# VLAN 簡介

網路一般由遮罩來決定子網路的大小，區網內資料傳遞是直接傳送，要傳到外網的資料經預設匣道送出。

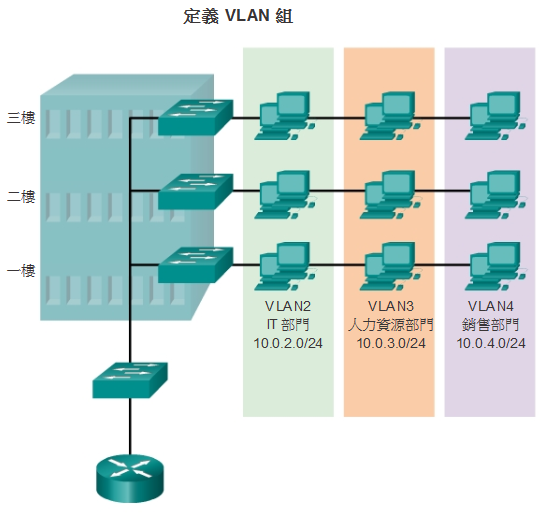
但要在區網內傳遞必須知道MAC才行，這就需要透過DHCP廣播才有辦法知道

廣播的動作由作業系統來處理，所以區域內廣播太多會影響到電腦的執行效能。

經過統計，區網內大約可以含70台電腦，效能是最好的。

24遮罩的區網有幾個 IP 可以用？扣除.0（第1個）是路由用的，以及.255（最後一個）是廣播用的，還有244個IP 可以用。

L3的設備（路由器，或稱第3層交換器）才能夠攔阻廣播。

現在有許多公司沒有固定的位置，那要怎麼去設計它的網路，才能不變動到實體裝備，又能夠區分不同部門的資料呢？透過VLAN來實現，把不同的網段接在同一個實體的裝備上。

VLAN在設計時，第1個考量是安全，將資料分隔開來，透過ACL來做，第2個是可以利用交換器其他的交換埠，降低實體裝備的成本，第3個是可以縮小廣播的領域，提高效能。

## VLAN的種類

### 預設VLAN

* 預設就有VLAN 1，不可以重新命名或刪除
* 預設原生VLAN是VLAN1
* 預設管理VLAN是VLAN1
* 除了VLAN 1，其他 VLAN 沒有 no shutdown。

### 資料VLAN

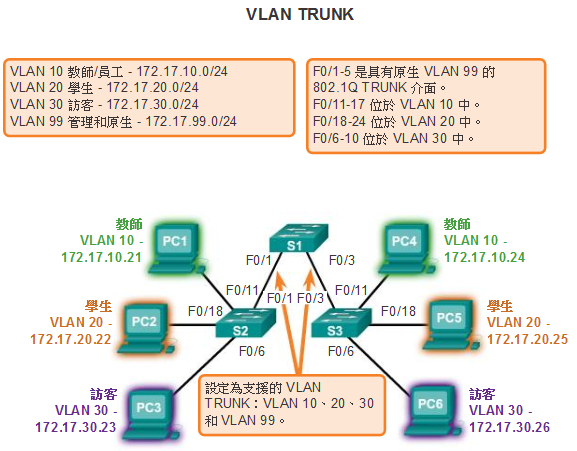
* 一般傳輸是資料VLAN，語音、網管用的會另外開VLAN，將流量區隔開來。
* 傳統電話，在傳輸時整條線路都是你在使用。
* 室內電話費70（月租費）+5（室內電話線路維護費）；原則上接線盒以外是電信公司，接線盒到家裡是自己負責，但中華電信有多收5元維護費，所以有問題也可以找他來處理。
* 集縮比，電話是100:20，100個用戶同時只能有20個用戶用，超過就會到佔線的聲音。
* VoIP需要足夠的頻寬、高優先權、延遲小於150ms來確保通話的品質，在資料擁塞時也能傳送；資料擁塞時，交換器預設就是將封包丟棄，但語音不能這樣；Cisco會優先處理VoIP的流量。

### 管理VLAN

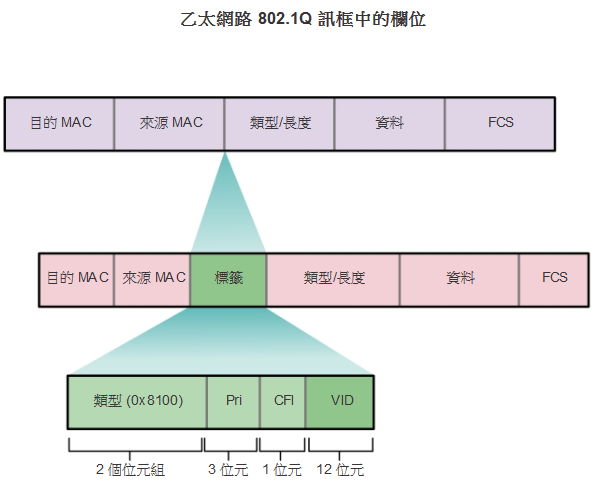
SNMP網管協定

### 原生VLAN

* 什麼是原生VLAN，原生 VLAN 分配給802.1Q TRUNK，802.1Q 協定會識別你是那個VLAN，並加上標籤；簡單說要經過交換器跟交換器之間傳輸的就要有標籤，才能決定分配給那個VLAN；沒有標籤的就加上原生VLAN的標籤。
* Trunk，主幹，兩台裝備間點對點的線路。主幹 (TRUNK) 是兩台網路裝置之間的點對點鏈路，負責傳輸多個 VLAN 的流量。
* 如果沒有 VLAN TRUNK，VLAN 並不是很有用。VLAN TRUNK 允許在交換器之間傳播所有 VLAN 流量，這樣位於同一 VLAN 但連線到不同交換器的裝置便可以通訊，不需要路由器的干預。
* VLAN TRUNK 不屬於特定的 VLAN，而是作為多個 VLAN 中交換器與路由器之間的管道。TRUNK 還可在網路裝置和伺服器或其他具有相應 802.1Q 網卡的裝置之間使用。預設情況下，在 Cisco Catalyst 交換器上，TRUNK 連接埠支援所有 VLAN。

**VLAN 標記欄位詳細資訊**

VLAN 標記欄位包含“類型”欄位、“優先順序”欄位、“規範格式識別碼”欄位和“VLAN ID”欄位。

* **類型** - 2 位元組值，稱為標記協定 ID (TPID) 值。對於乙太網路，它設定為十六進制 0x8100。
* **使用者優先順序** - 3 位元值，支援級別或服務實作。
* **規範格式識別碼 (CFI)** - 1 位元識別碼，便於在乙太網路鏈路上傳輸記號環訊框。
* **VLAN ID (VID)** - 12 位元 VLAN 標識號，最多支援 4096 個 VLAN ID。

識別QoS優先權

沒有標籤的訊框就是屬於原生的VLAN

不同等級的交換器，可以支援的VLAN數不同

VLAN的範圍

交換器上，普通範圍的 VLAN 編號為 1 到 1,005，延伸範圍的 VLAN 編號為 1,006 到 4,094。

**普通範圍的 VLAN**

* 用於中小型商業網路和企業網路。
* 從 1002 到 1005 的 ID 保留供記號環 VLAN 和 FDDI VLAN 使用。
* ID 1 和 ID 1002 到 1005 是自動新增的，不能刪除。
* 設定儲存在名為 vlan.dat 的 VLAN 資料庫檔案中。vlan.dat 檔案位於交換器的快閃記憶體中。
* VLAN 主幹協定 (VTP) 有助於管理交換器之間的 VLAN 設定，只能識別和儲存普通範圍的 VLAN。

**延伸範圍的 VLAN**

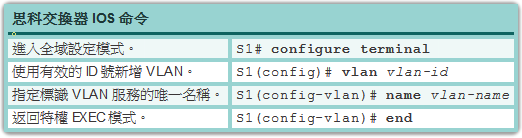
* 可讓服務供應商延伸自己的基礎建設以適應更多的客戶。某些跨國企業的規模很大，所以需要使用延伸範圍的 VLAN ID。
* VLAN ID 範圍從 1006 到 4094。
* 設定不會寫入 vlan.dat 檔案。
* 支援的 VLAN 功能比普通範圍的 VLAN 更少。
* 預設儲存在執行設定檔案中。
* VTP 無法識別延伸範圍的 VLAN。

延伸VLAN是給網路公司用的，這些資料不會寫入vlan.dat

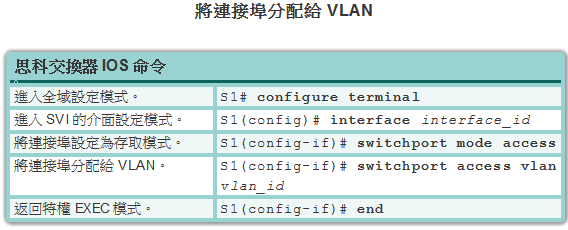
# VLAN

## 新增

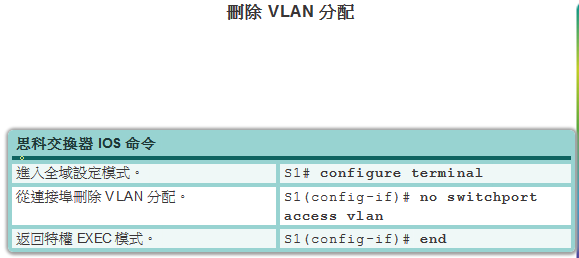
當設定普通範圍的 VLAN 時，設定詳細資訊儲存在交換器快閃記憶體中名為 vlan.dat 的檔案中。快閃記憶體是永久性的，不需要使用 **copy running-config startup-config** 命令。但是，由於在新增 VLAN 的同時通常也在思科交換器上設定了其他詳細資訊，比較好的做法是將執行設定更改儲存到啟動設定。



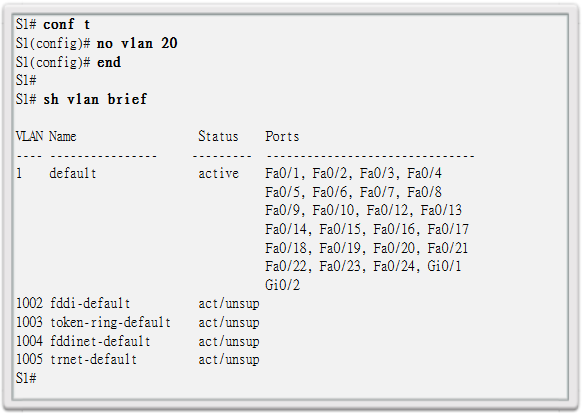
## 分配連接埠



## 更改 VLAN 連接埠成員

Cisco 中1個port只能屬於1個VLAN

## 刪除 VLAN



**delete flash:vlan.dat** 特權 EXEC 模式命令刪除整個 vlan.dat 檔案。這種方法能有效地將交換器的 VLAN 設定恢復為出廠預設狀態。

**注意**：對於 Catalyst 交換器，必須在重新載入之前同時使用 **erase startup-config** 命令和 **delete vlan.dat** 命令，才能將交換器恢復為出廠預設狀態。

密碼回復： google: cisco password recover/ cisco 密碼忘記

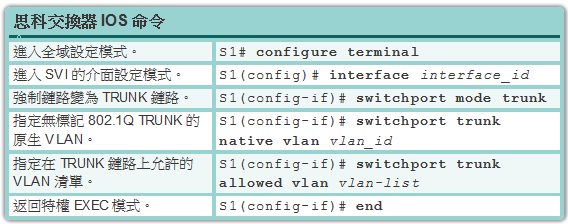
## 檢視 VLAN 資訊



故障排除時用

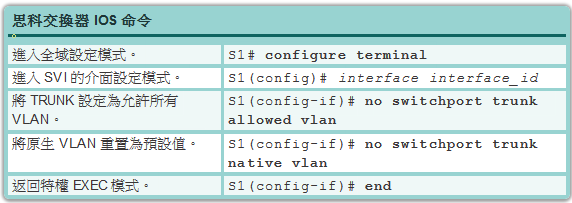
# VLAN TRUNK

## 設定



沒有設 allowed vlan 預設是全部都會過，但這樣會消耗頻寬，所以建議用不到的就把它濾掉。

## 重置



不同網段，沒有預設匣道、沒有路由器，是到不了的

# 動態主幹協定 (DTP)

當兩端的交換器 switchport mode 設定不同時，會造成網路不通。

Cisco 的設備有動態主幹協定 (DTP) 的功能，預設兩端設備會自動協商是否使用 trunk 設定。

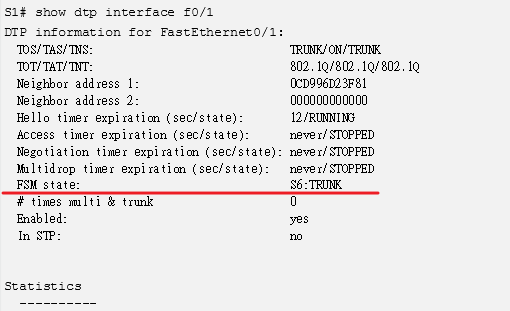
**switchport mode dynamic auto (DA) – 優先判斷為 switchport mode access**

**switchport mode dynamic desirable (DD) - 優先判斷為 switchport mode trunk**

建議儘量手動設定 TRUNK 鏈路。因為要用預設的 DTP 模式需要依賴於 Cisco IOS 軟體版本和平台有支援。

關閉 dtp 設定：**switchport nonegotiate**

要確定目前的 DTP 模式，指令為 **show dtp interface** 。



## 協商模式表



# VLAN 和 TRUNK 故障排除

## 常見問題

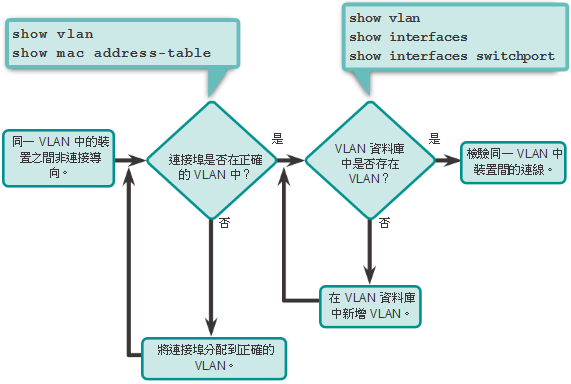


* 檢查時，習慣從終端（最底層）一層一層往上查。

## 檢查實體連線

## 檢查終端電腦 IP 設定

## 檢查 VLAN 設定



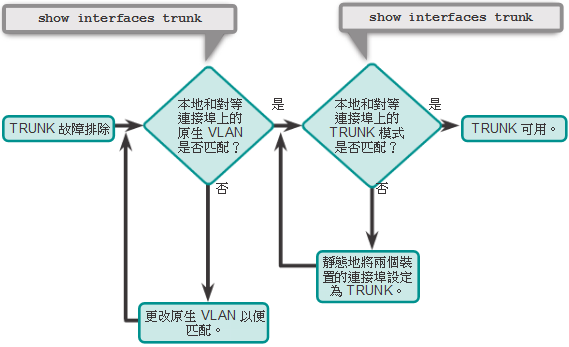
**第 1 步：** 使用 **show vlan** 命令檢查連接埠是否屬於期望的 VLAN。如果連接埠被分配到錯誤的 VLAN，請使用 **switchport access vlan** 命令更正 VLAN 成員關係。使用 **show mac address-table** 命令檢查交換器的特定連接埠上獲知了那些位址，以及該連接埠分配到那個 VLAN。

**第 2 步：** 如果連接埠分配到的 VLAN 被刪除，則該連接埠將變為無效。使用 **show vlan** 或 **show interfaces switchport** 命令。

要顯示 MAC 位址表，則使用 **show mac-address-table** 命令。圖 2 中的範例顯示在 F0/1 介面上獲取的 MAC 位址。可以看到 MAC 位址 000c.296a.a21c 是在 VLAN 10 中的 F0/1 介面上獲取的。如果此編號不是預期的 VLAN 編號，請使用 **switchport access vlan** 命令更改連接埠 VLAN 成員。

交換器中的每個連接埠均屬於 VLAN。如果刪除了連接埠所屬的 VLAN，則連接埠將變為非活動狀態。已刪除 VLAN 所屬的所有連接埠都將無法與網路中其他的裝置進行通訊。使用 **show interface f0/1 switchport** 命令檢查連接埠是否處於非活動狀態。如果連接埠處於非活動狀態，它將無法進行工作，直到使用 **vlan** *vlan\_id* 命令新增缺少的 VLAN。

## 檢查 TRUNK 設定



當沒有形成 TRUNK 或發生 VLAN 洩漏時，請按以下步驟排除故障：

**第 1 步：** 使用 **show interfaces trunk** 命令檢查本地和對等原生 VLAN 是否匹配。如果原生 VLAN 在兩端不匹配，則會出現 VLAN 洩漏。

**第 2 步：** 使用 **show interfaces trunk** 命令檢查是否已在交換器之間建立 TRUNK。儘可能靜態設定 TRUNK 鏈路。預設情況下，Cisco Catalyst 交換器連接埠使用 DTP 並嘗試協商 TRUNK 鏈路。

要顯示 TRUNK 的狀態、該 TRUNK 鏈路所用的原生 VLAN 和檢驗 TRUNK 建立情況，請使用 **show interfaces trunk** 命令。圖 2 中的範例顯示 TRUNK 鏈路一端上的原生 VLAN 已更改為 VLAN 2。如果 TRUNK 一端設定為原生 VLAN 99，另一端設定為原生 VLAN 2，那麼從一端的 VLAN 99 發出的訊框會在另一端的 VLAN 2 上接收。VLAN 99 洩漏到 VLAN 2 網段。

CDP 顯示 TRUNK 鏈路上原生 VLAN 不匹配的通知，顯示以下訊息：

\*Mar 1 06:45:26.232: %CDP-4-NATIVE\_VLAN\_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (2), with S2 FastEthernet0/1 (99).

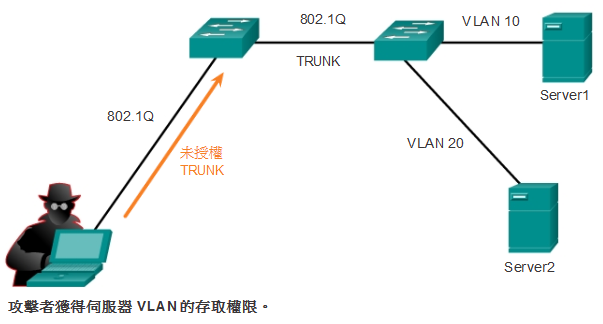
如果原生 VLAN 不匹配，網路中會發生連線問題。除設定的兩個原生 VLAN 之外，VLAN 的資料流量透過 TRUNK 鏈路成功傳播，但是與任一原生 VLAN 關聯的資料不能透過 TRUNK 鏈路成功傳播。

如圖 2 所示，原生 VLAN 不匹配問題不會阻止 TRUNK 的形成。要解決原生 VLAN 不匹配問題，請將鏈路兩端的原生 VLAN 設定為同一 VLAN。

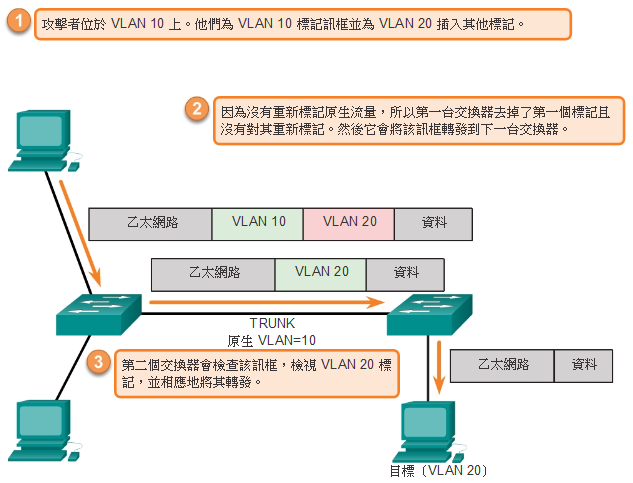
# VLAN 安全和設計

## 攻擊種類

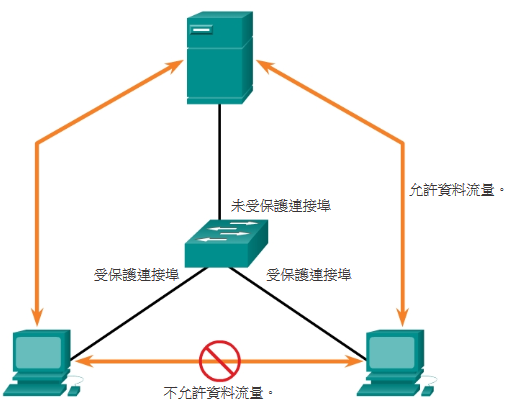
### 交換器欺騙



### Double-Tagging 雙重標籤攻擊



## 防護 – PVLAN Edge



PVLAN Edge 功能具有以下特點：

* 受保護連接埠不向同為受保護連接埠的任何其他連接埠轉發流量（單點傳送、多點傳送或廣播），但是控制流量除外。第 2 層的受保護連接埠之間無法轉發資料流量。
* 受保護連接埠和不受保護連接埠之間的轉發行為照常繼續。
* 必須手動設定受保護連接埠。

要設定 PVLAN Edge 功能，請在介面設定模式輸入 **switchport protected** 命令。

## 最佳的實作

* 就是不要使用預設的 VLAN 1 。
* 沒用的 port 都指到沒用的 VLAN （黑洞 VLAN）。
* 沒用的 port 都直接關閉不用，要用的人經過管理員同意及登記。
* 使用者資料、管理、語音…等，都隔離不同的 VLAN 。
* 不要使用 telnet ，改用 ssh 。
* 建議 DD 手動設定，不要設 DA 自動設定。