# LAN設計

## 無邊界交換網路的設計

建立原則：

* **階層式** - 有助於理解各層中每個裝置的作用，簡化部署、營運和管理，並減少各層的故障網域
* **模組化** - 根據需要實作無縫的網路擴張和整合服務的啟動

多層交換 / 路由器

* **恢復力** - 滿足使用者對保持網路始終運行的期望
* **靈活性** - 藉由使用所有網路資源來提供智慧流量負載分擔

### 存取層

存取層代表網路邊緣，流量將從這裡進出園區網路。傳統上，存取層交換器的主要功能是為使用者提供網路存取。存取層交換器與分布層交換器連線，分布層交換器實作網路基礎技術，如路由、服務品質和安全。

為了滿足網路應用程式和使用者的需求，現在下一代交換平台在網路邊緣向各種類型的端點提供更多統合、整合和智慧服務。建立智慧進入存取層交換器中，使應用程式能夠在網路上更加有效率且安全地執行。

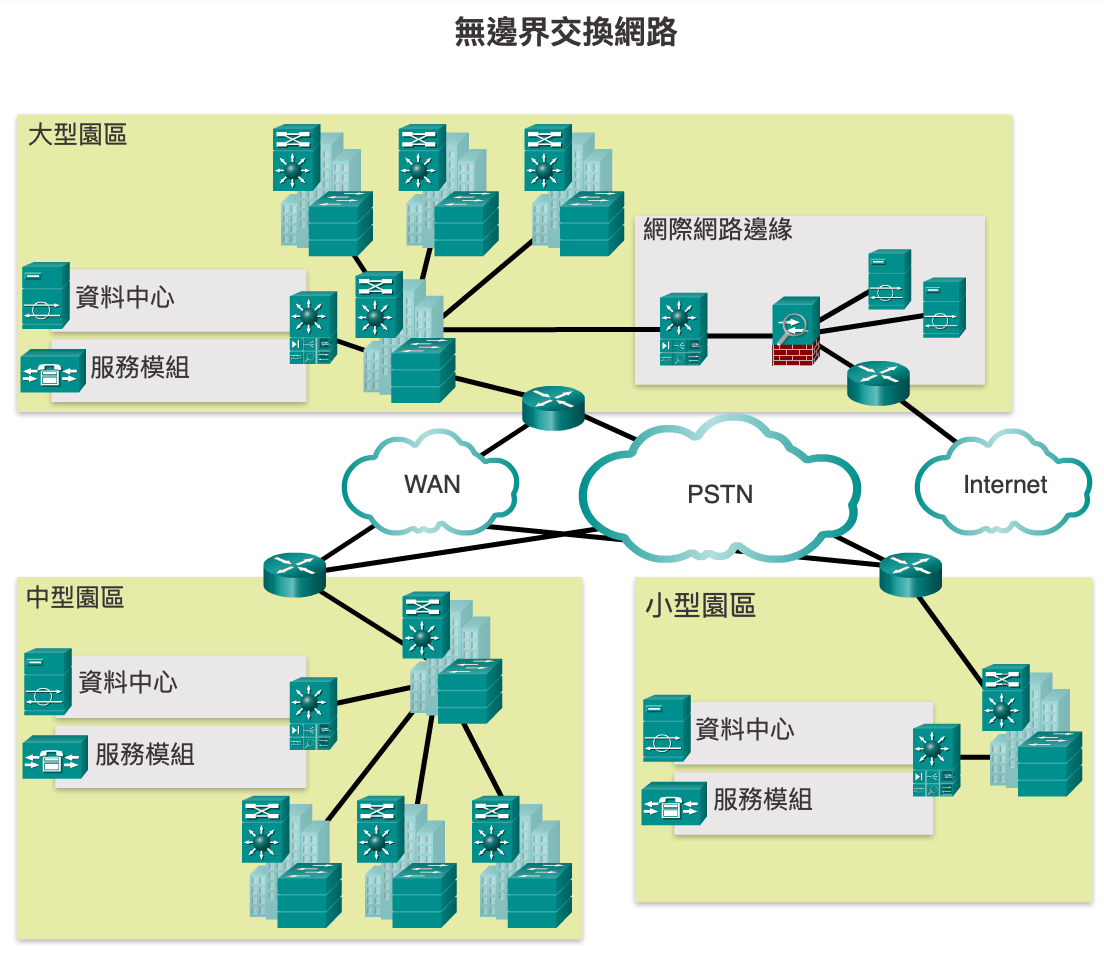
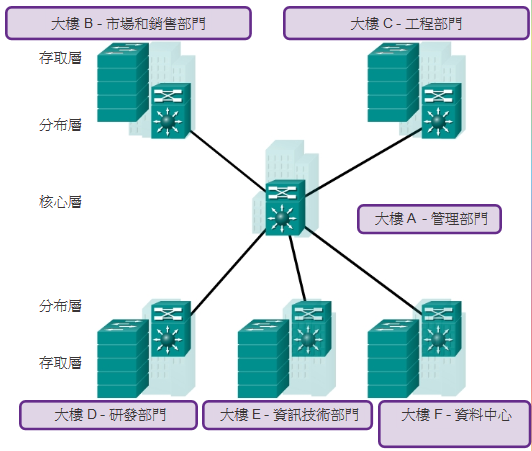
### 分布層

在存取層和核心層之間的分布層介面可以提供很多重要功能，包括：

* 匯集大規模的配線間網路
* 匯集第 2 層廣播領域和第 3 層路由邊界
* 提供智慧交換、路由和網路存取政策功能來存取網路的其餘部分
* 藉由連向使用者的備援分布層交換器和通往核心層的等價路徑提供高可用性
* 在網路邊緣為各種類別的服務應用提供差別服務

### 核心層

核心層是網路骨幹。它連線園區網的多個層。核心層充當其他所有園區區塊的整合者，並將園區和網路的其餘部分連接起來。核心層的主要用途是提供故障隔離和高速骨幹連線。



## 交換網路

### 選擇交換器的考量

* **成本** - 交換器的成本取決於介面的數量和速度、支援功能和延伸功能。
* **連接埠密度** - 網路交換器必須支援網路中合適數量的裝置。
* **電源** - 透過乙太網路供電為存取點、IP 電話，甚至緊湊型交換器供電現在都很常見。除了考慮使用 PoE 外，一些機殼式交換器支援備援電源。
* **可靠性** - 交換器應提供對網路的持續存取。
* **連接埠速度** - 網路連線的速度是使用者關注的主要問題。
* **訊框緩衝區** - 對於可能存在通往伺服器或網路其他區域的壅塞連接埠的網路中，交換器儲存訊框的能力非常重要。
* **可延伸性** - 網路中的使用者數量通常隨時間增加；因此，交換器應提供成長的可能。

## 訊框轉發

### 動態填充交換器 MAC 位址表

交換器獲知連接埠與裝置的關係後，就會構建一個 MAC 位址表或內容可定址記憶體 (CAM) 表。CAM 是一種特殊類型的記憶體，用於高速搜尋的應用。

交換器根據來源 MAC 位址填充 MAC 位址表。當交換器收到一個傳入的訊框，而其目的 MAC 位址在 MAC 位址表中找不到時，交換器會將該訊框轉發到除作為該訊框入口的連接埠之外的所有連接埠（泛洪）。當目的裝置作出回應時，交換器會將訊框的來源 MAC 位址和接收該訊框的連接埠增加到 MAC 位址表中。在多台交換器互連的網路中，MAC 位址表將包含與其他交換器連線的每個連接埠的多個 MAC 位址。

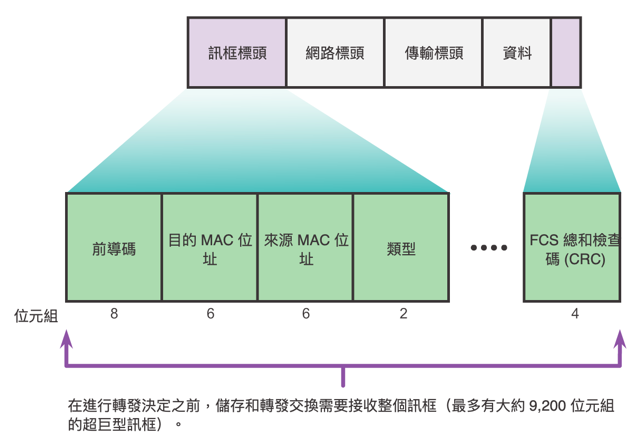
以下步驟描述了構建 MAC 位址表的過程：

1. 交換器在連接埠 1 上收到來自 PC 1 的訊框。
2. 交換器將檢查來源 MAC 位址並與 MAC 位址表進行比較。

* 如果位址不在 MAC 位址表中，它會在 MAC 位址表中將 PC1 的來源 MAC 位址與入口連接埠（連接埠 1）相對應。
* 如果 MAC 位址表中已經有該來源位址的對應條目，則它將重置老化計時器。MAC 位址條目通常可以保持五分鍾。

1. 在記錄了來源位址資訊後，交換器將檢查目的 MAC 位址。
   * 如果目的位址不在 MAC 表中，或者它是一個廣播 MAC 位址（以全 F 表示），則交換器會將該訊框泛洪到除入口連接埠以外的所有連接埠。
2. 目的裝置 (PC 3) 為了回應此訊框，發出目的位址為 PC 1 的單點傳送訊框。
3. 交換器將 PC 3 的來源 MAC 位址和入口連接埠的連接埠號輸入到位址表中。訊框的目的位址及其關聯的出口連接埠可在 MAC 位址表中找到。
4. 交換器現在無需泛洪即可在這些來源裝置和目的裝置之間轉發訊框，因為位址表中已經有了標識關聯連接埠的條目。

### 交換器轉發方法

* 儲存轉發交換

儲存轉發交換有兩個主要特徵使其區別於捷徑交換：錯誤檢查和自動緩衝。

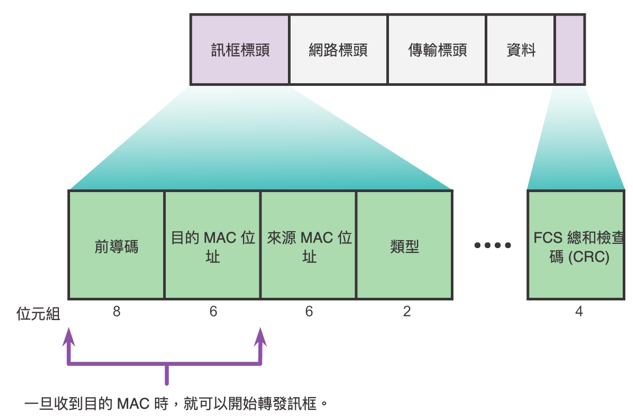
* + **錯誤檢查**：使用儲存轉發交換的交換器對傳入的訊框執行錯誤檢查。如圖所示，在入口連接埠收到整個訊框後，交換器將封包最後一個欄位中的訊框檢查序列 (FCS) 值與其自身的 FCS 計算進行比較。FCS 是一個錯誤檢查過程，有助於確保訊框中沒有實體和資料鏈結錯誤。如果訊框中沒有錯誤，則交換器會轉發訊框。否則，該訊框將被丟棄。
  + **自動緩衝**：儲存轉發交換器使用入口連接埠緩衝程序以靈活支援任意組合的乙太網路速度。例如，處理進入 100 Mb/s 乙太網路連接埠而必須從 1 Gb/s 介面發送出去的傳入訊框時將要求使用儲存轉發方法。如果入口連接埠和出口連接埠的速度不匹配，則交換器會將整個訊框儲存在緩衝區，計算 FCS 檢查，將其轉發到出口連接埠緩衝區，然後將其發送出去。

儲存轉發交換是思科主要的 LAN 交換方法。

儲存轉發交換器將丟棄未透過 FCS 檢查的訊框，因此並不轉發無效訊框。相反，捷徑交換器可能會轉發無效訊框，因為它並不執行 FCS 檢查。

網路環境內只使用switch，不使用 hub，則環境內不會發生碰撞，就可以使用捷徑交換，提升網速

* 捷徑交換

捷徑交換的一個優點就是使交換器開始轉發訊框的時間比儲存轉發交換早。捷徑交換有兩個主要特徵：快速訊框轉發和無碎片。

* + **快速訊框轉發**：使用捷徑交換方法的交換器一旦在其 MAC 位址表中查出訊框的目的 MAC 位址，就會做出轉發決策。交換器在執行轉發決策前不必等待訊框的其餘部分進入入口連接埠。  
    如今透過 MAC 控制器和 ASIC，使用捷徑交換方法的交換器可以迅速確定是否需要檢查訊框標頭的更多部分以進行另外的過濾。例如，交換器可以分析之前的前 14 個位元組（來源 MAC 位址、目的 MAC 和 EtherType 欄位），並檢查另外的 40 個位元組以便執行與 IPv4 第 3 層和第 4 層有關的更複雜的功能。  
    捷徑交換方法不會丟棄大多數無效訊框。有錯的訊框將轉發到網路的其他網段。如果網路中的錯誤率（無效訊框）很高，則捷徑交換會對帶寬頻來負面影響；所以頻寬被損壞和無效的訊框阻塞。
  + **無碎片**：無碎片交換是一種經過改良的捷徑交換，在這種交換方式中交換器在轉發訊框之前將等待碰撞視窗（64 個位元組）通過。這意味著對每個訊框的資料欄位都會進行檢查以確保不出現碎片。比起捷徑，無碎片模式能夠提供更好的錯誤檢查，而且幾乎不會增加延遲。  
    由於捷徑交換低延遲的速度優勢，它更適合要求程序到程序的延遲不大於 10 毫秒的極其嚴苛的高效能計算 (HPC) 應用。

## 交換網域

### 碰撞領域及廣播領域

將網路劃分為網段，以減少競爭頻寬的裝置數量；每個新網段將形成新的碰撞領域。網段中有更多的頻寬可供裝置使用，而且一個碰撞領域中的碰撞不會干擾其他網段。這也就是我們所說的微分段。

Switch 的每個 port 都是獨立的

交換器的每個連接埠都代表一個單獨的碰撞領域。

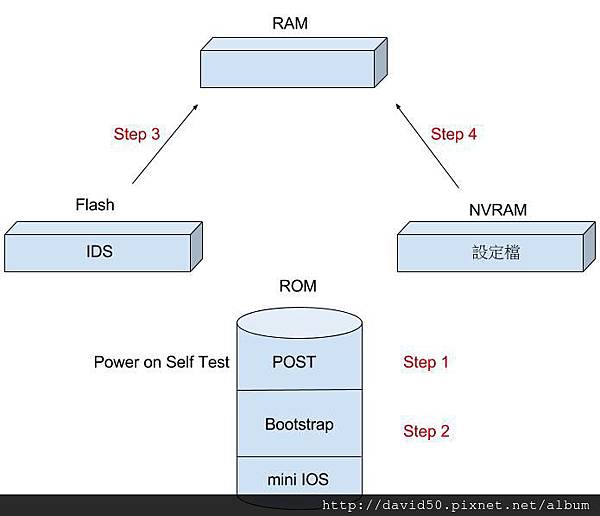
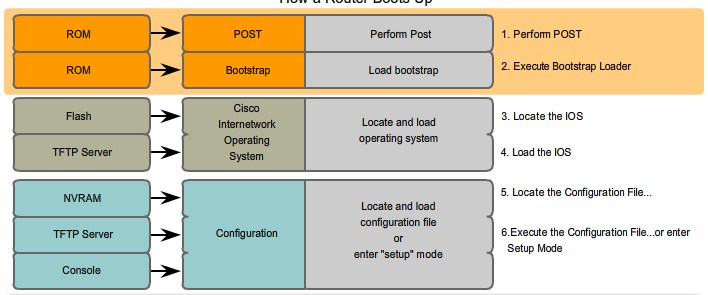
並且，交換器提供裝置之間全雙工通訊，可以同時承載發送和接收的訊號，能顯著提高 LAN 網路效能，對於 1 Gb/s 或更高的乙太網路速度是必需的。

碰撞會造成訊框長度改變

# 交換的概念及設定

## 基本設定

### switch啟動順序

switch 開機啟動順序：

* 1. 執行ROM 中的開機自我測試 (POST, Power On Self Test) 程式，確認各元件是否正常
     + DRAM
     + Flash Memory
     + Switch CPU
     + System Board
     + CPU Interface ASIC
     + Switch Core ASIC
     + Ethernet Controller ASIC
     + Ethernet Interfaces
     + 註：ASIC = Application-Specific Integrated Circuit
  2. 載入Bootstrap（啟動載入器，存在 ROM 中）啟動載入器執行低階 CPU 初始化。啟動載入器初始化 CPU 暫存器，暫存器控制實體記憶體的對映位置、記憶體量以及記憶體速度。啟動載入器初始化系統主機板上的快閃記憶體檔案系統。bootstrap 程式的主要任務是查詢 Cisco IOS 並將其載入到 RAM。開機區程式儲存於唯讀記憶體 ROM 中，他會到 Flash Memory 或 TFTP 去尋找 Cisco IOS 軟體來載入；若找不到IOS檔案，則執行mini IOS，進入ROM Monitor模式。
  3. 最後，啟動載入器尋找並將預設 IOS 作業系統軟體映像載入到記憶體，並將對交換器的控制權交給 IOS。載入IOS後，IOS會到 NVRAM (Non-Violatile Random Access Memory )去找 startup config，然後將 startup-config 複製到 RAM 中成為 running-config，接著執行 running-config 設定項目；若 startup-config 不在 NVRAM 中 （從未設定或設定遺失），Router 會透過所有介面去找尋 TFTP Server 找設定檔，若還是找不到則進入設定模式（Setup Mode）。

啟動載入器發現交換器的 Cisco IOS 映像如下：交換器嘗試使用 BOOT 環境變數中的資訊自動啟動。如果沒有設定此變數，則交換器嘗試透過在快閃記憶體檔案系統中執行遞迴的深度優先搜尋來載入並執行第一個可執行檔案。在目錄的深度優先搜尋中，在繼續來源目錄中的搜尋之前，對遇到的每個子目錄都會進行完全搜尋。在 Catalyst 2960 系列交換器上，映像檔案通常包含在與映像檔案同名（不包括 .bin 副檔名）的目錄中。

然後 IOS 作業系統使用設定檔（儲存在 NVRAM 中的啟動設定）中找到的 Cisco IOS 命令初始化介面。

一張含有 文字 的圖片

自動產生的描述一張含有 文字 的圖片

自動產生的描述  使用 **boot system** 全域設定模式命令設定 BOOT 環境變數。注意，IOS 位於一個不同的資料夾中，而且資料夾路徑已指定。使用 **show bootvar** 命令（在更早的 IOS 版本中使用 **show boot**）來檢視目前 IOS 啟動檔案的設定。

### 當機的恢復

如果由於系統檔案遺失或損壞而使作業系統不能使用，則啟動載入器將提供對交換器的存取。啟動載入器有一個命令列，可以提供對快閃記憶體中儲存的檔案的存取。透過主控台連線按照以下步驟存取啟動載入器：

**第 1 步**： 透過主控台纜線將 PC 連線到交換器主控台連接埠。設定終端機模擬軟體，使其連線到交換器。

**第 2 步**： 拔下交換器電源線。

**第 3 步**： 將電源線重新連線到交換器，在 15 秒鍾內按住“**模式**”按鈕不放，此時“系統”LED 仍呈綠色閃爍。

**第 4 步**： 繼續按住“**模式**”按鈕，直到“系統”LED 先後呈短暫的琥珀色和穩定的綠色；然後鬆開“**模式**”按鈕。

**第 5 步**： 啟動載入器的 **switch:** 提示字元會顯示在 PC 上的終端機模擬軟體

一張含有 文字 的圖片

自動產生的描述**啟動載入器**命令列支援用於格式化快閃記憶體檔案系統、重新安裝作業系統軟體和恢復已遺失或已忘記密碼的命令。例如，**dir** 命令可用於檢視指定目錄中的檔案清單（如圖所示）。

**注意**：注意在本範例中，IOS 位於快閃記憶體資料夾的根中。

### Switch 的指示燈

一張含有 螢幕擷取畫面, 室外, 街道, 停車 的圖片

自動產生的描述

網路供電

不亮： 10Mb/s

綠燈：100Mb/s

閃綠：1000Mb/s

備援電源系統

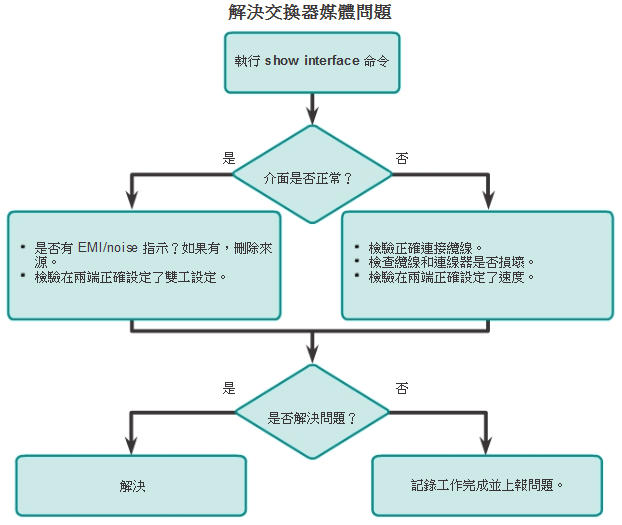
### 基本管理

|  |  |  |  |
| --- | --- | --- | --- |
| 項次 | 步驟 | 指令 | 說明 |
| 1. 設定管理介面 | 進全域設定模式  進 SVI 介面設定模式  設定 IP  啟用介面 | S1# **configure terminal**  S1(config)# i**nterface vlan** *99*  S1(config-if)# **ip address** *127.17.99.11 255.255.255.0*  S1(config-if)# **no shutdown** | VLAN 的操作，CCNA 必考  在交換器的管理 SVI 上透過 VLAN 介面設定模式設定 IP 位址和子網路遮罩 |
| 使用 vlan\_id 99 新增 VLAN 並將其與介面相關聯 | S1(config)# **vlan** *vlan\_id*  S1(config-vlan)# **name** *vlan\_name*  S1(config-vlan)# **exit**  S1(config)# **interface** *interface\_id*  S1(config-if)# **switchport access vlan** *vlan\_id* | 只有新增了 VLAN 99 並且有裝置連線到與 VLAN 99 關聯的交換器連接埠時 VLAN 99 的 SVI 才會顯示為“up/up”。 |
| 1. 設定預設匣道 | 進全域設定模式  設定預設匣道的 IP | S1# **configure terminal**  S1(config)# **ip default-gateway** *127.17.99.1* | 如果要透過 internet 遠端管理交換器，應該要幫交換器設定預設閘道。預設閘道是與交換器連線的路由器。交換器會把本地區網以外的目的 IP 封包轉發到預設閘道。 |
| 1. 檢查設定 | 確定實體介面和虛擬介面的狀態 | S1# **show ip interface brief** |  |

### 在實體層設定交換器連接埠

|  |  |  |  |
| --- | --- | --- | --- |
| 項次 | 步驟 | 指令 | 說明 |
| 設定雙工和速度 | 進全域設定模式  進介面設定模式  設定介面雙工  設定介面速度 | S1# **configure terminal**  S1(config)# **interface** *fastethernet0/1*  S1(config-if)# **duplex** *full*  S1(config-if)# **speed** *100* | 雙工模式要對接的2台機器設定都相同才行，不然就會以最低的設定為主。  例：switch + hub : 半雙工  速度設定不同會強制斷線  預設值都是 auto，手動設定表示不再偵測 |
| 檢驗auto-MDIX | 進全域設定模式  進介面設定模式  介面雙工設定為自動  介面速度設定為自動  MDIX設定為自動 | S1# **configure terminal**  S1(config)# i**nterface** *fastethernet0/1*  S1(config-if)# **duplex auto**  S1(config-if)# **speed auto**  S1(config-if)# **mdix auto** | 網路線有分直通及交叉，而現今的switch大都有自動偵測並設定的功能；啟用 auto-MDIX 功能後，介面就會自動檢測；當在介面上使用 auto-MDIX 時，介面速度和雙工必須設定為“auto”，這樣該功能才能正常執行。 |
| 檢查設定 | 顯示**MDIX**設定 | S1# **show controller Ethernet-controller** *fa 0/1* **phy | include Auto-MDIX** | 要檢查某個特定介面的 Auto-MDIX 設定，用 show controllers ethernet-controller 命令和關鍵字 phy。限定輸出為有Auto-MDIX 的行用 include Auto-MDIX 過濾器，顯示畫面如下所示：  Auto-MDIX : on [AdminState=1 Flags=0x00056248] |
| 顯示介面設定 | S1# **show interface** *[interface-id]* |  |
| 顯示介面 IP | S1# **show ip** *[interface-id]* |  |
| 顯示開機設定 | S1# **show startup-config** |  |
| 顯示當前設定 | S1# **show running-config** |  |
| 顯示快閃記憶體檔案內容 | S1# **show flash** |  |
| 顯示軟、硬體版本狀態 | S1# **show version** |  |
| 顯示歷史指令 | S1# **show history** |  |
| 顯示 MAC 位址表 | S1# **show mac address-table**  OR  S1# **show mac-address-table** |  |

|  |
| --- |
| 最大傳輸單位(MTU, maximum transmission unit)、頻寬(BW，bandwidth，要注意它的單位是kbit哦)、可靠度(reliability 255/255，其中的255/255為1表示良好)、負載(txload 1/255, rxload 1/255, 其中的1/255表示負載很小)  延遲碰撞是指在傳輸了 512 位元的訊框之後發生碰撞。最常見原因是纜線過長、或是串接太多台 switch。另一個常見原因是雙工設定錯誤。UTP雙絞線傳輸距離最多100M  collisions 表示有發生碰撞，switch 下的連接埠應該不會有，如果有可能是有串接 hub 所致。  干擾源  巨人封包 >4500bit  侏儒封包 <64bit  接收  傳輸  Level 2 |

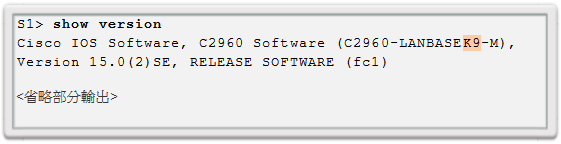


CCNA 目前為全選擇題，其中有1/5是考故障排除

Level 1

# 交換器安全與管理

## 安全遠端存取

* Telnet 是一種較早協定，對登入驗證（使用者名和密碼）和通訊裝置之間傳輸的資料都採用不安全的明文傳輸。攻擊者可以使用 Wireshark 監控封包。
* 安全外殼 (SSH) 是一種提供遠端裝置的安全（加密）管理連線的協定。應使用 SSH來替代 Telnet 連線。IOS版本訊息需包含“k9”才有支援。可show version 命令檢視交換器目前執行的 IOS 版本。

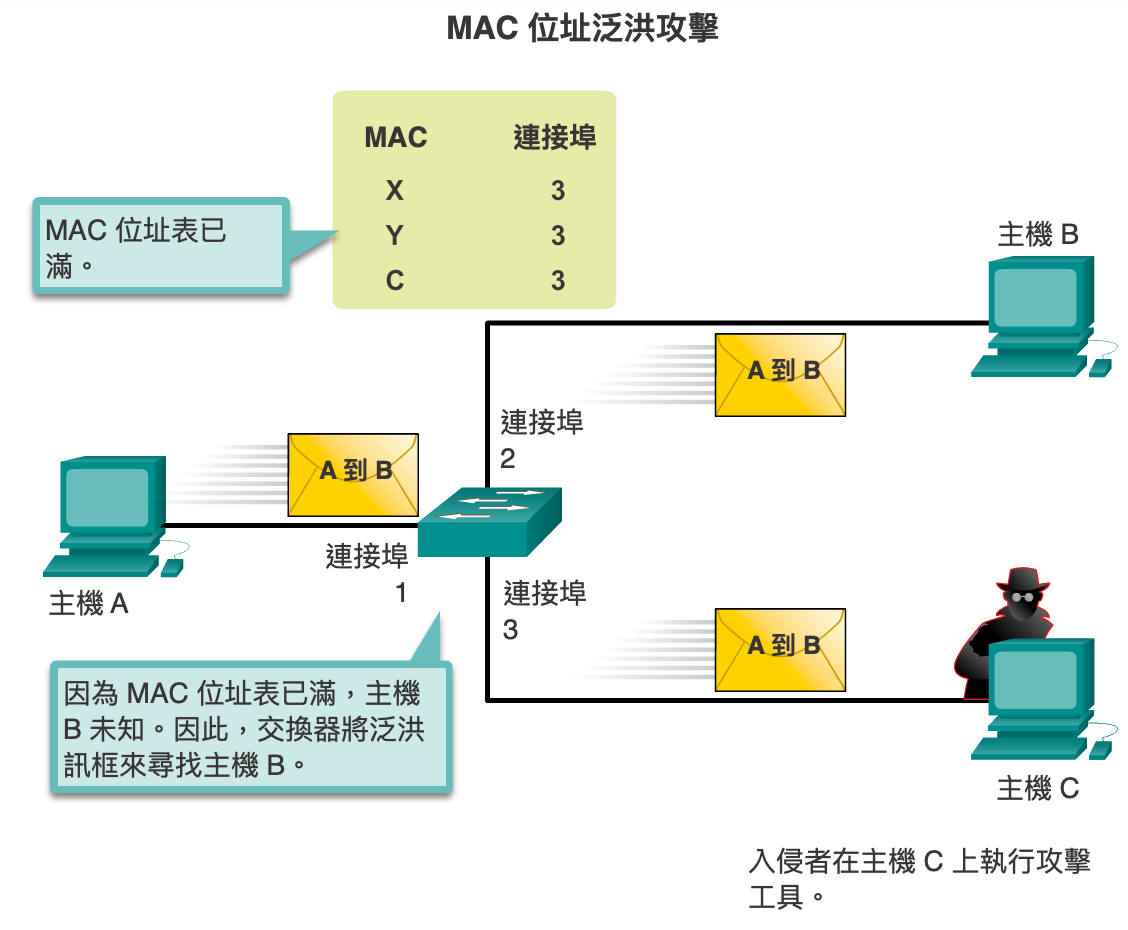
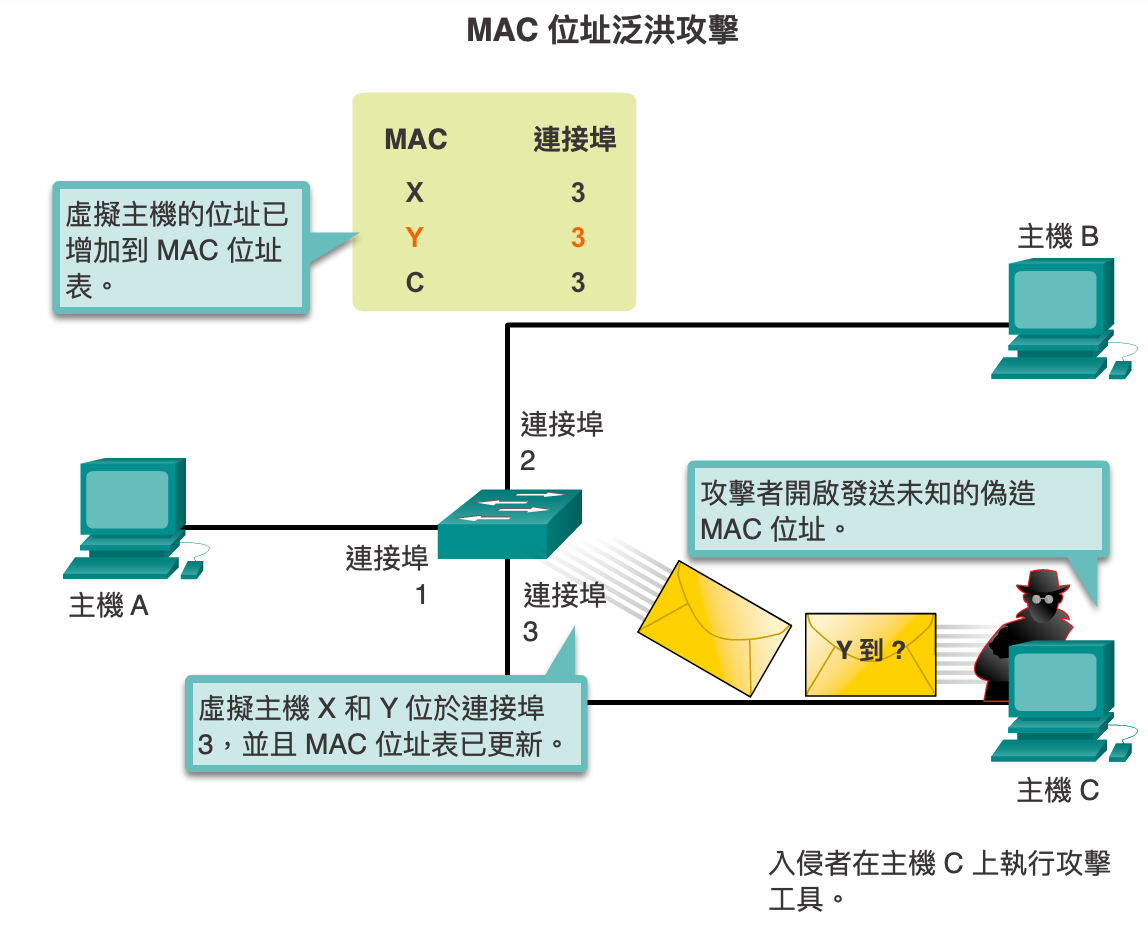
### 設定使用 SSH

|  |  |  |  |
| --- | --- | --- | --- |
| 項次 | 步驟 | 指令 | 說明 |
| 檢驗是否支援 SSH | 顯示IP SSH設定 | S1# **show ip ssh** | 如果交換器沒有執行支援加密功能的 IOS，則此命令將無法識別。 |
| 設定網域名稱 | 進全域設定模式  設定IP 網域名稱 | S1# **configure terminal**  S1(config)# **ip domain-name** *domain-name* |  |
| 產生 RSA 金鑰對 | 產生 RSA 金鑰對 | S1(config)# **crypto key generate rsa** | 產生 RSA 金鑰對將自動啟用 SSH時，系統會提示輸入模數長度。思科建議模數大小至少為 1024 位元  註：要刪除 RSA 金鑰對，請使用 crypto key zeroize rsa 全域設定模式命令。刪除 RSA 金鑰對之後，SSH 伺服器將自動停用。 |
| 設定使用者驗證 | 新增使用者帳密 | S1(config)# **username** *username* **secret** *password* |  |
| 設定 vty 線路 | 進 vty 線路設定模式  將連線導入SSH 協定  設定限用本地使用者帳密驗證 | S1(config)# **line vty** *0 15*  S1(config-line)# **transport input ssh**  S1(config-line)# **login local**  S1(config-line)# **exit** | Catalyst 2960 的 vty 線路範圍為 0 到 15。該設定將阻止除 SSH 之外的連線（如 Telnet），將交換器限制為僅接受 SSH 連線。使用 line vty 全域設定模式命令，然後使用 login local 線路設定模式命令來要求從本地使用者名資料庫進行 SSH 連線的本地驗證。 |
| 啟用 SSH 第 2 版 | 啟用 SSH 第 2 版 | S1(config-line)# **ip ssh version 2** | 預設情況下，SSH 同時支援第 1 版和第 2 版。如果支援兩種版本，在 show ip ssh 輸出中將顯示為支援版本 1.99。第 1 版存在已知漏洞。因此，建議只啟用第 2 版。  RSA 金鑰對配合第 2 版使用 1024 位元 |

## 常見攻擊

### MAC 泛洪

交換器對未知位址的 MAC 位址泛洪行為可被用來攻擊交換器。這種類型的攻擊稱為 MAC 位址表溢位攻擊。MAC 位址表溢位攻擊有時也稱為 MAC 泛洪攻擊和 CAM 表溢位攻擊。

緩解 MAC 位址表溢位攻擊的一種方法就是設定連接埠安全。

### DHCP 欺騙

對交換網路可以執行兩種類型的 DHCP 攻擊：DHCP 耗竭攻擊和 DHCP 欺騙。

* 在 DHCP 耗竭攻擊中，攻擊者將使用 DHCP 請求泛洪 DHCP 伺服器，以耗盡 DHCP 伺服器可以發出的所有可用 IP 位址。在發出這些 IP 位址後，伺服器無法發出更多位址，這種情況將導致新的客戶端不能獲得網路存取權限，所以實作阻斷服務 (DoS) 攻擊。DoS 攻擊是任何使用非法流量過載特定裝置和網路服務，所以阻止合法流量存取這些資源的攻擊。
* 在 DHCP 欺騙攻擊中，攻擊者在網路中設定虛假的 DHCP 伺服器向客戶端發出 IP 位址。這種攻擊的常見原因是強迫客戶端使用錯誤的網域名稱系統 (DNS) 或 Windows Internet 命名服務 (WINS) 伺服器並且使客戶端使用攻擊者或受攻擊者控制的電腦作為其預設閘道。

通常在 DHCP 欺騙攻擊之前會使用 DHCP 耗竭，以便對合法 DHCP 伺服器阻斷服務，使其更容易將虛假的 DHCP 伺服器引入網路。

### 利用CDP

思科發現協定 (CDP) 是思科專有協定，所有思科裝置都可設定為使用該協定。CDP 可以發現直接相連的其他思科裝置，這將允許裝置自動設定其連線。在某些情況下，這樣可以簡化設定和連線。

預設情況下，大多數思科路由器和交換器在所有連接埠上都啟用了 CDP。CDP 資訊會定期以未加密的廣播形式發送。該資訊會在每台裝置的 CDP 資料庫中進行本地更新。由於 CDP 是第 2 層協定，因此路由器不會傳播 CDP 訊息。

CDP 包含有關裝置的資訊，如 IP 位址、IOS 軟體版本、平台、效能和原生 VLAN。攻擊者會利用此資訊找到攻擊網路的方法，通常會採用阻斷服務 (DoS) 攻擊的形式。

透過 CDP 發現的 Cisco IOS 軟體版本特別有利於攻擊者確定該特定版本的 IOS 是否有任何特有的安全漏洞。此外，因為 CDP 不進行驗證，所以攻擊者可以偽造 CDP 封包並將其發送到直連的思科裝置上。

建議你使用 **no cdp run** 全域設定模式命令在無需使用 CDP 的裝置或連接埠上停用 CDP。可以針對每個連接埠停用 CDP。

### Telnet 攻擊

Telnet 協定是不安全的，可被攻擊者用來遠端侵入思科網路裝置。攻擊者可以利用工具來對交換器的 vty 線路實作暴力密碼破解攻擊。

### 暴力密碼攻擊

暴力密碼攻擊的第一階段是攻擊者使用一個常用密碼清單和一個專門設計的程式，這個程式使用字典清單中的每一個詞來嘗試建立 Telnet 會談。如果在第一階段沒有發現密碼，則開始第二階段。在暴力攻擊的第二階段，攻擊者又使用一個程式，這個程式新增順序字母組合，試圖猜測密碼。只要有足夠的時間，暴力密碼攻擊可破解幾乎所有使用的密碼。

要緩解暴力密碼攻擊，可以使用強密碼並經常更改。強密碼應該使用大寫和小寫字母的組合，而且應包括數字和符號（特殊字元）。使用存取控制清單 (ACL) 也可以限制對 vty 線路的存取。

註：ACL 的用途是在核心骨幹上控制流量。

### Telnet DoS 攻擊

Telnet 也可以被用來發起 DoS 攻擊。在 Telnet DoS 攻擊中，攻擊者利用了交換器上所執行的 Telnet 伺服器軟體中的一個弱點，這個弱點可使 Telnet 服務不可用。此類攻擊阻止管理者遠端存取交換器管理功能。在攻擊期間，此類攻擊可能與網路中的其他直接攻擊一起來共同嘗試阻止網路管理者存取核心裝置。

解決 Telnet 服務中的 DoS 攻擊漏洞的常用辦法是使用 Cisco IOS 更新修訂版中附帶的安全性修正程式。

注意：最好用 SSH 而不是 Telnet 進行遠端管理連線。

## 交換器連接埠安全

### 關閉沒用的port

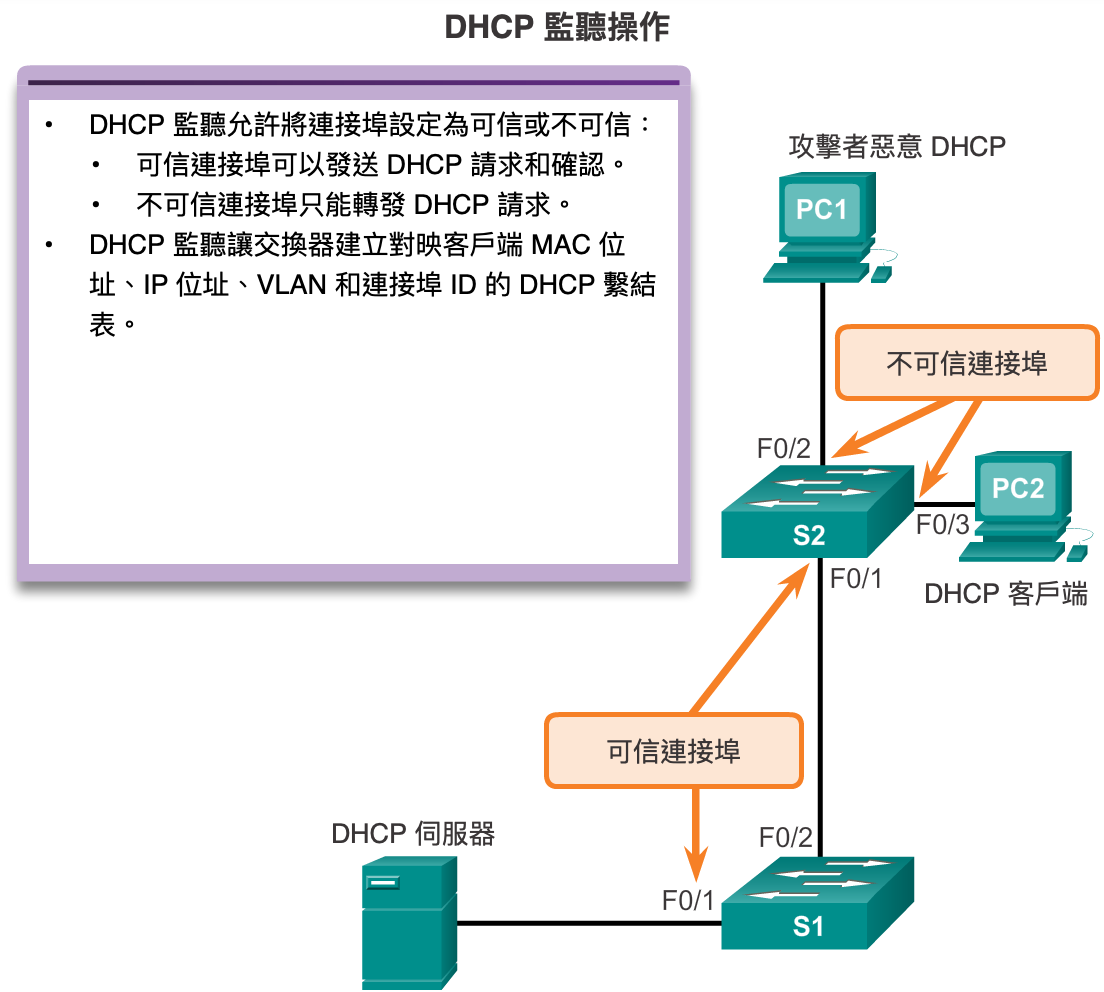
最簡單方法就是把交換器上所有沒在用的連接埠停用，這樣可以保護網路，避免未經授權的存取。

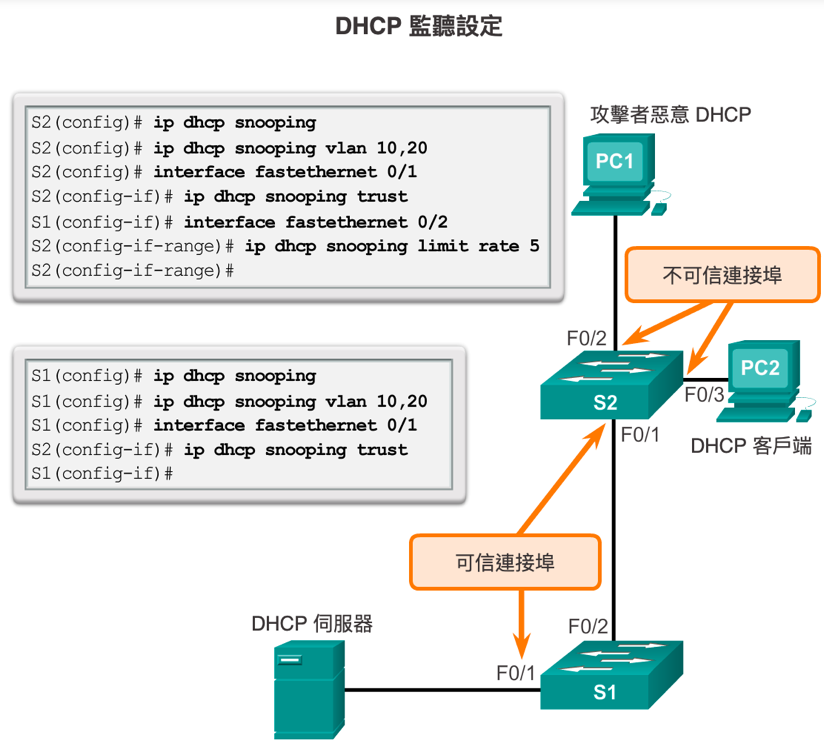
對交換器多個連接埠進行設定更改，可以用 interface range 指令。

Switch(config)# **interface range** *type module/first-number – last-number*

啟用和停用連接埠的過程比較耗時，但它可以加強網路安全，是值得付出的工作。

### DHCP 監聽



設定 DHCP 偵聽：

**第 1 步：** 使用 **ip dhcp snooping** 全域設定模式命令啟用 DHCP 偵聽。

**第 2 步：** 使用 **ip dhcp snooping vlan** *number* 命令對特定 VLAN 啟用 DHCP 偵聽。

**第 3 步：** 使用 **ip dhcp snooping trust** 命令定義可信連接埠，所以在介面級別將連接埠定義為可信。

**第 4 步：** （選擇性）使用 **ip dhcp snooping limit rate** *rate* 命令限制攻擊者透過不可信連接埠向 DHCP 伺服器連續發送偽造 DHCP 請求的速率。

### 連接埠安全：操作

一張含有 文字 的圖片

自動產生的描述一張含有 文字 的圖片

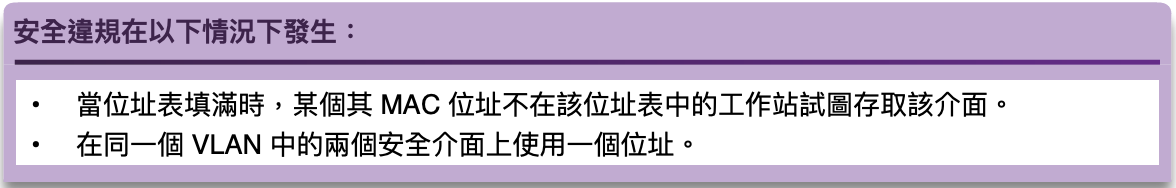
自動產生的描述

黏滯安全

安全位址的類型取決於設定，包括：

* **靜態安全**- 使用 **switchport port-security mac-address** *mac-address* 手動設定介面連接埠的白名單 MAC 位址。這裡的 MAC 位址會存在位址表中，並增加到交換器的執行設定中。
* **動態安全**- 透過動態獲取MAC 位址，並只存在位址表裡。這裡設定的 MAC 位址在交換器重新啟動時將被清除。
* **黏滯安全**- 可以透過動態獲取或手動設定MAC 位址，然後儲存到位址表中並增加到執行設定中。使用 **switchport port-security mac-address sticky** 指令。
  + 交換器會將所有動態獲取的 MAC 位址（包括在啟用黏滯獲取之前動態獲取的 MAC 位址）轉換為黏滯安全 MAC 位址。所有黏滯安全 MAC 位址都會增加到位址表和執行設定中。
  + 還可以手動定義黏滯安全 MAC 位址。使用 **switchport port-security mac-address sticky** *mac-address* 可以把所有指定位址都增加到位址表和執行設定中。
  + 把黏滯安全抓到的 MAC 位址存到啟動設定檔，就算交換器重啟或關閉介面，介面也都不用再重新抓位址。但如果沒有存，位址會不見。
  + no switchport port-security mac-address sticky 會停用黏滯安全，之前抓到的 MAC 位址仍會留在位址表裡，但執行設定裡不會留。
  + 注意，連接埠安全預設是關的，要用 switchport port-security 啟動才會運作。

### 連接埠安全：違規模式



安全違規模式有下列 3 種：

一張含有 桌 的圖片

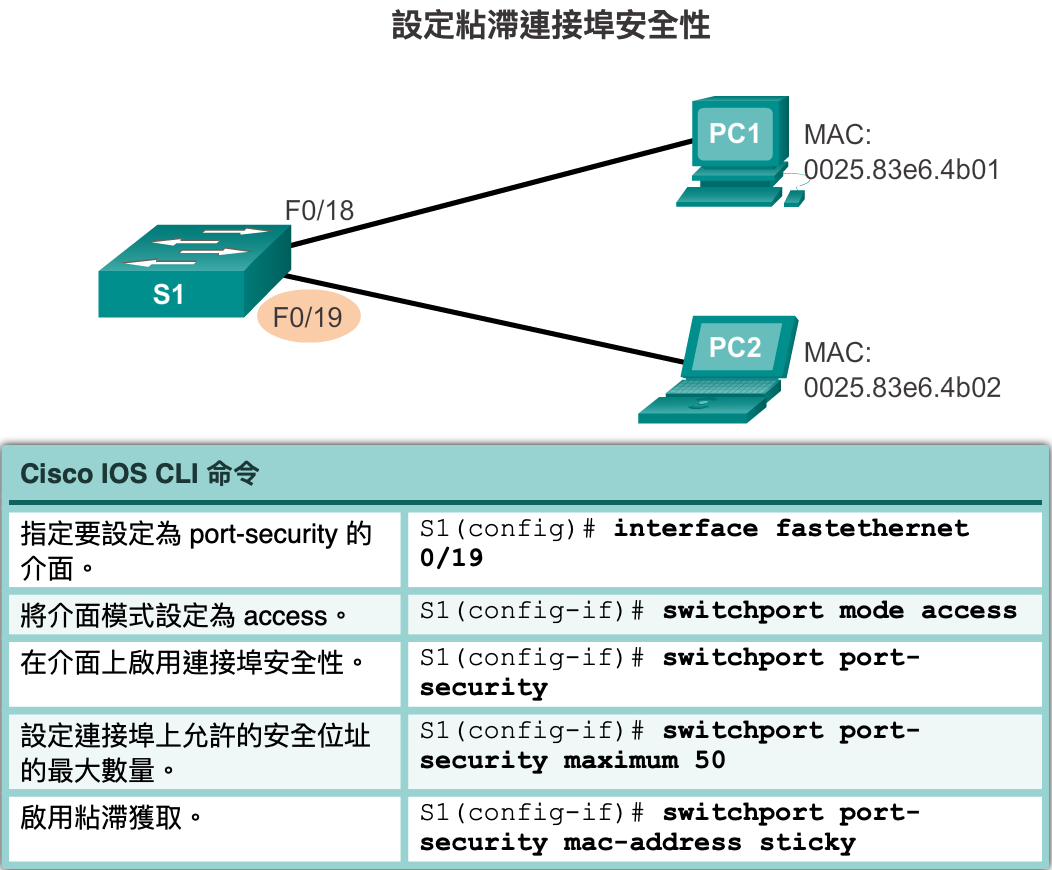
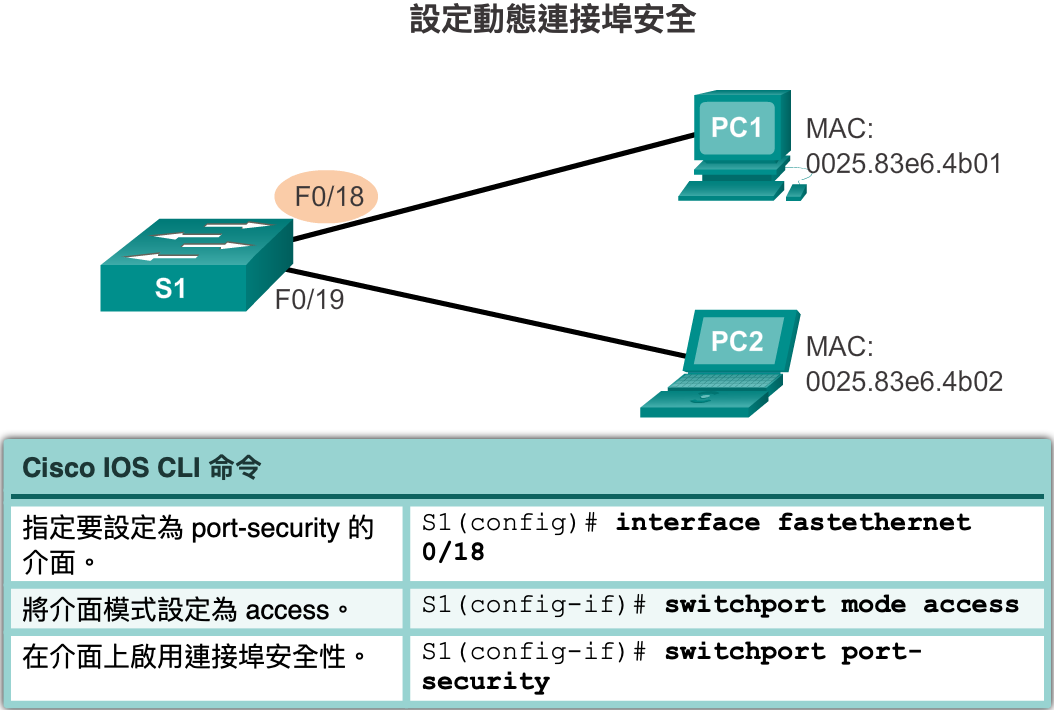
自動產生的描述

用 **switchport port-security violation** {**protect** | **restrict** | **shutdown**} 來設定交換器連接埠的違規模式。

### 連接埠安全：設定

交換器的預設連接埠安全設定。

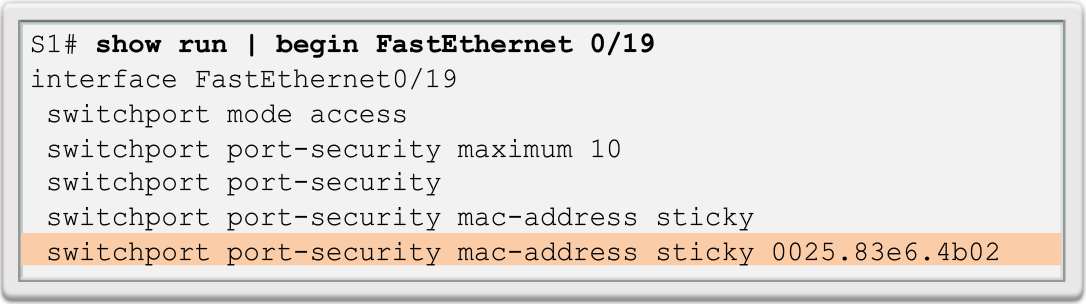
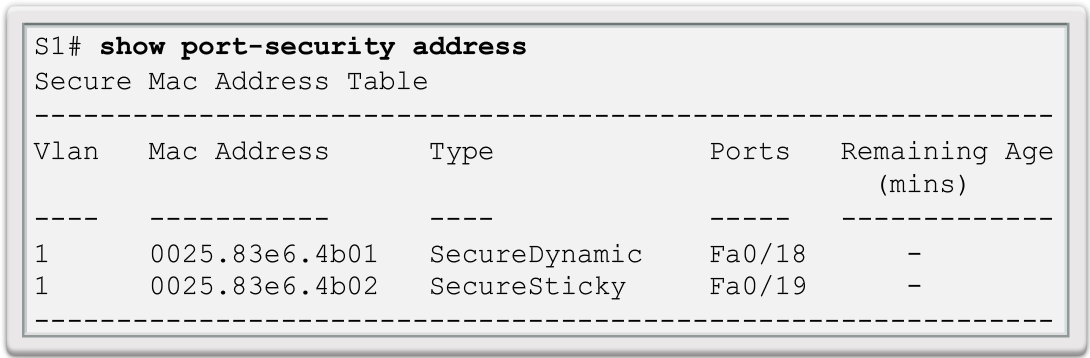
一張含有 桌 的圖片

自動產生的描述 

### 連接埠安全：檢查

一張含有 桌 的圖片

自動產生的描述 一張含有 桌 的圖片

自動產生的描述  

### 連接埠因為違規被錯誤停用

一旦設定了連接埠安全，使用者違規可能就會讓連接埠變為錯誤停用的狀態（實際上就是關的，這個連接埠不會發送或接收任何流量。

**一張含有 文字 的圖片

自動產生的描述注意**：連接埠協定和鏈路狀態變為關閉。



連接埠 LED 將被關掉。**show interfaces** 命令將連接埠狀態標識為 **err-disabled**。現在 **show port-security interface** 命令的輸出顯示介面狀態為 **secure-shutdown**。由於連接埠安全違規模式設定為關閉，因此出現安全違規的連接埠將進入錯誤停用狀態。一張含有 桌 的圖片

自動產生的描述

管理者應當在重新啟用連接埠之前確定導致安全違規的原因。如果有未經授權裝置連線到安全連接埠，則應當在安全威脅消除後再重新啟用連接埠。要重新啟用連接埠，請使用 **shutdown** 介面設定模式命令。一張含有 文字 的圖片

自動產生的描述然後，使用 **no shutdown** 介面設定命令使連接埠正常工作。

### 網路時間協定 (NTP)

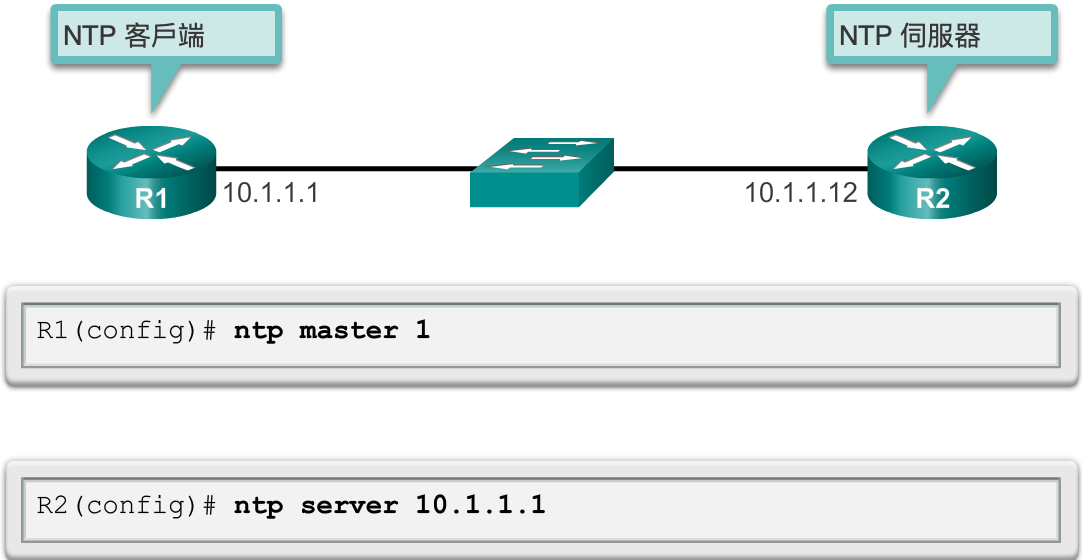
在網路中使用正確時間非常重要。需要使用正確時間戳記來精確追蹤網路事件（例如安全違規）。此外，時鐘同步對正確解讀系統日誌資料中的事件和數位憑證都非常重要。

網路時間協定 (NTP) 是一種用於跨封包交換、可變延遲資料網路以同步電腦系統時鐘的協定。NTP 可使網路裝置將其時間設定與 NTP 伺服器同步。從單一來源獲取時間和日期資訊的一組 NTP 客戶端的時間設定具有更高的一致性。

為網路提供時鐘的一種安全方法是，讓網路管理者利用衛星或無線電將其私有網路的主時鐘與 UTC 同步。但是，如果由於成本或其他原因，網路管理者不願實作自己的主時鐘，網路上還提供其他時鐘來源。NTP 可以從內部或外部時間來源獲得正確的時間，包括以下各項：

* 本地主時鐘
* 網路上的主時鐘
* GPS 或原子鍾

可將網路裝置設定為 NTP 伺服器或 NTP 客戶端。要允許 NTP 時鐘伺服器同步軟體時鐘，請在全域設定模式下使用 ntp server ip-address 命令。將路由器 R2 設定為 NTP 客戶端，而路由器 R1 充當權威 NTP 伺服器。



要將裝置設定為 NTP 主時鐘（供其他對等體與其同步），請在全域設定模式下使用 ntp master [stratum] 命令。層數的值是 1 到 15 之間的一個數，表示系統將要申請的 NTP 層數。如果將系統設定為 NTP 主裝置並且未指定層數，則會將其預設為第 8 層。如果 NTP 主裝置在較低層數上無法獲得任何時鐘，則系統會申請在已設定層數上進行同步，而且其他系統將希望使用 NTP 與其同步。

一張含有 文字 的圖片

自動產生的描述一張含有 文字 的圖片

自動產生的描述

要顯示 NTP 關聯的狀態，請在特權執行模式下使用 show ntp associations 命令。該命令將表示出同步到此對等體的任何對等裝置的 IP 位址、靜態設定的對等體以及層數。show ntp status 使用者執行命令可用於顯示此類資訊：NTP 同步的狀態、與該裝置同步的對等體以及裝置在那個 NTP 層上執行。