



NTPC

D-Link產品教育訓練

D-Link Taiwan 友訊科技台灣分公司

TTSS 電信技術支援課

Name:

Phone:02-66000123,

Email:

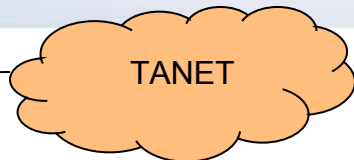
Agenda

- 現有架構說明
- 各類功能說明
- 行動學習箱使用說明
- 網路申請服務暨異動表

現有網路架構

未來學校網路架構

WiNOC認證Server
網頁集中認證伺服器



設備管理系統
Siraya Network Manager
SharkNet
Dview-7.0

DGS-3620-28TC



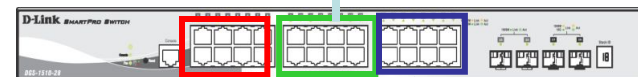
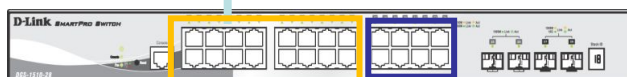
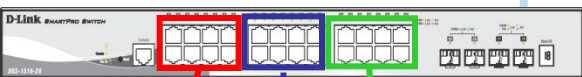
DWC-2000

DGS-1510-28XMP

10G

DGS-1510-28XMP

1G



無線網路

行政電腦

DWL-6610



電腦教室

DWL-6610

Intra-1:10.231.17.254/24



教學教室

行政電腦

無線網路

Intra-2:10.241.17.254/24

DWL-6610

LAN:163.20.169.254/24

WLAN:10.251.17.254/24

Vlan配置範例

Vlan	VID	網段	用途
Mgt	1	10.226.17.254/24	網管用
Wan	2	163.20.201.142/29	對外連結網段
Lan	5	163.20.169.254/24	行政用
dsa_wan	8	10.253.17.254/24	DSA-WAN IP (10.253.17.1)
Intra-1	10	10.231.17.254/24	電腦教室
Intra-2	20	10.241.17.254/24	教學教室
Voice	25	10.243.17.254/24	VoIP
Wlan	30	10.251.17.254/24	無線網路 (IP移至DWC-2000使用)
WPA2	35	10.245.17.254/24	無線WAP2用
MAC	36	10.247.17.254/24	無線Mobile用

無線網路認證之機制



SSID: NTPC-WPA2, eduroam

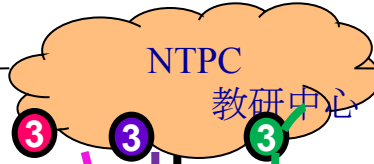


SSID: NTPC-Mobile



SSID: NTPC, TANet Roaming

WiNOC認證Server
網頁集中認證伺服器



設備管理系統
Siraya Network Manager
SharkNet
Dview-7.0

DGS-3620-28TC



1G or 10G



DWC-2000

提供5個SSID, 3種認證分流方式
不限品牌亦不用另建通道而影響效能

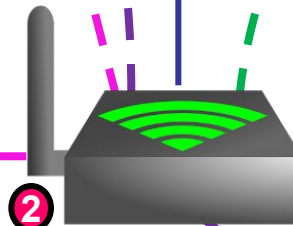
DGS-1510-28XMP



1



2



1



1



NTPC Web 認證



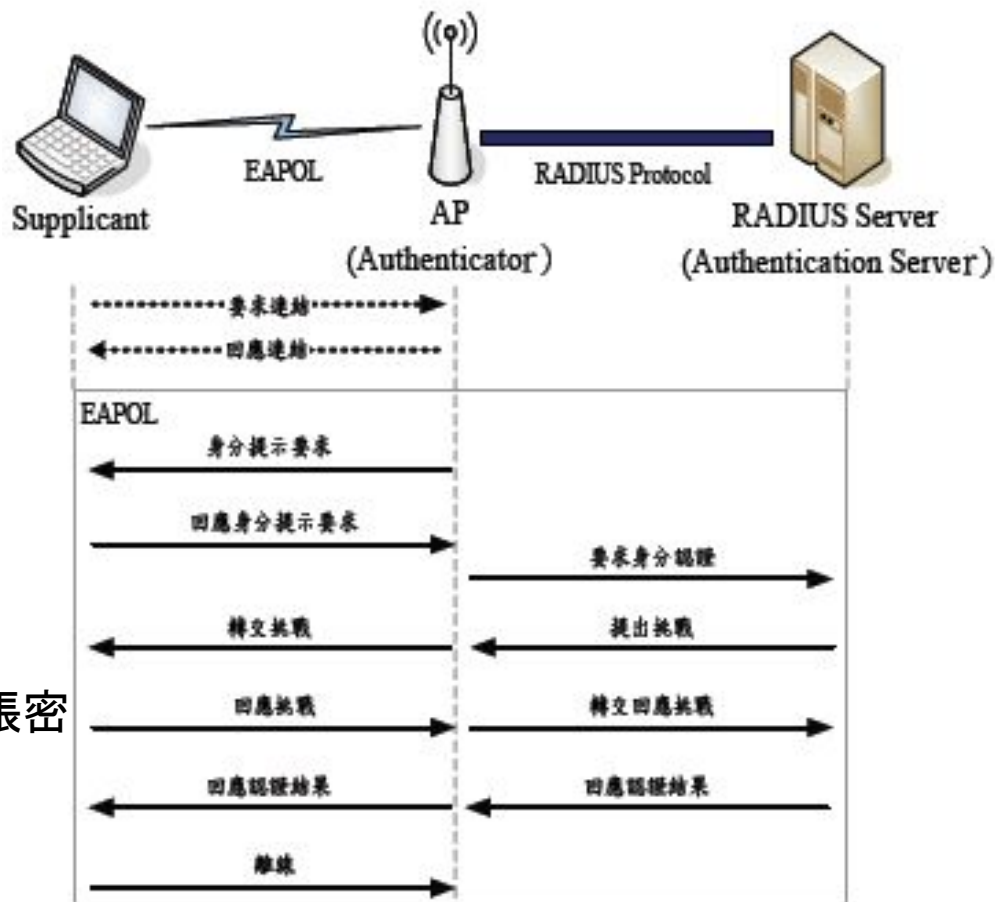
認證畫面須輸入使用者的校務行政帳密
登入之後，
使用者session 逾時，
會需要再重新認證

The screenshot shows the NTPC Web authentication page for the New Taipei City Government Education Bureau. The page features the bureau's logo and name in both Chinese and English. There are three language selection buttons: English, 繁體 (Traditional Chinese), and 簡體 (Simplified Chinese). The main text reads: '歡迎使用無線上網服務，如果您同意 [約定條款](#)，請輸入您的帳號密碼，再按下「確定」按鈕。' (Welcome to use the wireless internet service. If you agree to the [Terms of Service](#), please enter your account password and click the 'Confirm' button.) Below this, there are two input fields for '帳號' (Account) and '密碼' (Password). At the bottom, there is a checkbox labeled '我已經閱讀並同意 [約定條款](#)' (I have read and agree to the [Terms of Service](#)) and a '確定' (Confirm) button.

NTPC-WPA2 802.1x 認證



1. 認證畫面須輸入使用者的校務行政帳密
登入之後,裝置會紀錄使用者帳密
之後無須再輸入帳號密碼做驗證
即可連線無線上網



NTPC-WPA2 802.1x 認證



2. 加密方式請選PEAP
階段2驗證請選 MSCHAPV2



3. 之後再輸入校務行政系統帳號與密碼

NTPC-WPA2 802.1x 認證

WPA(Wi-Fi Protected Access)/WPA2

Wi-Fi 聯盟與IEEE 組織為了補足現有市場上無線網路產品安全性上的不足，合作訂定了WPA 的安全標準。它是為了可以立即取代現有市面上802.11 標準中的WEP 加密方式，直接透過軟體或韌體昇級即可達到較高的安全等級。它不但提供了較為強化的資料加密功能，也新增了原本在WEP 中沒有的使用者認證功能。

WPA 是IEEE 802.11i Draft 為藍圖，基本上仍然以RADIUS (Remote Authentication Dial-In User Service)為基礎，透過EAP(Extended Authentication Protocol)來進行使用者的驗證

NTPC-Mobile MAC認證

如果要新增使用者,學校管理者須先到Winoc 系統登入
登入之後再新增裝置本身的MAC資訊,以該MAC為使用者帳號做新增

新增之後,該裝置即可透過NTPC-Mobile SSID的方式登入上網
無須再跳認證畫面

NTPC-Mobile MAC認證



```
Command: show mac_based_access_control auth_state ports

(P): Port-based      Prio: Priority

Port      MAC Address          Original State      UID  Prio Aging Time/
          RX VID              Block Time
-----
12        80-01-84-13-0E-E3    36  Authenticated    -   -   1413
21        30-39-26-F1-95-91    36  Authenticated    -   -   857
22        58-48-22-B2-CF-B1    36  Blocked          -   -   245
22        7C-01-91-67-B3-1C    36  Blocked          -   -   151

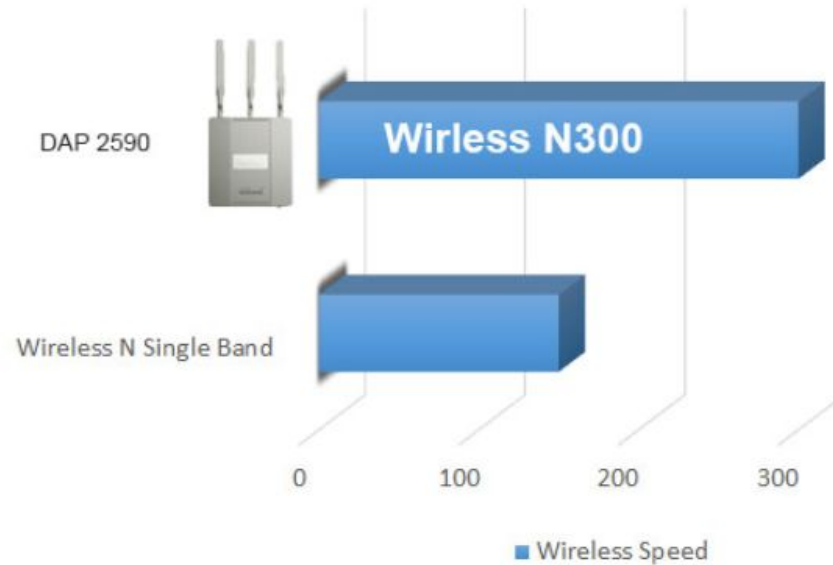
Total Authenticating Hosts : 0
Total Authenticated Hosts  : 2
Total Blocked Hosts        : 2
```

DWL-6610 VS DAP-2590



Compatibility and performance

With adjustable antennas, the DAP-2590 delivers 300Mbps per band performance



DWL-6610 VS DAP-2590



無線頻率

2.4GHz / 5GHz

最高無線訊號傳輸率

802.11 a/g: 54Mbps

802.11b: 11Mbps

802.11n: 300Mbps

802.11ac: 867Mbps

天線

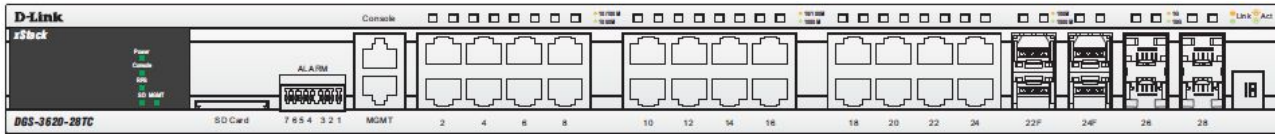
內建4組天線介面

核心交換器DGS-3620-28TC



1G 1G/10G

Layer 3 SW使用功能



- A. 學校內部各網段之間的Routing
- B. 提供DHCP Relay功能讓學校的電腦可以至中心端取得IP
- C. 提供無線NTPC-Mobile MAC認證功能
- D. 提供IPv6配發IP功能
- E. 使用vlan tag與各邊際交換器界接
- F. fiber port前四port是combo port
- G. 沒有提供POE功能

DGS-3620 IPv6 RA

在 IPv6 的環境裡, Router 的介面會定期的使用 multicast 發出 Router Advertisement (RA)。

這個 RA 包含了這個網路(網段)的 ipv6 prefix 資訊。

如果我們把介面設定成 IP 位址自動設定(autoconfiguration), 電腦的網路卡收到 RA 之後, 會利用這個 Prefix 再加上網路卡的 Interface ID (通常是使用 EUI-64 來取得) 組合成 128 bits 的 IPv6 位址。

L3使用功能:IPv6 RA

```
htjh-L3:admin#show ipv6 nd ipif lan
Command: show ipv6 nd ipif lan
```

```
Interface Name           : lan
Hop Limit                 : 64
NS Retransmit Time       : 0 (ms)
Router Advertisement      : Enabled
RA Max Router AdvInterval : 600 (sec)
RA Min Router AdvInterval : 198 (sec)
RA Router Life Time       : 1800 (sec)
RA Reachable Time        : 300000 (ms)
RA Retransmit Time       : 0 (ms)
RA Managed Flag           : Disabled
RA Other Configuration Flag : Disabled
Prefix                    Preferred Valid OnLink Autonomous
2001:288:22A3:5::/64      7200      14400    Enabled  Enabled
```

```
htjh-L3:admin#
```

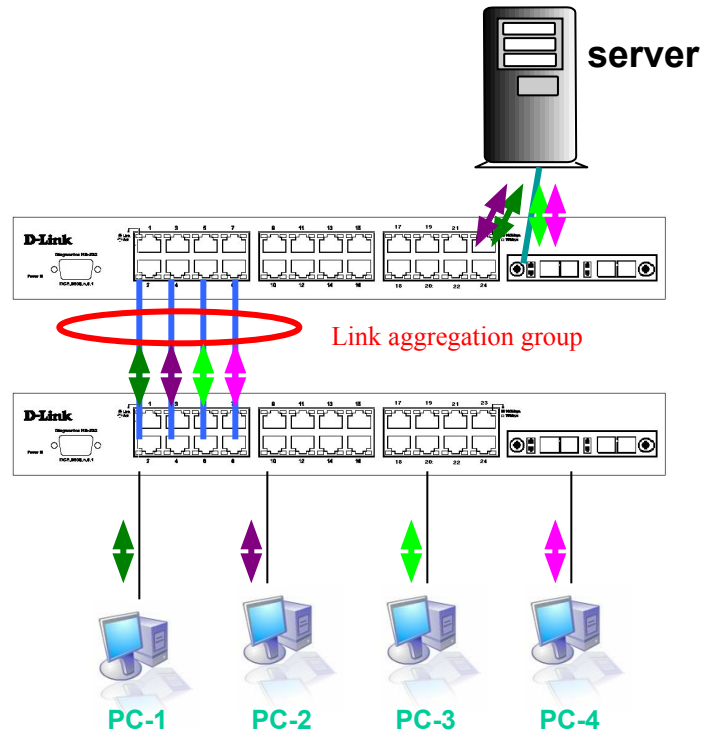


Link Aggregation

Link Aggregation

Link Aggregation主要功能有三

- (1)線路備援
- (2)頻寬加倍
- (3)流量分流



Two link Aggregation 類型

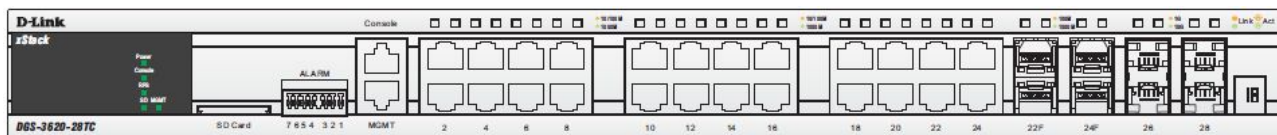
1. Static
2. IEEE 802.3ad
LACP, dynamic

L2 Switch:DGS-1510-28XMP



1G/10G

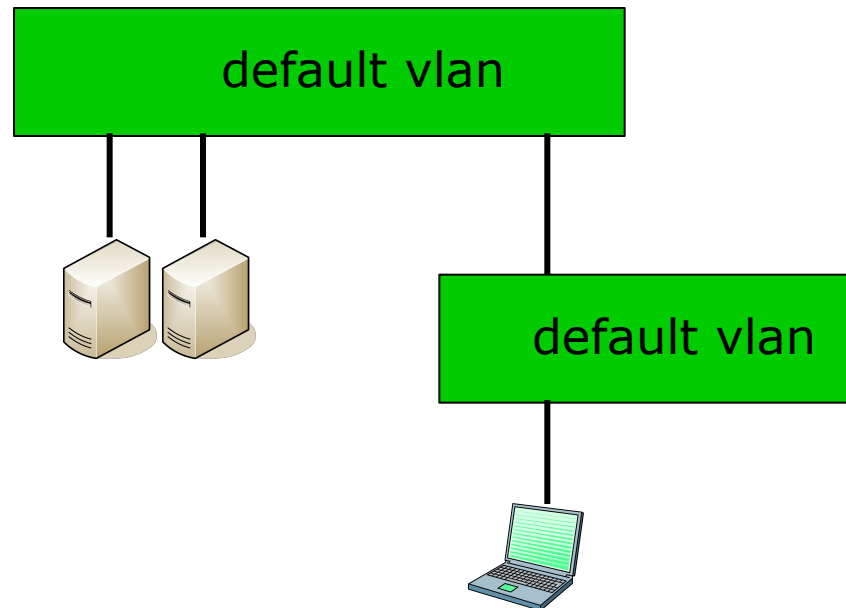
Layer 2 SW使用功能



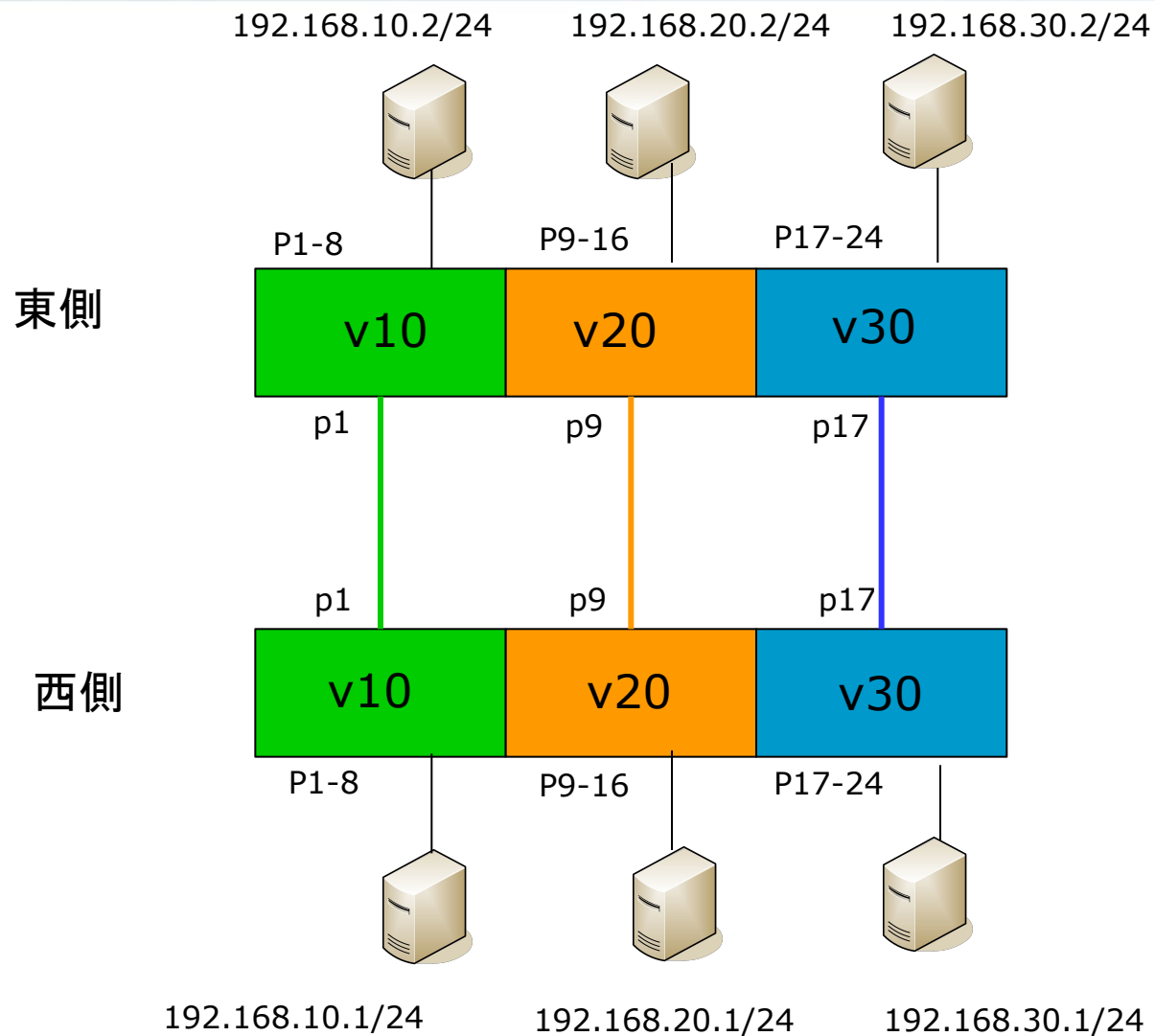
- A. 提供PoE供電能力給DWL-6610AP或是話機
- B. 提供vlan切割功能區分學校不同的內部網路
- C. 設定Loop偵測功能
- D. 設定非法DHCP Server功能

802.1Q vlan原理說明

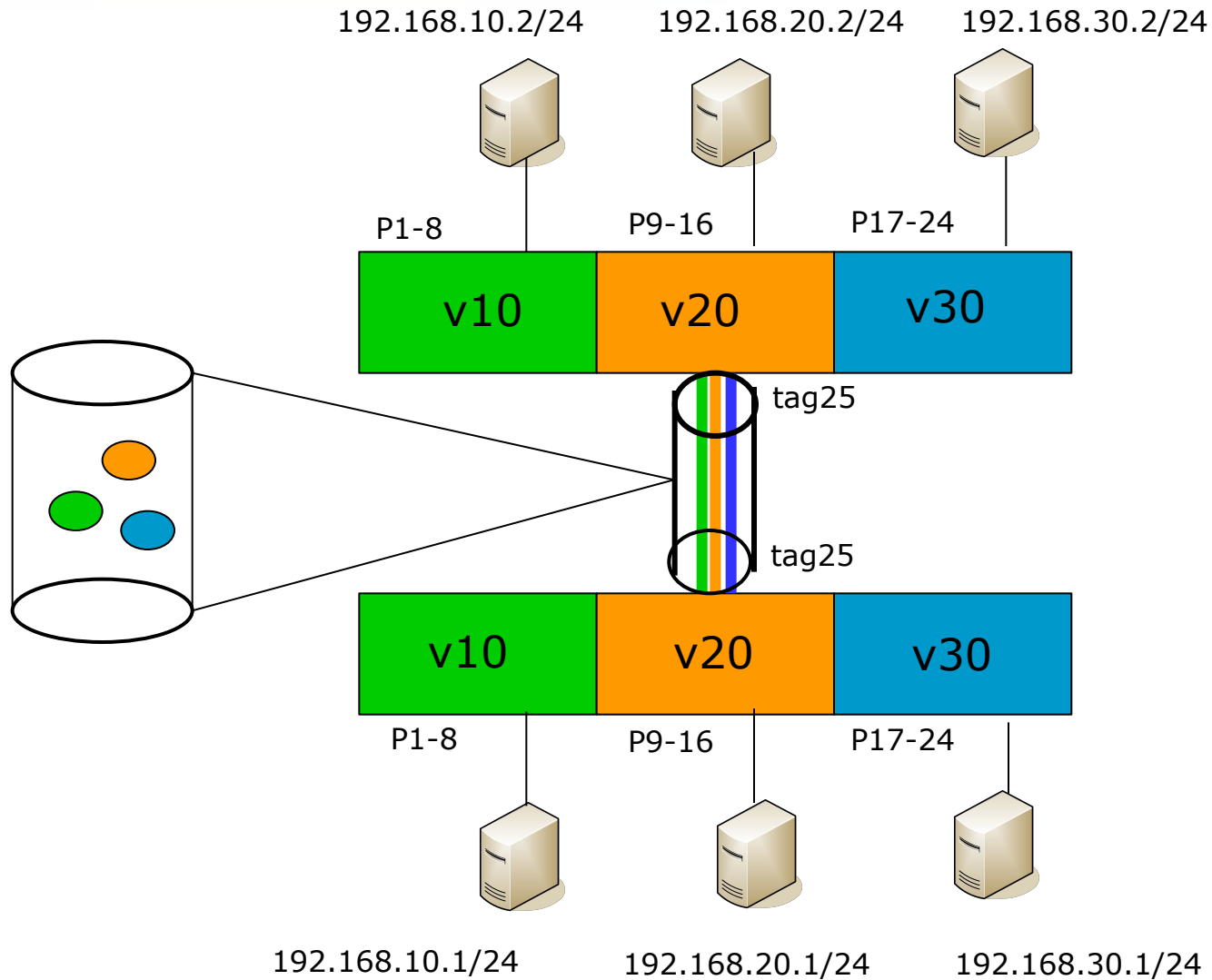
Port based vlan



Port based vlan



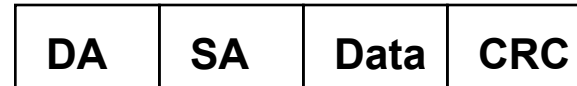
Tag based vlan



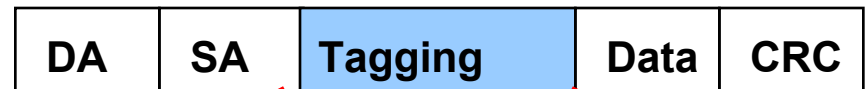
IEEE 802.1p/802.1q Frame Tagging

一般封包是untag類型,大小為
1518

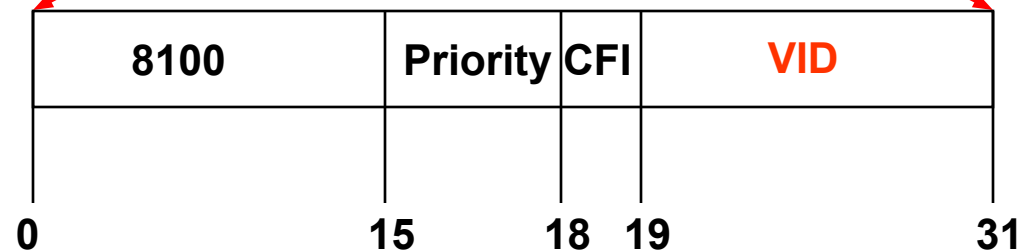
帶tag封包會加入4bytes,大小為
1522



Regular frame (or untagged frame)



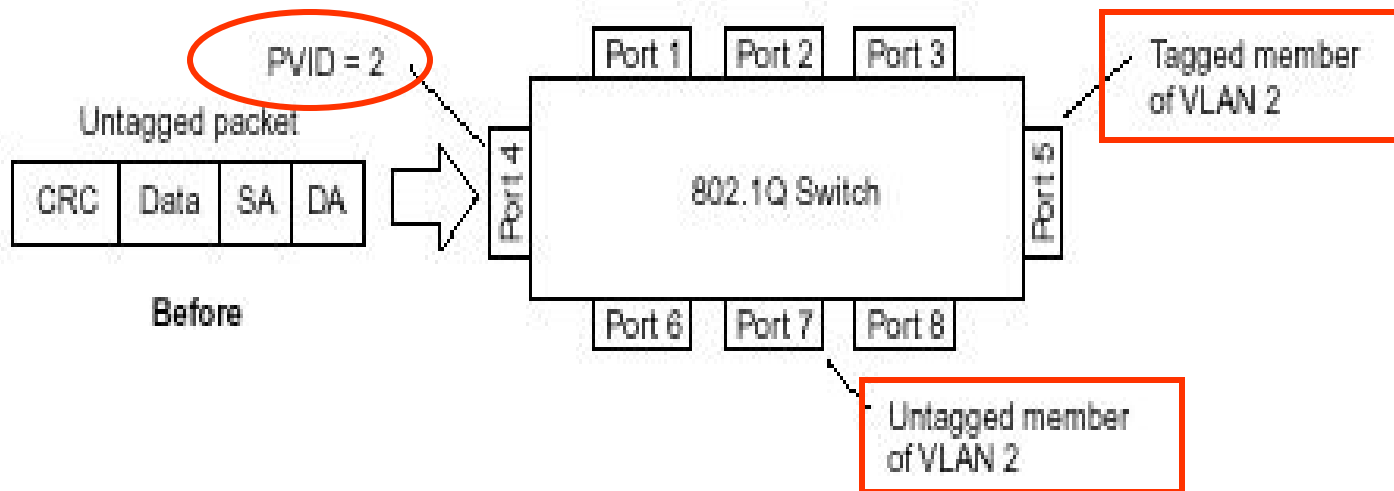
802.1q/1p tagged frame



Priority (1p) has 3 bits, 0-7.

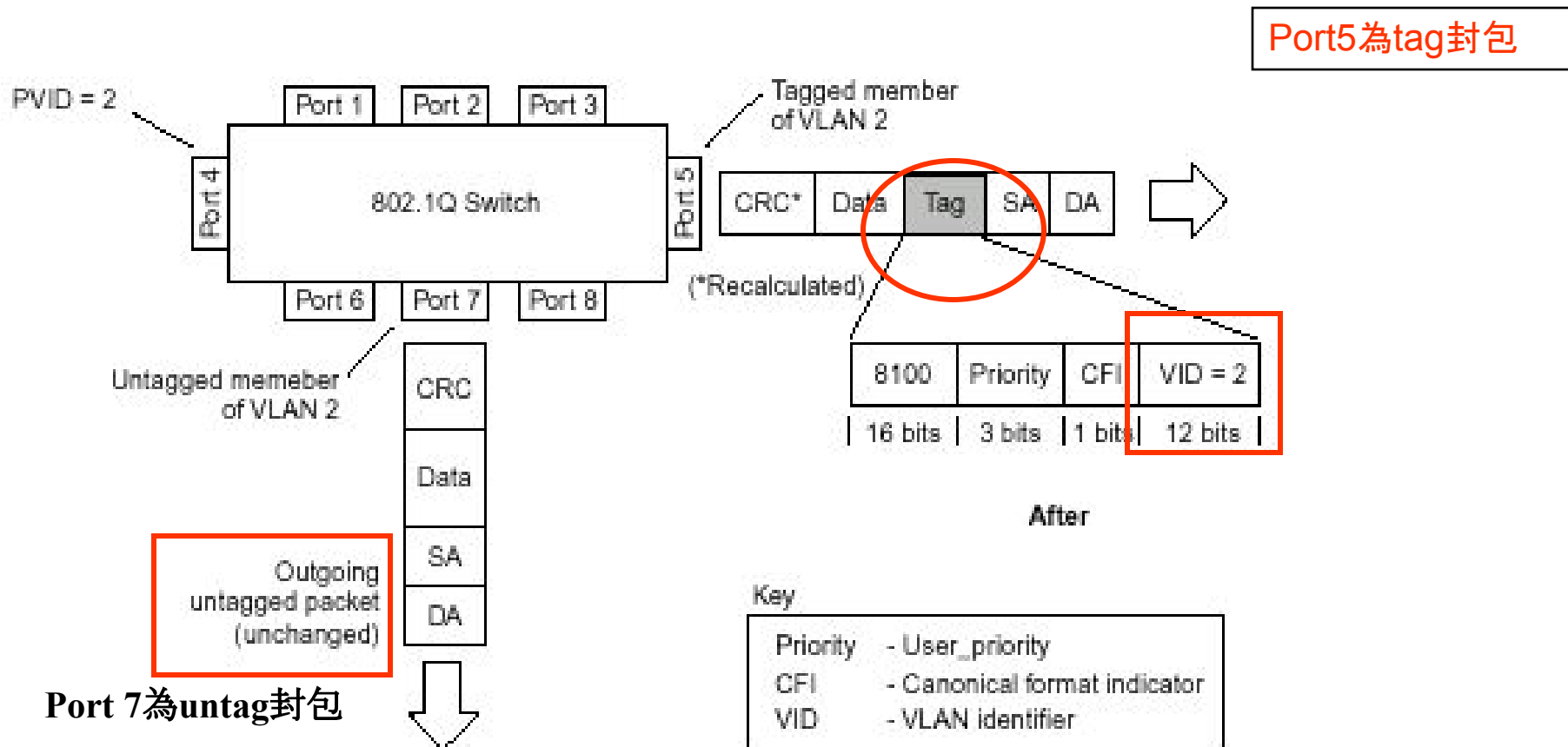
VLAN (1q) has 12 bits, 0-4095

802.1p/1q Untagged Incoming Frame



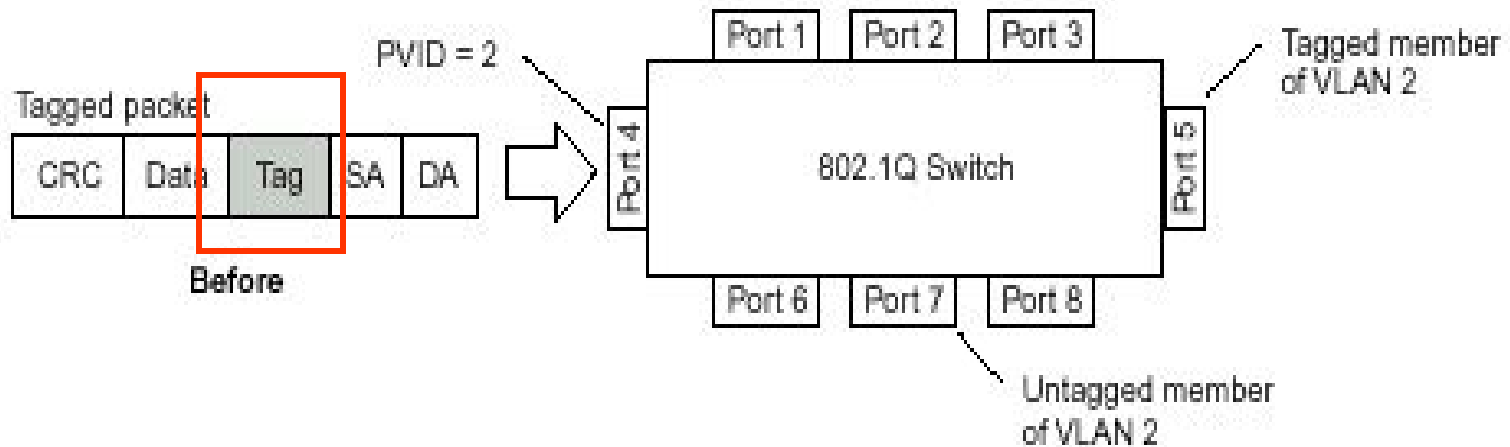
Port4收到的封包,從Port5出去為tag封包,若從Port7出去為untag封包

802.1p/1q Untagged Incoming Frame



BS45012A

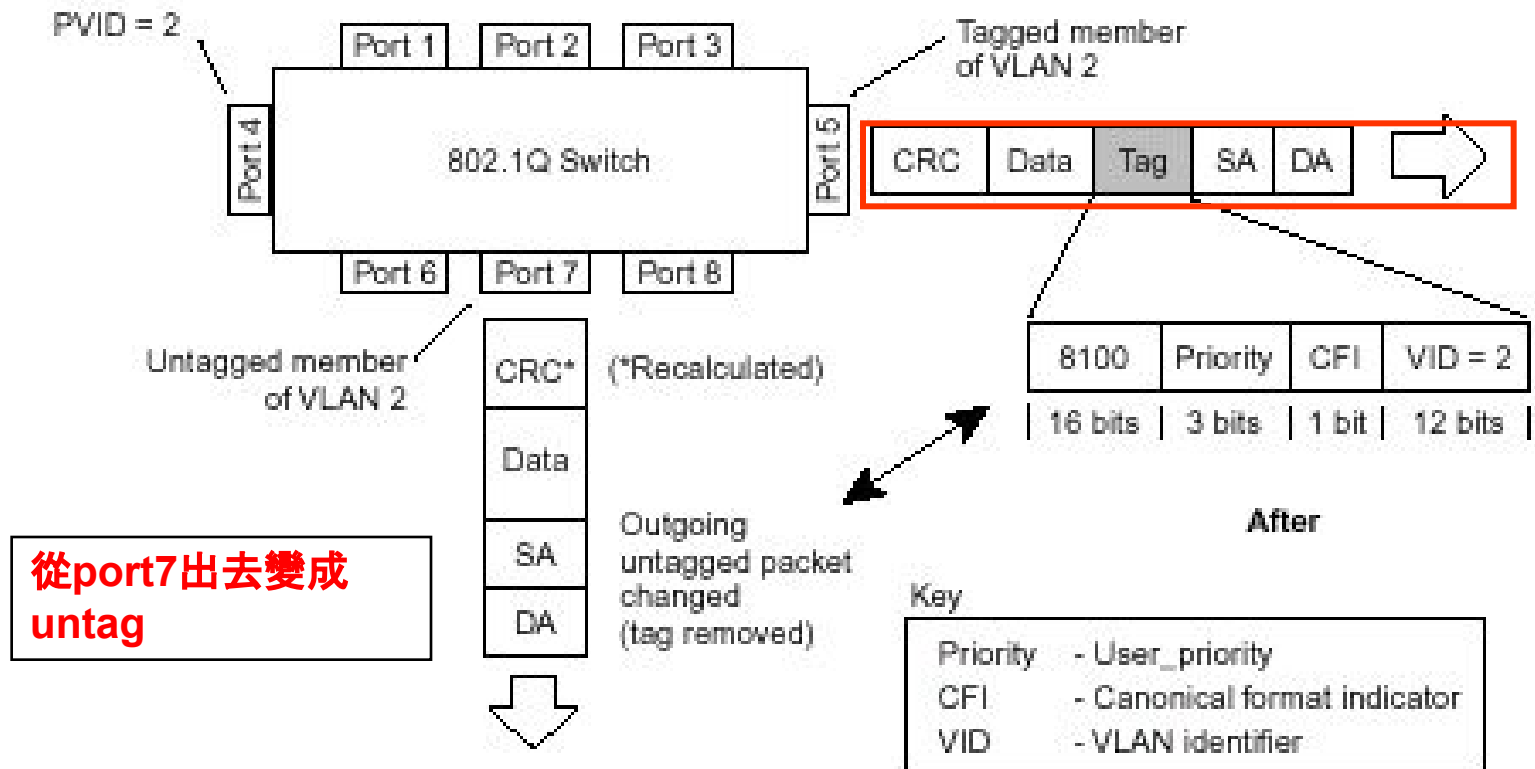
802.1p/1q Tagged Incoming Frame



Port4收到一個帶tag的封包

802.1p/1q Tagged Incoming Frame

從Port5出去變成tag

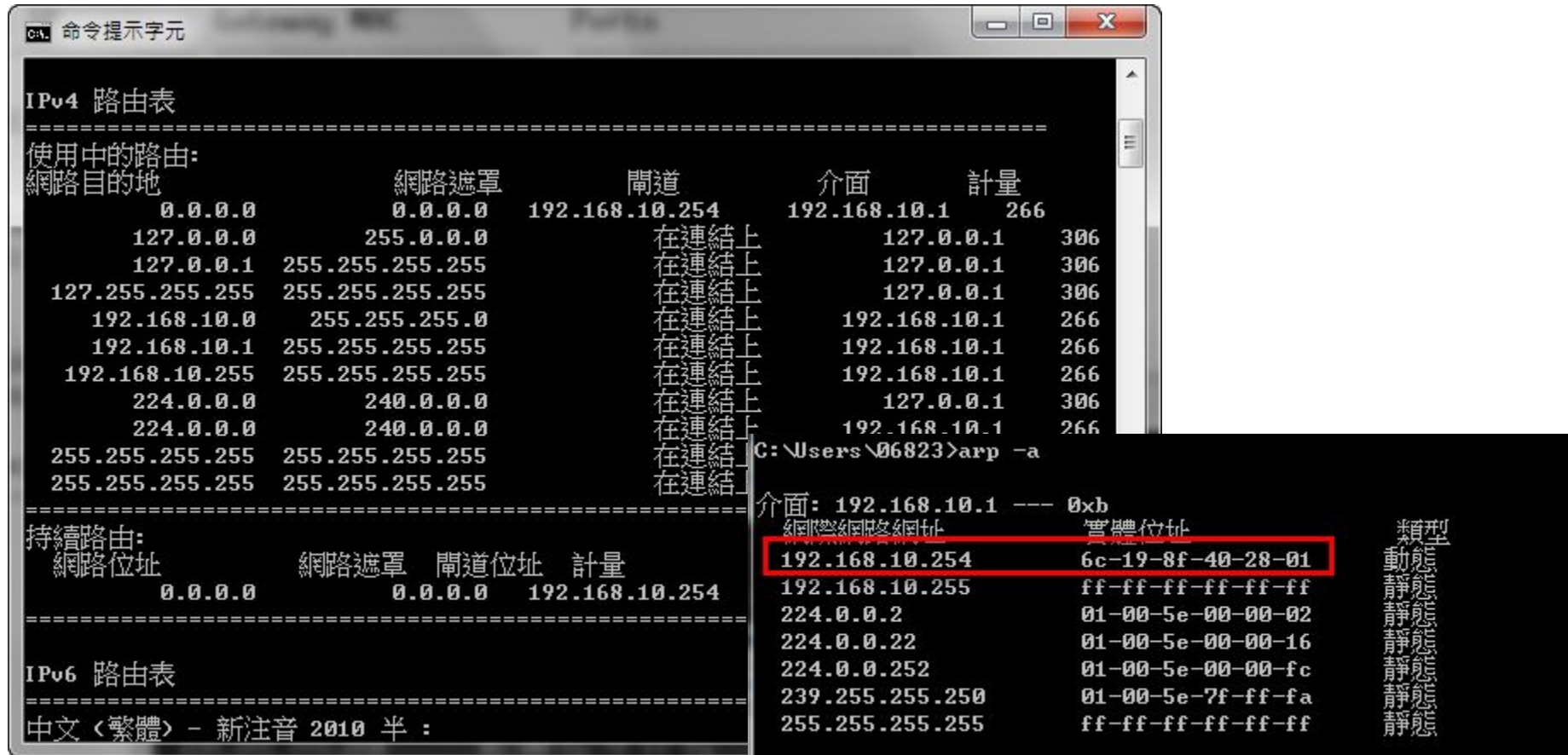


L3 routing 原理說明

Table比對順序(p1)

PC發送封包的檢查順序

- Routing table→ARP Table



The screenshot shows a Windows command prompt window titled "命令提示字元" (Command Prompt) with the following content:

```
IPv4 路由表
=====
使用中的路由:
網路目的地          網路遮罩          閘道          介面          計量
0.0.0.0              0.0.0.0           192.168.10.254  192.168.10.1   266
127.0.0.0            255.0.0.0         在連結上         127.0.0.1     306
127.0.0.1            255.255.255.255  在連結上         127.0.0.1     306
127.255.255.255     255.255.255.255  在連結上         127.0.0.1     306
192.168.10.0         255.255.255.0    在連結上         192.168.10.1  266
192.168.10.1         255.255.255.255  在連結上         192.168.10.1  266
192.168.10.255      255.255.255.255  在連結上         192.168.10.1  266
224.0.0.0            240.0.0.0         在連結上         127.0.0.1     306
224.0.0.0            240.0.0.0         在連結上         192.168.10.1  266
255.255.255.255     255.255.255.255  在連結上
255.255.255.255     255.255.255.255  在連結上

=====
持續路由:
網路位址          網路遮罩  閘道位址  計量
0.0.0.0           0.0.0.0   192.168.10.254
=====

IPv6 路由表
=====
中文 <繁體> - 新注音 2010 半 :
```

Below the routing table, the command prompt shows the execution of the ARP command:

```
C:\Users\06823>arp -a
介面: 192.168.10.1 --- 0xb
網路網路網路地址  實體位址  類型
192.168.10.254     6c-19-8f-40-28-01  動態
192.168.10.255     ff-ff-ff-ff-ff-ff  靜態
224.0.0.2           01-00-5e-00-00-02  靜態
224.0.0.22          01-00-5e-00-00-16  靜態
224.0.0.252         01-00-5e-00-00-fc  靜態
239.255.255.250     01-00-5e-7f-ff-fa  靜態
255.255.255.255     ff-ff-ff-ff-ff-ff  靜態
```

Table比對順序(p2)

Switch接收到封包後,要轉送的檢查順序

- Routing Table--> ARP Table --> FDB Table

Routing table

```
DGS-3620-28TC:admin#show iproute  
Command: show iproute
```

Routing Table

IP Address/Netmask	Gateway	Interface	Cost	Protocol
192.168.10.0/24	0.0.0.0	v10	1	Local
192.168.20.0/24	0.0.0.0	v20	1	Local
192.168.30.0/24	0.0.0.0	v30	1	Local

Total Entries: 3

Table比對順序(p2)

Switch接收到封包要轉送的檢查順序

- Routing Table--> ARP Table --> FDB Table

ARP table

```
DGS-3620-28TC:admin#show arpentry
Command: show arpentry
```

```
ARP Aging Time : 20
ARP Retry Times : 4
```

Interface	IP Address	MAC Address	Type
v10	192.168.10.0	FF-FF-FF-FF-FF-FF	Local/Broadcast
v10	192.168.10.1	00-1C-23-54-C6-D4	Dynamic
v10	192.168.10.254	6C-19-8F-40-28-01	Local
v10	192.168.10.255	FF-FF-FF-FF-FF-FF	Local/Broadcast
v20	192.168.20.0	FF-FF-FF-FF-FF-FF	Local/Broadcast
v20	192.168.20.254	6C-19-8F-40-28-02	Local
v20	192.168.20.255	FF-FF-FF-FF-FF-FF	Local/Broadcast
v30	192.168.30.0	FF-FF-FF-FF-FF-FF	Local/Broadcast
v30	192.168.30.254	6C-19-8F-40-28-03	Local
v30	192.168.30.255	FF-FF-FF-FF-FF-FF	Local/Broadcast

```
Total Entries: 10
```

Table比對順序(p2)

Switch接收到封包要轉送的檢查順序

- Routing Table--> ARP Table --> FDB Table

FDB table

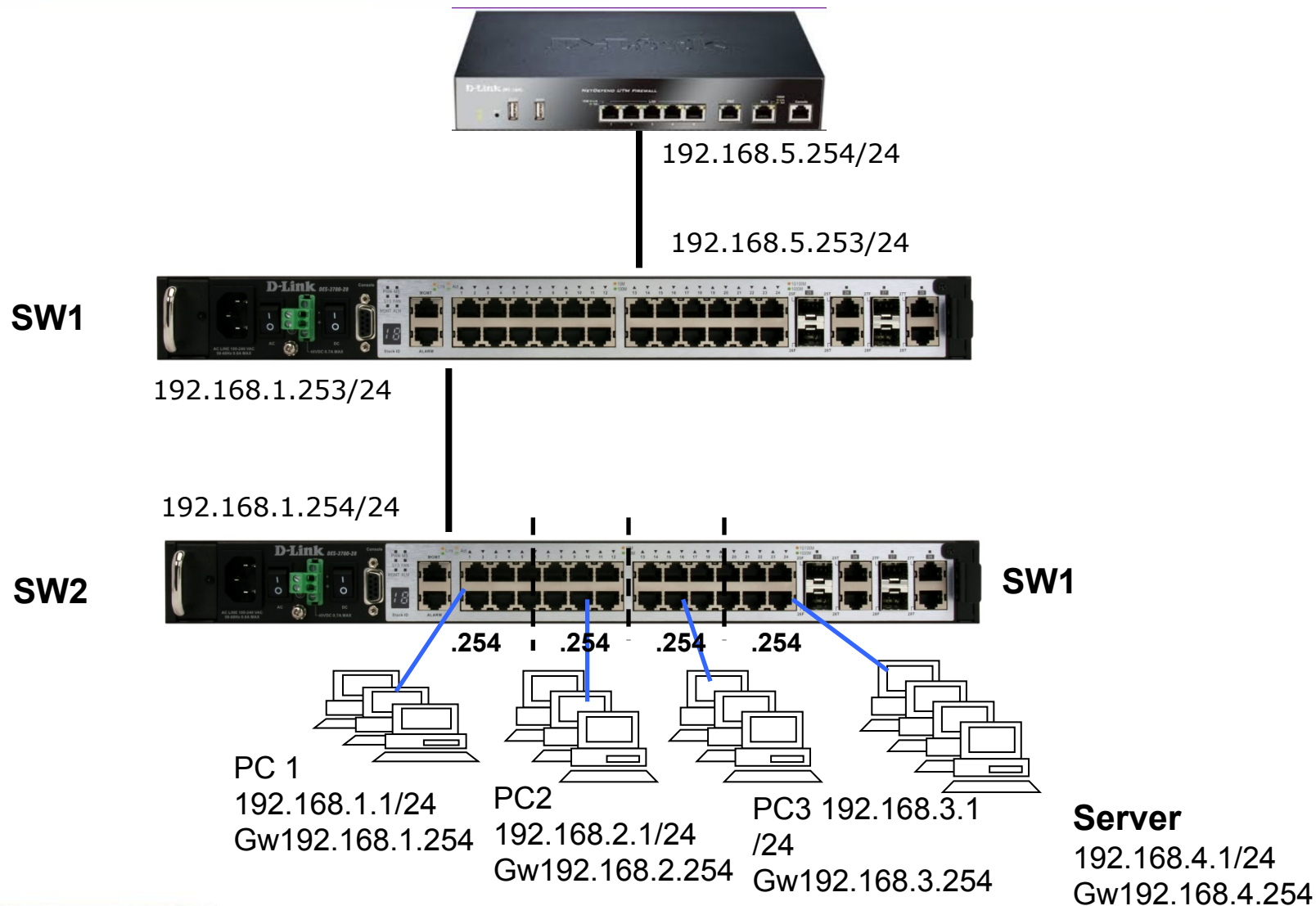
```
DGS-3620-28TC:admin#show fdb  
Command: show fdb
```

```
Unicast MAC Address Aging Time = 300
```

VID	VLAN Name	MAC Address	Port	Type	Status
1	default	6C-19-8F-40-28-00	CPU	Self	Forward
10	v10	00-1C-23-54-C6-D4	1	Dynamic	Forward
10	v10	6C-19-8F-40-28-01	CPU	Self	Forward
20	v20	6C-19-8F-40-28-02	CPU	Self	Forward
30	v30	6C-19-8F-40-28-03	CPU	Self	Forward

```
Total Entries: 5
```

跨設備的IP Routing—static route



PoE

PoE: power over ethernet

- 802.3af: 提供44~57V的電壓, 約350mA的直流電源, 每一port至少要可提供**15.4W**的功率, 而經過100米的cable線後, PD端可受到的瓦特數至少要有12.95W
- 802.3at: PSE端提供50~57V的電壓, 約600mA的直流電源, 每一port至少要可提供**30W**的功率, 經過100米CAT-5的電纜線後, PD端可收到的瓦特數至少要有25.5W

PSE:(Power sourcing equipment): 供電端

PD:(Powered Device) 受電端

PoE說明:

具備PoE功能的交換器,預設PoE功能是開啟,因此PD設備接上去後,

就會自動溝通取得class級別後供電使用,無需特別設定每台設備PoE供電總瓦數不同,

例如有些170W,有些為370W,因此不見得整台設備同時每個Port都

可以接上PD,因為可能已經超過總瓦數若PD設備需要使用30W的電

力,

需特別注意交換器是否有支援802.3at,以及是否每個port都可以支援802.3at還是只有特定幾個 port

PoE供電心線

- D-Link Switch follows the standard PSE (Power Sourcing Equipment) pinout *Alternative A*, whereby power is sent out over pins *1, 2, 3 and 6*.

Based on 802.3af/at PDs receive power according to the following classification:

Class	Maximum power available to PD
0	15.4W
1	4.0W
2	7.0W
3	15.4W
4	30W

PSE provides power according to the following classification:

Class	Max power used by PSE
0	16.2W
1	4.2W
2	7.4W
3	16.2W
User define	31.2W

POE DGS-3100 VS DGS-1510



具備24埠 10/100/1000Mbps + 4埠 1G combo SFP+獨立Console
埠
DGS-3100-24P - 802.3af/24/370W

Power Over Ethernet	802.3af PoE Support	Per 10/100/1000BASE-T Port
	Power Provision Per Port (Max.)	15.4 W
	System PoE Power Budget	370 W

POE DGS-3100 VS DGS-1510



具備24埠 10/100/1000Mbps + 4埠 10G SFP+ 網路連接埠與獨立 Console埠。

內建2個10G SFP+網路埠具備實體堆疊功能，支援40Gbps堆疊頻寬與6台交換器實體堆疊。

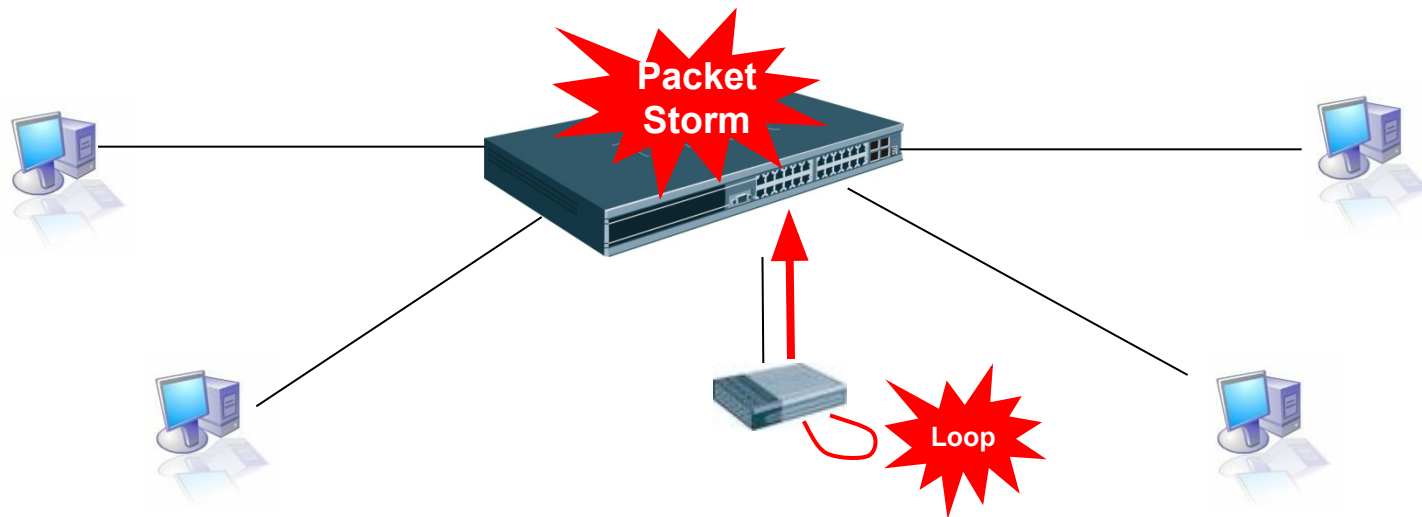
POE供電最大為370W。

PoE	
PoE Standard	IEEE 802.3af, 802.3at PoE Capable
PoE Capable Ports	Ports 1 to 24: Up to 30 W
PoE Power Budget	Max. 370 W

Loop detect

問題:網路迴圈

- 使用者以自備交換器連結網路，造成無法預期的迴圈。
- 迴圈導致封包風暴，癱瘓整個網路。



解決網路迴圈問題

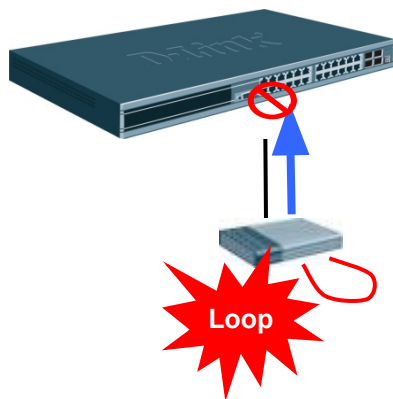
D-Link解決方案: Loopback Detection (LBD v4.04)

STP (Spanning Tree Protocol) Independent

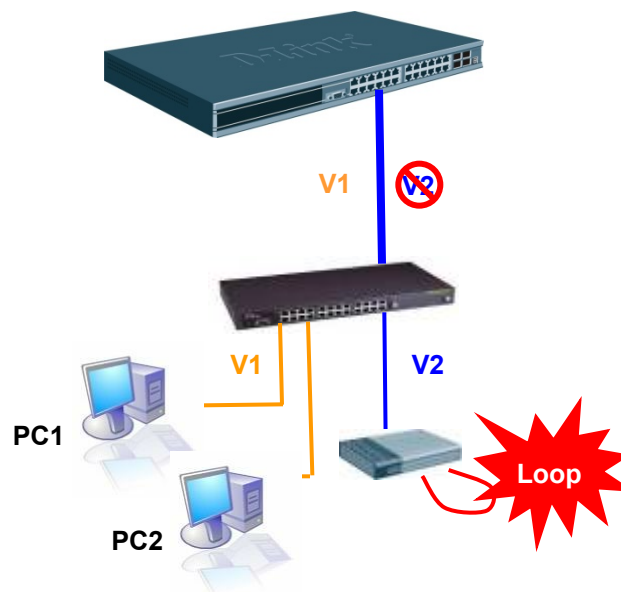
無網管型交換器不具備Spanning Tree Protocol功能。
D-Link交換器設計即使不開啟STP功能, 亦可偵測出Loop。

LBD彈性設定, 防止迴圈

Port-based
VLAN-based



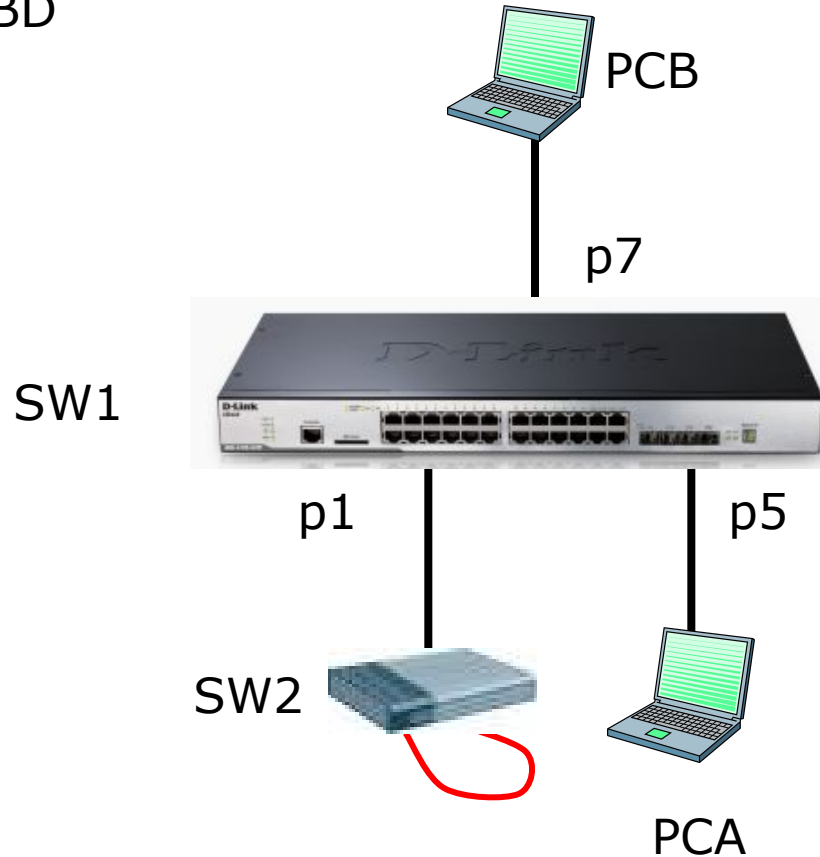
1. Port-based LBD
- 連接埠關閉, 無流量可通過。



2. VLAN-based LBD
- 依據發生迴圈的VLAN阻擋流量, 該連接埠不關閉。

Loopdetect-Topology1

Port based LBD



目前新北市所有學校的LBD功能全開啟偵測使用中

非法DHCP Server阻擋

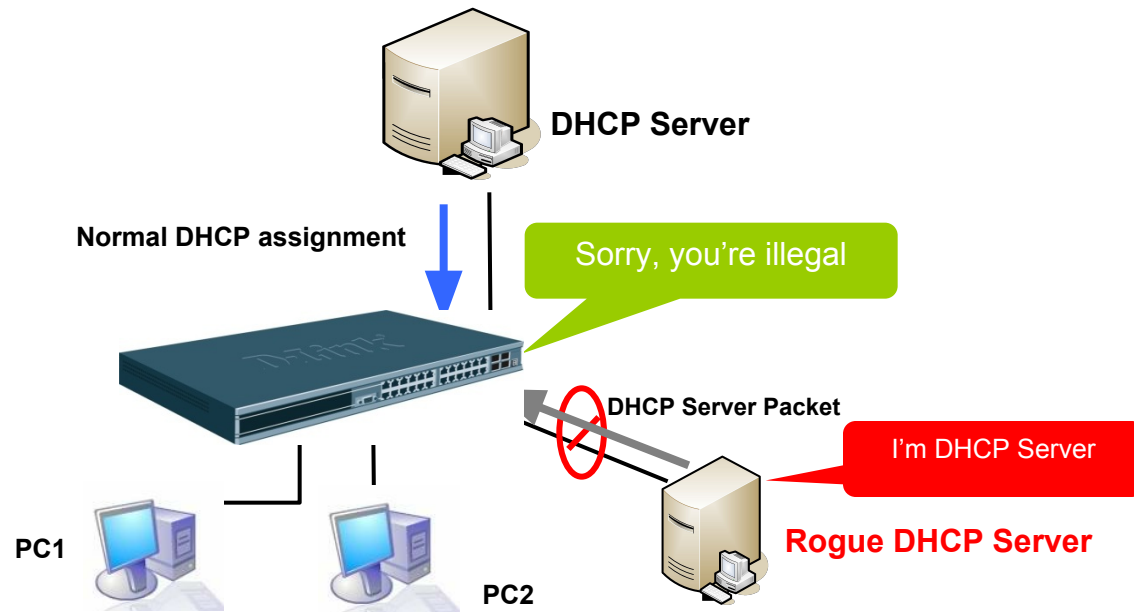
問題:非法DHCP Server

問題:使用者自行架設DHCP伺服器。

衝擊:IP指派不正確, 干擾網路連結。

D-Link解決方案: **DHCP Server Screening**

從使用者連接埠鎖定DHCP伺服器封包, 防止未授權IP指派。



阻擋非法DHCP Server

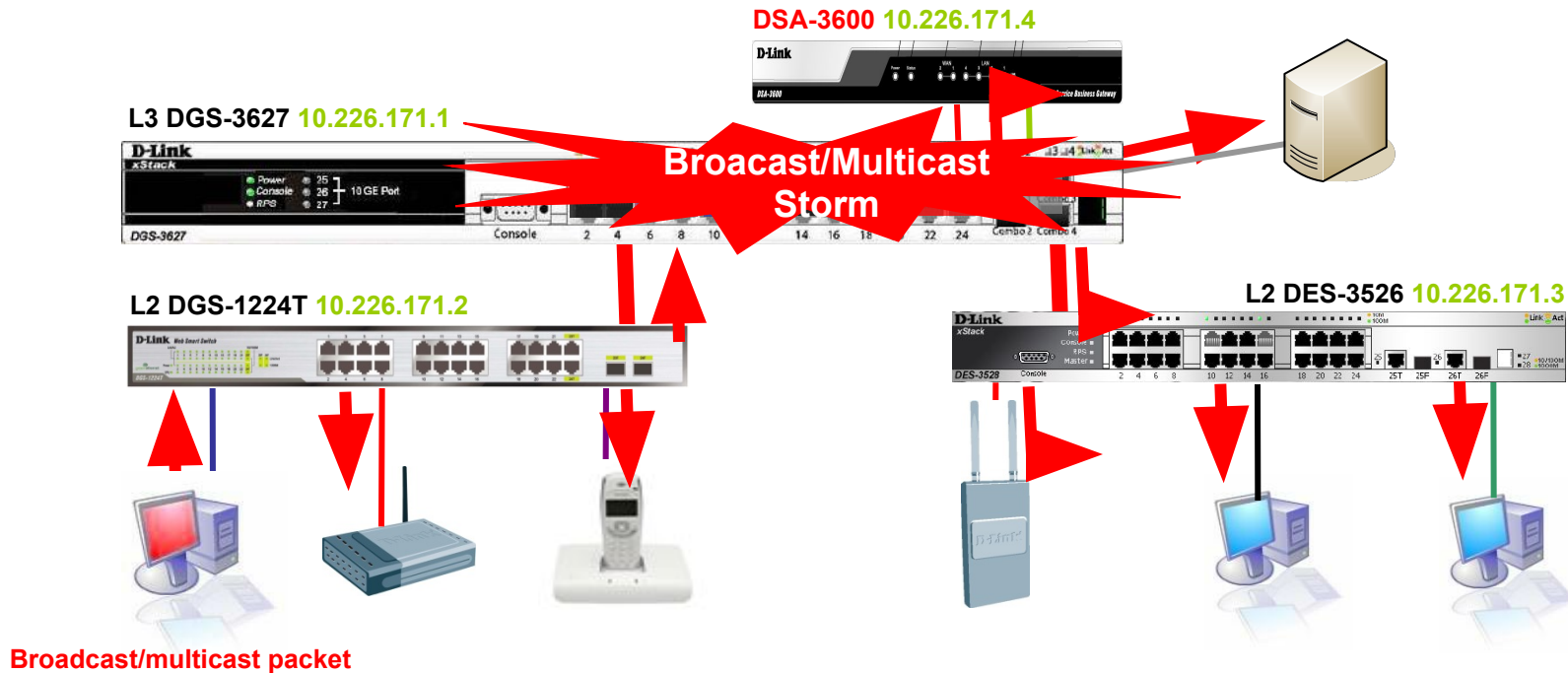
- Port24為uplink port
-
-
- 不指定DHCP Server IP,透過Port來限制,所以合法Server的port24不啟動
- Port1-23過濾非法DHCP Server
-
- Switch(config)#interface range ethernet 1/0/1-23
- Switch(config-if-range)#ip dhcp snooping server-screen
-
- Port 7上一台非法DHCP Server 192.168.1.1送出DHCP封包給client

電腦教室網路

- 如果電腦教室的vlan有架設DHCP Server而非使用教研中心的DHCP Server,那麼配於電腦教室的L2 Switch則於特定的Port關閉非法DHCP Server的功能!
- 要開啟關閉此功能,請先與教網中心確認該台交換器是否只有一port需要 dhcp server的發放行為
- 目前DHCP Server Screening預設不開,原因是怕影響到校內群準系統的運作

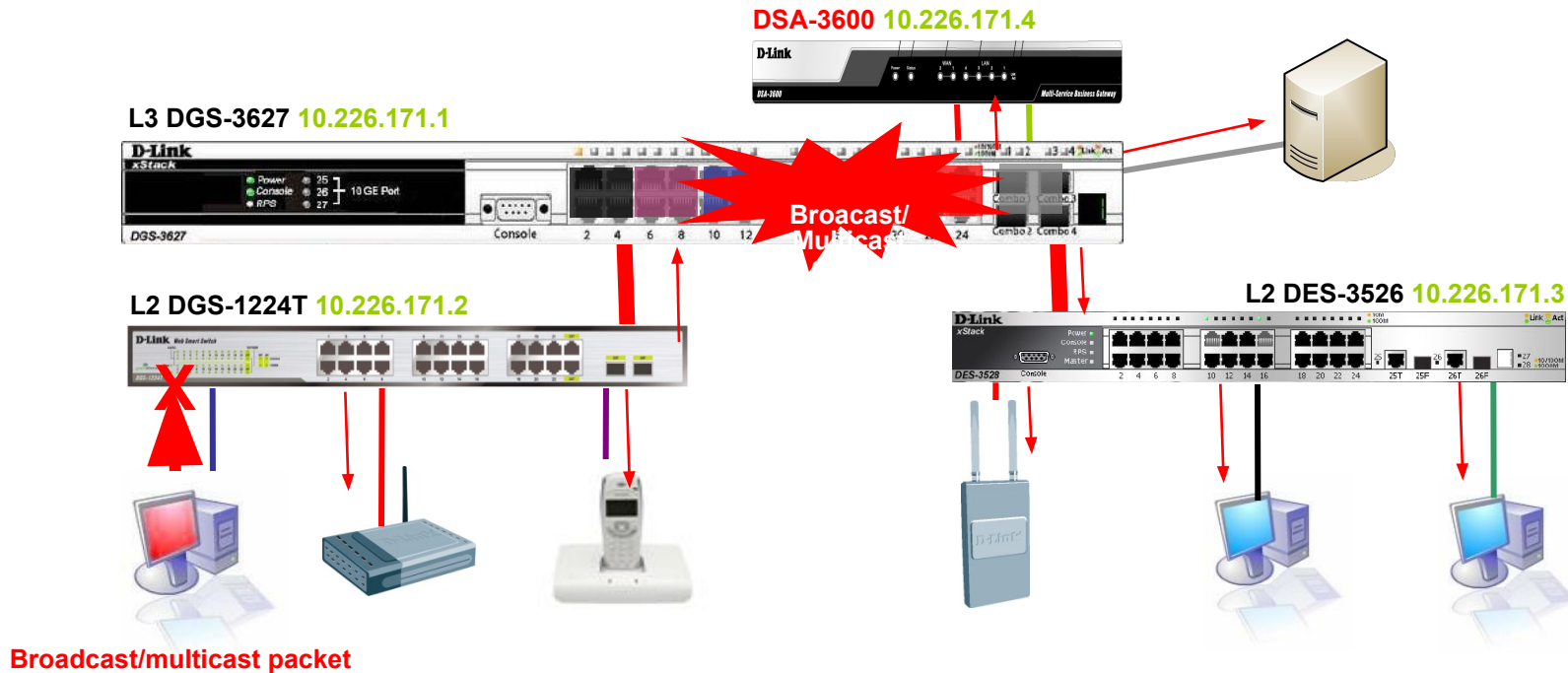
問題:廣播/群播攻擊

- 遭受病毒感染的PC,其攻擊行為是產生大量廣播或群播流量來癱瘓網路



解決方案:風暴抑制

- 藉由風暴抑制的功能可以選擇抑制流量或是關閉該Port來解決



DWC-2000無線控制器

無線網路認證之機制



SSID: NTPC-WPA2, eduroam

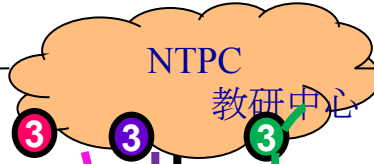


SSID: NTPC-Mobile



SSID: NTPC, TANet Roaming

WiNOC認證Server
網頁集中認證伺服器



設備管理系統
Siraya Network Manager
SharkNet
Dview-7.0

DGS-3620-28TC



1G or 10G



DWC-2000

提供5個SSID, 3種認證分流方式
不限品牌亦不用另建通道而影響效能

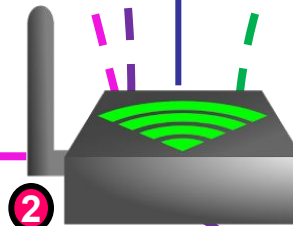
DGS-1510-28XMP



1



2



1



1



無線控制器功能

- A. 監控DWL-6610AP
- B. 統一調整DWL-6610AP設定檔或是昇級版本
- C. 提供WEB認證導外部WEB Server的功能
- D. 提供AP 802.1x認證的代理詢問角色

行動學習活動組

➤ 輕便型行動學習活動組

- 外觀尺寸:W(26) X D(18.5)X H(18)CM
- 放置DWL-6610x2+DGS-1008Px1

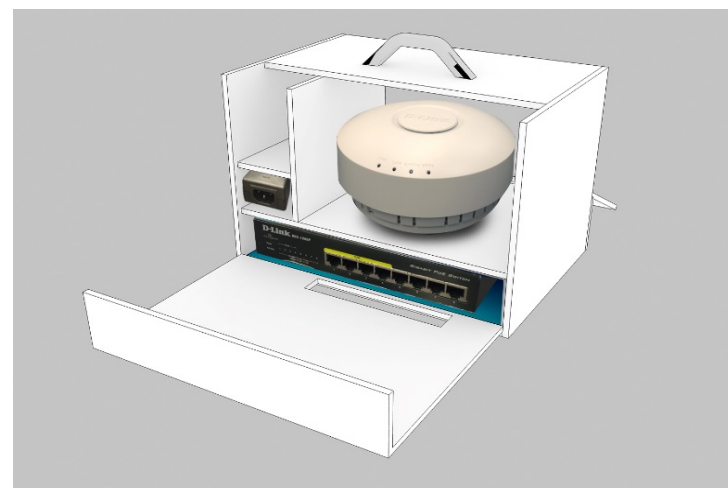
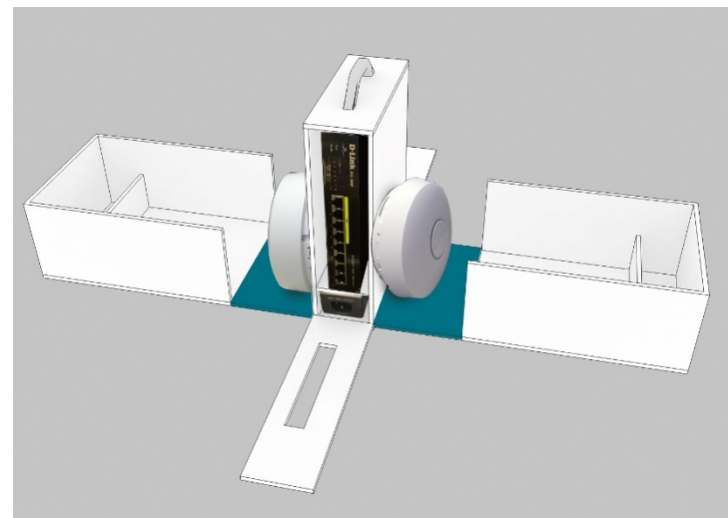
➤ 簡易型行動學習活動機箱

- 外觀尺寸:W(27)X D(17.5)X H(22.3)CM
- 放置DWL-6610x1+DGS-1008Px1

➤ 額外提供

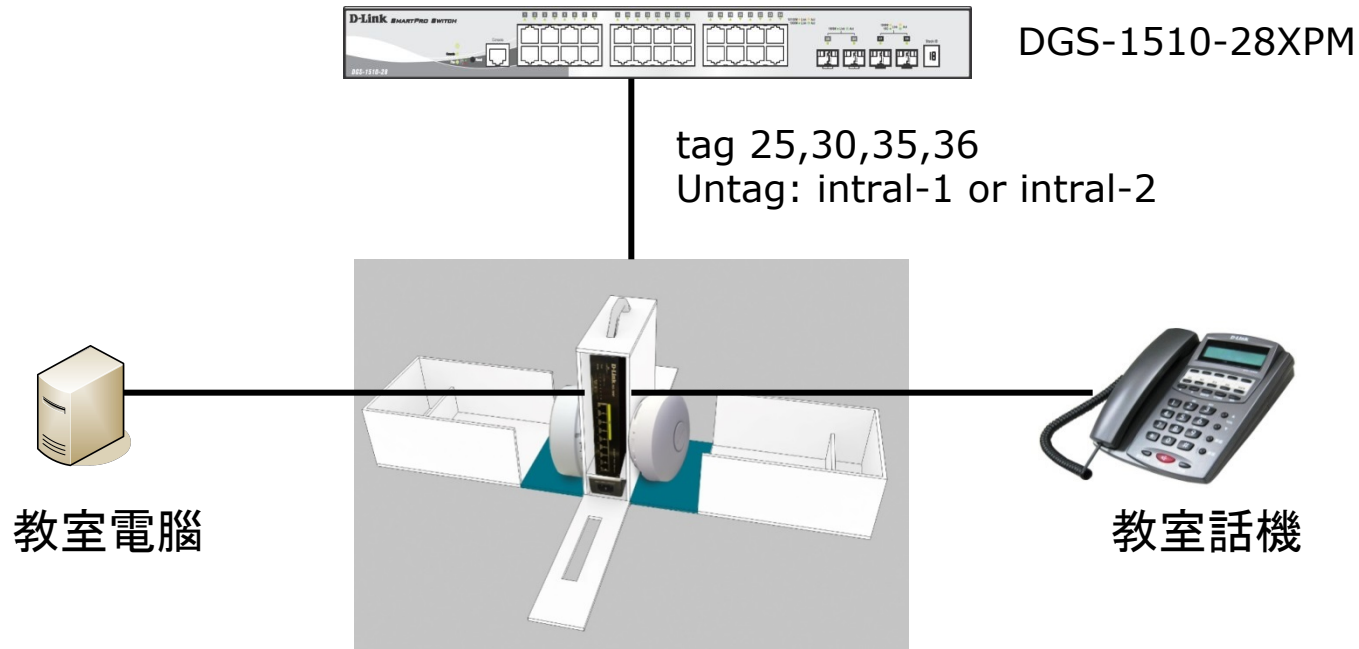
行動輕習新美學(無線型行動箱)管理功能

Safe, Solid, and Simple



行動學習活動組

- 屬於固定式AP的延伸,具備相同的5個SSID,即插即用



網路申請服務暨異動表



新北市政府教育局

教育網路服務

Informat

Quick Menu

- 組織簡介
- 認證服務
- 網路服務
- 資訊安全
- 校園網站服務
- 研習培訓及推廣
- 教學資源
- 專案活動
- 資訊教育成果
- 標案資訊
- 下載專區

首頁 > 下載專區

網路服務申請暨異動表

新北市政府教育局網路服務啟用暨異動申請表(20121211)

友善列印 分享

網路申請服務暨異動表

申請項目			
<input type="checkbox"/> DNS 伺服器集中管理： <input type="checkbox"/> 加入 <input type="checkbox"/> 退出 網域名稱_____			
退出者請續填： DNS 主機名稱_____ 主機位址_____			
<input type="checkbox"/> DHCP 設定變更：VLAN_____ / _____			
<input type="checkbox"/> IP Range：_____ ~ _____			
<input type="checkbox"/> Lease Time：_____			
<input type="checkbox"/> 其它補充說明 _____ _____			
承辦人 核章		單位主管 核章	機關首長 核章

網路申請服務暨異動表

如欲開啟需送申請單,並附註哪個port不需開啟,不開啟的原因稍微敘述
申請步驟同Siraya 之snm vlan設定申請,請在更新 如下圖範例

[有線設備] snm vlan 設定申請

申請項目

DNS 伺服器集中管理：加入 退出
網域名稱 _____
退出者請填寫：DNS 主機名稱 _____ 主機位址 _____

DHCP 設定變更：VLAN _____ / _____
 IP Range：_____ ~ _____
 Lease Time：_____

其它補充說明

承辦人 核 章	4.填寫申請內容	單位主管 核 章	機關首長 核 章
------------	----------	-------------	-------------

1.進入下載區

2.點選此表格

3.下載表格附件

4.填寫申請內容

- 申請snm vlan 設定申請的相關資訊
下載網址 <http://enctc.ntpc.edu.tw/>
下載位址 下載專區 / “網路服務申請暨異動表”
- 請填妥申請單,檢附相關附件,經貴機關首長核章後,正本郵寄至
22057 新北市板橋區橋中一街1-1號 新北市教育局教育研究發展科 資教股 收
急件請核章完後先行傳真至 (02) 89682278 並致電 (02) 80723456 #516 或 #517
或掃瞄所有頁面後,以電子郵件寄至 network@ntpc.edu.tw 並致電資教股

42



Q&A
Thank you