、IEEE 802.3ac  
VLAN tagging (VLAN 標籤)、  
IEEE 802.3x full-duplex flow control (全雙工流量控制) (ISO/IEC 8802-3)  
IEEE 802.3ad Link Aggregation Control Protocol (線路集束控制協定)、  
SNMP (RFC 1215、1907)、RMON (RFC 2819 群組 1、2、3、9)、MIB II (RFC 2863)、  
Bridge MIB (RFC 1493)、Etherlike MIB (RFC 1643/2665)、  
ARP (RFC 826)、IGMP (RFC 1112)、ICMP (RFC 792)



# 辭彙表

---

<b>1000BASE-T</b>	IEEE 802.3ab 規格標準，規範在兩對第 5 或 5e 類 100 歐姆 UTP 線路上架設的 Gigabit 乙太網路。
<b>1000BASE-X</b>	IEEE 802.3 的簡寫，規範使用 8B/10B 訊號的 1000 Mbps Gigabit 乙太網路。
<b>100BASE-TX</b>	IEEE 802.3u 規格標準，規範在兩對第 5 類 UTP 線路上架設的 100 Mbps 快速乙太網路。
<b>10BASE-T</b>	IEEE 802.3 規格標準，規範在兩對第 3、4 或 5 類 UTP 線路上架設的 10 Mbps 乙太網路。
<b>BOOTP</b>	開機通訊協定的一種，用以將作業系統載入到連接在網路上的裝置。
<b>CSMA/CD</b>	Carrier Sense Multiple Access/Collision Detect (偵測線路、多重存取/碰撞偵測) 的縮寫，為乙太網路與快速乙太網路所使用的通訊方式。
<b>Dynamic Host Control Protocol (DHCP，動態主機控制協定)</b>	可將組態資訊透過 TCP/IP 網路傳給主機的一種架構，是從 BOOTP (Bootstrap Protocol，開機通訊協定) 演變而來，多了自動分配可用網路位址與其它組態設定功能。
<b>GARP VLAN Registration Protocol (GVRP，GARP VLAN 註冊通訊協定)</b>	定義一種讓交換器彼此互傳 VLAN 資訊的方式，以便沿著 Spanning Tree 上的連接埠註冊所需的 VLAN 成員，讓每個交換器上定義的 VLAN 能自動跨越一個 Spanning Tree 網路運作。
<b>Generic Attribute Registration Protocol (GARP，通用屬性註冊通訊協定)</b>	GARP 是終端站與交換器在交換器組成的網路環境中，用來註冊與傳播廣播群組隸屬關係的一種通訊協定，讓群組廣播資料封包得以只傳給含有已註冊終端站的交換式 LAN 環境。此通訊協定原先稱為 Group Address Registration Protocol (群組位址註冊通訊協定)。
<b>Gigabit 乙太網路</b>	採用乙太網路與 CSMA/CD 存取方式的 1000 Mbps 網路通訊系統。
<b>Group Attribute Registration Protocol (群組屬性註冊通訊協定)</b>	請參閱 <i>Generic Attribute Registration Protocol (通用屬性註冊通訊協定)</i> 。

<b>IEEE 802.1D</b>	規範 MAC 橋接器通用運作方式，包括 Spanning Tree 通訊協定。
<b>IEEE 802.1p</b>	規範在乙太網路中提供服務品質 (quality of service, QoS) 的一項 IEEE 標準，利用最多可標示 8 種流量類別的封包標籤，讓交換器得以根據標籤所示優先等級傳輸封包。
<b>IEEE 802.1Q</b>	VLAN 標籤加註功能 — 定義傳達 VLAN 資訊的乙太網路封包標籤，讓交換器得以將終端站分派到不同的虛擬 LAN，並定義各 VLAN 透過交換式網路相互通訊的標準方式。
<b>IEEE 802.1w</b>	規範 Rapid Spanning Tree Protocol (RSTP, 快速 Spanning Tree 通訊協定) 的一項 IEEE 標準，其設計用來取代 IEEE 802.1D，在拓樸有任何變化時，RSTP 能以相當快的速度收斂。
<b>IEEE 802.3</b>	定義「偵測線路、多重存取/碰撞偵測」(carrier sense multiple access with collision detection, CSMA/CD) 存取方式與實體層規格的標準。
<b>IEEE 802.3ab</b>	定義 1000BASE-T 快速乙太網路所使用之 CSMA/CD 存取方法與實體層規格的標準。
<b>IEEE 802.3ac</b>	定義 VLAN 標籤的封包擴充功能。
<b>IEEE 802.3u</b>	定義 100BASE-TX 快速乙太網路所使用之 CSMA/CD 存取方法與實體層規格的標準。
<b>IEEE 802.3x</b>	定義乙太網路封包起始/結束要求，以及全雙工線路流量控制所使用的計時器。
<b>IEEE 802.3z</b>	定義 1000BASE Gigabit 乙太網路所使用之 CSMA/CD 存取方法與實體層規格的標準。
<b>IGMP Snooping</b>	傾聽 IP 群組廣播路由器與 IP 群組廣播主機群組之間傳輸的 IGMP Query (查詢) 與 IGMP Report (回報) 封包，以找出 IP 廣播群組的成員。
<b>Internet Control Message Protocol (ICMP, 網際網路控制訊息通訊協定)</b>	常用來傳輸 echo 訊息 (即 Ping)，達到監視的目的。
<b>Internet Group Management Protocol (IGMP, 網際網路群組管理通訊協定)</b>	主機向其當地路由器註冊群組廣播服務時所使用的通訊協定。若該子網路上的群組廣播路由器不只一台，其中一台路由器會擔任「查詢者」的角色，負責追查記錄群組中的成員。
<b>IP 群組廣播過濾</b>	此交換器將群組廣播流量傳給特定主機所依賴的方式。
<b>LAN 網段</b>	不同的 LAN 或碰撞領域。
<b>LED 指示燈</b>	用於監視裝置或網路狀態的發光二極體。
<b>Link Aggregation Control Protocol (LACP, 線路集束控制協定)</b>	讓連接埠得以與另一台裝置上具有 LCAP 功能的連接埠自動協商出一條集束線路。

<b>Local Area Network</b> (LAN, 區域網路)	一群相互連接的電腦與支援裝置。
<b>Management Information Base</b> (MIB, 管理資訊庫)	Management Information Base 縮寫, 由一組資料庫物件組成, 其中含有與裝置相關的資訊。
<b>Media Access Control</b> (MAC, 媒介控制存取)	網路通訊協定的一部份, 負責管控傳輸媒介的使用權, 以便網路節點之間能順利交換資料。
<b>Remote Authentication Dial-in User Service</b> (RADIUS, 遠端認證撥入使用者服務)	一種認證通訊協定, 使用中央伺服器控制外界對網路上具有 RADIUS 功能之裝置的存取權。RADIUS 伺服器可以設計成採用含有多筆使用者名稱與密碼的資料庫, 其中還有各使用者或群組要對此交換器進行管理時必須擁有的權限等級。
<b>Remote Monitoring</b> (RMON, 遠端監視)	RMON 提供非常完整的網路監視能力, 不僅消除標準 SNMP 所需的週期性輪詢動作, 同時還可以針對各種流量狀況 (包括錯誤類別及設定警報)。
<b>RJ-45 接頭</b>	雙絞線所使用的一種接頭。
<b>Shielded Twisted Pair</b> (STP, 遮蔽式雙絞) 線	外圍覆蓋鋁箔或銅網的雙絞線, 以便降低受到外界雜訊或輻射的干擾。
<b>Simple Network Management Protocol</b> (SNMP, 簡易網路管理協定)	整套網際網路通訊協定中, 提供網路管理服務的一種應用程式通訊協定。
<b>Spanning Tree Protocol</b> (STP, Spanning Tree 通訊協定)	檢查網路內是否有任何迴路出現的一種技術。結構較為複雜的網路或備援網路中, 常常會有迴路出現, Spanning Tree 可偵測到這種情形, 引導資料沿著最短路徑傳遞, 使網路的效能與效率達到最佳狀態。
<b>Telnet</b>	定義一種遠端通訊功能, 以便透過 TCP/IP 連上終端裝置。
<b>Terminal Access Controller Access Control System</b> (TACACS, 終端機存取控制器存取控制系統)	一種認證通訊協定, 使用中央伺服器控制外界對網路上具有 TACACS 功能之裝置的存取權。RADIUS 伺服器可以設計成採用含有多筆使用者名稱與密碼的資料庫, 其中還有各使用者或群組要對此交換器進行管理時必須擁有的權限等級。
<b>Transmission Control Protocol/Internet Protocol</b> (TCP/IP, 傳輸控制通訊協定/網際網路通訊協定)	一套完整的通訊協定, 以 TCP 為主要傳輸通訊協定, 並以 IP 作為網路層的通訊協定。
<b>Trivial File Transfer Protocol</b> (TFTP, 簡易檔案傳輸通訊協定)	一種 TCP/IP 通訊協定, 常用來進行軟體下載。

<b>Unshielded Twisted Pair (UTP, 裸露式雙絞) 線</b>	由兩條隔離的線路相互纏繞組成的線路，以降低電磁干擾，常用來當作一般的電話線。
<b>Virtual LAN (VLAN, 虛擬區域網路)</b>	VLAN 由一群網路節點組成，無論這些節點在網路中的實際位置與連接點為何，均同屬一個碰撞領域。VLAN 可視為沒有實體界線的邏輯工作群組，讓使用者得以共用資訊與資源，就好像大家都接在同一個 LAN 上一樣。
<b>XModem</b>	裝置之間彼此傳輸檔案所使用的一種通訊協定。將資料切成每 128 個位元組為一個區段，並具有修正錯誤的能力。
<b>乙太網路</b>	由 DEC、Intel 與 Xerox 共同研發與制定標準的一種網路通訊系統，採用基頻傳輸、CSMA/CD 存取方式、邏輯匯流排拓樸與同軸電纜。其後繼標準 IEEE 802.3 不僅能整合至 OSI 模型內，亦可在光纖、細軸與雙絞線線路上傳輸，再加上中繼器，大幅擴展其實體層與傳輸媒介的涵蓋範圍。
<b>交換連接埠</b>	位於埠同碰撞領域或 LAN 網段的連接埠。
<b>全雙工</b>	讓交換器與網路卡可同時收發資料的傳輸方式，可將線路的頻寬有效提昇至兩倍。
<b>自動協商</b>	訊號交換方式的一種，讓每個節點根據連線另一端節點的能力挑選最佳的運作模式（例如 10 Mbps 或 100 Mbps，半雙工或全雙工）。
<b>快速乙太網路</b>	採用乙太網路與 CSMA/CD 存取方式的 100 Mbps 網路通訊系統。
<b>第 2 層</b>	ISO 7 層資料通訊協定中的資料連結層，與網路裝置的硬體介面直接相關，負責根據 MAC 位址傳輸流量。
<b>第 3 層</b>	ISO 7 層資料通訊協定中的資料通訊層，提供路由功能，負責從一個開放的系統將資料傳到另一個系統上。
<b>終端站</b>	泛指不負責網路連接角色的工作站、伺服器或其他裝置。
<b>連接埠寬道</b>	定義一種網路線路集束與合併的方法，規範如何將數條低速實體線路結合起來，成為一條高速的邏輯線路。
<b>連接埠鏡射</b>	將一個通訊埠上的資料全部鏡射複製到另一個監視連接埠上，以使用邏輯分析儀或 RMON 感測器進行疑難排解的一種方法，可在完全不影響原連接埠的狀況下仔細檢驗其進出的資料。
<b>連結線段</b>	將兩個中繼器或一個中繼器與一台 PC 連起來的雙絞線或光纖線長度。
<b>透過網路以外的方式進行管理</b>	從沒有與網路連接之主機對該網路進行管理的方式。
<b>透過網路進行管理</b>	透過與網路直接連接的主機管理該網路。
<b>碰撞</b>	線路上傳遞之封包相互干擾的情形，會導致訊號難以判讀。這種狀況只會發生在半雙工的線路上。
<b>碰撞領域</b>	指單一 CSMA/CD LAN 網段。

<b>群組廣播交換</b>	根據交換器所連接之主機是否有註冊需要群組廣播服務，交換器將收到的群組廣播封包過濾掉或者將封包只轉送給廣播群組 VLAN 內所含連接埠的過程。
<b>線路集束</b>	參閱連接埠寬道。
<b>頻寬</b>	可傳輸網路訊號之最高頻率與最低頻率的差異，同時也是線路速度的同義詞，泛指資料沿線路傳輸的實際速度。
<b>頻寬使用率</b>	過去以來所收到之封包數量佔整體頻寬的百分比。



# 索引

---

## 字母

acceptable frame types , 4-108

BOOTP , 3-14 , 4-63

Class of Service 請參閱 CoS

CLI , 4-1

CoS

佇列對應 , 3-63 , 4-134

服務權重 , 3-68 , 4-133

配置 , 3-63 , 4-131

第 3/4 優先等級 , 3-69 , 4-131

預設優先等級 , 3-63 , 4-132

DHCP , 3-14 , 4-63

用戶端識別碼 , 3-11 , 4-65

Differentiated Services Code Point 請參閱 DSCP

DSCP , 3-73 , 4-138

GARP , 3-91 , 4-116

設定計時器 , 3-92 , 4-116

GARP VLAN Registration Protocol 請參閱 GVRP

Group Address Registration Protocol 請參閱 GARP

GVRP , 3-33 , 3-91 , 4-114

介面組態 , 3-92 , 4-114

全區設定 , 3-37 , 4-118

說明 , 3-33

IEEE 802.1D , 3-55 , 4-93

IEEE 802.1w , 3-55 , 4-93

IGMP , 3-43 , 4-120

Internet Group Management Protocol 請參閱 IGMP

IP 位址

BOOTP/DHCP 服務 , 3-14 , 4-62

手動設定 , 3-12 , 4-62

設定 , 3-10 , 4-62

IP 優先權 , 3-71 , 4-137

jumbo frame , 4-29

LACP , 3-86 , 4-146

Link Aggregation Control Protocol 請參閱 LACP

MIB , A-1

支援的 MIB , A-1

PVID , 3-91 , 4-110

預設 ID , 3-91 , 4-110

RADIUS , 3-23 , 4-41

Remote Authentication Dial-in User Service 請參閱

RADIUS

RSTP , 3-55 , 4-93

全區組態 , 3-61 , 4-93

說明 , 3-55

SC , 1-1 , 1-3

SNMP , 2-3

trap 接收者 , 2-5 , 3-29 , 4-50

trap , 支援的 , A-3

版本 , 2-3 , 3-29 , 4-50

配置 , 3-27 , 4-48

啟動 trap 功能 , 3-29 , 4-51

群體字串 , 2-4 , 3-28 , 4-48

Spanning Tree 通訊協定請參閱 STP

Spanning Tree 演算法請參閱 STA

SSC，1-xv，1-1，1-3

STA，3-55，4-91，4-92

    priority，4-99

    介面設定，3-100，4-102

    設定介面，3-104，4-91

    通訊協定遷移，3-107，4-101

    路徑成本，3-100，3-104

    說明，3-55

    線路種類，3-101，3-105，4-101

    優先等級，3-100，3-104

    邊緣連接埠，3-101，3-105，4-100

STP，3-55，4-93

TACACS，3-23，4-41

Telnet，4-2

Terminal Access Controller Access Control System

    請參閱 TACACS

trap 接收者，2-5，3-29，4-50

VLAN，3-32，3-91，4-104

    加註標籤，3-92，4-111

    未加註標籤，3-92，4-111

    成員連接埠，3-92，4-111

    配置，3-32，4-104

    禁止，3-92，4-112

    說明，3-32

Web 介面，3-2

    功能表清單，3-5

    存取需求，3-2

    首頁，3-3

    組態按鈕，3-4

    顯示面板，3-4

## 三畫

下連連接埠，1-3

下載軟體，3-18，4-17

上連連接埠，1-3

## 四畫

日誌，訊息，3-125

日誌訊息，B-4

## 五畫

主功能表，3-5，4-10

主控台連接埠

    配置，4-54

    連線，4-1

可接受的封包類別，3-91

## 六畫

交換器規格，C-1

交換器連接埠模式，3-91，4-107

交換器與系統控制器請參閱 SSC

## 七畫

位址表，3-75，4-87

    保留期限，3-77，4-88

伺服器葉片，1-1，1-3

序列埠

    配置，4-54

快速 Spanning Tree 通訊協定請參閱 RSTP

更新軟體，3-18，4-17

系統日誌，3-125，4-30，B-3

系統軟體，3-16，4-17

    上傳或下載，3-18，4-17

    從伺服器下載，3-18，4-17

## 八畫

使用者名稱，設定，3-23，4-41

狀態 LED，1-4

## 九畫

保留期限，3-77，4-88

指令行介面請參閱 CLI

## 十畫

記錄，訊息，4-30

## 十一畫

密碼，4-26，4-27，4-57

密碼，設定，3-23，4-41



- 統計數據，SNMP，3-122，4-52
- 統計數據，交換器，3-113，4-82
- 組態設定
  - 儲存，2-5
  - 儲存或復原，3-21，4-17
- 規格，C-1
- 軟體下載，3-18，4-17
- 軟體版本，顯示，3-16，4-40
- 通訊協定遷移，3-107，4-101
- 通訊埠鏡射，3-112
- 連接埠，設定，3-78，4-73
- 連接埠安全功能，3-97，4-89
- 連接埠優先等級，預設入口，3-63，4-132
- 連接埠鏡射，4-142

## 十二畫

- 登入
  - Web 介面，3-3
- 登入認證，3-23，4-41
- 開機組態檔案，建立，3-21，4-18
- 開機檔案
  - 設定，3-18，4-22
  - 顯示，3-18，4-34
- 韌體，更新，3-18，4-17
- 韌體版本，顯示，3-16，4-40

## 十三畫

- 經過加密的密碼，4-26，4-27，4-57
- 群組廣播
  - 配置，3-43，4-120
  - 路由器，3-47，4-129
- 群體字串，2-4，3-28，4-48
- 路徑成本，3-100
- 路徑成本，STA，3-104，4-97，4-98
- 路徑成本，方法，3-61，4-97
- 過濾流量，管理連接埠，3-108，4-69

## 十四畫

- 疑難排解，B-1
  - 交換器指示燈，B-1
  - 使用系統日誌，B-3

- 連接埠線路，B-2
- 管理介面，B-2
- 管理
  - 介面，Web，3-2
  - 介面，主控台，4-1
- 管理連接埠，1-3
- 管理連接埠，過濾流量，3-108，4-69
- 管理資訊庫請參閱 MIB

## 十五畫

- 寬道
  - LACP，3-87，4-146
  - 配置，3-86，4-144
  - 動態，3-87，4-146
  - 靜態，3-89，4-144
- 廣播風暴
  - 流量上限，3-53，4-80
  - 連接埠設定，3-83，4-80
- 線路種類，STA，3-101，3-105，4-101

## 十六畫

- 輸入過濾，3-92，4-109
- 錯誤訊息，B-5
  - Web 介面，B-8
  - 系統錯誤，B-5
  - 指令行錯誤，B-6
  - 記錄，4-30
- 靜態位址，設定，3-97，4-86

## 十七畫

- 優先等級，STA，3-100，3-104
- 優先等級，TA，4-96
- 優先等級，預設連接埠入口，3-63，4-132

## 十八畫

- 簡易網路管理通訊協定請參閱 SNMP

## 十九畫

- 邊緣連接埠，STA，3-101，4-100
- 鏡射通訊埠，設定，3-112，4-142

