# CISCO IOS 命令文件查詢

**第 1 步**： 連到 [www.cisco.com](http://www.cisco.com/)。

**第 2 步**： 按一下“**Support**”。

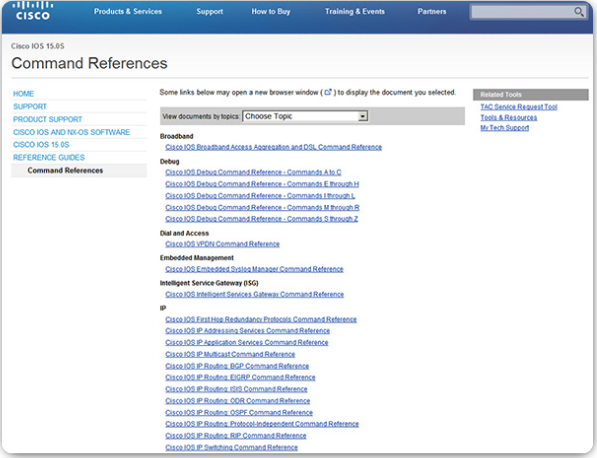
**第 3 步**： 按一下“**Network Software**”（IOS 和 NX-OS）。

**第 4 步**： 例如，按一下“**15.2M&T**”。

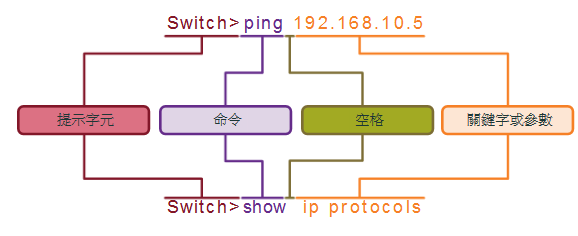
**第 5 步**： 按一下“**Documentation**”頁面。

**第 6 步**： 下拉到 “**Command References**” 的地方。

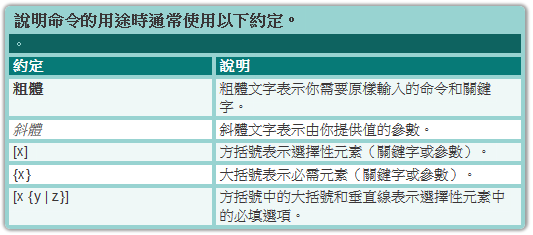
**第 7 步**： 按一下你想參考命令的具體技術。



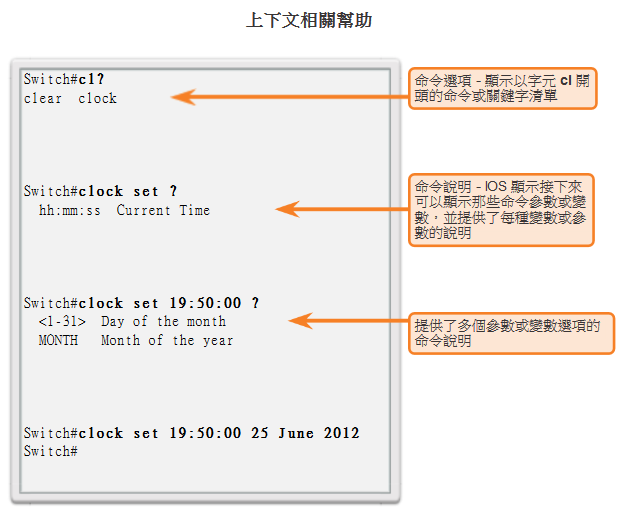
# 基本 IOS 命令結構



如下圖所示，粗體字表示輸入所示的命令和關鍵字，斜體字表示由你提供值的參數。對於 **description** 命令，參數是字串值。字串值可以是最多 80 個字元的任意文字字串。



**上下文相關幫助**



**命令語法檢查**



命令不正確

命令不明確

命令不完整

命令打錯，會進入搜尋模式，且畫面凍結，按 ctrl + shift + 6 可結束搜尋並跳出

IOS 檢查命令

若要驗證網路是否正常工作並排除故障，必須檢查裝置的工作情況。**show** 命令可提供有關思科交換器或路由器的設定、執行和狀態的資訊。**show** 後接具體的介面類型和插槽號/連接埠號。

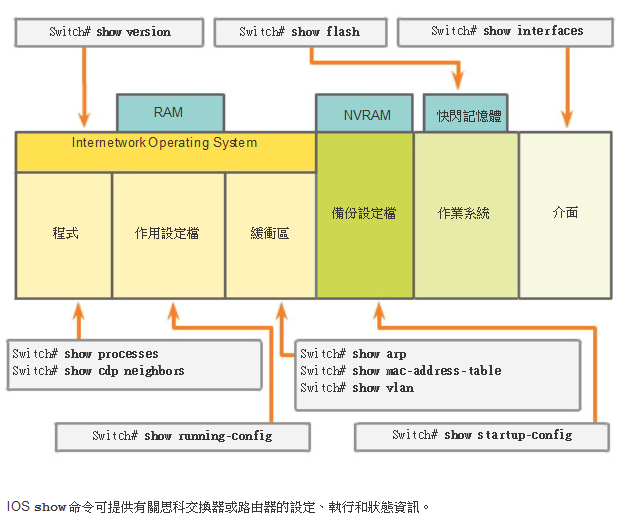
使用命令：

Switch# **show interfaces fastethernet 0/1** // 在 enable 模式顯示裝置上所有介面的統計資訊，常用！

**show startup-config** // 顯示儲存在 NVRAM 中的設定。

**show running-config** //顯示目前執行的設定檔的內容。

顯示資料無法在一頁內顯示完時，會出現 **More 提示字元** ，按**空格鍵**可檢視輸出的下一部分。如果僅需要顯示下一行，則按 **Enter** 鍵。如果按了其他任何鍵，則會取消輸出並返回到命令提示字元狀態。



NVRAM是類似硬碟的裝置，將設定檔存到這裡

IOS操作期間，所有設定存在RAM裡

Switch# **show version**

用來顯示目前載入的 IOS 版本以及硬體和裝置相關的資訊。遠端登入路由器或交換器時，**show version** 可快速尋找到關於特定相連裝置的有用摘要資訊。

* **軟體版本** - IOS 軟體版本（儲存在快閃記憶體中）
* **Bootstrap 版本** - Bootstrap 版本（儲存在 Boot ROM 中）
* **系統持續執行時間** - 自上次重新啟動以來的時間
* **系統重新啟動資訊** - 重新啟動方法（例如，重新通電或當機）
* **軟體映像名稱** - 儲存在快閃記憶體中的 IOS 檔名
* **路由器類型和處理器類型** - 型號和處理器類型
* **記憶體類型和分配情況（共用/主要）** - 主處理器 RAM 和共用封包輸入/輸出緩衝區
* **軟體功能** - 支援的協定/功能集
* **硬體介面** - 裝置的可用介面
* **組態暫存器** - 用於設定啟動規範、主控台速度設定和相關參數

設定 IOS 主機名稱

Switch(config)# **hostname Sw-Floor-1** // 從全域設定模式做設定

命令執行後，提示字元會變為：

Sw-Floor-1 (config)#

**exit** // 離開全域設定模式。

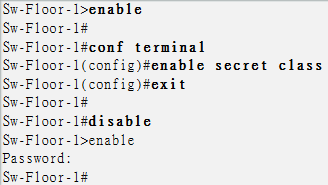
**注意**：要撤銷命令的影響，請在該命令前面增加 **no** 關鍵字。

Sw-Floor-1 (config)# **no hostname** // 刪除裝置的名稱。

Switch(config)# // 該交換器回復到其預設主機名稱“Switch”了。

設定密碼

IOS 使用階層式模式來提高裝置安全性。可以透過不同的密碼來提供不同的裝置存取權限。

* **主控台密碼** - 用於限制人員透過主控台連線存取裝置
* **特權密碼** - 用於限制人員存取特權 EXEC 模式
* **特權加密密碼** - 經加密，用於限制人員存取特權 EXEC 模式 只有這裡可以設定加密密碼
* **VTY 密碼** - 用於限制人員透過 Telnet 存取裝置

**enable secret** *password* // 設定特權加密密碼

在全域設定模式下來為主控台線路設定密碼：

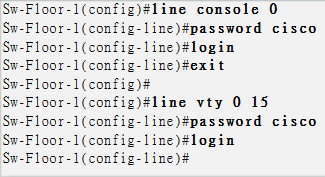
Switch(config)# **line console 0** // 0 代表第一個（而且在大多數情況下是唯一的一個）主控台介面。

Switch(config-line)# **password cisco** // 作為最低限度的安全措施，必須為所有網路裝置的主控台連接埠設定強密碼。這可降低未經授權的人員將纜線插入實際裝置來存取裝置的風險。

Switch(config-line)# **login**  // 用於將交換器設定為在使用者登入時要求驗證。

VTY 密碼

VTY 線路讓使用者可以透過 Telnet 存取思科裝置。預設情況下支援第 0 到 15 的 16 條 vty 線路。路由器最常見的數量設定是第 0 到 4 的 5 條線路。所有可用 vty 線路應該都要設密碼，可以把所有連線都設同一個密碼。但理想的做法是每一條線路都要設定不同的密碼；當其他連線均被佔用時，管理者還有保留的通道可以存取裝置，進行管理工作。

用於設定 vty 線路密碼的命令範例如下： 

預設情況下，IOS 自動為 VTY 線路執行了 **login** 命令。這可防止裝置在使用者透過 Telnet 存取裝置時不要求其進行驗證。如果使用者錯誤地使用了 **no login** 命令，則會取消驗證要求，這樣未經授權的人員就可透過 Telnet 連線到該線路。這是一項重大的安全風險。

加密設定檔內的明文密碼

**service password-encryption** //可在使用者設定密碼後使密碼進行弱加密，防止在顯示設定檔時顯示明文密碼。這種加密僅適用於設定檔中的密碼，密碼一旦加密，即使取消加密服務，也不會消除加密效果。

標題訊息

雖然要求使用者輸入密碼是防止未經授權的人員進入網路的有效方法，但還是必須向試圖存取裝置的人員聲明僅授權人員才可存取裝置。（警告性質）

當控告某人侵入裝置時，標語可在訴訟程序中起到重要作用。某些法律體系規定，若不事先通知使用者，則既不允許起訴該使用者，甚至連對該使用者進行監控都不允許。（包含台灣）

因為任何試圖登入的人員均可看到標語，因此標語訊息應該謹慎措辭。任何暗含“歡迎登入”或“邀請登入”意味的詞語都是不恰當的。如果標語有邀請意味，則當某人未經授權進入網路並進行破壞後，會很難舉證。標語的確切內容或措辭取決於當地法律和企業政策。下面列舉幾例可用在標語中的資訊：

* 僅授權人員才可使用裝置 (Use of the device is specifically for authorized personnel)。
* 活動可能被監控 (Activity may be monitored)。
* 未經授權擅自使用裝置將招致訴訟 (Legal action will be pursued for any unauthorized use)。

標語訊息有很多種。當日訊息 (Message of the DayM, OTD) 就是其中常用的一種。它常用於發佈法律通知，因為它會向連線的所有終端顯示。

**banner motd** 命令後接一個空格和一個分隔字元。隨後輸入代表標語訊息的一行或多行文字。當該分隔字元再次出現時，即表明訊息結束。分隔字元可以是未出現在訊息中的任意字元。經常使用“#”之類的字元。

從全域設定模式設定 MOTD 的語法如下：

Switch(config)# **banner motd #** *message* **#**

一旦命令執行完畢，系統將向之後存取裝置的所有使用者顯示該標語，直到該標語被刪除為止。

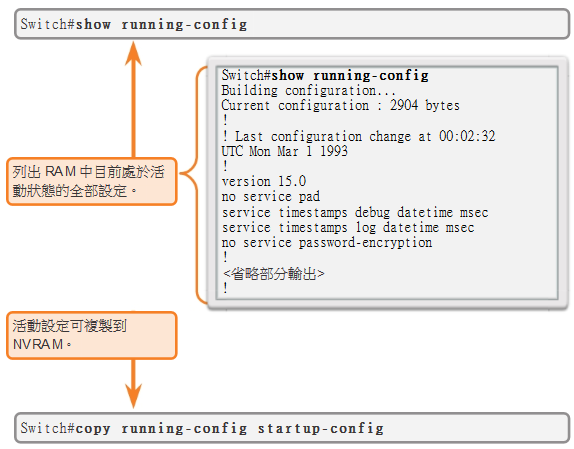
設定檔

修改正在執行的設定會立即影響思科裝置的執行。正在執行的設定會儲存在裝置的工作記憶體或隨機存取記憶體 (RAM) 中。也就是如果裝置斷電或重新啟動，所有未儲存的設定更改都會遺失。

把設定檔存到 NVRAM 中，可防止更改過的設定檔遺失。

在更改執行設定檔案之後，應考慮以下不同選項：

* 使裝置回復為其原始設定。
* 刪除裝置中的所有設定。
* 使更改後的設定成為新的啟動設定。



複製完後，最好透過重新啟動裝置來重新載入設定。

Switch# **reload**

將設備重新開機

Switch# **erase startup-config**  **//**清除所有設定，需要刪除啟動設定並重新啟動裝置。**erase NVRAM:startup-config 也可以。**

下指令後，交換器會提示確認：

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

Confirm 是預設回答。要確認並刪除啟動設定檔，請按 Enter 鍵。按其他任何鍵將中止該程序。

**注意：**使用 **erase** 命令時請多加注意。此命令可用於刪除裝置上的任何檔案。錯誤使用此命令會刪除 IOS 自身或其他重要檔案。

在交換器上，除了下 **erase startup-config** 指令，還要下**delete vlan.dat** 指令，重新啟動裝置來刪除 RAM 中的目前執行設定檔案，才能將裝置回復出廠設定（對比重置出廠設定）：

Switch# **delete vlan.dat**

Delete filename [vlan.dat]?

Delete flash:vlan.dat? [confirm]

Switch# **erase startup-config**

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

[OK]

Erase of nvram: complete

Switch#

備份設定檔

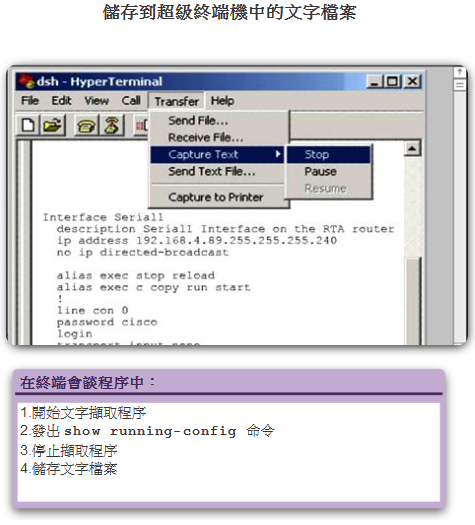
用 Tera Term （虛擬終端機）備份設定檔。



具體步驟如下：

* 在 File（檔案）功能表中按一下 **Log（記錄）**。
* 選好備份路徑後，Tera Term 將準備開始擷取文字。
* 馬上在 enable 模式執行 **show running-config** 或 **show startup-config** 命令。終端視窗中顯示的文字就會儲存到所選的檔案中。
* 擷取完成後，在“TeraTerm: Log”（TeraTerm：記錄）視窗中選擇“**Close**”（關閉）。
* 檢查輸出的內容是否正確。

用 HyperTerminal 備份設定檔。



還原備份檔

備份檔還原到到終端機後，IOS 會把每一行當作一個指令執行（類似 bat 檔或 shellscript 檔）。所以在還原備份檔後還需要將加密密碼更改為明文、刪除 “--More--”等非命令文字和 IOS 訊息。此外，還要初換到全域設定模式，才能接收並執行指令。

使用 Tera Term 時的步驟如下：

* 刪除非命令文字並儲存檔案。
* 在 **File（檔案）**功能表中按一下 **Send（發送）**。
* 找到要複製到裝置的檔案並按一下 **開啟**。
* Tera Term 會將該檔案貼上到裝置中。

# Packet Tracer - 設定初始交換器設定

第 1 部分: 檢驗預設交換器設定

第 1 步：     進入特權模式。

在特權模式下，你可以使用全部交換器指令。包括使用者模式的指令和用於存取其餘命令模式的 **configure** 命令。

a.       按一下 S1，然後按一下“CLI”頁標籤。按 <Enter>。

b.       輸入 enable 命令進入特權 EXEC 模式：

Switch> **enable**

Switch#

請注意特權執行模式下設定中提示字元的變化。

第 2 步：     檢查目前的交換器設定。

a.       輸入 show running-config 命令。 **//在enable 模式才能用show**

Switch# **show running-config**

b.       請回答以下問題：

* 交換器有多少個 FastEthernet 介面？
* 交換器有多少個 GigabitEthernet 介面？顯示的 vty 線路值範圍是什麼？
* 那條命令將顯示非揮發性隨機存取記憶體 (NVRAM) 中的當前內容？
* 為什麼交換器回應 startup-config is not present？

第 2 部分: 新增基本交換器設定

第 1 步：     為交換器指定名稱。

要在交換器上設定參數，你可能需要在各種設定模式之間切換。注意你導航交換器時提示字元的變化。

Switch# **configure terminal**

Switch(config)# **hostname S1 //在config 模式才能設 hostname**

S1(config)# **exit**

S1#

第 2 步：     保護對主控台線路的存取。

要保護對主控台線路的存取，請存取 config-line 模式並將主控台密碼設定為**letmein**。

S1# **configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

S1(config)# **line console 0**

S1(config-line)# **password letmein //各模式及線路都可以設密碼，所以要切換到相應的線路**

S1(config-line)# **login //密碼設定完要下 login 指令，登入時才會生效**

S1(config-line)# **exit**

S1(config)# **exit**

%SYS-5-CONFIG\_I: Configured from console by console

S1#

* 為什麼需要 **login** 命令？

第 3 步：     檢驗主控台存取是否受到保護。

退出特權模式，檢驗主控台連接埠密碼是否生效。

S1# **exit**

Switch con0 is now available

Press RETURN to get started.

User Access Verification

Password:

S1>

**注意：**如果交換器沒有提示你輸入密碼，那就是第 2 步中的**login**指令未設定。

第 4 步：     保護特權模式存取。

將**啓用**密碼設定為 **c1$c0**。此密碼用於保護對特權模式的存取。

**注意**：**c1$c0** 中的 **0** 是零，而不是大寫 O。此密碼在第 8 步中加密後才能被視為正確。

S1> **enable**

S1# **configure terminal**

S1(config)# **enable password c1$c0**

S1(config)# **exit**

%SYS-5-CONFIG\_I: Configured from console by console

S1#

第 5 步：     檢驗特權模式存取是否安全。

a.       再次輸入 **exit** 命令登出交換器。

b.       按 **<Enter>**，這次將會提示你輸入密碼：

User Access Verification

Password:

c.       第一個密碼是你為**line con 0** 設定的主控台密碼。輸入密碼切換到 user 模式。

d.       下指令切換到 enable模式。

e.       輸入enable模式的密碼（第2組）。

f.         檢視執行設定檔的設定值：

S1# **show running-config**

注意主控台和啓用密碼都是明文形式。如果有人在你後面，可能存在安全風險。

第 6 步：     設定加密密碼可保護對特權模式的存取。

**啓用密碼**應使用 **enable secret**命令替換為新的加密密碼。將啓用加密密碼設定為 **itsasecret**。

S1# **config t**

S1(config)# **enable secret itsasecret**

S1(config)# **exit**

S1#

**注意**：**啓用加密**密碼將覆蓋**啓用**密碼。如果兩者均在交換器上設定，必須輸入**啓用加密**密碼才能進入特權 EXEC 模式。

第 7 步：     檢驗啓用加密密碼是否已增加到設定檔。

a.       再次輸入 **show running-config**命令，檢驗新的**啓用加密**密碼是否已設定。

**注意：**你可以將**show running-config** 縮寫為

S1# **show run**

b.       **啓用加密**密碼顯示什麼？

c.       為什麼顯示的**啓用加密**密碼與我們設定的不同？

第 8 步：     加密啓用密碼和主控台密碼。

正如你在第 7 步所看到的，**啓用加密**密碼已加密，但**啓用**密碼和**主控台**密碼仍然以明文形式顯示。現在我們使用 **service password-encryption**命令將這些明文密碼加密。

S1# **config t**

S1(config)# **service password-encryption**

S1(config)# **exit**

如果你在交換器上設定其他密碼，它們將在設定檔中顯示明文形式還是加密形式？請說明理由。

第 3 部分: 設定 MOTD 標語

第 1 步：     設定當日訊息 (MOTD) 標語。

Cisco IOS 命令集中包含一項功能，用於設定登錄到交換器的任何人看到的訊息。這些訊息稱為當日訊息 (MOTD) 標語。應將標語文字括在引號中，也可以使用其他分隔字元，但分隔字元不能與 MOTD 字串中出現的任何字元相同。

S1# **config t**

S1(config)# **banner motd "This is a secure system. Authorized Access Only!"**

S1(config)# **exit**

%SYS-5-CONFIG\_I: Configured from console by console

S1#

* 什麼時候顯示標語？為什麼每台交換器都應該有 MOTD 標語？

第 4 部分: 將設定檔儲存到 NVRAM

第 1 步：     使用 show run 命令檢驗設定是否準確。

第 2 步：     儲存設定檔。

你已經完成交換器的基本設定。現在將執行設定檔案備份到 NVRAM，以確保所做的更改在系統重新開機或斷電時不會遺失。

S1# **copy running-config startup-config (以前舊指令write / wr 也可以用)**

Destination filename [startup-config]?**[Enter]**

Building configuration...

[OK]

* **copy running-config startup-config** 命令最短可以縮寫成什麼？

第 3 步：     檢查啟動設定檔。

那條命令將顯示 NVRAM 的內容？

檔案中記錄了之前輸入的所有變更嗎？

第 5 部分: 設定 S2

使用以下參數設定 S2：

a.       設備名稱：**S2**

b.       使用**letmein** 密碼保護主控台存取。

c.       設定啓用密碼 **c1$c0**和啓用加密密碼**itsasecret**。

d.       使用以下訊息設定登錄交換器時顯示的訊息：

Authorized access only. Unauthorized access is prohibited and violators will be prosecuted to the full extent of the law.

e.       加密所有純文字密碼。

f.         確保設定正確。

g.       如果交換器斷電，儲存設定檔以免遺失。