新北市校園網路
骨幹網路架構與維運管理

網管輔導員:李 煒
alfred@ntpc.edu.tw
80723456-517

新北市教網

學習經歷

思科網路證照
資安專業

思科CCIE/CCNP學科認證

資安健檢、核心網路
資安職能

封包分析

資安技術檢核
弱掃

資安鑑識調查資安專業

資訊安全證照
資安專業

個資證照
資安專業

網路安全專家

課程進行互動方式

- 若是操作Lab過程有疑問，請務必直接發問。
- 我們的Lab為漸進式，前後相關。
- 課程中隨時問問題，有疑問就直接問。

課程主題

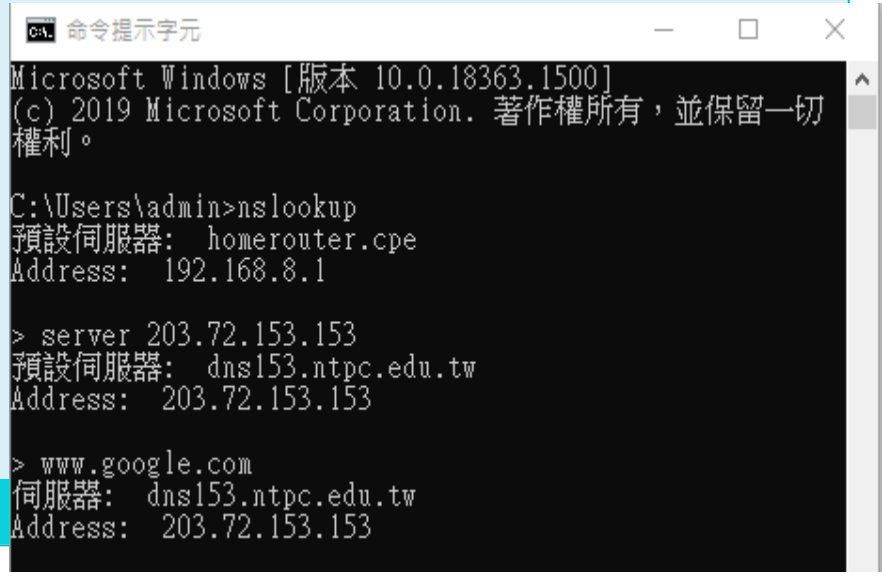
- 瞭解校園網路架構並進行實作，
- 瞭解各種交換器L2 、L3。
- 瞭解 網路除錯方向。
- 瞭解 教育網路服務。
- Case Study 近日問題討論。

課程安排

- 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、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)進階~~

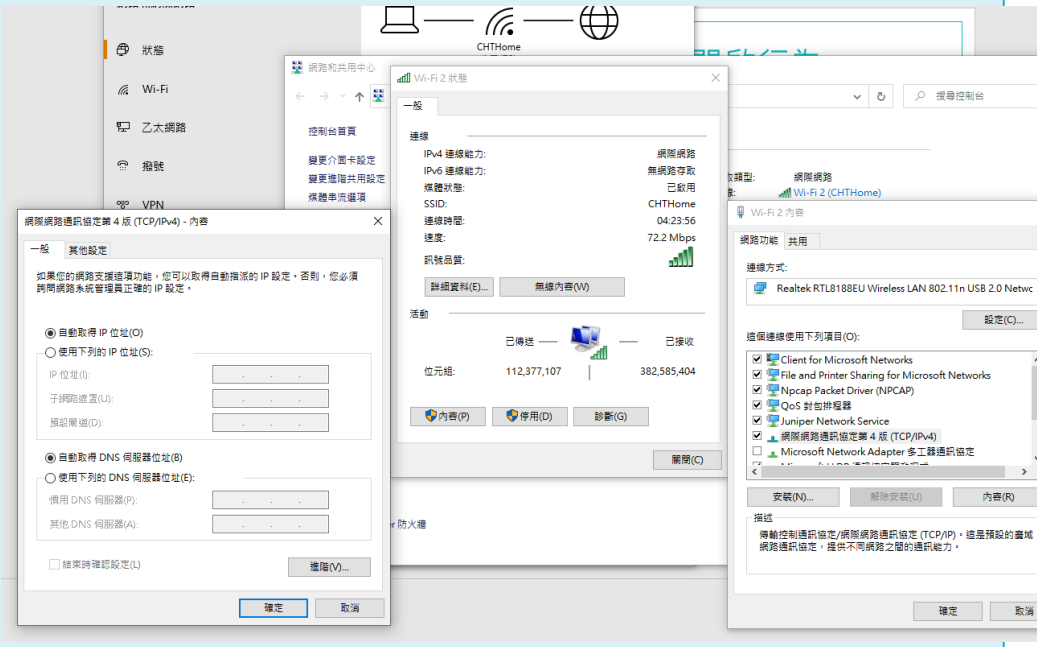
個人PC網路設定

- 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。(255.255.255.0)
- Gateway 用途， Gateway在哪裡??
- Cmd 命令提示字元　常用指令
  - Ipconfig/all　ipconfig/flushdns
  - Ping
  - Nslookup
  - Tracert –d　IP
  - Route print



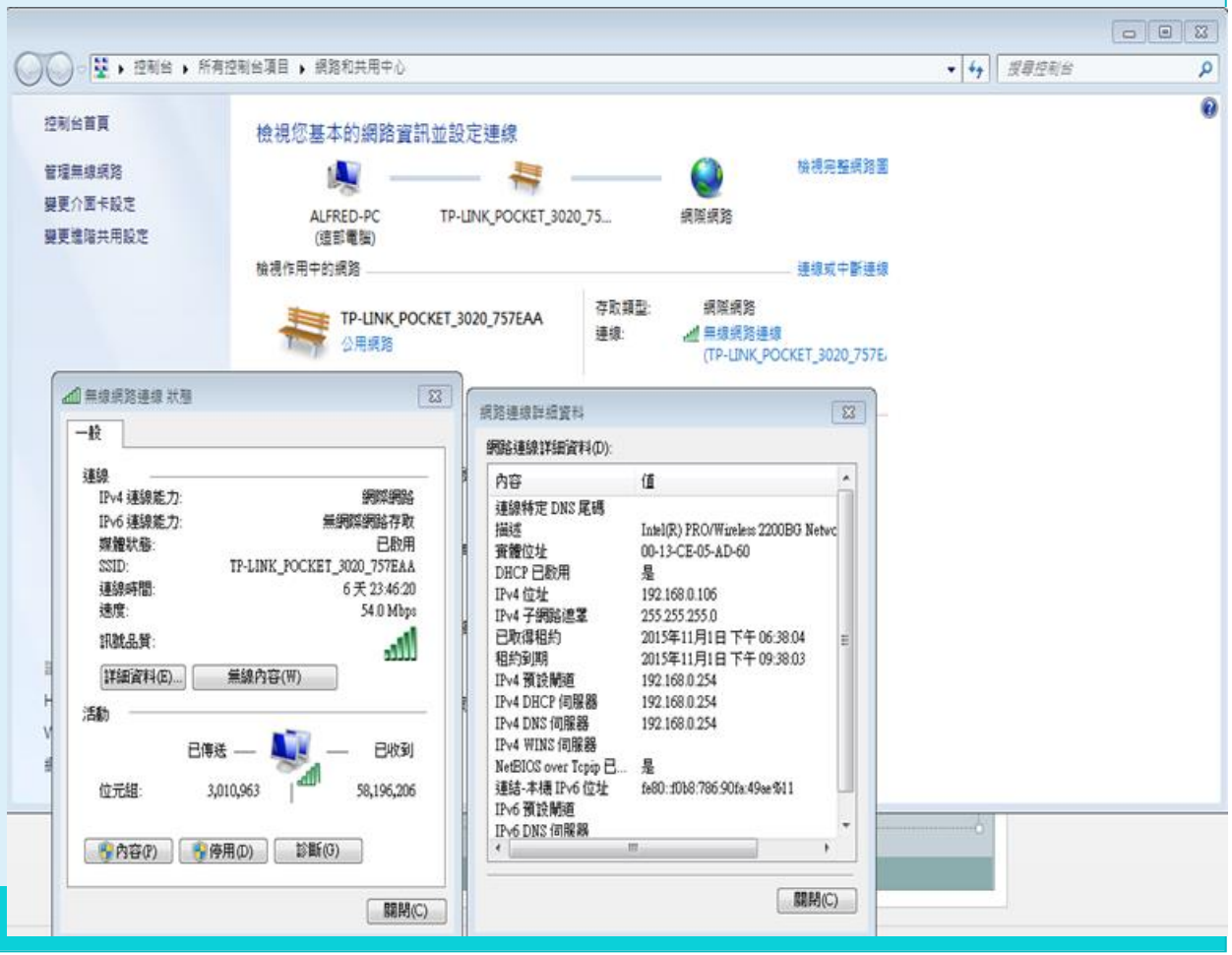
電腦開機程序及網頁開啟行為

- 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

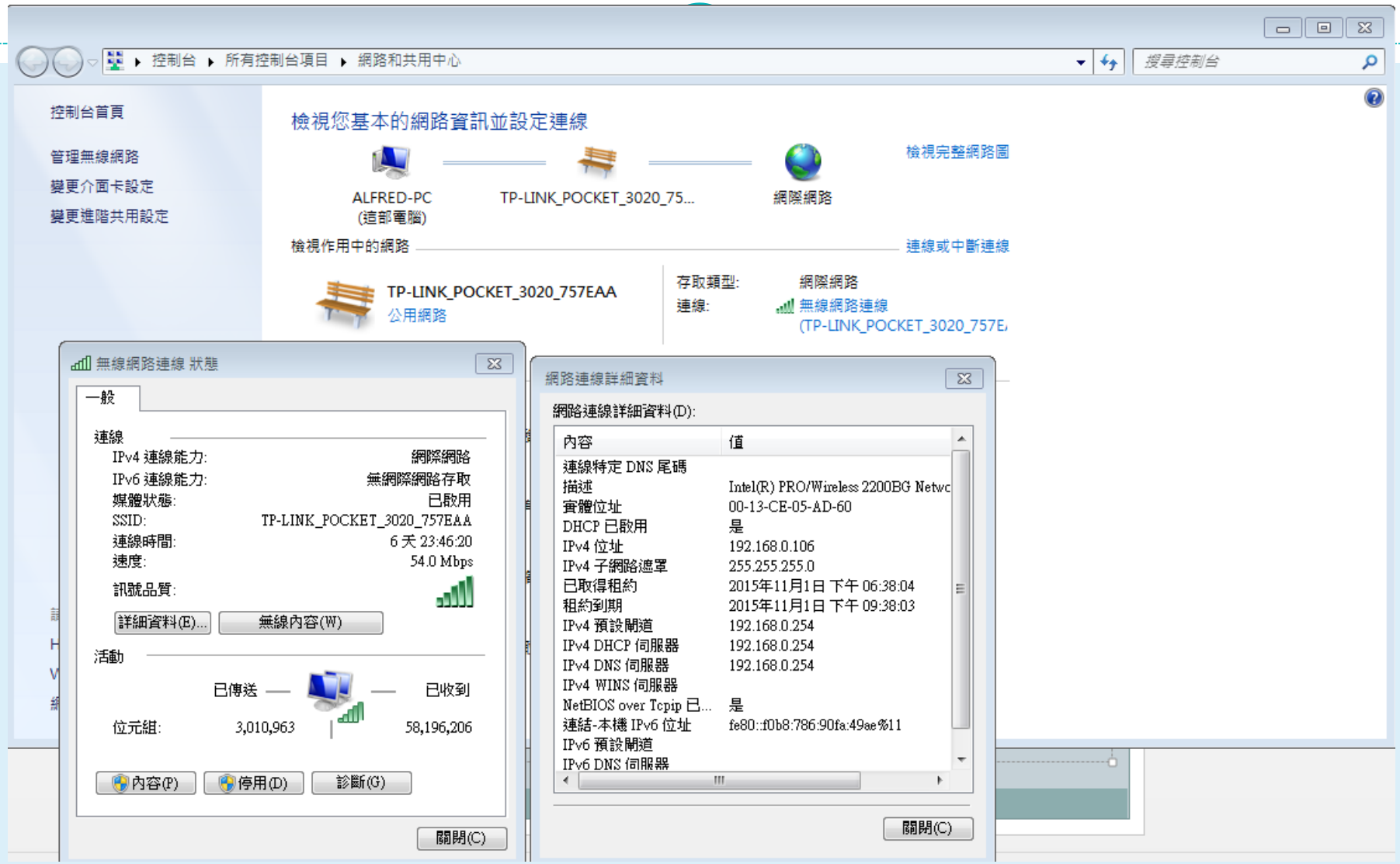


IP Address

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

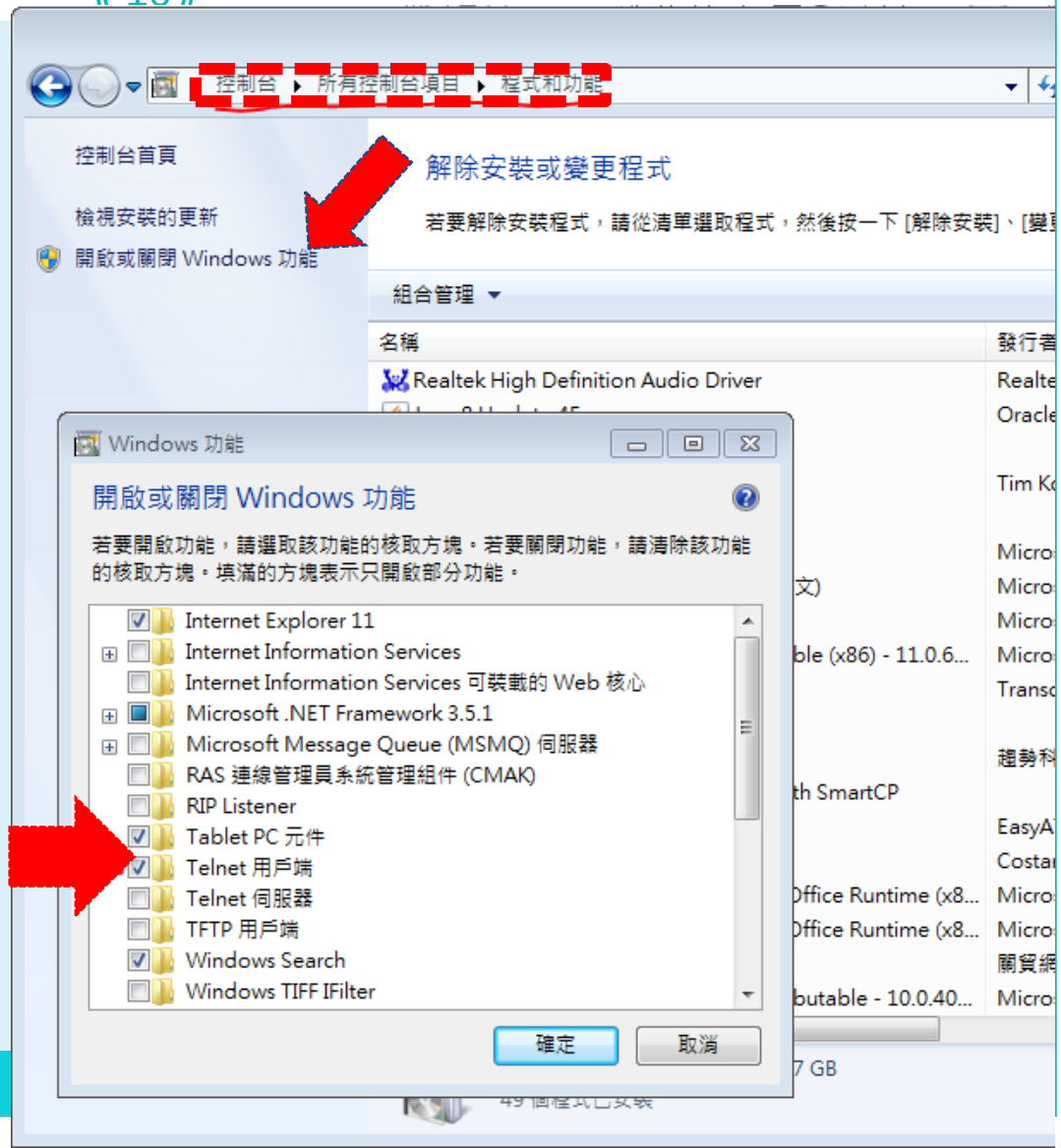


實體PC 網路設定


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
    - esa.ntpc.edu.tw
    - Cloud.ntpc.gov.tw



模擬器操作教學Lab簡介

- Cisco Packet Tracer簡介
- 模擬機PC網路設定
- Wireless WRT300N 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

- CISCO原廠開發
- 提供cisco wlc controller、CCNA、CCNP考試用
- 可以模擬校園網路
- 使用簡單、易懂

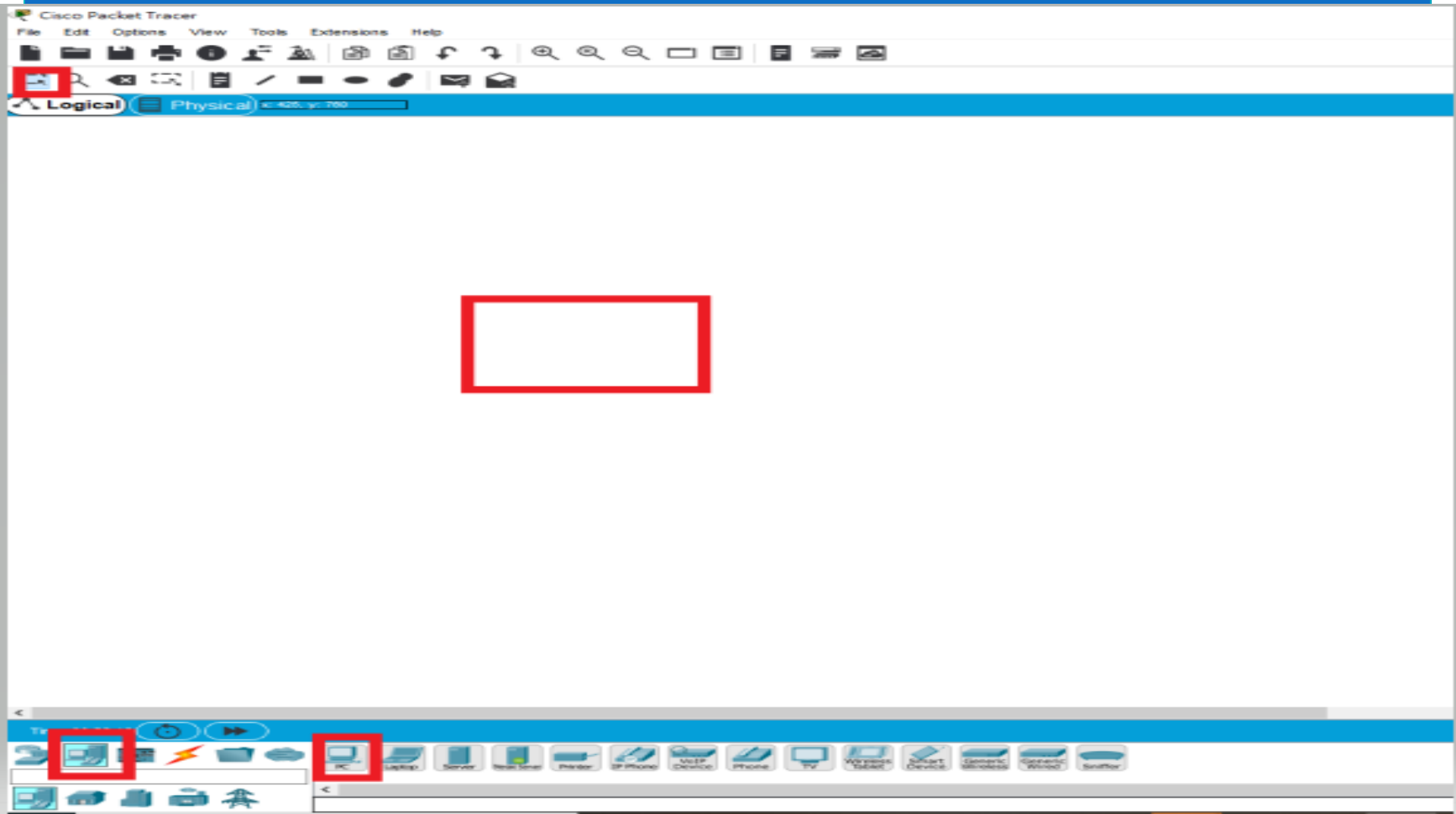
Cisco Packet Tracer

File Edit Options View Tools Extensions Help

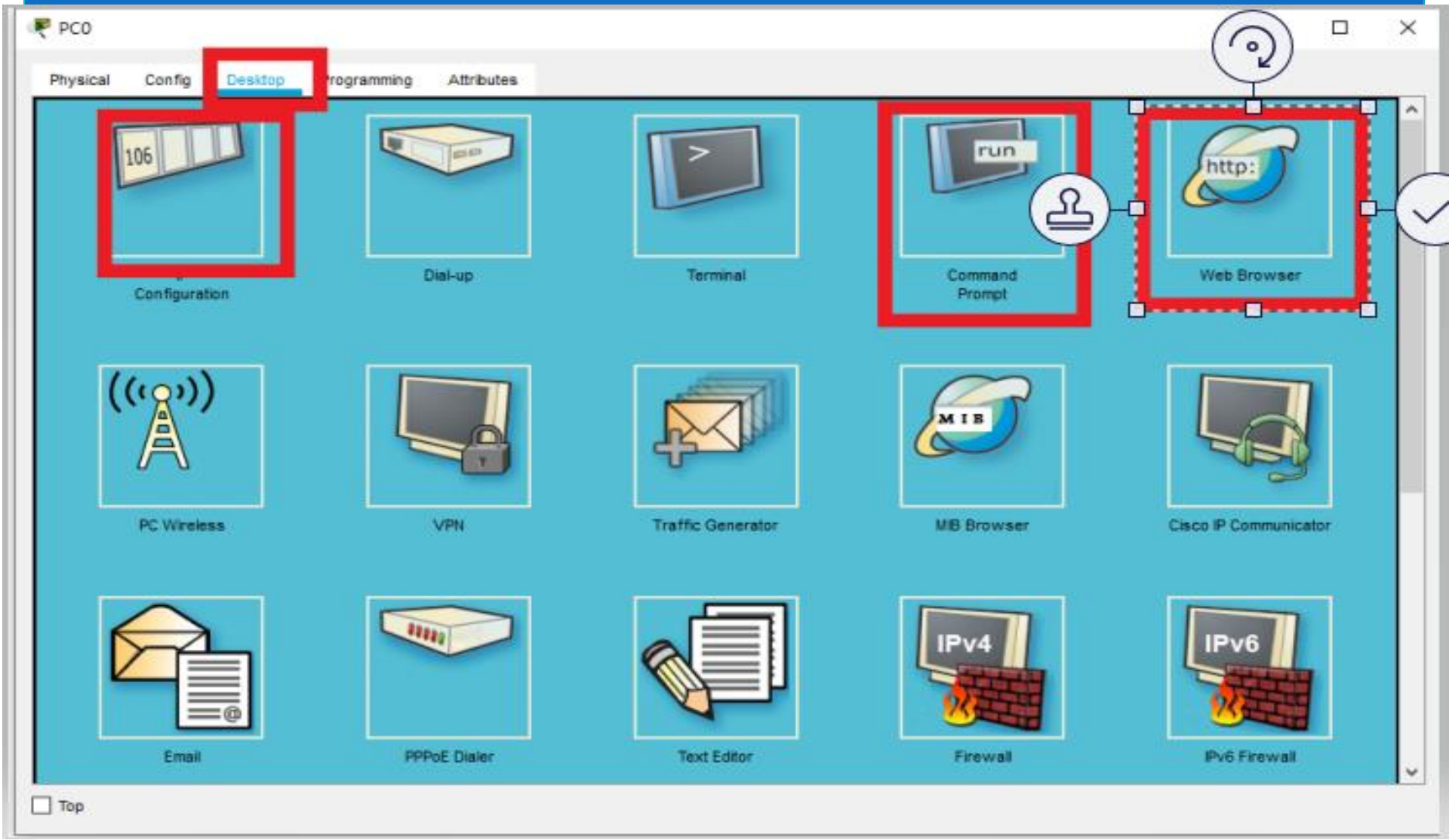
Logical Physical x: 471, y: 8

Time: 00:25:27

模擬PC網路設定


Cisco Packet Tracer
File
Edit
Options
View
Tools
Extensions
Help
Logical
Physical

設定PC網路


PC0
Physical
Config
Desktop
rogramming
Attributes
106
Configuration
Dial-up
Terminal
run
Command Prompt
http:
Web Browser
PC Wireless
VPN
Traffic Generator
MIB
MIB Browser
Cisco IP Communicator
Email
PPPoE Dialer
Text Editor
IPv4
Firewall
IPv6
IPv6 Firewall
Top

PC0

Physical | Config | Desktop | Programming | Attributes

GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Bluetooth

FastEthernet0

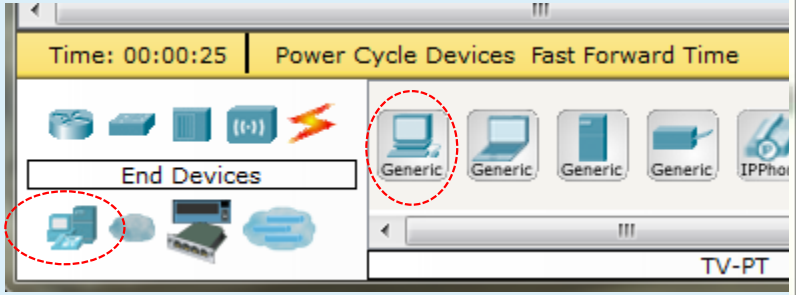
Port Status: [x] On
Bandwidth: (•) 100 Mbps ( ) 10 Mbps [x] Auto
Duplex: (•) Half Duplex ( ) Full Duplex [x] Auto
MAC Address: 0060.5C10.1A62

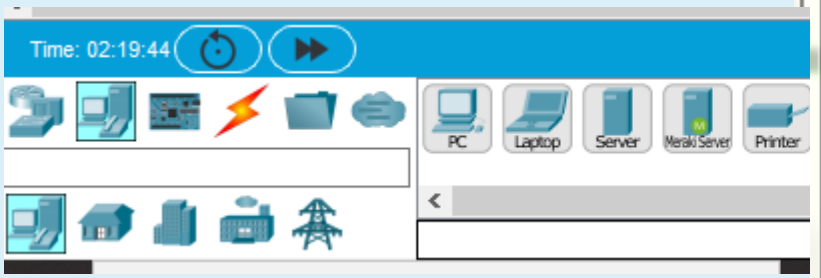
IP Configuration
( ) DHCP
(•) Static
IP Address:
Subnet Mask:

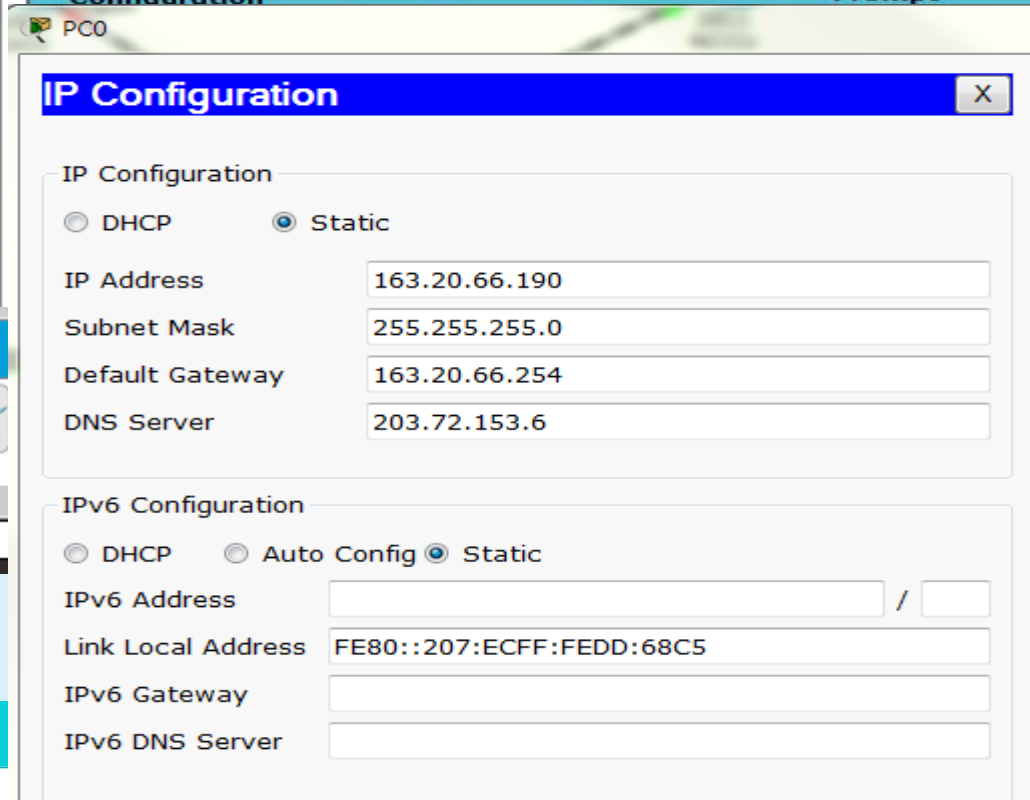
IPv6 Configuration
( ) DHCP
( ) Auto Config
(•) Static
IPv6 Address: /
Link Local Address: FE80::260:5CFF:FE10:1A62

Lab 1 PC 設定

- Packet Tracert
- PC 設定、使用

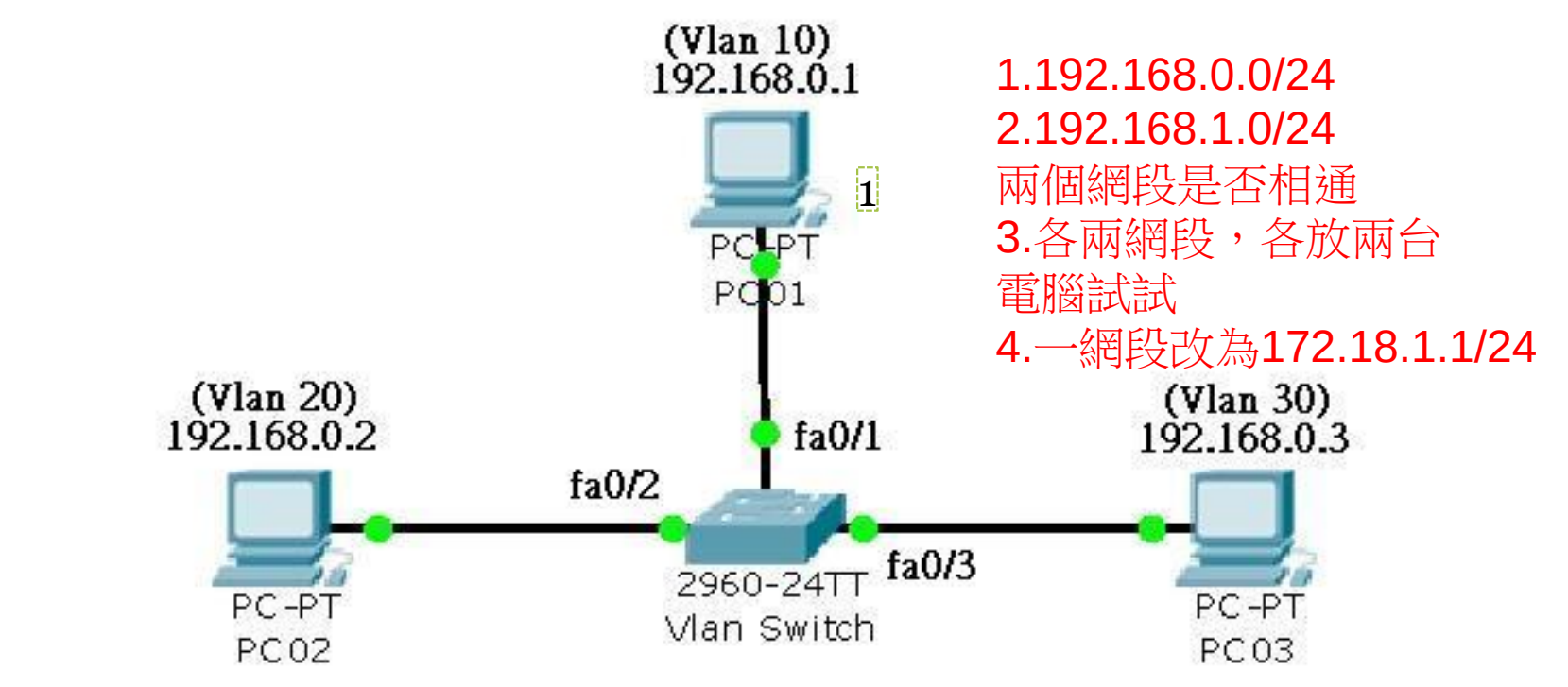






Lab　基本練習Hub、L2 的PC netmask運用

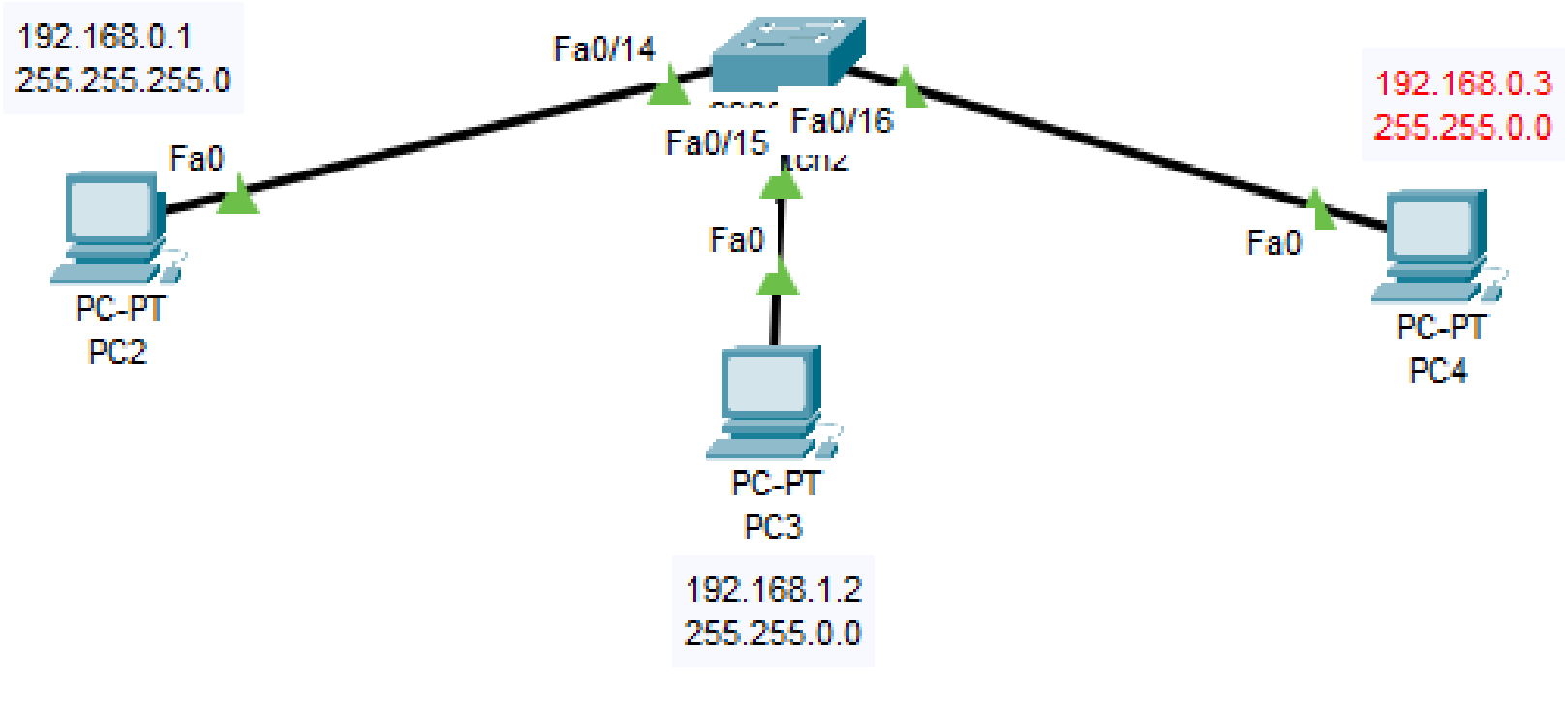
三台 PC 三個網段 、同網段可通、不同網段不通



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

此LAB讓學員，清楚了解netmask用途

看看netmask差異，ping不到為什麼



注意：ping icmp回頭方向，netmask觀念依舊存在。

若將PC3改255.255.255.0。雖PC4可達PC3，但回頭PC3會去找gw

家用無線AP (WRT300N)設定

設定分為三部分

WAN IP (internet)
對外連線

LAN IP
內部有線

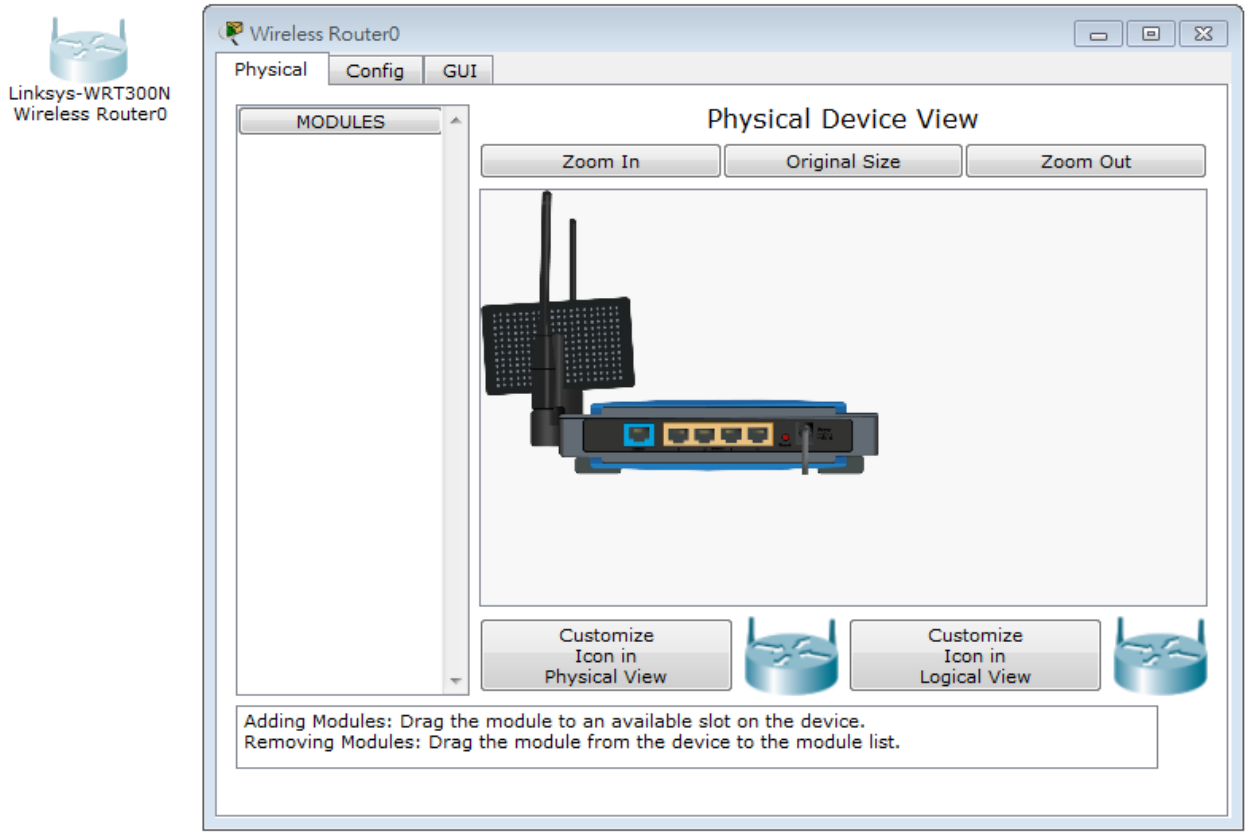
Wireless
內部無線

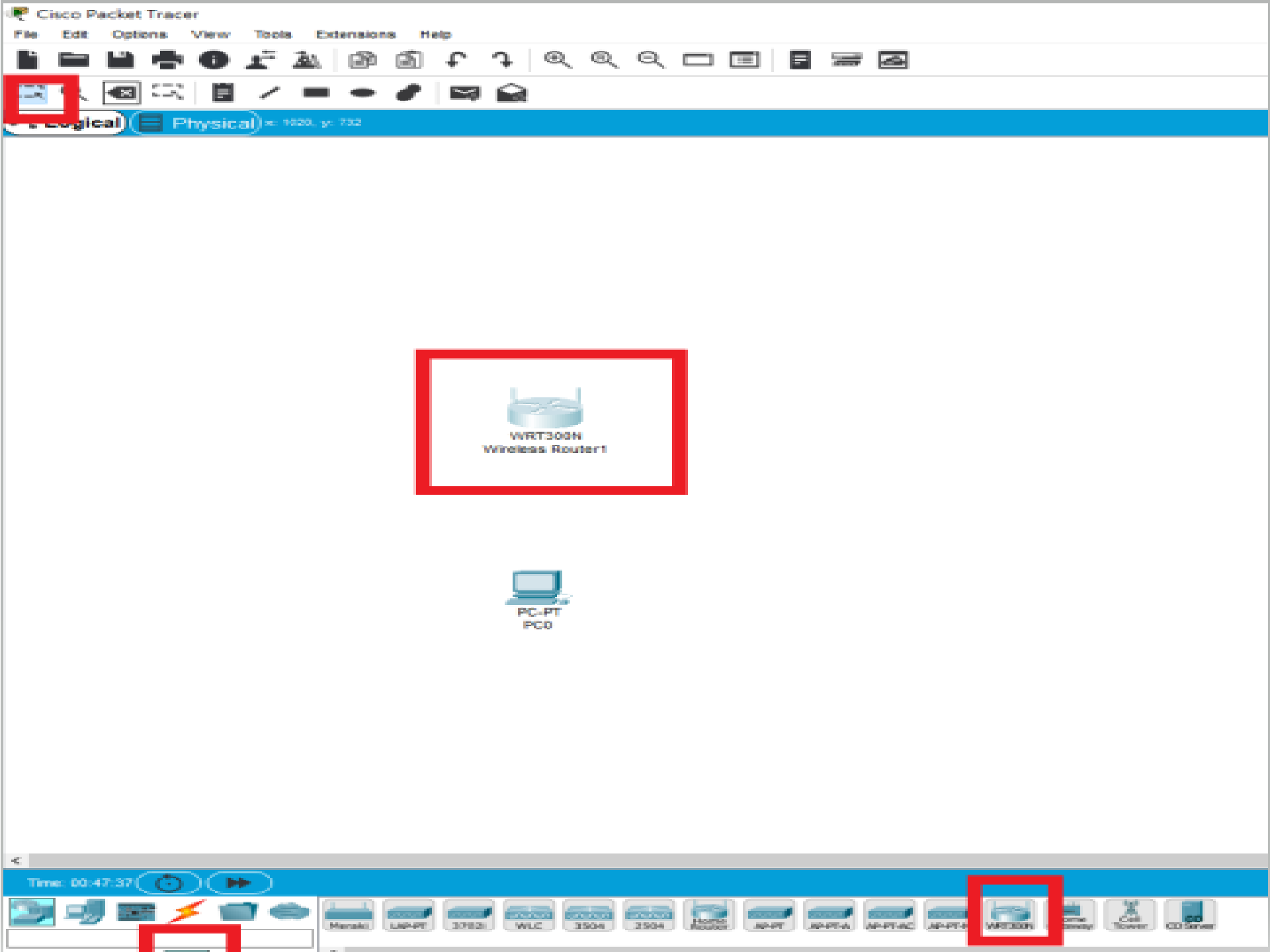
SSID

WPA2

Preshare key

Redius server




Cisco Packet Tracer
File
Edit
Options
View
Tools
Extensions
Help
Logical
Physical
WRT300N
Wireless Router1
PC-PT
PC0
Time: 00:47:37
Meraki
LAP-PT
3702i
WLC
3504
3504
AP-PT
AP-PT-A
AP-PT-AC
WRT300N
Cell Tower
CO Server

Wireless Router1

Physical | Config | GUI | Attributes

Wireless-N Broadband Router

Firmware Version: v0.93.3

Setup | Setup | Wireless | Security | Access Restrictions | Applications & Gaming | Administration | Status

Wireless-N Broadband Router WRT300N

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

Static DNS 2: 0 . 0 . 0 . 0

Static DNS 3: 0 . 0 . 0 . 0

WINS: 0 . 0 . 0 . 0

Help...

Wireless Router1

Physical | Config | GUI | Attributes

GLOBAL
- Settings
- Algorithm Settings

INTERFACE
- Internet
- LAN
- Wireless

Internet Settings

IP Configuration
- (●) DHCP
- ( ) Static
- ( ) PPPoE

UserName

Password

IP Address

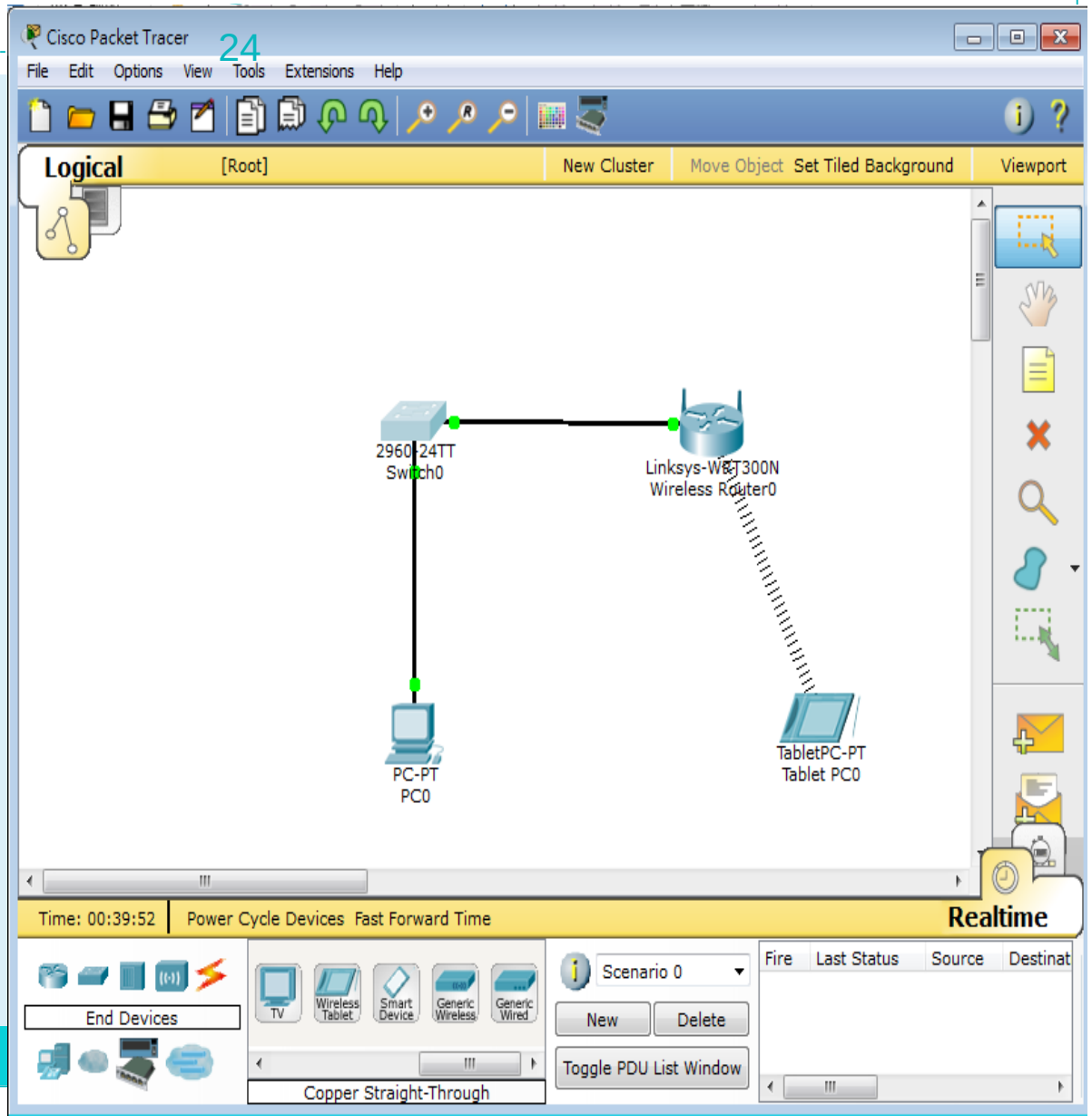
Subnet Mask

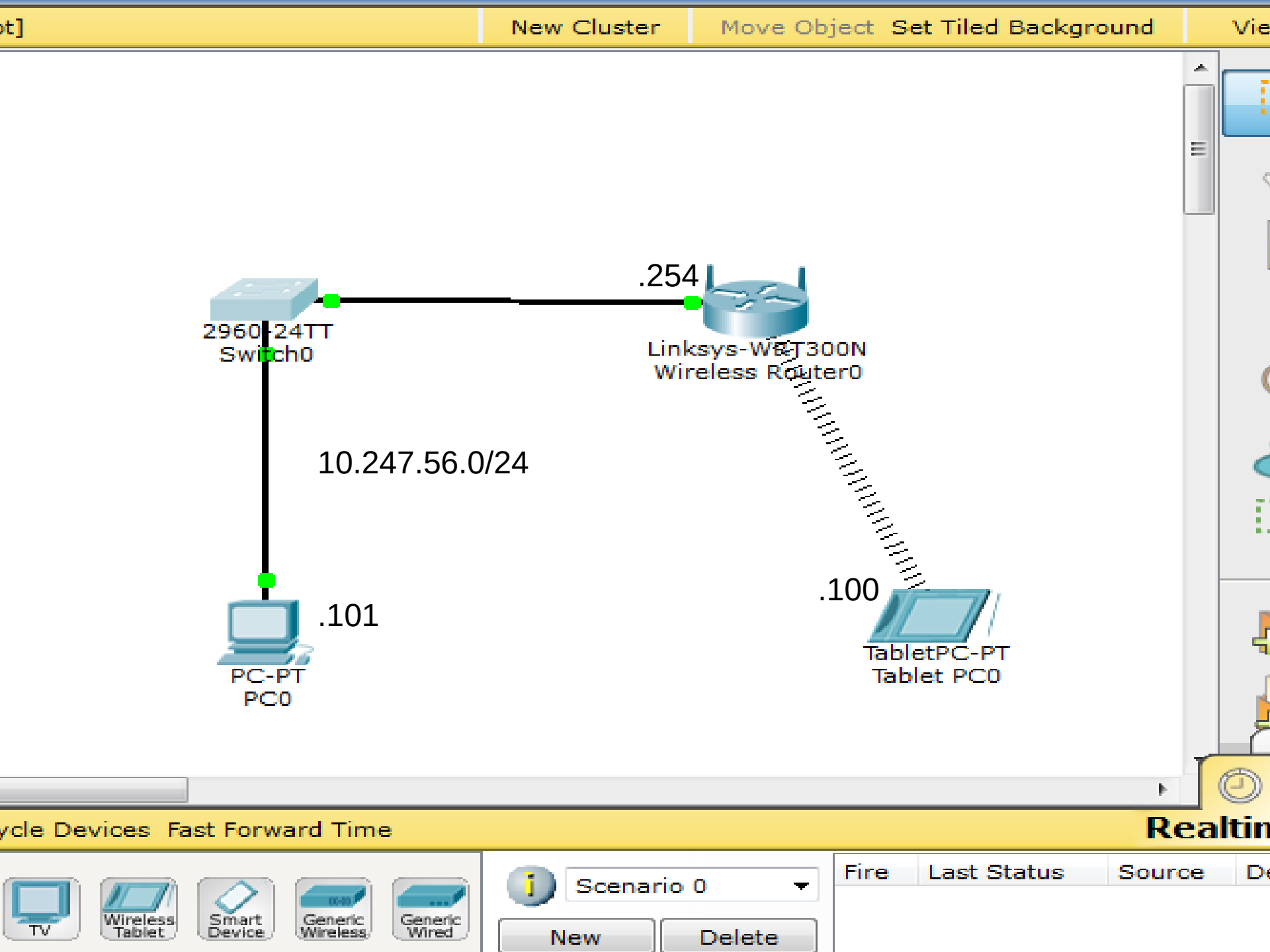
Default Gateway

DNS Server

基本網路設定Lab

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
.100
.101
PC-PT
PC0
TabletPC-PT
Tablet PC0
Fast Forward Time
Realtim
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

- 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

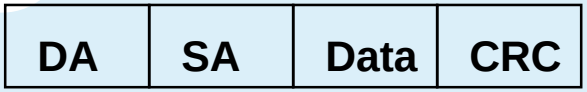
802.1Q vlan

IEEE 802.1p/802.1q Frame Tagging

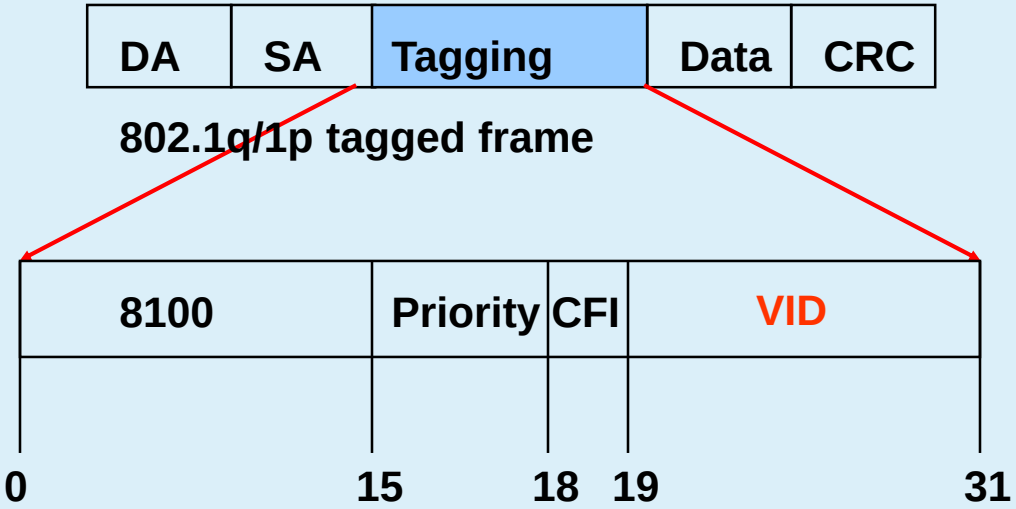
The 32-bit field (VLAN Tag) in the frame header that identifies the frame as belonging to a specific VLAN/priority.

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.



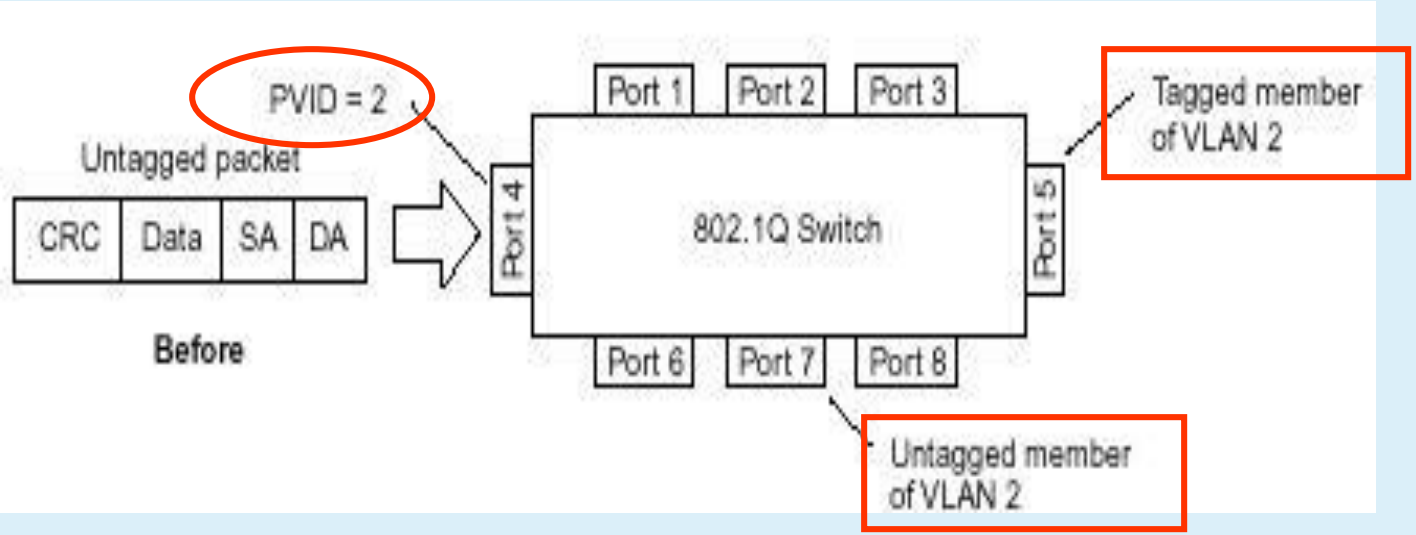
Regular frame (or untagged frame)



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

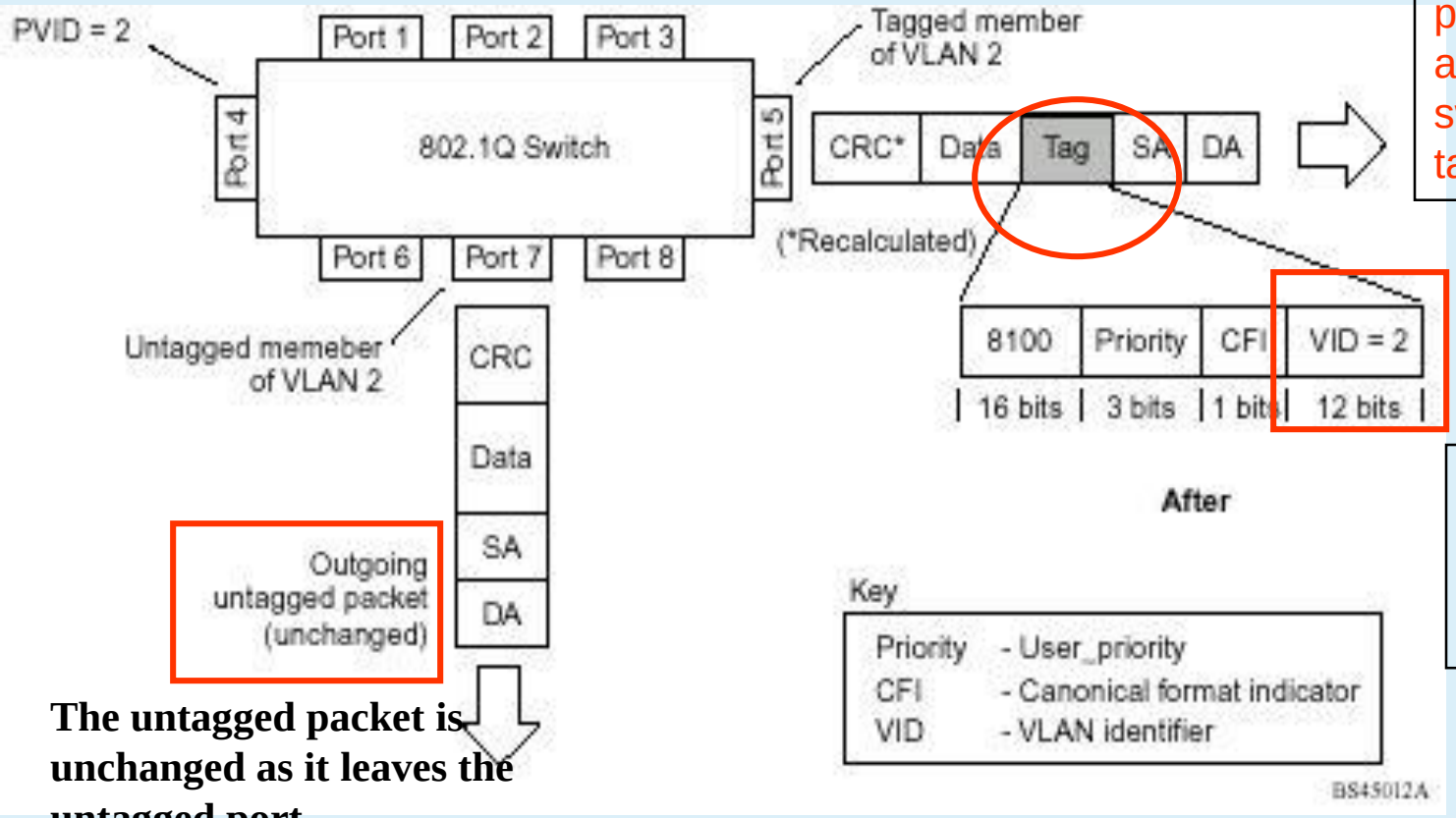
VLAN (1q) has 12 bits, 0-4095

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

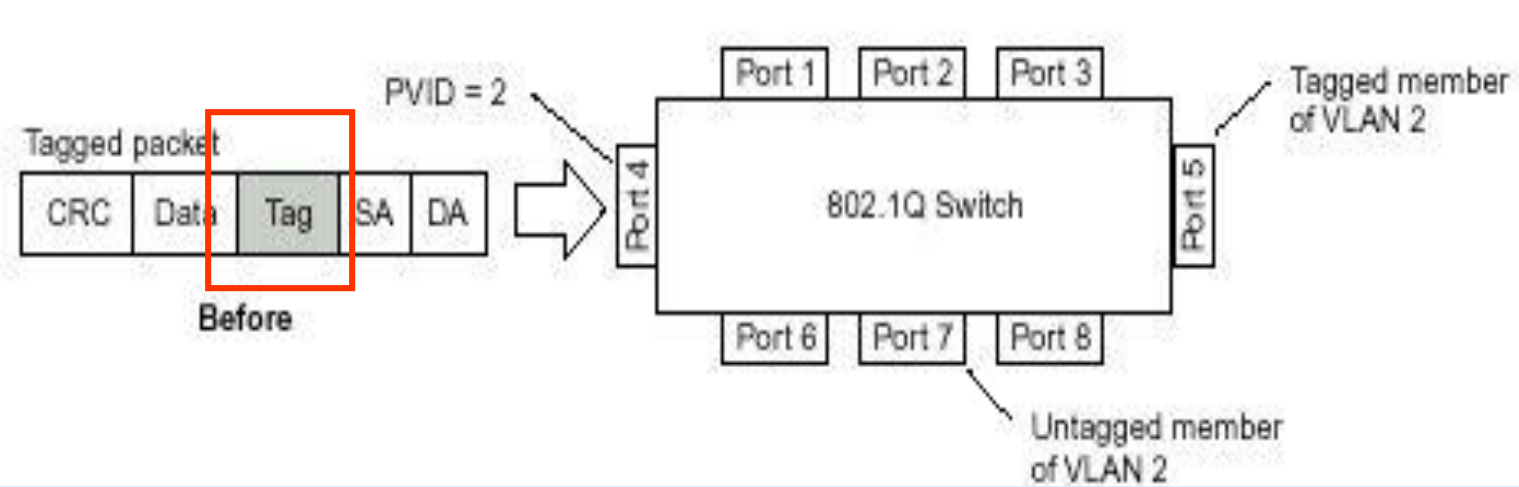


The untagged packet is tagged as it leaves the switch through tagged port

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

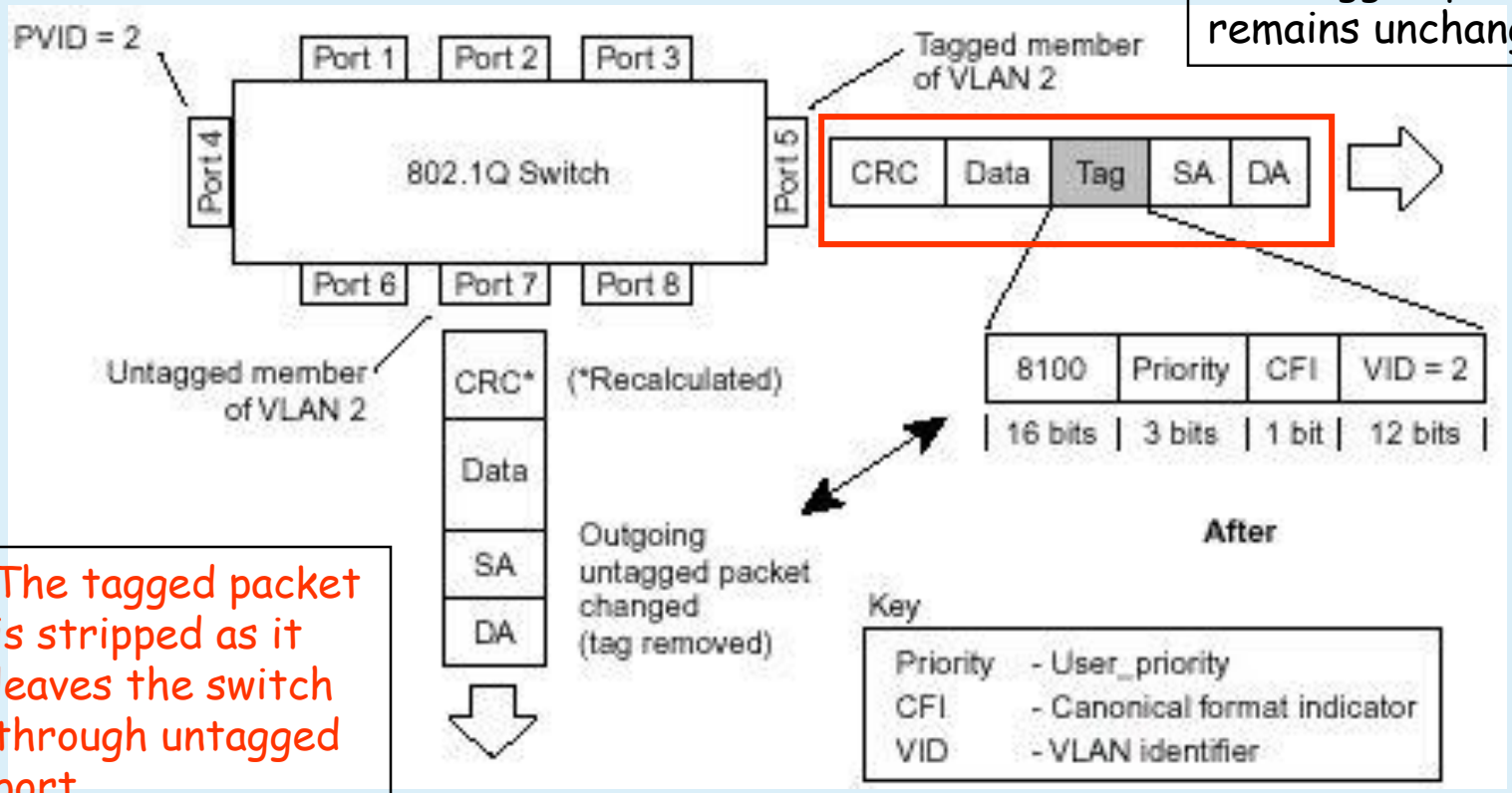


Assumed tagged incoming packet having vid=2/priority=0
Port5 is a tagged and port 7 is an untagged egress member of VLAN 2
This packet will be forwarded to port5 and port7

22=00100010

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):

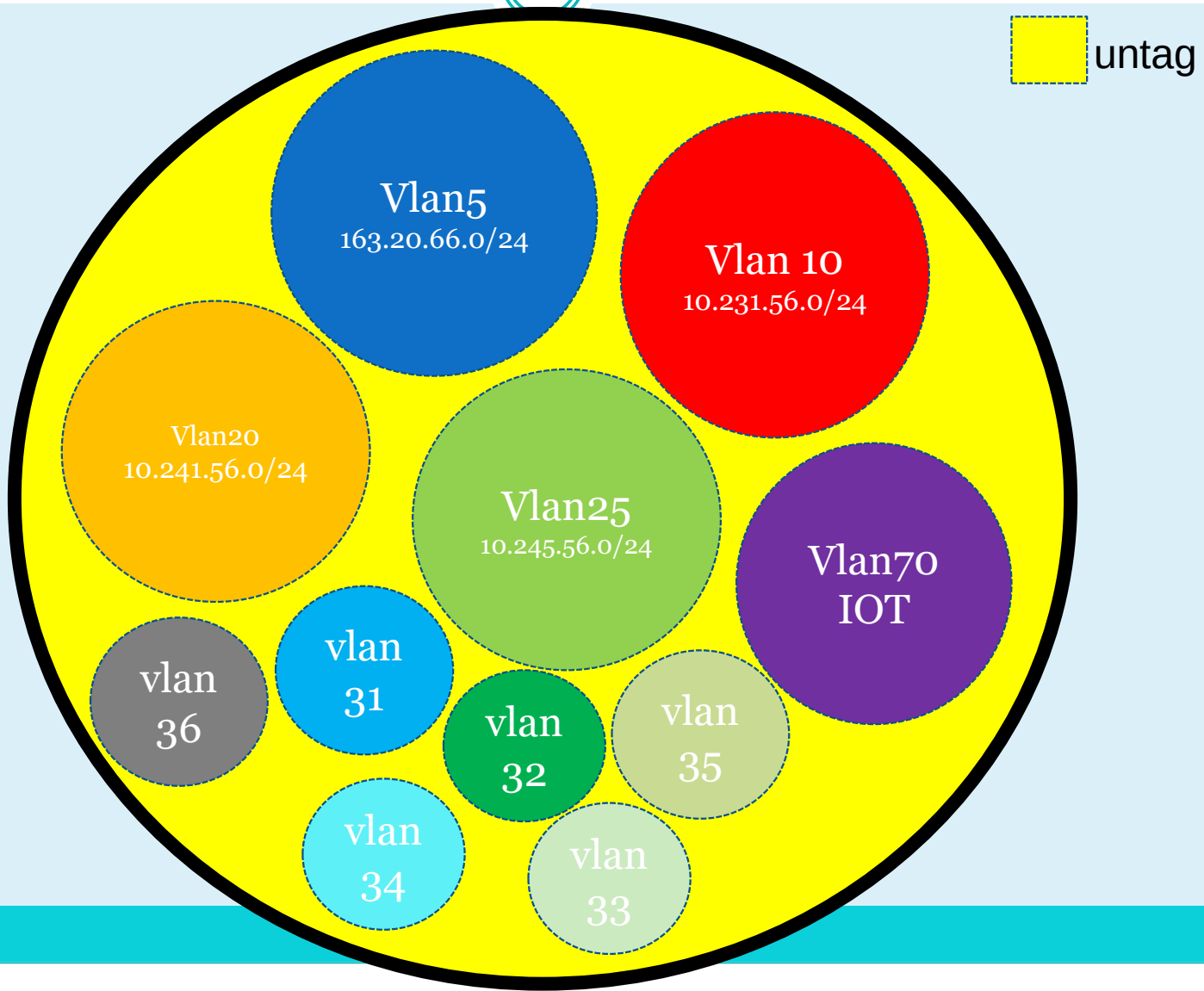
- **Untagged** egress port: Remove the tagging.
- **Tagged** Egress port: Un-change the tagging, so that the 1p/1q info can be carried to next 802.1p/q aware switch.

Vlan 水管理論

在大水管中，大管內壁(小水管外and大水管壁之間空隙)能接觸到的資料流是untag

在所有小水管中的資料流都是帶tag

VLAN大水管


untag
Vlan5
163.20.66.0/24
Vlan 10
10.231.56.0/24
Vlan20
10.241.56.0/24
Vlan25
10.245.56.0/24
Vlan70
IOT
vlan
36
vlan
31
vlan
32
vlan
35
vlan
34
vlan
33

Vlan tag

PDU Information at Device: Multilayer Switch0

OSI Model | Inbound PDU Details | Outbound PDU Details

PDU Formats

Ethernet 802.1q

0	4	8	Bytes
PREAMBLE: 101010..10	SFD	DEST ADDR:0001.963B.B604	
SRC ADDR:0090.2167.AA29	TPID:0x8100	TCI:0x000a	
DATA (VARIABLE LENGTH)			

IP

0	4	8
VER:4	IHL	DSCP:0x00
ID:0x0009		
TTL:128	PRO:0x01	
SRC I		
DS		
OPT:0x00000000		
DATA (VA		

PDU Information at Device: Switch0

OSI Model | Inbound PDU Details | Outbound PDU Details

PDU Formats

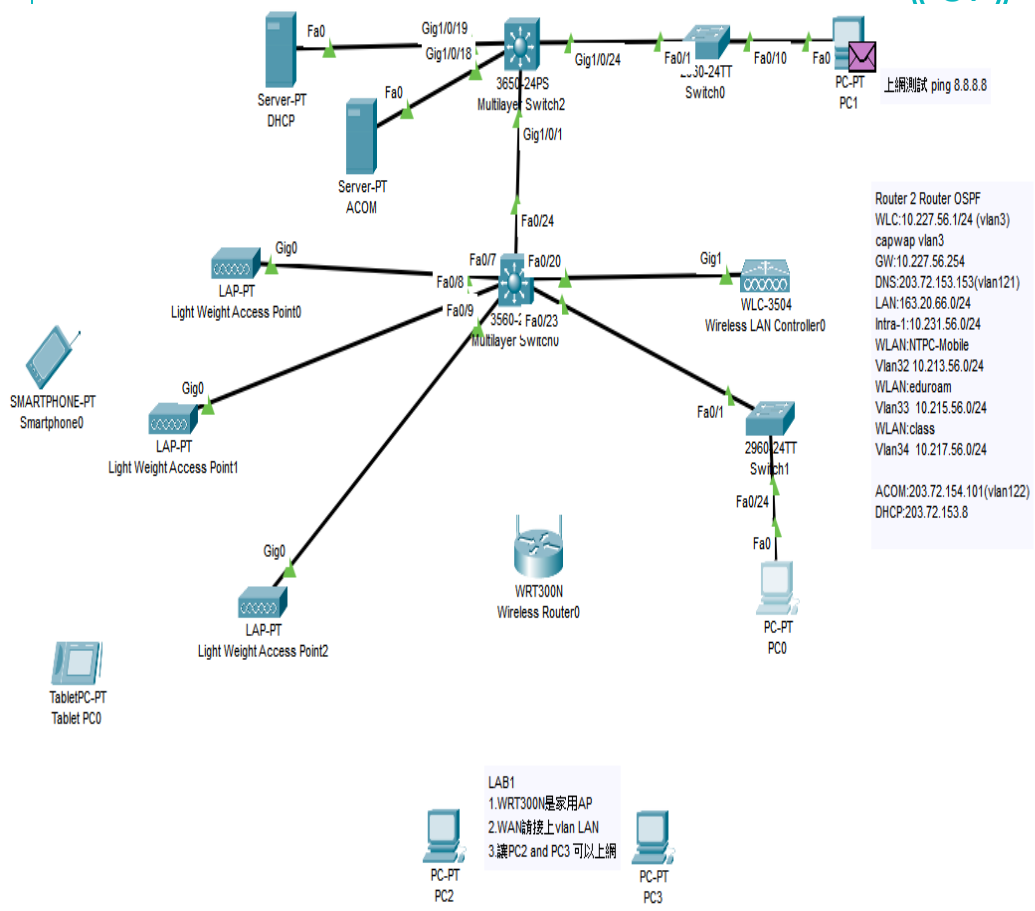
Ethernet 802.1q

0	4	8	Bytes
PREAMBLE: 101010..10	SF	DEST ADDR:000D.BD6B.DD96	
SRC ADDR:0000.0CC9.5A02	TPID:0x8100	TCI:0x0058	Type:0x1
DATA (VARIABLE LENGTH)		FCS:0x00000000	

IP

0	4	8	16	20	24	Bits
VER:4	IHL	DSCP:0x00	TL:128			
ID:0x0009			FLAGS:0x0	FRAG OFFSET:0x000		
TTL:126	PRO:0x01		CHKSUM			
SRC IP:10.231.56.1						
DST IP:8.8.8.8						
OPT:0x00000000			PADDING:0x00			

Simulation



Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC0	ICMP
	0.001	PC0	Switch1	ICMP
	0.002	Switch1	Multilayer Switch0	ICMP
	0.003	Multilayer Swit...	Multilayer Switch2	ICMP
	0.004	Multilayer Swit...	Switch0	ICMP
	0.005	Switch0	PC1	ICMP

Reset Simulation ☑ Constant Delay

Captured to: 0.005 s

Play Controls

Event List Filters - Visible Events

ACL Filter, ARP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRPv6, FTP, H.323, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, NDP, NETFLOW, NTP, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP

Edit Filters | Show All/None

Lab L2 Vlan建置說明

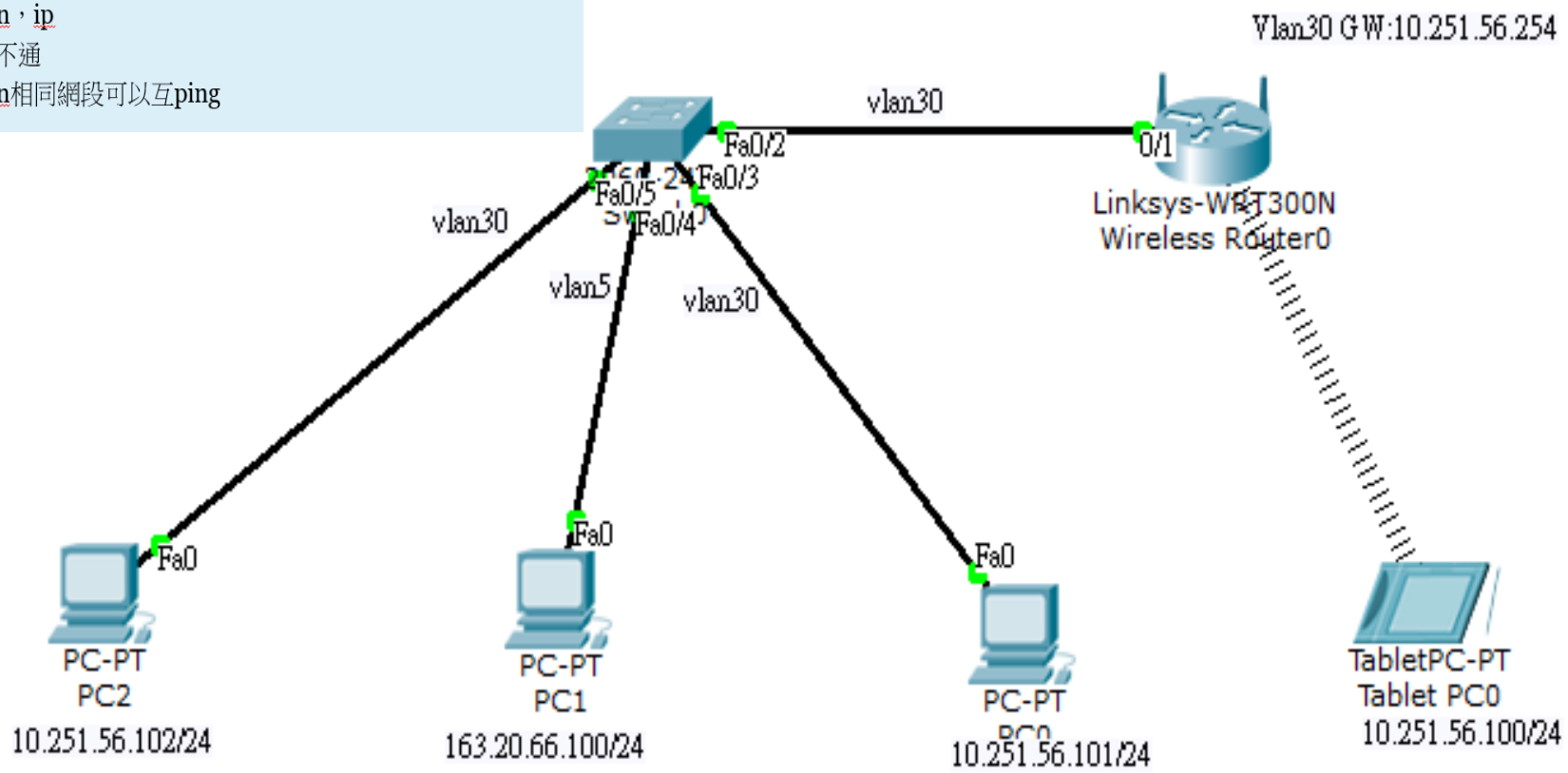
- 建立vlan 30 and vlan 5
- 將接L2與PC相連的port設定為正確vlan access port
- 測試
  - 相同vlan可以取得DHCP派發ip
    - 不同vlan，ip
    - 互 ping不通
    - 相同vlan相同網段可以互ping

Lab L2 Vlan

Lab L2 Vlan建置說明

39

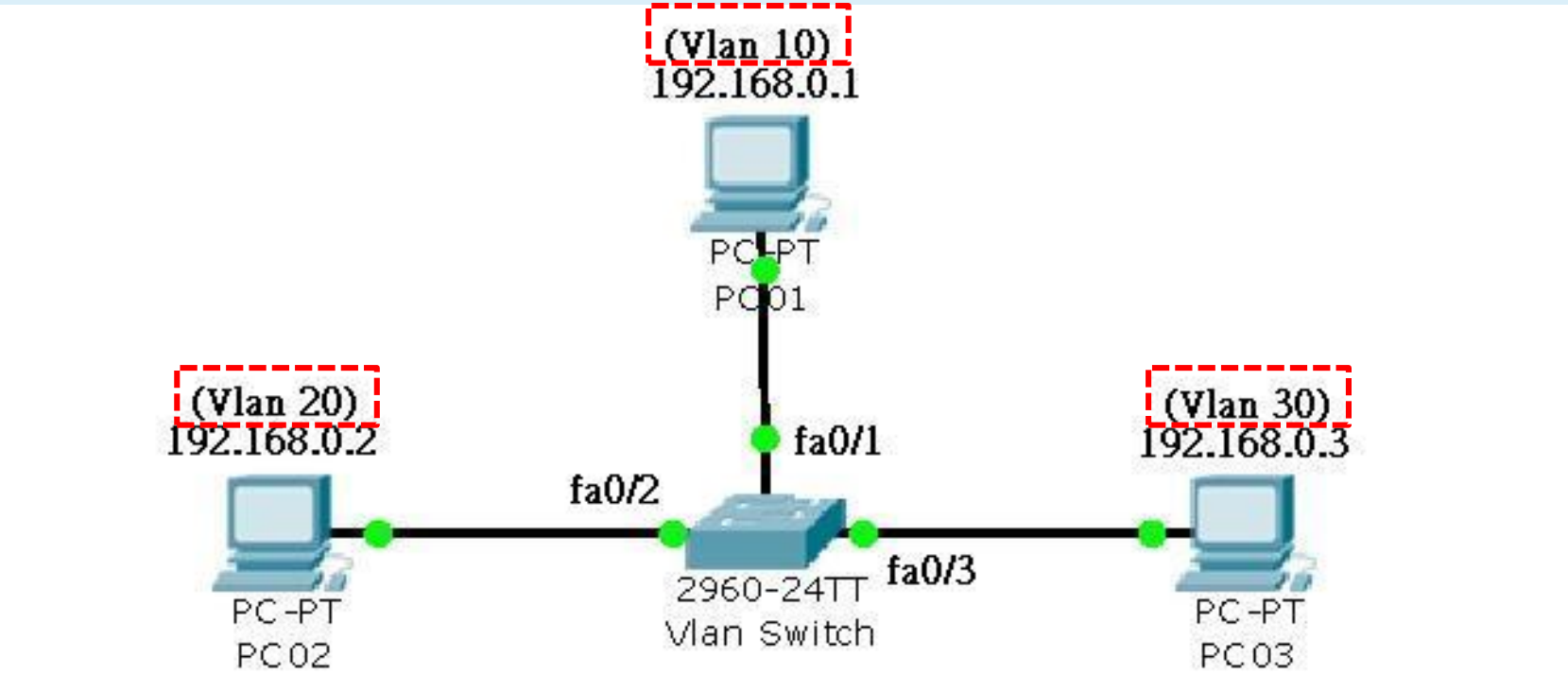
- 建立vlan 30 and vlan 5
- 將接L2與PC相連的port設定為正確vlan access port
- 測試
  - 相同vlan可以取得DHCP派發ip
    - 不同vlan，ip
    - 互 ping不通
    - 相同vlan相同網段可以互ping



Lab 基本練習Vlan

三個Vlan間三個網段 PC相互不通(Broadcast Domain)。

LAB目的知識：vlan能切割交換器成虛擬的多個區域網路



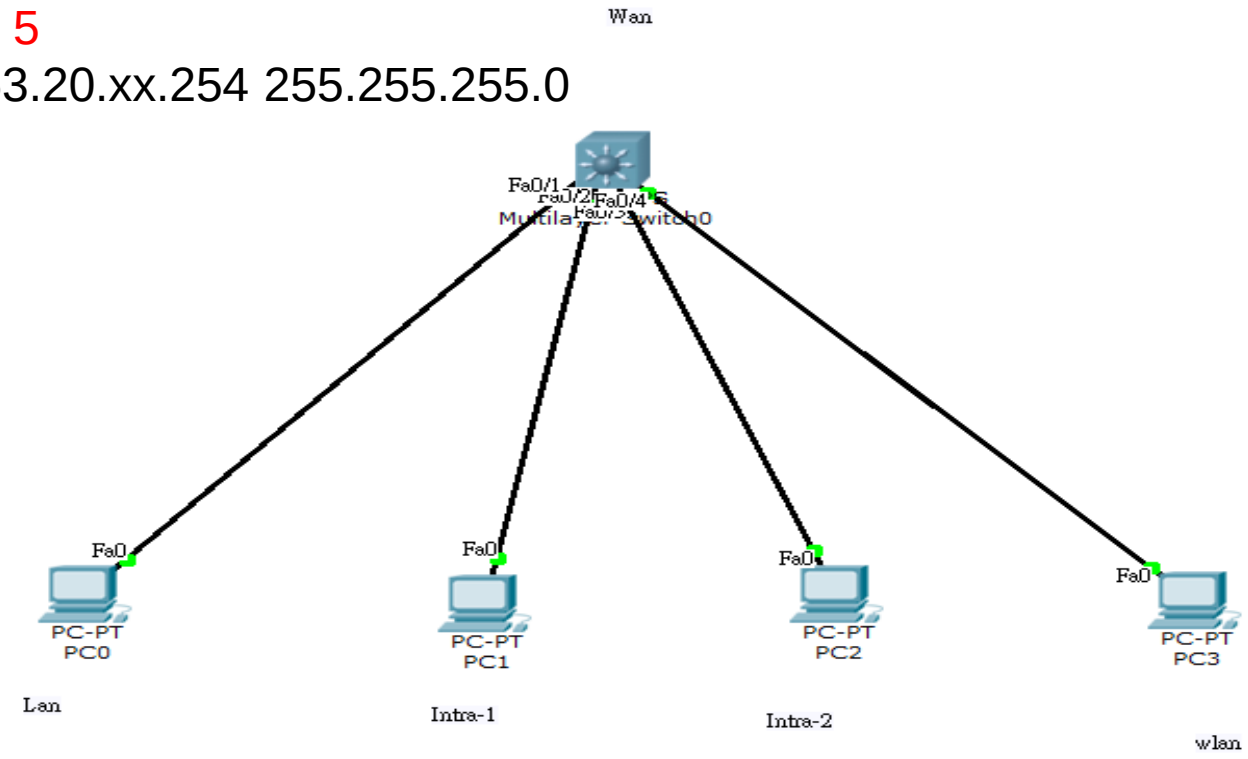
Lab 基本練習Vlan Interface

三個Vlan間三個網段 PC相互不通，做出每個網段Gateway。

LAB目的知識：不同網段要通，需透過路由器的路由表接通。

Inter vlan 5

Ip add 163.20.xx.254 255.255.255.0



校園網路Lab拓譜圖

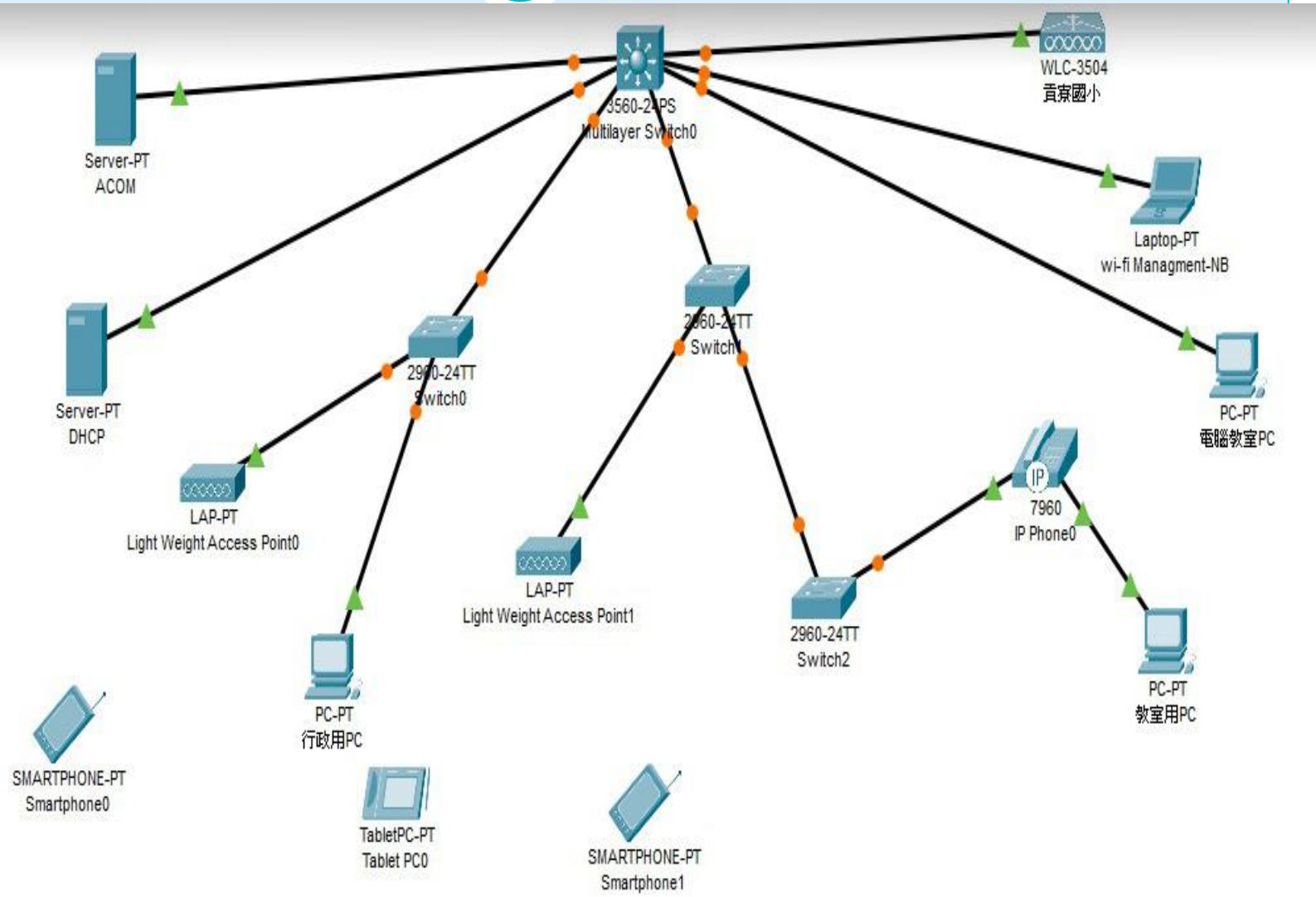
貢寮國小:
Gateway:10.229.12.254

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

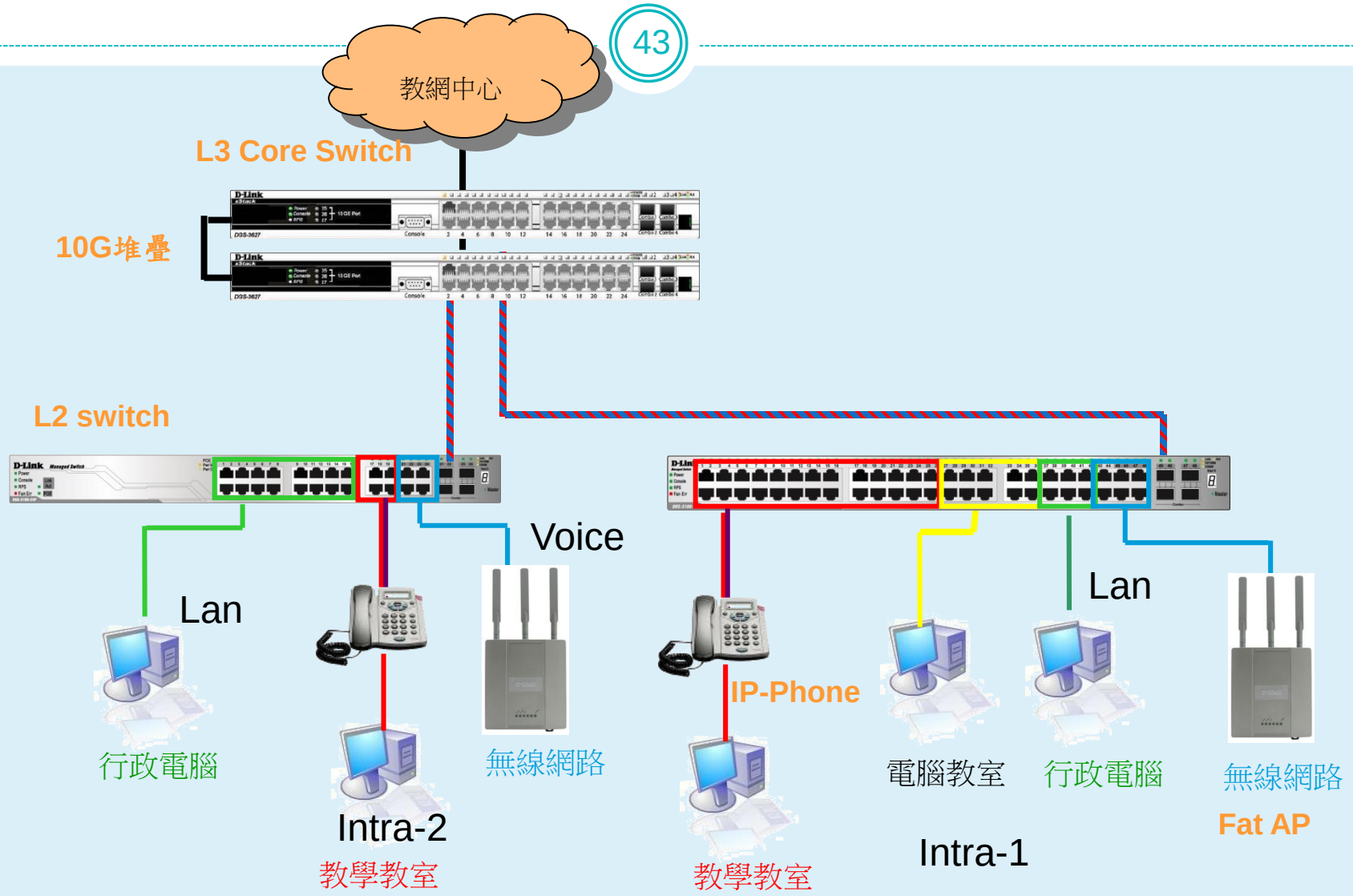
無線用31-TANetRoaming:10.212.12.0/24
無線用32-NTPC-Mobile :10.214.12.0/24
無線用33-Eduroam :10.216.12.0/24
無線用34-class:10.218.12.0/24

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



(實作資料) 學校ip分配表

- 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

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

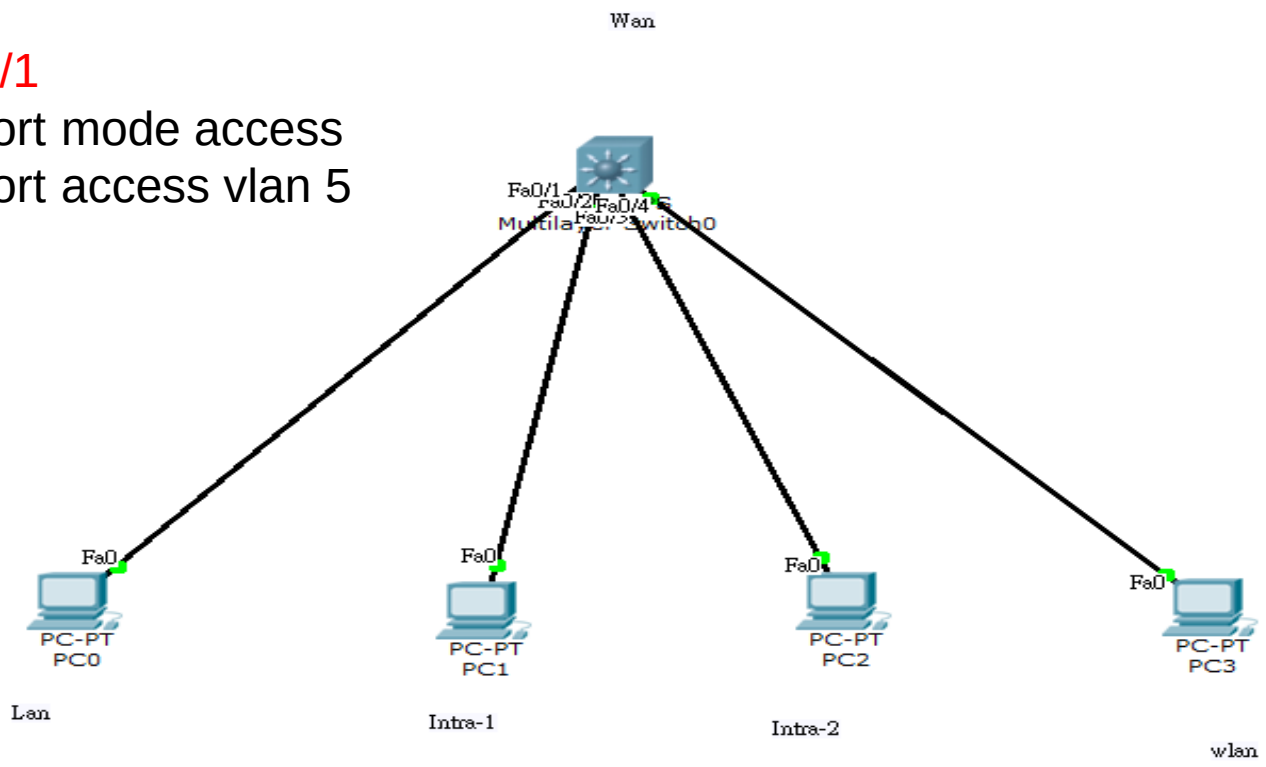
NEW

Vlan	VID	網段	IPv6	用途
TAnetRoaming	31	10.211.56.254	2001:288:22xx:31::/64	TAnetRoaming
NTPC-Mobile	32	10.213.56.254	2001:288:22xx:32::/64	NTPC-Mobile
eduroam	33	10.215.56.254	2001:288:22xx:33::/64	eduroam
class	34	10.217.56.254	2001:288:22xx:34::/64	class
IOT	70	10.239.56.254	2001:288:22xx:70::/64	IOT

Lab 基本練習Routing

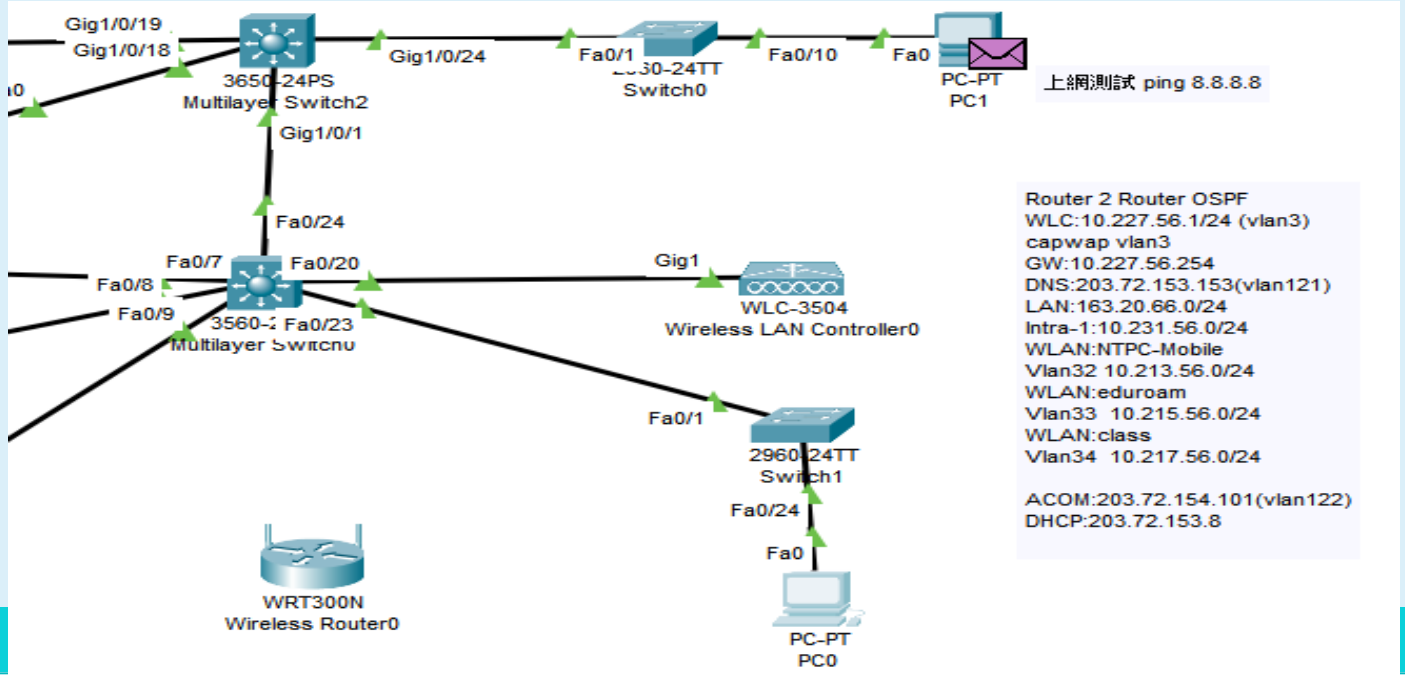
三個Vlan間三個網段 PC相互通。

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



唯一出口 Gateway 通往他國

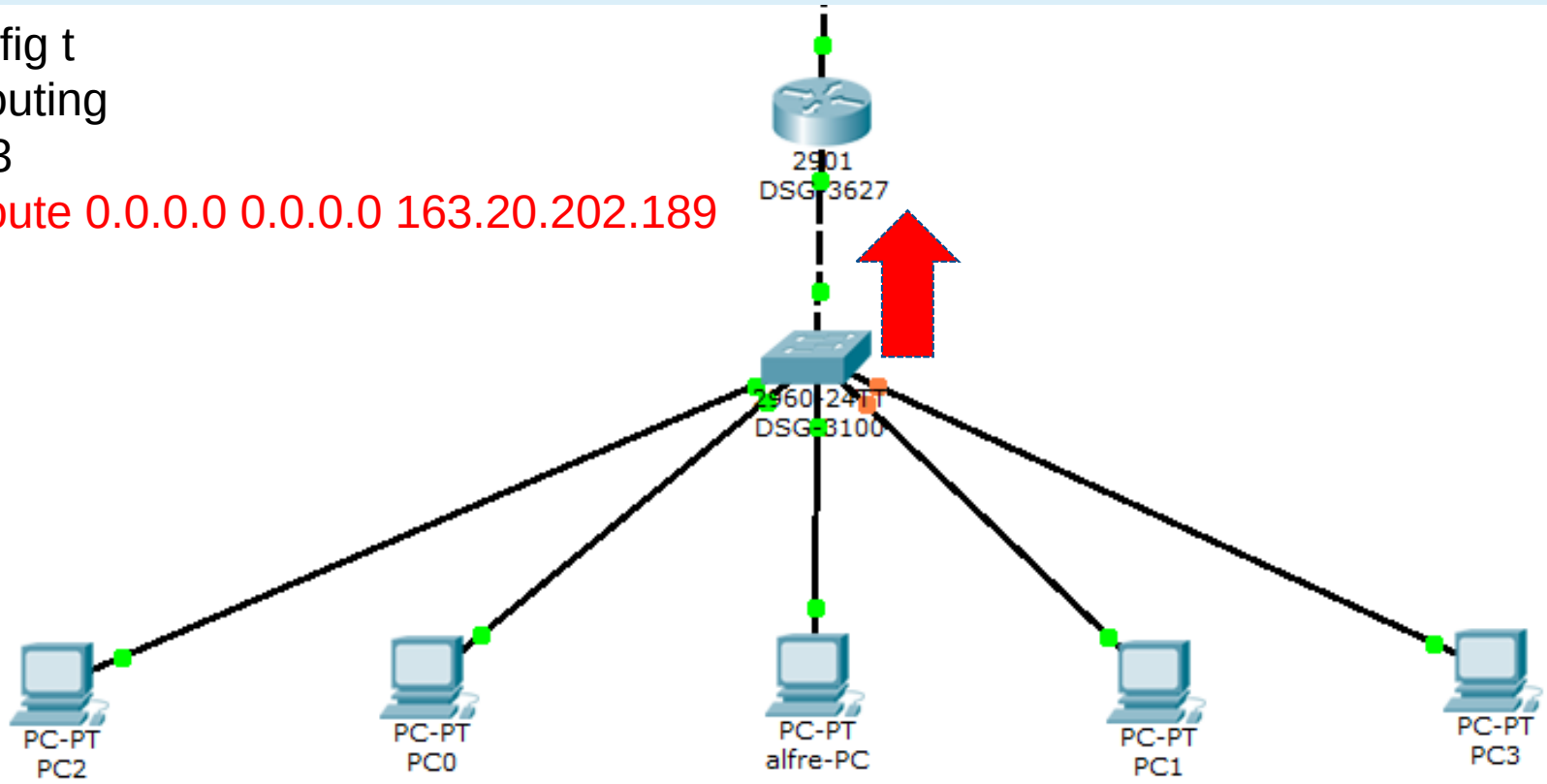
- 目的:了解GateWay閘道設定。
- 各個 vlan的出口 gateway，就是 vlan interface ip
- 校園網路出口(Gateway) 閘道wan (vlan2)。
- Route table中的default route 預設出口路由。
- Vlan擴充網段使用secondary ip



Lab 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
Ip route 0.0.0.0 0.0.0.0 163.20.202.189



Lab 與骨幹連結

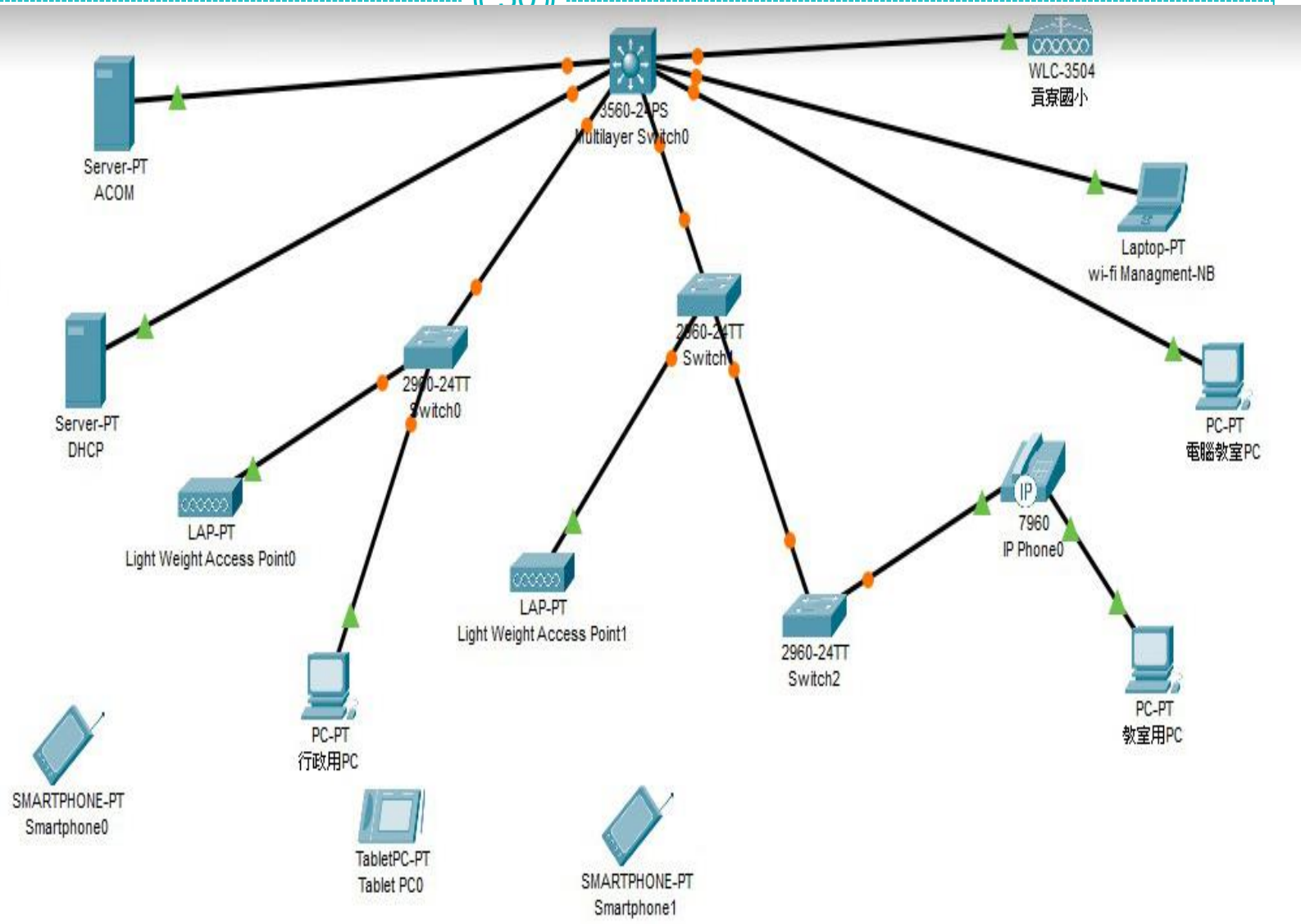
貢寮國小:
Gateway:10.229.12.254

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

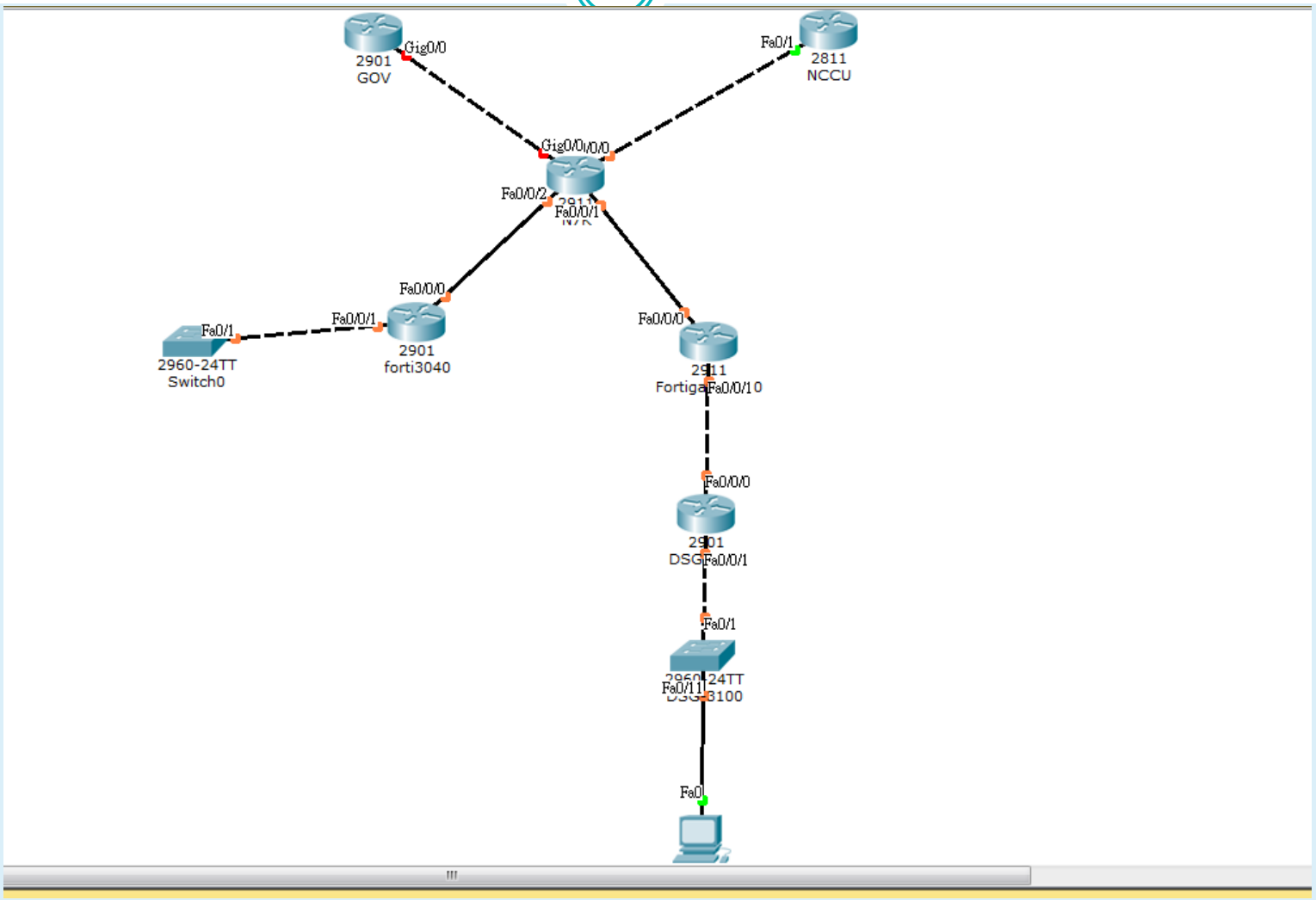
VLAN3-WLC
VLAN5-LAN
VLAN10-intra-1
VLAN20-intra-2
VLAN25-VOIP
VLAN31-TANetRoaming
VLAN32-NTPC-Mobile
VLAN33-eduroam
VLAN34-class
VLAN121-DHCP-DNS
VLAN122-Acom



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



END