

# Ruckus Wireless Training

**SMARTZONE**

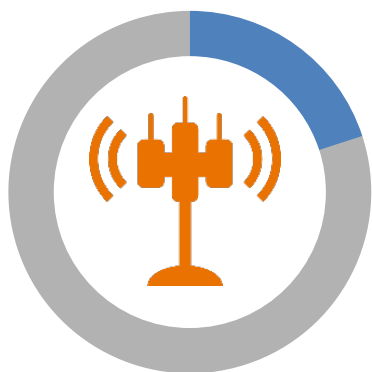
*Calman\_chang*  
*calman.chang@jlead.com.tw*



# 議程

- 無線網路趨勢
- Ruckus 無線技術 & 產品
- SMARTZONE 產品架構
- SMARTZONE initial
- AccessPoint initial
- Base config , WLAN config , others
- Lab

# 2021 全球流量預估統計



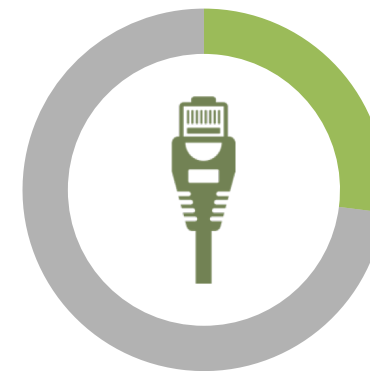
**20%**

行動通信



**53%**

無線網路



**27%**

有線網路

問題來了：您準備好了嗎？

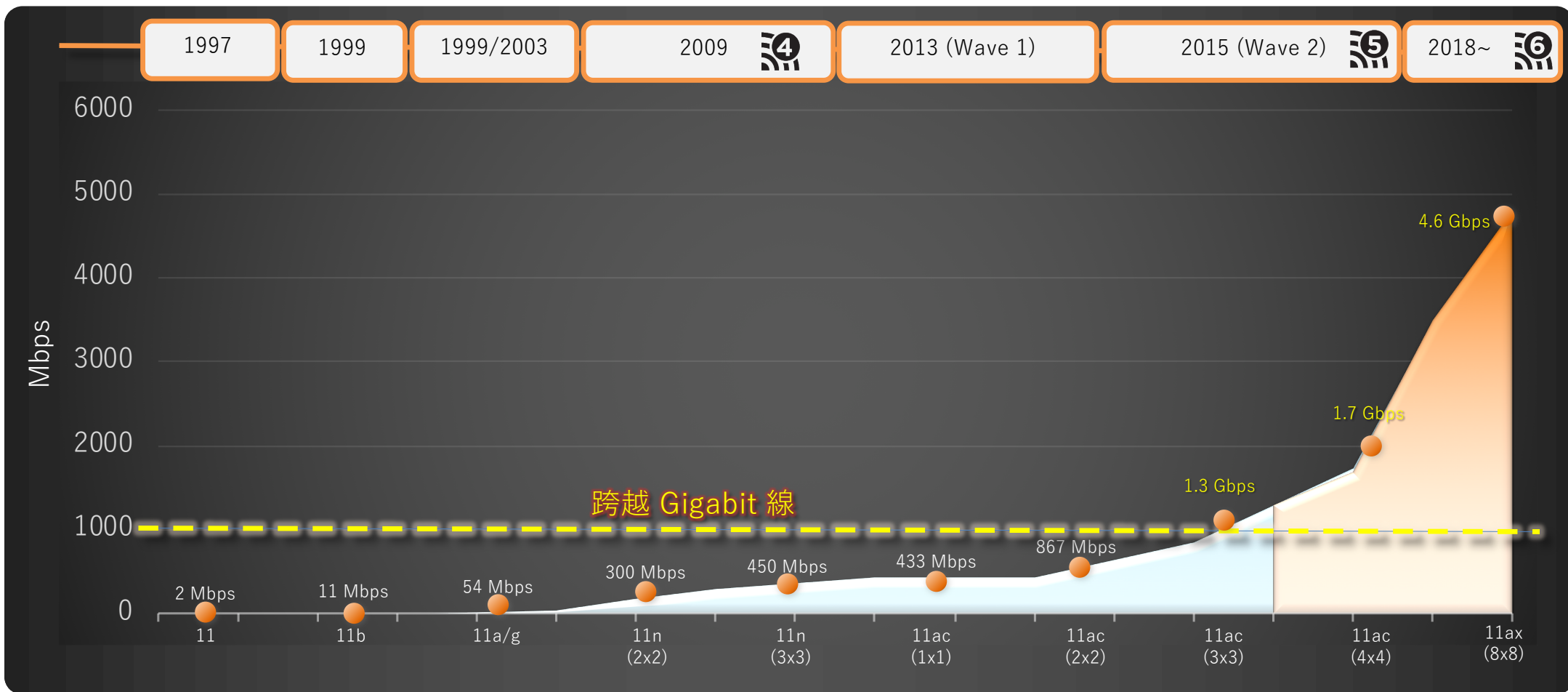
- 超過 1000 倍以上的頻寬用量
- 超過 200億個物聯網設備(IoT)
- 超過 50% 的設備與設備間互聯

資料來源: *Global Internet Traffic (2021)*



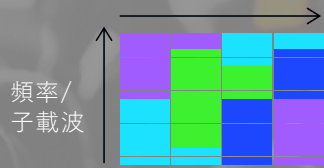
Ruckus 為您帶來全新無線體驗

# 越來越快的 WiFi 傳輸速度



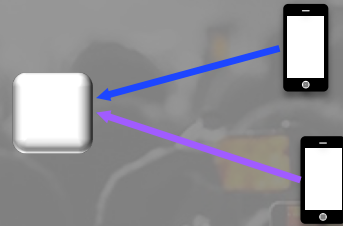
# 即將席捲全球的無線技術規格 802.11ax

更有效率



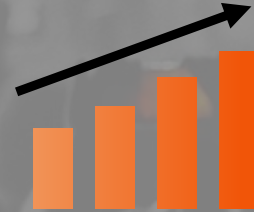
支援 OFDMA

更多設備



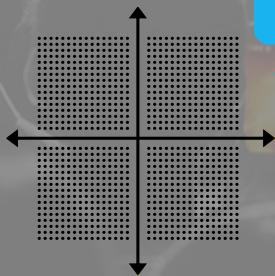
上行  
MU-MIMO

傳得更快



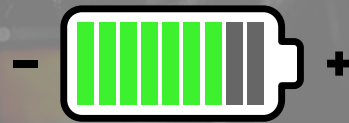
實體層及網路層效率提升

更有效率



更多相位 1024-QAM

用戶省電



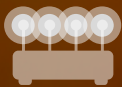
電源效率提升

更有效率



BSS 顏色識別技術

# OFDMA 如何提升傳輸效率



目前 WiFi 5 (11ac) 網路



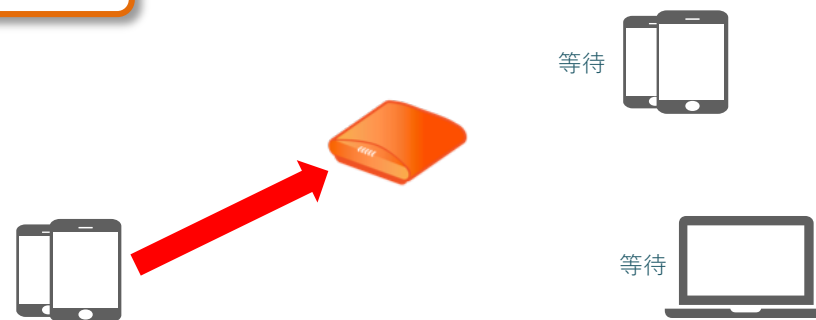
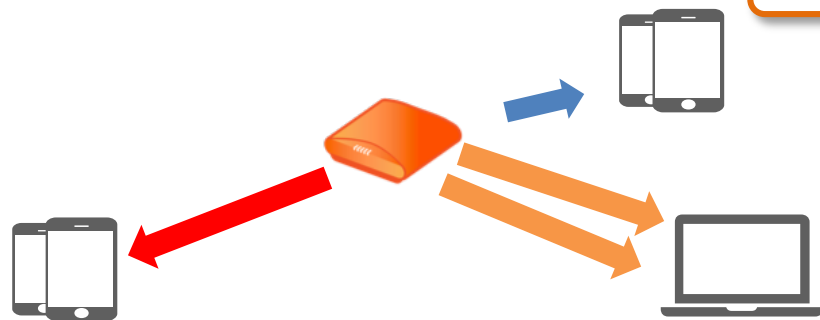
# OFDMA 如何提升傳輸效率



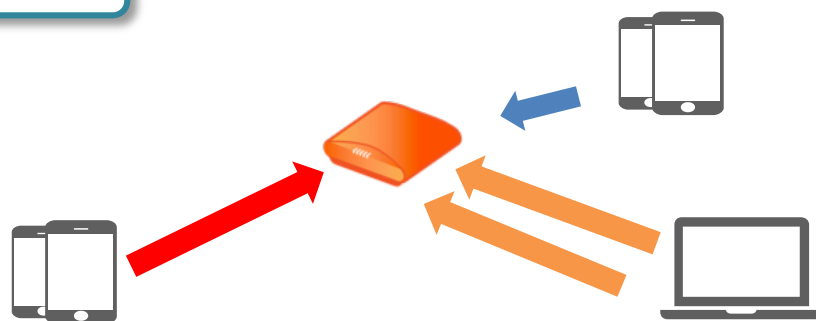
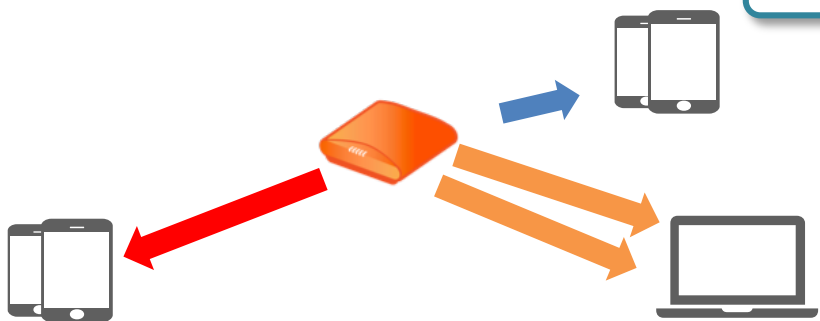
WiFi 6 網路(11ax)

# 上行 MU-MIMO

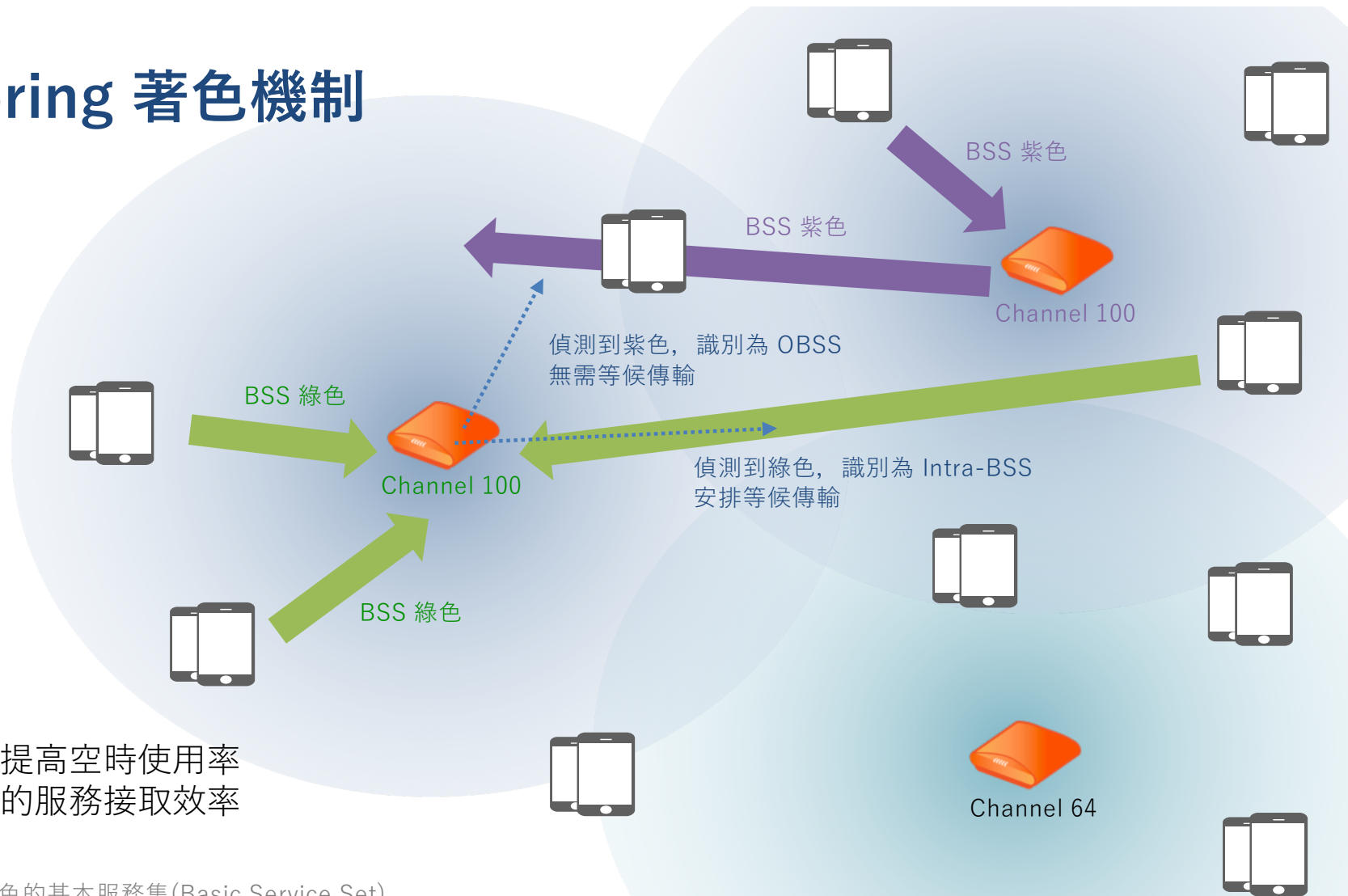
802.11ac 不支援上行 MU-MIMO



802.11ax 支援上行 MU-MIMO



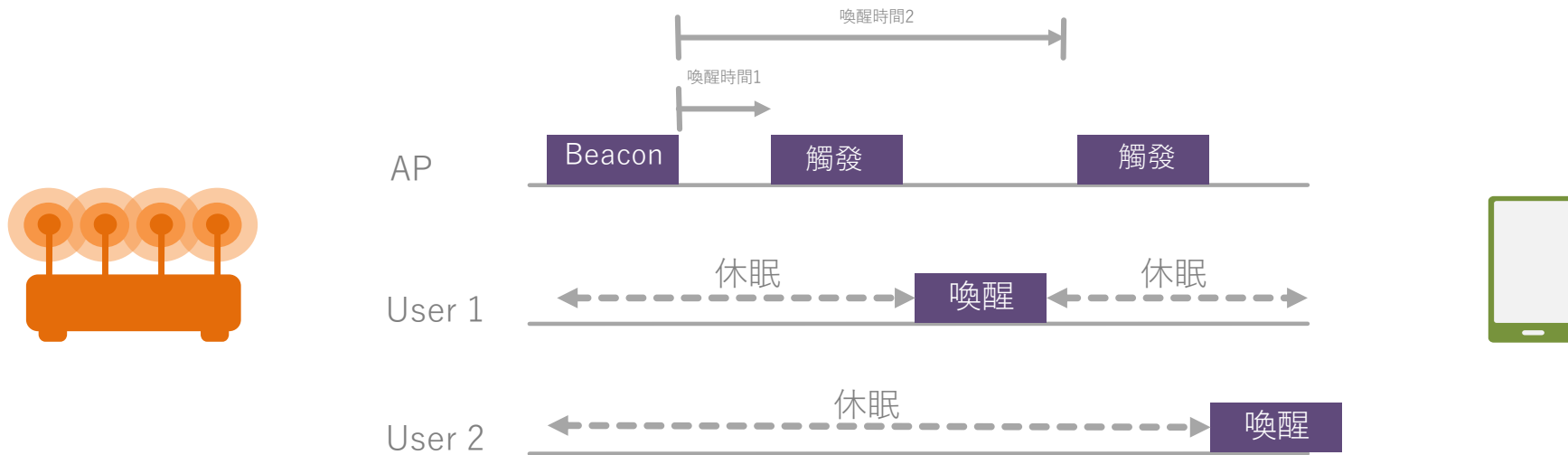
# BSS Coloring 著色機制



- 實現空間重複利用, 提高空時使用率
- 提升高密度部署環境的服務接取效率

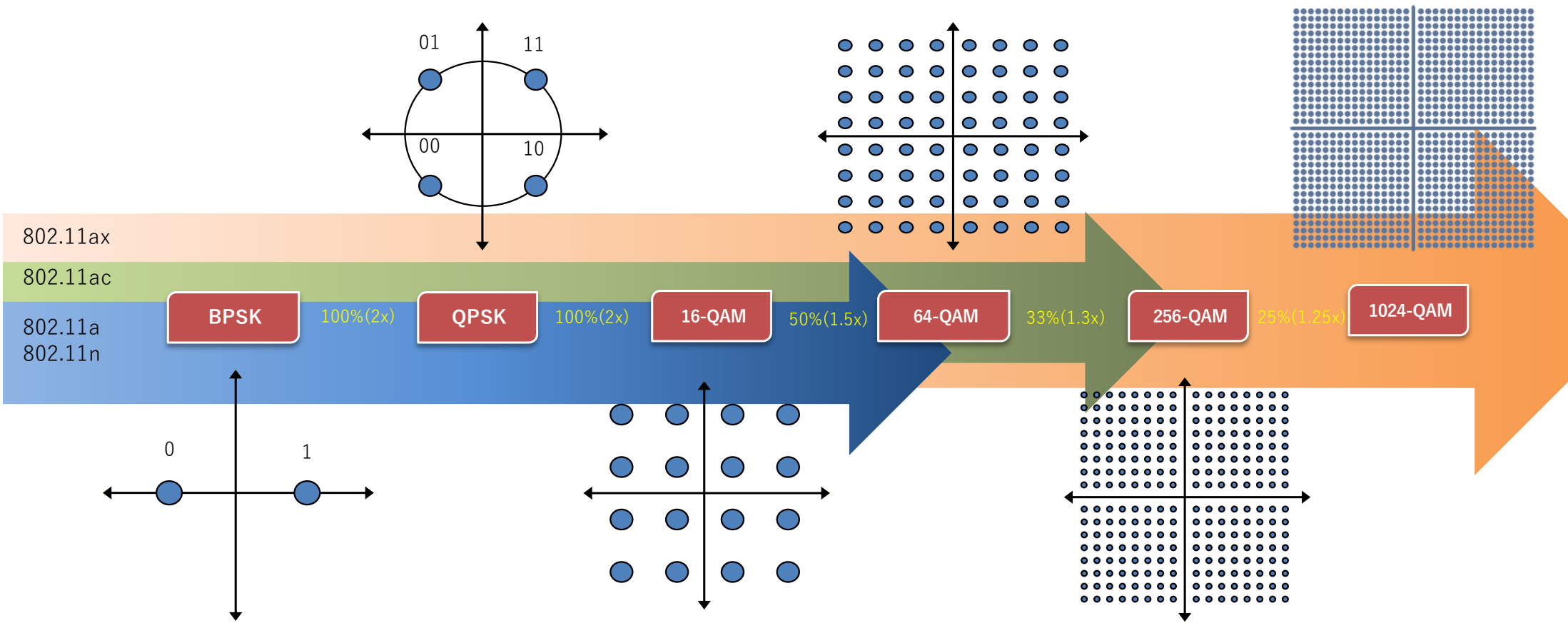
OBSS (Overlap BSS) : 重疊頻道非同色的基本服務集(Basic Service Set)

# 強化設備省電機制 Target Wake Time (TWT)



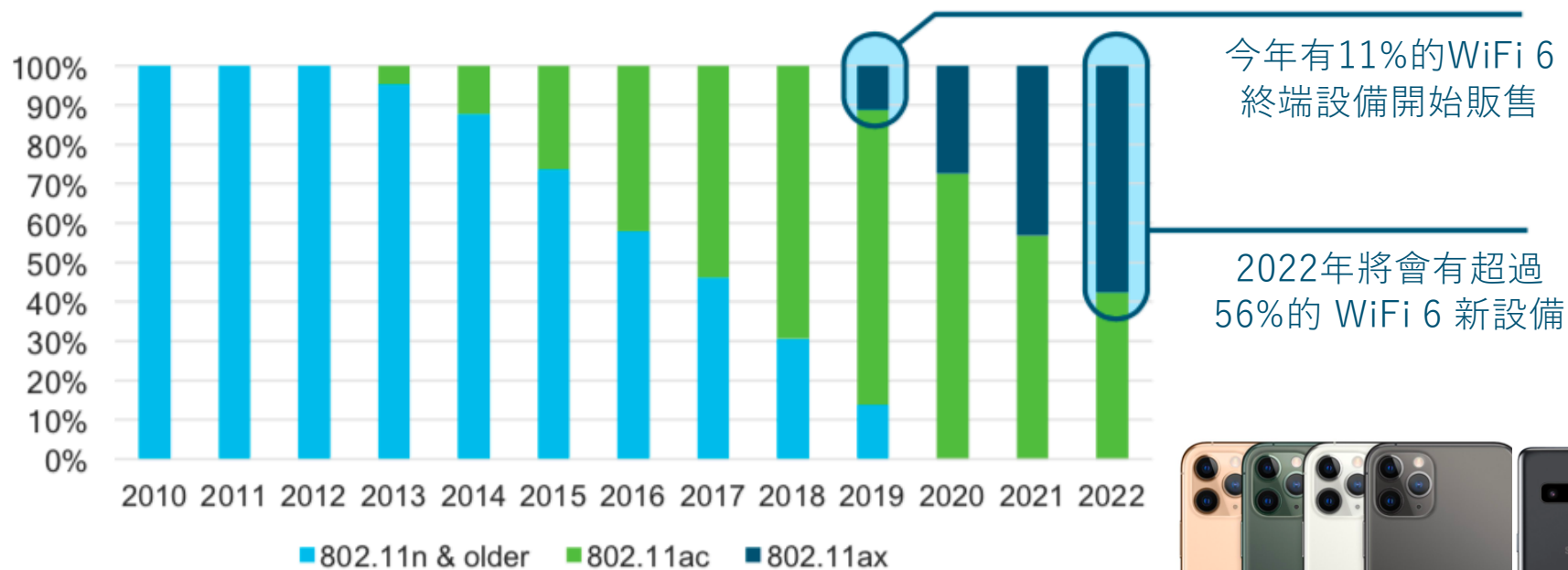
- 基地台會跟裝置協商，並且相互定義喚醒各自的時間
- 減少每個用戶端的爭用跟重疊時間
- 大幅增加設備休眠時間，以減少耗電

# 11ax 更密集的相位偏移調變模式



# 再不開始準備 WiFi 6, 就真的慢了

## 802.11ax 終端設備成長指數





# Ruckus 無線技術 & 產品

# 需要改變的是天線

*Ruckus 全新的天線設計突破了無線網路的最大瓶頸*

傳統的散射性天線  
針對終端設備信號源不一致  
(everyone else)



亮度不足的燈泡

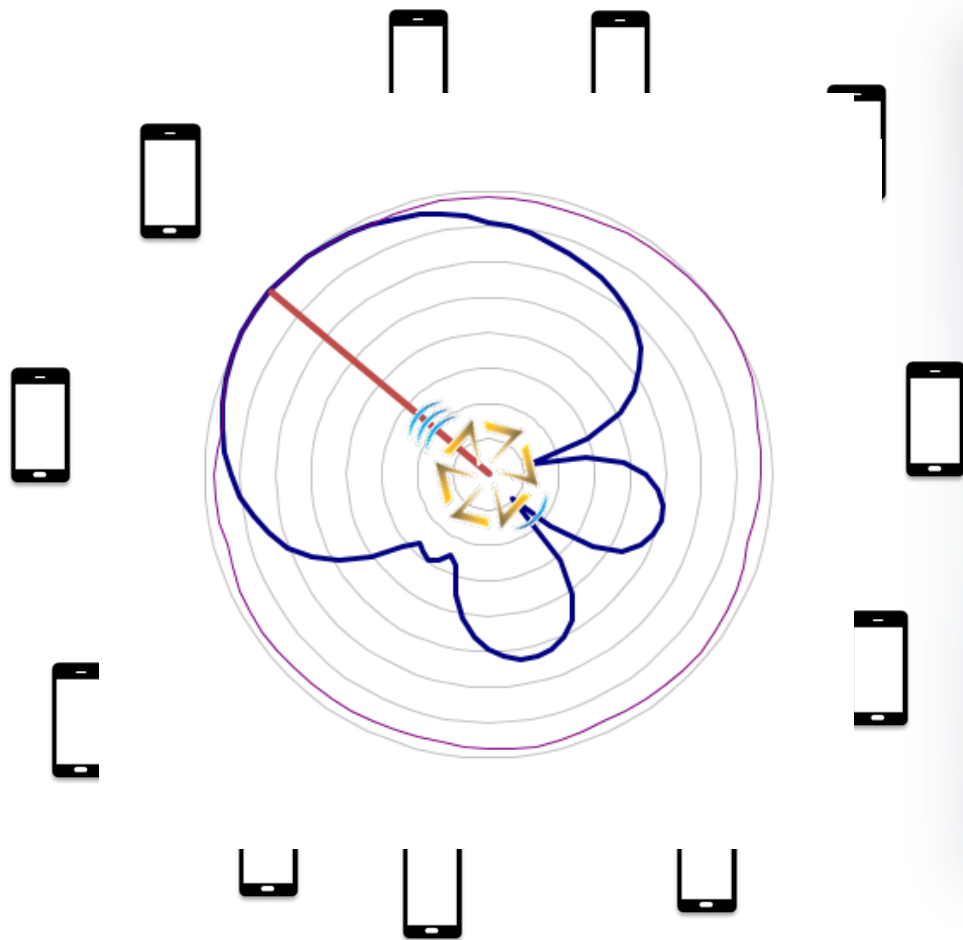


指向式智慧型天線  
針對終端設備提供最佳的訊號  
(Ruckus)



聚焦方向的探照燈

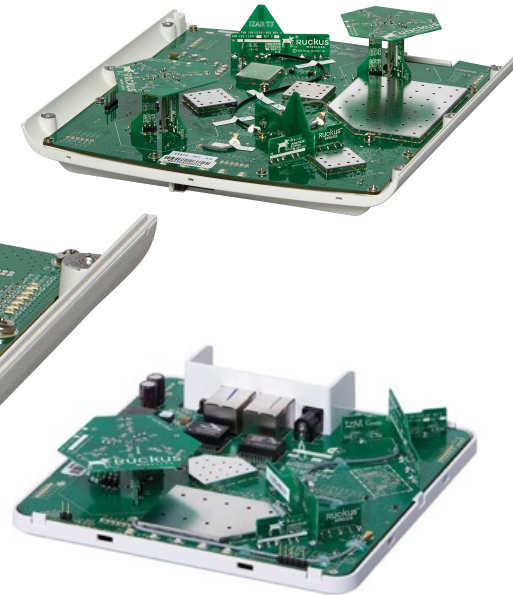
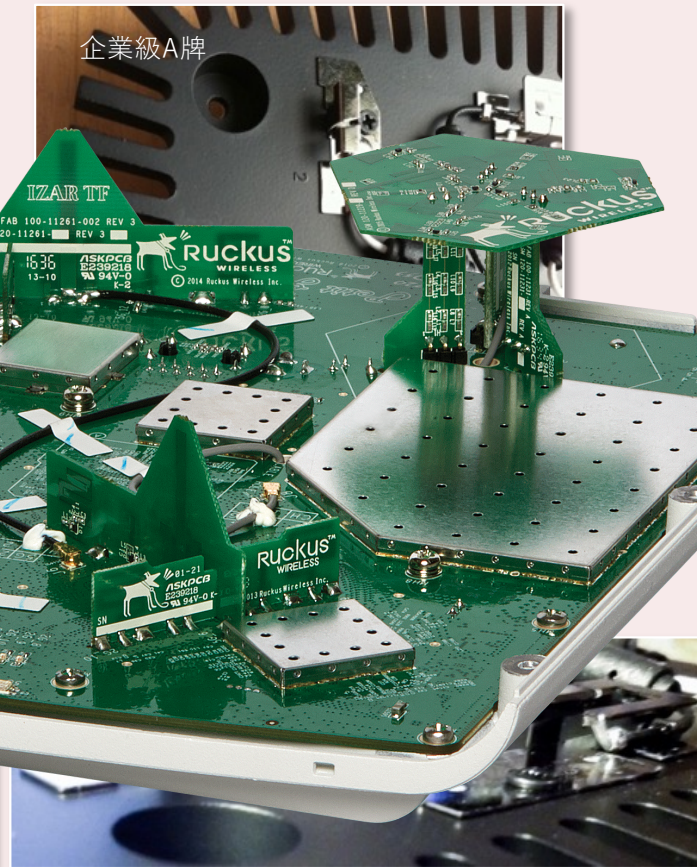
## 關鍵來自於專利 BeamFlex 技術



- 依終端的每個封包選擇傳輸的天線元素
- 適應天線適時地將資料傳遞到特定方位
- 指向天線能夠更加強力將訊號送往用戶端
- 針對周邊基地台跟用戶降低更少的干擾



# 來看看用料跟設計的差異



BeamFlex 智慧型矩陣天線

平面型倒F天線(Planar inverted-F antenna)(簡稱 PIFA)

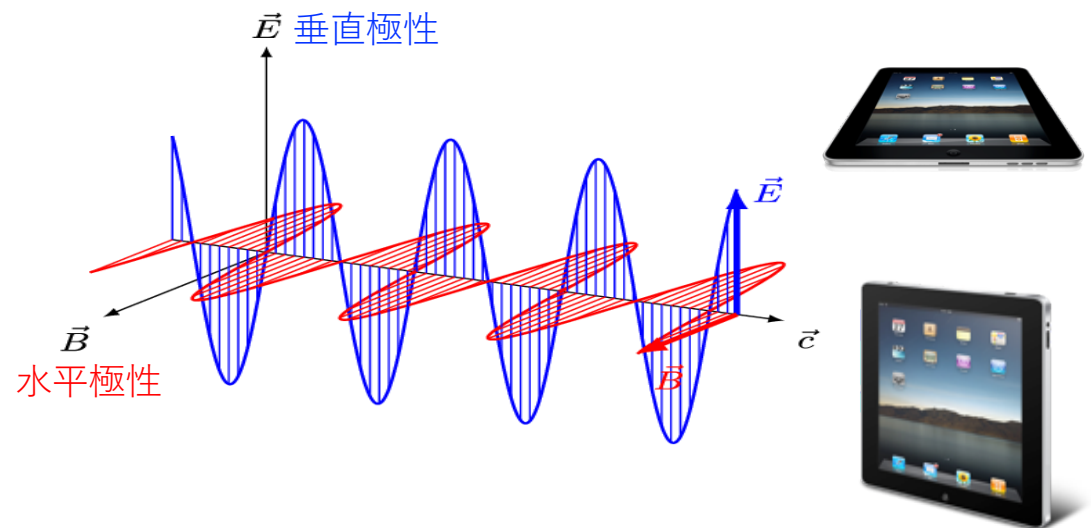
# 手持行動設備可以調整方向，但基地台的天線呢？

5x

因應設備角度，決定溝通天線極性，可以有效提升將近5倍的效率



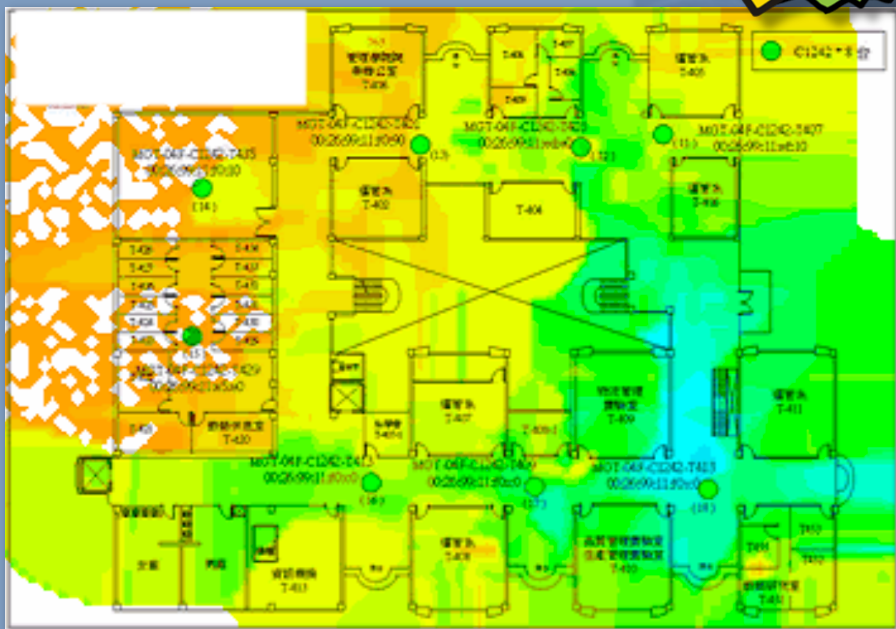
- 更好的接收能力：
  - 專利天線偏振分極技術(PD-MRC)讓手持設備能夠更清晰的接收訊號
- 更好的傳輸能力：
  - 依據設備角度給予正確的資料傳輸波型，可有效提高傳輸率



# Ruckus 給您涵蓋範圍更大的無線連線

實際大樓平面涵蓋分佈測試

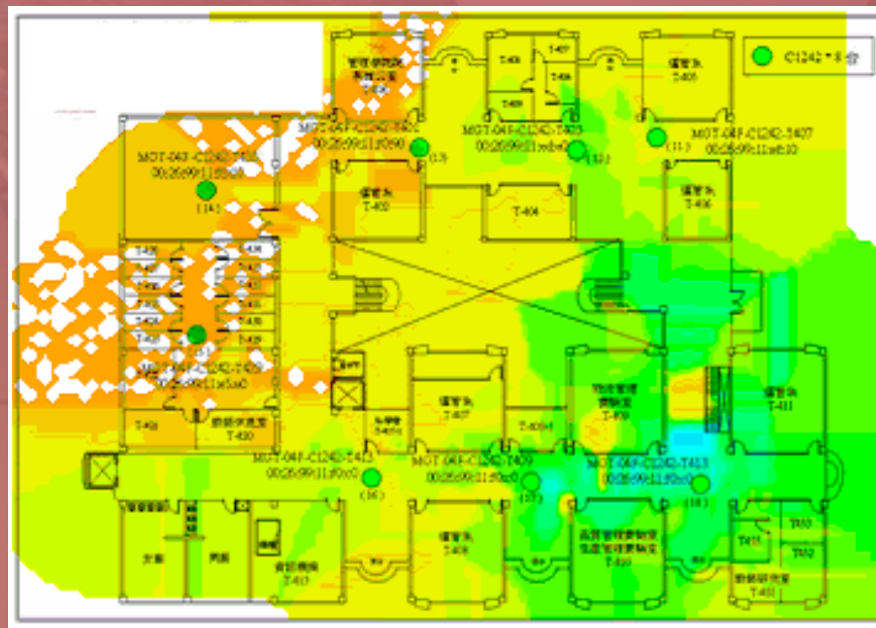
Ruckus 涵蓋範圍



WIN!

V.S

企業級 他牌 涵蓋範圍



# CommScope Ruckus 智慧網路全產品架構



軟體保固支援服務

Ruckus Cloud



Ruckus Analytics



Yagna<sup>®</sup> 雲端無線  
評估系統



行動設備  
APPS



IoT Suite  
物聯網套件

無線管理系統

- FlexMaster
- UMM(Unleashed Multi-Site Manager)



Cloudpath 入網認證系統



SmartCell Insight 無線分析系統



SPoT 智慧定位分析系統



Unleashed 可互管型基地台



ZoneDirector 無線控制器



SmartZone 無線控制器



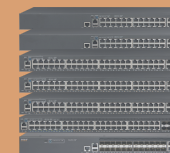
Smart Zone DP



無線網路  
基地台





























無線橋接  
基地台



ICX 交換器



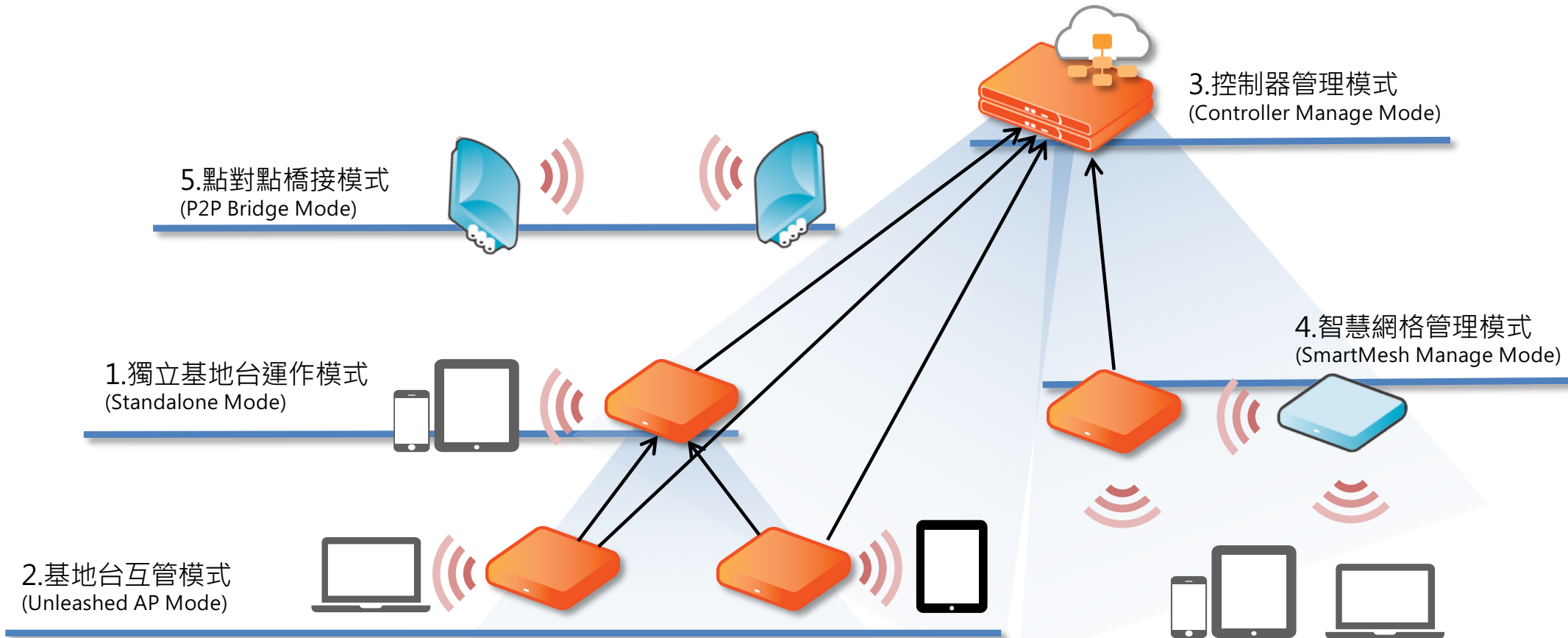
# Ruckus 全系列無線網路基地台

WiFi 6 802.11ax	8 x 8 : 8		R730 	R850 										
	4 x 4 : 4		R750 	R650 	T750 		R750 							
	2 x 2 : 2		R550 											
WiFi 5 801.11ac MU-MIMO	4 x 4 : 4		R710 	R720 	T610 	T710 	R710 	R720 	T610 	T710 				
	3 x 3 : 3		R610 				R610 							
	2 x 2 : 2	H510 	H320 	R320 	R510 	M510 	T310 	E510 	P300 	H510 	H320 	R510 	T310 	E510 
無線規格	壁掛型基地台 In Wall AP	室內型基地台 Indoor AP	戶外型基地台 Outdoor AP	戶外橋接基地台 Outdoor Bridge	可互管基地台 Unleashed AP									

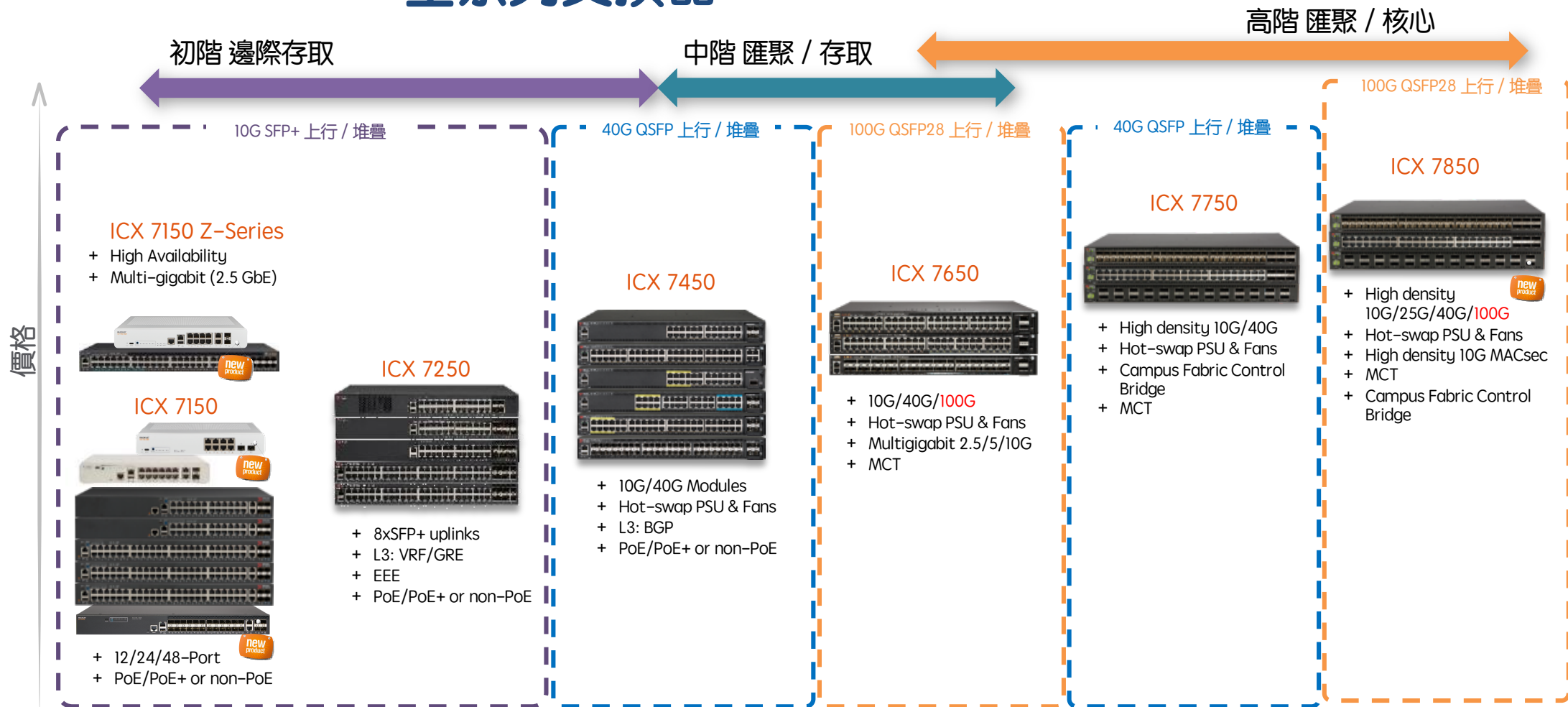
# Ruckus 控制器種類跟授權數

	小型架構		中小型架構		中大型架構		大型架構			
										
	Unleashed		ZD 1200		SZ-100		vSZ-E			
	<div style="display: flex; justify-content: space-around;"> <span>200.6</span> <span>200.7</span> </div>		<div style="display: flex; justify-content: space-around;"> <span>Version 9</span> <span>Version 10</span> </div>							
	25	50	75	150	1,024	1,024	10,000	10,000		
	512		2000		25,000	25,000	150,000	100,000		
	1024		4000		1RU	N/A	2RU	N/A		
	無控制器		桌上型		10 Gbps	vSZ-D	40 Gbps	vSZ-D		
	不支援		200Mbps		3+1 叢集 (Cluster)		3+1 叢集 (Cluster)			
	所有AP皆備援		Active-Standby							
					管理AP數:	3,000	3,000	30,000	30,000	
					管理用戶數:	60,000	60,000	450,000	300,000	
部署類型	小型單位(SMB) 單據點		中小型單位 多據點		中大型單位 企業多據點		中大型單位 企業多據點		服務供應商 管理服務	

# Ruckus 多種彈性設計帶來更多效益



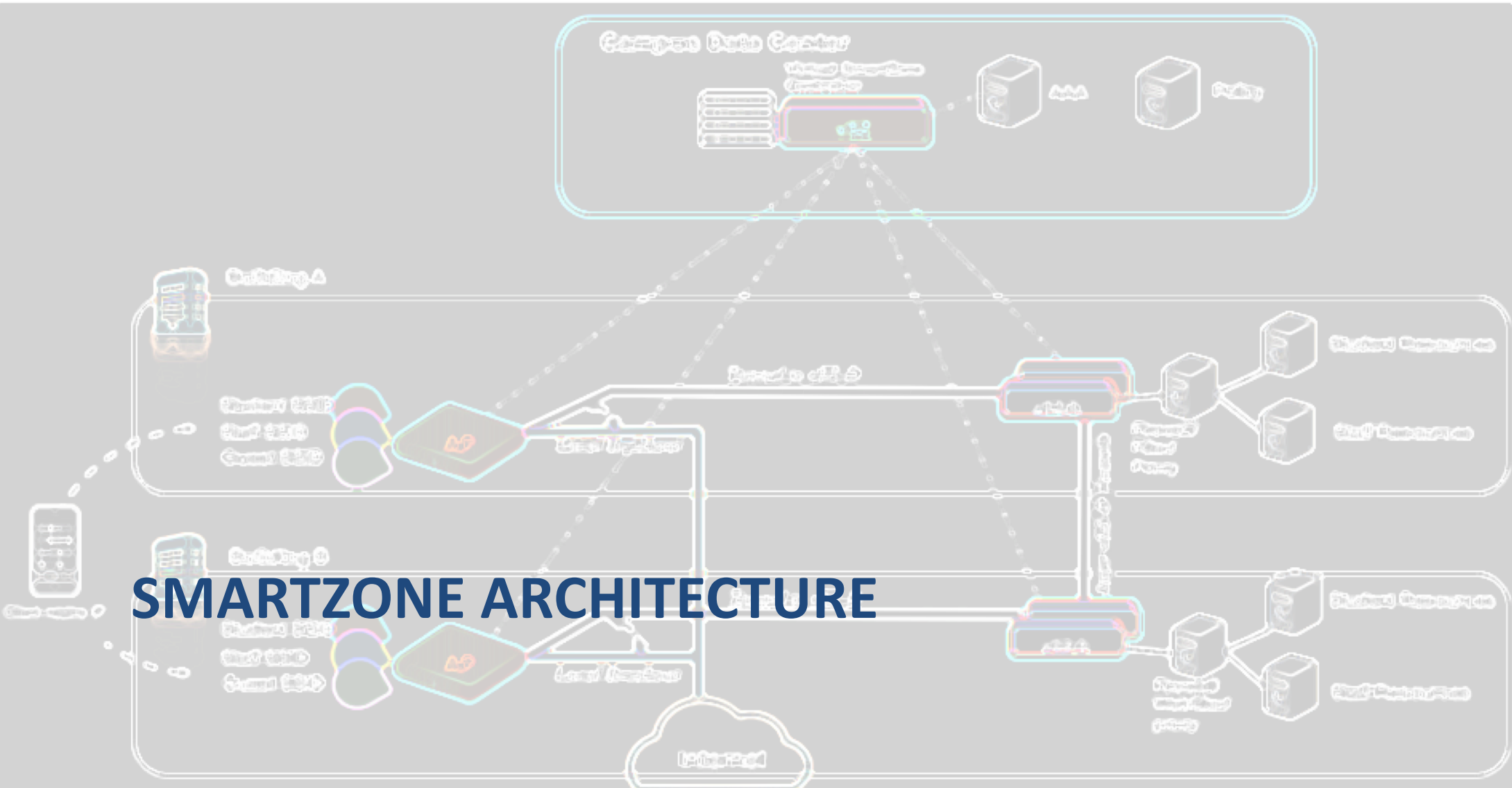
# Ruckus ICX 全系列交換器



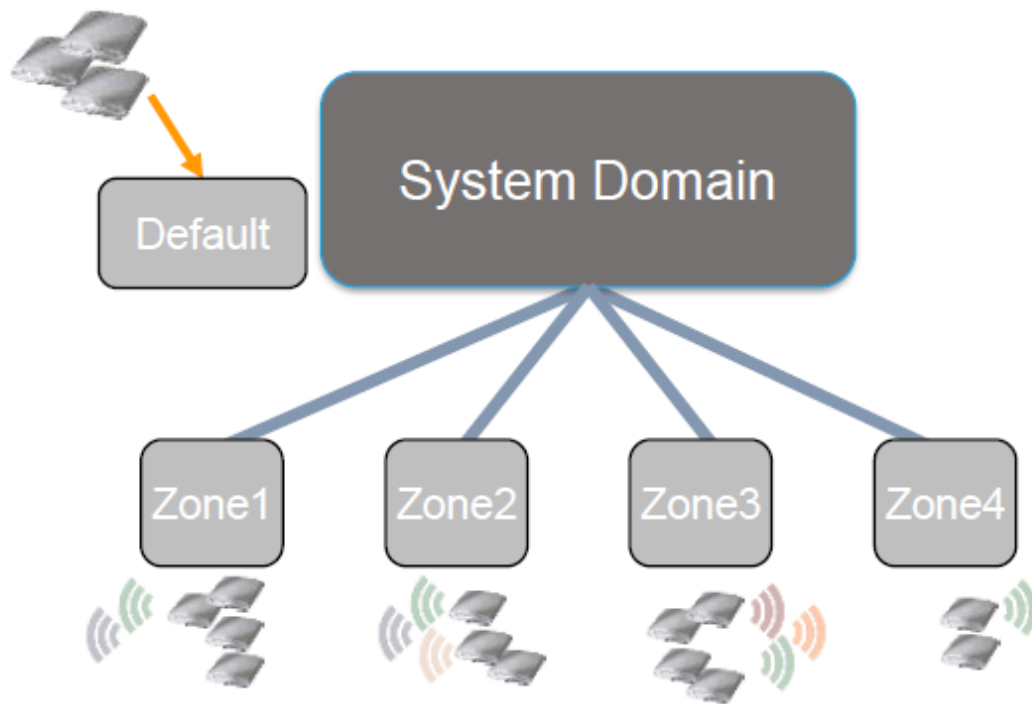
Function and Scalability



# SMARTZONE ARCHITECTURE



# Essentials Scale

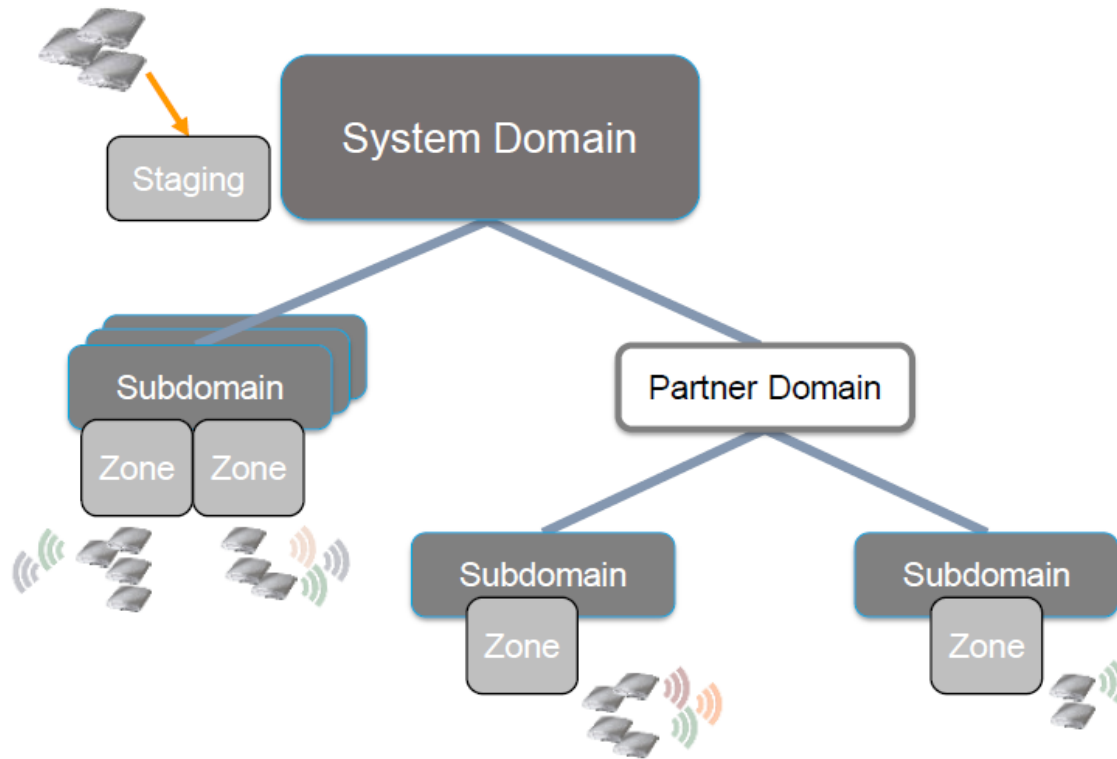


- SmartZone Essentials:

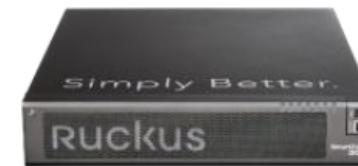


- Single System Domain
- Multiple Zones

# High Scale

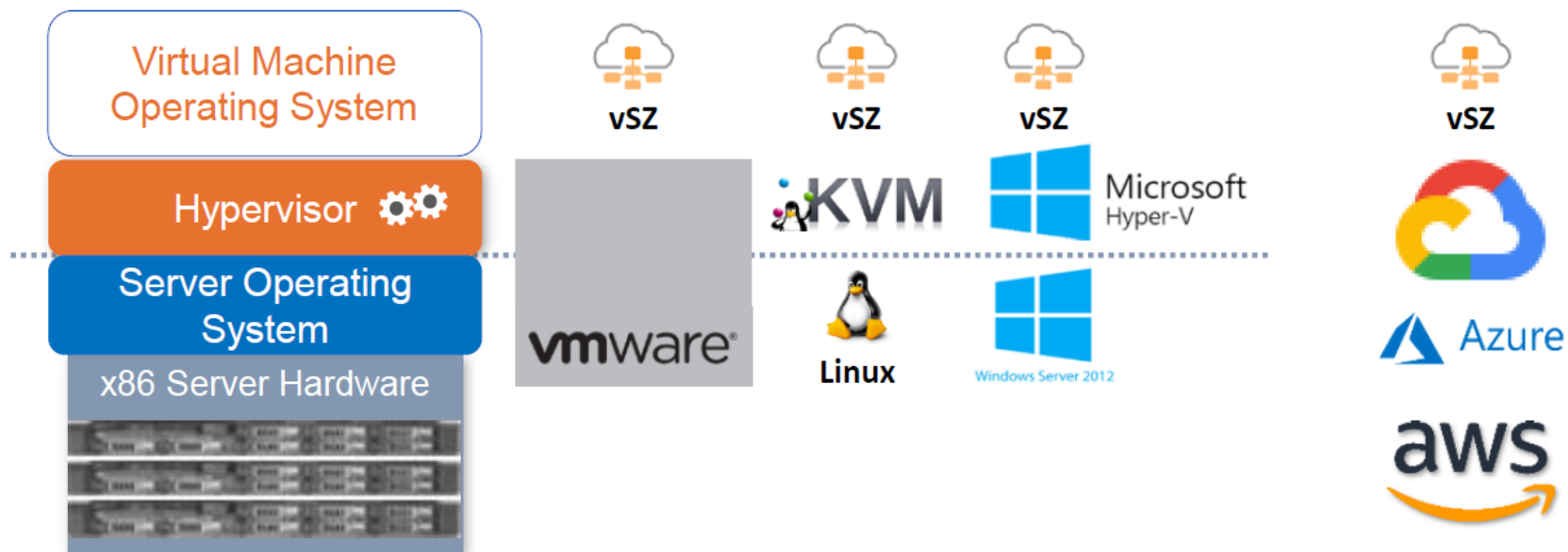


- SmartZone High Scale:



- Top level System Domain
- AP Staging Zone
- Multiple Subdomains
- Partner Domains

# Virtual



At the time this course was created, the supported options are:

- VMware
- Linux
- Microsoft Windows Server

• Minimum Requirements to run:

- 100GB disk space
- 13 GB of RAM

# Cloud Service

## Cloud-ready WLAN controller

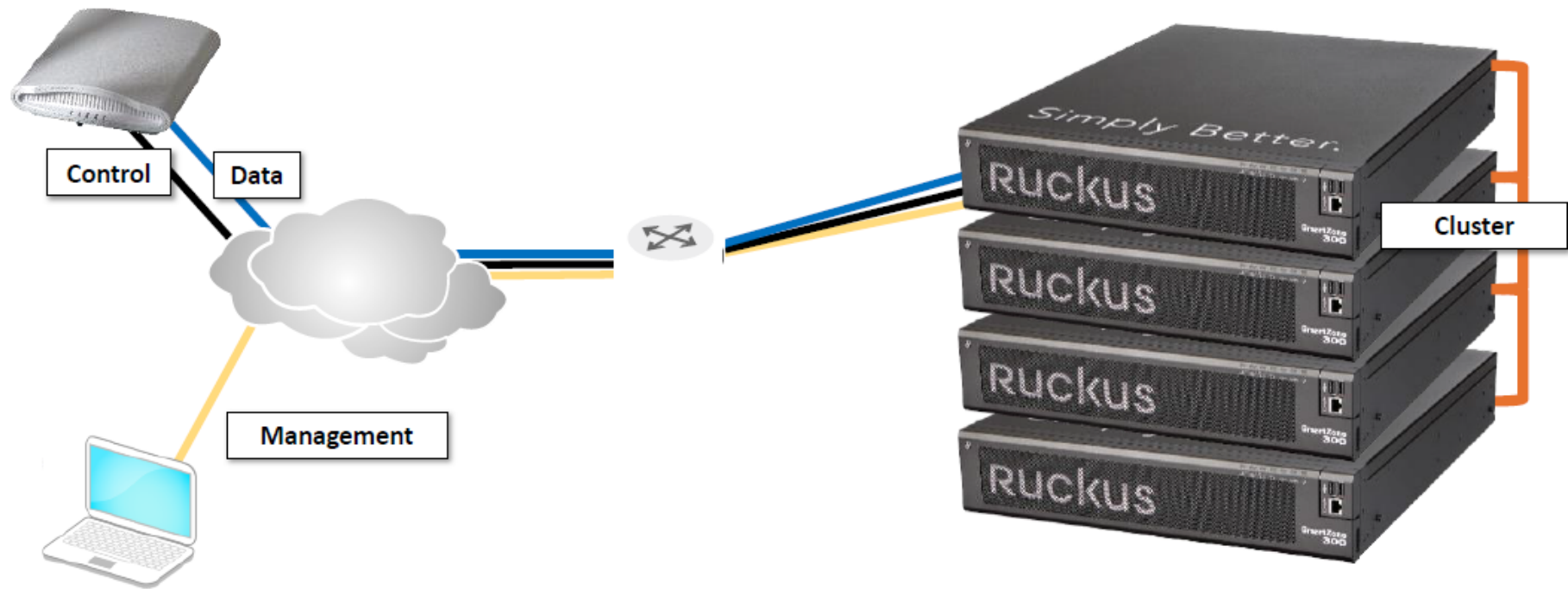
- Service providers and enterprises
- Flexibility, resiliency, and scale
- Can be deployed
- High Scale
- Essentials



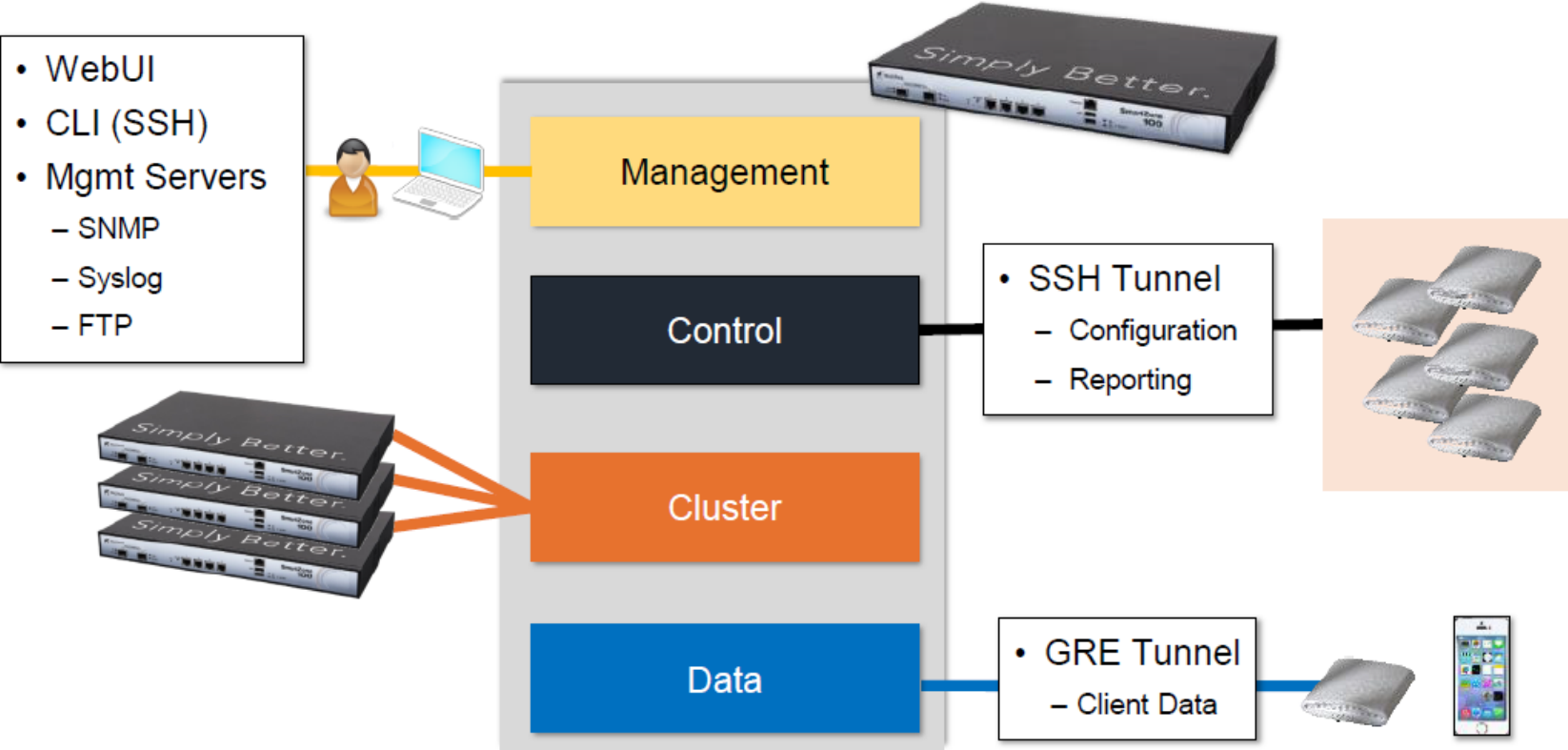
Azure



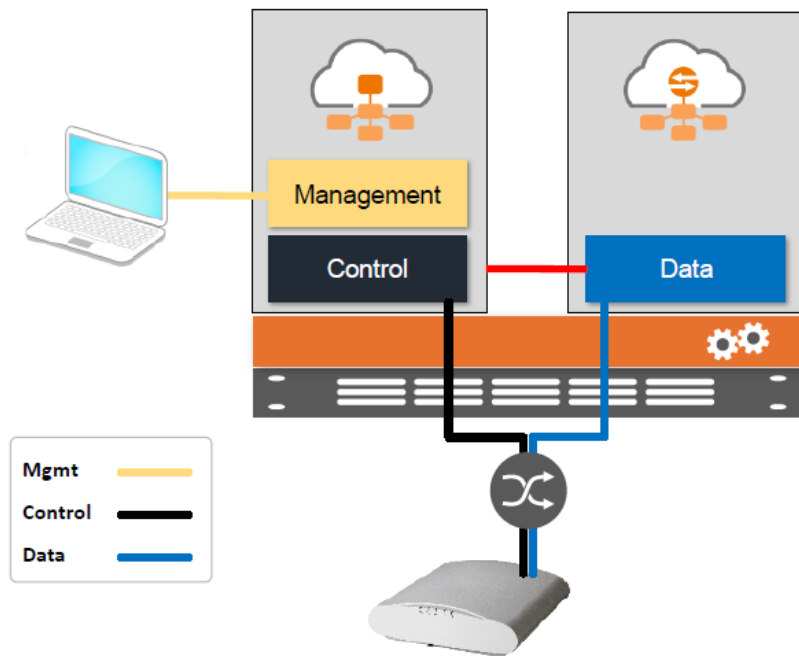
# Controller Interfaces Overview



# Controller Interfaces Communications

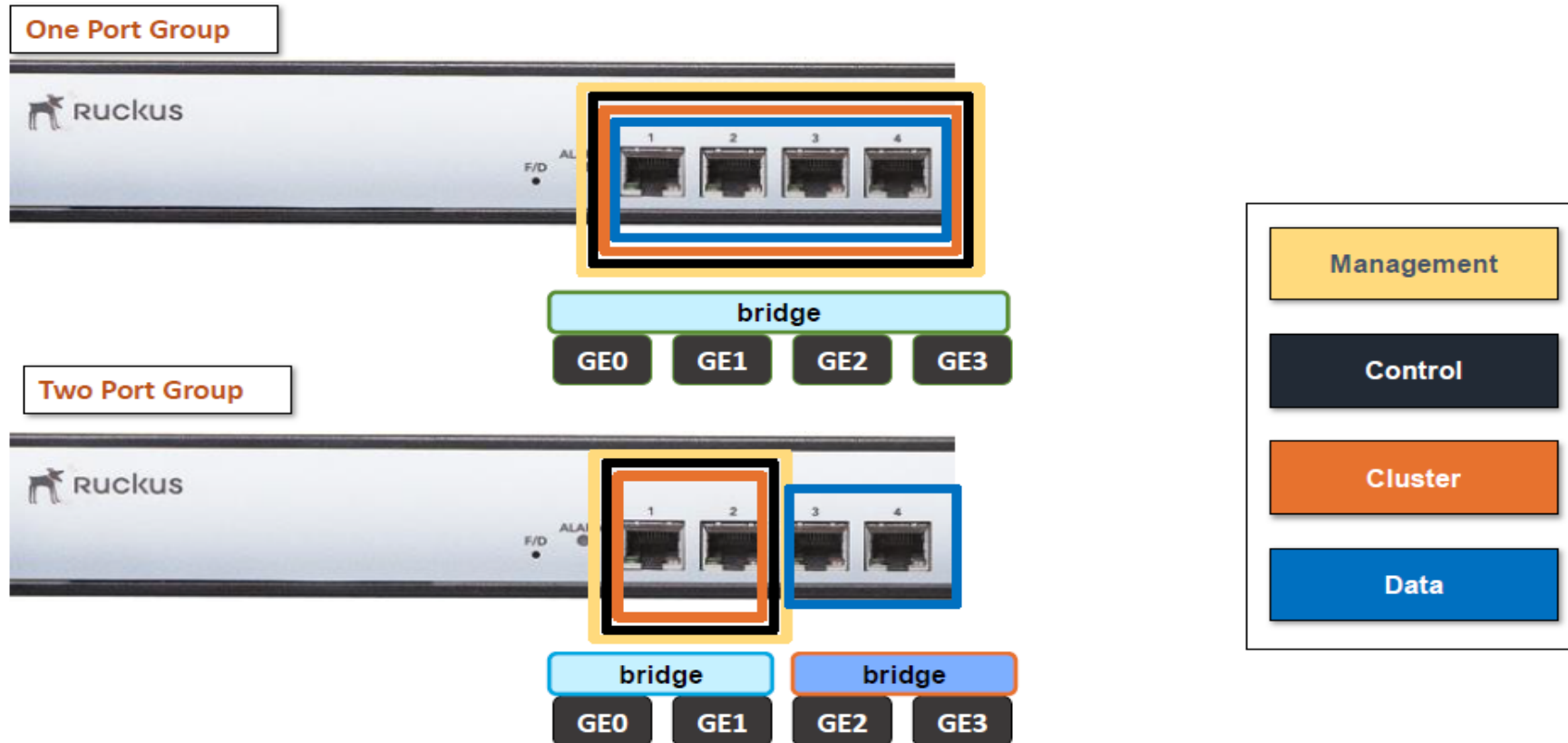


# Virtual SmartZone Data Plane (vSZ-D)



- NFV architecture
- Encrypts payload traffic
  - Compliance requirements
- Provides flexibility with:
  - Large deployments
    - Policy Control
    - QoS
  - Diverse environments

# SmartZone 100: S-104

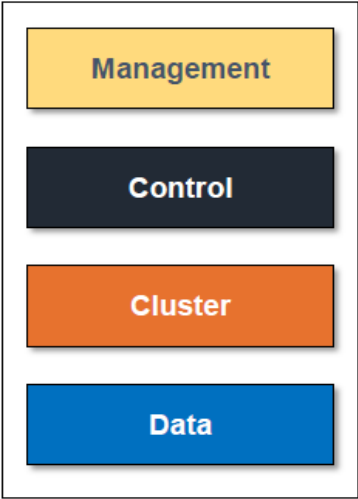


# SmartZone 100: S-124

One Port Group



Two Port Group





# SMARTZONE INITIAL

# vSZ initial

```
#####  
Welcome to vSZ #  
#####  
vSZ login: admin  
Password:  
Please wait. CLI initializing...  
  
Welcome to the Ruckus Virtual SmartZone Command Line Interface  
Version: 5.1.1.0.598  
  
vSZ> enable  
Password: *****  
  
vSZ# _
```

Default :  
admin/admin

```
vSZ# setup  
  
#####  
Start vSZ setup process:  
#####  
  
*****  
vSZ Profile  
*****  
1. Essentials  
2. High Scale  
Enter "i" for more information.  
*****  
select vSZ Profile (1/2): 1
```

# vSZ initial.

```
vSZ# setup
#####
start vSZ setup process:
#####

*****
vSZ Profile
*****
. Essentials
. High Scale
Enter "i" for more information.
*****
select vSZ Profile (1/2): 1
WARNING! You cannot change the vSZ profile once you complete setup. Are you sure
you want to install the "Essentials" profile? (y/n)[Y]
```

```
WARNING! You cannot change the vSZ profile once you complete setup. Are you sure
you want to install the "Essentials" profile? (y/n)[Y] y
network is not setup.

*****
IP Version Support
*****
. IPv4 only
. IPv4 and IPv6
*****
select address type: (1/2)
```

# vSZ initial.

```
*****
P Version Support
*****
. IPv4 only
. IPv4 and IPv6
*****
Select address type: (1/2) 1

*****
IPv4 address setup for Control,Cluster,Management
*****
. Manual
. DHCP
*****
Select IP configuration: (1/2) 1
IP Address: 192.168.0.150
Netmask: 255.255.255.0
Gateway: 192.168.0.2
Primary DNS: 8.8.8.8
Secondary DNS: 168.95.1.1
```

```
Current Network Settings (Before Applying)
*****
P Version Support Settings:
*****
P Version Support : IPv4 only

Interface IPv4 settings:
*****
Control,Cluster,Management:
*****
P Type : Manual
IP Address : 192.168.0.150
Netmask : 255.255.255.0
Gateway : 192.168.0.2

*****
DNS Server Settings:
*****
Primary DNS Server : 8.8.8.8
Secondary DNS Server : 168.95.1.1
*****
Enter 'y' to apply, 'n' to modify
Do you want to apply the settings? (y/n)
```

# vSZ initial.

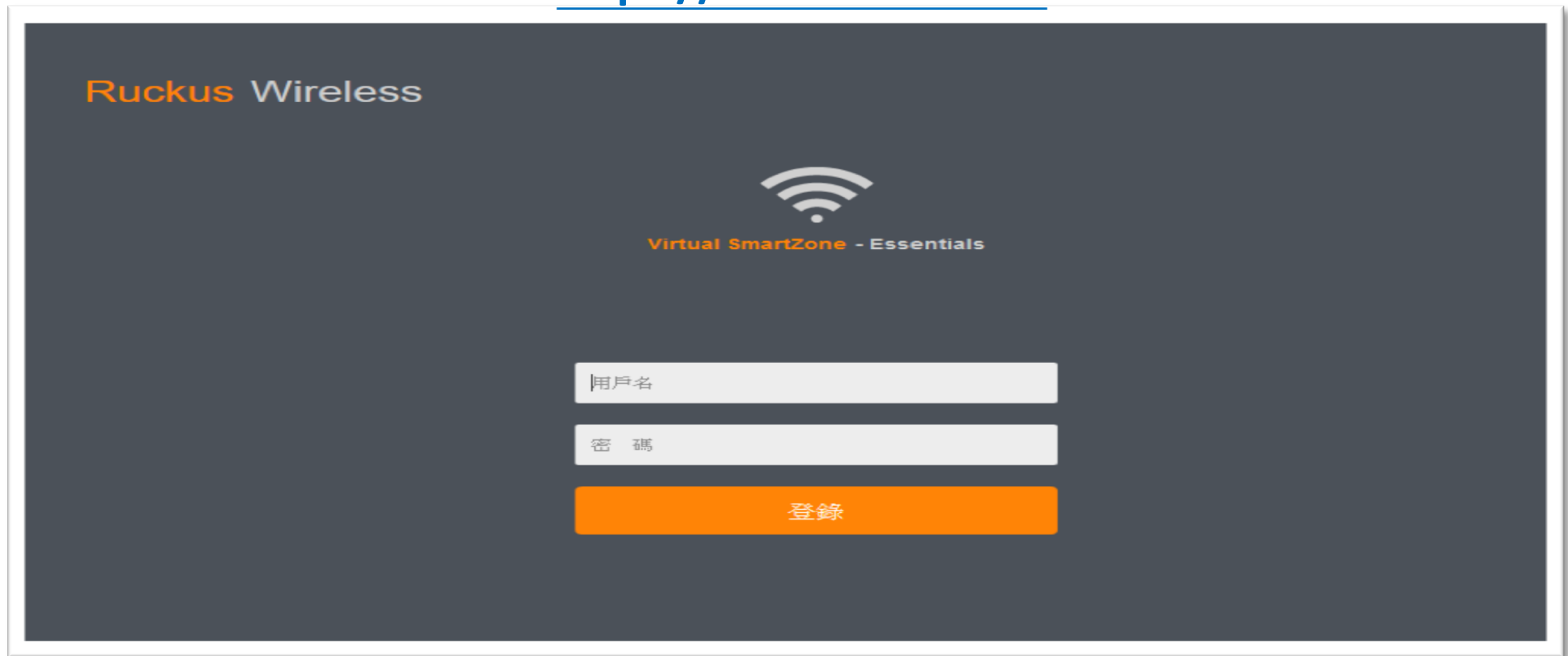
```
*****
Cluster:
*****
IP Type           : Manual
IP Address        : 10.145.64.151
Netmask           : 255.255.255.0
Gateway           : 10.145.64.254

*****
Management:
*****
IP Type           : Manual
IP Address        : 192.168.128.251
Netmask           : 255.255.255.0
Gateway           : 192.168.128.254

*****
DNS Server Settings:
*****
Primary DNS Server : 10.234.16.224
Secondary DNS Server : 8.8.8.8
*****
Enter 'y' to accept, 'n' to modify
Accept these settings and continue? (y/n) _
```

# vSZ initial.

<https://IP-address:8443>



The image shows the login interface for Ruckus Wireless Virtual SmartZone - Essentials. The background is dark gray. In the top left corner, the text "Ruckus Wireless" is displayed, with "Ruckus" in orange and "Wireless" in white. In the center, there is a white Wi-Fi signal icon above the text "Virtual SmartZone - Essentials", where "Virtual SmartZone" is in orange and "- Essentials" is in white. Below this, there are two white input fields: the top one is labeled "用戶名" (Username) and the bottom one is labeled "密碼" (Password). At the bottom center, there is a prominent orange button with the white text "登錄" (Login).

# vSZ initial.


The image displays the Ruckus Virtual SmartZone Setup Wizard interface. On the left is a navigation menu with the following items: Language, Profile, Management IP Address, Cluster Information (highlighted in orange), Administrator, Confirmation, and Configuration. The main content area shows the 'Cluster Information' section with the following fields:

- vSZ Cluster Setting: New
- Cluster Name: Lab
- Controller Name: vSZ-c
- Controller Description: vSZ-c
- Default Country Code: Taiwan
- NTP Server: ntp.ruc
- AP Conversion:  Convert
- Is this controller being replaced?

Three overlapping screenshots of the wizard steps are shown on the right:


- Setup Wizard > Language:** Shows the 'Language' selection screen.
- Setup Wizard > Profile:** Shows the 'Profile' selection screen with the instruction: "Please select profile configuration."
- Setup Wizard > Management IP:** Shows the 'Management IP' configuration screen. It includes a note: "Select how you want the Virtual SmartZone to obtain its IPv4 (and IPv6, if supported on your network) IP address settings. To obtain an IP address automatically using DHCP, click 'DHCP' for IPv4 or 'Auto Configuration' for IPv6. To specify an IP address, click 'Static' and then type the IP address settings in 'IP Address,' 'Netmask,' and 'Gateway.' An asterisk (\*) indicates required information." Below this, there are radio buttons for "IP Version Support":  IPv4 only,  IPv4 and IPv6. A section titled "Control(AP)/Cluster/Management(Web)" contains an "IPv4" configuration box with the following fields:
  - Static  DHCP
  - IP Address: 192.168.0.150
  - Netmask: 255.255.255.0
  - Gateway: (empty)Below the IPv4 box are fields for "Default Gateway", "Primary DNS Server" (8.8.8.8), and "Secondary DNS Server" (168.95.1.1).

# vSZ initial.

 <span style="float: right;">Setup Wizard - Virtual SmartZone</span> <span style="float: right;">version: 5.1.1.0.598</span>	
Language	<b>Administrator</b>
Profile	Enter Admin's password and password that permits administrative access to the Web interface. (Use this information to log into the Web interface after this setup is complete, to further configure your new wireless network.)
Management IP Address	<b>Admin Password *</b> <input type="password" value="••••••••"/> <b>Confirm Password *</b> <input type="password" value="••••••••"/>
Cluster Information	Enter CLI enable password and password that provides advance command <b>Enable Password *</b> <input type="password" value="••••••••"/> <b>Confirm Password *</b> <input type="password" value="••••••••"/>
<b>Administrator</b>	
Confirmation	
Configuration	

Next Back

# vSZ initial.



## Setup Wizard - Virtual SmartZone

version: 5.1.1.0.598

Language	<b>Confirmation</b>
Profile	Please review the following settings. If changes need to be made, click Back to edit your settings. If the settings are ready for use, click Finish.
Management IP Address	<b>Profile Type</b> Essentials <b>Cluster Name</b> Lab-Cluster <b>Protocol Type</b> TCP <b>Management IP</b> Control(AP)/Cluster/Management(Web): Manual 192.168.0.150
Cluster Information	<b>Default Country Code</b> TW System time will be automatically set.
Administrator	<b>System Time</b> Your current system time is ( 2019-07-11 15:00:20 Epoch : 1562828420 )
<b>Confirmation</b>	<b>System Time Zone</b> (GMT +08:00) Asia/Taipei <span style="color: red;">The field is only for UTC time calculation. Not vSZ timezone settings</span>
Configuration	* After completing the setup wizard, please check the <a href="#">Ruckus Wireless Support Web site</a> for the latest software updates. <b>Restore from Config Backup:</b> <input type="button" value="瀏覽..."/> 未選擇檔案。

# vSZ initial.

Setup Wizard > Configuration

**Ruckus™**  
Virtual SmartZone

## Setup Wizard - Virtual SmartZone

**Configuration**

The SmartZone is being configured. It may take up to 20 minutes to complete the setup process. Stretch your legs, grab some coffee, and if you changed the IP address during setup, don't forget to update the browser's URL.

0%

Bootstrapping

**WARNING** Please do not power off, reboot, disconnect, start another installation from a cluster member or change the IP address of any of the cluster members during the setup process. This will cause the initial setup to fail and you will have to start the setup process from the beginning.

20%

Blade Channel Opened

60%

Cassandra Initialized

100%

Done

Reconnect to the SmartZone's web interface  
<https://10.255.226.222:8443/vrsg/>

Language

Profile

Management IP Address

Cluster Information

Administrator

Confirmation

**Configuration**

# P.S\_vSZ VM

編輯設定 - vSZ (ESXi 5.0 虛擬機器)

虛擬硬體 虛擬機器選項

新增硬碟 新增網路介面卡 新增其他裝置

CPU	4	
記憶體	13312	MB
硬碟 1	100	GB
SCSI 控制器 0	LSI Logic SAS	
網路介面卡 1	VM Network	<input checked="" type="checkbox"/> 連線
網路介面卡 2	VM Network	<input checked="" type="checkbox"/> 連線
網路介面卡 3	VM Network	<input checked="" type="checkbox"/> 連線
視訊卡	指定自訂設定	

up to 16g

編輯設定 - vSZ (ESXi 5.0 虛擬機器)

虛擬硬體 虛擬機器選項

新增硬碟 新增網路介面卡 新增其他裝置

CPU	4	
記憶體	13312	MB
硬碟 1	100	GB
SCSI 控制器 0	LSI Logic SAS	
網路介面卡 1	VM Network	<input checked="" type="checkbox"/> 連線
視訊卡	指定自訂設定	

up to 16g

# P.S\_SZ100 initial

SZ100 Setup Wizard > Port Configuration

**Port Configuration**

Please select logical interface configuration.

- One Port Group**  
Management and AP Tunnel Traffic combined
- Two Port Group**  
Port Group 1: Management & AP Control  
Port Group 2: AP Tunnel Data

Diagram showing port configuration options: One Port Group (ports 1-4) and Two Port Group (PG1: ports 1-2, PG2: ports 3-4).

- Port Configuration offers two options:
  - One Port Group
  - Two Port Group
    - Separates management and AP control traffic (PG1) from AP tunnel traffic (PG2)
    - Requires additional settings

<https://192.168.2.2:8443>

# P.S\_SZ100 initial.

## SZ100 Setup Wizard > Two Port Group IP Settings

The screenshot displays the 'Setup Wizard - SmartZone' interface for a Ruckus SmartZone 100. The left sidebar contains a navigation menu with 'Port Group 1' highlighted in orange. The main content area is titled 'Port Group 1' and includes instructions on how to configure IP settings. Below the instructions, there are radio buttons for 'IP Version Support' with 'IPv4 only' selected. A blue callout box highlights the 'Management & AP Control' section, which contains an 'IPv4' configuration panel. This panel has radio buttons for 'Static' and 'DHCP' (selected), and input fields for 'IP Address' (10.176.208.22), 'Netmask' (255.255.252.0), and 'Gateway' (10.176.208.1). To the right of these fields are input fields for 'Primary DNS Server' (10.176.4.10) and 'Secondary DNS Server' (10.176.4.11). A second callout box highlights the 'Port Group 2' section, which is currently empty. A third callout box highlights the 'AP Tunnel Data' section, which has radio buttons for 'Manual' and 'DHCP' (selected), and input fields for 'IP Address', 'Netmask', and 'Gateway'.

- If Two Port Group is selected, separate IP settings are configured for:
  - Management & AP Control
  - AP Tunnel Data

# P.S\_three interface initial

Setup Wizard > Management IP Address

**Management IP**

Select how you want the Virtual SmartZone to obtain its IPv4 (and IPv6, click "DHCP" for IPv4 or "Auto Configuration" for IPv6. To specify an IP "Gateway." An asterisk (\*) indicates required information.

IP Version Support  IPv4 only  IPv4 and IPv6

1  Control(AP) 2  Cluster 3  Management(Web)

	IPv4	IPv6
Default Gateway*	<input type="text" value="Control(AP) Cluster Management(Web)"/>	<input type="text"/>
Primary DNS Server	<input type="text"/>	<input type="text" value="IPv6 Primary DNS"/>
Secondary DNS Server	<input type="text"/>	<input type="text" value="IPv6 Secondary DNS"/>

	IPv4	IPv6
Static/DHCP	<input checked="" type="radio"/> Static <input type="radio"/> DHCP	<input checked="" type="radio"/> Static <input type="radio"/> Auto Configuration
IP Address *	<input type="text"/>	<input type="text"/>
Netmask *	<input type="text"/>	
Gateway	<input type="text"/>	<input type="text"/>

# P.S\_SZ100 Upgrade software

**Ruckus** Setup Wizard - SmartZone 100

Port Configuration  
**IP Setting**  
Cluster Information  
Administrator  
Confirmation  
Configuration

### IP Setting

Select how you want the SmartZone 100 to obtain its IPv4 (and IPv6, if supported on your network) IP address settings. To obtain an IP address automatically using DHCP, click "DHCP" for IPv4 or "Auto Configuration" for IPv6. To specify an IP address, click "Static" and then type the IP address settings in "IP Address," "Netmask," and "Gateway." An asterisk (\*) indicates required information.

**IP Version Support**  IPv4 only  IPv4 and IPv6

**Upgrading Wireless Controller**

Please upload wireless controller firmware

**Choose File** No file chosen Close

Gateway \*   
NAT IP

Primary DNS Server  IPv4 Primary DNS  
Secondary DNS Server  IPv4 Secondary DNS

Ver. 3.4.0.0.97e **Upgrade** < Back Next >

# ACCOUNT POINT INITIAL



# AP initial



The image shows the Ruckus Wireless Admin login interface. At the top is the Ruckus Wireless logo, which features a black silhouette of a dog with orange signal waves above its head, followed by the text "RUCKUS™ WIRELESS". Below the logo is the title "Ruckus Wireless Admin" in blue. There are two input fields: "Username:" with the text "super" and "Password:" with ten black dots. To the right of the password field, the text "sp-admin" is written in red. Below the input fields is an orange rounded button labeled "Login". At the bottom of the page is a logo for "goahead WEB SERVER" where "goahead" is in small black text and "WEB SERVER" is in larger blue text.

Default IP: 192.168.0.1

super  
sp-admin

ver.112 or 114 default use "https"

# AP initial.

**Ruckus R500 Multimedia Hotzone Wireless AP**

**Status**  
Device  
Internet  
Local Subnets  
Radio 2.4G  
Radio 5G

**Configuration**  
Device  
Internet  
Local Subnets  
Radio 2.4G  
Radio 5G  
Ethernet Ports  
Hotspot

**Maintenance**  
Upgrade  
Reboot / Reset  
Support Info

**Administration**  
Management  
Diagnostics  
Log

**Status :: Device**

Device Name: RuckusAP  
Device Location:  
GPS Coordinates:  
MAC Address: 1C:B9:C4:16:28:20  
Serial Number: 171602403555  
**Software Version: 100.0.0.0.127**  
Uptime: 1 day 11 hrs 37 mins 44 secs  
Current Time (GMT): Sat Jun 9 14:51:18 2018

**LAN Port Status** [Refresh](#)

Port	Interface	802.1X	Logical Link	Physical Link	Label
0	eth0	None	Up	Up 1000Mbps full	10/100/1000 PoE
1	eth1	None	Down	Down	10/100/1000

# AP initial.

**Ruckus R500 Multimedia Hotzone Wireless AP**

**Configuration :: Internet**

**Status**  
Device  
Internet  
Local Subnets  
Radio 2.4G  
Radio 5G

**Configuration**  
Device  
**Internet**  
Local Subnets  
Radio 2.4G  
Radio 5G  
Ethernet Ports  
Hotspot

**Maintenance**  
Upgrade  
Reboot / Reset  
Support Info

**Administration**  
Management  
Diagnostics  
Log

NTP Server:

Management VLAN:  ( Need to reboot for change to take effect )

IPv4 Connection Type:  DHCP  **Static IP**  PPPoE

Internet Connection Settings

IPv4 Address:

IPv4 Subnet Mask:

IPv4 Gateway:

IPv4 DNS Mode :  Auto  Manual

IPv4 DNS IP Address Settings

IPv4 Primary DNS Server:

IPv4 Secondary DNS Server:

IPv6 Connection Type:  Auto Configuration  Static IP

IPv6 Primary DNS Server:

IPv6 Secondary DNS Server:

L2TP Connection

L2TP Connection:  Enable  Disable

[Restore previous settings](#)

目前的 R750 需注意

# AP initial.

Ruckus R310 Multimedia Hotzone Wireless AP

**Status**  
Device  
Internet  
Local Subnets  
Radio 2.4G  
Radio 5G

**Configuration**  
Device  
Internet  
Local Subnets  
Radio 2.4G  
Radio 5G  
Ethernet Ports  
Hotspot

**Maintenance**  
Upgrade  
Reboot / Reset  
Support Info

**Administration**  
Management  
Diagnostics  
Log

**Administration :: Management**

Network Profile: 4bss

Telnet Access?  Enabled  Disabled

Telnet Port:

SSH Access?  Enabled  Disabled

SSH Port:

HTTP Access?  Enabled  Disabled

HTTP Port:

HTTPS Access?  Enabled  Disabled

HTTPS Port:

Certificate Verification PASSED

Auto-provisioning?  Enabled  Disabled

Controller Discovery Agent (LWAPP)?  Enabled  Disabled

SmartCellGateway Agent?  Enabled  Disabled

Cloud Discovery Agent (FQDN)  Enabled  Disabled

**Set Controller Address (Reboot to take effect)**

Primary Controller Addr:

Secondary Controller Addr:

TR069 / SNMP Management Choice

Ruckus R310 Multimedia Hotzone Wireless AP

**Status**  
Device  
Internet  
Local Subnets  
Radio 2.4G  
Radio 5G

**Configuration**  
Device  
Internet  
Local Subnets  
Radio 2.4G  
Radio 5G  
Ethernet Ports  
Hotspot

**Maintenance**  
Upgrade  
Reboot / Reset  
Support Info

**Maintenance :: Reboot / Reset**

## What would you like to do?

Reboot with current settings?

Reset to factory settings? [Reset now](#)

Rebooting or resetting your device will cause your network to be unavailable during the reboot process.

# P.S\_ AP Join information - CLI

```
rkscli: get scg

----- SCG Information -----
SCG Service is enabled.
AP is managed by SCG.
State: IMG_REQ_STATE
Server List: 10.10.100.51
SSH tunnel connected to 10.10.100.51
Failover List: Not found
Failover Max Retry: 2
DHCP Opt43 Code: 6
Server List from DHCP (Opt43/Opt52): Not found
SCG default URL: RuckusController
SCG config|heartbeat intervals: 30|30
SCG gwloss|serverloss timeouts: 1800|7200
Controller Cert Validation : disable
-----
OK
rkscli: █
```

# P.S\_ AP Join information - LED



- Off: Standalone mode
- Green: The AP is being managed by a controller.
- Slow flashing green (one flash every two seconds):  
The AP is being managed by a controller, but is currently unable to communicate with the controller.
- Fast flashing green (two flashes every second):  
The AP is being managed by a controller and is currently receiving configuration settings (provisioning) or an image update.

# P.S\_R750 問題

R750 Default software > Ver.114

Join SMARTZONE > Ver.5.2

>>> 需要先在 AP 上面將 ip mode 指定 ipv4

```
[rkscli: set ipmode wan ipv4  
IP Mode is already set as ipv4.  
OK  
rkscli: █
```

```
[rkscli: set ip  
Commands starting with 'set ip' :  
set ipaddr : set ipaddr {wan|wan-lte|video|mgmt} [vlan <vlan id>] {options}  
-> <ipaddr> <netmask> <gateway> "static IP case"  
-> dynamic "DHCP case "  
For wan-lte, only dynamic configuration is supported  
-- Modify IP address  
set ipmode : set ipmode {wan|lan|video|mgmt} {ipv4 | ipv6 | dual }  
ipv6-only cannot be set when hotspot or router mode is enabled  
-- Modify IP Mode  
set ipv6addr : set ipv6addr {wan|video|mgmt} [vlan <vlan id>] {options}  
-> <ipv6addr> <prefixlen> <gateway> "static IP case,prefix length:<16..128>"  
-> autoconfig "auto configuration case"  
-- Modify IPv6 address  
set ipv6ctrl : set ipv6ctrl <wlan name> {options}  
-> [nd-proxy {enable|disable|counter-reset} ]  
-> [ns-suppress {enable|disable|counter-reset} ]  
-> [ra-proxy {enable|disable|counter-reset} ]  
-> [rsra-guard {enable|disable|counter-reset} ]  
-> [ra-throttle <enable maximum_ra_allowed time_interval_in_minutes> ]  
-> [ra-throttle disable|counter-reset ]  
-> [ counter-reset ]  
-- counter-reset - Reset the counter value to 0  
-- Set IPv6 Control features
```

# P.S\_Provision ID

## AP-CONFIG

**set scg ip 2xx.99.1xx.99 , 2xx.99.1xx.98**

**set provisioning-tag TID77888877**

Rule Description:

\* Zone Name:

Rule Type:  IP Address Range  Subnet  GPS Coordinates  Provision Tag

Provision Tag

\* Provision Tag:

# P.S\_Software Ver

5.x	
5.2.0.0.699	R750 只能夠搭配此版本
5.1.2.0.302	
5.1.1.0.598	
5.1.1.0.589	

3.x	
3.6.2.0.250	7982 , 7372
3.6.2.0.222	
3.6.1.0.227	

AP default
114.0.0.0.1392
112.1.0.0.2146
110.0.0.0.663
104.1.0..298

# Complete

The screenshot displays the Ruckus CMN interface. The main dashboard shows a 'Health' status with '1 Cluster', '1 AP', and '0 Client'. A red box highlights the '1 AP' indicator. Below this, a message states: 'Google Maps are not working due to an API key problem. If this problem persists, please contact your account manager. Google Maps feature is not available, you can still view the network topology. [Switch to Group Topology](#) [Configure the Google API Key](#)'. The right-hand panel shows 'System Info' and 'System Summary'. The 'System Summary' table includes the following data:

System Capacity of Cluster:	
Total Capacity:	1000 APs ( 200 Switches )
Connected AP:	1 APs
Connected Switch:	1 Switches
Remaining AP:	994 APs
Remaining Switch:	198 Switches

The 'System Info' section lists: Controller Version: 5.2.0.0.699, Control Plane Software Version: 5.2.0.0.770, and AP Firmware Version: 5.2.0.0.1412. The 'License Summary' section shows 3GPP Tunneling License (Consumed/Total): 0/0. The bottom navigation bar includes 'Performance' and 'Connection Failure' tabs.



vsZ license expires in 2 days >

[Show all messages](#)



default



System

General Settings

AP Settings

Switch Settings

Cluster

Maps

Certificates

Templates

Access Points

Switches

Wireless LANs

Clients

Firewall

System Info

Controller Version:	5.2.0.0.699
Control Plane Software Version:	5.2.0.0.770
[?] AP Firmware Version:	5.2.0.0.1412

System Summary

Cluster Name:	ac-demo
# of Planes (Control/Data):	1/0
System Name:	ac-demo-C
System Uptime:	87d 8h 15m
Serial Number:	9820353N5Q25RA0SUXLX7AKTHXUV
System Capacity of Cluster:	Total Capacity: 500 APs ( 100 Switches )
	Connected AP: 5 APs
	Connected Switch: 3 Switches
	Remaining AP: 480 APs
	Remaining Switch: 96 Switches

License Summary

3GPP Tunneling License (Consumed/Total):	0/0
AP Capacity License	4/5

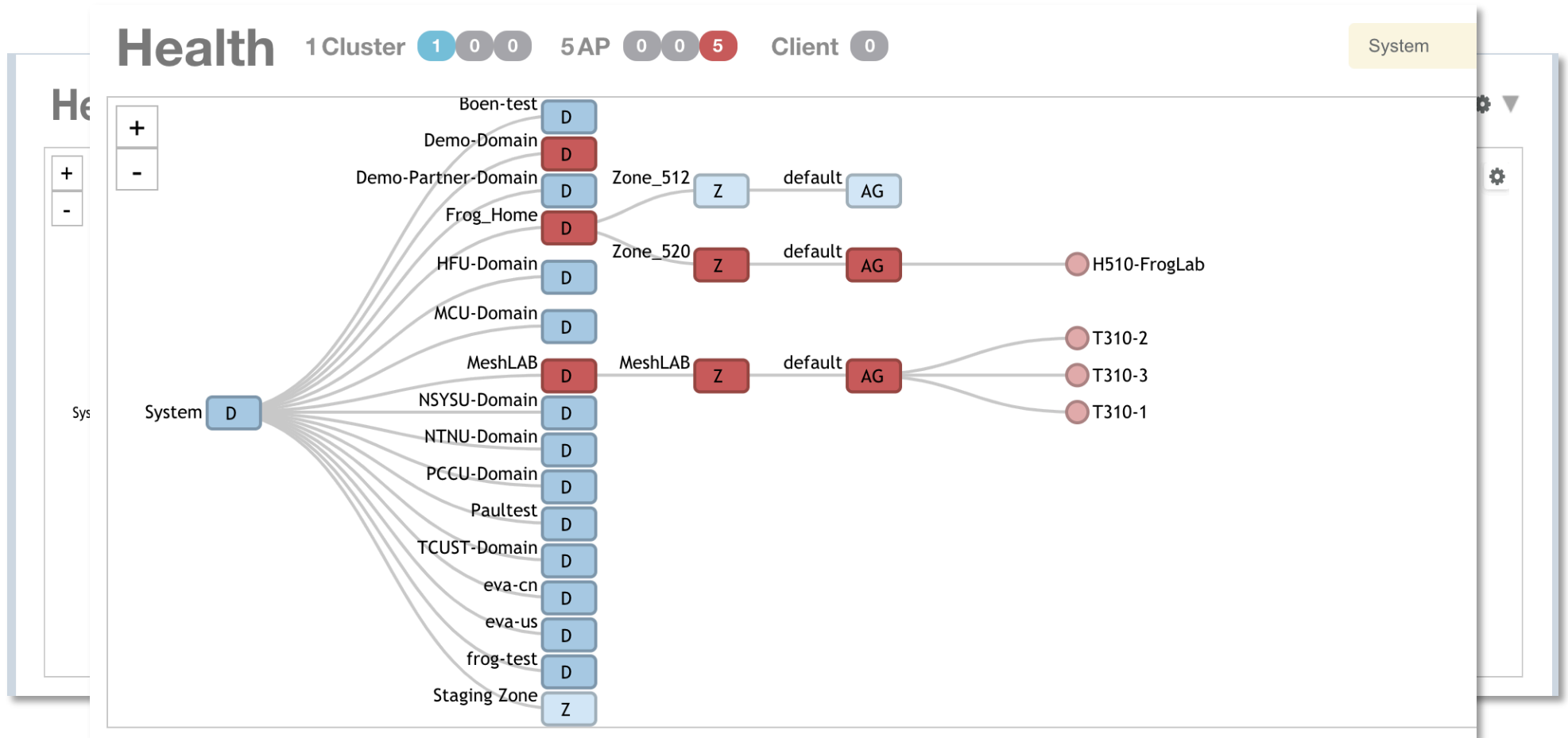
# SMARTZONE CONFIG



# Dashboard

The screenshot displays the Ruckus dashboard interface. At the top left, the Ruckus logo and 'Virtual SmartZone - High Scale' are visible. The top right shows the device name 'FrogLAB-987', the date and time '2020-07-01 15:09:35', a 'default' dropdown menu, and user information 'admin'. The main navigation sidebar on the left includes 'Dashboard', 'System', 'Access Points', 'Switches', 'Wireless LANs', 'Clients', 'Firewall', 'Services & Profiles', 'Report', 'Troubleshooting', 'Administration', 'Events & Alarms', and 'Diagnostics'. The 'System Info' section at the bottom of the sidebar shows 'Hostname: c1' and 'Version: 5.2.0.0.699'. The main content area features a 'Health' section with a status of 'No outstanding alarms' and a summary: '1 Cluster (1 0 0) 1 AP (1 0 0) Client 0'. A red error message states: 'Google Maps are not working due to an API key problem. If this problem persists, you can switch to a different map provider. Google Maps feature is not available, you can switch to a different map provider. [Switch to Group Topology View](#) [Configure the Google API Key](#)'. A 'Settings - Map' dialog box is open, showing 'View Mode' set to 'Map' and 'Tooltip' options for 'Map', 'Groups', 'Control Planes', and 'Data Planes', each with an 'ON' toggle. Other settings include 'Traffic (1hr)', 'Latency', 'Airtime Utilization', 'Connection Failure', and 'Show Mesh Links' (OFF). The dialog has 'OK' and 'Close' buttons. A gear icon in the top right of the main content area is also highlighted with a red box.

# Dashboard.



# System

Dashboard

System

- General Settings
- AP Settings
- Switch Settings
- Cluster
- Maps
- Certificates
- Templates
- Access Points
- Switches
- Wireless LANs
- Clients
- Firewall
- Services & Profiles
- Report

About Time Syslog Cloud Services Northbound Data Streaming WISPr Northbound Interface SNMP Agent SMTP FTP SMS Gateway Advanced Location Service

### System Info

Controller Version: 5.2.0.0.699

Control Plane Software Version: 5.2.0.0.770

[?] AP Firmware Version: 5.2.0.0.1412

### System Summary

Cluster Name: FrogLAB-987

# of Planes (Control/Data): 1/0

System Name: c1

System Uptime: 43d 21h 8m

Serial Number: 982M3W7FFBH5FBUPMMHX54CJTMVA

System Capacity of Cluster:	Total Capacity:	1000 APs ( 200 Switches)
	Connected AP:	1 APs
	Connected Switch:	1 Switches
	Remaining AP:	994 APs
	Remaining Switch:	198 Switches

### License Summary

3GPP Tunneling License (Consumed/Total): 0/0

AP Capacity License (Consumed/Total): 1/5

AP Direct Tunnel License (Consumed/Total): 0/5

Data Plane Capacity License (Consumed/Total): 0/10 (External-Virtual 0) (External-Physical 0)

### System Time


System Time: 2018-09-19 22:56:39 UTC

System UTC Time: 2018-09-19 22:56:39 UTC

\* NTP Server: ntp.ruckuswireless.com Sync Server

\* System Time Zone: (GMT+0:00) UTC

Refresh OK Cancel



# System.

Dashboard

System

- General Settings
- AP Settings
- Switch Settings
- Cluster
- Maps
- Certific
- Templa

AP Registration | Critical AP Tagging | Tunnel UDP Port | Country Code | AP Number Allocation | AP MAC OUI Validation

+ Create | Configure | Delete | Clone | Update Priorities | Up | Down

search table [Q] [Refresh] [Settings]

Priority ▲	Rule Type	Rule Description	Rule Parameters	Zone Name
------------	-----------	------------------	-----------------	-----------


No data << 1 >>

Approval | AP Registration | Critical AP Tagging | Tunnel UDP Port | Country Code

To enhance wireless security, deactivate this option. When this option is deactivated, you must manually "approve" each newly discovered AP.

ON Automatically approve all join requests from APs

Refresh | OK | Cancel



# System.

The screenshot displays a web application interface for managing switch registration rules. On the left is a dark sidebar with navigation items: Dashboard, System (highlighted), General Settings, AP Settings, Switch Settings (highlighted), Cluster, Maps, Certificates, and Templates. The main content area is titled 'Switch Registration' and features a toolbar with buttons for '+ Create', 'Configure', 'Delete', 'Clone', 'Update Priorities', 'Up', and 'Down'. Below the toolbar is a table with columns for 'Priority', 'Rule Type', and 'Rule Description'. A search bar labeled 'search table' and a refresh icon are located in the top right. A modal dialog titled 'Switch Registration Rule' is open, containing the following fields and options:

- Rule Description:
- \* Group Name:
- Rule Type:  IP Address Range,  Subnet,  Model Number
- IP Address Range section:
  - \* From IP:
  - \* To IP:

At the bottom of the modal are 'OK' and 'Cancel' buttons. In the background, a table shows '1 records' with navigation arrows.

# System.

**Cluster** DP Zone Affinity Flexi-VPN L3 Roaming

**Cluster (1)** 1 online 0 flagged 0 offline

**Control Planes**

Configure Delete Restart More

Name	Status	Management IP	Cluster IP	Control IP	Model	Serial Number	# of APs	MAC Address	Description
c1-C	Online	10.10.100.50	10.10.100.50	10.10.100.50	vSZ-H	982M3W7FF...	1	00:0C:29:84:77:...	c1

**Data Planes**

Configure Approve Delete More

**Summary**

**Cluster Info**

Name	FrogLAB-987
Total Control Planes	1
Total Data Planes	0

**Control Planes**

Configure Delete Restart More

Cluster IP	Control IP	Model	Serial Number	# of APs	MAC Address	Description	Firmware	Cluster Role	Uptime
10.10.100.50	10.10.100.50	vSZ-H	982M3W7FF...	1	00:0C:29:84:77:...	c1	5.2.0.0.770	Leader	43d 21h 24m

# System.

Dashboard

**System**

- General Settings
- AP Settings
- Switch Settings
- Cluster
- Maps**
- Certificates
- Templates
- Access Points
- Switches

## Maps

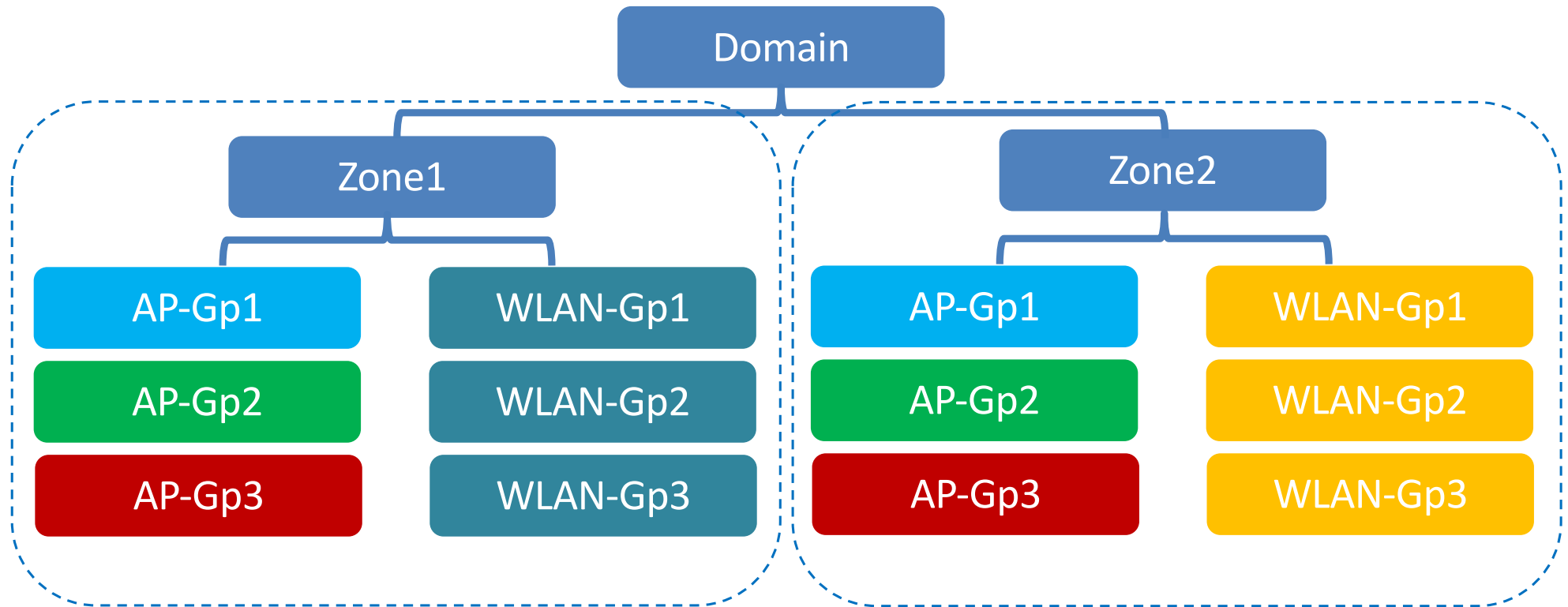
Map1

ON Show Signal Coverage  2.4 GHz  5 GHz

- D System
  - D FrogLAB
    - + Z Zone-362
    - + Z zone-512
    - Z zone-520
    - + AG default
    - Map1

-20 dBm  
-30 dBm  
-40 dBm  
-50 dBm  
-60 dBm  
-70 dBm  
-80 dBm  
-90 dBm  
-100 dBm

# Domain - Zone - Group



# Zone

Access Points > Group

## Access Points (2)

System > TeamXDomain

+ [edit] [delete] [refresh] [back] More ▾

- [D] System
  - + [D] PartnerXDomain
  - [D] TeamXDomain
  - + [Z] Staging Zone

## Create Group

Name: TeamXZone Description:

Type:  Domain  Zone  AP Group

Parent Group: TeamXDomain

# Zone.

## Configure Group

\* Name:

Description:

Type:  Zone  AP Group

Parent Group:

### Configuration

#### General Options

\* AP Firmware: 5.1.1.0.624

Country Code:

Different countries have different regulations on the usage of radio channels. To ensure that APs use authorized radio channels, select the correct country code for your location.

Location:  (example: Ruckus HQ)

Location Additional Information:  (example: 350 W Java Dr, Sunnyvale, CA, USA)

GPS Coordinates: Latitude:  Longitude:  (example: 37.411272, -122.019616)

Altitude:  meters

\* AP Admin Logon:

\* Logon ID:

\* Password:

# Zone.

Mesh Options

Enable mesh networking in this zone

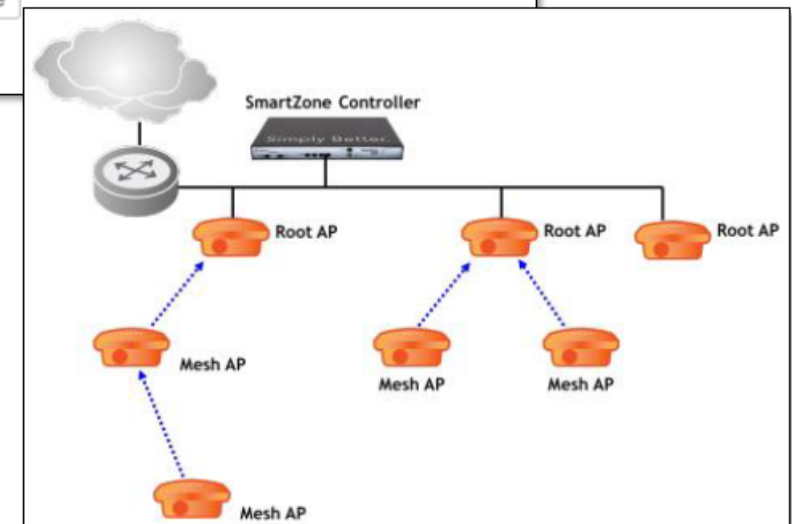
Zero Touch Mesh:  OFF

Mesh Name (ESSID):

Mesh Passphrase:

Mesh Radio Option:  2.4GHz  5GHz

- Mesh options
  - Zone ONLY
  - Document Mesh Name and Passphrase details for:
    - Troubleshooting
    - AP Recovery
  - Zero Touch for completely wireless setup



# Zone.

## Radio Options

- \* Channel Range (2.4G): 1 2 3 4 5 6 7 8 9 10 11
- \* Channel Range (5G)  
Indoor: 36 40 44 48 52 56 60 64 100 104 108  
112 116 120 124 128 132 136 149 153 157 161
- \* Channel Range (5G)  
Outdoor: 100 104 108 112 116 120 124 128 132 136 149  
153 157 161

### Radio Options (2.4 GHz)

- \* Channelization:  ▼
- \* Channel:  ▼
- Auto Cell Sizing:  OFF  Enable
- \* TX Power Adjustment:  ▼

### Radio Options a/n/ac (5 GHz)

- \* Channelization:  ▼
- \* Channel:  ▼
- \* Indoor:  ▼
- \* Outdoor:  ▼
- Auto Cell Sizing:  OFF  Enable
- \* TX Power Adjustment:  ▼

# Zone.

**Access Points > Group > Create New > Advanced Options > Auto Channel Selection**

## Advanced Options

Channel Mode:  OFF Allow indoor channels (allow ZoneFlex outdoor APs to use channels regulated as for indoor use only)

[?] Auto Channel Selection:  ON Automatically adjust 2.4 GHz channel using

ON Automatically adjust 5 GHz channel using

**Access Points > Group > Create New > Advanced Options > Background Scan**

[?] Background Scan:  ON Run background scan on 2.4 GHz radio every  seconds (1-65535) **3600**

ON Run background scan on 5 GHz radio every  seconds (1-65535) **3600**

# Zone.



AP Reboot Timeout: \* Reboot AP if it cannot reach default gateway after:

30 minutes ▼

\* Reboot AP if it cannot reach the controller after:

2 hours ▼

You can disable the reboot by setting the timer to 0 (Never Reboot). The range is from a minimum of 0 (Never Reboot) to a maximum of 24 hours. The timing should be set according to your redundancy strategy and your WLAN settings and requirements

# WLAN

Wireless LANs > Create WLAN Configuration

Dashboard

System

Access Points

Switches

**Wireless LANs**

Clients

### Wireless LANs

System > TeamXDomain > TeamXZone

+ Create

- D System
  - + D PartnerXDomain
  - D TeamXDomain
    - + Z TeamXZone

### Create WLAN Configuration

- General Options
- Authentication Options
- Encryption Options
- Data Plane Options
- Accounting Service
- Options
- RADIUS Options
- Advanced Options**

# WLAN.

Wireless LANs > Create WLAN Configuration > Authentication Options

**Authentication Options**

\* Authentication Type:  Standard usage (For most regular wireless networks)  Hotspot (WISPr)  Guest Access  Web Authentication

Hotspot 2.0 Access  Hotspot 2.0 Onboarding  WeChat

\* Method:  Open  802.1X EAP  MAC Address  802.1X & MAC

- Define the type of authentication flow for the WLAN

Authentication Type	Use
Standard	Regular WLAN
Hotspot (WISPr)	Hotspot
Guest Access + Hotspot 2.0 Onboarding	Guest access with Guest passes
Web Authentication	Web based logon
Hotspot 2.0 Access	Hotspot 2.0 Operator Profile
Hotspot 2.0 Secure Onboarding (OSEN)	Hotspot with Online Sign Up
WeChat	WeChat mobile app users

# WLAN.

## Encryption Options

\* Method:  WPA2  WPA3  WPA2/WPA3-Mixed  OWE  WPA-Mixed  WEP-64 (40 bits)  WEP-128 (104 bits)  None

\* Algorithm:  AES  AUTO  AES-GCMP-256

Passphrase:   OFF

802.11r Fast Roaming:  OFF

\* 802.11w MFP:  Disabled  Capable  Required

\* Dynamic PSK:  Disable  Internal  External

# WLAN.

Wireless LANs > Create WLAN Configuration > Options

Options

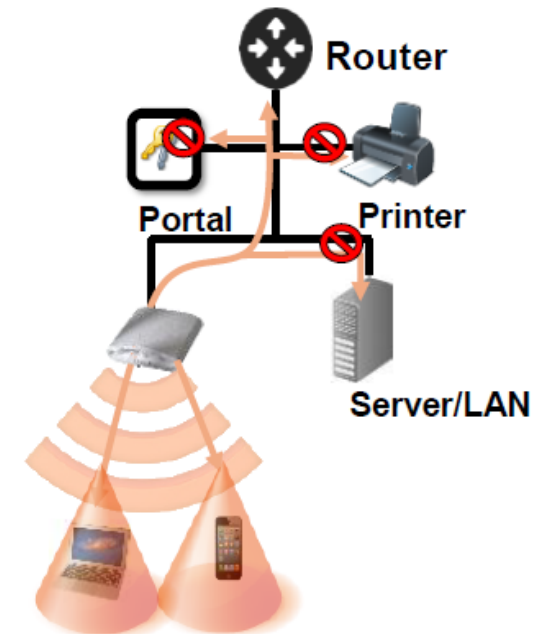
Wireless Client Isolation:  ON  Off Isolate wireless client traffic from all hosts on the same VLAN/subnet

Isolation Whitelist: Gateway Only (Automatic)

(The whitelist requires entries for the subnet gateway and other allowed hosts.)  
(The whitelist can only contain wired destinations; wireless clients are not supported on the whitelist.)

\* Priority:  High  Low

- Disable - devices are able to see all other devices on the subnet (default)
- Enable - devices are blocked from seeing other devices on the network
- Customized by User Traffic Profiles



# WLAN.

## Wireless LANs > Create WLAN Configuration > Advanced Options

Advanced Options

User Traffic Profile: System Default

L2 Access Control: Disable

OS Policy: Disable

Application Recognition & Control:  OFF

URL Filtering:  OFF

Wi-Fi Calling:  OFF

Client Fingerprinting:  ON

Access VLAN: VLAN ID

OFF Enable VLAN Pooling

Hide SSID:  OFF

Client Load Balancing:  Disable client load balancing for this WLAN service

Proxy ARP:  OFF

\* Max Clients: Allow up to  clients per AP radio to associate with this WLAN

802.11d:  ON

- Fine tune the WLAN including:
  - Device control
  - Load/band balancing
  - Data rates

# WLAN.

Wireless LANs > Create WLAN Configuration > Advanced Options

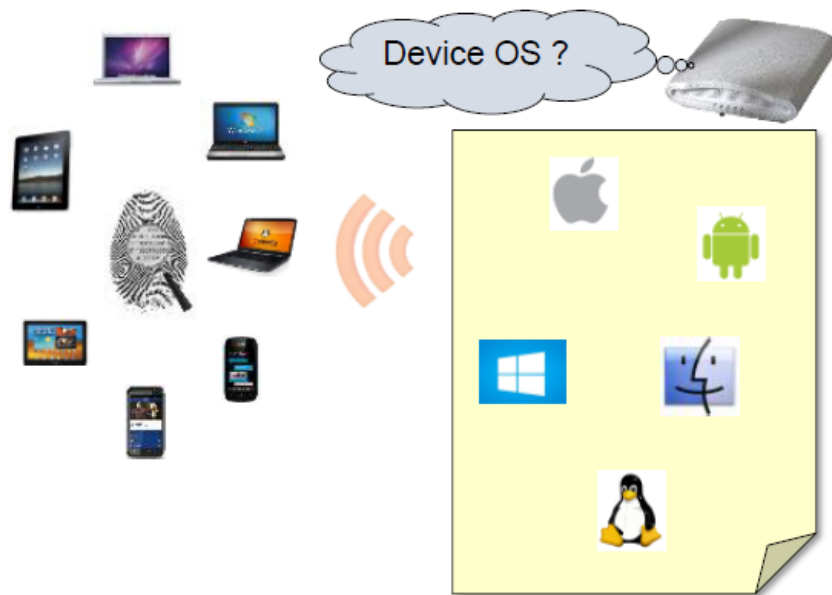


Application Recognition & Control:  OFF

- Allows the controller to identify the applications in use on the client devices

# WLAN.

Wireless LANs > Create WLAN Configuration > Advanced Options



Client Fingerprinting:  ON

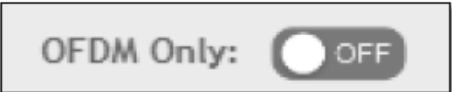
- Identifies device OS
- Enabled by default on a per WLAN basis

This feature is enabled on a per WLAN basis, and is enabled for all new WLANs by default.

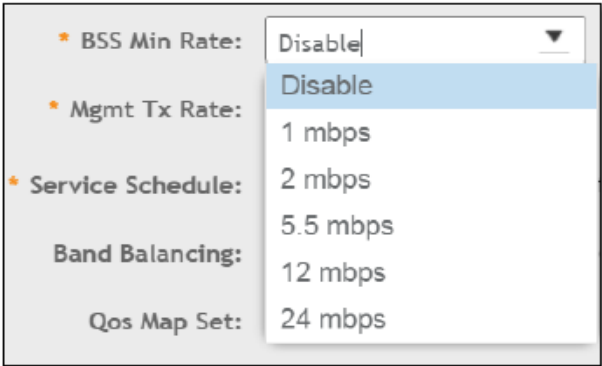
# WLAN.

Wireless LANs > Create WLAN Configuration > Advanced Options

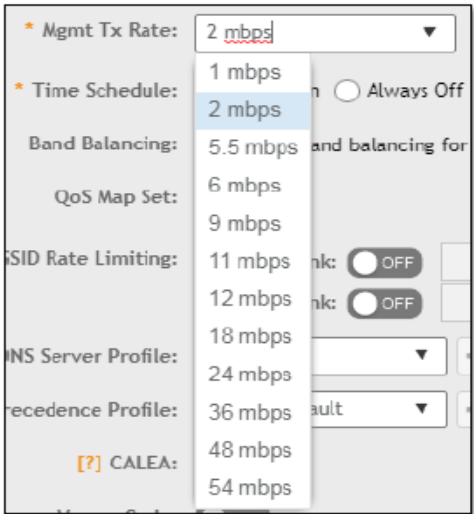
- Disables DSSS/HR-DSSS



- Minimum rate for data frames



- TX rate for management frames
- Disabled by OFDM Only



# WLAN.

Wireless LANs > Create WLAN Configuration > Advanced Options

- Enforces an aggregate rate limit for all users of the WLAN

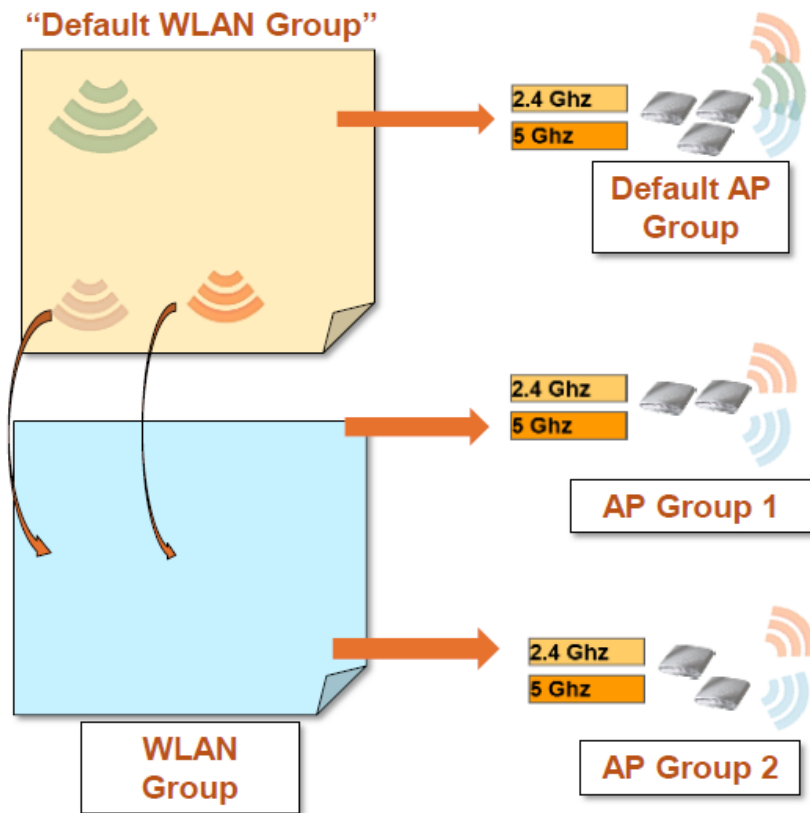
**[?] SSID Rate Limiting:**

Uplink:  OFF  mbps (1-200)

Downlink:  OFF  mbps (1-200)

Rate limiting in user traffic profile will not work if SSID rate limiting is enabled.

# Domain - Zone - Group.



- WLAN Groups

- Create the WLANs
- Create the WLAN Group
- Add the WLANs to the Group
- Associate the WLAN Group with the AP Group

A WLAN Group can include a maximum of 27 member WLANs

For dual radio APs, each radio can be assigned to only one WLAN Group

# Domain - Zone - Group.

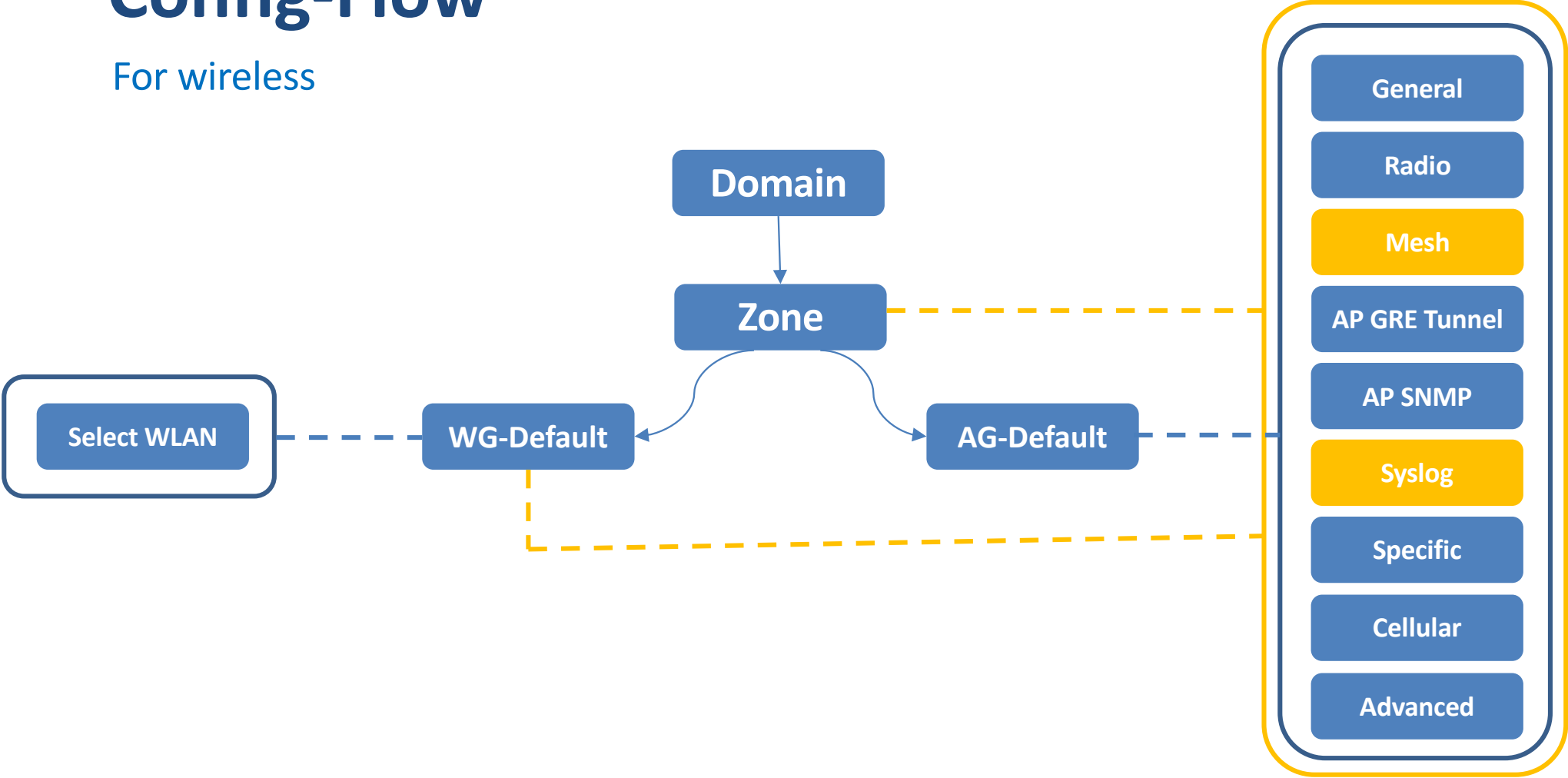
Access Points > Create Group > Configuration > Radio Options

- Create a new AP Group, or edit an existing AP Group to add the WLAN Group

The image shows two screenshots from a network management interface. The left screenshot, titled 'Access Points', shows a hierarchical tree structure under 'System > TeamXDomain > TeamXZ'. The tree includes 'System', 'PartnerXDomain', 'PartnerXZone', 'TeamXDomain', 'TeamXZone', and 'Staging Zone'. A blue box highlights a '+' icon in the top toolbar, and a blue arrow points from it to the right screenshot. The right screenshot, titled 'Configuration', shows the 'Radio Options' for a radio group. It has two sections: 'Radio b/g/n (2.4 GHz)' and 'Radio a/n/ac (5 GHz)'. In the 2.4 GHz section, the 'WLAN Group' is set to 'ON' and 'default', with a blue box around the 'WLAN Group' label and another blue box around the '+' icon in the dropdown menu. A dropdown menu is open, showing 'default' and 'TeamX WLAN Group', with 'TeamX WLAN Group' highlighted by a blue box. In the 5 GHz section, the 'WLAN Group' is set to 'OFF' and 'default', with a blue box around the 'WLAN Group' label.

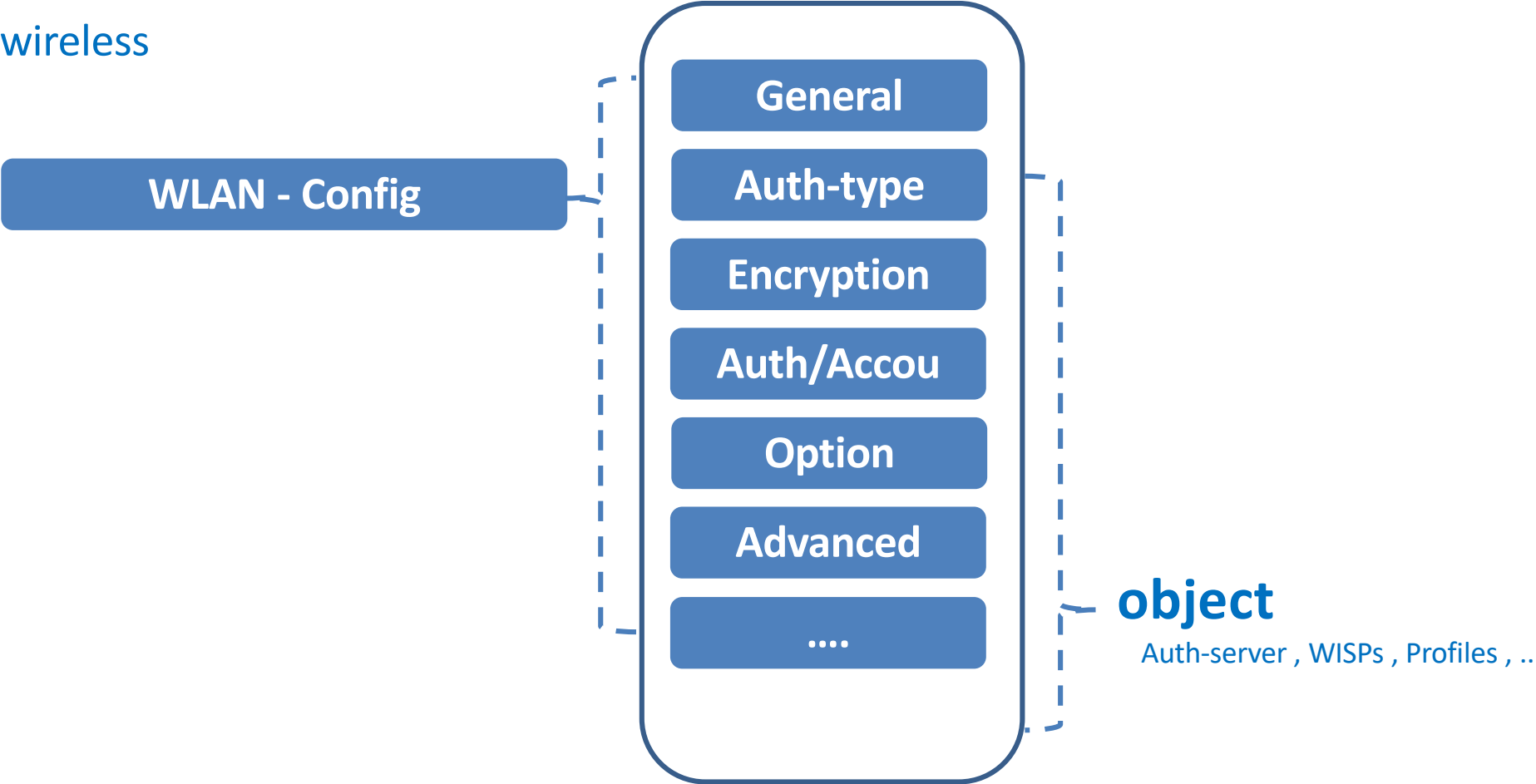
# Config-Flow

For wireless



# Config-Flow.

For wireless



# WLAN CONFIG



# WLAN-1\_PSK

建立 PSK 驗證方式的無線環境

General Options

\* Name:

\* SSID:

Description:

\* Zone:

\* WLAN Group:

# WLAN-1\_PSK.

## Authentication Options

1

- \* Authentication Type:  Standard usage (For most regular wireless networks)  Hotspot (WISPr)  Guest Access  Web Authentication  
 Hotspot 2.0 Access  Hotspot 2.0 Onboarding  WeChat
- \* Method:  Open  802.1X EAP  MAC Address  802.1X EAP & MAC

## Encryption Options

2

- \* Method:  WPA2  WPA3  WPA2/WPA3-Mixed  OWE  WPA-Mixed  WEP-64 (40 bits)  WEP-128 (104 bits)  None
- \* Algorithm:  AES  AUTO  AES-GCMP-256

3

Passphrase:   OFF Show

802.11r Fast Roaming:  OFF

\* 802.11w MFP:  Disabled  Capable  Required

\* Dynamic PSK:  Disable  Internal  External

# WLAN-1\_PSK.

Advanced Options

Wi-Fi Calling:  OFF

Client Fingerprinting:  ON

**4** [?] Access VLAN: VLAN ID

OFF Enable VLAN Pooling

If DHCP/NAT is enabled on an AP, the VLANs configured should be aligned with the VLANs in the DHCP Profile(s). Clients will have connectivity issues if the client resolves a VLAN other than those in the DHCP profile(s).

Hide SSID:  OFF

# WLAN-2\_802.1x

## 建立 802.1x 驗證方式的無線環境

Authentication Options

**1** \* Authentication Type:  Standard usage (For most regular wireless networks)  Hotspot (WISPr)  Guest Access  Web Authentication  
 Hotspot 2.0 Access  Hotspot 2.0 Onboarding  WeChat

**2** \* Method:  Open  802.1X EAP  MAC Address  802.1X EAP & MAC

Encryption Options

**3** \* Method:  WPA2  WPA3  WPA2/WPA3-Mixed  OWE  WPA-Mixed  WEP-64 (40 bits)  WEP-128 (104 bits)  None

\* Algorithm:  AES  AUTO  AES-GCMP-256

802.11r Fast Roaming:  OFF

\* 802.11w MFP:  Disabled  Capable  Required

# WLAN-2\_802.1x.

## Authentication & Accounting Service

\*  Authentication Service:  ON  OFF Use the controller as proxy

4

OFF RFC 5580 Location Delivery Support: Requires that Authentication Service be set to 'Use the controller as a proxy'

Accounting Service:  OFF  ON Use the controller as proxy

## Advanced Options

Wi-Fi Calling:  ON  OFF

Client Fingerprinting:  ON  OFF

5

 Access VLAN: VLAN ID

OFF  ON Enable VLAN Pooling

If DHCP/NAT is enabled on an AP, the VLANs configured should be aligned with the VLANs in the DHCP Profile(s). Clients will have connectivity issues if the client resolves a VLAN other than those in the DHCP profile(s).

# WLAN-2\_802.1x.

The interface shows a navigation menu on the left with 'Authentication' selected. The main content area has tabs for different authentication methods: 'Non-Proxy (AP Authenticator)', 'Proxy (SZ Authenticator)', 'Realm Based Proxy', 'EAP-SIM', and 'EAP-AKA'. The 'Proxy (SZ Authenticator)' tab is active. Below the tabs are action buttons: '+ Create', 'Configure', 'Clone', 'Test AAA', and 'Delete'. A tree view on the left shows a 'System' folder containing several domains: Demo-Partner-Domain, MeshLAB, Paultest, eva-cn, eva-us, and frog-test. A table on the right lists the configurations:

Name	Manage By	Friendly Name	Protocol	Descript
10.10.100.46	System	N/A	RADIUS	N/A
AAA-1-10.100.100.1	System	N/A	RADIUS	N/A
BoenNPS	System	N/A	RADIUS	N/A
FrogRadius	System	N/A	RADIUS	N/A
Guest	System	N/A	GUEST	N/A
Hfu_Rad2	System	N/A	RADIUS	N/A
Local Database	System	N/A	LOCAL_DB	N/A
Proxy-ntnupeap	System	N/A	RADIUS	N/A
proxyAD	System	N/A	AD	N/A

# WLAN-2\_802.1x.

## Edit Authentication Service FrogRadius

\* Name:

Friendly Name:

Description:

\* Service Protocol:  RADIUS  Active Directory  LDAP

### RADIUS Service Options

RFC 5580 Out of Band Location  
Delivery:  OFF  Enable for Ruckus AP Only

### Primary Server

\* IP Address:

\* Port:

\* Shared Secret:

\* Confirm Secret:

# WLAN-2\_802.1x.

## Edit Authentication Profile: FrogRadius

\* Name:

Description:

OFF Configure PLMN identifier

**Realm Based Authentication Service**

Realm	Protocol
No Match	RADIUS
Unspecified	RADIUS

### Edit Realm Based Authentication Service: No Match

\* Realm:

\* Service:

\* Auth Method:

Dynamic VLAN ID:

Note: If device onboarding was done with credential type 'remote', then map your 'realm' value to its respective authentication service PLUS define 'Unspecified' realm & map it to corresponding authentication service to properly handle legacy (non-Hotspot 2.0) devices.



# WLAN-3\_Guest

## Authentication Options

1

\* Authentication Type:  Standard usage (For most regular wireless networks)  Hotspot (WISPr)  Guest Access  Web Authentication  
 Hotspot 2.0 Access  Hotspot 2.0 Onboarding  WeChat

2

\* Method:  Open  802.1X EAP  MAC Address  802.1X EAP & MAC

## Encryption Options

3

\* Method:  WPA2  WPA3  WPA2/WPA3-Mixed  OWE  WPA-Mixed  WEP-64 (40 bits)  WEP-128 (104 bits)  None

## Encryption Options

3

\* Method:  WPA2  WPA3  WPA2/WPA3-Mixed  OWE  WPA-Mixed  WEP-64 (40 bits)  WEP-128 (104 bits)  None

\* Algorithm:  AES  AUTO  AES-GCMP-256

Passphrase:   ON  Show

802.11r Fast Roaming:  OFF

\* 802.11w MFP:  Disabled  Capable  Required

# WLAN-3\_Guest.

Guest Access Portal

**4** \* Guest Portal Service: FrogGAP-1

**5** Bypass CNA:  OFF

\* Guest Authentication: Guest

Guest Accounting:  OFF Use the controller as proxy  
Disable

# WLAN-3\_Guest.

## Edit Guest Access Portal: FrogGAP-1

### General Options

\* Portal Name:

Portal Description:

\* Language:

### Redirection

Start Page: After user is authenticated,

Redirect to the URL that user intends to visit.  Redirect to the following URL:

\*

# WLAN-4\_web

## 建立 web 802.1x 驗證方式的無線環境

Authentication Options

**1** Authentication Type:  Standard usage (For most regular wireless networks)  Hotspot (WISPr)  Guest Access  Web Authentication

Hotspot 2.0 Access  Hotspot 2.0 Onboarding  WeChat

**2** \* Method:  Open  802.1X EAP  MAC Address  802.1X EAP & MAC

Encryption Options

**3** \* Method:  WPA2  WPA3  WPA2/WPA3-Mixed  OWE  WPA-Mixed  WEP-64 (40 bits)  WEP-128 (104 bits)  None

# WLAN-4\_web.

**Hotspot Portal**

4 \* Hotspot (WISPr) Portal: HP-1

5 Bypass CNA: OFF

6 \* [?] Authentication Service: ON Use the controller as proxy ON Use Realm-based profile  
FrogRadius

Accounting Service: OFF Use the controller as proxy  
Disable

**Advanced Options**

Wi-Fi Calling: OFF

Client Fingerprinting: ON

7 [?] Access VLAN: VLAN ID 987  
OFF Enable VLAN Pooling

If DHCP/NAT is enabled on an AP, the VLANs configured should be aligned with the VLANs in the DHCP Profile(s). Clients will have connectivity issues if the client resolves a VLAN other than those in the DHCP

# WLAN-4\_web.

## Edit Hotspot Portal: HP-1

### General Options

\* Portal Name:

Portal Description:

### Redirection

Smart Client Support:  None  Enable  Only Smart Client Allowed

Logon URL:  Internal  External

\* Redirected MAC Format:

Start Page: After user is authenticated,  
 Redirect to the URL that user intends to visit.  Redirect to the following URL:

\*

HTTPS Redirect:  ON  OFF The AP will try to redirect HTTPS requests to the hotspot portal

# WLAN-4\_web.

### Portal Settings

Portal Language:

\* Portal Title:

[?] Portal Logo:

Portal Terms & Conditions:  OFF

Terms of Use

By accepting this agreement and accessing the wireless network, you acknowledge that you are of legal age, you have read and understood, and agree to be bound by this agreement.

### User Session

\* Session Timeout:  Minutes (2-14400)

\* Grace Period:  Minutes (1-14399)

Use of .PNG file format is highly recommended for the logo. The maximum file size is 250 KB, and logo's width \* height must not exceed 526 \* 200 pixels.

# Others

- L2/L3 filter >>> Firewall profile

- Service & Profile

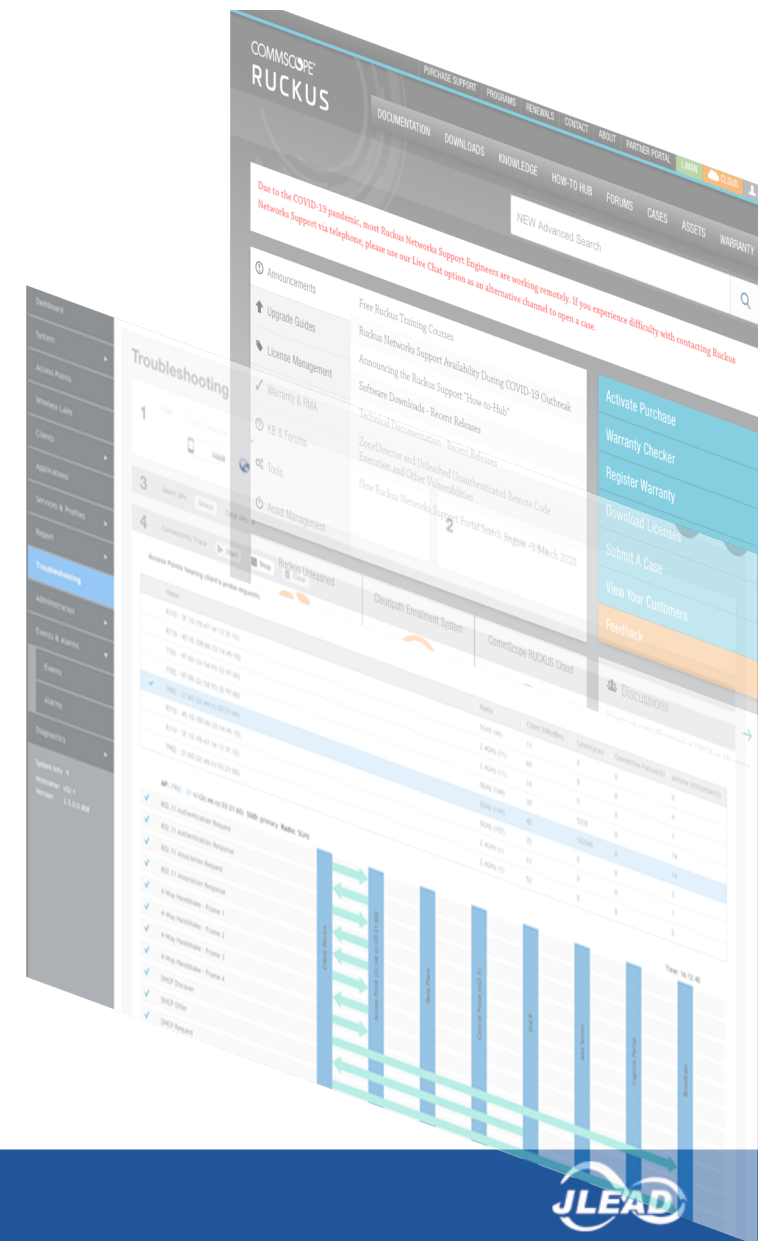
- Authentication
- Hotspots&Portals

- Management

- Cluster
- Troubleshooting
- Event & Alarm

- License & Service

- Smart License , LiMAN



# Other.

Source	Port	Destination	Plane	Purpose
Controller	21 TCP	FTP	Control	FTP upload of reports, stats and config backups
AP	22 TCP	Controller	Control	SSH Tunnel
AP	91,11443 TCP	Controller	Control	Access Point firmware upgrade
AP	443 TCP	Controller	Control	Registration Request
SWIPE App	7443 TCP	Controller	Management	SWIPE App communication
Any	8443 TCP	Controller	Management	Access to web interface via HTTPS
AP	23232 TCP	Controller	Data	GRE Tunnel
AP	23233 TCP	Controller	Data	GRE Tunnel (GRE over UDP)
AP	12222,12223 UDP	Controller	Control	LWAPP Discovery
Controller/AP	1812,1813	AAA	Management	AAA Authentication and Accounting



- JLEAD\_AC-Demo\_21
- JLEAD\_AC-Demo\_22
- JLEAD\_AC-Demo\_443
- JLEAD\_AC-Demo\_8443



**Thank  
You!**