

新北市校園有線網路實作研習

網管輔導員:李 煒
助教: **ERIC、DANIEL**
alfred@ntpc.edu.tw
80723456-517

課程問題及時提問slido

2

請開網頁
slido.com
#17962



課程進行互動方式

3

- 若是操作**Lab**過程有疑問，請務必直接**slido**發問。
- 我們的**Lab**為漸進式，**前後相關**。因此要與同組一同討論。兩人做一個**Lab**也是ok。
- 課程中隨時**slido**問問題，有疑問就直接**slido**。

網管組業務職掌

4

- 1、教育局所屬各級學校實體及無線網路規劃與建置。
- 2、新北市教育學術網路(TANet)骨幹及各級學校網路維運、監控、管理、分析與統計。
- 3、提供VPN、NLB等各項網路基礎服務。
- 4、集中式防火牆及不當入侵防禦系統規劃與管理。
- 5、各級學校集中式防毒軟體維運及管理。
- 6、教育網路中心內部網路環境管理。

網管組相關專業證照

5

- CHFI
 - Computer Hacking Forensic Investigator
- 資安證照 ISO27001 LAC
- 個資證照 BS10012 LAC
- NSPA
 - Network Security of Packet Analysis



這門課程內容涵蓋那些網管知識？



- 電腦上網設定
 - TCP/IP網路概論
 - DNS基本原理
 - DHCP基本原理
- L2交換器
 - 有線網路接線
 - 網路訊框frame基本概念
 - ✦ Broadcast
 - VLAN
 - ✦ Access、trunk、trunk native.
- L3路由器
 - ✦ 閘道 Gateway (vlan interface)
 - ✦ 靜態路由原理
 - ✦ DHCP forward
- 無線網路
- VPN基本原理
 - ✦ Tunnel mode
 - ✦ Splite Tunnel
- 網路認證
 - ✦ radius基本原理
 - ✦ eduroam
- 電腦及網路安全
 - ✦ KMS and 授權網站
 - ✦ 弱點掃描

課程安排

7

● 8/13

- PC網路設定
- PC基本網路設定及問題除錯
- 基礎服務介紹及實作：DNS、DHCP、VPN、Radius
- L2 Switch基本介紹及運用實作
- **L2 switch Vlan**原理及實作
- L3 Switch Routing (ipv4 and ipv6)

● 8/14

- Wireless路由 (NTPC、NTPC-WPA2、NTPC-Mobile、**class**)
 - ✦ **Acom**認證實作
- 繪製校園網路拓譜圖。
- 架設及設定建置自己學校之校園網路實作。
- 前瞻案**CISCO WLC**控制及設計一個符合校園的無線網路環境。
- 設備弱掃，找出自己架設校網伺服器的漏洞及弱點。

個人PC網路設定

8

- 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 -d
 - route print

IP Address

9

- A.B.C.D 0-255
- NetMask 遮罩
- Gateway
- DNS
- DHCP
- IPv6

The screenshot displays the Windows Network and Sharing Center. The main window shows the network status for 'ALFRED-PC (這部電腦)'. It indicates that the network is connected via a wireless adapter (TP-LINK_POCKET_3020_75EAA). Below this, two windows are open:

無線網路連線 狀態 (Wireless Network Connection Status):

- 連線 (Connection): 網際網路 (Internet)
- IPv4 連線能力 (IPv4 Connectivity): 網際網路 (Internet)
- IPv6 連線能力 (IPv6 Connectivity): 無網際網路存取 (No Internet Access)
- 媒體狀態 (Media Status): 已啟用 (Enabled)
- SSID: TP-LINK_POCKET_3020_75EAA
- 連線時間 (Connection Time): 6 天 23:46:20
- 速度 (Speed): 54.0 Mbps
- 訊號品質 (Signal Quality): 良好 (Good)
- 活動 (Activity): 已傳送 (Sent) 3,010,963 位元組; 已收到 (Received) 58,196,206 位元組

網路連線詳細資料 (Network Connection Details):

| 內容 (Content) | 值 (Value) |
|---|---------------------------------------|
| 連線特定 DNS 尾碼 (Connection-specific DNS Suffix) | |
| 描述 (Description) | Intel(R) PRO/Wireless 2200BG Netwo... |
| 實體位址 (Physical Address) | 00-13-CE-05-AD-60 |
| DHCP 已啟用 (DHCP Enabled) | 是 (Yes) |
| IPv4 位址 (IPv4 Address) | 192.168.0.106 |
| IPv4 子網路遮罩 (IPv4 Subnet Mask) | 255.255.255.0 |
| 已取得租約 (Obtained IP Address) | 2015年11月1日 下午 06:38:04 |
| 租約到期 (Lease Expires) | 2015年11月1日 下午 09:38:03 |
| IPv4 預設閘道 (IPv4 Default Gateway) | 192.168.0.254 |
| IPv4 DHCP 伺服器 (IPv4 DHCP Server) | 192.168.0.254 |
| IPv4 DNS 伺服器 (IPv4 DNS Server) | 192.168.0.254 |
| IPv4 WINS 伺服器 (IPv4 WINS Server) | |
| NetBIOS over Tcpip 已... (NetBIOS over TCP/IP Enabled) | 是 (Yes) |
| 連結-本機 IPv6 位址 (Link-local IPv6 Address) | fe80::01b:786:90fa:49ee%11 |
| IPv6 預設閘道 (IPv6 Default Gateway) | |
| IPv6 DNS 伺服器 (IPv6 DNS Server) | |

實體PC 網路設定

控制台 > 所有控制台項目 > 網路和共用中心

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

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

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: 3,010,963
- 已收到: 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):

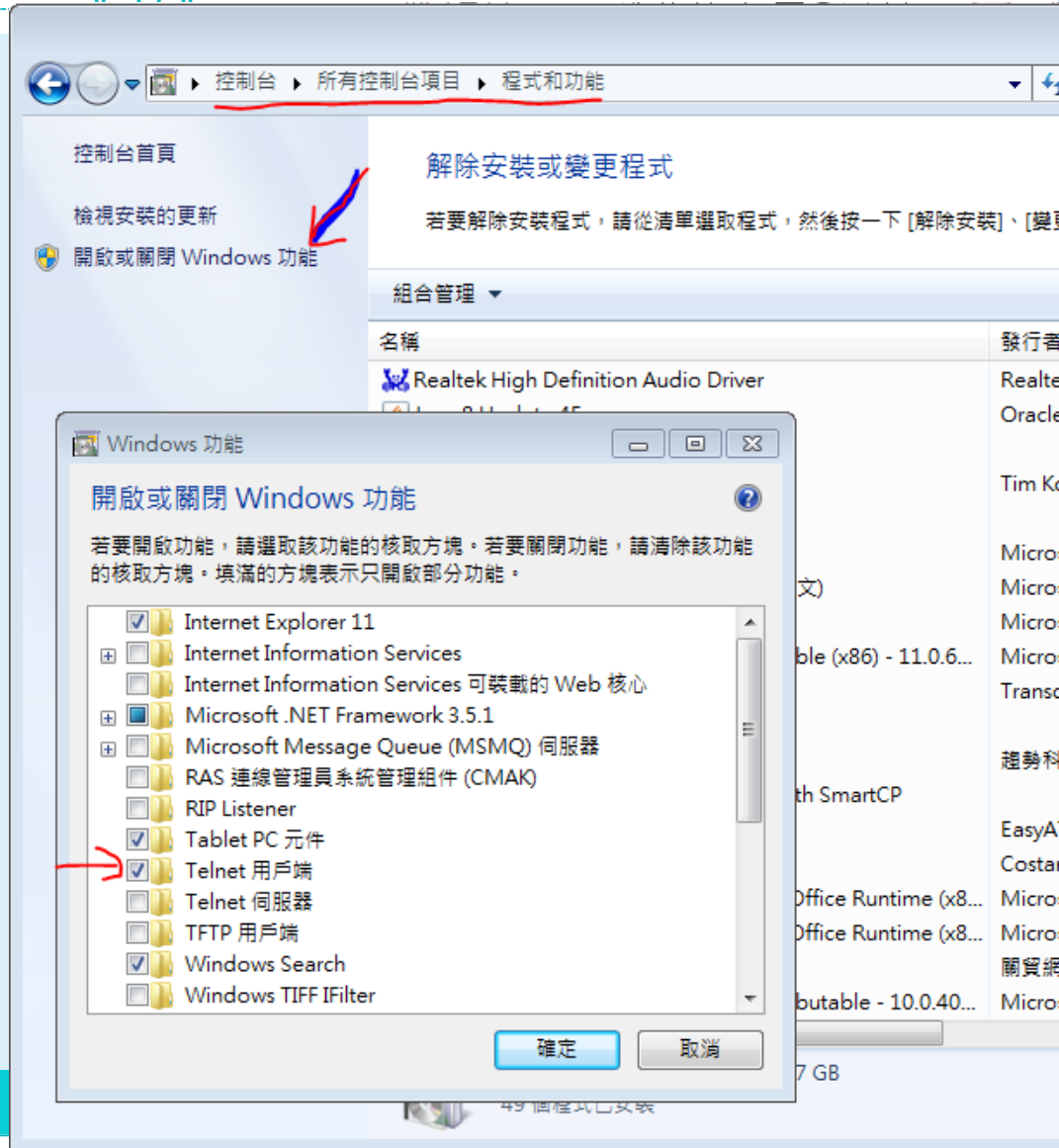
| 內容 | 值 |
|-------------------------|--------------------------------------|
| 連線特定 DNS 尾碼 | |
| 描述 | Intel(R) PRO/Wireless 2200BG Netw... |
| 實體位址 | 00-13-CE-05-AD-60 |
| DHCP 已啟用 | 是 |
| IPv4 位址 | 192.168.0.106 |
| IPv4 子網路遮罩 | 255.255.255.0 |
| 已取得租約 | 2015年11月1日 下午 06:38:04 |
| 租約到期 | 2015年11月1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

11

- 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`



電腦開機程序及網頁開啟行為

12

- 電腦開機程序
 - 找尋DHCP server
 - DHCP取得ip、netmask、gateway、dns
 - 自訂ip、netmask、gateway、dns
- 網頁開啟行為
 - 向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

模擬器操作教學Lab簡介

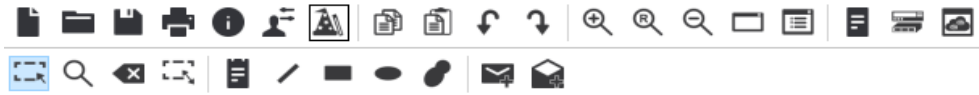
13

- 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中可模擬DHCP、Radius Server

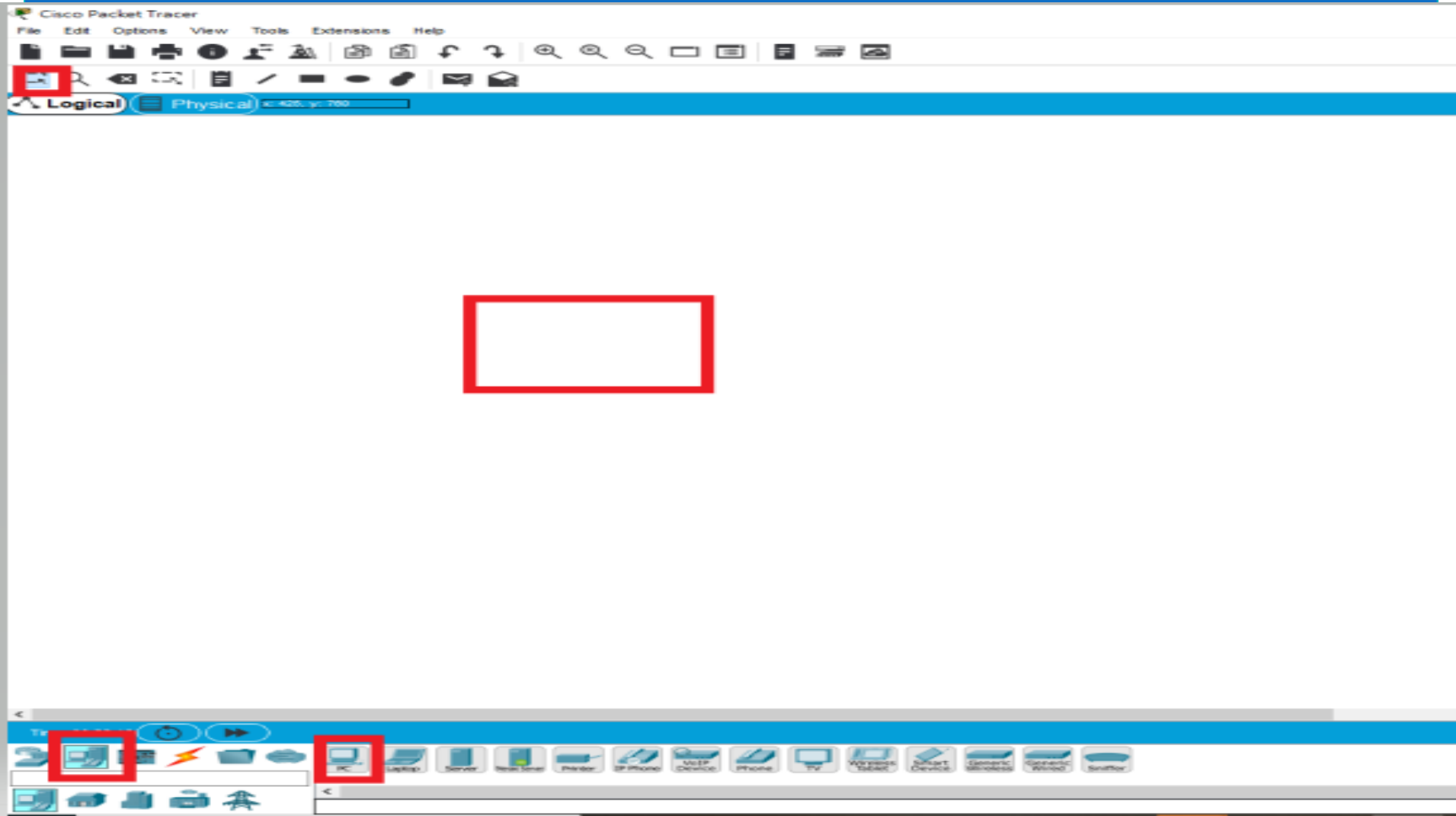
Packet Tracer基本使用介紹

14

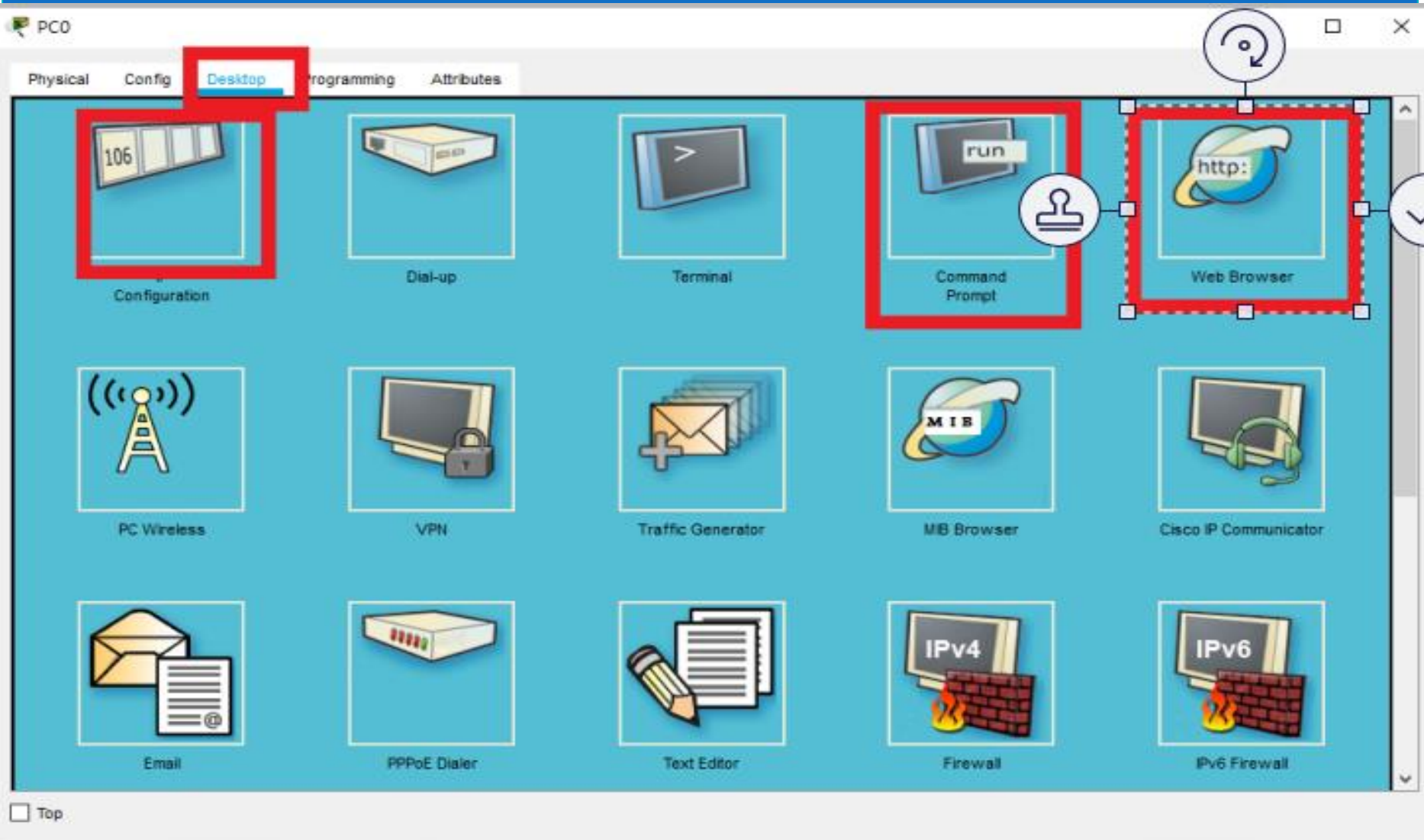
- CISCO原廠開發
- 提供cisco wlc controller、CCNA、CCNP考試用
- 可以模擬大部分狀況
- 使用簡單易懂



模擬PC網路設定



設定PC網路



Physical **Config** Desktop Programming Attributes

GLOBAL

Settings

Algorithm Settings

FastEthernet0

FastEthernet0

Port Status On
Bandwidth 100 Mbps 10 Mbps Auto
Duplex Half Duplex Full Duplex Auto
MAC Address 0060.5C10.1A62

IP Configuration

- DHCP
- Static

IP Address

Subnet Mask

IPv6 Configuration

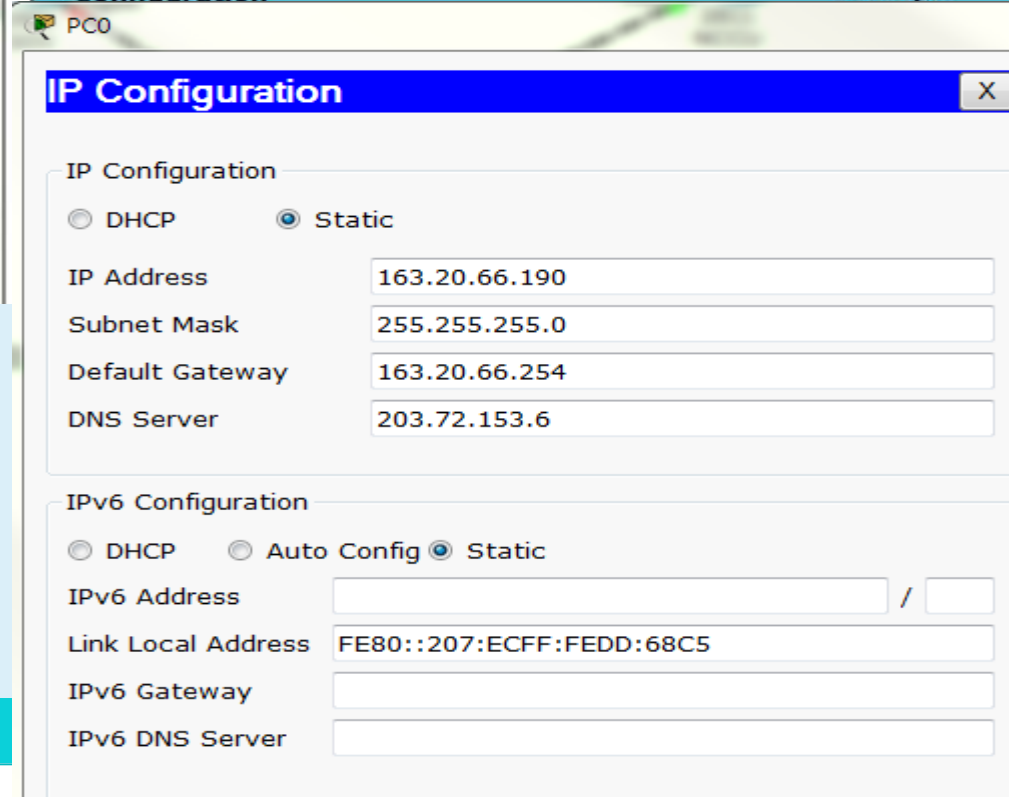
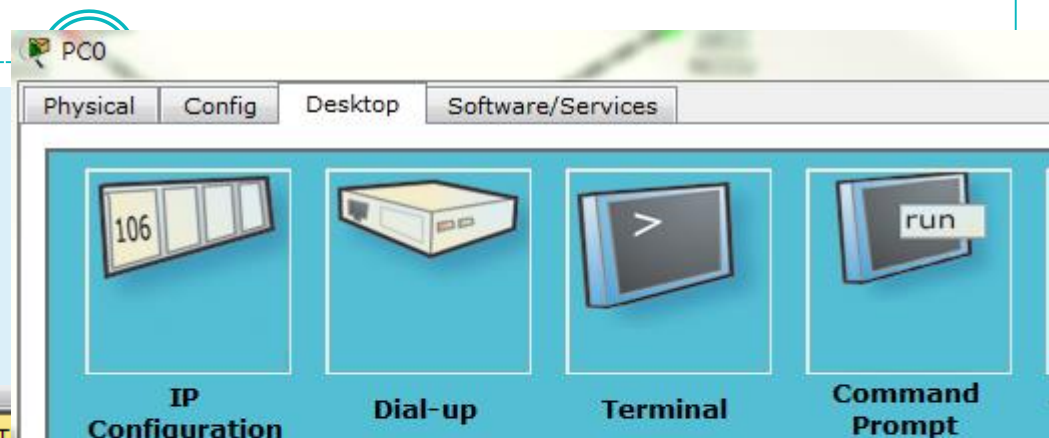
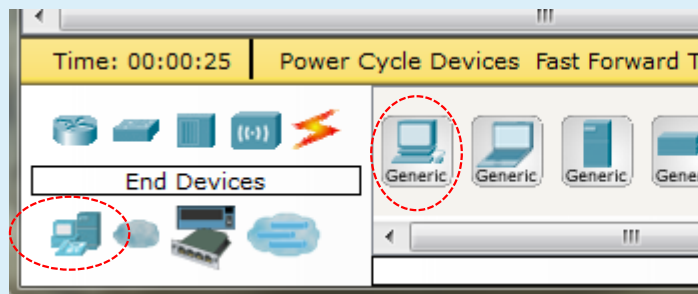
- DHCP
- Auto Config
- Static

IPv6 Address

Link Local Address: FE80::260:5CFF:FE10:1A62

Lab 1 PC 設定

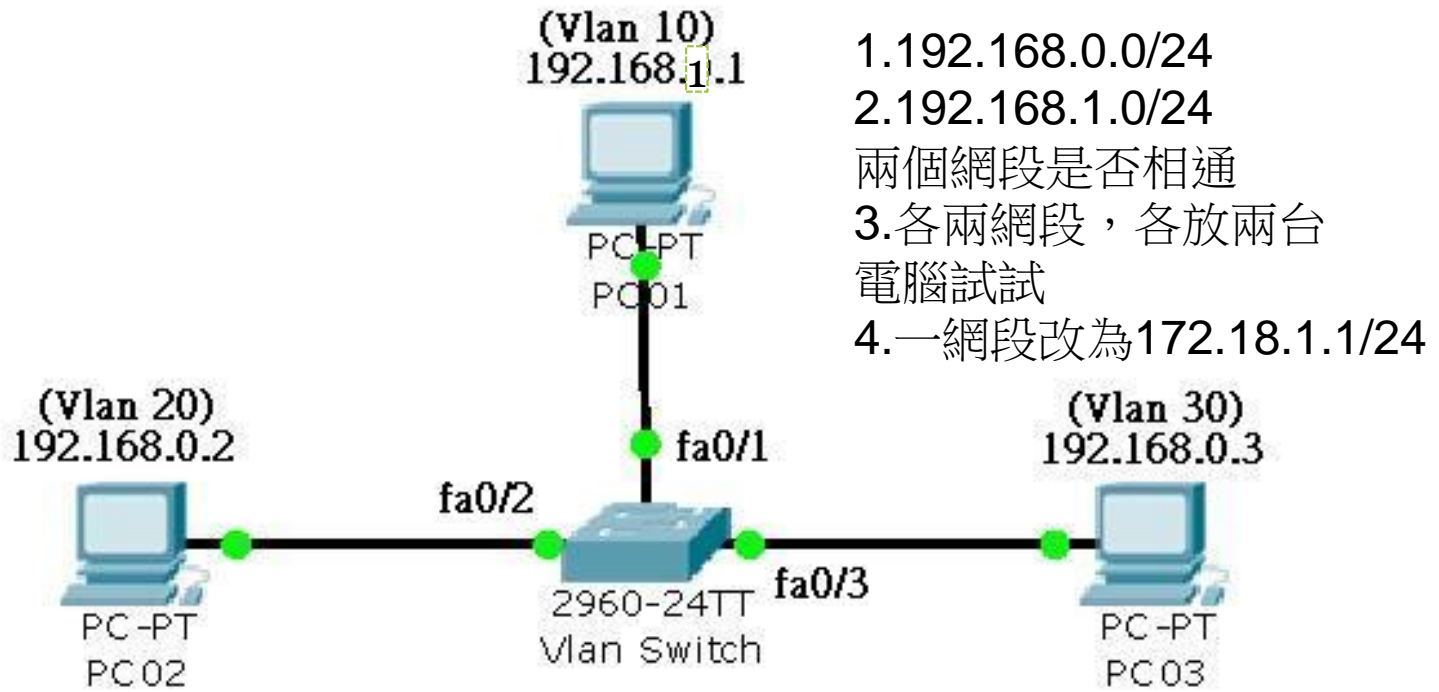
- Packet Tracer
- PC 設定、使用



Lab 3-1 基本練習Hub、L2、家用AP (NetMask)

20

三台 PC 三個網段、同網段可通、不同網段不通



家用無線AP設定

21

設定分為三部分

WAN IP (internet)
對外連線

LAN IP
內部有線

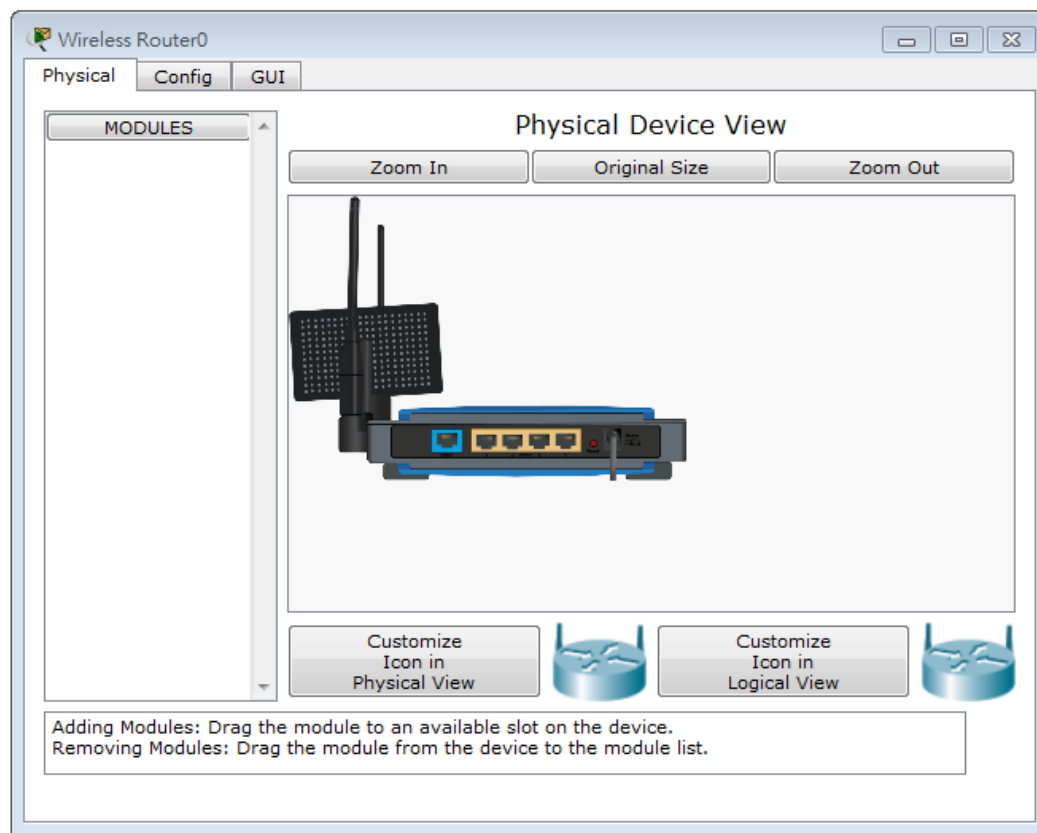
Wireless
內部無線

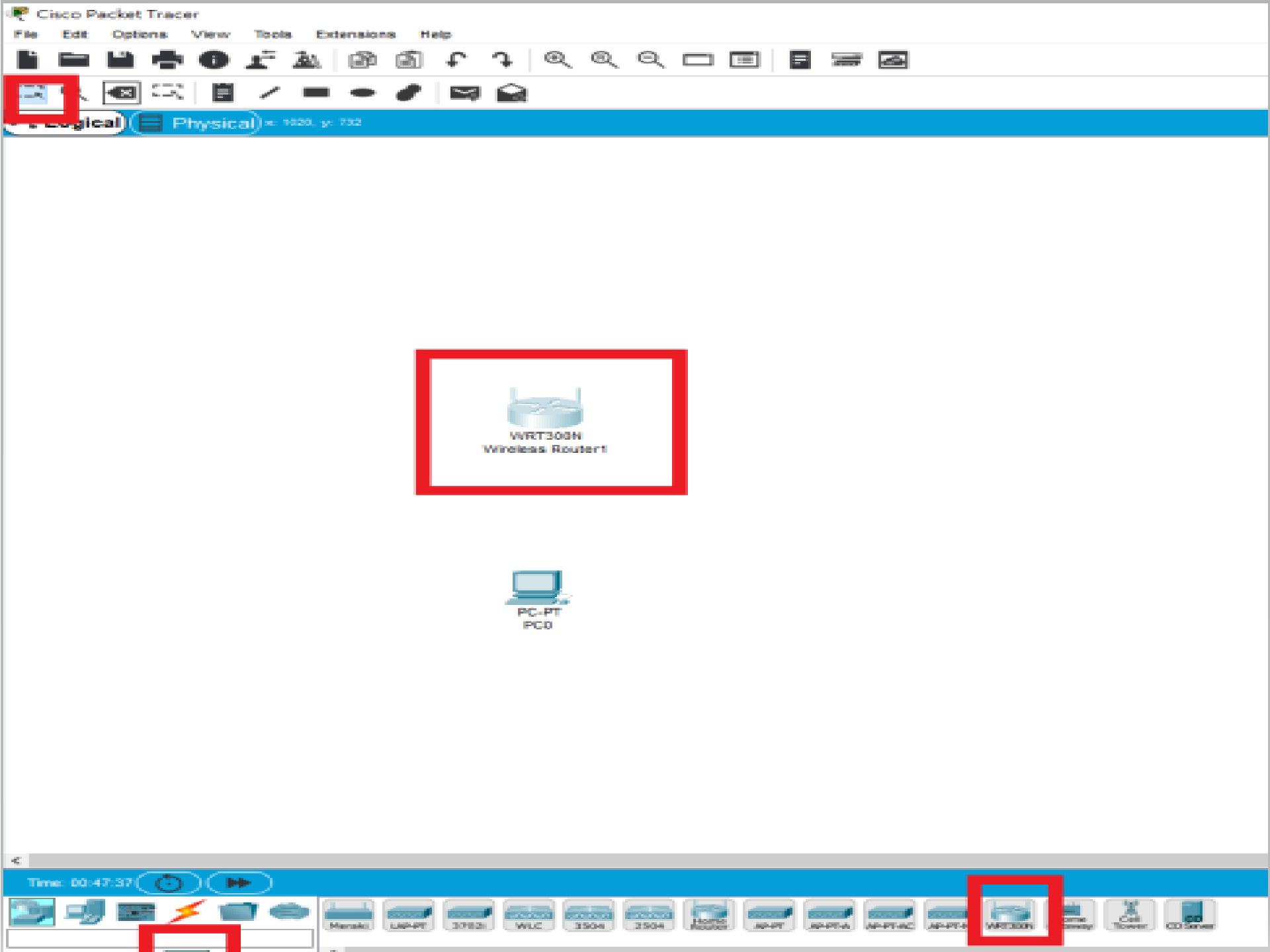
SSID

WPA2

Preshare key

Radius server





Wireless-N Broadband Router

Firmware Version: v0.93.3

Setup

Setup

Wireless

Security

**Access
Restrictions****Applications
& Gaming**

Administration

Wireless-N Broadband Router

WRT300N

Status

Basic Setup

DDNS

MAC Address Clone

Advanced Routing

Internet SetupInternet
Connection type

Automatic Configuration - DHCP ▾

Optional Settings
(required by some
internet service
providers)Host Name: Domain Name: MTU: Size: 1500[Help...](#)**Network Setup**

Router IP

IP Address: 192 168 0 1Subnet Mask: 255.255.255.0 ▾DHCP Server
SettingsDHCP Server: Enabled DisabledDHCP
ReservationStart IP Address: 192.168.0. 100Maximum 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 0Static DNS 2: 0 0 0 0Static DNS 3: 0 0 0 0WINS: 0 0 0 0

- GLOBAL
 - Settings
 - Algorithm Settings
- INTERFACE
 - Internet**
 - LAN
 - Wireless

Internet Settings

IP Configuration

- DHCP
- Static
- PPPoE

UserName

Password

IP Address

Subnet Mask

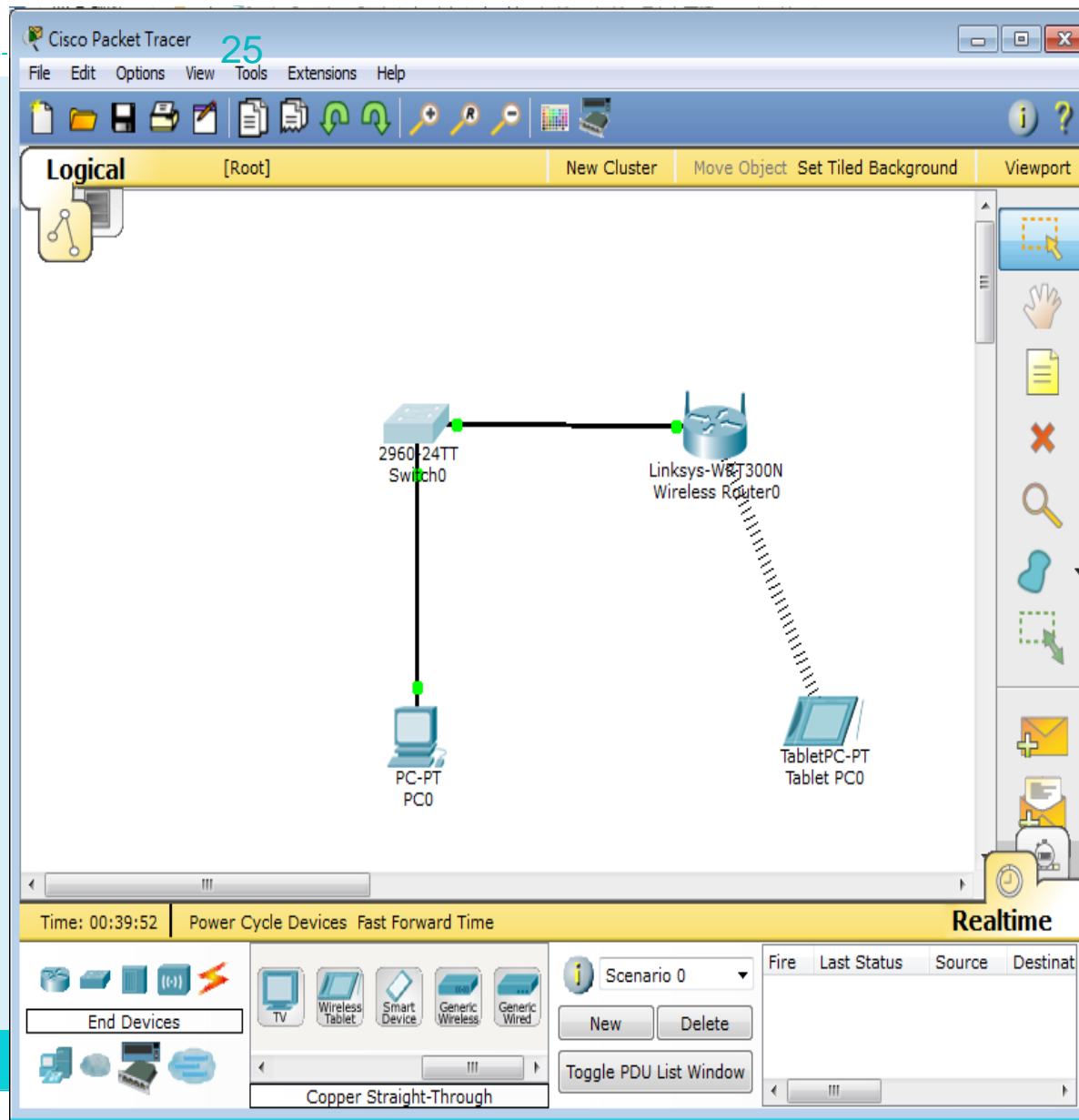
Default Gateway

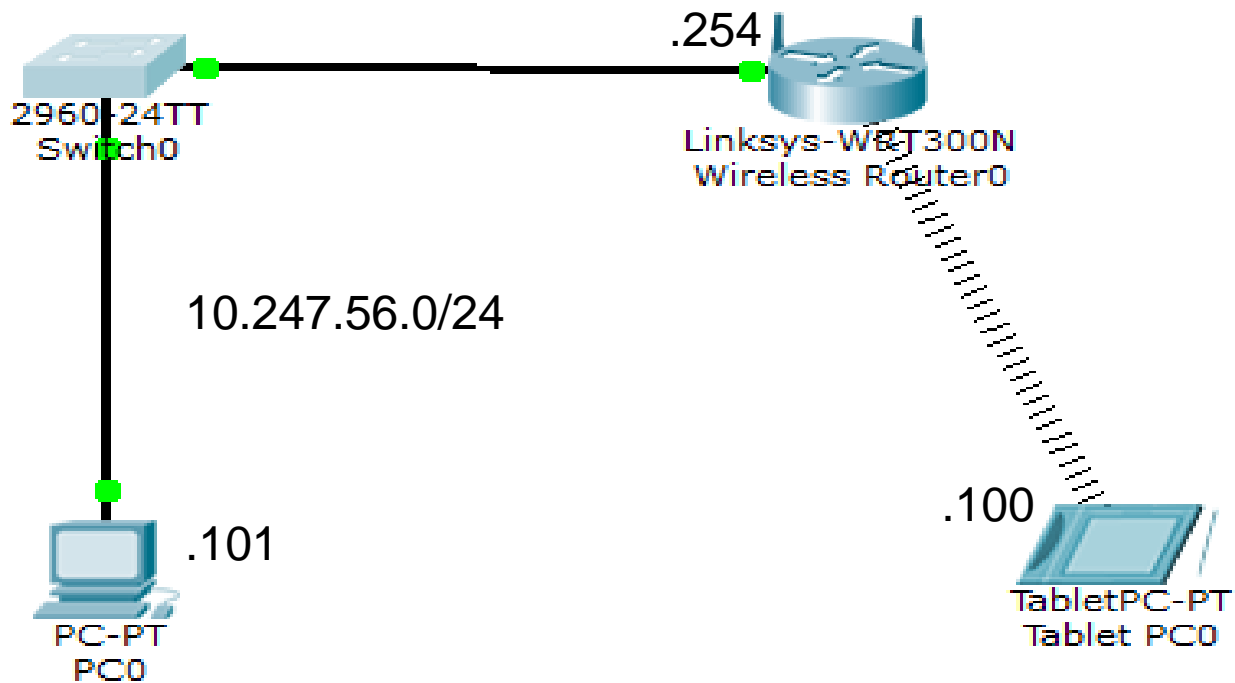
DNS Server

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





TV Wireless Tablet Smart Device Generic Wireless Generic Wired

Scenario 0

New Delete

Fire Last Status Source De

DHCP問題發生原因LAB及排除

27

- 家用無線網路 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mis.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

Daniel Lee

Vlan

29

- Vlan

- 用一台交換器切割虛擬網路，取代多台獨立的hub。
- 用一台交換器切割虛擬網路，隔離多個網段。
- 可以避免廣播風暴。
- 可以透過路由器將各網段連結起來。
- <https://www.youtube.com/watch?v=jC6MJTh9fRE>



VLAN解釋

PowerCert Animated Videos ✓ 觀看次數：53萬次 · 2年前

什麼是VLAN？這是一個動畫視頻，解釋了VLAN是什麼以及它是如何工作的。虛擬局域網。#VLAN

字幕

IEEE 802.1p/802.1q Frame Tagging

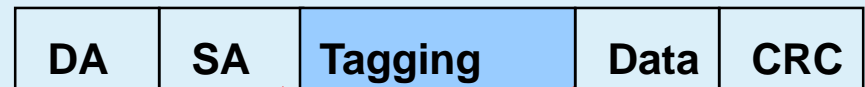
The 32-bit field (VLAN Tag) in the frame header that identifies the frame as belonging to a specific VLAN/priority.

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

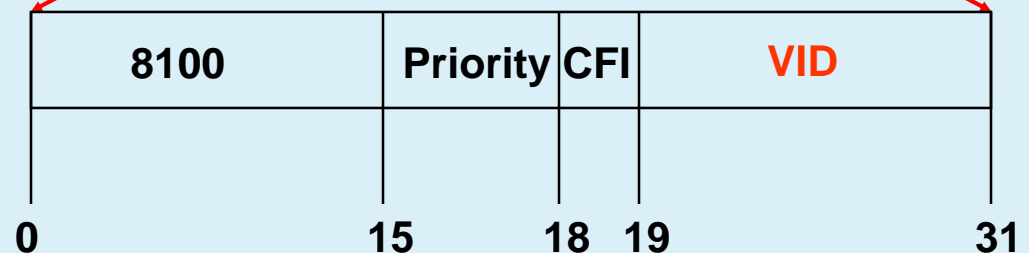
The frame without VLAN tag, we call it as Untagged Frame or Frame.



Regular frame (or untagged frame)



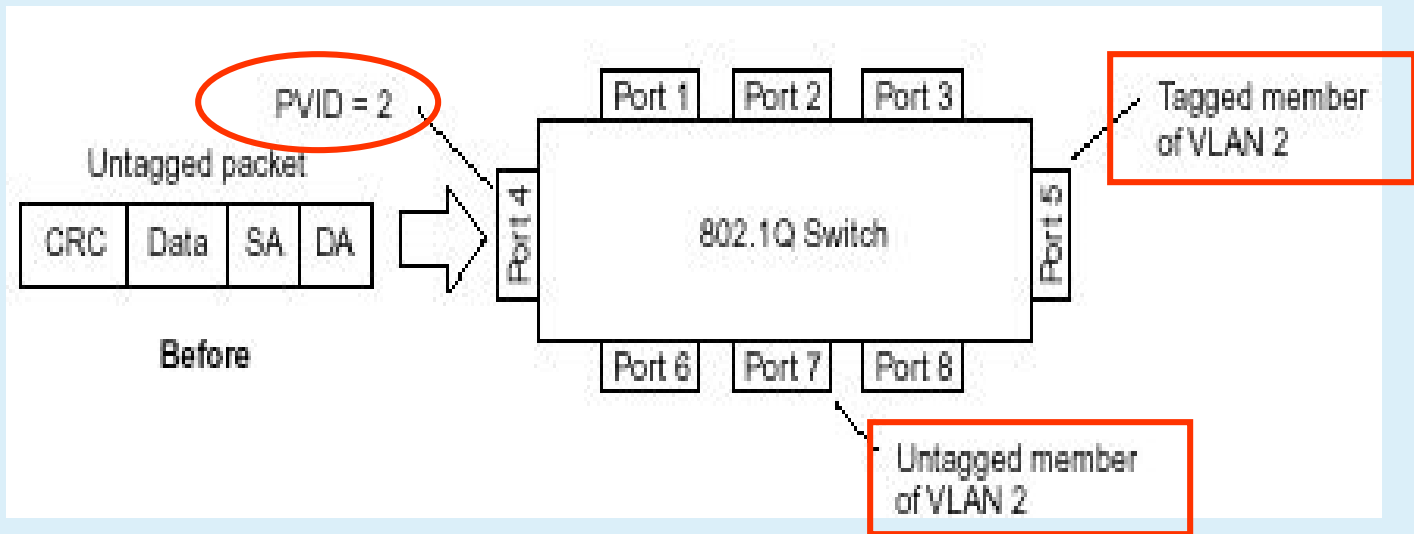
802.1q/1p tagged frame



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

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

802.1p/1q Untagged Incoming Frame



Assumed the PVID of port4 is 2 and default priority=0

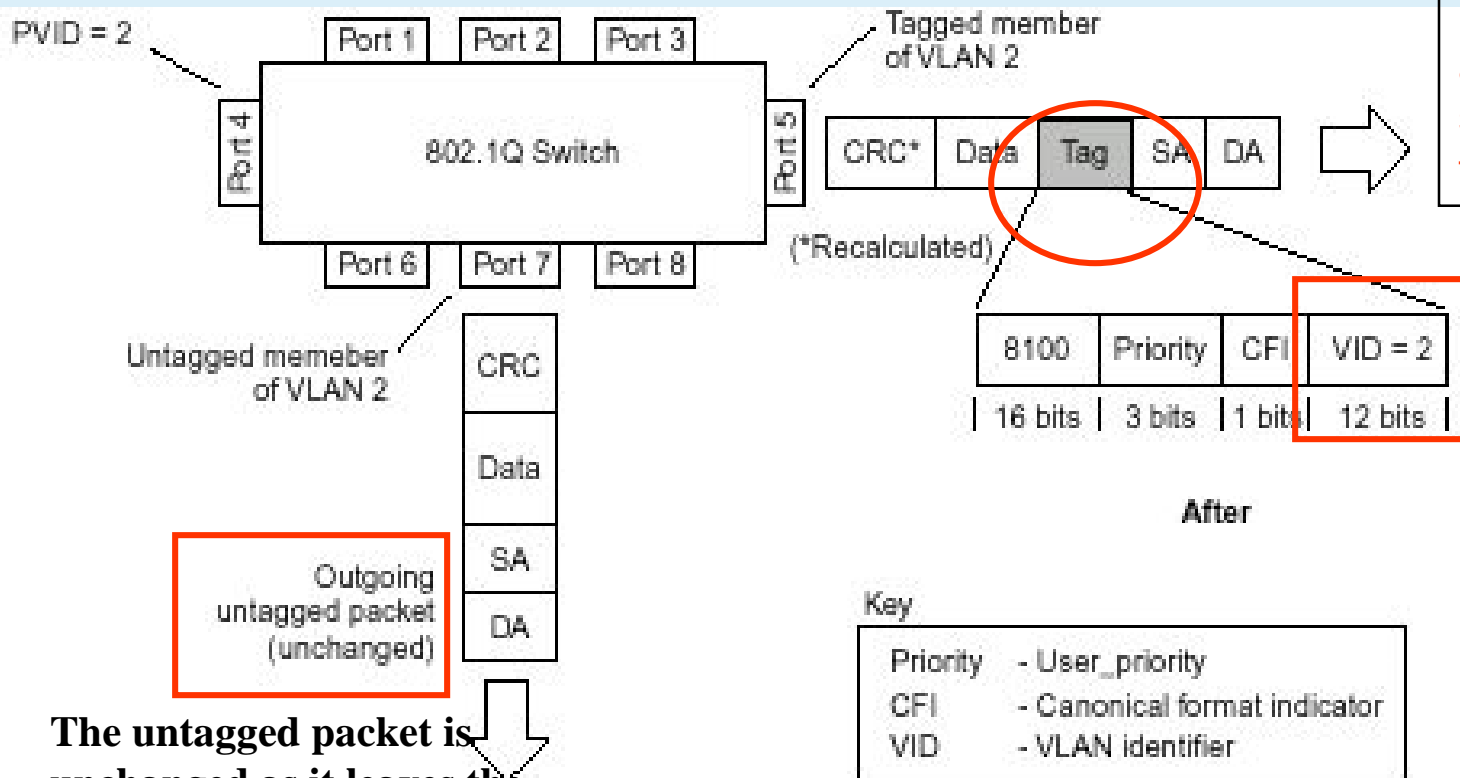
The incoming untagged packet will be assigned to VLAN 2/priority=0

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

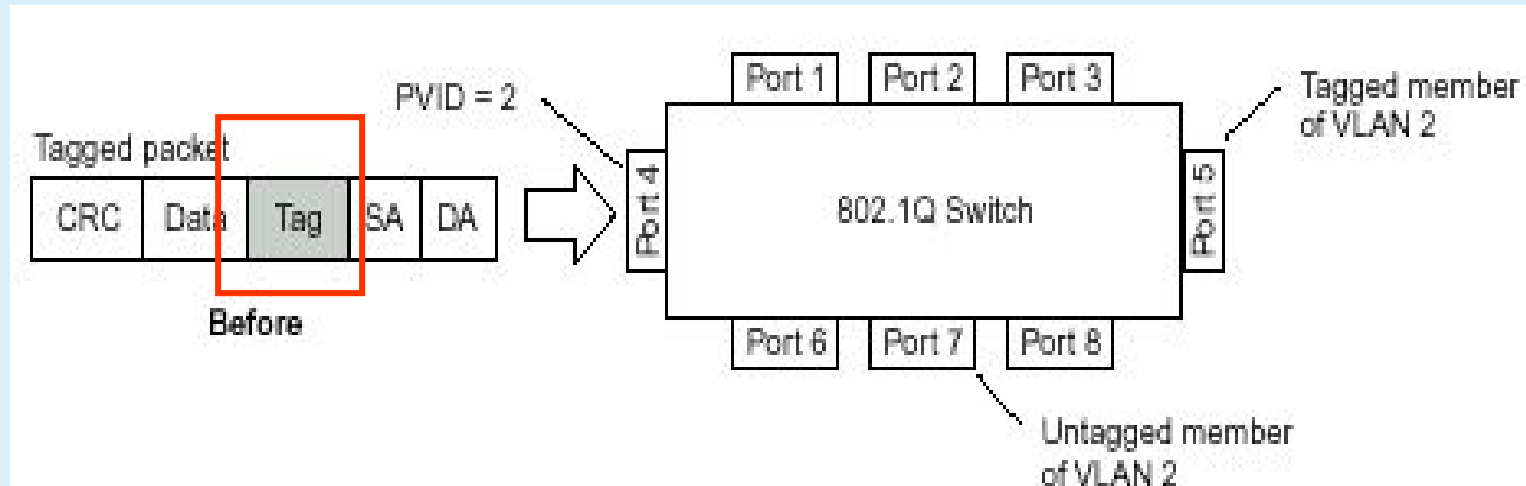


The untagged packet is tagged as it leaves the switch through tagged port

The untagged packet is unchanged as it leaves the untagged port

The VID is related to PVID of the incoming port

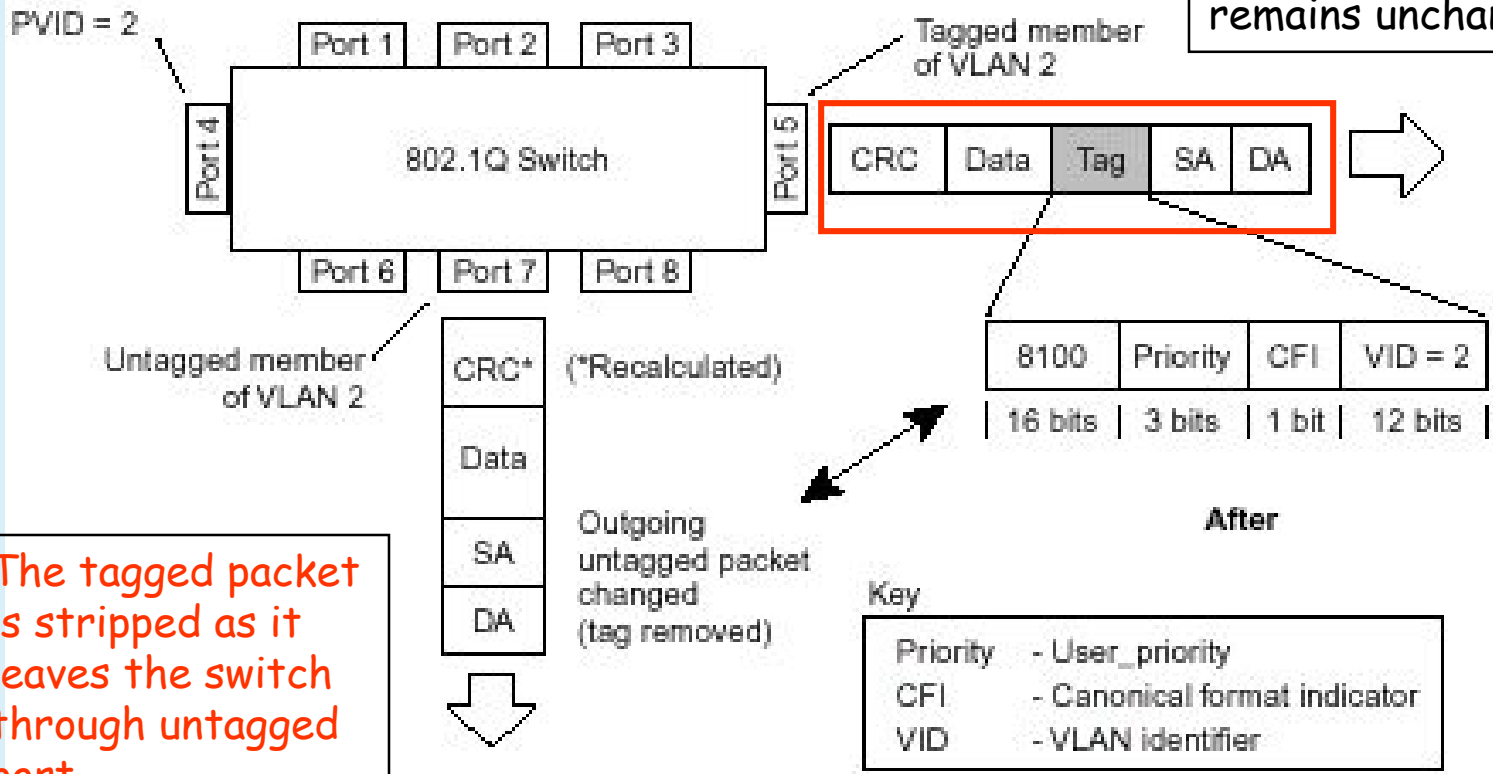
802.1p/1q Tagged Incoming Frame



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

The tagged packet remains unchanged



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

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.

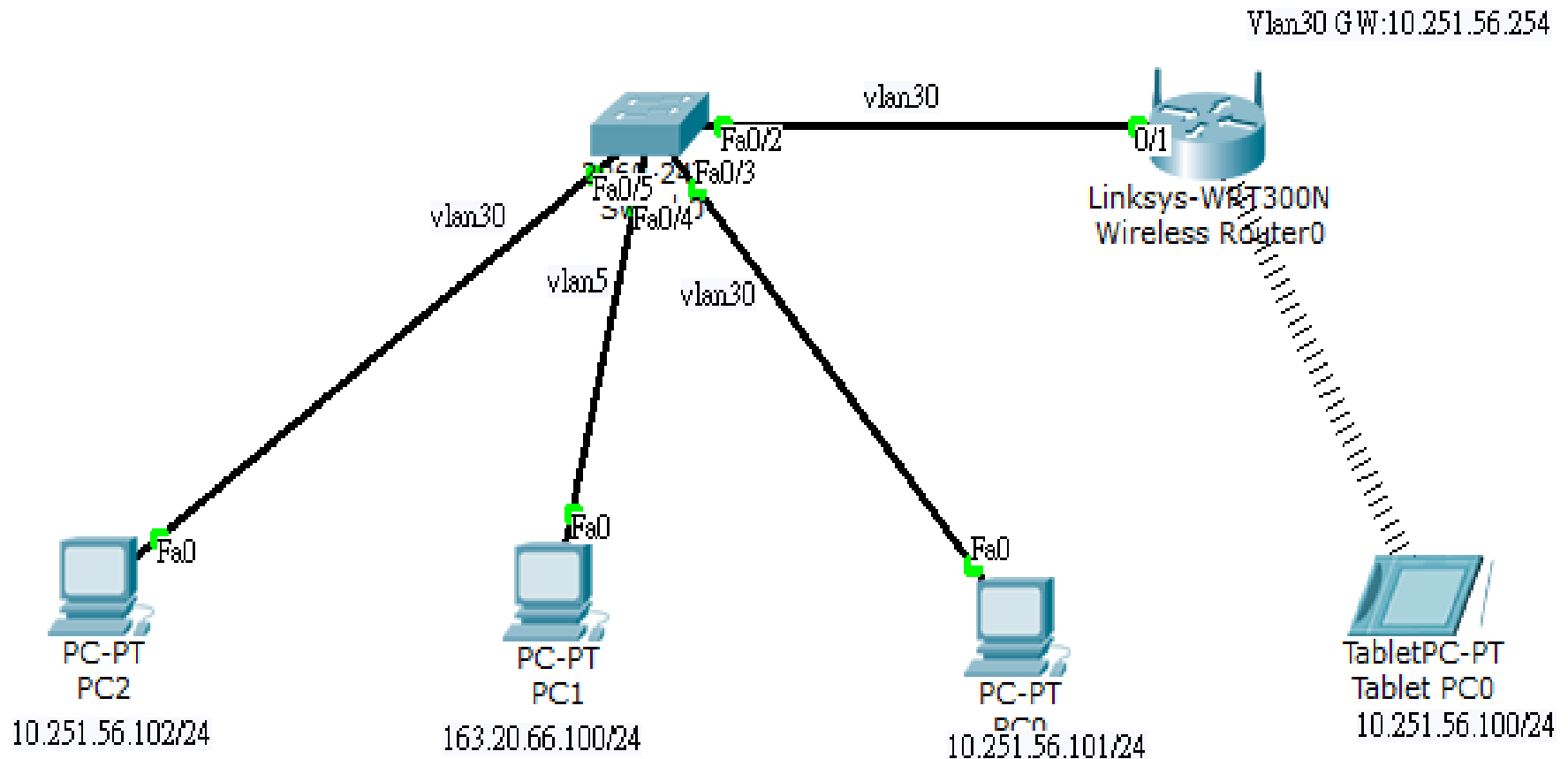
L2 Lab Vlan建置說明

36

- 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

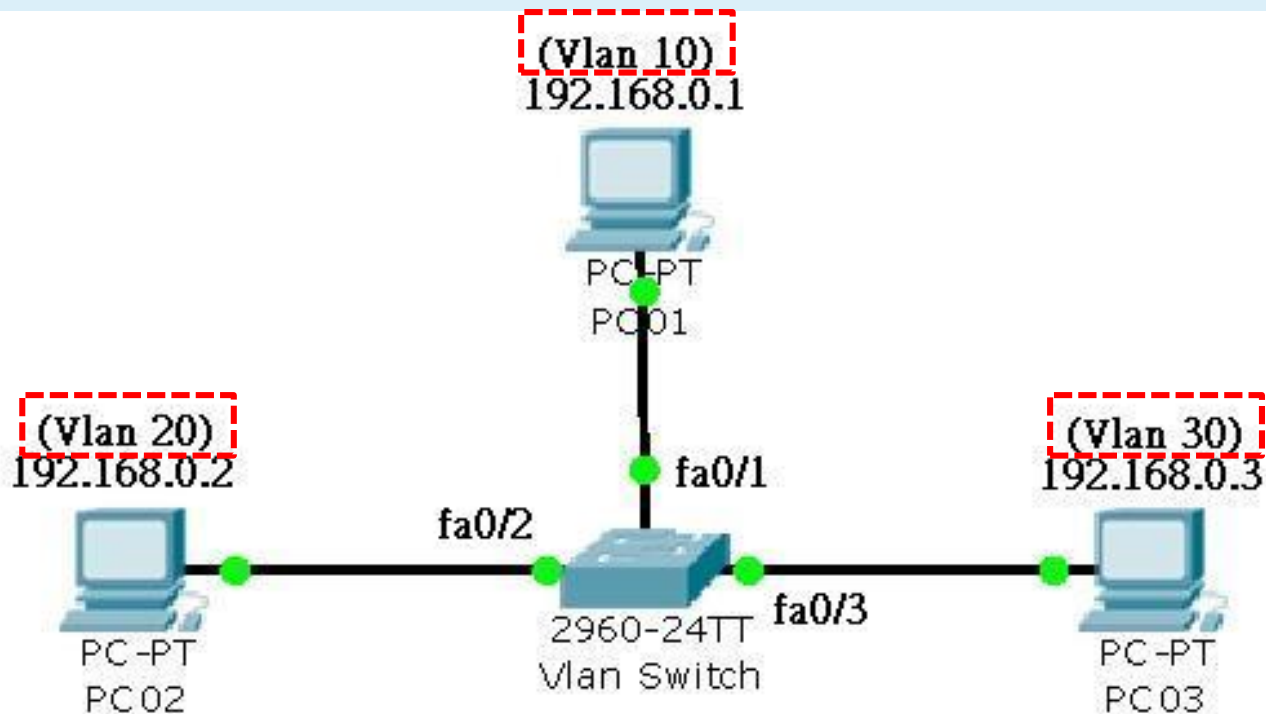
(37)



Lab 3-2 基本練習Vlan

38

三個Vlan間三個網段 PC相互不通(Broadcast Domain)。



山城 城門在哪？

39



Gateway(閘道)

40



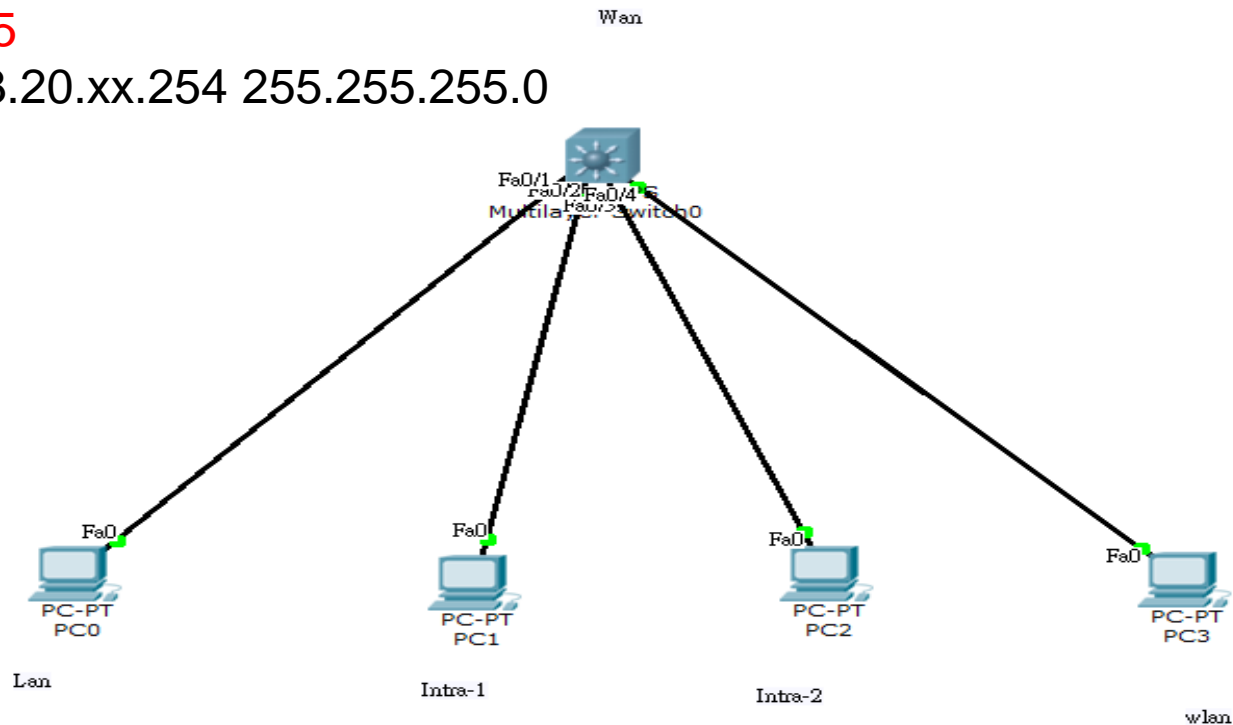
Lab 4 基本練習Vlan Interface

41

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



Radius Server 203.72.154.101 (vlan122)

42

The screenshot displays the ACOM configuration interface for the AAA service. The interface is divided into several sections:

- Services List:** A vertical list on the left includes HTTP, DHCP, DHCPv6, TFTP, DNS, SYSLOG, AAA (highlighted with a red box), NTP, EMAIL, FTP, IoT, VM Management, and Radius EAP.
- AAA Service Configuration:** The main area shows the AAA service is set to "On". The "Radius Port" is configured to "1812".
- Network Configuration:** This section contains input fields for "Client Name", "Client IP", and "Secret". The "ServerType" is set to "Radius". Below this is a table with one entry:

| | Client Name | Client IP | Server Type | Key | |
|---|-------------|-------------|-------------|----------|--|
| 1 | enctc | 10.227.56.1 | Radius | ntpcacom | <input type="button" value="Add"/> <input type="button" value="Save"/> <input type="button" value="Remove"/> |

- User Setup:** This section contains input fields for "Username" and "Password". Below this is a table with two entries:

| | Username | Password | |
|---|----------|----------|--|
| 1 | alfred | 12345678 | <input type="button" value="Add"/> <input type="button" value="Save"/> <input type="button" value="Remove"/> |
| 2 | daniel | 87654321 | |

At the bottom left, there is a "Top" button.

DHCP Server 203.72.153.8 (Vlan121)

43

Physical **Config** Services Desktop Programming Attributes

SERVICES

- HTTP
- DHCP**
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DHCP

Interface: FastEthernet0 Service: On Off

Pool Name: eduroam

Default Gateway: 10.215.56.254

DNS Server: 203.72.153.153

Start IP Address: 10 215 56 100

Subnet Mask: 255 255 255 0

Maximum Number of Users: 156

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

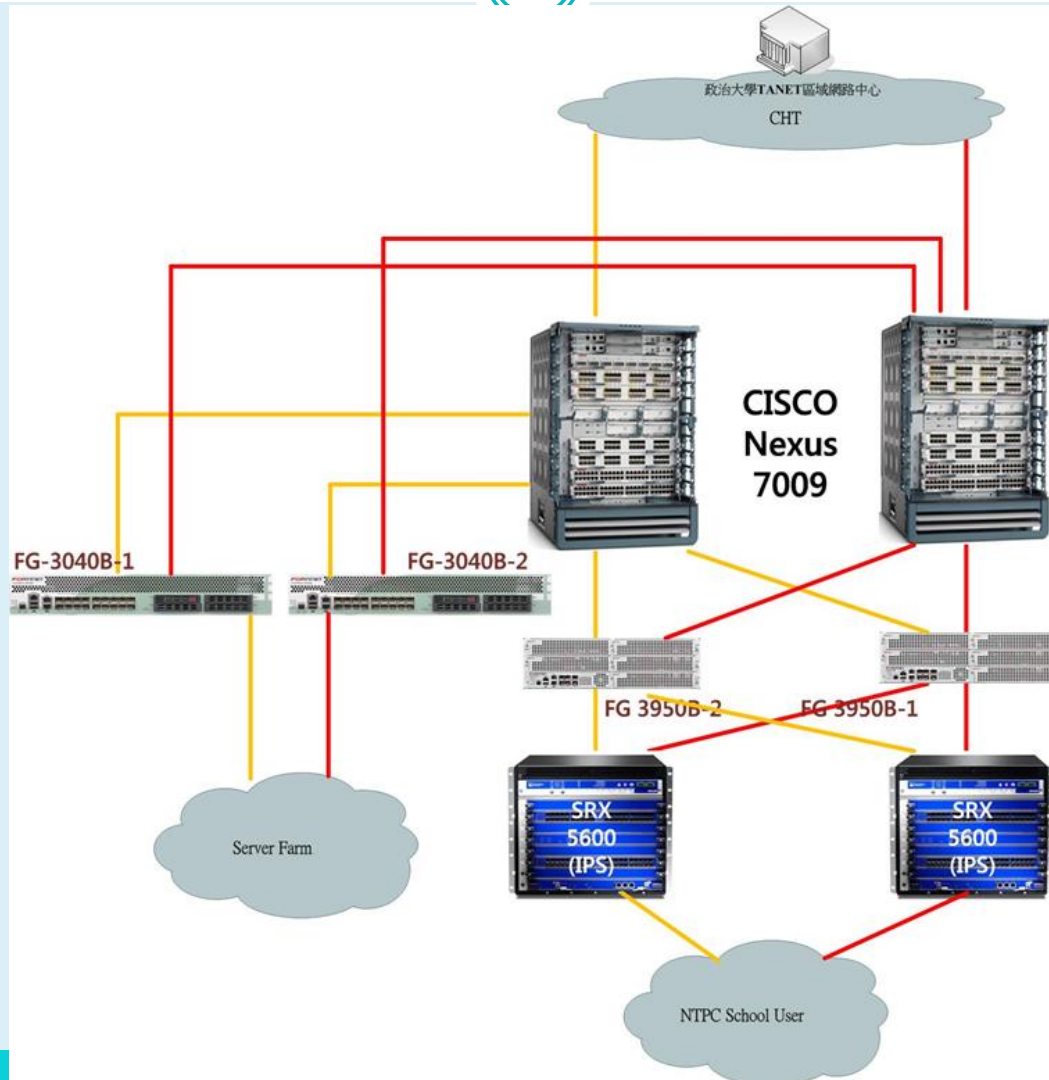
Add Save Remove

| Pool Name | Default Gateway | DNS Server | Start IP Address | Subnet Mask | Max User | TFTP Server | WLC Address |
|----------------|----------------------|-----------------------|----------------------|----------------------|------------|----------------|----------------|
| class | 10.217.56.254 | 203.72.153.153 | 10.217.56.100 | 255.255.255.0 | 100 | 0.0.0.0 | 0.0.0.0 |
| eduroam | 10.215.56.254 | 203.72.153.153 | 10.215.56.100 | 255.255.255.0 | 156 | 0.0.0.0 | 0.0.0.0 |
| Mobile | 10.213.56.254 | 203.72.153.153 | 10.213.56.100 | 255.255.255.0 | 156 | 0.0.0.0 | 0.0.0.0 |
| capwap | 10.227.56.254 | 203.72.153.153 | 10.227.56.100 | 255.255.255.0 | 156 | 0.0.0.0 | 10.227.56.1 |
| serverPool | 0.0.0.0 | 0.0.0.0 | 203.72.153.0 | 255.255.255.0 | 255 | 0.0.0.0 | 0.0.0.0 |

Top

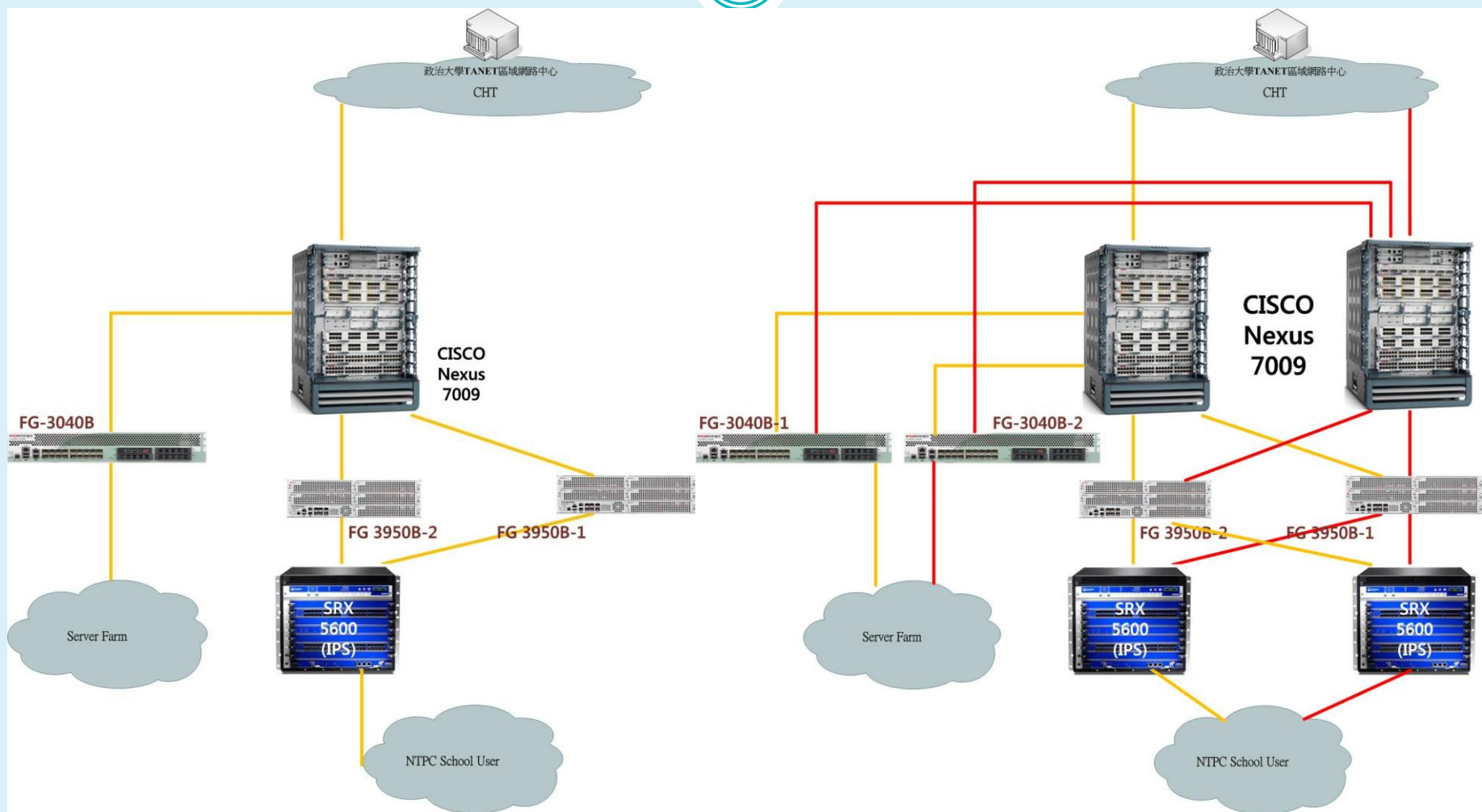
L3 Switch Routing (ipv4 and ipv6)

44



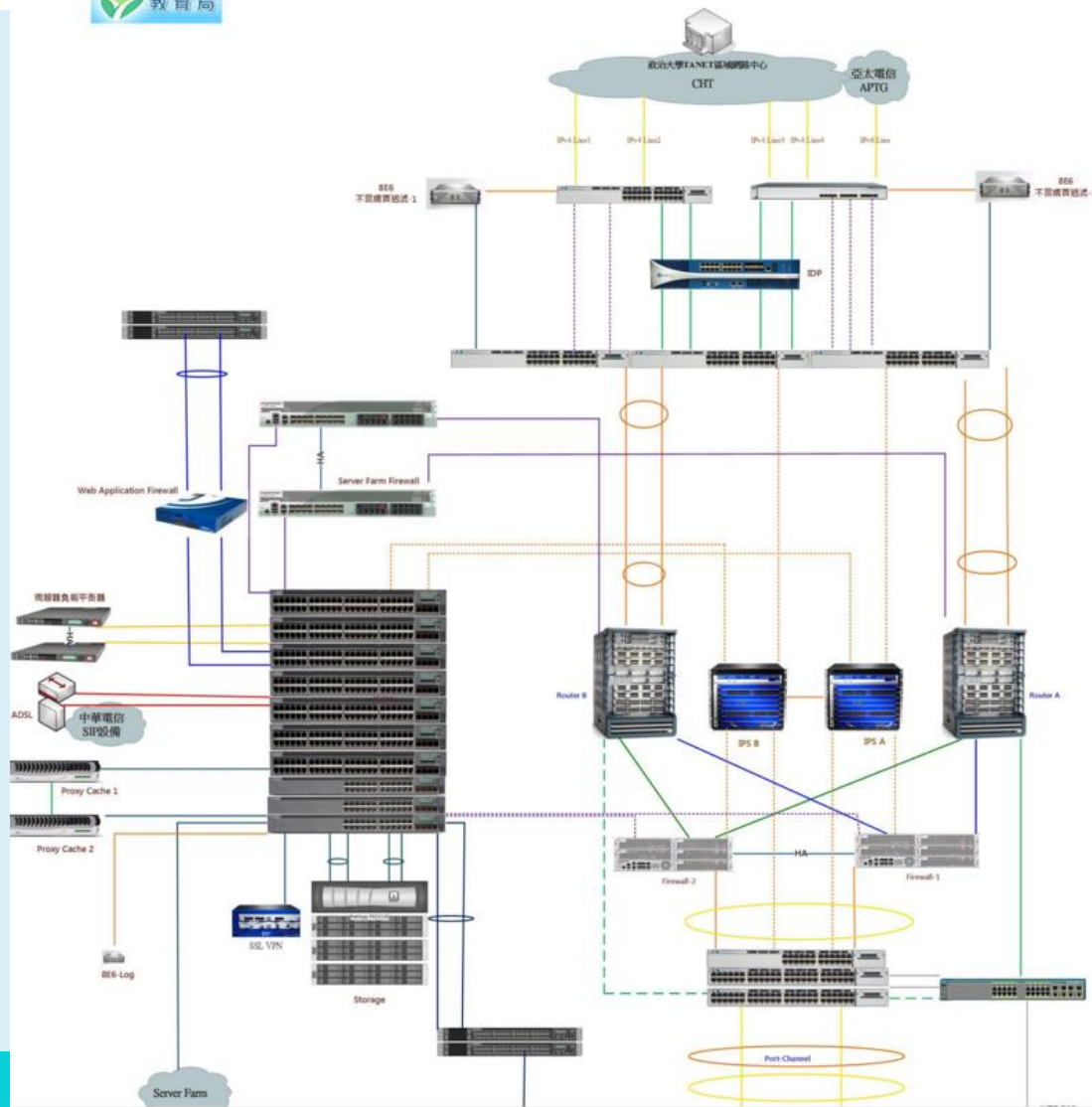
新北市教育網骨幹新舊比較圖

45



新北市拓譜圖

20150327



校園網路Lab拓譜圖

17

貢寮國小:

Gateway:10.229.12.254

LAN:163.20.53.192/24

intra-1: 10.232.12.0/24

intra-2:10.242.12.0/24

VoIP:10.244.12.0/24

無線用31-TANetRoaming:10.212.12.0/24

無線用32-NTPC-Mobile :10.214.12.0/24

無線用33-Eduroam :10.216.12.0/24

無線用34-class:10.218.12.0/24

WLC:10.229.12.1/24

admin/Admin123

DNS:203.72.153.153/24

DHCP:203.72.153.8

Acom:203.72.154.101

VLAN3-WLC

VLAN5-LAN

VLAN10-intra-1

VLAN20-intra-2

VLAN25-VOIP

VLAN31-TANetRoaming

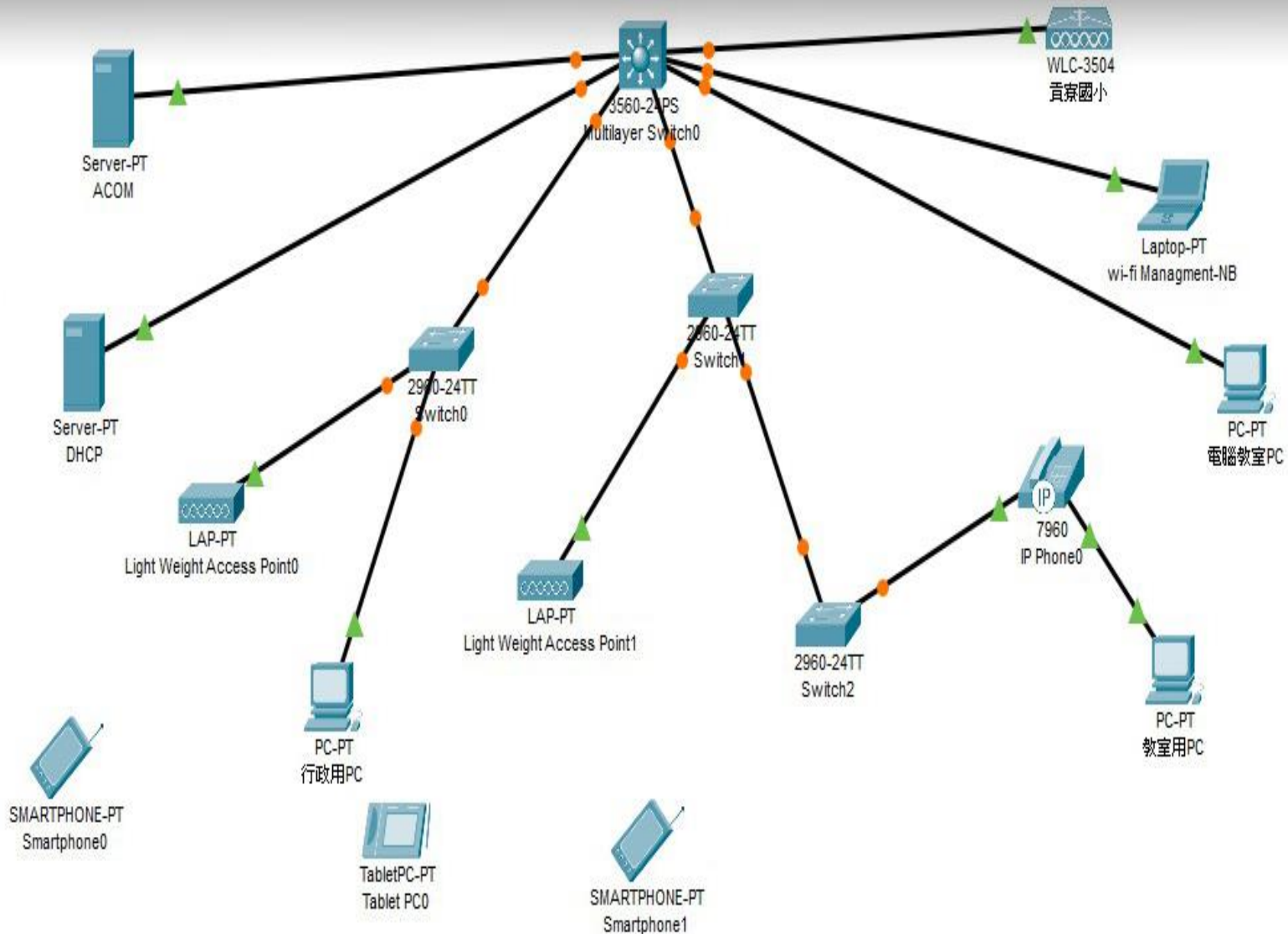
VLAN32-NTPC-Mobile

VLAN33-eduroam

VLAN34-class

VLAN121-DHCP-DNS

VLAN122-Acom



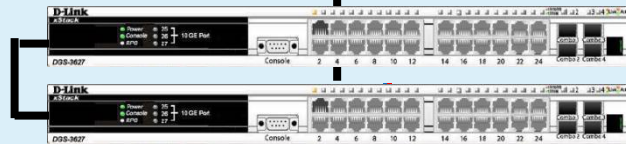
新北市高國中小學校園網路架構圖

48

教網中心

L3 Core Switch

10G堆疊



L2 switch



Voice

Lan



行政電腦



Intra-2

教學教室



無線網路



IP-Phone



教學教室



電腦教室



行政電腦



無線網路

Fat AP

Intra-1

(實作資料) 學校ip分配表

49

- <http://mis.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

50

| 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 |

Lab 5 基本練習Routing

51

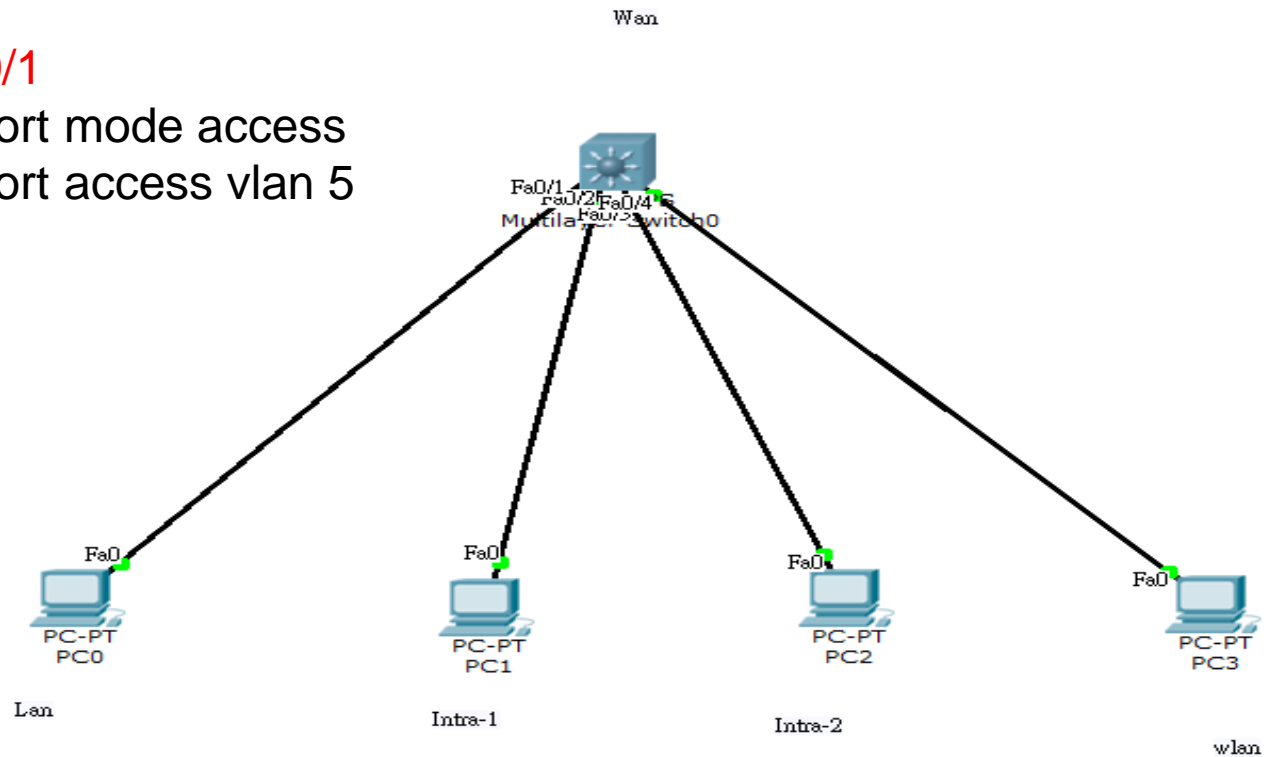
三個Vlan間三個網段 PC相互通。

Config t

Inter fa0/1

Switchport mode access

Switchport access vlan 5



唯一出口通往他國

52

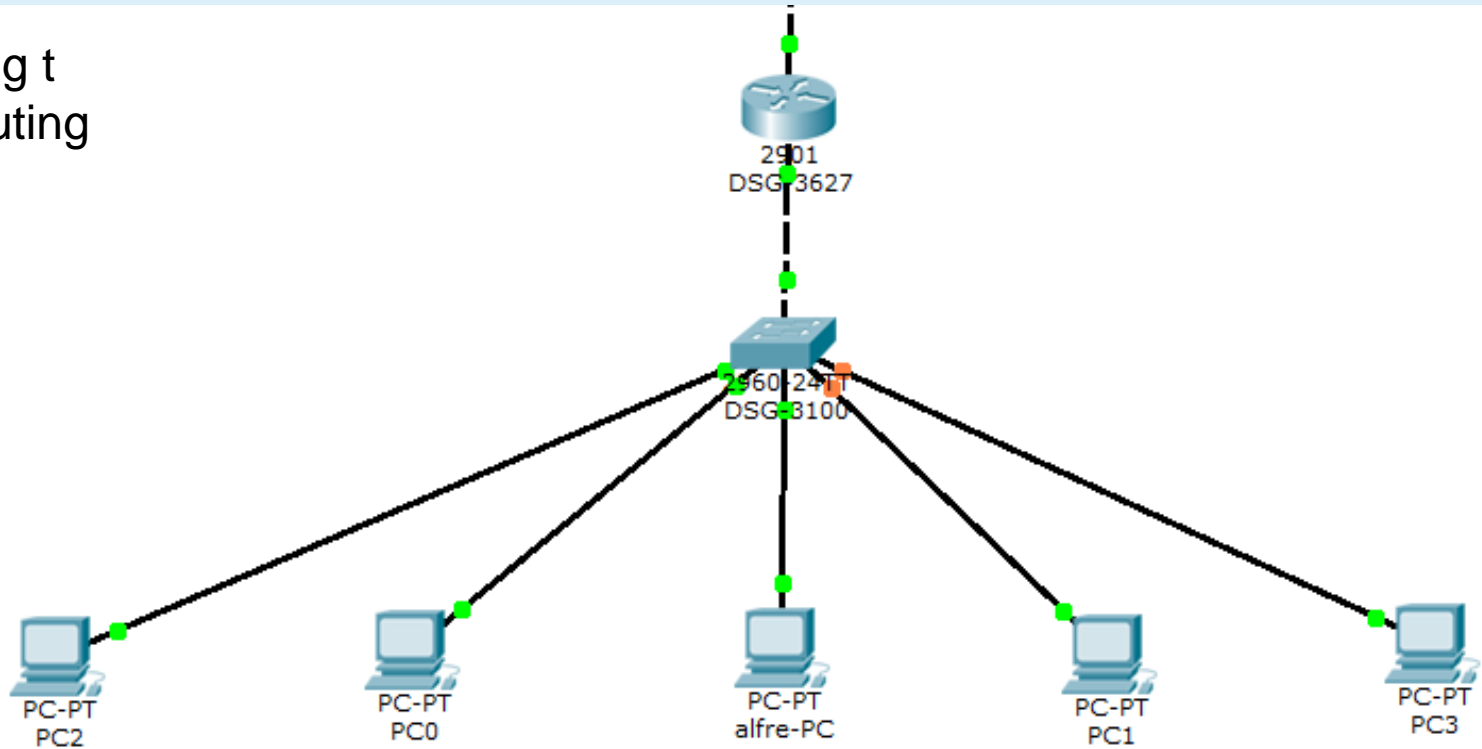
- 目的:了解Gateway設定
- 城池出口(Gateway)。
- 萬里長城 雁門關 WAN Route。
- ECMP

Lab 6基本練習Default Route

53

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

54

貢獻國小:

Gateway:10.229.12.254

LAN:163.20.53.192/24

intra-1: 10.232.12.0/24

intra-2:10.242.12.0/24

VoIP:10.244.12.0/24

無線用31-TANetRoaming:10.212.12.0/24

無線用32-NTPC-Mobile :10.214.12.0/24

無線用33-Eduroam :10.216.12.0/24

無線用34-class:10.218.12.0/24

WLC:10.229.12.1/24

admin/Admin123

DNS:203.72.153.153/24

DHCP:203.72.153.8

Acom:203.72.154.101

VLAN3-WLC

VLAN5-LAN

VLAN10-intra-1

VLAN20-intra-2

VLAN25-VOIP

VLAN31-TANetRoaming

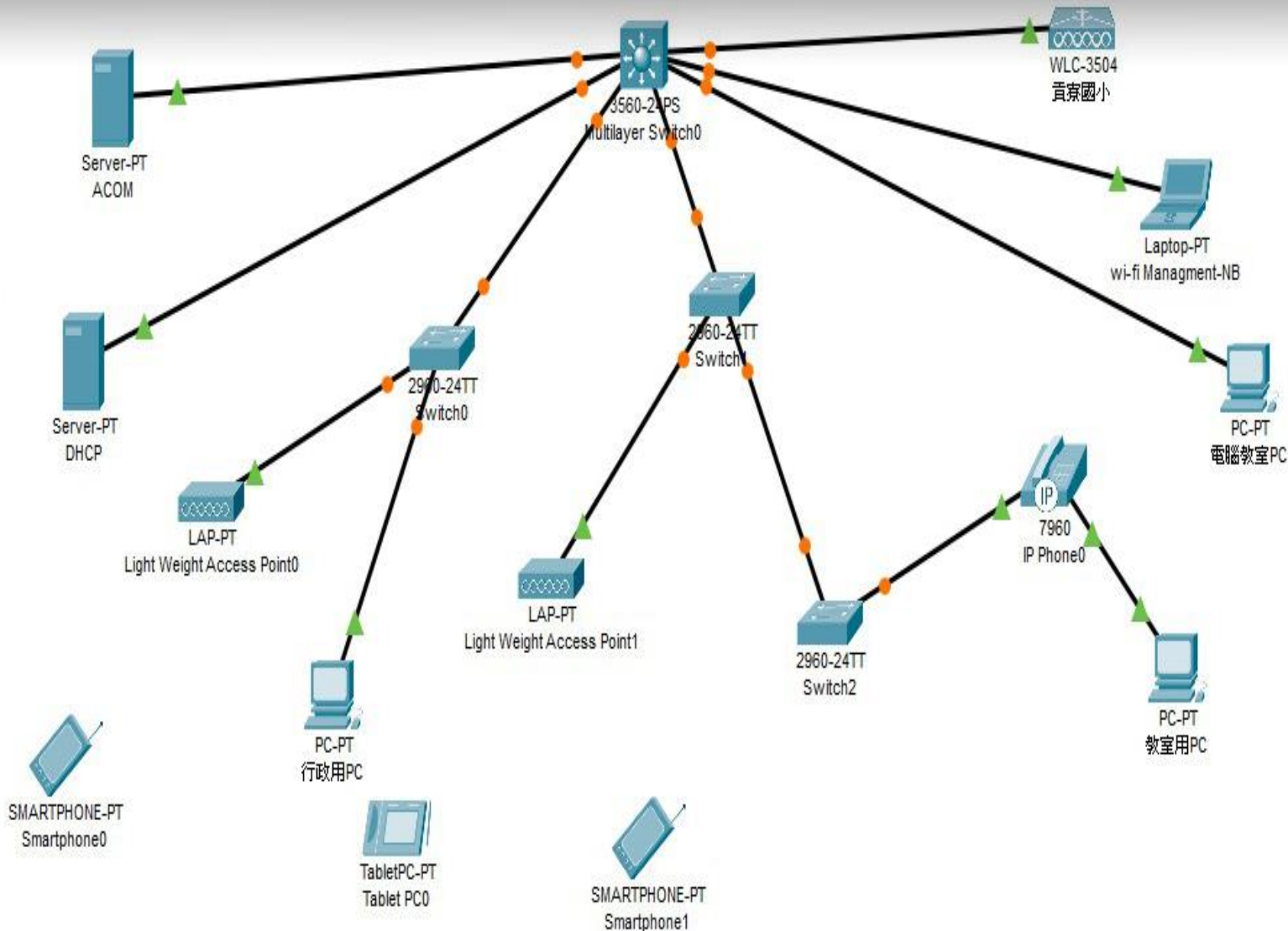
VLAN32-NTPC-Mobile

VLAN33-eduroam

VLAN34-class

VLAN121-DHCP-DNS

VLAN122-Acom



網路資安常用軟體及網站

55

- Wapplayzer網站分析工具
 - 配合cvedetail.com查詢版本
- SSL安全性測試
 - <https://www.ssllabs.com/ssltest/>
- 校園網段開放服務查詢
 - <https://censys.io/>
- 惡意檔案檢測服務 Virus Check
 - <https://viruscheck.tw/>
- **Process Explorer**(microsoft執行中的程式查詢)
- <https://www.shodan.io/> (設備查詢)
 - <https://www.slideshare.net/TonyLin31/shodanio-70219922>

Case Study

56

- 1、校園電子圍牆案。
 - 需求:校內通，可以讓特定IP通內網，校內有行政網段可以看監控。(Firewall)
- 2、DHCP轉移工程，同一個Vlan不連續兩個網段。
 - (竹林中學例)
- 3、因學校縮班，導師或行政辦公室搬家。變更教室為辦公室。
 - 混合環境設定
- 5、中華電信進線因大樓擴柱工程，改校門口警衛室進線。
 - Vlan Wan
- 6、無線網路特殊用途規範。因應活動需求新增SSID。
 - Thin AP SSID
- 7、特殊教學需求，尖峰流量需求申請。
 - N7k PBR route and Fortinet Tunnel Mode
- 8、無線行動包對教學運用的特殊需求及設定。
 - Tunnel Mode with Splite Tunnel

Case實作

57

- 1.問題討論
- 2.拓譜圖
- 3.路由設計
- 4.動手實作

Cisco指令 and Dlink指令對照表

58

- L3維護指令
- L2常用維護指令
- Cisco維護指令

創Vlan

59

- 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 Access port

60

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

61

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

66

- Vlan database
- Config t
- Interface vlan interface fao/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

模擬斷線除錯

67

- 1.vlan斷線 或是被攻擊(要做出三台電腦測試)
- 2.學校L3故障
- 3.中華電信到教網線路斷線。
- 4.教網firewall掛點
- 5.教網ServerFarm掛點
- 教網核心交換器掛點
- 政大區網掛點

一般公文、公務雲除錯

68

- 需協助，Teamviewer裝起來。
- 公務雲在骨幹GOV段
- Nslookup看DNS解析是否為172.18.x.x not 61.60.x.x
- Ping cloud.ntpc.gov.tw doc2.ntpc.gov.tw
- Tracert看路由走法

一般學校網路除錯

69

- 電話:80723456----542 工程師
- Ping gateway
- Ping wan
- Ping firewall
- Ping serverfarm
- Ping gov
- Ping nccu
- Ping www.google.com
- Tracert看路由

校園無線網路簡介

行動包Thin AP架構

D-Link Taiwan 友訊科技台灣分公司

TTSS 電信技術支援課

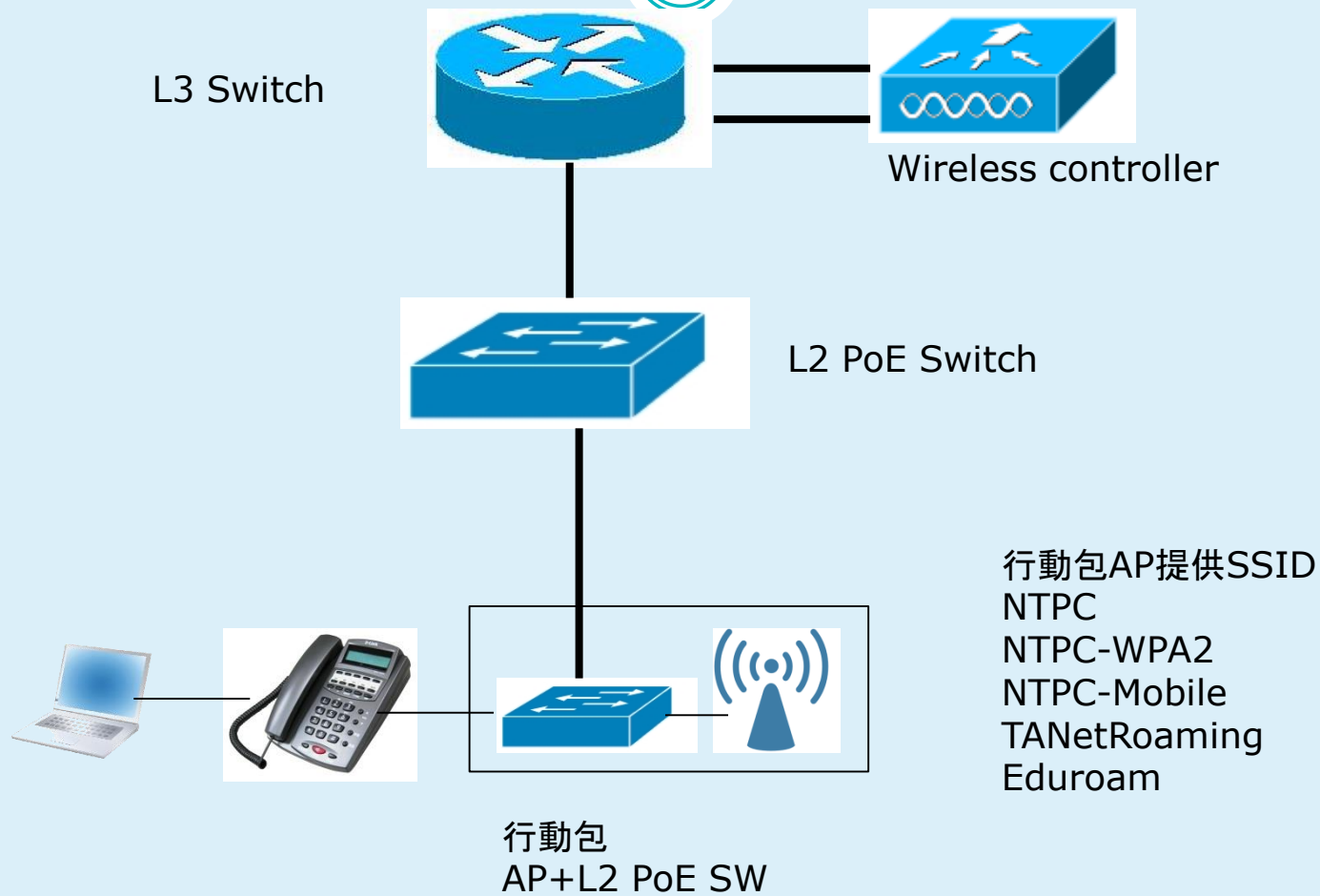
Name:

Phone:02-66000123,

Email:

行動包Thin 架構

72



行動包架構說明

73

- 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**可以自動連回無線控制器上更新資訊!
- 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**WEB**認證,**WPA2**認證與**MAC**認證的接入點!

固定式Thin AP架構

D-Link Taiwan 友訊科技台灣分公司

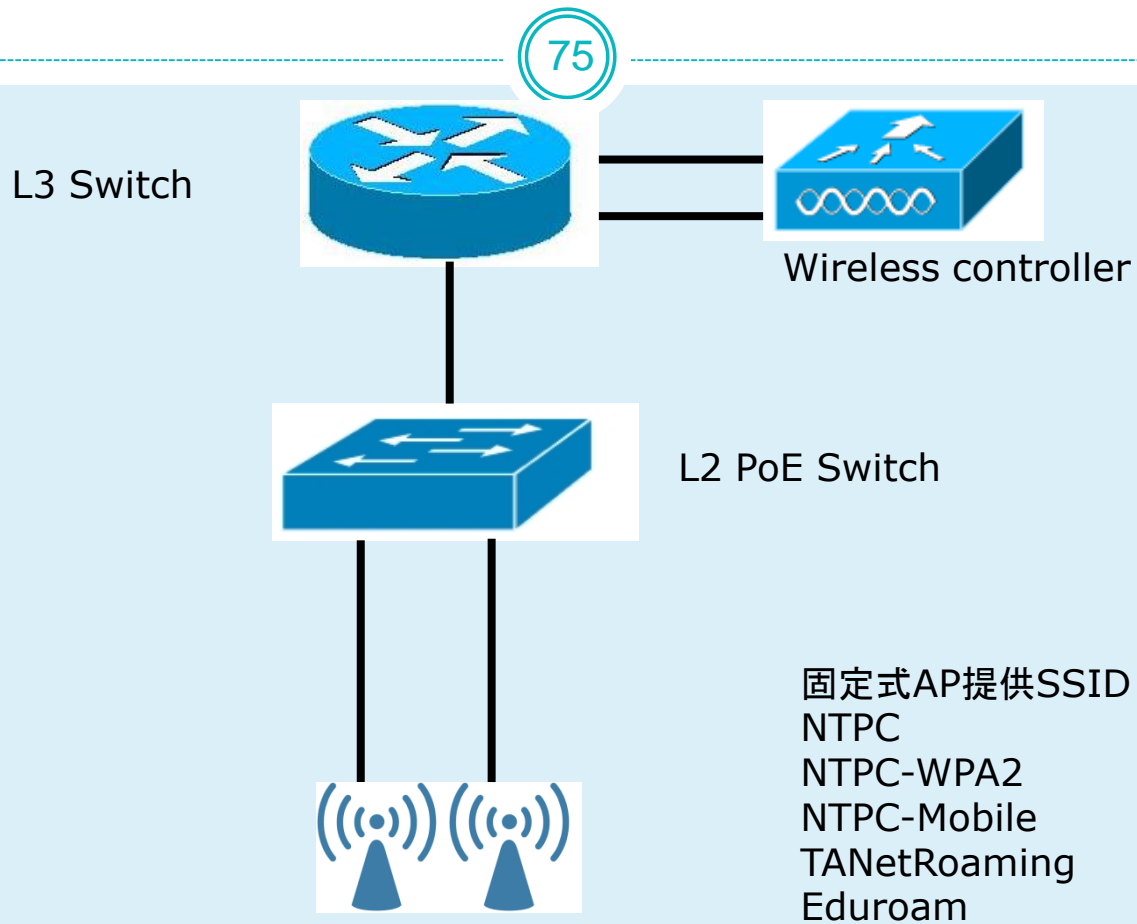
TTSS 電信技術支援課

Name:

Phone:02-66000123,

Email:

固定式Thin AP架構



固定式架構說明

76

- 固定式無線AP透過L2 PoE switch供電
- 固定式無線AP建立5組SSID提供後端WEB認證,WPA2認證與MAC認證的接入點!
- 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

WiNOC Server
(Radius Server)



L3 Switch

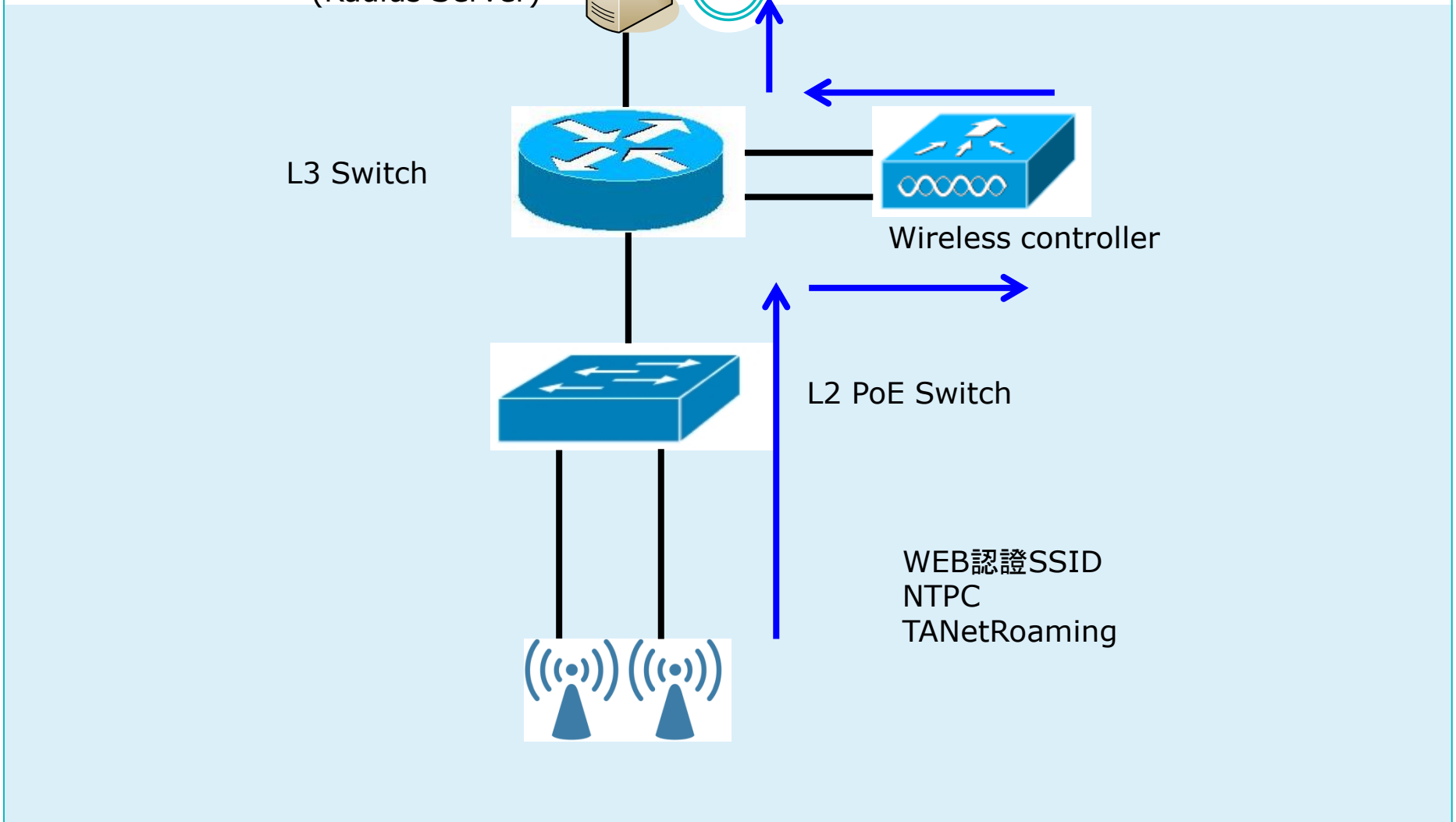


Wireless controller

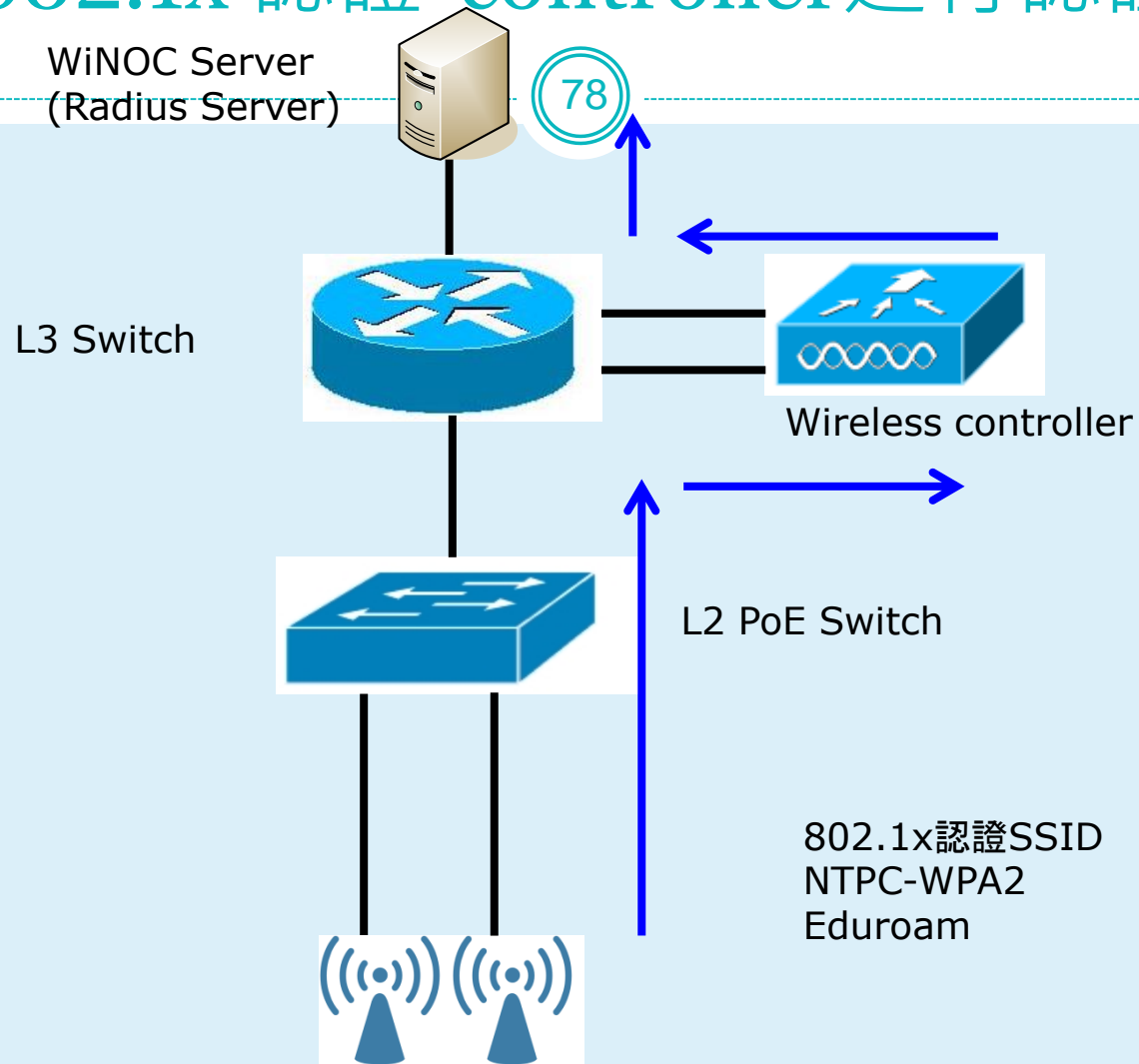
L2 PoE Switch



WEB認證SSID
NTPC
TANetRoaming



802.1x 認證-controller進行認證

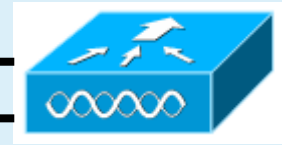


MAC 認證-L3 switch進行認證

WiNOC Server
(Radius Server)



L3 Switch



Wireless controller



L2 PoE Switch



MAC認證SSID
NTPC-Mobile



行動包Thin AP架構

D-Link Taiwan 友訊科技台灣分公司

TTSS 電信技術支援課

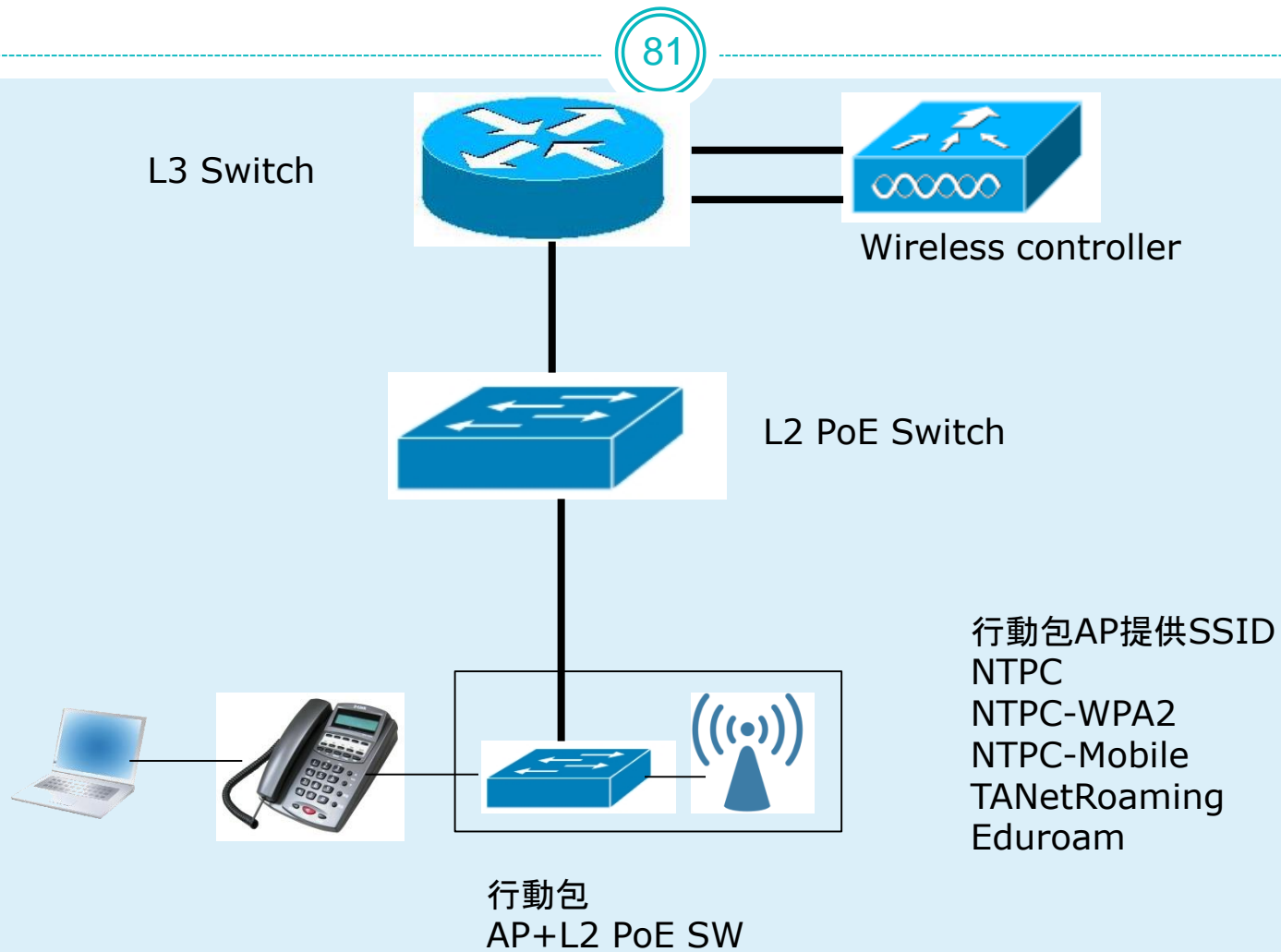
Name:

Phone:02-66000123,

Email:

行動包Thin 架構

81



行動包架構說明

82

- 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可以自動連回無線控制器上更新資訊!
- 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WEB認證,WPA2認證與MAC認證的接入點!
- Ap透過WPA2 vlan至AC取得config後啟動。因此行動包AP manager ip為10.245.x.x or 10.246.x.x
- 固定式為10.226.x.x or 10.227.x.x
- **Tips : WPA2阻擋認證位置在AP，因此有線直接接WPA2 Vlan是可以直接work**

Case Study

83

1、校園電子圍牆案。

需求:校內通，可以讓特定IP通內網，校內有行政網段可以看監控。(Firewall)

2、DHCP轉移工程，同一個Vlan不連續兩個網段。

3、大樓老舊拆除，整棟大樓搬遷作業，L2 Switch搬家。

4、因學校縮班，導師或行政辦公室搬家。變更教室為辦公室SOP。

5、中華電信進線因大樓擴柱工程，改校門口警衛室進線。

6、無線網路特殊用途規範。因應活動需求新增SSID。

7、特殊教學需求，尖峰流量需求申請。

8、無線行動包對教學運用的特殊需求及設定。

9、KMS是否開放無線網路認證?

10、snm拓譜圖之重要性。