# 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         ※ 若小校無教室碼,則依棟號+樓層編號+教室編號(由左至右數)。       203.72.153.38						

## 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-Mobile <mark>5G</mark>	32	MAC	
eduroam	33	802.1x	
Class NTPC-Mobile <mark>2.4G</mark>	34	學校名稱+教室碼 (ex. SCPS-101) MAC	

## Cisco 3504 WLC/AC Interface 設定

iliilii cisco		MONITOR	<u>W</u> L∕ <sub>I</sub> Ns	<u>C</u> ONTROLL IR	WIRELESS	<u>s</u> ecurity m <u>a</u>		<u>o</u> mmands	S HE <u>L</u> P <u>F</u> EEDB	ACK	_	Sa <u>v</u> e Cor
Controller		Interface	Ma	nagment								
General												
Icons		Interface N	lame		VLAN Ide	ntifier IP Address	Interf	асе Туре	Dynamic AP Mana	gement IPv6 Addr	ess	
Inventory		managemen	t		3	10.228.67.1	Static		Enabled	::/128		
Interfaces		redundancy-	manageme	int	3	0.0.0.0	Static		Not Supported			
Interface Group	s	redundancy-	port		untagged	0.0.0.0	Static		Not Supported	(100		
Multicast		service-port			N/A	0.0.0.0	DHCP		Disabled	::/128		
Network Routes		virtual			N/A	1.1.1.1	Static		Not Supported			
Fabric Configura	tion					cisco	MONITOR WI ANS	CONTROLLER	WIRELESS SECURITY	MANAGEMENT COMMAND	HELP FEEDBACK	
Controller	Interf	aces > Edit				cisco						
						Controller	IPv6 Gateway	L				
General						General	Link Local IPv6 Addres	is i	fe80::ce70:edff:fe15:c2e5/64			
Icons	Gener	eral Information				Icons	<b>Physical Informatio</b>	Physical Information				
Inventory	Inter	Interface Name management				Inventory	Port Number	[	5			
Interfaces	Inter					Interfaces	Backup Port		0			
Interface Groups	MAC	Address	ess cc:70:ed:15:c2:e0			Interface Groups	Active Port		5			
Multicast	Config	figuration				Multicast	Enable Dynamic AR Ma	anagement .	<u>,</u>	_		
Network Routes						Network Routes	Enable Dynamic AF Hanagement					
Fabric Configuration	Quar	antine				Fabric Configuration	abric Configuration DHCP Information					
Redundancy	Quar	rantine Vlan Id	0			Redundancy	Primary DHCP Server	[	10.228.67.254			
Internal DHCP Server	NAT A	ddress				Internal DHCP Server	Secondary DHCP Serve	er 🛛	0.0.0.0			
Mobility Management						Mobility Management	DHCP Proxy Mode		Global V			
Ports	Enac	DIE NAT Address				Ports	Enable DHCP Option 82	2				
▶ NTP	Interf	ace Address				NTP	Enable DHCP Option 6	OpenDNS				
CDP	VLAN	Identifier		2		CDP						
PMTPv6	VLAN					PMIPv6	Access Control List					
Tunneling	IP Ad	ddress		10.228.67.1		Tunneling	ACL Name		none 🗸		IPv6 ACL Name	none 🗸
h TDuc	Netn	nask		255.255.255.0		IPv6	URL ACL	[	none 🗸			
1940	Gate	way		10.228.67.254		mDNS						
▶ mDNS	IPv6	Address		::		Advanced	mDNS					
Advanced	Prefi	x Length		128		Lawful Interception	mDNS Profile		none V			
I suful Interception							Alexandre Changelong Alex Takend	£	a second a first that a first hard a second	consults of the help of a soul along a second second	where the second second which the state	an anna allanka

սիսիս	r								Sa <u>v</u> e C	onfiguration	<u>P</u> ing	Logout <u>R</u> e
CISCO	<u>M</u> ONITOR	VLANs	<u>C</u> ontroller	W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P	<u>F</u> EEDBACK			<mark>î</mark> <u>I</u>
WLANs	WLANs									-	Entries 1	2 3 ▶ ■
WLANs	Current Filter	No	ne [ <u>Chang</u>	<u>e Filter] [Clear</u>	<u>Filter</u> ]		Create Ne	W	Go			
Advanced								ſ				
	$\Box$ wlan id	Туре	Profile N	Name	ſ	WLAN SSID			Admin Status	Security Pol	icies	
	<u>1</u>	WLAN	manager	nent		management			Enabled	[WPA2][Auth	(PSK)]	
	<u>2</u>	WLAN	TANetRoa	aming		TANetRoaming			Enabled	Web-Auth		
	<u>3</u>	WLAN	NTPC-Mo	bile		NTPC-Mobile			Enabled	MAC Filtering	ļ	
	<u>4</u>	WLAN	eduroam			eduroam			Enabled	[WPA2][Auth	(802.1X)	
	<u>5</u>	WLAN	class			class			Enabled	[WPA2][Auth	(PSK)]	

#### SSID 要走的介面

Veb Browser												
< > URL https://10.227.5	6.1/frameWlanEdit.	html									Go	St
										Save Configuration	<u>P</u> ing   Lo	ogout   <u>R</u> e
cisco	MONITOR M	VLANs <u>C</u> ON	TROLLER	W <u>I</u> RELESS <u>S</u> EC	JRITY M <u>a</u> na	GEMENT	COMMANDS	HELP	FEEDBACK			<mark>е н</mark>
WLANs	WLANs > E	dit 'class1	•			_				< BA	СК	Apply
WLANs	General	Security	QoS	Policy-Mapping	Advanced							
Advanced	Clear Hot						NAC State N	one	•			*
AP Groups	Client use	er idle timeout(					Load Balancing a	nd Band	Select			
	100000)						Client Load Bal					
	Client use 1000000			0 Bytes								
	Radius N/						Passive Client					
	Off Channel	Scanning Def	fer				Passive Client					
	Scan Defe	er Priority	0 1	2 3 4 5 6 7			Voice					
							Media Session	Snooping		🗍 Enab	led	
	Scan Defe		100									
	ElexConnect	t	100		•							
	FlawConn	set Local			<u> </u>		Radius Client Pro	ofiling				
	Switching	j <b>2</b>	<b></b>	Enabled			DHCP Profiling					
	FlexConn	ect Local Auth	12 🕑	Enabled								
	Loorn Clic	ant ID Addroso	5 🖉	Enabled			Local Client Prof	iling				
	Vlan base						DHCP Profiling					
	Switching	<u>13</u>										
	Central D						Universal AP Adr	nin Supp	ort			
	Ouerride											

WLANS	
	Create New V
WLAN ID         Type         Profile Name         WLAN SSID	Admin Status Security Policies
1 WLAN Managment Managment	Enabled [WPA2][Auth(802.1X)]
WLANs > Edit 'Managment'	OSEN Policy
	Authentication Key Management 19
General Security QoS Policy-Mapping Advanced	802.1X Enable
Layer 2 Security 💁 WPA+WPA2	CCKM Enable
MAC Filtering <sup>2</sup>	PSK Z Enable
Fast Transition	FT 802.1X Enable
Fast Transition Adaptive V	FT PSK Enable
Over the DS	PSK Format ASCII V
Reassociation Timeout 20 Seconds	
Protected Management Frame	SUITEB-1X Enable
PMF Disabled V	SUITEB192-1X Enable
WPA+WPA2 Parameters	WPA gtk-randomize State
WPA Policy	
WPA2 Policy	Lobby Admin Configuration
WPA2 Encryption CCMP256 GCMP128	GCMP256 Lobby Admin Access
OSEN Policy MON	ITOR <u>W</u> LANS <u>C</u> ONTROLLER WIRELESS <u>S</u> ECURITY MANAGEMENT C <u>O</u> MMANDS HELP
'LANs > Edit 'Managment'	ANs > Edit 'Managment'
Ge	eneral Security QoS Policy-Mapping Advanced
	Layer 2 Layer 3 AAA Servers
General Security QoS Policy-Mapping Advanced	elect AAA servers below to override use of default servers on this WLAN
	ADIUS Servers
Layer 2 Layer 3 AAA Servers	RADIUS Server Overwrite interface     Enabled       Apply Cisco ISE Default Settings     Enabled
Laver 3 Security None X	Enabled     Enabled     Enabled     Enabled     Enabled     Enabled
	Server 1 IP:203.72.154.101, Port:1812 V IP:203.72.154.101, Port:1813 V Server 2 IP:203.72.154.102, Port:1812 V IP:203.72.154.102, Port:1813 V
Captive Network Assistant Bypass None 🗸	Server 3 None V None V
	Server 4 None V
	Server 5 None V None V
	Authorization ACA Server Accounting ACA Server
	Enabled Enabled

IONITOR <u>W</u> LANs IONTROLLER WIRELESS <u>S</u> E	CURITY MANAGEMENT COMMANDS HE	LP MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANI	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS
VLANs > Edit 'eduroam'		WLANs > Edit 'eduroam'	WLANs > Edit 'eduroam'
General Security QoS Policy-Mapping	Advanced	General Security QoS Policy-Mapping Advanced	General Security QoS Policy-Mapping Advanced
Profile Name       eduroam         Type       WLAN         SSID       eduroam         Status       Inabled         Security Policies       [WPA2][Auth(802.1X)         Radio Policy       [Modifications done under         Interface/Interface Group(G       All         Multicast Vlan Feature       Enabled         Broadcast SSID       Inone	D] r security tab will appear after applying the changes	Layer 2       Layer 3       AAA Servers         Layer 2 Security <sup>6</sup> WPA+WPA2           Procent Price P	Layer 2       Layer 3       AAA Servers         WPA+WPA2 Parameters       WPA Policy         WPA2 Policy       Image: Comparison of the second
<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ONTROLLER WIRELESS <u>S</u> ECURITY M <u>A</u> NAGEN	WLANs > Edit 'eduroa	802.1X Enable	Lobby Admin Configuration
WLANs > Edit 'eduroam'	Layer 2 Layer 3 Select AAA servers below	AAA Servers	LAN
General     Security     QoS     Policy-Mapping     Advanced       Layer 2     Layer 3     AAA Servers	RADIUS Servers RADIUS Server Overwrit Apply Cisco ISE Default Authenticat Enabled	te interface Enabled Settings Enabled tion Servers Accounting Servers Enabled	EAP Parameters Enable
Layer 3 Security None  Captive Network Assistant Bypass None	Server 1 IP:203.72.1 Server 2 IP:203.72.1 Server 3 None Server 4 None Server 5 None Server 6 None Authorizatio	101, Port:1612       IP:203.72.154.101, Port:1         102, Port:1812       IP:203.72.154.102, Port:1         101       None         102       None         103       None         104       None         105       None         106       None         107       None         108       Income         109       None         100       Income	

## Cisco 3504 WLC/AC RADUIS Authentication

<u>M</u> ONITOR	<u>W</u> LANs <u>C</u> C	ONTROLLE	ER W <u>I</u>	RELESS	<u>s</u> ecurity	M <u>a</u> nagement	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK	<u>.</u> <u>.</u> <u>.</u>	<u>H</u> ome
RADIUS	Authenticat	ion Ser	vers								Apply
Auth Cal	lled Station ID T <sub>y</sub>	ype	Address		V						
Use AES	Key Wrap		)esigned	for FIPS o	ustomers and	requires a key wrap	o compliant RADI	US serve	r)		
MAC Del	imiter	H	/phen	$\checkmark$							
Framed	MTU	13	800								
Network User	Management	Tunnel Proxy	Server Index	Se	rver Address	(Ipv4/Ipv6)			Port	IPSec	Admin S
			<u>1</u>	* 20	3.72.154.101				1812	Disabled	Enabled
			<u>2</u>	* 20	3.72.154.102				1812	Disabled	Enabled
			<u>3</u>	* 20	3.72.154.115				1812	Disabled	Enabled
	MONITOR RADIUS Auth Cal Use AES MAC Del Framed  Network User	MONITOR WLANS CO   RADIUS Authentication   Auth Called Station ID To   Use AES Key Wrap   MAC Delimiter   Framed MTU     Network   User   Management   IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	MONITOR WLANS CONTROLLE   RADIUS Authentication Server   Auth Called Station ID Type IP   Use AES Key Wrap (I   MAC Delimiter Hy   Framed MTU 13	MONITOR WLANS CONTROLLER WI   RADIUS Authentication Servers   Auth Called Station ID Type IP Address   Use AES Key Wrap (Designed)   MAC Delimiter Hyphen   Framed MTU 1300     Network Management Proxy   Use 1   I 2   I 2   I 3	MONITOR WLANS CONTROLLER WIRELESS   RADIUS Authentication Servers   Auth Called Station ID Type IP Address   Use AES Key Wrap (Designed for FIPS of MAC Delimiter   MAC Delimiter Hyphen   Framed MTU 1300     Network Management   User Management   Proxy Index   2 *	MONITOR WLANS CONTROLLER WIRELESS SECURITY   RADIUS Authentication Servers   Auth Called Station ID Type IP Address    Use AES Key Wrap (Designed for FIPS customers and   MAC Delimiter Hyphen    Framed MTU 1300     Network Tunnel Server   Management Proxy Index   Server Address   I * 203.72.154.101   I I 2 *   I I 203.72.154.102   I I I 203.72.154.102	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT   RADIUS Authentication Servers   Auth Called Station ID Type IP Address    Use AES Key Wrap (Designed for FIPS customers and requires a key wrap   MAC Delimiter Hyphen   Framed MTU 1300     Network Tunnel Server   User Management Proxy   Index Server Address(Ipv4/Ipv6)   I * 203.72.154.101   I I 2   I 3 *   2 * 203.72.154.115	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS   RADIUS Authentication Servers   Auth Called Station ID Type IP Address ~   Use AES Key Wrap   (Designed for FIPS customers and requires a key wrap compliant RADI   MAC Delimiter Hyphen ~   Framed MTU 1300     Network Tunnel Server   User Management Proxy   Index Server Address(Ipv4/Ipv6)   I *   2	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP   RADIUS Authentication Servers   Auth Called Station ID Type IP Address ~   Use AES Key Wrap (Designed for FIPS customers and requires a key wrap compliant RADIUS server   MAC Delimiter Hyphen   Framed MTU 1300     Network Tunnel Server   User Management Proxy   I * 203.72.154.101   I 2 *   2 * 203.72.154.115	MONITOR       WLANS       CONTROLLER       WIRELESS       SECURITY       MANAGEMENT       COMMANDS       HELP       FEEDBACK         RADIUS Authentication Servers         Auth Called Station ID Type       IP Address	MONITOR       WLANS       CONTROLLER       WIRELESS       SECURITY       MANAGEMENT       COMMANDS       HELP       FEEDBACK         RADIUS Authentication Servers         Auth Called Station ID Type       IP Address       ~         Use AES Key Wrap       (Designed for FIPS customers and requires a key wrap compliant RADIUS server)       MAC Delimiter       Hyphen       ~         Framed MTU       1300       1300       Port       IPSec         Image:       Image:       Server       Server Address(Ipv4/Ipv6)       Port       IPSec         Image:       Image:       Image:       1       * 203.72.154.101       1812       Disabled         Image:       Image:

#### Cisco 3504 WLC/AC RADUIS Authentication

#### RADIUS Authentication Servers > Edit

RADIUS Authentication Servers > Edit

Server Index	1
Server Address(Ipv4/Ipv6)	203.72.154.101
Shared Secret Format	ASCII ∨
Shared Secret	•••
Confirm Shared Secret	•••
Key Wrap	Oceasigned for FIPS custome
Apply Cisco ISE Default settings	
Apply Cisco ACA Default settings	
Port Number	1812
Server Status	Enabled ∨
Support for CoA	Disabled ∨
Server Timeout	5 seconds
Network User	Enable
Management	Enable
Management Retransmit Timeout	5 seconds
Tunnel Proxy	Enable

	Server Index	2
	Server Address(Ipv4/Ipv6)	203.72.154.102
	Shared Secret Format	ASCII V
	Shared Secret	•••
	Confirm Shared Secret	•••
ers and	Key Wrap	O (Designed for FIPS customers and requires a key wrap compliant RADIUS serve
	Apply Cisco ISE Default settings	
	Apply Cisco ACA Default settings	
	Port Number	1812
	Server Status	Enabled V
	Support for CoA	Disabled V
	Server Timeout	5 seconds
[	Network User	Enable
	Management	Enable
	Management Retransmit Timeout	5 seconds
	Tunnel Proxy	Enable

Server Index

Server Address(Ipv4/Ipv6)
Shared Secret Format

Shared Secret

Confirm Shared Secret

Key Wrap

Apply Cisco ISE Default settings

RADIUS Authentication Servers > Edit

3

Apply Cisco ACA Default settings

 Port Number
 1812

 Server Status
 Enabled ∨

 Support for CoA
 Disabled ∨

Server Timeout 5 seconds

Network User 🗌 Enable

Management	Enable				
Management Retransmit Timeout	5	seconds			
Tunnel Proxy	E	nable			

•••	
ASCII V	
203.72.154.115	

igsquirin (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

#### Cisco 3504 WLC/AC RADUIS Accounting server

MONITOR WLAN	5 <u>C</u> ONT	ROLLER	W <u>I</u> RELESS	SECURITY	MANAGE		C <u>o</u> mmands	HELP	<u>F</u> EEDBA	CK		
RADIUS Accour	nting Se	rvers										
Acct Called Station	n ID Type	IP Add Colon	dress ~	~			(		RADUI	s		
Network Tunnel Vser Proxy	Server Index 1 2 3		Server Addres 203.72.154.10 203.72.154.10 203.72.154.11	ss(Ipv4/Ipv6 1 2 5	5)			Port 1813 1813 1813	IPSec Disablec Disablec Disablec	d d d	Admin Status Enabled Enabled Enabled	
MONITOR WLANS CONTROLL	er W <u>i</u> reless	SECURITY M	MONITOR WLANS CO	ONTROLLER W <u>I</u> REL	ESS <u>S</u> ECURITY	M <u>A</u> NAGEMEN	T C <u>O</u> MMANDS H	E <u>L</u> P <u>F</u> MONITOR	R <u>w</u> lans <u>c</u> ontrolle	ER W <u>I</u> RELESS <u>S</u> ECURITY	M <u>a</u> nagement c <u>o</u> mmands i	ie <u>l</u> p <u>F</u> eedback
RADIUS Accounting Server         Server Index         Server Address(Ipv4/Ipv6)         Shared Secret Format         Shared Secret         Confirm Shared Secret         Apply Cisco ACA Default settings         Port Number         Server Status         Server Timeout         Network User         Tunnel Proxy         Realm LIST         PAC Provisioning         IPSec         Cisco ACA	1 203.72.154.101 ASCII ✓ ••• 1813 Enabled ✓ 5 seconds ✓ Enable Enable Enable Enable		RADIUS Accounting Server Index Server Address(Ipv4/Ipv6 Shared Secret Format Shared Secret Confirm Shared Secret Apply Cisco ACA Default s Port Number Server Status Server Timeout Network User Tunnel Proxy Realm List PAC Provisioning IPSec Cisco ACA	Servers > Edit 2 2 2 2 2 2 2 2 2	e			RADIUS Server Server Shared Confirm Apply C Port Nu Server Server Vetwor Tunnel PAC Pro IPSec Cisco A	S Accounting Servers Index (Priority) IP Address(Ipv4/Ipv6) Secret Format Secret Secret Status Timeout k User Proxy CA	s > New 3 ∨ 203.72.154.115 ASCII ∨ 		

# Cisco 3504 WLC/AC 設定

cisco	<u>M</u> ONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMEN	T C <u>O</u> MMANDS	HE <u>L</u> P <u>I</u>	<u>F</u> EEDBACK	
WLANs	Ap Group	s > Edit	'default-gro	up'						
<b>WLANs</b>	General	WLAN	s APs	802.11u	Location	Ports/Modul	e Intelligen	t Capture		
<ul> <li>Advanced</li> <li>AP Groups</li> </ul>	APs curre	ently in the	e Group		-	Add APs	to the Group			Add APs
	AP Na	me	Ethern	et MAC			ame	Group Na	ame	
	<b>772AP</b>	Ad001	6c:8b:	d3:21:24:4e		<b>A</b>				
	772AP4	418	74:88:	bb:ce:91:70						
	772AP1	114	74:88:	bb:c0:3b:18						
	772AP2	212	74:88:	bb:c0:3b:1c						
	<b>772AP</b>	315	74:88:	bb:ce:98:ac						
	772AP3	318	74:88:	bb:c0:3d:7e						
	<b>772AP</b>	314	74:88:	bb:53:66:64						
	772AP5	521	74:88:	bb:53:63:68						
	772AP4	416	74:88:	bb:c2:e6:08						
	<b>772AP</b>	313	74:88:	bb:68:d5:f8						
	772AP2	218	74:88:	bb:68:d5:26						
	<b>772AP</b>	321	74:88:	bb:53:62:5a						

# Cisco 3504 WLC/AC設定

ululu cisco	<u>M</u> onitor <u>W</u> lans <u>C</u> o	NTROLLER WIRELESS	s <u>s</u> ecurity m <u>a</u> nagi	EMENT C WLANS	Save Contiguration Ping Logou MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK WLANS > Edit 'TANetRoaming'
General RADIUS Authentication	Access Control Lists			<ul> <li>WLANs</li> <li>WLANs</li> <li>Advanced</li> </ul>	General     Security     QoS     Folicy-Mapping     Advanced       Layer 2     Layer 3     AAA Servers
Auth Cached Users	Enable Counters				Layer 3 Security Web Policy V Captive Network Assistant Bypass None V
DNS	Name		Type		Authentication
Downloaded AVP	Destable		ID-4		Conditional Web Redirect
TACACS+	Preauto		1204		○ Splash Page Web Redirect
LDAP	Fact Natas				On MAC Filter failure <sup>10</sup>
MAC Filtering	root notes				Web policy done locally on Apwarning
Disabled Clients	1. Counter configuration is g	lobal for acl, urlacl and lay	er2acl.		Preauthentication ACL IPv4 PreAuth V IPv6 None V WebAuth Flex IPV4 Acl None V WebAuth Flex IPV6 Acl None V
User Login Policies		Access Control I	ists > Rules > New		Sleeping Client Enable
AP Policies			1010 - 110100 - 11011		Sleeping Client Auto Authenticate 🗹 Enable
		Sequence	1		Override Global Config <sup>20</sup> Enable
dvanced EAP		Source	Any 🗸	ACL	
riority Order		Destination	Any 🗸	police	
ertificate		Protocol	Any 🗸		
ccess Control		DSCP	Any 🗸		
Access Control Lists		Direction	Any 🗸		
CPU Access Control Lists		Action	Deny V		
FlexConnect ACLs			Deny		
Layer2 ACLs					



- ➤ 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:

AP對AC的自動發現及AP和AC的狀態機運行,維護。
 AC對AP進行管理,設定配置下發。
 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:<u>https://www.youtube.com/watch?v=fXAVcls8yh0</u>

#### CAPWAP Bridge Mode Traffic Flow



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





▶ 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>



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

