USER MANUAL

WS5/7/10G2

Wireless LAN Controller

Revision: 3.2.1

TABLE OF CONTENTS

Chapter 1. INTRODUCTION

Hyperion is a Wireless LAN Controller (WLC) product series which includes three models of WS5G2, WS7G2 and WS10G2, particularly suitable for the SMB and IoT applications. This series of products is designed based on Intel Atom platform, providing 1G and 10G Ethernet ports in the form of RJ45 and SFP+ to meet with the requirements in every kind of applications. The Hyperion series WLC mainly faces the small scale Wi-Fi network where the deployed access points are not exceeding 1000. In this scenario, the wireless clients could be regular user endpoints and also the IoT sensors, such as mobile phone, notebook computer, IP-CAM, and industrial sensors and controllers. In the era of industry 4.0, the artificial intelligence and internet of everything depending on wireless network communication will grow up explosively, so that the Wi-Fi coverage infrastructure and even the long range Wi-Fi bridge could be possibly expanding in a large scale. This means that the Hyperion series WLC will have much more application opportunities in the new era.

WLC is such a product which helps customer to centralized manage and provision wireless access points in a way of migrating the management function originally resided in each access point to WLC while the AP only remains its fundamental wireless access and security capabilities. Hence, the WLC focuses on AP's configuration, user authentication, traffic forwarding, radio resource management, access control, QoS and load balancing; while the thin AP focuses on the underlying functions defined by IEEE802.11 specifications. For a complicated Wi-Fi system, this architecture is an ideal model that is controllable and manageable. In the Wi-Fi system with WLC, thin AP has zero configurations initially; it is configured by downloading profiles from WLC. Thin AP and WLC are connected through CAPWAP tunnel which is established by thin AP during its DHCP discovery process with option43 response.

In SMB and IoT applications, the capacity of the access point is usually less than 1000, and the total traffic throughput is less than 20Gbps. Therefore, a small-sized WLC is required as the centralized controller. Hyperion series WLC based on Intel Atom platform (such as WS5G2, WS7G2 and WS10G2) was born for these deployments.

1.1. MANUAL STATEMENT

1.1.1. SYNTAX DECLARATION

Syntax conventions in the command line:

Format	Meaning
Bold	Command names are represented by **bold** characters.
Italics	Command arguments (the values following the command name) are represented by *italic* characters.
[ ]	Represents the optional parts in the command line.
//	Represents comments without action.
|	Represent the OR logic for multiple parameter options.

1.1.2. Graphical UI Declaration

Buttons and interfaces involved in the web page configuration are as follows.

Format	Meaning
/	The multiple level menu delimiter.

1.1.3. Sign Declaration

This manual uses a variety of eye-catching signs to emphasize the importance in the configuration process.

⚠ **Warning:** Careful attention must be paid to the warning message next to this sign. Not heeding to this advice could lead to improper operation and may cause injury.

📝 **Note:** Attention can be paid to the message next to this sign. The information included is usually important, very helpful, or a quick summary.

1.1.4. Glossary

Term	Meaning
STA (Station or Terminal)	WLAN (Wireless LAN) stations such as the handsets, PCs, notebooks, or other CPE equipment are referred to as STAs.
UE (User Endpoint)	Small mobile devices such as the handsets, PCs, notebooks, or other CPE equipment with Wi-Fi capabilities are referred to as UEs.
AP (Access Point)	Base station equipment for STAs, to access the wired network, or other STAs from the wireless network are referred to as APs.
TAP (Thin Access Point)	The Access Point managed by the WLC.
WLC (Wireless LAN Controller)	Edge gateway equipment between Wi-Fi APs and the core network are referred to as WLCs. The WLC is used for access control, security, management, centralized data forwarding, and switching.
SSID (Service Set Identifier)	The SSID is used to identify a group of STAs and its associated AP. Only those STAs and their AP, in the same SSID, can communicate with each other, something like the concept of VLANs (Virtual LANs) in wired networks.
Captive Portal	A server that pushes a web page to user endpoint for entering the user name and password for authentication.
Radius	A server that authenticates the user legitimacy with secure methods.
OTP	One time password which is delivered in short message service for user authentication.
LDAP	A server that uses the Light Directory Access Protocol for user authentication.
SMS	Short message service provided by mobile communication operator.

Chapter 2. Hardware Components

2.1. Package Contents

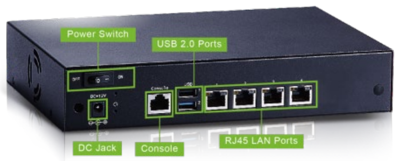
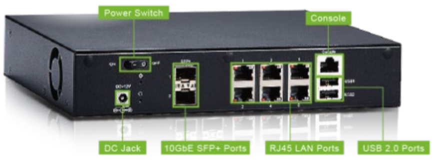
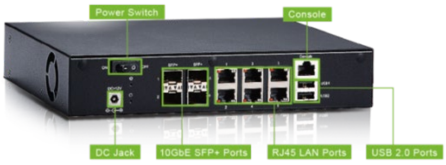
Carefully remove all the items from the packing of Hyperion series WLC. The following items should be included in the packaging:

Package Content	WS5G2	WS7G2	WS10G2
Power Adapter (DC)	1	1	1
Power Cord (AC)	1	1	1
Mounting Screws (For Disk Drive)	Yes	Yes	Yes
SATA Cables (Data Cable & Power Cable)	Yes	Yes	Yes
Plastic Stand (For Stack-up)	Yes	Yes	Yes
10G SPF+ Optical Transceiver Module	-	-	-
LC-LC Multi-Mode Optical Fiber	-	-	-

Note: If any of the items, mentioned above, is not included in the packaging or are damaged in any way, contact your reseller immediately.

2.2. Physical Ports

The following physical ports and LED indicators are available on the WS5/7/10G2.

Front Panels		
WS5G2	WS7G2	WS10G2
Rear Panels		
WS5G2	WS7G2	WS10G2
 Power Switch USB 2.0 Ports DC Jack Console RJ45 LAN Ports	 Power Switch Console DC Jack 10GbE SFP+ Ports RJ45 LAN Ports USB 2.0 Ports	 Power Switch Console DC Jack 10GbE SFP+ Ports RJ45 LAN Ports USB 2.0 Ports

The following table describes the hardware components available on the rear panel of the WLC.

	WS5G2	WS7G2	WS10G2
Power Switch	1	1	1
DC Power Port	1	1	1

	WS5G2	WS7G2	WS10G2
Reset Switch	1	1	1
Default Switch	1	1	1
SFP+ Ports (10 Gbps)	-	2	4
RJ45 LAN Ports (1 Gbps)	4	6	6
Console Port (RJ45)	1	1	1
USB 2.0 Ports	2	2	2

Hardware Component	Description
Power	WS5/7G2: One 12V/5A DC adapter WS10G2: One 12V/7A DC adapter
Reset Switch	One
Default Switch	One
SFP+ Ports	The default IP address of the WLC through the VIF SFP+ ports is ***192.168.3.228***. **Note:** All 10G SFP+ Ports in WLC support mono mode optic fiber.
RJ45 Ports	• The management port must be the first RJ45 1GbE port. The default IP address of the WLC through the ***Mgmt*** port is ***192.168.2.228***. • The WLAN port is for thin AP accessing and wireless clients' data tunnel, which could be a RJ45 port other than the Management Port.
Console Port	The Console Port is for debug or troubleshooting by IT staff.
USB 2.0 Ports	Two USB 2.0 ports, which are reserved for further applications.

2.3. LED Indicators

The following table describes the LED indicators available on the front panel of the WS5/7/10G2.

LED Indicator	Color	Behavior	Description
Power	Green	Solid On	The system is powered on.
		Off	The system is powered off.
HDD	Green	Blinking	Data transfer activity is taking place.
		Off	No data transfer activity is taking place.
SFP+ LEDs	Orange	Solid On (Right)	Connection active at 1 Gbps
		Blinking (Left)	Sending and receiving data
		Off	No connection active or port is disabled.
RJ45 LAN LEDs	Green	Solid On (Right)	Connection active at 10/100 Mbps
	Orange	Blinking (Left)	Sending and receiving data
		Off	No connection active or port is disabled.

Chapter 3. SYSTEM FOUNDATION

3.1. SYSTEM ARCHITECTURE

The Wi-Fi system architecture using Hyperion series WLC and Thin APs is illustrated below.

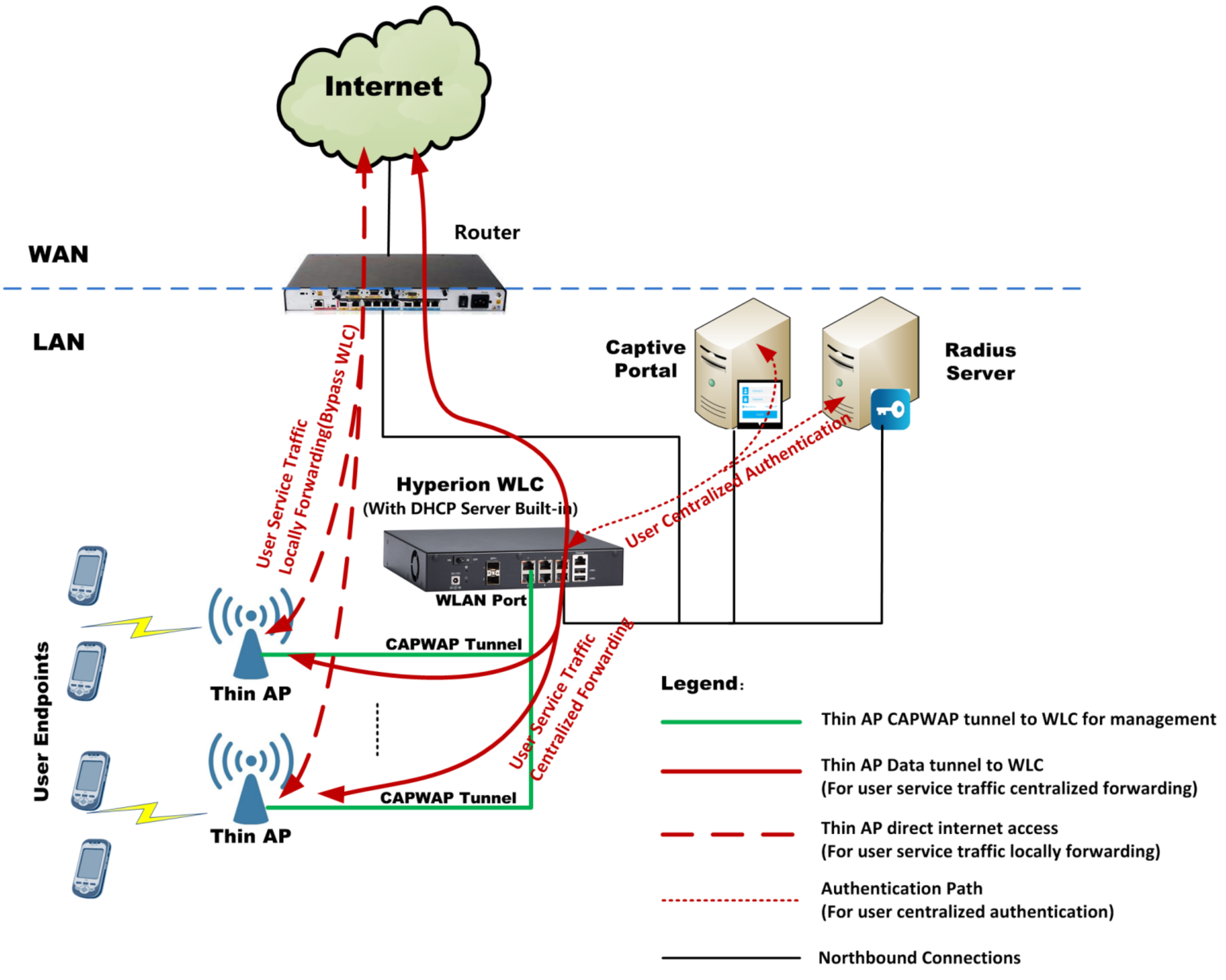

Internet
Router
WAN
LAN
Captive Portal
Radius Server
User Service Traffic Locally Forwarding(Bypass WLC)
Hyperion WLC (With DHCP Server Built-in)
User Centralized Authentication
WLAN Port
CAPWAP Tunnel
User Service Traffic Centralized Forwarding
Thin AP
CAPWAP Tunnel
Thin AP
User Endpoints
Legend:
Thin AP CAPWAP tunnel to WLC for management
Thin AP Data tunnel to WLC (For user service traffic centralized forwarding)
Thin AP direct internet access (For user service traffic locally forwarding)
Authentication Path (For user centralized authentication)
Northbound Connections

Figure 3-1 Wi-Fi System Architecture using WLC

The WLC has a southbound interface named the WLAN port. This port is the accessing port for all Thin APs connecting to WLC; while the northbound ports based on WLC internal VLAN Interfaces (VIF) connect to the Portal / Radius for user authentication and Internet for user services.

Two types of tunnel are established from Thin AP to WLC and will take charge of all communications:

- The CAPWAP tunnel, an access stratum management tunnel, focuses on provisioning AP and all statistics reports.
- The WLTP data tunnel focuses on UE (User Endpoint) non-access stratum data transmission, including service traffic and authentication messages.

Both tunnels start at the thin AP.

The Thin AP has zero configurations in its initial state. During its power-on stage, it firstly discovers the WLC by DHCP protocol and obtains up to 4 WLC IP addresses settled in DHCP Option 43, and then uses the first WLC IP address to establish the primary CAPWAP tunnel, and the others as the redundant WLC purpose. Then, thin AP downloads the profiles from the WLC through the CAPWAP tunnel to complete its configuration; while user clients associate to thin AP and start authentication and data services through WLTP tunnel.

The 1'st internet service initiated by user client through WLTP data tunnel will be intercepted by WLC to check whether it is an legal user, if not, this accessing will be redirected to the Captive Portal where the user name and password input and then authenticated by Radius server.

3.2. Connection and Configuration

There are two configuration modes for WLC management: one is the ***CLI*** (Command Line Interface) mode which is entered by SSH, Telnet and RS232 serial console accessing; another is the ***web*** mode which is entered by using browser to access the management web page for provisioning.

The Web provisioning mode (HTTP/HTTPS) is a user-friendly management method and can be accessed by using any standard Web browsing software, like Internet Explorer or Chrome. The Web interface simplifies system management and configuration, even if the administrator is a junior engineer. The CLI mode, however, is for the advanced customer and can be entered by SSH, Telnet, and the RS-232 console accessing. More knowledge about network communication protocols and command instructions are required to effectively configure and manage the WLC through the CLI mode.

The following section will briefly explain how to connect WLC for its configuration and management:

- **Ethernet Connection：** Configuration host connects to the WLC ***Mgmt*** port over Ethernet cable.
- **RS232 Serial Connection：** Configuration host connects to the WLC ***console port*** over RJ45-RS232 serial cable. The console port serial baud rate is **38400**.

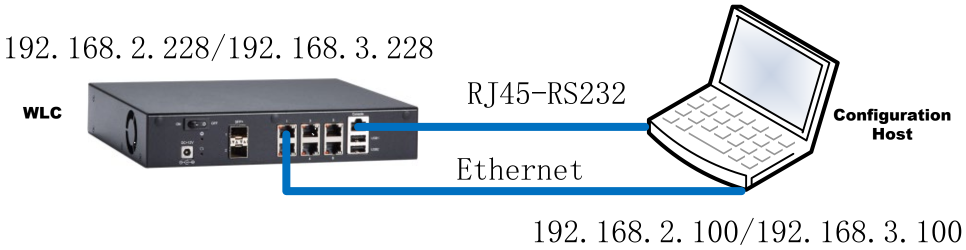


Figure 3-2 Configuration host Connects to the WLC for Management

The following default IP addresses are preset in the WLC:

- The default management IP address of the WLC through the ***Mgmt*** port is ***192.168.2.228***. The host PC or notebook must be assigned with an IP address in the same subnet, for example, ***192.168.2.100***.
- The default service IP address of the WLC through the VIF port is ***192.168.3.228***. The host PC or notebook must be assigned with an IP address in the same subnet, for example, ***192.168.3.100***.

Software tools which support SSH, Telnet and Serial communications, such as **SecureCRT**, **XShell**, or **PuTTY,** can be used to configure and manage WLC in CLI mode.

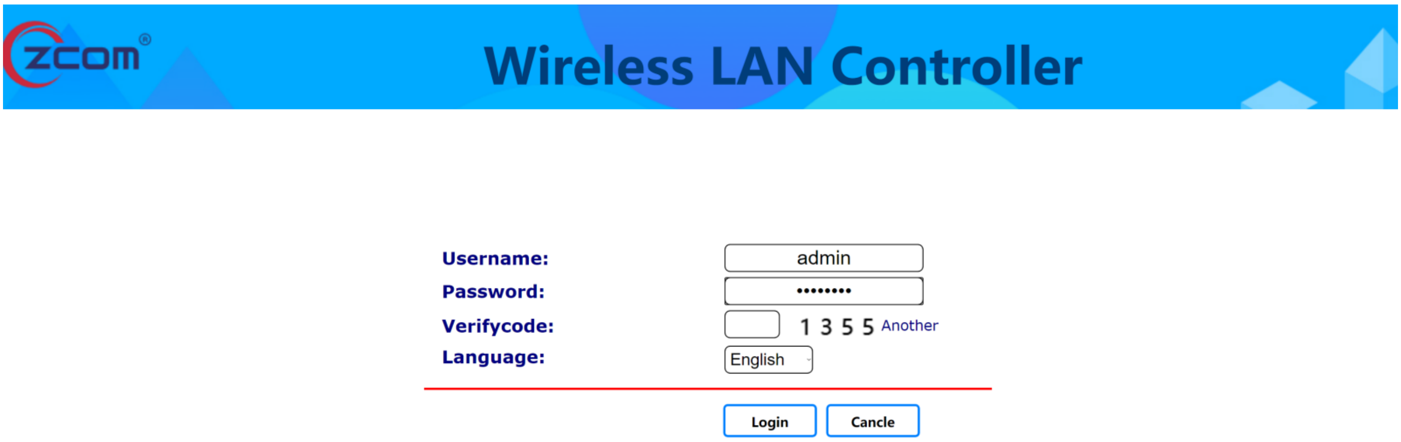
The default login credentials for WLC management is as the following:

- **Username:** *admin*
- **Password:** *password*

3.3. Entrance of Web Mode Provision

Compared with the CLI mode configuration, the WLC provides a more user-friendly management interface called the Web mode provisioning that can be accessed by any standard Web browser software like Internet Explorer or Chrome using the HTTP/HTTPS protocol.

To access the Web provisioning, entering the default IP address (**192.168.2.228** accessing in the management port or **192.168.3.228** accessing in the WLAN port) in the address bar of the web browser and press the **Enter** key to get into the login page, as shown below.



Username: admin

Password: ••••••••

Verifycode: 1 3 5 5 Another

Language: English

Figure 3-3 Web Interface (Login Page)

Enter the **Username, Password** and verification code, select the appropriate language in the pull-down menu, and click the **Login** button to enter the Web provisioning page of the WLC.

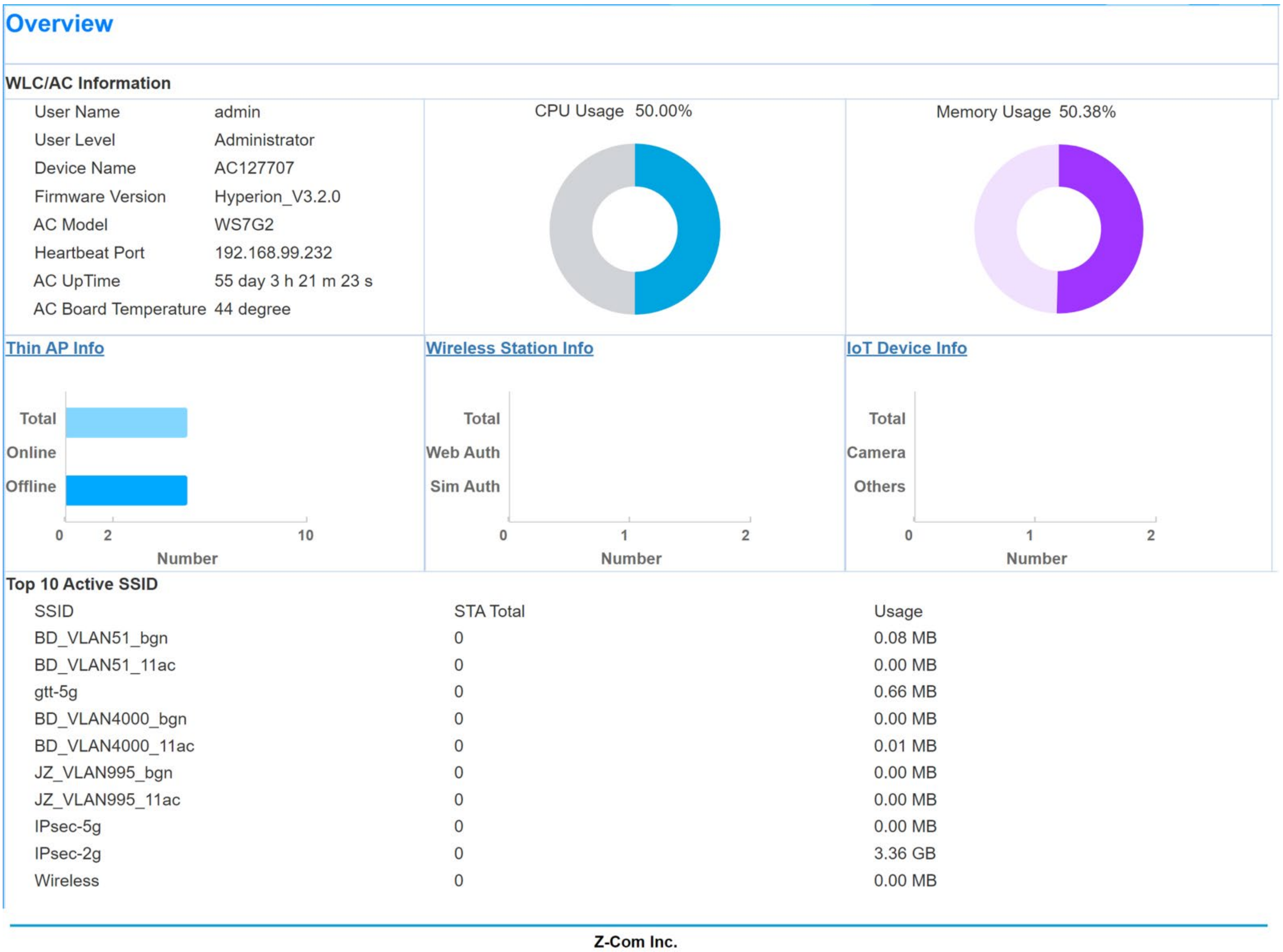
Note: The default Username is ***admin*** and Password is ***password***.

3.4. System Basic

The **[system basic]** menu provides two functions of ‘**System Information Overview**’ and ‘**System Quick Setting**’.

3.4.1. Information Overview

The **[system Information]** menu provides a information summary page, shown as below. It is displayed immediately after a successful login.



Overview

WLC/AC Information

User Name	admin
User Level	Administrator
Device Name	AC127707
Firmware Version	Hyperion_V3.2.0
AC Model	WS7G2
Heartbeat Port	192.168.99.232
AC UpTime	55 day 3 h 21 m 23 s
AC Board Temperature	44 degree

Top 10 Active SSID

SSID	STA Total	Usage
BD_VLAN51_bgn	0	0.08 MB
BD_VLAN51_11ac	0	0.00 MB
gtt-5g	0	0.66 MB
BD_VLAN4000_bgn	0	0.00 MB
BD_VLAN4000_11ac	0	0.01 MB
JZ_VLAN995_bgn	0	0.00 MB
JZ_VLAN995_11ac	0	0.00 MB
IPsec-5g	0	0.00 MB
IPsec-2g	0	3.36 GB
Wireless	0	0.00 MB

Z-Com Inc.

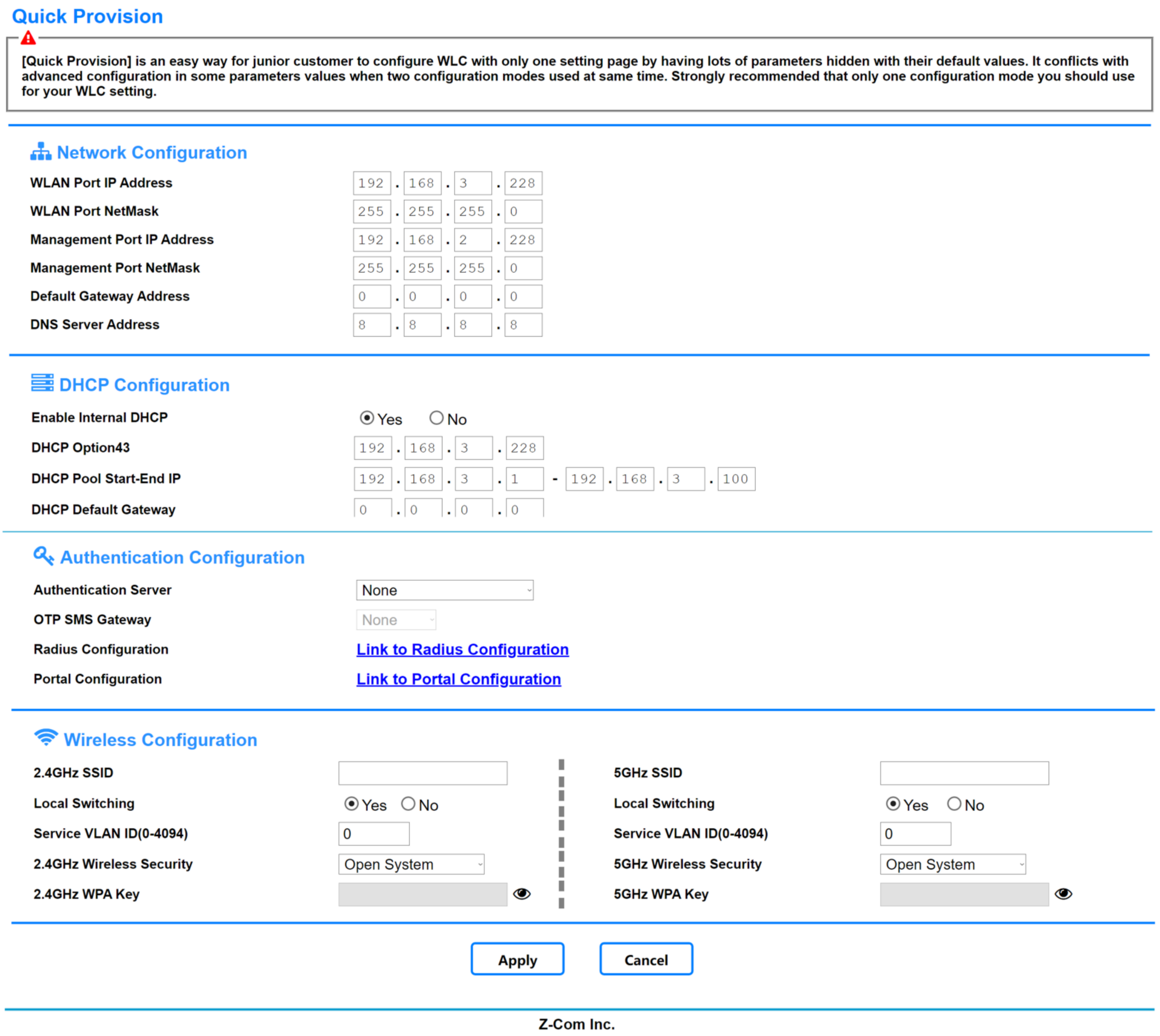
Figure 3-4 System Information Overview Page

In this system information overview page, it provides the hardware information and firmware information of WLC, and also reports the statistics information of Thin APs and user endpoints through charts and graphics.

3.4.2. Quick Setting

The **[Quick Setting]** is a shortcut way for junior customer to provision WLC in a simple mode with few parameters configuration. It can help customers use WLC to build their Wi-Fi system in a short time.

Select **[System Basic** > **Quick Setting]** in the menu to enter the configuration page. In **[Quick Setting]** page, those basic parameters including wireless, network and authentication are uniformly configured, they are sufficient for WLC to operate in a simple mode.



Quick Provision

[Quick Provision] is an easy way for junior customer to configure WLC with only one setting page by having lots of parameters hidden with their default values. It conflicts with advanced configuration in some parameters values when two configuration modes used at same time. Strongly recommended that only one configuration mode you should use for your WLC setting.

Network Configuration

WLAN Port IP Address	192 . 168 . 3 . 228
WLAN Port NetMask	255 . 255 . 255 . 0
Management Port IP Address	192 . 168 . 2 . 228
Management Port NetMask	255 . 255 . 255 . 0
Default Gateway Address	0 . 0 . 0 . 0
DNS Server Address	8 . 8 . 8 . 8

DHCP Configuration

Enable Internal DHCP	● Yes ○ No
DHCP Option43	192 . 168 . 3 . 228
DHCP Pool Start-End IP	192 . 168 . 3 . 1 - 192 . 168 . 3 . 100
DHCP Default Gateway	0 . 0 . 0 . 0

Authentication Configuration

Authentication Server	None
OTP SMS Gateway	None
Radius Configuration	Link to Radius Configuration
Portal Configuration	Link to Portal Configuration

Wireless Configuration

2.4GHz SSID		5GHz SSID	
Local Switching	● Yes ○ No	Local Switching	● Yes ○ No
Service VLAN ID(0-4094)	0	Service VLAN ID(0-4094)	0
2.4GHz Wireless Security	Open System	5GHz Wireless Security	Open System
2.4GHz WPA Key		5GHz WPA Key	

Figure 3-5 Quick Setting for WLC

These parameters in **[Quick Setting]** page are described in details as following:

Parameter	Description
Network Configuration	▪ **WLAN Port IP Address:** WLAN port is the southbound port for WLC to connect Thin APs. Thin AP establishes CAPWAP management tunnel to this WLAN port. This IP address is actually the CAPWAP tunnel termination IP. Default value is ***192.168.3.228***. ▪ **WLAN Port Netmask:** The netmask is used to divide which subnet the WLAN port is belonged to. ▪ **Management Port IP Address:** The management port is 1’st 1GbE port in

Parameter	Description
	WLC. It is used for customer to configure or maintain the WLC. However, in practical applications, it is also used as the heartbeat port for 1+1 backup. Default value is ***192.168.2.228***. ▪ **Management Port Netmask:** The netmask is used to divide which subnet the management port is belonged to. ▪ **Default Gateway IP Address:** The default gateway is used to process data packets whose destination IP address is not in the same subnet as the current network. If it is necessary to route data packets to another subnet or the Internet, you must specify it. ▪ **DNS Server IP Address:** The DNS server is used to convert domain names into IP addresses during Internet access. Entering the available DNS IP address here.
DHCP Configuration	▪ **Enable Internal DHCP:** WLC has the DHCP server built in. In practical applications, DHCP server could be either provided externally or internally. If no external DHCP server provided, customer can use WLC built-in DHCP server here by enabling it. ▪ **DHCP Option43:** This is an option for DHCP protocol. Option 43 of DHCP is used to deliver the WLC IP address to tell thin AP where to establish the CAPWAP management tunnel. ▪ **DHCP Pool Start-End IP Addresses:** The built-in DHCP server of WLC uses this IP address pool to allocate IP addresses to thin APs and user clients. The start IP and end IP limit the range of available IP addresses. ▪ **DHCP Default Gateway IP Address:** This default gateway IP address can be allocated to thin APs or user clients through the built-in DHCP server.
Authentication Configuration	▪ **Authentication Server:** Select whether using the WLC built-in Portal / Radius server or external Portal / Radius server for authentication purpose: ○ **Internal Portal&Radius:** WLC built-in Portal / Radius server as the authentication server. ○ **External Portal&Radius:** External 3'rd party Portal / Radius server as the authentication server. ▪ **OTP SMS Gateway:** OTP stands for '**O**ne **T**ime **P**assword'. The password generated by WLC will be delivered in the short message for user to input it in the Captive Portal page for authentication. Therefore, the SMS gateway providing OTP service must be designated. Here now have two options of **'aliyun'** and **'every8D'** for customer to select. **Note:** Before this configuration, customer must have registered as the legal subscriber of SMS gateway and have the user name and password officially released. ▪ **Radius Configuration:** This is a hyperlink to Radius Server configuration page. Customer can get there to have related parameters set. ▪ **Portal Configuration:** This is a hyperlink to Portal Server configuration page. Customer can get there to have related parameters set.

Parameter	Description	
Wireless Configuration	In the thin AP of 802.11ac, there are two radio modules in 2.4GHz band and 5GHz band so that they should be configured respectively.	
	2.4GHz Module	▪ **2.4GHz SSID:** Allocate a SSID for 2.4GHz radio module in thin AP to identify its service for wireless clients operating in 2.4GHz band to discover. ▪ **Local Switching:** This tells the 2.4GHz module in thin AP whether the user service traffic from user clients is local directly forwarding to internet or centralized to WLC for forwarding: ○ **Yes:** 2.4GHz module in thin AP Locally forwarding. ○ **No:** WLC centralized forwarding. ▪ **Service VLAN ID:** Due to thin AP has the access stratum tunnel CAPWAP for AP management, and the non-access stratum tunnel WLTP for user service traffic and authentication, therefore, it is necessary to distinguish them by VLAN. Here to assign the service VLAN ID to user traffic path for 2.4GHz module in thin AP. ▪ **2.4GHz Security:** There are three types of wireless security provided for 2.4GHz radio module to select: ○ **Open System:** When the wireless client associates with the 2.4GHz radio module, only SSID are required for authentication and the authentication does not require encryption. ○ **WPA2-PSK:** When wireless client associates with the 2.4GHz radio module in thin AP, it must be authenticated by WPA2 with the preset PSK key encryption. ○ **WPA2&Radius:** When wireless client associates with the 2.4GHz radio module in thin AP, it must be authenticated by WPA2, and the encryption key for authentication is issued by Radius server temporarily rather than the preset like the WPA2-PSK. ▪ **2.4GHz WPA Key:** If WPA2-PSK security selected for 2.4GHz radio module, the preset PSK key must be entered here in the form of character string.
	5GHz Module	▪ **5GHz SSID:** Allocate a SSID for 5GHz radio module in thin AP to identify its service for wireless clients operating in 5GHz band to discover. ▪ **Local Switching:** This tells the 5GHz module in thin AP whether the user service traffic from user clients is local directly forwarding to internet or centralized to WLC for forwarding: ○ **Yes:** 5GHz module in thin AP Locally forwarding.

Parameter	Description	
		○ **No:** WLC centralized forwarding. ▪ **Service VLAN ID:** Due to thin AP has the access stratum tunnel CAPWAP for AP management, and the non-access stratum tunnel WLTP for user service traffic and authentication, therefore, it is necessary to distinguish them by VLAN. Here to assign the service VLAN ID to user traffic path for 5GHz module in thin AP.. ▪ **5GHz Security:** There are three types of wireless security provided for 5GHz radio module to select: ○ **Open System:** When the wireless client associates with the 5GHz radio module, only SSID are required for authentication and the authentication does not require encryption. ○ **WPA2-PSK:** When wireless client associates with the 5GHz radio module in thin AP, it must be authenticated by WPA2 with the preset PSK key encryption. ○ **WPA2&Radius:** When wireless client associates with the 5GHz radio module in thin AP, it must be authenticated by WPA2, and the encryption key for authentication is issued by Radius server temporarily rather than the preset like the WPA2-PSK. . ▪ **5GHz WPA Key:** If WPA2-PSK security selected for 5GHz radio module, the preset PSK key must be entered here in the form of character string.

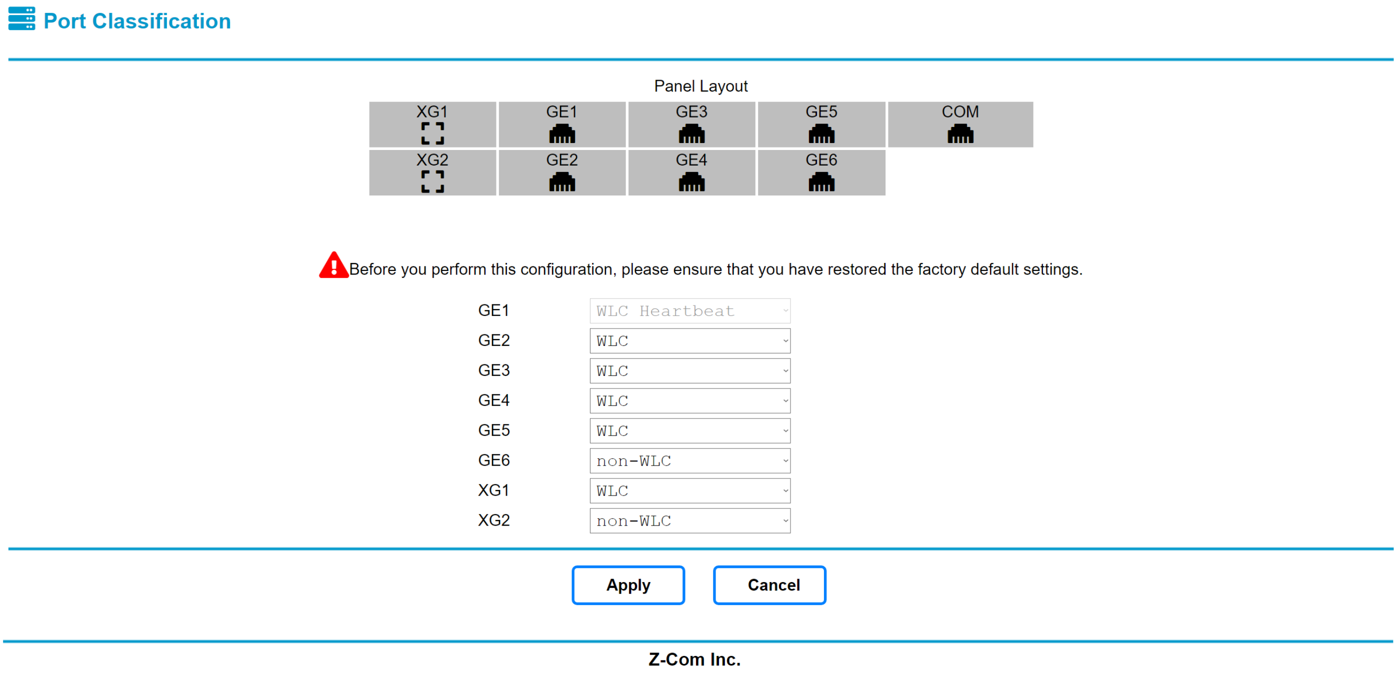
⚠ **Warning:** [Quick Setting] is a one page mode for junior customer to configure WLC in an easy way by having numbers of parameters hidden in their default values; however, it is possible to conflict with their values configured in advanced setting mode. Strongly recommended that only one configuration mode for customer to use for WLC setting.

Chapter 4. Network Configuration

4.1. Port Classification

Hyperion series WLC includes WS5G2, WS7G2 and WS10G2 three models, and their panels have multiple 1G and 10G physical Ethernet ports. Before using, it is necessary to specify which ports the WLC uses and which ports the other applications use. The specifying port usage is called as Port Classification.

Select **[Network** > **Port Classification]** in the menu to enter the configuration page as following (here is the Port Layout of WS7G2 as the example):



⚠Before you perform this configuration, please ensure that you have restored the factory default settings.

GE1	WLC Heartbeat
GE2	WLC
GE3	WLC
GE4	WLC
GE5	WLC
GE6	non-WLC
XG1	WLC
XG2	non-WLC

Z-Com Inc.

Figure 4-1 WLC Port Classification

These parameters in **[Network** > **Port Classification]** page is described in details as following:

Parameter	Description
GE1	This is the default management port for WLC, also used as the heartbeat port for 1+1 backup.
GE2~6	There are five 1000Base-T ports in the form of RJ45. They can be classified into two types according to the usage: ▪ **WLC:** This port is specially allocated to WLC as the CAPWAP tunnel for thin AP management and the central switching for user data traffic. ▪ **Non-WLC:** This port is allocated to Linux OS or other applications running in this platform.
XG1~2	There are two 10GBase-T ports in the form of SFP+. They can be classified into two types according to the application: ▪ **WLC:** This port is specially allocated to WLC as the CAPWAP tunnel for thin

Parameter	Description
	AP management and the central switching for user data traffic. ▪ **Non-WLC:** This port is allocated to Linux OS or other applications running in this platform.

Click the **Apply** button to accept the changes.

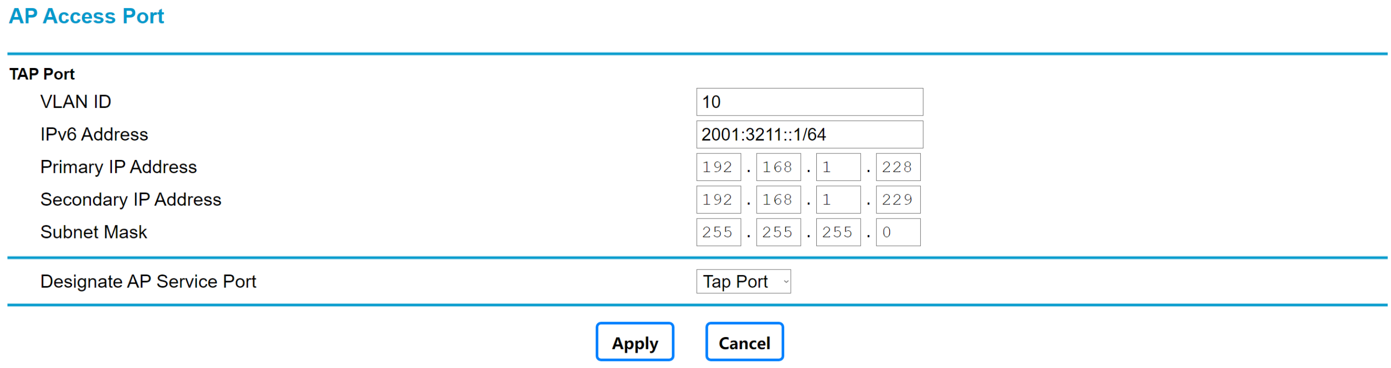
Note: Usually one or two ports being allocated to WLC usage are sufficient for most of Wi-Fi system networking requirements!

Note: If the Port Classification is changed, it must reboot WLC to make it being effective!

4.2. AP Access Port

The port in WLC used to connect the thin AP is the 'AP Access Port', and it is also called as WLAN port. This port is the WLC southbound interface for establishing the CAPWAP tunnel with thin AP.

Select **[Network** > **AP Access Port]** in the menu to enter the configuration page as following:



AP Access Port

TAP Port

VLAN ID	10
IPv6 Address	2001:3211::1/64
Primary IP Address	192 . 168 . 1 . 228
Secondary IP Address	192 . 168 . 1 . 229
Subnet Mask	255 . 255 . 255 . 0
Designate AP Service Port	Tap Port

Figure 4-2 AP Access Port Configuration

These parameters in **[Network** > **AP Access Port]** page is described in details as following:

Parameter	Description
VLAN ID	Allocate a VLAN ID to the 'AP Access Port' for AP management which is distinguished with service VLAN of user client. **Note:** This VLAN ID cannot be any value, it must be an available VLAN which is previously created in [**Network > VLAN**].
IPv6 Address	It is necessary to allocate an IPv6 address to the 'AP Access Port' if the WLC is deployed in an IPv6 network.
Primary IP Address	Allocate an IPv4 address to the 'AP Access Port' as the primary IP address.
Secondary IP Address	Allocate an IPv4 address to the 'AP Access Port' as the secondary IP address for

Parameter	Description
	backup purpose.
Subnet Mask	Allocate a netmask for the 'AP Access Port' to divide which subnet the WLAN port is belonged to.
Designate AP Service Port	The AP service port in the WLC is used for user client traffic, which is different from the AP access port used for AP management. However, this port can be located on the same physical port as the thin AP access port (TAP), and distinguished by VLAN ID; or it can be located on other VLAN interfaces (VIF1~VIF8). The default value is the TAP port.

Click the **Apply** button to accept the changes.

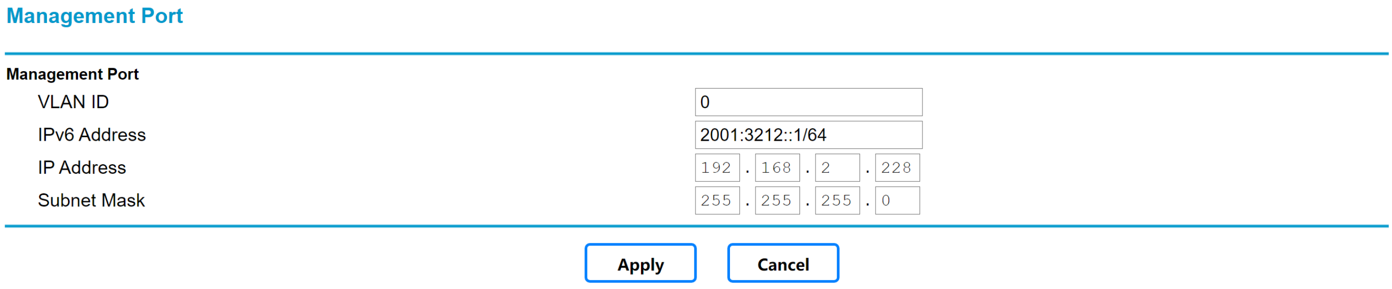
Click the **Cancel** button to discard the changes.

Note: If these parameters modified, it is necessary to **Save Configuration** and then reboot system to make them to take effect.

4.3. MANAGEMENT PORT

The first 1000Base-T RJ45 port (that is, the GE1 port) must be the management port of the WLC. Customers mainly use the management port to manage, maintain and configure WLC. The default IP address of the management port is ***192.168.2.228***.

Select **[Network** > **Management Port]** in the menu to enter the configuration page as following:



Management Port

Management Port

VLAN ID: 0

IPv6 Address: 2001:3212::1/64

IP Address: 192 . 168 . 2 . 228

Subnet Mask: 255 . 255 . 255 . 0

Figure 4-3 Management Port Configuration Page

These parameters in **[Network** > **Management Port]** page is described in details as following:

Parameter	Description
VLAN ID	If the external switching device or host connected to WLC is configured with a VLAN, this port must be assigned a VLAN ID for WLC management and maintenance.
IPv6 Address	It is necessary to allocate an IPv6 address to the 'Management Port' if the WLC is deployed in an IPv6 network.

Parameter	Description
IP Address	Assign an IPv4 address to the "management port" as the WLC management IP address. The default IP address is ***192.168.2.228***.
Subnet Mask	Allocate a netmask for the 'Management Port' to divide which subnet the WLC is belonged to.

Click the **Apply** button to accept the changes.

Click the **Cancel** button to discard the changes.

4.4. VLAN CREATION

If the Wi-Fi system is deployed in a VLAN-configured network, it is needed to create VLANs in the WLC for user data forwarding and WLC itself communication. Figure 4-4 shows the types of VLAN in WLC, where data plane VLANs are used for physical ports and control plane VLANs are used for VIF interfaces.

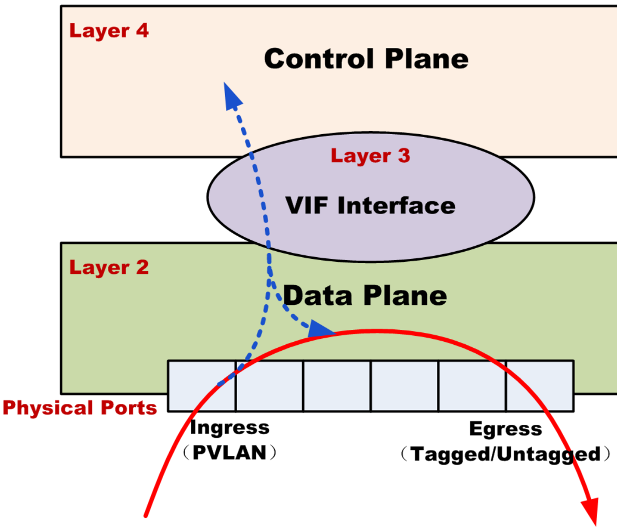
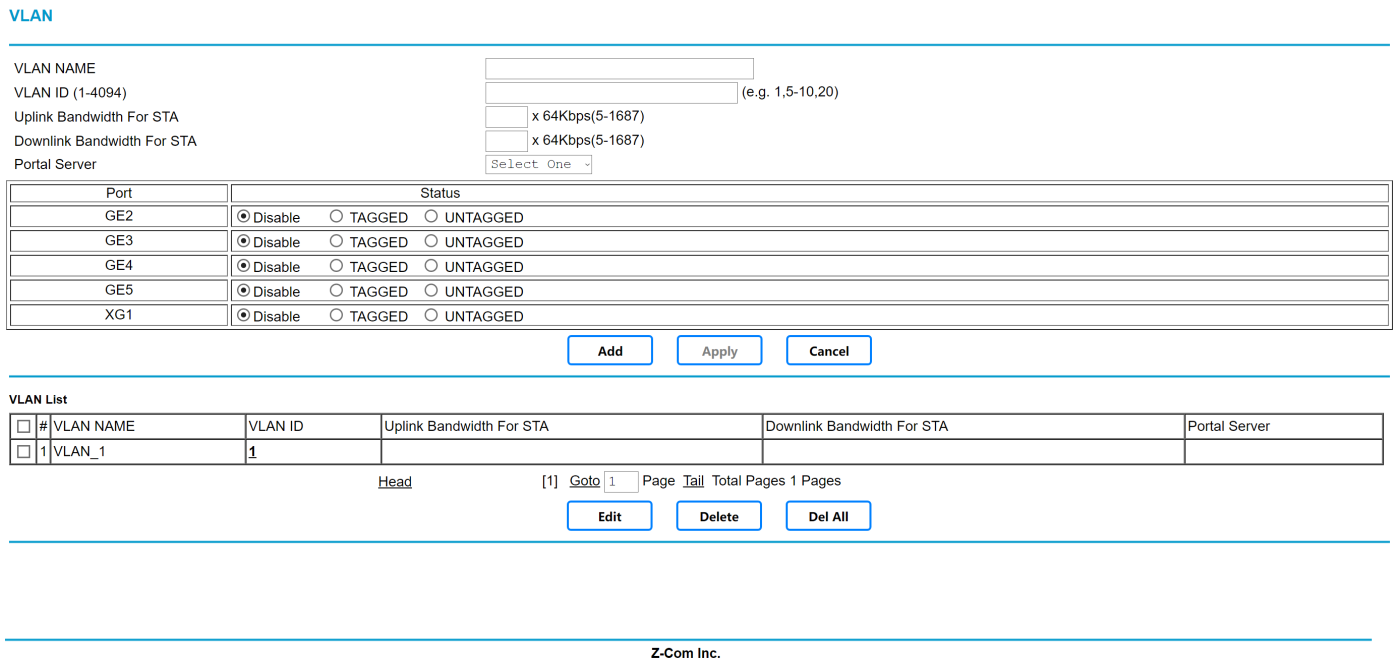


Figure 4-4 The VLAN types in WLC

Select **[Network** > **VLAN Creation]** in the menu to enter the configuration page as following:



VLAN

VLAN NAME
VLAN ID (1-4094) (e.g. 1,5-10,20)
Uplink Bandwidth For STA x 64Kbps(5-1687)
Downlink Bandwidth For STA x 64Kbps(5-1687)
Portal Server Select One

Port	Status
GE2	● Disable ○ TAGGED ○ UNTAGGED
GE3	● Disable ○ TAGGED ○ UNTAGGED
GE4	● Disable ○ TAGGED ○ UNTAGGED
GE5	● Disable ○ TAGGED ○ UNTAGGED
XG1	● Disable ○ TAGGED ○ UNTAGGED

VLAN List

□	#	VLAN NAME	VLAN ID	Uplink Bandwidth For STA	Downlink Bandwidth For STA	Portal Server
□	1	VLAN_1	1			

Head [1] Goto 1 Page Tail Total Pages 1 Pages

Z-Com Inc.

Figure 4-5 VLAN Configuration Page

These parameters in **[Network** > **VLAN Creation]** page is described in details as following:

Parameter	Description	
VLAN NAME	Assign a literal name for the new VLAN in order to mnemonic.	
VLAN ID	Allocate a numeric identifier to the new VLAN.	
Uplink Bandwidth for STA	User uplink traffic from wireless clients through this VLAN will be limited to a fixed bandwidth during transmission.	
Downlink Bandwidth for STA	User downlink traffic to the wireless client through this VLAN will be limited to a fixed bandwidth during transmission	
Portal Server	Bind the Portal server to the new VLAN, so user clients in this VLAN will use this Portal server for authentication.	
Physical Ports **Note:** Only those ports which have been classified to WLC type in [**Port Classification**] can be listed out here for VLAN binding.	**GE2**	The egress of this GbE port can be configured as: ▪ **TAGGED:** Outgoing packet with the VLAN tag. ▪ **UNTAGGED:** Outgoing packet with the VLAN tag stripped off.
	GE3	The egress of this GbE port can be configured as: ▪ **TAGGED:** Outgoing packet with the VLAN tag. ▪ **UNTAGGED:** Outgoing packet with the VLAN tag stripped off.
	GE5	The egress of this GbE port can be configured as: ▪ **TAGGED:** Outgoing packet with the VLAN tag. ▪ **UNTAGGED:** Outgoing packet with the VLAN tag stripped off.
	XG1	The egress of this 10G port can be configured as: ▪ **TAGGED:** Outgoing packet with the VLAN tag. ▪ **UNTAGGED:** Outgoing packet with the VLAN tag stripped off.

Parameter	Description
VLAN List	Click <**Add**> button to append above new VLAN configuration to the VLAN list for displaying. Only those VLAN IDs in this list are available for WLC configuration.

Click the **Add** button to append new VLAN to VLAN list.

Click the **Delete** button to remove a VLAN from VLAN list.

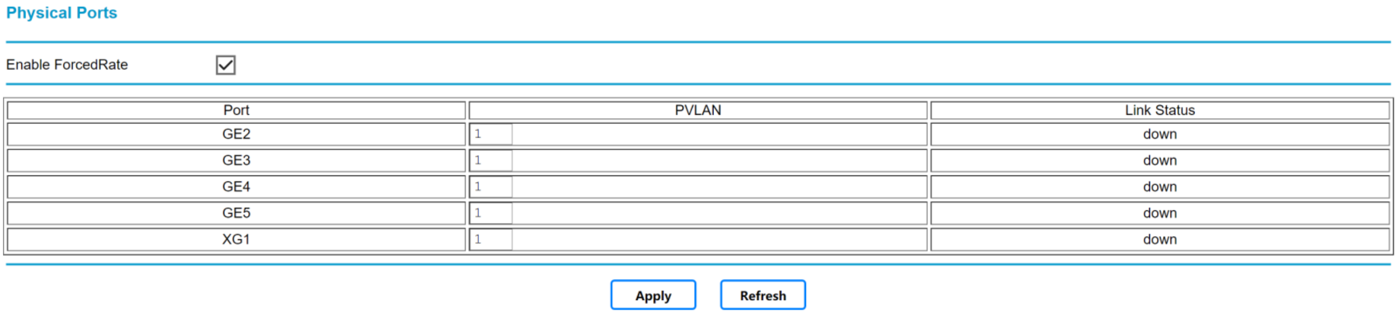
Click the **Edit** button to modify VLAN configuration in VLAN list.

4.5. Port VLAN

Since the physical port is the entrance for external data packets to enter the WLC, if the WLC is deployed in a VLAN-configured network, the physical port as the ingress should have its PVLAN (Port VLAN) been configured to handle the incoming packets.

Note: Only those ports which have been classified to WLC type in [**Port Classification**] can be listed out here for physical ports configuration.

Select **[Network** > **Port VLAN]** in the menu to enter the configuration page as following:



Physical Ports

Enable ForcedRate ☑

Port	PVLAN	Link Status
GE2	1	down
GE3	1	down
GE4	1	down
GE5	1	down
XG1	1	down

Figure 4-6 Physical Ports Page

These parameters in **[Network > Port VLAN]** page is described in details as following:

Parameter	Description
Enable ForcedRate	This is a switch to disable the speed auto-negotiation function for all physical ports.
GE2~GE5	The GbE physical port as the ***ingress*** is configured as: ▪ **PVLAN:** The PVLAN ID for this GbE physical port is used to match the incoming packets tagged by a VLAN ID. Note, this VLAN ID must be the available one which is created in [**Network** > **VLAN Creation**]. ▪ **Link Status:** Two status for this GbE physical port: **Up** indicates it is activated; **Down** indicates it is disabled.
XG1	The 10G physical port as the ***ingress*** is configured as: ▪ **PVLAN:** The PVLAN ID for this 10G physical port is used to adaptive to the incoming packets tagged by a VLAN ID. Note, this VLAN ID must be the

Parameter	Description
	available one which is created in [**Network** > **VLAN Creation**]. ▪ **Link Status:** Two status for this 10G physical port: **Up** indicates it is activated; **Down** indicates it is disabled.

Click the **Apply** button to accept the changes.

Click the **Refresh** button to update link status.

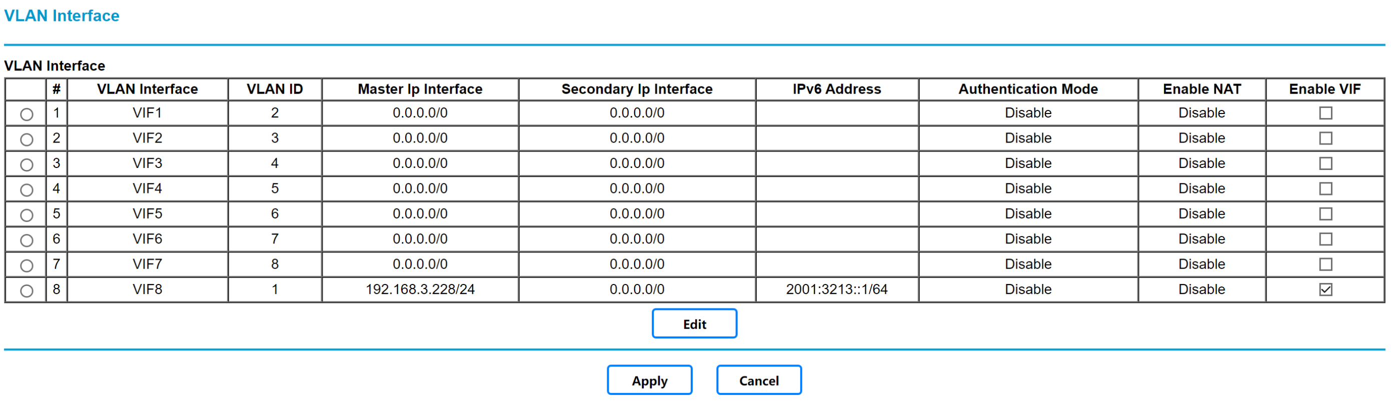
Summary of WLC VLAN:

- VLANs in WLC are classified to two types: 1) VLAN for data plane; 2) VLAN for control plane.
- VLANs for Data Plane: Egress configured by Untagged or Tagged flag; Ingress configured by PVLAN ID.
- VLANs for Control Plane: VIF interface configured by VLAN ID.

4.6. VLAN INTERFACE

The VLAN Interface (VIF) is a layer 3 virtual interface, which is used by WLC upper control plane applications to communicate with the outside world. Since the WLC has an underlying data plane for packet forwarding or upward transmission, the VIF interface actually becomes the communication layer between the control plane and the data plane in the WLC. The packets sent to WLC control plane from external applications, such as the packets of Radius, DHCP, CAPWAP etc., shall transmit via VIF interface. If the external hosts are configured with a VLAN, then the VIF interface must be allocated a VLAN to match the incoming packets from external host.

Select **[Network** > **VLAN Interface]** in the menu to enter the configuration page as following:



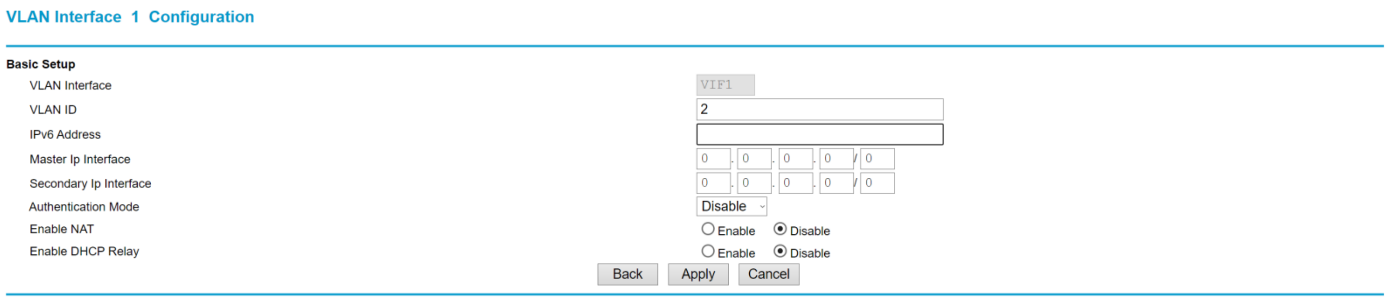
VLAN Interface

VLAN Interface

	#	VLAN Interface	VLAN ID	Master Ip Interface	Secondary Ip Interface	IPv6 Address	Authentication Mode	Enable NAT	Enable VIF
○	1	VIF1	2	0.0.0.0/0	0.0.0.0/0		Disable	Disable	□
○	2	VIF2	3	0.0.0.0/0	0.0.0.0/0		Disable	Disable	□
○	3	VIF3	4	0.0.0.0/0	0.0.0.0/0		Disable	Disable	□
○	4	VIF4	5	0.0.0.0/0	0.0.0.0/0		Disable	Disable	□
○	5	VIF5	6	0.0.0.0/0	0.0.0.0/0		Disable	Disable	□
○	6	VIF6	7	0.0.0.0/0	0.0.0.0/0		Disable	Disable	□
○	7	VIF7	8	0.0.0.0/0	0.0.0.0/0		Disable	Disable	□
○	8	VIF8	1	192.168.3.228/24	0.0.0.0/0	2001:3213::1/64	Disable	Disable	☑

Figure 4-7 VLAN Interface List

Select the VLAN Interface which you want to use by click the radio button in above list and then click <**Edit**> button to enter the edit page as below:



VLAN Interface 1 Configuration

Basic Setup

VLAN Interface: VIF1

VLAN ID: 2

IPv6 Address:

Master Ip Interface: 0 . 0 . 0 . 0 / 0

Secondary Ip Interface: 0 . 0 . 0 . 0 / 0

Authentication Mode: Disable

Enable NAT: ○ Enable ● Disable

Enable DHCP Relay: ○ Enable ● Disable

Figure 4-8 VLAN Interface Edit Page

These parameters in **[Network > VLAN Interface]** edit page are described in details as following:

Parameter	Description
VIF1~7	These VLAN Interfaces are used as user service interfaces: ▪ **VLAN ID:** Allocate a VLAN ID to this VLAN Interface, this VLAN ID must be the available one which is created in [**Network** > **VLAN Creation**]. ▪ **Master IP Address:** Allocate an IP address for this L3 interface as the primary IP address. ▪ **Secondary IP Address:** Allocate another IP address for this L3 interface as the secondary IP address for backup purpose. ▪ **IPv6 Address:** Allocate an IPv6 address for this L3 interface if WLC is deployed in IPv6 network. ▪ **Authentication Mode:** Two authentication modes for selection: o **Disable:** No authentication for this VLAN. o **Radius:** All uses in this VLAN will be authenticated by Radius. ▪ **Enable NAT:** NAT (Network Address Translation) function will be enabled for this VLAN. ▪ **Enable VIF:** The radio button will activate this VLAN Interface.
VIF8	This VLAN Interface is default used as WLAN port (i.e., the WLC southbound port for thin AP accessing, also called as TAP port). The default IP address is ***192.168.3.228***.

Click the **Edit** button to enter into VLAN Interface edit page.

Click the **Apply** button to accept the changes.

Click the **Cancel** button to discard the changes.

4.7. L2GRE TUNNEL

In some virtual network operator (VNO) application scenarios, the Wi-Fi users are grouped according to the VNO operator they belong to, and the services of each user group reach each VNO core network through different paths for authentication and Internet access. Generally speaking, the different virtual AP (represented by different SSID) in the thin AP identifies different VNO operator, and the Wi-Fi users only find their own SSID to associate. For VNO operators, the service path of their Wi-Fi users should be protected through L2GRE tunnels (customers here need to know more about L2GRE technology). Figure 4-8 illustrates an example where two SSIDs are used to identify two VNO operators: SSID A and SSID B. There are two L2GRE tunnels respectively established from WLC northbound ports to the remote edge L2GRE Bridges to reach their core networks.

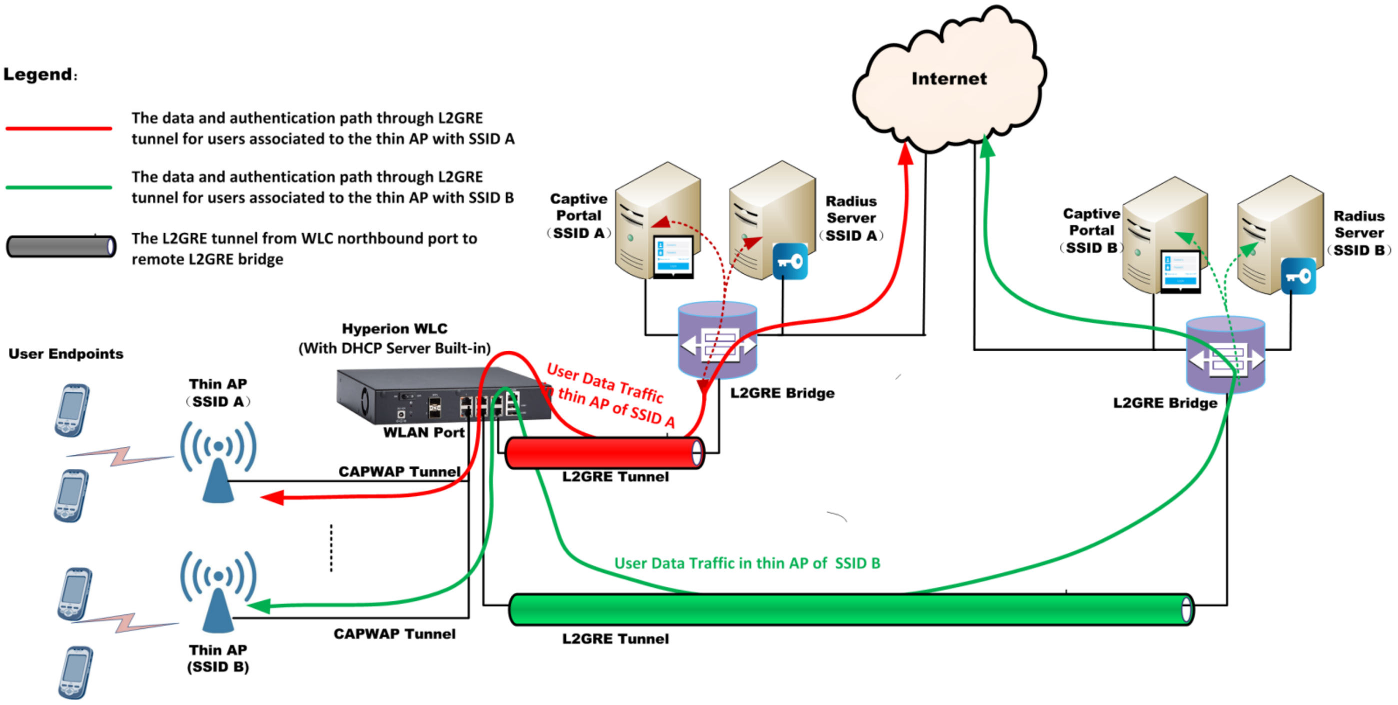
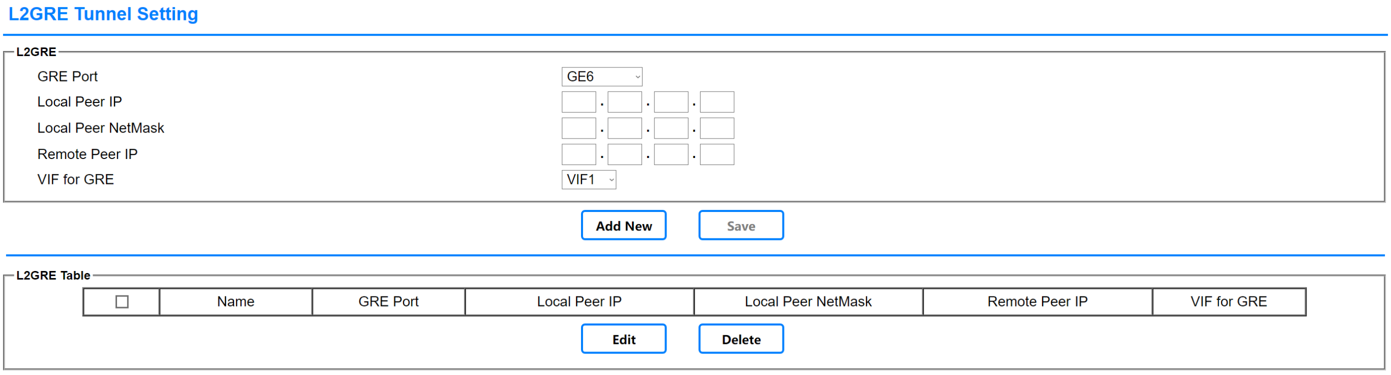

Legend:
The data and authentication path through L2GRE tunnel for users associated to the thin AP with SSID A
The data and authentication path through L2GRE tunnel for users associated to the thin AP with SSID B
The L2GRE tunnel from WLC northbound port to remote L2GRE bridge
Internet
Captive Portal (SSID A)
Radius Server (SSID A)
Captive Portal (SSID B)
Radius Server (SSID B)
User Endpoints
Hyperion WLC (With DHCP Server Built-in)
Thin AP (SSID A)
WLAN Port
User Data Traffic thin AP of SSID A
L2GRE Bridge
L2GRE Bridge
CAPWAP Tunnel
L2GRE Tunnel
User Data Traffic in thin AP of SSID B
Thin AP (SSID B)
CAPWAP Tunnel
L2GRE Tunnel

Figure 4-9 L2GRE tunnel application in Wi-Fi system

Select **[Network** > **L2GRE]** in the menu to enter the configuration page as following:



L2GRE Tunnel Setting

L2GRE

GRE Port	GE6
Local Peer IP	. . .
Local Peer NetMask	. . .
Remote Peer IP	. . .
VIF for GRE	VIF1

L2GRE Table

□	Name	GRE Port	Local Peer IP	Local Peer NetMask	Remote Peer IP	VIF for GRE

Figure 4-10 L2GRE Tunnel Configuration Page

These parameters in **[Network > L2GRE]** page is described in details as following:

Parameter	Description
GRE Port	Specify the physical port of WLC as the local peer of L2GRE tunnel. Note, this must be the port which has been classified to **non-WLC** type due to this port is under controlled by Linux Kernel.
Local Peer IP	Allocate an IP address for local peer of L2GRE tunnel in WLC.
Local Peer Netmask	Allocate a netmask for the local peer of L2GRE tunnel to divide which subnet it is belonged to.

Parameter	Description
Remote Peer IP	Enter the IP address of remote peer of L2GRE tunnel, otherwise, the L2GRE tunnel cannot be established.
VIF for GRE	**Importance:** Linux L2GRE must use a dedicated VLAN interface (VIF) to link to WLC applications, such as Radius authentication and user data traffic forwarding, and this VLAN interface (VIF) must have not been configured yet as a service VIF in [**Network> VLAN Interface**]. Here, bind a blank VLAN interface to this L2GRE tunnel configuration.
L2GRE Table	Above L2GRE configuration could be appended to a L2GRE table by click <**Add New**> button. Total number of L2GRE tunnels for WLC is limited to 4. Each L2GRE tunnel configuration in this table can be modified by selection and then click the <**Edit**> button under the table.

Click the **Add New** button to append a L2GRE configuration to the table.

Click the **Edit** button to modify a L2GRE configuration in table.

Click the **Delete** button to remove a L2GRE configuration from the table.

4.8. IPSec / VPN

In some application scenarios, user authentication messages and service data must be prevented from being hacked. Therefore, the northbound path from WLC to the operator's core network and Internet should be protected by a secure link. The secure link is usually an IPSec tunnel.

Figure 4-11 illustrates an example where an IPSec tunnel is established from WLC northbound port to the remote edge IPSec Gateway to reach the core network and Internet.

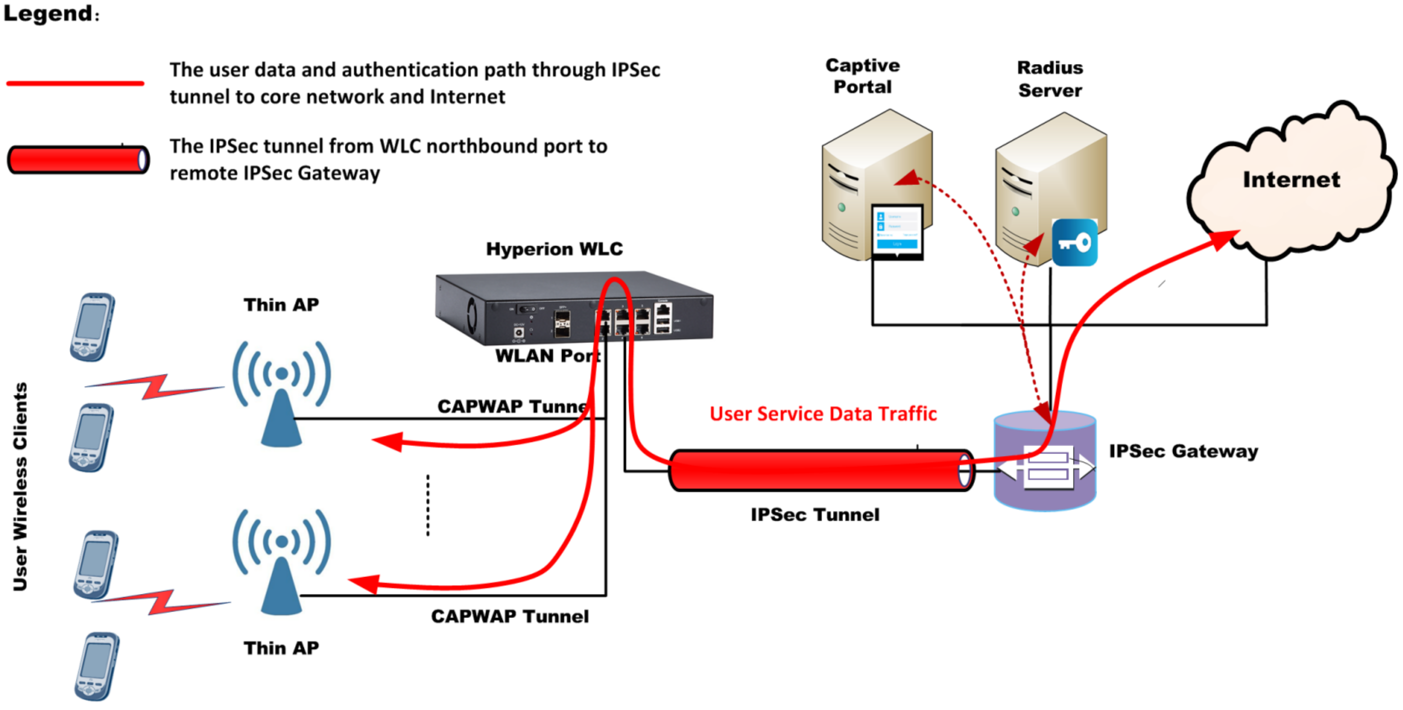
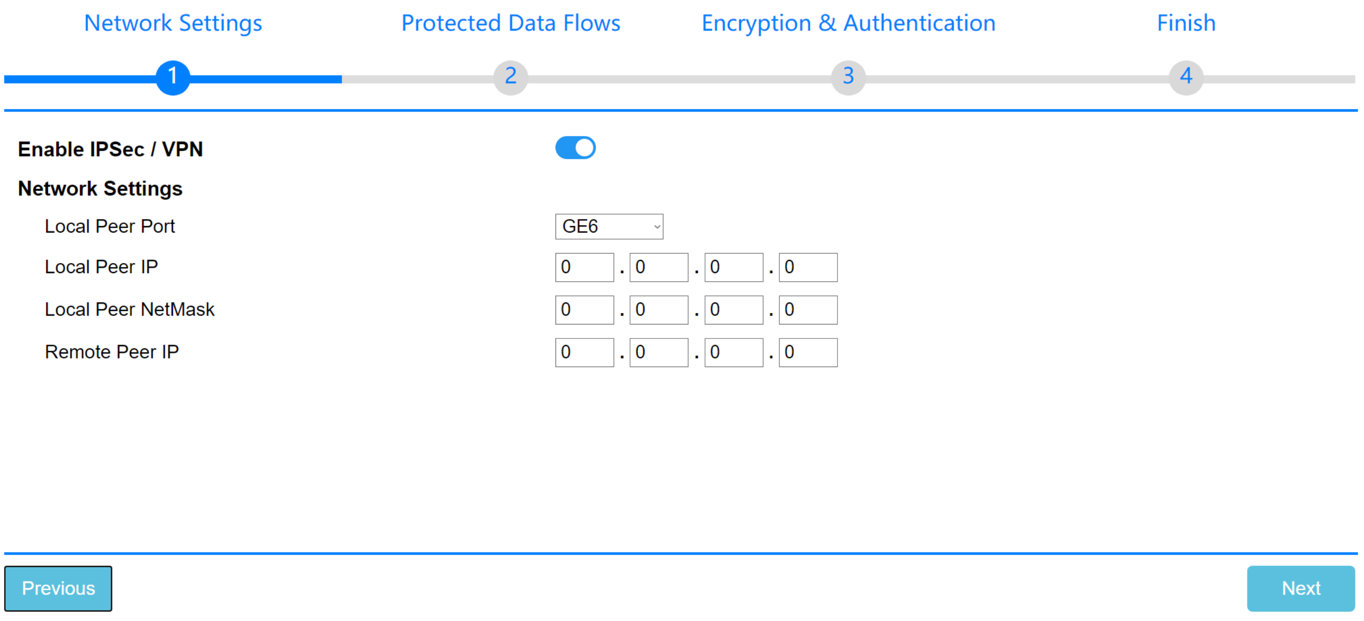

Legend:
The user data and authentication path through IPSec tunnel to core network and Internet
The IPSec tunnel from WLC northbound port to remote IPSec Gateway
Captive Portal
Radius Server
Internet
Hyperion WLC
Thin AP
WLAN Port
CAPWAP Tunnel
User Service Data Traffic
IPSec Gateway
IPSec Tunnel
User Wireless Clients
CAPWAP Tunnel
Thin AP

Figure 4-11 IPSec Tunnel Application in Wi-Fi System

Select **[Network** > **IPSec / VPN]** in the menu to enter the configuration page as following:



Enable IPSec / VPN ●

Network Settings

Local Peer Port GE6

Local Peer IP 0 . 0 . 0 . 0

Local Peer NetMask 0 . 0 . 0 . 0

Remote Peer IP 0 . 0 . 0 . 0

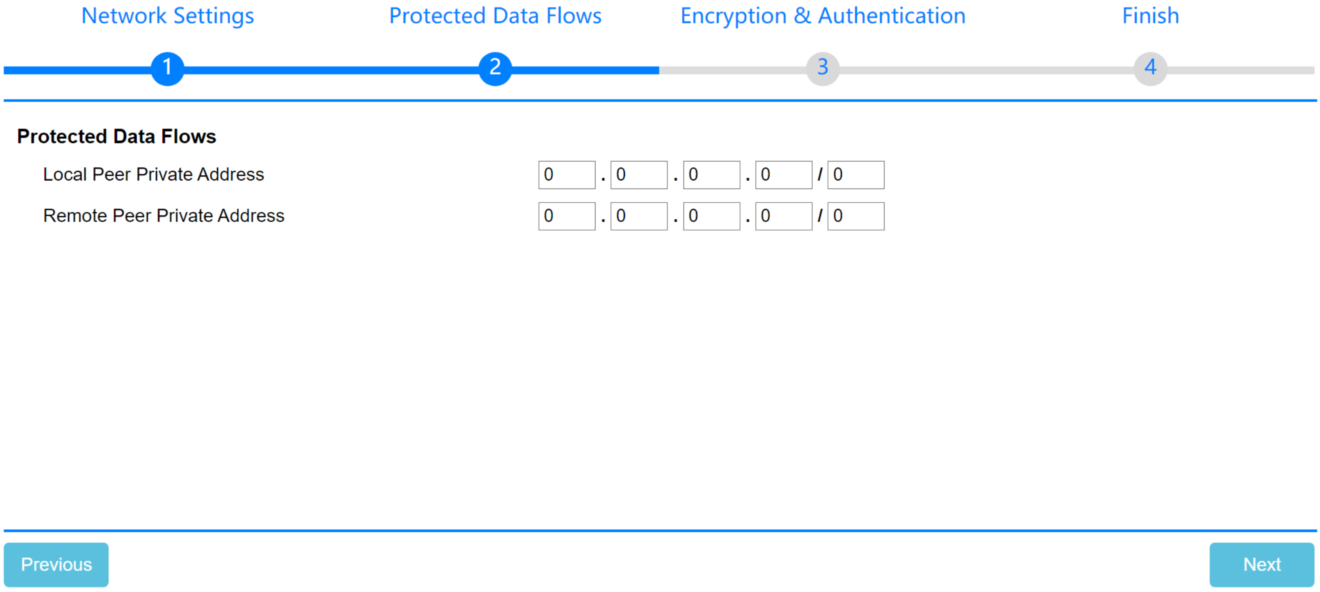
Figure 4-12 IPSec Tunnel Network Configuration Page

These parameters in above page are described in details as following:

Parameter	Description
Network Settings	▪ **Enable IPSec / VPN:** If customer needs to use IPSec tunnel from WLC to core network and Internet for user traffic security, this switch must be opened here to enable IPSec / VPN function in WLC. ▪ **Local Peer Port:** Select the WLC physical port to be bound as the local peer

Parameter	Description
	of the IPSec tunnel. ▪ **Local Peer IP:** Allocate an IP address to this local peer of IPSec tunnel. ▪ **Local Peer Netmask:** Allocate a netmask for the local peer of IPSec tunnel to divide which subnet it is belonged to. ▪ **Remote Peer IP:** Enter the IP address of remote IPSec Gateway as the remote peer IP address of this IPSec tunnel.

After complete this page configuration, click <**Next**> button to enter the next page:



Protected Data Flows

Local Peer Private Address 0 . 0 . 0 . 0 / 0

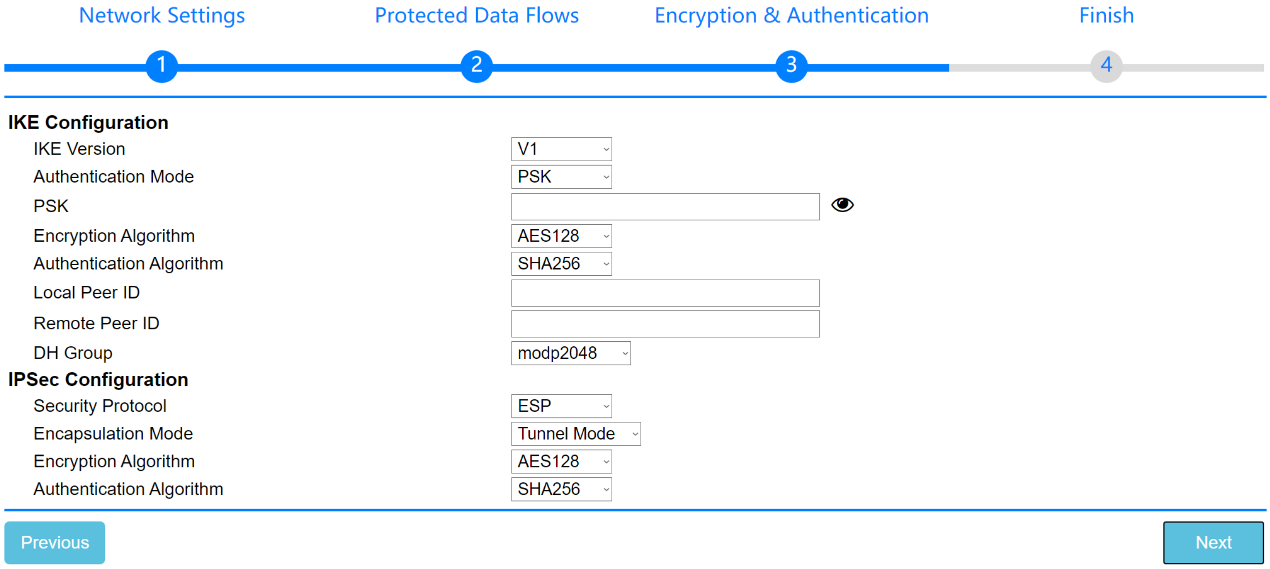
Remote Peer Private Address 0 . 0 . 0 . 0 / 0

Figure 4-13 IPSec Tunnel Protected Data Flows Configuration Page

These parameters in above page are described in details as following:

Parameter	Description
Protected Data Flows	The protected data flow stands for the local private network and destination private network in VPN. They will be encapsulated in the IPSec tunnel as the inner IP header for protection: ▪ **Local Peer Private Address:** Enter the subnet address with its netmask length of local private network. ▪ **Remote Peer Private Address:** Enter the subnet address with its netmask length of destination private network.

Again, after complete this page configuration, click <**Next**> button to enter the next page:



IKE Configuration

IKE Version: V1

Authentication Mode: PSK

PSK:

Encryption Algorithm: AES128

Authentication Algorithm: SHA256

Local Peer ID:

Remote Peer ID:

DH Group: modp2048

IPSec Configuration

Security Protocol: ESP

Encapsulation Mode: Tunnel Mode

Encryption Algorithm: AES128

Authentication Algorithm: SHA256

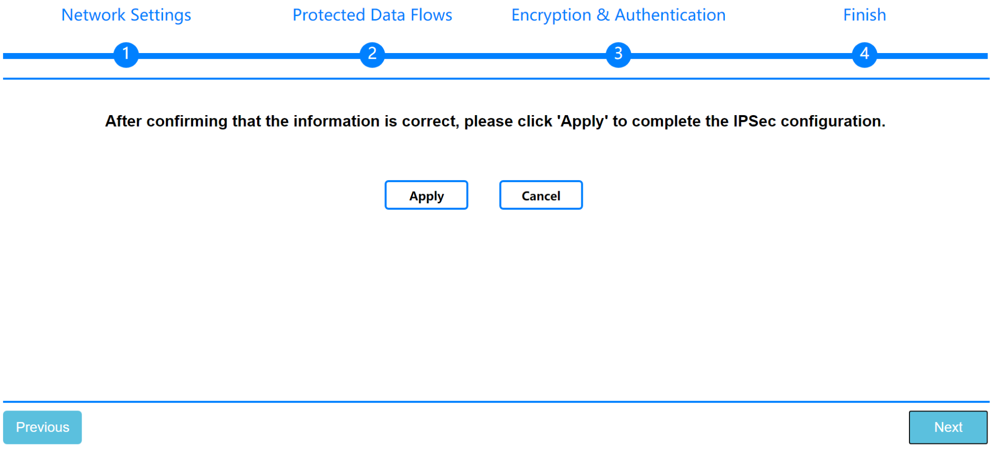
Figure 4-14 IPSec Tunnel Encryption and Authentication Configuration Page

These parameters in above page are described in details as following:

Parameter	Description
Encryption &. Authentication	**Note:** Here the parameters configuration must be consistent with the remote IPSec Gateway; otherwise, the IPSec tunnel cannot be established successfully. **IKE Configuration:** ▪ **IKE Version:** IKE is Internet Key Exchange protocol which is used to set up a security association of IPsec tunnel. It has two versions for selection: ***V1*** and ***V2,*** according to remote IPSec Gateway configuration ▪ **Authentication Mode:** Only the preset **PSK** supported. ▪ **PSK:** Enter the PSK key according to remote IPSec Gateway configuration. ▪ **Encryption Algorithm:** Select one from **AES128**, **AES192** and **AES256** according to remote IPSec Gateway configuration. ▪ **Authentication Algorithm:** Select one from **SHA256**, **SHA384** and **SHA512** according to remote IPSec Gateway configuration. ▪ **Local Peer ID:** Enter local peer IP address to identify the local peer of IPSec tunnel. ▪ **Remote Peer ID:** Enter the IP address of IPSec Gateway to identify the destination peer of the IPSec tunnel. ▪ **DH Group:** Select one from **Modep2048**, **Modep3072, Modep4096, ECP256** and **CURVECP25519** according to remote IPSec Gateway configuration. **IPSec Configuration:** ▪ **Security Protocol:** Only **ESP** supported. ▪ **Encapsulation Mode:** Only **Tunnel Mode** supported.

Parameter	Description
	▪ **Encryption Algorithm:** Select one among **AES128**, **AES192** and **AES256** according to remote IPSec Gateway configuration. ▪ **Authentication Algorithm:** Select one from **SHA256**, **SHA384** and **SHA512** according to remote IPSec Gateway configuration.

Further, after complete this page configuration, click <**Next**> button to enter the last page:



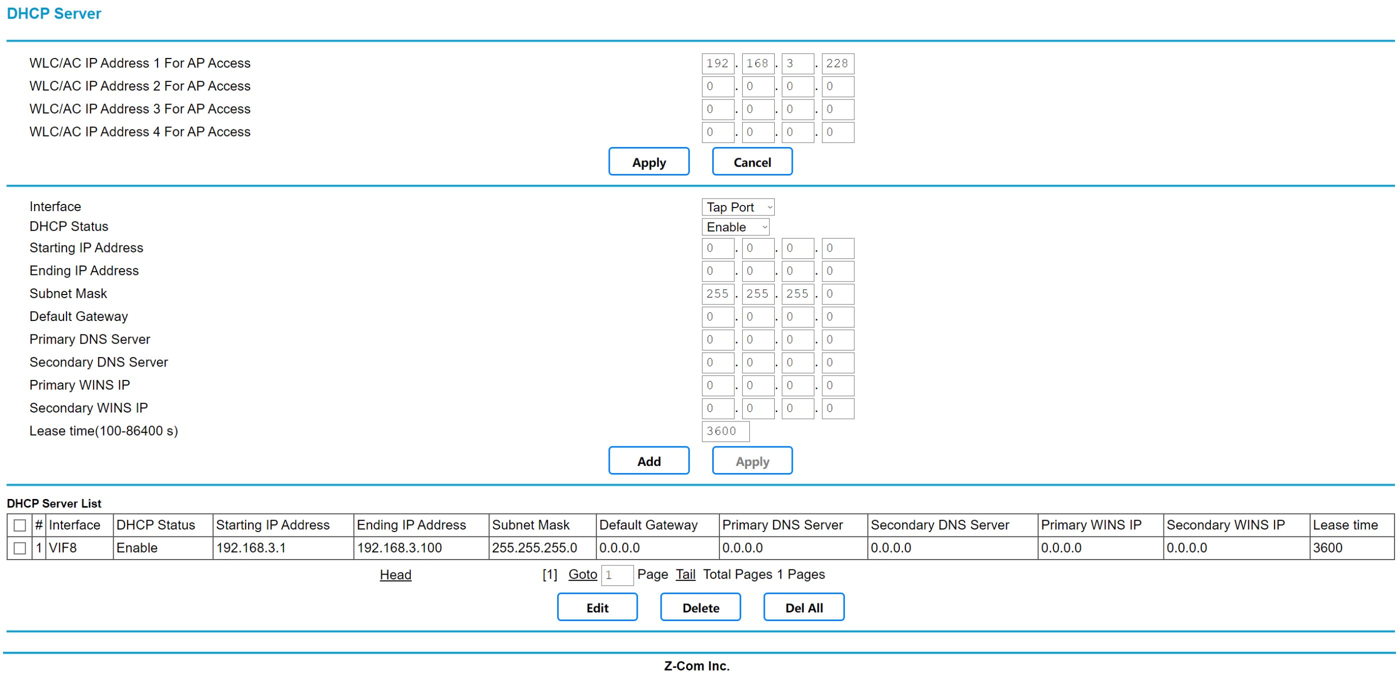
After confirming that the information is correct, please click 'Apply' to complete the IPSec configuration.

Figure 4-15 IPSec Tunnel Configuration Finish Page

4.9. DHCP SETTINGS

The Hyperion series WLC has a built-in DHCP server for allocating IP addresses to thin APs and wireless user clients. In this section, the DHCP server is bound to interfaces, such as the TAP port (AP Access Port or WLAN port) to allocate IP addresses to thin APs, and the VLAN interface (VIF) to allocate IP addresses to wireless user clients.

Select **[Network** > **DHCP Setting]** in the menu to enter the configuration page as following:



DHCP Server

WLC/AC IP Address 1 For AP Access 192 . 168 . 3 . 228
WLC/AC IP Address 2 For AP Access 0 . 0 . 0 . 0
WLC/AC IP Address 3 For AP Access 0 . 0 . 0 . 0
WLC/AC IP Address 4 For AP Access 0 . 0 . 0 . 0

Interface Tap Port
DHCP Status Enable
Starting IP Address 0 . 0 . 0 . 0
Ending IP Address 0 . 0 . 0 . 0
Subnet Mask 255 . 255 . 255 . 0
Default Gateway 0 . 0 . 0 . 0
Primary DNS Server 0 . 0 . 0 . 0
Secondary DNS Server 0 . 0 . 0 . 0
Primary WINS IP 0 . 0 . 0 . 0
Secondary WINS IP 0 . 0 . 0 . 0
Lease time(100-86400 s) 3600

DHCP Server List

□	#	Interface	DHCP Status	Starting IP Address	Ending IP Address	Subnet Mask	Default Gateway	Primary DNS Server	Secondary DNS Server	Primary WINS IP	Secondary WINS IP	Lease time
□	1	VIF8	Enable	192.168.3.1	192.168.3.100	255.255.255.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	3600

Figure 4-15 Static Route Page

These parameters in **[Network** > **DHCP Setting]** page is described in details as following:

Parameter	Description
WLC/AC IP Address 1~4 for AP Access	A thin AP can access up to 4 WLCs to achieve redundant security. Once the primary WLC fails, the thin AP can automatically switch to another redundant WLC. The four IP addresses provided here stand for four available WLCs. These IP addresses are actually the CAPWAP tunnel termination IP addresses in the WLC, which will be delivered in the form of DHCP option 43 during the thin AP DHCP process to tell the thin AP where to establish the CAPWAP management tunnel. Usually, one WLC is enough!
Interface	Binding current DHCP server configuration to the port: ▪ **TAP:** The thin AP port which is the WLAN port for thin AP accessing to WLC, therefore, the DHCP server bound to this port is used for allocating IP addresses to thin AP. ▪ **VIF1~8:** Totally 8 VLAN Interfaces in WLC as the virtual ports for user services, therefore, the DHCP server bound to these ports are used for allocating IP addresses to wireless user clients.
Starting IP Address	The 1'st IP address in this DHCP address pool for allocation.
Ending IP Address	The last IP address in this DHCP address pool for allocation.
Subnet Mask	Allocate a netmask to this DHCP address pool to divide which subnet it is belonged to.
Default Gateway	The default gateway IP address for allocation together in current DHCP address pool.
Primary DNS Server	The 1'st DNS server IP address for allocation together in current DHCP address pool.

Parameter	Description
Secondary DNS Server	The backup DNS server IP address for allocation together in current DHCP address pool.
Primary WINS IP	WINS refers to Windows Internet Name Server. Here entering the 1'st WINS IP address for allocation together in current DHCP address pool.
Secondary WINS IP	WINS refers to Windows Internet Name Server. Here entering the backup WINS IP address for allocation together in current DHCP address pool.
Lease Time (100~86400 Seconds)	It is not a permanently effective IP address for a client after DHCP allocation, it has a limited lifetime till it expires. This limited lifetime is the lease time which makes the IP address can be shared by more clients. The default lease time is 3600 seconds.

Click the **Add** button to append a new entry to the list.

Click the **Apply** button to accept the changes.

Click the **Cancel** button to discard the changes.

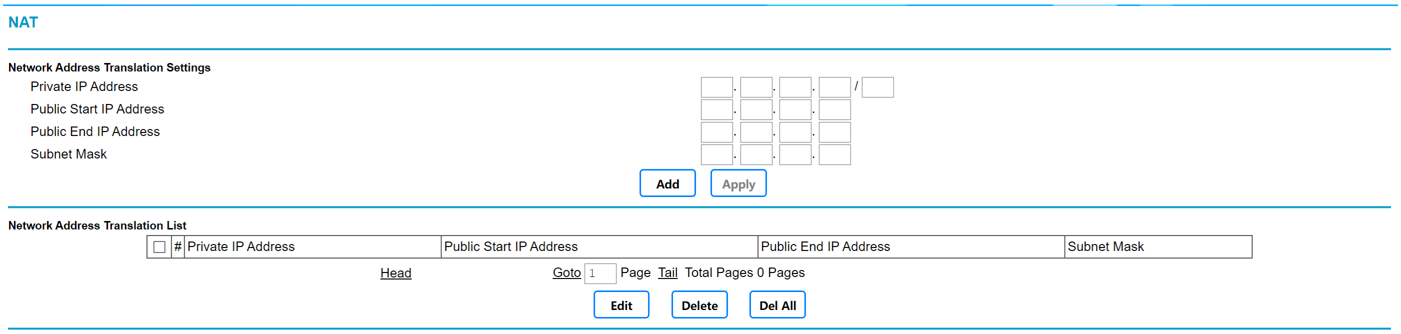
Click the **Delete** button to remove the selected entry.

Click the **Edit** button to modify the selected entry.

4.10. NAT

NAT stands for Network Address Translation, and it is a layer 3 functions that takes effect when the packets traverse crossing different subnets. In fact, NAT replaces the source IP address and destination IP address of the request/response packet with its own inner and outer IP addresses, so that the packet is located on the same subnet as the destination. The inner IP address of the NAT is the private network IP address, and the outer IP address of the NAT is the public network IP address.

Select **[Network** > **NAT]** in the menu to enter the configuration page as following:



NAT

Network Address Translation Settings

Private IP Address
Public Start IP Address
Public End IP Address
Subnet Mask

Network Address Translation List

□	#	Private IP Address	Public Start IP Address	Public End IP Address	Subnet Mask

Head Goto 1 Page Tail Total Pages 0 Pages

Figure 4-4 NAT Configuration Page

These parameters in **[Network** > **NAT]** page is described in details as following:

Parameter	Description

Parameter	Description
Private IP Address	This is the private network at NAT inner side specified by the IP address with its subnet mask length.
Public Start IP Address	This is the NAT outer side 1'st IP address facing the public network.
Public End IP Address	This is the NAT outer side last IP address facing the public network.
Subnet Mask	Allocate a netmask to the segment of public IP address to divide which subnet it is belonged to.

Click the **Add** button to append a new entry to the list.

Click the **Apply** button to accept the changes.

Click the **Cancel** button to discard the changes.

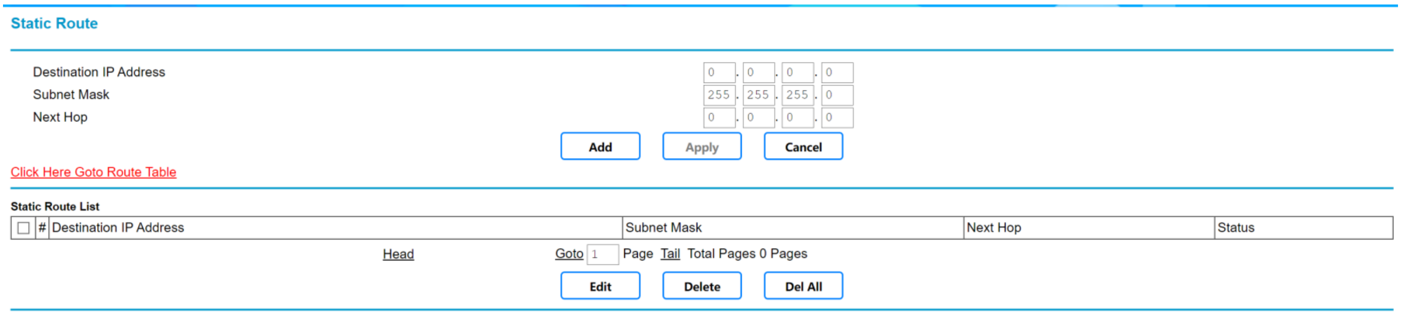
Click the **Delete** button to remove the selected entry.

Click the **Edit** button to modify the selected entry.

4.11. STATIC ROUTE

When a data packet is sent to a specific target IP address in a different subnet from the originator, since the route is unknown, the customer can specify a known next hop for the data packet and reach the destination hop by hop. Binding the known next hop to a specific target IP address is configuring the static routing.

Select **[Network** > **Static Route]** in the menu to enter the configuration page as following:



Static Route

Destination IP Address 0 . 0 . 0 . 0
Subnet Mask 255 . 255 . 255 . 0
Next Hop 0 . 0 . 0 . 0

Click Here Goto Route Table

Static Route List

□	#	Destination IP Address	Subnet Mask	Next Hop	Status

Head Goto 1 Page Tail Total Pages 0 Pages

Figure 4-17 Static Rote Configuration Page

These parameters in **[Network** > **Static Route]** page is described in details as following:

Parameter	Description
Destination IP Address	This is the specific IP address which should be matched with packet destination IP address for routing to a known next hop.
Subnet Mask	Allocate a netmask to this specific destination IP address to divide which subnet it is belonged to.

Parameter	Description
Next Hop	When the destination IP of a packet is matched with the above specific one, it will be directed to the IP address here to for further routing.
Subnet Mask	Allocate a netmask to the segment of public IP address to divide which subnet it is belonged to.

Click the **Add** button to append a new entry to the list.

Click the **Apply** button to accept the changes.

Click the **Cancel** button to discard the changes.

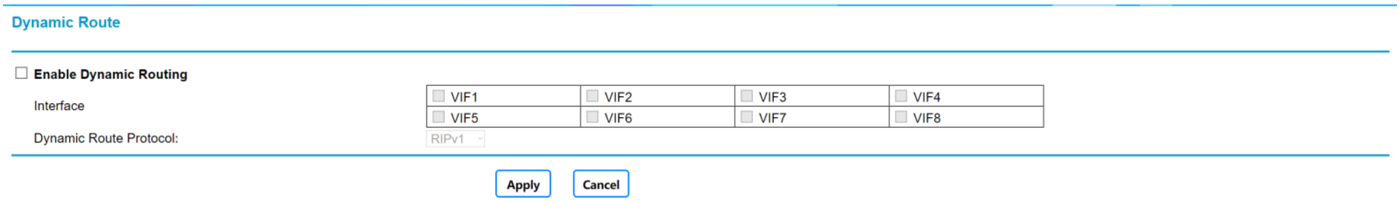
Click the **Delete** button to remove the selected entry.

Click the **Edit** button to modify the selected entry.

4.12. Dynamic Route

Dynamic routing is different from static routing. The next hop of dynamic routing is automatically selected by algorithm, rather than manually specified. The routing algorithm is based on routing protocols including RIPv1 and OSPF. Need to bind dynamic routing to the VLAN interface (VIF) through which the user service traffic passes and routes to the destination.

Select **[Network** > **Dynamic Route]** in the menu to enter the configuration page as following:



Dynamic Route

☐ Enable Dynamic Routing

Interface: ☐ VIF1 ☐ VIF2 ☐ VIF3 ☐ VIF4 ☐ VIF5 ☐ VIF6 ☐ VIF7 ☐ VIF8

Dynamic Route Protocol: RIPv1

Figure 4-18 Dynamic Rote Configuration Page

These parameters in **[Network** > **Dynamic Route]** page is described in details as following:

Parameter	Description
Enable Dynamic Routing	This switch is used to open the dynamic routing function for WLC.
Interface	Binding the dynamic routing function to specific VLAN Interface through which the user services traffic passes.
Dynamic Routing Protocol	Select the proper dynamic routing protocol: ***RIP*** or ***OSPF***.

Click the **Add** button to append a new entry to the list.

Click the **Apply** button to accept the changes.

Click the **Cancel** button to discard the changes.

Click the **Delete** button to remove the selected entry.

Click the **Edit** button to modify the selected entry.

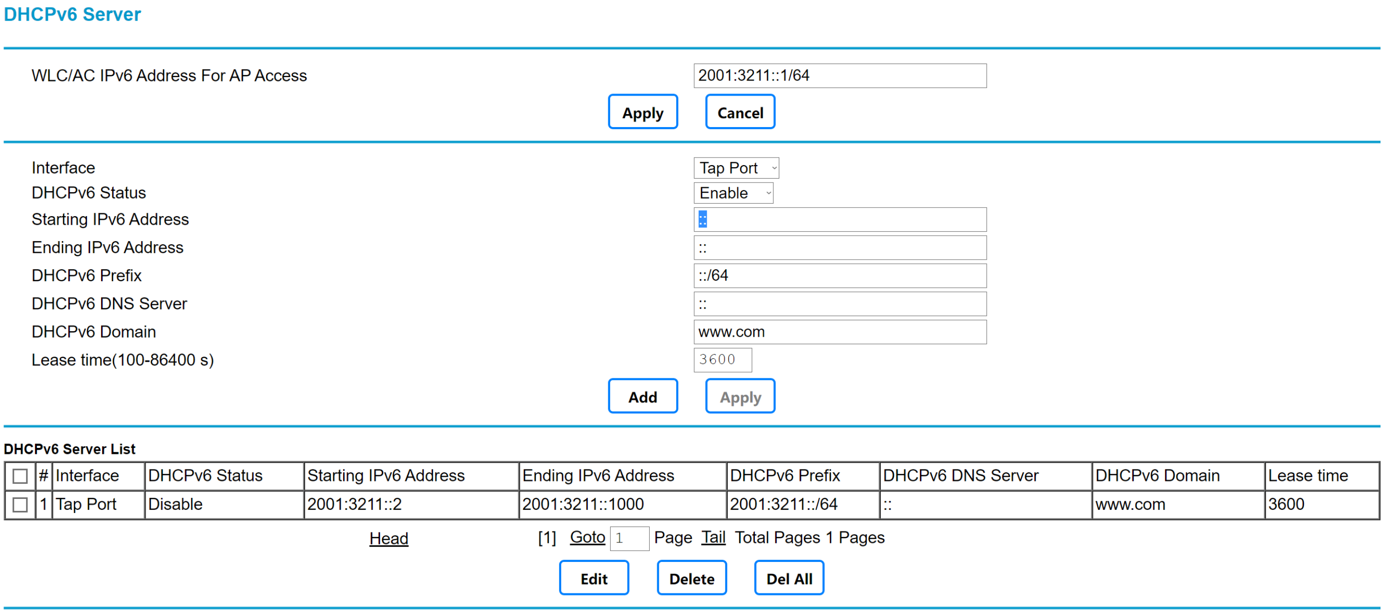
Chapter 5. IPv6 CONFIGURATION

If WLC is deployed in an IPv6 network environment, it is necessary to have some related parameters configured for WLC to adapt to the IPv6 infrastructure.

5.1. DHCP SERVER

In a IPv6 network environment, DHCP will allocate IP addresses to thin APs or wireless user clients in IPv6 format, therefore, the DHCP server in WLC should be configured according to DHCPv6 specification.

Select **[IPv6 Configuration > DHCP Server]** in the menu to enter the configuration page as following:



DHCPv6 Server

WLC/AC IPv6 Address For AP Access	2001:3211::1/64

Interface	Tap Port
DHCPv6 Status	Enable
Starting IPv6 Address	::
Ending IPv6 Address	::
DHCPv6 Prefix	::/64
DHCPv6 DNS Server	::
DHCPv6 Domain	www.com
Lease time(100-86400 s)	3600

DHCPv6 Server List

□	#	Interface	DHCPv6 Status	Starting IPv6 Address	Ending IPv6 Address	DHCPv6 Prefix	DHCPv6 DNS Server	DHCPv6 Domain	Lease time
□	1	Tap Port	Disable	2001:3211::2	2001:3211::1000	2001:3211::/64	::	www.com	3600

Figure 5-1 DHCPv6 Server Configuration Page

These parameters in **[IPv6 Configuration > DHCP Server]** page is described in details as following:

Parameter	Description
WLC/AC IPv6 Address For AP Access	Here providing an IPv6 address actually represents the CAPWAP tunnel termination IPv6 addresses in WLC which will be delivered in DHCPv6 option 43 during the thin AP DHCPv6 procedure to tell Thin APs where to establish their CAPWAP management tunnels to WLC.
DHCPv6 State	This is a switch to enable or disable WLC internal DHCPv6 server.
Starting IPv6 Address	The 1'st IPv6 address in DHCPv6 server address pool available for clients.
Ending IPv6 Address	The last IPv6 address in DHCPv6 server address pool available for clients.
IPv6 Prefix	IPv6 prefix represents the routing or a subnet of a segment of IPv6 addresses. The default length is 64 bits.
DHCPv6 DNS	The DNS server IPv6 address for allocation together in current DHCPv6 address pool.

Parameter	Description
DHCPv6 Domain	
Lease Time (100 - 86400 s)	It is not a permanently effective IPv6 address for a client after DHCPv6 allocation; it has a limited lifetime till it expires. This limited lifetime is the lease time which makes the IPv6 address can be shared by more clients. The default lease time is 3600 seconds.

Click the **Add** button to append a new DHCPv6 server entry to the server list.

Click the **Apply** button to accept the changes.

Click the **Cancel** button to discard the changes.

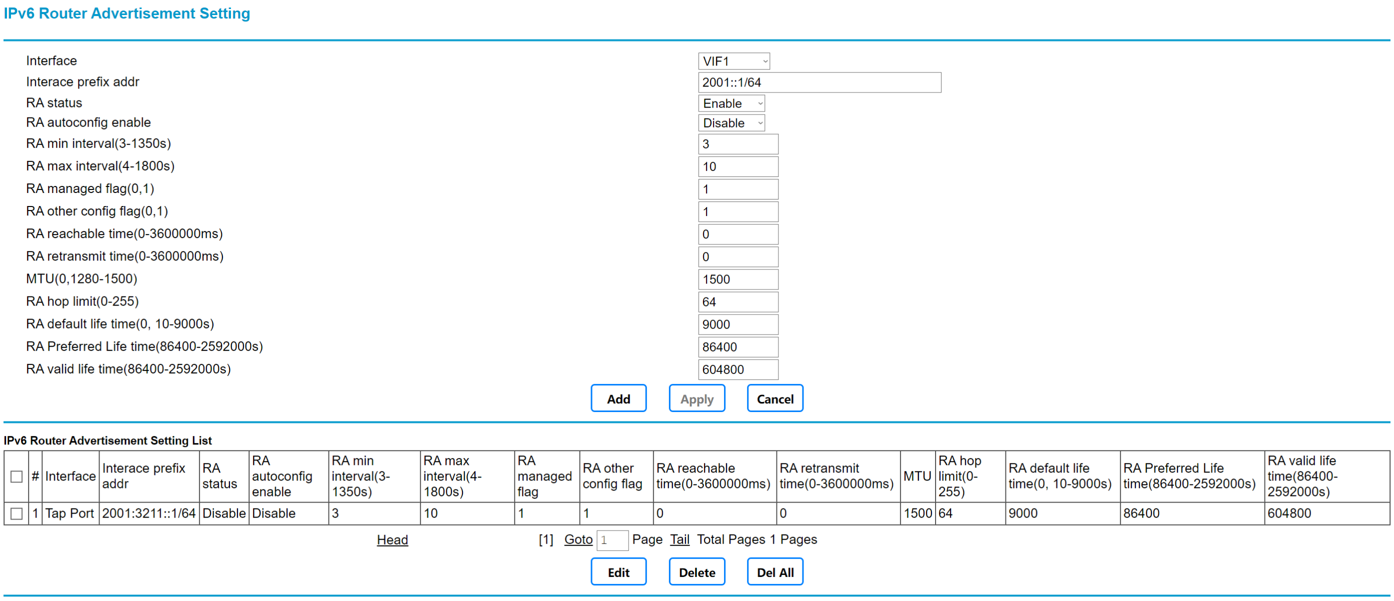
Click the **Delete** button to remove the selected DHCPv6 server entry from list.

Click the **Edit** button to modify the selected DHCPv6 server entry.

5.2. ROUTE ADVERTISEMENT

The IPv6 Router Advertisement messages include unsolicited and solicited. The IPv6 routers send unsolicited Router Advertisement (RA) messages pseudo-periodically, that is, the interval between unsolicited advertisements is randomized to reduce synchronization issues when there are multiple advertising routers on a link. While the solicited Router Advertisement messages is the response to the Router Solicitation message. The Router Advertisement message contains the information of the link prefixes, the link MTU, specific routes, flag of address auto-configuration, and the valid and preferred lifetime of auto-configured address, which are used by the host to determine its own routing configuration.

Select **[IPv6 Configuration** > **DHCP Advert]** in the menu to enter the configuration page as following:



IPv6 Router Advertisement Setting

Interface	VIF1
Interace prefix addr	2001::1/64
RA status	Enable
RA autoconfig enable	Disable
RA min interval(3-1350s)	3
RA max interval(4-1800s)	10
RA managed flag(0,1)	1
RA other config flag(0,1)	1
RA reachable time(0-3600000ms)	0
RA retransmit time(0-3600000ms)	0
MTU(0,1280-1500)	1500
RA hop limit(0-255)	64
RA default life time(0, 10-9000s)	9000
RA Preferred Life time(86400-2592000s)	86400
RA valid life time(86400-2592000s)	604800

IPv6 Router Advertisement Setting List

☐	#	Interface	Interace prefix addr	RA status	RA autoconfig enable	RA min interval(3-1350s)	RA max interval(4-1800s)	RA managed flag	RA other config flag	RA reachable time(0-3600000ms)	RA retransmit time(0-3600000ms)	MTU	RA hop limit(0-255)	RA default life time(0, 10-9000s)	RA Preferred Life time(86400-2592000s)	RA valid life time(86400-2592000s)
☐	1	Tap Port	2001:3211::1/64	Disable	Disable	3	10	1	1	0	0	1500	64	9000	86400	604800

Figure 5-2 IPv6 Route Advertisement Configuration Page

These parameters in **[IPv6 Configuration** > **DHCP Advert]** page is described in details as following:

Parameter	Description
Interface	Specify the VLAN Interface (VIF) on which the current Router Advertisement setting will act.
Prefix Addr	IPv6 prefix represents the routing or a subnet of a segment of IPv6 addresses. The default length is 64 bits.
RA Status	This is a switch to enable or disable the IPv6 Router Advertisement function in WLC.
RA Autoconfig Enable	IPv6 Neighbor Discover (ND) function will auto-configure the addresses, address prefixes, routes, and other configuration parameters. This switch is used open or close the ND autoconfig function in WLC.
RA Min Interval (3-1350 s)	The minimum periodically time interval for WLC to send Router Advertisement message.
RA Max Interval (4-1800 s)	The maximum periodically time interval for WLC to send Router Advertisement message.
RA Managed Flag (0, 1)	A flag indicating that the WLC can auto-configured the address using DHCP server besides using Router Advertisements (RA). This function needs to enable DHCPv6 for address.
RA Other Config Flag (0, 1)	A flag indicating that the WLC can auto-configured the other (non-address) information using administered (stateful) protocol. This function needs to enable DHCPv6 for other information.
RA Reachable Time (0-360000 ms)	This is the Neighbor Discover Reachable time in milliseconds within which the WLC assumes a neighbor is reachable after receiving a reachability confirmation.
RA Retransmit Time (0-360000 ms)	This is the Neighbor Discover Retransmit time in milliseconds after which the WLC can retransmit the Neighbor Solicitation messages.
MTU (0, 1200-1500)	This is the Router Advertisement (RA) maximum transmission unit (MTU), It must be the MTU value that all nodes on a link use.
RA Hop Limit (0-255)	It is the default value to be placed in the Hop Count field of the IPv6 header for outgoing (unicast) IPv6 packets.
RA Default Life Time (0, 10-9000 s)	The lifetime associated with the default router in seconds. A value of 0 indicates that the router is not a default router and will not appear on the default router list. The router lifetime applies only to the router's usefulness as a default router; it does not apply to information contained in other message fields or options.
RA Preferred Life Time (86400-2592000 s)	The RA preferred lifetime in seconds associated with the default router.
RA Valid Life Time (86400-2592000 s)	The RA valid lifetime in seconds associated with the default router.
RA Setting List	Above settings can be appended to the RA setting list as a new entry.

Click the **Add** button to append a new IPv6 router advertisement entry to the server list.

Click the **Apply** button to accept the changes.

Click the **Cancel** button to discard the changes.

Click the **Delete** button to remove the selected IPv6 router advertisement entry from list.

Click the **Edit** button to modify the selected IPv6 router advertisement entry.

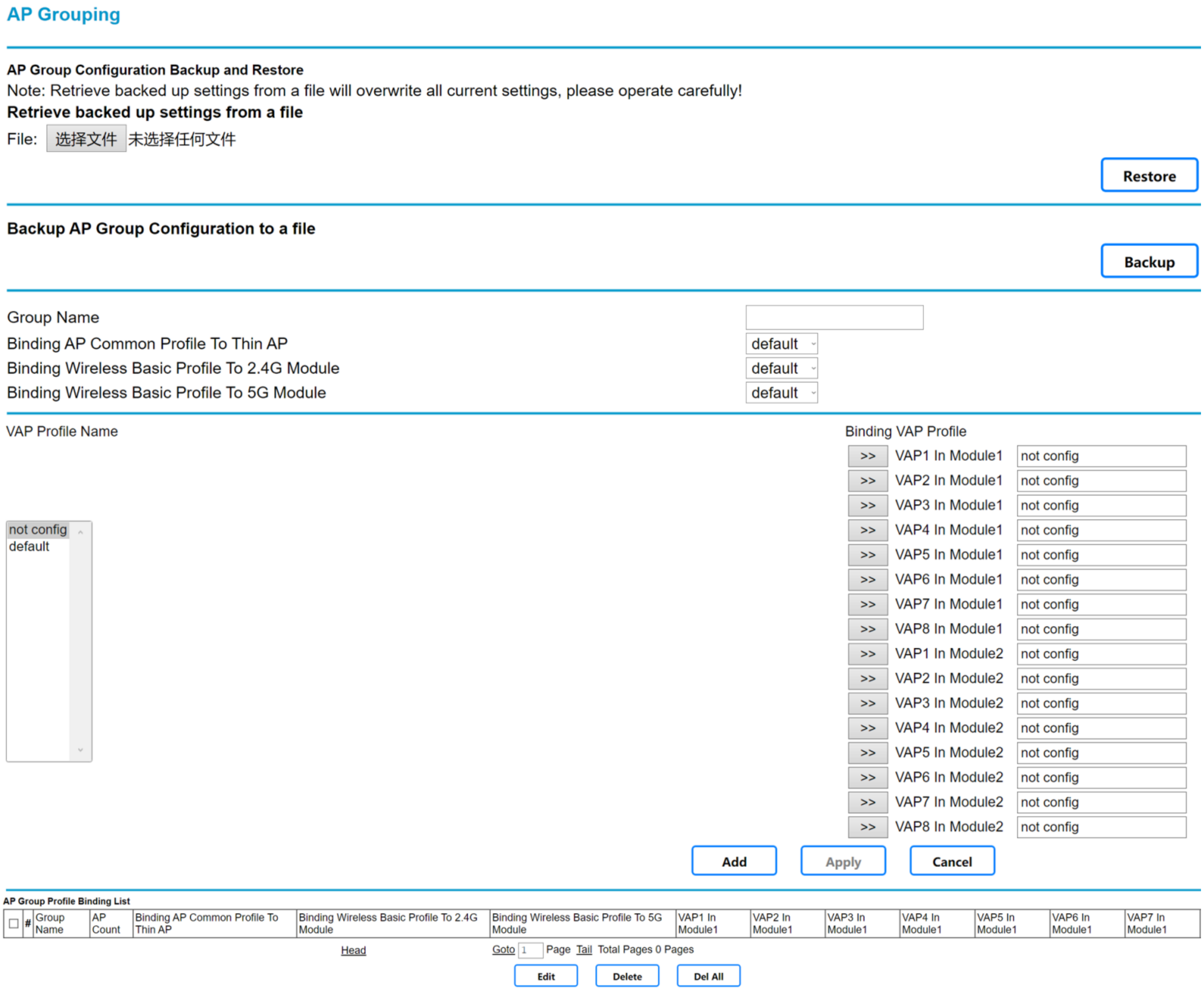
Chapter 6. Thin AP Configuration Profiles

There is no configuration on the thin AP (TAP). After power on, during the DHCP process, it discovers the WLC from the DHCP Option 43 broadcast by the WLC. Then, the thin AP attempts to establish a CAPWAP management tunnel to the WLC based on the IP address in DHCP option 43. After establishing a CAPWAP tunnel between the thin AP and WLC, the thin AP requests and downloads a set of profiles from the WLC to complete the configuration of the thin AP. The configuration files of the thin AP include Common Profile, Wireless Profile and VAP (virtual AP) Profile, which can be combined to implement the provisioning of the thin AP.

6.1. AP Grouping

We know that the thin AP is configured by downloading profiles from the WLC through the CAPWAP tunnel. However, if a profile is used for only one thin AP, too many profiles are required to meet these requirements, thus occupying too much space in the WLC. At the same time, the management and maintenance of profiles becomes a difficult task for administrators. Therefore, it is necessary to divide the thin APs into different groups according to different attributes of the thin APs, and the thin APs in a group share the same profiles to reduce the profiles number.

Select **[Thin AP Configuration** > **AP Grouping]** in the menu to enter the configuration page as following:



AP Grouping

AP Group Configuration Backup and Restore

Note: Retrieve backed up settings from a file will overwrite all current settings, please operate carefully!

Retrieve backed up settings from a file

File: 选择文件 未选择任何文件

Backup AP Group Configuration to a file

Group Name	
Binding AP Common Profile To Thin AP	default
Binding Wireless Basic Profile To 2.4G Module	default
Binding Wireless Basic Profile To 5G Module	default

VAP Profile Name: not config, default

Binding VAP Profile	
VAP1 In Module1	not config
VAP2 In Module1	not config
VAP3 In Module1	not config
VAP4 In Module1	not config
VAP5 In Module1	not config
VAP6 In Module1	not config
VAP7 In Module1	not config
VAP8 In Module1	not config
VAP1 In Module2	not config
VAP2 In Module2	not config
VAP3 In Module2	not config
VAP4 In Module2	not config
VAP5 In Module2	not config
VAP6 In Module2	not config
VAP7 In Module2	not config
VAP8 In Module2	not config

AP Group Profile Binding List

□	#	Group Name	AP Count	Binding AP Common Profile To Thin AP	Binding Wireless Basic Profile To 2.4G Module	Binding Wireless Basic Profile To 5G Module	VAP1 In Module1	VAP2 In Module1	VAP3 In Module1	VAP4 In Module1	VAP5 In Module1	VAP6 In Module1	VAP7 In Module1

Head Goto 1 Page Tail Total Pages 0 Pages

Figure 6-1 AP Grouping Configuration Page

These parameters in **[Thin AP Configuration** > **AP Grouping]** page is described in details as following:

Parameter	Description
Restore AP Grouping	Customer could recover a AP grouping from a backup file.
Backup AP Grouping	Customer could save current AP grouping into a file for backup.
Group Name	Create a new group by specifying a mnemonic name for it.
Binding AP Common Profile to Thin AP	Select a configured **AP Common Profile** for current AP group.
Binding Wireless Basic Profile to 2.4G Module	For dual-band thin AP, select a configured **Wireless Basic Profile** for the 2.4GHz module.
Binding Wireless Basic Profile to 5G Module	For dual-band thin AP, select a configured **Wireless Basic Profile** for the 5GHz module.
VAP Profile Binding	One dual-band thin AP consists of 8 virtual APs for each radio module, the configured VAP profiles will be listed in the left window for selection. Select a VAP profile in left window and then click the **>>** button to bind it to the VAP in each radio module. Module 1 is the 2.4GHz module while Module 2 is the 5GHz module for a dual-band thin AP.
AP Group Profiles Binding List	Click the **Add** button to create a AP group with binding profiles and append it into the list. Existing groups can be modified by clicking the **Edit** button.

Click the **Add** button to append a new AP grouping entry to the group list.

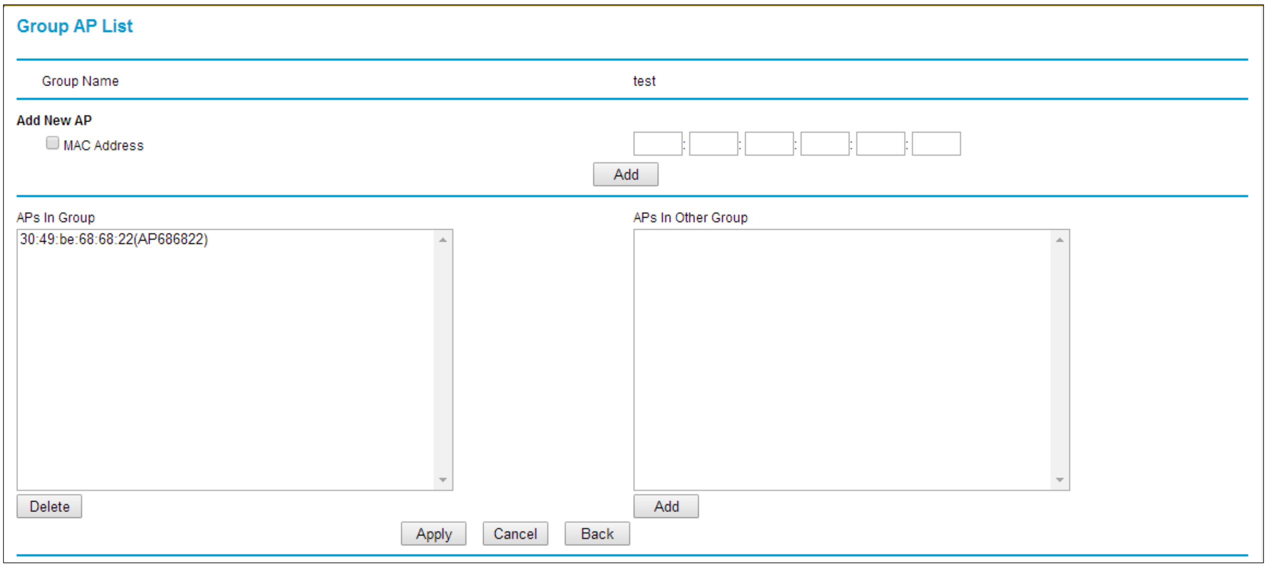
Click the **Apply** button to accept the changes.

Click the **Cancel** button to discard the changes.

Click the **Delete** button to remove the selected AP grouping entry from list.

Click the **Edit** button to modify the selected AP grouping entry.

Next after AP group creation, the thin APs should be added into the groups according to their attributes. Select one group in the list, click <**Edit**> button to enter the Adding AP in group page as following:



Group AP List

Group Name test

Add New AP

□ MAC Address

APs In Group

30:49:be:68:68:22(AP686822)

APs In Other Group

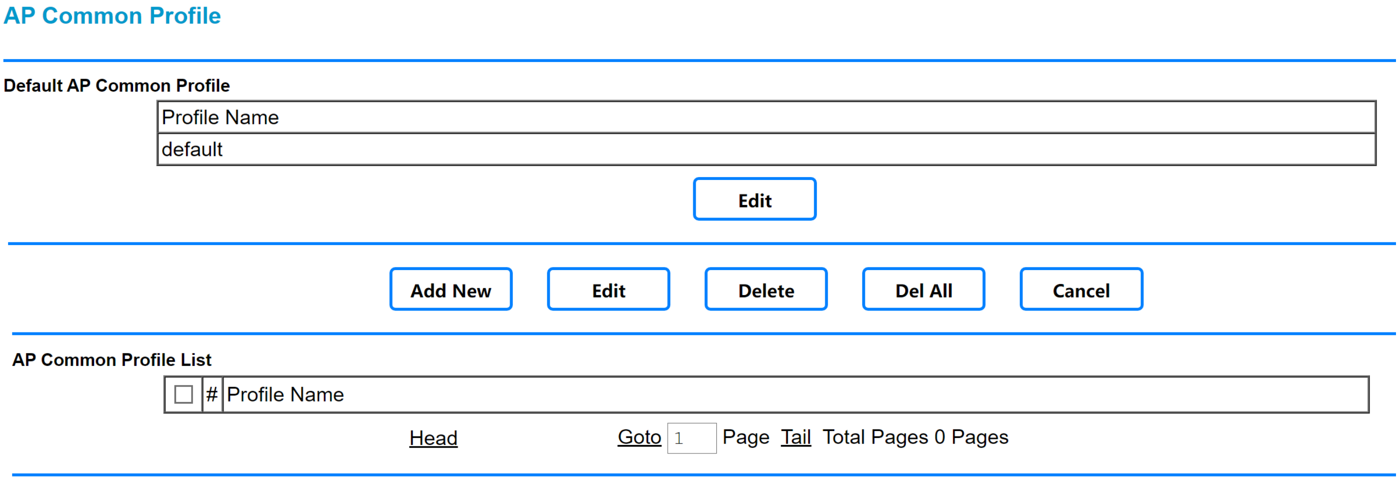
Figure 6-2 Adding Thin AP to Group

The customer can add a new thin AP to the current group by entering its MAC address, or click the <**Add**> button at the bottom of the right window to add the existing thin APs in other groups in the right window to the current group in the left window..

6.2. COMMON PROFILE

The **Common Profile** takes effect globally for all thin APs in the same AP group. Those general parameters and configurations of thin AP in the same group are collected into one configuration file called the common profile. There is already a preset common profile with default parameter settings in WLC; it can be modified to match the actual application of the customer. Customers can also create new common profiles for different AP groups.

Select **[Thin AP Configuration** > **Common Profile]** in the menu to enter the configuration page as following:



AP Common Profile

Default AP Common Profile

Profile Name
default

AP Common Profile List

□	#	Profile Name

Head Goto 1 Page Tail Total Pages 0 Pages

Figure 6-3 AP Common Profile Page (Entrance Page)

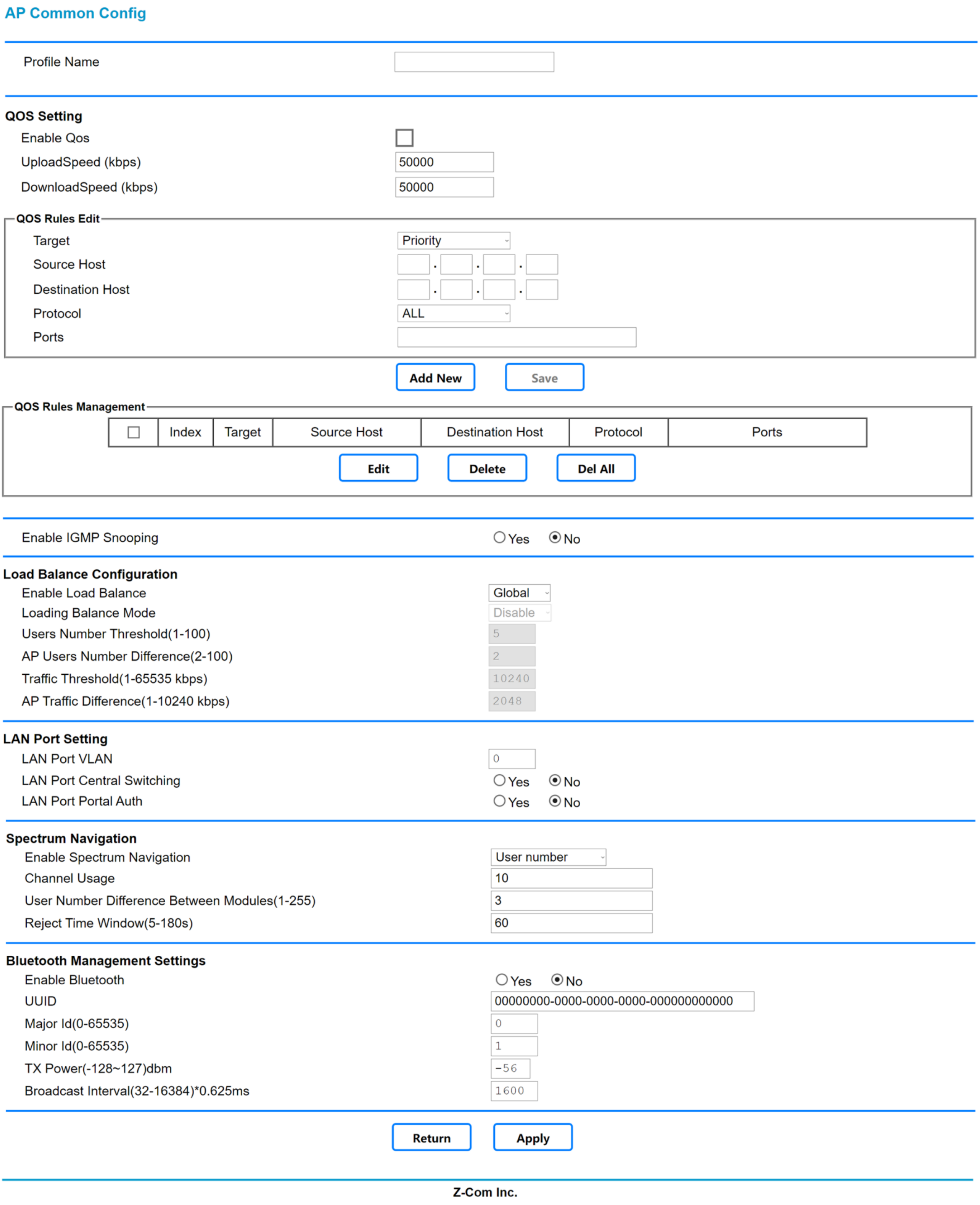
Click the **Edit** button to modify the default common profile.

Click the **Add New** button to create and edit a new common profile.

Click the **Delete** button to remove a profile from list.

Click the **Cancel** button to discard the modifications.

Click <**Add New**> or <**Edit**> button to enter the sub-page for profile creation and edition as following:



AP Common Config

Profile Name	

QOS Setting

Enable Qos	□
UploadSpeed (kbps)	50000
DownloadSpeed (kbps)	50000

QOS Rules Edit

Target	Priority
Source Host	. . .
Destination Host	. . .
Protocol	ALL
Ports	

QOS Rules Management

□	Index	Target	Source Host	Destination Host	Protocol	Ports

Enable IGMP Snooping	○ Yes ● No

Load Balance Configuration

Enable Load Balance	Global
Loading Balance Mode	Disable
Users Number Threshold(1-100)	5
AP Users Number Difference(2-100)	2
Traffic Threshold(1-65535 kbps)	10240
AP Traffic Difference(1-10240 kbps)	2048

LAN Port Setting

LAN Port VLAN	0
LAN Port Central Switching	○ Yes ● No
LAN Port Portal Auth	○ Yes ● No

Spectrum Navigation

Enable Spectrum Navigation	User number
Channel Usage	10
User Number Difference Between Modules(1-255)	3
Reject Time Window(5-180s)	60

Bluetooth Management Settings

Enable Bluetooth	○ Yes ● No
UUID	00000000-0000-0000-0000-000000000000
Major Id(0-65535)	0
Minor Id(0-65535)	1
TX Power(-128~127)dbm	-56
Broadcast Interval(32-16384)*0.625ms	1600

Figure 6-4 Create and Edit AP Common Profile Page

These parameters in **[Thin AP Configuration** > **Common Profile]** page is described in details as following:

Parameter	Description
Profile Name	Give a mnemonic name for the new profile to simplify the management of system configuration.
QoS Setting	**Basic Setting:** ▪ **Enable QoS:** This is a switch to open or disable QoS function in thin AP. ▪ **UploadSpeed(kbps):** The uplink rate of wireless clients associated to this thin AP is limited beneath this threshold. ▪ **DownloadSpeed(kbps):** The downlink rate of wireless clients associated to this thin AP is limited beneath this threshold. **QoS Rules Edit:** ▪ **Target:** This is the priority level for packet processing: o **Priority:** The highest priority. o **Express:** The higher priority. o **Normal:** The normal priority. o **Bulk:** The lower priority. ▪ **Source Host:** Entering a specific IP address to match the source IP address of the packet, and QoS rule will be applied to the matched packet. ▪ **Destination Host:** Entering a specific IP address to match the destination IP address of the packet, and QoS rule will be applied to the matched packet. ▪ **Protocol:** Select the protocol to match the packet for applying QoS rules: o **All:** QoS rule will be applied to all packets. o **TCP:** QoS rule will be applied to TCP packet. o **UDP:** QoS rule will be applied to UDP packet. o **ICMP:** QoS rule will be applied to ICMP packet. ▪ **Ports:** Entering the specific communication ports separated by commas to match the packet, and QoS rule will be applied to the matched packet. **QoS Rules Management:** New QoS rule can be added to the QoS Rules List by click <**Add**> button after configuration. In the QoS Rules list, customer can modify each rule by click <**Edit**> button; also can remove the selected rule or rules from list by click <**Delete**> or <**Delete All**> button.
Enable IGMP Snooping	Multicast members are created depending on IGMP, and the multicast packets are only forwarded to those members in multicast list. Enable IGMP monitoring here to obtain multicast members.
Load Balance Configuration	Load balancing is applied to thin APs to reasonably distribute user clients among each thin AP. The balancing policy is configured as follows: ▪ **Enable Load Balance** - Two options for selection: o **Global** - Selecting **Global** means that the load balance policy for current group is overlaid by that configured in [**AP Configuration** >

Parameter	Description
	Optimization], which is globally effective for thin APs in all groups. ○ **Group** - Selecting **Group** means that the load balance policy for current group configured here takes effect. ▪ **Balance Mode** - Selecting load balancing algorithm: ○ **Disable** - The load balancing policy will not be applied to the thin APs in current group. ○ **Users** - The load balancing policy is based on the number of user clients associated to the thin AP. ○ **Traffic** - The load balancing policy is based on the traffic pressure on the thin AP. ▪ **Users Number Threshold** - If the balance mode "**Users**" is selected set the maximum number of user clients allowed to associate with the thin AP here. When the number of associated user clients reaches this threshold, any new client attempting to associate with this thin AP will be rejected. ▪ **AP Users Number Difference** - If the balance mode "**Users**" is selected, set the maximum difference in the number of user clients allowed between two thin APs here. When the difference touches this threshold, any new client attempting to associate with the AP who has more users will be rejected. ▪ **Traffic Threshold** - If the balance mode "**Traffic**" is selected, set the maximum throughput threshold allowed in a thin AP here. When the traffic in a thin AP reaches this threshold, any new client attempting to associate with this thin AP will be rejected. ▪ **AP Traffic Difference** - If the balance mode "**Traffic**" is selected, set the maximum throughput difference allowed between two thin APs here. When the traffic throughput difference reaches this threshold, any new client attempting to associate with the AP who has heavier traffic will be rejected.
LAN Port Setting	Thin AP has more than one Ethernet ports, one is for WLAN connecting to WLC, and another is for LAN using. The LAN port of thin AP is configured here. ▪ **LAN Port VLAN** - Allocate a VLAN to this LAN port of thin AP if the LAN port connects to a device configured with VLAN. ▪ **LAN Port Central Switching** - The traffic passing through this LAN port of the thin AP can also be concentrated to WLC for centralized forwarding, just like wireless client traffic. ▪ **LAN Port Portal Auth** - The host connect to this LAN port of the thin AP also will be authenticated by captive portal, just like a wireless client.
Spectrum Navigation	The so-called “Spectrum Navigation” actually stands for the load balance between two radio modules in the dual-band thin AP. ▪ **Enable Spectrum Navigation** - Turn on the spectrum navigation function, and balance the load between the radio modules according to the following strategy: ○ **Disable** - No load balance for this AP group. ○ **Users Number** - Choose the difference in the number of users as the strategy to balance the load between two radio modules in the

Parameter	Description
	dual-band thin AP. o **Channel Loading** - Select channel busyness as the strategy to balance the load of the two radio modules in the dual-band thin AP. ▪ **Channel Usage** - If **Channel Loading** is selected for "Enable Spectrum Navigation", set the channel usage rate threshold here to indicate the channel busyness and idleness. When the channel usage of the radio module touches this threshold, any new client attempting to associate with this radio module will be rejected. ▪ **Users Number Difference Between Modules** - If **Users Number** is selected for "Enable Spectrum Navigation", set the difference threshold in the number of users between two radio modules here. When the difference touches this threshold, any new client attempting to associate with the radio module who has more users will be rejected. ▪ **Reject Time Window** - If the user client is rejected by the radio module due to the load balancing policy, the module will no longer accept association requests from the rejected client until the rejection time window is shifted off.
Bluetooth Management Settings	This function is for the specific AP to support Apple ***iBeacon***, which is the Apple's implementation of Bluetooth low-energy (BLE) wireless technology used to create a different way of providing location-based information and services to iPhones and other iOS devices. ▪ **Enable Bluetooth** - This switch opens the iBeacon Bluetooth function for thin AP. ▪ **UUID** - This is Bluetooth unique service ID for thin AP which will be broadcast in beacon. ▪ **Major ID** - This is an ID of iBeacon. ▪ **Minor ID** - This is an ID of iBeacon. ▪ **TX Power (-128~ 127)dBm** - The radio transmit power of iBeacon's beacon broadcast. ▪ **Broadcast Interval (32~16384)*0.625ms** - The radio transmit interval of iBeacon's beacon broadcast.

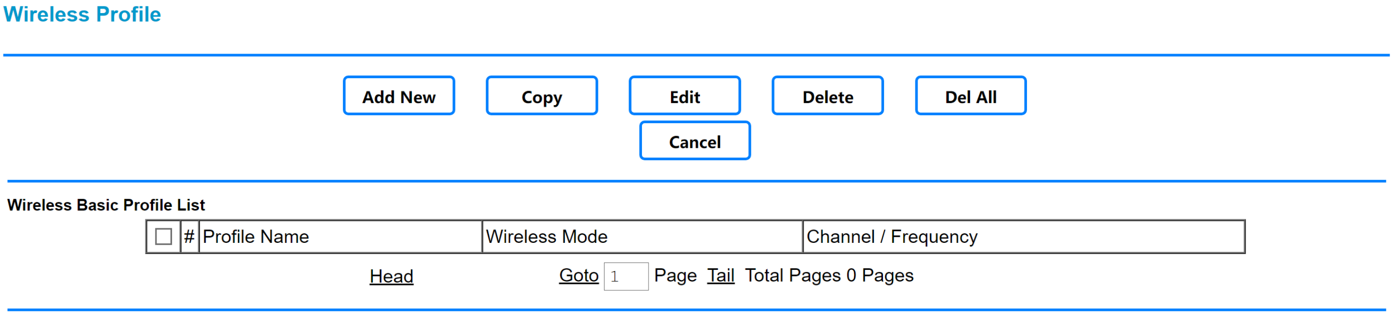
Click the **Apply** button to accept the changes.

Click the **Return** button to discard the changes and back to the previous page.

6.3. Wireless Profile

The **Wireless Profile** is a set of wireless parameters that act on the air interface side of the thin AP. These parameters in the wireless profile are strictly defined by the IEEE-802.11 specification, which is the most important part for the wireless client to associate with the access point. Before configuring these wireless parameters, customer needs more knowledge about Wi-Fi systems.

Select **[Thin AP Configuration** > **Wireless Profile]** in the menu to enter the configuration page as following:



Wireless Basic Profile List

□	#	Profile Name	Wireless Mode	Channel / Frequency

Head Goto 1 Page Tail Total Pages 0 Pages

Figure 6-5 Wireless Profile Entrance Page

There is already a preset wireless profile with default parameter settings in WLC; it can be modified to meet with the customer's practical application. Also customer can create new wireless profiles for different AP groups.

Click the **Edit** button to modify an existing profile in the list.

Click the **Select All** button to select all profiles in the list.

Click the **Add New** button to append a new profile to the list.

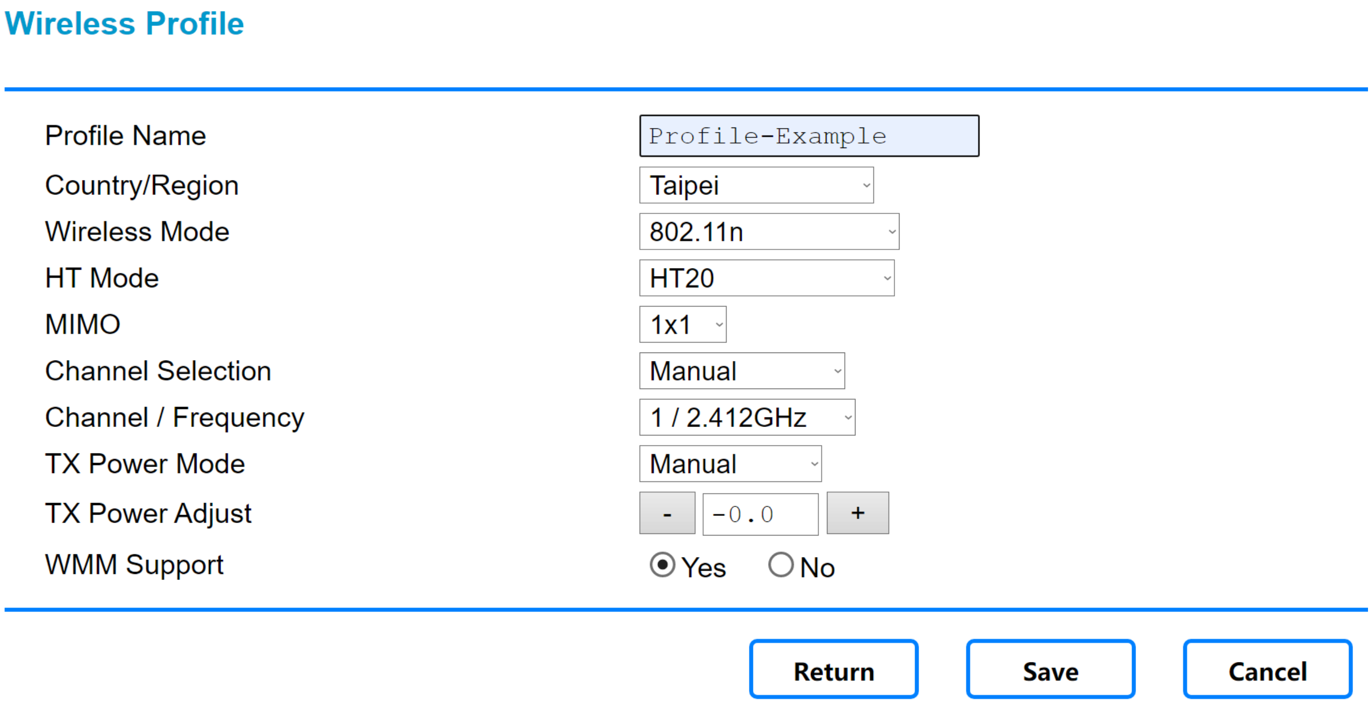
Click the **Copy** button to copy an existing profile in the list.

Click the **Delete** button to remove a profile.

Click the **Del All** button to remove all profiles from the list.

Click the **Cancel** button to discard the modifications.

Click the <**Add New**> or <**Edit**> button to access the Wireless Profile Configuration page as following:



Profile Name	Profile-Example
Country/Region	Taipei
Wireless Mode	802.11n
HT Mode	HT20
MIMO	1x1
Channel Selection	Manual
Channel / Frequency	1 / 2.412GHz
TX Power Mode	Manual
TX Power Adjust	- -0.0 +
WMM Support	● Yes ○ No

Figure 6-6 Wireless Profile Configuration Page

These parameters in **[Thin AP Configuration** > **Wireless Profile]** page is described in details as following:

Parameter	Description
Profile Name	Give a mnemonic name for the new profile to simplify the management of system configuration.
Country/Region	Select the Country/Region code for where the Wi-Fi system is deployed. The authorized Wi-Fi channels vary in different country/region because of different law regulation.
Wireless Mode	Select an IEEE 802.11 specification for the thin AP. The available specifications are: ▪ **11n** - Thin AP operates under the 802.11n specification in the 2.4GHz band. The air interface data rate is 600Mbps. ▪ **11ac** - Thin AP operates under the 802.11ac specification in the 5GHz band. The air interface data rate is 1Gbps. ▪ **11ax(2.4GHz)** - The radio module in dual-band AP operates under the IEEE 802.11ax specification in the 2.4GHz band. The air interface data rate is 10Gbps. ▪ **11ax(5GHz)** - The radio module in dual-band AP operates under the IEEE 802.11ax specification in the 5GHz band. The air interface data rate is 10Gbps.
HT Mode	HT (High Throughput) is a bandwidth aggregation technology derived from 802.11n. The latest 802.11 specification supports multiple HT modes, including HT20, HT40, HT80 and even HT160, which are integer multiples of the 20MHz bandwidth. The larger the suffix number of HT, the higher the data rate of the air interface.
MIMO	Multiple input multiple output technology, which uses independent Tx and Rx paths in the air to achieve spatial stream multiplexing. The maximum number of MIMO for 802.11n is 2, for 802.11ac is 4, and for 802.11ax is 8.
Channel Selection	Configure the channel selection policy of the thin AP: ▪ **Manual** - Set the operating channel and band manually for current AP group. ▪ **Auto Channel** - The operating channel and band of the thin AP in current group will be automatically selected according to the policy configured in [**AP Configuration** > **Optimization**] which is globally effective to the thin APs in all groups.
Channel / Frequency	If **Manual** mode is selected in above “Channel Selection”, then manually set its operating channel and corresponding frequency here.
TX Power Mode	Configure the radio transmit (TX) power adjustment policy of the thin AP: ▪ **Manual** - Manually set the radio TX power for the thin AP in current group. ▪ **Auto Power** - The transmit power of the thin AP in current group will be adjusted automatically according to the policy configured in [**AP Configuration** > **Optimization**] which is globally effective to the thin APs in all groups.

Parameter	Description
TX Power Adjust	If **Manual** mode is selected in above "TX Power Mode", then manually click on the add (**+**) or subtract (**-**) button here to increase or decrease the transmit power. The adjustment step value is 0.5 dBm one time.

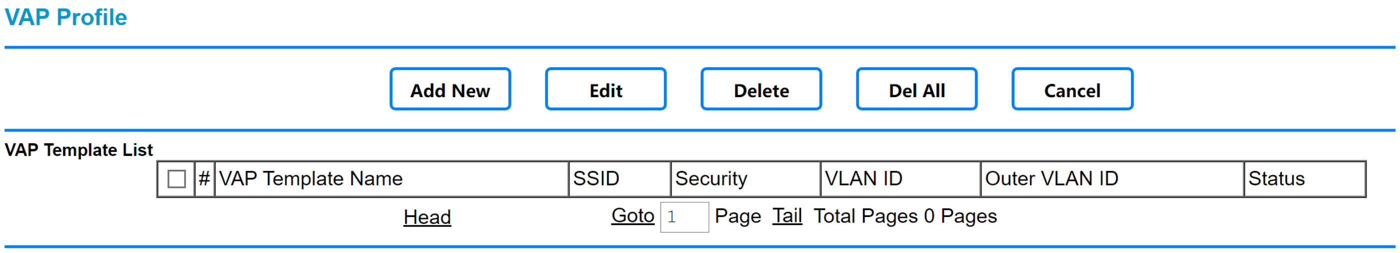
Click the **Apply** button to accept the changes made.

Click the **Cancel** button to discard the changes made.

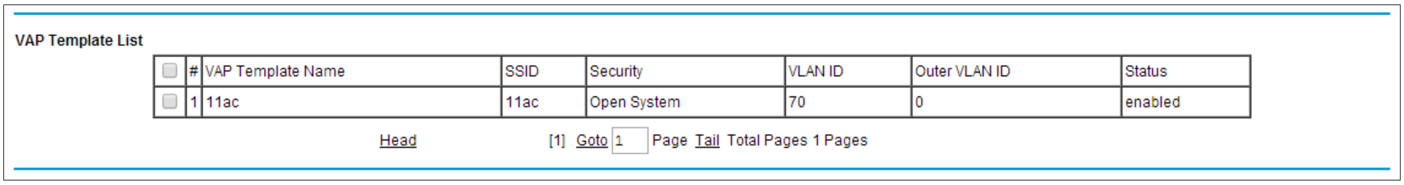
6.4. VAP PROFILE

A physical thin AP can be logically divided into up to 8 virtual APs identified by different SSID, and these virtual APs share the same **Common Profile** and **Wireless Profile**. However, each virtual AP may have some parameter settings independent of each other; therefore, a specific virtual AP configuration file called a **VAP Profile** must be configured for different virtual APs.

Select **[Thin AP Configuration** > **VAP Profile]** in the menu to enter the configuration page as following:



□	#	VAP Template Name	SSID	Security	VLAN ID	Outer VLAN ID	Status



□	#	VAP Template Name	SSID	Security	VLAN ID	Outer VLAN ID	Status
□	1	11ac	11ac	Open System	70	0	enabled

Figure 6-7 VAP Profile Entrance Page

Click the **Cancel** button to discard the changes.

Click the **Add New** button to add a new profile.

Click the **Backup** button to save the profile to the file in local PC.

Click the **Delete** button to remove a profile.

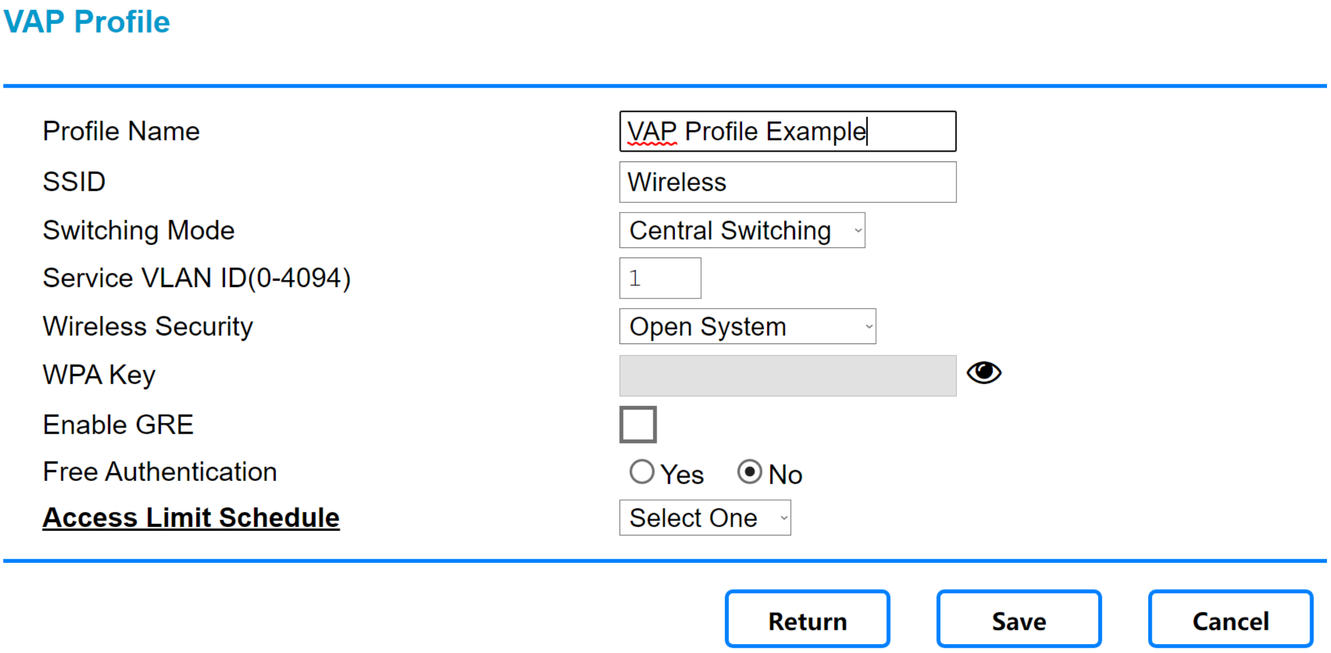
Click the **Delete All** button to remove all profiles from the list.

Click the **Edit** button to modify an existing profile in the list.

Click the **Restore** button to recover a profile from the file in the local PC.

Click the **Select All** button to select all profiles in the list.

Click the <**Add New**> or <**Edit**> button to access the VAP Profile Configuration page as following:



VAP Profile

Profile Name	VAP Profile Example
SSID	Wireless
Switching Mode	Central Switching
Service VLAN ID(0-4094)	1
Wireless Security	Open System
WPA Key	
Enable GRE	□
Free Authentication	○ Yes ● No
Access Limit Schedule	Select One

Figure 6-8 VAP Profile Configuration Page

These parameters in **[Thin AP Configuration** > **VAP Profile]** page are described in details as following:

Parameter	Description
Profile Name	Give a mnemonic name for the new profile to simplify the management of system configuration.
SSID	Specify a SSID to identify current virtual AP.
Switching Mode	This mode selection is used to tell the Virtual AP how to forward the data traffic coming from the associated user clients: ▪ **Central Switching:** The user data traffic is ***concentrated*** to WLC through a data tunnel, and then ***forwarded*** to the Internet. ▪ **Local Switching:** The user data traffic bypasses WLC and is forwarded directly from the thin AP to the Internet.
Service VLAN	Assign a service VLAN ID for the virtual AP according to its SSID requirement. Note, that the VLAN must be an available VLAN created in **[Network > VLAN Creation]**.
Wireless Security	There are three types of wireless security provided for virtual AP to select: ▪ **Open System:** When the wireless client associates to this VAP, only the SSID is used for authentication, and authentication does not require encryption. ▪ **WPA2-PSK:** When the wireless client associates to this VAP, it will be authenticated by WPA2, and the authentication will be encrypted by the preset PSK key. ▪ **WPA2&Radius:** When the wireless client associates to this VAP, it will be authenticated by WPA2, and the authentication will be encrypted using a temporary key generated by the Radius server instead of a preset key such as WPA2-PSK.
WPA Key	If **WPA2-PSK** security is selected for this virtual AP, you must enter the preset PSK

Parameter	Description
	key in the form of a string here.
Enable GRE	If the Wi-Fi network is divided into different virtual network operators and identified by different SSIDs, each operator has its own core network for its wireless user authentication. This requires the user service data to be forwarded to different core networks connected in different northbound ports through the GRE tunnels. In such a Wi-Fi network, the VAP must be bound to a GRE tunnel by enabling the GRE function for it here.
Free Webauth	If ***Web Authentication*** is enabled for the current Wi-Fi system, the virtual AP can turn on this "***Free Webauth***" switch to make the user clients associated to it get free from Web authentication. The selection is **Yes** or **No**.
Access Limit Schedule	The Access Limit Schedule is used to prohibit the user clients from accessing Wi-Fi system within the specific time period. This is the hyperlink directing to [**Authentication > Access Time Control**] for customers to configure the time plan table.

Click the **Save** button to accept the changes.

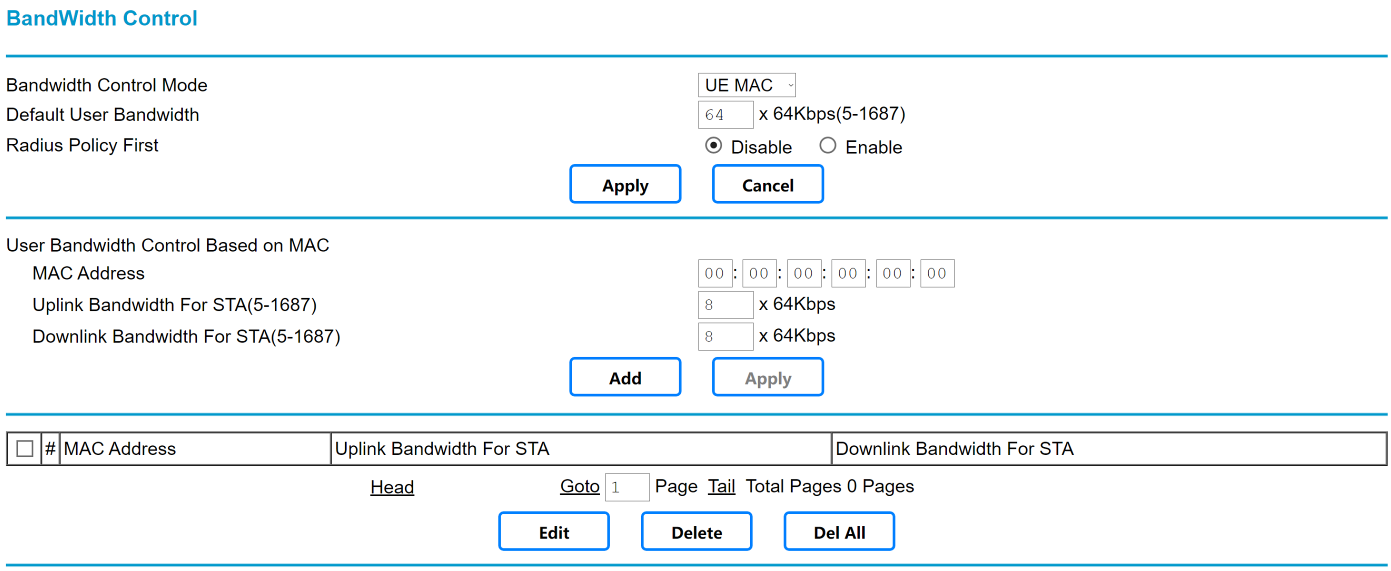
Click the **Return** button to discard the changes and back to the previous page.

Click the **Cancel** button to discard the changes.

6.5. Bandwidth Control

In some application, there are required to limit the bandwidth of the specific user clients either for uplink or downlink. The specific user client is identified by its MAC address.

Select **[Thin AP Configuration** > **Bandwidth Control]** in the menu to enter the configuration page as following:



BandWidth Control

Bandwidth Control Mode: UE MAC
Default User Bandwidth: 64 x 64Kbps(5-1687)
Radius Policy First: ● Disable ○ Enable

Apply Cancel

User Bandwidth Control Based on MAC
MAC Address: 00 : 00 : 00 : 00 : 00 : 00
Uplink Bandwidth For STA(5-1687): 8 x 64Kbps
Downlink Bandwidth For STA(5-1687): 8 x 64Kbps

Add Apply

□	#	MAC Address	Uplink Bandwidth For STA	Downlink Bandwidth For STA

Head Goto 1 Page Tail Total Pages 0 Pages

Edit Delete Del All

Figure 6-9 Bandwidth Control Configuration Page

These parameters in **[Thin AP Configuration** > **Bandwidth Control]** page are described in details as following:

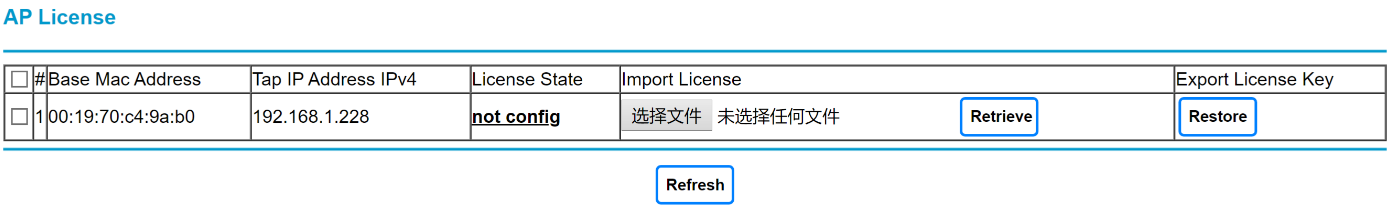
Parameter	Description
Bandwidth Control Mode	Select **UE MAC**, i.e., using the MAC address of user endpoint as the client identifier to control its bandwidth.
Default User Bandwidth	If “Bandwidth Control Mode” is enabled with **UE MAC**, each user client will reserve a default bandwidth of 64×64kbps (i.e., 4Mbps) for uplink and downlink. This default value can be changed by customer, click <**Apply**> button to accept this change.
Radius Policy First	If this switch is enabled, the preferred policy of bandwidth control is from Radius, otherwise, is from here that locally configured.
User Bandwidth Control Based on MAC	Here configuring the local policy of bandwidth control based on user client MAC: ▪ **MAC Address:** Enter the MAC address of user client to which you want to apply the bandwidth control. ▪ **Uplink Bandwidth:** The data transmitting bandwidth of the user client corresponding to this MAC address. ▪ **Downlink Bandwidth:** The data receiving bandwidth of the user client corresponding to this MAC address.
Bandwidth Control Policy List	▪ Click <**Add**> button to append this new policy to the list.

Click the **Edit** button to modify the policy in the list.

6.6. AP LICENSE

WLC uses AP License file to control the capacity of thin AP in Wi-Fi system. If the WLC has been installed on-site, the AP License file must be imported to the WLC immediately; otherwise, many thin APs cannot access to WLC except the default few. The AP License file is created and delivered by the WLC vendor.

Select **[Thin AP Configuration** > **AP License]** in the menu to enter the configuration page as following:



AP License

□	#	Base Mac Address	Tap IP Address IPv4	License State	Import License	Export License Key
□	1	00:19:70:c4:9a:b0	192.168.1.228	not config	选择文件 未选择任何文件 Retrieve	Restore

Figure 6-10 Bandwidth Control Configuration Page

Click the <**Browse** > button to select the AP License in the directory of local host, then upload it into WLC.

These parameters in **[Thin AP Configuration** > **AP License]** page is described in details as following:

Parameter	Description

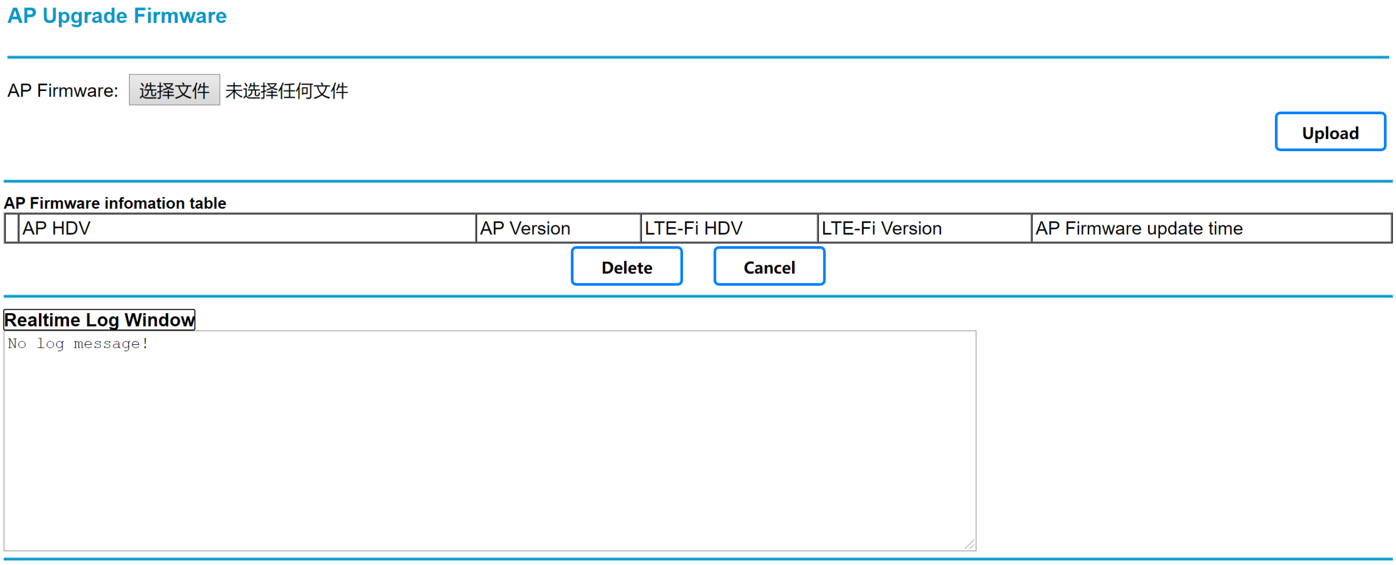
Parameter	Description
Base MAC Address	The MAC address of current WLC management port.
TAP IP Address IPv4	The IPv4 address of current WLC WLAN port (i.e., thin AP access port).
License State	If AP License is not imported yet, the state here is “**not config**”.
Import License	A button to perform the operation of importing the AP License file from local host directory.
Export License	A button to perform the operation of exporting the AP License file to local host directory.

Click the **Refresh** button to update the AP License state.

6.7. AP FW UPGRADE

In the Wi-Fi system with WLC, the thin AP can upgrade its firmware through WLC centrally, instead of upgrading one at a time. It can be done by entering **[Thin AP Configuration> AP Firmware Upgrade]**.

Select **[Thin AP Configuration** > **AP FW Upgrade]** in the menu to enter the configuration page as following:



AP Upgrade Firmware

AP Firmware: 选择文件 未选择任何文件

AP Firmware infomation table

	AP HDV	AP Version	LTE-Fi HDV	LTE-Fi Version	AP Firmware update time

Realtime Log Window

```
No log message!
```

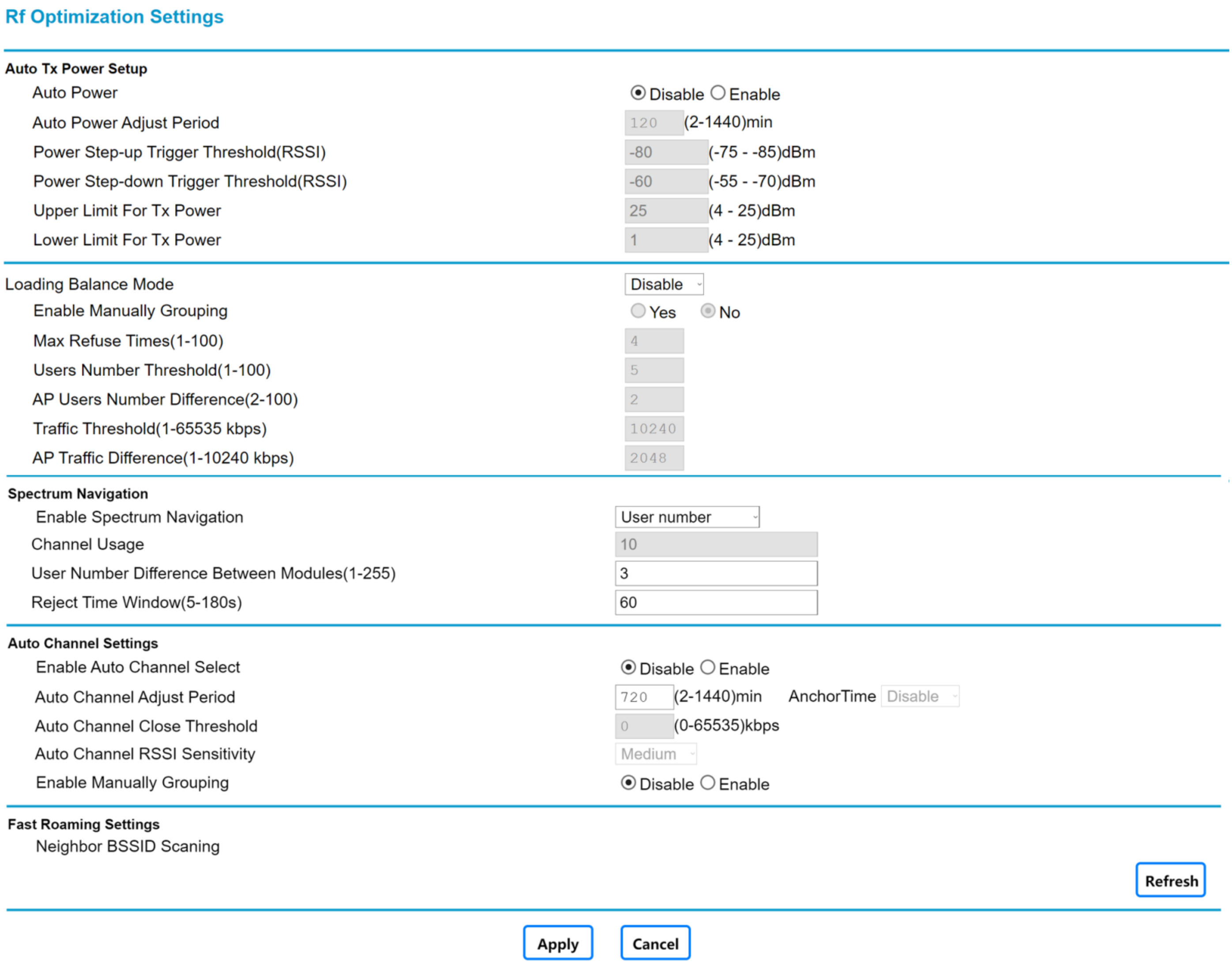
Figure 6-11 AP Firmware Upgrade Page

Click <**Browse**> button to select the new version of thin AP firmware from local host directory, then click <**Upload**> button to load the new version firmware to WLC to inform the thin APs for upgrading. The upgrading information of each thin AP will be displayed in the **Realtime Log Window**.

6.8. OPTIMIZATION

In most practical applications, the environment variation results in Wi-Fi system performance degradation, therefore, the parameters optimization has to be performed to improve it.

Select **[Thin AP Configuration** > **Optimization]** in the menu to enter the configuration page as following:



Rf Optimization Settings

Auto Tx Power Setup

Auto Power	● Disable ○ Enable
Auto Power Adjust Period	120 (2-1440)min
Power Step-up Trigger Threshold(RSSI)	-80 (-75 - -85)dBm
Power Step-down Trigger Threshold(RSSI)	-60 (-55 - -70)dBm
Upper Limit For Tx Power	25 (4 - 25)dBm
Lower Limit For Tx Power	1 (4 - 25)dBm
Loading Balance Mode	Disable
Enable Manually Grouping	○ Yes ● No
Max Refuse Times(1-100)	4
Users Number Threshold(1-100)	5
AP Users Number Difference(2-100)	2
Traffic Threshold(1-65535 kbps)	10240
AP Traffic Difference(1-10240 kbps)	2048

Spectrum Navigation

Enable Spectrum Navigation	User number
Channel Usage	10
User Number Difference Between Modules(1-255)	3
Reject Time Window(5-180s)	60

Auto Channel Settings

Enable Auto Channel Select	● Disable ○ Enable
Auto Channel Adjust Period	720 (2-1440)min AnchorTime Disable
Auto Channel Close Threshold	0 (0-65535)kbps
Auto Channel RSSI Sensitivity	Medium
Enable Manually Grouping	● Disable ○ Enable

Fast Roaming Settings

Neighbor BSSID Scaning

Figure 6-12 AP Optimization Configuration Page

These parameters in **[Thin AP Configuration** > **Optimization]** page is described in details as following:

Parameter	Description
Auto TX Power Setup	The Auto Tx Power policy configured here will globally affect thin APs in all group by overlaying the thin AP its own auto Tx power policy configured in wireless profile as long as the "Tx Power Mode" in the wireless profile is enabled by the **Auto** option: ▪ **Auto Power:** This switch is opened to enable the function of auto Tx power for all thin APs. ▪ **Auto Power Adjust Period:** The automatic adjustment of transmit power is a dynamic process varied with environment which performs intermittently. The time interval for adjustment is set here. The value is neither too short nor too long, both will degrade system performance. ▪ **Power Step-up Trigger Threshold (RSSI):** This is the threshold of the

Parameter	Description
	signal strength (dBm) of the user client on the AP side. If the signal strength of the user client is too weak and below this threshold, the AP will start to increase its Tx power. ▪ **Power Step-down Trigger Threshold (RSSI):** This is the threshold of the signal strength (dBm) of the user client on the AP side. If the signal strength of the user client is too strong and above this threshold, the AP will start to decrease its Tx power. ▪ **Upper Limit of Tx Power:** This is the maximum Tx power allowed by the thin AP, and the Tx power cannot be adjusted higher than it. ▪ **Lower Limit of Tx Power:** This is the minimum Tx power allowed by the thin AP, and the Tx power cannot be adjusted lower than it.
Load Balance	The load balance policy configured here will globally affect thin APs in all group by overlaying the thin AP its own load balance policy configured in common profile as long as the "Load Balancing" in the common profile is enabled by the **Global** option: ▪ **Load Balancing Mode:** Three modes are provided for selection: ○ **Disable:** No global load balancing function needed.. ○ **Users:** The load balancing policy is based on the number of user clients associated to the thin AP. ○ **Traffic:** The load balancing policy is based on the user traffic pressure in the thin AP. ▪ **Enable Manually Grouping** -A thin AP usually scans neighbor APs to be automatically grouped. If manual grouping is selected, the thin APs which are using the same configuration profile should be grouped in the same group. AP grouping is a good method for accelerating the load balance process. ▪ **Max Refuse Time (1-100)**- If load balancing is enabled, once an user client is kicked out due to load balancing requirement, then its re-association to current thin AP will be refused for a given time. This is the refuse time. ▪ **Users Number Threshold** - If the balance mode "**Users**" is selected set the maximum number of user clients allowed to associate with the thin AP here. When the number of associated user clients reaches this threshold, any new client attempting to associate with this thin AP will be rejected. ▪ **AP Users Number Difference** - If the balance mode "**Users**" is selected, set the maximum difference in the number of user clients allowed between two thin APs here. When the difference touches this threshold, any new client attempting to associate with the AP who has more users will be rejected. ▪ **Traffic Threshold** - If the balance mode "**Traffic**" is selected, set the maximum throughput threshold allowed in a thin AP here. When the traffic in a thin AP reaches this threshold, any new client attempting to associate with this thin AP will be rejected.

Parameter	Description
	▪ **AP Traffic Difference** - If the balance mode "**Traffic**" is selected, set the maximum throughput difference allowed between two thin APs here. When the traffic throughput difference reaches this threshold, any new client attempting to associate with the AP who has heavier traffic will be rejected.
Spectrum Navigation	The so called "Spectrum Navigation" actually refers to the load balance between two radio modules in the dual-band thin AP. ▪ **Enable Spectrum Navigation** - Open the spectrum navigation function and balance the loading between radio modules followed by the policy below: o **Disable** - No load balance for this AP group. o **Users Number** - Select the users number difference as the policy to balance the loading of two radio modules in dual-band thin AP. o **Channel Loading** - Select the channel busyness as the policy to balance the loading of two radio modules in dual-band thin AP. ▪ **Channel Usage** - If **Channel Loading** is selected in "Enable Spectrum Navigation", here to set the channel usage rate threshold to indicate the channel busyness and idleness. When the channel usage of radio module touches this threshold, any new client attempting to associate with this radio module will be rejected. ▪ **Users Number Difference Between Modules** - If **Users Number** is selected in "Enable Spectrum Navigation", here to set the users number difference threshold between two radio modules. When the difference number touches this threshold, any new client attempting to associate with the radio module who has more users will be rejected. ▪ **Reject Time Window** - If a user client is rejected by the radio module due to load balancing, this module will not accept the association request from the rejected client anymore until the reject time window shifted off.
Auto Channel Settings	The Auto Channel policy configured here will globally affect thin APs in all group by overlaying the thin AP its own auto channel selection policy configured in wireless profile as long as the "Channel Selection" mode in the wireless profile is enabled by the **Auto Channel** option: ▪ **Enable Auto Channel Select:** Click the radio button to enable auto channel function for thin AP. ▪ **Auto Channel Adjust Period:** Thin AP switching its operating channel automatically is a dynamic process variation with the RF environment, so it performs intermittently. The time interval of channel switching is set here. The value is neither too short nor too long, both will degrade system performance. ▪ **Anchor Time:** This is used to specify the time in a day when the automatic channel function works. At other times, the automatic channel function remains inactive. ▪ **Auto Channel Close Threshold:** During automatic channel switching,

Parameter	Description
	the performance of the thin AP is severely degraded. Therefore, in order to prevent performance degradation, a traffic threshold must be set for the thin AP. Once the traffic on a thin AP touches the threshold, the auto channel function will stop. ▪ **Auto Channel RSSI Sensitivity:** Thin AP measures the signal strength of neighboring AP, if it is higher than the threshold, it triggers the channel switching. The triggering level can be set by **High**, **Medium**, and **Low**. ▪ **Enable Manually Grouping** - Thin AP usually scans neighbor APs to be automatically grouped. If manual grouping is selected, the thin APs which are using the same configuration profile should be grouped in the same group. AP grouping is a good method for accelerating the load balance process.
Fast Roaming Settings	This is required by 802.11r specification, i.e., thin AP scans RF environment to find neighboring APs and synchronizes the BSSIDs each other. Click <**Refresh**> button to do once.

Click the **Apply** button to accept the changes.

Click the **Cancel** button to discard the changes.

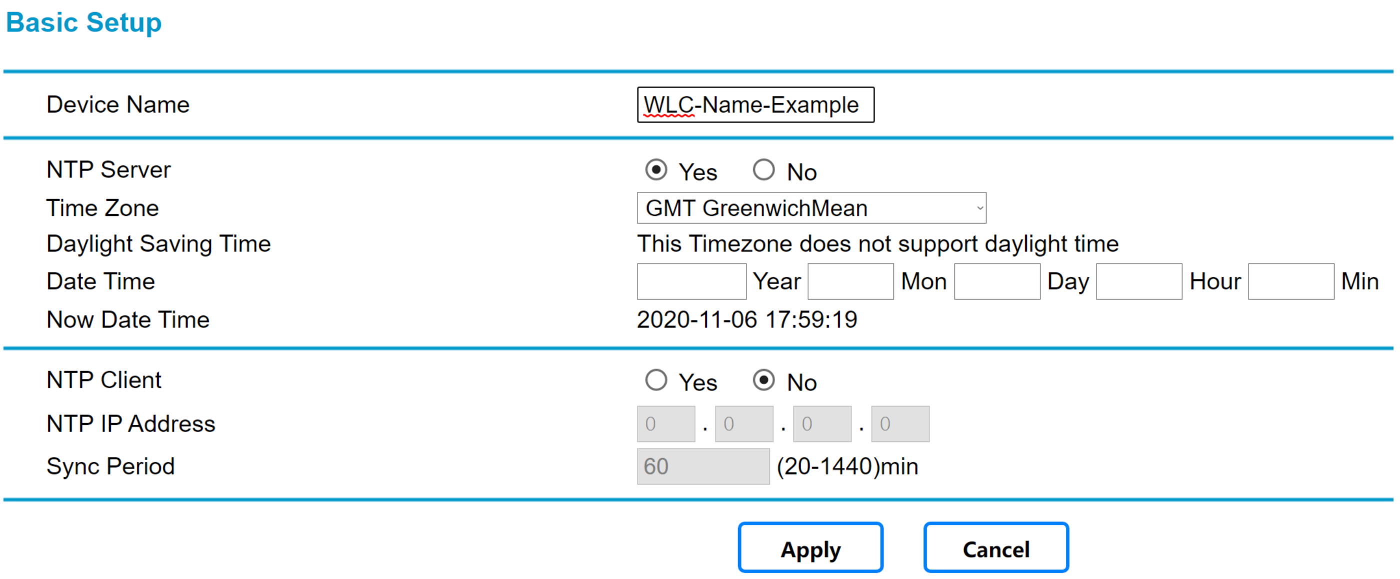
Chapter 7. WLC Configuration

As the gateway, the WLC is responsible for accessing front-end devices in the operator's core network or public data network. It is important to ensure the security of the core network and protect it from intrusion by illegal devices. **Access Control** is the barrier established on the WLC for accepting trusted devices and rejecting untrusted devices.

7.1. TimeZone and Date

WLC is deployed in site, and then the local settings, such as Country/Region code and time zone etc., should have been properly configured. Here is the local setting about time zone and date time for WLC deployment.

Select **[WLC Configuration** > **TimeZone and Date]** in the menu to enter the configuration page as following:



Basic Setup

Device Name	WLC-Name-Example
NTP Server	● Yes ○ No
Time Zone	GMT GreenwichMean
Daylight Saving Time	This Timezone does not support daylight time
Date Time	Year Mon Day Hour Min
Now Date Time	2020-11-06 17:59:19
NTP Client	○ Yes ● No
NTP IP Address	0 . 0 . 0 . 0
Sync Period	60 (20-1440)min

Figure 7-1 TimeZone and Datetime Configuration Page

These parameters in **[WLC Configuration** > **TimeZone and Date]** page is described in details as following:

Parameter	Description
Device Name	Assign a literal name for this WLC equipment in order to be mnemonic.
NTP Server	Thin AP cannot maintain the date time on board when power off; therefore it needs a common source for time service. WLC can be such a time source; its built-in NTP server can provide all thin APs with time synchronization service.
Time Zone	Select the proper time zone for where the WLC is deployed.
Daylight Saving Time	Some countries and regions use daylight saving time in summer, here configure it.
Date Time	Manually set the date time here for WLC.
Now Date Time	Display current date time in WLC.
NTP Client	WLC as the NTP server providing thin AP with time service, its own date time also needs to be calibrated by a precise time source, thus, it is also a NTP client to the precise public NTP server.

Parameter	Description
NTP IP Address	The IP address of the public precise NTP server.
Sync Period	WLC as the client of a public precise NTP server has to periodically synchronize its date time, here configure the time interval of synchronization.

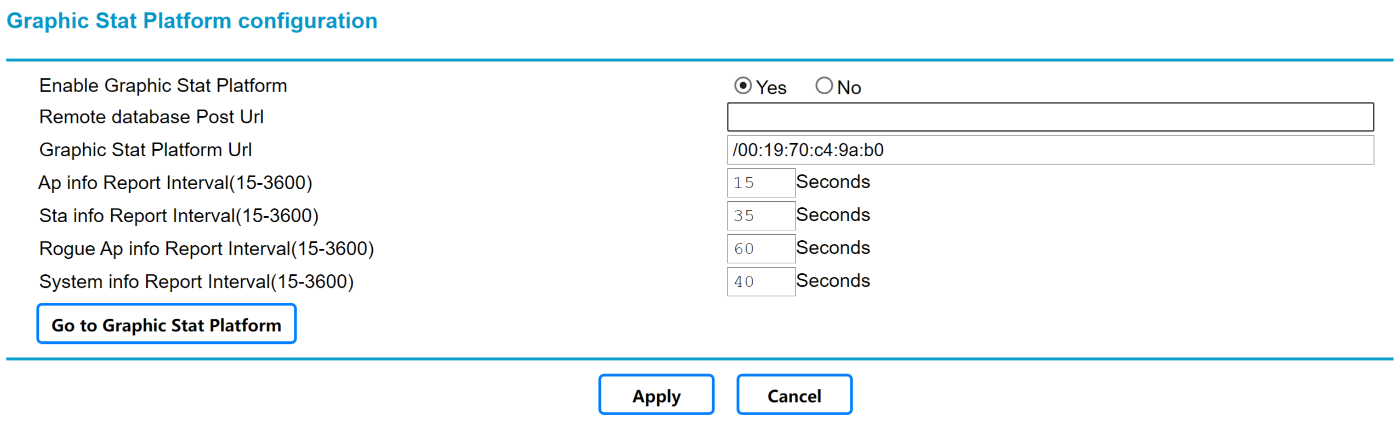
Click the **Apply** button to accept the changes.

Click the **Cancel** button to discard the changes.

7.2. GRAPHIC STAT PLATFORM

Hyperion series WLC supports 3'rd party remote graphic statistics platform, i.e., the WLC periodically sends statistics data and status information of both user clients and thin APs to remote statistics platform in ***Rest API*** protocol for graphically displaying.

Select **[WLC Configuration** > **Graphic Stat Platform]** in the menu to enter the configuration page as following:



Graphic Stat Platform configuration

Enable Graphic Stat Platform	● Yes ○ No
Remote database Post Url	
Graphic Stat Platform Url	/00:19:70:c4:9a:b0
Ap info Report Interval(15-3600)	15 Seconds
Sta info Report Interval(15-3600)	35 Seconds
Rogue Ap info Report Interval(15-3600)	60 Seconds
System info Report Interval(15-3600)	40 Seconds

Figure 7-2 Graphic Statistics Platform Configuration Page

These parameters in **[WLC Configuration** > **Graphic Stat Platform]** page is described in details as following:

Parameter	Description
Enable Graphic Stat Platform	This switch opens the ***Rest API*** function for remote graphic statistics platform.
Remote Data Base Post URL	Data is put into database by POST method, while the database is in remote platform; therefore, WLC needs to know the URL to remotely post Data.
Graphic Stat Platform URL	The Rest API protocol needs to know the remote platform URL for remotely communication.
AP Info Report interval (15-3600)	WLC periodically sends the APs information to remote graphic statistics platform for displaying; here configure the time interval for sending.
STA Info Report interval (15-3600)	WLC periodically sends the user clients information to remote graphic statistics platform for displaying; here configure the time interval for sending.
Rogue AP Info Report interval	WLC periodically sends the Rogue APs information to remote graphic

Parameter	Description
(15-3600)	statistics platform for displaying; here configure the time interval for sending.
System Info Report interval (15-3600)	WLC periodically sends the system information to remote graphic statistics platform for displaying; here configure the time interval for sending.

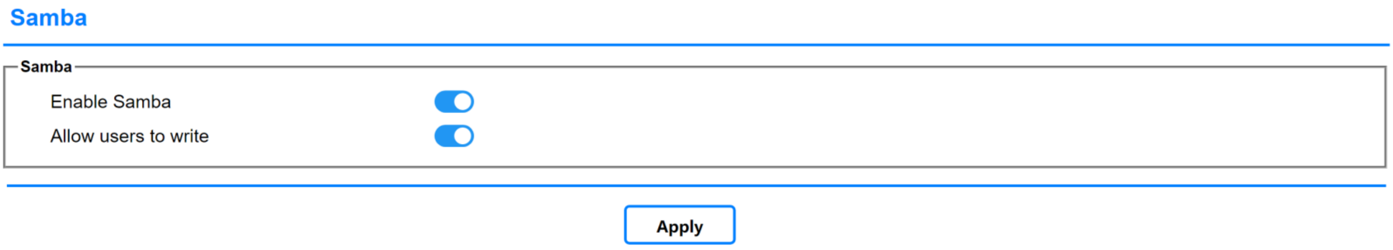
Click the **Apply** button to accept the changes.

Click the **Cancel** button to discard the changes.

7.3. SAMBA

Samba is the Linux network neighbor technology which makes local hard disk spaces sharing with other devices. For example, in the application of video surveillance, WLC can share its hard disk spaces with NAS.

Select **[WLC Configuration** > **Samba]** in the menu to enter the configuration page as following:



Samba

Samba

Enable Samba ●

Allow users to write ●

Figure 7-3 WLC Samba Configuration Page

These parameters in **[WLC Configuration** > **Samba]** page is described in details as following:

Parameter	Description
Enable Samba	Open the Samba function in WLC that means that part of disk spaces in WLC can be shared with other devices.
Allow Users to Write	This switch is opened to enable the authority of write for other devices to write files into WLC disk spaces.

Click the **Apply** button to accept the changes.

7.4. DPI

DPI stands for Deep Packet Inspection, which inspects the part above layer 4 in the packet for user behavior analysis. User behavior analysis is an important task for operators in the Internet era, but it takes up more system resources and may even degrade system performance.

Select **[WLC Configuration** > **DPI]** in the menu to enter the configuration page as following:

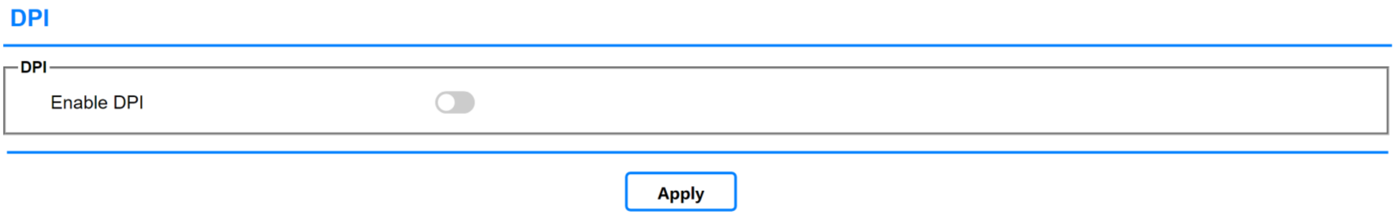


Figure 7-4 Deep Packet Inspect Configuration Page

These parameters in **[WLC Configuration** > **DPI]** page is described in details as following:

Parameter	Description
Enable DPI	Open the switch to enable DPI function for WLC. The DPI results will be graphically displayed in [**Statistics > DPI**]. Default state is disabling.

Click the **Apply** button to accept the changes.

7.5. Packet Capture

Packet Capture is a Wi-Fi system maintenance tool for customers to check for faults by analyzing the incoming and outgoing data packets. The captured packets can be exported to a specific file for **Wireshark** to review.

Select **[WLC Configuration** > **Packet Capture]** in the menu to enter the configuration page as following:

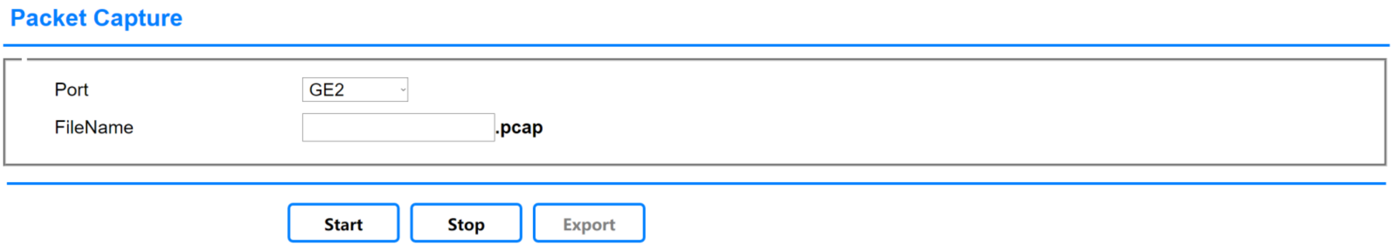


Figure 7-5 RADIUS Server Page

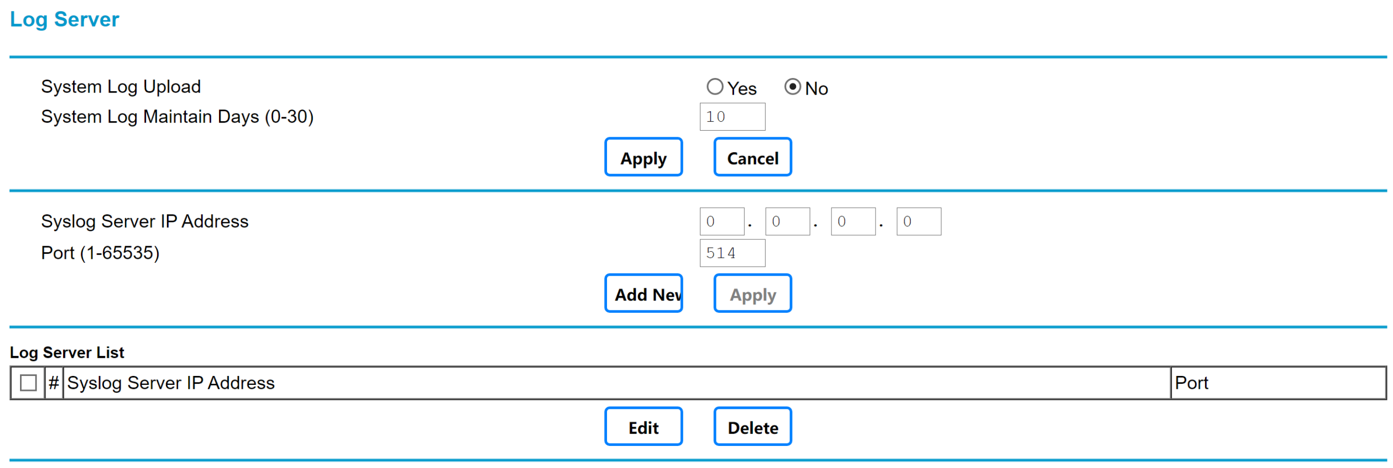
These parameters in **[WLC Configuration** > **Packet Capture]** page is described in details as following:

Parameter	Description
Port	Specify the physical port where you want to capture the incoming and outgoing packets.
File Name	The captured packets will be saved to a file in ***Wireshark*** format, which can be used for offline analysis.
<Start>	This is the button to start the capture.
<Stop>	This is the button to stop the capture.
<Export>	This is the button to export the captured packets to a file in Wireshark format, it is effective only after the <**Stop**> button clicked.

7.6. Log Server

The WLC can locally record system running logs, and also can upload the logs to a remote server which is configured here.

Select **[WLC Configuration** > **Log Server]** in the menu to enter the configuration page as following:



Log Server

System Log Upload ○ Yes ● No

System Log Maintain Days (0-30) 10

Syslog Server IP Address 0 . 0 . 0 . 0

Port (1-65535) 514

Log Server List

□	#	Syslog Server IP Address	Port

Figure 7-6 WLC Log Server Configuration Page

These parameters in **[WLC Configuration** > **Log Server]** page is described in details as following:

Parameter	Description
System Log Upload	This is a switch to enable WLC to upload logs to the remote server.
System Log Maintain Days (0-30)	The log file should be reserved on the remote log server for a period of time, and the retention days are configured here.
Syslog Server IP Address	Entering the IP address of the remote Log Server.
Port	Entering the communication port the remote Log Server.
Log Server List	WLC supports multiple log servers. You can add the log server configured above to the server list by clicking the <**AddNew**> button.

Click the **Apply** button to accept the changes.

Click the **AddNew** button to append new log server to the list.

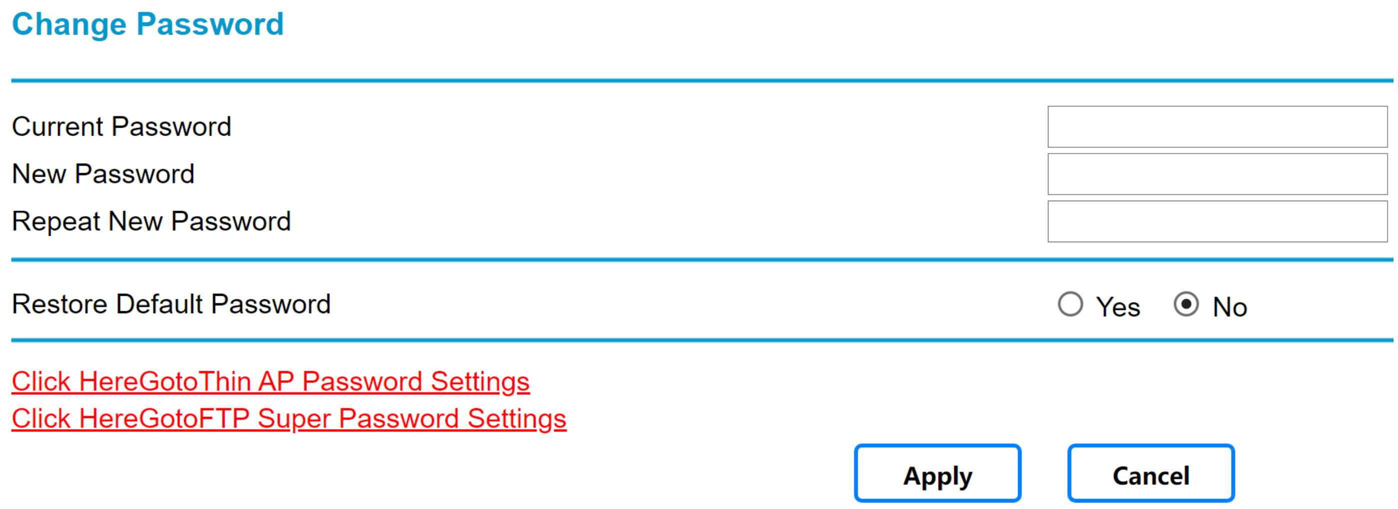
Click the **Edit** button to modify the selected log server in the list.

Click the **Delete** button to remove the selected log server in the list.

7.7. Change Password

WLC has a default user ***admin***, whose password is ***password*** by default. In actual deployment, this default password obviously must be changed by the customer. Here to provide customers with a way to change it.

Select **[WLC Configuration** > **Change Password]** in the menu to enter the configuration page as following:



Change Password

Current Password

New Password

Repeat New Password

Restore Default Password ○ Yes ● No

Click HereGotoThin AP Password Settings

Click HereGotoFTP Super Password Settings

Figure 7-7 Change the password of WLC Administrator

These parameters in **[WLC Configuration** > **Change Password]** page is described in details as following:

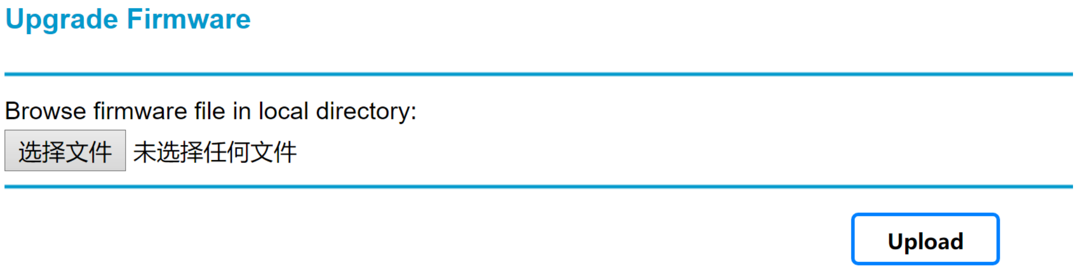
Parameter	Description
Current Password	Entering the password you get into this configuration page this time.
New Password	Entering the new password you want to change to.
Repeat New Password	Entering the new password again to confirm it is not wrong.
Restore Default Password	Restore the password which is set in factory.
Thin AP Password Setting	This is a hyperlink which to the thin AP password setting page.
FTP Super Password Setting	WLC has a built-in FTP server for system maintenance purpose. This is a hyperlink to the FTP server super password setting page.

Click the **Apply** button to accept the changes.

Click the **Cancel** button to discard the changes.

7.8. WLC FW UPGRADE

If a new version of WLC firmware released by vendor, customer can upgrade the WLC by getting into following **[WLC Configuration** > **WLC FW Upgrade]** page. Browse the new firmware in the directory on local host, and then click <**Upload**> button to start the upgrade.



Upgrade Firmware

Browse firmware file in local directory:

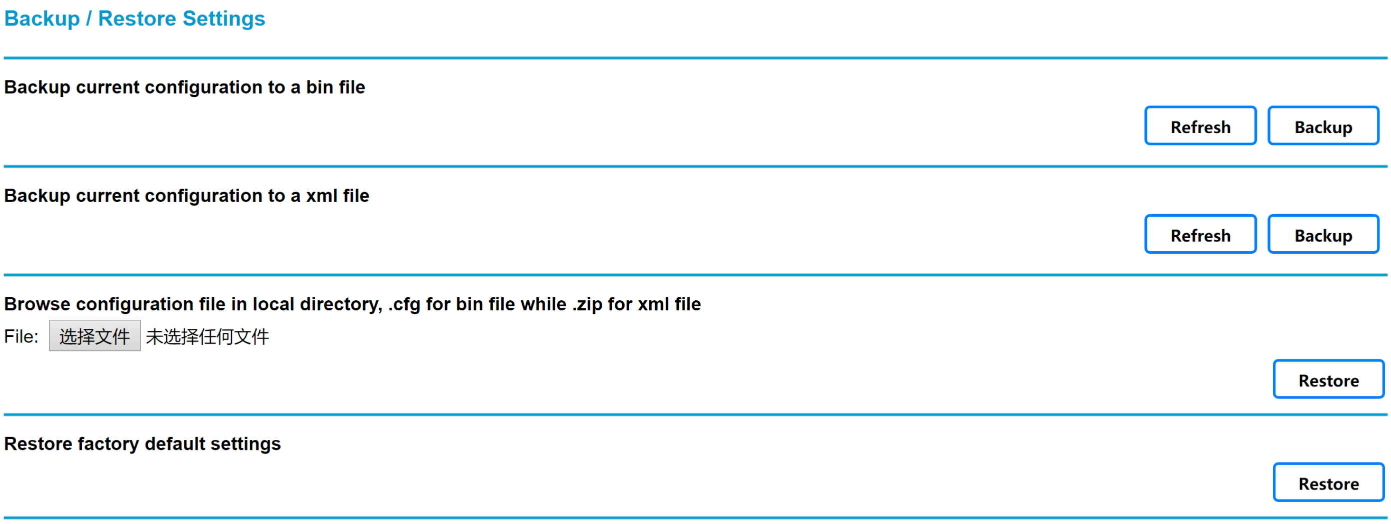
选择文件 未选择任何文件

Figure 7-8 WLC Firmware Upgrade Page

7.9. BACKUP / RESTORE

The overall configuration of WLC can be saved as the file and exported in multiple formats, such as binary format and XML format. The exported configuration file can be used later to restore the configuration for a new WLC installation.

Select **[WLC Configuration** > **Backup/Restore]** in the menu to enter the configuration page as following:



Backup / Restore Settings

Backup current configuration to a bin file

Backup current configuration to a xml file

Browse configuration file in local directory, .cfg for bin file while .zip for xml file

File: 选择文件 未选择任何文件

Restore factory default settings

Figure 7-9 WLC Configuration Backup and Restore Page

These parameters in **[WLC Configuration** > **Backup/Restore]** page are described in details as following:

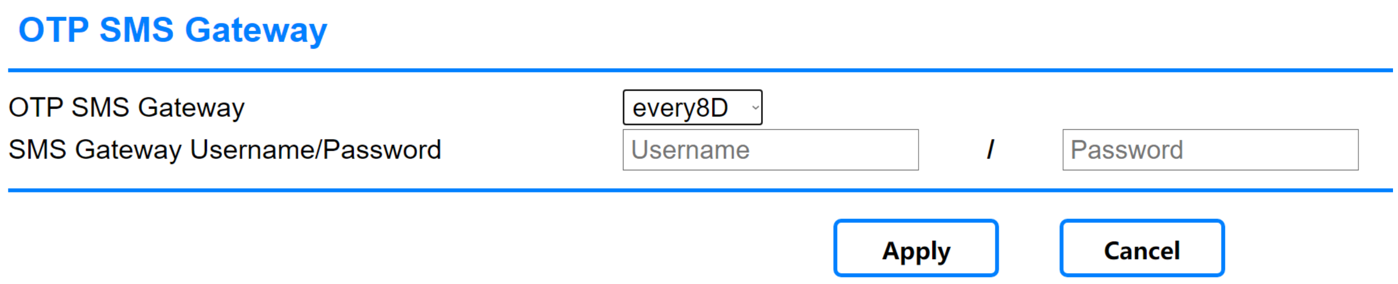
Parameter	Description
Backup Current Configuration to A Bin File	Save current configuration of WLC to a binary file. Click the <**Backup**> button to start saving. Sometimes it needs to click the <**Refresh**> button to refresh browser for security.
Backup Current Configuration to A XML File	Save current configuration of WLC to a XML file. Click the <**Backup**> button to start saving. Sometimes it needs to click the <**Refresh**> button to refresh browser for security.
Restore Configuration	Restore the WLC configuration from the file in the local host directory. The suffix of ***.cfg*** is a binary file, and the suffix of ***.zip*** is an XML file. Click the <**Restore**> button to start restoring.
Restore Factory Default Setting	Restore the default factory configuration of WLC. Click the <**Restore**> button to start restoring.

Chapter 8. Authentication

8.1. OTP SMS Gateway

OTP stands for '**O**ne **T**ime **P**assword'. The password of wireless user client authentication for this time is delivered in a short message from telecom operator and the password is valid just for one time. The password is generated by WLC and provided to the user via short message; therefore, WLC needs to connect to the short message service (SMS) gateway to send the password. Before using the OTP function for user authentication, the WLC must firstly be registered as a legitimate subscriber of the specific SMS gateway. Hyperion series WLC so far has two SMS gateway providers supported, one is **aliyun**, and another is **every8D**, furthermore, new SMS gateway providers may be added according to the specific requirements of customers.

Select **[Authentication** > **OTP SMS Gateway]** in the menu to enter the configuration page as following:



OTP SMS Gateway

OTP SMS Gateway: every8D

SMS Gateway Username/Password: Username / Password

Figure 8-1 OTP SMS Gateway Configuration Page

These parameters in **[Authentication** > **OTP SMS Gateway]** page is described in details as following:

Parameter	Description
OTP SMS Gateway	Select one short message service gateway to be the OTP gateway. There are two SMS gateways for selection, one is **aliyun**, and another is **every8D**. Note, WLC must be registered as a legitimate subscriber of the SMS gateway before the OTP authentication is enabled.
SMS Gateway Username/Password	Entering the user name and password which is officially provided by short message service gateway operator after customer successfully registering as the legitimate subscriber.

Click the **Apply** button to accept the changes.

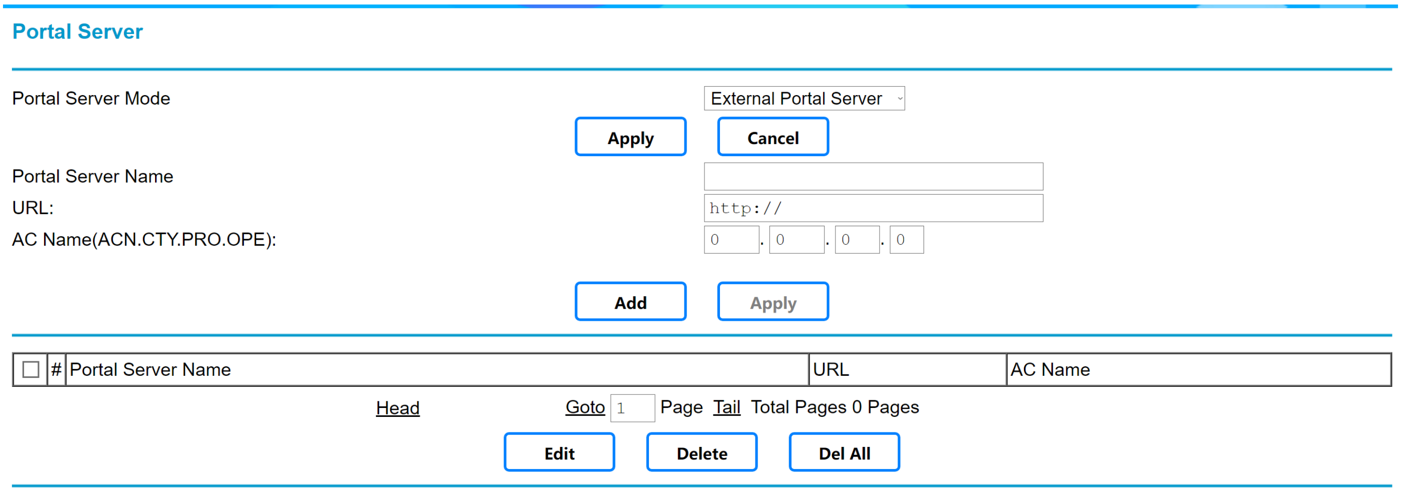
Click the **Cancel** button to discard the changes.

8.2. Portal Server

Portal server provides an entrance of user authentication through web. As long as the user client has not been authenticated as a legitimate user, the portal page will be firstly pushed to the user client that is initiating Internet access. The portal page is for the user to enter the user name and password for further authentication by the Radius server.

Hyperion series WLC has a built-in portal server, so it can use an internal portal server or an external portal server for Web authentication according to customer requirement.

Select **[Authentication** > **Portal Server]** in the menu to enter the configuration page as following:



Portal Server

Portal Server Mode: External Portal Server

Portal Server Name:

URL: http://

AC Name(ACN.CTY.PRO.OPE): 0 . 0 . 0 . 0

□	#	Portal Server Name	URL	AC Name

Head Goto 1 Page Tail Total Pages 0 Pages

Figure 8-2 Portal Server Configuration Page

These parameters in **[Authentication** > **Portal Server]** page is described in details as following:

Parameter	Description
Portal Server Mode	Choose the Portal server for the Wi-Fi system from the internal one or the external one.
Portal Server Name	Assign a literal name for this Portal Server in order to be mnemonic. .
URL	Enter the Uniform Resource Locator (URL) of Portal Server.
AC Name(ACN.CTY.PRO.OPE)	The full name of WLC, in the format of Network Access Site ID (NAS-ID), which is the Host-Name.Deployed-City.Province.Operator.This name in WLC, Portal Server and Radius Server must be matched.
Portal Server List	WLC supports multiple Portal servers. Above portal server configuration is completed, click <**Add**> button to append it to the Portal server list.

Click the **Apply** button to accept the changes.

Click the **Cancel** button to discard the changes.

Click the **Add** button to add a new Portal server to the list.

Click the **Edit** button to modify the selected Portal server in list.

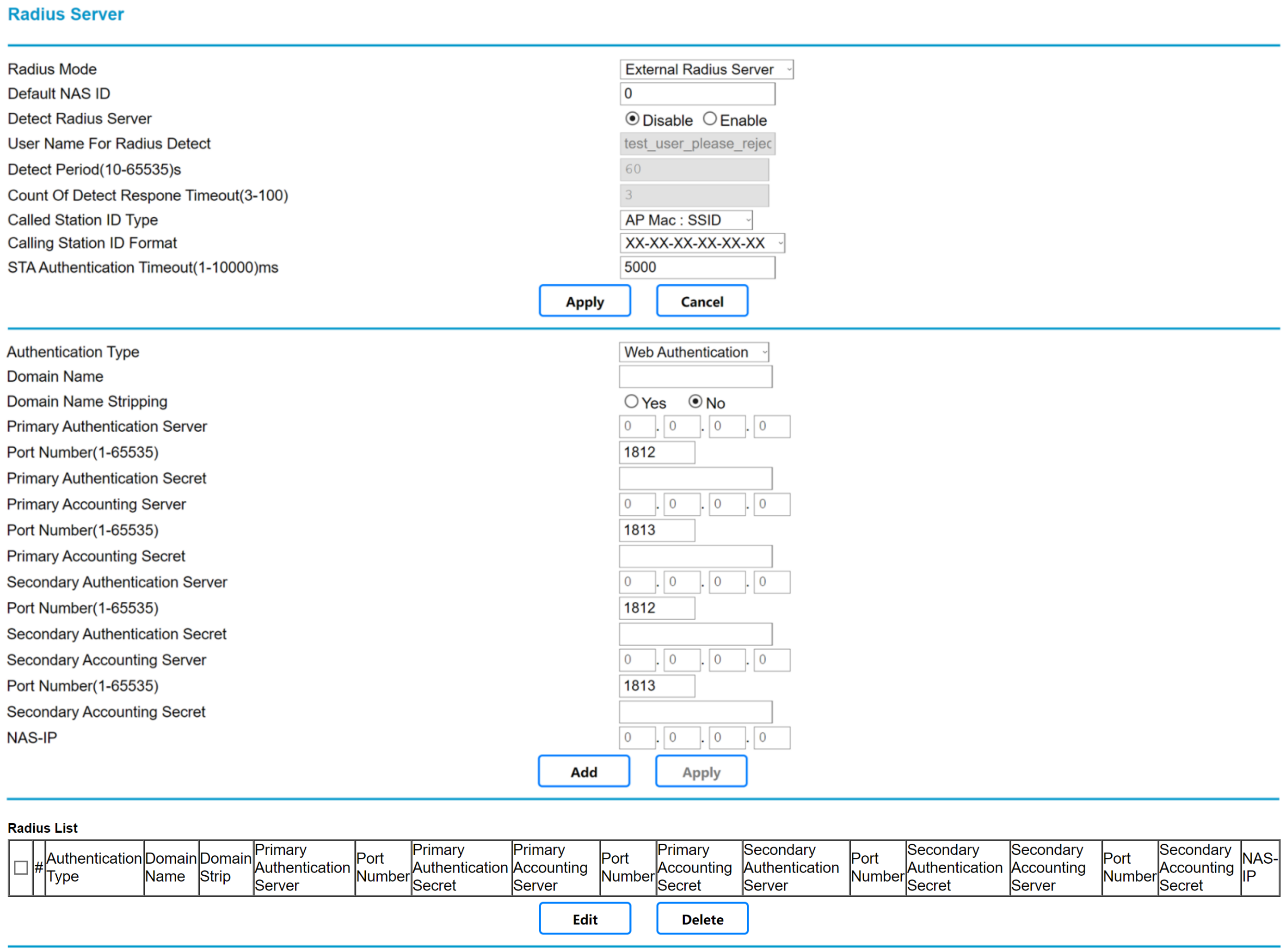
Click the **Delete** button to remove the selected Portal server from the list.

Click the **Del All** button to remove all the Portal servers from the list.

8.3. Radius Server

Radius server is the core element in Wi-Fi system for user authentication behind the portal server. It contains all registered users information in its database, and matches the username and password coming from the portal server with the information contained in the Radius server for user authentication. Hyperion series WLC has a built-in Radius server, so it can use an internal Radius server or an external Radius server according to customer requirement.

Select **[Authentication** > **Radius Server]** in the menu to enter the configuration page as following:



Radius Server

Radius Mode	External Radius Server
Default NAS ID	0
Detect Radius Server	● Disable ○ Enable
User Name For Radius Detect	test_user_please_rejec
Detect Period(10-65535)s	60
Count Of Detect Respone Timeout(3-100)	3
Called Station ID Type	AP Mac : SSID
Calling Station ID Format	XX-XX-XX-XX-XX-XX
STA Authentication Timeout(1-10000)ms	5000

Apply Cancel

Authentication Type	Web Authentication
Domain Name	
Domain Name Stripping	○ Yes ● No
Primary Authentication Server	0 . 0 . 0 . 0
Port Number(1-65535)	1812
Primary Authentication Secret	
Primary Accounting Server	0 . 0 . 0 . 0
Port Number(1-65535)	1813
Primary Accounting Secret	
Secondary Authentication Server	0 . 0 . 0 . 0
Port Number(1-65535)	1812
Secondary Authentication Secret	
Secondary Accounting Server	0 . 0 . 0 . 0
Port Number(1-65535)	1813
Secondary Accounting Secret	
NAS-IP	0 . 0 . 0 . 0

Add Apply

Radius List

□	#	Authentication Type	Domain Name	Domain Strip	Primary Authentication Server	Port Number	Primary Authentication Secret	Primary Accounting Server	Port Number	Primary Accounting Secret	Secondary Authentication Server	Port Number	Secondary Authentication Secret	Secondary Accounting Server	Port Number	Secondary Accounting Secret	NAS-IP

Edit Delete

Figure 8-3 Radius Server Configuration Page

These parameters in **[Authentication** > **Radius Server]** page are described in details as following:

Parameter	Description
Radius Mode	Choose the Radius server for the Wi-Fi system from the internal one or the external one.
Default NAS-ID	The full name of WLC, in the format of Network Access Site ID (NAS-ID), which is the Host-Name.Deployed-City. Province.Operator. This name in WLC, Portal Server and Radius Server must be matched.
Detect Radius Server	WLC supports multiple Radius servers for redundancy purposes, so you can turn on this switch for WLC to detect whether the current Radius server is active, so as to switch to a backup Radius server when the current Radius fails.

Parameter	Description
Username For Radius Detect	WLC detecting Radius requires an username to login the Radius server.
Detect Period (10-65535 s)	The WLC detects the radius intermittently, so the detection interval should be given here.
Count of Detect Response Timeout (3-100)	This is the threshold for the WLC to determine whether the radius is active. If the WLC does not receive a detection response message within this set time, it is judged as a Radius failure.
Called Station ID Type	Radius authentication requires the type of the Called Station ID, the types include: ▪ **AP MAC: SSID** ▪ **AP MAC** ▪ **AP Name: SSID** ▪ **AP Name** Different Radius server requires different type. Please choose it according to the Radius server requirement.
Calling Station ID Format	Radius authentication requires the Calling Station ID, its format is of: ▪ **XX-XX-XX-XX-XX-XX** ▪ **XX:XX:XX:XX:XX:XX** Different Radius server requires different format. Please choose it according to the Radius server requirement.
STA Authentication Timeout (1-10000 ms)	This is the threshold for the WLC to determine whether the user authentication is failure. If the WLC does not receive a authentication result within this set time, it is judged as an authentication failure.
Authentication Type	Tell the Radius server what kind authentication is used for it: ▪ **Web Authentication:** the Radius server verifies the username and password provided by the Portal server for authentication. ▪ **PPPoE:** the Radius server is used for the user client dialing up authentication. ▪ **WPA/WPA2:** the Radius server is used for WPA/WPA2 key distribution and authentication when the user client associates to thin AP.
Domain Name	For web authentication, it must allocate a domain name here in order to complete the username sent to Radius in the format of ***Username@domain***.
Domain Name Stripping	This switch is used for WLC to remove the suffix of ***@domain*** in the username before it is sent to the Radius server.
Primary Authentication Server	The IP address of the primary authentication server.
Port Number (1-65535)	The protocol port number of the primary authentication server.
Primary Authentication Secret	This is the key for WLC to prove that it is a legitimate device of the primary Radius server. The secret key is an ASCII string.
Primary Accounting Server	The IP address of the primary accounting server.

Parameter	Description
Port Number (1-65535)	The protocol port number of the primary accounting server.
Primary Accounting Secret	This is the key for WLC to prove that it is a legitimate device of the primary Accounting server. The secret key is an ASCII string.
Secondary Authentication Server	The IP address of the secondary authentication server.
Port Number (1-65535)	The protocol port number of the secondary authentication server.
Secondary Authentication Secret	This is the key for WLC to prove that it is a legitimate device of the secondary Radius server. The secret key is an ASCII string.
Secondary Accounting Server	The IP address of the secondary accounting server.
Port Number (1-65535)	The protocol port number of the secondary accounting server.
Secondary Accounting Secret	This is the key for WLC to prove that it is a legitimate device of the secondary Accounting server. The secret key is an ASCII string.
NAS-IP	This is a field that Radius server required, its value is given by the Radius server.

Click the **Apply** button to accept the changes.

Click the **Cancel** button to discard the changes.

Click the **Add** button to add a new entry.

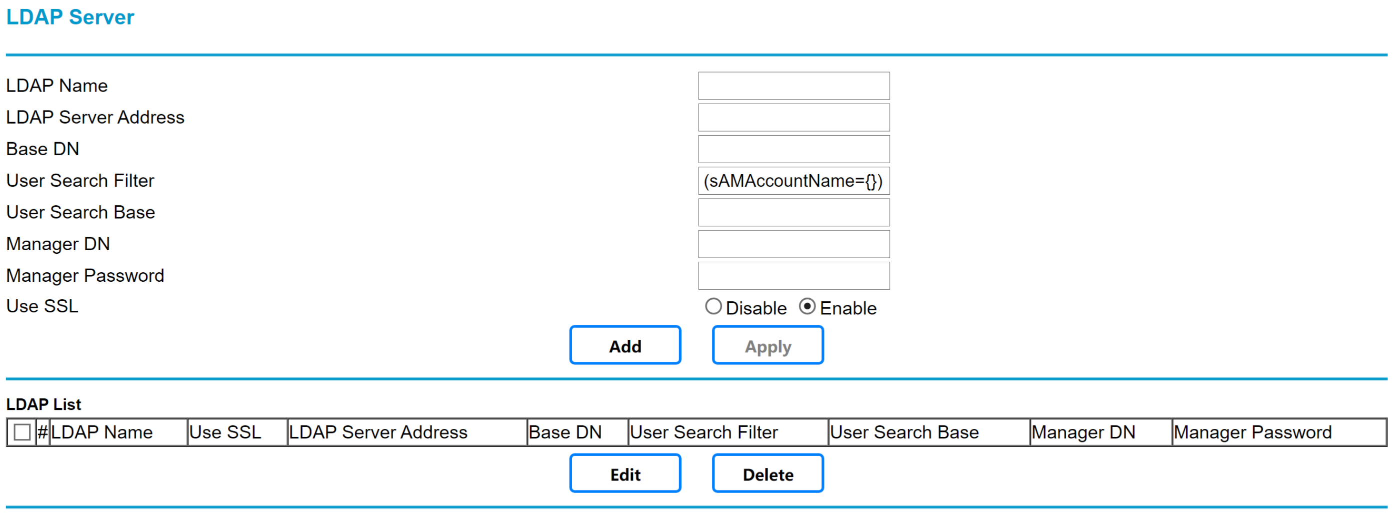
Click the **Edit** button to modify the selected entry.

Click the **Delete** button to remove the selected entry.

8.4. LDAP SERVER

In some non-carrier grade Wi-Fi systems, the LDAP (Light Directory Access Protocol) servers, such as MS Active Directory, OpenLDAP or OpenDJ, are used for authentication instead of Radius servers. LDAP server authentication has the advantages of light weight, flexibility and simplicity, which is very convenient for customers to easily build their own Wi-Fi systems.

Select **[Authentication** > **LDAP Server]** in the menu to enter the configuration page as following:



LDAP Server

LDAP Name

LDAP Server Address

Base DN

User Search Filter (sAMAccountName={})

User Search Base

Manager DN

Manager Password

Use SSL ○ Disable ● Enable

LDAP List

□	#	LDAP Name	Use SSL	LDAP Server Address	Base DN	User Search Filter	User Search Base	Manager DN	Manager Password

Figure 8-4 LDAP Server Configuration Page

These parameters in **[Authentication** > **LDAP Server]** page is described in details as following:

Parameter	Description
LDAP Name	Assign a literal name for this LDAP Server in order to be mnemonic.
LDAP Server Address	Fully Qualified Domain Name (FQDN) or IP address of LDAP server.
Base DN	The Distinguished Name (DN) will be used to bind to the LDAP server. This happened before any user comes to authenticate. You will have to supply a full DN like ***cn=admin,dc=example,dc=com***, each objective is separated by comma.
User Search Filter	A user search filter provides a mechanism for defining the criteria for matching entries in an User Search Request. Its syntax supports the =, ~=, <, <=, >, >= and ! operators, and provides limited substring matching using the * operator. **Note, it is recommended to use the default value, the customer does not need to change it.**
User Search Base	The user search base defines the starting point for the user search in the directory tree. A search base comprises multiple objects separated by commas. These objects include: ▪ **cn:** common name. ▪ **ou:** organizational unit ▪ **o:** organization ▪ **c:** country ▪ **dc:** domain
Manager DN	The DN of LDAP server administrator. A full DN like ***cn=admin,dc=example,dc=com***, each objective is separated by comma.
Manager Password	Password of LDAP server administrator.
Use SSL	With this switch on, SSL (Secure Socket Layer) can be applied on the link between WLC and LDAP server.

Parameter	Description
LDAP Server List	WLC supports multiple LDAP servers. Above LADP server configuration is completed, click <**Add**> button to append it to the LDAP server list.

Click the **Apply** button to accept the changes.

Click the **Cancel** button to discard the changes.

Click the **Add** button to add a new entry.

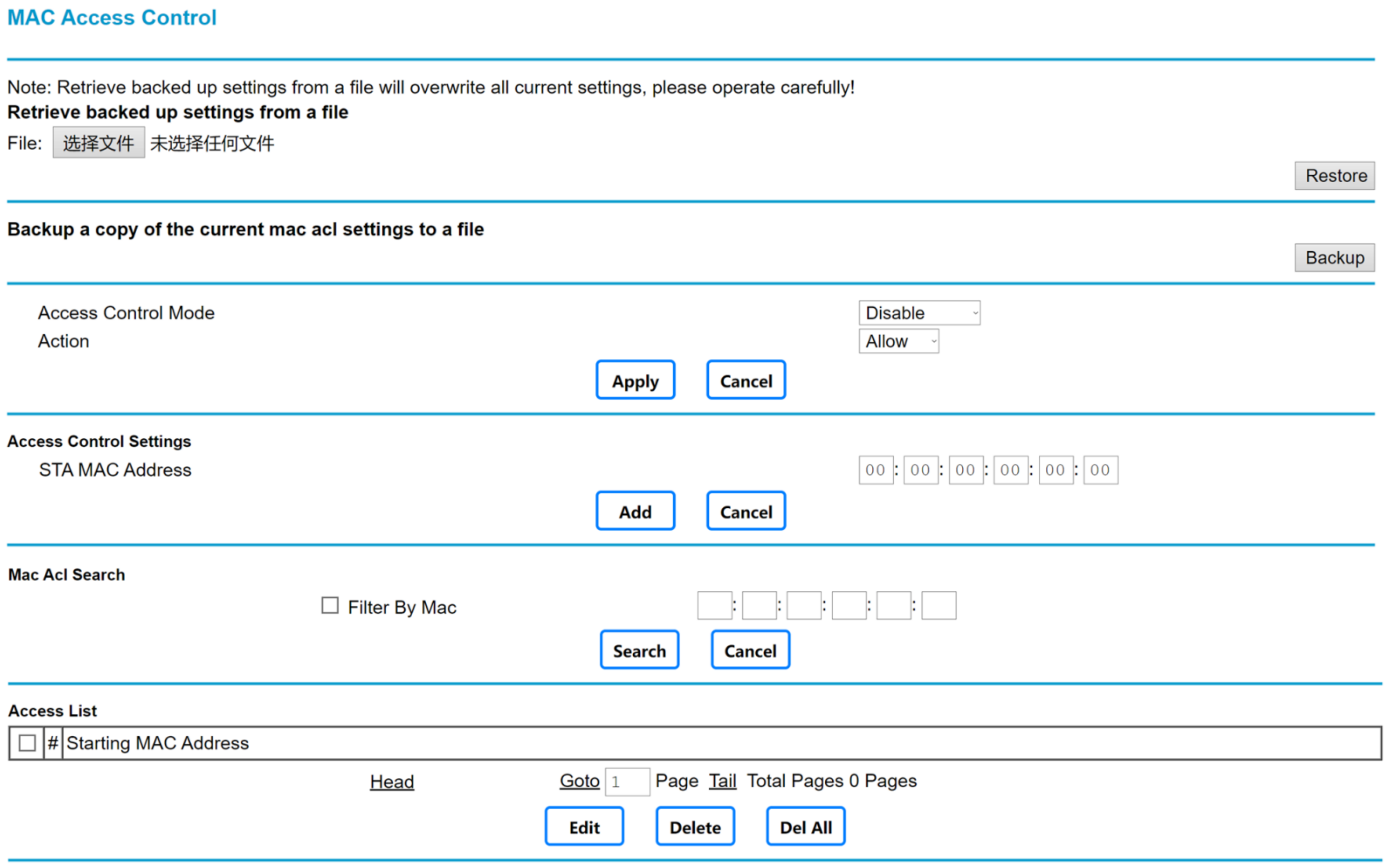
Click the **Edit** button to modify the selected entry.

Click the **Delete** button to remove the selected entry.

8.5. MAC ACCESS CONTROL

This is a black and white list based on the MAC address of the user client to allow or prohibit the user client to access the thin AP. The user clients in the white list will be allowed to associate with the thin AP, and the user clients in the blacklist will be refused to associate with the thin AP. The black and white list is created in WLC, and the thin AP downloads it to control the association of user clients. This is actually the ACL based on MAC.

Select **[Authentication** > **MAC Access Control]** in the menu to enter the configuration page as following:



MAC Access Control

Note: Retrieve backed up settings from a file will overwrite all current settings, please operate carefully!

Retrieve backed up settings from a file

File: 选择文件 未选择任何文件

Backup a copy of the current mac acl settings to a file

Access Control Mode: Disable

Action: Allow

Access Control Settings

STA MAC Address: 00 : 00 : 00 : 00 : 00 : 00

Mac Acl Search

☐ Filter By Mac

Access List

☐	#	Starting MAC Address

Head Goto 1 Page Tail Total Pages 0 Pages

Figure 8-5 MAC Access Control Configuration Page

These parameters in **[Authentication** > **MAC Access Control]** page is described in details as following:

Parameter	Description
Access Control Mode	Four access control modes provided for user clients based: - **Disable:** No MAC access control will be applied to thin AP. - **MAC:** The access control of user client is only based on its MAC address. - **MAC@VAP:** The access control only affects the virtual AP whose SSID is identified her. - **Special MAC:** The special MAC is the VIP client; it is not only allowed to associate, but also free from authentication.
Action	Define the action attribute for above selected access control mode: - **Allow:** This is the attribute that allows the user client to associate with the thin AP. - **Reject:** This is the attribute that prohibits the user client to associate with the thin AP.
STA MAC Address	Enter the MAC address of the user client to be added to the access control list by click <**Add**> button.
MAC ACL Search	With the radio button of ***Filter by MAC*** checked, entering a MAC address to be searched in the access control list.
Access List	List the MAC address of each user client and its access control attribute for display.

Click the **Apply** button to accept the changes.

Click the **Cancel** button to discard the changes.

Click the **Add** button to add a new Access Control entry to the list.

Click the **Edit** button to modify the selected Access Control entry in list.

Click the **Delete** button to remove the selected Access Control entry from the list.

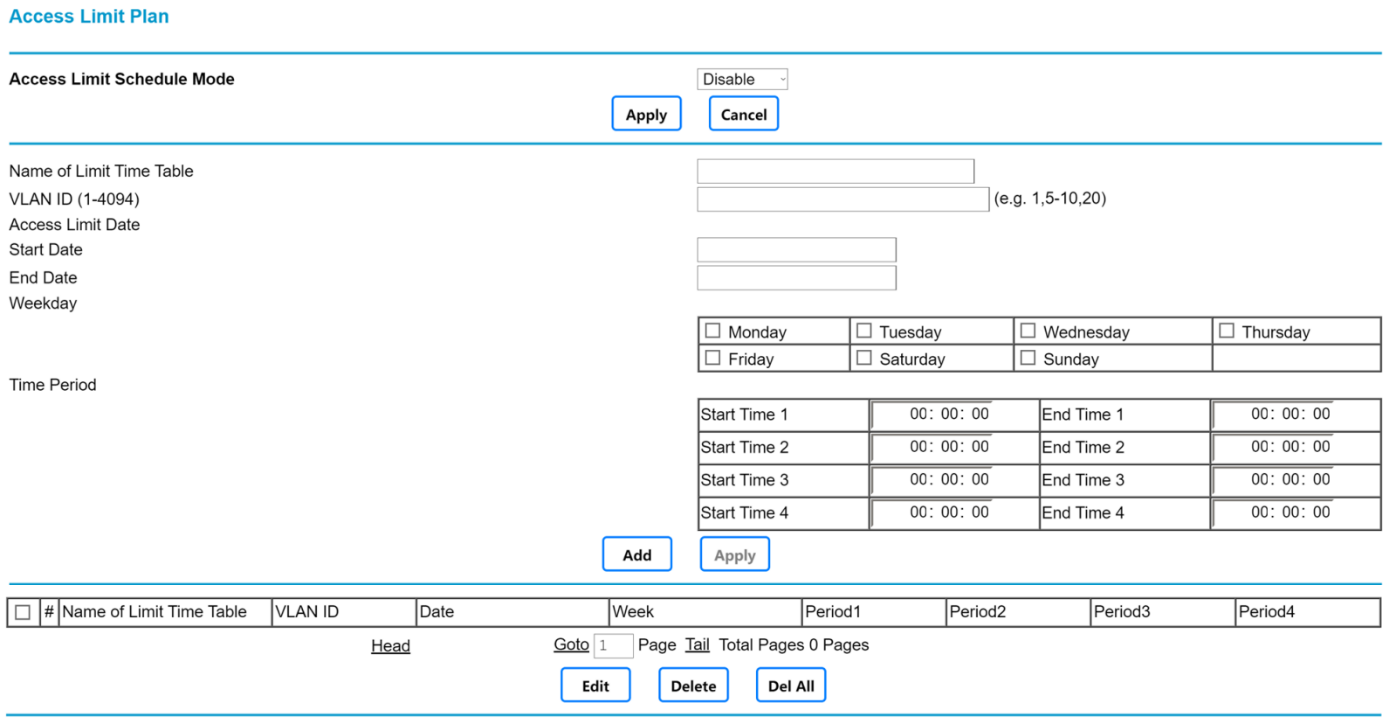
Click the **Del All** button to remove all the Access Control entry from the list.

Click the **Search** button to find the specific user client in Access Control entry list.

8.6. Access Time Control

Access Time Control is a time schedule for the access limit function configured in the VAP profile. It plans the specific day and time of the week for thin AP to close its air channel to prevent user clients associating with it. This is usually a very useful feature for campus Wi-Fi network.

Select **[Authentication** > **Access Time Control]** in the menu to enter the configuration page as following:



Access Limit Plan

Access Limit Schedule Mode: Disable

Apply Cancel

Name of Limit Time Table

VLAN ID (1-4094) (e.g. 1,5-10,20)

Access Limit Date

Start Date

End Date

Weekday

□ Monday	□ Tuesday	□ Wednesday	□ Thursday
□ Friday	□ Saturday	□ Sunday	

Time Period

Start Time 1	00: 00: 00	End Time 1	00: 00: 00
Start Time 2	00: 00: 00	End Time 2	00: 00: 00
Start Time 3	00: 00: 00	End Time 3	00: 00: 00
Start Time 4	00: 00: 00	End Time 4	00: 00: 00

Add Apply

□	#	Name of Limit Time Table	VLAN ID	Date	Week	Period1	Period2	Period3	Period4

Head Goto 1 Page Tail Total Pages 0 Pages

Edit Delete Del All

Figure 8-6 Access Time Control Configuration Page

These parameters in **[Authentication** > **Access Time Control]** page are described in details as following

Parameter	Description
Access Limit Schedule Mode	Three options may be selected for access restriction: ▪ **Disable:** Thin AP is always opened for user client association, and there is no access restriction. ▪ **By VAP:** The access limit schedule takes effect for the VAP with the identified SSID. ▪ **By VLAN:** The access limit schedule takes effect for those user clients tagged with specific VLAN ID.
Name of Limit Time Table	Assign a literal name for this Access Time Schedule table in order to be mnemonic.
VLAN ID	If "**Access Limit Schedule Mode**" selects "**By VLAN**", specify the VLAN ID here. User clients tagged with this VLAN ID will be denied association with the thin AP according to the Access Limit Schedule.
Start Date	The date when the access limit schedule started. It is selected from the graphical calendar.
End Date	The date when the access limit schedule stopped. It is selected from the graphical calendar.
Weekday	Choose the days from Monday, Tuesday, Wednesday, Thursday, Friday, Saturday and Sunday. This is a checkbox that allows multiple selections.
Time Period	The time windows in a day during which the access restriction are enforced. Multiple time windows in a day are allowed.

Click the **Apply** button to accept the changes.

Click the **Cancel** button to discard the changes.

Click the **Add** button to add a new Access Limit Time entry to the table.

Click the **Edit** button to modify the selected Access Limit Time in table.

Click the **Delete** button to remove the selected Access Limit Time entry from the table.

Click the **Del All** button to remove all the Access Limit Time entries from the table.

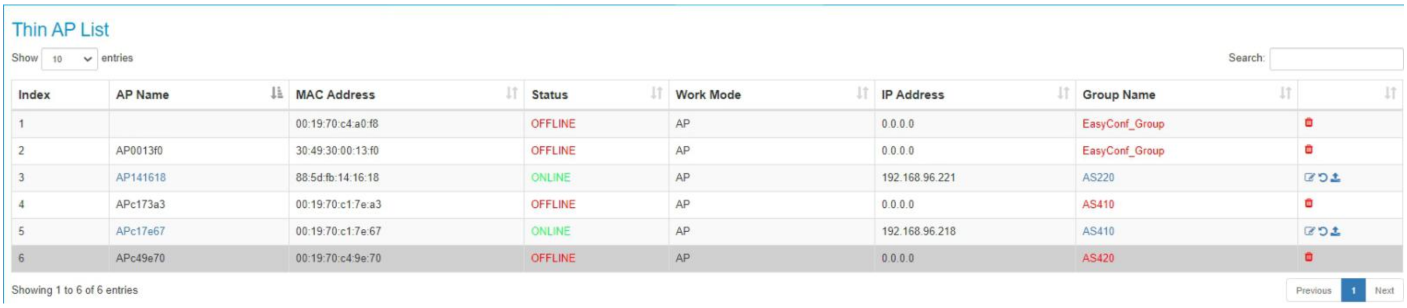
Chapter 9. STATISTICS

WLC provides a variety of statistics information for system maintenance and management.

9.1. THIN AP LIST

As long as the thin AP has accessed to the WLC, whatever it is now online or offline, it will be added to the thin AP list for displaying, illustrated as following.

Select **[Statistics** > **Thin AP List]** in the menu to display as following:



Thin AP List

Show 10 entries Search:

Index	AP Name	MAC Address	Status	Work Mode	IP Address	Group Name	
1		00:19:70:c4:a0:f8	OFFLINE	AP	0.0.0.0	EasyConf_Group	
2	AP0013f0	30:49:30:00:13:f0	OFFLINE	AP	0.0.0.0	EasyConf_Group	
3	AP141618	88:5d:fb:14:16:18	ONLINE	AP	192.168.96.221	AS220	
4	APc173a3	00:19:70:c1:7e:a3	OFFLINE	AP	0.0.0.0	AS410	
5	APc17e67	00:19:70:c1:7e:67	ONLINE	AP	192.168.96.218	AS410	
6	APc49e70	00:19:70:c4:9e:70	OFFLINE	AP	0.0.0.0	AS420	

Showing 1 to 6 of 6 entries

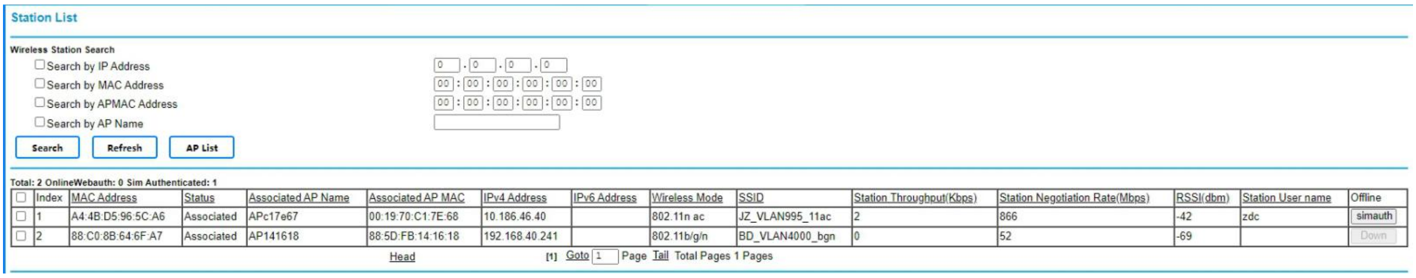
Figure 9-1 Thin AP List

Click the **Previous and Next** buttons to turn page if this list is too big in size.

9.2. STATION LIST

Station is the user wireless client. As long as the user client has associated to the thin AP, whatever it is now online or offline, it will be added to the station list for displaying, illustrated as following.

Select **[Statistics** > **Station List]** in the menu to display as following:



Station List

Wireless Station Search

☐ Search by IP Address 0 . 0 . 0 . 0

☐ Search by MAC Address 00 : 00 : 00 : 00 : 00 : 00

☐ Search by APMAC Address 00 : 00 : 00 : 00 : 00 : 00

☐ Search by AP Name

Total: 2 OnlineWebauth: 0 Sim Authenticated: 1

☐	Index	MAC Address	Status	Associated AP Name	Associated AP MAC	IPv4 Address	IPv6 Address	Wireless Mode	SSID	Station Throughput(Kbps)	Station Negotiation Rate(Mbps)	RSSI(dbm)	Station User name	Offline
☐	1	A4:4B:D5:96:5C:A6	Associated	APc17e67	00:19:70:C1:7E:68	10.186.46.40		802.11n ac	JZ_VLAN995_11ac	2	866	-42	zdc	simauth
☐	2	88:C0:8B:64:6F:A7	Associated	AP141618	88:5D:FB:14:16:18	192.168.40.241		802.11b/g/n	BD_VLAN4000_bgn	0	52	-69		Down

Head [1] Goto 1 Page Tail Total Pages 1 Pages

Figure 9-1 User Clients List

Customer can search the specific user client in the list by filtered with its IP address, MAC address, or AP's MAC and AP name.

Click **Search** button to start search.

Click **Refresh** button to update the station list.

9.3. DPI

DPI is the statistical information of user service types obtained by inspecting the 4th and higher layers of the packets transmission through the WLC. It is very useful for analyzing user behavior. This requires the Wi-Fi system is operating in the “Central Switching” mode, i.e., the user traffic is firstly concentrated to WLC and then centralized forwarded to internet.

Select **[Statistics** > **DPI]** in the menu to display as following:

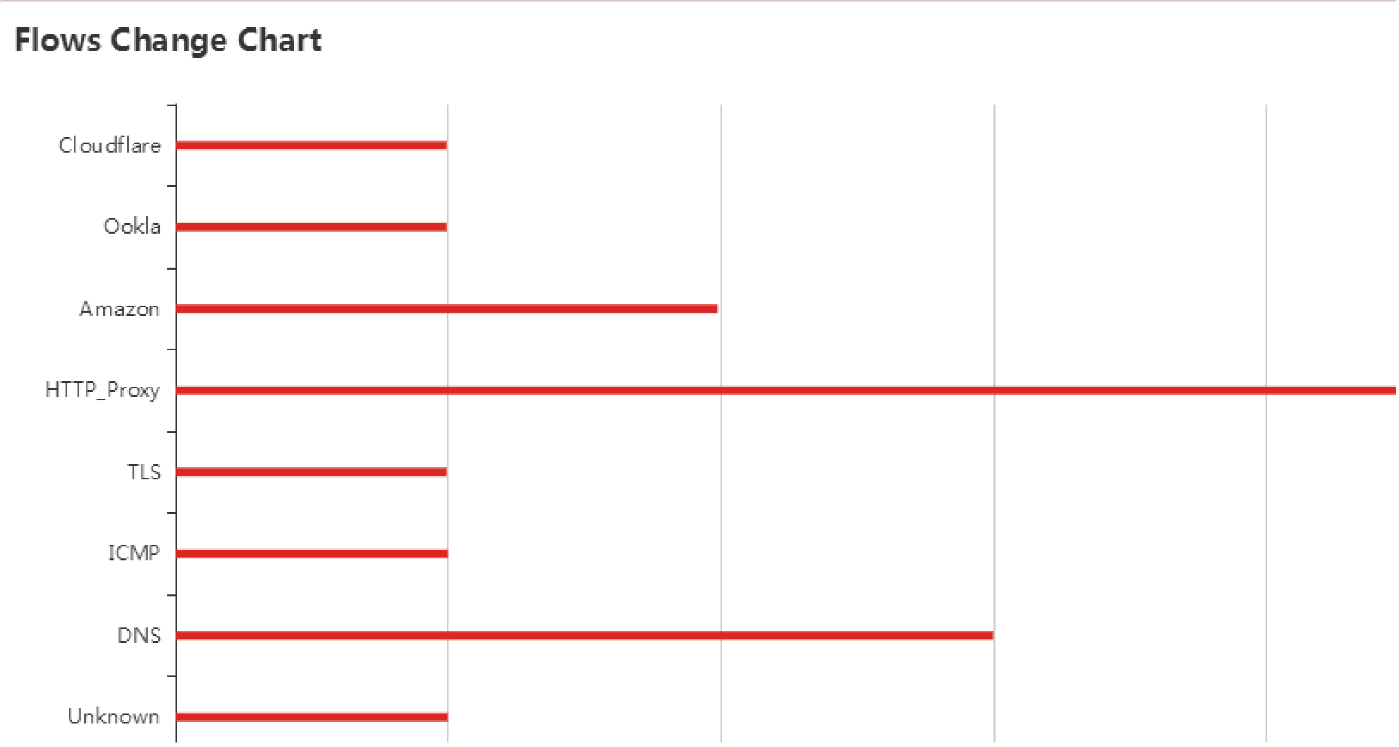


Figure 9-2 The Traffic Fluctuation Chart

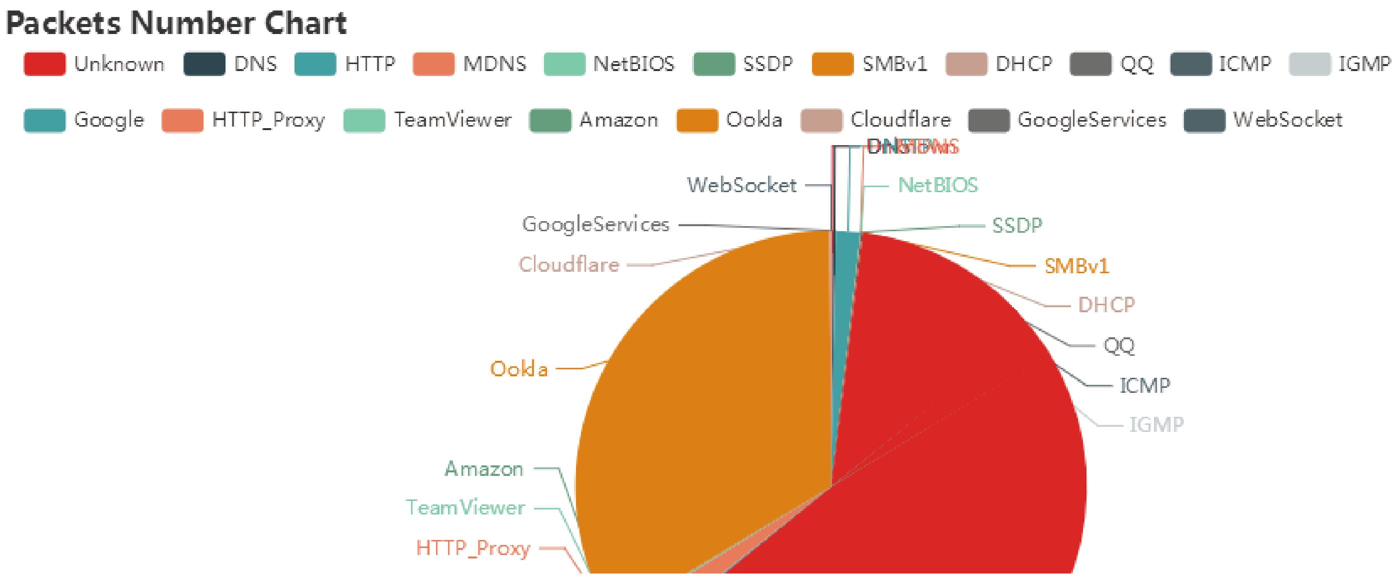


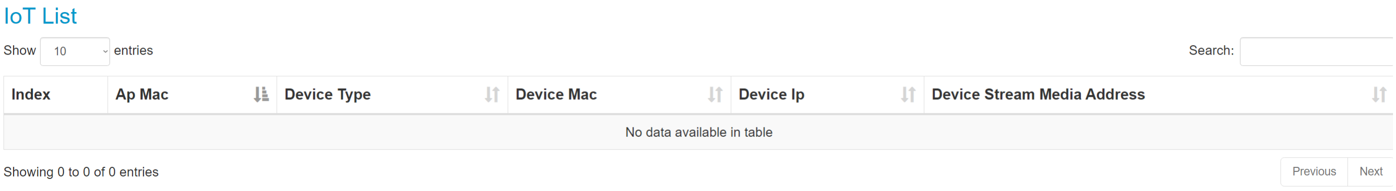
Figure 9-4 The Service Types Pie Chart

Click the **Clear** button to initialize the statistics to zero.

9.4. IoT List

WLC is the central switching element for IoT devices through Wi-Fi CPE, so if they are online, IoT devices, such as sensors and IP cameras, can be displayed here.

Select **[Statistics** > **IoT]** in the menu to display as following:



IoT List

Show 10 entries Search:

Index	Ap Mac	Device Type	Device Mac	Device Ip	Device Stream Media Address
No data available in table					

Showing 0 to 0 of 0 entries

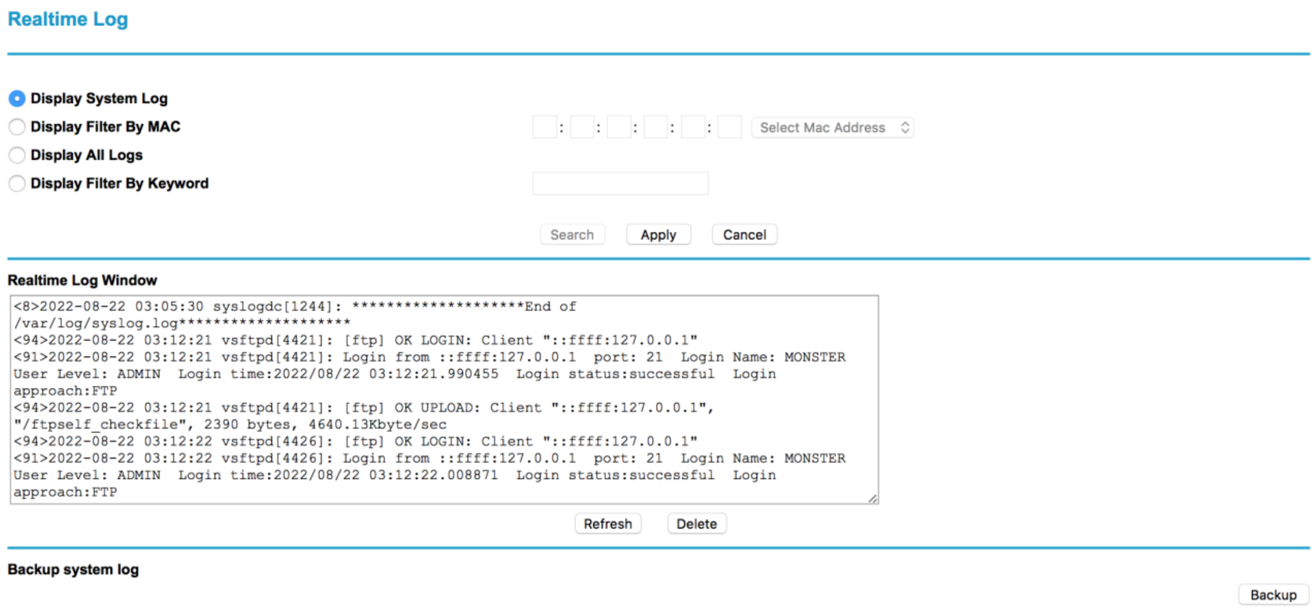
Figure 9-5 IoT Devices List

Click the **Previous and Next** buttons to turn page if this list is too big in size.

9.5. Realtime Log

The real-time system log is the current log, which shows what is happening in the WLC system. Therefore, the log information will scroll quickly in the "Real-time Log" window. This is a useful method for administrators to monitor the operation of the WLC. Because it is real-time, it will take up too much system resources, thereby reducing performance, so don’t use it for a long time.

Select **[Statistics** > **Realtime Log]** in the menu to display as following:



Realtime Log

● Display System Log
○ Display Filter By MAC
○ Display All Logs
○ Display Filter By Keyword

Realtime Log Window

```
<8>2022-08-22 03:05:30 syslogdc[1244]: ********************End of
/var/log/syslog.log********************
<94>2022-08-22 03:12:21 vsftpd[4421]: [ftp] OK LOGIN: Client "::ffff:127.0.0.1"
<91>2022-08-22 03:12:21 vsftpd[4421]: Login from ::ffff:127.0.0.1  port: 21  Login Name: MONSTER
User Level: ADMIN  Login time:2022/08/22 03:12:21.990455  Login status:successful  Login
approach:FTP
<94>2022-08-22 03:12:21 vsftpd[4421]: [ftp] OK UPLOAD: Client "::ffff:127.0.0.1",
"/ftpself_checkfile", 2390 bytes, 4640.13Kbyte/sec
<94>2022-08-22 03:12:22 vsftpd[4426]: [ftp] OK LOGIN: Client "::ffff:127.0.0.1"
<91>2022-08-22 03:12:22 vsftpd[4426]: Login from ::ffff:127.0.0.1  port: 21  Login Name: MONSTER
User Level: ADMIN  Login time:2022/08/22 03:12:22.008871  Login status:successful  Login
approach:FTP
```

Backup system log

Figure 9-6 Realtime Log Page

Click the **Backup** button to export the real-time log to a file for offline analysis.

Chapter 10. Technical Specifications

Physical Specification		WS5G2	WS7G2	WS10G2
Power Supply	**Volts (V)**	12V DC	12V DC	12V DC
	Amps (A)	5 A	5 A	7 A
Dimensions	**(Height)**	44 mm	44 mm	44 mm
	(Width)	232 mm	231 mm	231 mm
	(Depth)	152 mm	197 mm	197 mm
	Form Factor	1U	1U	1U
Weight		2.7 kg	2.7 kg	2.7 kg
Ports	**RJ45 (1G)**	4	6	6
	SFP+ (10G)	-	2	4
CPU QTY		1	1	1
Memory	**Size**	8 GB	16 GB	32 GB
	Type	DDR3	DDR4	DDR4
Storage (Primary)	**Size**	64 GB	64 GB	64 GB
	Type	SSD	SSD	SSD

Software Specification	WS5G2	WS7G2	WS10G2
AP Capacity	128	256	512
MAC Address Table	8K	16K	30K
Max. Number of VLANs	4K	4K	4K

Environment Specification		WS5G2	WS7G2	WS10G2
Temperature	**Operating**	0°C to 40°C (32°F to 104°F)		
Humidity	**Operating**	10% to 90% (Non-condensing)		

Chapter 11. APPENDIX

11.1. WARRANTY

11.1.1. GENERAL WARRANTY

The warranty period stated below replaces the warranty period as stated in the user manuals for the relevant Products. If there is no proof indicating the purchase date, the manufacture date shall be considered as the beginning of the warranty period. The Warranty extends only to the original end-user purchaser and is not transferable to anyone who obtains ownership of the Product from the original end-user purchaser.

1. Z-COM provides one year of conditional warranty depends on different models.
2. Lifetime warranty covers product itself, excluding consumable products, accessories, second-hand products, and software. Lifetime warranty is only effective when products are still in the Z-COM Product list. After the EOL (End of Life) announcement for any Products, the warranty will be one year from the date of such Product EOL announcement. To grant the lifetime warranty, Products should have a proof of purchase (such as the invoice or sales receipt) must be provided upon receiving warranty service. The standard warranty period for any Product had a proof of purchase shall be one year from the date of purchase or manufacture.
3. Products are considered as DOA (Dead on Arrival) after conclusive test within the first 30 days of its shipping date from Z-COM. After 30 days from the shipping date, defective products covered within the warranty are considered as RMA (Return Material Authorization).
4. Z-COM reserves the right to inspect all defective products which must be returned and paid shipping fee by purchasers.

11.1.2. WARRANTY CONDITIONS

Warranty service will be excluded if following conditions occurred:

1. The product has been tampered, repaired and/or modified by non-authorized personnel
2. The SN (Serial Number) or MAC (Media Access Control) address has been changed, cancelled, or removed
3. The damage is caused by third party software or virus
4. The software loss or data loss that may occur during repair or replacement

11.1.3. DISCLAIMER

PRODUCTS ARE NOT WARRANTED TO OPERATE UNINTERRUPTED OR ERROR FREE. Z-COM NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS. Z-COM SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, FOREC MAJEURE EVENT OR ANY OTHER HAZARD. THE INFORMATION CONTAINED HEREIN IS SUBJECT TO CHANGE WITHOUT NOTICE.

11.2. Certifications and Compliance

11.2.1. CE Marking

CE marking on this product represents the product is in compliance with all directives that are applicable to it.

11.2.2. RoHS Compliance Statement

European Directive 2012/19/EU requires that the equipment bearing this symbol on the product and/ or its packaging must not be disposed of with unsorted municipal waste. The symbol indicates that this product should be disposed of separately from regular household waste streams. It is your responsibility to dispose of this and other electric and electronic equipment via designated collection facilities appointed by the government or local authorities. Correct disposal and recycling will help prevent potential negative consequences to the environment and human health. For more detailed information about the disposal of your old equipment, please contact your local authorities, waste disposal service, or the shop where you purchased the product.

11.3. Declaration of Conformity

Hereby, Z-COM, Inc. declares that the equipment listed above is in compliance with Directive 2014/30/EU and 2014/35/EU. The full text of the EU declaration of conformity is available at the following internet address: https://www.zcom.com.tw/index/downloads

11.4. List of Compatibility

Model Name		AS220V2	AS420	SP220V2	SP420	SP230
Description		Indoor		Outdoor		
		Dual-Band 802.11ac Wave2				
Antenna Configuration		2x2	4x4	2x2	4x4	2x2
Max. Data Rate	2.4GHz	1167Mbps	2333Mbps	1167Mbps	2533Mbps	1167Mbps
Max. Transmit Power	2.4GHz	32 dBm	28 dBm	32 dBm	28 dBm	32 dBm
	5GHz	29 dBm	28 dBm	29 dBm	28 dBm	29 dBm