新北市教育網路
SNGN校園骨幹架構
基礎網路實作

輔導員

李 煒

alfred@ntpc.edu.tw

80723456#517

新北市教網

課程時間分配

時間	課程內容
09:00-12:00	網路基本原理 IP netmask gateway dns Local Dhcp DHCP Proxy L2 Vlan L3 NAT VPN 500M
13:00-16:00	無線網路架構說明、 認證伺服器Radius Server、 NTPC、NTPCRoaming、NTPC-Mobile NTPC-WPA2 、EduRoam 話機VOIP、IPPBX Winoc 、Siraya
	校園監視器、電子圍籬、地震系統
	Nts.tanet.edu.tw

個人PC網路設定

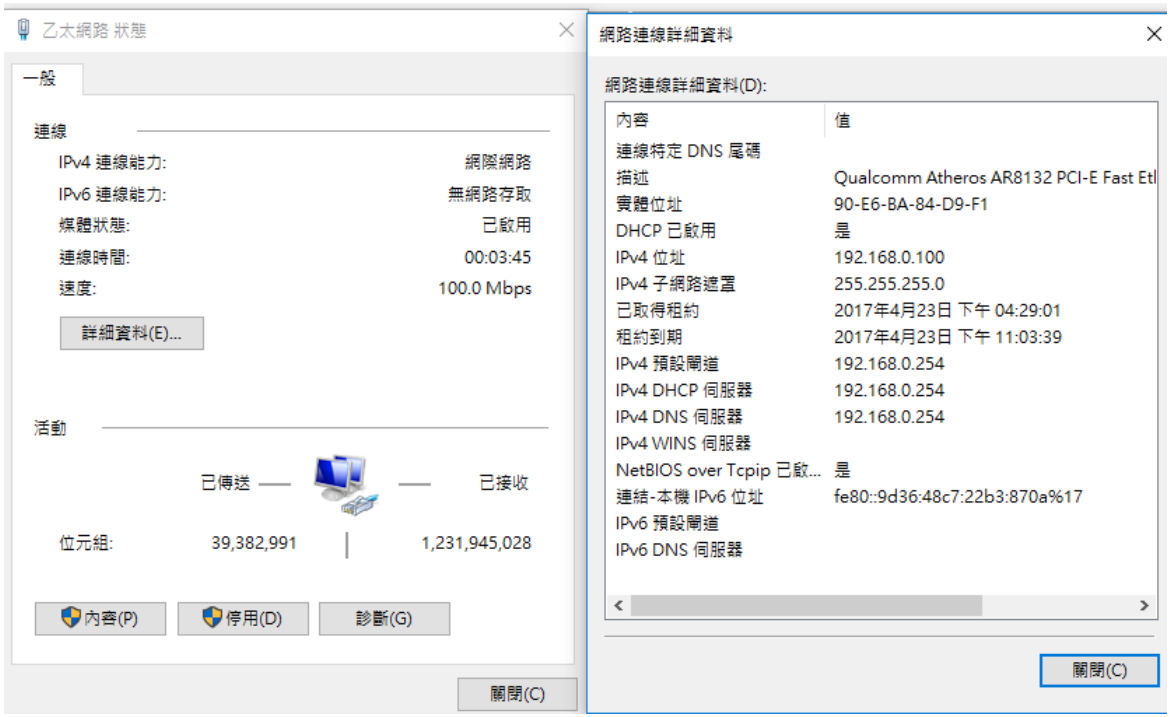
- 目的：了解PC網路設定
- IP 地址-IPv4 and IPv6
- 遮罩用途: 演算內外網判別。
- Gateway 用途， Gateway在哪裡??
- 常用指令
  - Ipconfig/all ipconfig/flushdns
  - Ping
  - Nslookup
  - Tracert
  - Route print

電腦開機程序及網頁開啟行為

- 電腦開機程序
  - 找尋DHCP server
  - DHCP取得ip或是自訂ip
  - DHCP取得dns或是自訂dns
- 網頁開啟行為
  - DNS 詢問IP
  - 取得ip上網
  - PC->L 3 Switch GW->F/W->Core->DNS
  - PC->L 3 Switch GW->F/W->Core->NCCU

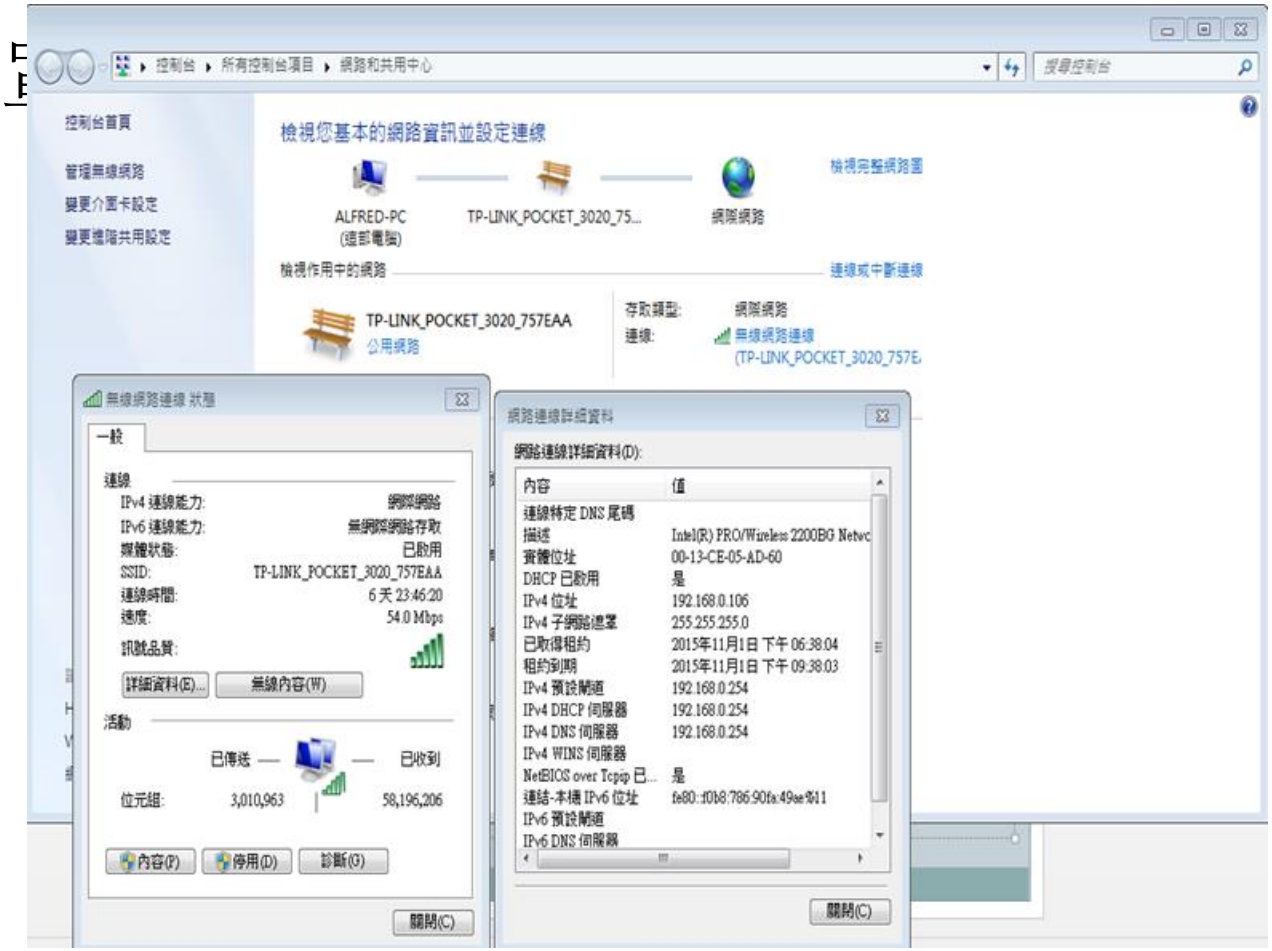
IP 網路設定

- Ip address
- 動態、固定
- private
  - 192.168/16
  - 172.16-31/12
  - 10/8
- Netmask
- Gateway
- DNS

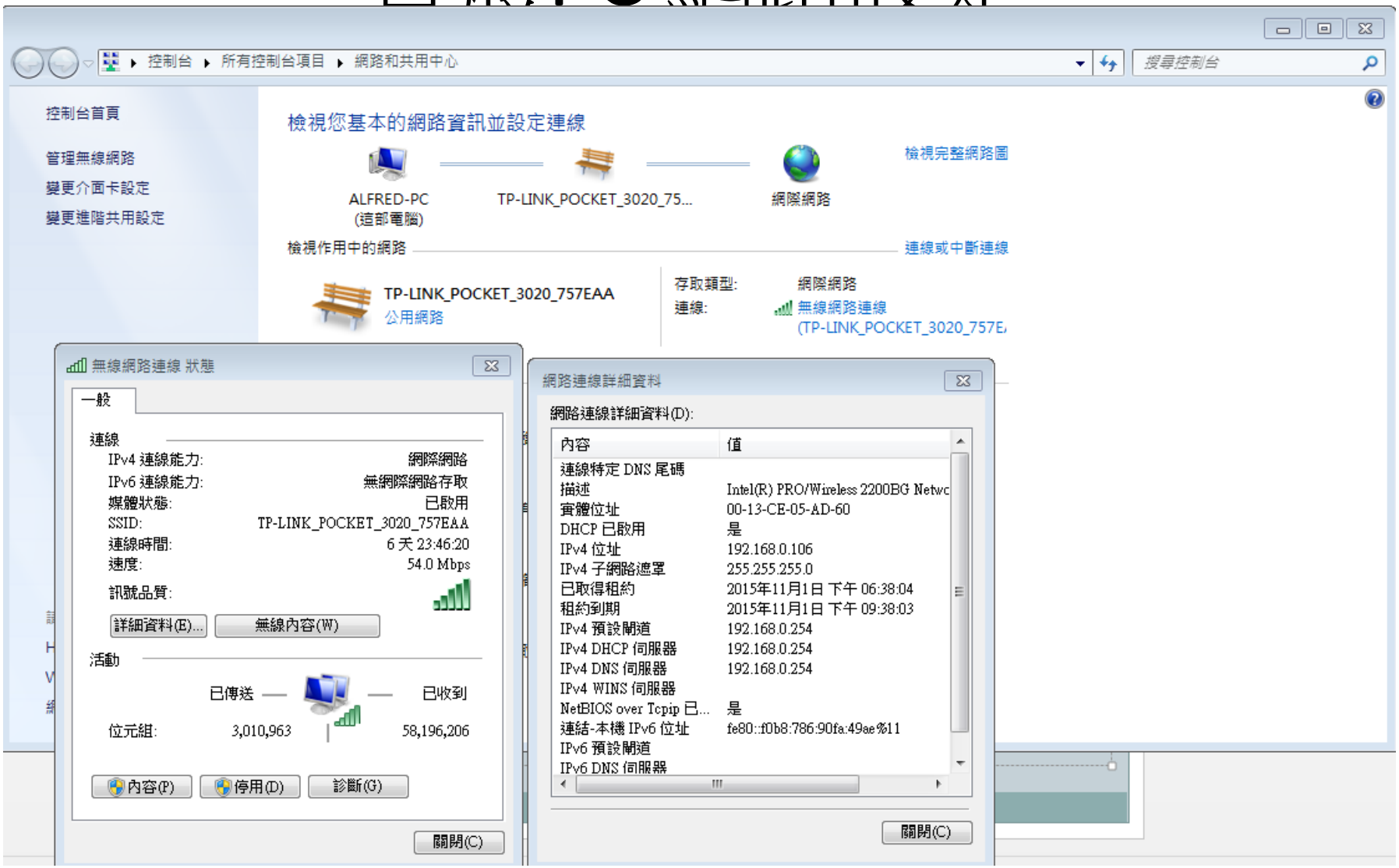


IP Address

- A.B.C.D　　0-255
- NetMask 遮罩
- Gateway
- DNS
- DHCP
- Ipv6

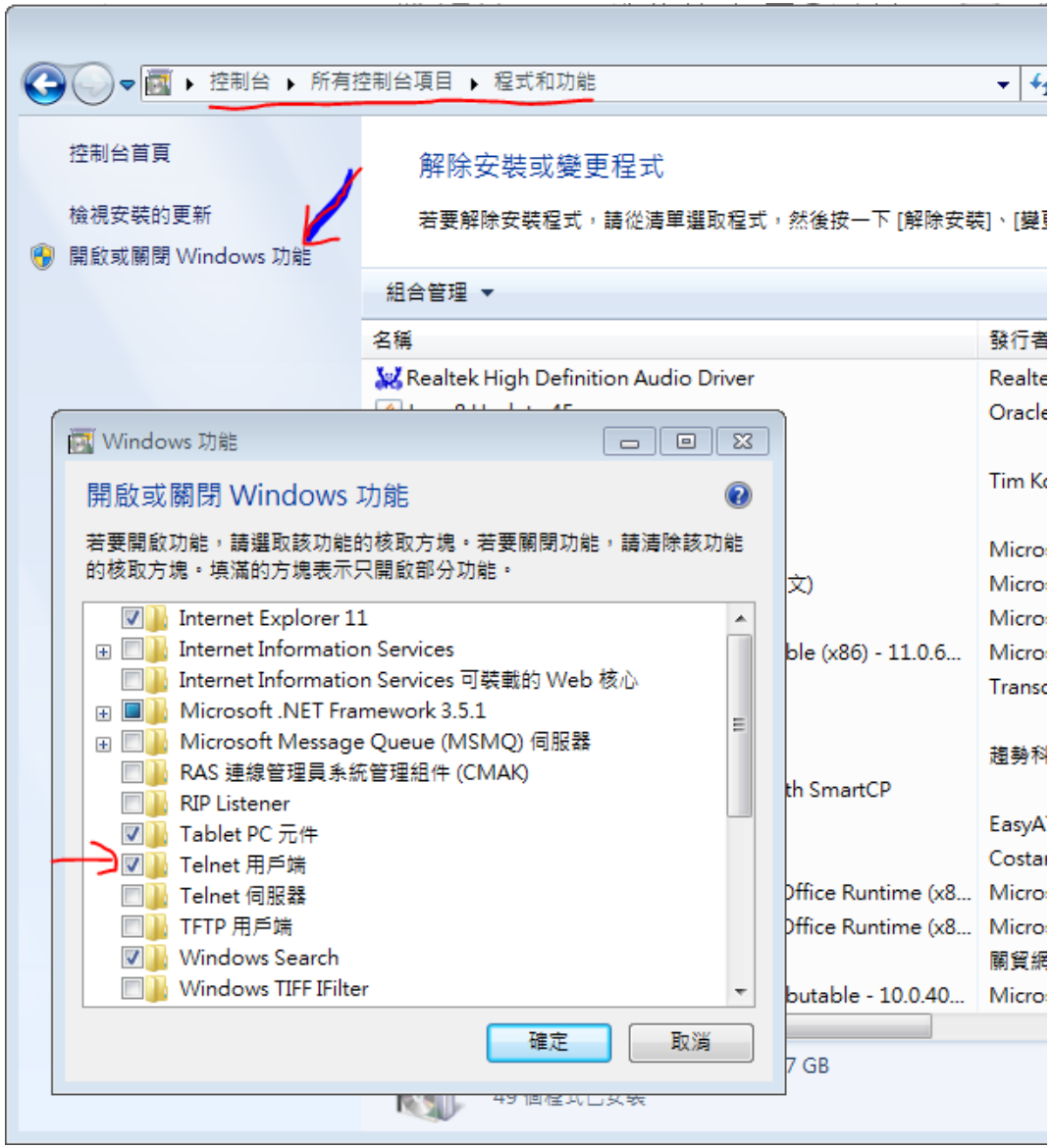


實體PC 網路設定

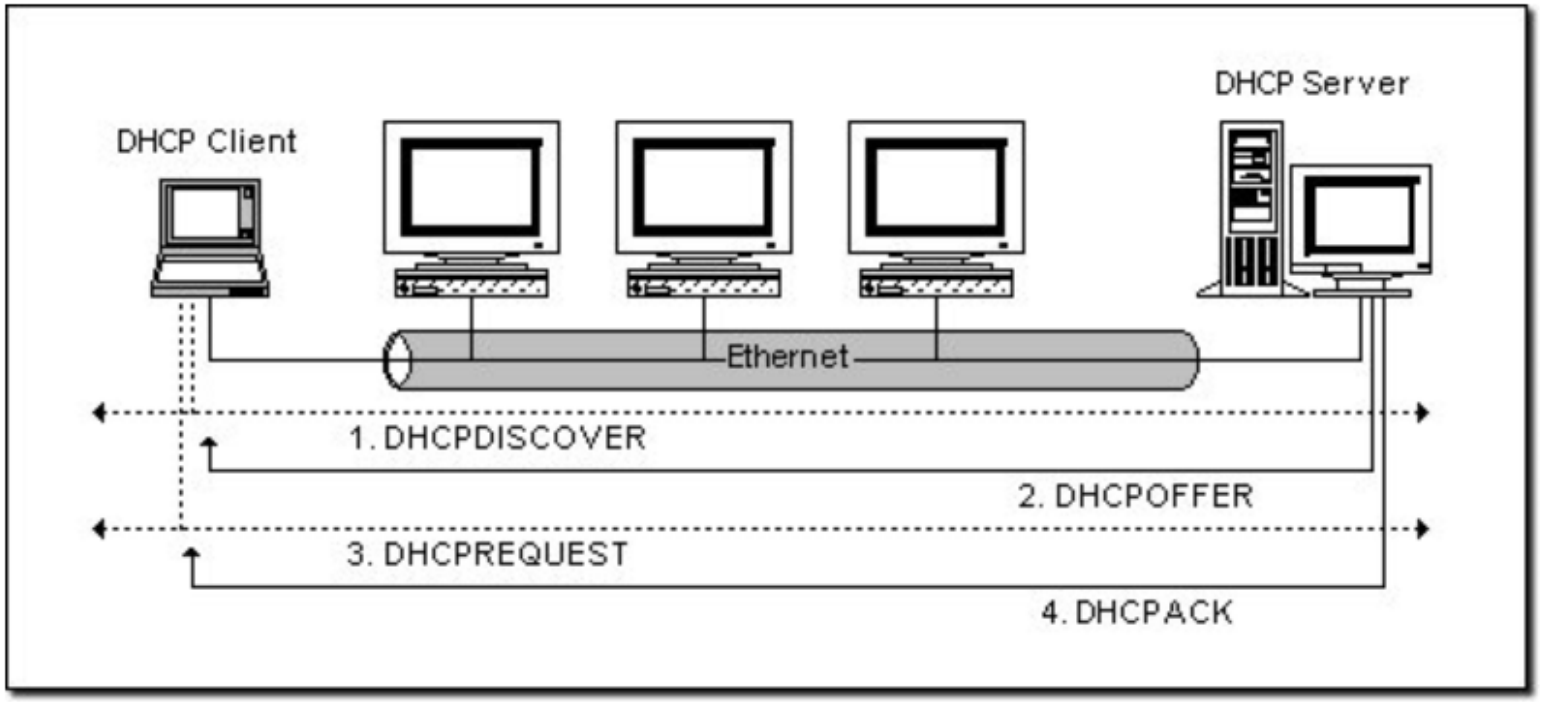

控制台 ▸ 所有控制台項目 ▸ 網路和共用中心
搜尋控制台
控制台首頁
管理無線網路
變更介面卡設定
變更進階共用設定
檢視您基本的網路資訊並設定連線
檢視完整網路圖
ALFRED-PC
(這部電腦)
TP-LINK_POCKET_3020_75...
網際網路
檢視作用中的網路
連線或中斷連線
TP-LINK_POCKET_3020_757EAA
公用網路
存取類型: 網際網路
連線: 無線網路連線
(TP-LINK_POCKET_3020_757E
無線網路連線 狀態
一般
連線
IPv4 連線能力: 網際網路
IPv6 連線能力: 無網際網路存取
媒體狀態: 已啟用
SSID: TP-LINK_POCKET_3020_757EAA
連線時間: 6 天 23:46:20
速度: 54.0 Mbps
訊號品質:
詳細資料(E)...
無線內容(W)
活動
已傳送
已收到
位元組: 3,010,963 58,196,206
內容(P)
停用(D)
診斷(G)
關閉(C)
網路連線詳細資料
網路連線詳細資料(D):
內容
值
連線特定 DNS 尾碼
描述 Intel(R) PRO/Wireless 2200BG Netwc
實體位址 00-13-CE-05-AD-60
DHCP 已啟用 是
IPv4 位址 192.168.0.106
IPv4 子網路遮罩 255.255.255.0
已取得租約 2015年11月1日 下午 06:38:04
租約到期 2015年11月1日 下午 09:38:03
IPv4 預設閘道 192.168.0.254
IPv4 DHCP 伺服器 192.168.0.254
IPv4 DNS 伺服器 192.168.0.254
IPv4 WINS 伺服器
NetBIOS over Tcpip 已... 是
連結-本機 IPv6 位址 fe80::f0b8:786:90fa:49ae%11
IPv6 預設閘道
IPv6 DNS 伺服器
關閉(C)

個人電腦網路設定基本概念

- DOS指令
(命令提示字元)
或 執行 cmd
  - ipconfig /all
  - Nslookup
  - Ping
  - Tracert –d DST ip
  - Pathping
  - telnet ip port



DHCP 發放流程



DHCP 發放流程

摘錄自:http://www.pcnet.idv.tw/pcnet/network/network_ip_dhcp.htm

跨網路的 DHCP 運作

- DHCDISCOVER 是以廣播方式進行的，其情形只能在同一網路之內進行，因為 router 是不會將廣播傳送出去的。但如果 DHCP 伺服器安設在其它的網路上面呢？由於 DHCP 客戶端還沒有 IP 環境設定，所以也不知道 Router 位址，而且有些 Router 也不會將 DHCP 廣播封包傳遞出去，因此這情形下 DHCPDISCOVER 是永遠沒辦法抵達 DHCP 伺服器那端的，當然也不會發生 OFFER 及其他動作了。要解決這個問題，我們可以用 DHCP Agent (或 DHCP Proxy)主機來接管客戶的 DHCP 請求，然後將此請求傳遞給真正的 DHCP 伺服器，然後將伺服器的回覆傳給客戶。這裡，Proxy 主機必須自己具有路由能力，且能將雙方的封包互傳對方。
- 若不使用 Proxy，您也可以在每一個網路之中安裝 DHCP 伺服器，但這樣的話，一來設備成本會增加，而且，管理上面也比較分散。當然囉，如果在一個十分大型的網路中，這樣的均衡式架構還是可取的。端視您的實際情況而定了。

DHCP問題發生原因LAB及排除

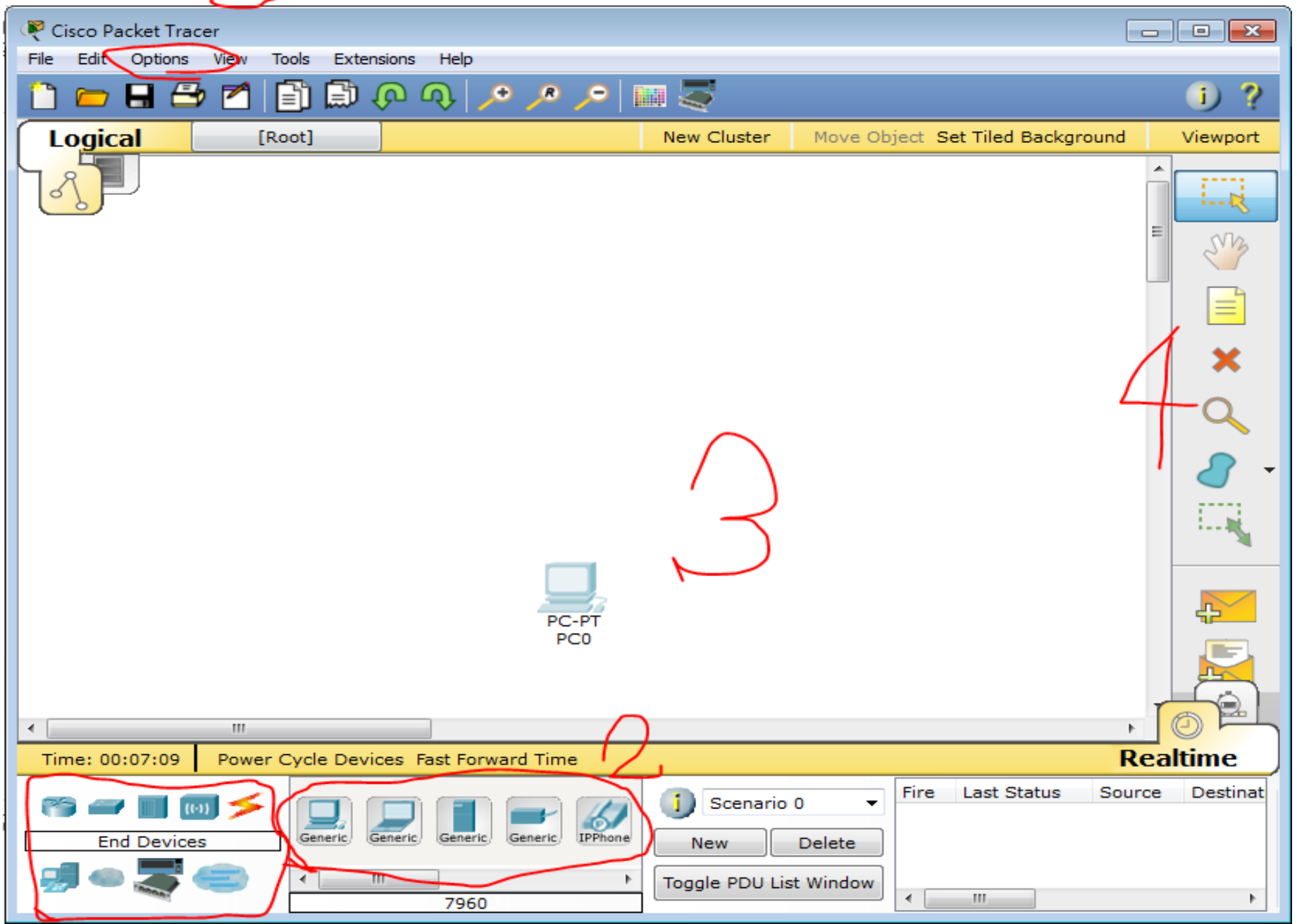
- Linksys LAB
- 內網DHCP取得192.168.X.X問題
- 判斷方式及故障排除
  是否取得正確的vlan ip上enctc.ntpc.edu.tw確認
- 若有錯誤ip,請工程師查出發dhcp的port，shutdown port
- 校內若是沒有私設DHCP請工程師上DHCP snooping設定。
  - DHCP snooping防堵私自架設**DHCP**伺服器

模擬器操作教學Lab簡介

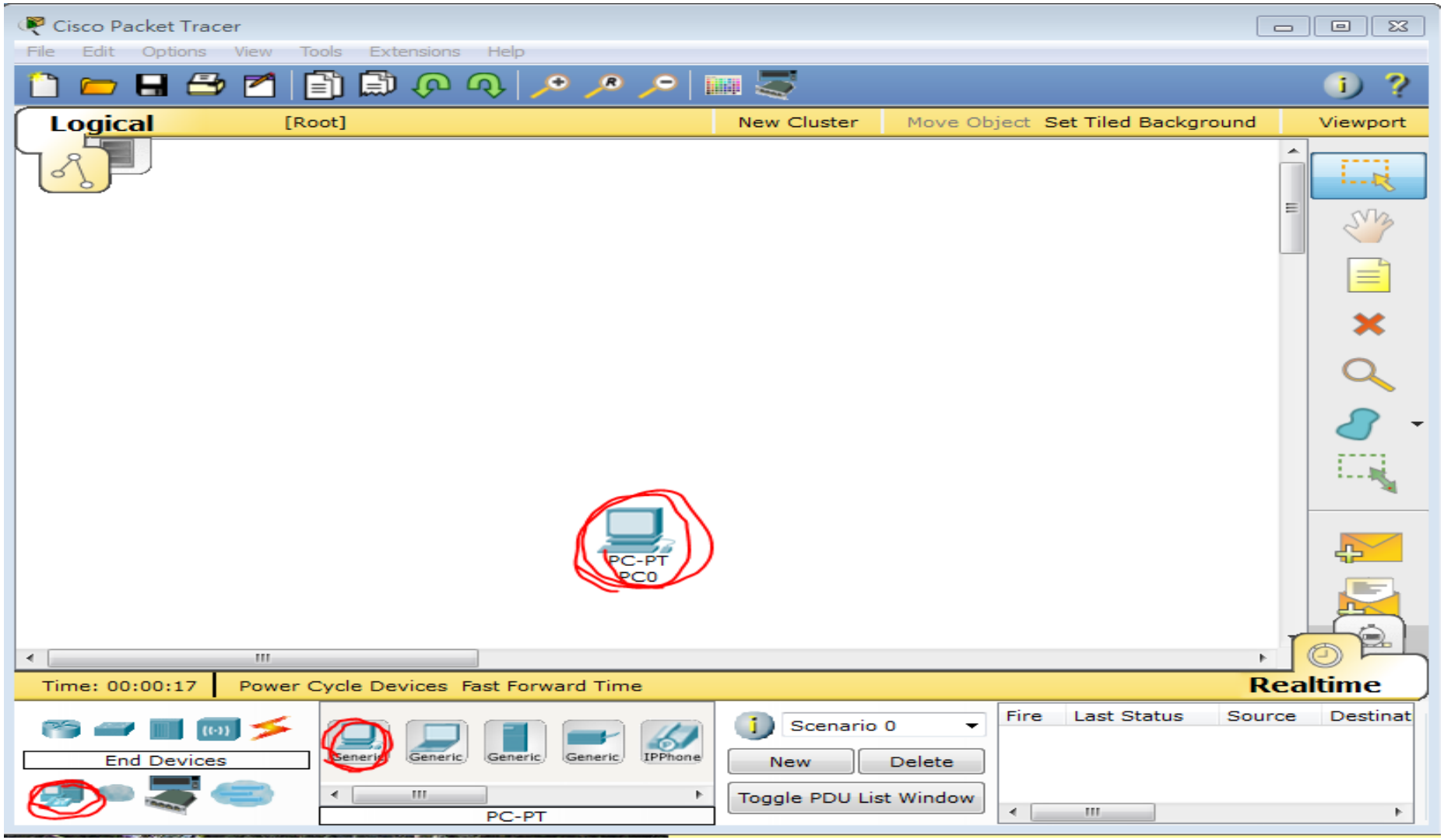
- Cisco Packet Tracer簡介
- 模擬機PC網路設定
- Wireless Device Linksys 無線分享器設定
  - LAN
  - WAN
  - Wireless
- L2 Switch 設定教學
- L3 Switch設定教學
- Packet Tracert Lab中可用Linksys 模擬DHCP Server

Packet Tracer基本使用介紹

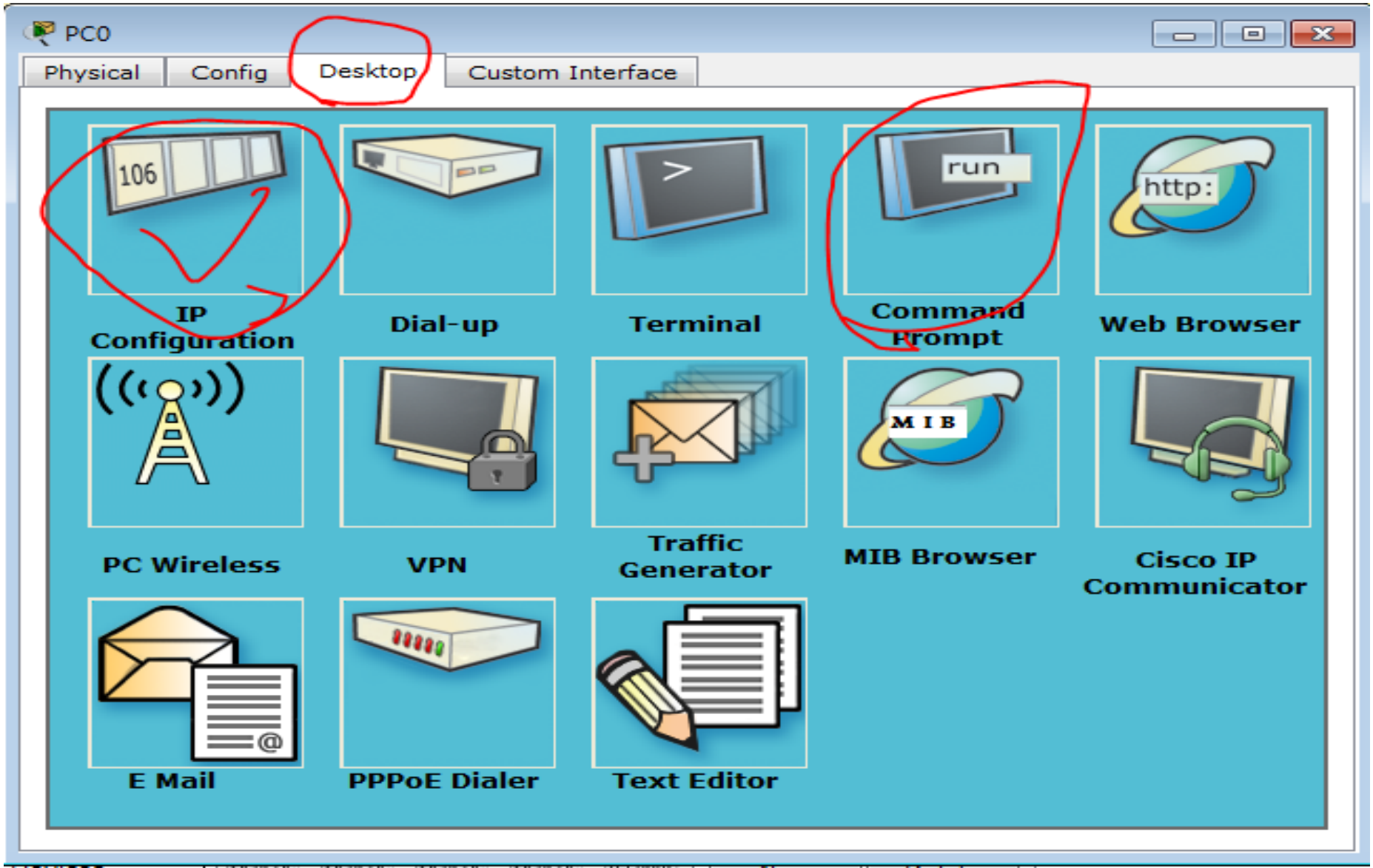
- CISCO原廠開發
- 提供CCNA,CCNP考試用
- 可以模擬大部分狀況
- 使用簡單易懂

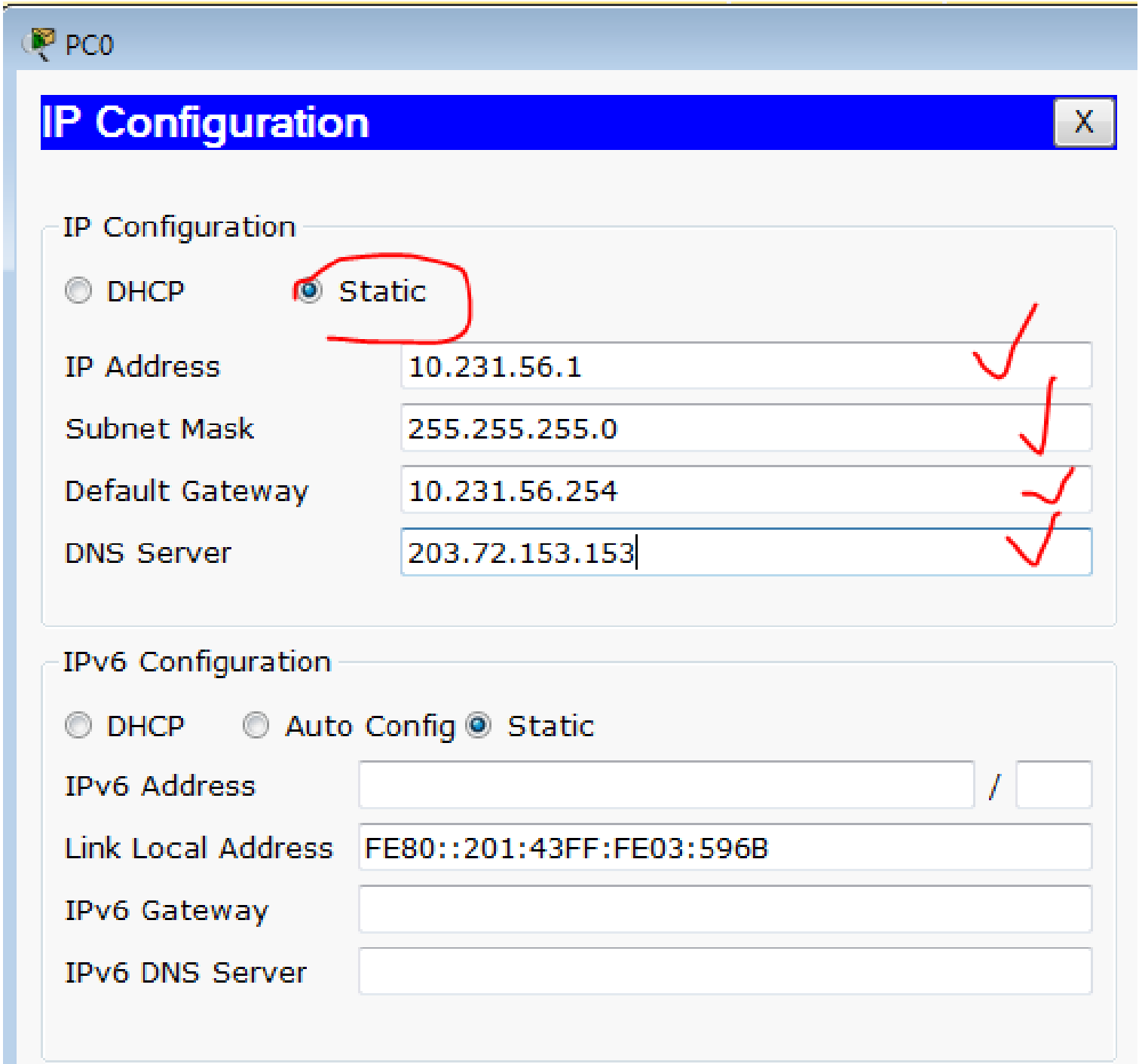

Cisco Packet Tracer
File
Edit
Options
View
Tools
Extensions
Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
PC-PT
PC0
Time: 00:07:09
Power Cycle Devices
Fast Forward Time
Realtime
End Devices
Generic
Generic
Generic
Generic
IPPhone
7960
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destinat
1
2
3
4
5

模擬PC網路設定


Cisco Packet Tracer
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
PC-PT
PC0
Time: 00:00:17
Power Cycle Devices
Fast Forward Time
Realtime
End Devices
Generic
Generic
Generic
Generic
IPPhone
PC-PT
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destinat

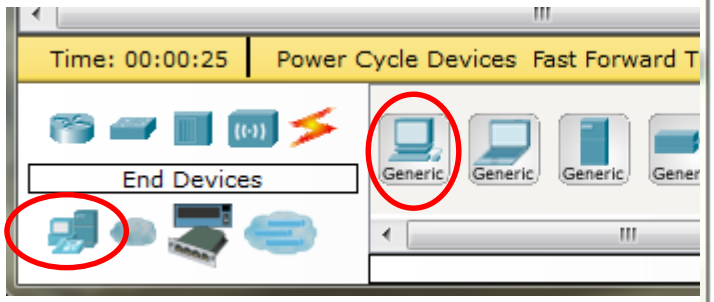
設定PC網路

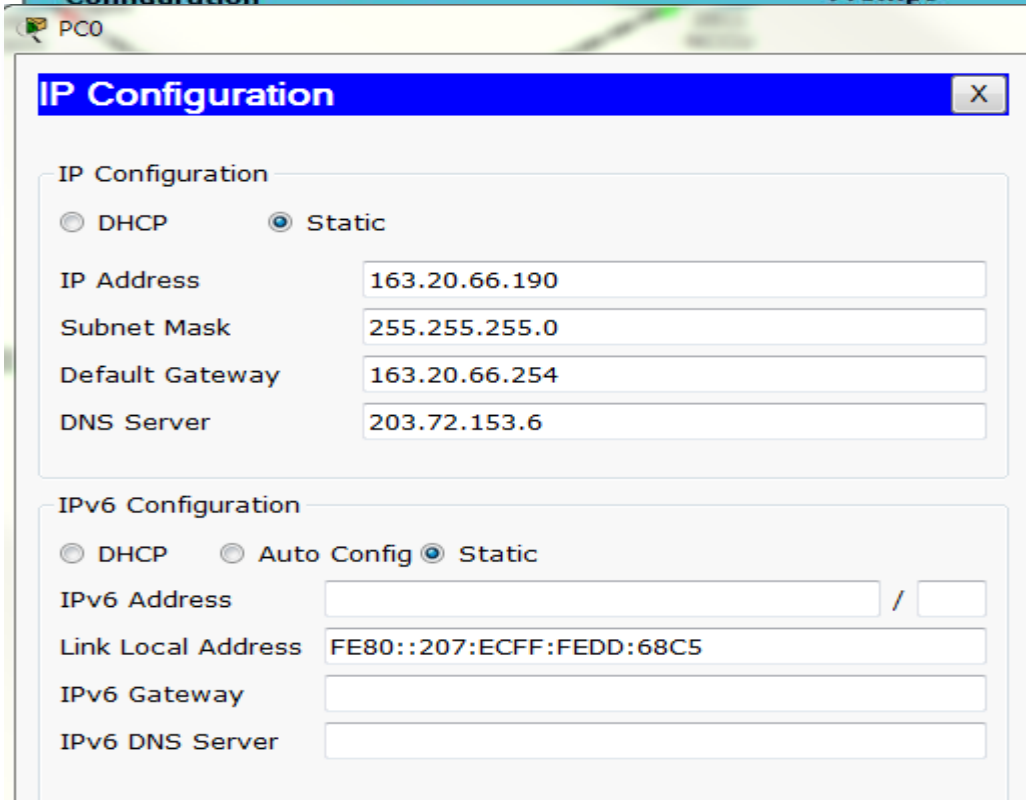

PC0
Physical
Config
Desktop
Custom Interface
106
IP Configuration
Dial-up
Terminal
run
Command Prompt
http:
Web Browser
PC Wireless
VPN
Traffic Generator
MIB
MIB Browser
Cisco IP Communicator
E Mail
PPPoE Dialer
Text Editor


PC0
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
10.231.56.1
Subnet Mask
255.255.255.0
Default Gateway
10.231.56.254
DNS Server
203.72.153.153
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::201:43FF:FE03:596B
IPv6 Gateway
IPv6 DNS Server

Lab 1 PC 設定

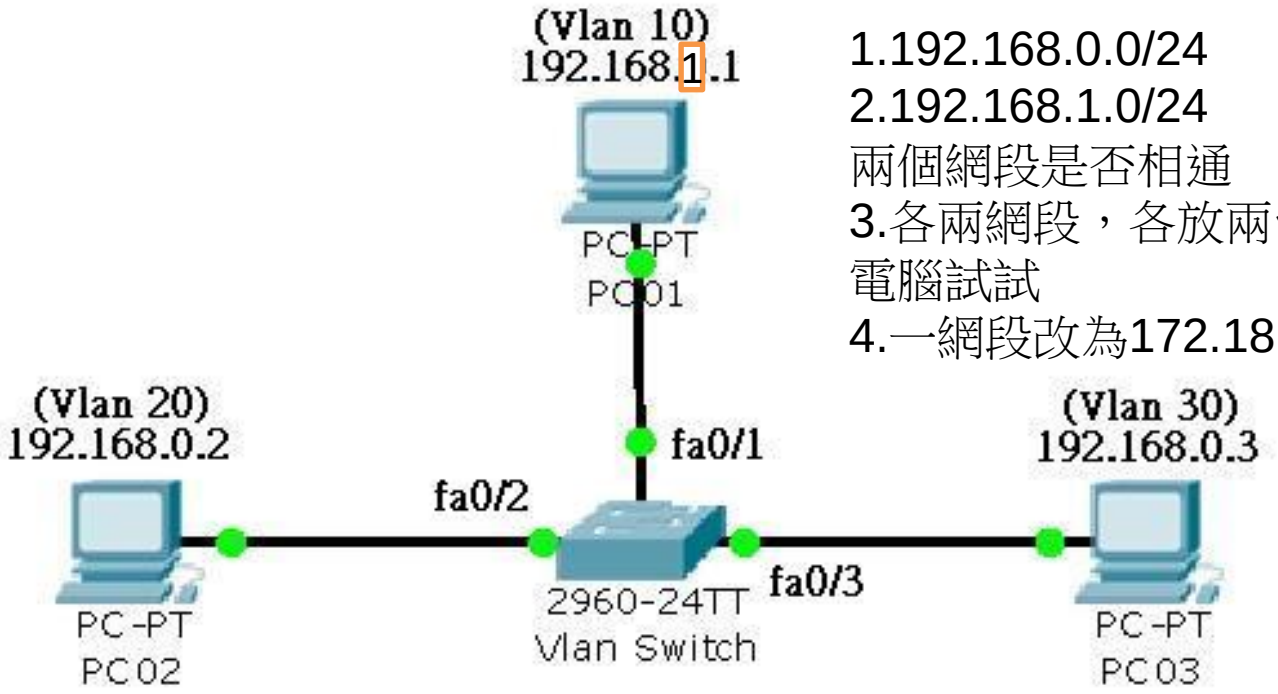
- Packet Tracert 6.1
- PC 設定、使用





Lab 3-1 基本練習Hub、L2、家用AP

三台 PC 三個網段 、同網段可通、不同網段不通



1.192.168.0.0/24
2.192.168.1.0/24
兩個網段是否相通
3.各兩網段，各放兩台
電腦試試
4.一網段改為172.18.1.1/24

家用無線AP設定

設定分為三部分

WAN IP (internet)
對外連線

LAN IP
內部有線

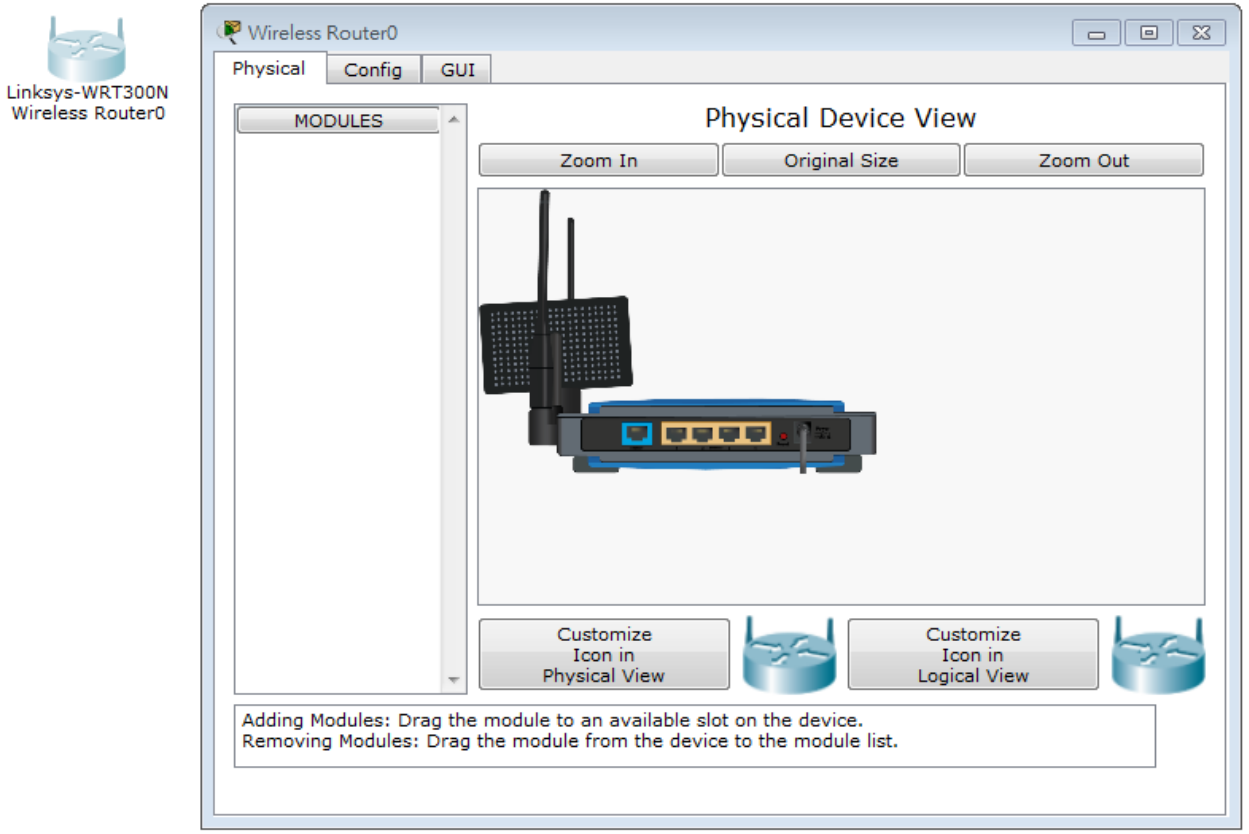
Wireless
內部無線

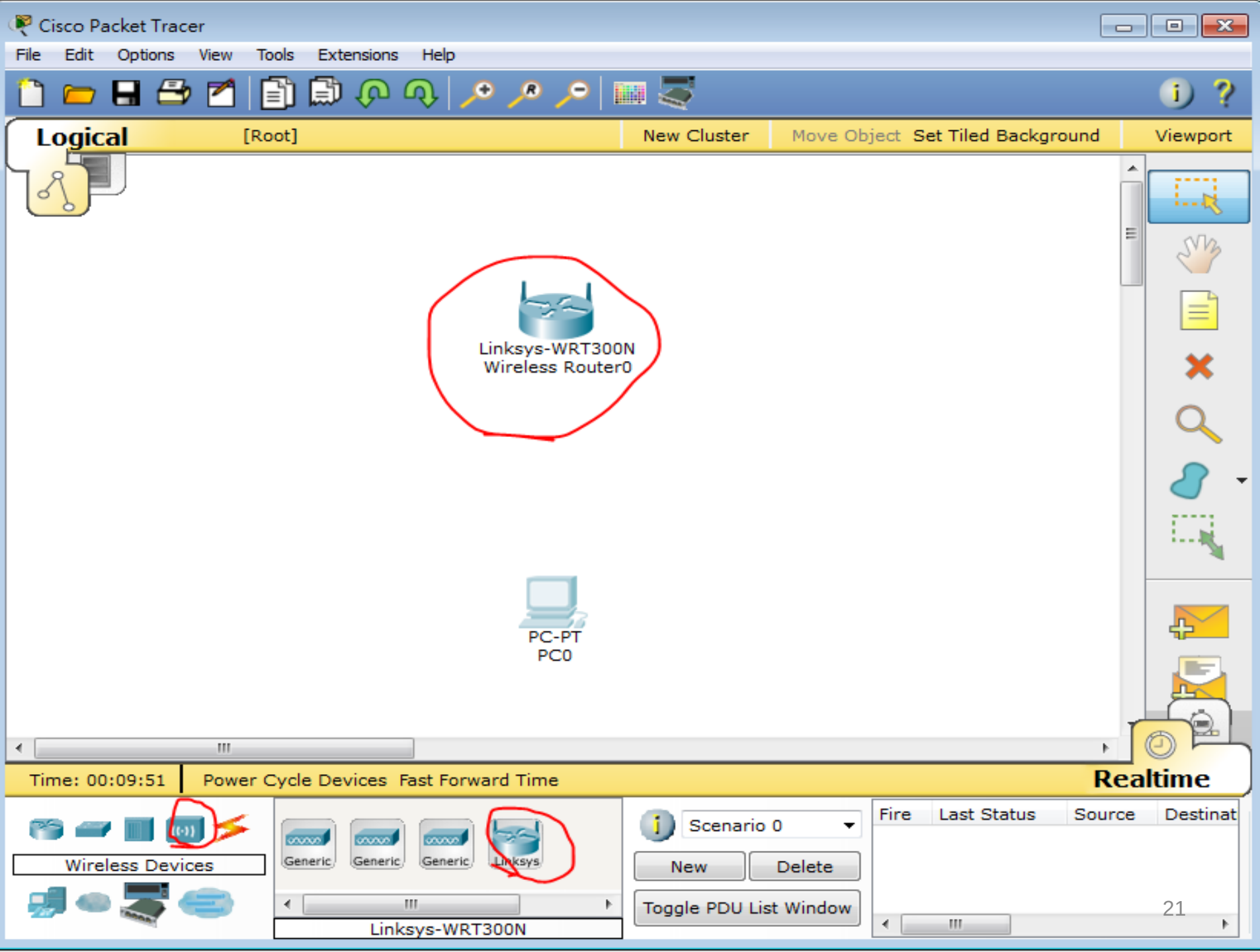
SSID

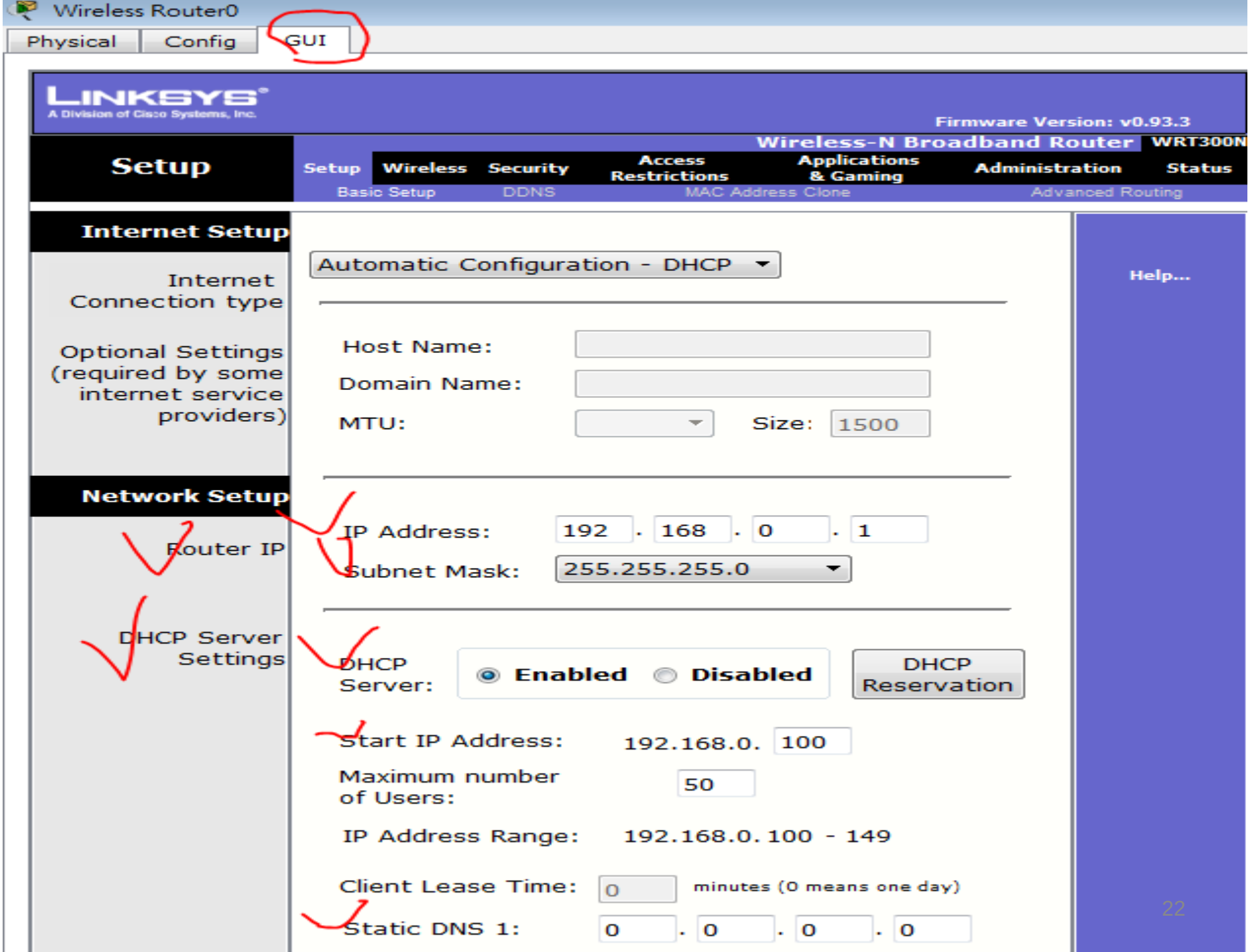
WPA2

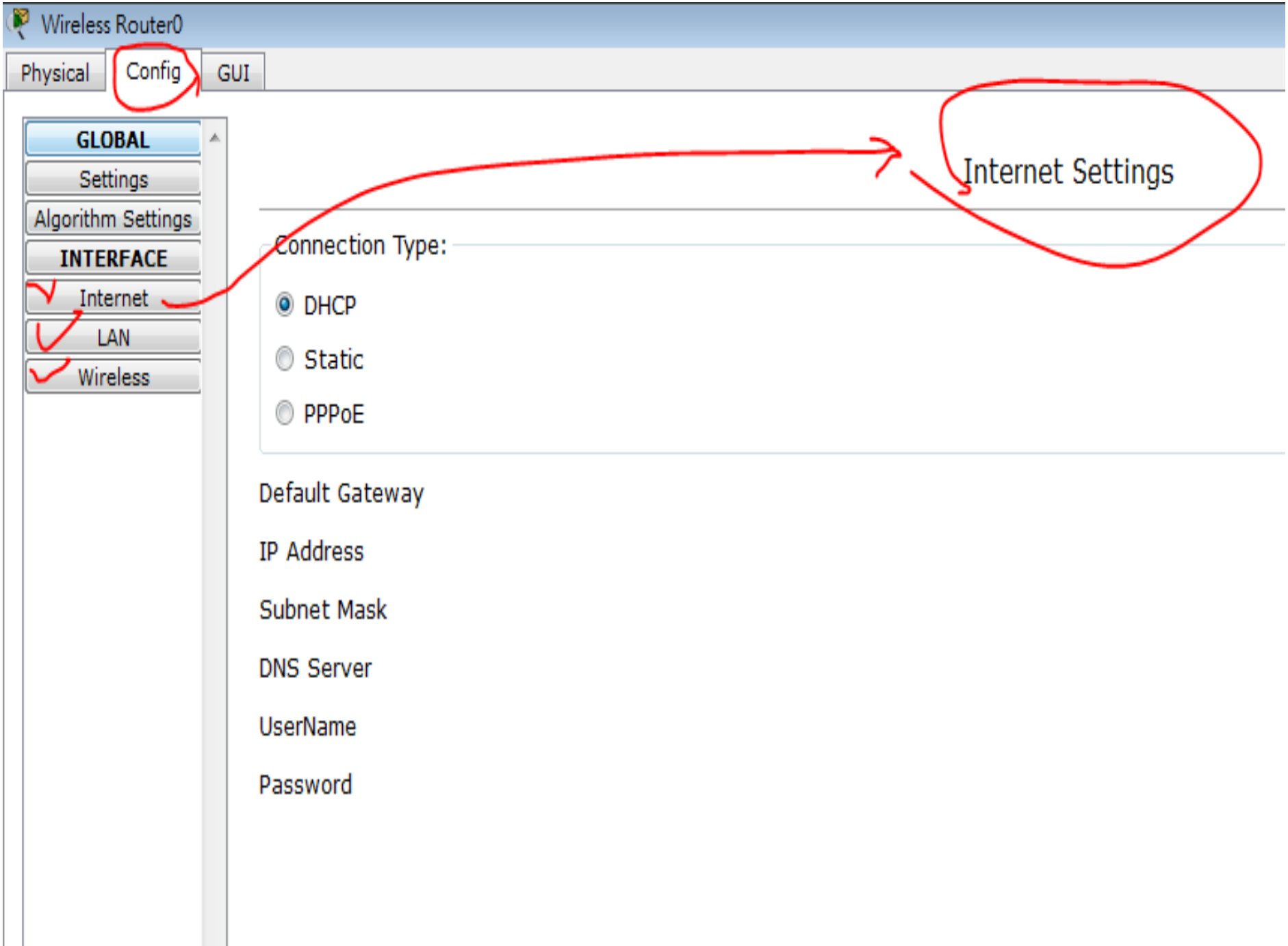
Preshare key

Redius server



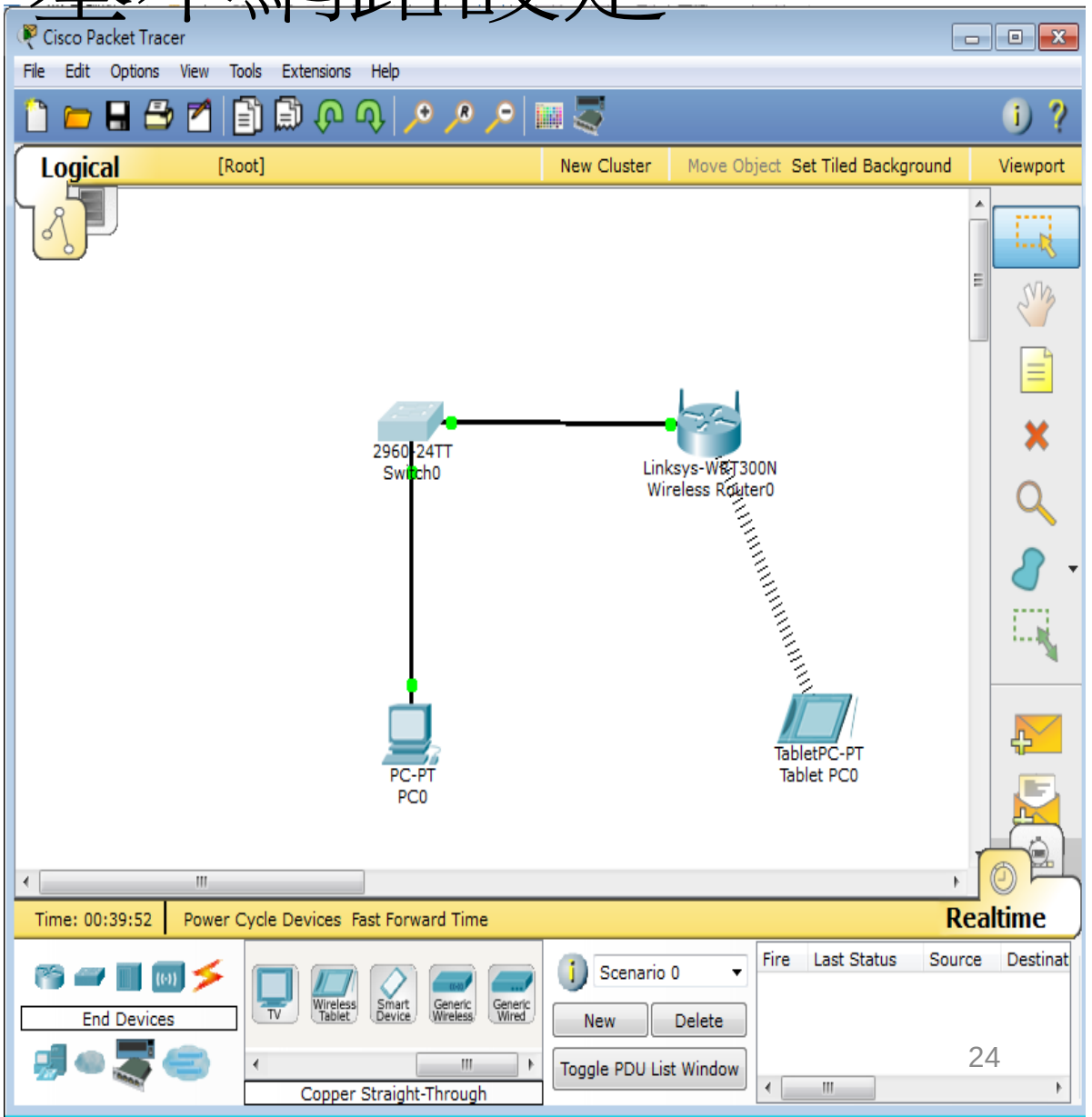

Cisco Packet Tracer
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
Linksys-WRT300N
Wireless Router0
PC-PT
PC0
Time: 00:09:51
Power Cycle Devices
Fast Forward Time
Realtime
Wireless Devices
Generic
Generic
Generic
Linksys
Linksys-WRT300N
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destinat

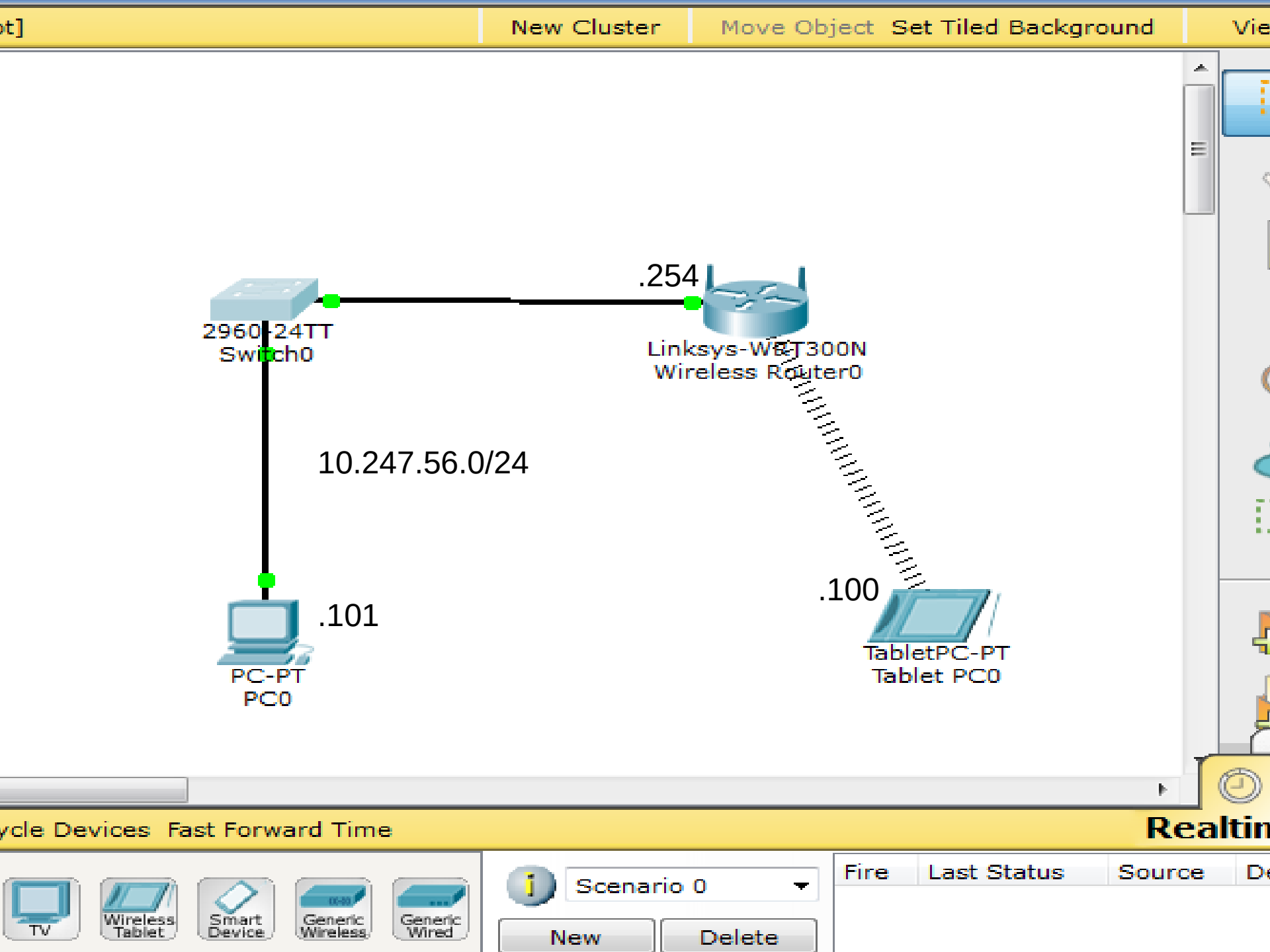

Wireless Router0
Physical
Config
GUI
LINKSYS
A Division of Cisco Systems, Inc.
Firmware Version: v0.93.3
Wireless-N Broadband Router WRT300N
Setup
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Administration
Status
Basic Setup
DDNS
MAC Address Clone
Advanced Routing
Internet Setup
Internet Connection type
Automatic Configuration - DHCP
Optional Settings (required by some internet service providers)
Host Name:
Domain Name:
MTU:
Size:
1500
Network Setup
Router IP
IP Address:
192 . 168 . 0 . 1
Subnet Mask:
255.255.255.0
DHCP Server Settings
DHCP Server:
Enabled
Disabled
DHCP Reservation
Start IP Address:
192.168.0.
100
Maximum number of Users:
50
IP Address Range:
192.168.0.100 - 149
Client Lease Time:
0
minutes (0 means one day)
Static DNS 1:
0 . 0 . 0 . 0
Help...


Wireless Router0
Physical
Config
GUI
GLOBAL
Settings
Algorithm Settings
INTERFACE
Internet
LAN
Wireless
Internet Settings
Connection Type:
DHCP
Static
PPPoE
Default Gateway
IP Address
Subnet Mask
DNS Server
UserName
Password

Lab2 基本網路設定

功能要求
1.用一台L2 switch
2.接一台無線AP
3.讓PC可以取得ip
4.讓無線載具可以取得ip
5.無線載具與PC互ping會通




New Cluster
Move Object
Set Tiled Background
.254
2960-24TT
Switch0
Linksys-WRT300N
Wireless Router0
10.247.56.0/24
.101
.100
PC-PT
PC0
TabletPC-PT
Tablet PC0
Fast Forward Time
TV
Wireless Tablet
Smart Device
Generic Wireless
Generic Wired
Scenario 0
New
Delete
Fire
Last Status
Source

DHCP問題發生原因LAB及排除

- Linksys LAB
- 內網DHCP取得192.168.X.X問題
- 判斷方式及故障排除

  是否取得正確的vlan ip上enctc.ntpc.edu.tw確認

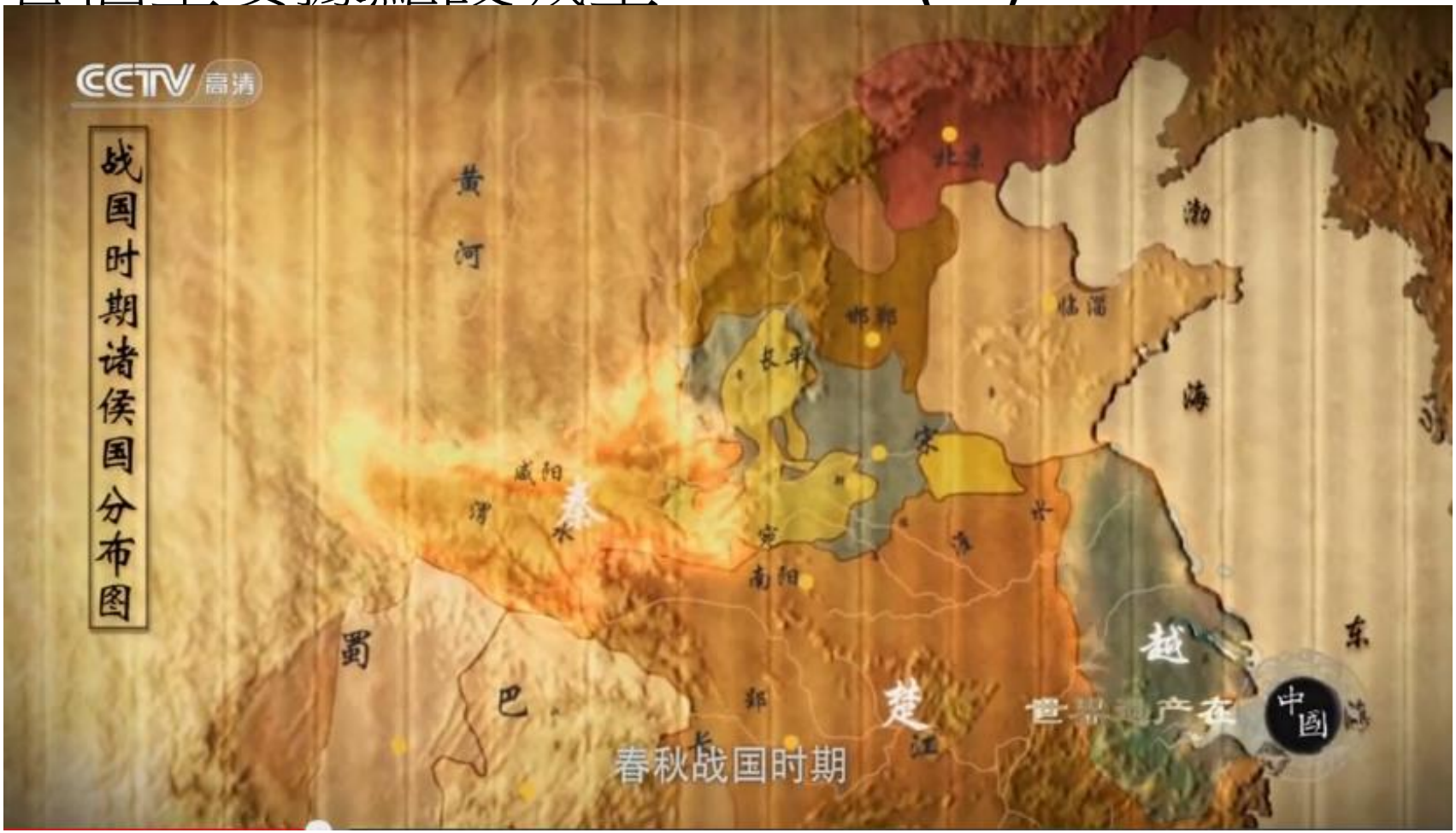
  由arp table找出非法網段Gateway

  若有錯誤ip,請工程師查出發dhcp的port，shutdown port

802.1Q vlan

Vlan

- 各個重要據點設城堡。Vlan （L2）

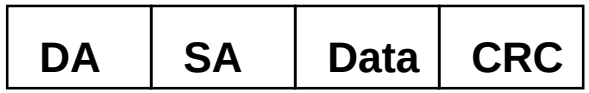


IEEE 802.1p/802.1q Frame Tagging

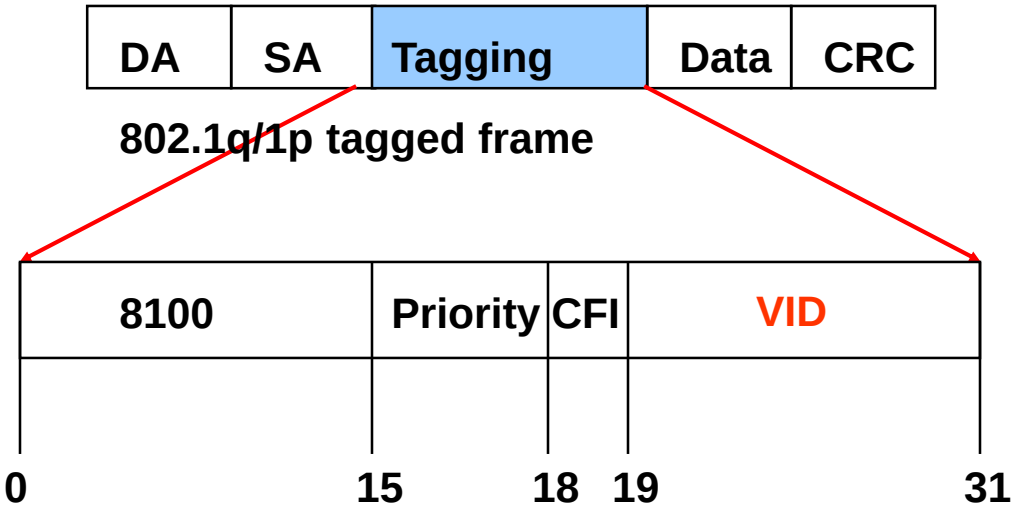
The 32-bit field (VLAN Tag) in the frame header that identifies the frame as belonging to a specific VLAN/priority.

The Max. size of a Tagged Ethernet Frame is 1522 Bytes (1518+ 4 bytes tagging).

The frame without VLAN tag, we call it as Untagged Frame or Frame.



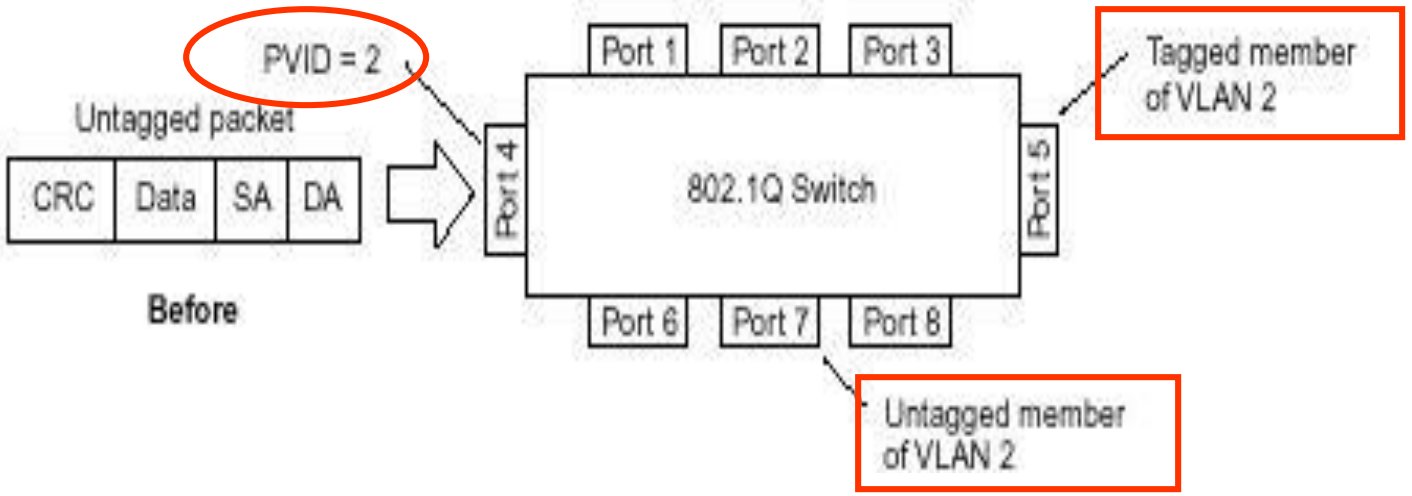
Regular frame (or untagged frame)



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

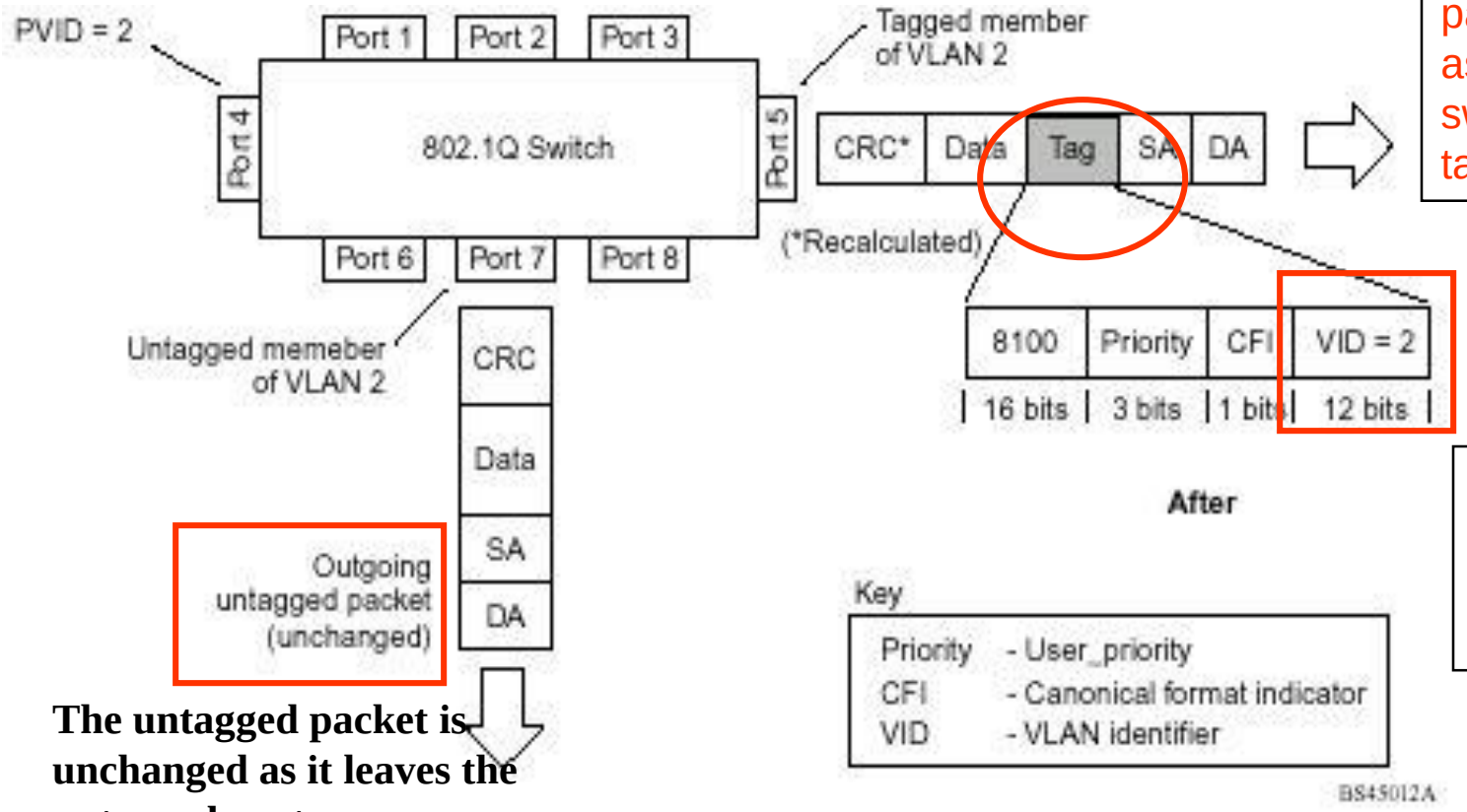
VLAN (1q) has 12 bits, 0-4095

802.1p/1q Untagged Incoming Frame



Assumed the PVID of port4 is 2 and default priority=0
The incoming untagged packet will be assigned to VLAN 2/priority=0
Port5 is tagged and port 7 is untagged egress member of VLAN 2
This packet will be forwarded to port5 and port7 with tagged and untagged respectively.
Priority tagging (802.1p) follows the similar rule as 802.1q tagging.

802.1p/1q Untagged Incoming Frame

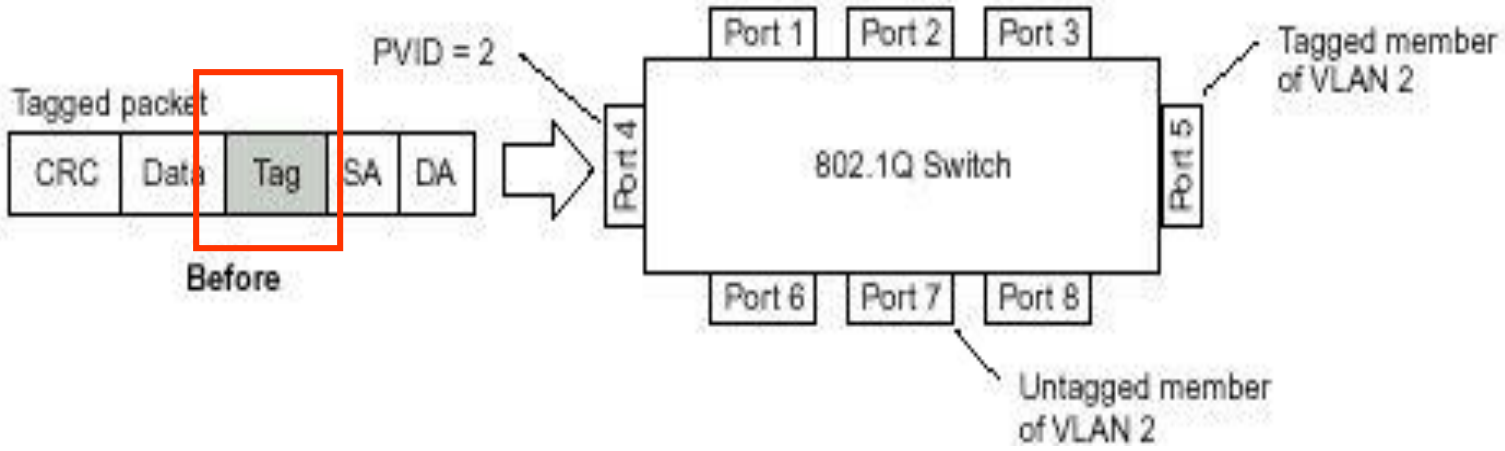


The untagged packet is tagged as it leaves the switch through tagged port

The VID is related to PVID of the incoming port

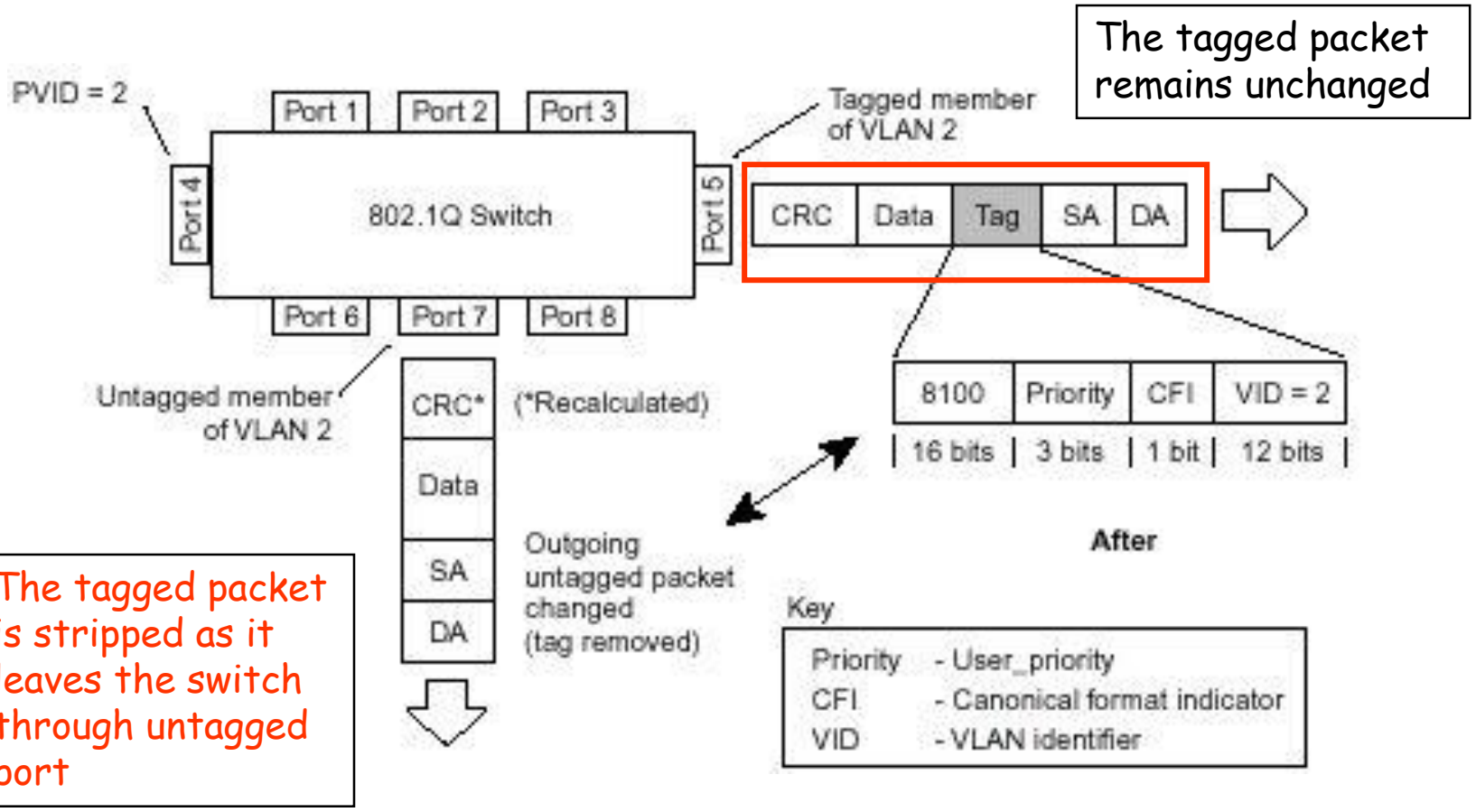
The untagged packet is unchanged as it leaves the untagged port

802.1p/1q Tagged Incoming Frame



Assumed tagged incoming packet having vid=2/priority=0
Port5 is a tagged and port 7 is an untagged egress member of VLAN 2
This packet will be forwarded to port5 and port7

802.1p/1q Tagged Incoming Frame



802.1p/1q Tagging summary

Ingress (incoming frame):

- If receiving **untagged** frame, add the tag into this frame with VID=PVID and priority= 802.1p default priority
- If receiving **tagged** frame, the VID/priority values are unchanged.

Inside the Switch (all frames are tagged)

- For VLAN, based on the VID to lookup the VLAN table, and forward frame to member ports of this VLAN.
- For priority, based on the “Class of Service mapping” to process the frame with associated priority Queue.

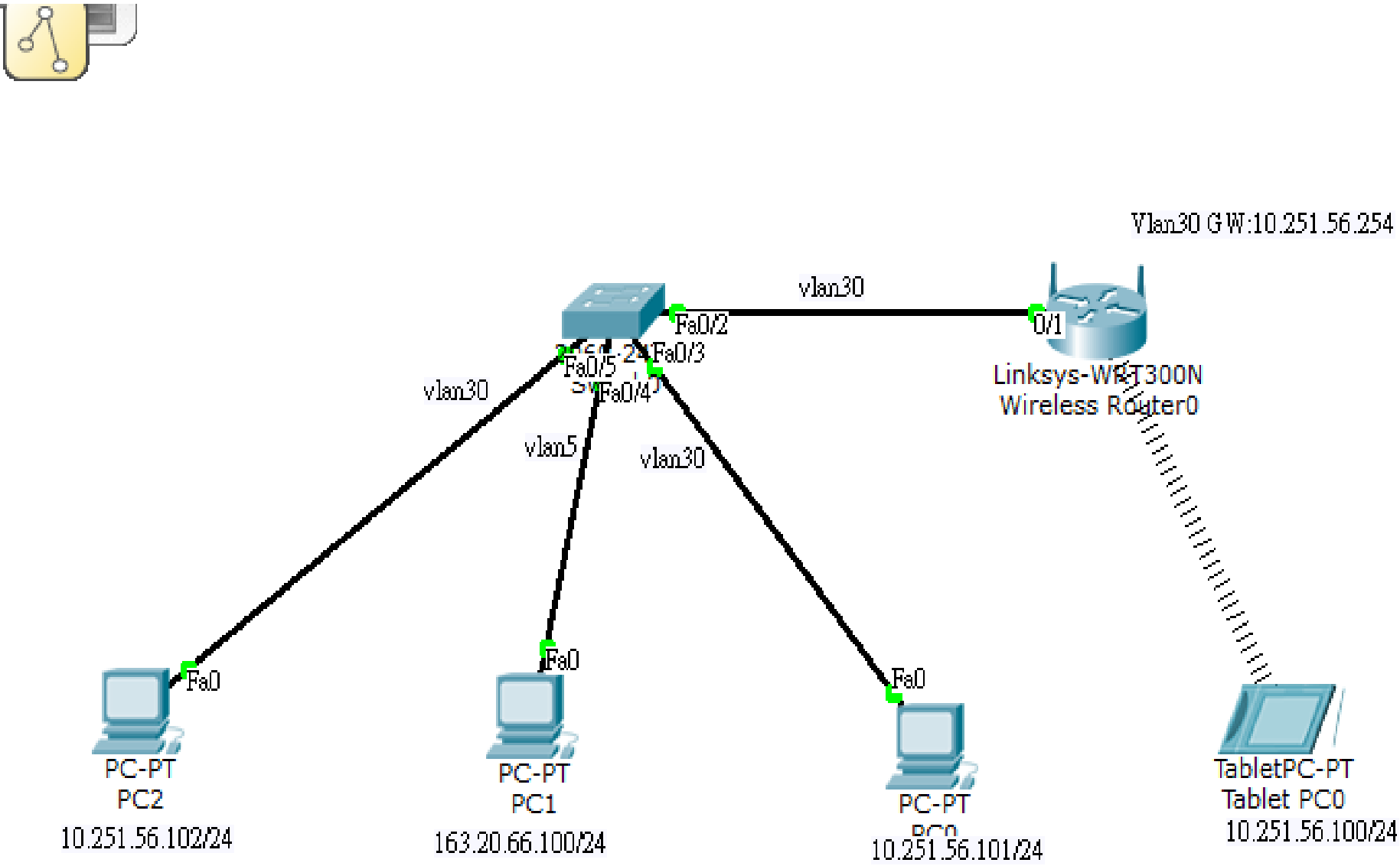
Egress (outgoing frame):

- **Untagged** egress port: Remove the tagging.
- **Tagged** Egress port: Un-change the tagging, so that the 1p/1q info can be carried to next 802.1p/q aware switch.

L2 Lab Vlan建置說明

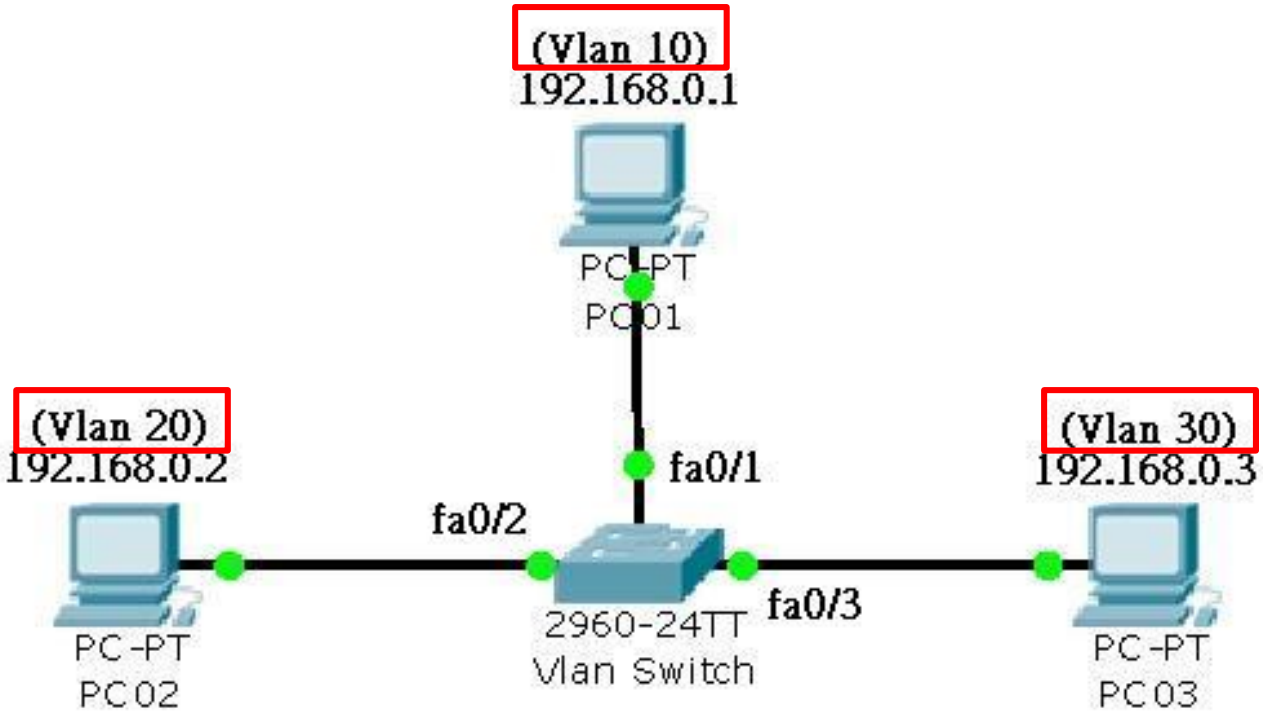
- 建立vlan 30 and vlan 5
- 將接L2與PC相連的port設定為正確vlan access port
- 測試
  - 相同vlan可以取得DHCP派發ip
    - 不同vlan，ip
    - 互 ping不通
    - 相同vlan相同網段可以互ping

Lab3 L2 Vlan


Vlan30 GW:10.251.56.254
vlan30
Fa0/2
0/1
Fa0/3
Fa0/5
Fa0/4
vlan30
vlan5
vlan30
Linksys-WRT300N
Wireless Router0
Fa0
Fa0
Fa0
PC-PT
PC2
10.251.56.102/24
PC-PT
PC1
163.20.66.100/24
PC-PT
10.251.56.101/24
TabletPC-PT
Tablet PC0
10.251.56.100/24

Lab 3-2 基本練習Vlan

三個Vlan間三個網段 PC相互不通(Broadcast Domain)。

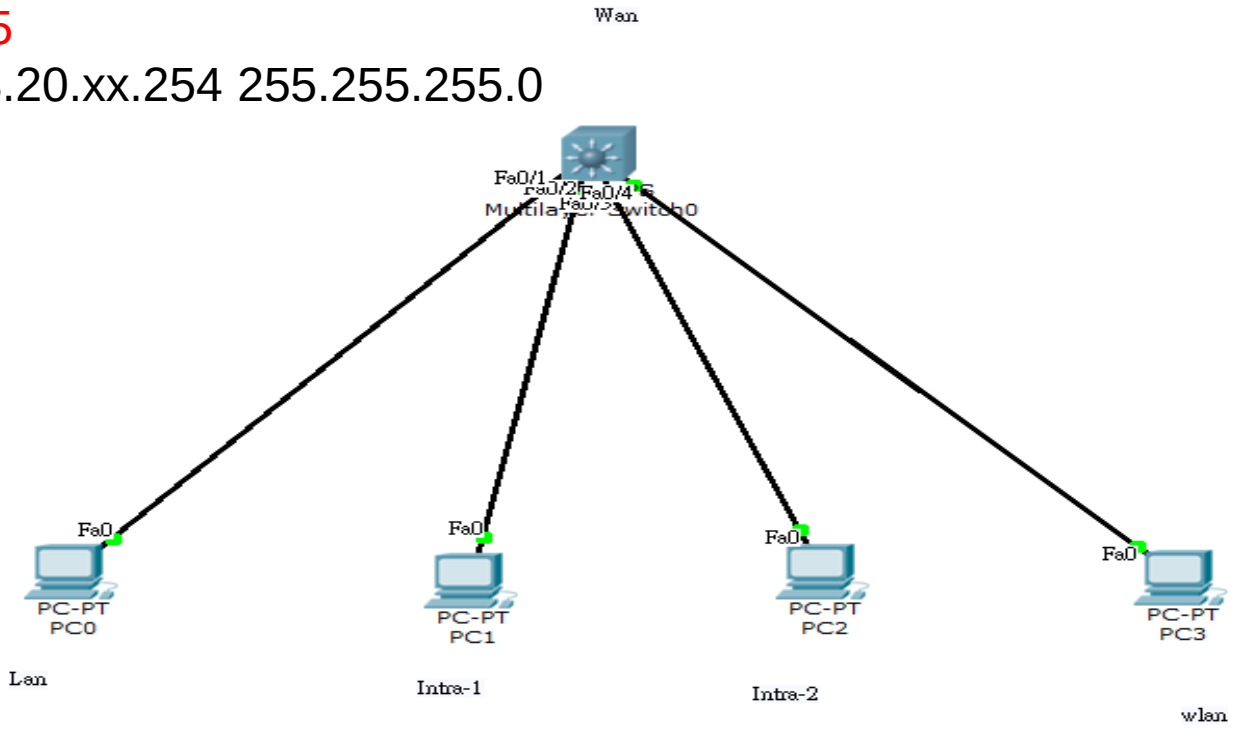


Lab 4 基本練習Vlan Interface

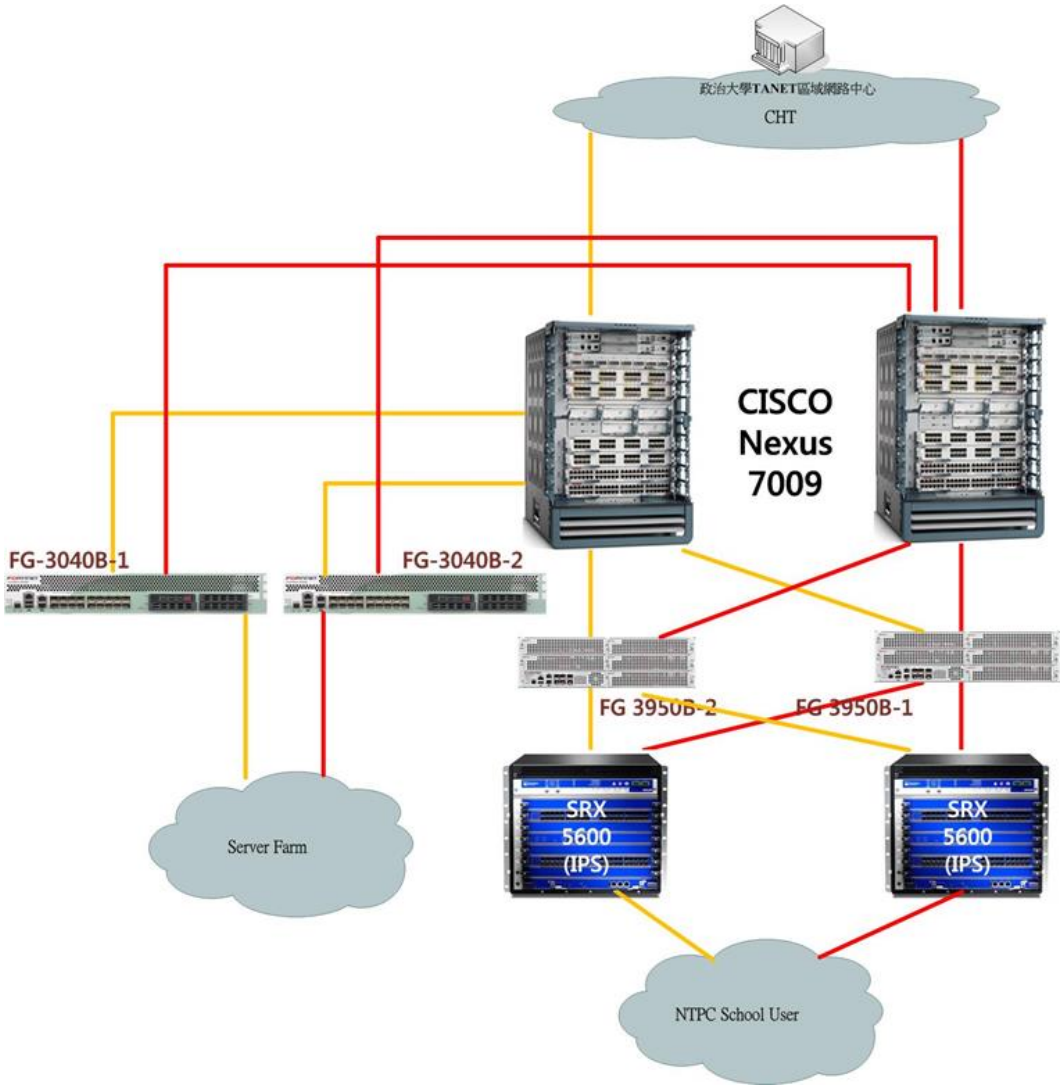
三個Vlan間三個網段 PC相互不通，做出每個網段Gateway。

Inter vlan 5

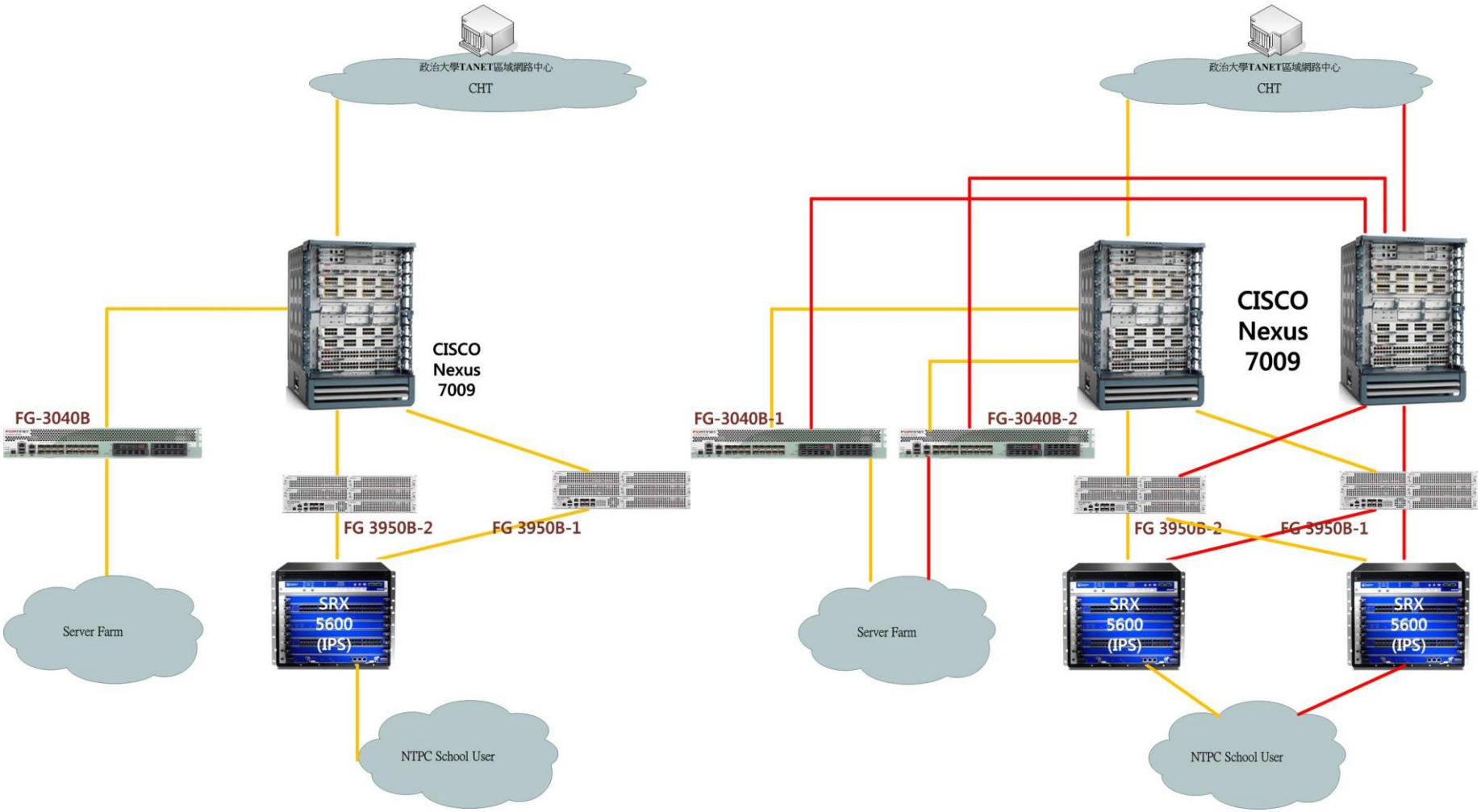
Ip add 163.20.xx.254 255.255.255.0



L3 Switch Routing (ipv4 and ipv6)

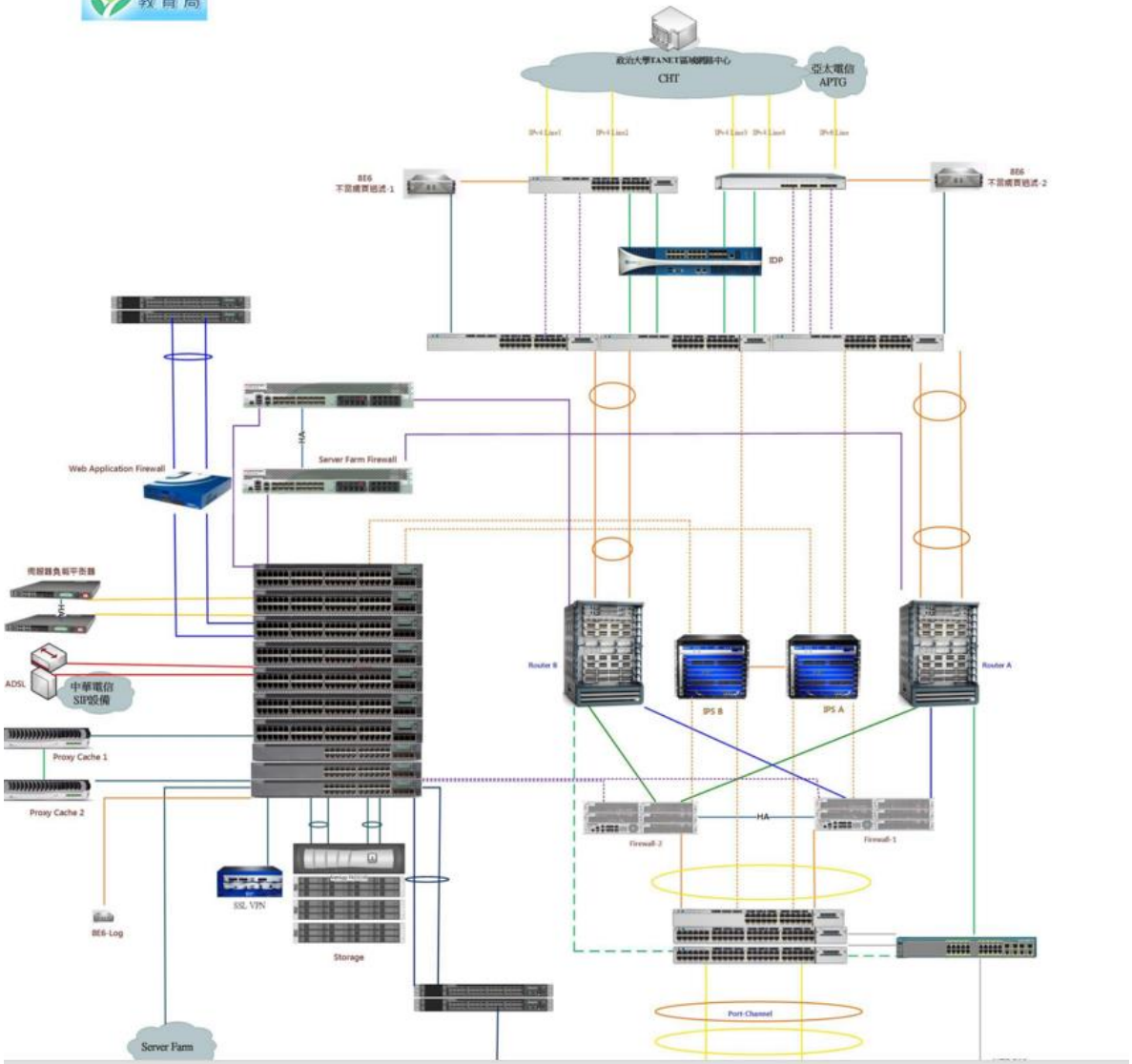


新北市教育網骨幹新舊比較圖

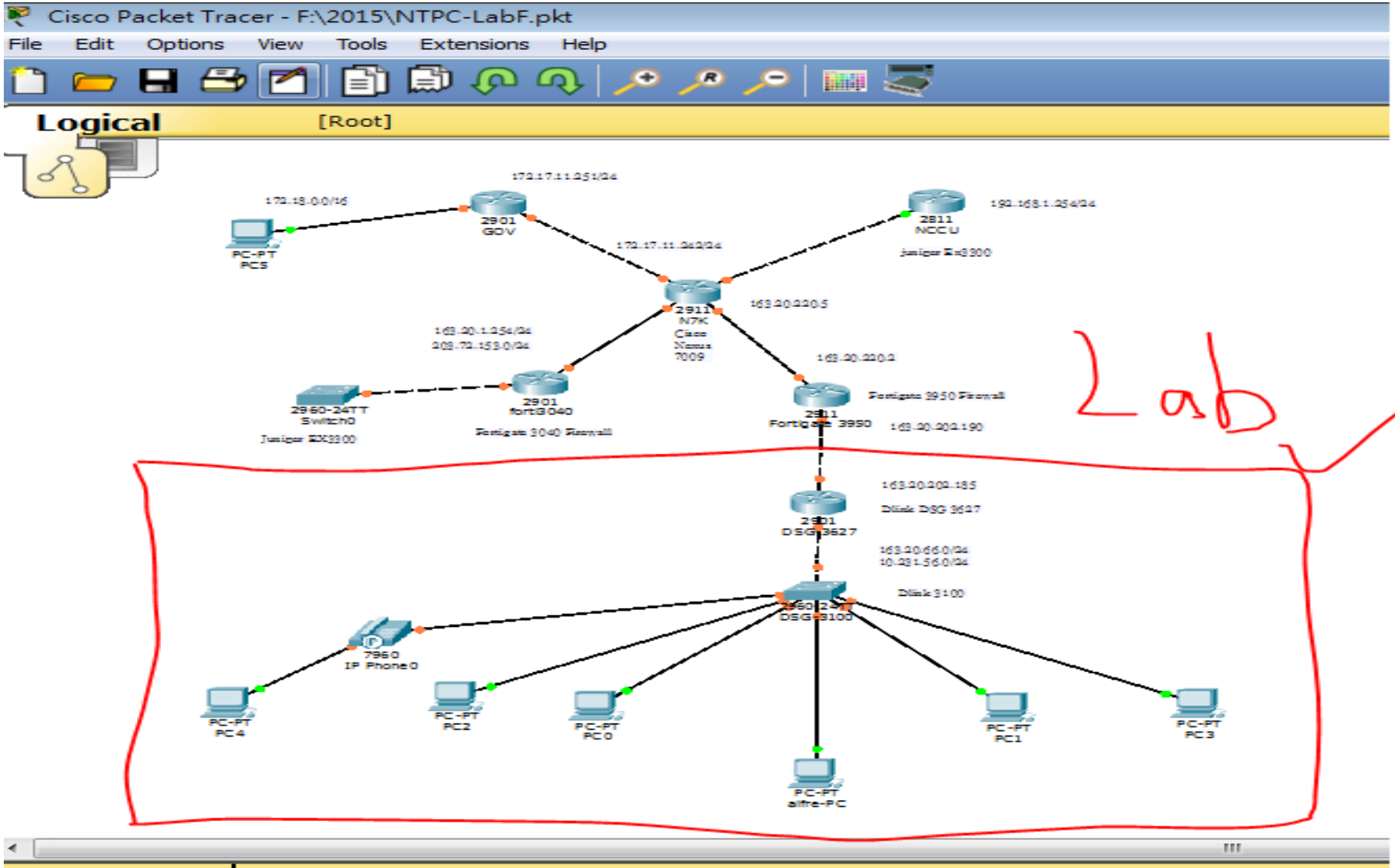


新北市拓撲圖

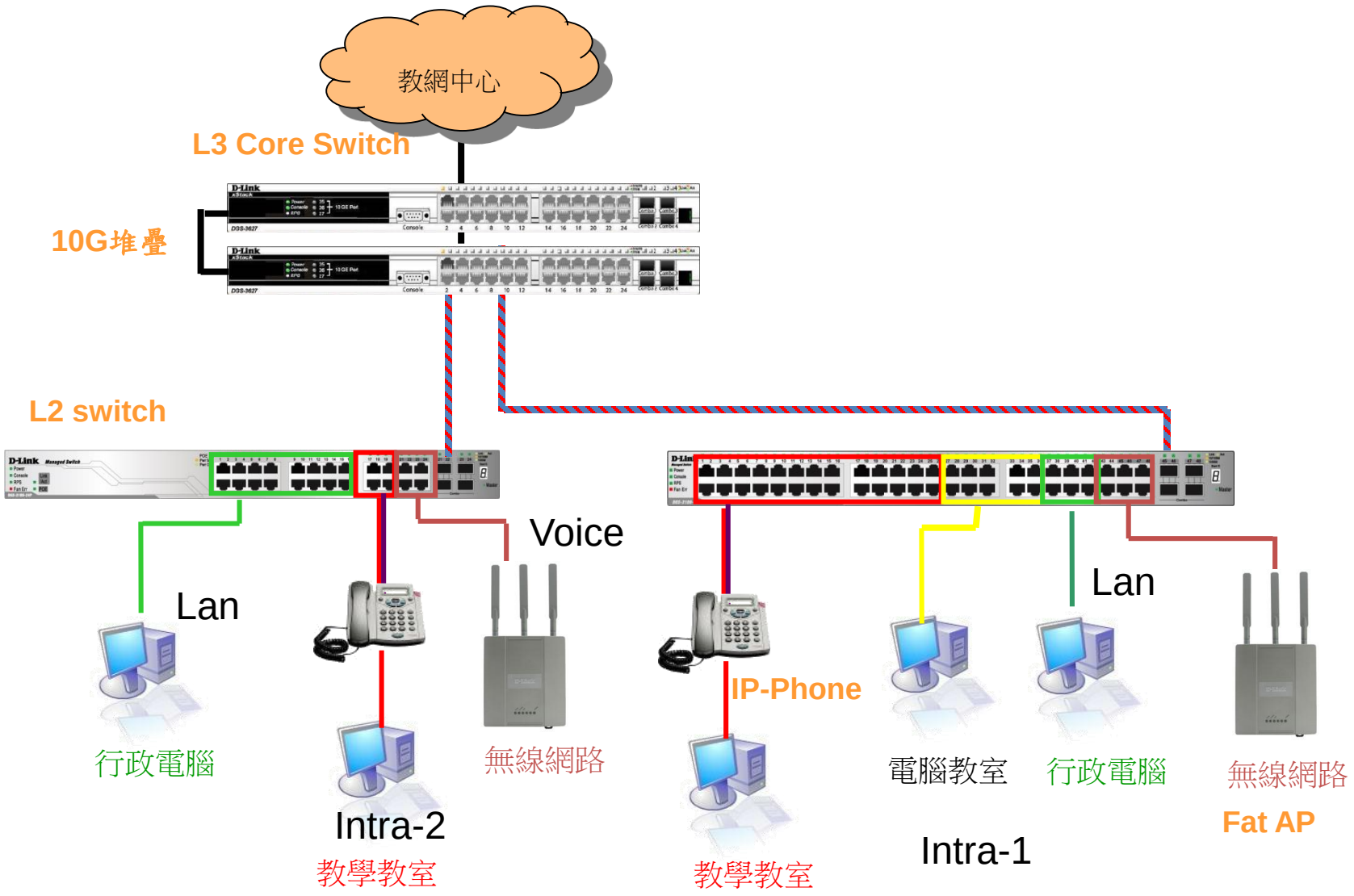
20150327



校園網路Lab拓譜圖


Cisco Packet Tracer - F:\2015\NTPC-LabF.pkt
File Edit Options View Tools Extensions Help
Logical
[Root]
172.17.11.251/24
172.18.0.0/16
2901
GOV
PC-PT
PC5
172.17.11.242/24
192.168.1.254/24
2811
NCCU
Juniper Ex8300
2911
N7K
Cisco
Nexus
7009
163.20.220.5
163.20.1.254/24
203.72.153.0/24
163.20.220.2
2960-24TT
Switch0
Juniper EX3300
2901
fort3040
Fortigate 3040 Firewall
2911
Fortigate 3950
Fortigate 3950 Firewall
163.20.202.190
Lab
2901
DSG3627
163.20.202.185
Dlink DSG 3627
163.20.66.0/24
10.231.56.0/24
Dlink 3100
2960-24TT
DSG3100
7960
IP Phone0
PC-PT
PC4
PC-PT
PC2
PC-PT
PC0
PC-PT
alfre-PC
PC-PT
PC1
PC-PT
PC3

新北市高國中小學校園網路架構圖



(實作資料) 學校ip分配表

- http://enctc.ntpc.edu.tw
- 網路服務
- 網路設定
- 連線單位Ipv4分配
- 連線單位Ipv6分配
- 光纖連線單位

學校IP基本網段

Vlan	VID	網段	IPv6	用途
Mgt	1	10.226.56.254	2001:288:22xx:1::/64	網管用 >101 L2,>201 AP
Wan	2	163.20.202.184/29	2001:288:2201::xx/124	對外連結網段
Lan	5	163.20.66.254/24	2001:288:22xx:5::/64	行政用 保留<10 ;>250
dsa_wan	8	10.253.56.254/24	2001:288:22xx:8::/64	DSA-WAN IP (10.253.56.1)
Intra-1	10	10.231.56.254/24	2001:288:22xx:10::/64	電腦教室
Intra-2	20	10.241.56.254/24	2001:288:22xx:20::/64	教學教室
Voice	25	10.243.56.0/24	2001:288:22xx:25::/64	VoIP
Wlan	30	10.251.56.254/24	2001:288:22xx:30::/64	無線網路 (IP移至DSA-3600使用)
WPA2	35	10.245.56.0/24	2001:288:22xx:35::/64	無線WAP2用
MAC	36	10.247.56.0/24	2001:288:22xx:36::/64	無線Mobile用

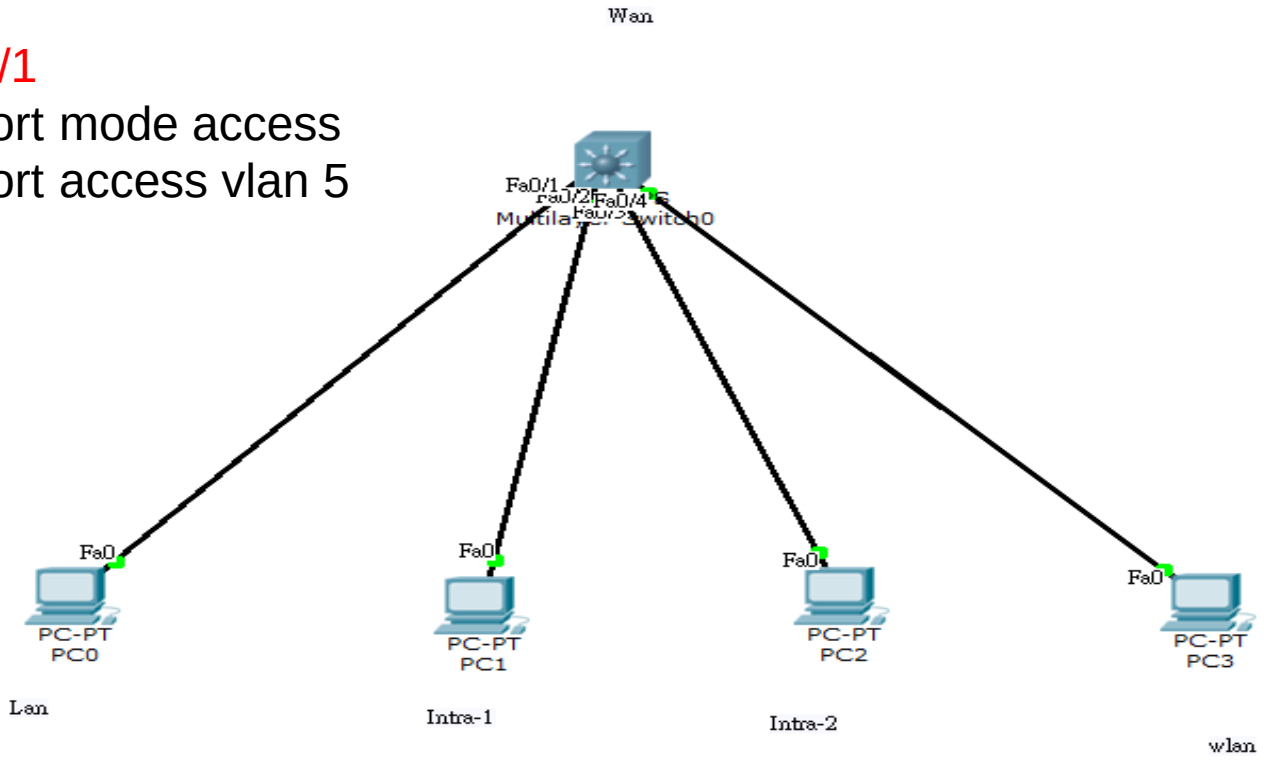
城門在哪?

Gateway(閘道)

Lab 5 基本練習Routing

三個Vlan間三個網段 PC相互通。

Config t
Inter fa0/1
Switchport mode access
Switchport access vlan 5



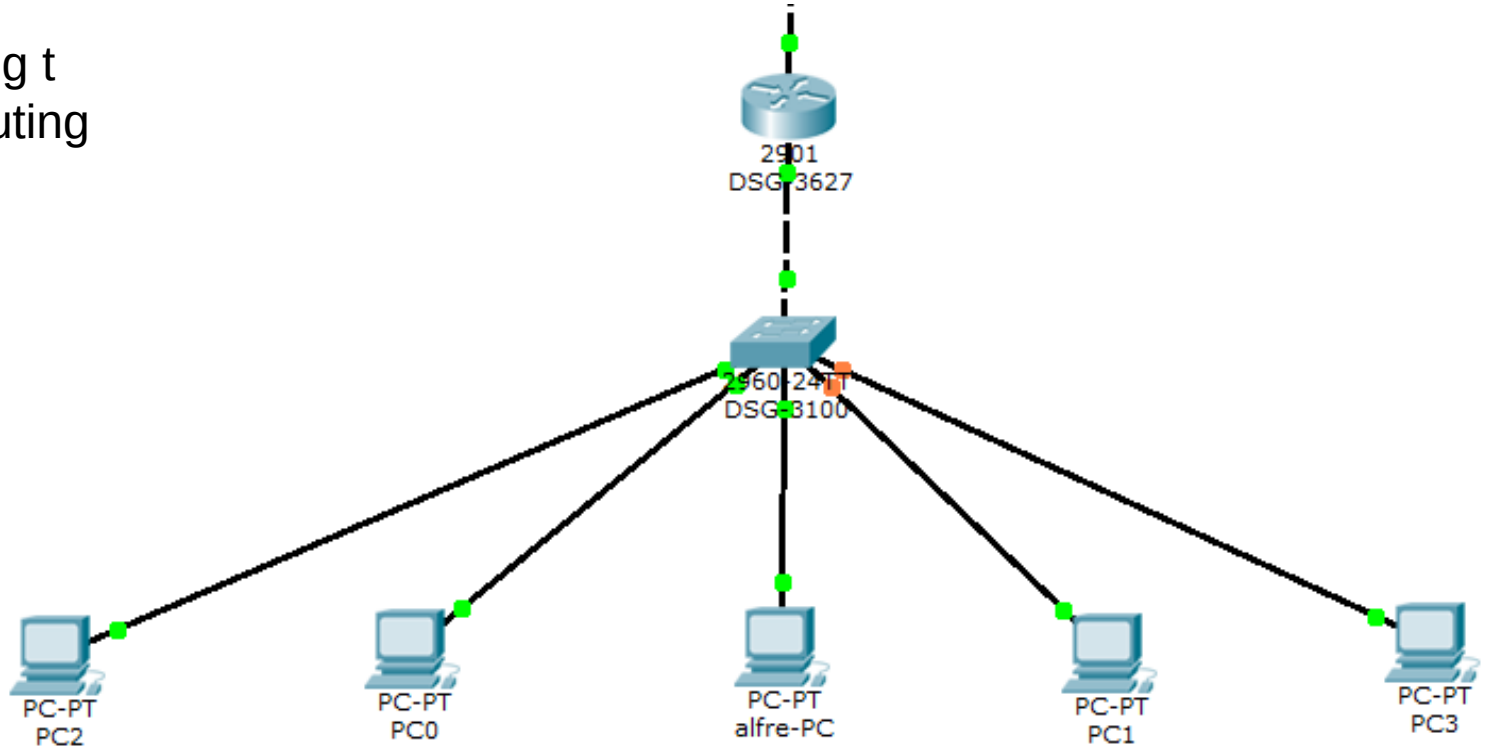
唯一出口通往他國

- 目的:了解GateWay設定
- 城池出口(Gateway)。
- 萬里長城 雁門關 WAN Route。
- ECMP

Lab 6基本練習Default Route

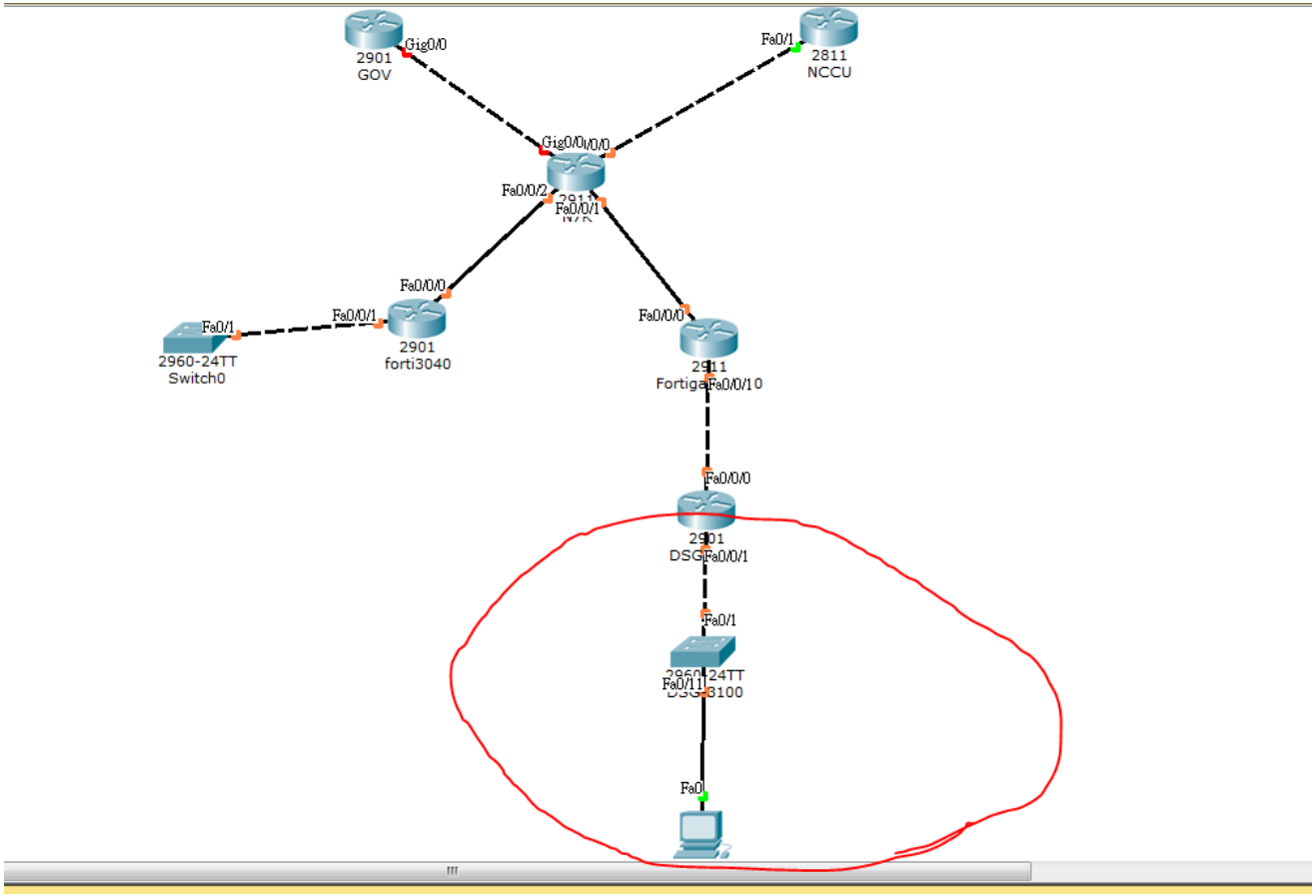
三個Vlan間三個網段 PC相互通，可上Internet。

Config t
Ip routing
變L3



Lab 7 與骨幹連結

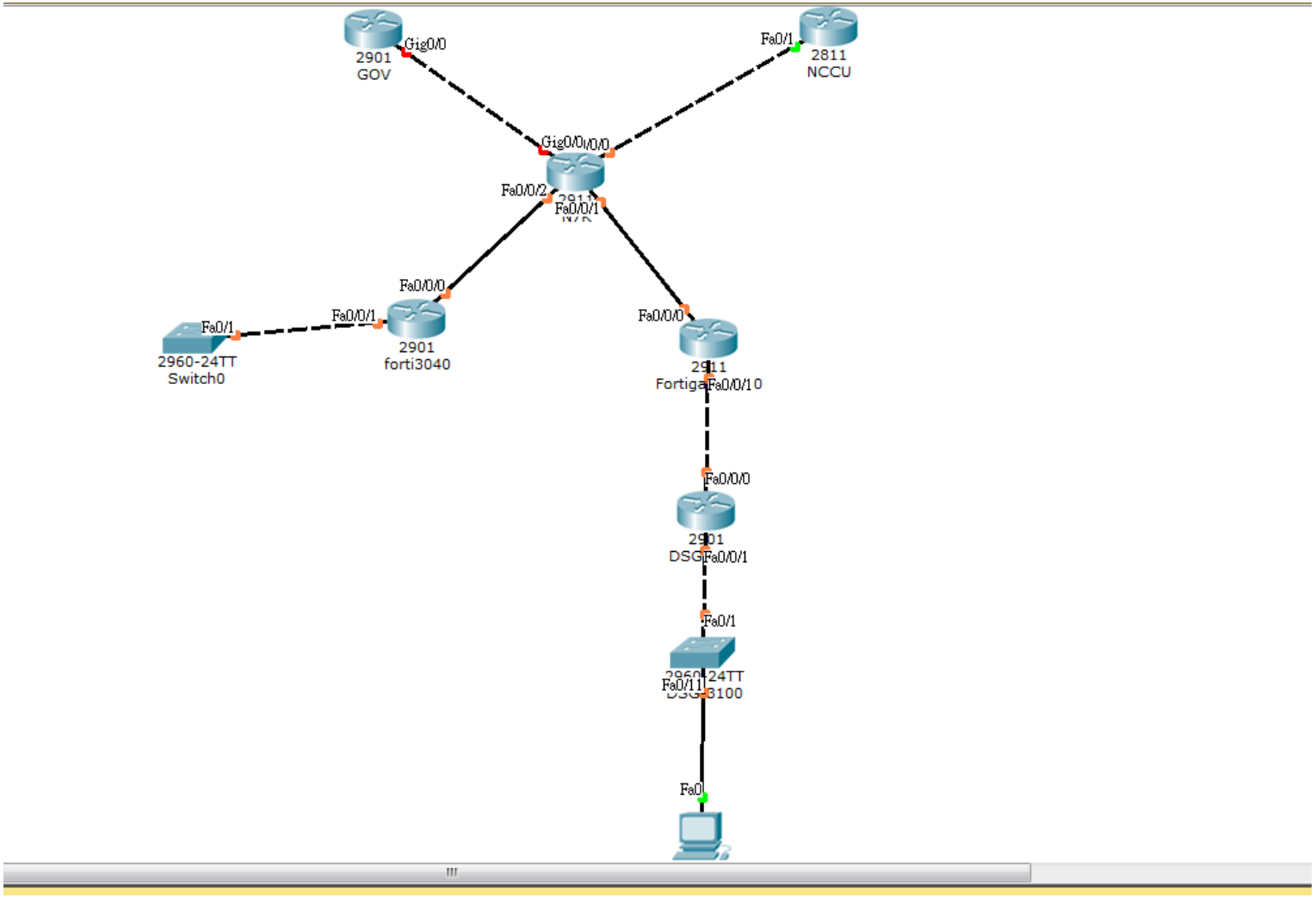
部分設備transparent mode不討論



PC搭配拓譜之Troubleshoot

- Ping Local GateWay
- Ping Wan ip
- Ping Firewall
- Ping Serverfarm
- Ping ISIS interface ip
- Ping ntpc.gov
- Ping nccu
- Ping www.google.com
- Tracert –d 看路由

Lab 8 Trouble Shoot



Cisco指令 and Dlink指令對照表

- L3維護指令
- L2常用維護指令
- Cisco維護指令

創Vlan

- DGS-3620
- create vlan lan tag 5

- DGS-1510
- configure terminal
- vlan 5
- name lan

- Cisco-3750X
- C3750X_CHT_F1-3(config)#vlan 5

設定vlan_port Accesc port

DGS-3620

- Config vlan lan add untagged 1
-

  DGS-1510
- configure terminal
- interface ethernet 1/0/1
- switchport hybrid native vlan 5
- switchport hybrid allowed vlan untagged 5
-

  Cisco-3750X
- C3750X_CHT_F1-3(config) interface TenGigabitEthernet1/1/1
- C3750X_CHT_F1-3(config) switchport mode access
- C3750X_CHT_F1-3(config) switchport access vlan 5
-

trunk port

- DGS-3620
- Config vlan default add untagged 1
- Config vlan intra-1 add tagged 1
- Config vlan intra-2 add tagged 1
- DGS-1510
- configure terminal
- interface ethernet 1/0/1
- switchport hybrid native vlan 1
- switchport hybrid allowed vlan untagged 1
- switchport hybrid allowed vlan tagged 10,20
- Cisdo-3750X
- interface TenGigabitEthernet1/1/1
- switchport trunk encapsulation dot1q
- switchport trunk allowed vlan 10,20
- switchport mode trunk

查看arp

- DGS-3620
- Sh arpentry

- DGS-1510
- Sh arp

- Cisco-3750X
- Sh arp

DGS-3620

```
ERDC-L3:admin#show arpentry
Command: show arpentry

 ARP Aging Time : 20
 ARP Retry Times : 4

Interface       IP Address        MAC Address         Type
--------------  ----------------  ------------------  ---------------
System          10.226.56.0       FF-FF-FF-FF-FF-FF   Local/Broadcast
System          10.226.56.2       54-B8-0A-C6-39-E0   Dynamic
System          10.226.56.4       54-B8-0A-C6-78-00   Dynamic
System          10.226.56.5       54-B8-0A-C6-78-80   Dynamic
```

DGS-1510

```
ERDC-L2-02>sh arp


S - Static Entry

IP Address         Hardware Addr      IP Interface   Age (min)
-----------------  -----------------  -------------  ---------------
  10.226.56.2      54-B8-0A-C6-39-E0  vlan1          forever
  10.226.56.254    3C-1E-04-B6-C2-00  vlan1          20

Total Entries: 2
```

Cisco-3750X

```
C3750X_CHT_F1-3#sh arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.1.1.1                -   c067.af06.a2c0  ARPA   Vlan1
Internet  163.20.202.185        191   0009.0fab.7a9d  ARPA   Vlan256
Internet  163.20.202.187        119   3c1e.04b6.c201  ARPA   Vlan256
Internet  163.20.202.188          -   c067.af06.a2c3  ARPA   Vlan256
Internet  163.20.202.190          0   0009.0f09.0008  ARPA   Vlan256
```

查看mac

```
ERDC-L3:admin#sh fdb
Command: show fdb

 Unicast MAC Address Aging Time  = 300

 VID  VLAN Name                        MAC Address        Port  Type     Status
 ---- -------------------------------- ------------------ ----- -------- -------
 1    default                          00-21-91-A7-1E-00 20    Dynamic Forward
 1    default                          00-21-91-A7-1E-FF 20    Dynamic Forward
 1    default                          3C-1E-04-B6-C2-00 CPU   Self    Forward
 1    default                          54-B8-0A-C6-39-E0 23    Dynamic Forward
 1    default                          54-B8-0A-C6-6E-C0 20    Dynamic Forward
 1    default                          54-B8-0A-C6-77-E0 23    Dynamic Forward
```

DGS-1510

```
ERDC-L2-02>sh mac-address-table

VLAN   MAC Address         Type         Ports
----   ----------------    ----------   ------------------------
   1   3C-1E-04-B6-C2-00   Dynamic      eth1/0/24
   1   3C-1E-04-B6-C3-16   Dynamic      eth1/0/24
   1   54-B8-0A-C6-39-E0   Static       CPU
   1   54-B8-0A-C6-77-E0   Dynamic      eth1/0/24
   1   54-B8-0A-C6-78-1A   Dynamic      eth1/0/24
```

Cisco-3750X

```
C3750X_CHT_F1-3#sh mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address         Type        Ports
----    -----------         --------    -----
 All    0100.0ccc.cccc      STATIC      CPU
 All    0100.0ccc.cccd      STATIC      CPU
 All    0180.c200.0000      STATIC      CPU
```

Sh vlan

六.查看vlan

DGS3620

```
ERDC-L3:admin#show vlan
Command: show vlan

VLAN Trunk State           : Disabled
VLAN Trunk Member Ports    :

VID                : 1                   VLAN Name         : default
VLAN Type          : Static              Advertisement     : Enabled
Member Ports       : 5,8,19-23,26-28
Static Ports       : 5,8,19-23,26-28
Current Tagged Ports    :
Current Untagged Ports: 5,8,19-23,26-28
Static Tagged Ports     :
Static Untagged Ports   : 5,8,19-23,26-28
Forbidden Ports         :
```

DGS1510

```
ERDC-L2-02#show vlan

 VLAN 1
   Name : default
   Tagged Member Ports    :
   Untagged Member Ports : 1/0/24-1/0/26,2/0/24-2/0/26

 VLAN 5
   Name : lan
   Tagged Member Ports    : 1/0/24-1/0/26,2/0/24-2/0/26
   Untagged Member Ports :
```

Cisco3750X

```
C3750X_CHT_F1-3#sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------
1    default                          active    Gi1/0/22, Gi1/0/23
```

Sh port

五.查看port狀態

DGS-3620

```
ERDC-L3:admin#show ports
Command: show ports

Port       State/          Settings            Connection          Address  AutoSpeed
           MDIX     Speed/Duplex/FlowCtrl Speed/Duplex/FlowCtrl Learning Downgrade
-------- --------- --------------------- --------------------- -------- ---------
1          Enabled   Auto/Disabled         1000M/Full/None       Enabled  Disabled
            Auto
2          Enabled   Auto/Disabled         1000M/Full/None       Enabled  Disabled
            Auto
3          Enabled   Auto/Disabled         1000M/Full/None       Enabled  Disabled
```

DGS-1510

```
ERDC-L2-02#sh interfaces status

Port            Status          VLAN            Duplex   Speed            Type
--------------- --------------- --------------- -------- ---------------- --------------
eth1/0/1        not-connected 20              auto     auto             1000BASE-T
eth1/0/2        not-connected 20              auto     auto             1000BASE-T
eth1/0/3        not-connected 20              auto     auto             1000BASE-T
eth1/0/4        connected       20              a-full   a-100            1000BASE-T
eth1/0/5        not-connected 20              auto     auto             1000BASE-T
eth1/0/6        not-connected 20              auto     auto             1000BASE-T
```

Cisco-3750X

```
C3750X_CHT_F1-3#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  10.1.1.1        YES NVRAM  up                    down
Vlan40                 163.20.250.254  YES NVRAM  up                    up
Vlan200                unassigned      YES unset  up                    up
Vlan256                163.20.202.188  YES NVRAM  up                    up
Vlan626                unassigned      YES unset  up                    up
FastEthernet0          unassigned      YES NVRAM  administratively down down
GigabitEthernet1/0/1   unassigned      YES unset  down                  down
GigabitEthernet1/0/2   unassigned      YES unset  down                  down
GigabitEthernet1/0/3   unassigned      YES unset  down                  down
GigabitEthernet1/0/4   unassigned      YES unset  up                    up
GigabitEthernet1/0/5   unassigned      YES unset  up                    up
```

LAB用指令

- Vlan database
- Config t
- Interface vlan　　interface fa0/X
- Switchport mode
- Switchport access vlan xx
- Switchport trunk allow vlan xx
- Ip add xx.xx.xx.xx　xx.xx.xx.xx　xx.xxx.xx.xx
- Ip route xx.xx.xx.xx xx.xx.xx.xx aa.aa.aa.aa

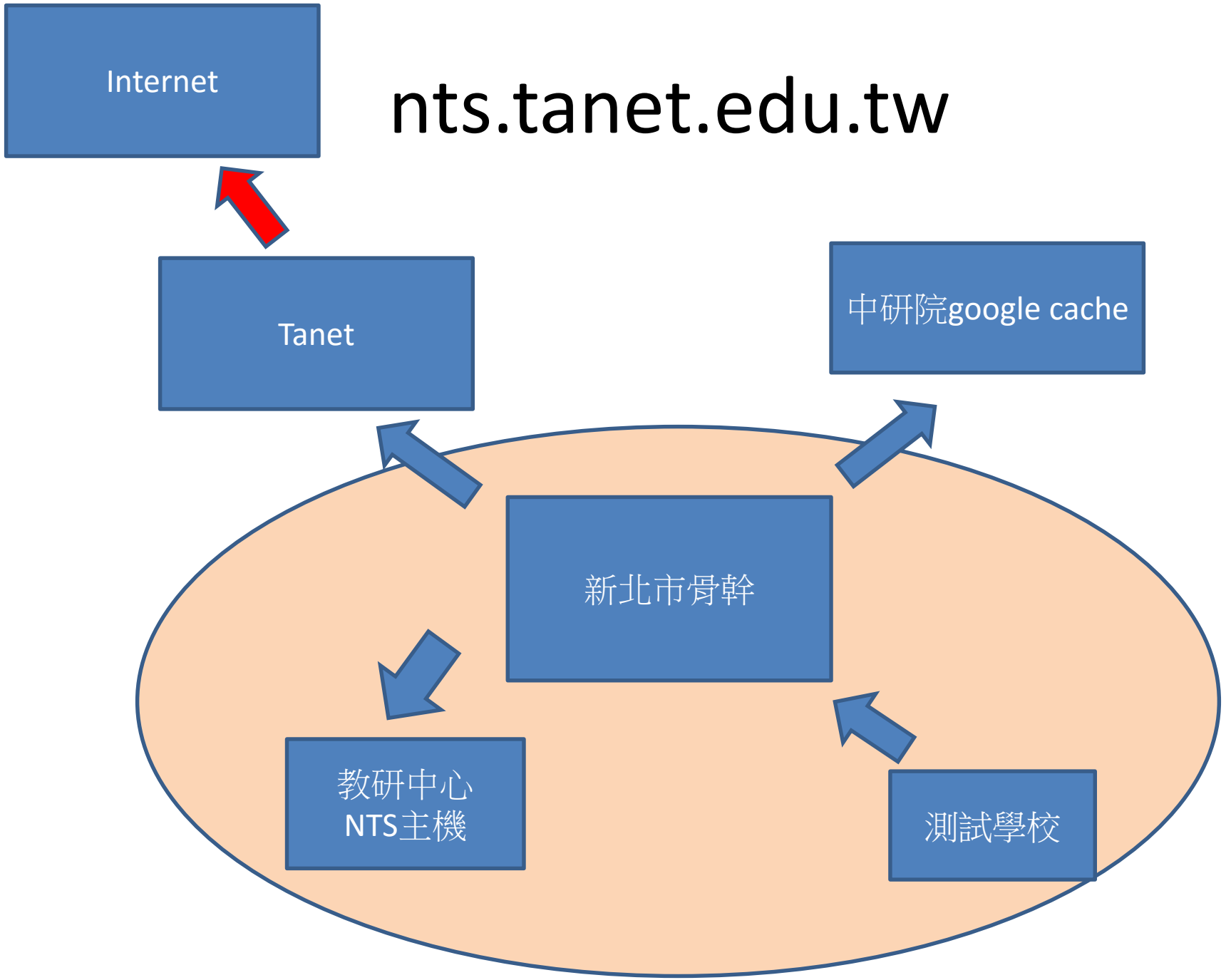
重要宣導

- 校園設備使用數量統計表
- 預計工程
  - 更換骨幹光纖、學校UTP線路
  - 班班有無線

如何檢測速率

- nts.tanet.edu.tw
  - 測試新北市教網
  - 台北區網二(政大)
  - 中研院(google)

nts.tanet.edu.tw



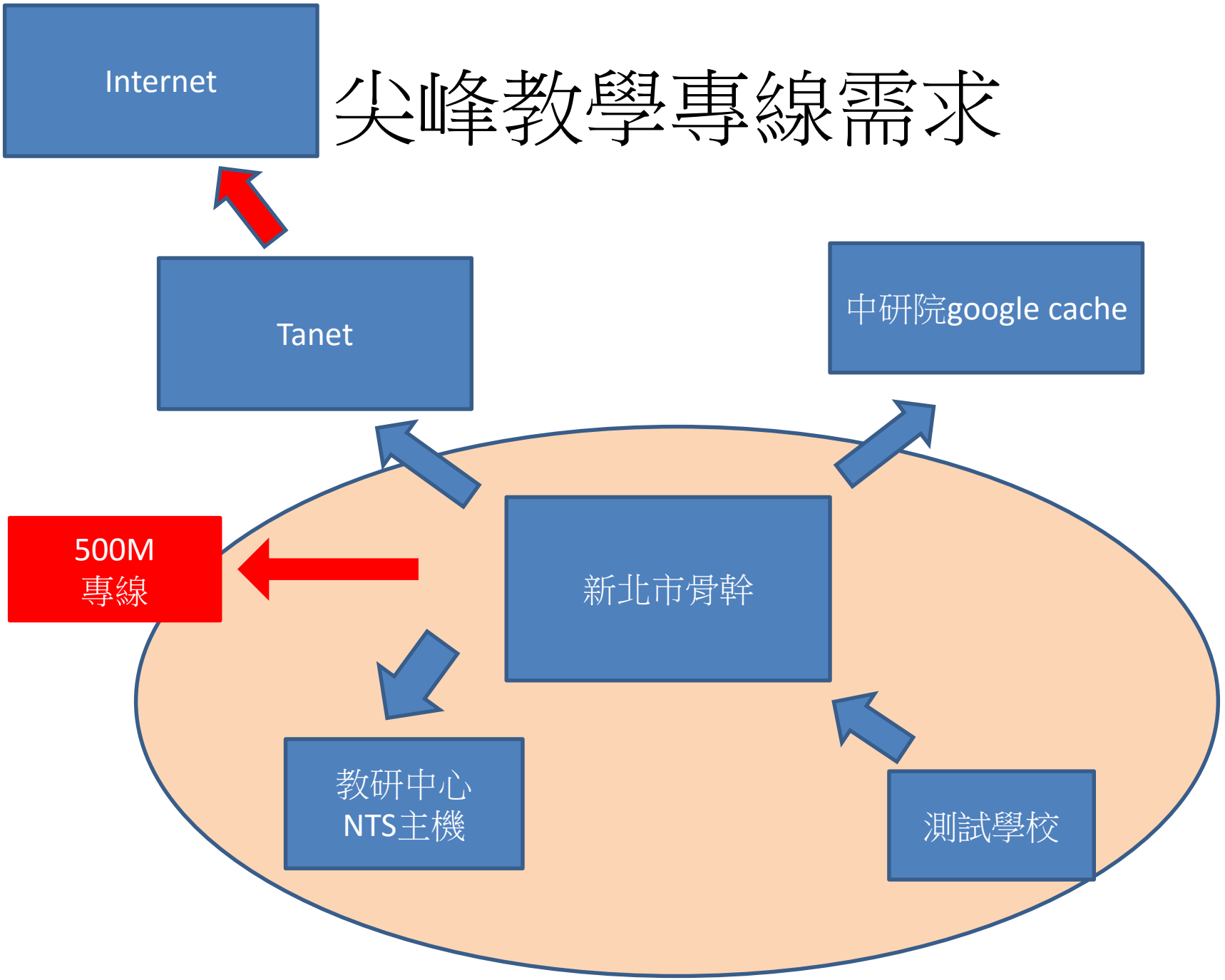
Network Address Translation
縮寫為NAT

- NAT使用說明及應用
  - source interface、
  - source pool
  - Destinatation pool

VPN技術說明及應用

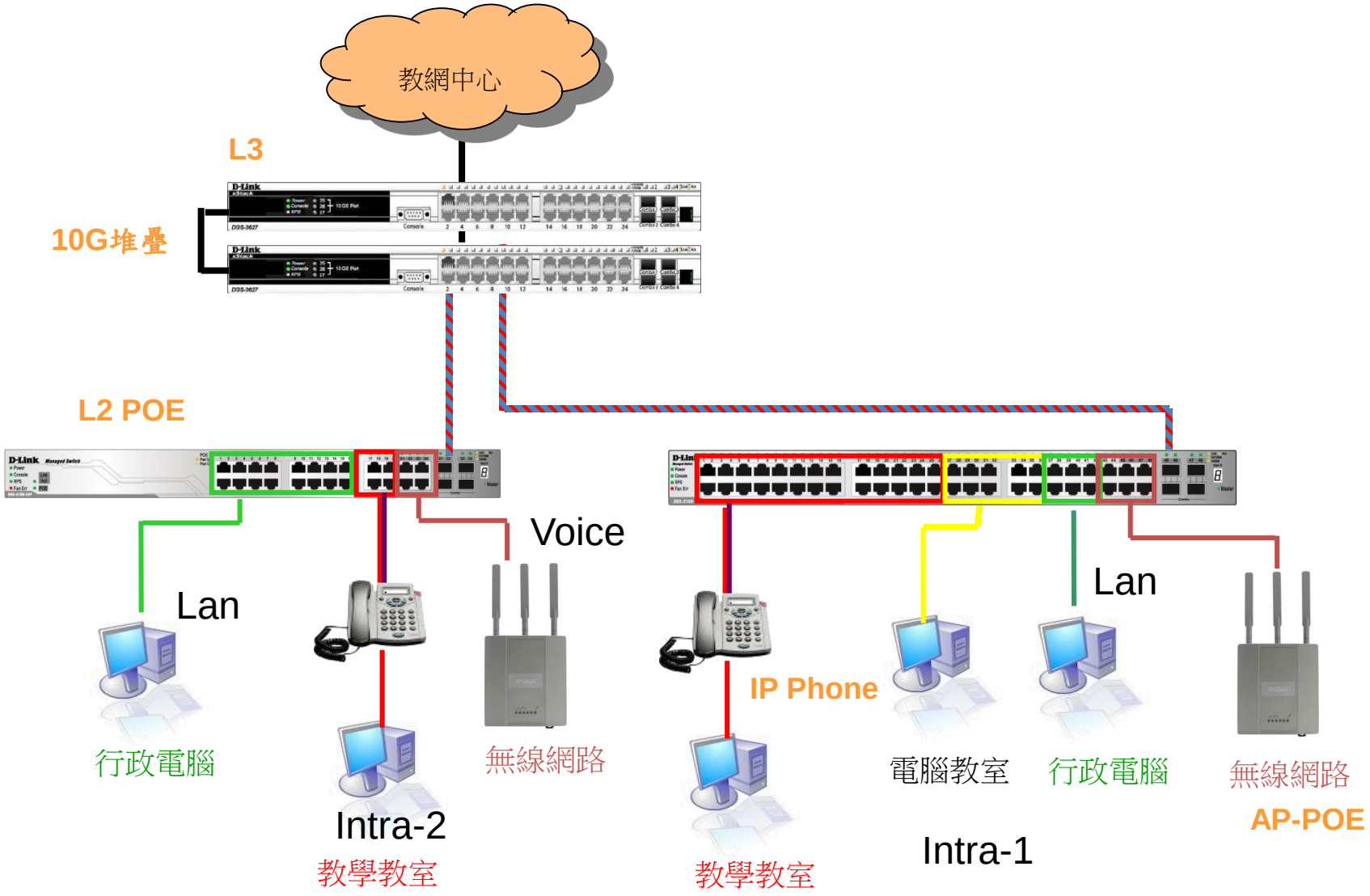
- SSL-VPN
- Tunnel
- Splite Tunnel

尖峰教學專線需求


Internet
Tanet
中研院google cache
500M
專線
新北市骨幹
教研中心
NTS主機
測試學校

- Firewall
  - Firewall security Authentication
  - Firewall security Policy
  - Firewall security IDP
  - Firewall security UTM
    - Anti-spam
    - Anti-virus
    - Content Filtering
    - Web Filtering
- LTM
  - VIP Pool Node

新北市高國中小學校園網路架構



學校IP網段說明

Vlan	VID	網段	IPv6	用途
Mgt	1	10.226.76.254	2001:288:22xx:1::/64	網管用
Wan	2	163.20.203.89/29	2001:288:2201::/124	對外連結網段
Lan	5	163.20.172.254/24	2001:288:22xx:5::/64	行政用
dsa_wan	8	10.253.76.254/24	2001:288:22xx:8::/64	DSA-WAN IP (10.253.76.1)
Intra-1	10	10.231.76.254/24	2001:288:22xx:10::/64	電腦教室
Intra-2	20	10.241.76.254/24	2001:288:22xx:20::/64	教學教室
Voice	25	10.243.76.0/24	2001:288:22xx:25::/64	VoIP
Wlan	30	10.251.76.254/24	2001:288:22xx:30::/64	無線網路 (IP移至DSA-3600使用)
WPA2	35	10.245.76.0/24	2001:288:22xx:35::/64	無線WAP2用
MAC	36	10.247.76.0/24	2001:288:22xx:36::/64	無線Mobile用

各校分配網段查詢
https://enctc.ntpc.edu.tw

首頁 > 網路服務 > 網路設定 > 連線單位IPv4分配

連線單位IPv4分配

連線單位	行政用LAN網段	電腦教室 (intra-1)	教學用 (intra-2)	網路電話VoIP	無線網路NTPC	無線網路WPA2	無線網路Mobile	NAT IP Range
欽賢國中-鼻頭分校	163.20.182.64/27	10.231.0.0/24	10.241.0.0/24	10.243.0.0/24	10.251.0.0/24	10.245.0.0/24	10.247.0.0/24	163.20.242.252
福和國中	163.20.173.0/24	10.231.67.0/24	10.241.67.0/24	10.243.67.0/24	10.251.67.0/24	10.245.67.0/24	10.247.67.0/24	163.20.242.1
中和國中	163.20.120.0/24	10.231.2.0/24	10.241.2.0/24	10.243.2.0/24	10.251.2.0/24	10.245.2.0/24	10.247.2.0/24	163.20.242.2
三峽國中	163.20.129.0/24	10.231.3.0/24	10.241.3.0/24	10.243.3.0/24	10.251.3.0/24	10.245.3.0/24	10.247.3.0/24	163.20.242.3
中園國小	163.20.62.0/25	10.231.4.0/24	10.241.4.0/24	10.243.4.0/24	10.251.4.0/24	10.245.4.0/24	10.247.4.0/24	163.20.242.4
安溪國小	163.20.95.128/25	10.231.5.0/24	10.241.5.0/24	10.243.5.0/24	10.251.5.0/24	10.245.5.0/24	10.247.5.0/24	163.20.242.5
昌福國小	163.20.239.128/25	10.231.6.0/24	10.241.6.0/24	10.243.6.0/24	10.251.6.0/24	10.245.6.0/24	10.247.6.0/24	163.20.242.6

Vlan 2 Default Route

路由器位址：學校Dlink L3 vlan2 interface ip
預設閘道：中心端Fortigate 3950 firewall Vdom interface ip

首頁 > 網路服務 > 網路設定 > 光纖連線單位

光纖連線單位

單位名稱	分區別	區	專線號碼	路由器位址	子網路遮罩	預設閘道
青山國中小	七星分區	汐止區	264YD000013	163.20.202.57	255.255.255.248	163.20.202.62
樟樹國中	七星分區	汐止區	264YD000014	163.20.202.65	255.255.255.248	163.20.202.70
長安國小	七星分區	汐止區	264YD000020	163.20.202.169	255.255.255.248	163.20.202.174
北峰國小	七星分區	汐止區	264YD000002	163.20.208.193	255.255.255.248	163.20.208.198
北港國小	七星分區	汐止區	264YD000003	163.20.208.201	255.255.255.248	163.20.208.206
汐止國中	七星分區	汐止區	264YD000004	163.20.208.209	255.255.255.248	163.20.208.214
市立秀峰高中	七星分區	汐止區	264YD000005	163.20.209.1	255.255.255.248	163.20.209.6
秀峰國小	七星分區	汐止區	264YD000006	163.20.209.9	255.255.255.248	163.20.209.14
金龍國小	七星分區	汐止區	264YD000007	163.20.209.17	255.255.255.248	163.20.209.22
東山國小	七星分區	汐止區	264YD000010	163.20.209.25	255.255.255.248	163.20.209.30
崇德國小	七星分區	汐止區	264YD000008	163.20.209.97	255.255.255.248	163.20.209.102
樟樹國小	七星分區	汐止區	264YD000009	163.20.209.169	255.255.255.248	163.20.209.174
白雲國小	七星分區	汐止區	227YD000208	163.20.209.193	255.255.255.248	163.20.209.198
汐止國小	七星分區	汐止區	264YD000011	163.20.209.233	255.255.255.248	163.20.209.238
保長國小	七星分區	汐止區	264YD000012	163.20.209.241	255.255.255.248	163.20.209.246

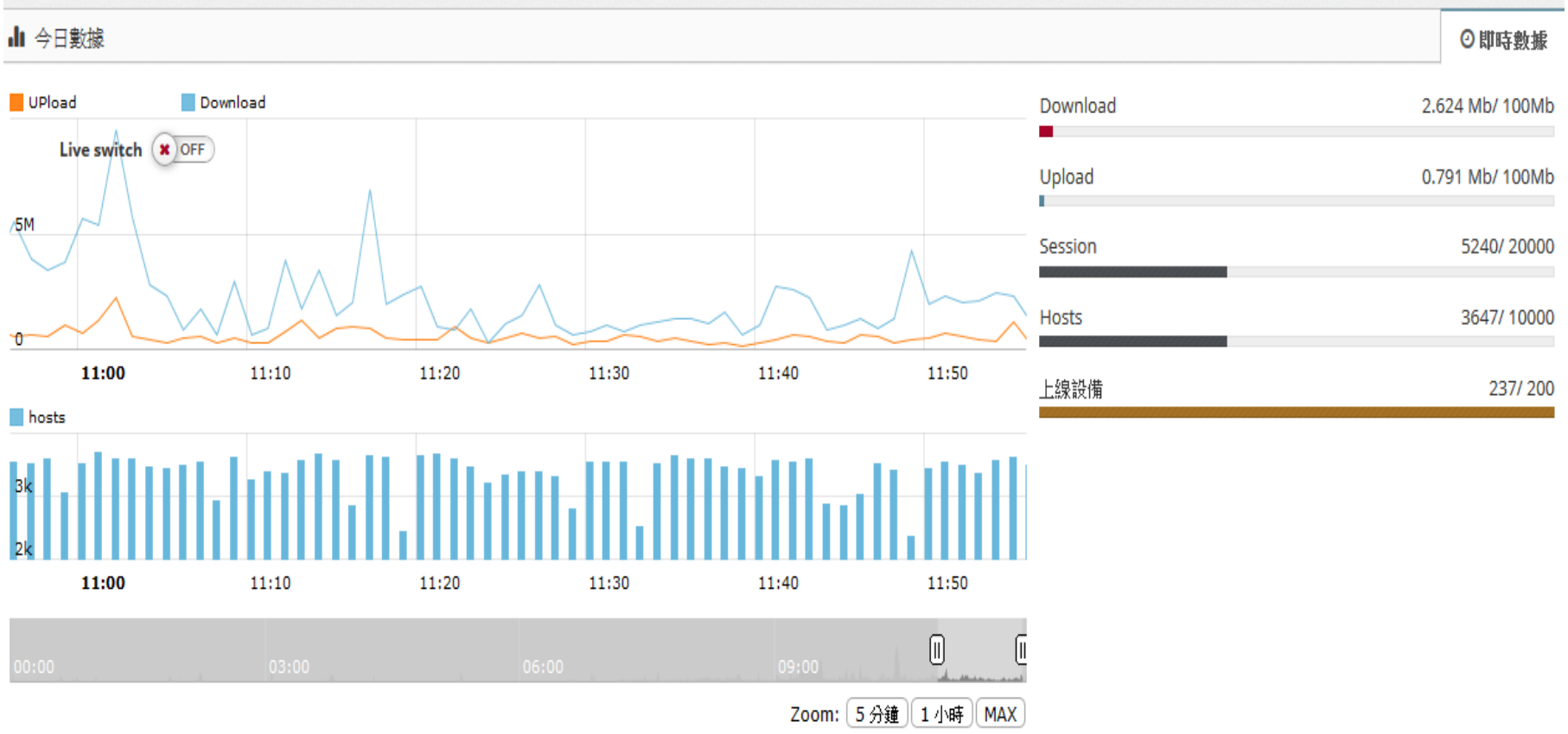
SNGN管理網站及用途

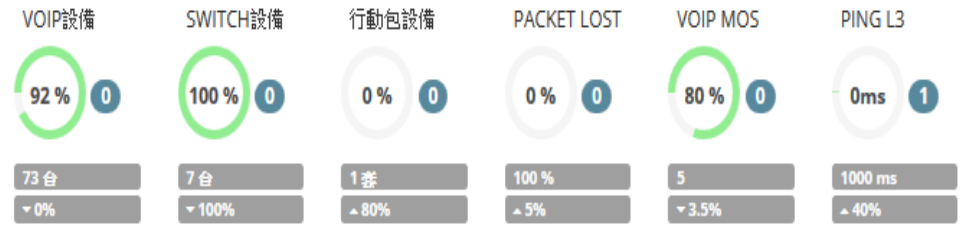
- Sngn.enctc.ntpc.edu.tw
- 網路拓譜圖
- 無線網路拓譜圖
- L3 ip
- L2 ip
- AP Controller ip
- TroubleShoot

編碼說明

- S site survey 場勘時的設備
- N 新設備
- O 舊設備
- Sn 堆疊n台
- 已使用port
- 預估使用port
- 學校目前線上待換L2 switch數
- 使用總port數=已使用port+ol2 port數
- 冗餘port　尚未使用port

SNGN 設備監控


今日數據
即時數據
UPload
Download
Live switch
OFF
5M
0
11:00
11:10
11:20
11:30
11:40
11:50
hosts
3k
2k
00:00
03:00
06:00
09:00
Zoom:
5 分鐘
1 小時
MAX
Download 2.624 Mb/ 100Mb
Upload 0.791 Mb/ 100Mb
Session 5240/ 20000
Hosts 3647/ 10000
上線設備 237/ 200


VOIP設備
92 %
0
73 台
0%
SWITCH設備
100 %
0
7 台
100%
行動包設備
0 %
0
1 套
80%
PACKET LOST
0 %
0
100 %
5%
VOIP MOS
80 %
0
5
3.5%
PING L3
0ms
1
1000 ms
40%

校園無線網路介紹

WIFI Analyzer

- 在2.4GHz頻段下它的理論速度能達到450Mbps。在5GHz頻段下它的理論速度更能達到1300Mbps，比目前的802.11n路由器快三倍

家用無線AP設定

設定分為三部分

WAN IP (internet)
對外連線

LAN IP
內部有線

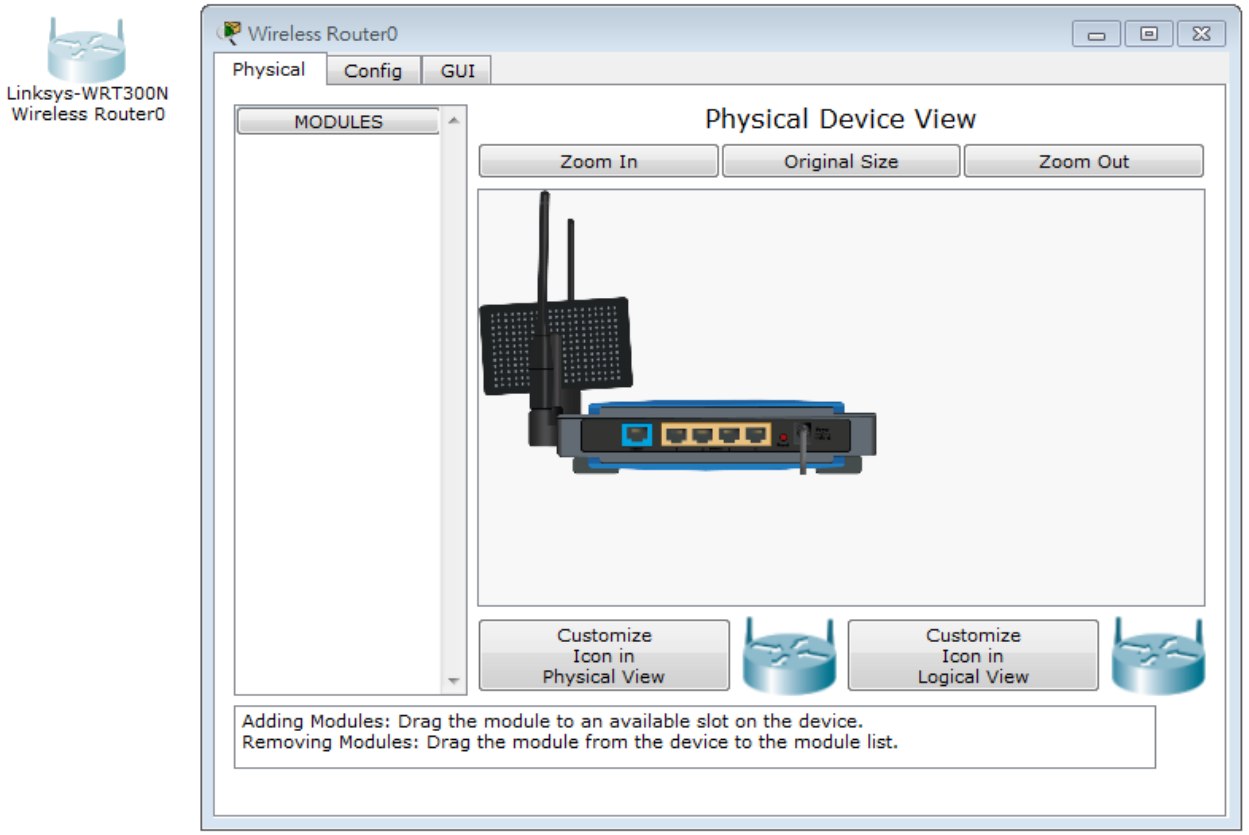
Wireless
內部無線

SSID

WPA2

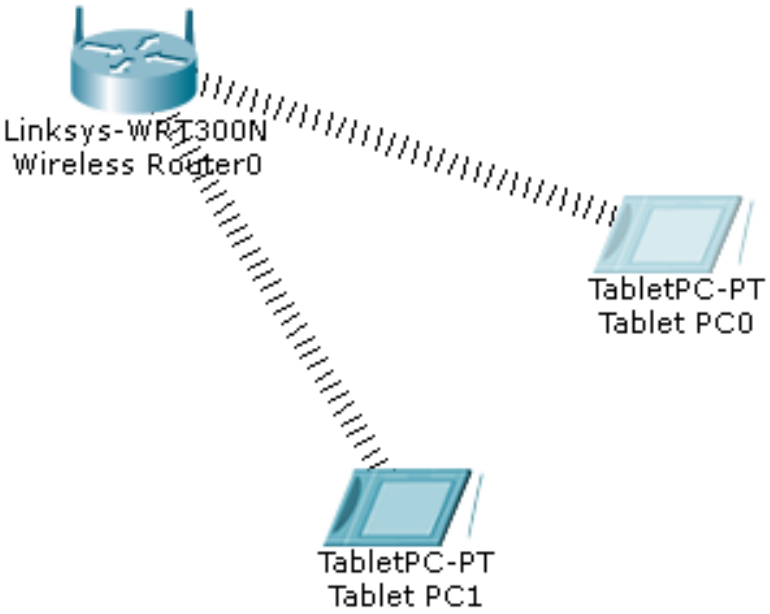
Preshare key

Redius server



家庭式網路

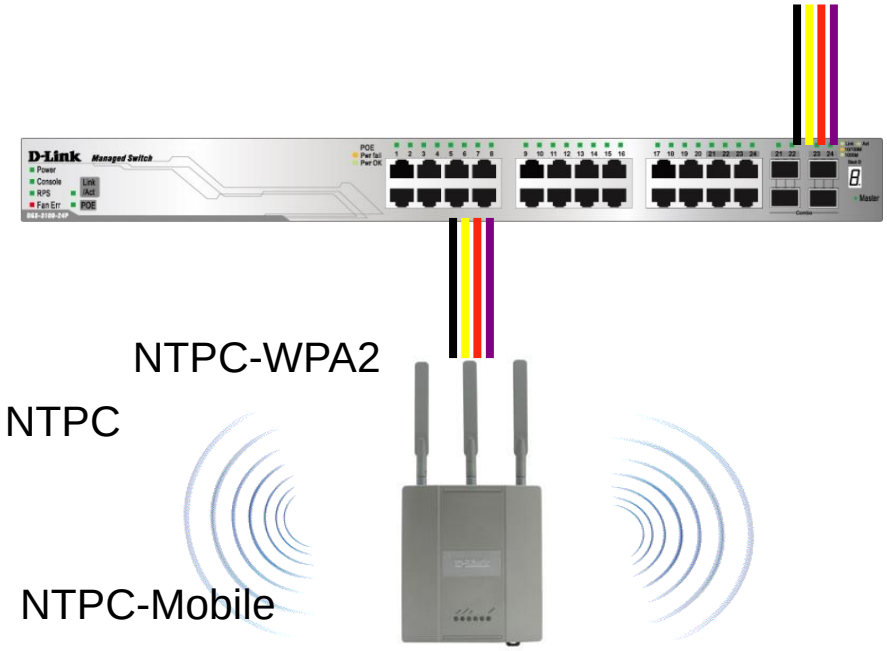
- Cisco PT6.0
- 模擬AP設定
  - WAN(PPPoE,Static ip)
  - WLAN
  - LAN
  - DHCP
  - NAT



無線網路環境類型

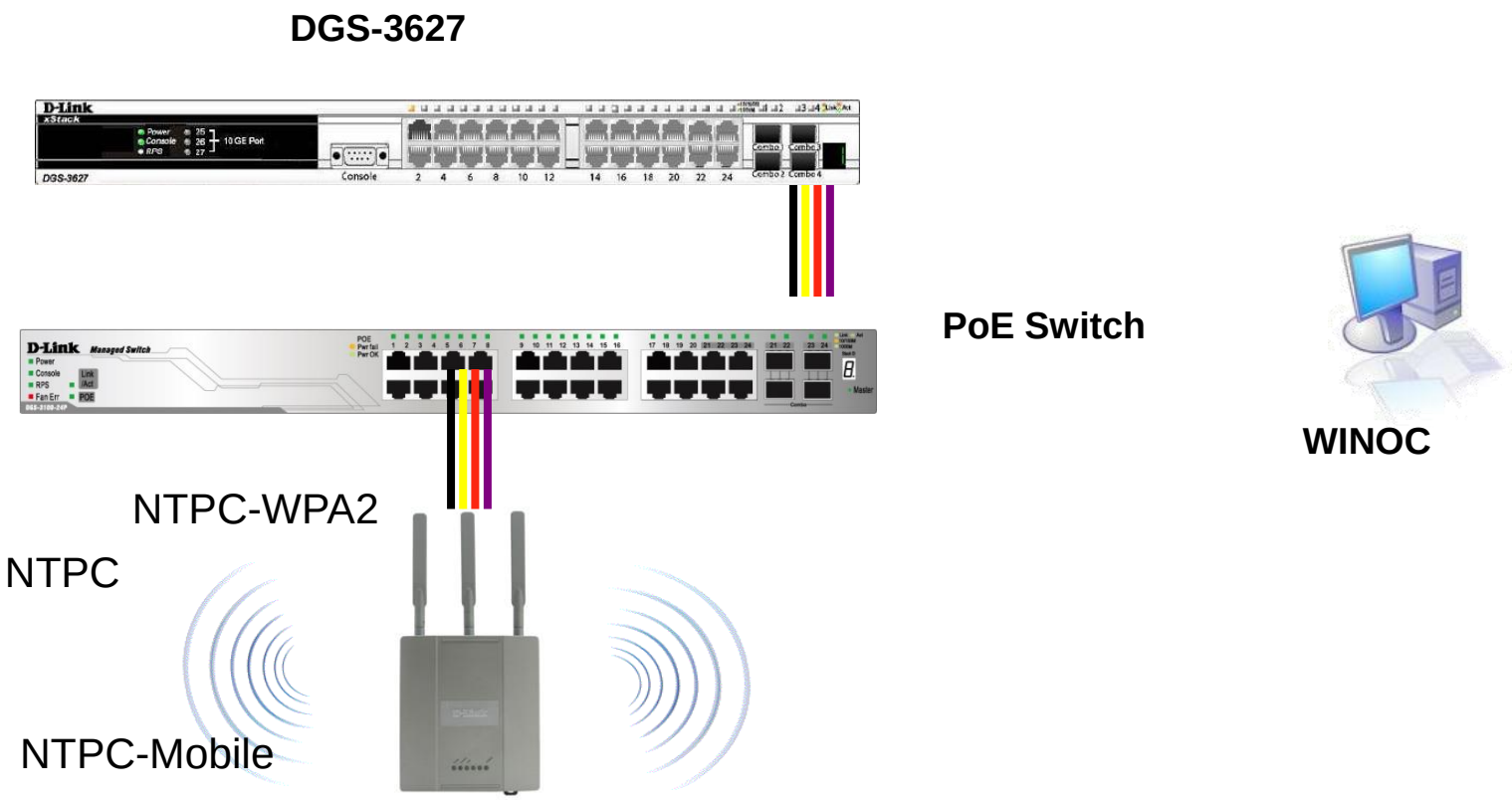
- 家庭小型無線網路環境
  - Cisco LinKsys、Dlink…
  - 隱藏SSID + Password
- 中型校園網路
  - 學校SNGN架構，路由設定
  - Local User認證
- 大型區域網路
  - Radius認證
  - Thin AP

SNGN無線AP架構應用說明



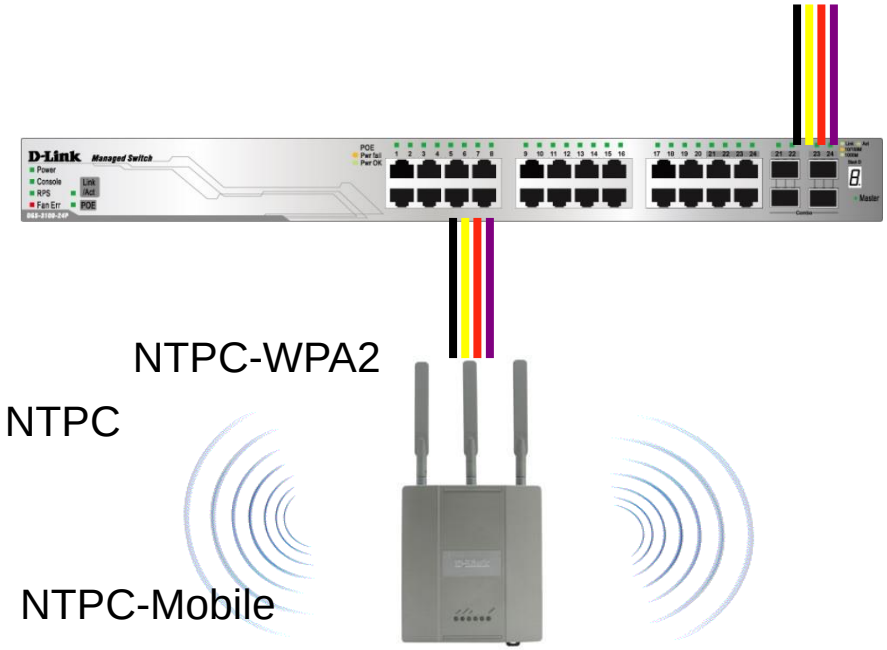
每台無線AP提供四組SSID,
NTPC、NTPC-Roaming提供web認證功能
NTPC-WPA2、EduRoam提供WPA2認證功能
NTPC-Mobile提供行動裝置MAC認證功能

無線AP認證機制說明



SSID NTPC 、NTPC-Roaming認證
　　透過Web-Portal與DWC-2000或Fortigate 3950B系統進行驗證
SSID NTPC-WAP2 、EduRoam則透過AP與後端認證系統進行
SSID NTCP-Mobile則透過L3 Switch與後端系統進行驗證

SNGN無線AP架構應用說明



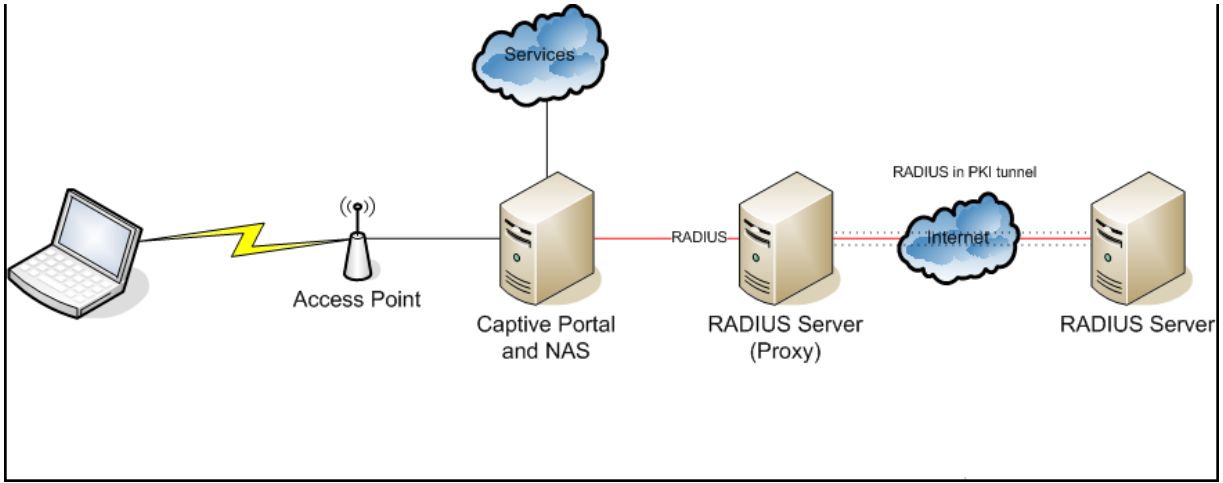
每台無線AP提供四組SSID,
NTPC、NTPC-Roaming提供web認證功能
NTPC-WPA2、EduRoam提供WPA2認證功能
NTPC-Mobile提供行動裝置MAC認證功能

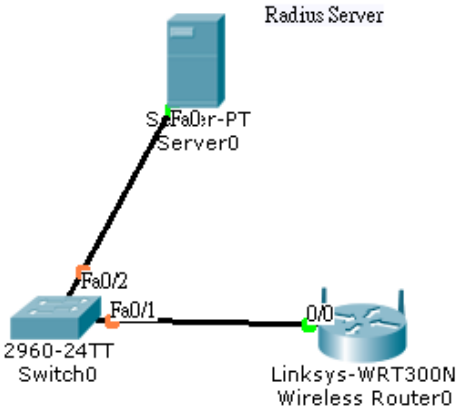
Portal認證行為模式

- 1.Client連上SSID NTPC
- 2. DWC-2000無線網路控制器 or firewall認證
  - Radius Server 203.72.153.61—62 port UDP 1812 -1813
- 3.帶DWC-2000 ip (Vlan 8)送radius認證
- 4.認證通過放行
- 5.認證沒過不能用，也不會清ip
- 6.Gateway在DWC-2000 WLan

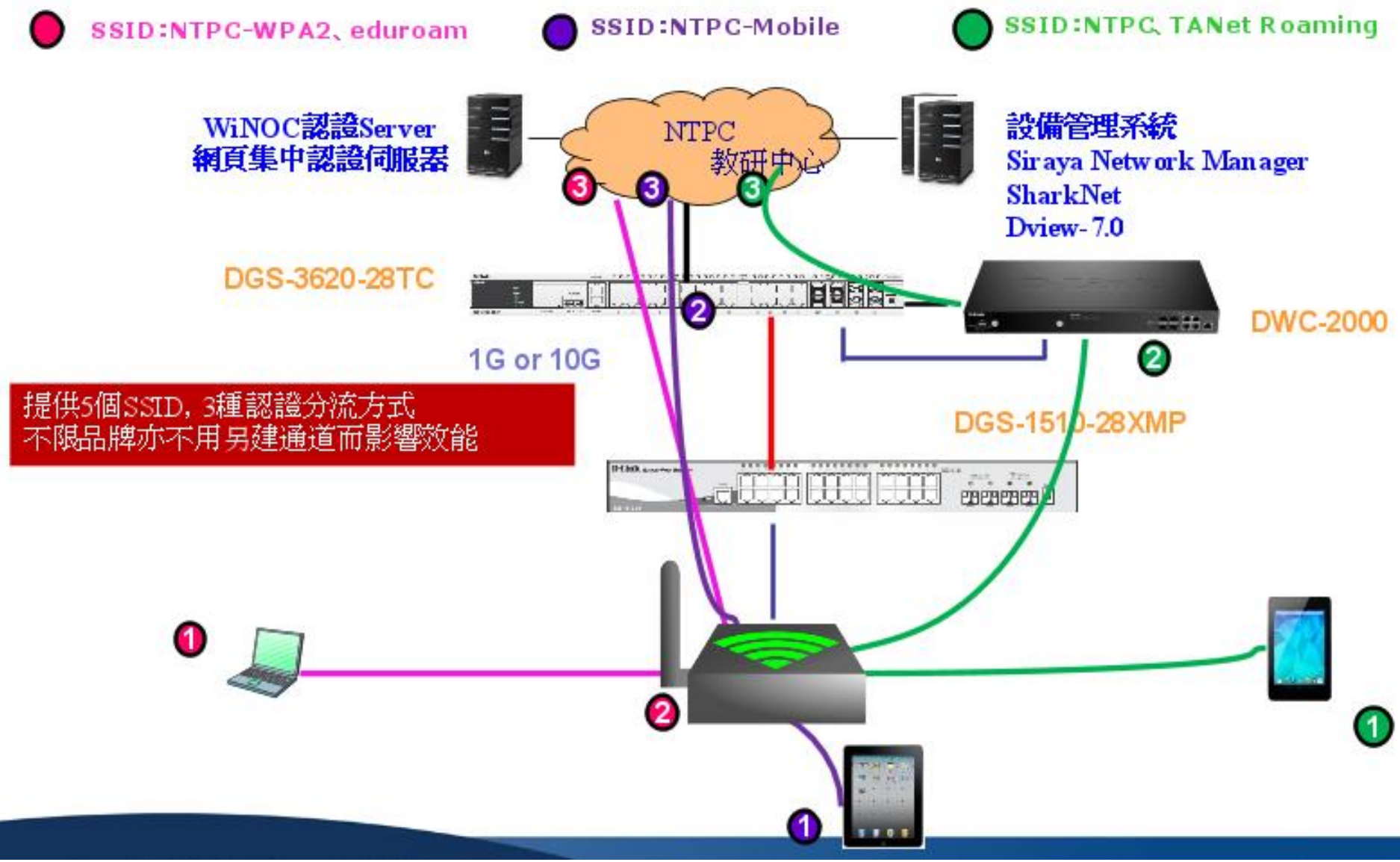
認證:Radius Server

- Authenticator(Dlink 3620)帶的HOST IP
- Radius Server(Winoc)是否已經加入 Authenticator ip
- Key「共享密碼」 (Shared secret)
- Firewall udp port 1812-1813





無線網路認證之機制



NTPC-WPA2須由DWC2000協助認證後，才走3路由上網。

Winoc設定設備radius key

WLAN認證架構圖

WINOC

TANET

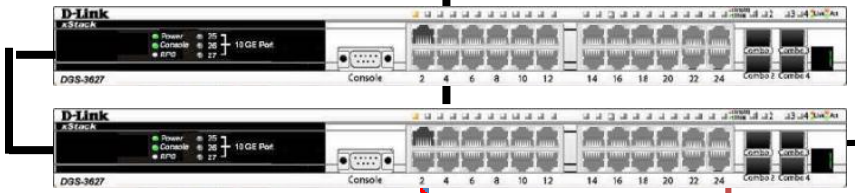
DGS-3627

Vlan 8

10.253.x.1

DWC-2000

10G堆疊



Vlan 8

10.251.X.254

Vlan Wlan (Vlan 30)

DGS-3100-24P

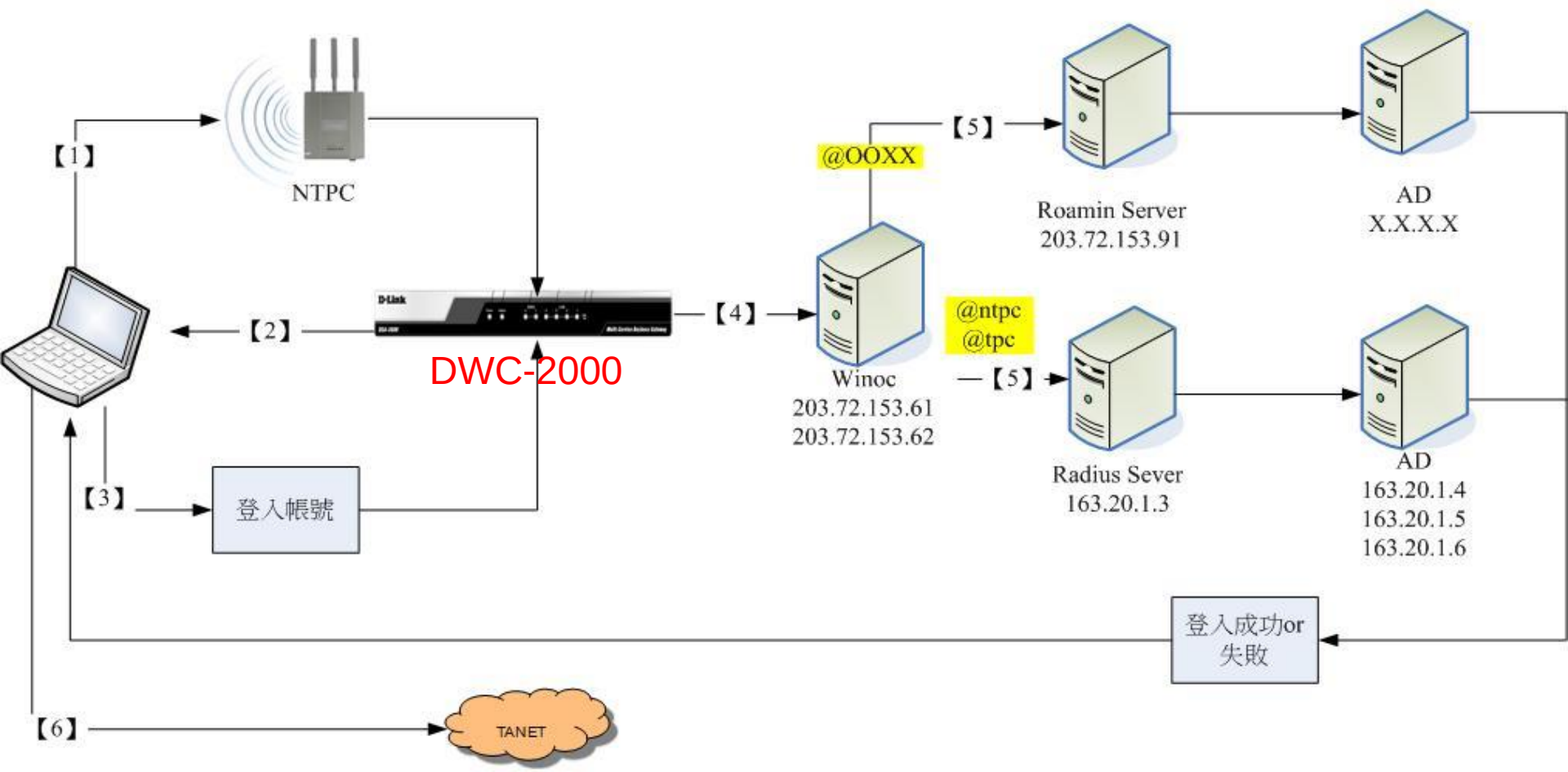
1、ip 10.251.x.x由DHCP配發

2、L3 10.251.xx.0 Default Rout 10.253.xx.1

3. DWC-2000 Wan GW 10.253.xx.254

AP

新北市無線網路NTPC架構圖

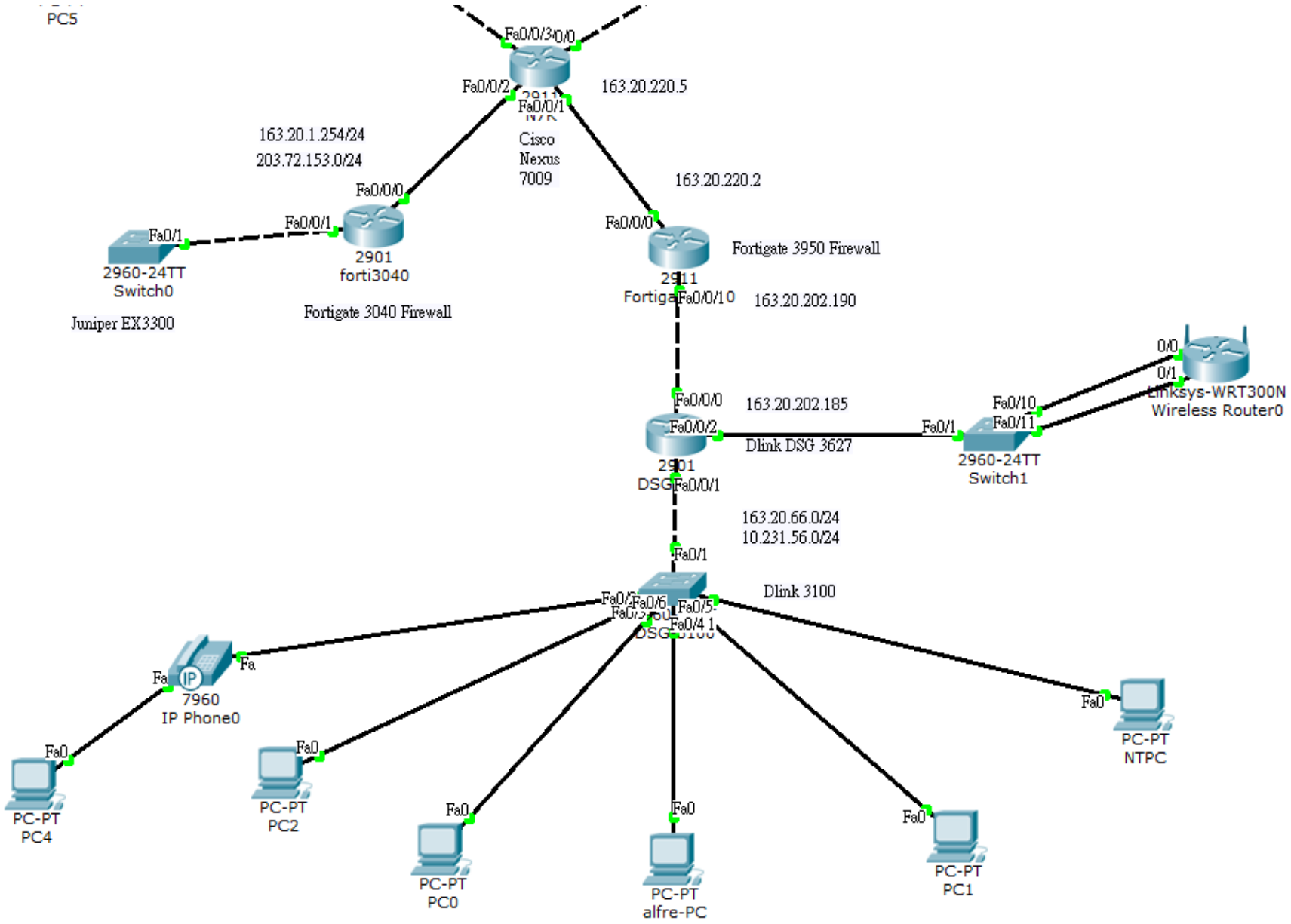


【1】電腦連線NTPC
【2】電腦取得10.251 or 10.252網段
【3】使用者key 入帳號密碼
【4】如使用者只輸入帳號，未輸入domain，
【5】查看domain，判斷要往哪裡送
【6】如登入成功，可以上網

LAB用指令

- Vlan database
- Config t
- Interface vlan　　interface fa0/X
- Switchport mode
- Switchport access vlan xx
- Switchport trunk allow vlan xx
- Ip add xx.xx.xx.xx　xx.xx.xx.xx　xx.xxx.xx.xx
- Ip route xx.xx.xx.xx xx.xx.xx.xx aa.aa.aa.aa

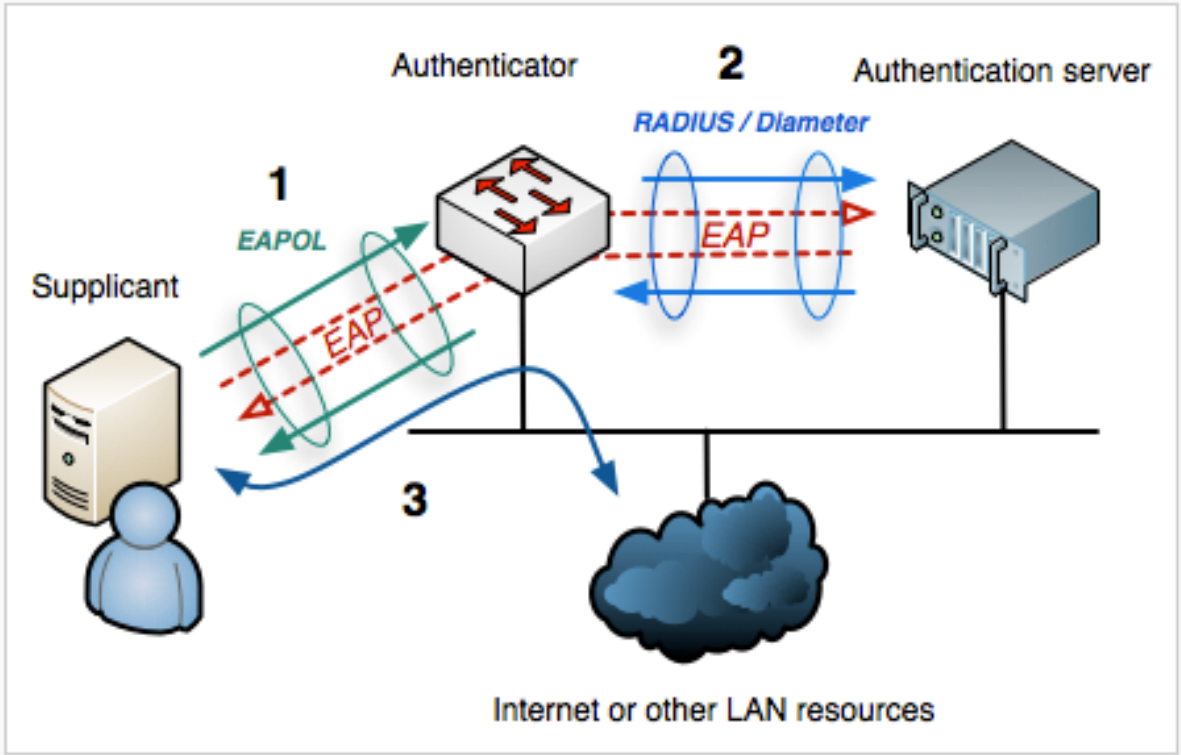
整體架構Lab


PC5
Fa0/0/3
Fa0/0/2
Fa0/0/1
163.20.220.5
Cisco
Nexus
7009
163.20.1.254/24
203.72.153.0/24
Fa0/0/0
Fa0/0/1
Fa0/1
2960-24TT
Switch0
Juniper EX3300
2901
forti3040
Fortigate 3040 Firewall
163.20.220.2
Fa0/0/0
Fortigate 3950 Firewall
Fa0/0/10
163.20.202.190
0/0
0/1
Linksys-WRT300N
Wireless Router0
Fa0/0/0
163.20.202.185
Fa0/0/2
Fa0/10
Fa0/11
Fa0/1
Dlink DSG 3627
2960-24TT
Switch1
Fa0/0/1
163.20.66.0/24
10.231.56.0/24
Fa0/1
Dlink 3100
Fa0/6
Fa0/5
Fa0/4
Fa
IP
7960
IP Phone0
Fa0
PC-PT
PC4
PC-PT
PC2
PC-PT
PC0
PC-PT
alfre-PC
PC-PT
PC1
PC-PT
NTPC

Dlink MAC auth

- 1.Client 發出EAP封包
- 2.經L2由Vlan 36 引導至L3 Switch
- 3.L3收到MAC ，帶MAC帳號及變更後的密碼，向Radius發出認證請求。
- 4.認證通過，unblockPort
- 5.Client取得ip後上網。
- 6.Gateway在L3
- 建議設MAC設備：
  - 列表機，無線ip phone手機….

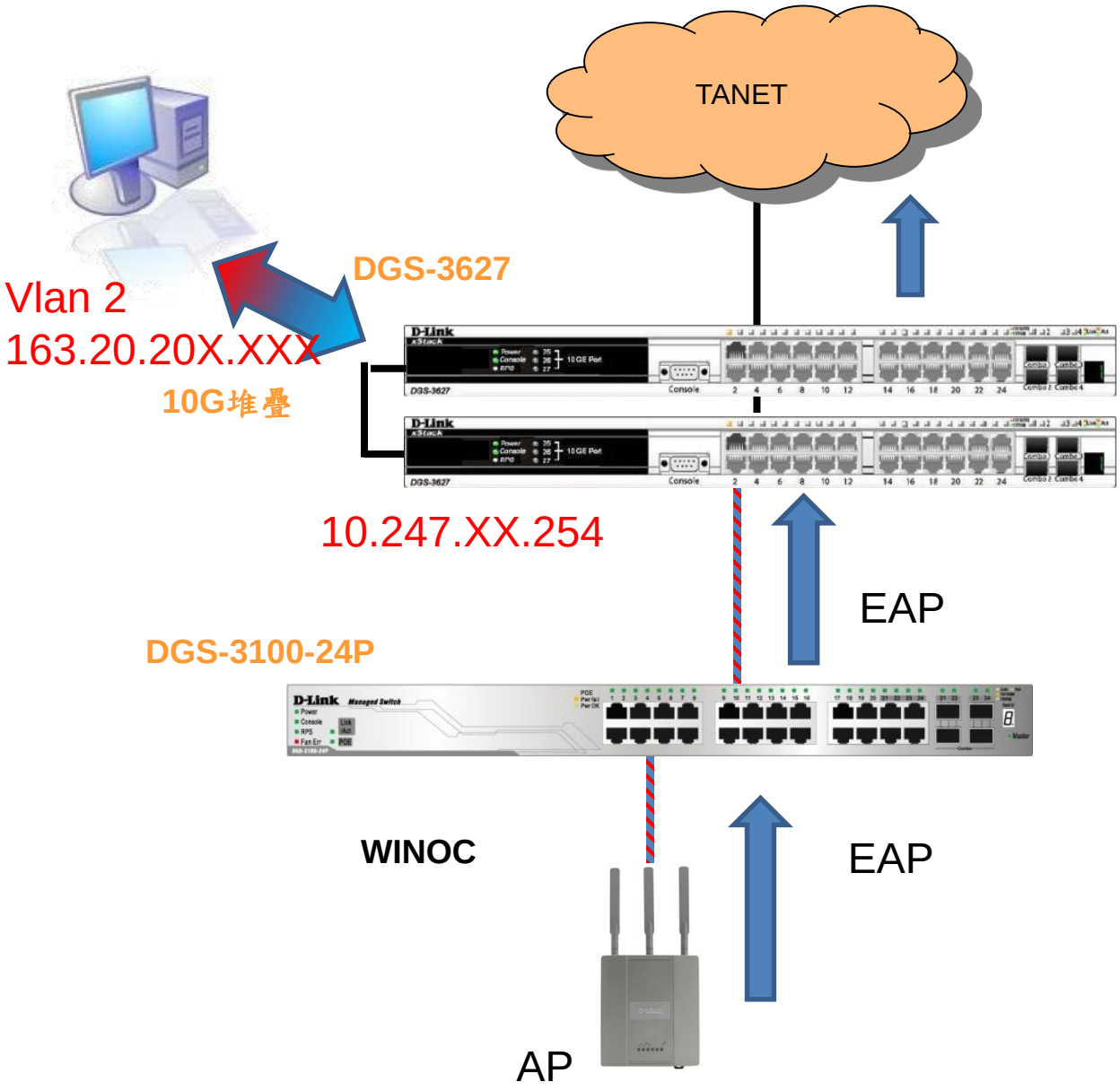
802.1x



EAP數據首先被封裝在EAPOL幀中，傳輸於申請者（Supplicant）和驗證者（Authenticator）之間。隨後又封裝在RADIUS或Diameter，傳輸於驗證者和驗證伺服器（Authentication server）之間。

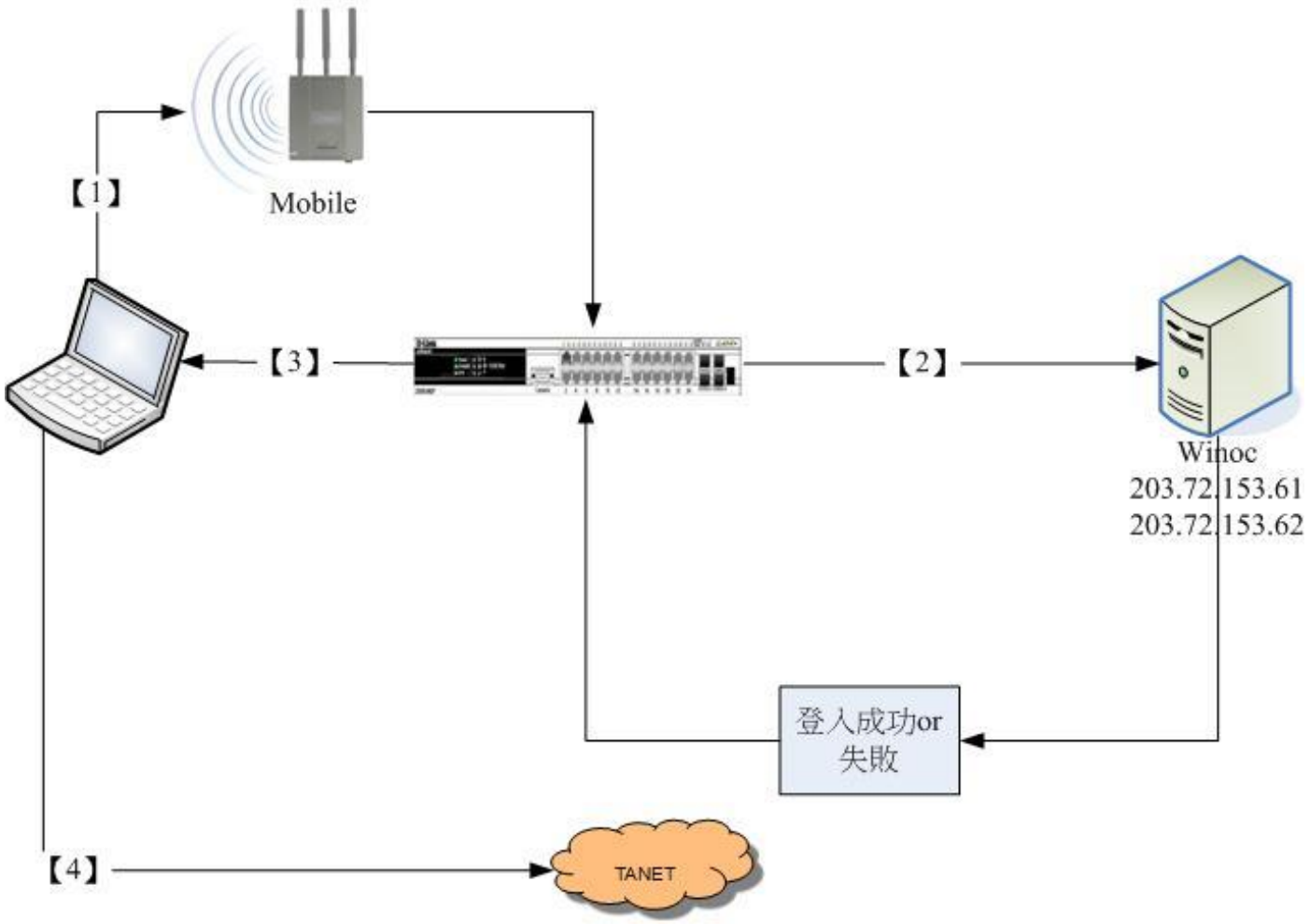
- 取自wiki

MAC認證架構圖


TANET
DGS-3627
Vlan 2
163.20.20X.XXX
10G堆疊
10.247.XX.254
EAP
DGS-3100-24P
WINOC
EAP
AP

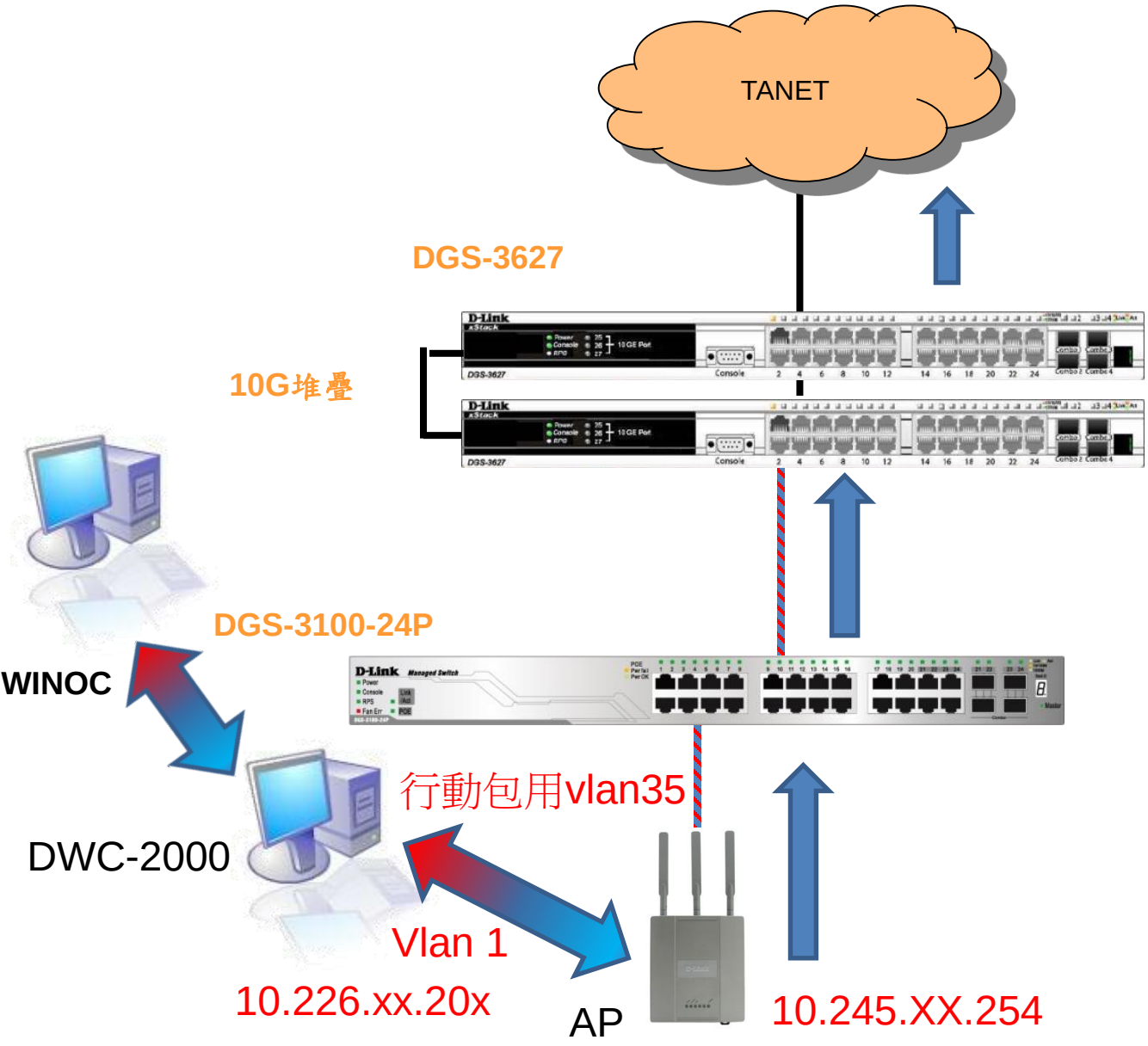
Winoc設定設備radius key

新北市無線網路Mobile架構圖

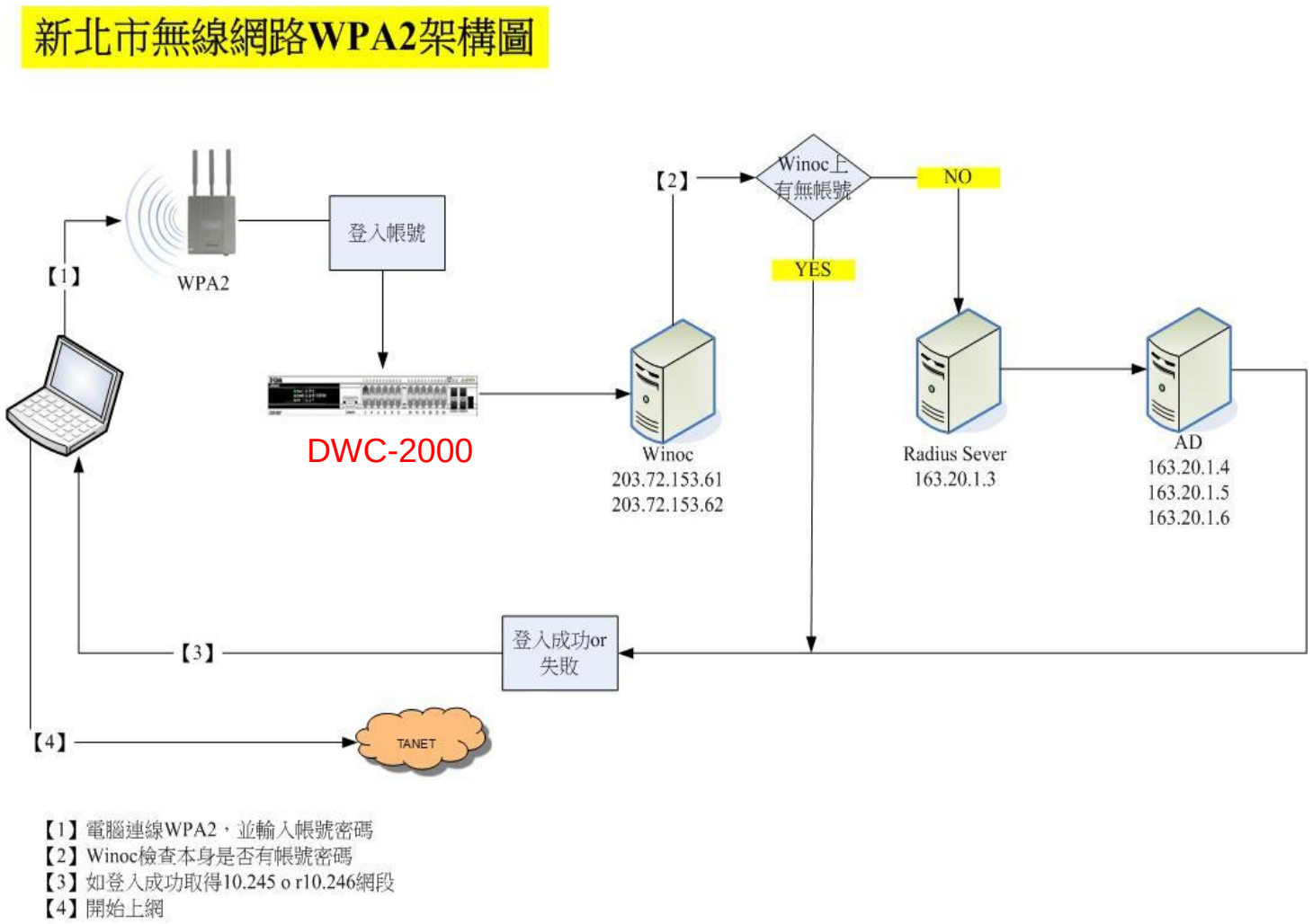


【1】電腦連線Mobile
【2】3627會送出電腦MAC及密碼0000
【3】如登入成功取得10.247 o r10.248網段
【4】開始上網

WPA2認證架構圖

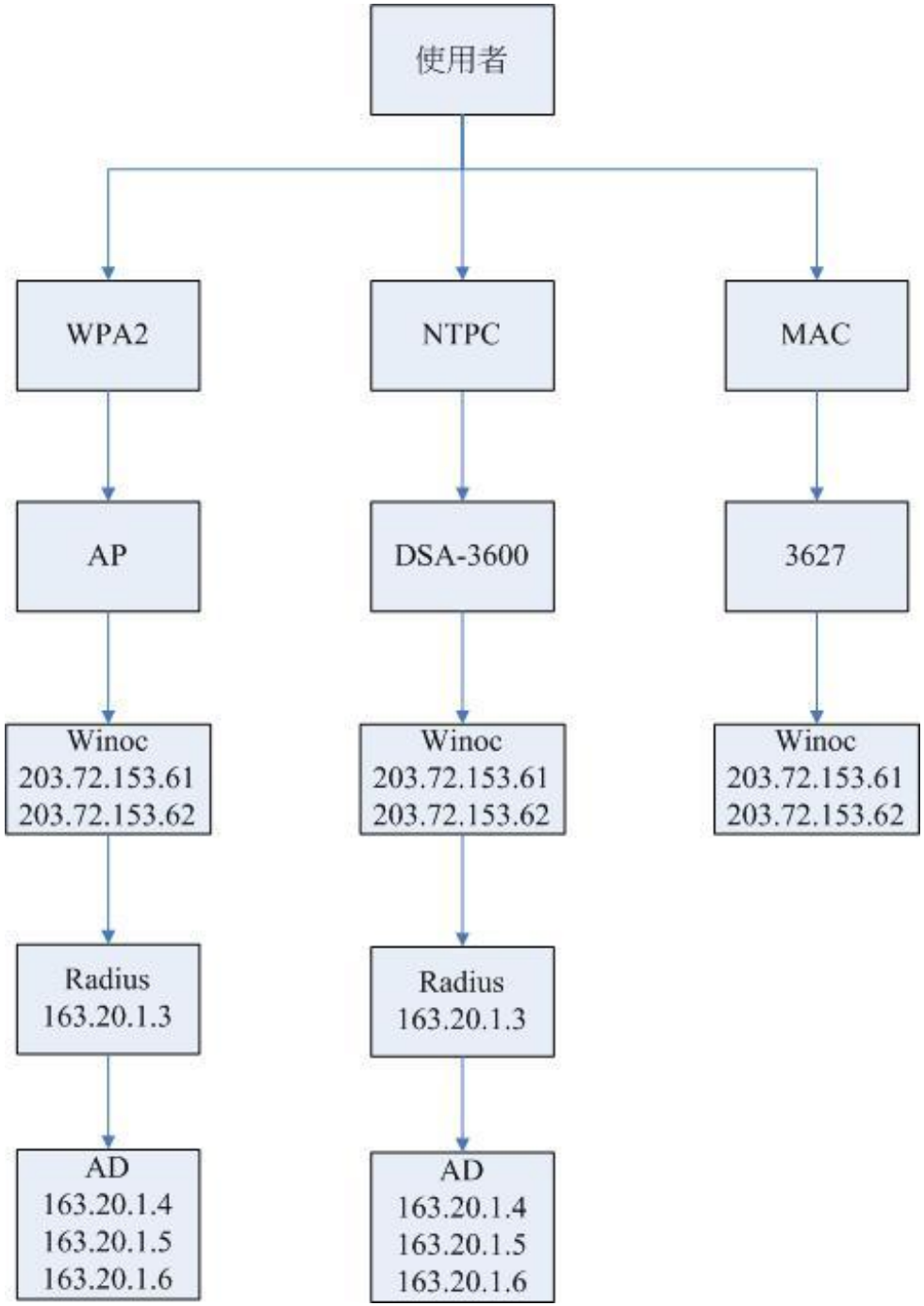

TANET
DGS-3627
10G堆疊
DGS-3100-24P
WINOC
DWC-2000
行動包用vlan35
Vlan 1
10.226.xx.20x
AP
10.245.XX.254

WPA2認證行為



【1】電腦連線WPA2，並輸入帳號密碼
【2】Winoc檢查本身是否有帳號密碼
【3】如登入成功取得10.245 o r10.246網段
【4】開始上網

Winoc設定設備radius key


使用者
WPA2
NTPC
MAC
AP
DSA-3600
3627
Winoc
203.72.153.61
203.72.153.62
Winoc
203.72.153.61
203.72.153.62
Winoc
203.72.153.61
203.72.153.62
Radius
163.20.1.3
Radius
163.20.1.3
AD
163.20.1.4
163.20.1.5
163.20.1.6
AD
163.20.1.4
163.20.1.5
163.20.1.6

AAA

- 認證(Authentication):Radius Server
- 授權(Authorization):FireWall
- 稽核(Audit)及報表功能:syslog
-

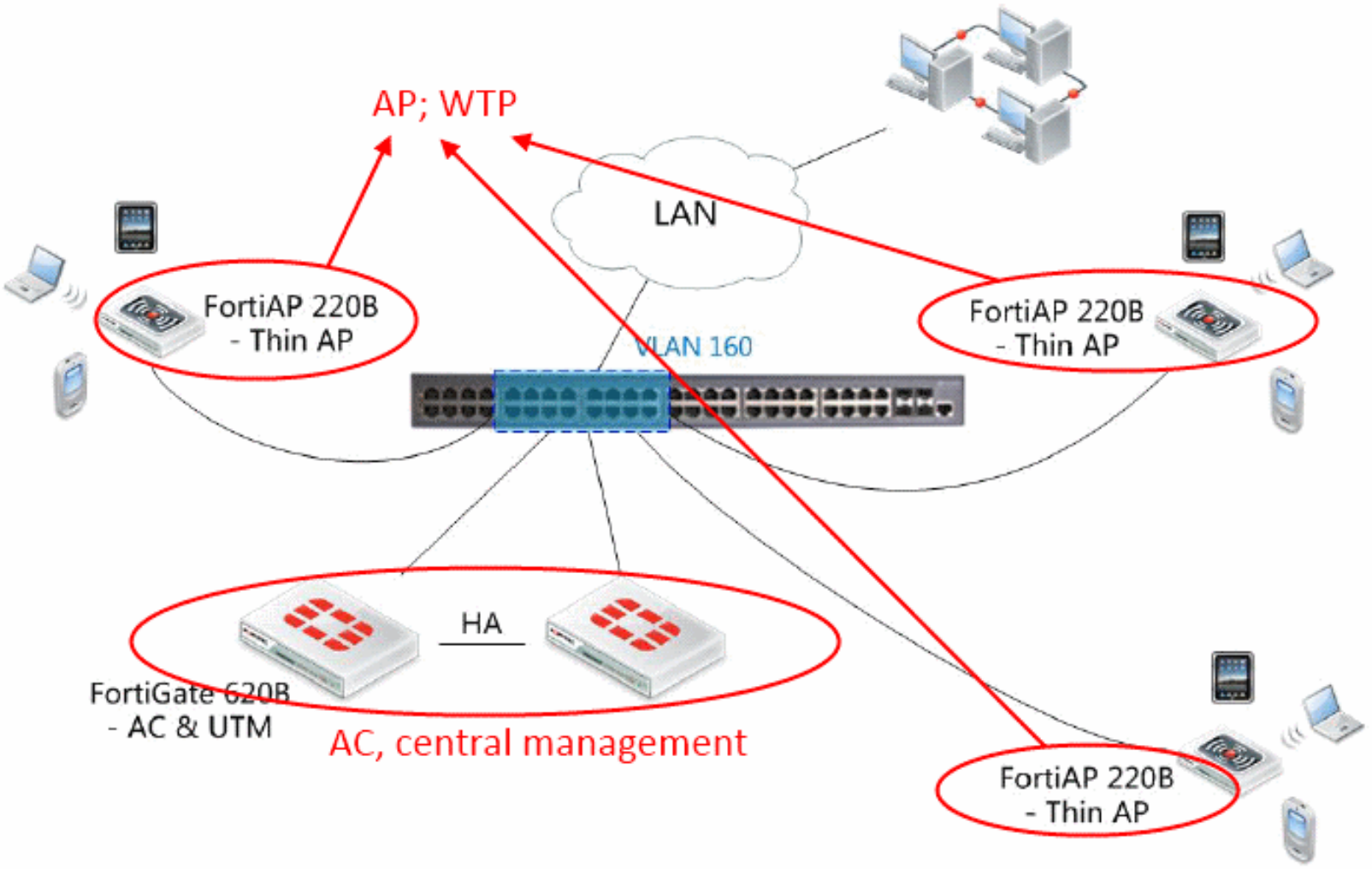
ThinAP啟動細部說明

- 什麼是Thin AP?
- CAPWAP是甚麼?
- Thin AP 啟動過程
- 啟動細部行為

Thin AP架構

- Thin AP的設計是遵循CAWAP(Control And Provisioning of Wireless Access Points)規範, 意味著AP本身的大多業務是交由上層AC來處理, CAWAP標準可以參考RFC-5415及RFC-5416文件:

Thin AP架構圖



引用自http://www.osslab.com.tw/Hardware/Router/FortiAP_220B(Zero-config)

- 透過CAWAP的實作, ThinAP架構規劃了兩種實體設備類型, 負責不同的業務操作: AP(WTP)和AC.
  1. AP: Access Point, 即無線收發端本身, 通常僅是單純對無線數據(wireless frames)的收發送操作, 又稱WTP(*).
  2. AC: Access Controller, 當AP傳送過來的數據, 將會轉交由AC單元進行處理, AC會乘載大多業務操作
- WTP: Wireless Termination Point

Thin AP 啟動過程及其行為

- AP 開啟取得AP ip
  - 可以設定固定ip or DHCP自動取得ip
- AP以AP ip 當Souce ip連接AC
  - 因此AP ip網段須能與AC互通(Routing要能到)
- AP由AC取得config啟動AP設備
- AC 給予AP config設定中包含
  - 2.4G and 5G 訊號頻道設定
  - SSID設定(包含網段、名稱、認證方式)
- AC本身擔任：
  - Route Mode GW portal認證
  - Bride Mode data traffice monitor工作

Thin AP架構細部文件參考

- IP不夠用處理方式，Client發B Class
- Firewall做NAT
- 設一個C做ip NAT Pool
- Policy管理存取權
- http://www.pcdvd.com.tw/showthread.php?t=984768

線路規格及施工規範

行動運用拓譜討論

SNGN校園無線網路簡介

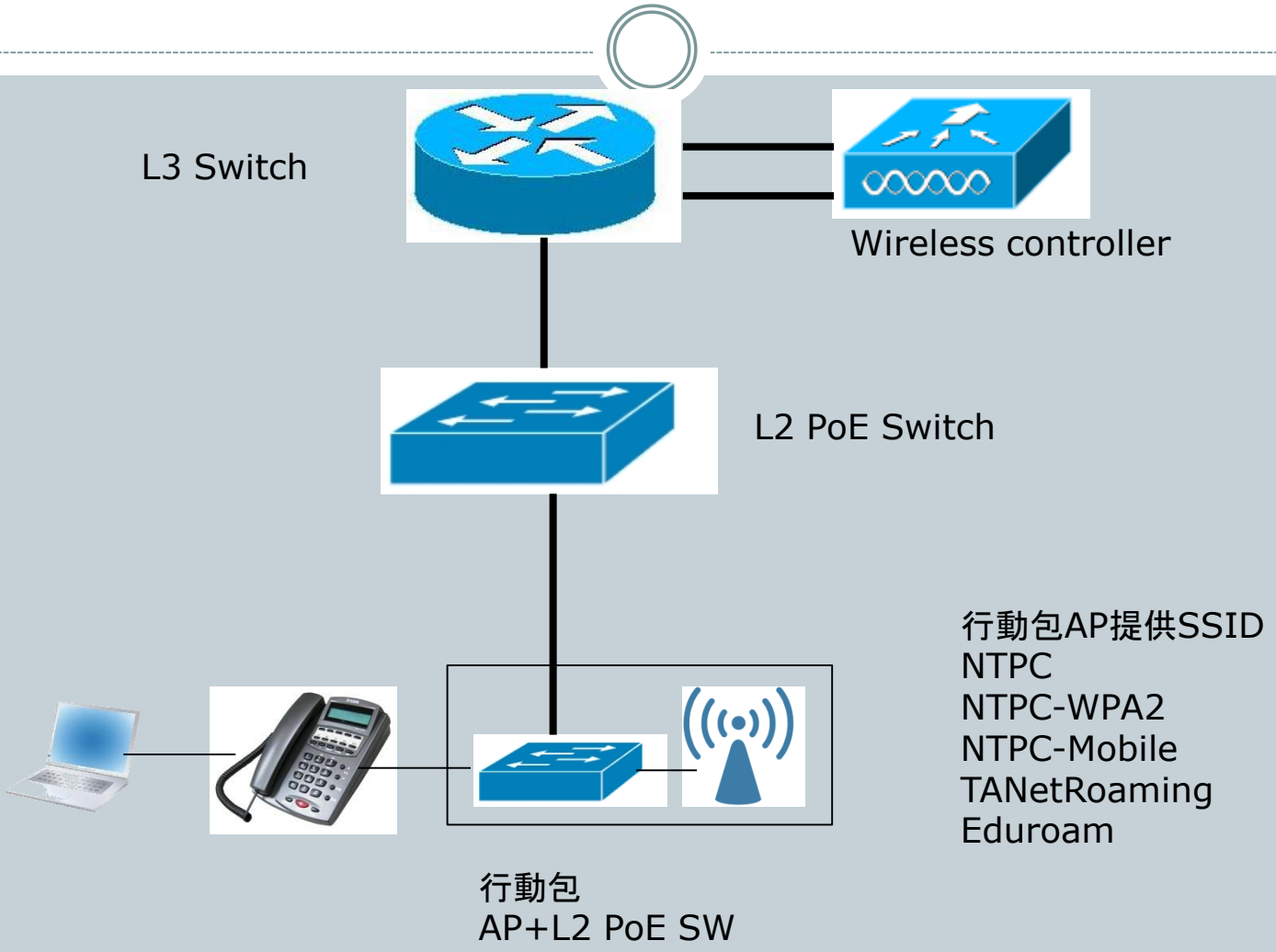
行動包Thin AP架構

無線網路控制器設計

- 無線網路控制器透過vlan 8與 Dlink 3620做routing
- AP取得config Source ip
  - 固定式走Vlan1
  - 行動包走Vlan35
- SSID NTPC GateWay在無線網路控制器
- SSID NTPC-Mobile GateWay在Dlink 3620
- SSID NTPC-WPA2 GateWay在Dlink 3620

- Data traffice 僅NTPC走無線網路控制器
- 無線網路控制器收集所有無線訊號log

行動包Thin 架構

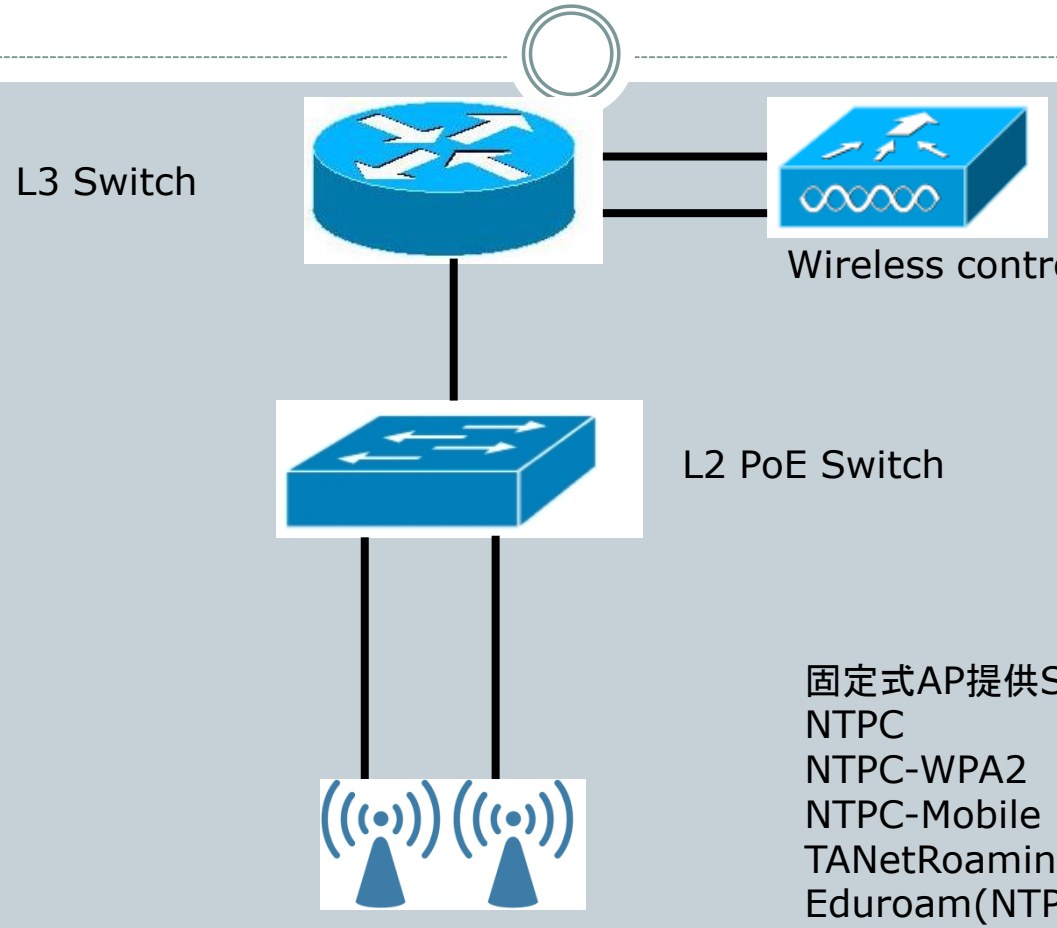

L3 Switch
Wireless controller
L2 PoE Switch
行動包AP提供SSID
NTPC
NTPC-WPA2
NTPC-Mobile
TANetRoaming
Eduroam
行動包
AP+L2 PoE SW

行動包架構說明

- 行動包無線AP透過行動包內的PoE switch供電
- 行動包的PoE Switch可以任意接上L2 PoE Switch的Port上,AP可以透過Vlan 35(WPA2)自動連回無線控制器上取得config及更新資訊!
- 行動包如果使用話機的網點,將可將話機接上PoE switch,後端電腦接於話機上,依然可以正常使用
- 行動包AP須提供5組SSID提供後端
  NTPC(WEB認證)
  NTPC-WPA2
  NTPC-Mobile
  TANetRoaming(NTPC)
  Eduroam(NTPC-WPA2)

固定式Thin AP架構

固定式Thin AP架構

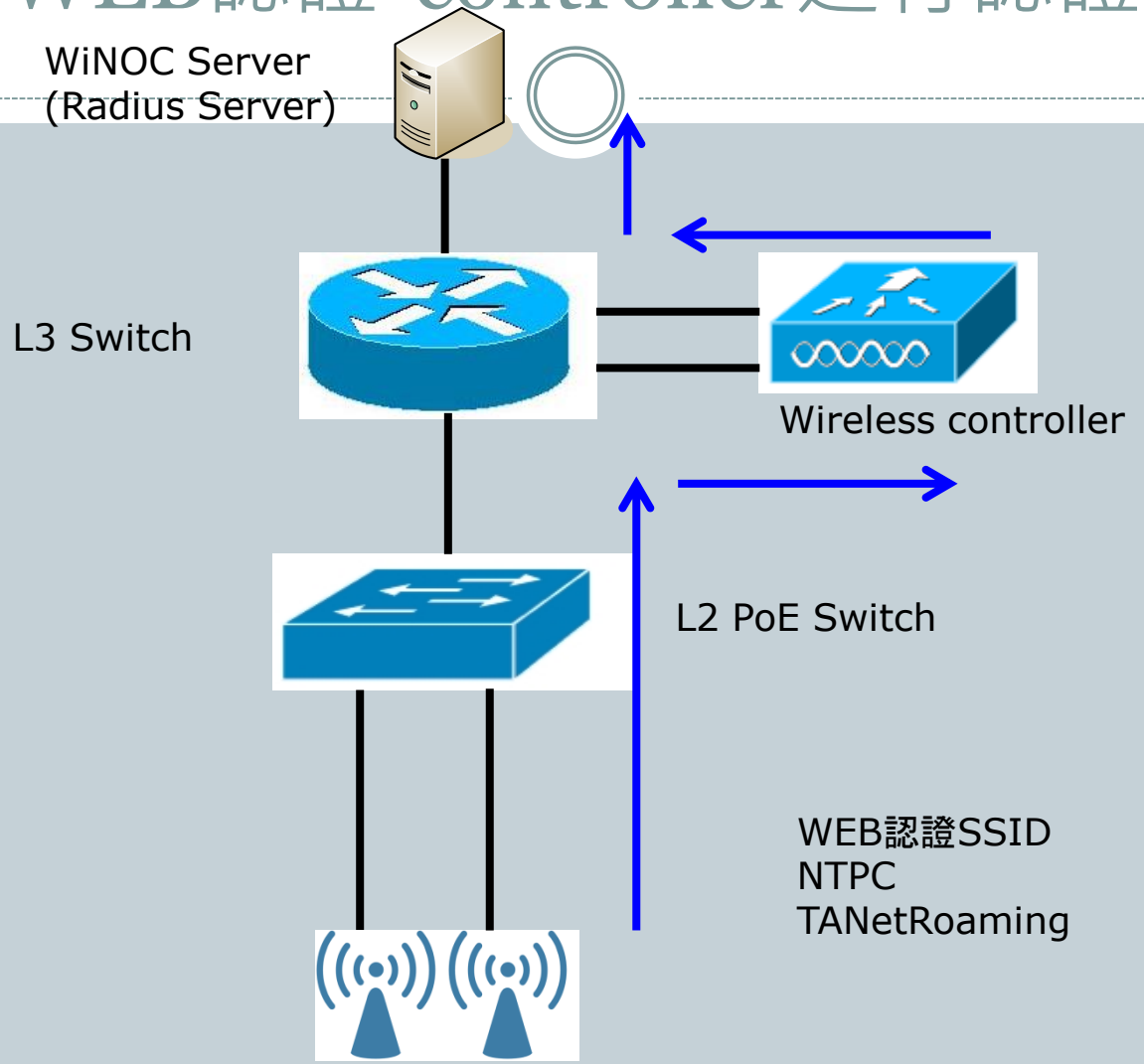


固定式AP提供SSID
NTPC
NTPC-WPA2
NTPC-Mobile
TANetRoaming(NTPC)
Eduroam(NTPC-WPA2)

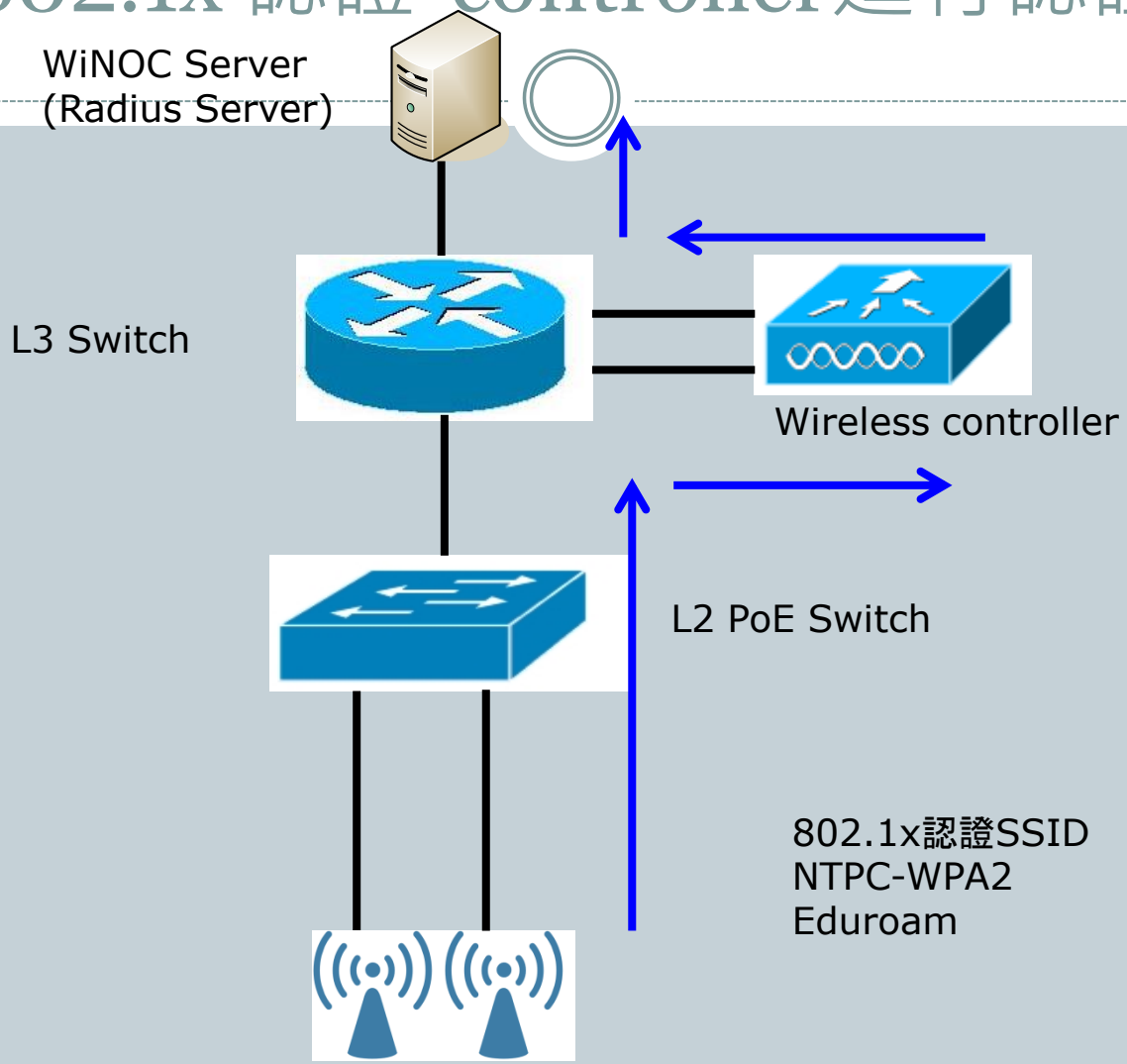
固定式架構說明

- 固定式無線AP透過L2 PoE switch供電
- 行動包的PoE Switch可以任意接上L2 PoE Switch的Port上,AP可以透過Vlan 1(Vlan MGT)自動連回無線控制器上取得config及更新資訊!
- 固定式無線AP建立5組SSID
  NTPC(WEB認證)
  NTPC-WPA2
  NTPC-Mobile
  TANetRoaming(NTPC)
  Eduroam(NTPC-WPA2)
- 固定式無線AP由無線網路控制器進行控管,可統一配發設定資料與韌體升級等

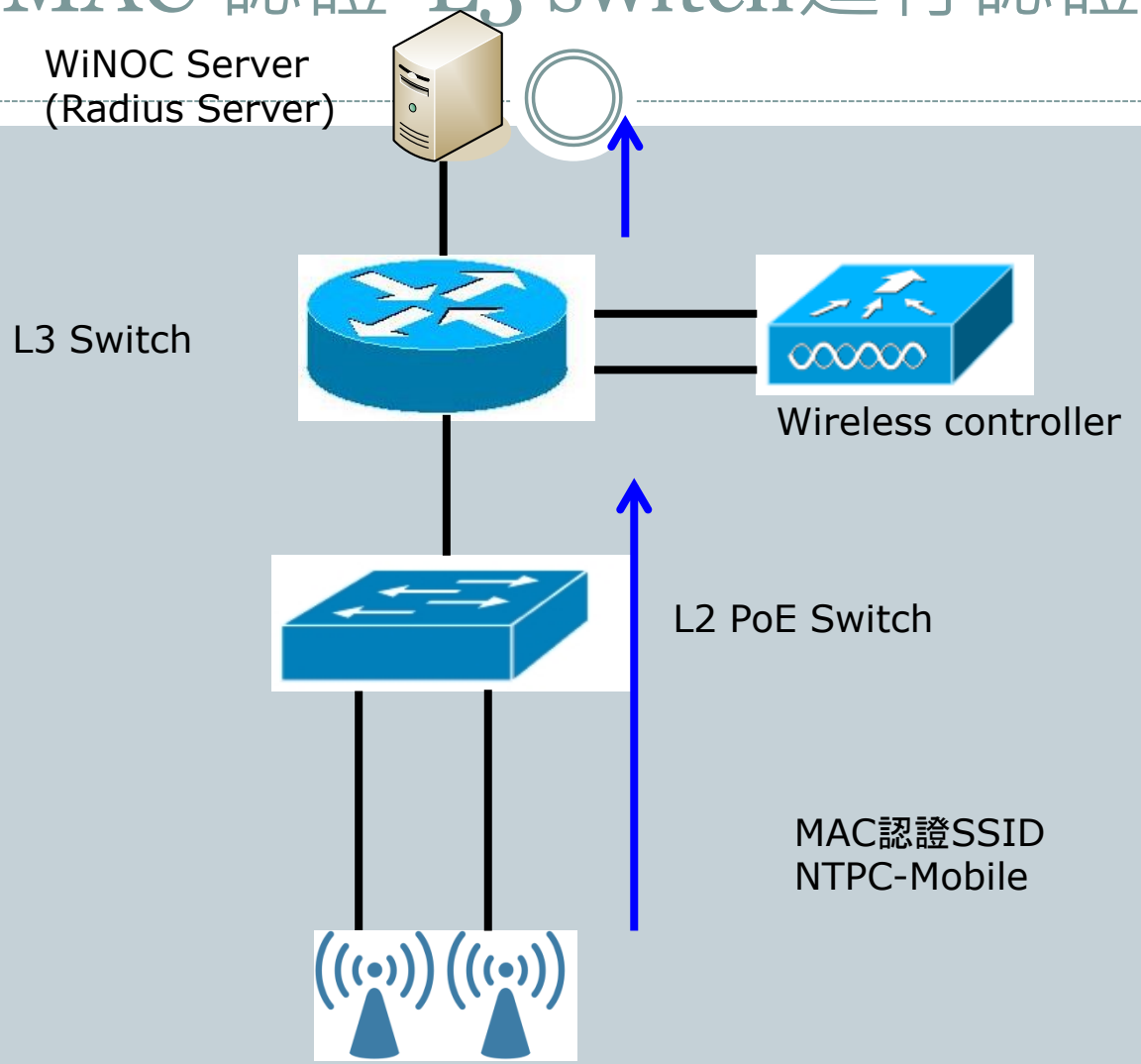
WEB認證-controller進行認證



802.1x 認證-controller進行認證



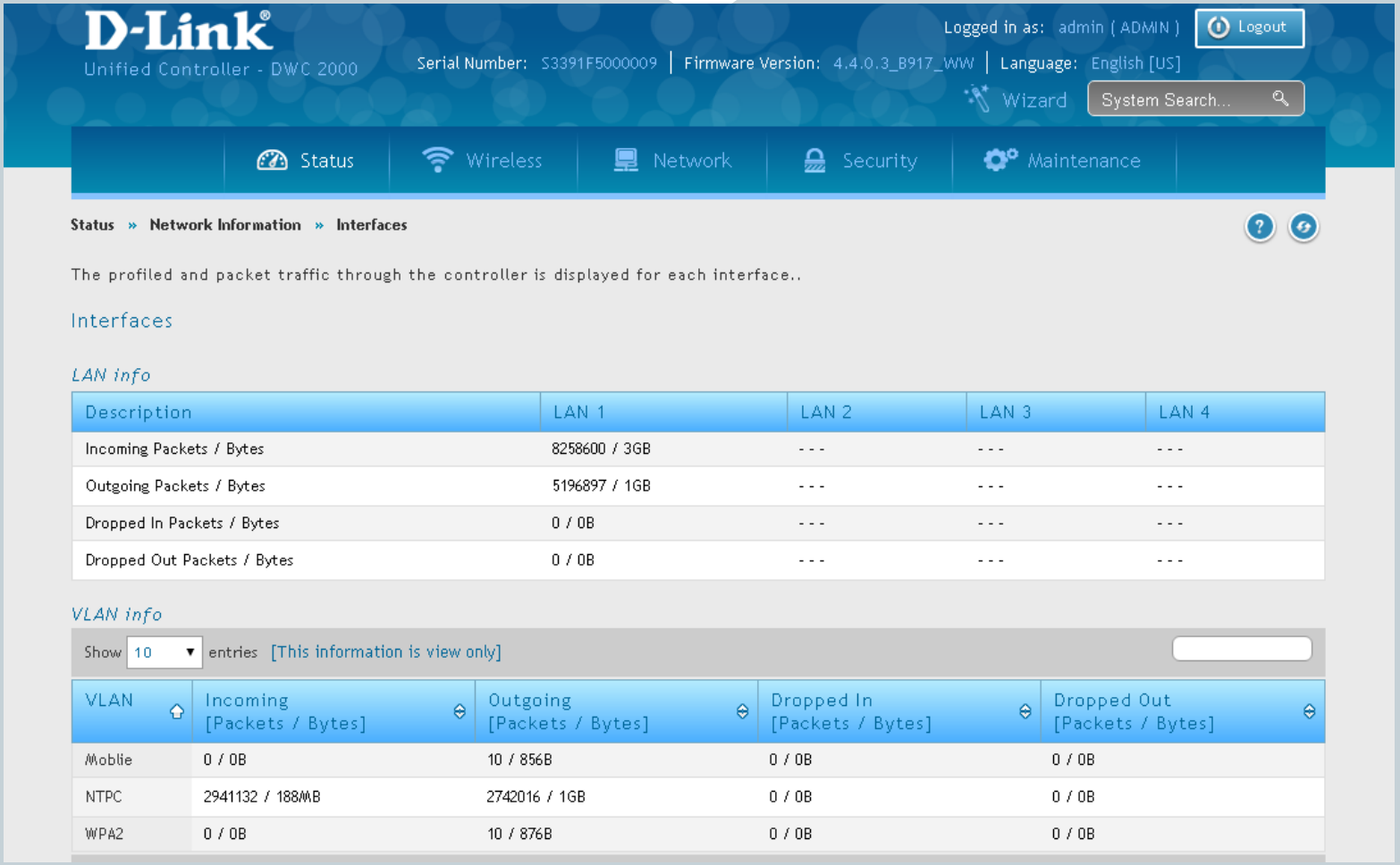
MAC 認證-L3 switch進行認證

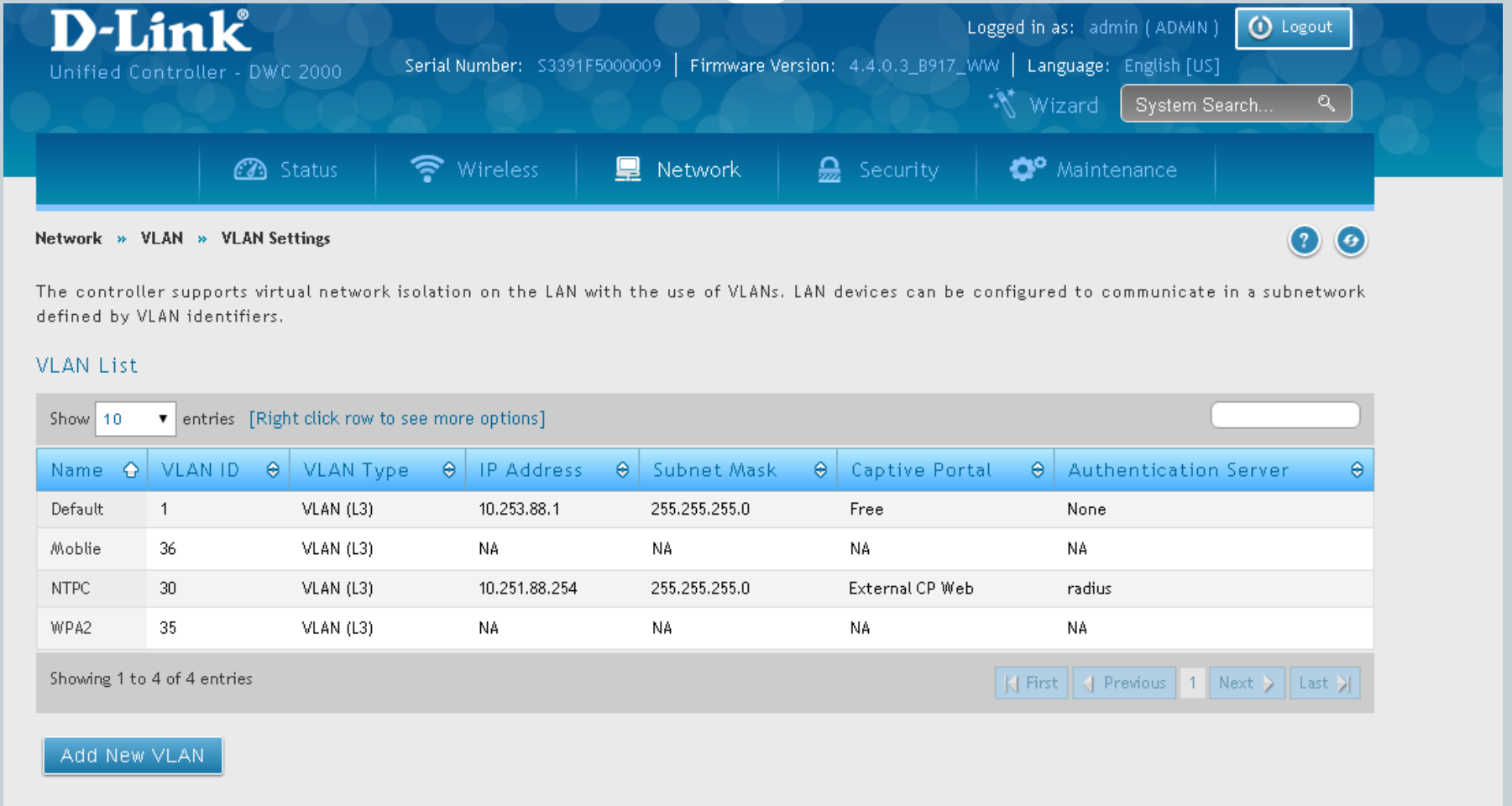


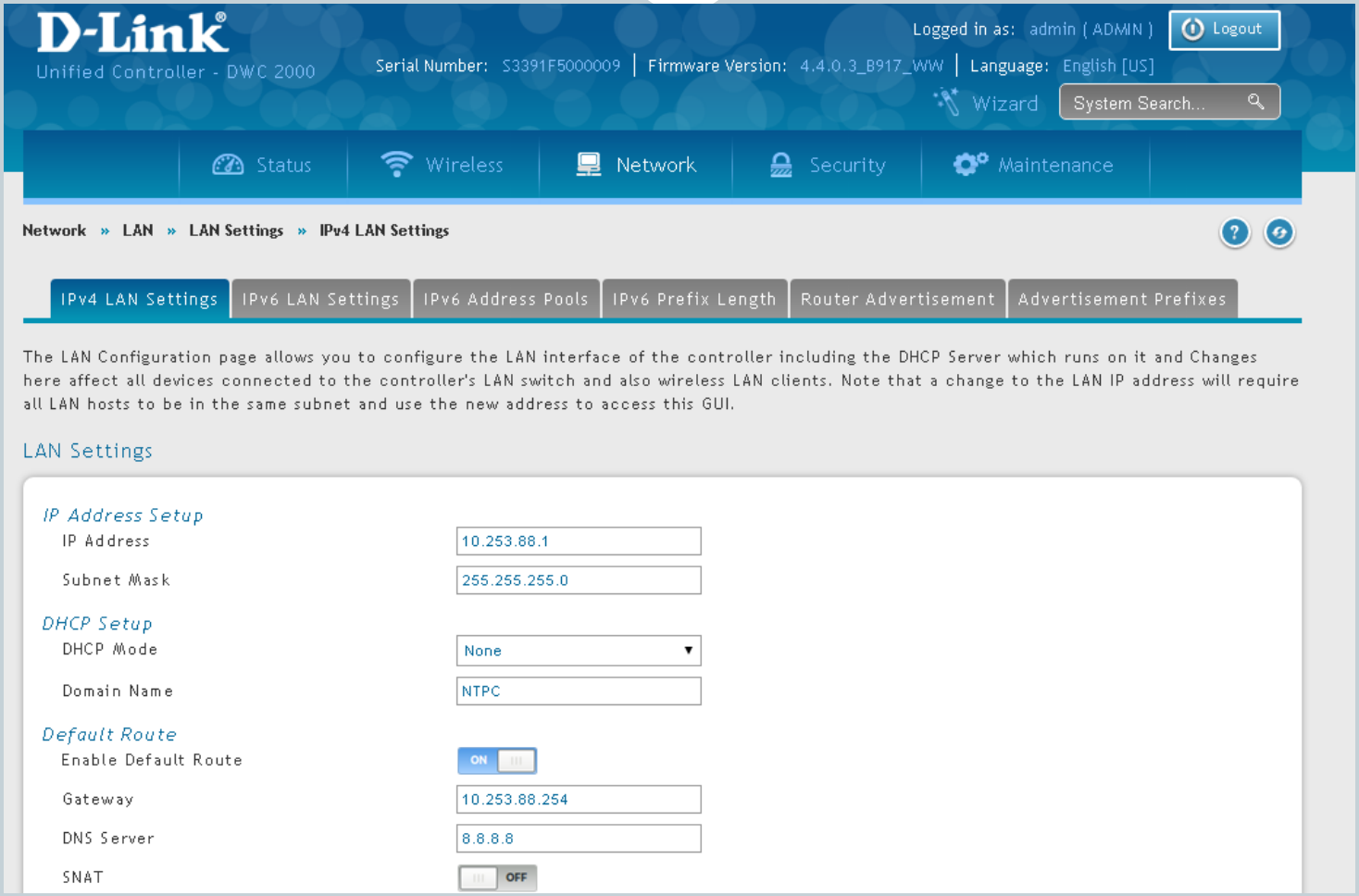
Thin AP controller設定及做法

- 將Linksys 的Lan接到需派發ip的 L2 vlan 該Vlan即可取得該vlan網段ip
- 將WPA2及Mobile GW設在 L3 switch
- NTPC GW設在 AC controller
- 將AC controller與L3 switch間設定vlan8 ，並將 vlan 30 路由透過vlan8送到L3 switch
- L3 switch將vlan30網段 route送至AC的vlan8 wan interface 即可完成路由設定。

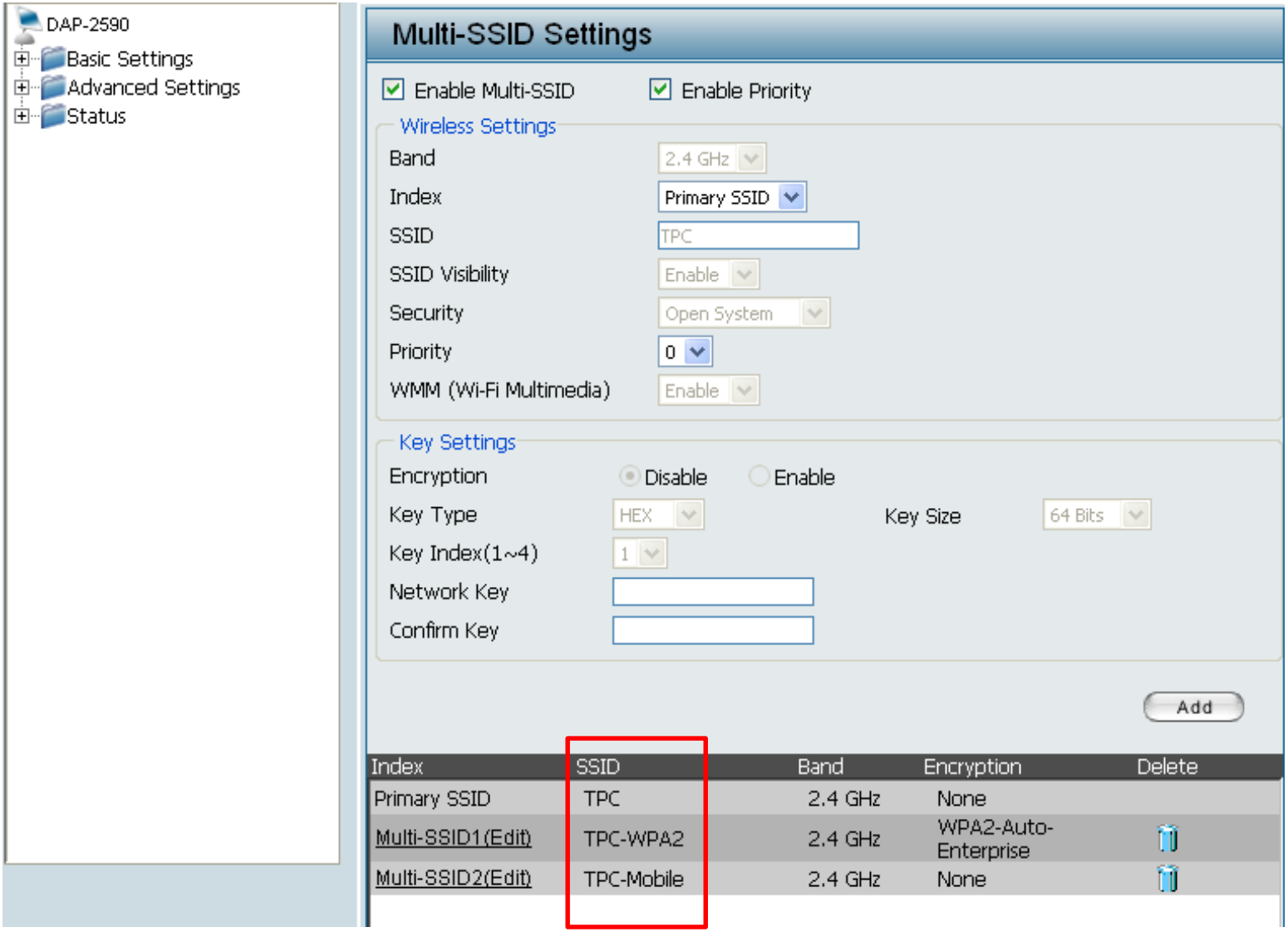
AC Controller interface vlan設定



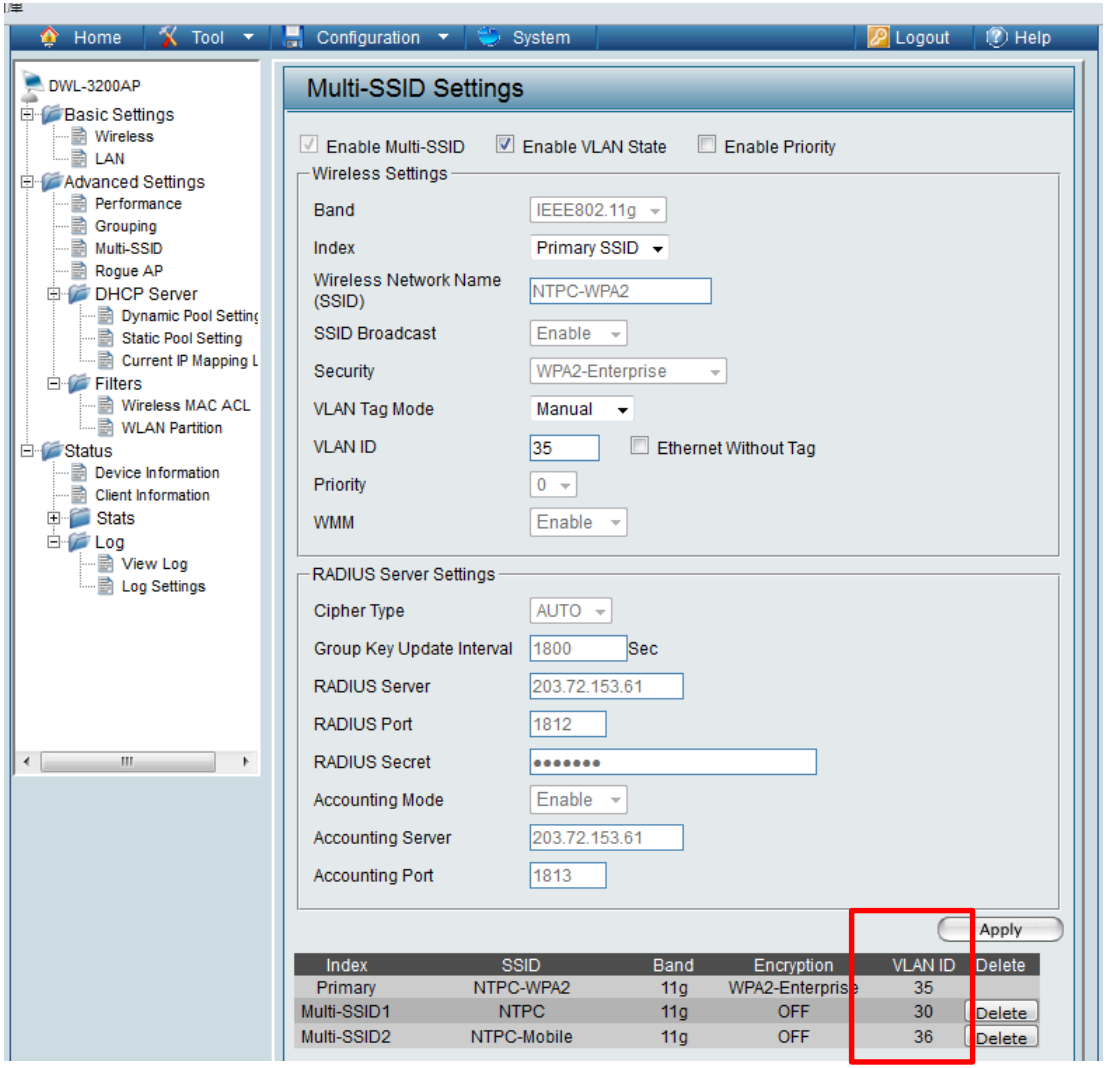

D-Link
Unified Controller - DWC 2000
Logged in as: admin (ADMIN)
Logout
Serial Number: S3391F5000009
Firmware Version: 4.4.0.3_B917_WW
Language: English [US]
Wizard
System Search...
Status
Wireless
Network
Security
Maintenance
Network » VLAN » VLAN Settings
The controller supports virtual network isolation on the LAN with the use of VLANs. LAN devices can be configured to communicate in a subnetwork defined by VLAN identifiers.
VLAN List
Show 10 entries [Right click row to see more options]
Name
VLAN ID
VLAN Type
IP Address
Subnet Mask
Captive Portal
Authentication Server
Default 1 VLAN (L3) 10.253.88.1 255.255.255.0 Free None
Moblie 36 VLAN (L3) NA NA NA NA
NTPC 30 VLAN (L3) 10.251.88.254 255.255.255.0 External CP Web radius
WPA2 35 VLAN (L3) NA NA NA NA
Showing 1 to 4 of 4 entries
First
Previous
1
Next
Last
Add New VLAN


D-Link
Unified Controller - DWC 2000
Logged in as: admin (ADMIN)
Logout
Serial Number: S3391F5000009
Firmware Version: 4.4.0.3_B917_WW
Language: English [US]
Wizard
System Search...
Status
Wireless
Network
Security
Maintenance
Network » LAN » LAN Settings » IPv4 LAN Settings
IPv4 LAN Settings
IPv6 LAN Settings
IPv6 Address Pools
IPv6 Prefix Length
Router Advertisement
Advertisement Prefixes
The LAN Configuration page allows you to configure the LAN interface of the controller including the DHCP Server which runs on it and Changes here affect all devices connected to the controller's LAN switch and also wireless LAN clients. Note that a change to the LAN IP address will require all LAN hosts to be in the same subnet and use the new address to access this GUI.
LAN Settings
IP Address Setup
IP Address
10.253.88.1
Subnet Mask
255.255.255.0
DHCP Setup
DHCP Mode
None
Domain Name
NTPC
Default Route
Enable Default Route
ON
Gateway
10.253.88.254
DNS Server
8.8.8.8
SNAT
OFF

Fat AP上SSID狀態

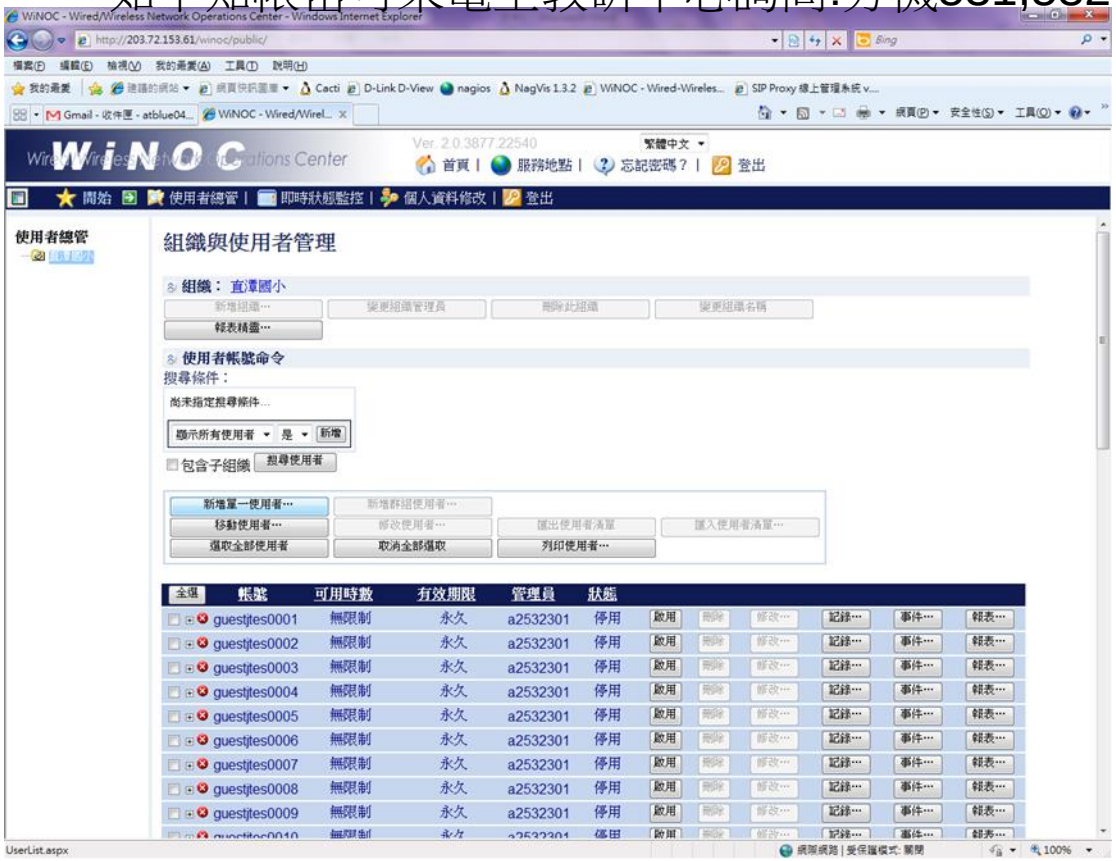


Fat AP Vlan設定



Winoc教學 ntpc-Mobile

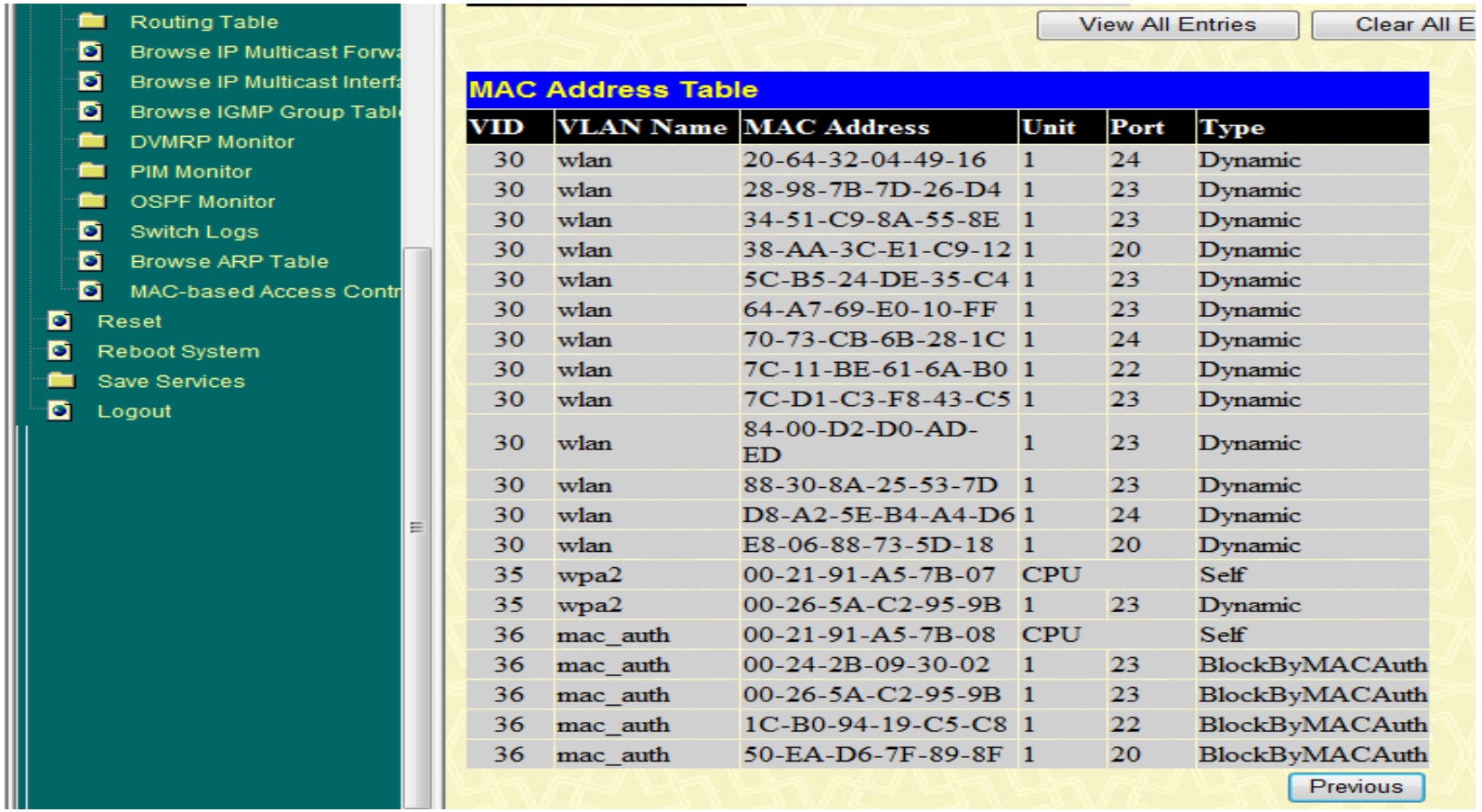
如不知帳密可來電至教研中心詢問:分機531,532



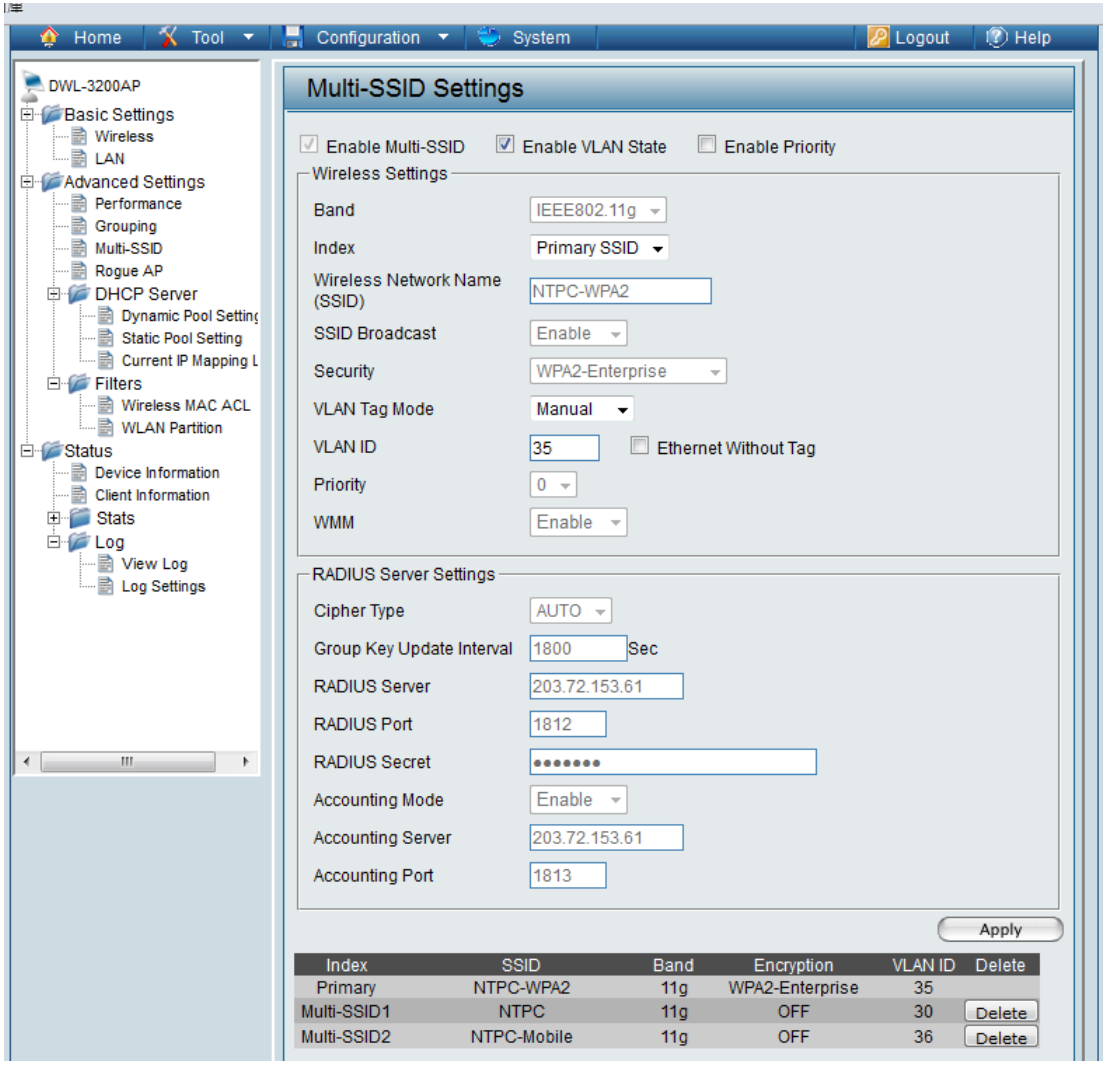

WiNOC - Wired/Wireless Network Operations Center - Windows Internet Explorer
http://203.72.153.61/winoc/public/
WiNOC
Ver. 2.0.3877.22540
繁體中文
首頁 | 服務地點 | 忘記密碼？ | 登出
開始 使用者總管 | 即時狀態監控 | 個人資料修改 | 登出
使用者總管
直潭國小
新增單一使用者
姓名：
張小棠
帳號：
00251167953F
密碼：
狀態：
啟用 停用
可用時數：
無限制
10小時 20小時 30小時 40小時 50小時
分鐘
有效期限：
無限制
當天 1天後 1週後 1個月後
天後 週後 個月後
到 年 月 日
類型：
MAC
電子郵件：
電話號碼：
備註：
頻寬(下載/上傳)：
無限制
無限制
確認
取消
AddUser.aspx
網際網路 | 受保護模式: 關閉
100%

Ntpc-Mobile 除錯ARP Table

L3透過Winoc做認證,由L3決定是否放行unBlockByMACAuth



Fat Ntpc-WPA2 Debug

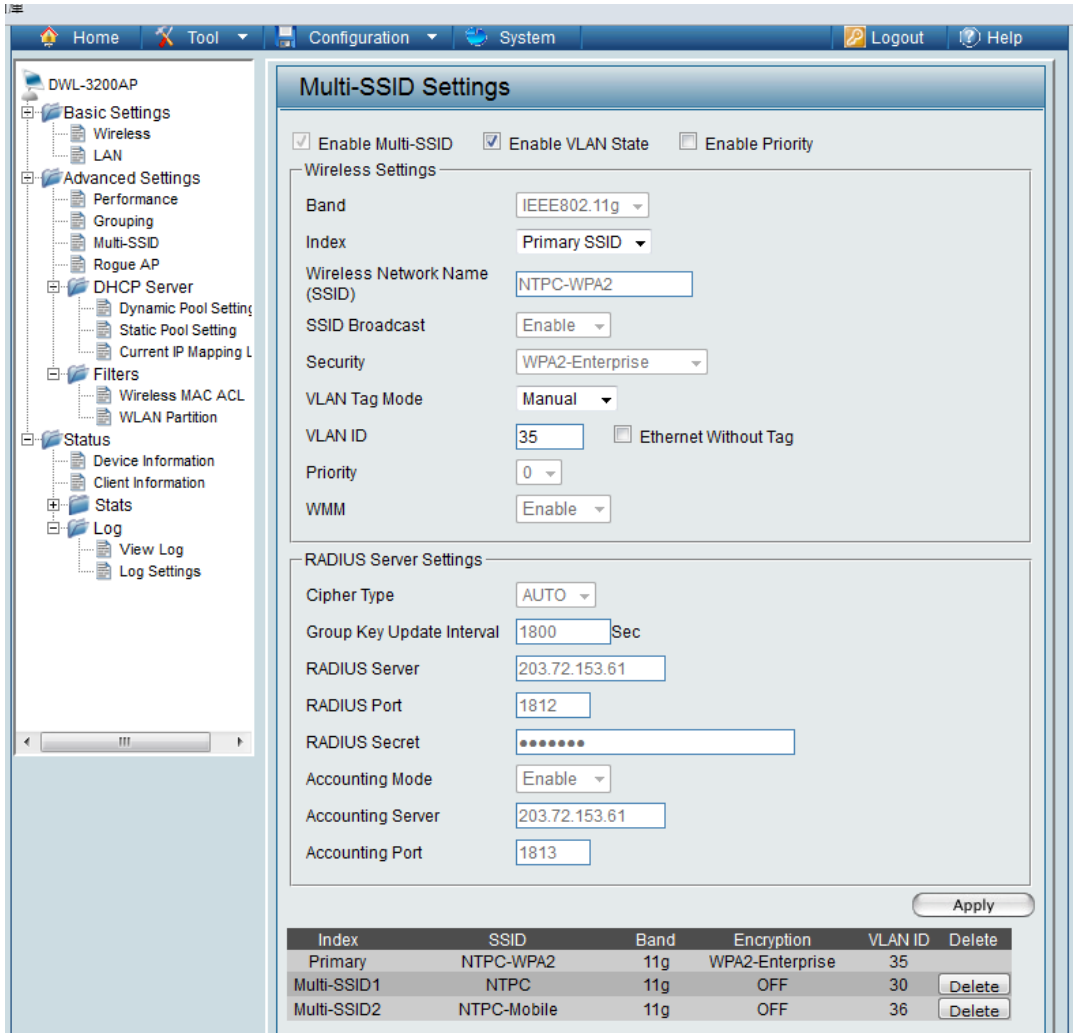


各校AP IP配置

- 10.226.x.201-205

or

- 10.227.x.201-205



Routing Table

Add

IPv4 Static/Default Route Settings

IP Address	Subnet Mask	Gateway	Metric	Protocol	Backup	Weight	Status	Delete
0.0.0.0	0.0.0.0	163.20.209.182	1	Default	Primary	None	Active	
10.252.29.0	255.255.255.0	10.254.29.1	1	Static	Primary	None	Active	

Total Entries: 2

監控除錯

提供設備項目 - L2 POE交換器

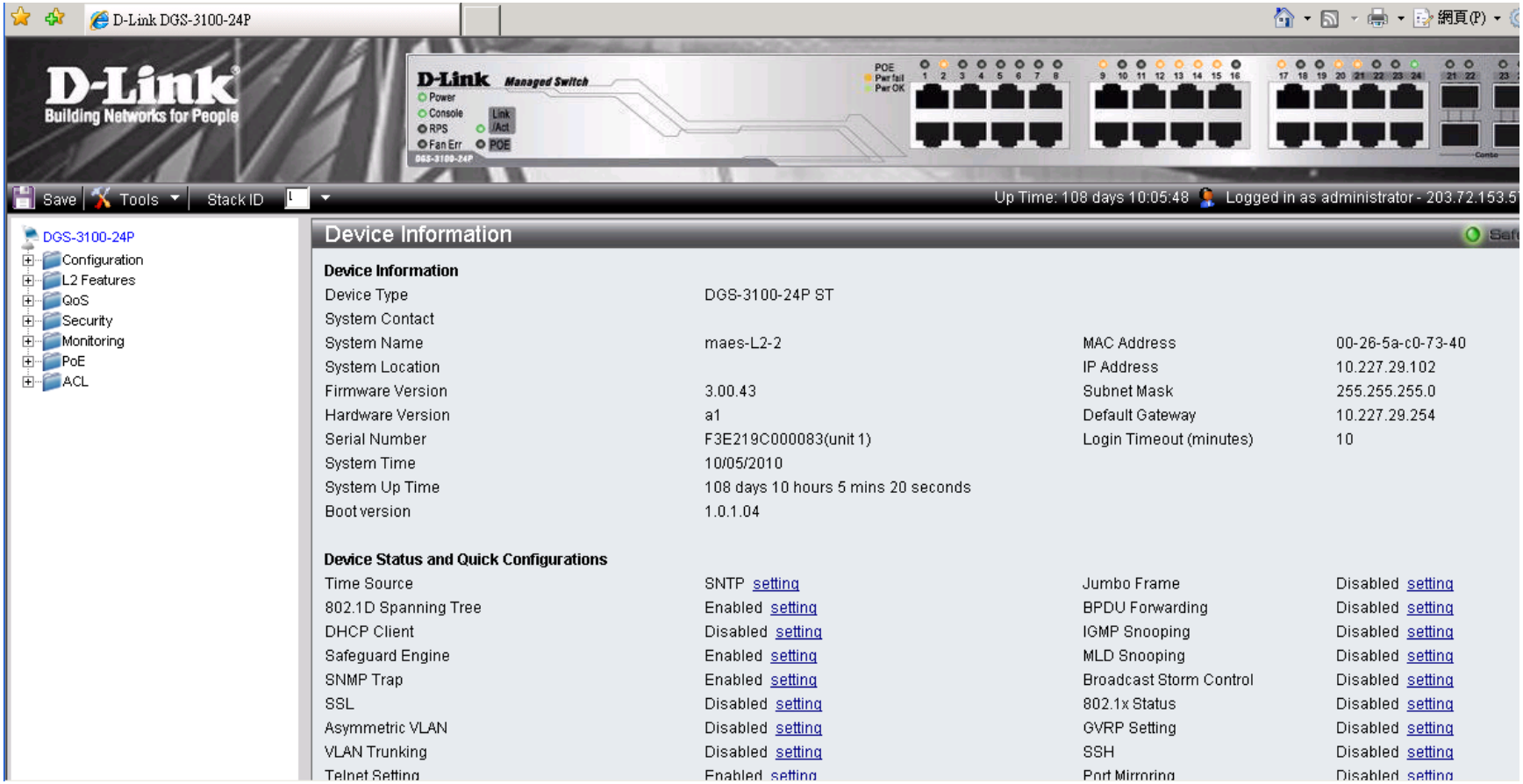
L2 POE交換器

DGS-3100-24P/48P

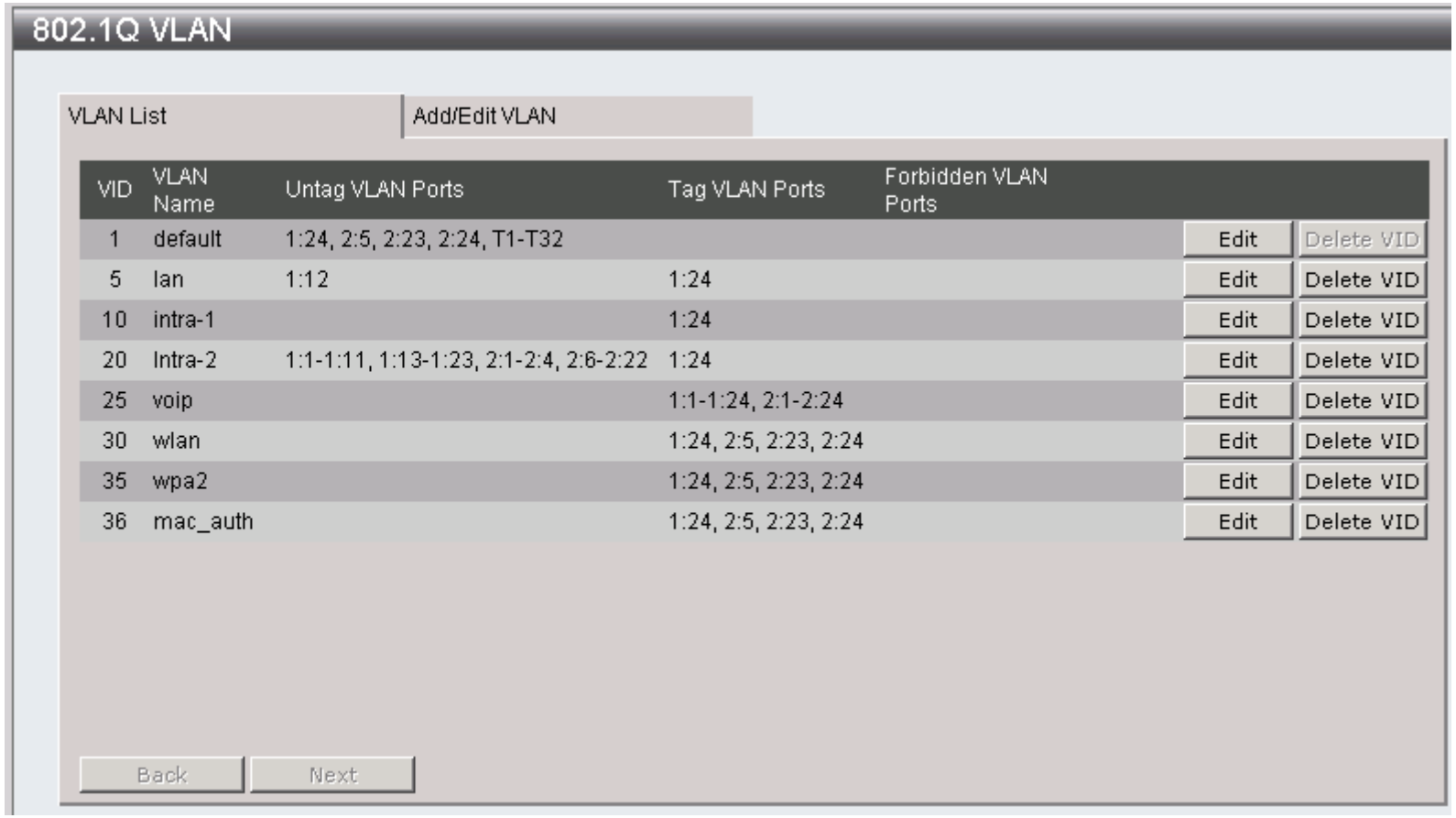
- 提供高擴充性
  - 提供實體堆疊功能
- 整合多元化網路應用
  - 提供IPv6 MLD Snooping、QoS及ACL機制
- 提供穩定安全網路連線
  - 實測每埠皆滿足網路電話及無線基地台所需電力
- 節能減碳
  - 搭配WiNOC排程功能可自動開啟或關閉POE無線基地台或POE網路電話，以節省電費

L2基礎操作及簡易故障排除

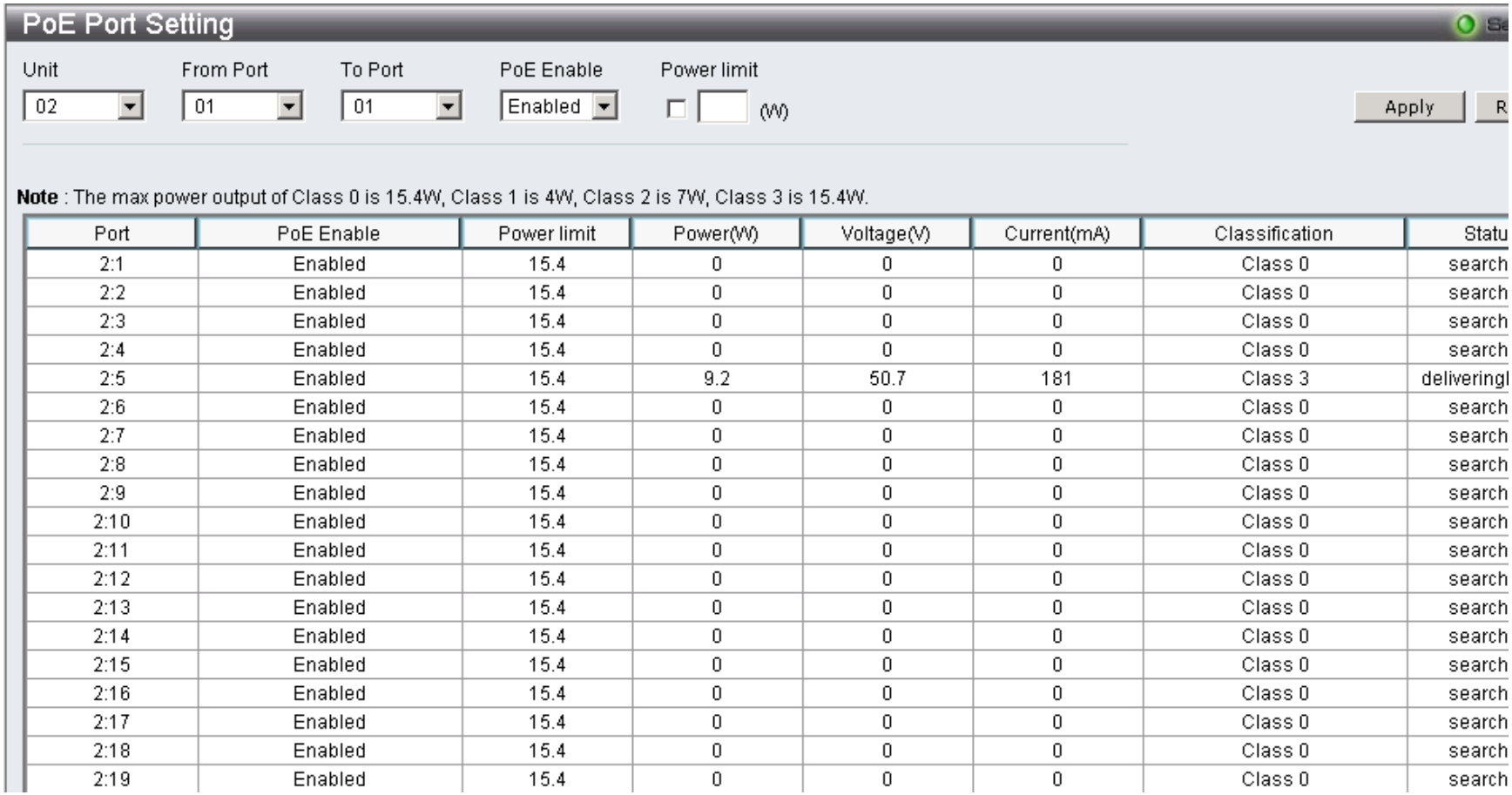
設備狀態


D-Link DGS-3100-24P
網頁(P)
D-Link
Building Networks for People
D-Link Managed Switch
Power
Console
RPS
Fan Err
Link /Act
POE
Save
Tools
Stack ID
Up Time: 108 days 10:05:48
Logged in as administrator - 203.72.153.5
DGS-3100-24P
Configuration
L2 Features
QoS
Security
Monitoring
PoE
ACL
Device Information
Device Information
Device Type DGS-3100-24P ST
System Contact
System Name maes-L2-2
System Location
Firmware Version 3.00.43
Hardware Version a1
Serial Number F3E219C000083(unit 1)
System Time 10/05/2010
System Up Time 108 days 10 hours 5 mins 20 seconds
Boot version 1.0.1.04
MAC Address 00-26-5a-c0-73-40
IP Address 10.227.29.102
Subnet Mask 255.255.255.0
Default Gateway 10.227.29.254
Login Timeout (minutes) 10
Device Status and Quick Configurations
Time Source SNTP setting
802.1D Spanning Tree Enabled setting
DHCP Client Disabled setting
Safeguard Engine Enabled setting
SNMP Trap Enabled setting
SSL Disabled setting
Asymmetric VLAN Disabled setting
VLAN Trunking Disabled setting
Telnet Setting Enabled setting
Jumbo Frame Disabled setting
BPDU Forwarding Disabled setting
IGMP Snooping Disabled setting
MLD Snooping Disabled setting
Broadcast Storm Control Disabled setting
802.1x Status Disabled setting
GVRP Setting Disabled setting
SSH Disabled setting
Port Mirroring Disabled setting

Vlan資訊


802.1Q VLAN
VLAN List
Add/Edit VLAN
VID
VLAN Name
Untag VLAN Ports
Tag VLAN Ports
Forbidden VLAN Ports
1 default 1:24, 2:5, 2:23, 2:24, T1-T32 Edit Delete VID
5 lan 1:12 1:24 Edit Delete VID
10 intra-1 1:24 Edit Delete VID
20 Intra-2 1:1-1:11, 1:13-1:23, 2:1-2:4, 2:6-2:22 1:24 Edit Delete VID
25 voip 1:1-1:24, 2:1-2:24 Edit Delete VID
30 wlan 1:24, 2:5, 2:23, 2:24 Edit Delete VID
35 wpa2 1:24, 2:5, 2:23, 2:24 Edit Delete VID
36 mac_auth 1:24, 2:5, 2:23, 2:24 Edit Delete VID
Back
Next

PoE資訊



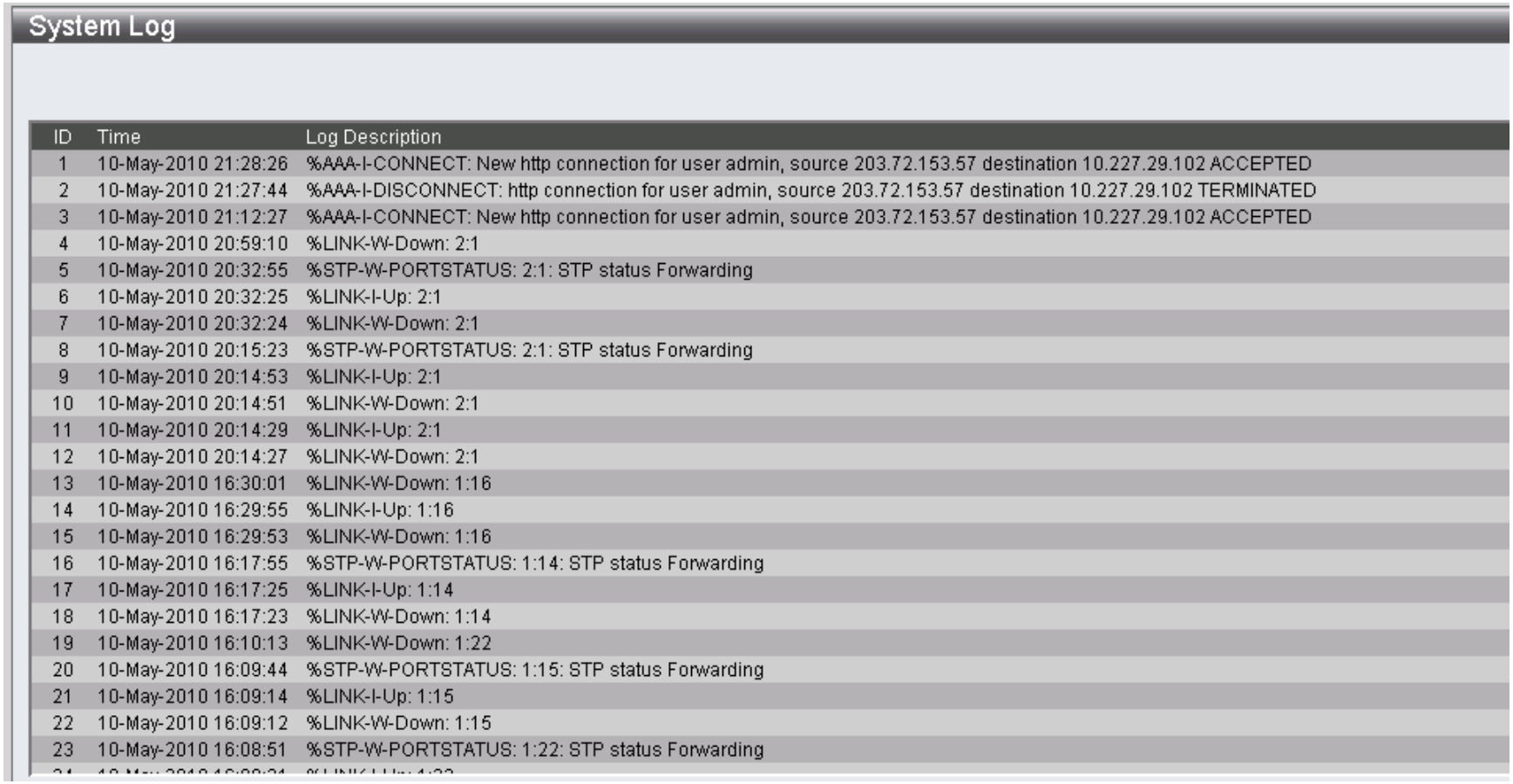
PoE Port Setting

Unit: 02 | From Port: 01 | To Port: 01 | PoE Enable: Enabled | Power limit: (W) | Apply

Note : The max power output of Class 0 is 15.4W, Class 1 is 4W, Class 2 is 7W, Class 3 is 15.4W.

Port	PoE Enable	Power limit	Power(W)	Voltage(V)	Current(mA)	Classification	Statu
2:1	Enabled	15.4	0	0	0	Class 0	search
2:2	Enabled	15.4	0	0	0	Class 0	search
2:3	Enabled	15.4	0	0	0	Class 0	search
2:4	Enabled	15.4	0	0	0	Class 0	search
2:5	Enabled	15.4	9.2	50.7	181	Class 3	deliveringl
2:6	Enabled	15.4	0	0	0	Class 0	search
2:7	Enabled	15.4	0	0	0	Class 0	search
2:8	Enabled	15.4	0	0	0	Class 0	search
2:9	Enabled	15.4	0	0	0	Class 0	search
2:10	Enabled	15.4	0	0	0	Class 0	search
2:11	Enabled	15.4	0	0	0	Class 0	search
2:12	Enabled	15.4	0	0	0	Class 0	search
2:13	Enabled	15.4	0	0	0	Class 0	search
2:14	Enabled	15.4	0	0	0	Class 0	search
2:15	Enabled	15.4	0	0	0	Class 0	search
2:16	Enabled	15.4	0	0	0	Class 0	search
2:17	Enabled	15.4	0	0	0	Class 0	search
2:18	Enabled	15.4	0	0	0	Class 0	search
2:19	Enabled	15.4	0	0	0	Class 0	search

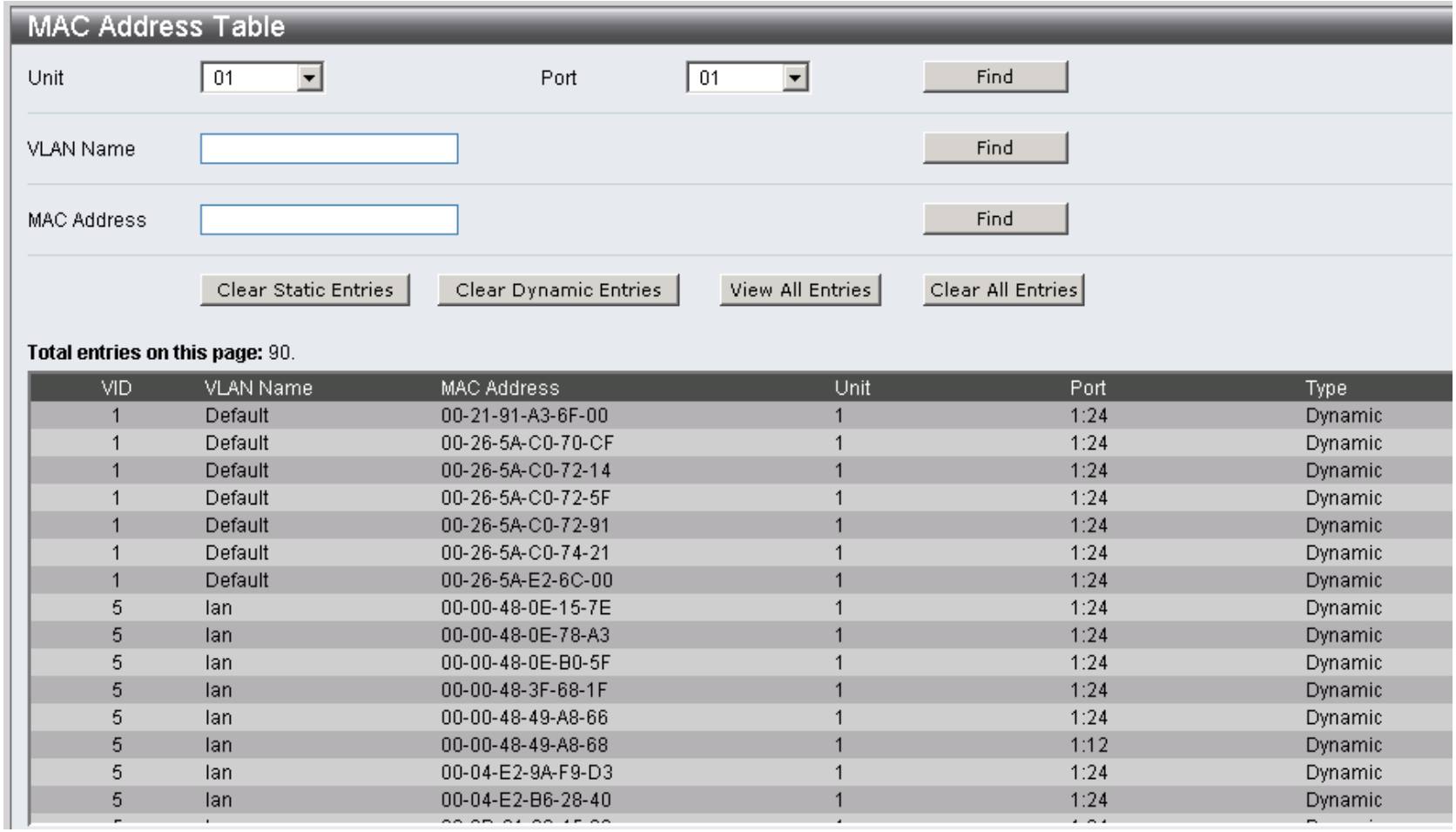
Log



System Log

ID	Time	Log Description
1	10-May-2010 21:28:26	%AAA-I-CONNECT: New http connection for user admin, source 203.72.153.57 destination 10.227.29.102 ACCEPTED
2	10-May-2010 21:27:44	%AAA-I-DISCONNECT: http connection for user admin, source 203.72.153.57 destination 10.227.29.102 TERMINATED
3	10-May-2010 21:12:27	%AAA-I-CONNECT: New http connection for user admin, source 203.72.153.57 destination 10.227.29.102 ACCEPTED
4	10-May-2010 20:59:10	%LINK-W-Down: 2:1
5	10-May-2010 20:32:55	%STP-W-PORTSTATUS: 2:1: STP status Forwarding
6	10-May-2010 20:32:25	%LINK-I-Up: 2:1
7	10-May-2010 20:32:24	%LINK-W-Down: 2:1
8	10-May-2010 20:15:23	%STP-W-PORTSTATUS: 2:1: STP status Forwarding
9	10-May-2010 20:14:53	%LINK-I-Up: 2:1
10	10-May-2010 20:14:51	%LINK-W-Down: 2:1
11	10-May-2010 20:14:29	%LINK-I-Up: 2:1
12	10-May-2010 20:14:27	%LINK-W-Down: 2:1
13	10-May-2010 16:30:01	%LINK-W-Down: 1:16
14	10-May-2010 16:29:55	%LINK-I-Up: 1:16
15	10-May-2010 16:29:53	%LINK-W-Down: 1:16
16	10-May-2010 16:17:55	%STP-W-PORTSTATUS: 1:14: STP status Forwarding
17	10-May-2010 16:17:25	%LINK-I-Up: 1:14
18	10-May-2010 16:17:23	%LINK-W-Down: 1:14
19	10-May-2010 16:10:13	%LINK-W-Down: 1:22
20	10-May-2010 16:09:44	%STP-W-PORTSTATUS: 1:15: STP status Forwarding
21	10-May-2010 16:09:14	%LINK-I-Up: 1:15
22	10-May-2010 16:09:12	%LINK-W-Down: 1:15
23	10-May-2010 16:08:51	%STP-W-PORTSTATUS: 1:22: STP status Forwarding

MAC Address Table



MAC Address Table

Unit 01 Port 01 Find

VLAN Name Find

MAC Address Find

Clear Static Entries | Clear Dynamic Entries | View All Entries | Clear All Entries

Total entries on this page: 90.

VID	VLAN Name	MAC Address	Unit	Port	Type
1	Default	00-21-91-A3-6F-00	1	1:24	Dynamic
1	Default	00-26-5A-C0-70-CF	1	1:24	Dynamic
1	Default	00-26-5A-C0-72-14	1	1:24	Dynamic
1	Default	00-26-5A-C0-72-5F	1	1:24	Dynamic
1	Default	00-26-5A-C0-72-91	1	1:24	Dynamic
1	Default	00-26-5A-C0-74-21	1	1:24	Dynamic
1	Default	00-26-5A-E2-6C-00	1	1:24	Dynamic
5	lan	00-00-48-0E-15-7E	1	1:24	Dynamic
5	lan	00-00-48-0E-78-A3	1	1:24	Dynamic
5	lan	00-00-48-0E-B0-5F	1	1:24	Dynamic
5	lan	00-00-48-3F-68-1F	1	1:24	Dynamic
5	lan	00-00-48-49-A8-66	1	1:24	Dynamic
5	lan	00-00-48-49-A8-68	1	1:12	Dynamic
5	lan	00-04-E2-9A-F9-D3	1	1:24	Dynamic
5	lan	00-04-E2-B6-28-40	1	1:24	Dynamic

Thin AP Debug

- 確認校內路由正常
- 所有設定都在AC
- 確認AC與Winoc運作正常

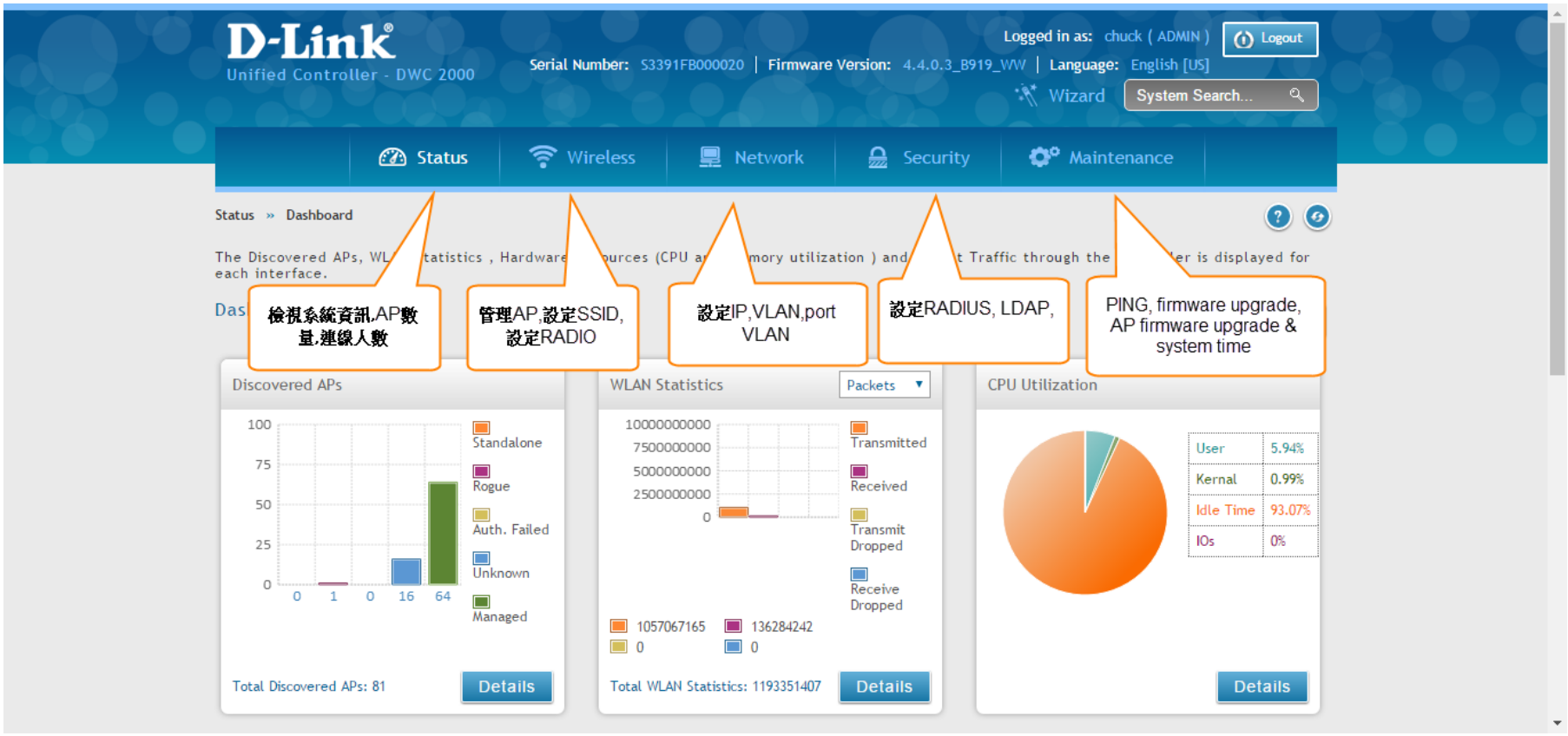
DWC-2000 設定原理

大綱

1. 系統基本介紹
2. Interface介紹
3. 如何管理AP & 升級AP firmware
4. 如何修改AP profile
5. 如何設定 captive portal
6. 應用案例介紹

系統基本介紹

- 設備預設IP是 192.168.10.1
- 登入URL為 http://192.168.10.1
- 帳號/密碼: admin/admin
- 在沒有額外購買AP license情況下,可以管理64台AP
- 支援RADIUS和AD認證
- 可以針對不同VLAN派發IP, 但要在route mode架構下


D-Link
Unified Controller - DWC 2000
Serial Number: S3391FB000020 | Firmware Version: 4.4.0.3_B919_WW | Language: English [US]
Logged in as: chuck (ADMIN)
Logout
Wizard
System Search...
Status
Wireless
Network
Security
Maintenance
Status » Dashboard
檢視系統資訊,AP數量,連線人數
管理AP,設定SSID,設定RADIO
設定IP,VLAN,port VLAN
設定RADIUS, LDAP,
PING, firmware upgrade, AP firmware upgrade & system time
Discovered APs
Standalone
Rogue
Auth. Failed
Unknown
Managed
Total Discovered APs: 81
Details
WLAN Statistics
Packets
Transmitted
Received
Transmit Dropped
Receive Dropped
1057067165
136284242
0
0
Total WLAN Statistics: 1193351407
Details
CPU Utilization
User 5.94%
Kernal 0.99%
Idle Time 93.07%
IOs 0%
Details

Interface介紹

- 設備正面有四個RJ-45 interface 和 4個SFP介面,總共八個interface, 但他們是combo port, 意思是說當我如果接上RJ-45 port1的話,SFP的port1會無法使用.
- 在default configuration的情況下,四個interface都是同一個VLAN.
- 設備支援L3 VLAN 和 VLAN routing
- 設備支援route mode 和 NAT mode.

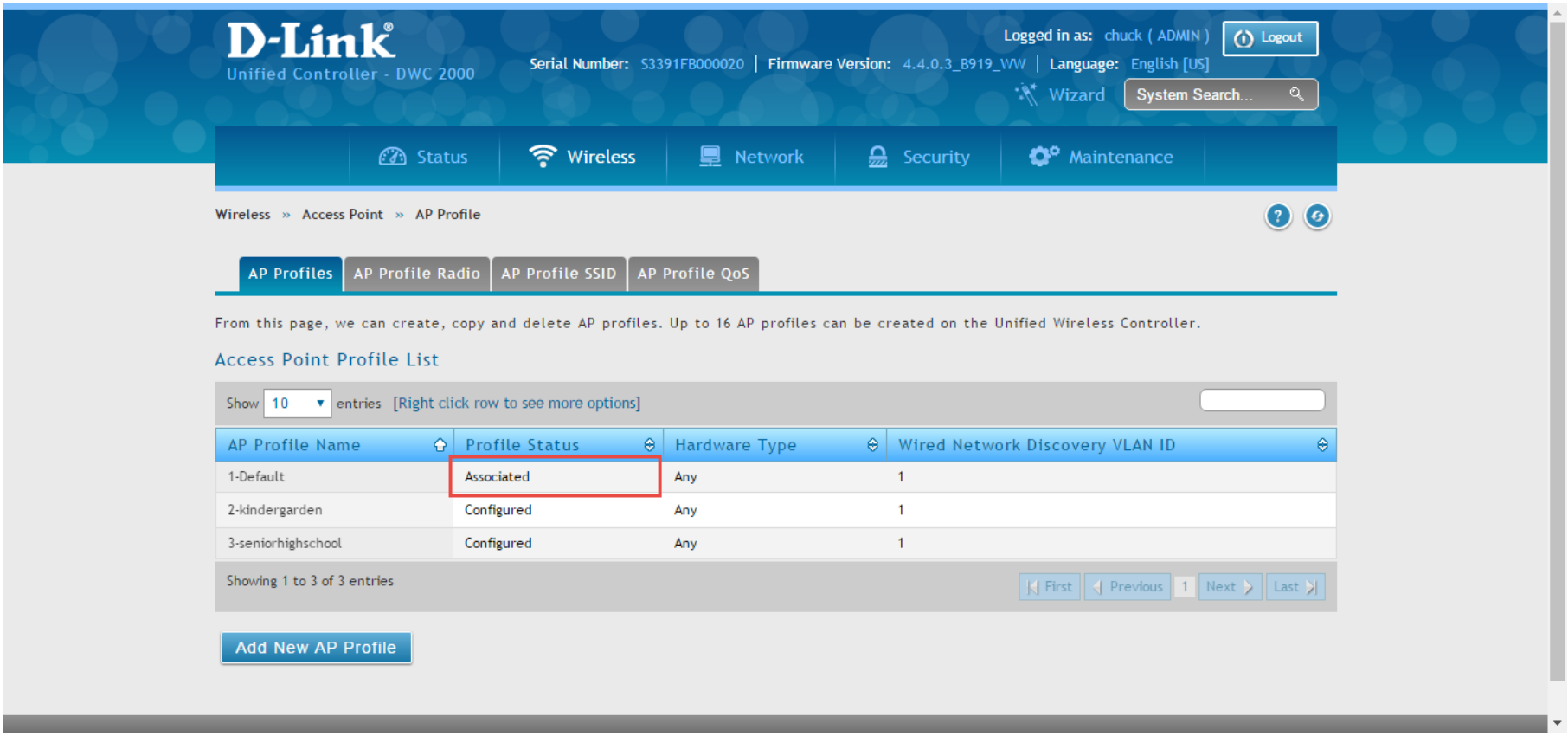
如何管理AP & 升級AP firmware

- DWL-8610AP & DWL-6610AP 一但被DWC-2000管理之後,便無法直接使用telnet & http 的方式去操作AP並且幫他做firmware upgrade, 要從DWC-2000的 Maintenance»Firmware»AP Firmware Download 去幫AP 做 firmware upgrade.
- 由於此操作只能用tftp的方式進行,請先在電腦上準備好 tftp server, 推薦使用 tftpd32 (http://tftpd32.jounin.net/tftpd32_download.html)
- 整個AP升級過程大約要五分鐘

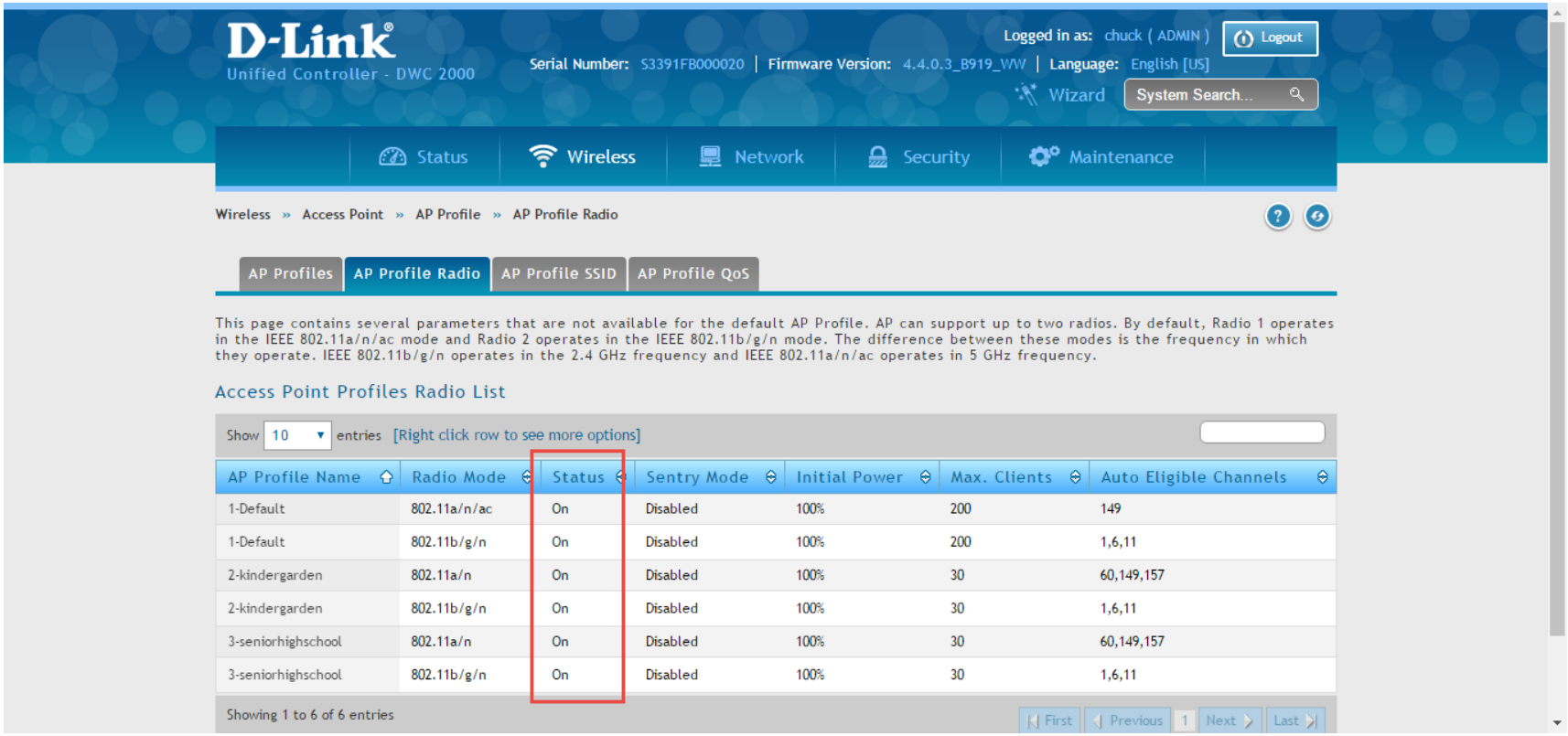

D-Link
Unified Controller - DWC 2000
Logged in as: chuck (ADMIN) Logout
Serial Number: S3391FB000020 | Firmware Version: 4.4.0.3_B919_WW | Language: English [US]
Wizard
System Search...
Status
Wireless
Network
Security
Maintenance
Maintenance » Firmware » AP Firmware Download
It may take about 12 minutes for the upgrade process to complete for an AP.
AP Firmware Download
AP Firmware Status
The Unified Wireless Controller can upgrade software on the APs that it manages. The Cluster Controller can update code on APs managed by peer wireless controllers.
AP Firmware Download
Server Address
Img_dwl8600
D-Link 8600 AP Radios
File Path
File Name
Img_dwl3600/6600
D-Link 3600/6600 AP Radios
File Path
File Name
Img_dwl2600
D-Link 2600 AP Radios
File Path
File Name
Img_dwl8610
D-Link 8610 AP Radios
File Path
File Name
Img_dwl6700
D-Link 6700 AP Radios
File Path
File Name
Img_dwl6610
D-Link 6610 AP Radios
File Path
File Name
Img_dwl8710
D-Link 8710 AP Radios
File Path
File Name
Group Size
6
[Default: 64, Range: 1 - 192]
Image Download Type
DWL-6610AP
Managed AP
All
3c:1e:04:f8:ed:c0-10.192.92.100 -
3c:1e:04:f8:f1:00-10.192.130.100 -
3c:1e:04:f8:f1:40-10.192.129.100 -
3c:1e:04:f8:f4:40-10.192.115.100 -
3c:1e:04:f8:f4:80-10.192.116.100 -
3c:1e:04:f8:f4:c0-10.192.123.100 -
3c:1e:04:f8:f5:00-10.192.122.100 -
Save
Start
Refresh
請輸入 TFTP server IP address
輸入firmware檔名,例如 dwl-6610_fw_v_4.3.0.4.tar
Group size建議用 6 ~ 8, 這是指一次幫幾台ap做升級動作.
選擇哪一款ap要做升級,這邊我們選 6610AP
最後按下 save. 切記,要先save 再start.
Copyright © 2014 D-Link Corporation.

如何修改AP profile

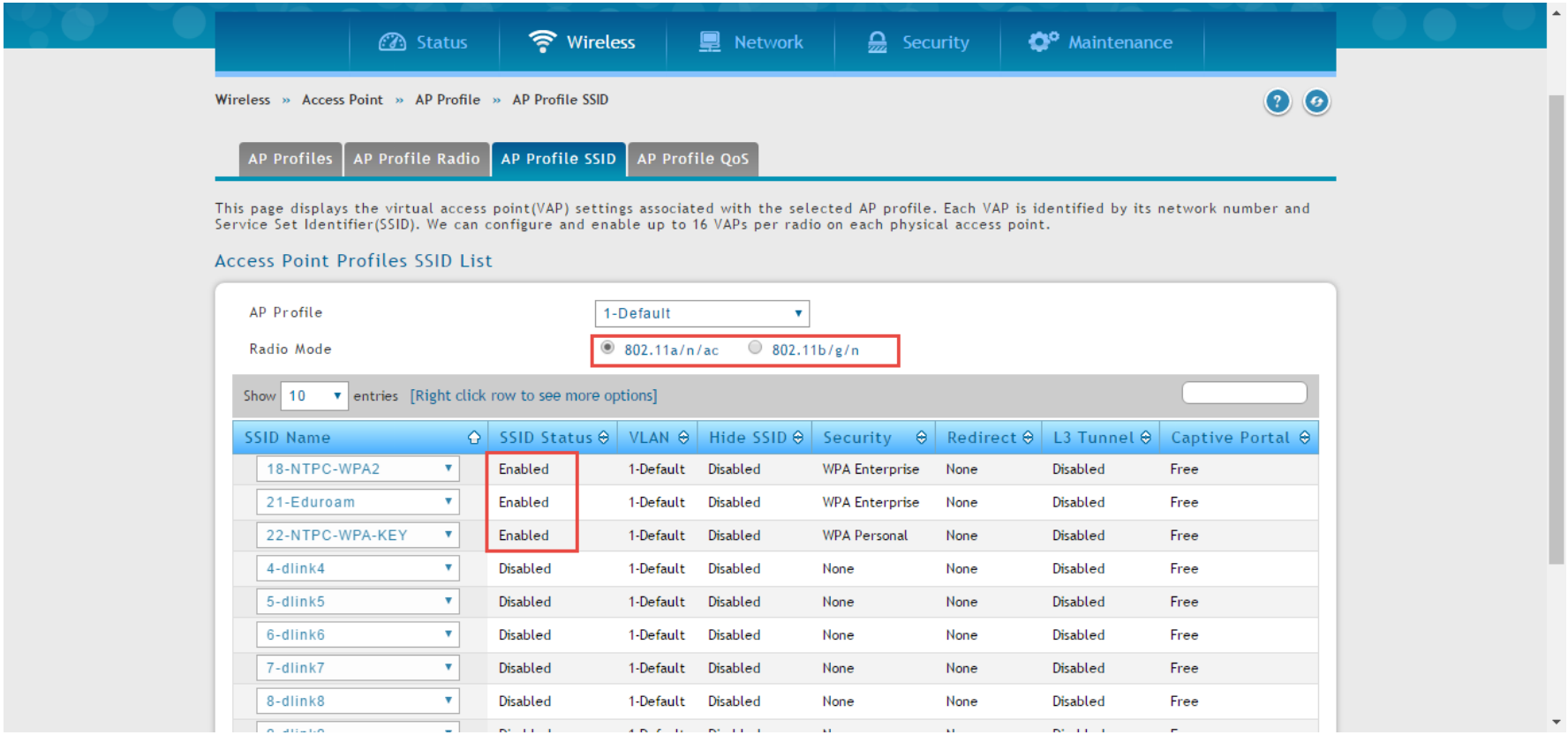
- 最多可以建立64個 AP profile. Profile 裡面又包含了 radio & SSID.
- SSID 最多可以建立50個.



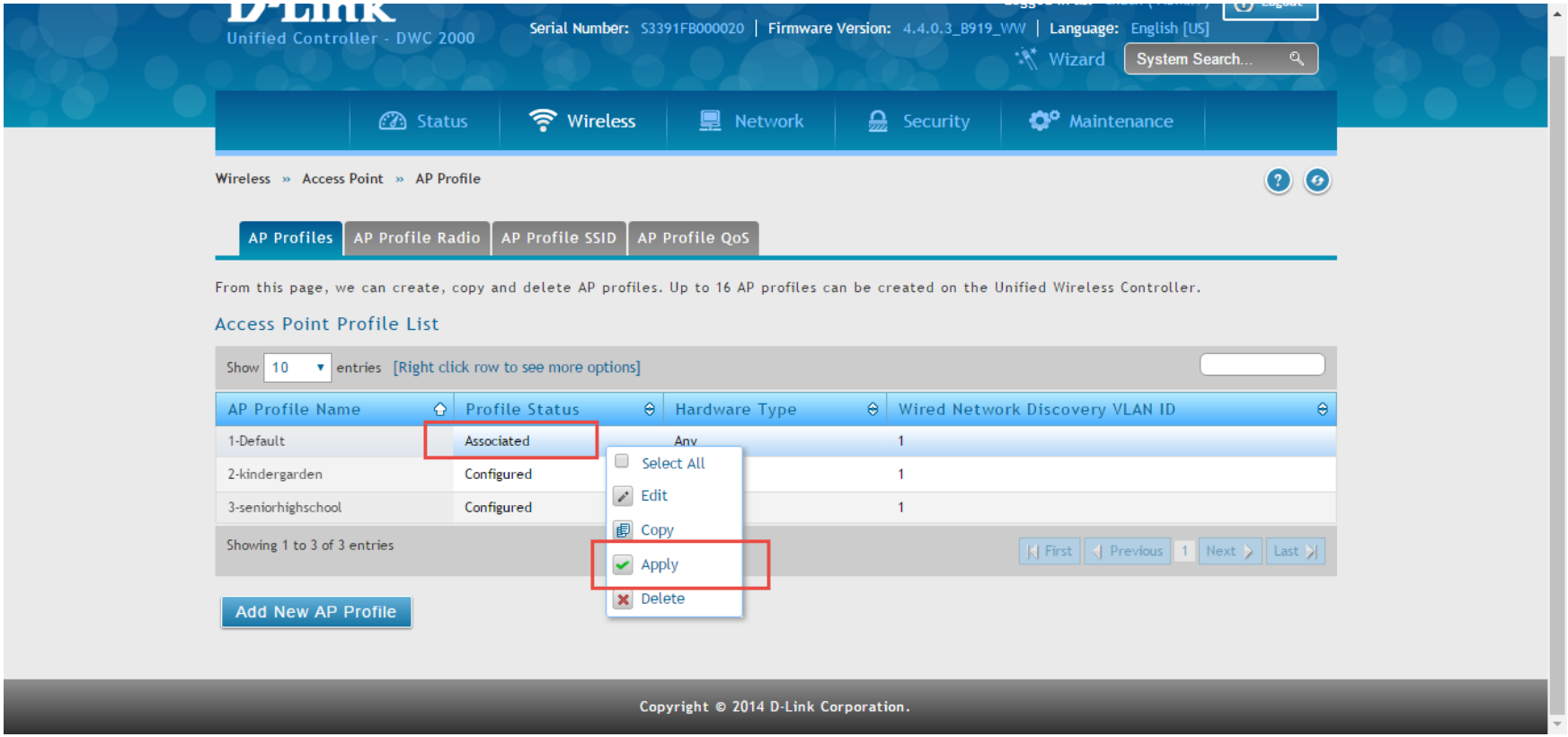
- 紅色框框是代表這個radio是開還是關,如果有某一個radio不想使用,就設定成off



- 只有第一個SSID會預設就是enable, 如果有使用二個以上,請記得要把他設定成enable, 2個radio都要設定



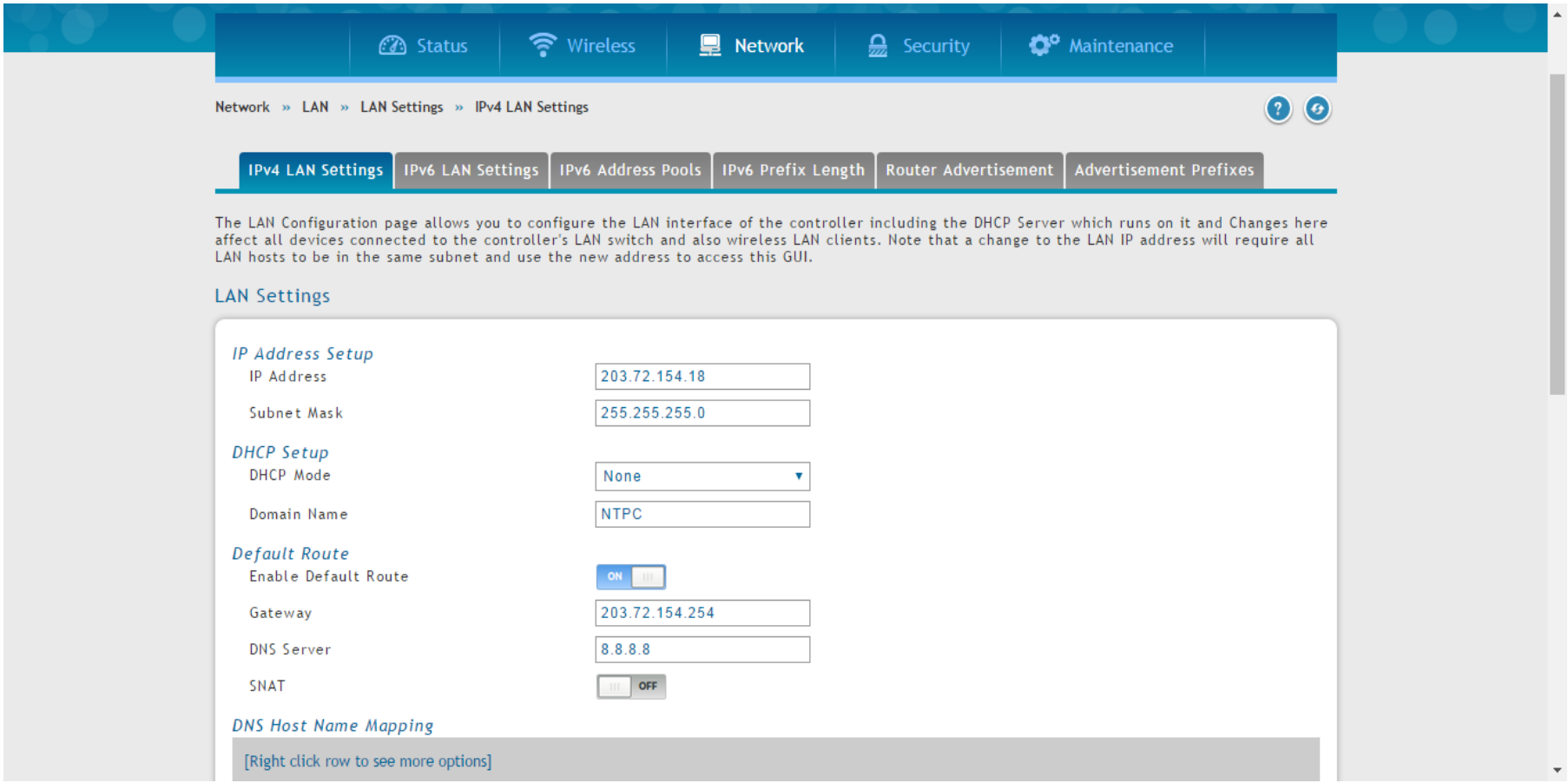
- 有更改radio or SSID設定的話,請記得要選 apply 去把設定推給AP.
- Associated 代表這個 AP profile有管理AP



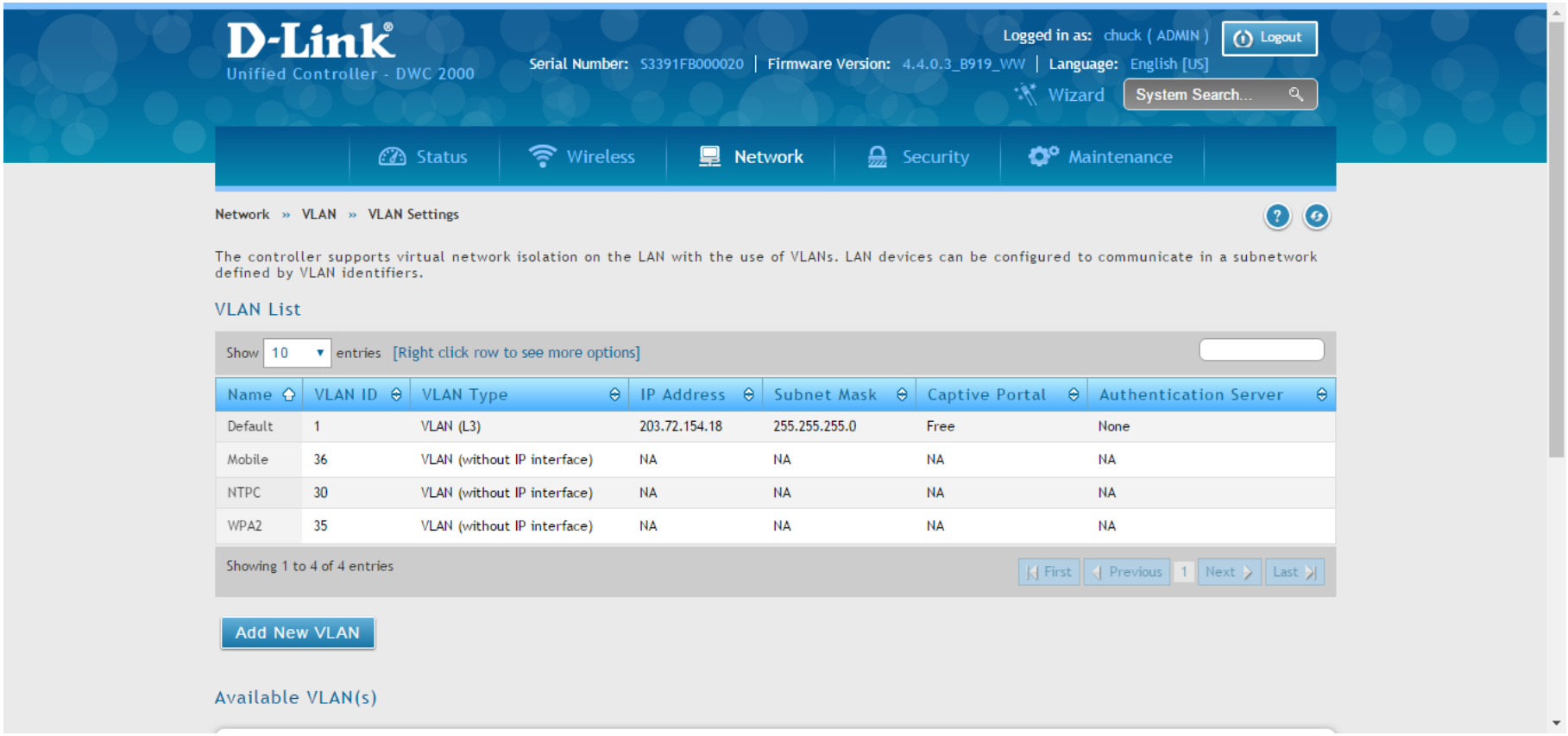
如何設定 captive portal

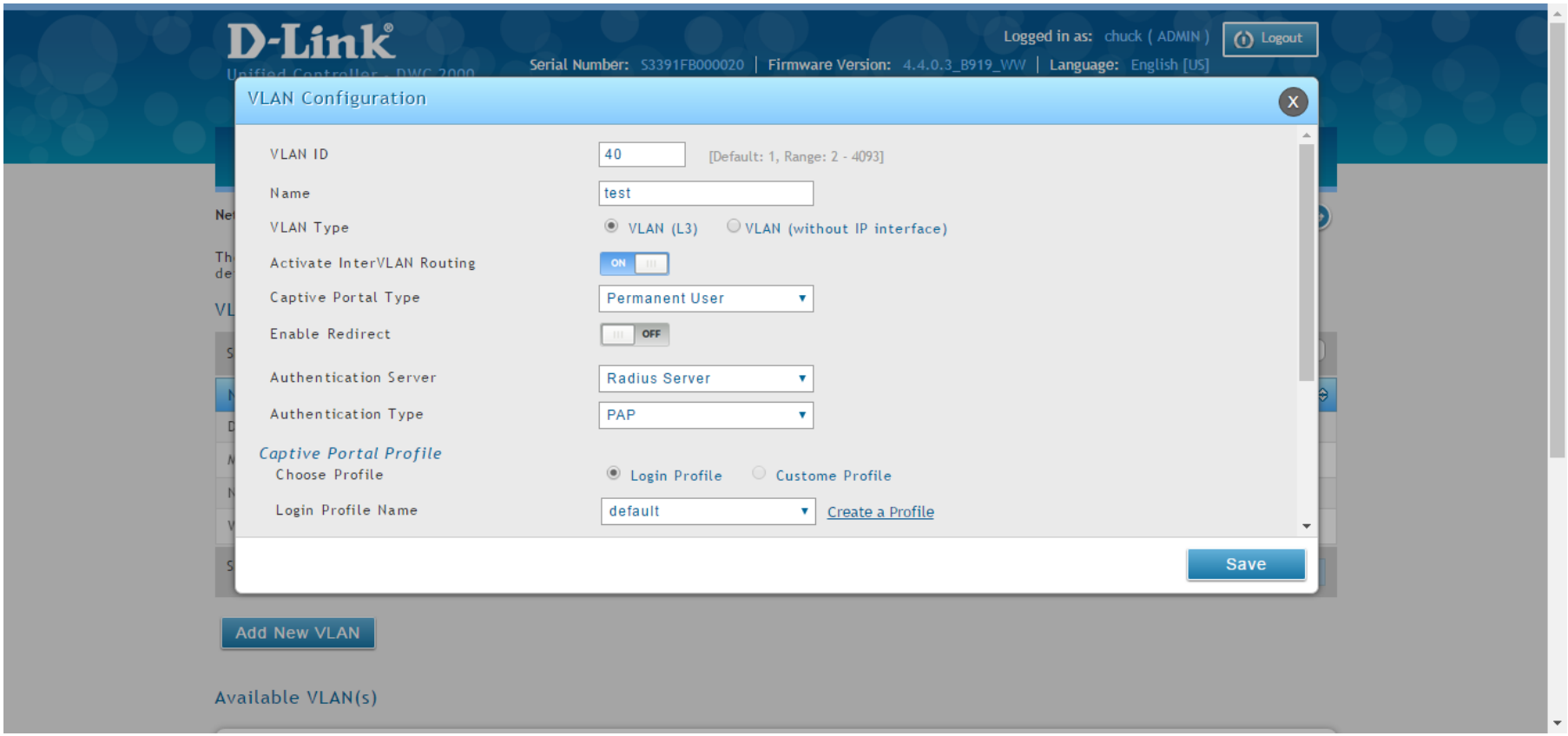
- 要在DWC-2000上面使用captive portal有二種方式, switch mode & route mode. 由於使用route mode的認證速度較快,在此我們只介紹這種架構.
- 要使用route mode意味者dwc-2000要有二個網段,一個是uplink subnet, 另一個是 downlink subnet.
- Route mode架構請使用 FW_4.4.0.3_B931 以上的版本.
- Uplink一定要使用 VLAN1, downlink可以自行設定
- 模擬架構圖如下:

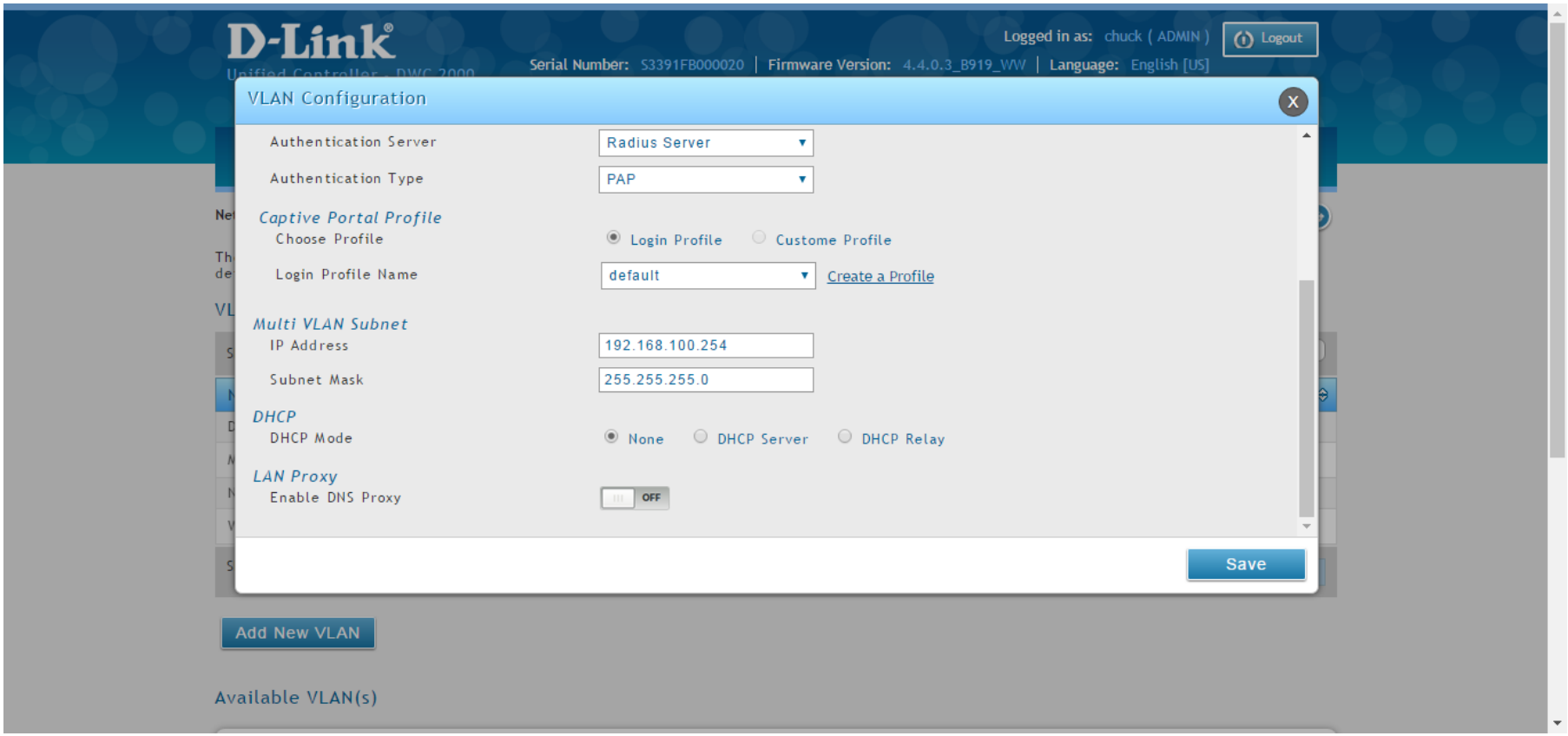
- **203.72.154.18(port 1 vlan1) DWC (port 2 vlan40) 192.168.100.254**


Status
Wireless
Network
Security
Maintenance
Network » LAN » LAN Settings » IPv4 LAN Settings
IPv4 LAN Settings
IPv6 LAN Settings
IPv6 Address Pools
IPv6 Prefix Length
Router Advertisement
Advertisement Prefixes
The LAN Configuration page allows you to configure the LAN interface of the controller including the DHCP Server which runs on it and Changes here affect all devices connected to the controller's LAN switch and also wireless LAN clients. Note that a change to the LAN IP address will require all LAN hosts to be in the same subnet and use the new address to access this GUI.
LAN Settings
IP Address Setup
IP Address
203.72.154.18
Subnet Mask
255.255.255.0
DHCP Setup
DHCP Mode
None
Domain Name
NTPC
Default Route
Enable Default Route
ON
Gateway
203.72.154.254
DNS Server
8.8.8.8
SNAT
OFF
DNS Host Name Mapping
[Right click row to see more options]

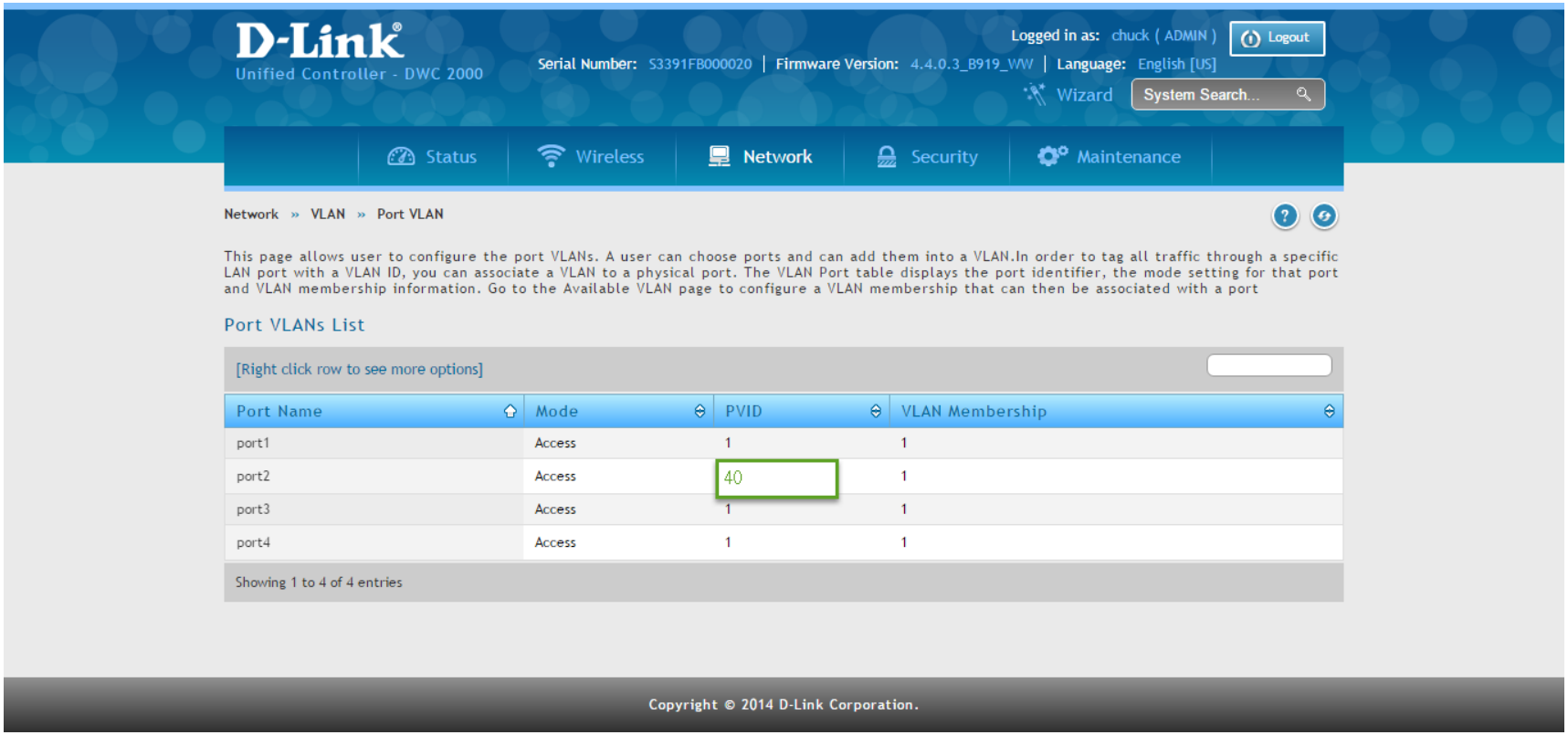
- 從 VLAN list可以新增修改VLAN 設定



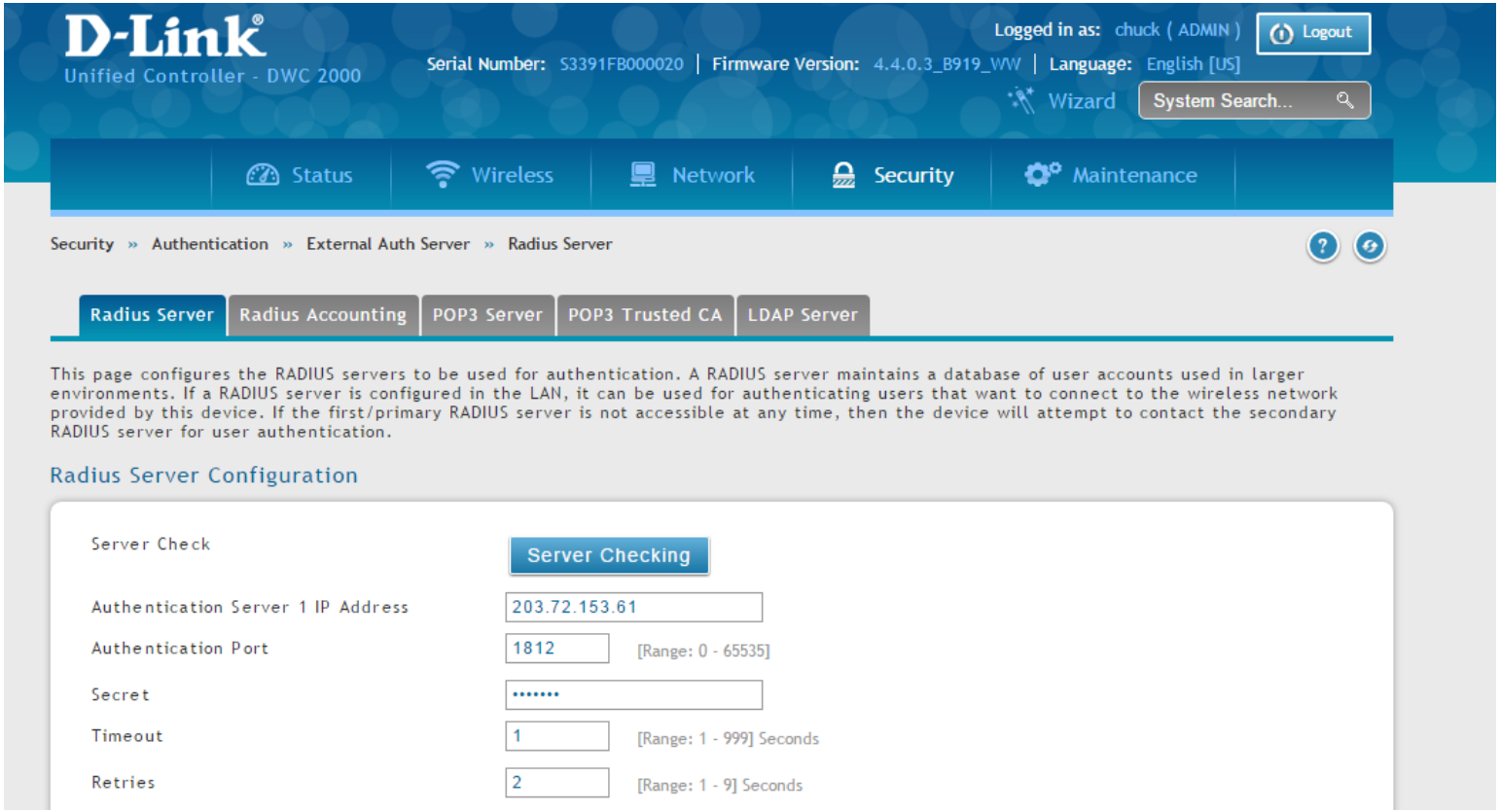

D-Link
Unified Controller - DWC-2000
Serial Number: S3391FB000020 | Firmware Version: 4.4.0.3_B919_WW | Language: English [US]
Logged in as: chuck (ADMIN)
Logout
VLAN Configuration
VLAN ID
40
[Default: 1, Range: 2 - 4093]
Name
test
VLAN Type
VLAN (L3)
VLAN (without IP interface)
Activate InterVLAN Routing
ON
Captive Portal Type
Permanent User
Enable Redirect
OFF
Authentication Server
Radius Server
Authentication Type
PAP
Captive Portal Profile
Choose Profile
Login Profile
Custome Profile
Login Profile Name
default
Create a Profile
Save
Add New VLAN
Available VLAN(s)


D-Link
Unified Controller - DWC-2000
Serial Number: S3391FB000020 | Firmware Version: 4.4.0.3_B919_WW | Language: English [US]
Logged in as: chuck (ADMIN)
Logout
VLAN Configuration
Authentication Server
Radius Server
Authentication Type
PAP
Captive Portal Profile
Choose Profile
Login Profile
Custome Profile
Login Profile Name
default
Create a Profile
Multi VLAN Subnet
IP Address
192.168.100.254
Subnet Mask
255.255.255.0
DHCP
DHCP Mode
None
DHCP Server
DHCP Relay
LAN Proxy
Enable DNS Proxy
OFF
Save
Add New VLAN
Available VLAN(s)

- Port VLAN 可以設定每個port使用哪個VLAN



- 此處設定RADIUS server 參數



附錄

- DWC-2000 firmware 4.4.0.3_B931_WW_Q
- https://drive.google.com/file/d/0B1qEQfkSaQCrZXA0cTBjRTZoN0E/view?usp=sharing

- DWL-6610AP firmware 4.3.0.4
- https://drive.google.com/file/d/0B1qEQfkSaQCrZ0p5YWxpeExVY2s/view?usp=sharing

NTPC除錯

- 1.Vlan 30 Trunk Port 對嗎?
- 2.Vlan 30 GW是否到的了
- 3. DWC-2000是否掛點?
- 4. DWC-2000是否認證成功?
- 5.Vlan 8路由正常否?
- 6. DWC-2000看user log
- 7.Firewall上查Policy。
- 8.Core Routing

NTPC-Mobile除錯

- 1.Vlan 36 Trunk port
- 2.AP MAC
- 3.L2 MAC
- 4.L3 MAC
- 5.L3 unblock
- 6.Wan ip 是否有發radius服務
- 7.firewall Policy
- 8.vlan interface and routing

WPA2-除錯

- Vlan 35 trunk port
- Vlan 1 or Vlan35 AP ip to Radius
- AP MAC
- Check Policy
- Vlan interface and Routing

Thin AP除錯

- 1.AC Discovery
- 2.Tunnel Mode or Bridge Mode
- 3.Radius Server
- 4.DHCP
- 5.IP Pool setup
- 6.Firewall Routing
- 7.Bridge switch setup(Check MAC)
- 8.Policy

Firewall Sniffer

- Config vdom
- Edit v256-vd
- Diagnose sniffer packet any “host X.X.X.X” 4

Sflow Local Traffice監控

- 校園設定一台PC，安裝sFlowTrend.jnlp and java
- 請中心工程師在3620下達指令

1. enable sflow
2. create sflow analyzer_server 1 owner NTPC timeout infinite collectoraddress 163.20.66.190 collectorport 6343 maxdatagramsize 1400
3. create sflow flow_sampler ports 1:1-24 analyzer_server_id 1 rate 1 tx_rate 1 maxheadersize 256
4. delete sflow flow_sampler ports 1:1-24

Sflow與中心端Siraya之差異

- Local traffice監控
- 骨幹出問題時可以知道校內流量及原因。
- 詳細的Local Traffice

舊有FAT AP納管

- 學校內的舊FAT AP可完全支援所有認證方式
  - 舊有AP功能可支援NTPC-WPA2及NTPC-Mobile設定部份可參考以下兩者進行調整
  - NTPC規劃設定Vlan8 10.253.XX.254 and Vlan 30傳送Data traffice 。
  - NTPC-WPA2認證部分，
    - FAT AP認證系統需要加入此AP ip (Vlan1)，並帶(Vlan35)傳送Data traffice。
  - NTPC-Mobile 認證依舊由L3 Switch進行認證。
    - 認證系統需要加入L3 switch ip (Vlan1)，並帶(Vlan36傳送Data traffice 。

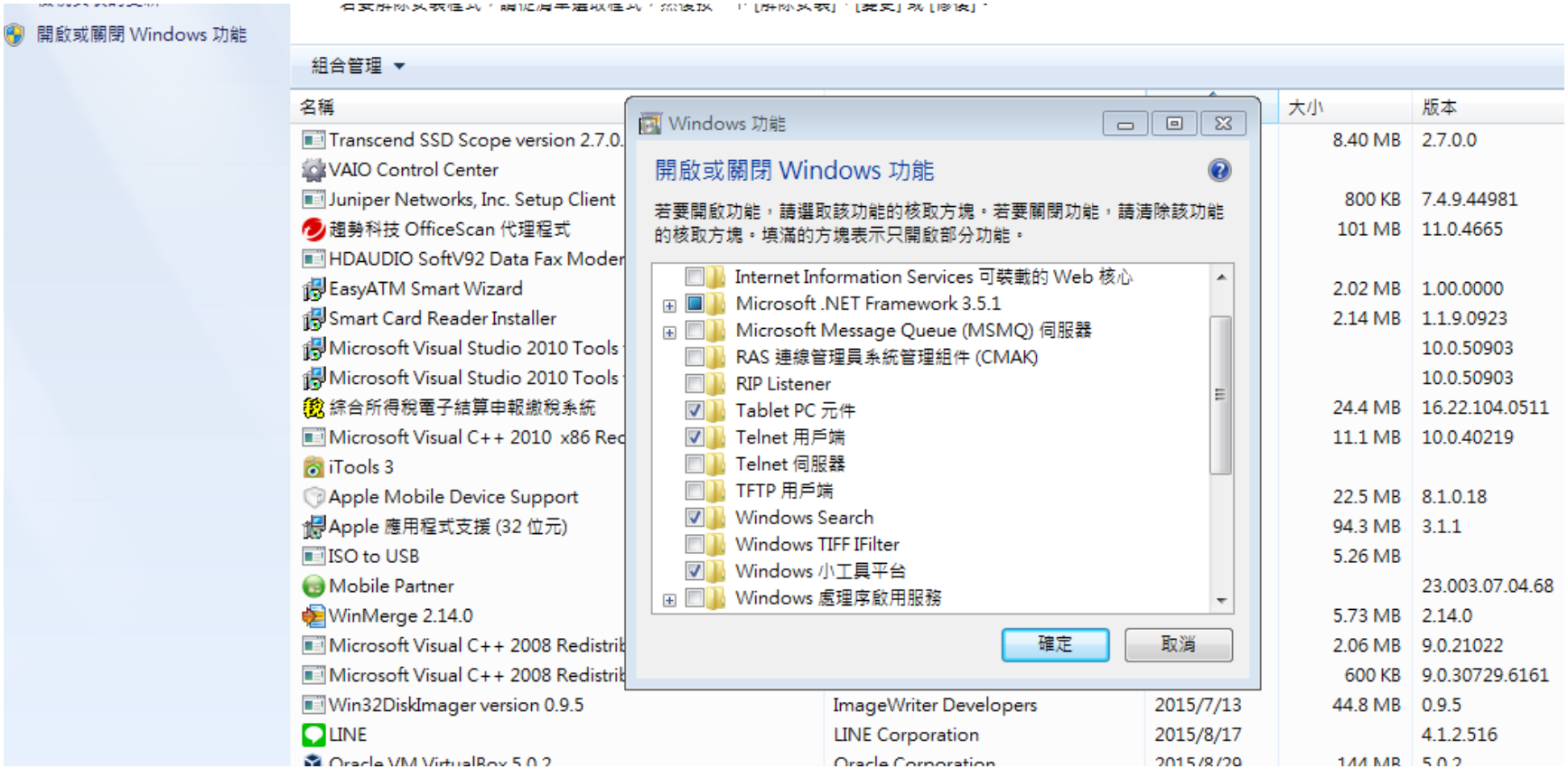
問題討論

- 訊號不佳
  - Wifi analyzer
- 無法進入認證可能問題
  - 測Radius
- 特定網路位址不通，服務不通?
  - Firewall policy
- 無法辦公文?
  - DNS

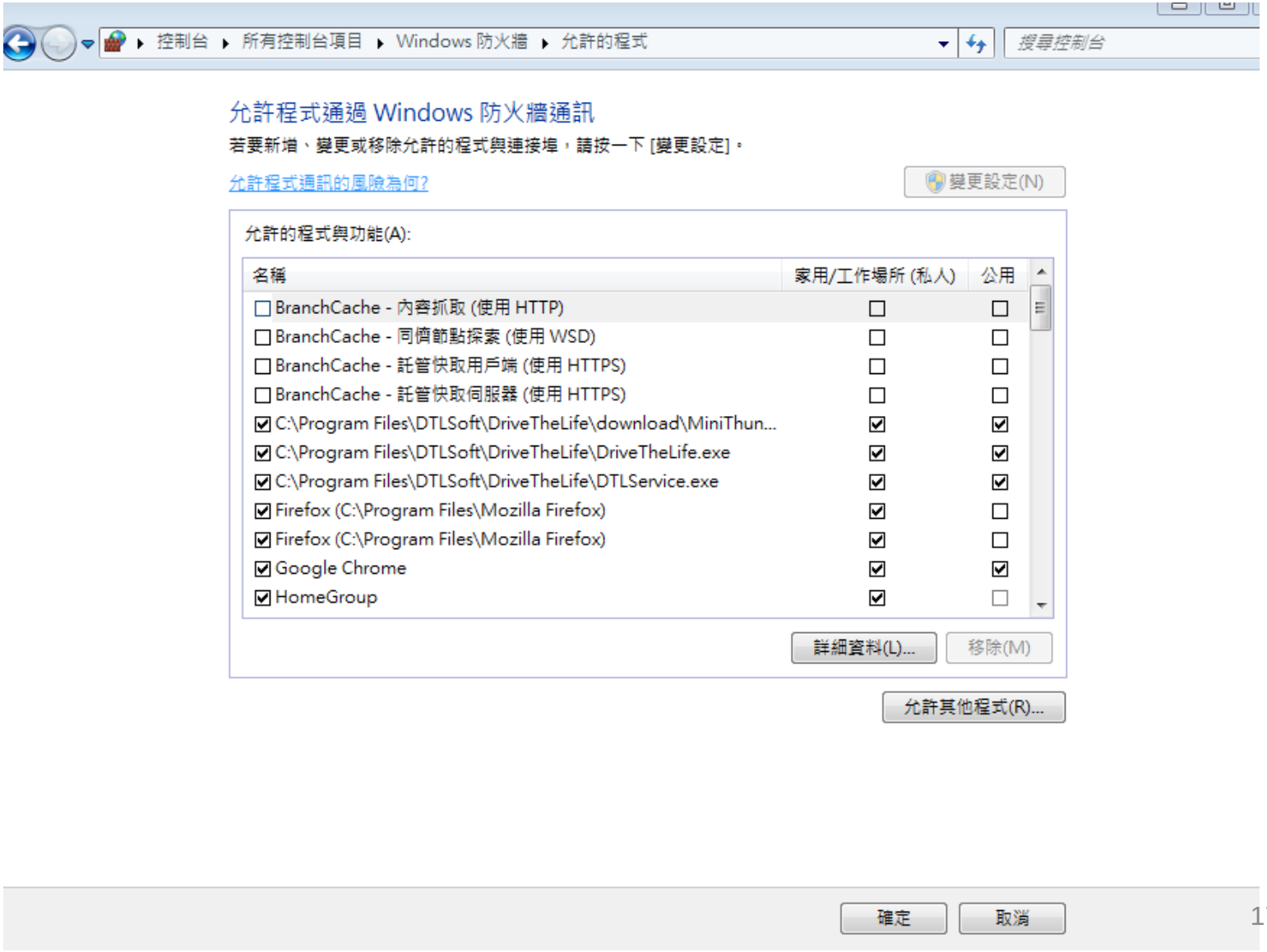
總 結

- Wifi analyzer頻譜，分析訊號強弱。
- Wireless :
  - NTPC Web portal、 NTPC- WPA2 、NTPC- Mobile 、 EduRoaming 、 TanetRoam
- Radius認證(Winoc)
  - 納管FAT AP Radius 認證及MAC Auth帳號。
  - 處理AC Radius認證
- FireWall Policy
  - 處理10.128/9 做NAT(163.20.242~243/23)
  - 引導網段至Winoc做Radius認證
- Thin AP 架構及啟動行為設計
- IP不夠用問題：
  - 舊架構擴充發四個C
  - 新架構一個B，原來的C當ip pool

附錄
windows 7 開啟telent 功能



Win7 firewall



中心firewall功能

- 做10網段NAT
- 對單一ip做session limit
- 阻擋P2P
- 做動態路由交換ospf
- 各校邏輯上的firewall分割Vdom
- IPS功能
- 監控封包除錯功能

Dlink DWL 6610AP設定

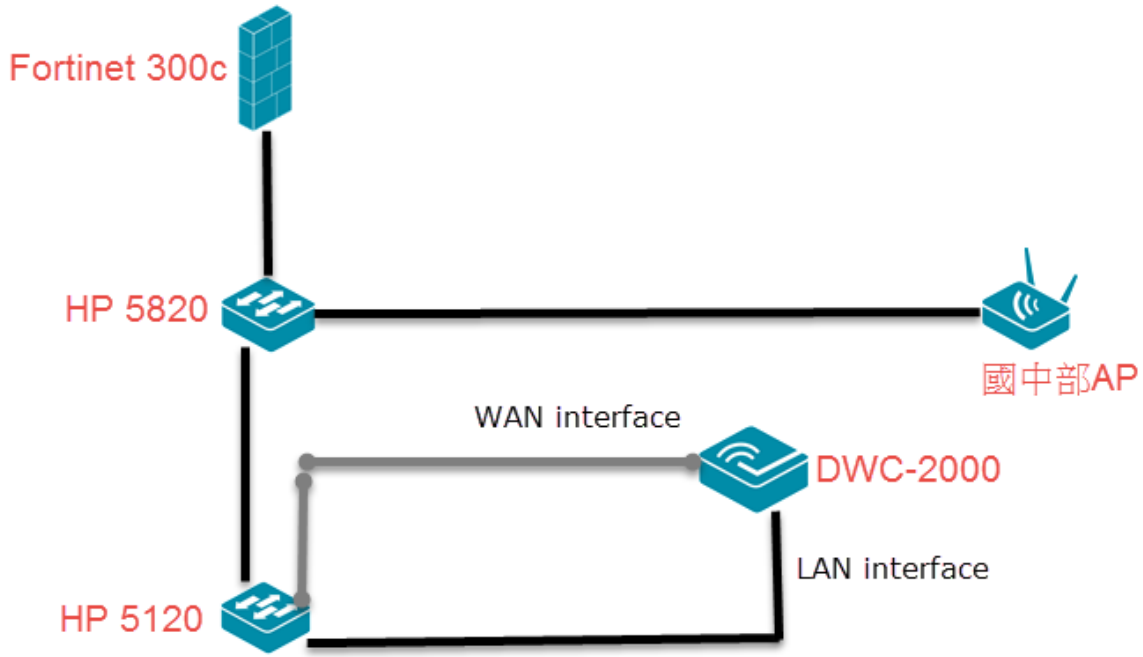
- 先至AC開啟AP debug,設定admin password
- telnet 連上
- 設定AP ip
- 設定AC ip

Dlink DWL 6610AP

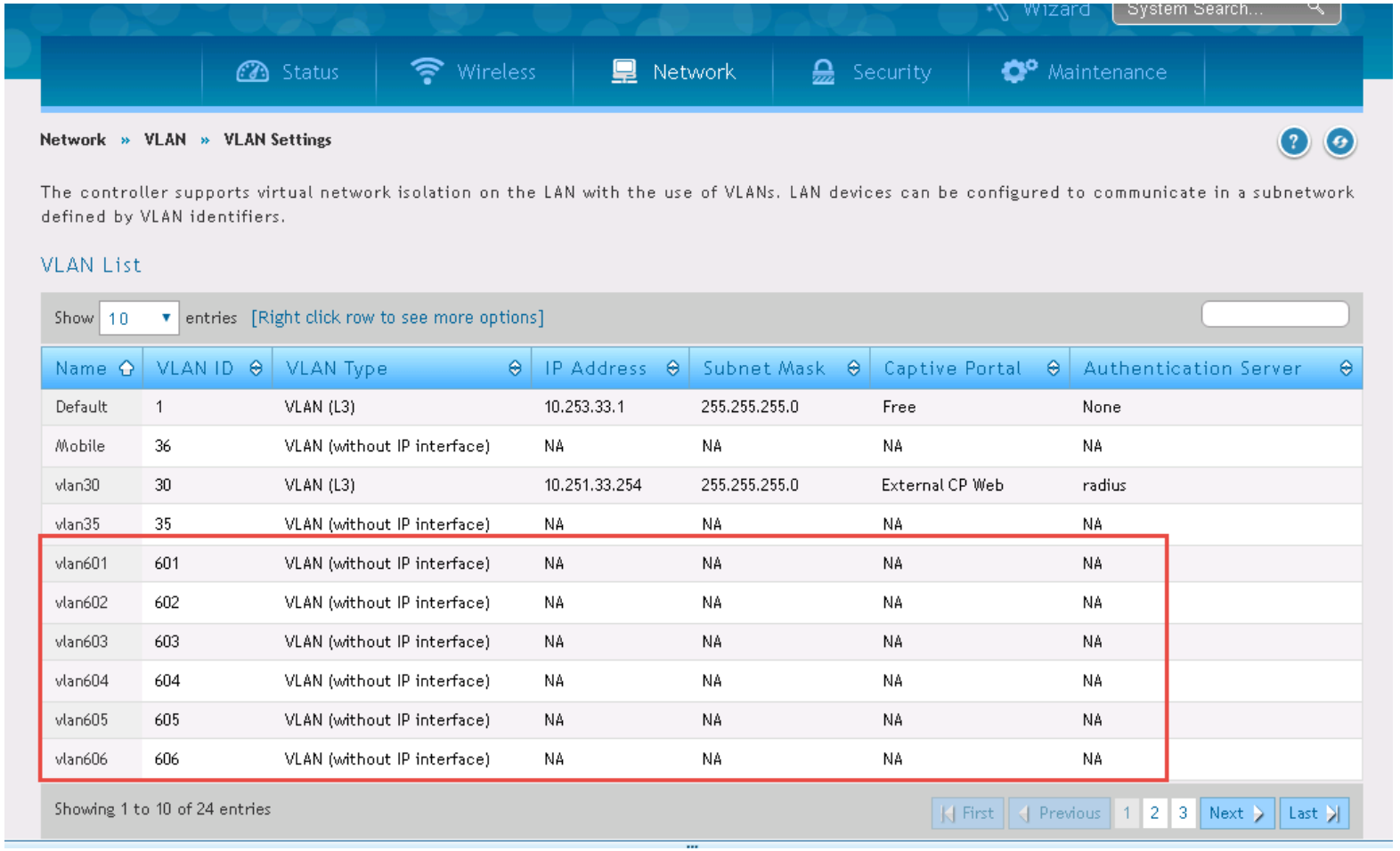
- set management dhcp-status down
  set management static-ip 10.226.161.117
  set management static-mask 255.255.255.0
  set static-ip-route gateway 10.226.161.254
  set host id AP117
  set managed-ap switch-address-1 10.253.161.1
  set telnet status up
  set web-server http-status up
  save-running

應用案例:三峽明德中學國中部無線網路架構

- 在每一間教室裝一間AP, 並且SSID名稱要跟教室名稱一樣,代表了每間教室的SSID都是不同的並且每個AP要用不同的AP profile.
- 設定順序如下:
- 設定L2 VLAN ID (GateWay)(Route)
- 設定SSID
- 設定 AP profile
- 把SSID拉進去匹配的AP profile
- 納管AP, 每台AP用不同的AP profile.


Fortinet 300c
HP 5820
國中部AP
WAN interface
DWC-2000
LAN interface
HP 5120

- 設定L2 VLAN ID

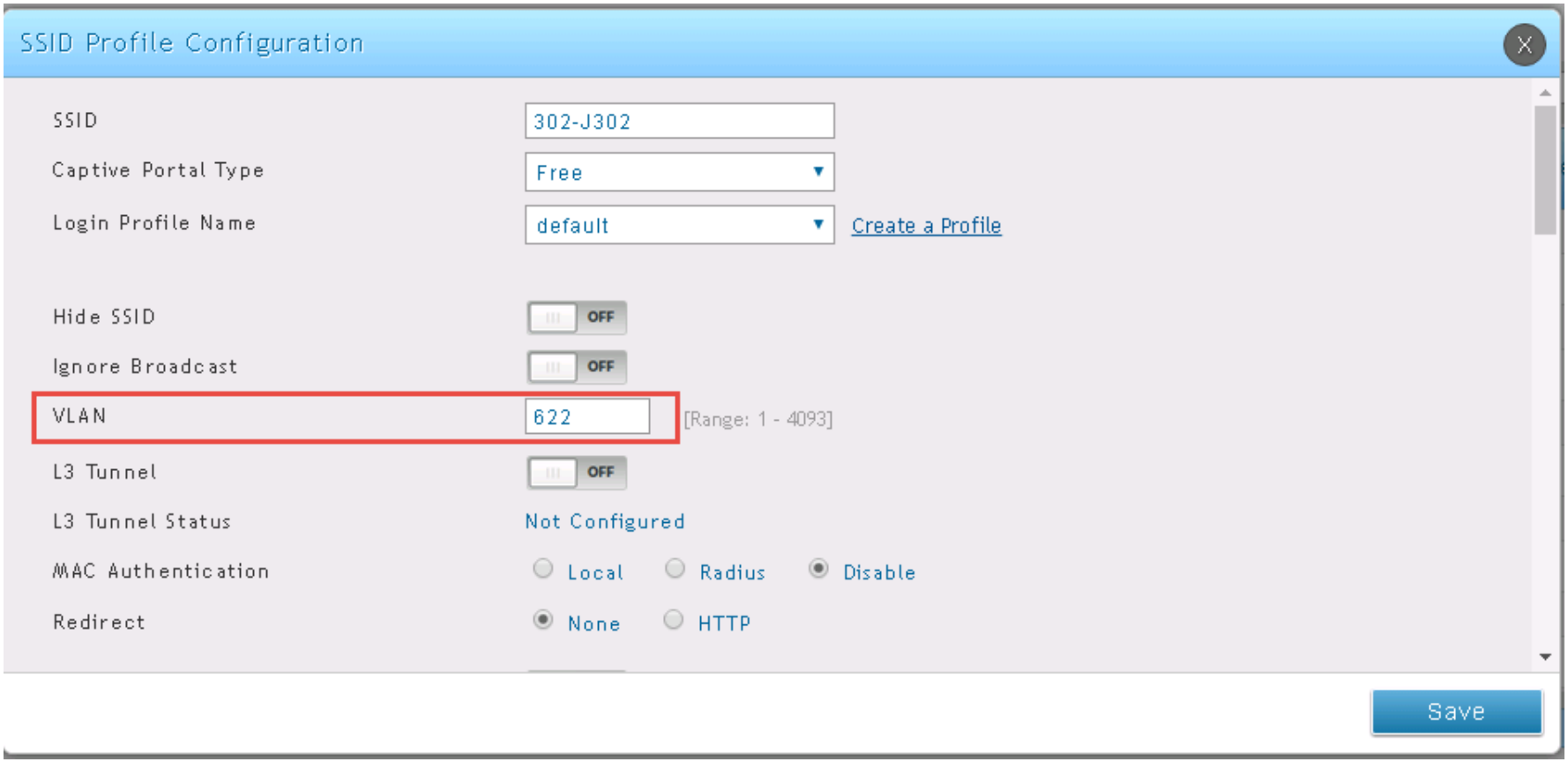

Wizard
System Search...
Status
Wireless
Network
Security
Maintenance
Network » VLAN » VLAN Settings
The controller supports virtual network isolation on the LAN with the use of VLANs. LAN devices can be configured to communicate in a subnetwork defined by VLAN identifiers.
VLAN List
Show 10 entries [Right click row to see more options]
Name | VLAN ID | VLAN Type | IP Address | Subnet Mask | Captive Portal | Authentication Server
Default | 1 | VLAN (L3) | 10.253.33.1 | 255.255.255.0 | Free | None
Mobile | 36 | VLAN (without IP interface) | NA | NA | NA | NA
vlan30 | 30 | VLAN (L3) | 10.251.33.254 | 255.255.255.0 | External CP Web | radius
vlan35 | 35 | VLAN (without IP interface) | NA | NA | NA | NA
vlan601 | 601 | VLAN (without IP interface) | NA | NA | NA | NA
vlan602 | 602 | VLAN (without IP interface) | NA | NA | NA | NA
vlan603 | 603 | VLAN (without IP interface) | NA | NA | NA | NA
vlan604 | 604 | VLAN (without IP interface) | NA | NA | NA | NA
vlan605 | 605 | VLAN (without IP interface) | NA | NA | NA | NA
vlan606 | 606 | VLAN (without IP interface) | NA | NA | NA | NA
Showing 1 to 10 of 24 entries
First
Previous
1
2
3
Next
Last

- 設定SSID

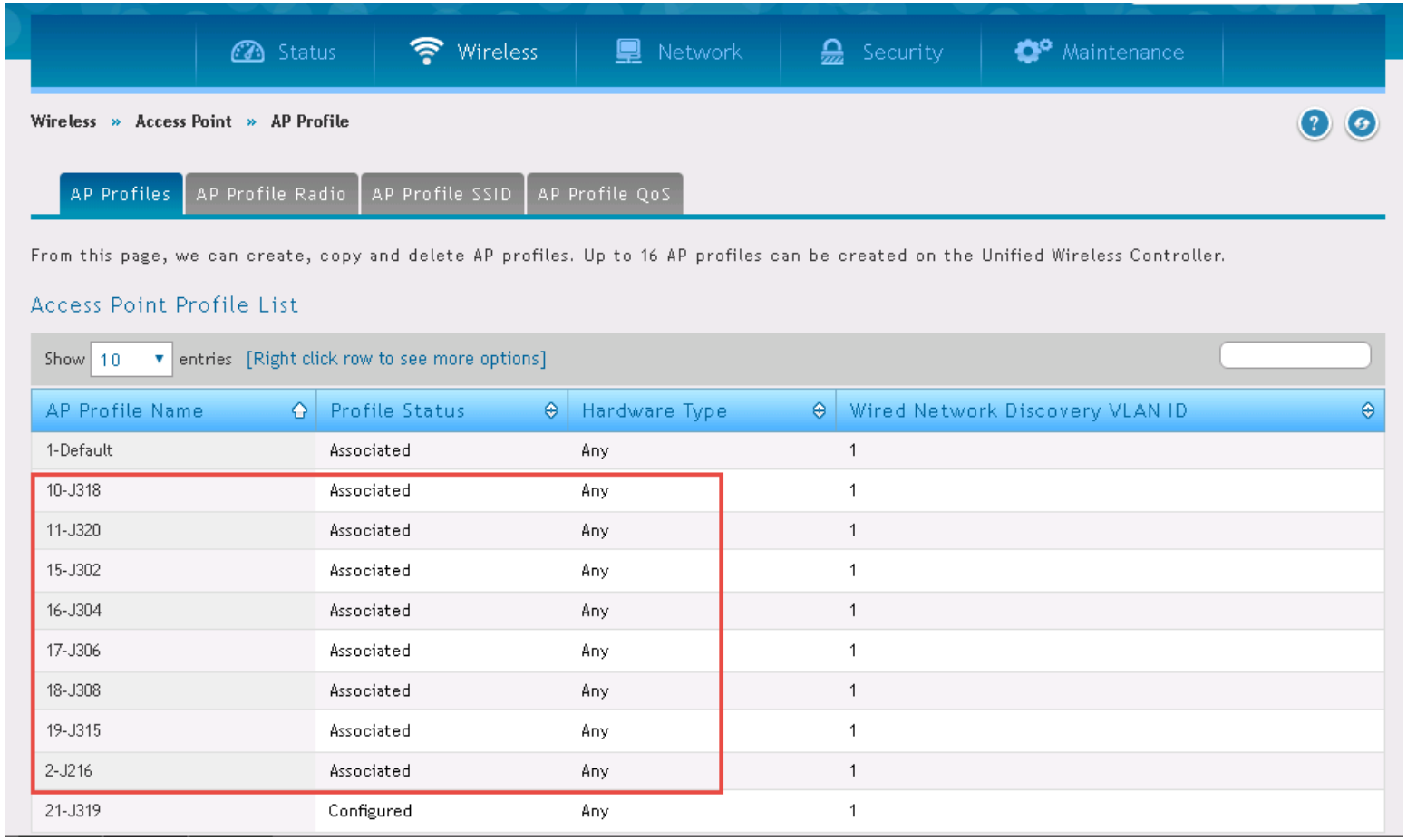
SSID Profile List

Show 25 entries [Right click row to see more options]

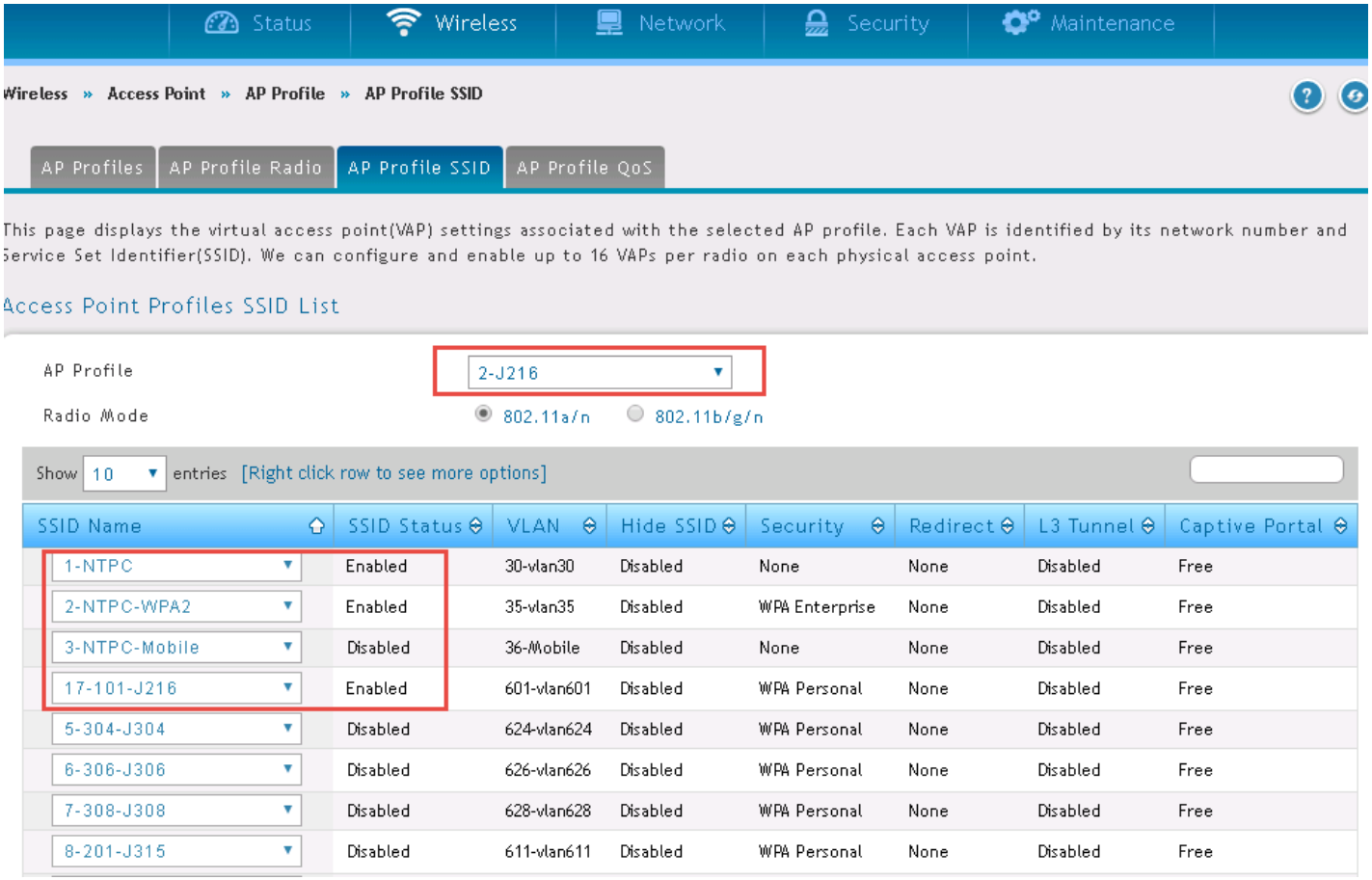
SSID Id	Name	VLAN	Hide SSID	Security	Redirect	L3 Tunnel	Captive Portal	Authentication Server
1	NTPC	30-vlan30	Disabled	None	None	Disabled	Free	None
2	NTPC-WPA2	35-vlan35	Disabled	WPA ENTERPRISE	None	Disabled	Free	None
3	NTPC-Mobil...	36-Mobile	Disabled	None	None	Disabled	Free	None
4	302-J302	622-vlan622	Disabled	WPA PERSONAL	None	Disabled	Free	None
5	304-J304	624-vlan624	Disabled	WPA PERSONAL	None	Disabled	Free	None
6	306-J306	626-vlan626	Disabled	WPA PERSONAL	None	Disabled	Free	None
7	308-J308	628-vlan628	Disabled	WPA PERSONAL	None	Disabled	Free	None
8	201-J315	611-vlan611	Disabled	WPA PERSONAL	None	Disabled	Free	None
9	203-J317	613-vlan613	Disabled	WPA PERSONAL	None	Disabled	Free	None
10	205-J319	615-vlan615	Disabled	WPA PERSONAL	None	Disabled	Free	None
11	207-J321	617-vlan617	Disabled	WPA PERSONAL	None	Disabled	Free	None
12	209-J323	619-vlan619	Disabled	WPA PERSONAL	None	Disabled	Free	None
13	dlink13	1-Default	Disabled	None	None	Disabled	Free	None
14	dlink14	1-Default	Disabled	None	None	Disabled	Free	None
15	dlink15	1-Default	Disabled	None	None	Disabled	Free	None
16	dlink16	1-Default	Disabled	None	None	Disabled	Free	None


SSID Profile Configuration
SSID
302-J302
Captive Portal Type
Free
Login Profile Name
default
Create a Profile
Hide SSID
OFF
Ignore Broadcast
OFF
VLAN
622
[Range: 1 - 4093]
L3 Tunnel
OFF
L3 Tunnel Status
Not Configured
MAC Authentication
Local
Radius
Disable
Redirect
None
HTTP
Save

- 設定 AP profile.



- 把SSID拉進去匹配的AP profile



- 納管AP, 每台AP用不同的AP profile.