計算機網路概論

虛擬橋接網路
Virtual Bridged LANs
(IEEE 802.1Q)

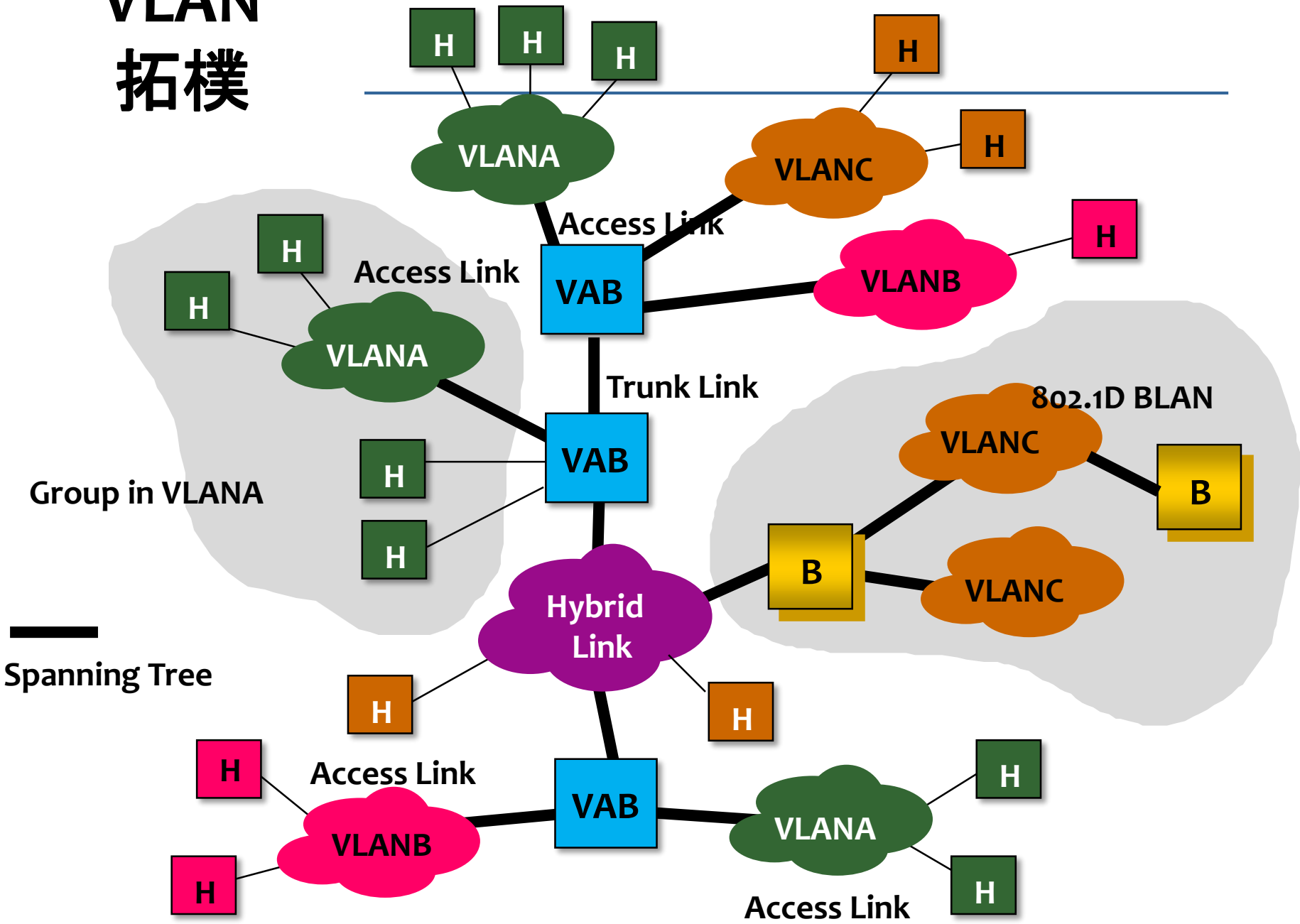
大綱

- 虛擬區域網路 (VLAN) 簡介
- 虛擬區域網路架構
- 基於埠號的虛擬區域網路
- 虛擬區域網路標籤
- 總結

虛擬區域網路 (VLAN) 的目的與優點

- 沒有虛擬區域網路時，第二層的交換機/橋接器將會轉送收到的廣播 (broadcast) 與 群播 (multicast) 訊框至所有埠 (ports)
  - 頻寬浪費問題
  - 安全問題
- 簡單管理邏輯群組內的主機，包含從群組中移除、加入、修改成員等
- 虛擬區域網路具有類似防火牆的機制，不同的虛擬區域網路間的廣播與群播的流量傳遞將會受限

VLAN 拓樸


H
H
H
VLANA
H
VLANC
H
Access Link
H
Access Link
VAB
VLANB
H
H
VLANA
Trunk Link
802.1D BLAN
VLANC
VAB
B
H
Group in VLANA
H
B
VLANC
Hybrid Link
Spanning Tree
H
H
H
Access Link
VAB
VLANA
H
VLANB
H
H
Access Link

虛擬區域網路的目的與優點

- 支持共享式傳輸媒體 (shared media) 以及點對點式傳輸鏈路 (point-to-point media)
- 每個虛擬區域網路有獨立的"虛擬區域網路辨識碼" (VLAN ID, 簡稱 VID)
- 保持現有的橋接器/交換機和主機的相容性
- 減少虛擬區域網路的參數配置設定，使得交換機/橋接器支援隨插即用特性 (Plug-and-Play)

虛擬區域網路 (VLAN) 概述

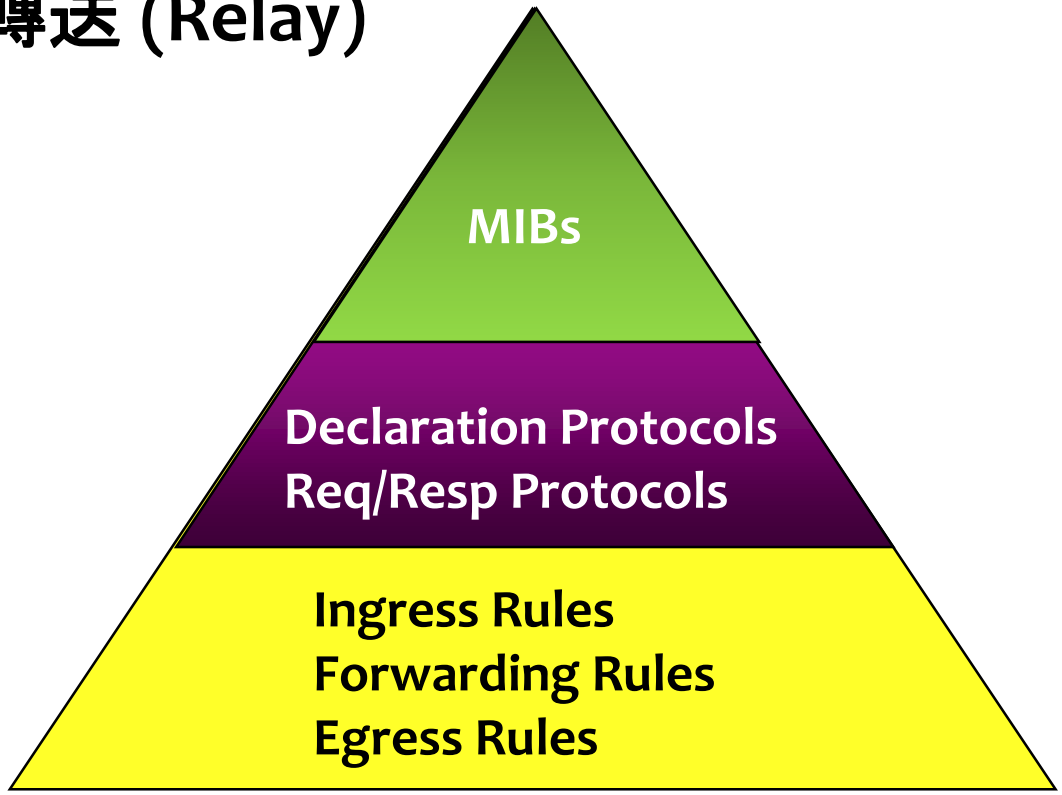
- 虛擬區域網路服務(VLAN Services) 建立於橋接網路
- 需要轉送程序來支援虛擬橋接區域網路服務
- 需要過濾資料庫來支援虛擬橋接區域網路服務
- 虛擬區域網路服務必須提供協議和程序來配送虛擬區域網路成員的資訊(成員可動態加入或退出)
- 需要管理服務和運作程序來設定與管理虛擬橋接網路服務

大綱

- 虛擬區域網路 (VLAN) 簡介
- 虛擬區域網路架構
- 基於埠號的虛擬區域網路
- 虛擬區域網路標籤
- 總結

虛擬區域網路架構

- 基於三層式模型:
  - 參數設定 (Configuration)
  - 配送/解析 (Distribution/Resolution)
  - 訊框轉送 (Relay)



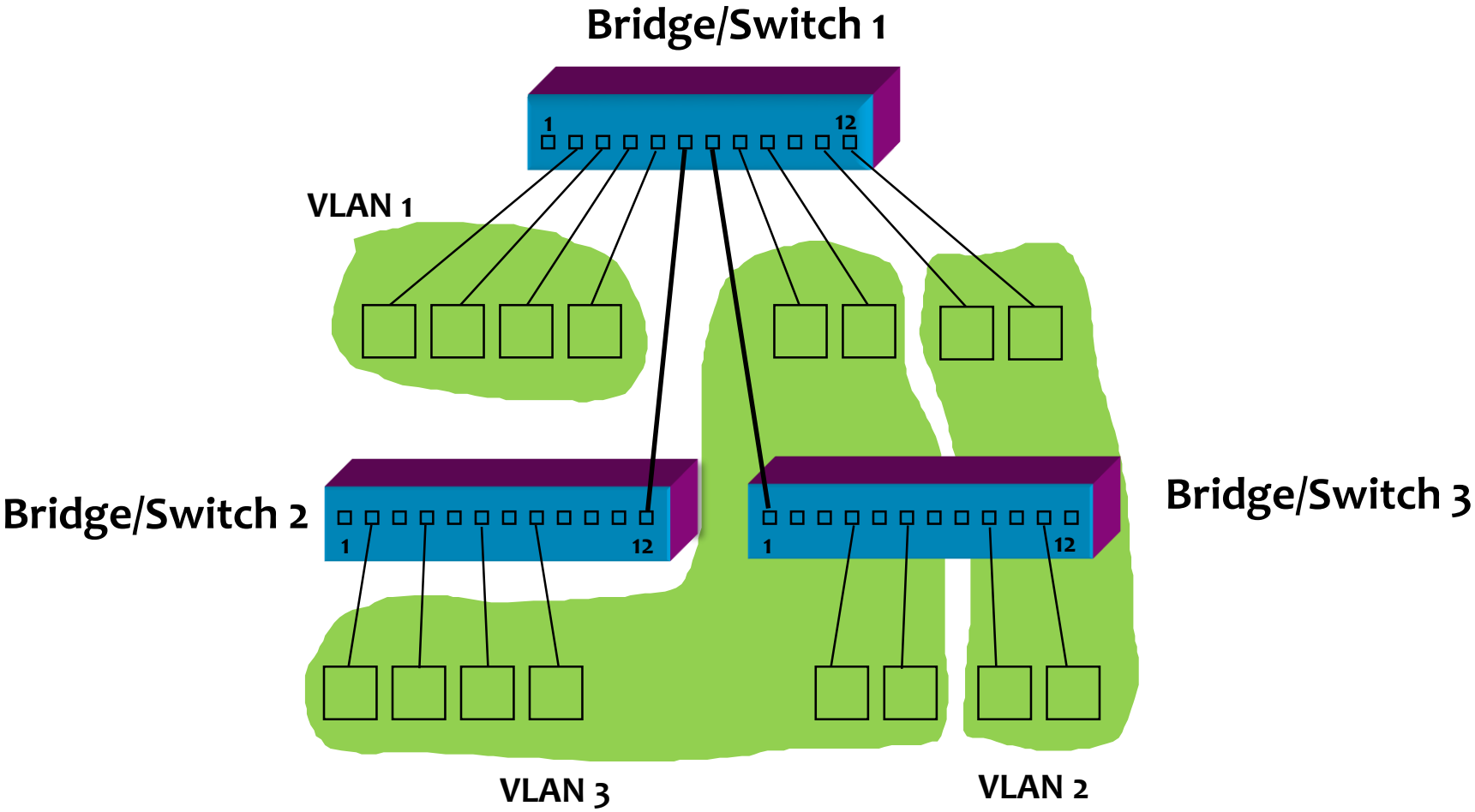
參數設定 (Configuration)

- 虛擬區域網路的參數設定為首要的工作
- 設定虛擬區域網路的參數 (如每個虛擬區域網路包含哪幾個接口或是埠號)

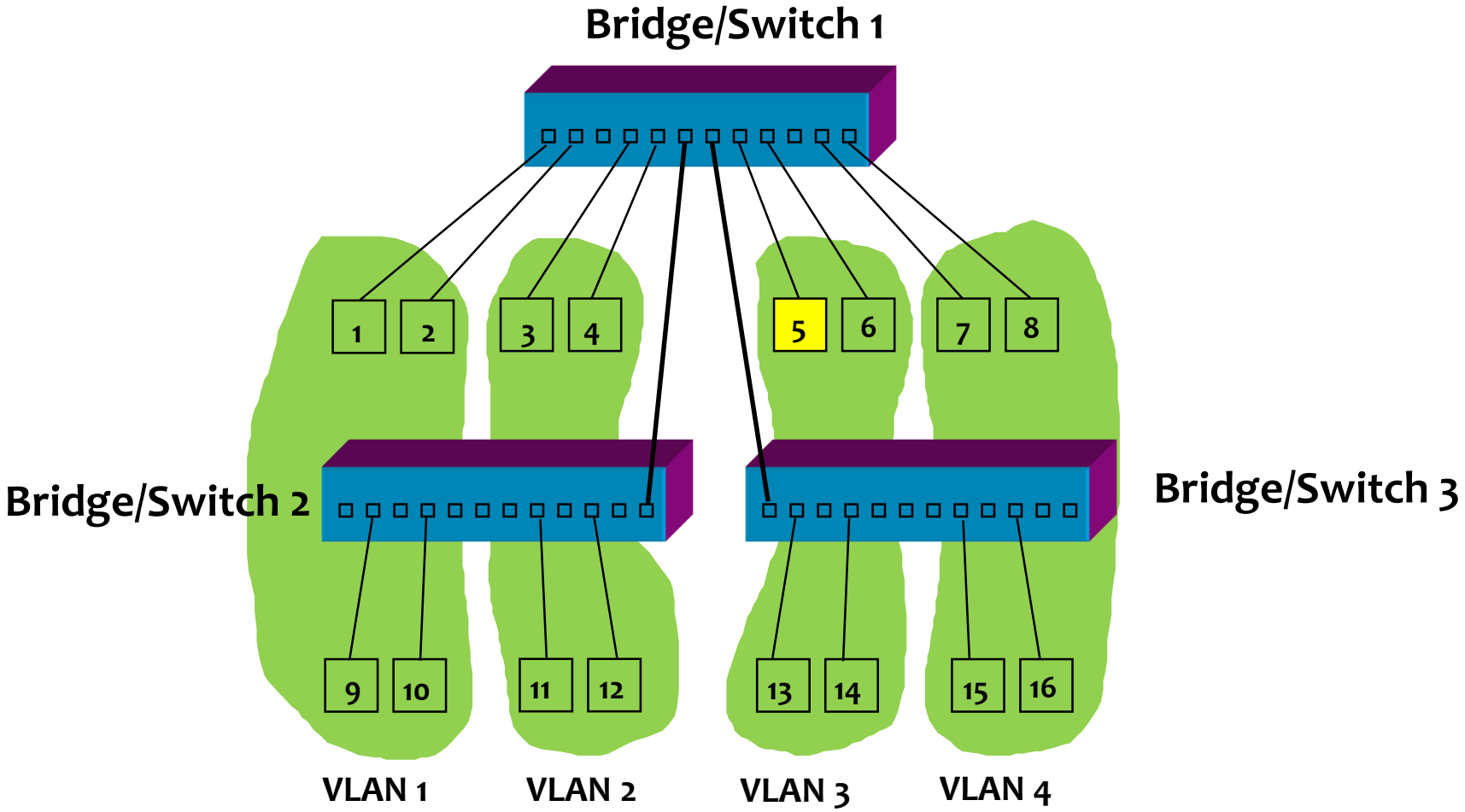
虛擬區域網路組成方式

- 基於埠號的虛擬區域網路
- 基於 MAC 位址的虛擬區域網路
- 基於子網域的虛擬區域網路
- 基於第三層協議的虛擬區域網路

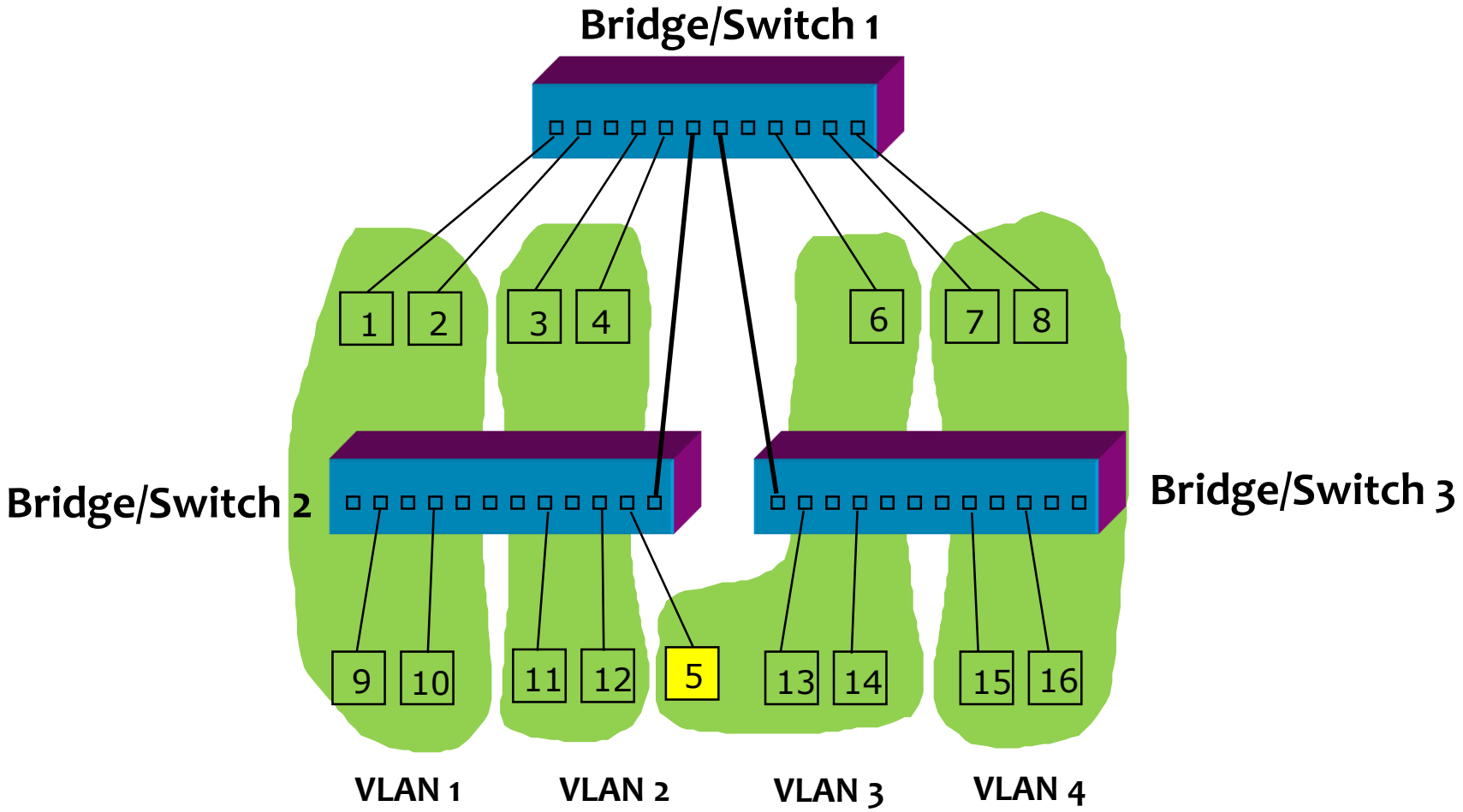
基於埠號的虛擬區域網路



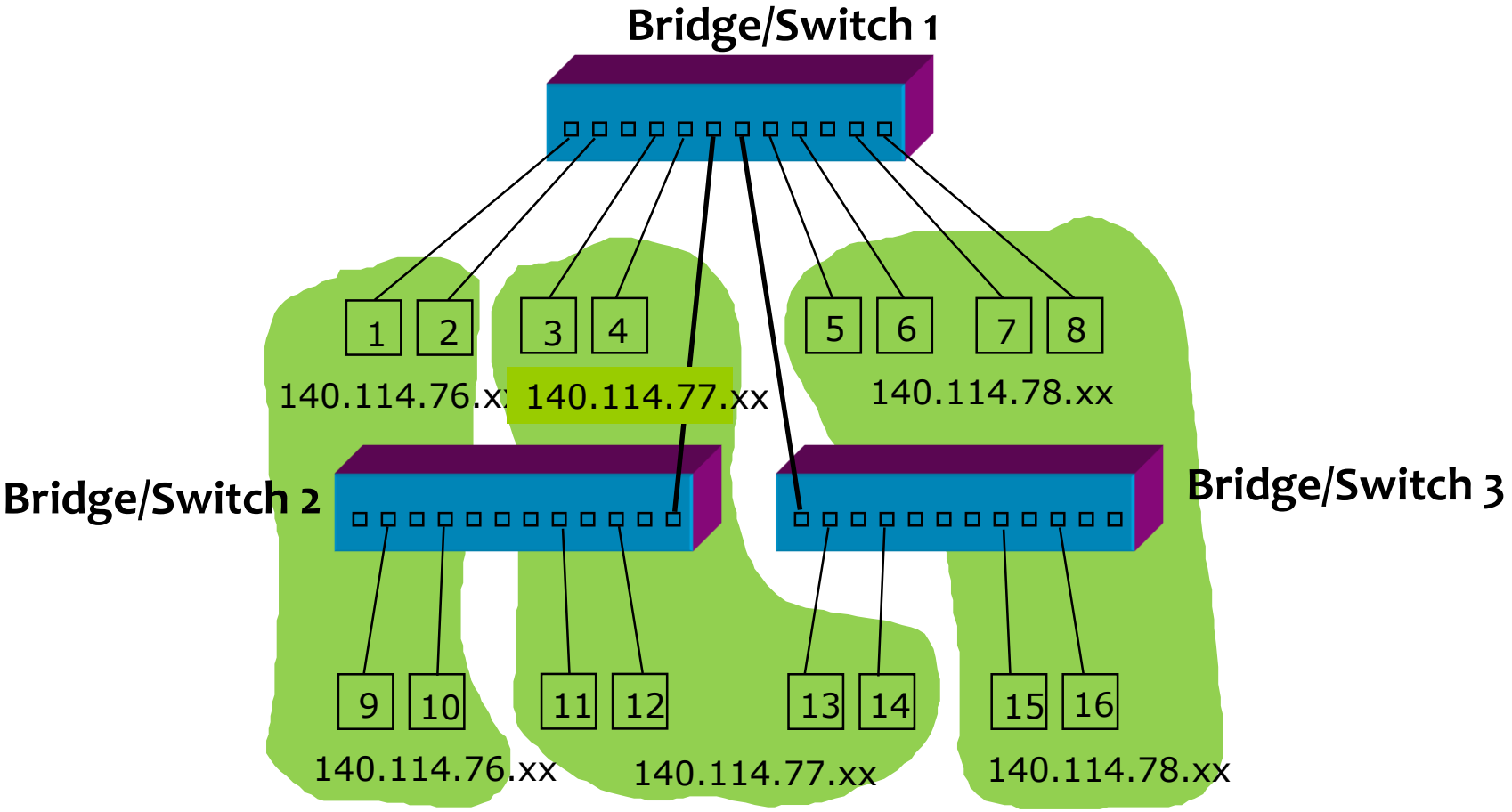
基於 MAC 位址的虛擬區域網路



基於 MAC 位址的虛擬區域網路 -- MAC_5移動

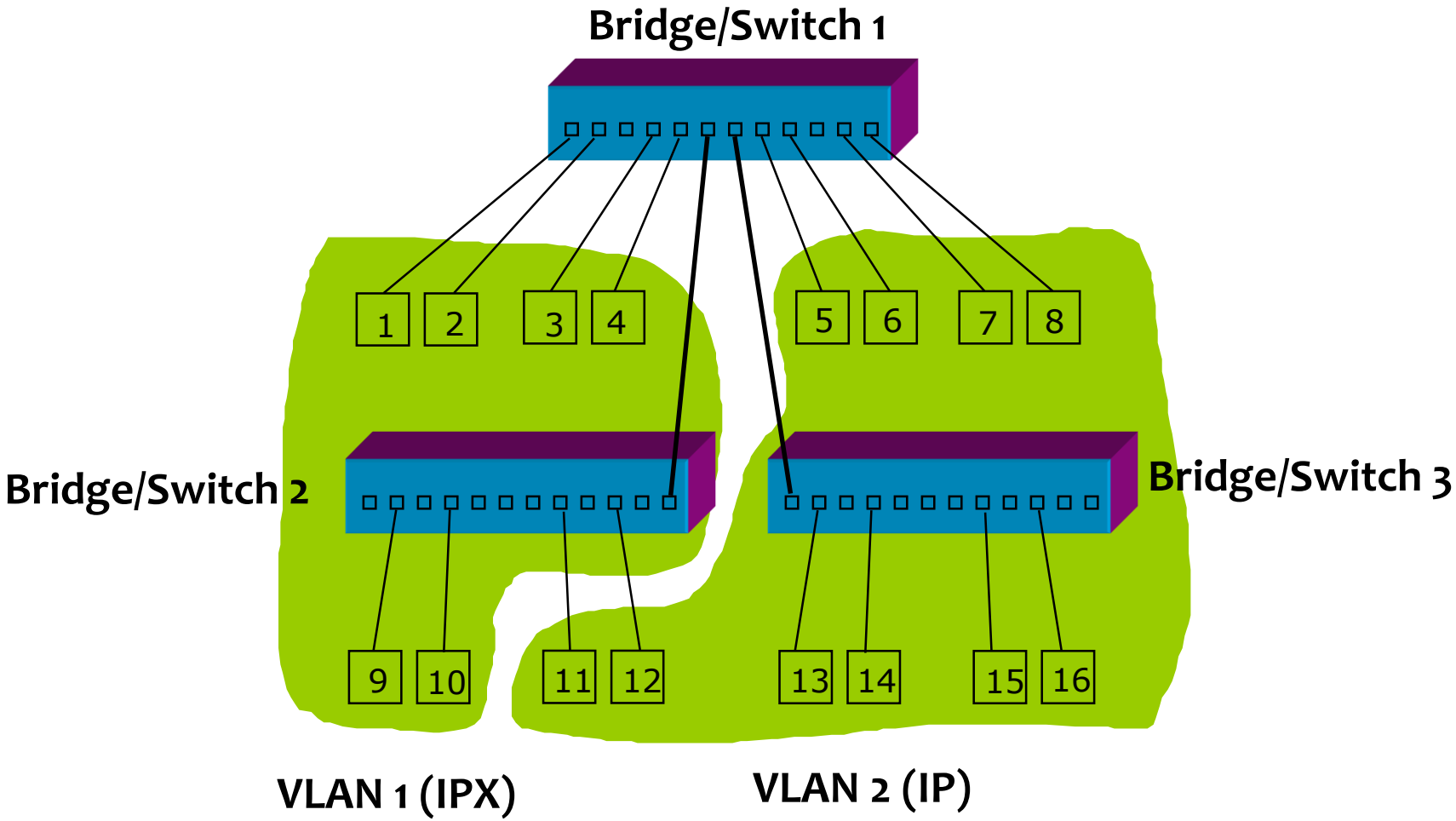


基於子網域的虛擬區域網路



VLAN 1 = IP subnet 140.114.76
VLAN 2 = IP subnet 140.114.77
VLAN 3 = IP subnet 140.114.78

基於第三層協議的虛擬區域網路



配送 (Distribution)

- 配送虛擬區域網路成員的資訊至所有橋接器，使之有能力決定要將收到的訊框轉傳至哪個虛擬區域網路
- 多種方法可達到配送功能:
  - 透過宣告協議 (Declaration Protocols)來配送虛擬區域網路的關聯資料
    - GARP (Generic Attributes Registration Protocol) 通用屬性註冊協議, 用來在橋接器間配送虛擬區域網路成員資訊
  - 透過請求/回應的協議 (Request/Response protocols)來取得特定的虛擬區域網路的關聯資料 (如 SNMP 簡易網路管理協議)

訊框轉送 (Relay)

- 此流程負責增加、修改、或移除位於訊框上的標籤 (tag)
- 虛擬區域網路訊框格式攜帶有 VLAN IDs (VIDs)
- 輸入規則 (Ingress rules)
  - 將接收到的訊框對應至不同的虛擬區域網路
- 轉送規則 (Forwarding rules)
  - 決定接收之訊框應由哪些埠轉送
- 輸出規則 (Egress rules)
  - 針對不同輸出埠號, 轉換欲轉送訊框的格式 (添加標籤或移除標籤)

訊框轉送 (Relay)

- 此為基於埠號的方法, 根據虛擬區域網路成員的關係規範了**輸入規則**、**轉送規則**、**輸出規則**使得橋接器得以:
  - 將所有收到的**無標籤訊框**分類至特定的虛擬區域網路 (**PVID, Port VID**).
  - 由已收到的**有標籤訊框上辨識其 VID**.
  - 利用此 VID 來轉發或過濾此訊框.
  - 根據 Port/VLAN 配對的規則，將訊框以貼標籤或無標籤的格式傳送.

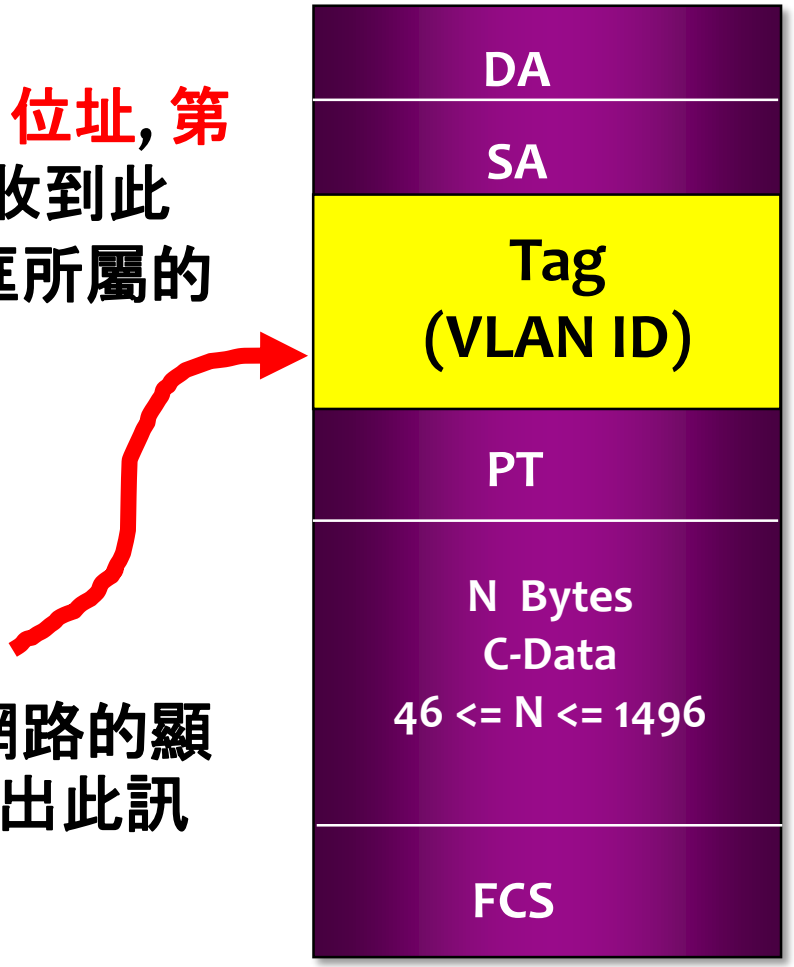
訊框標籤

隱性標籤

- 利用訊框本身的資料 (MAC 位址, 第三層協議辨識碼等等)或接收到此訊框的連接埠來辨別此訊框所屬的虛擬區域網路.

顯性標籤

- 訊框本身就帶有虛擬區域網路的顯性編號 (VLAN ID) 可以辨識出此訊框所屬的虛擬區域網路.



輸入規則/輸出規則

- 每個接收到的訊框都會被辨識且歸類到一個虛擬區域網路, 並且給予一個 VID
- 辨識工作可經由下列方法完成
  - 顯性標籤 : 訊框所攜帶的 VID 值
  - 隱性標籤 : 接收到此訊框的連接埠的 PVID
- 假如此訊框的輸出埠不在此虛擬區域網路的成員集合 (Member set) 中，則此訊框將會被過濾掉

大綱

- 虛擬區域網路 (VLAN) 簡介
- 虛擬區域網路架構
- 基於埠號的虛擬區域網路
- 虛擬區域網路標籤
- 總結

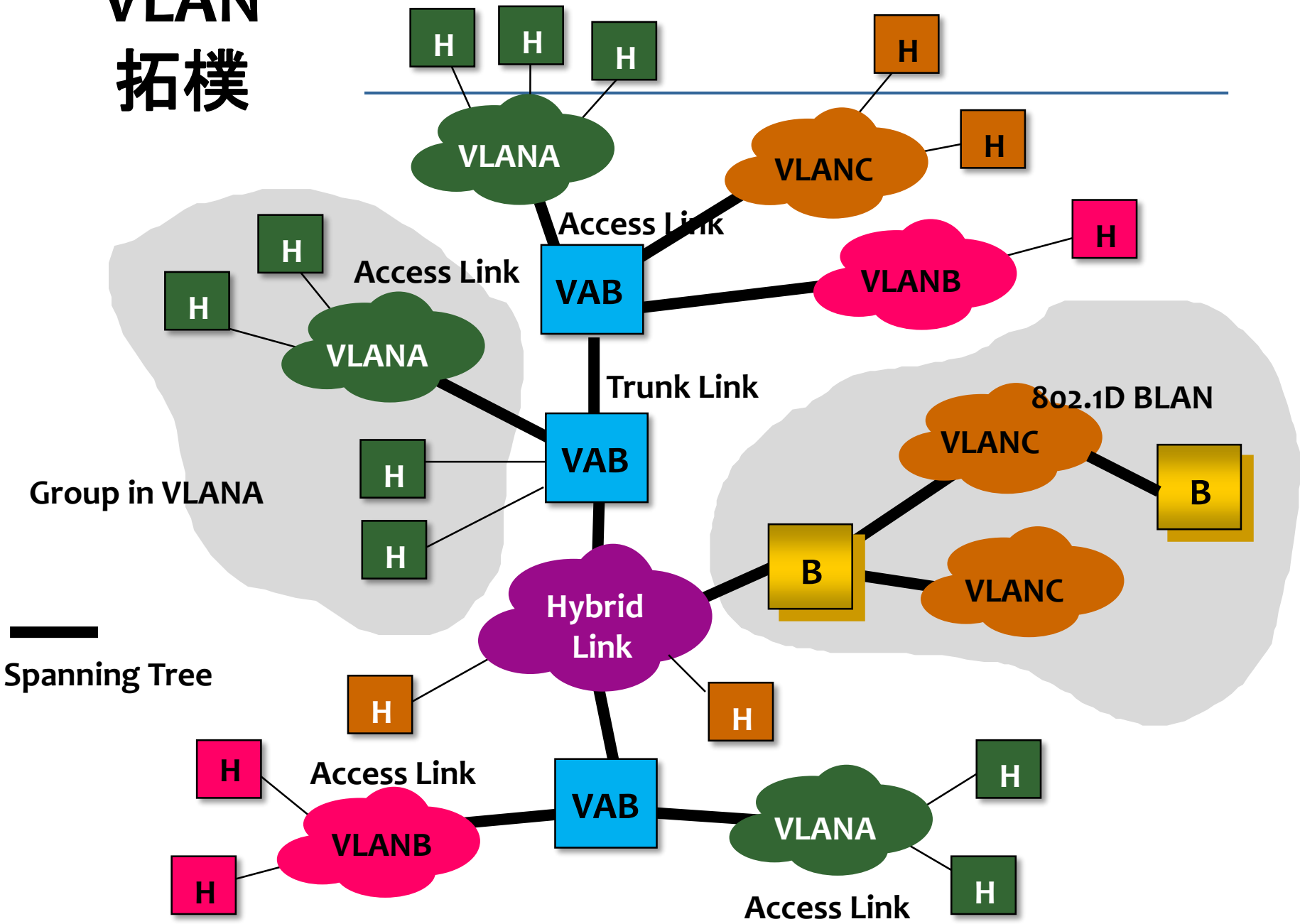
定義基於埠號的虛擬區域網路

- **虛擬網路設備(VLAN aware devices):** 能識別虛擬區域網路成員資訊與虛擬區域網路訊框的設備
- **非虛擬網路設備(VLAN unaware devices)**
- **存取鏈路(Access Link)** 是一個網路區段, 用來將一台或多台非虛擬網路設備連接至虛擬網路橋接器的一個接口
  - 所有位於存取鏈路的訊框都使用**隱性標籤**
  - 存取鏈路上**不會有貼上 VLAN 標籤的訊框**
  - 可視為網絡的最外邊緣
  - 可以連接到其他 802.1D 相容的橋接器（BLAN）

定義

- 主幹鏈路 (Trunk Link) 是一個網路區段, 用來在虛擬網路橋接器之間轉送屬於不同 VLANs 的訊框
  - 所有連接至主幹鍊路的設備必須為虛擬網路設備
  - 所有在主幹鍊路上的訊框(包含最末端主機的訊框)都具有顯性標籤 (VLAN ID)
- 混合鏈路(Hybrid Link) 是一個網路區段, 用來連接虛擬網路設備與非虛擬網路設備
  - 此鏈路上可以有貼標籤的訊框與未貼標籤的訊框，但這兩種訊框必須屬於不同的虛擬區域網路
  - 屬於同一個虛擬區域網路的訊框必須全部貼標籤或全部不貼標籤

VLAN 拓樸


H
H
H
VLANA
H
VLANC
H
Access Link
H
Access Link
VAB
VLANB
H
H
VLANA
Trunk Link
802.1D BLAN
VLANC
VAB
B
H
Group in VLANA
H
B
VLANC
Hybrid Link
Spanning Tree
H
H
H
Access Link
VAB
VLANA
H
VLANB
H
H
Access Link

在混合鏈路中訊框貼標籤的規則

- 對於每個虛擬區域網路，所有經過一個混合鏈路的訊框都必須遵守相同的標籤規則:
  - 所有訊框皆為隱性標籤 (未貼標籤) 或
  - 所有訊框都攜帶同樣的顯性標籤 (貼標籤)
- 混合鏈路上可以有已貼標籤和未貼標籤的訊框，但這兩種訊框必須屬於不同的虛擬區域網路
- 範例中的混合鏈路
  - 所有虛擬區域網路 A 和 B的訊框都是顯性標籤
  - 所有虛擬區域網路 C 的訊框都是隱性標籤

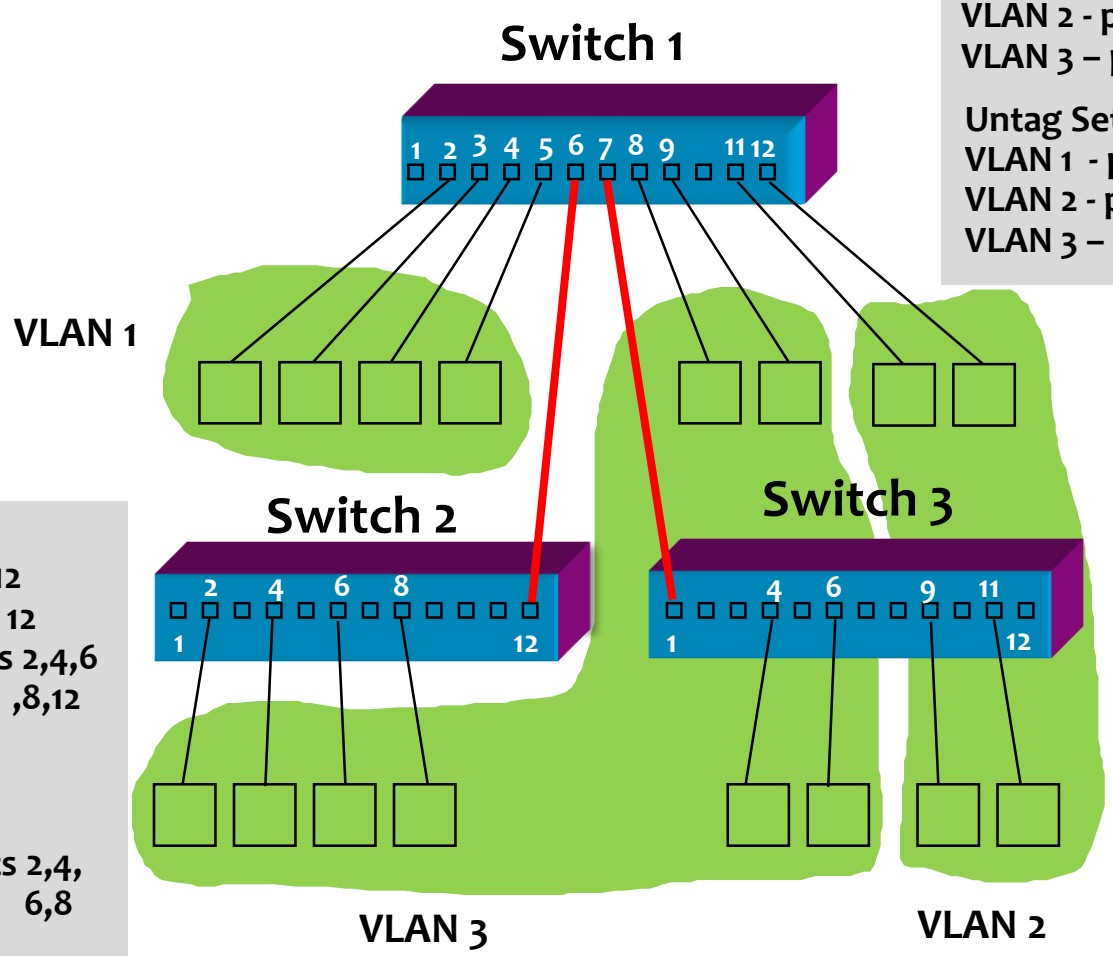
擴張樹和虛擬區域網路

- 擴張樹消除了橋接網路中的迴圈
- 擴張樹提供任一對主機之間的傳輸路徑
- 所有虛擬區域網路的傳輸路徑都沿著擴張樹建構
- 一個虛擬區域網路的傳輸路徑可以定義為擴張樹的子集合
- 每個虛擬區域網路的傳輸路徑彼此可以有不同區段的重疊或完全不重疊
- 每個虛擬區域網路的拓撲是動態改變的 (成員可以動態加入或是退出)

橋接器在虛擬區域網路上的運作

- 橋接器利用過慮封包來確保要傳送給特定虛擬區域網路的訊框只會被轉送到那些有路徑可以到達此虛擬區域網路成員的接口(ports)上
- 對於每個虛擬區域網路，橋接器須記錄兩個集合:
  - 成員集合(Member set, Port IDs)
  - 無標籤集合(Untagged set, Port IDs)

成員集合與無標籤集合的範例



Member Set：
VLAN 1 - ports 2, 3, 4, 5
VLAN 2 - ports 7, 11, 12
VLAN 3 – ports 6, 7, 8, 9

Untag Set：
VLAN 1 - ports 2,3,4,5
VLAN 2 - ports 11, 12
VLAN 3 – ports 8, 9

Member Set：
VLAN 1 - port 12
VLAN 2 – port 12
VLAN 3 – ports 2,4,6 ,8,12

Untag Set：
VLAN 1 -
VLAN 2 -
VLAN 3 – ports 2,4, 6,8

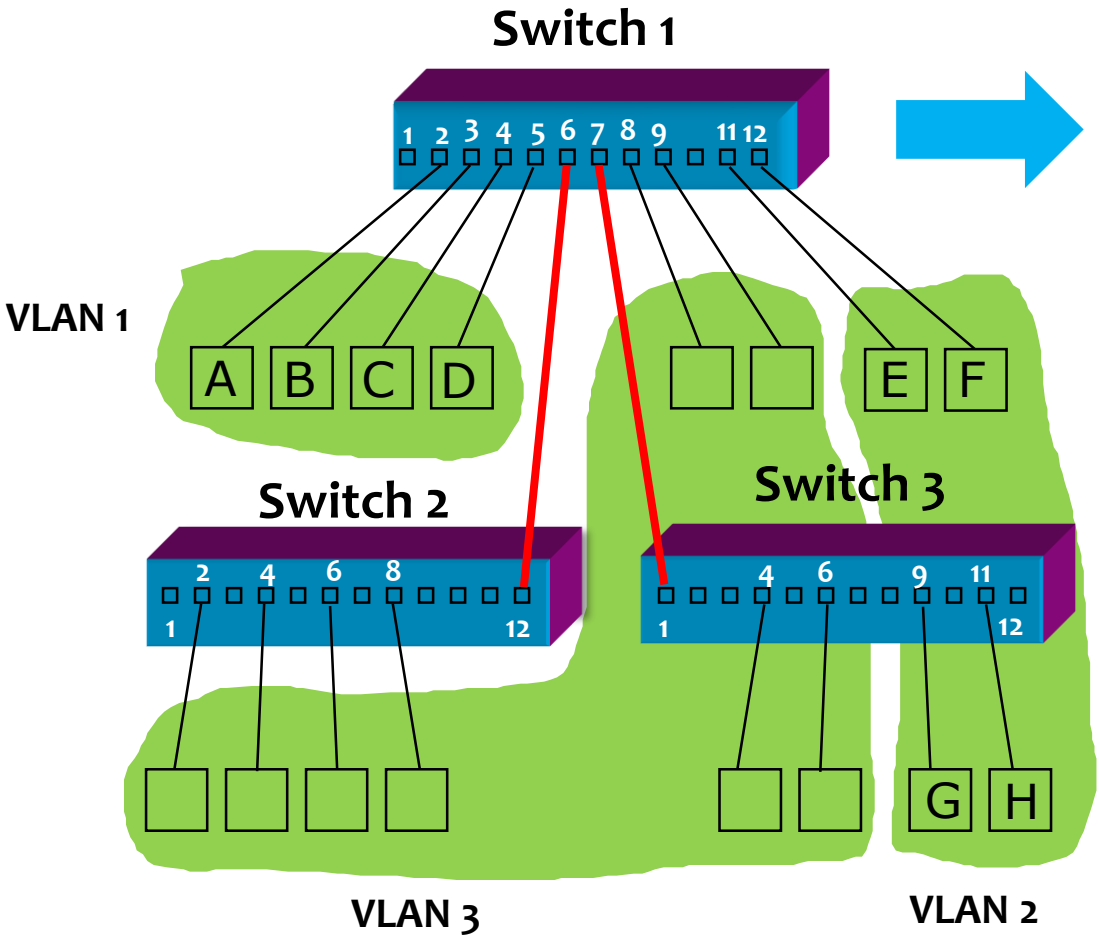
Member Set：
VLAN 1 - port 1
VLAN 2 – ports 1 9, 11
VLAN 3 – ports 1, 4, 6

Untag Set：
VLAN 1 -
VLAN 2 - ports 9, 11
VLAN 3 – ports 4, 6

虛擬區域網路之位址學習

- 共享式虛擬網路學習模式 (Shared VLAN Learning, SVL)
  - 每個虛擬區域網路學習到的位址將會與所有虛擬區域網路共享
- 獨立式虛擬網路學習模式 (Independent VLAN Learning, IVL)
  - 每個虛擬區域網路學習到的位址將自己使用，不與其他虛擬區域網路共享
- 在大部分的情況，無論使用 SVL 或 IVL 會得到相同結果
- 但是在一些特殊情況下，我們必須指定橋接器的學習模式

SVL 和 IVL 的範例



FD of VLAN 1

MAC Addr	Port	Time (S)
A	2	20
B	3	18
C	4	25
D	5	4

MAC Addr	Port	Time (S)
E	11	20
F	12	18
G	7	25
H	7	4

FD of VLAN 2

IVL 範例 -- 多個獨立的虛擬區域網路

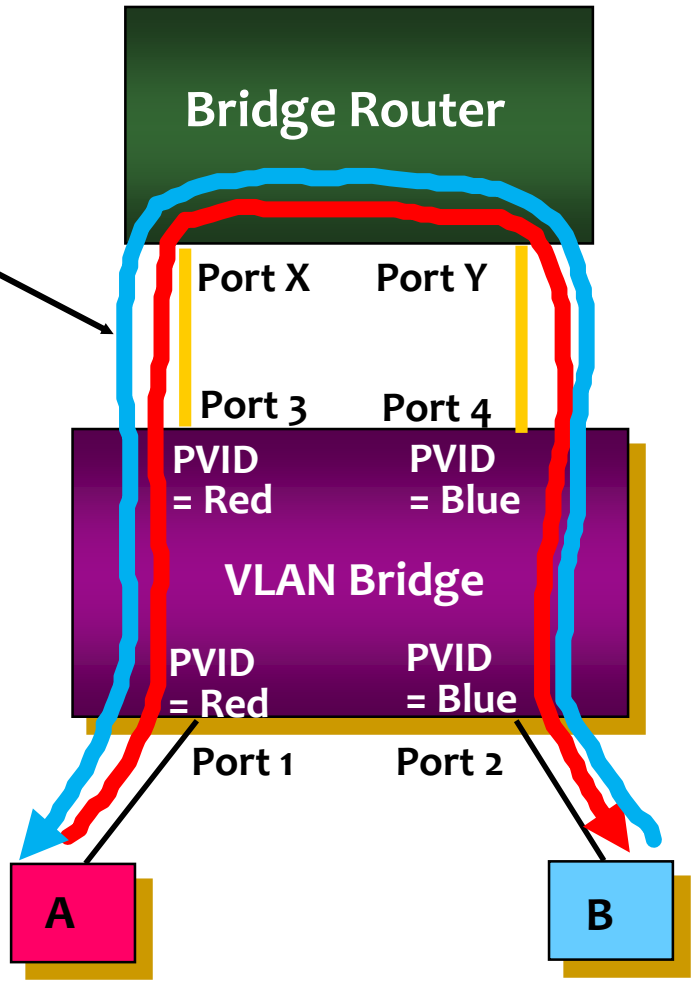
- 伺服器(橋接器-路由器、連接器)連接多個獨立的虛擬區域網路
- 連接器和主機為非虛擬網路設備(未貼標籤)
- 連接器關閉擴張樹演算法功能
- VLAN Red (A) <--> VLAN Blue (B) 之間的訊框將會被發送連接器(防火牆功能)
- 此例中, 過濾資料庫應該為獨立式學習模式 (IVL)
- 否則, 橋接器 將會經由埠號1,4 來交替學習 MAC A 位址,而經由埠號 2,3 來交替學習 MAC B 位址
- 最後導致由A(B)至B(A)的訊框會被傳送至錯誤的路徑

IVL 範例 -- 多個獨立的虛擬區域網路

正確路徑
For A->B and B->A

Member Set：
Red - Ports 1,3
Blue - Ports 2,4

Untag Set：
Red - Ports 1,3
Blue - Ports 2,4



過濾資料庫

MAC	Port
A	X
B	Y

VLAN Red

MAC	Port
A	1
B	3

VLAN Blue

MAC	Port
A	4
B	2

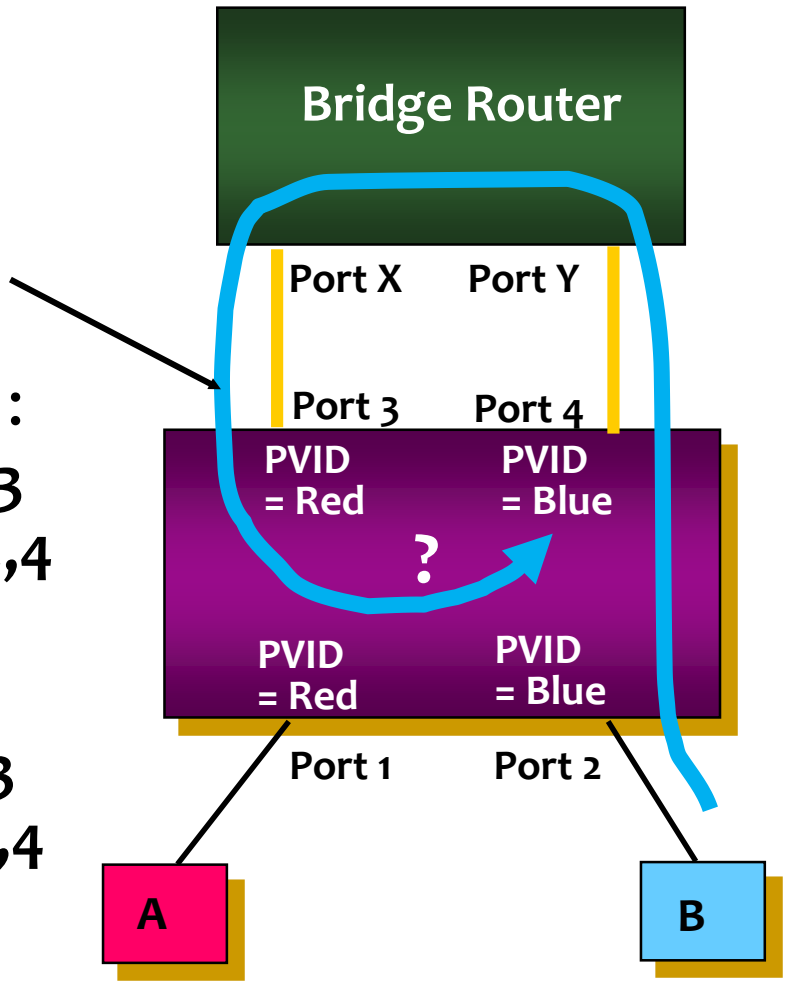
假如於此範例使用 SVL 模式

錯誤路徑

For B --->A

Member Set：
Red - Ports 1,3
Blue - Ports 2,4

Untag Set：
Red - Ports 1,3
Blue - Ports 2,4



過濾資料庫

MAC	Port
A	X
B	Y

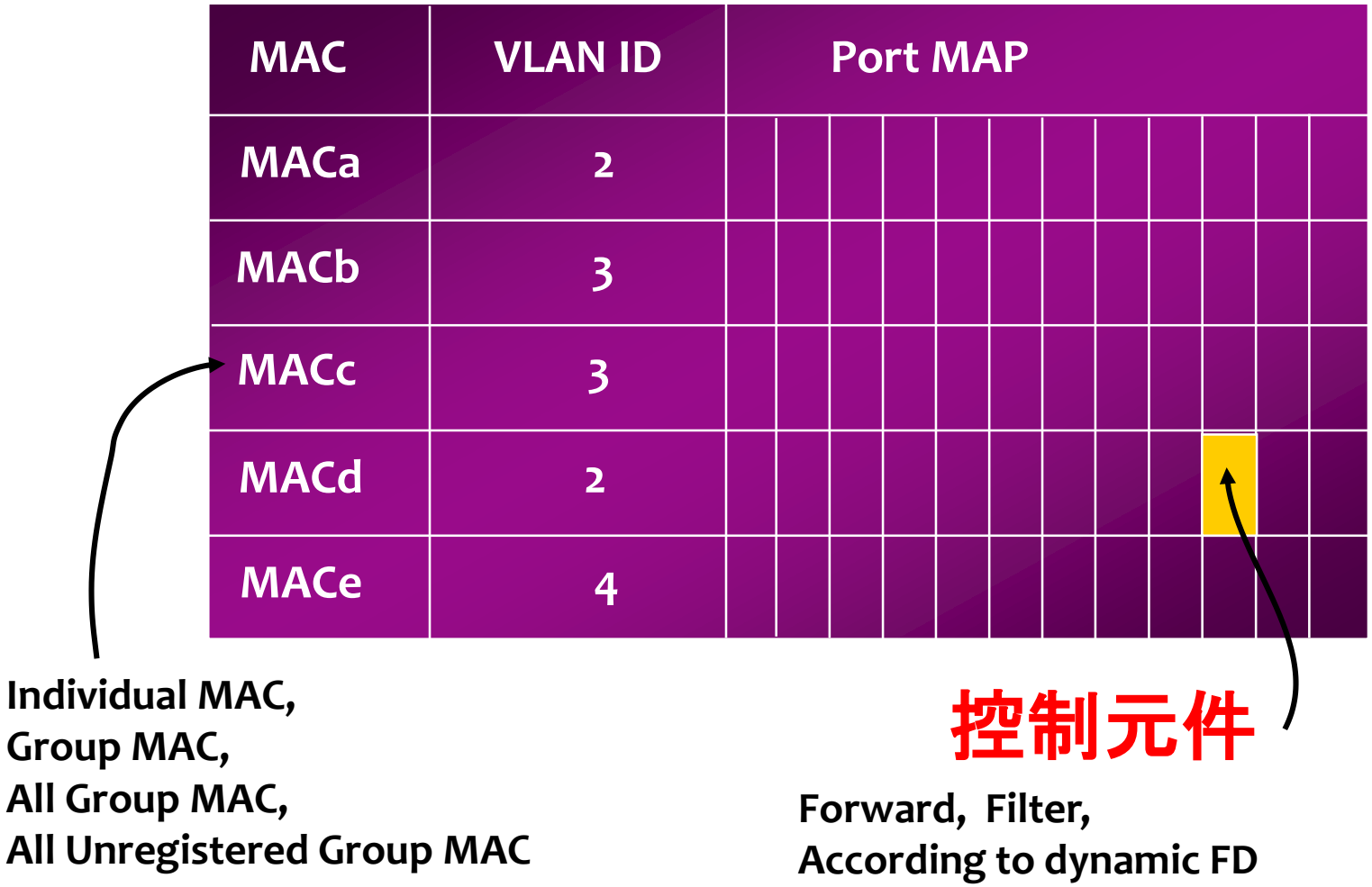
SVL (Red, Blue)

MAC	Port
A	4
B	3

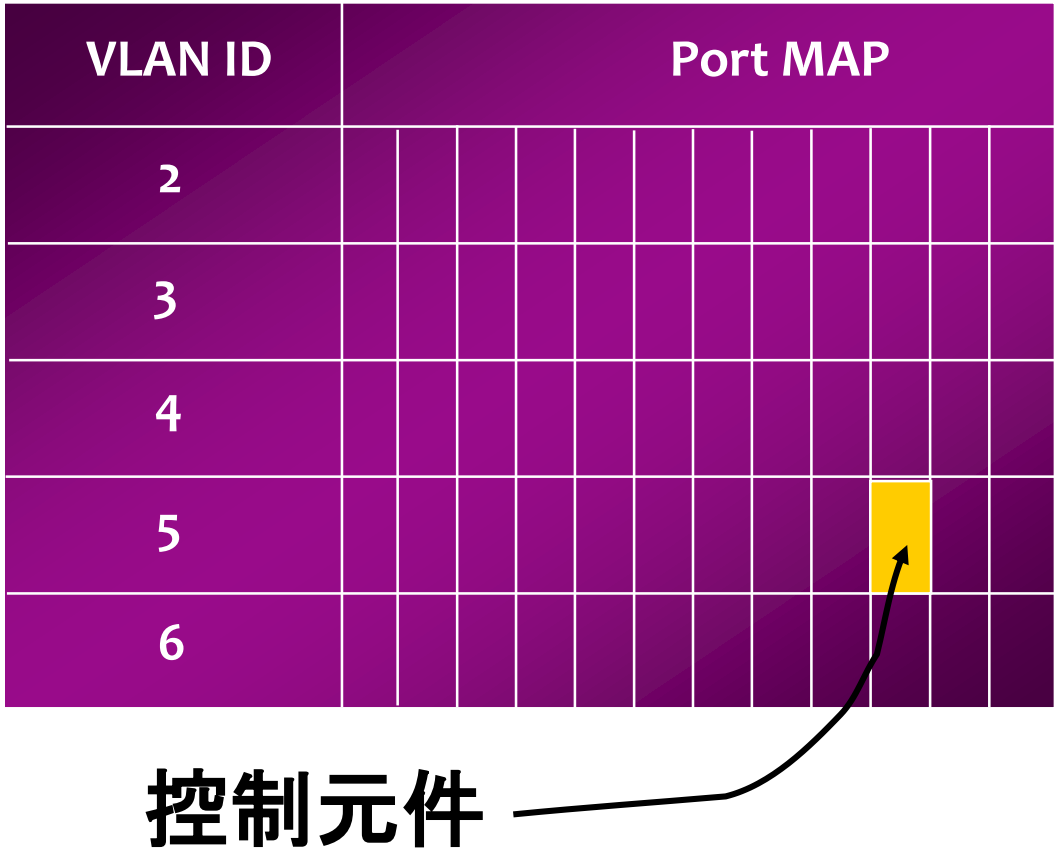
虛擬區域網路的過濾資料庫

- 靜態過濾項目(Static Filtering Entry)
- 靜態虛擬網路註冊項目(Static VLAN Registration Entry)
- 動態過濾項目(Dynamic Filtering Entry)
- 動態虛擬網路註冊項目(Dynamic VLAN Registration Entry)

靜態過濾項目

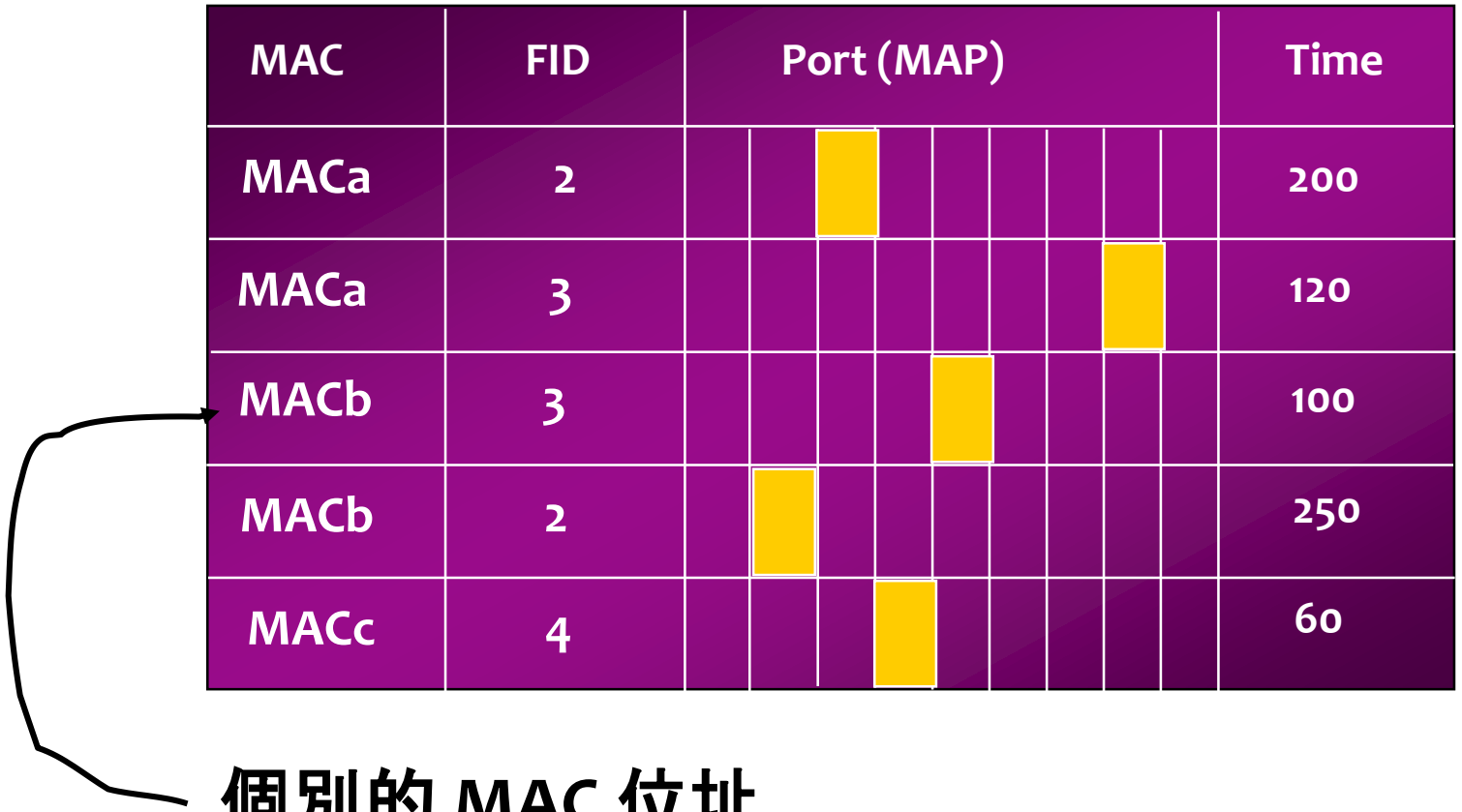

MAC
VLAN ID
Port MAP
MACa
2
MACb
3
MACc
3
MACd
2
MACe
4
Individual MAC,
Group MAC,
All Group MAC,
All Unregistered Group MAC
控制元件
Forward, Filter,
According to dynamic FD

靜態虛擬網路註冊項目

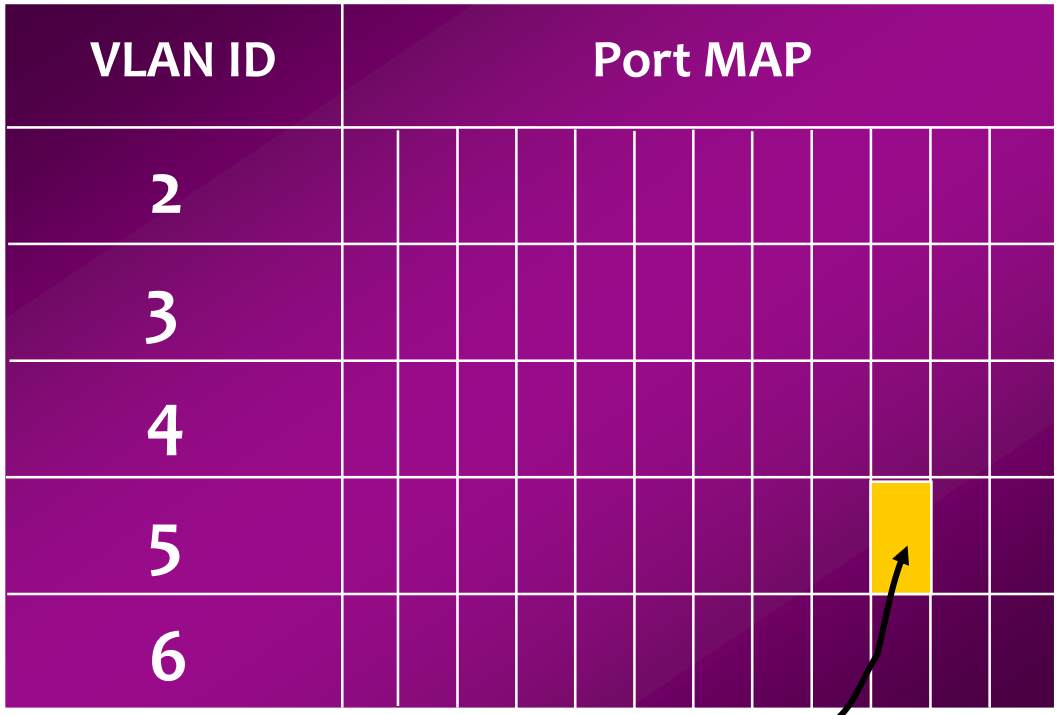


GVRP Registrar Administrative Control :
Registration Fixed, Forbidden, Normal.
Tagged/Untagged

動態過濾項目(藉由學習機制)



動態虛擬網路註冊項目



控制元件

VID is registered on this port ?

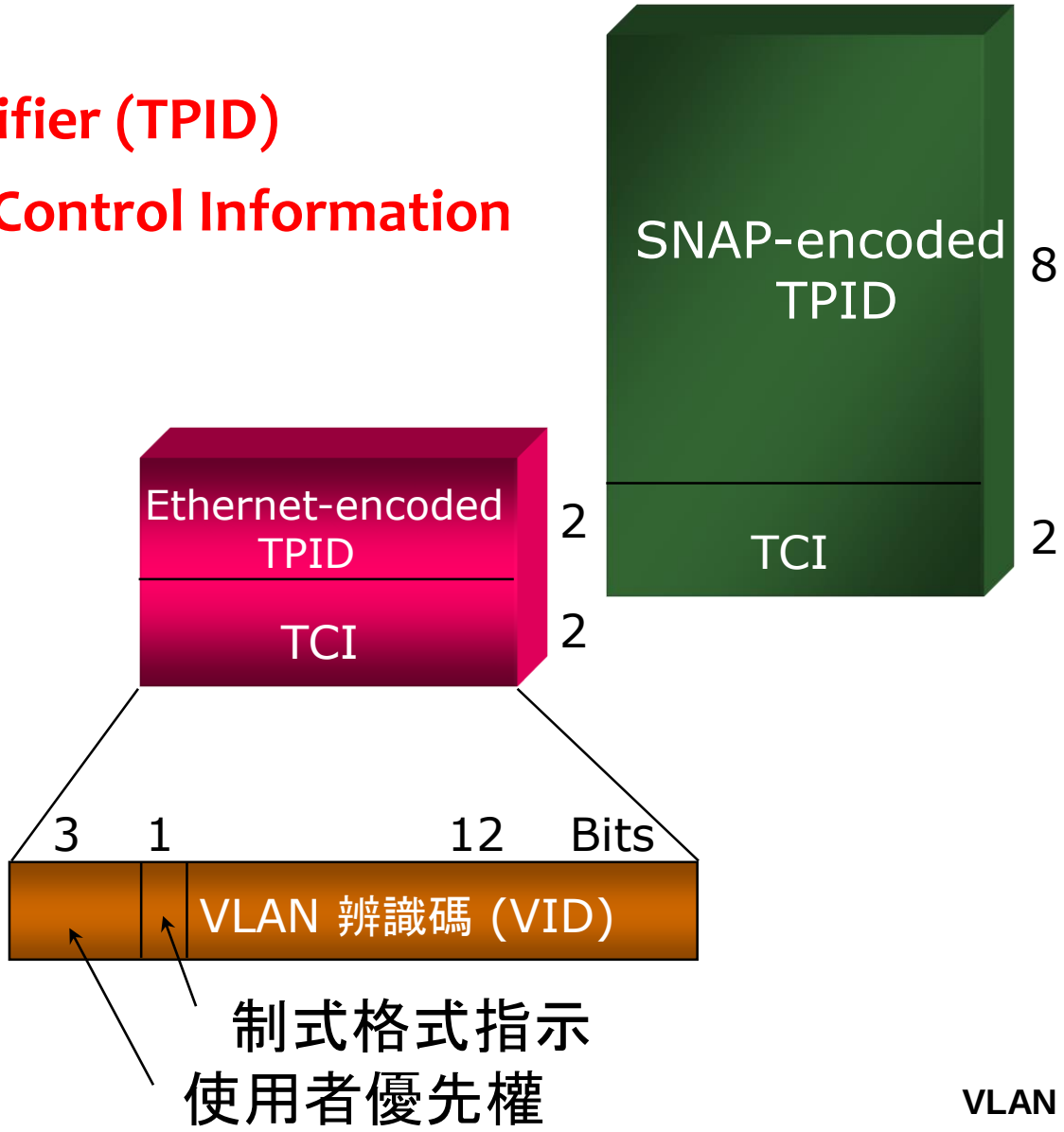
大綱

- 虛擬區域網路 (VLAN) 簡介
- 虛擬區域網路架構
- 基於埠號的虛擬區域網路
- 虛擬區域網路標籤
- 總結

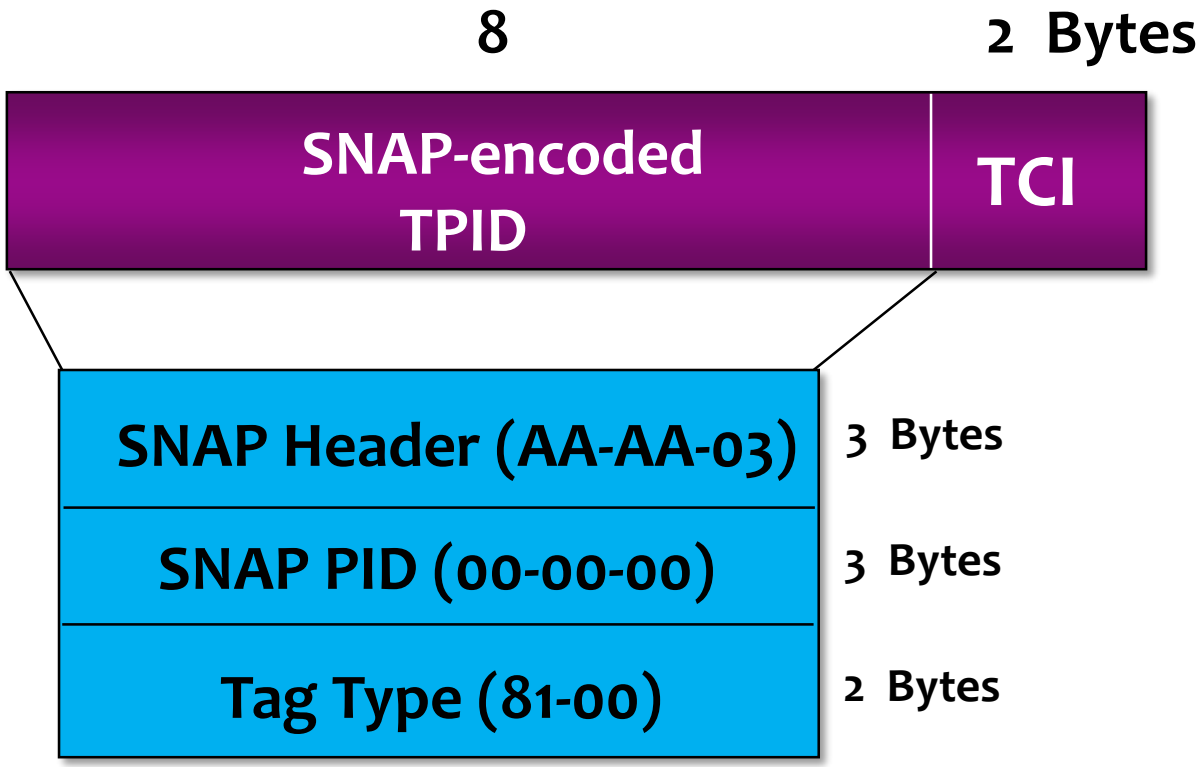
虛擬區域網路標籤結構

- **標籤協議辨識碼**

  Tag Protocol Identifier (TPID)
- **標籤控制訊息Tag Control Information (TCI)**
  - 使用者優先權
  - 制式格式指示
  - VID 辨識碼



標籤格式 (SNAP-編碼)



SNAP: SubNetwork Access Protocol(子網路存取協議)

SNAP為 在 IEEE802 區域網路上傳輸 IP 封包的標準協議. 換句話說, IP 封包可以藉由封裝到 802.2 LLC 和 SNAP 資料鏈結層和 802.3, 802.4 或 802.5 實體網路層，來達到在 IEEE802 區域網路中傳輸的目的

總結

- 虛擬區域網路用來將一群主機以邏輯的方式連接起來, 好似這些主機就連接在同一個區域網路上
- 虛擬區域網路的成員可以動態加入或移除
- 沒有虛擬區域網路的話, 所有廣播訊框和群播訊框將會被轉傳到所有埠號, 造成
  - 頻寬浪費
  - 安全問題
- 有虛擬區域網路時，不同的虛擬區域網路間的廣播與群播的流量是受到限制的

總結

- 不同虛擬區域網路間無法直接通訊. 彼此之間的通訊需要經過路由器
- IEEE 802.1Q 標準定義的是 基於埠號的虛擬區域網路
- 三階段模式
  - 虛擬區域網路參數設定與配送
  - 宣告/配送虛擬區域網路成員訊息到所有橋接器
  - 訊框傳遞
- VLAN ID 長度為 12 位元 (最多可以有 4096 VLANs)

總結

- 三種類型的鏈結:
  - 存取鏈路: 所有訊框皆不貼標籤
  - 主幹鏈路: 所有訊框皆須貼標籤
  - 混合鏈路: 可以有貼標籤的訊框與未貼標籤的訊框，但這兩種訊框必須屬於不同的虛擬區域網路
- 對於每個虛擬區域網路，橋接器須記錄兩個集合:
  - 成員集合(Member set, Port IDs)
  - 無標籤集合(Untagged set, Port IDs)