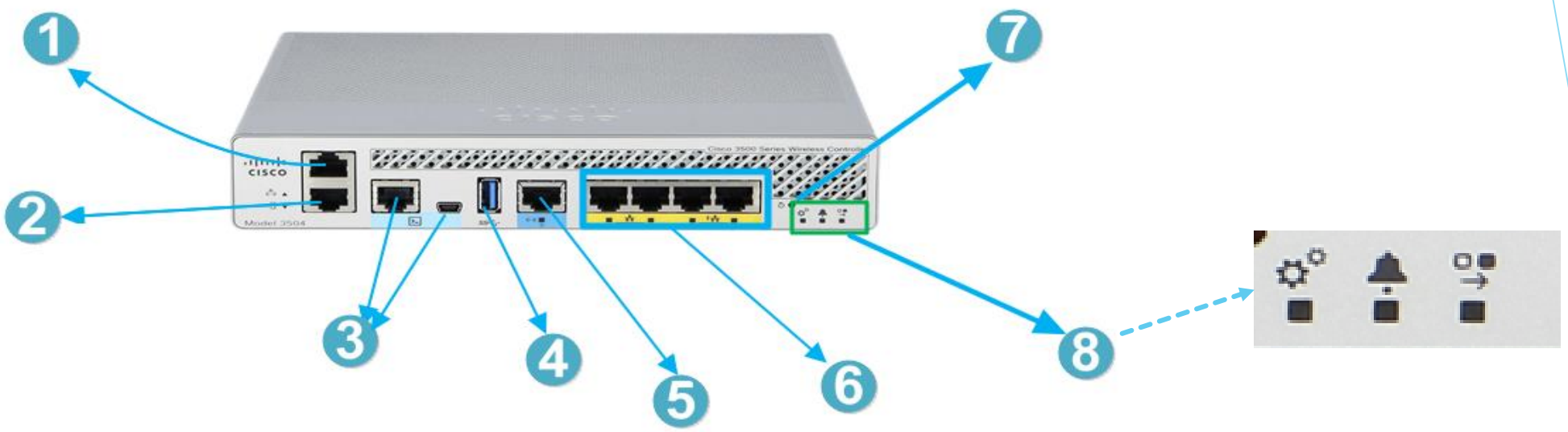
設備命名、IP設定規則

設備	Hostname	IP Address	數量
Cisco WLC 3504	校碼後三碼+WLC	10.xxx.xxx.1	1
保留		10.xxx.xxx.2~10	9
Cisco AP 2802	校碼後三碼+AP+教室碼	10.xxx.xxx.11~125	115
LevelOne 5 Port Switch	校碼後三碼+5P+教室碼	10.xxx.xxx.126~240	115
Cisco Switch 2960 24/48 Port	校碼後三碼+L2+棟號+樓層編號	10.xxx.xxx.241~252	12
保留		10.xxx.xxx.253	1
Gateway		10.xxx.xxx.254	1
Cisco WLC 8540	NTPC_WLC	203.72.154.115	1
Cisco ISE 3515	NTPC_ISE	203.72.154.116	1
NTP Server		163.20.254.254	
DNS Server		203.72.153.153, 203.72.153.154	
DHCP Server		203.72.153.8, 203.72.153.9， 203.72.153.38	

※ 若小校無教室碼，則依棟號+樓層編號+教室編號（由左至右數）。

Cisco 3504 WLC/AC



1	Service Port for Out-of-Band Management port
2	Redundancy Port
3	console ports There is a serial RJ45 console port and a mini USB port
4	USB 3.0 Port used to perform Software Updates
5	mGig Port Data Connectivity configured
6	GiGE Ports (⚡ Port 3 and Port 4 have Poe out)
7	Reset
8	Status LED(System LED, Alarm LED and High Availability LED.)

Cisco 3504 WLC/AC設定

- 進行WLC 3504出廠
- 按完Reset扭，注意看會有要按ESC 然後選擇1，接著才有步驟精靈
- 初始化使用Console Port 進入
- 如使用Service Port進入，預設是192.168.0.x網段 http://192.168.0.1

Cisco 3504 WLC/AC設定

CLI Wizard初始化設定：

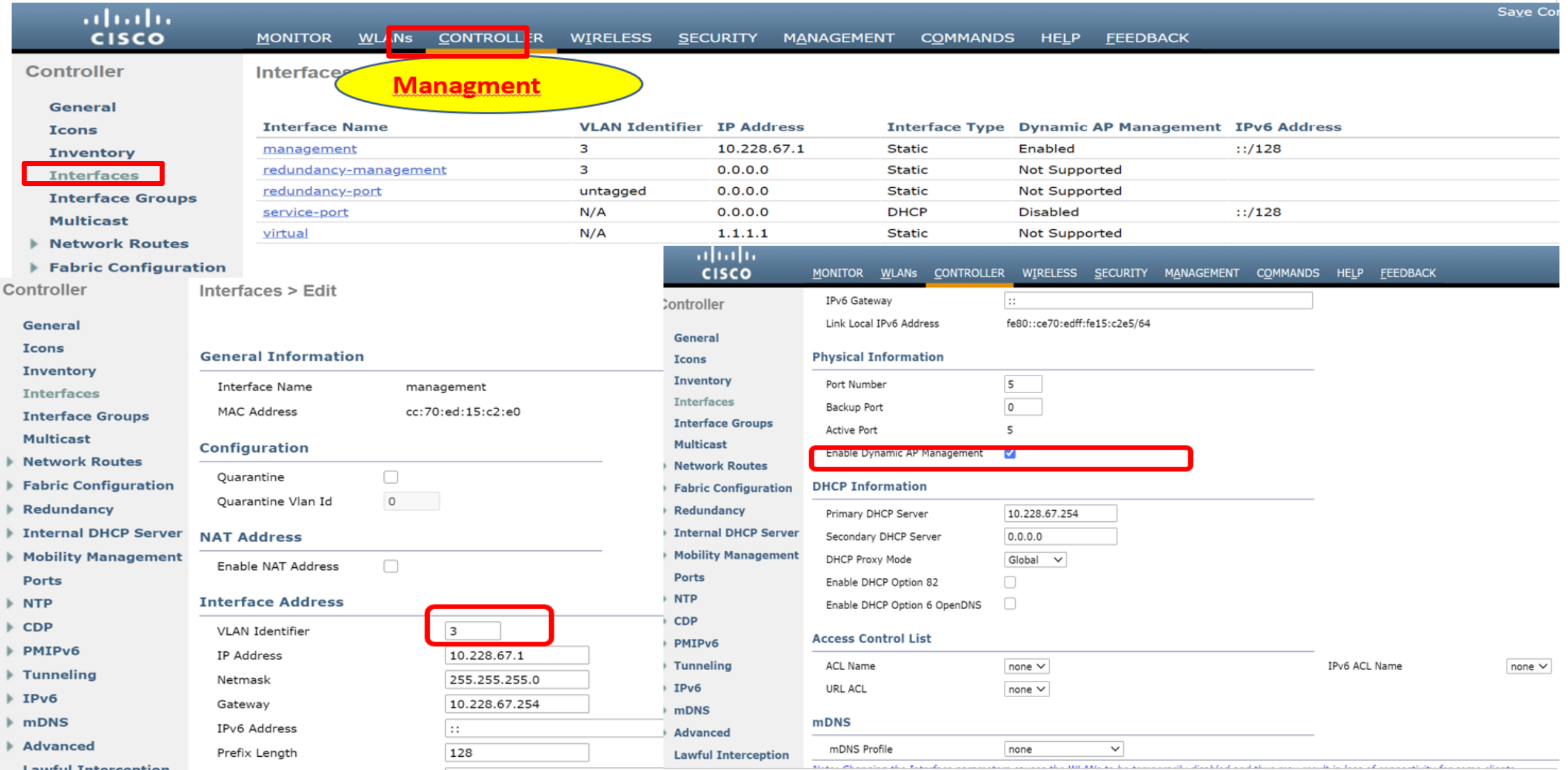
AUTO-INSTALL: process terminated -- no configuration loaded

Enter Administrative User Name (24 characters max):Cisco
Enter Administrative Password (3 to 24 characters):
Re-enter Administrative Password:
→ 建立管理者的帳號及密碼。
Service Interface IP Address Configuration [static][DHCP]:
→ Out Band Management 的設定，沒特殊定義時可直接Enter或設定DHCP。
Enable Link Aggregation (LAG) [yes][NO]: NO
→ 目前環境不啟用LAG，啟用LAG會將所有的 Port 一起啟用。
mGig Port Max Speed [1000][2500][5000]:1000
→ 目前環境速度設定 1G。
Management Interface IP Address:
Management Interface Netmask:
Management Interface Default Router
Cleaning up Provisioning SSID
Management Interface VLAN Identifier (0 = untagged):
Management Interface Port Num [1 to 5]: 5
Management Interface DHCP Server IP Address:
→ 目前環境定義的以第五Port拿來做管理界面。

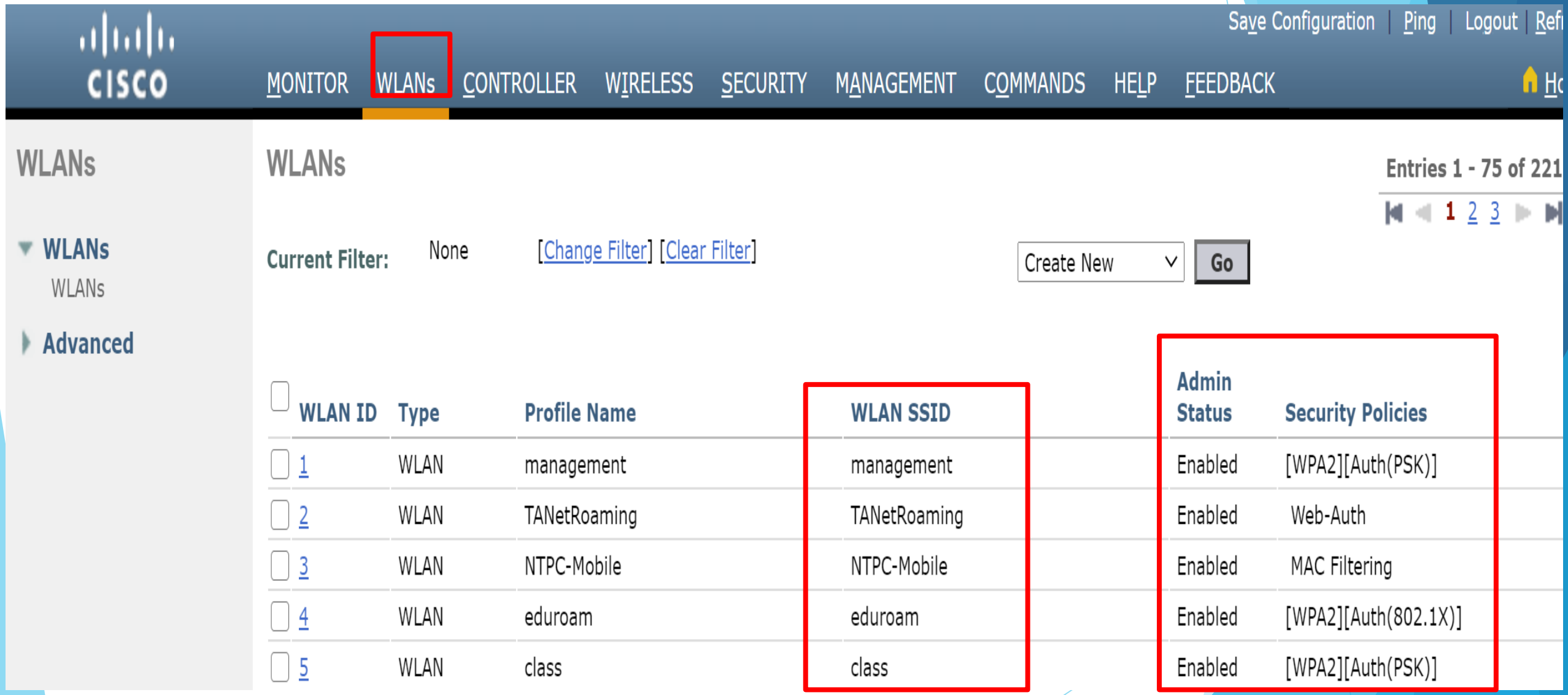
SSID 及加密認證方式

SSID	Vlan	認證
TANetRoaming	31	Web Portal
NTPC-Mobile5G	32	MAC
eduroam	33	802.1x
Class NTPC-Mobile2.4G	34	學校名稱+教室碼 (ex. SCPS-101) MAC

Cisco 3504 WLC/AC　Interface 設定

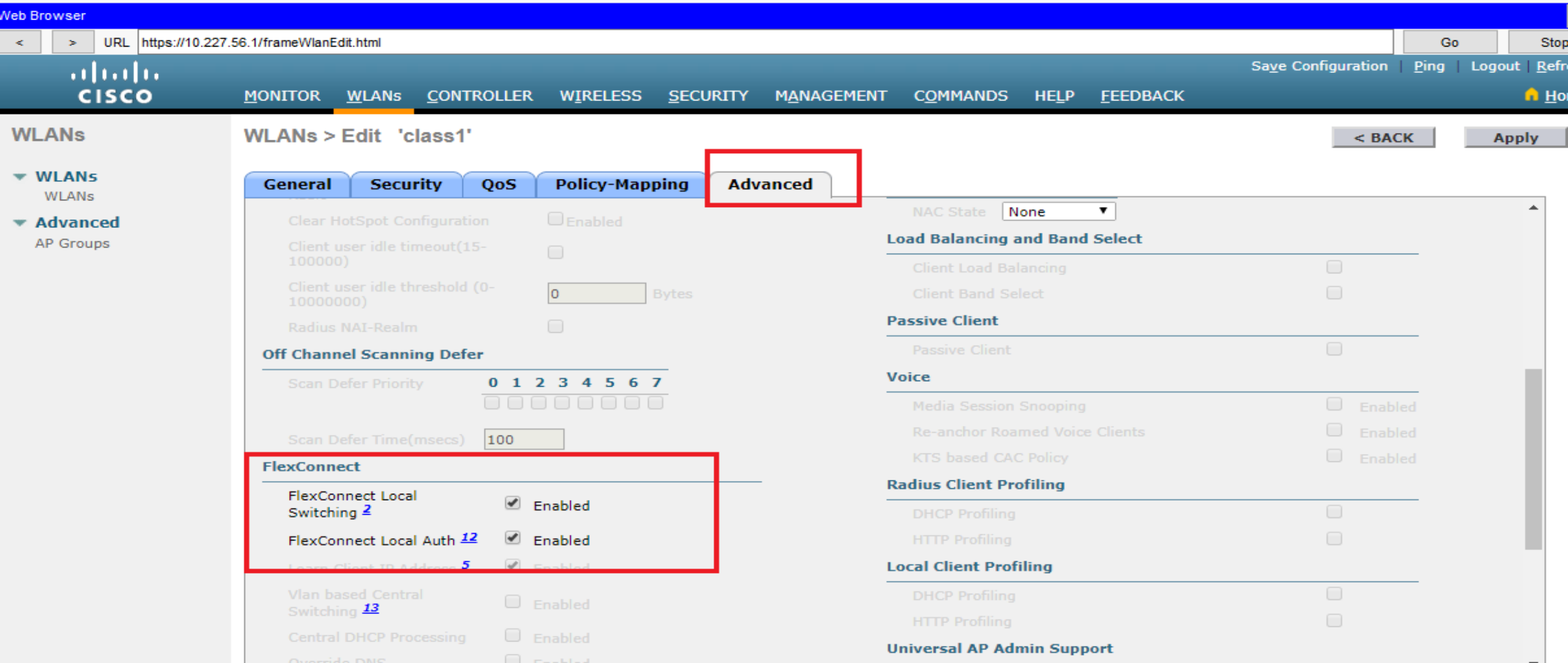


Cisco 3504 WLC/AC　WLAN SSID設定

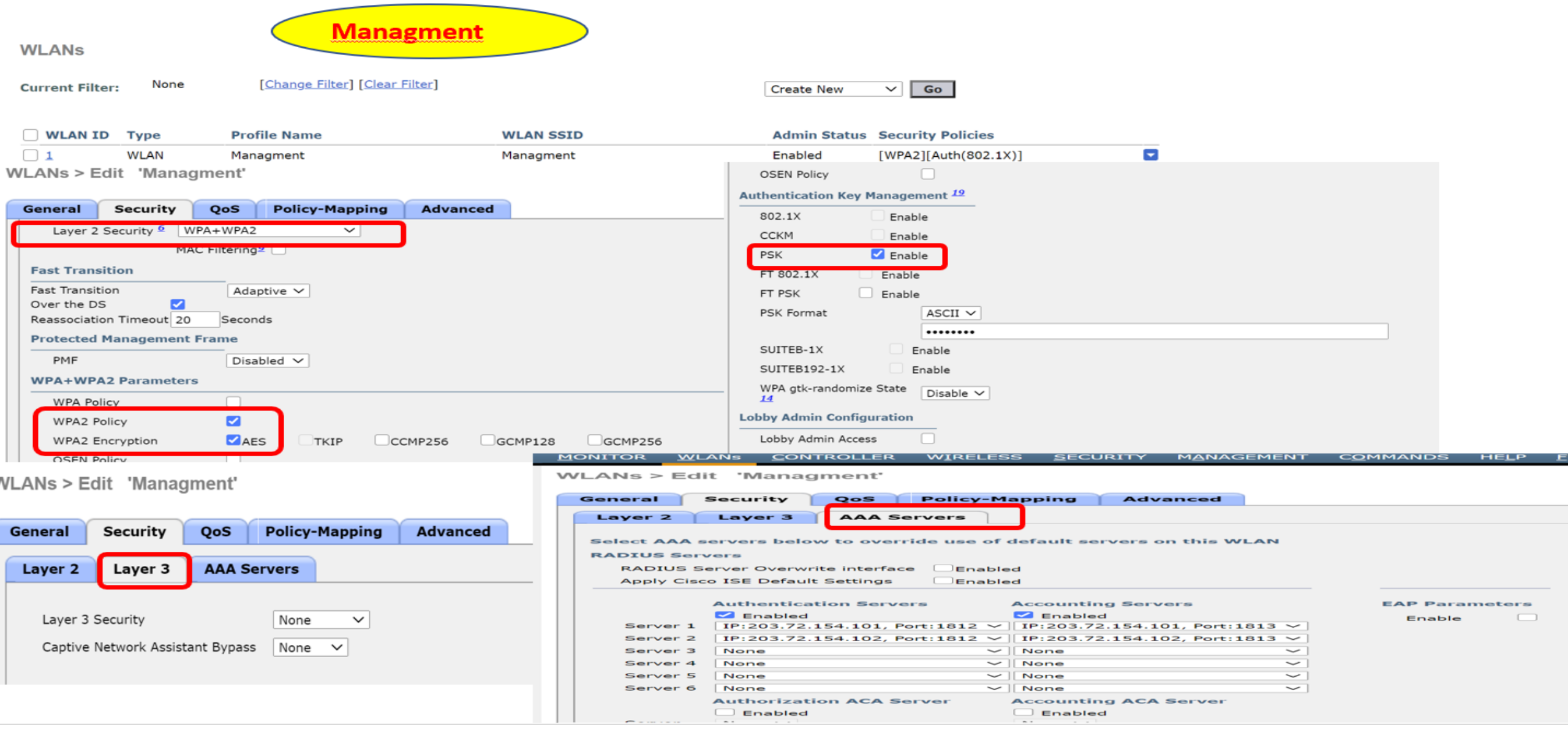


Cisco 3504 WLC/AC　WLAN SSID設定

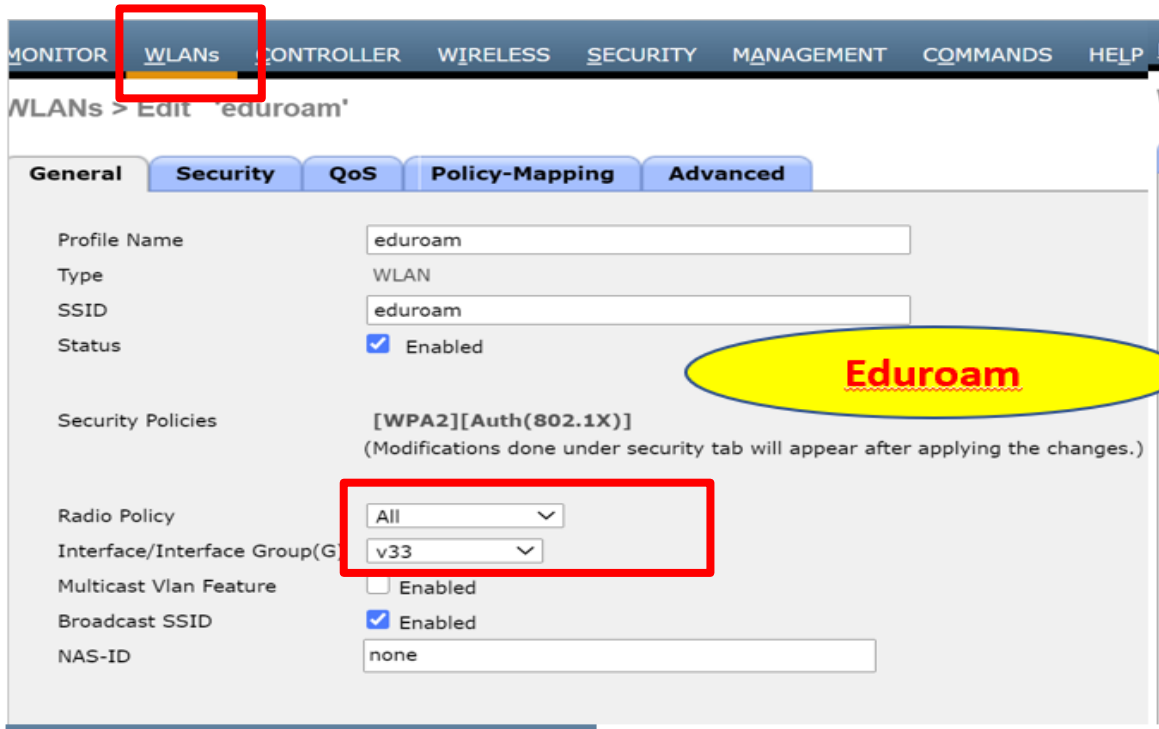
SSID 要走的介面

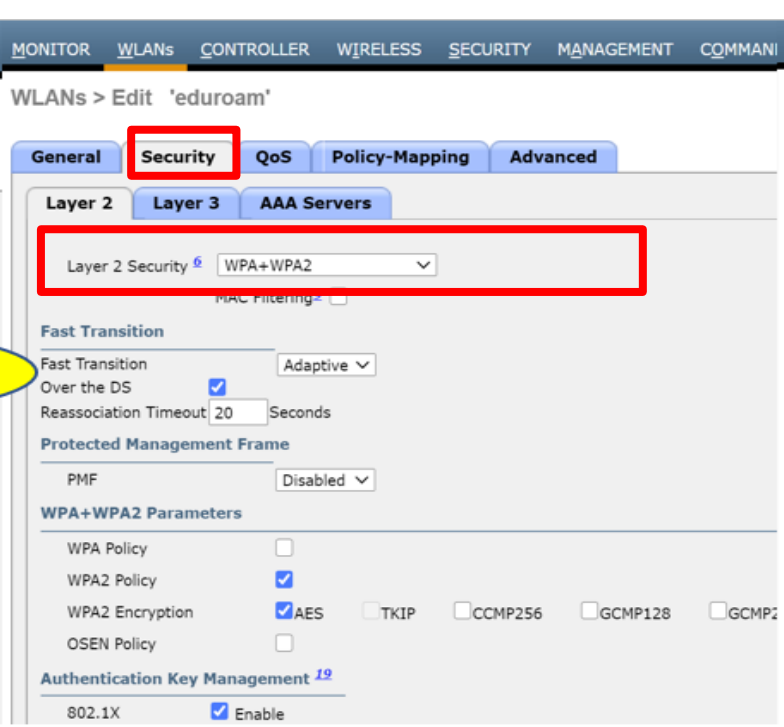


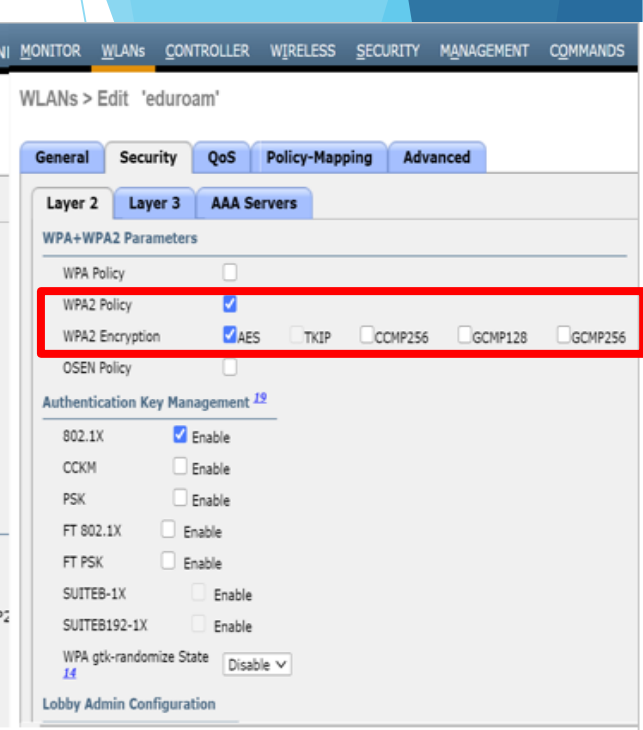
Cisco 3504 WLC/AC　WLAN SSID設定

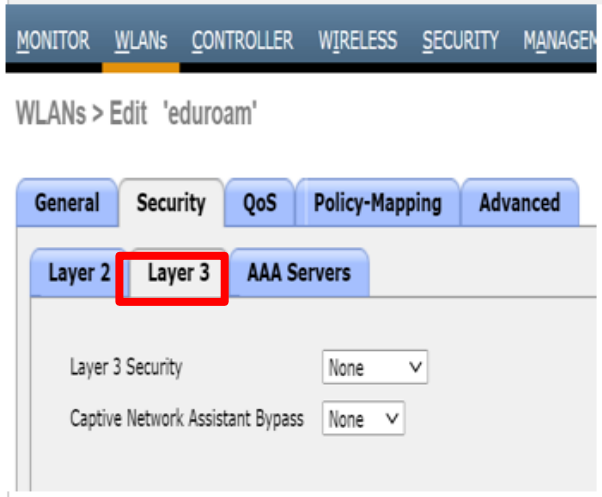


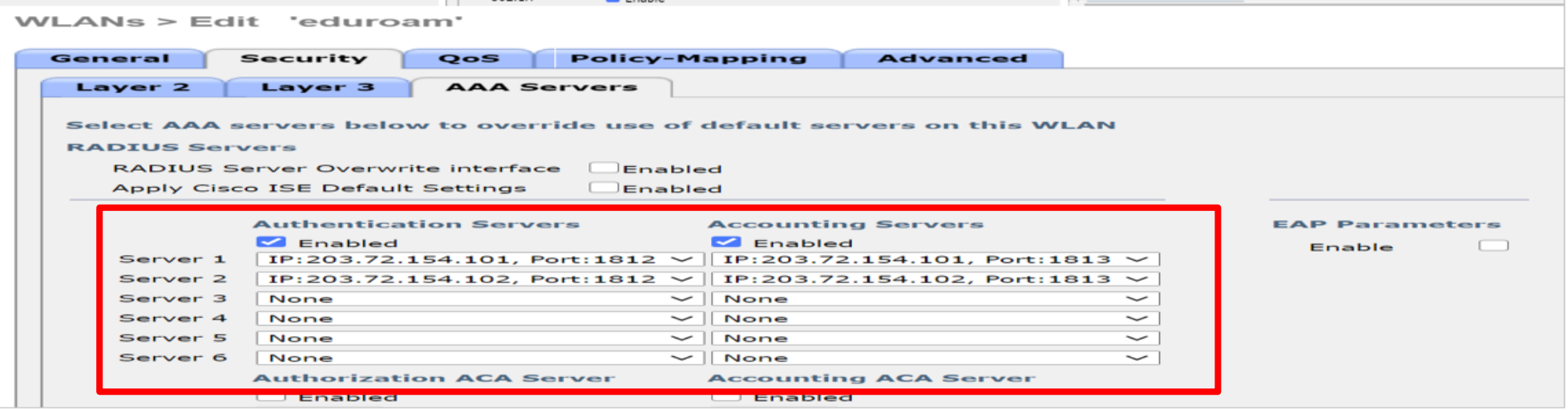
Cisco 3504 WLC/AC　WLAN SSID設定



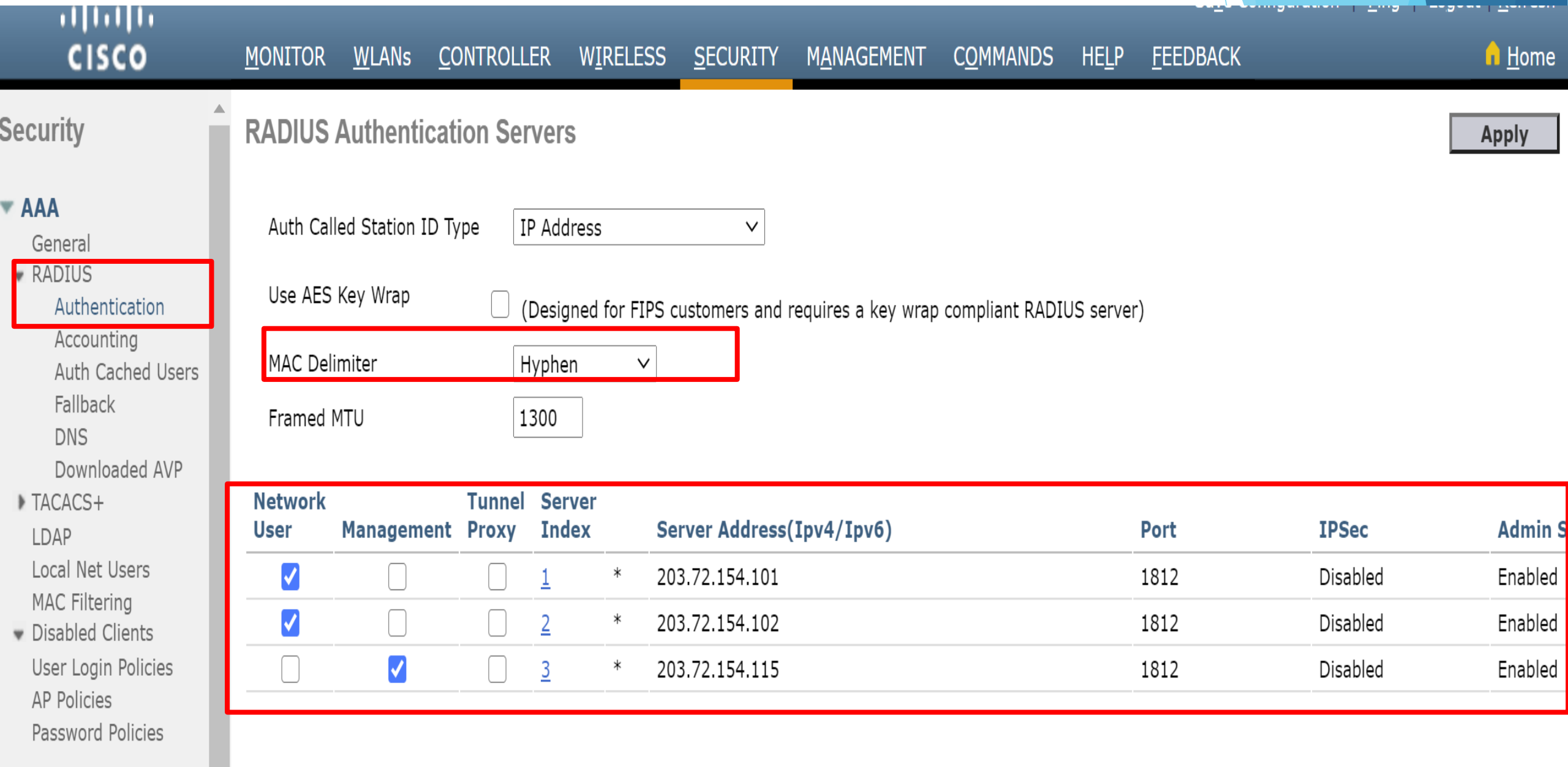




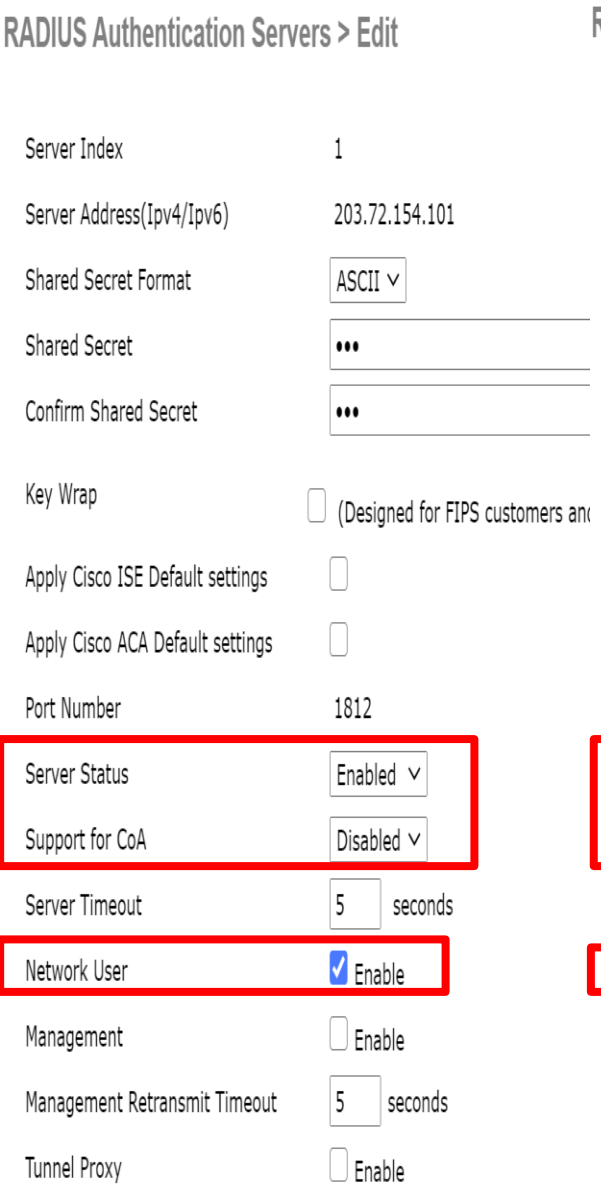


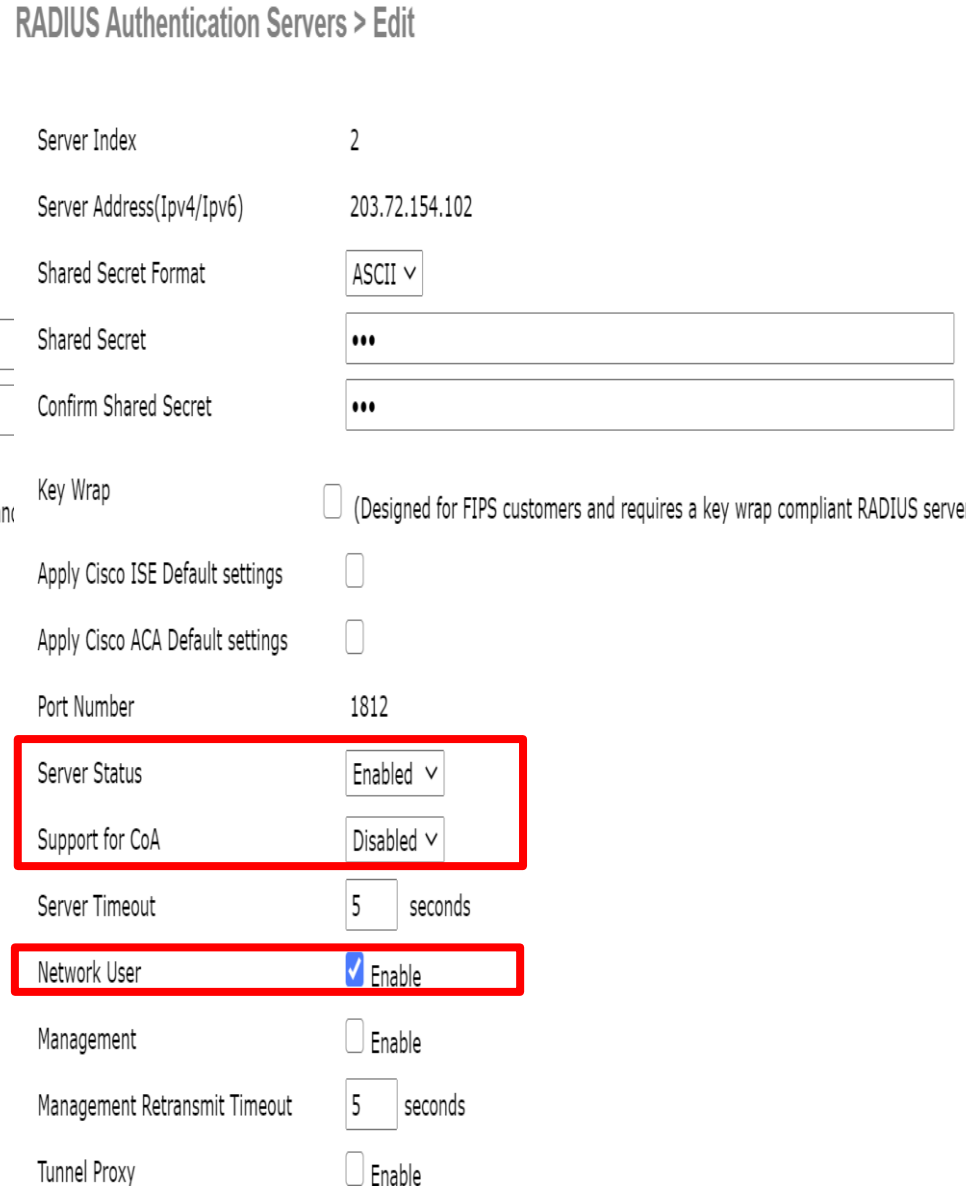


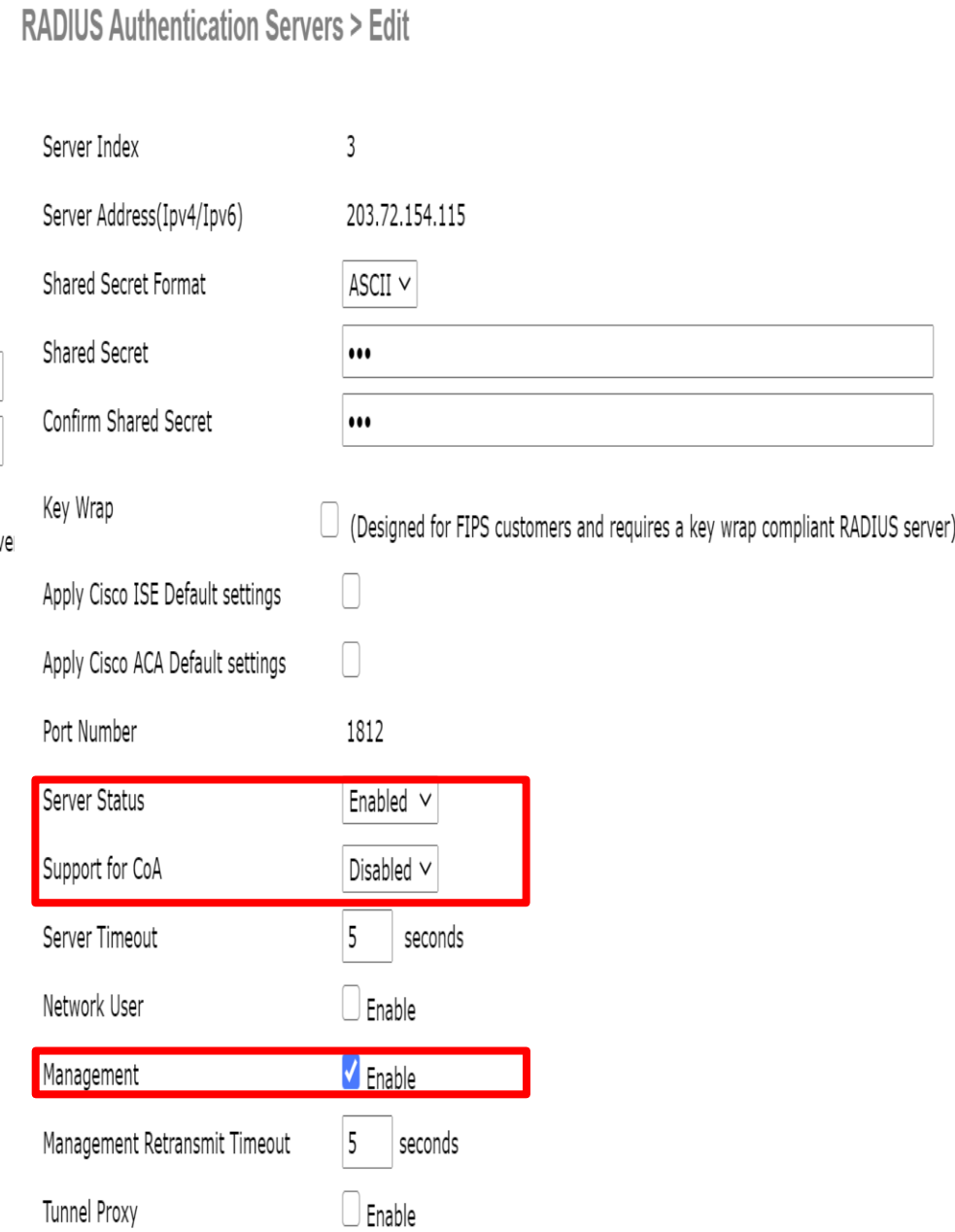
Cisco 3504 WLC/AC RADUIS Authentication



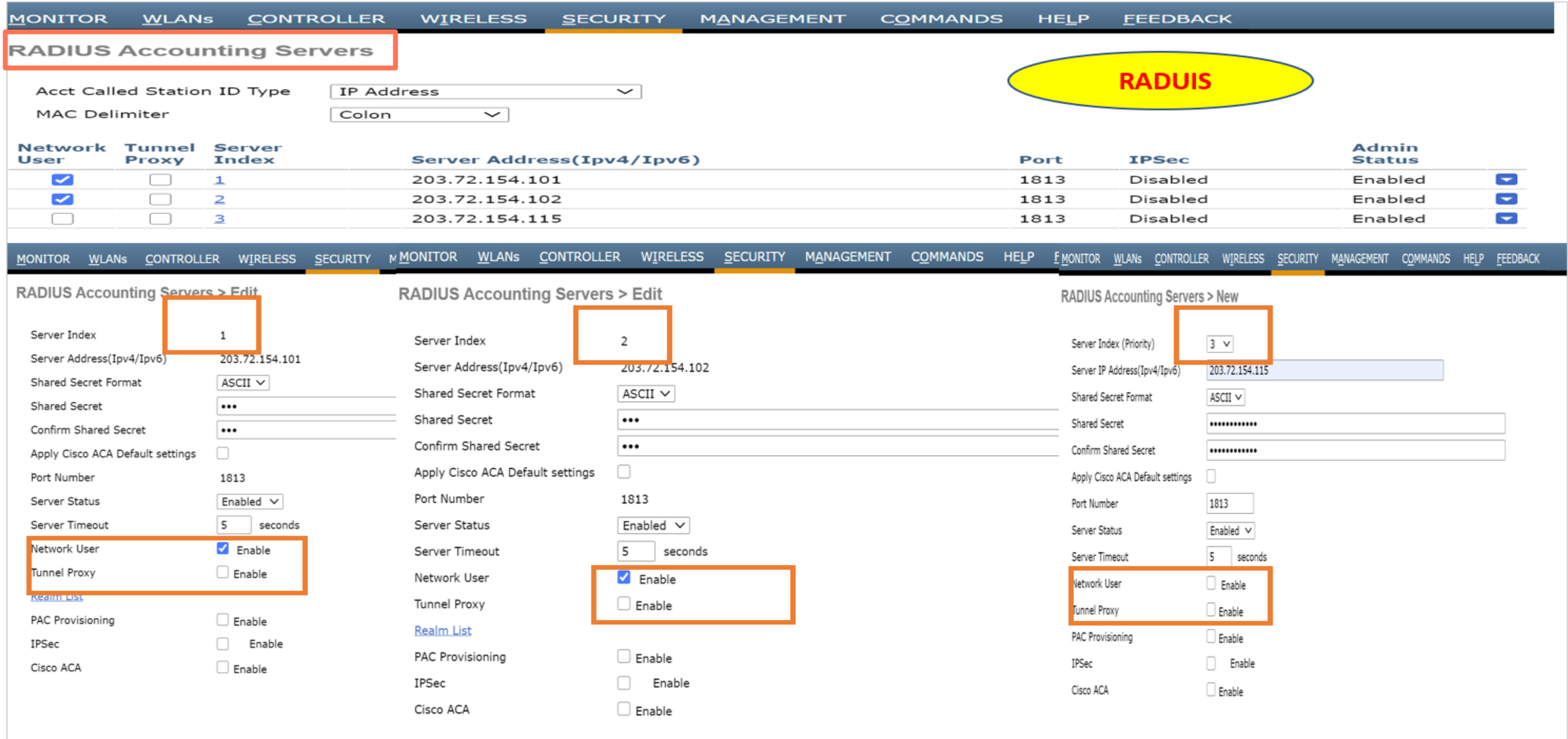
Cisco 3504 WLC/AC RADUIS Authentication



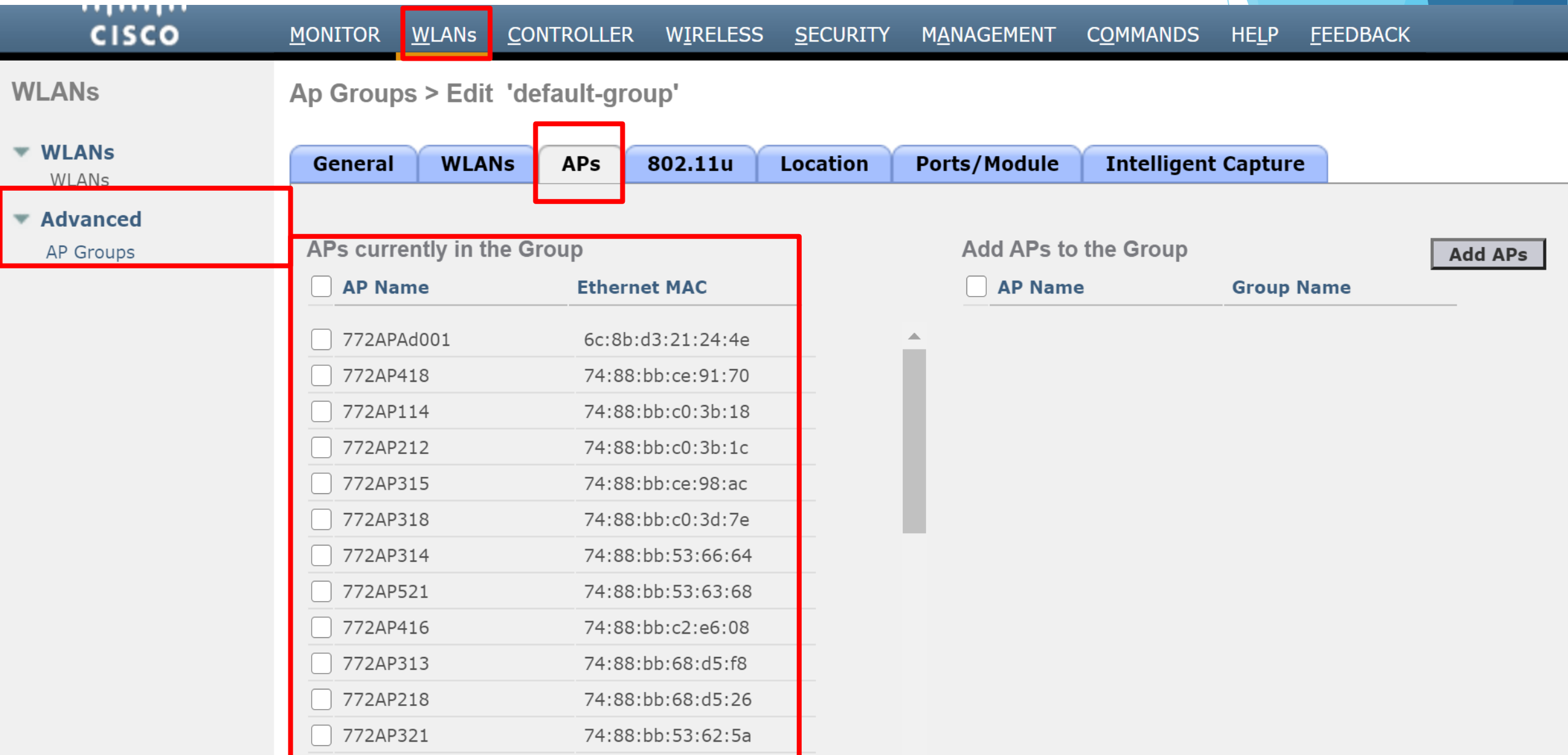




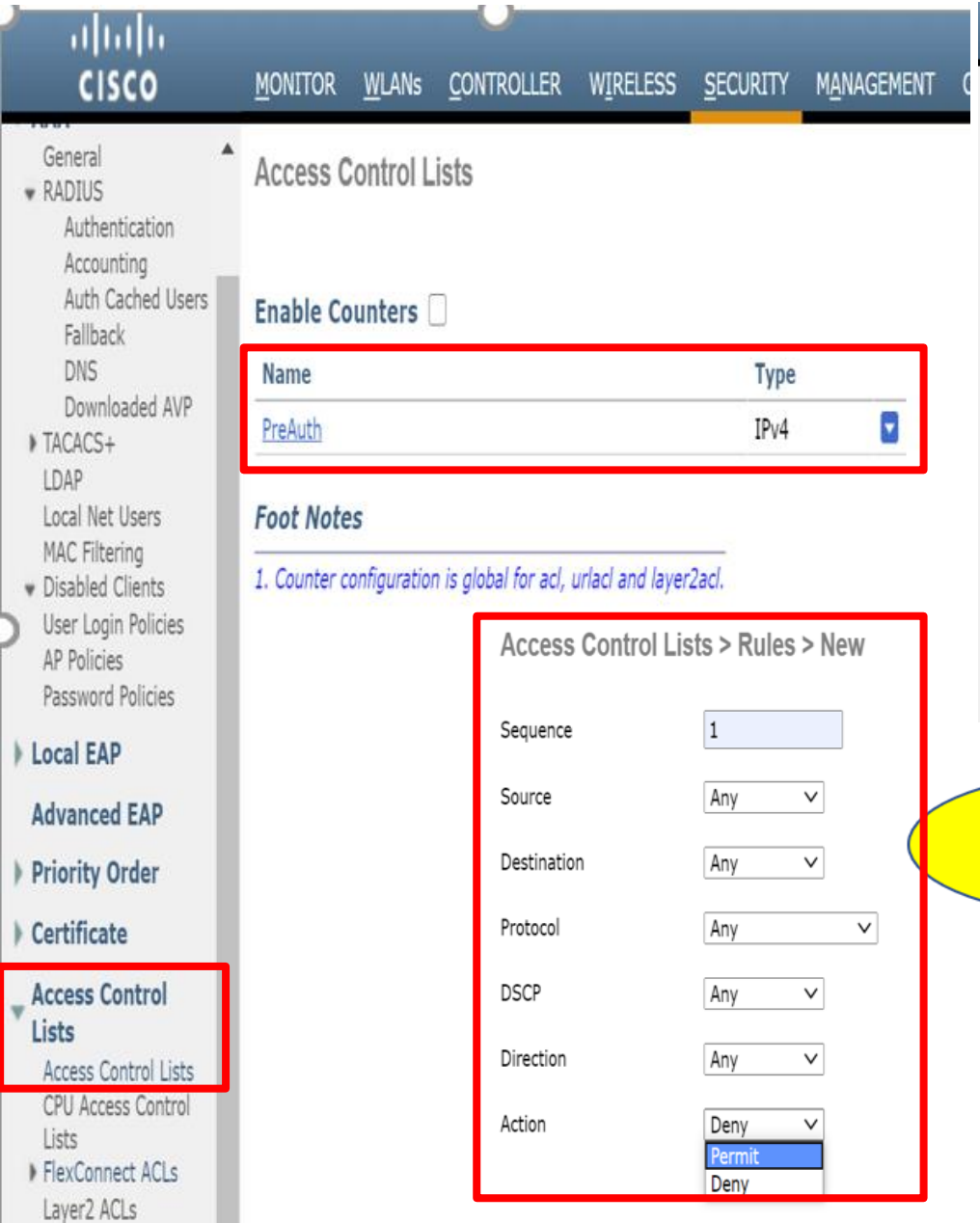
Cisco 3504 WLC/AC RADUIS Accounting servers

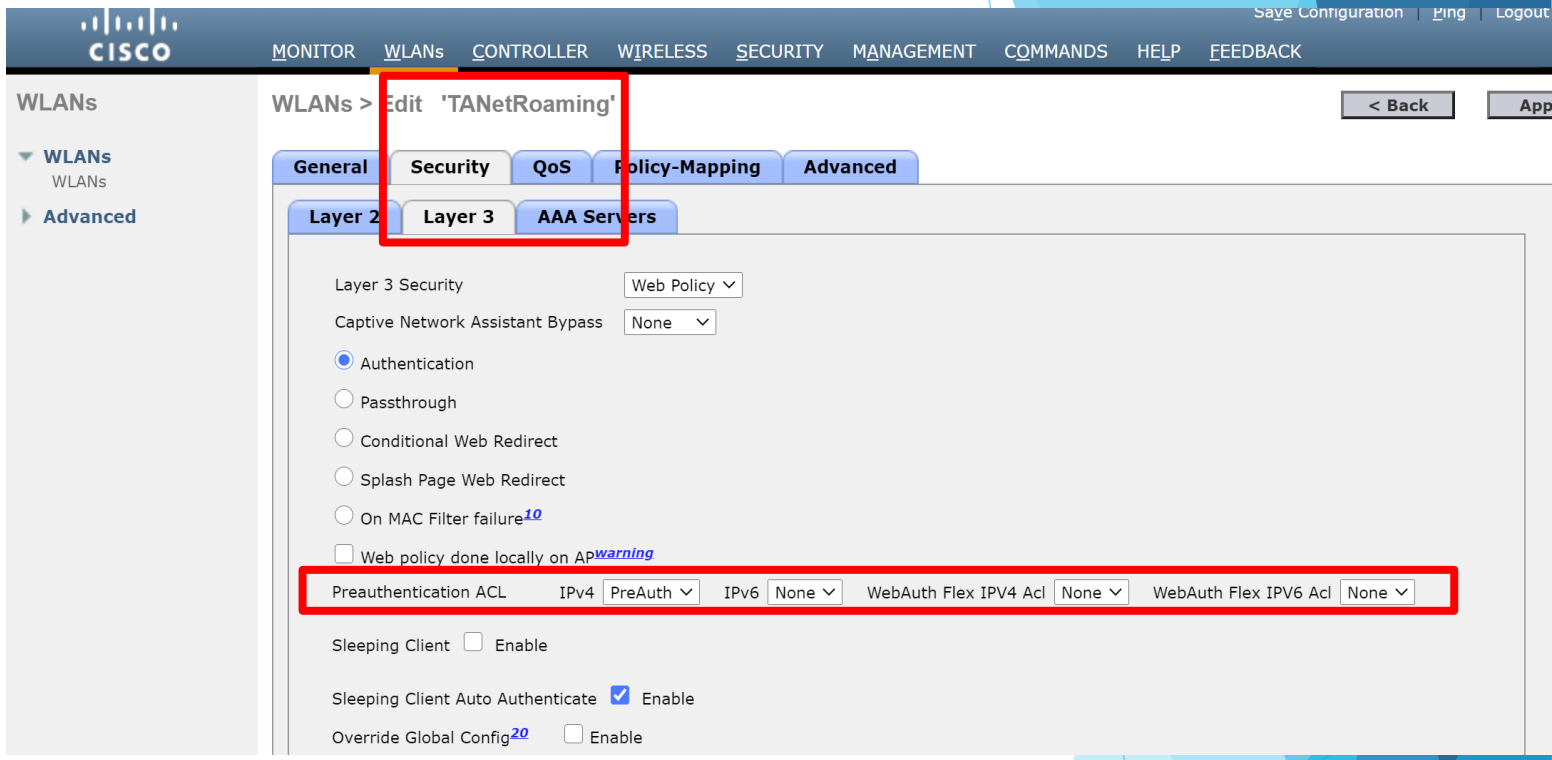


Cisco 3504 WLC/AC設定



Cisco 3504 WLC/AC設定





ACL police

CAPWAP 介紹

- CAPWAP (Control and Provisioning of Wireless Access Points)
  傳統的WLAN體系結構已經無法滿足大規模組網的需求，因此，IETF成立了CAPWAP (無線接入點的控制和配置協議) 工作組，研究WLAN的解決方案 。以實現各個廠家控制器與AP間的互通。

- 提供佈建由 WiFi Controller 控管下的 WiFi 網路間的通訊, Thin AP的設計是遵循CAWAP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。

- CAPWAP協議從發現階段開始，ＡＰs發送一個發現請求消息，任何接收到這個請求的ＷＬＣ將會回應一個發現回應資訊。接收到發現響應資訊，ＡＰ選擇一個ＷＬＣ來建立一個 基於DTLS的安全會話。

CAPWAP 協議主要功能

- CAPWAP（無線接入點控制和配置協議），用於無線終端接入點（AP）和無線網絡控制器（AC）之間的通信交互，實現AC進行所關聯的AP集中管理和控制。

該協議包含的主要內容有：

1.AP對AC的自動發現及AP和AC的狀態機運行，維護。
2.AC對AP進行管理，設定配置下發。
3.STA數據封裝CAPWAP隧道進行轉發。

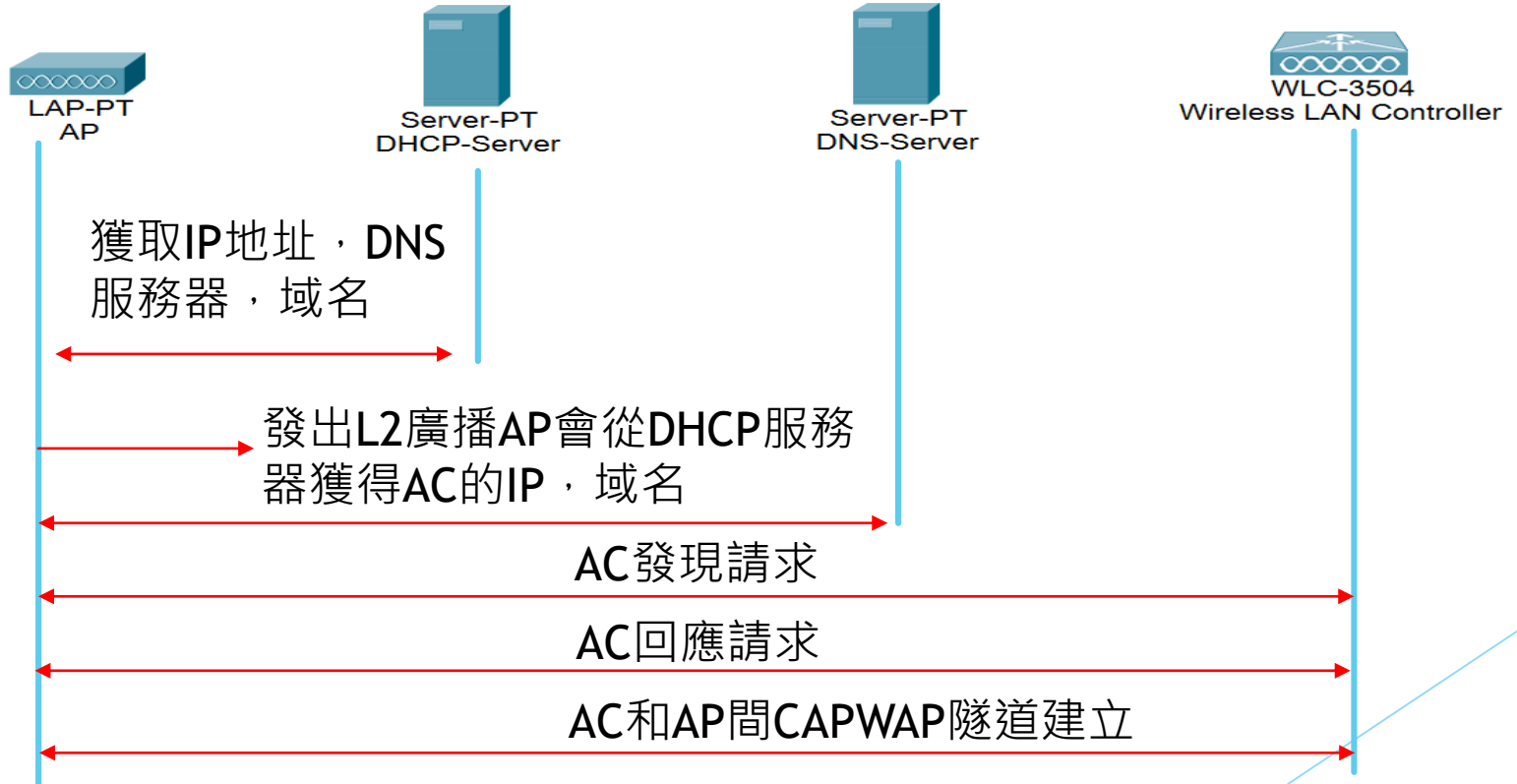
CAPWAP運作(AP Discover AC)

- 當存在預配置的AC IP列表時，則AP直接啟動預配置靜態發現流程並與指定的AC連接。如果未配置AC IP列表，則啟動AP動態發現AC機制，執行DHCP / DNS /廣播發現流程後與AC連接。

1.AP啟動以後會通過DHCP獲取IP地址，DNS服務器，域名。

2.AP發出L2廣播請求試圖聯繫一個AC。

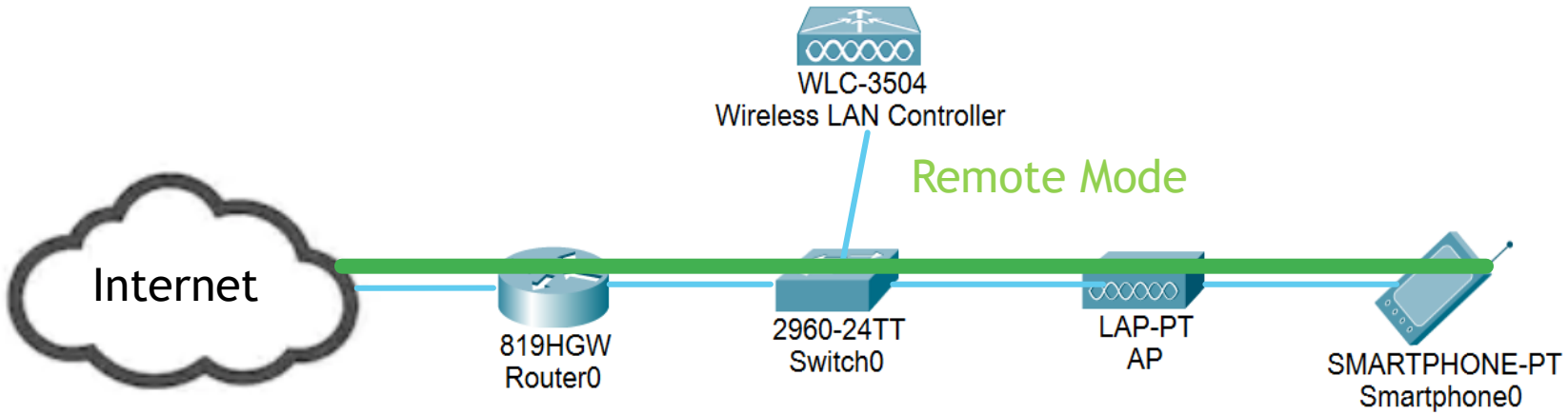
3.AP會從DHCP服務器通過Option43獲得AC的IP，或者通過Option15獲得AC的域名，AP向該IP地址（域名）發送發現請求。接收到發現請求的AC會檢查該AP是否有接收本機的權限，如果有則回應發現響應。AC和AP間建立CAPWAP隧道。



CAPWAP Bridge Mode 傳送流量模式

Bridge Mode 特點

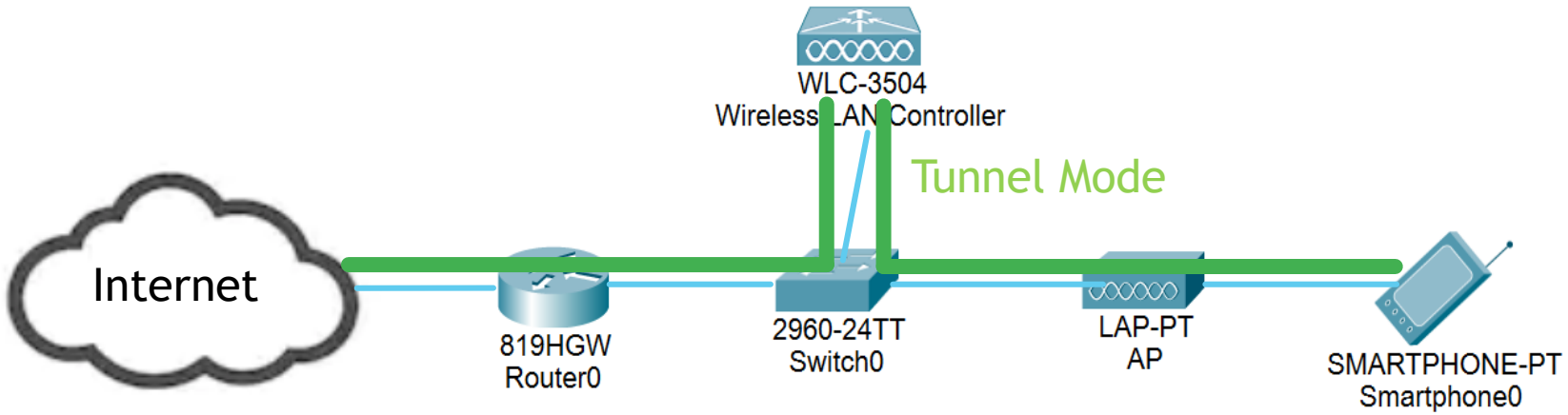
- 提高多人在無線區域網路內傳送檔案的速度
- 提高單台WLC可納管的AP數量
- 可控制定義AP的Profile



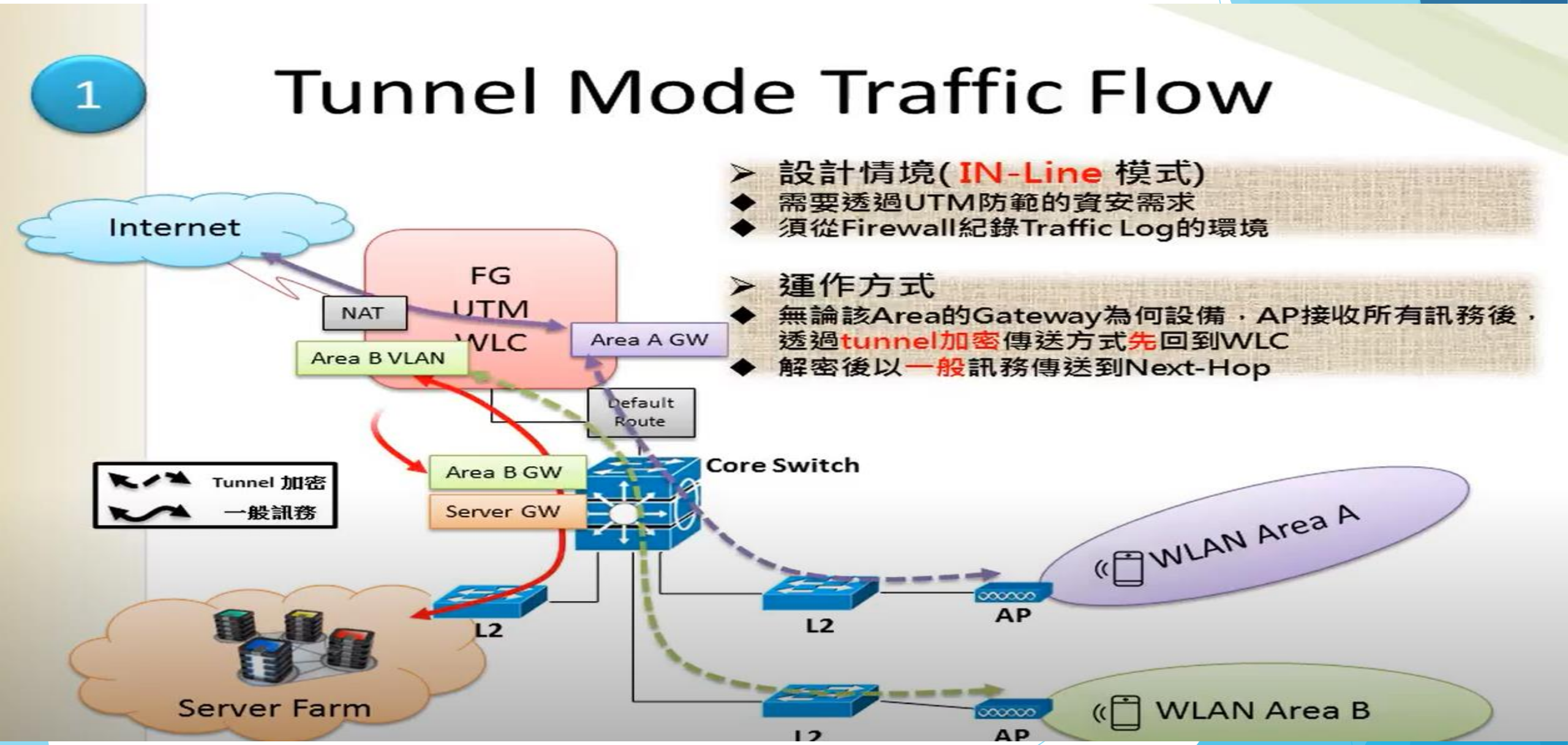
CAPWAP Tunnel Mode 傳送流量模式

Tunnel Mode特點

- 由AP至WLC之間的傳輸皆可透過加密保護
- 所有網路流量可受到多一層設備資安功能保護
- 可控制定義AP的Profile，可完整監視或防護所有無線網路流量

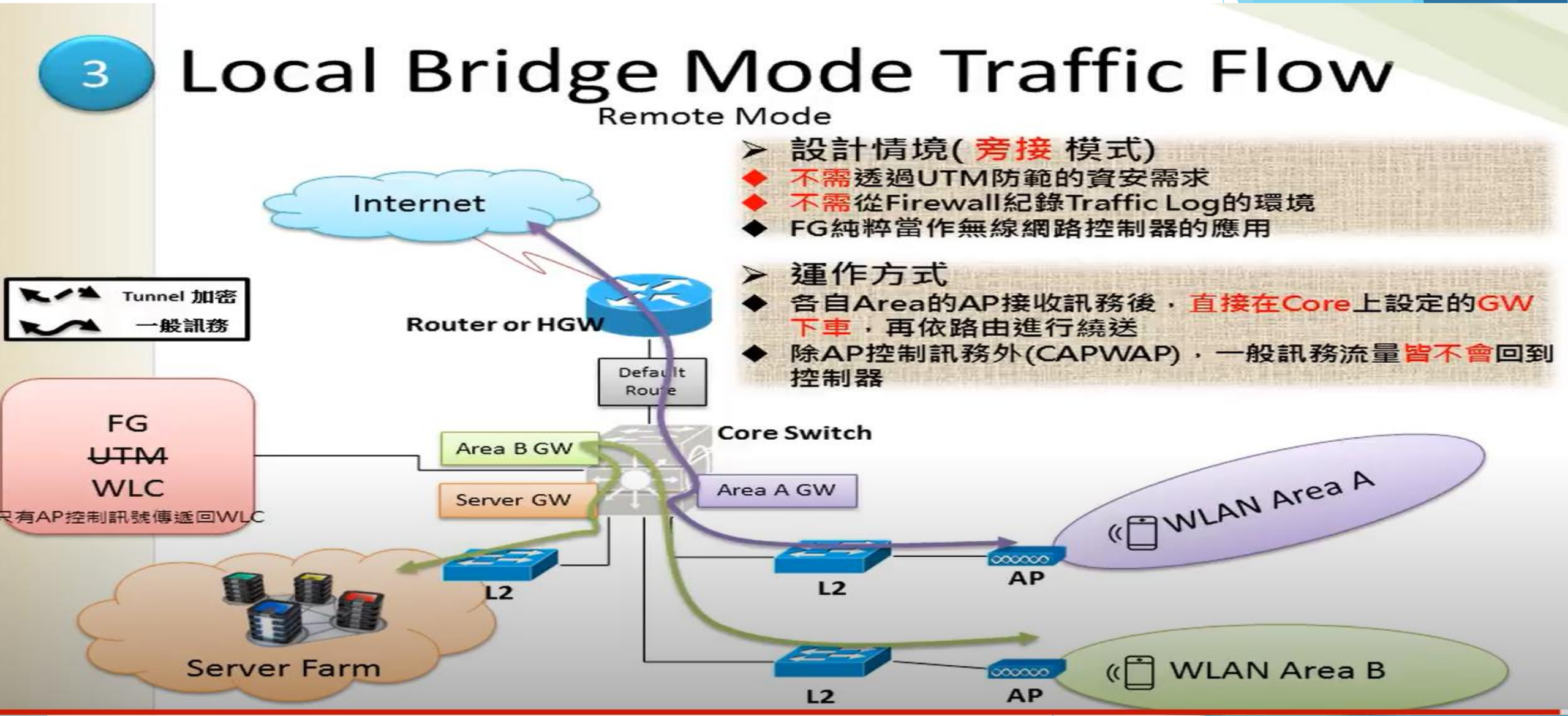


CAPWAP Tunnel Mode Traffic Flow



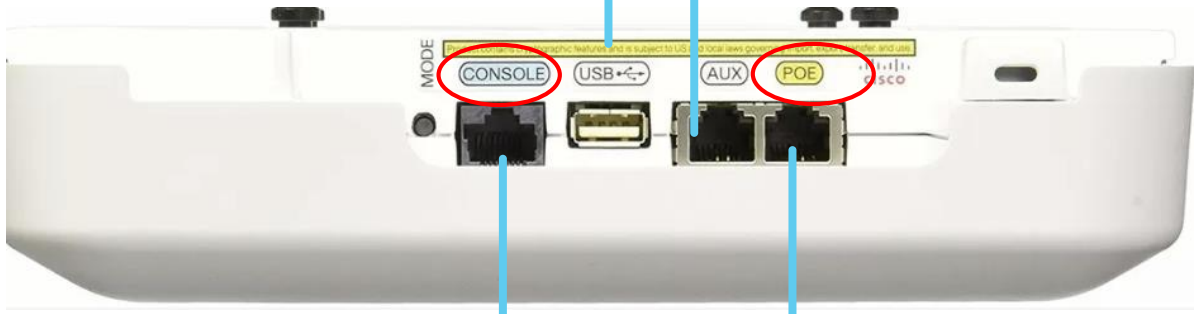
引用:https://www.youtube.com/watch?v=fXAVcls8yh0

CAPWAP Bridge Mode Traffic Flow



引用:https://www.youtube.com/watch?v=fXAVcls8yh0

Cisco AP 2802i



USB可用軟體
更新等

AUX終端設備

Console管理設定

連接POE Switch

燈號顯示代表-

綠燈:正常待命狀態

藍燈:設備連接中狀態

紅燈:裝置異常

紅綠燈:未正常與WLC溝通

Cisco AP 2802i設定指令

- 進行AP還原出廠
- 重開後按住MODE，系統會跑計數器20秒，**按完20秒放開**，系統就會清除
- ***capwap ap ip <ip_addr> <subnet_mask> <default_gateway>***
- ***capwap ap primary-base <名稱><ip_addr>***

學校架構

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