USER MANUAL

WS200/500/1000G2

Wireless LAN Controller

Revision: 3.2.1

TABLE OF CONTENTS

Chapter 1. INTRODUCTION

Titan is a new generation of Wireless LAN Controller (WLC) product series developed by Z-COM Inc., which includes three models of WS200G2, WS500G2 and WS1000G2, and are particularly suitable for carrier-grade Wi-Fi networks and the IoT applications. Based on the Intel XEON platform design, this series of products can provide 1G, 10G and 40G Ethernet ports in the form of RJ45, SFP+ and QSPF to meet with the requirements of various network applications. Titan series Wireless LAN Controllers are mainly oriented to the large-scale Wi-Fi networks with more than 10,000 access points, in which the wireless clients can be either the conventional mobile endpoints and laptop computers, or the IoT devices such as IP-CAMs, industrial sensors and controllers etc. In the era of industry 4.0, the artificial intelligence applications and IoT applications that are highly dependent on wireless communication will grow explosively, therefore, the extremely high throughput Wi-Fi network and Wi-Fi distributed system may get into a large-scale expansive period. This also means that Titan series Wireless LAN Controllers will have more opportunities in the new era.

By migrating the management functions originally resided in each individual wireless access point (AP) to the Wireless LAN Controller to implement the centralized management and maintenance, while the access point (AP) only reserves its fundamental wireless access and security functions, this is why the wireless access point (AP) in a Wi-Fi system with Wireless LAN Controller is called as thin AP (TAP). Obviously, in such a centralized Wi-Fi system, the Wireless LAN Controller mainly focuses on high-level capabilities such as AP configuration, user authentication, user traffic forwarding, RF resource management, access control, QoS, and load balancing; the thin AP only focuses on the basic functions defined by the IEEE802.11 specification. For a complex Wi-Fi system, such architecture is an ideal model that is completely controllable and manageable. In the Wi-Fi system that uses the Wireless LAN Controller, the thin AP is a totally zero-configured device, it obtains the IP address of the Wireless LAN Controller through DHCP Option 43 during the booting up stage. Thin AP uses this IP address to establish the CAPWAP tunnel with Wireless LAN Controller, and then downloads the profiles from it through CAPWAP tunnel to complete the thin AP self-configuration.

In the carrier-grade Wi-Fi system and IoT application, the capacity of the access point AP is usually far more than 10,000, and the total traffic throughput of the system is greater than 40Gbps. Therefore, only the large-size Wireless LAN Controller can handle such a large amount of system information and endure such a huge pressure. Titan series Wireless LAN Controller based on Intel XEON platform was born for this kind of deployment.

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 Interface 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

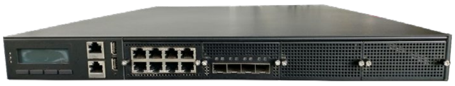
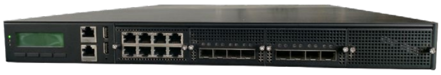
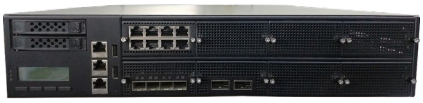
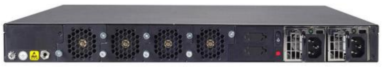
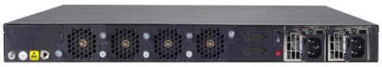
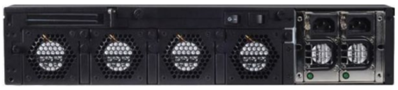
Carefully remove all the items from the packing of WLC. The following items should be included in the packaging:

Package Content	WS200G2	WS500G2	WS1000G2
Power Adapter (DC)	-	-	-
Power Cord (AC)	1	1	1
Mounting Screws (For Disk Drive)	-	-	-
SATA Cables (Data Cable & Power Cable)	-	-	-
Plastic Stand (For Stack-up)	-	-	-
CPU (Intel XEON Family)	1	2	2
10G SFP+ NIC Module (4 Ports)	1	2	1
40G QSFP NIC Module (2 Ports)	-	-	1

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.

<table>
<tr><th colspan="3">Front Panels</th></tr>
<tr><td>WS200G2
</td><td>WS500G2
</td><td>WS1000G2
</td></tr>
<tr><th colspan="3">WS200G2</th></tr>
<tr><td>WS200G2
</td><td>WS500G2
</td><td>WS1000G2
</td></tr>
</table>

The following physical ports are available on the WLC.

Package Content	WS200G2	WS500G2	WS1000G2
RJ45 Ports (10/100/1000Base_TX)	8	8	8
SFP+ Ports (10 GbE)	4	8	4

Package Content	WS200G2	WS500G2	WS1000G2
QSFP Ports (40 GbE)	-	-	2
Console Port (RJ45-RS232)	1	1	1
USB 2.0 Ports	2	2	2
Hard Disk Rack	-	-	2
AC Power Modules	2	2	2
DC Power Port	-	-	-

Chapter 3. SYSTEM FOUNDATION

3.1. SYSTEM ARCHITECTURE

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

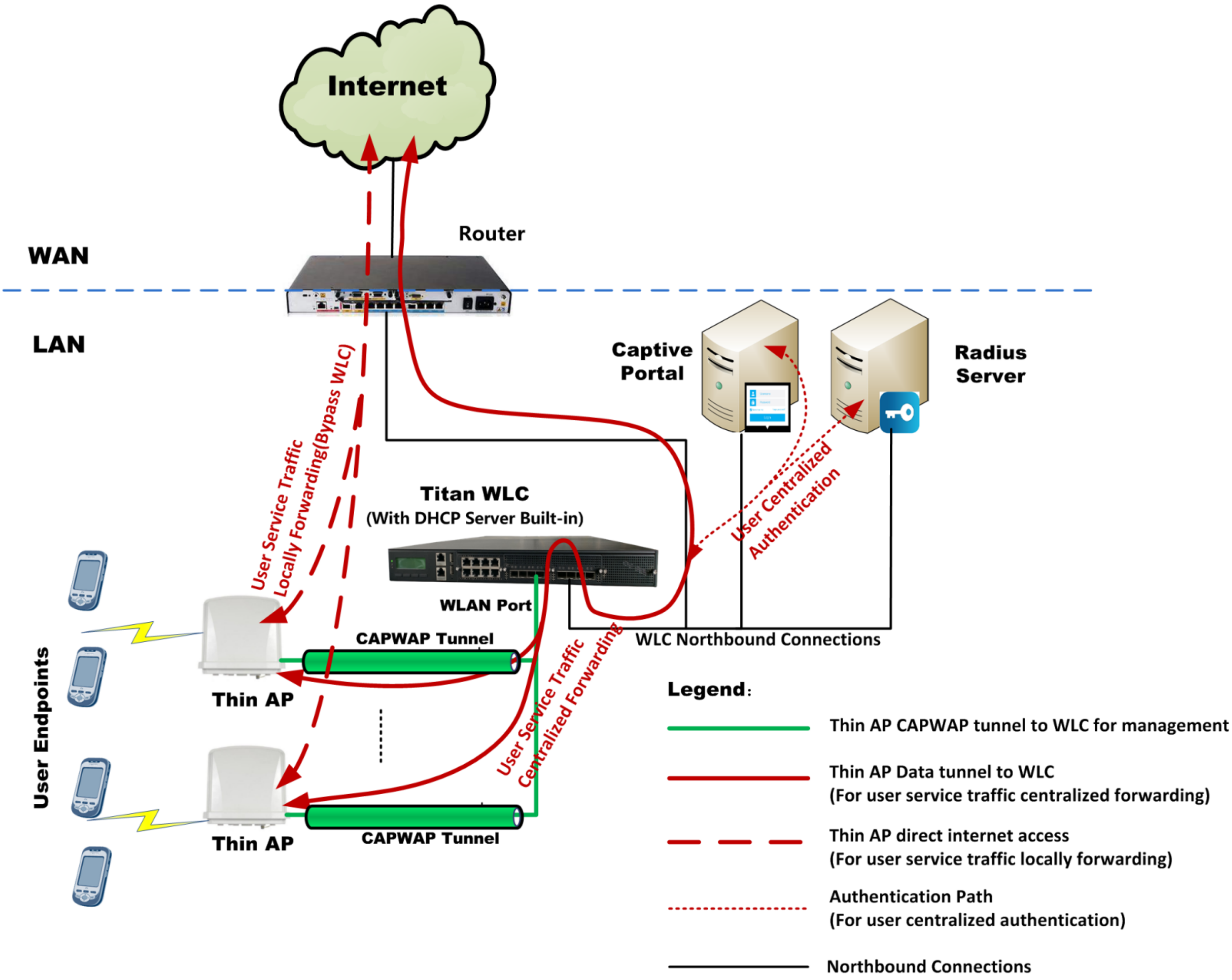

Internet
Router
WAN
LAN
Captive Portal
Radius Server
User Service Traffic Locally Forwarding(Bypass WLC)
Titan WLC
(With DHCP Server Built-in)
User Centralized Authentication
WLAN Port
CAPWAP Tunnel
WLC Northbound Connections
Thin AP
User Endpoints
User Service Traffic Centralized Forwarding
Thin AP
CAPWAP Tunnel
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 Titan WLC

The WLC has a southbound interface named WLAN port to connect to thin APs, and the northbound ports based on WLC internal layer 3 interfaces (VIF) to connect to the core network in which there are Portal / Radius servers for user authentication and accounting, and the PDN gateway for user Internet services.

Two types of tunnel are established from Thin AP to WLC:

- The **CAPWAP** tunnel: an access stratum management tunnel, focusing on provisioning AP and statistics reports.
- The **WLTP** data tunnel: focusing on wireless clients non-access stratum data transmission, including user data traffic and authentication messages.

Both tunnels start at the thin AP.

The initial state of the thin AP is zero configured. At the power-on stage, it firstly discovers the Wireless LAN Controller through the DHCP protocol, and obtains the IP addresses of up to 4 available WLCs from the DHCP Option 43 response message. Thin AP uses the first IP address to establish the main CAPWAP tunnel to master WLC, other redundant WLCs are used as backup equipment in case of the master failure. After the CAPWAP tunnel is established, the thin AP downloads profiles from the WLAN Controller through the CAPWAP tunnel to complete its self-configuration. Finally, the wireless clients associate with the thin AP and initiate authentication and data services through the WLTP data tunnel.

The first data service initiated by the wireless client will be intercepted by the WLAN Controller to check whether it is an authenticated legal user. If not, this access will be redirected to the Captive Portal server, and an entrance web page for user to enter the name and password is forcibly pushed to the user endpoint. The user name and password entered in the portal page is forwarded to the Radius server for authentication through the WLAN Controller.

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 **115200**.

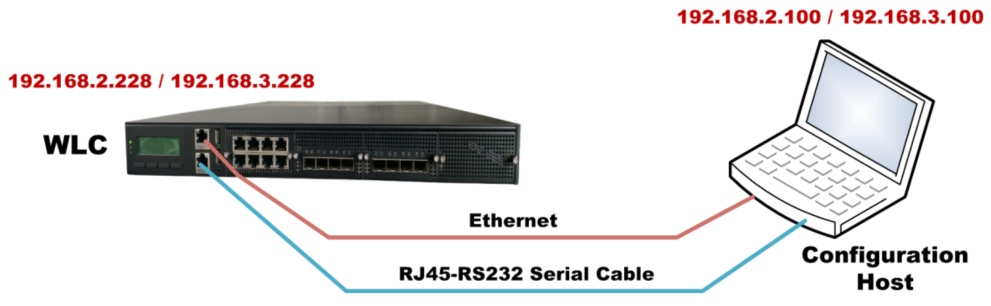


Figure 3-2 Host Laptop Connects to the WLC for Configuration and Maintenance

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 layer 3 interface (VIF) 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.

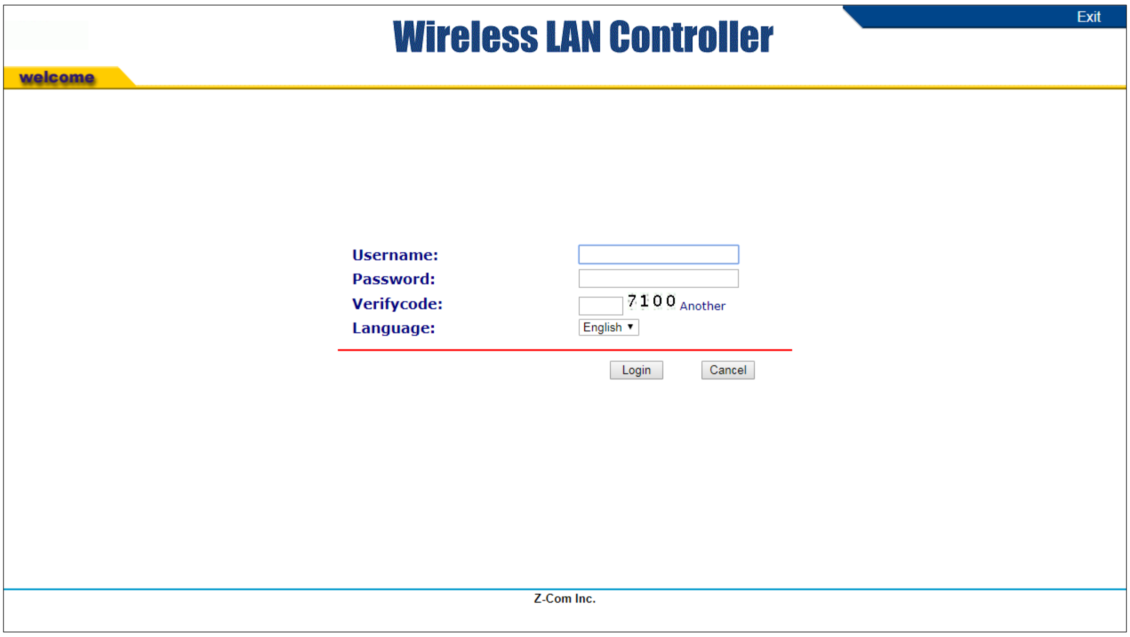
The default login credentials for WLC management is as the following:

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

3.3. ENTRANCE OF WEB MODE PROVISION

Compared with the CLI mode, the WLAN controller also provides a user-friendly management interface, that is, the management and provisioning interface in the Web mode. Customers can use standard browsers (such as IE, Chrome or Firefox, etc.) to access through HTTP/HTTPS protocol.

Open the browser on the configuration host, enter the default IP address (**192.168.2.228** to access the management port, or **192.168.3.228** to access the service port) in the address bar, and get into the web page shown in the figure below:



Wireless LAN Controller

Username:

Password:

Verifycode: 7100

Language: English

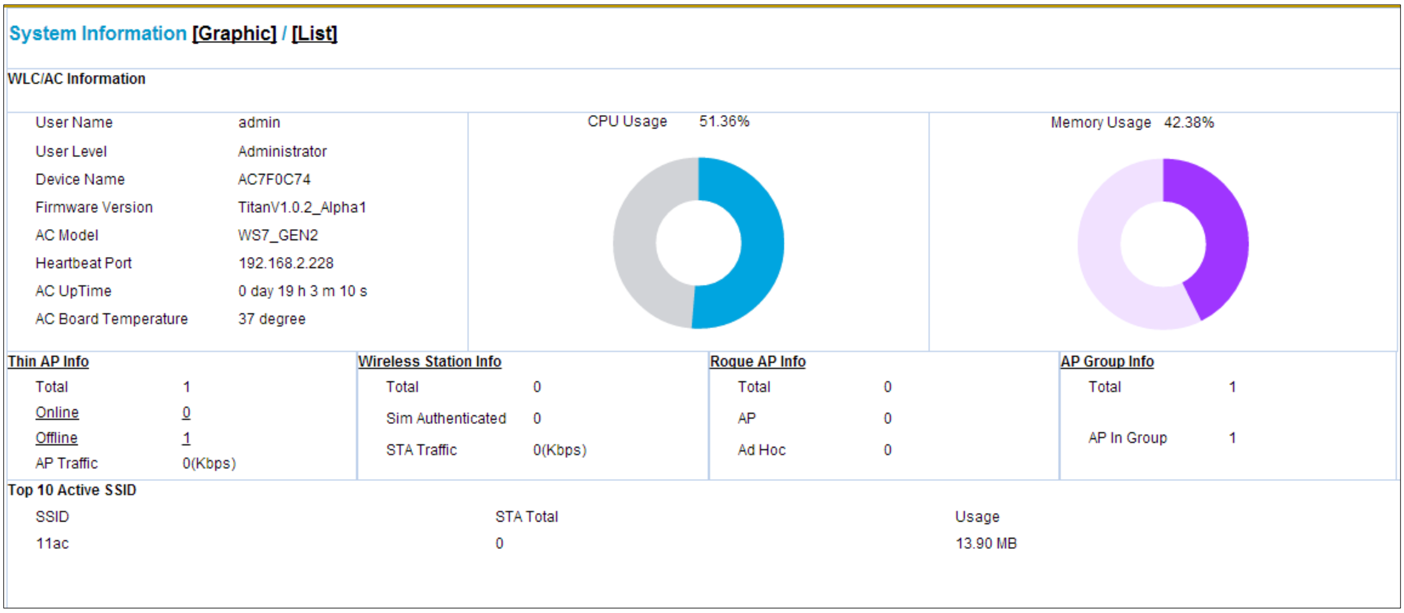
Figure 3-3 Web Management Interface (Login Page)

Enter the user name and password with the random generated verification code on the login page, and click the <**Login**> button to enter the provisioning page of the WLAN controller.

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

3.4. System Information

After successfully login the provisioning web page, the system overview page shown in the figure below will pop up firstly:



System Information [Graphic] / [List]

WLC/AC Information

User Name	admin
User Level	Administrator
Device Name	AC7F0C74
Firmware Version	TitanV1.0.2_Alpha1
AC Model	WS7_GEN2
Heartbeat Port	192.168.2.228
AC UpTime	0 day 19 h 3 m 10 s
AC Board Temperature	37 degree

CPU Usage 51.36%

Memory Usage 42.38%

Thin AP Info

Total	1
Online	0
Offline	1
AP Traffic	0(Kbps)

Wireless Station Info

Total	0
Sim Authenticated	0
STA Traffic	0(Kbps)

Rogue AP Info

Total	0
AP	0
Ad Hoc	0

AP Group Info

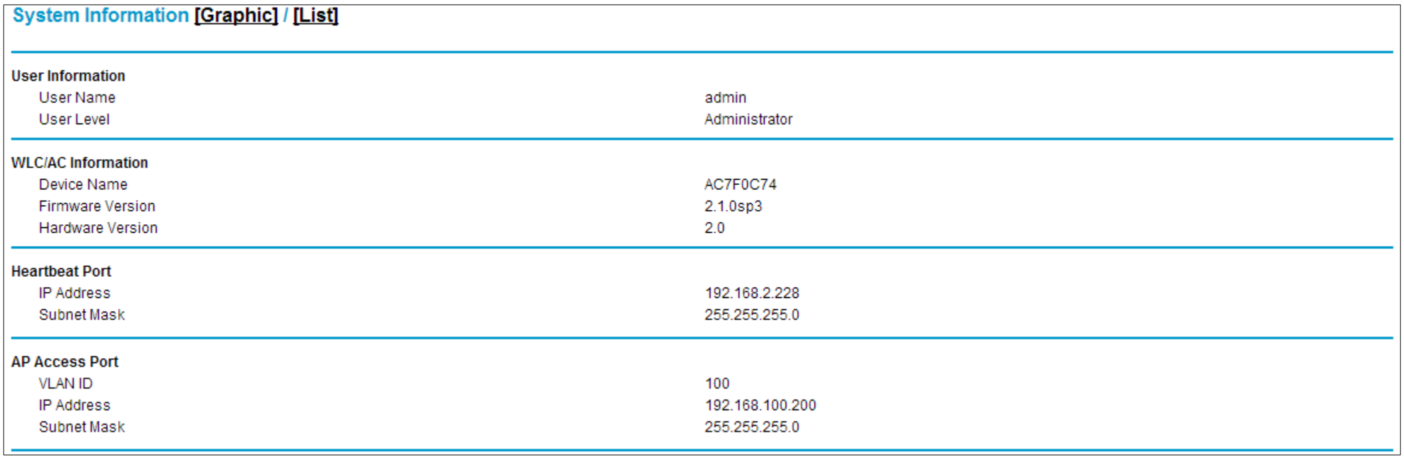
Total	1
AP In Group	1

Top 10 Active SSID

SSID	STA Total	Usage
11ac	0	13.90 MB

Figure 3-4 System Information Page (Graphic Mode)

The WLAN Controller provides two system summary information display modes: graphic mode and list mode. The user can choose to enter the desired mode by clicking the hyperlink on the upper left. The default mode is the graphics mode shown in the figure above. The list mode is shown below:



System Information [Graphic] / [List]

User Information	
User Name	admin
User Level	Administrator
WLC/AC Information	
Device Name	AC7F0C74
Firmware Version	2.1.0sp3
Hardware Version	2.0
Heartbeat Port	
IP Address	192.168.2.228
Subnet Mask	255.255.255.0
AP Access Port	
VLAN ID	100
IP Address	192.168.100.200
Subnet Mask	255.255.255.0

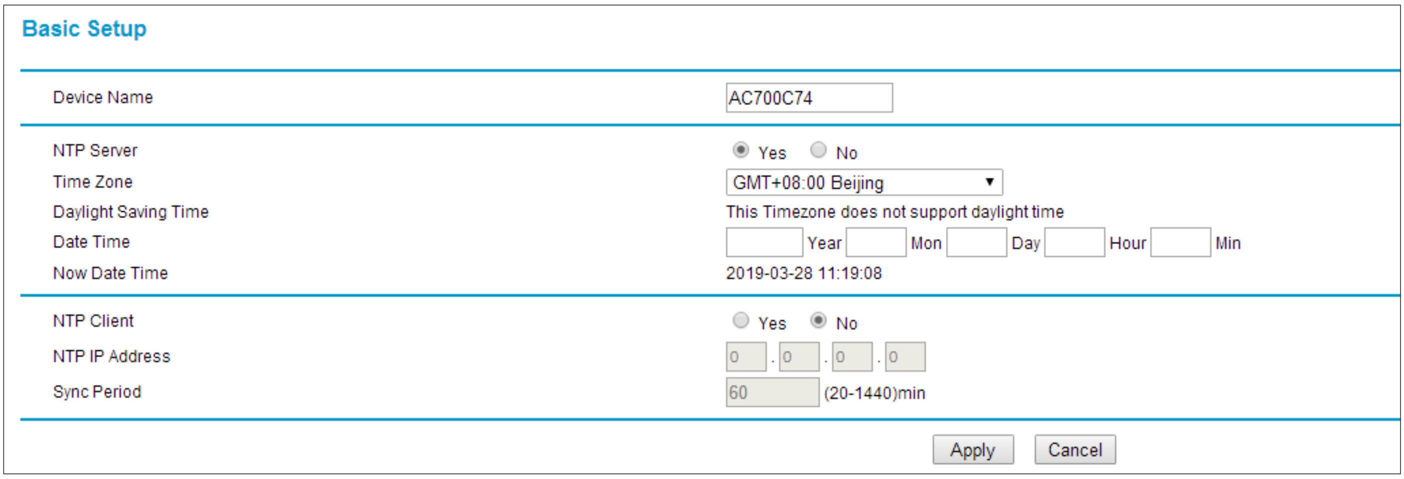
Figure 3-5 System Information Page (List Mode)

Due to the limitation of the screen area, the two display modes can only display part of the system information respectively. Therefore, if need to obtain the complete information, the contents of the two display modes should be combined.

3.5. Basic Setup

The basic setting refers to the setting of parameters related to the field site after the WLAN Controller is deployed, such as time zone and date time. It is also necessary to assign the WLC a literal name for engineering management.

Select **[Basic Setup]** in the menu to enter the configuration page as following:



Basic Setup

Device Name: AC700C74

NTP Server: ● Yes ○ No

Time Zone: GMT+08:00 Beijing

Daylight Saving Time: This Timezone does not support daylight time

Date Time: Year Mon Day Hour Min

Now Date Time: 2019-03-28 11:19:08

NTP Client: ○ Yes ● No

NTP IP Address: 0 . 0 . 0 . 0

Sync Period: 60 (20-1440)min

Figure 3-6 Basic Setup Page

These parameters in **[Basic Setup]** page is described in details as following:

Parameter	Description
Device Name	Assign a literal name for this WLC for engineering management.
NTP Server	The thin AP cannot keep the time on board after power down, and it needs to obtain the time reference from the outside when it works. The WLAN Controller has a built-in NTP server, which can provide time synchronization services for the thin AP during its running.
Time Zone	Select the time zone where the WLAN Controller is deployed.
Daylight Saving Time	If the area where the WLAN Controller is deployed uses daylight saving time, select the adjustment compensation here.
Date Time	Manually set the date time here for WLC.
Now Date Time	Display current date time in WLC.
NTP Client	As the time reference of the thin AP, the WLC itself must have its time been calibrated frequently. For this reason, it has a built-in NTP client for time synchronization with an external precise time source. Open the switch here to enable the built-in NTP client for time calibration.
NTP IP Address	Enter the IP address of the NTP server that is the external precise time source of the WLC.
Sync Period	The WLAN Controller periodically calibrate and synchronize its time with an external precise time source. Here, set the time interval of calibration for the WLC.

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

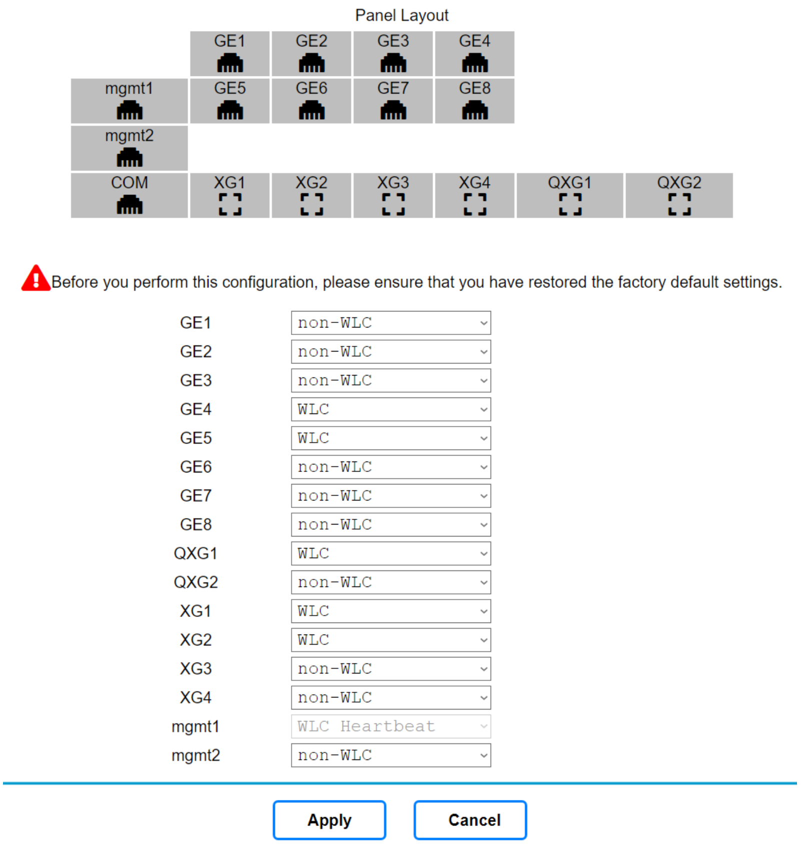
Click the **Cancel** button to discard the changes.

Chapter 4. Network Configuration

4.1. Port Classification

Titan series WLC include three models of WS200G2, WS500G2 and WS1000G2, which provide a different number of 1G, 10G and 40G network ports. However, the WLAN Controller itself does not need to use all physical ports. Therefore, the ports on the panel must be classified before running, that is, to divide which ports will be used by the WLAN Controller, and which ports will be used by OS and other applications.

Select **[Network Setup** > **Port Classification]** in the menu to enter the configuration page as following (here is the Port Layout of ***WS1000G2*** as the example):



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

GE1	non-WLC
GE2	non-WLC
GE3	non-WLC
GE4	WLC
GE5	WLC
GE6	non-WLC
GE7	non-WLC
GE8	non-WLC
QXG1	WLC
QXG2	non-WLC
XG1	WLC
XG2	WLC
XG3	non-WLC
XG4	non-WLC
mgmt1	WLC Heartbeat
mgmt2	non-WLC

Figure 4-1 WLC Port Classification (WS1000G2 as example)

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

Parameter	Description
Mgmt1~2	Two local management 1GbE ports directly connected to CPU1 and CPU2 (if existed). **Note:** The mgmt-1 port is also the heartbeat port for 1+1 backup scheme.
GE1~8	There are eight 1G ports in the form of RJ45. They can be classified into two types according to the usage: ▪ **WLC:** This port is used by the WLC. It can be used either as the thin AP

Parameter	Description
	access port or as the service port for user authentication and user traffic central switching. ▪ **Non-WLC:** This port is used by the OS or other applications.
XG1~4	There are four 10G ports in the form of SFP+. They can be classified into two types according to the application: ▪ **WLC:** This port is used by the WLC. It can be used either as the thin AP access port or as the service port for user authentication and user traffic central switching. ▪ **Non-WLC:** This port is used by the OS or other applications.
QXG1~2	There are two 40G ports in the form of QSFP. They can be classified into two types according to the application: ▪ **WLC:** This port is used by the WLC. It can be used either as the thin AP access port or as the service port for user authentication and user traffic central switching. ▪ **Non-WLC:** This port is used by the OS or other applications.

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

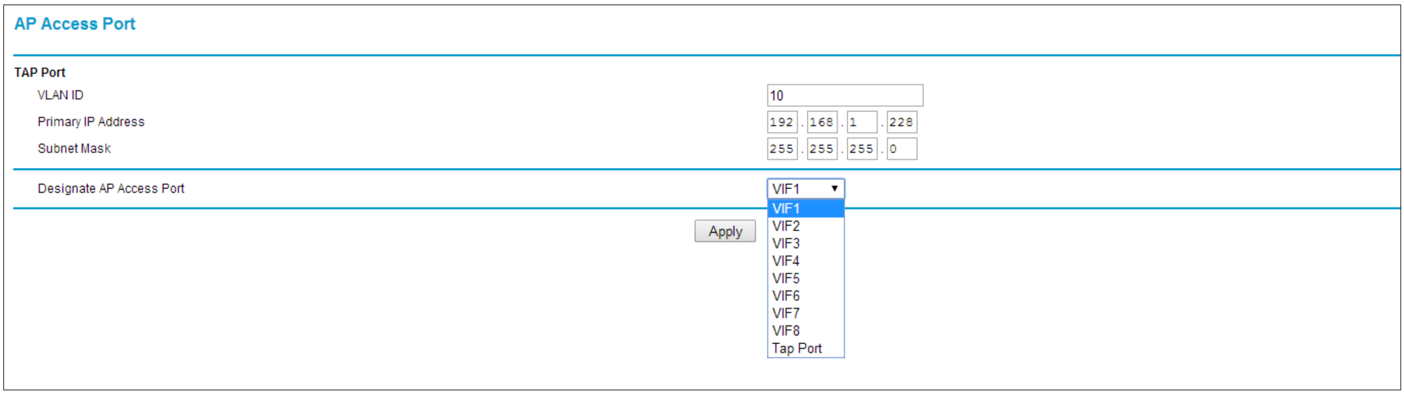
Note: Usually one or two ports being allocated to WLC usage are sufficient for most of Wi-Fi networking requirements!

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

4.2. AP Access Port

The WLC has a southbound WLAN port facing the radio access network (RAN), it is exactly used as the thin AP access port (TAP port). Thin AP establishes a CAPWAP tunnel with the WLC at this port to implement its configuration, management, and statistics reporting. The AP access port can also be reassigned to another internal layer 3 interface (VIF) except the TAP port, but this is not recommended.

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



AP Access Port

TAP Port

VLAN ID: 10

Primary IP Address: 192.168.1.228

Subnet Mask: 255.255.255.0

Designate AP Access Port: VIF1

Figure 4-2 AP Access Port Page

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

Parameter	Description
VLAN ID	Assign a management VLAN ID to the thin AP access port to distinguish it from the user service VLAN on the same physical port (if the user data tunnel is also established at the same physical port). **Note:** This VLAN ID cannot be an any value, it must be an available VLAN which is previously created in [**Network > VLAN Creation**].
IPv6 Address	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 as backup.
Subnet Mask	Allocate a netmask for the 'AP Access Port' to divide which subnet the WLAN port belongs to.
Designate AP Service Port	AP service port is distinguished from the AP access port, it is used to transmit user service traffic on the WLC. It can be any internal Layer 3 interface (VIF), or it may share the thin AP access port (TAP)　(at this time, the management packets and user service traffic must be distinguished by VLAN). The default is to share the TAP port.

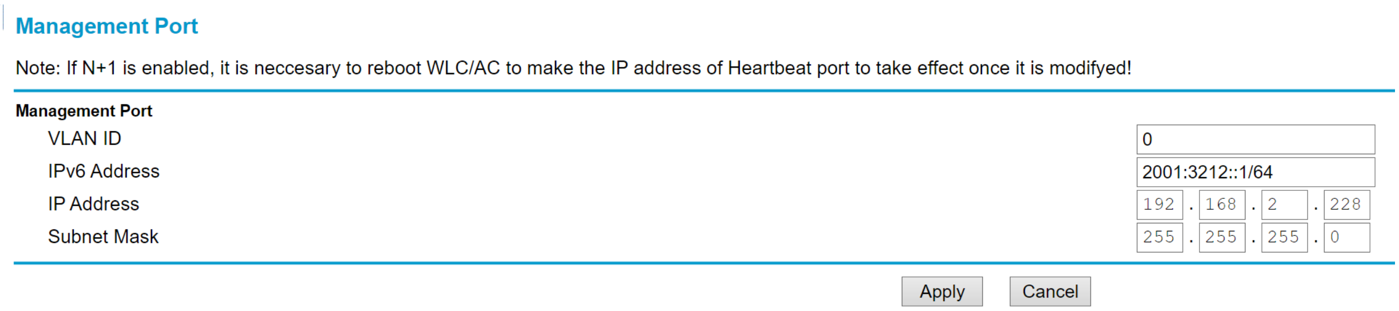
Click the **Apply** button to accept the changes.

Note: The TAP port defaults to the thin AP access port, and the thin AP access port can also be assigned to other layer 3 interface (VIF), but it is not recommended! .

4.3. HEARTBEAT PORT

When the WLC works in the 1+1 backup mode, it needs to exchange and synchronize the configuration parameters, and the state information of thin AP and user clients between the master and standby equipment through a specific heartbeat port. This heartbeat port is fixed to be the first management port (***mgmt-1***). Refer to Figure 10-3 for details of 1+1 backup system connection

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



Management Port

Note: If N+1 is enabled, it is neccesary to reboot WLC/AC to make the IP address of Heartbeat port to take effect once it is modifyed!

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 Heartbeat Port Settings Page

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

Parameter	Description
VLAN ID	Allocate a VLAN ID to the Heartbeat port (i.e., the mgmt-1 port) if the WLC deployed in a VLAN-configured network.
IPv6 Address	Allocate an IPv6 address to the Heartbeat port (i.e., the mgmt-1 port) if the WLC is deployed in an IPv6 network.
IP Address	Allocate an IPv4 address to the Heartbeat port (i.e., the mgmt-1 port).
Subnet mask	Specify which subnet the Heartbeat port belongs to.

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

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

Note: If these parameters are modified, it is necessary to perform the **Save Configuration** firstly and then **reboot** system to make this modification to take effect.

4.4. VLAN CREATION

If the Wi-Fi system is deployed in a VLAN-configured network, in order to ensure that the packets correctly traverse through each port of the WLC, it must divide the ports into corresponding VLANs. Figure 4-4 shows where and how the VLAN is configured in the WLC. The VLAN of the data plane is used for the user traffic forwarding path, and the VLANs of the control plane in TAP port and layer 3 interfaces are used for CAPWAP, Portal, Radius, DHCP and SNMP packets which are distinguished from the user traffic.

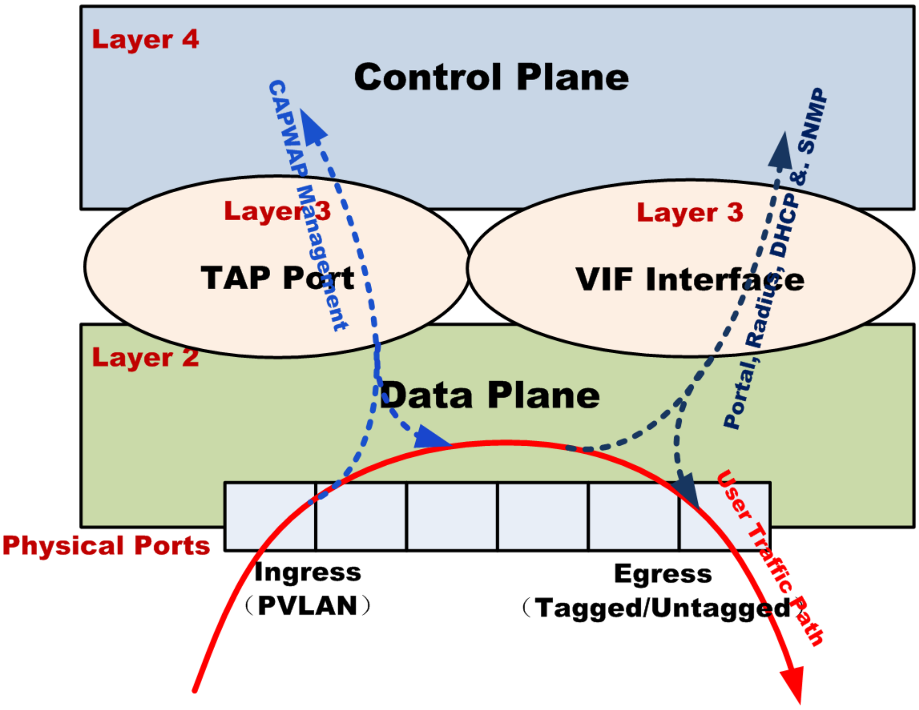
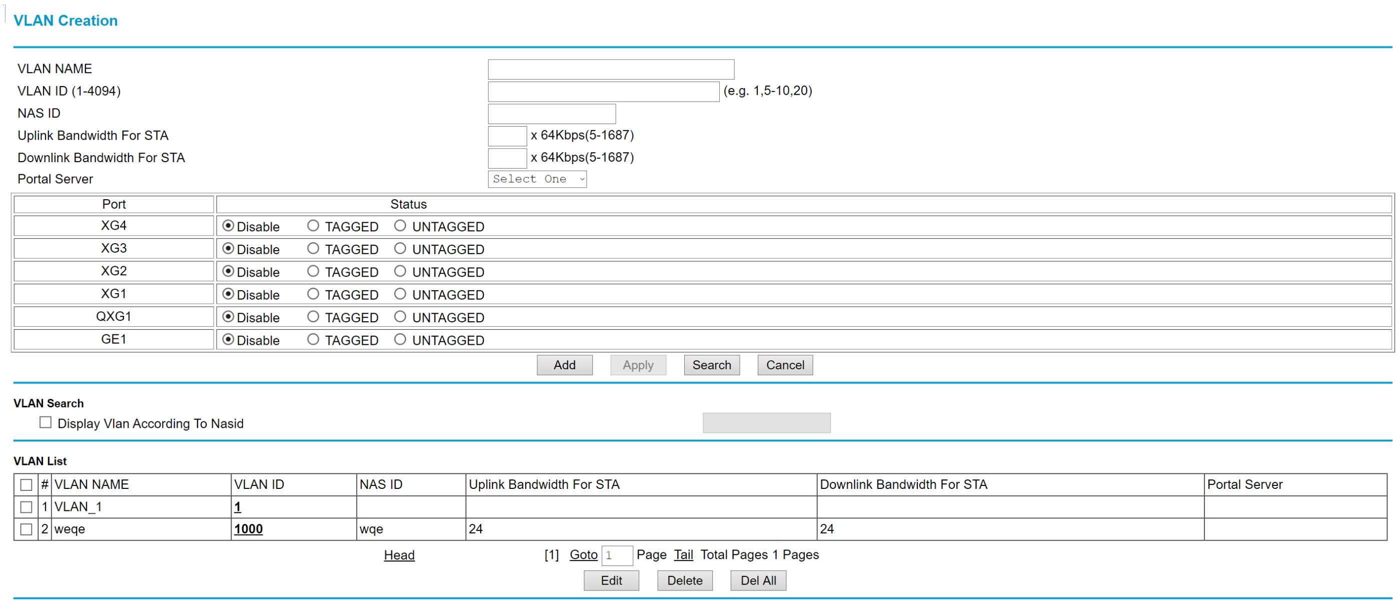


Figure 4-4 The VLAN types in WLC

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



VLAN Creation

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

Port	Status
XG4	● Disable ○ TAGGED ○ UNTAGGED
XG3	● Disable ○ TAGGED ○ UNTAGGED
XG2	● Disable ○ TAGGED ○ UNTAGGED
XG1	● Disable ○ TAGGED ○ UNTAGGED
QXG1	● Disable ○ TAGGED ○ UNTAGGED
GE1	● Disable ○ TAGGED ○ UNTAGGED

VLAN Search

☐ Display Vlan According To Nasid

VLAN List

☐	#	VLAN NAME	VLAN ID	NAS ID	Uplink Bandwidth For STA	Downlink Bandwidth For STA	Portal Server
☐	1	VLAN_1	1				
☐	2	weqe	1000	wqe	24	24	

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

Figure 4-5 VLAN Configuration Page

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

Parameter	Description	
VLAN NAME	Assign a literal name for the new VLAN for engineering management.	
VLAN ID	Allocate a numeric identifier to the new VLAN.	
NAS ID	**NAS-ID** is the abbreviation of **N**etwork **A**ccess **S**ite ID which is required by Radius server for roaming charging and clearing. Its format is as of ***HOST.CITY.PROVICE.OPERATOR.NATION***, for example 0046.0028.280.00.460 in which the exact meaning of each segment depends on the definition of local telecommunication operator.	
Uplink Bandwidth for STA	Uplink rate of wireless clients on this VLAN will be limited within this threshold.	
Downlink Bandwidth for STA	Downlink rate of wireless clients on this VLAN will be limited within this threshold.	
Portal Server	Select a Portal server for the new VLAN, so user clients on this VLAN will use this Portal server for authentication. The Portal Server must be the one configured in [**Authentication** > **Portal Server**].	
Physical Ports **Note:** Only those ports which have been classified to WLC type in [**Port Classification**] can be listed out here for VLAN binding.	**GE1**	The egress of this GbE port can be configured as: ▪ **TAGGED:** Outgoing packet has the VLAN tag. ▪ **UNTAGGED:** Outgoing packet with the VLAN tag stripped off.
	XG1	The egress of this 10GbE port can be configured as: ▪ **TAGGED:** Outgoing packet has the VLAN tag. ▪ **UNTAGGED:** Outgoing packet with the VLAN tag stripped off.
	XG2	The egress of this 10GbE port can be configured as: ▪ **TAGGED:** Outgoing packet has the VLAN tag. ▪ **UNTAGGED:** Outgoing packet with the VLAN tag stripped off.

Parameter	Description	
	XG3	The egress of this 10GbE port can be configured as: ▪ **TAGGED:** Outgoing packet has the VLAN tag. ▪ **UNTAGGED:** Outgoing packet with the VLAN tag stripped off.
	XG4	The egress of this 10GbE port can be configured as: ▪ **TAGGED:** Outgoing packet has the VLAN tag. ▪ **UNTAGGED:** Outgoing packet with the VLAN tag stripped off.
	QXG1	The egress of this 40GbE port can be configured as: ▪ **TAGGED:** Outgoing packet has the VLAN tag. ▪ **UNTAGGED:** Outgoing packet with the VLAN tag stripped off.
VLAN List	Click <**Add**> button to append above new VLAN configuration to the VLAN list. Only those VLAN IDs in this list are available for WLC configuration.	

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

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

Click the **Search** button to search for an entry based on the information specified.

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

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

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

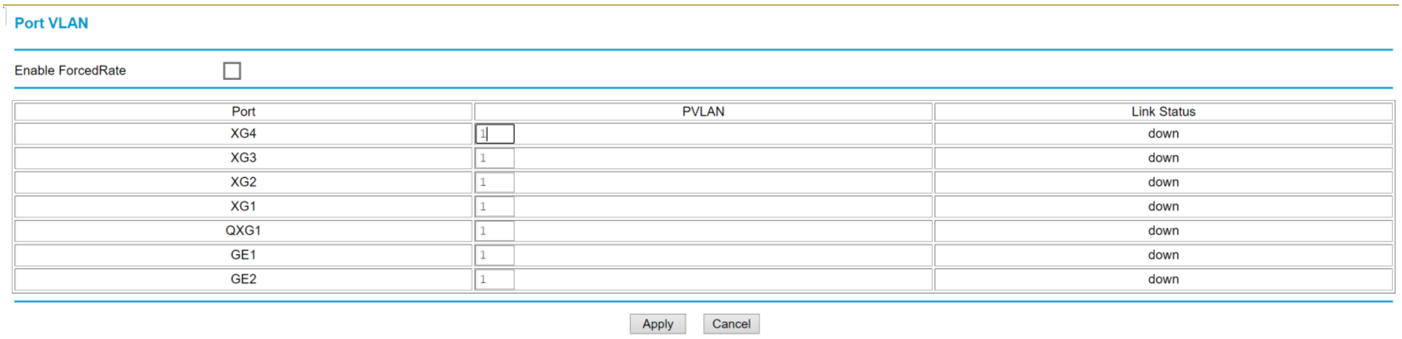
Click the **Del All** button to remove all the entries from the list.

4.5. Port VLAN

The physical port is the entrance for external data packets to enter the WLC. If it is deployed in a VLAN-configured network, the physical port as the packet ***ingress*** must configure the PVLAN for it so as 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 VLAN configuration.

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



Port VLAN

Enable ForcedRate □

Port	PVLAN	Link Status
XG4	1	down
XG3	1	down
XG2	1	down
XG1	1	down
QXG1	1	down
GE1	1	down
GE2	1	down

Figure 4-6 Port VLAN Configuration Page

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

Parameter	Description
Enable ForcedRate	Turn on this switch to disable the speed auto-negotiation function for all physical ports.
GE1~GE2	The GbE physical port as the ***ingress*** is configured as: ▪ **PVLAN:** The PVLAN ID for these GbE physical ports are used to match the incoming packets tagged with the VLAN IDs. Note, the 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~XG4	The 10G physical port as the ***ingress*** is configured as: ▪ **PVLAN:** The PVLAN ID for this 10G physical port is used to match the incoming packets tagged with 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 10G physical port: **Up** indicates it is activated; **Down** indicates it is disabled.
QXG1	The 40G physical port as the ***ingress*** is configured as: ▪ **PVLAN:** The PVLAN ID for this 40G physical port is used to match the incoming packets tagged with 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 40G physical port: **Up** indicates it is activated; **Down** indicates it is disabled.

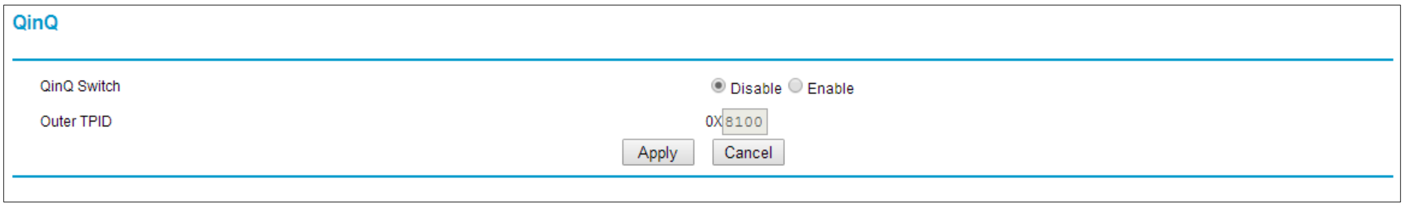
Click the **Apply** button to accept the changes.

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

4.6. QinQ

QinQ is derived from the IEEE-802.1ad standard. It is a VLAN stacking technology that can implement multi-layer VLAN encapsulation. When a packet is transmitted via the public network, in order to distinguish and isolate different services, the operator requires a public VLAN to be encapsulated in the outer layer of the packet, while the user private VLAN is in the inner layer. The packet reaches the opposite gateway, the outer layer public VLAN is stripped off, and the inner packet is taken out to achieve safe traversal of the public network.

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



QinQ

QinQ Switch ● Disable ○ Enable

Outer TPID 0X 8100

Figure 4-7 QinQ Configuration Page

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

Parameter	Description
QinQ Switch	Open this switch to enable the **QinQ** (VLAN-Stacking) function in WLC.
Outer TPID	The outer public VLAN tag is identified by this TPID (Tag Protocol Identifier). By default, this is 0x8100.

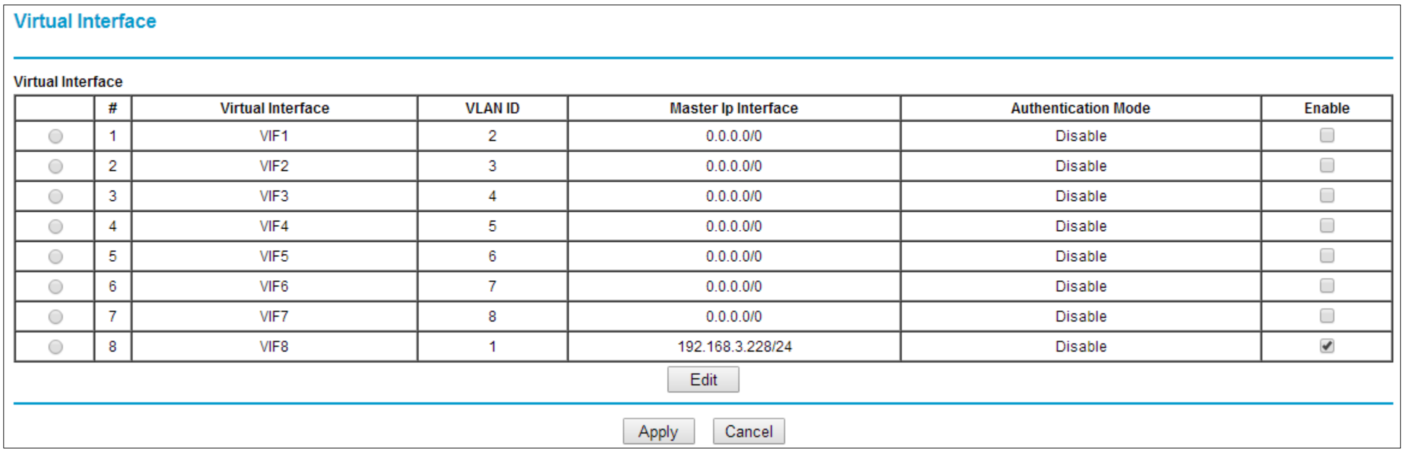
Click the **Apply** button to accept the changes.

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

4.7. VLAN INTERFACE

The VLAN interface (VIF) is the layer 3 interface inside the WLC, through which the upper-layer functional modules such as Portal, Radius, DHCP, CAPWAP, SNMP and so on, communicate with the outside world. Referring to Figure 4-4, since the packets at physical port of WLC are totally distributed by the data plane, the VLAN interface is actually the interface between the control plane and the data plane, so that the layer 3 VLAN interfaces also have to be configured with corresponding management VLAN IDs.

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



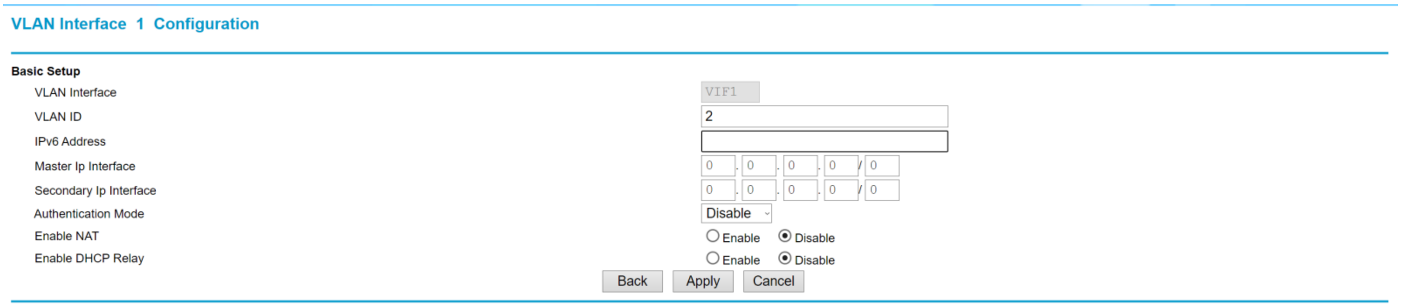
Virtual Interface

Virtual Interface

	#	Virtual Interface	VLAN ID	Master Ip Interface	Authentication Mode	Enable
○	1	VIF1	2	0.0.0.0/0	Disable	□
○	2	VIF2	3	0.0.0.0/0	Disable	□
○	3	VIF3	4	0.0.0.0/0	Disable	□
○	4	VIF4	5	0.0.0.0/0	Disable	□
○	5	VIF5	6	0.0.0.0/0	Disable	□
○	6	VIF6	7	0.0.0.0/0	Disable	□
○	7	VIF7	8	0.0.0.0/0	Disable	□
○	8	VIF8	1	192.168.3.228/24	Disable	☑

Figure 4-8 VLAN Interface Configuration Page

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 4-9 VLAN Interface Edit Page

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

Parameter	Description
VIF1~7	These VLAN Interfaces are configured as below: ▪ **VLAN Interface:** Select a layer 3 interface to configure. ▪ **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 as backup. ▪ **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 on this VLAN will be authenticated by Radius. ▪ **Enable NAT:** NAT(Network Address Translation) function will be enabled for this VLAN. ▪ **Enable DHCP Relay:** External DHCP server can use this layer 3 VLAN Interface for IP address allocation.
VIF8	This VLAN Interface is default used as WLAN port (i.e., the WLC southbound port for thin AP to access, 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.

4.8. L2GRE Tunnel

In the virtual network operator (VNO) application solution, the same Wi-Fi infrastructure can be leased by different virtual operators. Therefore, for management and accounting, it is necessary to logically divide the VNO operators for wireless clients to know whom they belong to. Generally, the VNO operators are represented with virtual AP (identified by different SSID) . The wireless clients just search for the SSIDs to which they belong, and their data paths are connected to their own core networks through different L2GRE tunnels from the northbound ports of the WLC. Figure 4-10 shows a model of this application scenario, where two SSIDs are used to identify two virtual operators: SSID A (representing VNO A) and SSID B (representing VNO B). There are two L2GRE tunnels, which are connected from the northbound port of the WLC to the remote edge L2GRE bridges to reach their core networks.

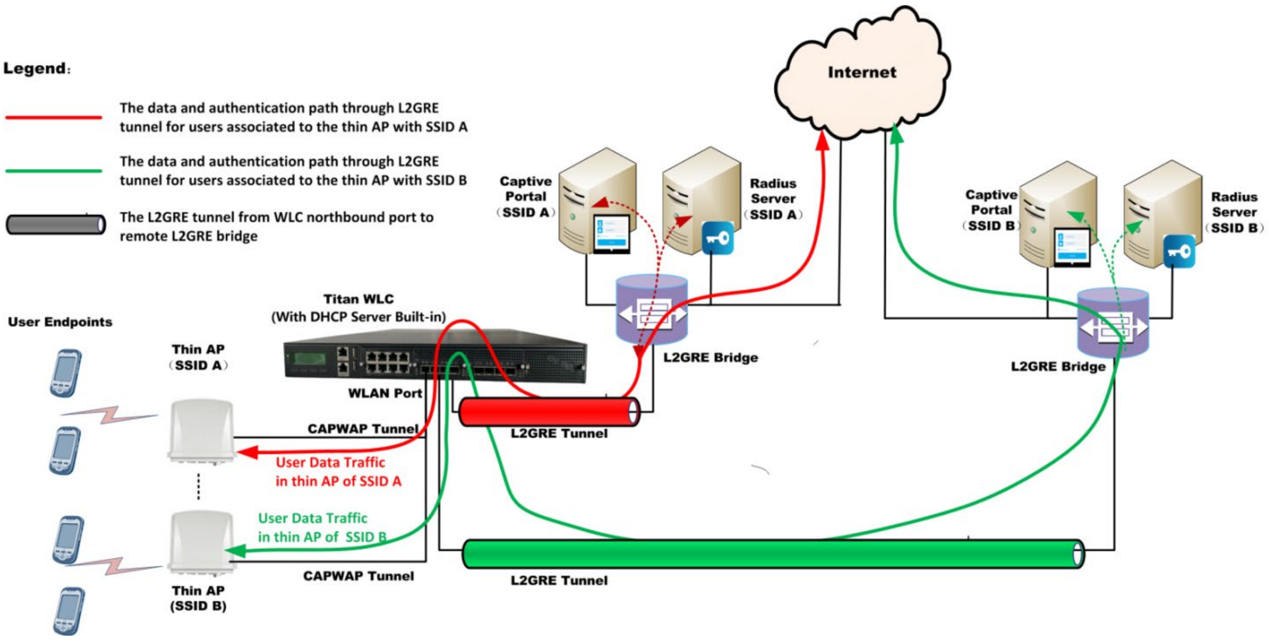
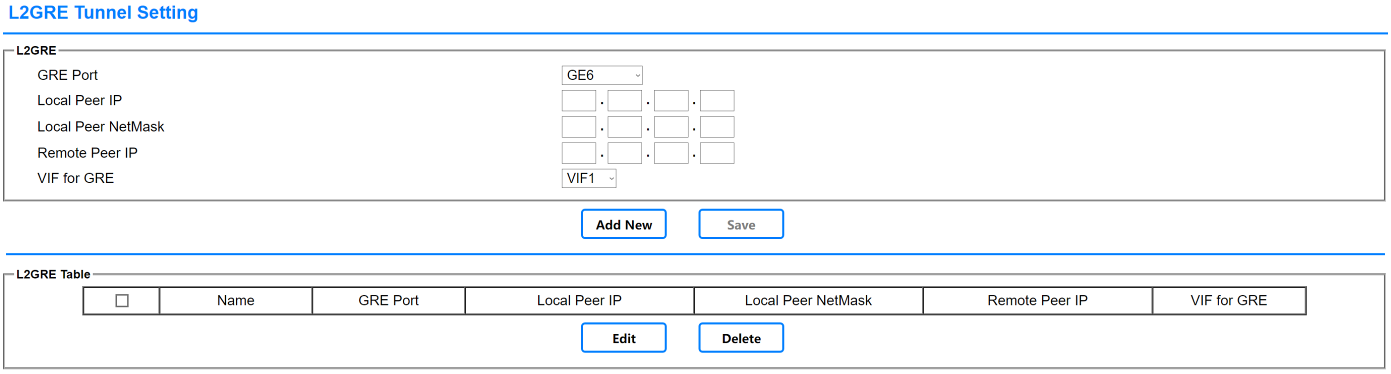

Legend:
The data and authentication path through L2GRE tunnel for users associated to the thin AP with SSID A
The data and authentication path through L2GRE tunnel for users associated to the thin AP with SSID B
The L2GRE tunnel from WLC northbound port to remote L2GRE bridge
Internet
Captive Portal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

Figure 4-10 L2GRE tunnel application in Wi-Fi system

Select **[Network Setup** > **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

Add New Save

L2GRE Table

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

Edit Delete

Figure 4-11 L2GRE Tunnel Configuration Page

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

Parameter	Description
GRE Port	Select a physical port of WLC as the local peer of L2GRE tunnel. **Note**, this port must be the one which has been classified to **non-WLC** type due to this port is under the control of Linux Kernel.
Local Peer IP	Allocate an IP address for WLC local peer of L2GRE tunnel.
Local Peer Netmask	Allocate a netmask for WLC local peer of L2GRE tunnel to divide which subnet it belongs to.
Remote Peer IP	Enter the IP address of remote peer of L2GRE tunnel, i.e., the IP address of remote L2GRE bridge.
VIF for GRE	**Importance:** L2GRE port must use a dedicated layer 3 interface (VIF) to link to WLC upper layer

Parameter	Description
	applications, such as Radius authentication and user data traffic forwarding, and this layer 3 interface (VIF) must have not been configured yet as a service VIF in [**Network> VLAN Interface**]. Here, bind an idle VIF interface to this L2GRE tunnel configuration.
L2GRE Table	Above L2GRE configuration could be appended to a L2GRE table by click <**Add New**> button. The WLC only supports maximum four L2GRE tunnels. Each L2GRE tunnel configuration in this table can be modified by checking it and then click the <**Edit**> button to enter the configuration page.

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.

4.9. **IPSEC / VPN**

In many applications, the northbound link between the WLC and the Wi-Fi core network is required to be secure to protect user data from being hacked, that is, the link is better to be a point-to-point encrypted tunnel. IPSec can meet with this requirement.

Figure 4-12 shows an example of the application, in which the WLC northbound link uses an IPSec tunnel to connect to core network.

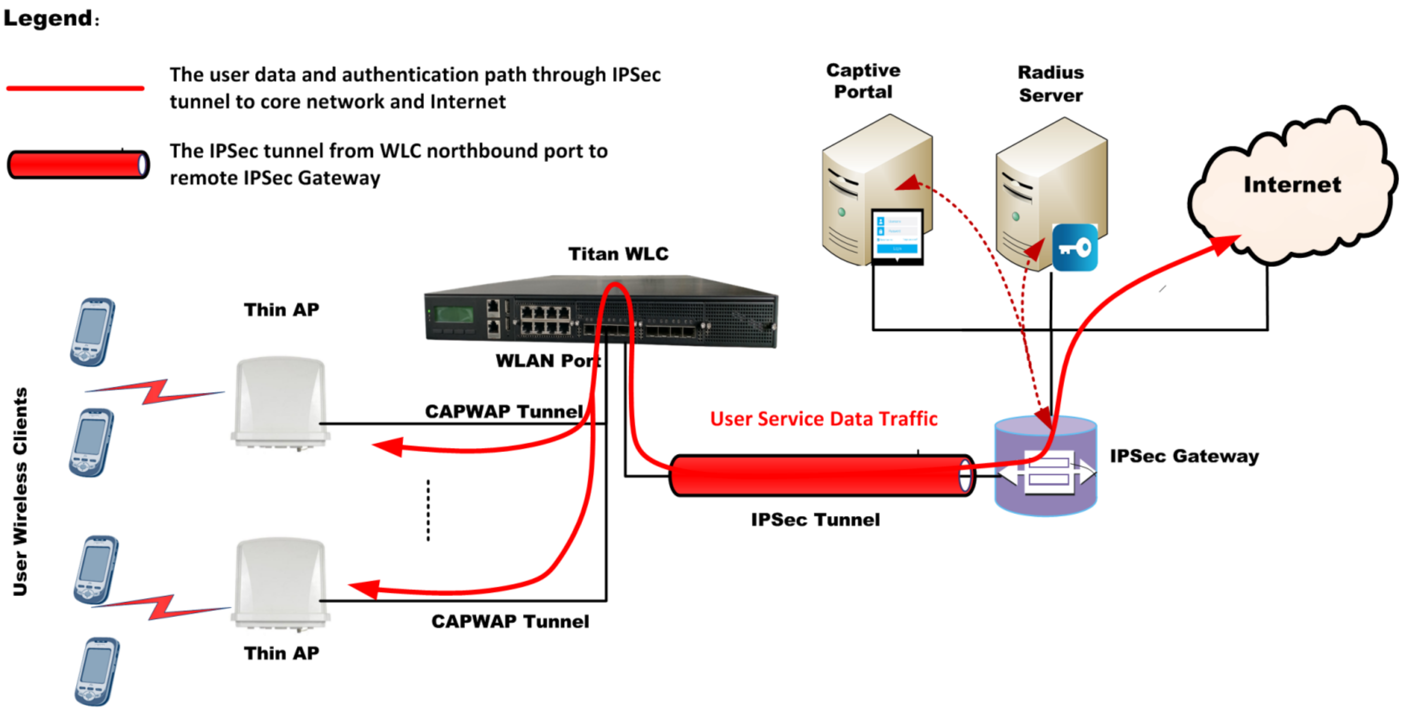
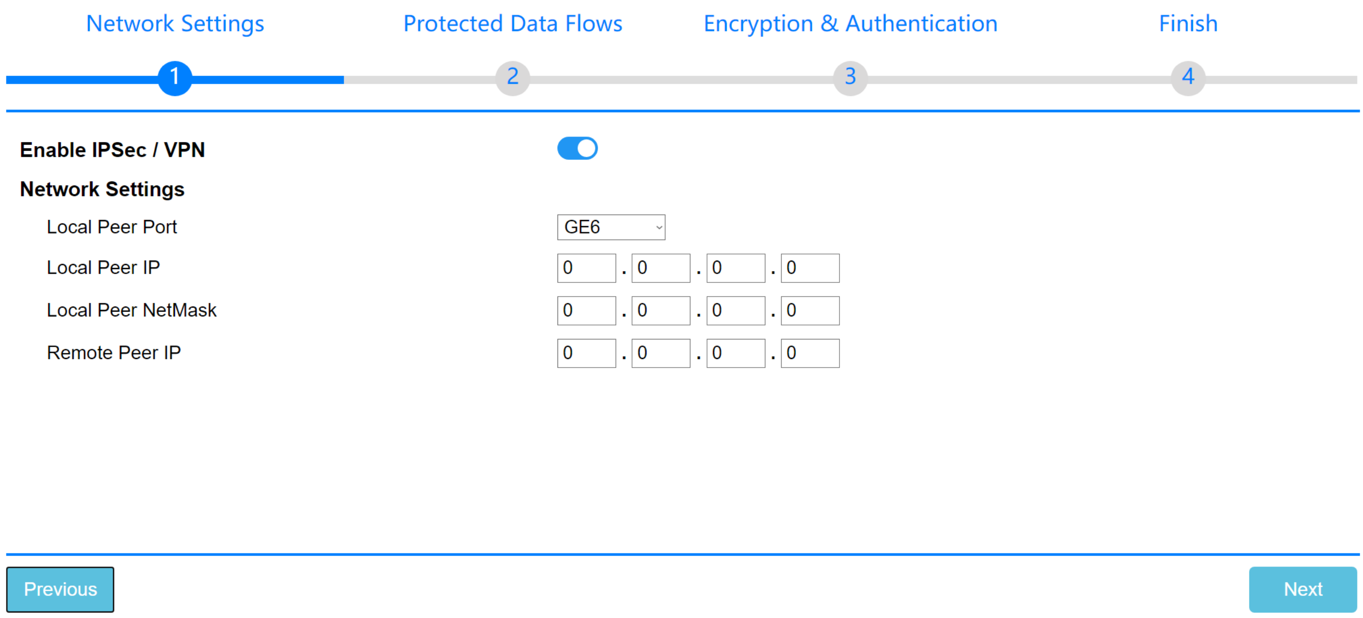

Legend:
The user data and authentication path through IPSec tunnel to core network and Internet
The IPSec tunnel from WLC northbound port to remote IPSec Gateway
Captive Portal
Radius Server
Internet
Titan WLC
Thin AP
WLAN Port
CAPWAP Tunnel
User Service Data Traffic
IPSec Gateway
IPSec Tunnel
User Wireless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

Figure 4-12 IPSec Tunnel Application in Wi-Fi System

Select **[Network Setup** > **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

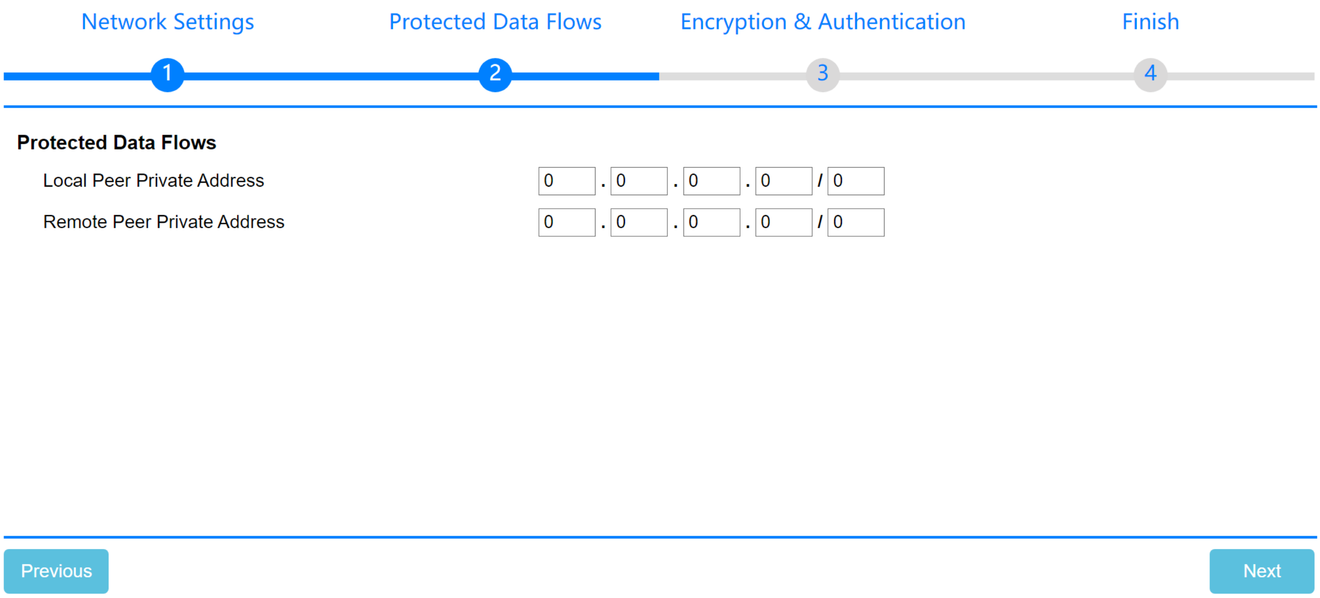
Remote Peer IP: 0 . 0 . 0 . 0

Figure 4-13 IPSec Tunnel Network Configuration Page

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

Parameter	Description
Network Settings	▪ **Enable IPSec / VPN:** Turn on this switch to enable WLC to establish the IPSec tunnel from its northbound port to core network. ▪ **Local Peer Port:** Select a WLC physical port to be the local peer 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 specify which subnet it belongs to. ▪ **Remote Peer IP:** Enter the opposite peer IP address of the IPSec tunnel, in most cases, the IP address of remote IPSec Gateway.

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

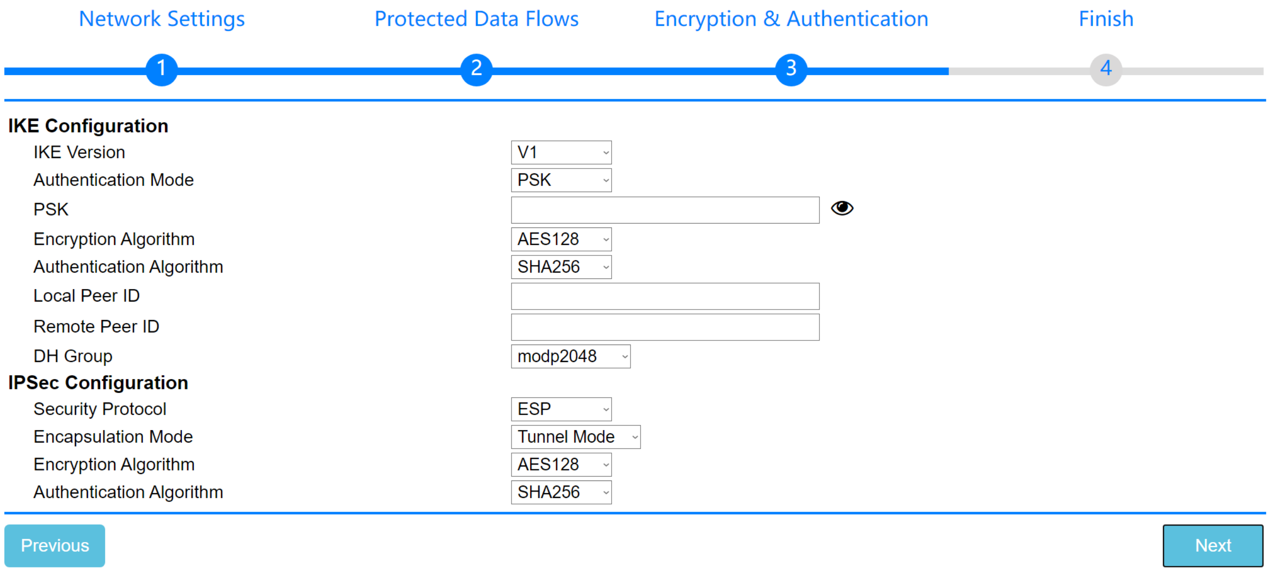
Remote Peer Private Address 0 . 0 . 0 . 0 / 0

Figure 4-14 IPSec Tunnel Protected Data Flows Configuration Page

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

Parameter	Description
Protected Data Flows	The protected data flow stands for the local private network and destination private network behind both ends of IPSec tunnel. They will be encapsulated in the IPSec tunnel as the inner layer: ▪ **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

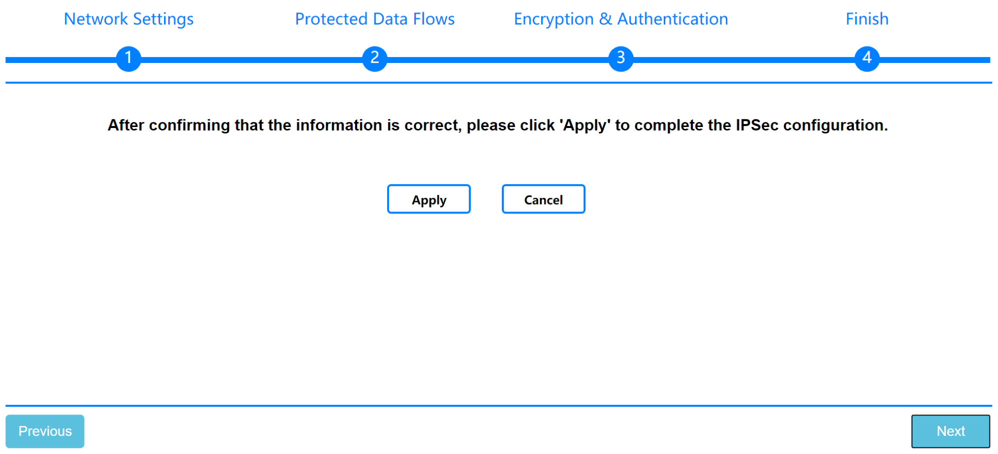
Authentication Algorithm SHA256

Figure 4-15 IPSec Tunnel Encryption and Authentication Configuration Page

These parameters in above page is 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,*** depending on 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 the 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. ▪ **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:



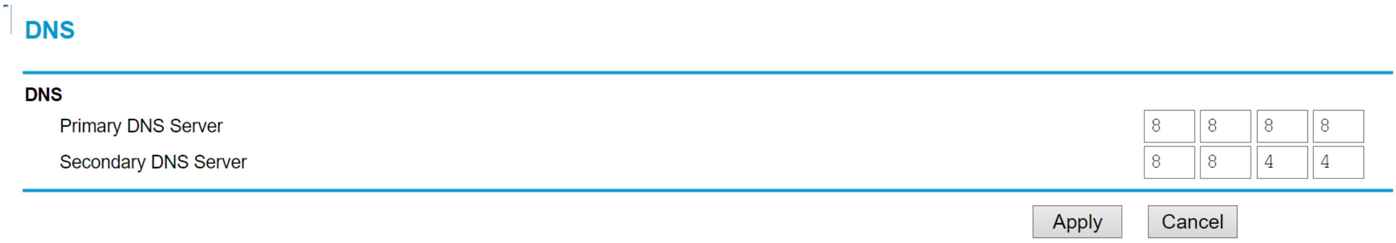
After confirming that the information is correct, please click 'Apply' to complete the IPSec configuration.

Figure 4-16 IPSec Tunnel Configuration Finish Page

4.10. **DNS**

Domain Name Server is necessary in most cases for WLC to have domain name URLs been translated to IP addresses.

Select **[Network Setup** > **DNS]** in the menu to enter the configuration page as followingg:



DNS

DNS

Primary DNS Server 8 . 8 . 8 . 8

Secondary DNS Server 8 . 8 . 4 . 4

Figure 4-17 DNS Page

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

Parameter	**Description**
Primary DNS Server	Enter the IP address of a DNS server that is the most stable and fastest in the WLC deployment area as the primary DNS.
Secondary DNS Server	Enter the IP address of a DNS server that is most widely used in the WLC deployment area as the backup DNS server.

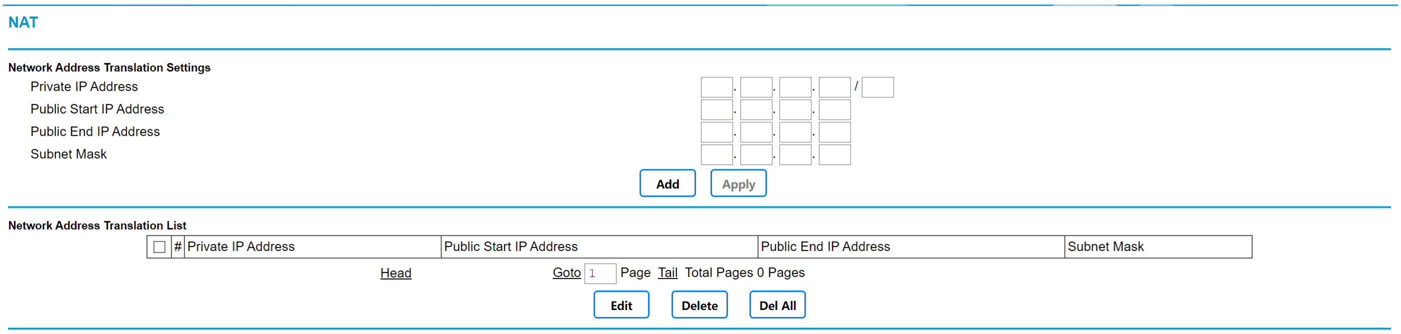
Click the **Apply** button to accept the changes.

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

4.11. **NAT**

NAT is the abbreviation of "Network Address Translation". This is a layer 3 network function, which is usually used on a gateway to implement IP address replacement when packets traverse across different subnets. This section actually statically maps the internal private network IP addresses to the specific external IP addresses to complete the correct IP address replacement and restoration when the packets traverse.

Select **[Network Setup** > **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 4-18 NAT Configuration Page

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

Parameter	Description
Private IP Address	This is the subnet address of private network at NAT inner side.
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 public IP addresses to specify which subnet they belong 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.

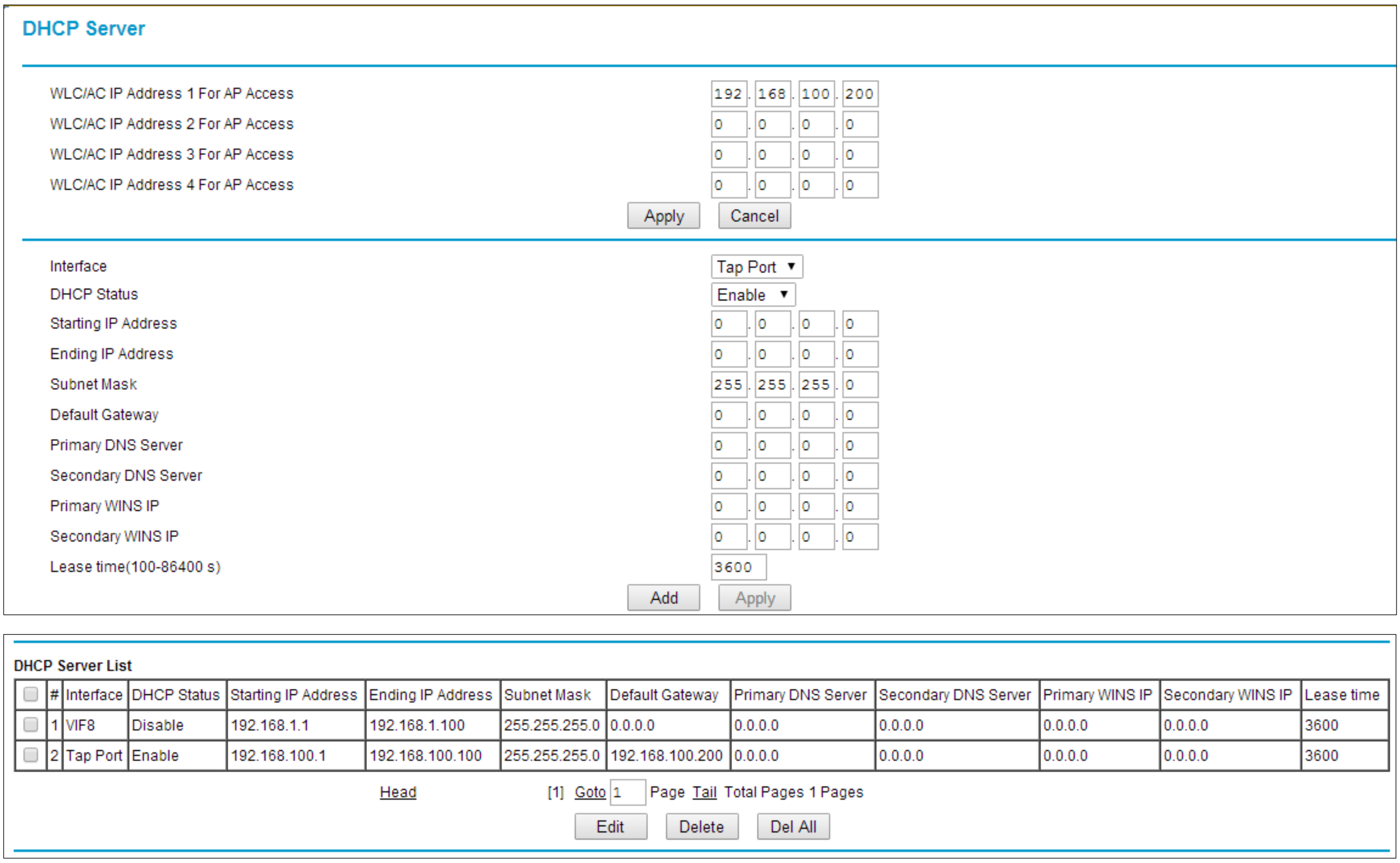
Click the **Delete** button to remove the selected entry.

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

4.12. DHCP SERVER

The WLC has a built-in DHCP server, which can be used to automatically allocate IP addresses to thin APs and wireless clients. To make it work, it is necessary to bind the built-in DHCP server to the internal layer 3 interfaces, such as: TAP (thin AP access port) interface to allocate IP addresses to thin APs; VIF (layer 3 Interface) interface to allocate IP addresses to wireless clients.

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



DHCP Server

WLC/AC IP Address 1 For AP Access	192 . 168 . 100 . 200
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	Disable	192.168.1.1	192.168.1.100	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
□	2	Tap Port	Enable	192.168.100.1	192.168.100.100	255.255.255.0	192.168.100.200	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	3600

Figure 4-19 DHCP Server Configuration Page

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

Parameter	Description
WLC/AC IP Address 1~4 for AP Access	Here the 4 IP addresses represent that up to 4 WLCs can be provided for a thin AP to access. The first IP address represents the main WLC, and the rest serve as alternate equipment. The IP addresses of these WLCs will be told to the thin AP through DHCP Option 43, and the thin AP usually establishes only one CAPWAP tunnel with the main WLC based on the first IP address.
Interface	Binding current DHCP server to the interface below: ▪ **TAP:** The "thin AP access port" is the WLAN port for thin AP accessing to WLC, therefore, the DHCP server bound to this port to allocate IP addresses to thin APs. ▪ **VIF1~8:** Totally 8 layer 3 Interfaces in WLC as the virtual ports for user data services, therefore, the DHCP server bound to these ports to allocate IP addresses to wireless 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	The netmask of current DHCP address pool to specify which subnet this pool belongs to.
Default Gateway	The default gateway IP address for current address pool.
Primary DNS Server	The 1'st DNS server IP address of current DHCP address pool.
Secondary DNS Server	The backup DNS server IP address of current DHCP address pool.
Primary WINS IP	WINS refers to Windows Internet Name Server. Here entering the 1'st WINS IP address for current DHCP address pool.
Secondary WINS IP	WINS refers to Windows Internet Name Server. Here entering the backup WINS IP address for current DHCP address pool.
Lease Time (100~86400 Seconds)	In order to improve the multiplexing rate of the limited IP addresses in the address pool, the IP addresses allocated by DHCP usually have a life cycle, and are invalid when expire. This is the DHCP lease time, the default is 3600 seconds.

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

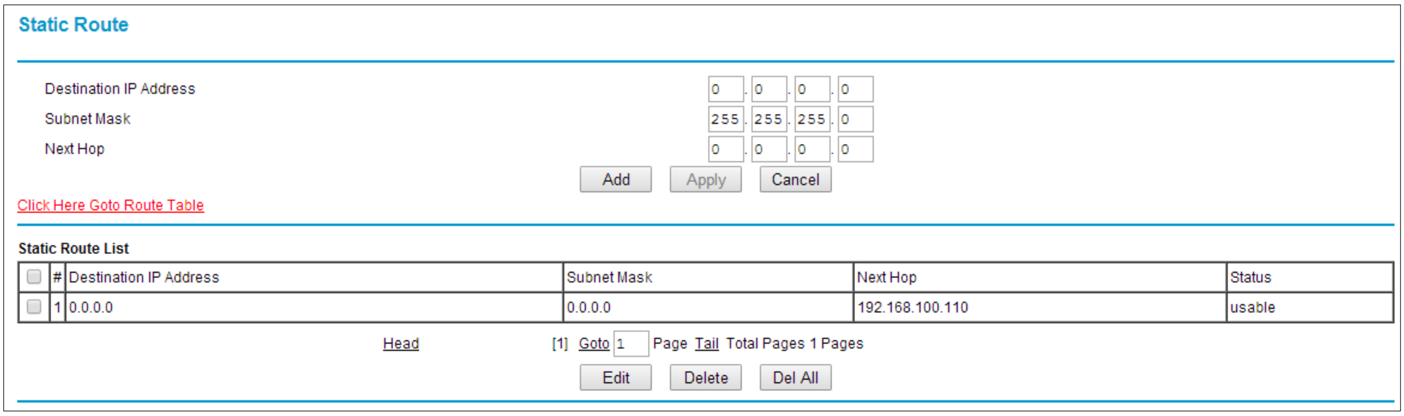
Click the **Del All** button to remove all the entries from the configuration.

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

4.13. STATIC ROUTE

When a packet is sent to a specific destination address that is not in the same subnet as the originator's IP address, it can statically bind the specific destination IP address to a fixed hop address because the route is unknown. Once the destination IP of the packet matches the specific IP address, the packet is immediately redirected to the fixed hop address for the next route. In this way, the packet is sent to the final destination IP step by step. The binding relationship of this specific destination IP address to the fixed hop is the static routing.

Select **[Network Setup** > **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

Add Apply Cancel

Click Here Goto Route Table

Static Route List

□	#	Destination IP Address	Subnet Mask	Next Hop	Status
□	1	0.0.0.0	0.0.0.0	192.168.100.110	usable

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

Edit Delete Del All

Figure 4-20 Static Route Configuration Page

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

Parameter	Description
Destination IP Address	This is the specific IP address which is used to match with the destination address of packets so as to redirect to a known next hop.
Subnet Mask	Allocate a netmask to this specific destination IP address to specify which subnet it belongs to.
Next Hop	The static redirect target address for the packet whose destination IP is matched with the above specific IP address. It is for next routing.

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

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.

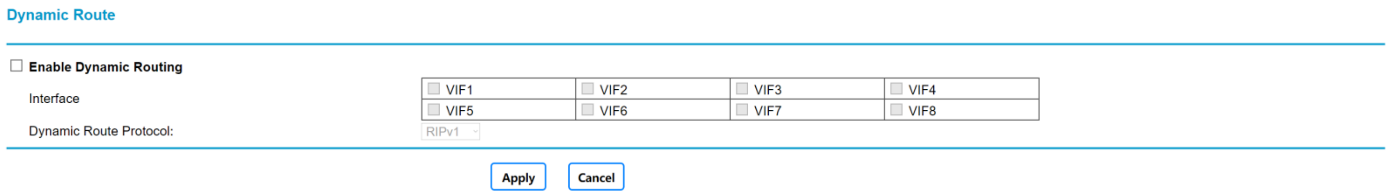
Click the **Del All** button to remove all the entries from the configuration.

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

4.14. DYNAMIC ROUTE

The difference between dynamic routing and static routing is that the next hop IP address is not statically bound but automatically selected by routing algorithms. ***RIPv1*** and ***OSPF*** are two usual routing algorithms, which can be mapped to the Layer 3 interface (VIF) of the WLC to implement dynamic routing of user data packets.

Select **[Network Setup** > **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 4-21 Dynamic Rote Configuration Page

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

Parameter	Description
Enable Dynamic Routing	Open this switch enables the dynamic routing function for WLC.
Interface	Binding the dynamic routing function to WLC internal specific layer 3 Interface (VIF) for user services traffic routing.
Dynamic Routing Protocl	Select the proper dynamic routing protocol: ***RIP*** or ***OSPF***.

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

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

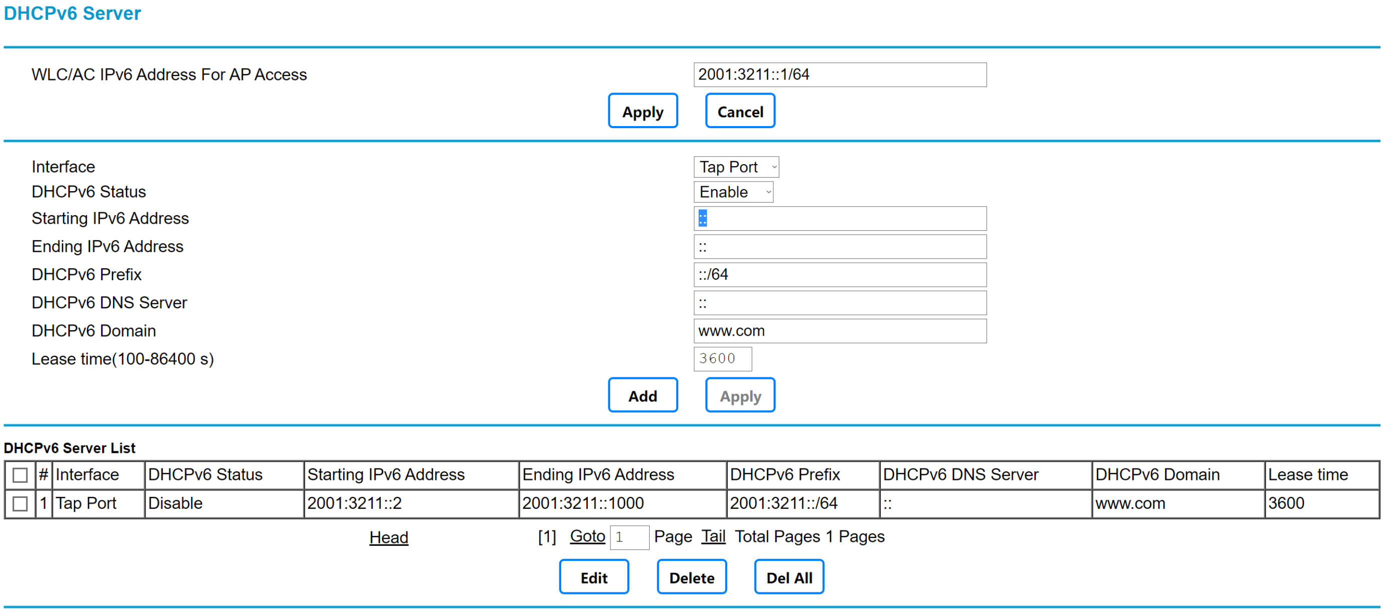
Chapter 5. IPv6 CONFIGURATION

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 the IPv6 network, the built-in DHCP server of the WLC will provide IPv6 address allocation services for thin APs and wireless clients. Therefore, its DHCP server must be configured in accordance with the 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	The IPv6 address of the WLC, which the thin AP obtains through DHCPv6 Option 43 to establish a CAPWAP tunnel with WLC.
Interface	The DHCPv6 server has to be bound to the WLC interfaces to take effect: ▪ **TAP:** The “thin AP access port” is the WLAN port for thin AP accessing to WLC, therefore, the DHCPv6 server bound to this port to allocate IP addresses to thin APs. ▪ **VIF1~8:** Totally 8 layer 3 Interfaces in WLC as the virtual ports for user data services, therefore, the DHCPv6 server bound to these ports to allocate IP addresses to wireless clients.
DHCPv6 State	Open this switch to activate the internal DHCPv6 server of WLC, otherwise it is sleeping.

Parameter	Description
Starting IPv6 Address	The 1'st IPv6 address in DHCPv6 server address pool available for allocation.
Ending IPv6 Address	The last IPv6 address in DHCPv6 server address pool available for allocation.
IPv6 Prefix	IPv6 prefix is something like the IPv4 net mask, which indicates the subnet of IPv6 addresses. The default length is 64 bits.
DHCPv6 DNS	The IPv6 address of DNS server in current DHCPv6 address pool.
DHCPv6 Domain	The Domain name for IPv6 address.
Lease Time (100 - 86400 s)	In order to improve the multiplexing rate of the limited IPv6 addresses in the address pool, the addresses allocated by DHCPv6 usually have a life cycle, and are invalid when expire. This is the DHCPv6 lease time, the default 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.

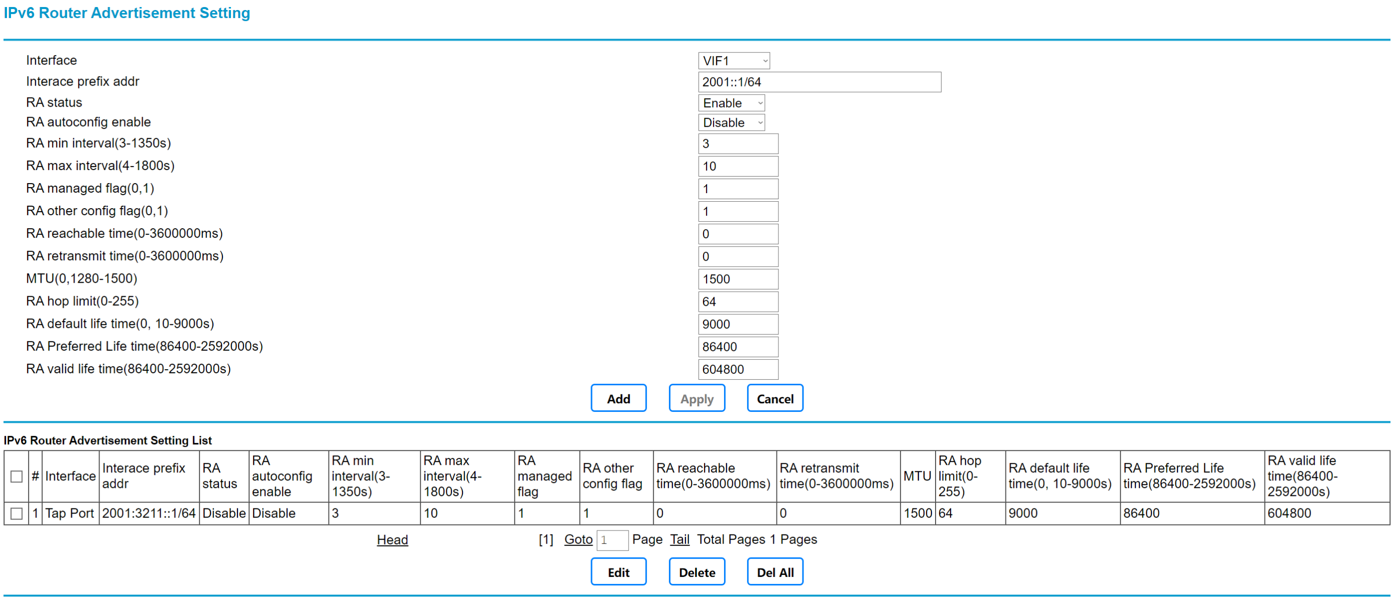
Click the **Delete** button to remove the selected DHCPv6 server entry from list.

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

5.2. ROUTE ADVERTISEMENT

IPv6 router advertisements include unsolicited advertisements and solicited advertisements. The unsolicited IPv6 router advertisement (RA) is broadcast in a pseudo-period; the solicited router advertisement is a passive response to the router solicitation message. The router advertisement contains the following information: link prefix, link MTU, specific route, address auto-configuration flag, and the 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	Binding current Router Advertisement setting to WLC internal layer 3 interface to take effect.
Prefix Addr	IPv6 prefix is something like the IPv4 net mask, which indicates the subnet of IPv6 addresses. The default length is 64 bits.
RA Status	Open this switch to enable the IPv6 Router Advertisement function in WLC.
RA Autoconfig Enable	Open this switch to enable WLC to auto-configure its addresses, address prefixes, routes, and other configuration parameters during IPv6 Neighbor Discover (ND) process.
RA Min Interval (3-1350 s)	The minimum time interval in a pseudo-period for WLC to send Router Advertisement message.
RA Max Interval (4-1800 s)	The maximum time interval in a pseudo-period for WLC to send Router Advertisement message.
RA Managed Flag (0, 1)	A flag indicates that the WLC is allowed to auto-configure 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 indicates that the WLC is allowed to auto-configure 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 it the WLC assumes a neighbor is reachable after receiving a Neighbor Solicitation confirmation.
RA Retransmit Time (0-360000 ms)	The time interval for retransmitting Neighbor Solicitation message, used for neighbor unreachable detection and address resolution.
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.

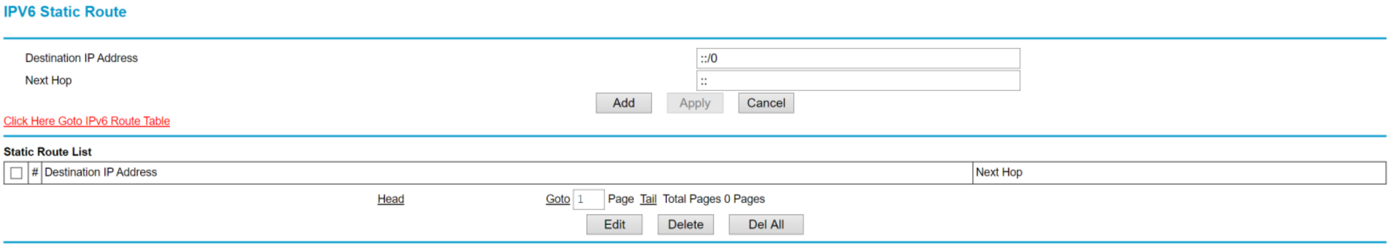
Click the **Delete** button to remove the selected IPv6 router advertisement entry from list.

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

5.3. STATIC ROUTE

When a packet is sent to a specific destination address that is not in the same subnet as the originator's IPv6 address, it can statically bind the specific destination IPv6 address to a fixed hop address because the route is unknown. Once the destination address of the packet matches the specific IPv6 address, the packet is immediately redirected to the fixed hop address for the next route. In this way, the packet is sent to the final destination IPv6 address step by step. The binding relationship of this specific destination IPv6 address to the fixed hop is the static routing.

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



IPV6 Static Route

Destination IP Address ::/0
Next Hop ::

Add Apply Cancel

Click Here Goto IPv6 Route Table

Static Route List

□	#	Destination IP Address	Next Hop

Head Goto 1 Page Tail Total Pages 0 Pages

Edit Delete Del All

Figure 5-3 IPv6 Static Route Configuration Page

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

Parameter	Description
Destination IP Address	This is the specific IPv6 address which is used to match with the destination address of packets so as to redirect to a known next hop.
Next Hop	The static redirect address for the packet whose destination address is matched with the above specific IPv6 address. It is for next routing.

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

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.

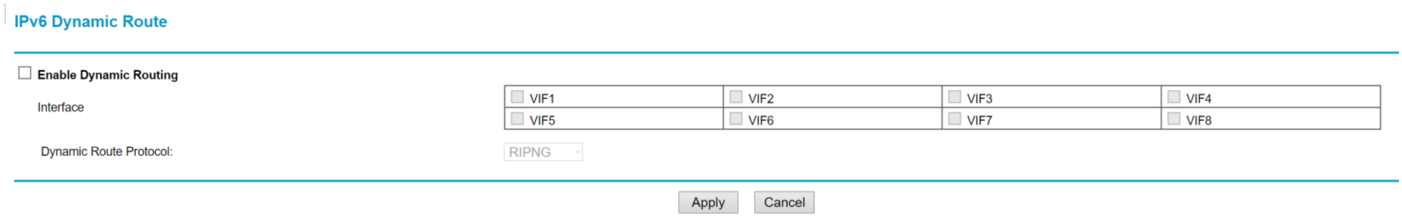
Click the **Del All** button to remove all the entries from the configuration.

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

5.4. Dynamic Route

The difference between dynamic routing and static routing is that the next hop address is not statically bound but automatically selected by routing algorithms. ***RIPNG*** and ***OSPFv3*** are two usual IPv6 routing algorithms, which can be mapped to the Layer 3 interface (VIF) of the WLC to implement dynamic routing of user data packets.

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



IPv6 Dynamic Route

☐ Enable Dynamic Routing

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

Dynamic Route Protocol: RIPNG

Figure 5-4 IPv6 Dynamic Rote Configuration Page

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

Parameter	Description
Enable Dynamic Routing	Open this switch to enable IPv6 dynamic routing function for WLC.
Interface	Binding the dynamic routing function to WLC internal specific layer 3 Interface (VIF) for user services traffic routing.
Dynamic Routing Protocl	Select the proper dynamic routing protocol: ***RIPNG*** or ***OSPFv3***.

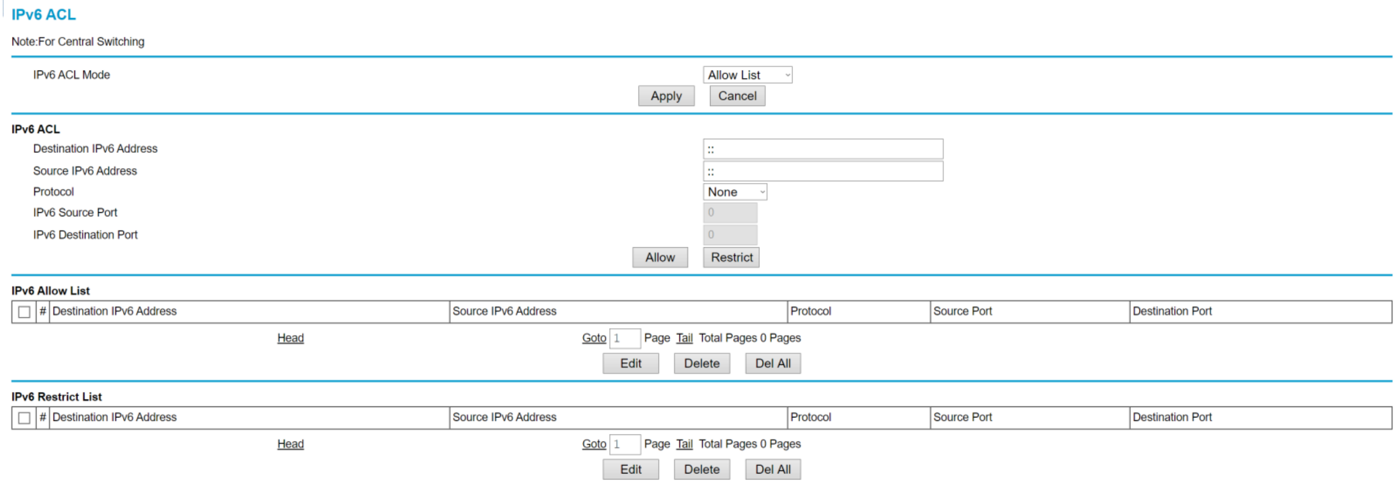
Click the **Apply** button to accept the changes.

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

5.5. ACL

This is an access control list established based on the IPv6 addresses of the user clients, which is used to allow or prohibit the user client to associate with the thin AP. The user clients in the white list are allowed, and the user clients in the blacklist are prohibited. The black and white list are created in WLC, and the thin AP downloads them for checking whether it is allowed when the user client initiates an association.

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



IPv6 ACL

Note:For Central Switching

IPv6 ACL Mode: Allow List

Apply Cancel

IPv6 ACL

Destination IPv6 Address: ::

Source IPv6 Address: ::

Protocol: None

IPv6 Source Port: 0

IPv6 Destination Port: 0

Allow Restrict

IPv6 Allow List

□	#	Destination IPv6 Address	Source IPv6 Address	Protocol	Source Port	Destination Port

Head Goto 1 Page Tail Total Pages 0 Pages

Edit Delete Del All

IPv6 Restrict List

□	#	Destination IPv6 Address	Source IPv6 Address	Protocol	Source Port	Destination Port

Head Goto 1 Page Tail Total Pages 0 Pages

Edit Delete Del All

Figure 5-5 IPv6 Access Control List Configuration Page

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

Parameter	Description
IPv6 ACL Mode	Three access control modes provided for thin AP to select: ▪ **Disable:** All thin APs do not use IPv6 access control for wireless clients. ▪ **Allow List:** Thin AP uses IPv6 white list for wireless client access control. ▪ **Restrict List:** Thin AP uses IPv6 blacklist for wireless client access control.
Destination IPv6 Address	Enter the destination IPv6 address which is under the ACL control.
Source IPv6 Address	Enter the source IPv6 address which is under the ACL control.
Protocol	Select which protocol below is under the ACL control: ▪ **None:** No protocol will be controlled by ACL. ▪ **TCP:** TCP protocol will be controlled by ACL. ▪ **UDP:** UDP protocol will be controlled by ACL. ▪ **ICMPv6:** ICMPv6 protocol will be controlled by ACL.
IPv6 Source Port	Enter the source port number which is under the ACL control.
IPv6 Destination Port	Enter the destination port number which is under the ACL control.
Action Button	▪ **Allow:** Current configuration will be added to the white list. ▪ **Restrict:** Current configuration will be added to the blacklist.
Access List	Two lists are shown: White list and Blacklist. Customer can edit any entry by checking the radio button in those lists.

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.

Chapter 6. Thin AP Profiles

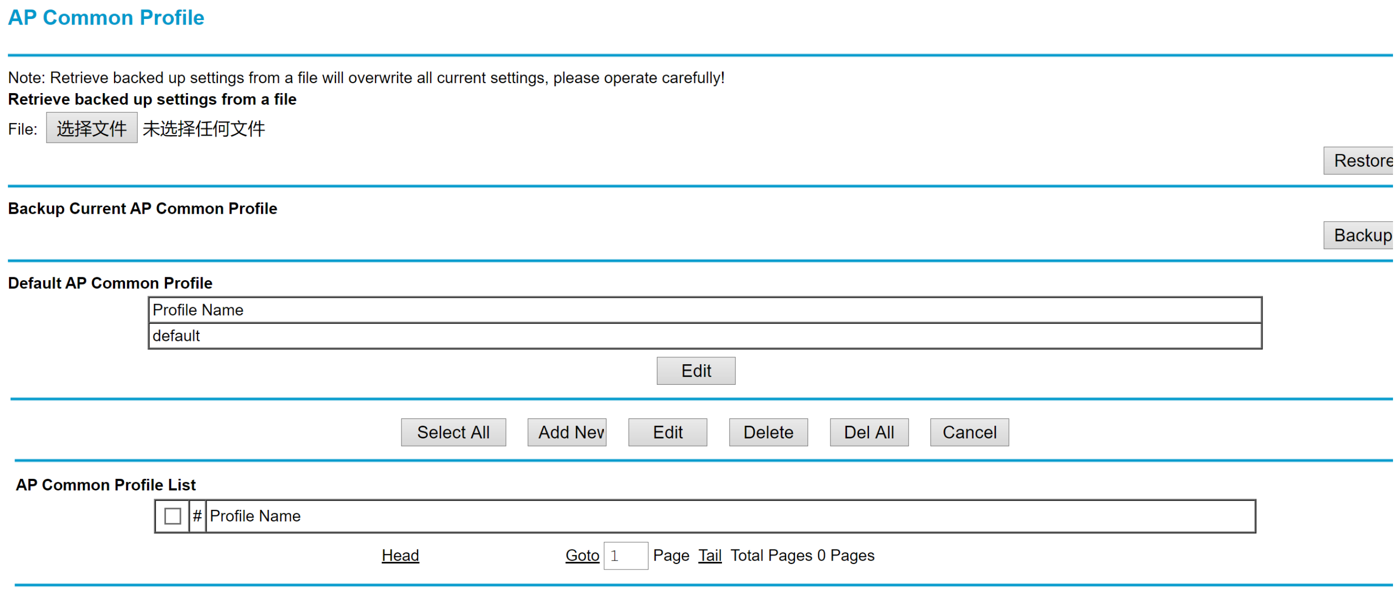
A thin AP is an initially zero-configured device. After powered on, it firstly initiates the DHCP process for two purposes: one is to obtain and configure its own IP address from the DHCP server; the other is to discover the WLC by picking up the IP addresses delivered in DHCP Option 43 message. Based on the IP address in Option 43, thin AP attempts to establish the CAPWAP management tunnel with the WLC. After that, thin AP downloads a set of profiles from WLC including the common profile, the wireless profile and VAP (virtual AP) profile, and uses them together to complete the configuration of the thin AP.

.

6.1. Common Profile

The parameters and configurations contained in the **common profile** are those generic parameters and configurations shared among the thin APs in the same group, and they are abstracted and collected into a file called the common profile. The WLC usually has a default common profile built in with preset parameters and configuration, and the customer can modify it to match the practical application. In addition, customers can also create different common profiles for different thin AP groups to adapt to various application requirements.

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



AP Common Profile

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 Current 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 6-1 AP Common Profile Entrance Page

Click the **Restore** button to restore the AP common profile from backed up settings.

Click the **Backup** button to save the AP common profile settings to the local PC.

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

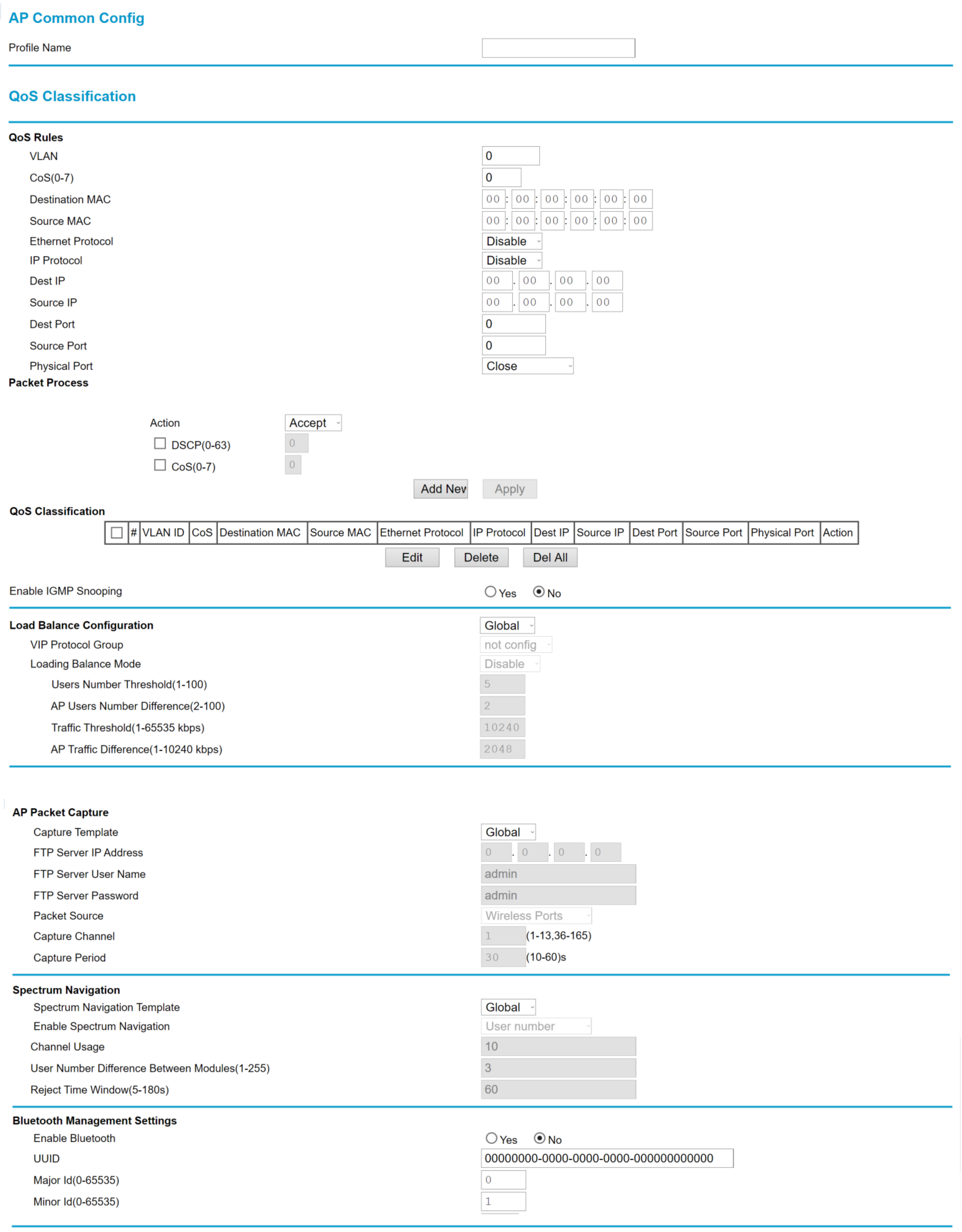
Click the **Select All** button to select all the profile .

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

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

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

Click the <**Add New**> or <**Edit**> button to enter the following parameters configuration page:



AP Common Config

Profile Name	

QoS Classification

QoS Rules

VLAN	0
CoS(0-7)	0
Destination MAC	00 : 00 : 00 : 00 : 00 : 00
Source MAC	00 : 00 : 00 : 00 : 00 : 00
Ethernet Protocol	Disable
IP Protocol	Disable
Dest IP	00 . 00 . 00 . 00
Source IP	00 . 00 . 00 . 00
Dest Port	0
Source Port	0
Physical Port	Close

Packet Process

Action	Accept
□ DSCP(0-63)	0
□ CoS(0-7)	0

QoS Classification

□	#	VLAN ID	CoS	Destination MAC	Source MAC	Ethernet Protocol	IP Protocol	Dest IP	Source IP	Dest Port	Source Port	Physical Port	Action

Enable IGMP Snooping	○ Yes ● No

Load Balance Configuration	Global
VIP Protocol Group	not config
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

AP Packet Capture

Capture Template	Global
FTP Server IP Address	0 . 0 . 0 . 0
FTP Server User Name	admin
FTP Server Password	admin
Packet Source	Wireless Ports
Capture Channel	1 (1-13,36-165)
Capture Period	30 (10-60)s

Spectrum Navigation

Spectrum Navigation Template	Global
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

Figure 6-2 AP Common Profile Parameters Page

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

Parameter	Description
Profile Name	Give a literal name for the new common profile for engineering management.
QoS Classification	**QoS Rules:** Define a set of rules to match the sub items of protocol unit in a packet to classify it to QoS or non-QoS. The matched packet will be treated by a specific method to guarantee QoS. The matching rules are defined as follows: ▪ **VLAN:** This VLAN ID is used for matching the VLAN ID in a packet. ▪ **CoS(0-7):** CoS stands for "Service Code", which is a layer 2 identifier of QoS used with VLAN ID (and ToS is a layer 3 identifier). The larger the value, the higher the priority. ▪ **Destination MAC:** This MAC address is used for matching the destination MAC address in a packet. ▪ **Source MAC:** This MAC address is used for matching the source MAC address in a packet. ▪ **Network Protocol:** Select a protocol from the pull-down menu as the key for matching the packet, including: ○ **Disable:** No network protocol is used for matching packet. ○ **ARP:** ARP packet will be matched to be QoS packet. ○ **IPv4:** IPv4 packet will be matched to be QoS packet. ○ **IPv6:** IPv6 packet will be matched to be QoS packet. ○ **PPPoE:** PPPoE packet will be matched to be QoS packet. ▪ **Transport Protocol:** Select a transport layer protocol from the pull-down menu as the key for matching the packet, including: ○ **Disable:** No transport layer protocol is used for matching packet. ○ **TCP:** TCP packet will be matched to be QoS packet. ○ **UDP:** UDP packet will be matched to be QoS packet. ○ **ICMP:** ICMP packet will be matched to be QoS packet. ▪ **Dest IP:** This IP address is used for matching the destination IP address in a packet. ▪ **Source IP:** This IP address is used for matching the source IP address in a packet. ▪ **Dest Port:** This port number is used for matching the destination port number in a packet. ▪ **Source Port:** This pot number is used for matching the source port number in a packet. ▪ **Physical Port:** Select a physical port from the pull-down menu for matching where the packet comes from, including: ○ **Close:** Do not care where the packet is coming from. ○ **Wire Port:** The packet coming from the wire port will be matched to be QoS packet. ○ **Wireless Port:** The packet coming from air interface will be matched to be QoS packet. **Packet Process:**

Parameter	Description
	▪ **Action:** How to handle those matched packets: o **Accept:** The matched packet will be accepted. o **Drop:** The matched packet will be dropped. ▪ **DSCP(0-63):** The **DSCP** field of the matched packet will be replaced with the value assigned here. ▪ **CoS(0-7):** The **CoS** field of the matched packet will be replaced with the value assigned here. **QoS Classification List:** New QoS classification will be added to the list by click <**Add New**> button, and can be modified by click <**Edit**> button. Also customer can select the matching rule in the list to remove it by click <**Delete**> or <**Delete All**> button.
Enable IGMP Snooping	Multicast members creation is dependent on IGMP, and the multicast packets are only forwarded to those members in multicast list. Enable IGMP snooping here to create multicast members in WLC.
Load Balance Configuration	The load balancing policy applied to thin APs to make the wireless clients on each thin AP evenly distributed and prevent unreasonable congestion. The balance policy is configured as follows: ▪ **Load Balance Configuration** - Two options for selection: o **Global** - Selecting **Global** means that the load balance policy for current group is overlaid by that configured in [**Access Control** > **Advanced Setting**], which is globally effective for thin APs in all groups. o **Group** - Selecting **Group** means that the effective load balance policy for current group is configured here. ▪ **Loading Balance Mode** - Actually is to select load balancing algorithm: o **Disable** - No load balancing policy for current thin AP group. o **Users** - The load balancing is dependent on the number of user clients on the thin APs. o **Traffic** - The load balancing is dependent on the traffic pressure on the thin AP. ▪ **Users Number Threshold** - If the "**Users**" is selected for the load balance mode, here to set the allowed maximum number of wireless clients on a thin AP. Once the number of wireless clients associated with the thin AP reaches this threshold, any new user association will be rejected. ▪ **AP Users Number Difference** - If the balance mode "**Users**" is selected, here to set the allowed maximum difference of the number of user clients between two thin APs. When the difference touches this threshold, any new client attempting to associate with the thin AP who has more users will be rejected. ▪ **Traffic Threshold** - If the balance mode "**Traffic**" is selected, here to set the allowed maximum throughput threshold on a thin AP. When the traffic 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, here to set the allowed maximum throughput difference between two thin APs. When the traffic

Parameter	Description
	throughput difference reaches this threshold, any new client attempting to associate with the thin AP who has more traffic will be rejected.
AP Packet Capture	This is a function that facilitates engineers to maintain the Wi-Fi system remotely. Engineers can use this function to capture packets from the thin AP and upload them to the FTP server for analysis. ▪ **Capture Template** - Select the configuration source for Packet Capture: o **Global** - Selecting **Global** means that the capture configuration is overlaid by that configured in [**RF Management** > **Optimization**], which is globally effective for thin APs in all groups. o **Group** - Selecting **Group** means that the capture configuration for current group is configured here below. ▪ **FTP Server IP Address** - The captured packets could be uploaded to a FTP server, here entering the IP address of this FTP server. ▪ **FTP Server User name** - Uploading the captured packets to FTP server needs an user name to remotely login the FTP server. ▪ **FTP Server Password** - Uploading the captured packets to FTP server needs a password of user to remotely login the FTP server.. ▪ **Packet Source** - The packet capture can be performed on either the air interface or the wired port, please select one as the packet source. ▪ **Capture Channel** - Specify the radio channel in which the packet is captured. ▪ **Capture Period** - Specify the time interval to perform the packet capture.
Spectrum Navigation	The "Spectrum Navigation" refers to the load balancing between the two radio modules on a dual-band thin AP that is, reasonably guiding the wireless client to associate with the preferable radio module. ▪ **Spectrum Navigation Template** - Select the configuration source for Spectrum Navigation : o **Global** - Selecting **Global** means that the Spectrum Navigation configuration is overlaid by that configured in [**RF Management** > **Optimization**], which is globally effective for thin APs in all groups. o **Group** - Selecting **Group** means that the Spectrum Navigation configuration for current group is configured here below. ▪ **Enable Spectrum Navigation** - Selecting the spectrum navigation algorithms for the radio modules: o **Disable** - No load balancing between radio modules for this thin AP group. o **Users Number** - The load balancing is dependent on the number of user clients. o **Channel Loading** - The load balancing is dependent on the radio channel utilization of two radio modules in the dual-band thin AP. ▪ **Channel Usage** - If **Channel Loading** is selected above, here to set the channel utilization threshold. When the channel usage of the radio module touches this threshold, any new client attempting to associate with this radio module will be rejected.

Parameter	Description
	- **Users Number Difference Between Modules** - If **Users Number** is selected above, here to set the difference threshold in the number of users between two radio modules. 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, to encourage it to associate with another radio module, current module will no longer accept the association requests from the rejected client within the rejection time window.
Bluetooth Management Settings	This is a function that supports Apple ***iBeacon***. iPhone and other iOS devices use this feature to implement location-based information services. - **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.

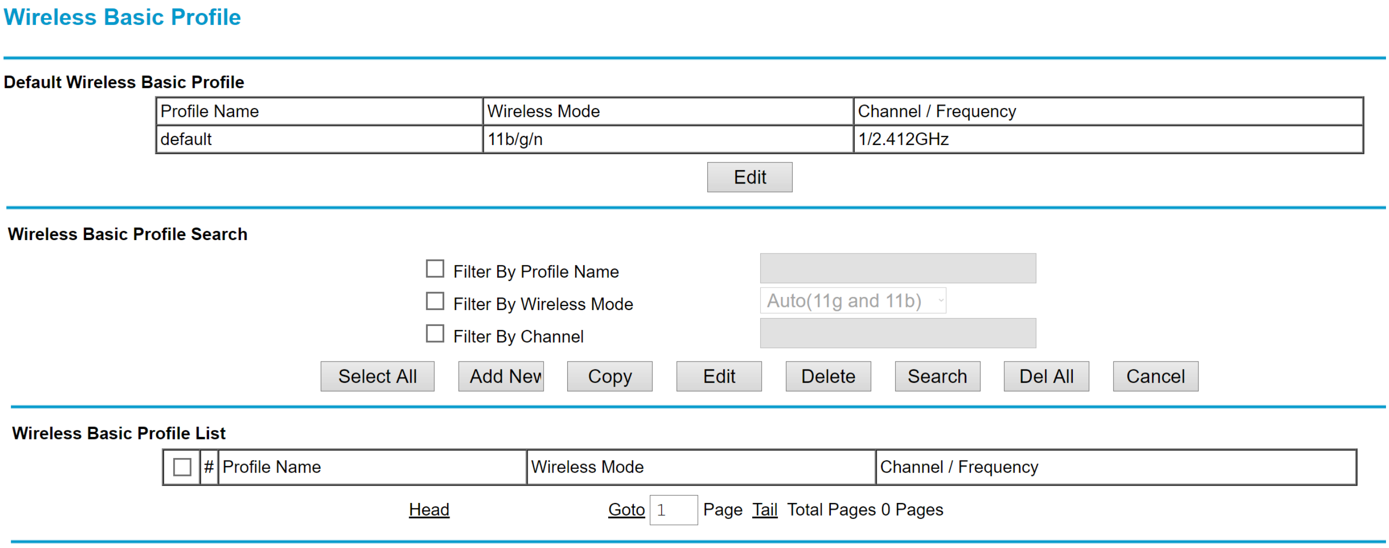
Click the **Apply** button to accept the changes.

Click the **Back** button to discard the changes made and return to the previous page.

6.2. WIRELESS PROFILE

The **Wireless Profile** is a group of wireless parameters that affect 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 wireless client to associate with the thin AP. Before configuring these wireless parameters, customers need to learn more about IEEE-802.11 technical specifications.

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



Wireless Basic Profile

Default Wireless Basic Profile

Profile Name	Wireless Mode	Channel / Frequency
default	11b/g/n	1/2.412GHz

Wireless Basic Profile Search

□ Filter By Profile Name

□ Filter By Wireless Mode Auto(11g and 11b)

□ Filter By Channel

Wireless Basic Profile List

□	#	Profile Name	Wireless Mode	Channel / Frequency

Head Goto 1 Page Tail Total Pages 0 Pages

Figure 6-3 Wireless Profile Entrance Page

The default wireless profile with preset parameters has been built in the WLC. Customers can modify it directly to meet with the actual application, and can also create new wireless profiles for different AP groups to adapt to different application requirements.

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

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

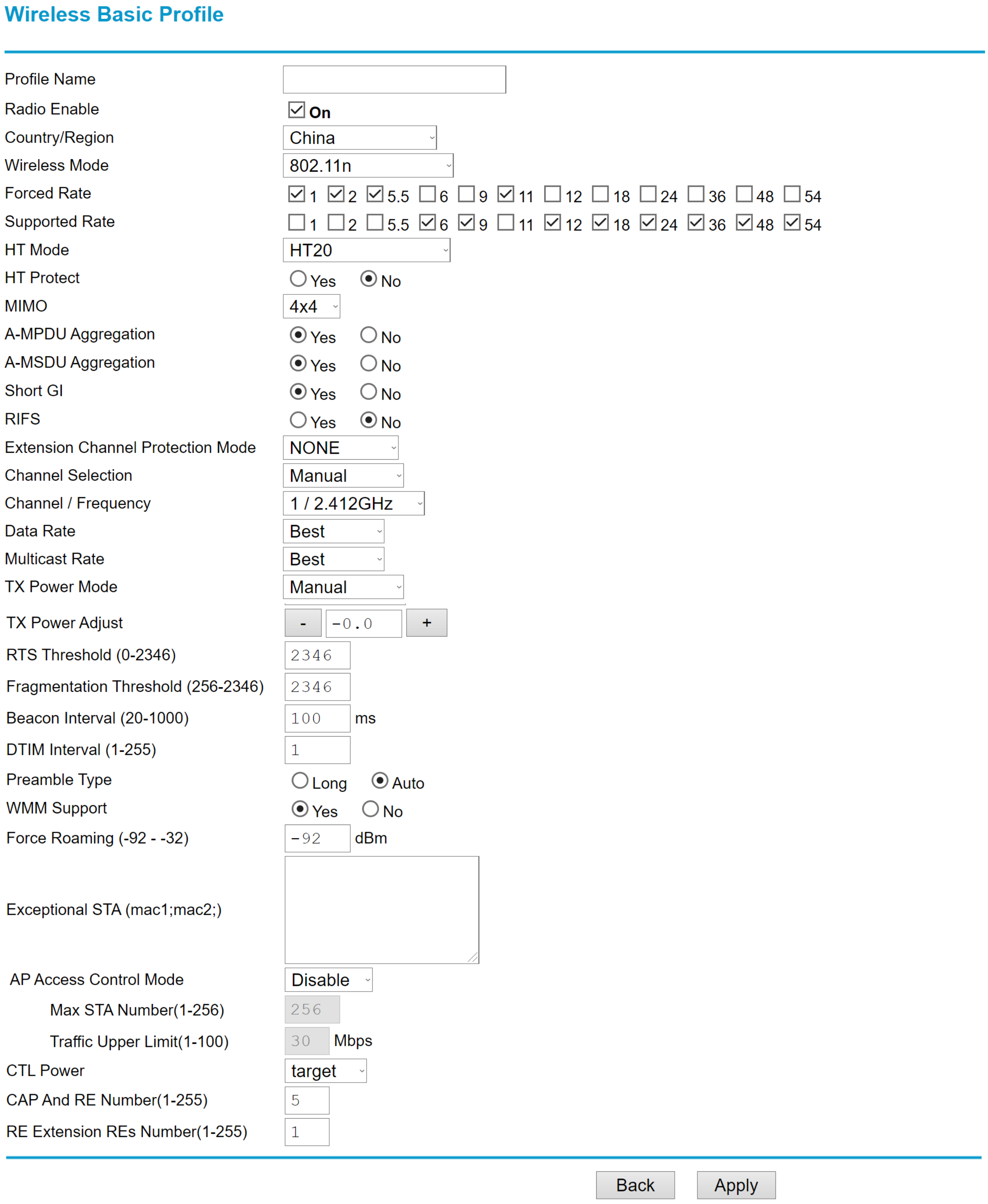
Click the **Copy** button to copy an existing profile in the list.

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:



Wireless Basic Profile

Profile Name	
Radio Enable	☑ **On**
Country/Region	China
Wireless Mode	802.11n
Forced Rate	☑1 ☑2 ☑5.5 □6 □9 ☑11 □12 □18 □24 □36 □48 □54
Supported Rate	□1 □2 □5.5 ☑6 ☑9 □11 ☑12 ☑18 ☑24 ☑36 ☑48 ☑54
HT Mode	HT20
HT Protect	○ Yes ● No
MIMO	4x4
A-MPDU Aggregation	● Yes ○ No
A-MSDU Aggregation	● Yes ○ No
Short GI	● Yes ○ No
RIFS	○ Yes ● No
Extension Channel Protection Mode	NONE
Channel Selection	Manual
Channel / Frequency	1 / 2.412GHz
Data Rate	Best
Multicast Rate	Best
TX Power Mode	Manual
TX Power Adjust	- -0.0 +
RTS Threshold (0-2346)	2346
Fragmentation Threshold (256-2346)	2346
Beacon Interval (20-1000)	100 ms
DTIM Interval (1-255)	1
Preamble Type	○ Long ● Auto
WMM Support	● Yes ○ No
Force Roaming (-92 - -32)	-92 dBm
Exceptional STA (mac1;mac2;)	
AP Access Control Mode	Disable
Max STA Number(1-256)	256
Traffic Upper Limit(1-100)	30 Mbps
CTL Power	target
CAP And RE Number(1-255)	5
RE Extension REs Number(1-255)	1

Figure 6-4 Wireless Profile Parameters Configuration Page

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

Parameter	**Description**
Profile Name	Give a literal name for the new wireless profile for engineering management.
Radio Enable	This is the switch of RF transmitter; turn it on/off to enable/disable the RF power transmitting of the thin AP. The default state is "**ON**".
Country/Region	Select the proper country/region code where the WLC is deployed. Due to different regulations, the authorized Wi-Fi channels vary in different countries and regions. This should be paid attention to.

Parameter	Description
Wireless Mode	Select a proper IEEE 802.11 specification for current thin AP group: ▪ **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.
Forced Rate	The mandatory air interface rate carried in the beacon of thin AP to inform the wireless clients to perform according to its own capabilities.
Supported Rate	The allowable air interface rate carried in the beacon of thin AP to inform the wireless clients to perform according to its own capabilities.
HT Mode	HT (High Throughput) is a bandwidth aggregation technology derived from 802.11n (a combination of several 20MHz bandwidths). The latest 802.11 specification supports multiple bandwidth aggregation, including HT20, HT40, HT80 and even HT160 (the suffix number is an integer multiple of the 20MHz bandwidth). The higher the number, the higher the rate.
HT Protect	HT technology uses a double-preamble mechanism to be compatible with low-rate legacy wireless clients (for example, 802.11b/g/a stations), that is, the thin AP will firstly send the traditional preamble before sending the HT preamble. Obviously, this double-preamble mechanism reduces the system throughput. To protect the high-rate clients from pollution by low-rate clients in a hybrid mode Wi-Fi network, the HT clients use the ***CTS-To-Self***-control frame to take up channel to transmit. This is the HT protection mode.
MIMO	Multiple Input Multiple Outputs technology; it 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.
A-MPDU Aggregation	The aggregated MPDU (MAC Protocol Data Unit) is a frame aggregation technology for IEEE 802.11n/ac to improve system throughput. Multiple smaller MPDU protocol frames are aggregated into a larger A-MPDU (Aggregated-MPDU) to reduce the number of preambles and protocol headers in the physical layer. The A-MPDU by default is enabled.
A-MSDU Aggregation	The aggregate MSDU (MAC Service Data Unit) is a frame aggregation technology for IEEE 802.11n/ac to improve system throughput. Several smaller MSDU data frames are aggregated into a larger A-MSDU (Aggregated-MSDU) to reduce the number of preambles and protocol headers in the physical layer. The A-MSDU by default is enabled.
Short GI	The effect of multipath reflection may cause the data blocks at the receiving end to be out of order and require re-transmitting. Therefore, 802.11n/ac defines a time

Parameter	Description
	interval between the sequential data blocks, which is the guard interval (GI). Obviously, a longer guard interval can provide higher phase noise suppression, but reduces the system rate; a shorter guard interval increases the system rate but produces higher phase noise. After the switch is turned on, the default guard interval is ***400ns***.
RIFS	802.11n defines a very short frame spacing of ***2μS*** to reduce the waiting time for sending frames and increase the air interface rate. The default is **ON**.
Extension Channel Protect Mode	In a hybrid Wi-Fi network, to protect the HT extension channel (channels above the lowest 20GHz channel in the aggregated bandwidth) of the thin AP from being affected by the low-rate 802.11b/g/a clients. There are three protection modes: ▪ **NONE** - No protection is provided for the extension channel. ▪ **CTS-To-Self** - The 802.11n/ac station sends a ***CTS-To-Self*** control frame including the Duration field, to inform the low rate stations to back off within this duration and then take up the channel for data transmission. ▪ **RTS/CTS** - The 802.11n/ac station sends a ***RTS*** control frame to thin AP to request to take up the channel for transmission. The AP responses it with the ***CTS*** frames to allow the requester to transmit.
Channel Selection	How do the thin APs in current group select their operating channels: ▪ **Manual** - Select the operating channel and band manually for current AP group. ▪ **Global Auto** - Automatically switch the operating channel, and the auto-switch policy is configured in [**RF Management** > **Optimization**] which is globally effective to the thin APs in all groups. ▪ **Group Auto** - Automatically switch the operating channel, and the auto-switch policy is configure here below: o **VIP Protocol** - Channel automatically switches according to the preset VIP protocol. o **DCA Channels** - Channel automatically switches according to DCA (Dynamic Channel Allocation) mechanism.
Channel / Frequency	If **Manual** mode is selected in above “Channel Selection”, then manually set its operating channel and corresponding frequency here.
Data Rate	The allowed maximum data rate for unicast packet transmission. The default option is **Best**.
Multicast Rate	The allowed maximum data rate for multicast packet transmission. The default option is **Best**.
TX Power Mode	How do the thin APs in current group set their transmit power: ▪ **Manual** - Manually set the transmitter power for the thin AP in current group. ▪ **Global Auto** - Adaptive adjust the transmitter power of thin APs, and the adaptive-adjustment policy is configured in [**RF Management** > **Optimization**] which is globally effective to the thin APs in all groups. ▪ **Group Auto** - Adaptive adjust the transmitter power of thin APs in current

Parameter	Description
	group, and the adaptive-adjustment policy is configured here below : ○ **Power Step-up Trigger Threshold** - If the signal strength of the neighboring AP is higher than this threshold, the thin AP will increase its TX power for suppression. ○ **Power Step-down Trigger Threshold** - If the signal strength of the neighboring AP is lower than this threshold, the thin AP will decrease its TX power. ○ **Upper Limit for TX Power** - This is the allowed maximum Tx power for the thin AP to increase its Tx power. ○ **Lower Limit for TX Power** - This is the allowed minimum Tx power for the thin AP to decrease its Tx power.
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.
RTS Threshold	The RTS mechanism is a technology introduced to solve the "**hidden node**" problem. If two wireless clients are located at the right opposite sides of the AP and too far apart to hear each other, the two wireless clients may simultaneously take up channel to transmit, thus, both signals arrive at the AP at the same time to interfere each other. This is the issue of "hidden node". To solve this problem by sending a "request to send" (RTS) control frame firstly instead of directly sending data. Even if the two clients compete to send RTS at the same time, the interference at most results in retransmitting the shorter RTS frame. However, for the RTS winner, the AP responds with a CTS frame to allow it to preferably send data, and other wireless clients back off for waiting. The RTS depends on the congestion inside the wireless clients. The RTS threshold is 0, indicating that RTS is always activated; the RTS threshold is a value between 0 and 2347, indicating that the RTS depends on the jammed packets; the RTS threshold is 2374, indicating that the RTS will never be used.
Fragmentation Threshold	If a packet is too long, it can be divided into several smaller fragments, and the length of each fragment cannot exceed the threshold set here.
Beacon Interval	The beacon frame periodically broadcast by the thin AP, which contains a lot of important information for stations to associate with the thin AP. The customer should give a reasonable time interval based on experience.
DTIM Interval	DTIM (Delivery Traffic Indication Message) is used for power saving of stations. Customer needs to adjust this value by experience to get the best effect.
Preamble Type	Asynchronous communication uses the preamble to wake up and synchronize the receiver, and is also used for channel evaluation. It has two types: long code and short code. The long code is mainly used for low-rate transmission, while the short code is used for high-rate transmission. It is recommended to use " **Automatic Mode**".
WMM Support	WMM (Wireless Multimedia) is the QoS of air interface on thin AP. It is recommended to enable it.

Parameter	Description
Force Roaming	If the signal strength (RSSI) of the wireless client measured by the AP is very low, it means that the client is too far to ensure communication. Here to set the RSSI threshold, if the client signal strength is lower than this value, the AP will kick the client out immediately and force it to search a nearest AP for association.
Exception STA	This is used together with "Force Roaming". The wireless clients whose MAC addresses in this list will not take part in the forced roaming.
AP Access Control Mode	Thin AP can restrict wireless clients association under certain conditions. These conditions are:: ▪ **Disable** - No restriction for stations to associate with current thin AP. ▪ **Users** - When the number of associated users on current AP reaches the threshold below, it will no longer accept any association request from new station: o **Max STA Number -** Thin AP allowed max number of associated clients. ▪ **Traffic** - When the traffic on current AP reaches the upper threshold below, it will no longer accept any association request from new station. o **Traffic Upper Limit -** Thin AP allowed max user traffic throughput.
CTL Power	The AP uses this field in the beacon frame to control the power of the wireless station: ▪ **Target** - Open loop power control, that is, the user client increases or decreases its own transmit power based on measuring the AP signal strength. ▪ **Control** - Closed loop power control, that is, the user client measures the AP signal strength and reports it to the AP, and then the AP informs the client to increase or decrease the transmit power based on the measurement report.
Number of root REs associated with CAP	The number of root REs associated with the central AP in the Wi-Fi-SON network.
Number of extension REs associated with root RE	The number of extension REs associated with the root RE in the Wi-Fi-SON network.

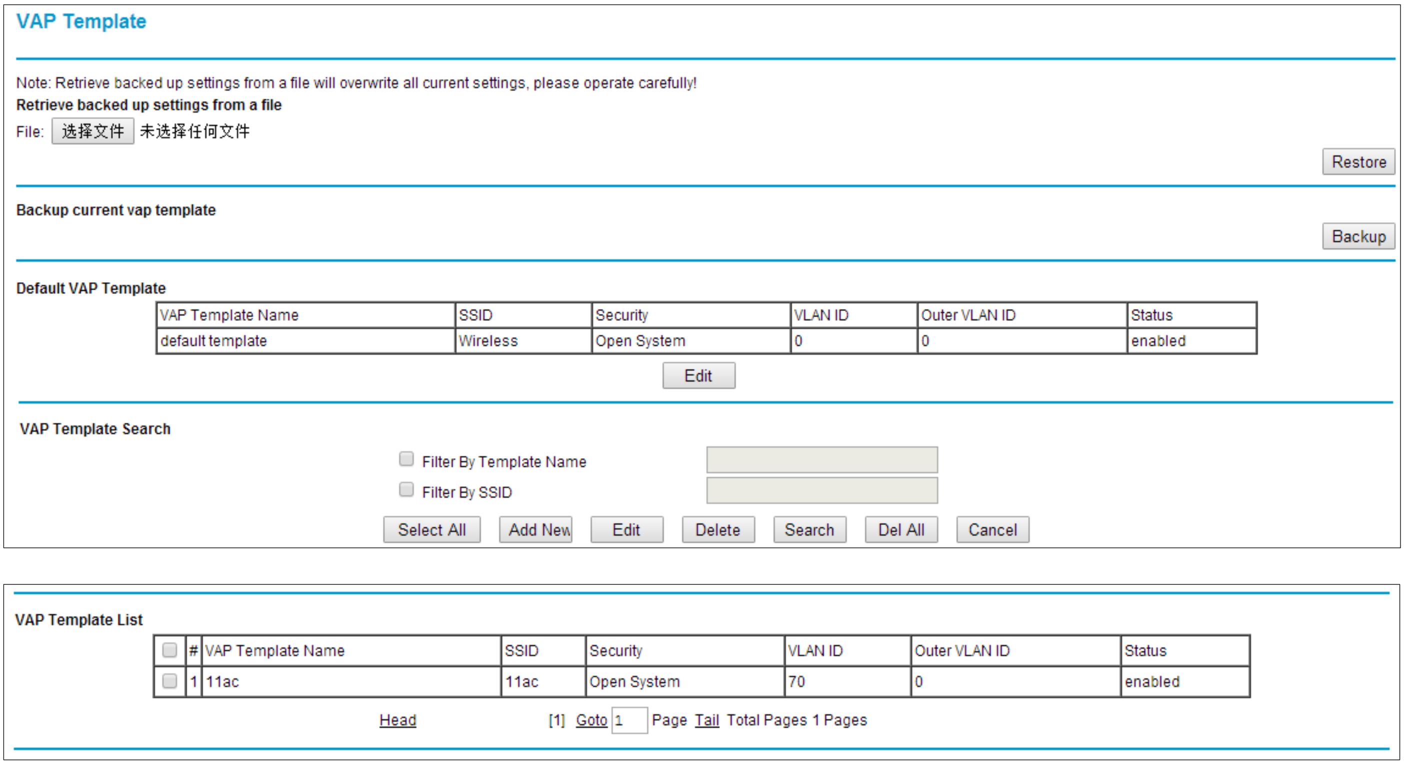
Click the **Apply** button to accept the changes.

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

6.3. VAP PROFILE

Logically, a physical thin AP can be divided into up to 8 virtual APs identified by different SSIDs, and these virtual APs share the same common profile and wireless profile. However, each virtual AP is different at service layer so that they are relatively independent from each other. Obviously, each virtual AP must have its own specific profile which is called as "**VAP Profil**e".

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



VAP Template

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 current vap template

Default VAP Template

VAP Template Name	SSID	Security	VLAN ID	Outer VLAN ID	Status
default template	Wireless	Open System	0	0	enabled

VAP Template Search

☐ Filter By Template Name

☐ Filter By SSID

VAP Template List

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

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

Figure 6-5 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.

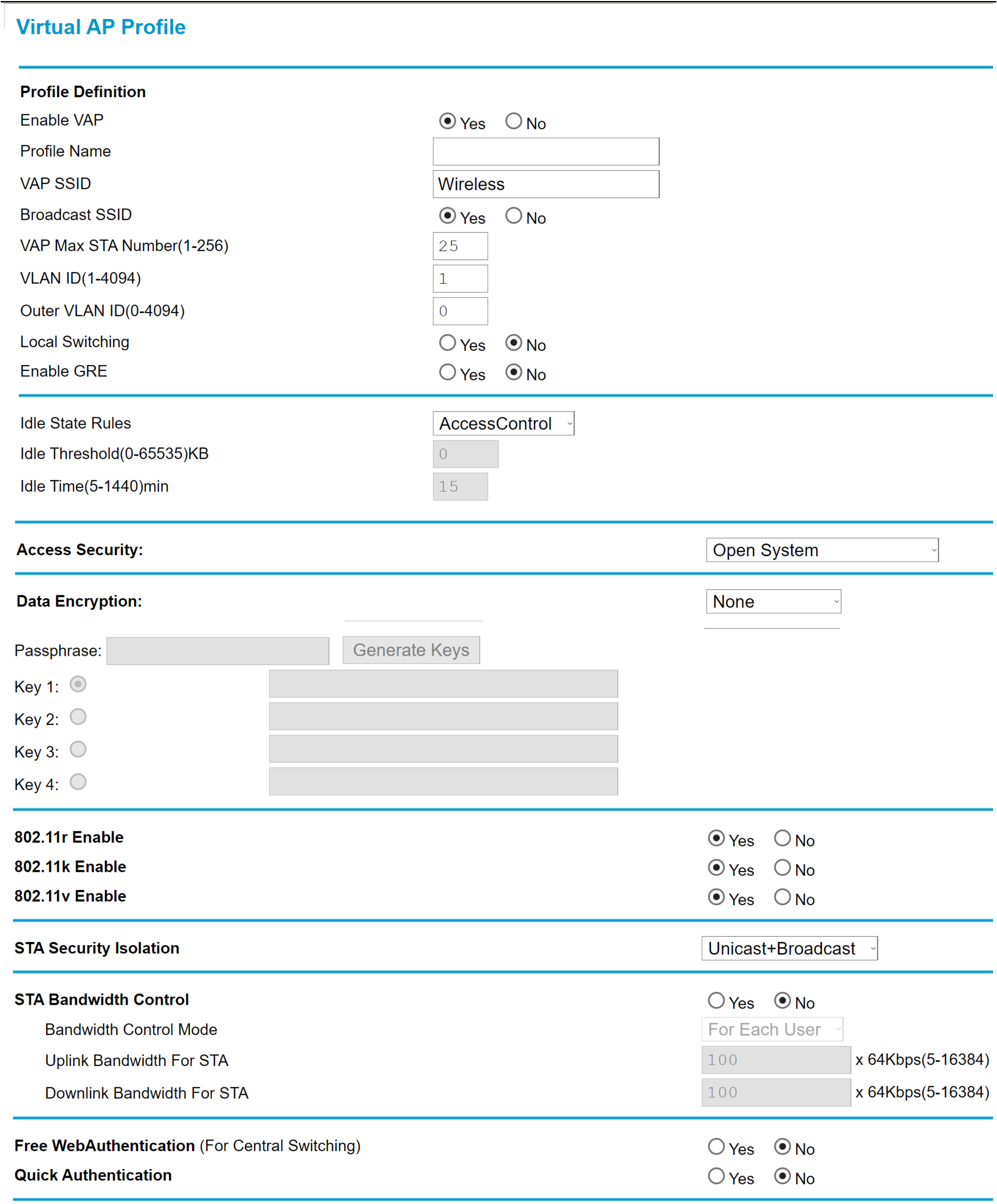
Click the **Delete All** button to remove all profiles from the list.

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:



Virtual AP Profile

Profile Definition

Enable VAP	● Yes ○ No
Profile Name	
VAP SSID	Wireless
Broadcast SSID	● Yes ○ No
VAP Max STA Number(1-256)	25
VLAN ID(1-4094)	1
Outer VLAN ID(0-4094)	0
Local Switching	○ Yes ● No
Enable GRE	○ Yes ● No
Idle State Rules	AccessControl
Idle Threshold(0-65535)KB	0
Idle Time(5-1440)min	15

Access Security: Open System

Data Encryption: None

Passphrase: Generate Keys

Key 1: ●

Key 2: ○

Key 3: ○

Key 4: ○

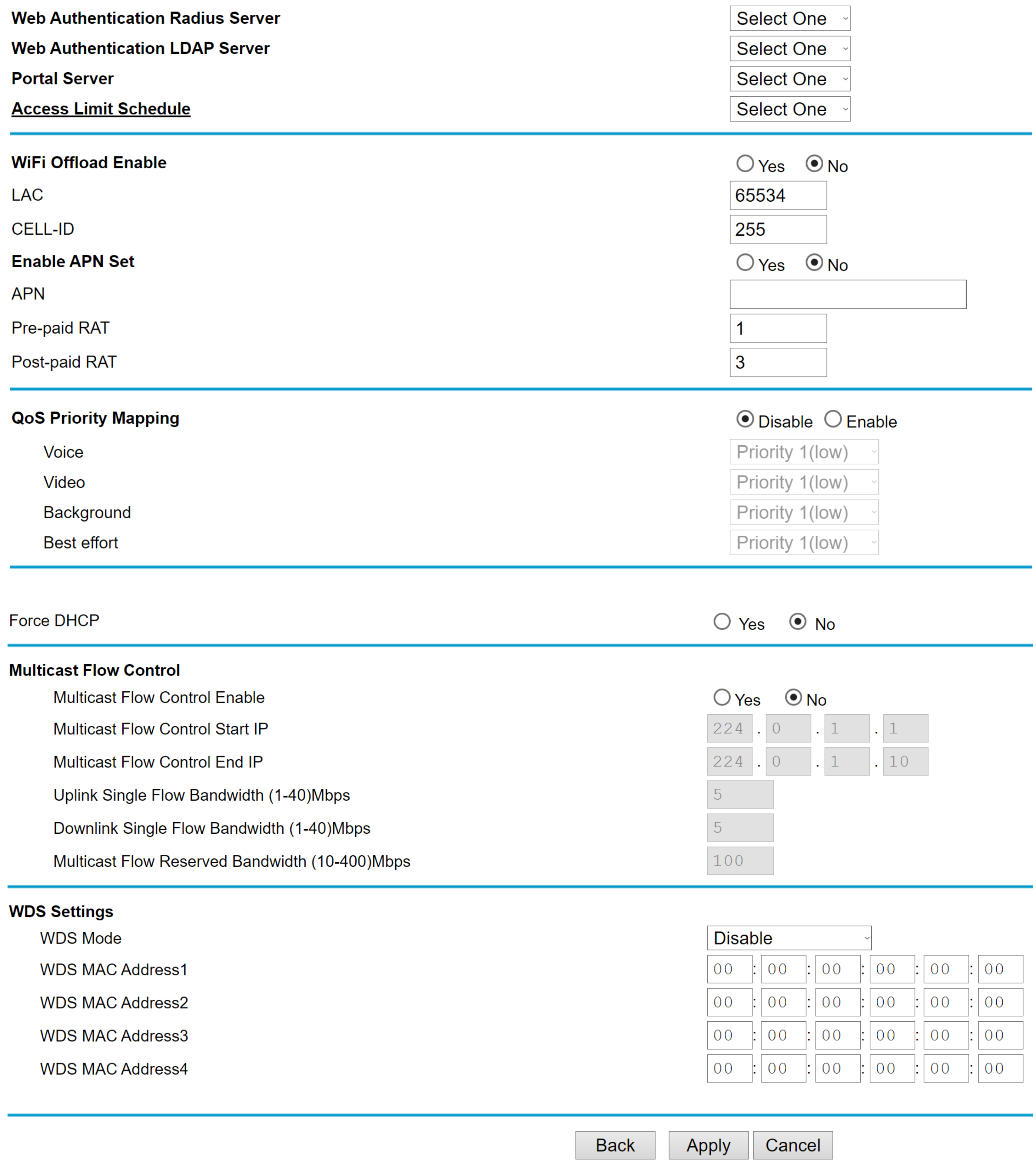
802.11r Enable	● Yes ○ No
802.11k Enable	● Yes ○ No
802.11v Enable	● Yes ○ No

STA Security Isolation Unicast+Broadcast

STA Bandwidth Control	○ Yes ● No
Bandwidth Control Mode	For Each User
Uplink Bandwidth For STA	100 x 64Kbps(5-16384)
Downlink Bandwidth For STA	100 x 64Kbps(5-16384)

Free WebAuthentication (For Central Switching)	○ Yes ● No
Quick Authentication	○ Yes ● No

Figure 6-6 VAP Profile Parameters Configuration Page (to be continued)



Web Authentication Radius Server Select One

Web Authentication LDAP Server Select One

Portal Server Select One

Access Limit Schedule Select One

WiFi Offload Enable ○ Yes ● No

LAC 65534

CELL-ID 255

Enable APN Set ○ Yes ● No

APN

Pre-paid RAT 1

Post-paid RAT 3

QoS Priority Mapping ● Disable ○ Enable

Voice Priority 1(low)

Video Priority 1(low)

Background Priority 1(low)

Best effort Priority 1(low)

Force DHCP ○ Yes ● No

Multicast Flow Control

Multicast Flow Control Enable ○ Yes ● No

Multicast Flow Control Start IP 224 . 0 . 1 . 1

Multicast Flow Control End IP 224 . 0 . 1 . 10

Uplink Single Flow Bandwidth (1-40)Mbps 5

Downlink Single Flow Bandwidth (1-40)Mbps 5

Multicast Flow Reserved Bandwidth (10-400)Mbps 100

WDS Settings

WDS Mode Disable

WDS MAC Address1 00 : 00 : 00 : 00 : 00 : 00

WDS MAC Address2 00 : 00 : 00 : 00 : 00 : 00

WDS MAC Address3 00 : 00 : 00 : 00 : 00 : 00

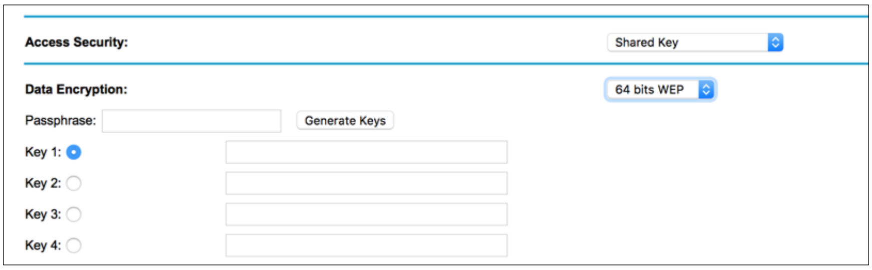
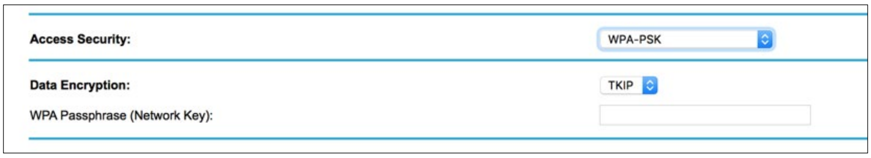
WDS MAC Address4 00 : 00 : 00 : 00 : 00 : 00

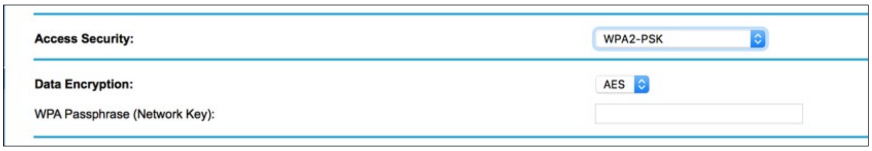
Figure 6-7 VAP Profile Parameters Configuration Page (Completed)

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

Parameter	Description
Enable VAP	Create a new VAP profile.
Profile Name	Give a literal name to the new VAP profile for engineering management.
VAP SSID	Assign a SSID to identify current virtual AP.
Broadcast Wireless Network	This radio button is checked **"Yes"** to enable the VAP broadcasting its SSID in the

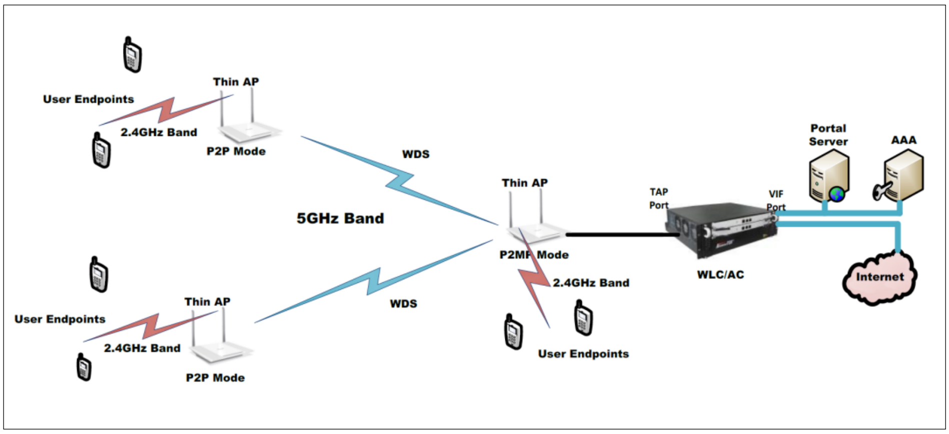
Parameter	Description
Name	beacon frame.
VAP Max STA Number	The maximum number of user clients allowed to associate with the current virtual AP.
VLAN ID	Assign a service VLAN ID to this VAP for tag its user traffic packets. If QinQ is enabled, this is a private VLAN.
Outer VLAN ID	If QinQ enabled, a public VLAN ID is needed as the outer VLAN to encapsulate the packet to traverse on the public network.
Local Switching	This radio button is used to inform the virtual AP, how the traffic of its user clients will be forwarded: ▪ **No:** It refers to that the **Central Switching** mode is selected, that is, the user data traffic is ***concentrated*** to WLC through a data tunnel, and then forwarded to the Internet. ▪ **Yes:** It refers to that the **Local Switching** mode selected, that is, the user data traffic ***bypasses*** WLC and is forwarded directly from the thin AP to the Internet.
Enable GRE	This radio button is used to guide current VAP traffic to a WLC northbound GRE tunnel, that is, all user traffic from current VAP to core network will go through a GRE tunnel.
User Client Idle	▪ **Idle State Rules:** Select the rules source for determination whether the user client is idle: o **Disable:** Do not care whether the user client is idle. o **Access Control:** The rule is configured in [**Authentication** > **Web Authentication**], which is globally effective to all VAPs. o **Local:** The rule is configured here below, and just effective to current VAP. ▪ **Idle Threshold:** If **Local** is selected, here to set the traffic threshold as one condition of the user client idle judgement. When user client traffic is lower than this threshold for a long time, the user client is idle. ▪ **Idle Time:** The idle state should be determined based on the traffic threshold together with the duration of low traffic. Here to set the duration of low traffic as one condition of the idle judgement.
Access Security	When a wireless client associates with a virtual AP, it must be authenticated before it access. The optional authentication modes are provided as follows: ▪ **Open System:** When the wireless client associates to this VAP, only the SSID is used for authentication, and the authentication does not be encrypted. ▪ **Shared Key:** This is the **WEP** scheme. A preset share key is required for the user client and virtual AP for authentication and encryption. Not recommended. ▪ **802.1X:** This authentication mode requires a RADIUS Server. The user client sends the username and password to the VAP to forward to the RADIUS server for authentication.

Parameter	Description
	▪ **WPA With Radius:** The user client associates with VAP using WPA scheme for authentication, which is encrypted with a temporary key issued by Radius server. ▪ **WPA2 With Radius:** The user client associates with VAP using WPA2 scheme for authentication, which is encrypted with a temporary key issued by Radius server. ▪ **WPA & WPA2 With Radius:** The user client associates with VAP using WPA or WPA2 scheme for authentication depending on itself, which is encrypted with a temporary key issued by Radius server. ▪ **WPA-PSK:** When the user client associates to this VAP, it will be authenticated by WPA scheme, and the authentication will be encrypted by the preset PSK key. ▪ **WPA2-PSK:** When the user client associates to this VAP, it will be authenticated by WPA2 scheme, and the authentication will be encrypted by the preset PSK key. ▪ **WPA-PSK & WPA2-PSK:** When the user client associates to this VAP, it will be authenticated by WPA or WPA2 scheme depending on itself, and the authentication will be encrypted by the preset PSK key. ▪ **MAC With Radius:** When the user client associates with VAP, it sends the MAC address of endpoint to VAP and then forward to the Radius server for authentication. This MAC address must be registered in Radius server in advance.
Data Encryption	The data encryption is used for the preset key security, and the Shared Key (WEP) mode, WPA-PSK mode and WPA2-PSK mode have different algorithms as follows: ▪ **Shared Key Mode:** The WEP key is either in 64-bit, 128-bit, or 152-bit as below:  **Access Security:** Shared Key **Data Encryption:** 64 bits WEP Passphrase: Key 1: ● Key 2: ○ Key 3: ○ Key 4: ○ Select the key length from the **Data Encryption** drop-down menu and enter an ASCII string in **Passphrase** textbox. Click the <**Generate Key**> button to generate a WEP key which will be displayed it in the textboxes of **Key 1 - 4** . ▪ **WPA-PSK Mode:** The WPA preset key is entered in the format as below:  **Access Security:** WPA-PSK **Data Encryption:** TKIP WPA Passphrase (Network Key): Select **TKIP** from the pull-down menu of **Data Encryption** and enter an ASCII string in the **Passphrase** textbox as the WPA preset key.

Parameter	Description
	▪ **WPA2-PSK Mode:** The WPA2 preset key is entered in the format as below:  Access Security: WPA2-PSK Data Encryption: AES WPA Passphrase (Network Key): Select **AES** from the pull-down menu of **Data Encryption** and enter an ASCII string in the **Passphrase** textbox as the WPA2 preset key.
802.11r Enable	802.11r is a fast roaming (FT) protocol, which is used to reduce the time of re-authentication for user clients during roaming. Theoretically, the roaming shall be completed within 50 milliseconds. It is suitable for PSK and 802.11x authentication mode. Default is "**Disable**".
802.11k Enable	802.11k is a wireless network measurement protocol. It evaluates channel quality and RF environment through measurement of neighboring APs, and informs wireless clients with the measurement results. It helps wireless clients quickly select the best roaming target. Default is "**Disable**".
802.11v Enable	802.11v is a wireless network management protocol. It creates a network node information database by collecting the capability information of wireless clients and their reporting data. It helps wireless clients rapidly roaming and load balancing across the network. Default is "**Disable**".
STA Security Isolation	For safety reasons, it is necessary to prevent the broadcast or unicast packets from transmission between user clients through the VAP. The isolation policies are provided below: ▪ **Disable:** Current VAP will not isolate any data packet transmission between user clients. ▪ **Unicast:** Current VAP will isolate the unicast packets transmission between user clients. ▪ **Broadcast:** Current VAP will isolate the broadcast packets transmission between user clients. ▪ **Unicast + Broadcast:** Current VAP will isolate the unicast and broadcast packets transmission between user clients.
STA Bandwidth Control	Turn on this switch to enable current virtual AP to limit the bandwidth of the wireless clients according to the following rules: ▪ **Bandwidth Control Mode:** Select the bandwidth control objective, each user client or the current VAP: o **Client:** Bandwidth of each wireless client on current virtual AP has been limited. o **VAP:** Bandwidth of current virtual AP has been limited. ▪ **Uplink Bandwidth:** The user client or VAP (depending on the selected Bandwidth Control Mode) uploading data does not exceed this rate (the rate is an integer multiple of 64kbps). ▪ **Downlink Bandwidth:** The user client or VAP (depending on the selected Bandwidth Control Mode) downloading data does not exceed this rate (the

Parameter	Description
	rate is an integer multiple of 64kbps).
Free WebAuthentication (For Central Switching)	Turn on this switch to enable the user clients to associate with the current virtual AP without web authentication. **Default is No.**
Quick Authentication	Turning on this switch to enable current VAP to reserve an authentication information copy for each user client after it is authenticated. Therefore, if the user client re-associates with this VAP, it is authenticated by using the copy to speed up the process of user authentication. **Default is No.**
Web Authentication Radius Server	Select a RADIUS server configured in [**Authentication > Radius Server**] from the drop-down menu to bind to current VAP. If Web-Authentication mode is selected, the user clients associated with this VAP will be authenticated by this Radius Server.
Web Authentication LDAP Server	Select a LDAP server configured in [**Authentication > LDAP Server**] from the drop-down menu to bind to current VAP. If Web-Authentication mode is selected, the user clients associated with this VAP will be authenticated by this LDAP Server.
Portal Server	Select a Portal server configured in [**Authentication > Portal Server**] from the drop-down menu to bind to current VAP. If Web-Authentication mode is selected, the user clients associated with this VAP will be authenticated by this Portal Server.
Access Limit Schedule	The VAP uses the Access Limit Schedule configured in [**Access Control > Access Time Control**] to prohibit user clients from association with current VAP in specific days and times.
Wi-Fi Offload Enable	If the Wi-Fi system is converged with UMTS (Universal Mobile Telecommunication System) for offloading traffic from the mobile network, then the switch here should be turned on. **Default is No.**
LAC	Entering the LAC code (Location Area Code) which is used in UMTS network for paging.
Cell-ID	This is the concept of 3GPP used to identify an individual radio unit in the base station; it is allocated by the mobile operator.
Enable APN set	The APN (Access Point Name) is a 3GPP concept used to identify an external PDN (Public Data Network) on the network.
APN	If APN set is enabled, an APN name allocated from mobile operator must be entered here.
Pre-paid RAT	Operator allocates an unique prepaid code for each radio access technology (GSM, UMTS, LTE, Wi-Fi), here to enter the prepaid code assigned by the operator for Wi-Fi.
Post-paid RAT	Operator allocates an unique post-paid code for each radio access technology (GSM, UMTS, LTE, Wi-Fi), here to enter the post-paid code assigned by the operator for Wi-Fi.
QoS Priority Mapping	QoS takes quality control by setting different priorities for packets of different services. The higher the priority of the packet, the earlier and faster it is processed: ▪ **Voice:** Voice is the service most sensitive to latency. The shorter the transmission time, the better the communication quality. So it is the

Parameter	Description
	highest priority. ▪ **Video:** Video is the service most sensitive to packet loss. The less the packet loss, the better the video quality. So it is the second highest priority. ▪ **Background:** Background is the service of bulk data transmission, such as FTP and SMTP. It is most sensitive to data integrity and always needs to be retransmitted, so it has a lower priority. ▪ **Best Effort:** Best-effort is the service which do not guarantee the delivery of data to the target and packet loss is acceptable, such as web surf. So it has the lowest priority.
Force DHCP	This is a security function based on the DHCP snooping technology. Only clients that use the IP address allocated by their own DHCP server are allowed to access. The clients using IP addresses allocated by other DHCP servers will be rejected.
Multicast Flow Control	Multicast is easy to cause network congestion. Therefore, it is necessary to limit the bandwidth of individual multicast stream to reserve sufficient bandwidth for other services. The following is the policy for multicast bandwidth limitation: ▪ **Multicast Flow Control Enable:** This is a radio button, which is checked to enable the function of multicast stream control. **Default is No**. ▪ **Multicast Flow Control Start IP:** Multicast flow control can be applied to a group of multicasts. Enter the first multicast IP address in this multicast group. ▪ **Multicast Flow Control End IP:** Multicast flow control can be applied to a group of multicasts. Enter the last multicast IP address in this multicast group. ▪ **Uplink Single Flow Bandwidth:** This is the upper limit of uplink bandwidth for each individual flow in a multicast. ▪ **Downlink Single Flow Bandwidth:** This is the upper limit of downlink bandwidth for each individual flow in a multicast. ▪ **Multicast Flow Reserved Bandwidth:** If the total bandwidth occupied by multicast members reaches this threshold, either the bandwidth of each multicast member or the number of members must be reduced to ensure that there is enough remaining bandwidth for other services.
WDS Mode	WDS (Wireless Distributed System) is such a system in which a central point AP is bridged with multiple edge point APs. Usually the edge point AP is a dual-band device, in which the 2.4GHz module is responsible for coverage, and the 5GHz module is used for the backhaul link. The figure below shows an example of a simple WDS system.

Parameter	Description
	 User Endpoints Thin AP 2.4GHz Band P2P Mode WDS 5GHz Band Thin AP P2MP Mode 2.4GHz Band User Endpoints TAP Port VIF Port WLC/AC Portal Server AAA Internet User Endpoints Thin AP 2.4GHz Band P2P Mode WDS In the above architecture, the central point AP is the AP close to the WLC, and the edge point AP is the AP far away from the WLC. The central point AP works in P2MP (point-to-multipoint) mode, while the edge point AP works in P2P (point-to-point) mode. So, properly select the operating mode for AP according to its role in WDS: ▪ **Disable:** No WDS architecture used in current Wi-Fi system. ▪ **Peer-to-Peer Mode:** The edge AP in WDS selects this mode. ▪ **Peer-to-MultiPeer:** The central AP in WDS selects this mode.
MAC Address 1-4	Each AP in the WDS must know the MAC address of the associated peer. The central AP supports up to 4 edge APs, so 4 edge AP MAC addresses must be entered for it. The edge AP only associates with one central AP, so the MAC address of the central AP must be entered for it.

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

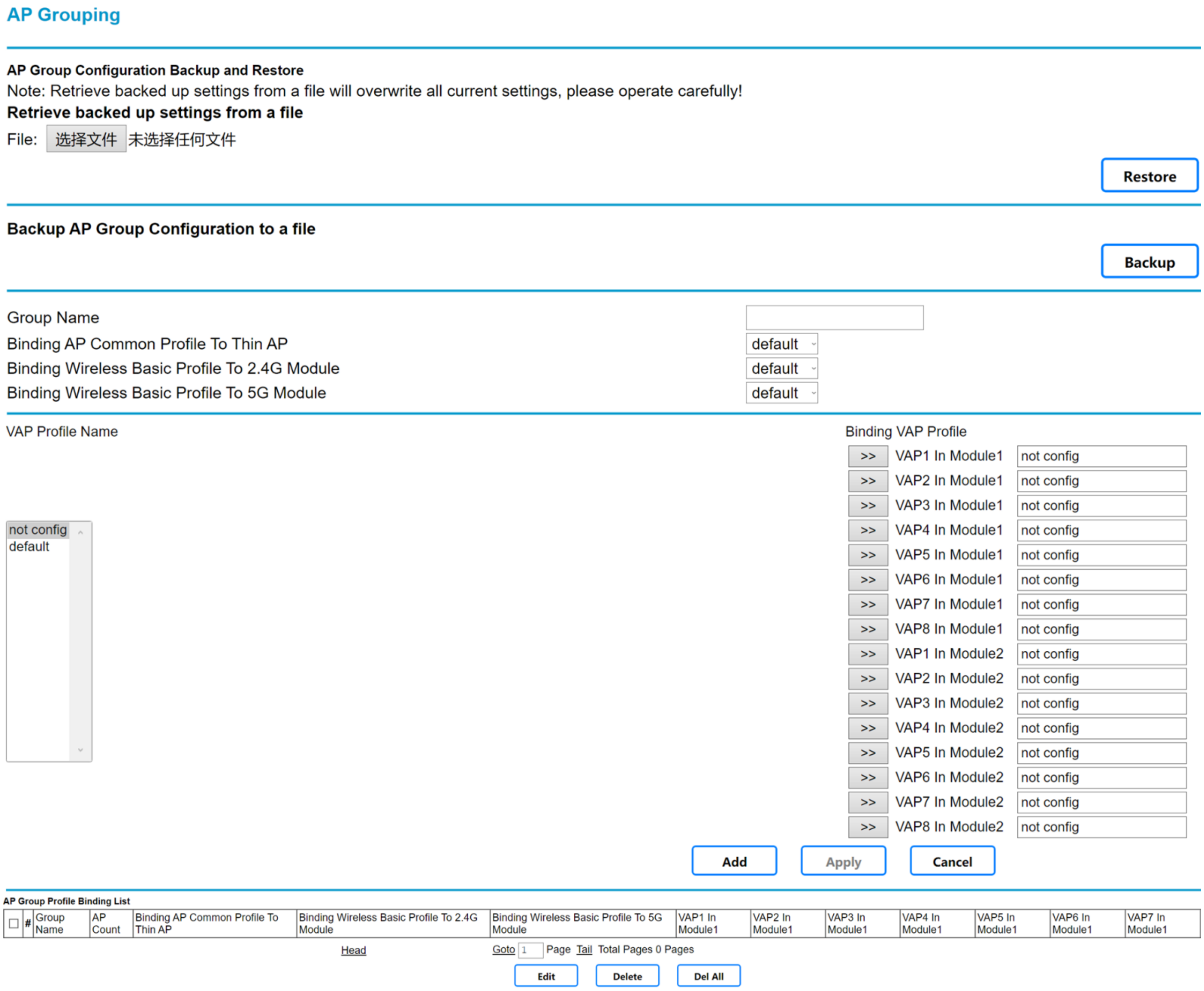
Click the **Back** button to discard the changes made and return to the previous page.

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

6.4. **AP GROUPING**

As known that thin APs implement self-configuration by downloading profiles from WLC through CAPWAP tunnels. However, if each thin AP has an individual profile, as the growth of the number of thin APs in the network, the number of profiles will become more massive to occupy a huge amount of space. At the same time, managing and maintaining these massive profiles will be a challenge for administrator. Therefore, it is necessary to divide thin APs into different groups according to their attributes, and the thin APs in the same group share the same profiles, so as to achieve the purpose of reducing the number of profiles.

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 literal name for it.
Binding AP Common Profile to Thin AP	Select a configured **Common Profile** for current AP group.
Binding Wireless Basic Profile to 2.4G Module	For dual-band thin AP, select a configured **Wireless Profile** for the 2.4GHz module.
Binding Wireless Basic Profile to 5G Module	For dual-band thin AP, select a configured **Wireless Profile** for the 5GHz module.
VAP Profile Binding	The two radio modules of a dual-band AP can logically be divided into up to 8 virtual APs (16 VAPs in total). Therefore, it is needed to select a configured **[VAP Profile]** for each virtual AP. These available VAP Profiles

Parameter	Description
	are listed in the left window, the customer selects one of them, and then clicks the "**>>**" button to bind the selected VAP profile to the radio module on the right side of the button. Among them, Module 1 is a 2.4GHz module; Module 2 is a 5GHz module.
AP Group Profiles Binding List	Click the <**Add**> button to create an AP group with bound profiles and append it into the group list. Customer can modify it by clicking the <**Edit**> button.

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

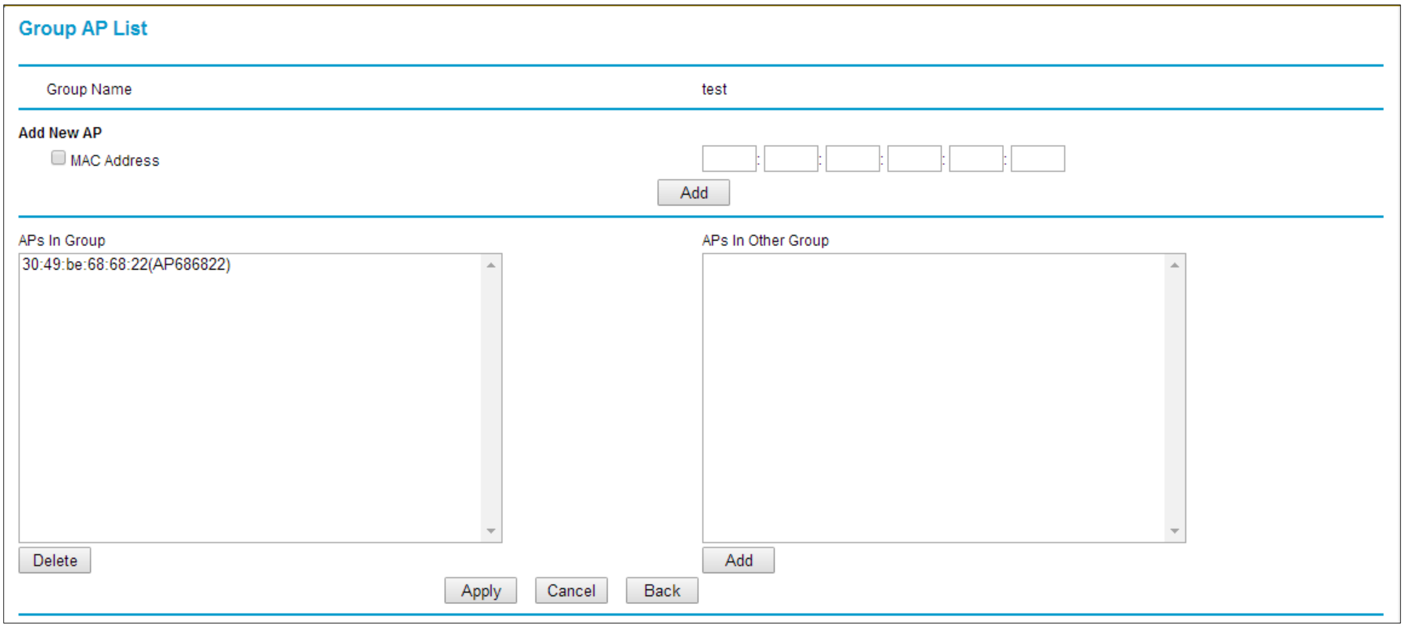
Click the **Apply** button to accept the changes.

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.

The above just completes the creation of the blank group. So it is important to add new members to this group. Select a thin AP group that needs to add new members from the group list, and click its "**Group Name**" to enter the add AP page as shown in the figure below:



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

Enter the MAC address of the thin AP, click the <**Add**> button to become a new member of current group, and it will be displayed in the left window; also it can select the thin AP that already exists in other AP groups from the right window to become a member of current group.

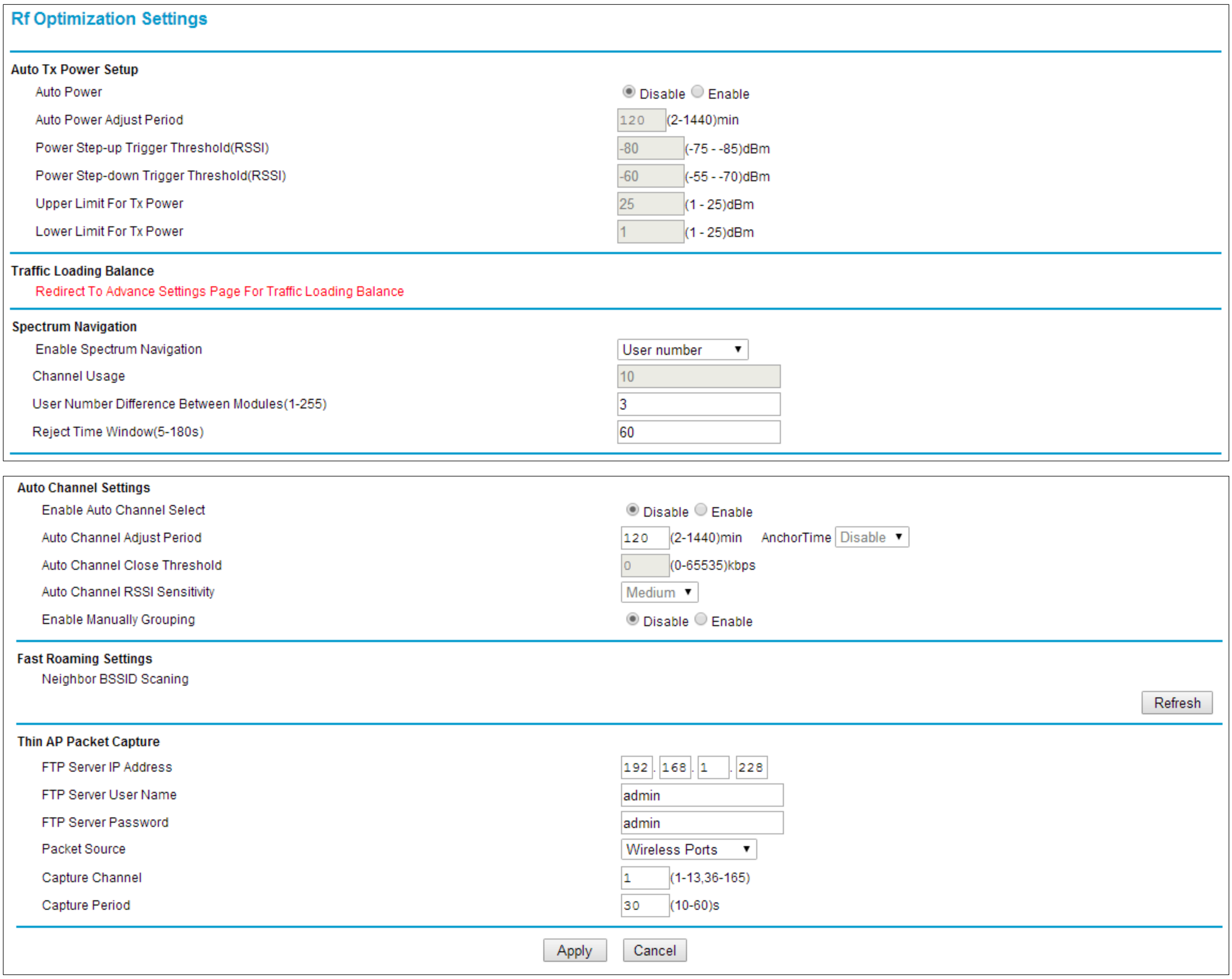
Chapter 7. RF MANAGEMENT

In this chapter, we will discuss the measures how to analyze, optimize and improve RF environment on the WLC, help field engineers to simplify the system maintenance, installation and management.

7.1. OPTIMIZATION

In most practical applications, the variation of the RF environment will cause the degradation of Wi-Fi system performance. Therefore, it is necessary to analyze the field conditions and optimize the parameters to improve the communication quality.

Select **[RF Management** > **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 (1 - 25)dBm
Lower Limit For Tx Power	1 (1 - 25)dBm

Traffic Loading Balance

Redirect To Advance Settings Page For Traffic Loading Balance

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	120 (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

Thin AP Packet Capture

FTP Server IP Address	192 . 168 . 1 . 228
FTP Server User Name	admin
FTP Server Password	admin
Packet Source	Wireless Ports ▼
Capture Channel	1 (1-13,36-165)
Capture Period	30 (10-60)s

Figure 7-1 RF Optimization Configuration Page

These parameters in **[RF Management** > **Optimization]** page is described in details as following:

Parameter	Description
Auto Tx Power Setup	▪ **Auto Power:** Turn on this switch to create a globally effective automatic Tx power adjustment policy for the entire system: ▪ **Auto Power Adjust Period:** Set the time interval for thin AP to measure the signal strength of neighboring APs to determine whether starting the Tx power adjustment. ▪ **Power Step-up Trigger Threshold:** If the signal strength of the neighboring AP is higher than this threshold, the thin AP will increase its TX power for suppression. ▪ **Power Step-down Trigger Threshold:** If the signal strength of the neighboring AP is lower than this threshold, the thin AP will decrease its TX power. ▪ **Upper Limit for TX Power:** The TX power cannot be adjusted higher than this level. ▪ **Lower Limit for TX Power:** The TX power cannot be adjusted lower than this level.
Traffic Loading Balance	See **Advanced Settings** for more information.
Spectrum Navigation	Here to set the policy for load balancing between the radio modules of the dual-band thin AP. This policy is effective globally for all APs in the system: ▪ **Enable Spectrum Navigation:** It is actually to choose the load balancing algorithm for radio modules: o **Disable:** No load balancing used for radio modules. o **Users Number:** Load balancing depends on the number of users on radio module. o **Channel Loading:** Load balancing depends on the channel usage of radio module. ▪ **Channel Usage:** If the "**Channel Loading**" is selected for load balancing, here to set the allowed highest channel utilization for the radio module. Once the channel utilization rate of the radio module reaches this threshold, any new client association attempts will be rejected by this radio module. ▪ **Users Number Difference Between Modules:** If the "**Users Number**" is selected for load balancing, here to set the allowed maximum difference value in the number of users associated with two radio modules. Once the difference reaches this threshold, any wireless client association with the radio module who has more users will be rejected. ▪ **Reject Time Window:** If the user client is rejected by the radio module, to encourage it to associate with another radio module, current module will no longer accept the association requests from the rejected client within the rejection time window.
Auto Channel Settings	▪ **Enable Auto Channel Select:** Turn on this switch to create a globally effective automatic channel selection policy for the entire system: ▪ **Auto Channel Adjust Period:** To prevent the thin AP from too frequently performing RF measurement and switching channel, resulting in the worse user experience, a reasonable action time interval of auto-channel shall be set according to the actual RF environment, the cleaner the RF environment, the

Parameter	Description
	longer the time interval. ○ **Anchor Time:** Auto-channel selection performs only at the fixed time specified here. ▪ **Auto Channel Close Threshold:** Too busy traffic shall close thin AP's automatic channel switching to protect user services. Here to set the traffic threshold of close auto-channel selection. ▪ **Auto Channel RSSI Sensitivity:** The thin AP measures the signal strength of the neighboring AP before channel switching. Once the measured signal strength is higher than the threshold here, indicating that current channel has been polluted, and it must immediately switch to a cleaner channel. Here to set the fuzzy threshold of the signal strength of the neighboring AP: ○ **High:** Fuzzy value, the signal strength that can cause serious interference. ○ **Medium:** Fuzzy value, the signal strength that can cause slight interference. ○ **Low:** Fuzzy value, the signal strength that cannot cause the interference. ▪ **Enable Manual Grouping:** By default, thin AP automatically scan the neighboring APs for grouping by themselves. But if the "**Manual Grouping**" is enabled here, customer can manually scan neighboring APs for grouping, and the thin APs in the same group share the profiles.
Fast Roaming Settings	If using IEEE 802.11r for fast roaming, the thin AP needs to obtain the information of the neighboring APs and inform the wireless clients of the information. Click the <**Refresh**> button here to scan the neighboring APs and exchange information with the neighboring APs.
Thin AP Packet Capture	Here to set the globally effective rules for AP Packet Capture. If the thin AP packet capture rule configured in the [**Common Profile**] selects the "**Global**" option, then use the rules configured here: ▪ **FTP Server IP Address:** The IP address of the FTP server for uploading captured packets. ▪ **FTP Server Username:** The username for remotely login the FTP server. ▪ **FTP Server Password:** The password for remotely login the FTP server. ▪ **Packet Source:** Select the packet capture point here: ○ **Wireless Port:** The packets from air interface of thin AP will be captured. ○ **Wired Port:** The packets from wired port of thin AP will be captured. ▪ **Capture Channel:** The packets from the specific radio channel of thin AP will be captured. ▪ **Capture Time:** Specify how long the capturing will last. The action of capture is initiated at [**Statistics** > **Thin AP List**].

Click the **Refresh** button to restart the scan.

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

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

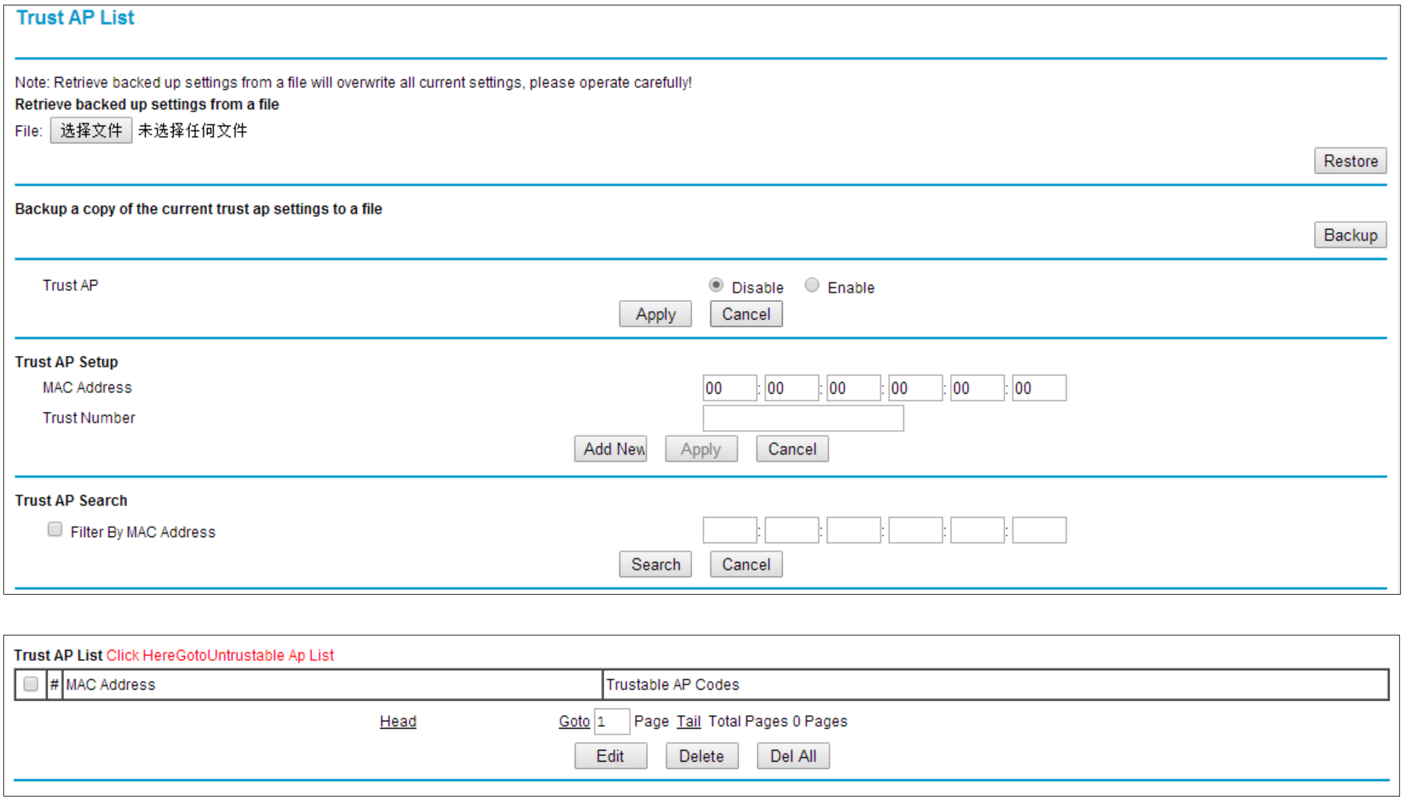
Chapter 8. ACCESS CONTROL

As a gateway, the WLC is the entrance for the Wi-Fi radio access network to enter the core network. Therefore, it is important to ensure the security of the core network and protect it from illegal device invading. The access control is a security barrier erected in the WLC so that it can only accept access from "trusted devices" and deny access of "non-trusted devices".

8.1. AP ACCESS CONTROL

The thin AP access to the WLC can be controlled through the "Trusted AP" list. The list contains the thin APs that are allowed to access the WLC, while the APs not included in this list are naturally "Untrusted APs" and therefore prohibited from accessing the WLC. Creation of the "trusted AP" list is a fundamental security measure to ensure that the WLC is protected from illegal APs intrusion.

Select **[Access Control > Trust AP List]** in the menu to enter the configuration page as following:



Trust AP List

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 trust ap settings to a file

Trust AP ● Disable ○ Enable

Trust AP Setup

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

Trust Number

Trust AP Search

□ Filter By MAC Address

Trust AP List Click HereGotoUntrustable Ap List

□	#	MAC Address	Trustable AP Codes

Head Goto 1 Page Tail Total Pages 0 Pages

Figure 8-1 Trust AP List Page

These parameters in **[Access Control > Trust AP List]** page is described in details as following:

Parameter	Description
Restore Trusted AP List	Recover the trusted AP list from a backup file.
Backup Trusted AP List	Save the trusted AP list to a file.
Trust AP	Turn on this switch to allow WLC to use the "trusted AP list" to check the credit of

Parameter	Description
	thin APs to control their access; Turn off this switch to prohibit WLC to use the trusted AP list for access control. **Default is Disable.**
MAC Address	Enter the MAC address of the thin AP that is trusted.
Trust Number	Assign an unique ID for this trusted AP.
<Add New>	Click the <**Add New**> button to append this thin AP to the trust AP list.
Filter By MAC Address	A search condition to find the thin AP by MAC address in trusted list.

Click the **Restore** button to recover the trusted AP list from a backup file on the local PC.

Click the **Backup** button to back up the list to the local PC.

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

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

Click the **Search** button to search for an entry based on the information specified.

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

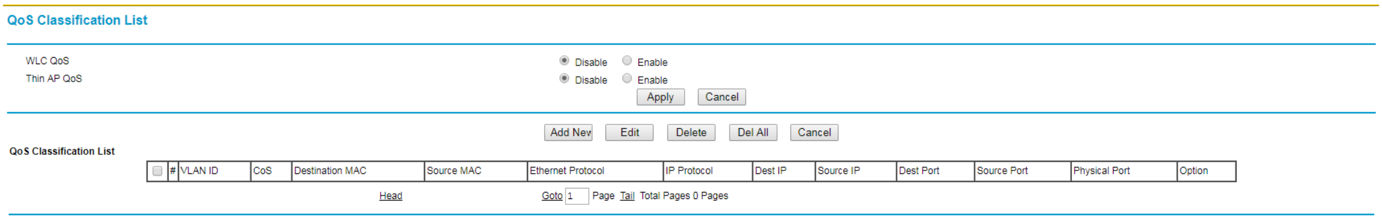
Click the **Delete** button to remove the selected entry.

Click the **Del All** button to remove all the entries from the configuration.

8.2. QoS Classification

QoS classification actually creates a set of matching rules for input packets, and binds treatment methods for the matched packets. For example, the matched packets can be "Dropped" or "Accepted". For packets classified as QoS, the DSCP and CoS fields should also be replaced with customer-defined values, and then forwarded to next path.

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



QoS Classification List

WLC QoS ● Disable ○ Enable

Thin AP QoS ● Disable ○ Enable

QoS Classification List

□	#	VLAN ID	CoS	Destination MAC	Source MAC	Ethernet Protocol	IP Protocol	Dest IP	Source IP	Dest Port	Source Port	Physical Port	Option

Head Goto 1 Page Tail Total Pages 0 Pages

Figure 8-2 QoS Classification Entrance Page

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

Parameter	Description
WLC QoS	Turn on this switch to enable WLC to use QoS classification rules to match the "central switching" user data packets. The default is "**Disable**".

Parameter	Description
Thin AP QoS	Turn on this switch to enable thin AP to use QoS classification rules to match the "local switching" user data packets. The default is "**Disable**".

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

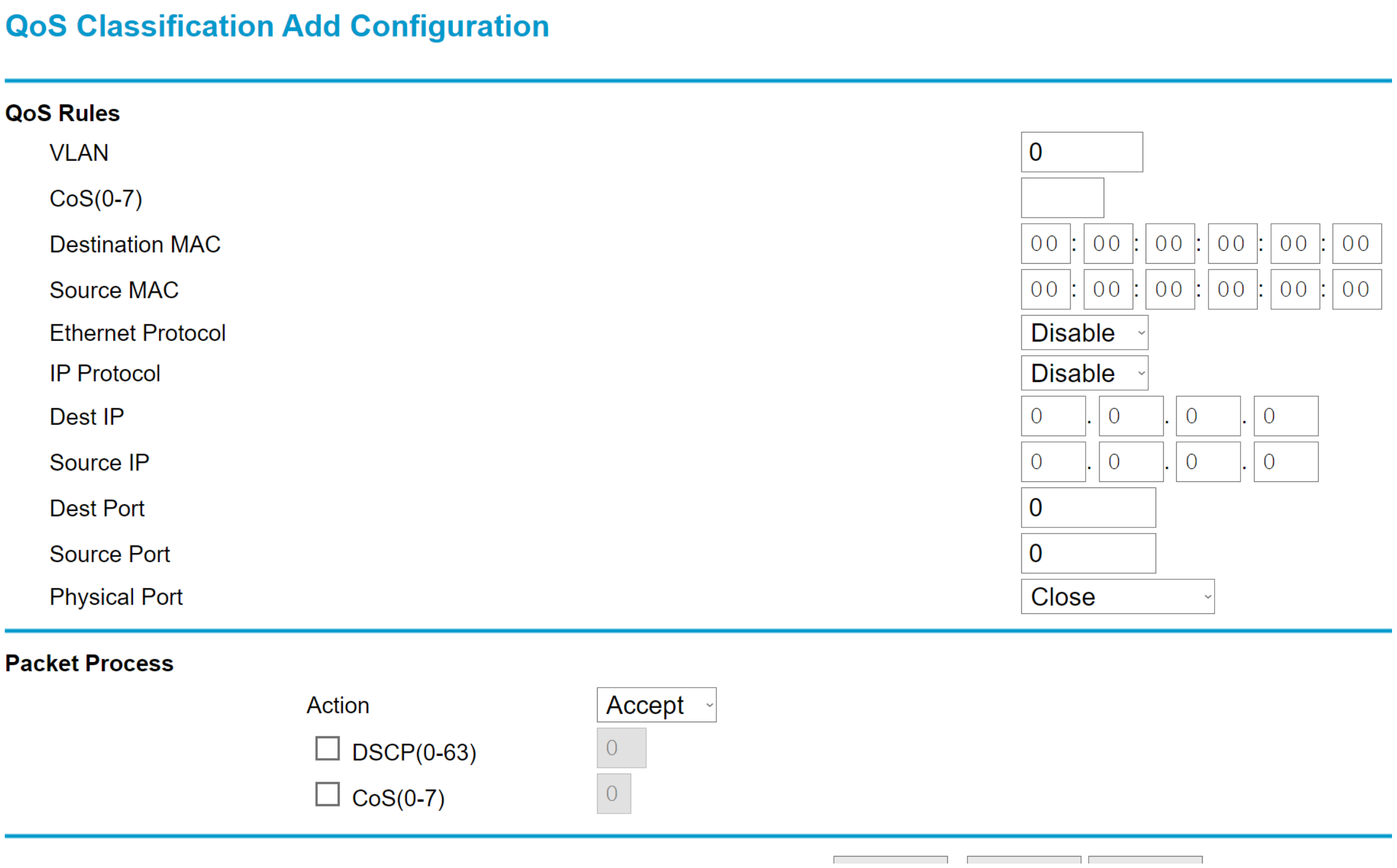
Click the **Cancel** button to discard the changes.

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.

Click the <**Add New**> or <**Edit**> button to enter the parameters configuration page as following:



QoS Classification Add Configuration

QoS Rules

VLAN	0
CoS(0-7)	
Destination MAC	00 : 00 : 00 : 00 : 00 : 00
Source MAC	00 : 00 : 00 : 00 : 00 : 00
Ethernet Protocol	Disable
IP Protocol	Disable
Dest IP	0 . 0 . 0 . 0
Source IP	0 . 0 . 0 . 0
Dest Port	0
Source Port	0
Physical Port	Close

Packet Process

Action	Accept
□ DSCP(0-63)	0
□ CoS(0-7)	0

Figure 8-3 QoS Classification Parameters Configuration Page

Define a set of rules to match the sub items in protocol unit of the data packet to divide it into QoS or non-QoS type. The matched packets will be handled according to specific methods to ensure QoS. The matching rules are defined as follows:

Parameter	Description
VLAN	This VLAN ID is used for matching the VLAN ID in a packet.
CoS	CoS stands for "Service Code", which is a layer 2 identifier of QoS used together with VLAN ID (and ToS is a layer 3 identifier). The larger the value, the higher the priority.
Destination MAC	This MAC address is used for matching the destination MAC address in a packet.

Parameter	Description
Source MAC	This MAC address is used for matching the source MAC address in a packet.
Ethernet Protocol	Select a Ethernet protocol from the pull-down menu as the matching key, including: ▪ **Disable:** No Ethernet protocol is used for matching packet. ▪ **ARP:** ARP packet will take part in matching. ▪ **IPv4:** IPv4 packet will take part in matching. ▪ **IPv6:** packet will take part in matching. ▪ **PPPoE:** PPPoE packet will take part in matching.
IP Protocol	Select a transport layer protocol from the pull-down menu as the matching key, including: ▪ **Disable:** No transport layer protocol is used for matching packet. ▪ **TCP:** TCP packet will take part in matching. ▪ **UDP:** UDP packet will take part in matching. ▪ **ICMP:** ICMP packet will take part in matching.
Dest IP	This IP address is used for matching the destination IP address in a packet.
Source IP	This IP address is used for matching the source IP address in a packet.
Dest Port	This port number is used for matching the destination port number in a packet.
Source Port	This pot number is used for matching the source port number in a packet.
Physical Port	**Physical Port:** Select a physical port from the pull-down menu to match where the packet comes from, including: ▪ **Close:** Don't care where the packet is coming from. ▪ **Wire Port:** The packet coming from wire port will take part in matching. ▪ **Wireless Port:** The packet coming from air interface will take part in matching.

Matching packets should be processed as described below:

Parameter	Description
Action	The matched packets will be handled as:
	● **Accept:** if ingress packet is matched one of above rules, it will be **ACCEPTed**.
	● **Drop:** if ingress packet is matched one of above rules, it will be **DROPPed.**
DSCP	The DSCP field of the matched packet should be replaced with the specific value here.
CoS	The CoS field of the matched packet should be replaced with the specific value here.

Click the **Back** button to discard the changes made and return to the previous page.

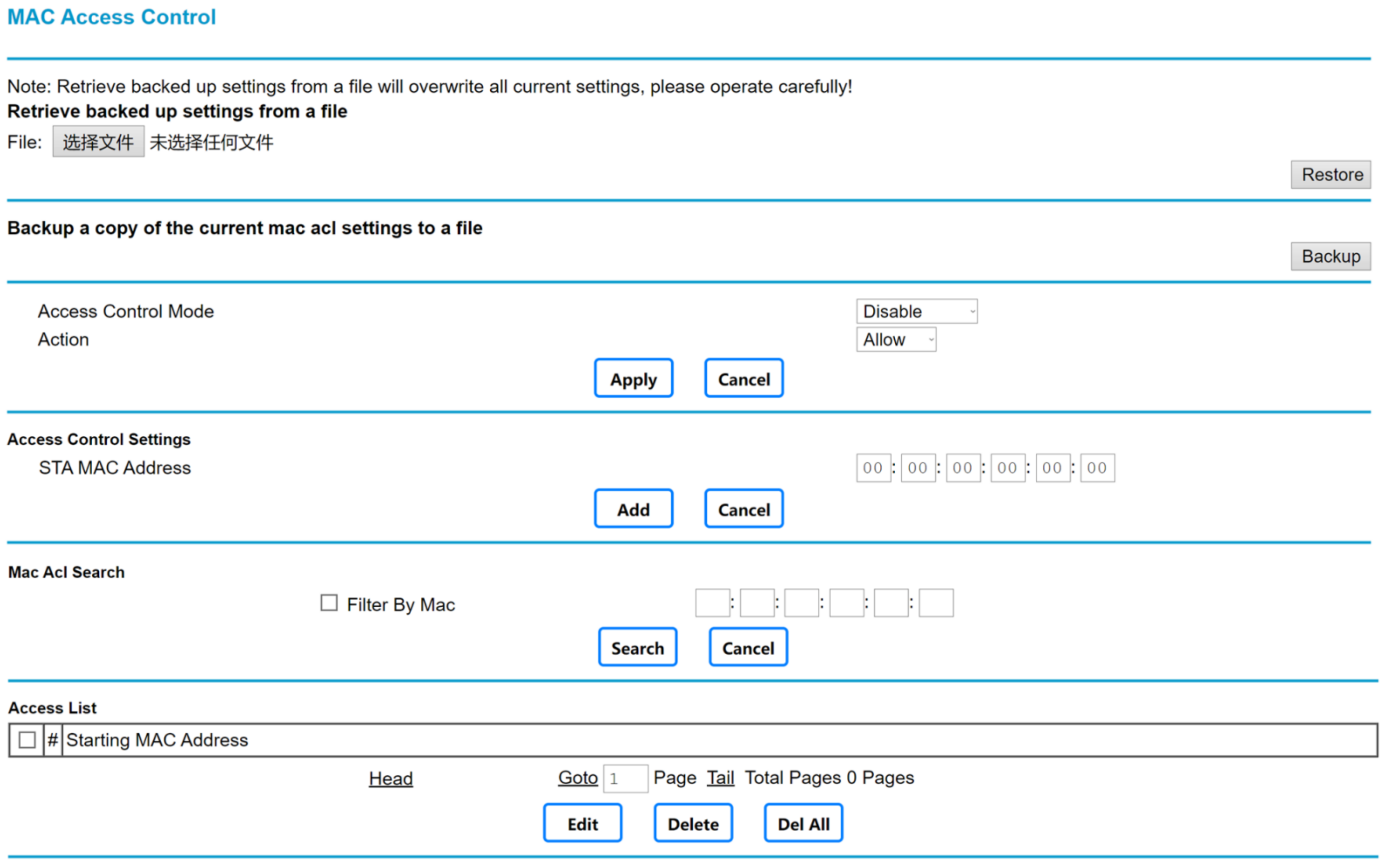
Click the **Apply** button to accept the changes.

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

8.3. USER ACCESS CONTROL

The user client association with thin AP can be controlled through the "black and white list based on the client MAC address". If the user client attribute in this list is "allowed", the association request will be accepted by the thin AP; and if the user client attribute in the list is “Reject", the association request will not be accepted by the thin AP. The black and white list is created in the WLC, and the thin AP downloads it to local to control the association of the user clients. This is actually a user MAC-based ACL.

Select **[Access Control** > **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 8-4 MAC Access Control Page

Click the **Backup** button to back up the settings to the local PC.

Click the **Restore** button to restore the settings from a backup file on the local PC.

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

Parameter	Description
Access Control Mode	There are four MAC-based user access control modes: ▪ **Disable:** Thin AP does not control the user clients association. ▪ **MAC:** Thin AP controls the user client association based on its MAC address. ▪ **MAC@VAP:** The virtual AP with the SSID specified here controls the user client association based on its MAC address. ▪ **Special MAC:** The special MAC represents the VIP client, it is allowed to

Parameter	Description
	associate with thin AP without authentication.
Action	Bind the attribute for selected access control mode: ▪ **Allow:** This attribute indicates that the user client is permitted to associate with thin AP. ▪ **Reject:** This attribute indicates that the user client is prohibited to associate with thin AP.
STA MAC Address	Enter the user client MAC address 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 addresses of all user clients under control and their control attributes.

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.

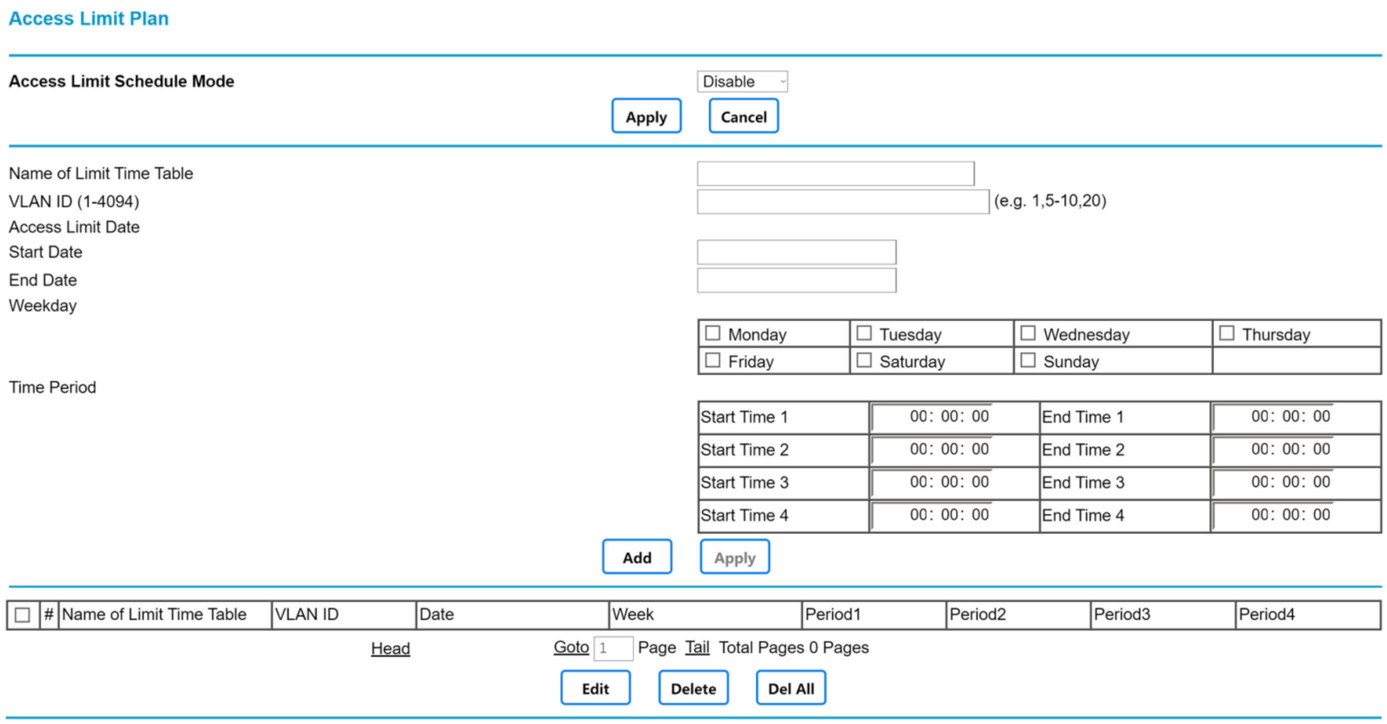
Click the **Del All** button to remove all the Access Control entry from the list.

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

8.4. Access Time Control

"Access time control" means that wireless clients are not allowed to access the Wi-Fi network during the specific time periods, that is, the thin AP rejects all wireless clients' association requests during those periods. For campus Wi-Fi network, this is a very useful function.

Select **[Access Control** > **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 8-5 Access Time Control Configuration Page

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

Parameter	Description
Access Limit Schedule Mode	There are three control modes for choose: ▪ **Disable:** No restriction for user clients accessing Wi-Fi network at any time. . ▪ **By VAP:** The access time control plan is only applied to the virtual AP identified by the SSID specified here. The configured access time control plan will be bound to a specific virtual AP in the [**VAP Profile**]. ▪ **By VLAN:** The access time control plan only controls the wireless clients on the VLAN specified here.
Name of Limit Time Table	Assign a literal name for this Access Time Schedule table for management.
VLAN ID	If "**Access Limit Schedule Mode**" selects "**By VLAN**", specify the under control 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	Select the start date for the access control schedule from the calendar.
End Date	Select the end date for the access control schedule from the calendar.

Parameter	Description
Weekday	Select the days of the week that need to implement the access time control.
Time Period	There are four time periods in each day that allow access time control. Please fill in the start and end times of these time periods.

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.

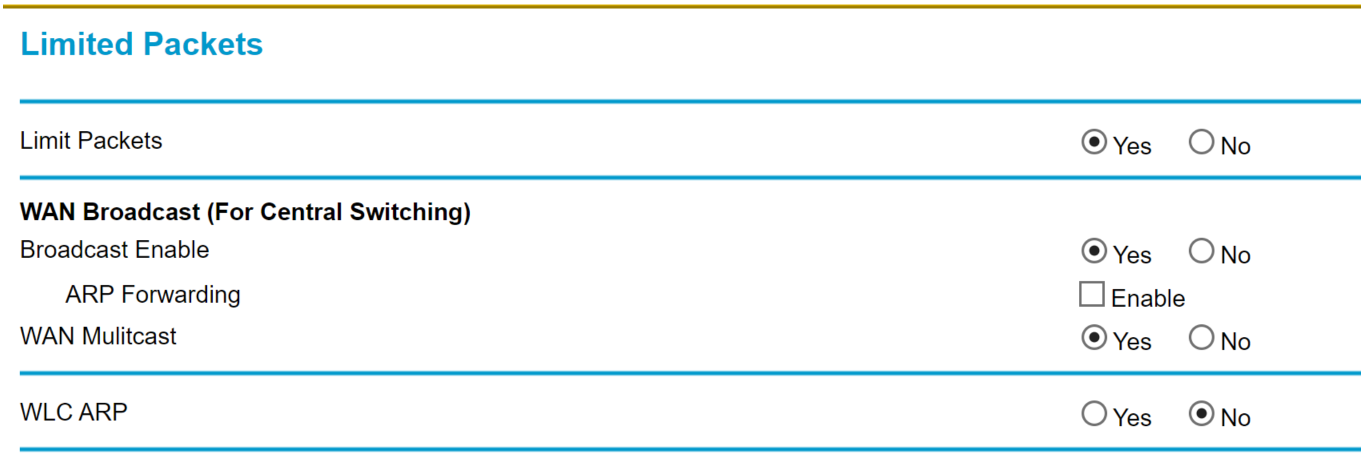
Click the **Delete** button to remove the selected Access Limit Time entry from the table.

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

8.5. Limited Packets

To enhance system security and avoid congestion caused by malicious packets, the WLC should take effective measures to restrict specific types of packets to prevent data flooding and protect the system from paralysis.

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



Limited Packets

Limit Packets ● Yes ○ No

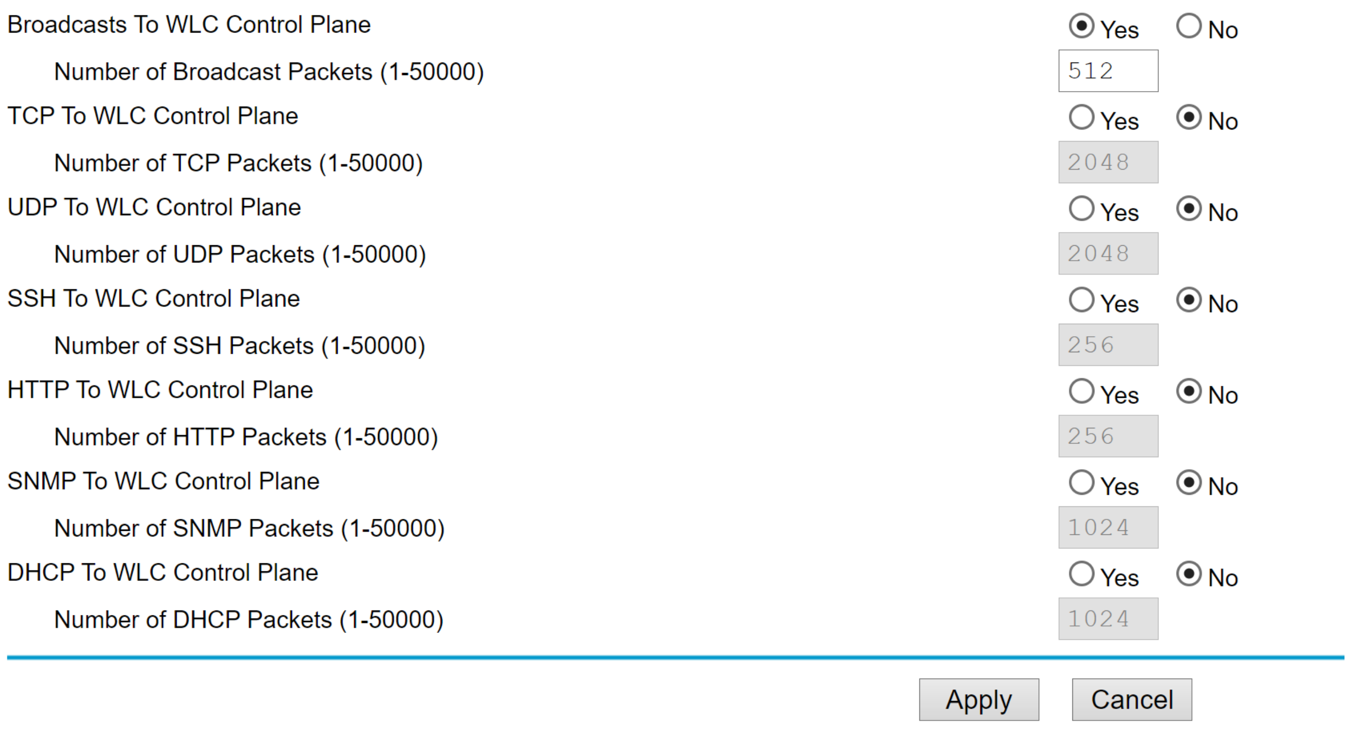
WAN Broadcast (For Central Switching)

Broadcast Enable ● Yes ○ No

ARP Forwarding □ Enable

WAN Mulitcast ● Yes ○ No

WLC ARP ○ Yes ● No



Broadcasts To WLC Control Plane ● Yes ○ No

Number of Broadcast Packets (1-50000) 512

TCP To WLC Control Plane ○ Yes ● No

Number of TCP Packets (1-50000) 2048

UDP To WLC Control Plane ○ Yes ● No

Number of UDP Packets (1-50000) 2048

SSH To WLC Control Plane ○ Yes ● No

Number of SSH Packets (1-50000) 256

HTTP To WLC Control Plane ○ Yes ● No

Number of HTTP Packets (1-50000) 256

SNMP To WLC Control Plane ○ Yes ● No

Number of SNMP Packets (1-50000) 1024

DHCP To WLC Control Plane ○ Yes ● No

Number of DHCP Packets (1-50000) 1024

Figure 8-6 Limited Packets Configuration Page

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

Parameter	Description
Limit Packets	Turn on this switch to enable the protection of flooding for WLC. **Default is Yes.**
WAN Broadcast **(Only for Central Switching)**	▪ **Broadcast Enable:** The broadcast packets are isolated at WLC northbound port. **Default is Yes.** ▪ **ARP Forwarding:** The ARP packet is allowed to be forwarded at WLC northbound ports. **Default is Disable.** ▪ **WAN Multicast:** The multicast packets are isolated at WLC northbound port. **Default is Yes.**
WLC ARP	Turn on this switch to enable WLC to generate its own ARP packet. **Default is No.**
Broadcasts To WLC Control Plane	Turn on this switch to limit the broadcast packets entering WLC. **Default is Yes.** ● **Number of Broadcast Packets:** If the above switch selects "**Yes**", here to set the threshold of the number of broadcast packets allowed to enter, and the broadcast packets that exceed this threshold will be discarded.
TCP To WLC Control Plane	Turn on this switch to limit external TCP packets entering the WLC. **Default is No.** ● **Number of TCP Packets:** If the above switch selects "**Yes**", here to set the threshold of the number of TCP packets allowed to enter, and the TCP packets that exceed this threshold will be discarded.
UDP To WLC Control Plane	Turn on this switch to limit external UDP packets entering the WLC. **Default is No.** ● **Number of UDP Packets:** If the above switch selects "**Yes**", here to set the threshold of the number of UDP packets allowed to enter, and the UDP packets that exceed this threshold will be discarded.

Parameter	Description
SSH To WLC Control Plane	Turn on this switch to limit external SSH packets entering the WLC. **Default is No.**
	● **Number of SSH Packets:** If the above switch selects "**Yes**", here to set the threshold of the number of SSH packets allowed to enter, and the SSH packets that exceed this threshold will be discarded.
HTTP To WLC Control Plane	Turn on this switch to limit external HTTP packets entering the WLC. **Default is No.**
	● **Number of HTTP Packets:** If the above switch selects "**Yes**", here to set the threshold of the number of HTTP packets allowed to enter, and the HTTP packets that exceed this threshold will be discarded.
SNMP To WLC Control Plane	Turn on this switch to limit external SNMP packets entering the WLC. **Default is No.**
	● **Number of SNMP Packets:** If the above switch selects "**Yes**", here to set the threshold of the number of SNMP packets allowed to enter, and the SNMP packets that exceed this threshold will be discarded.
DHCP To WLC Control Plane	Turn on this switch to limit external DHCP packets entering the WLC. **Default is No.**
	● **Number of DHCP Packets:** If the above switch selects "**Yes**", here to set the threshold of the number of DHCP packets allowed to enter, and the DHCP packets that exceed this threshold will be discarded.

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

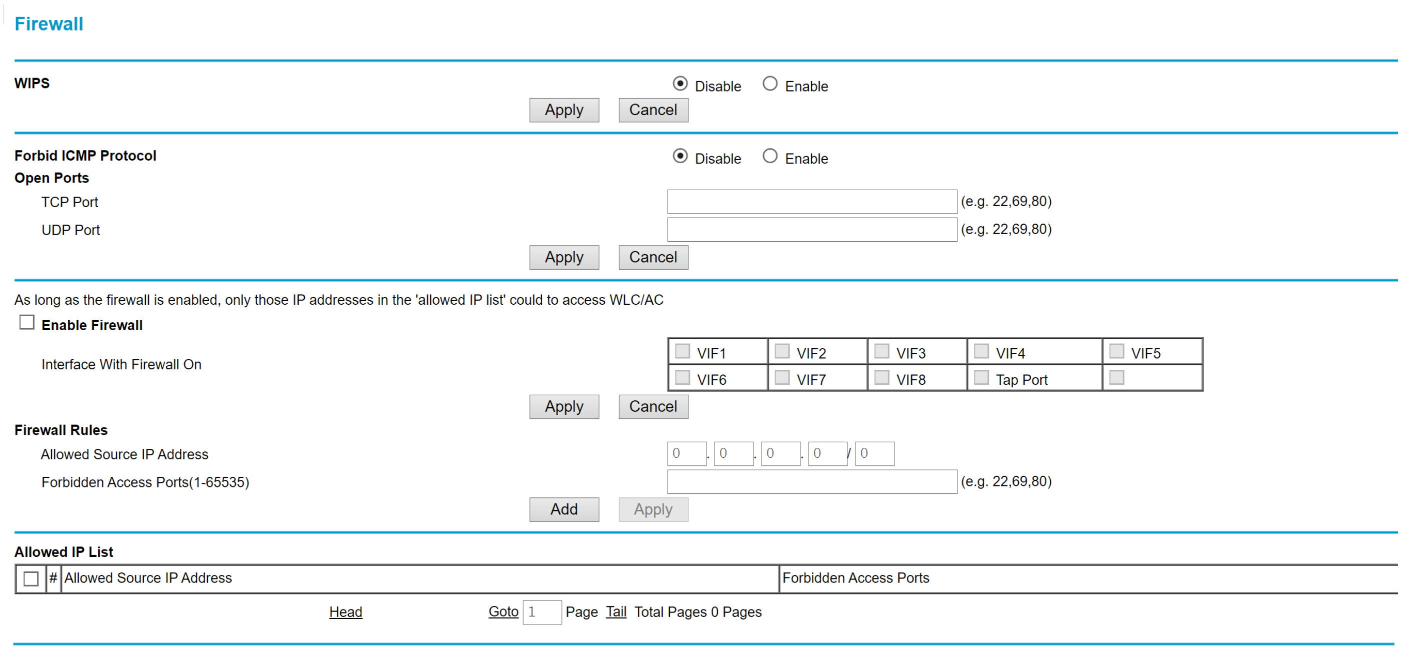
Click the **Cancel** button to discard the changes.

8.6. FIREWALL

The firewall is used to protect the WLC from external hackers. It ensure that the access packets are under control by opening only limited communication ports, authorizing and filtering the specific IP addresses. All packets that do not meet with the rules are rejected.

WIPS is a wireless firewall for thin APs. Enabling it can ensure that packets initiated by illegal wireless users are blocked on the air interface of thin AP.

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



Firewall

WIPS ● Disable ○ Enable

Apply Cancel

Forbid ICMP Protocol ● Disable ○ Enable

Open Ports

TCP Port (e.g. 22,69,80)

UDP Port (e.g. 22,69,80)

Apply Cancel

As long as the firewall is enabled, only those IP addresses in the 'allowed IP list' could to access WLC/AC

□ Enable Firewall

Interface With Firewall On

□ VIF1	□ VIF2	□ VIF3	□ VIF4	□ VIF5
□ VIF6	□ VIF7	□ VIF8	□ Tap Port	□

Apply Cancel

Firewall Rules

Allowed Source IP Address 0 . 0 . 0 . 0 / 0

Forbidden Access Ports(1-65535) (e.g. 22,69,80)

Add Apply

Allowed IP List

□	#	Allowed Source IP Address	Forbidden Access Ports

Head Goto 1 Page Tail Total Pages 0 Pages

Figure 8-7 Firewall Configuration Page

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

Parameter	Description
WIPS	Turn on this switch to enable the thin AP to open its WIPS protection for air interface. **Default is Disable.**
Forbid ICMP Protocol	Turn on this switch to prevent ***ping*** packets from entering WLC. **Default is Disable.**
Open Ports	Allow external sources to access the open ports(Multiple ports can be separated by commas): ▪ **TCP Port:** Entering the TCP ports allowing external sources to access. Multiple TCP port numbers can be separated by commas. ▪ **UDP Port:** Entering the UDP ports allowing external sources to access. Multiple UDP port numbers can be separated by commas.
Enable Firewall	Check the radio button to enable WLC to use the firewall rules to its internal layer 3 interfaces: ▪ **VIF1~8:** Bind the firewall rules to the selected layer 3 interfaces. ▪ **TAP Port:** Bind the firewall rules to the thin AP access port (i..e., the WLAN port).
Firewall Rules	▪ **Allowed Source IP Address:** Only the packet with its source IP address matching with the specific IP address here is accepted by WLC. ▪ **Forbidden Access Ports:** Enter the specific ports to be blocked from external accessing, and multiple port numbers can be separated by commas.

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.

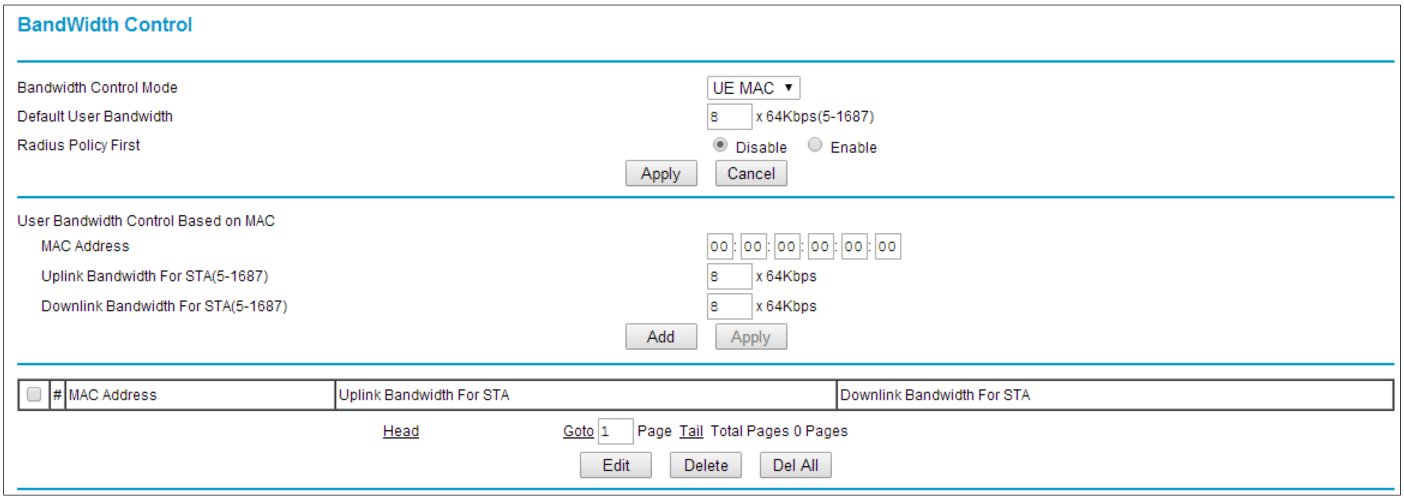
Click the **Delete** button to remove the selected entry.

Click the **Del All** button to remove all the entries from the configuration.

8.7. BANDWIDTH CONTROL

The total bandwidth of the system is always limited. Therefore, the system bandwidth can be divided into two parts: one is used as competitive bandwidth, that is, the evenly distributed bandwidth for each user fluctuates according to the number of online users; the other part is used as guaranteed bandwidth, that is, regardless the fluctuation of the number of online users, a fixed bandwidth is always reserved for those specific users. Usually the two types of bandwidth coexist in a system, depending on the bandwidth allocation policy.

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



BandWidth Control

Bandwidth Control Mode: UE MAC

Default User Bandwidth: 8 x 64Kbps(5-1687)

Radius Policy First: ● Disable ○ Enable

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

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

Head Goto 1 Page Tail Total Pages 0 Pages

Figure 8-8 Bandwidth Control Configuration

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

Parameter	**Description**
Bandwidth Control Mode	Select where the bandwidth control policy is configured and the scope of the bandwidth control policy takes effect: ▪ **Disable:** No bandwidth control is required for any user client. ▪ **UE MAC:** Bandwidth control is based on the user client MAC addresses, the matched user clients on all thin APs will have its bandwidth restricted. ▪ **VAP:** The bandwidth control policy is configured in the [**VAP profile**], and only act to the user clients on that VAP. ▪ **VLAN:** The bandwidth control policy is configured in the [**VLAN Creation**], and only act to the user clients on that VLAN .
Radius Policy First	Turn on this switch to enable thin AP firstly adopt the bandwidth control

Parameter	Description
	policy from the Radius server. Only fails to obtain the policy, will the policy configured in WLC be used instead.
Default User Bandwidth	In the **UE MAC** mode, 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.
User Bandwidth Control Based on MAC	In the **UE MAC** mode, here to set the bandwidth control policy based on user client MAC address: ▪ **MAC Address:** Enter the MAC address of user client which is under the bandwidth control. ▪ **Uplink Bandwidth:** The rate of uploading data for the user client with this MAC address. ▪ **Downlink Bandwidth:** The rate of downloading data for the user client with this MAC address.

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.

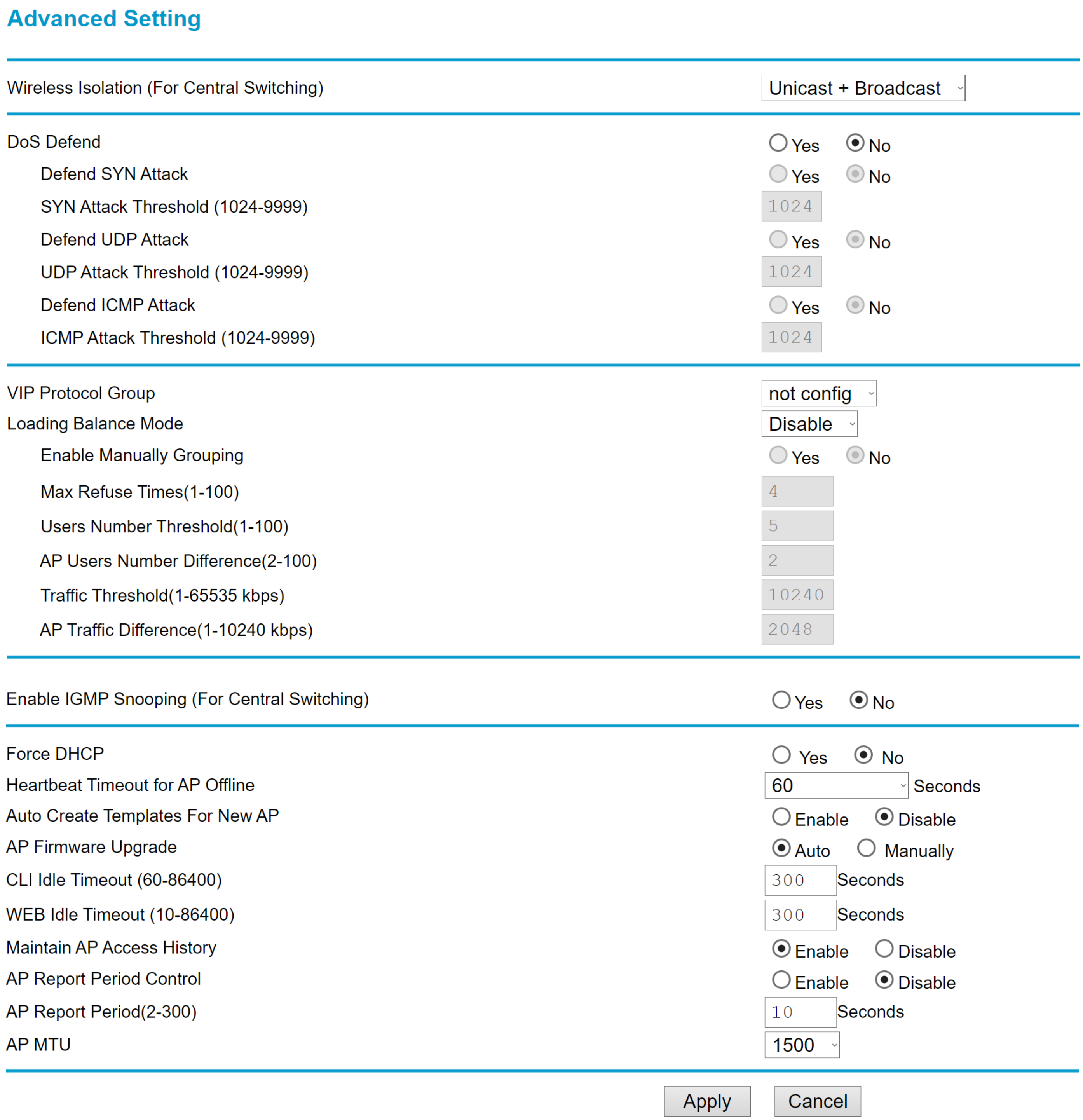
Click the **Delete** button to remove the selected entry.

Click the **Del All** button to remove all the entries from the configuration.

8.8. ADVANCED SETTINGS

"**Advanced Settings**" requires the system administrator to have a deeper understanding of Wi-Fi system and network communication, because these parameters may be helpful to improve system performance, expand system functions, and achieve some fine control to the system.

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



Advanced Setting

Wireless Isolation (For Central Switching): Unicast + Broadcast

DoS Defend: ○ Yes ● No

Defend SYN Attack: ○ Yes ● No

SYN Attack Threshold (1024-9999): 1024

Defend UDP Attack: ○ Yes ● No

UDP Attack Threshold (1024-9999): 1024

Defend ICMP Attack: ○ Yes ● No

ICMP Attack Threshold (1024-9999): 1024

VIP Protocol Group: not config

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

Enable IGMP Snooping (For Central Switching): ○ Yes ● No

Force DHCP: ○ Yes ● No

Heartbeat Timeout for AP Offline: 60 Seconds

Auto Create Templates For New AP: ○ Enable ● Disable

AP Firmware Upgrade: ● Auto ○ Manually

CLI Idle Timeout (60-86400): 300 Seconds

WEB Idle Timeout (10-86400): 300 Seconds

Maintain AP Access History: ● Enable ○ Disable

AP Report Period Control: ○ Enable ● Disable

AP Report Period(2-300): 10 Seconds

AP MTU: 1500

Figure 7-1 Advanced Setting Page

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

Parameter	Description
Wireless Isolation	For wireless network security, it is usually necessary to isolate wireless clients to prevent unicast or broadcast packets from transmission between wireless clients through virtual AP. The isolation policy configured below will be globally effective for all virtual APs in entire network: ▪ **Disable:** No packets transmission isolation between wireless clients. ▪ **Unicast:** Only unicast packets are blocked from transmission between

Parameter	Description
	wireless clients. ▪ **Broadcast:** Only broadcast packets are blocked from transmission between wireless clients. ▪ **Unicast+Broadcast:** Both broadcast and unicast packets are blocked from transmission between wireless clients.
DoS Defend	Turn on this switch (the default is off), the WLC will be protected from DoS attacks. The following provides several attack protection strategies:
	● **Defend SYN Attack:** SYN attack is an usual DoS attack method. The hacker initiates a TCP connection to the target server, and then uses vulnerability of TCP three-way handshake, continuously sending SYNs instead of ACKs, filling up the queue of TCP request in target server to stop it to respond to other normal TCP connections request. Turn on this switch to prevent SYN attacks. ● **SYN Threshold:** If SYN attack protection is enabled, set the upper threshold of the number of SYN packets, those SYN packets exceeding the threshold will be dropped.
	● **Defend UDP Attack:** UDP is a transportation protocol without handshake, hence it is easy for hacker to use it to flood the target server. Turn on this switch to enable UDP attack protection. ● **UDP Threshold:** If UDP attack protection is enabled, set the upper threshold of the number of UDP packets, those UDP packets exceeding the threshold will be dropped.
	● **Defend ICMP Attack:** ICMP is a protocol for link state detection without handshake. It is easy for hacker to use it to flood the target. Turn on this switch to enable ICMP attack protection. ● **ICMP Threshold:** If ICMP attack protection is enabled, set the upper threshold of the number of ICMP packets, those ICMP packets exceeding the threshold will be dropped.
VIP Protocol Group	No discussion here.
Load Balance Mode	The load balancing policy configured here is globally effective for the entire network, and the thin AP group can use it after enabling the "**Global** " configuration in its [**Common Profile**]: ▪ **Load Balancing Mode:** Three modes are provided for selection: ○ **Disable:** No global load balancing function will be applied. ○ **Users:** The load balancing is based on the number of user clients on the thin AP. ○ **Traffic:** The load balancing is based on the user traffic pressure on the thin AP. ▪ **Enable Manually Grouping** - By default, thin AP automatically scan the neighboring APs for grouping by themselves. But if the "**Manual Grouping**" is enabled here, customer can manually scan neighboring APs for grouping, and the thin APs in the same group share the profiles. ▪ **Max Refuse Time (1-100)**- Even if the user client is kicked out due to load

Parameter	Description
	balancing, it is allowed to associate again with the thin AP, but the number of times for re-association is limited to the fixed threshold set here. if the re-association is not successful within the threshold, the thin AP will no longer accept association requests from this client. ▪ **Users Number Threshold** - If the balance mode "**Users**" is selected, here to set the maximum number of user clients allowed to associate with the thin AP. 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, here to set the maximum difference in the number of user clients between two thin APs. When the difference touches this threshold, any new client attempting to associate with the thin AP who has more users will be rejected. ▪ **Traffic Threshold** - If the balance mode "**Traffic**" is selected, here to set the maximum throughput threshold allowed on the thin AP. When the traffic on 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, here to set the maximum throughput difference between two thin APs. When the traffic throughput difference reaches this threshold, any new client attempting to associate with the thin AP who has more traffic will be rejected.
Enable IGMP Snooping	Multicast members are created depending on IGMP, and the multicast streams are only forwarded to those members in multicast group. Enable IGMP snooping here to support multicast.
Force DHCP	This is a security function based on the DHCP snooping technology. Only clients that use the IP address allocated by their own DHCP server are allowed to access. The clients using IP addresses allocated by other DHCP servers will be rejected.
Heartbeat Timeout for AP Offline	Once the thin AP is connected to the WLC, the heartbeat message is used as the connection indicator. If the WLC does not receive a heartbeat message from the thin AP during the specific time period, it is determined that the thin AP is offline. The time period are **60**, **300**, **600**, **1200** seconds optional. If "never offline" option is selected, the WLC does not care the AP offline state.
Auto Create Profile for New AP	If enabled, the WLC will automatically copy the default profiles to the newly online thin AP for configuration.
AP Firmware Upgrade	Select the way for the thin AP to upgrade its firmware:
	● **Auto:** If the latest version firmware of thin AP is available on the WLC, the thin APs will automatically download it from WLC and upgrade.
	● **Manually:** Customer manually downloads the latest version firmware to thin AP by FTP or HTTP, and then upgrade.
CLI Idle Timeout	If there is no any operation in the “Command Line Interface” mode of WLC console for a specific period of time set here, the CLI is considered idle and then closed. If

Parameter	Description
	customer wants to enter the CLI mode again, it is necessary to re-login. The idle timeout can be set here.
WEB Idle Timeout	If there is no any operation on the WEB provisioning page of WLC for a specific period of time set here, the web page is considered idle and then exit. If customer wants to enter the provisioning web page again, it is necessary to re-login. The idle timeout can be set here.
Maintain AP Access History	Turn on this switch to enable WLC to reserve the record of access history of the thin APs for customer review.
AP Report Period Control	Turn on this switch to enable thin AP periodically to report users information and itself status to the WLC. **Default is OFF**. ▪ **AP Report Period:** If above radio button is checked to enable, here to set the time interval for thin AP reporting.
AP MTU	Enter the MTU (Maximum Transmit Unit) value for thin AP here.

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

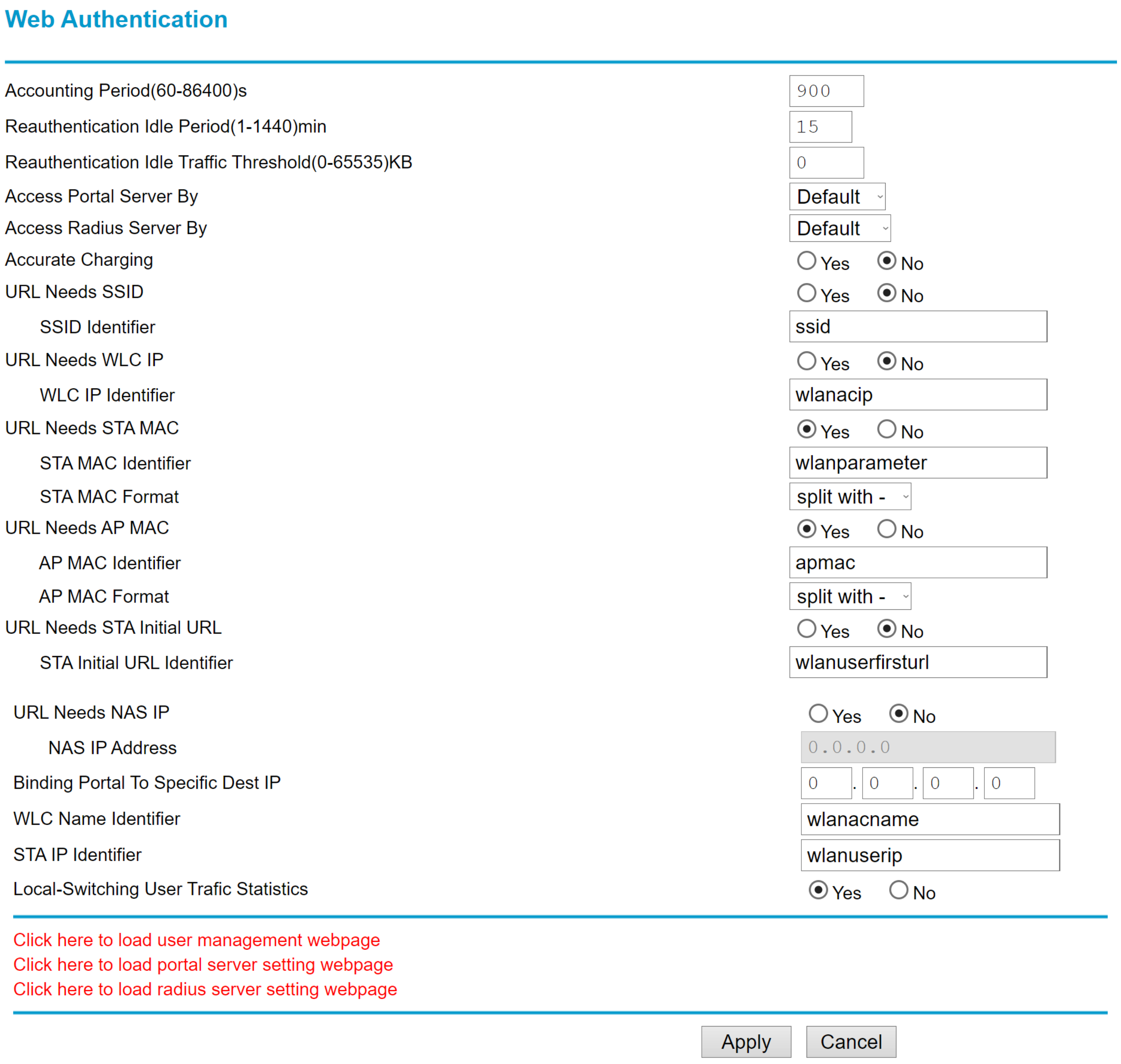
Click the **Cancel** button to discard the changes.

Chapter 9. Authentication

9.1. Web Authentication

Web authentication is used to authenticate wireless clients when they access the Wi-Fi system. This authentication mode uses the combination of Portal server and Radius server. When the wireless client attempts to start the data service for the first time, the Portal server will immediately pushes the username and password input web page to the client screen where the user enters the username and password and then forwarded to the Radius server for authentication. After authentication, the user client can start its data services, including Internet surfing.

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



Web Authentication

Accounting Period(60-86400)s	900
Reauthentication Idle Period(1-1440)min	15
Reauthentication Idle Traffic Threshold(0-65535)KB	0
Access Portal Server By	Default
Access Radius Server By	Default
Accurate Charging	○ Yes ● No
URL Needs SSID	○ Yes ● No
SSID Identifier	ssid
URL Needs WLC IP	○ Yes ● No
WLC IP Identifier	wlanacip
URL Needs STA MAC	● Yes ○ No
STA MAC Identifier	wlanparameter
STA MAC Format	split with -
URL Needs AP MAC	● Yes ○ No
AP MAC Identifier	apmac
AP MAC Format	split with -
URL Needs STA Initial URL	○ Yes ● No
STA Initial URL Identifier	wlanuserfirsturl
URL Needs NAS IP	○ Yes ● No
NAS IP Address	0.0.0.0
Binding Portal To Specific Dest IP	0 . 0 . 0 . 0
WLC Name Identifier	wlanacname
STA IP Identifier	wlanuserip
Local-Switching User Trafic Statistics	● Yes ○ No

Click here to load user management webpage
Click here to load portal server setting webpage
Click here to load radius server setting webpage

Figure 9-1 Web Authentication Configuration Page

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

Parameter	Description
Accounting Period	Here to set the billing cycle during which the WLC sends the users status information to the RADIUS server for accounting.
Re-authentication Idle Period	The user client is considered idle depending on it keeps in a lower traffic for a specific time period. Here to set the threshold for this specific time period.
Re-authentication Idle Traffic Threshold	The user client is considered idle depending on it keeps in a lower traffic for a specific time period. Here to set the threshold for this low traffic.
Access Portal Server By	Bind the Portal server to the resources below: ▪ **Default:** All users are authenticated by 1'st Portal server. This is for most scenarios. ▪ **VAP:** Virtual AP uses the Portal server configured in its own [**VAP Profile**]. ▪ **VLAN:** Different VLANs use the Portal servers configured in the [**VLAN Creation**].
Access Radius Server By	Bind the Radius server to the resources below: ▪ **Default:** All users are authenticated by 1'st Radius server. This is for most scenarios. ▪ **VAP:** Virtual AP uses the Radius server configured in its own [**VAP Profile**]. ▪ **Domain:** If the Portal server provides the output in format of ***username@domain***, it needs the specific Radius server to accept this format username.
Accurate Charging	This is used for billing based on time. The billing information will exclude the idle time of the user client to provide a more accurate active duration. **Default is disabling.**
URL Needs SSID	Turn on this switch to enable the Portal URL for wireless client redirection to contain the SSID query key (not the SSID itself). **Default is No.** ▪ **SSID Identifier:** If above switch is turned on, the SSID query key in the URL has to be given a literal name (not the SSID itself). **Default query key name is "*ssid*"**.
URL Needs WLC IP	Turn on this switch to enable the Portal URL for wireless client redirection to contain the WLC IP query key (not the WLC IP itself). **Default is No.** ▪ **WLC IP Identifier:** If above switch is turned on, the WLC IP query key in the URL has to be given a literal name (not the WLC IP itself). **Default query key is "*wlanacip*"**.
URL Needs STA MAC	Turn on this switch to enable the Portal URL for wireless client redirection to contain the STA MAC query key (not the STA MAC itself). **Default is YES**. ▪ **STA MAC Identifier:** If above switch is turned on, the STA MAC query key in the URL has to be given a literal name (not the STA MAC itself). **Default query key is "*wlanparameter*"**. ▪ **STA MAC Format:** Select whether the STA MAC address is split by "**:**" or "**-**".
URL Needs AP MAC	Turn on this switch to enable the Portal URL for wireless client redirection to contain

Parameter	Description
	the AP MAC query key (not the AP MAC itself). **Default is YES**. ▪ **AP MAC Identifier:** If above switch is turned on, the AP MAC query key in the URL has to be given a literal name (not the AP MAC itself). **Default query key is "*apmac*"**. ▪ **AP MAC Format:** Select whether the AP MAC address is split by "**:**" or "**-**".
URL Needs STA Initial URL	Turn on this switch to enable the Portal URL for wireless client redirection to contain the Initial URL query key (not the Initial URL itself). **Default is No**. ▪ **STA Initial URL Identifier:** If above switch is turned on, the Initial URL query key in the URL has to be given a literal name (not the Initial URL itself). **Default query key is "*wlanuserfirsturl*"**..
URL Needs NAS IP	The NAS stands for "Network Access Site". In most cases, it is the WLC itself, but if the WLC is deployed behind the NAT, the NAS is the public side the NAT. Turn on this switch to enable the Portal URL for wireless client redirection to contain the NAS IP address. **Default is No**. ▪ **NAS IP Address:** If the switch is turn on, here to enter the WLC (or the NAT public) IP Address that will be carried in the portal URL.
Binding Portal To Specific Dest IP	If the wireless client accesses a specific destination IP address, the WLC will redirect this access to the Portal server. Here to enter the specific IP address.
WLC Name Identifier	Here to enter the literal name for the query key of WLC name (not WLC name itself) that will be carried in the portal URL. **Default query key is "*wlanacname*"**.
STA IP Identifier	Here to enter the literal name for the query key of STA IP (not STA IP address itself) that will be carried in the portal URL. **Default query key is "*wlanuserip*"**.
Local-Forwarding User Traffic Statistics	If the thin AP works in the "**Local Switching**" mode, turn on this switch to inform thin APs to report user traffic statistics to the WLC.

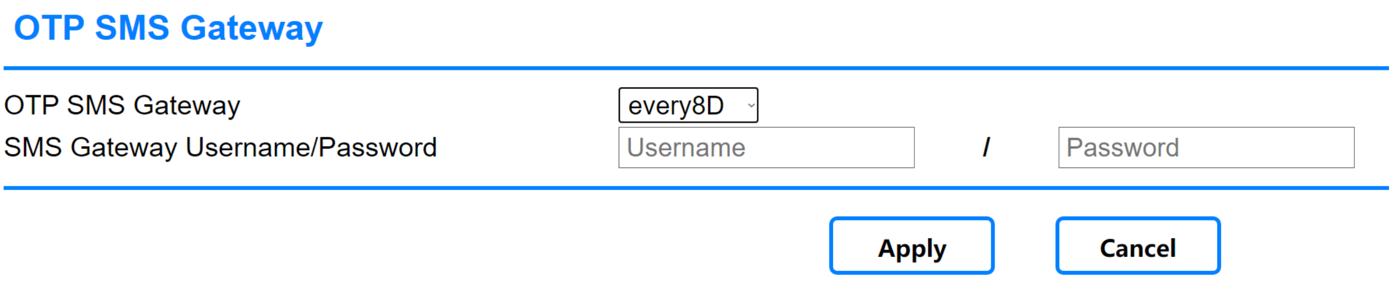
Click the **Apply** button to accept the changes.

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

9.2. **OTP SMS GATEWAY**

Wi-Fi network often uses "One Time Password" for user authentication. The one-time-valid authentication codes of wireless users are generated by the WLC and forwarded to the wireless user clients in the form of short messages through the short message gateway (SMS Gateway). The WLC has to be connected to a SMS gateway to achieve password push. This requires that the WLC should be registered as a legal user of the specific SMS gateway in advance. Currently, Titan series WLC have supported two SMS gateway vendors, one is ***aliyun***, and the other is ***every8D***. In the future, new SMS gateway providers can also be added according to customer requirements.

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 9-2 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 service gateway. There are two SMS gateways for selection, one is **aliyun**, another is **every8D**. Note, WLC must register as a legitimate subscriber of the SMS gateway before the OTP authentication is enabled.
SMS Gateway Username/Password	Enter the user name and password officially released by the vendor of short message service gateway after customer successfully registered as its legitimate subscriber.

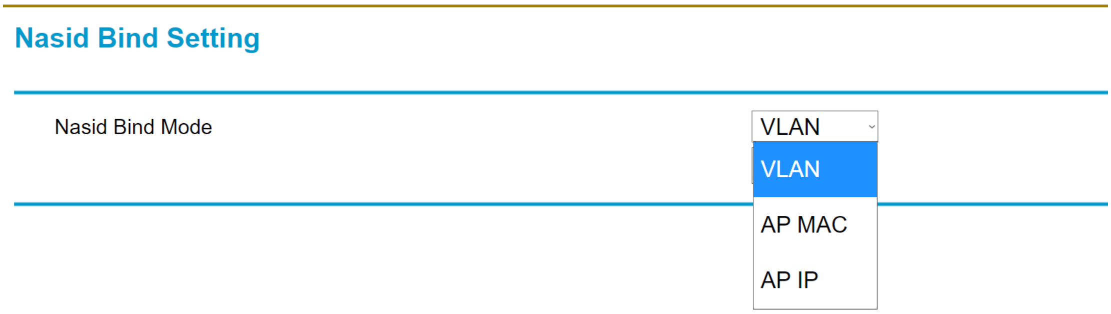
Click the **Apply** button to accept the changes.

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

9.3. NASID BINDING

NAS-ID is the abbreviation of **N**etwork **A**ccess **S**ite ID which is required by Radius server for roaming charging and clearing. It is usually assigned by operator in the format of ***HOST.CITY.PROVICE.OPERATOR.NATION***, for example 0046.0028.280.00.460 in which the exact meaning of each segment depends on the definition of local mobile operator.

Select **[Authentication** > **NAS ID Binding]** in the menu to enter the configuration page as following:



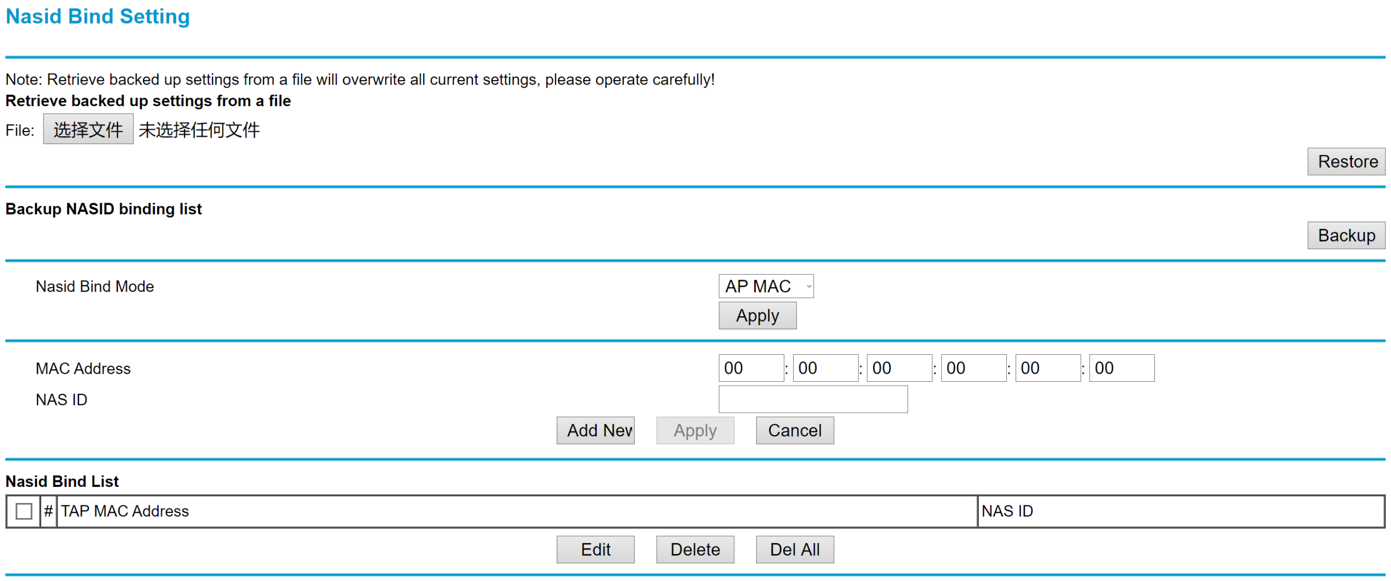
Nasid Bind Setting

Nasid Bind Mode: VLAN

Figure 9-2 NAS-ID Binding Entrance Page

There are three options for NAS-ID binding: ***VLAN***, ***AP MAC*** and ***AP IP***. If the ***NAS-ID*** is bound to ***VLAN*** here, then each VLAN has its own NAS-ID configured in [**Network Setup** > **VLAN Creation**].

If the ***NAS-ID*** is bound to ***AP MAC*** here, then entering the configuration page as shown below:



Nasid Bind Setting

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

Restore

Backup NASID binding list

Backup

Nasid Bind Mode: AP MAC

Apply

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

NAS ID:

Add Nev Apply Cancel

Nasid Bind List

□	#	TAP MAC Address	NAS ID

Edit Delete Del All

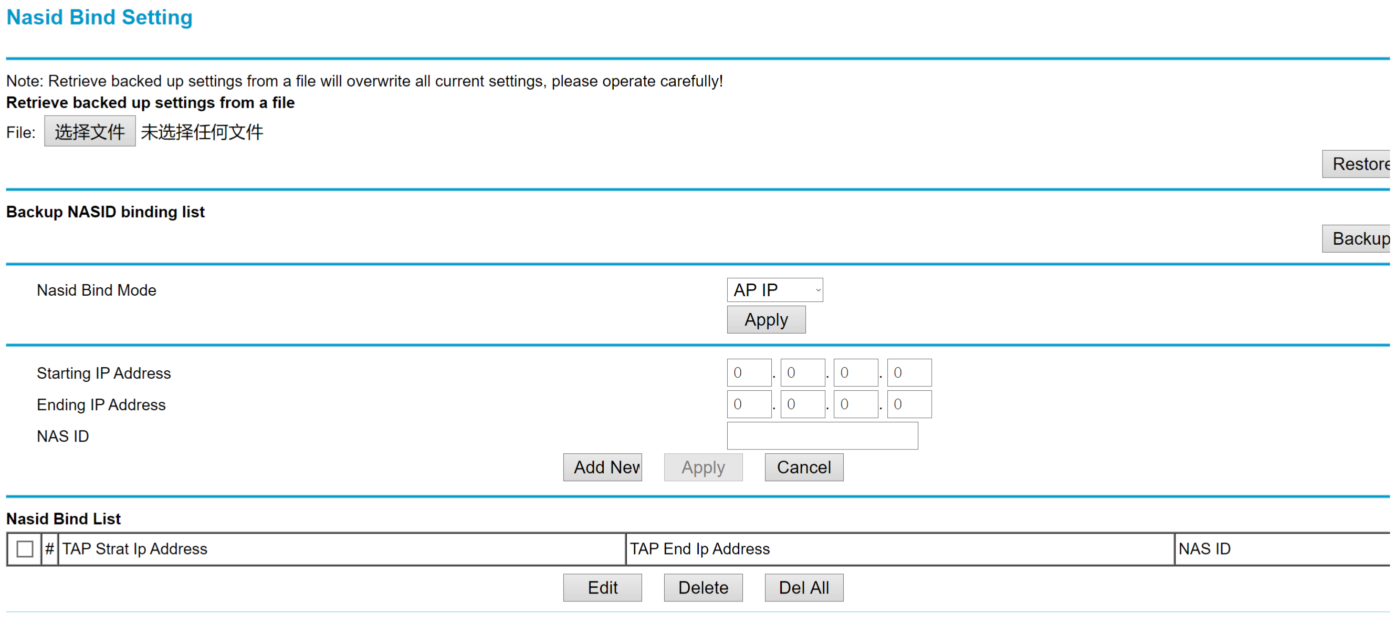
Figure 9-4 NAS-ID Binds to AP MAC Address

These parameters in **[Authentication** > **NAS-ID Binding > AP MAC]** page is described in details as following:

Parameter	Description
Nasid Bind Mode	**AP MAC** is selected.
MAC Address	Enter the MAC address of a thin AP to identify this thin AP will be bound to current NAS-ID.
NAS ID	Allocate a **NAS-ID** to bind to the thin AP identified by this MAC address.

Click the <**Add New**> button to append the new binding to the list.

If the ***NAS-ID*** is bound to ***AP IP*** here, then entering the configuration page as shown below:



Nasid Bind Setting

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

Restore

Backup NASID binding list

Backup

Nasid Bind Mode: AP IP

Apply

Starting IP Address: 0 . 0 . 0 . 0

Ending IP Address: 0 . 0 . 0 . 0

NAS ID:

Add Nev Apply Cancel

Nasid Bind List

□	#	TAP Strat Ip Address	TAP End Ip Address	NAS ID

Edit Delete Del All

Figure 9-5 NAS-ID Binds to AP IP Address

These parameters in **[Authentication** > **NAS-ID Binding > AP IP]** page is described in details as following:

Parameter	Description
Nasid Bind Mode	**AP IP** is selected. A group of thin APs identified by IP addresses can be bound to one NAS-ID.
Starting IP Address	The first thin AP identified by this IP address in the group needs to be bound to the NAS-ID.
Ending IP Address	The last thin AP identified by this IP address in the group needs to be bound to the NAS-ID.
NAS ID	Allocate a **NAS-ID** to bind to the group of thin APs identified by a segment of IP addresses.

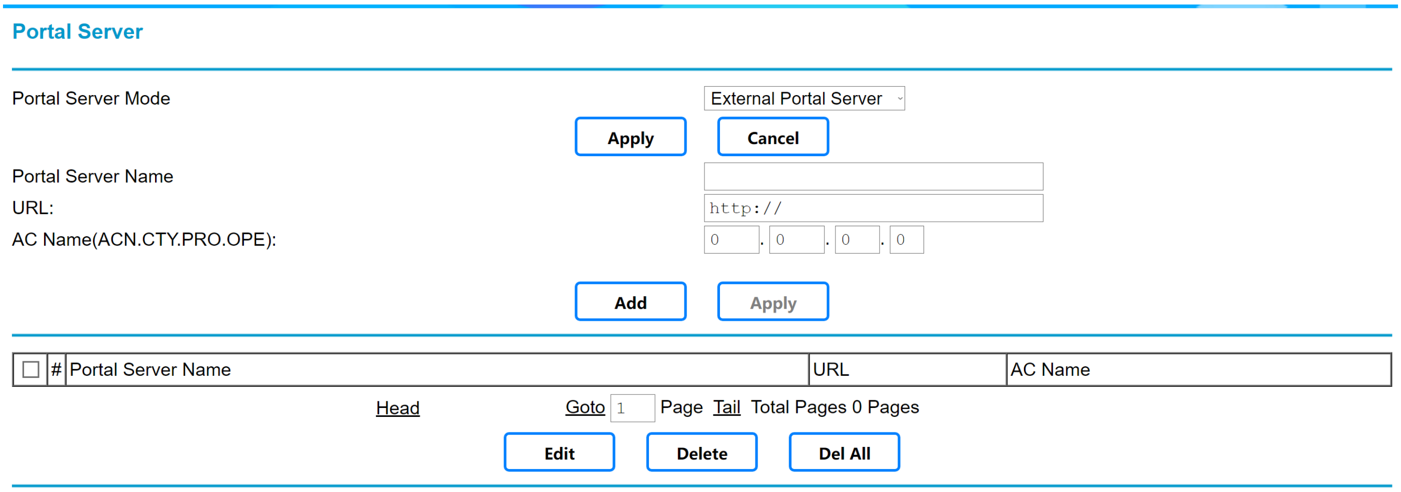
Click the <**Add New**> button to append the new binding to the list.

9.4. PORTAL SERVER

Portal server provides an entrance for user authentication through web by push a web page to the user endpoint for entering the user name and password. If the WEB authentication is enabled, as long as an unauthenticated wireless client initiates a data service, the visited URL will be intercepted by WLC, and then forcibly redirected to the Portal server, and the Portal server will push the entrance web page to the wireless endpoint. Finally, the Portal server forwards the username and password entered by the user to the Radius server to complete the authentication.

The Titan series WLC has a built-in Portal server, so it can provide either internal Portal service or external Portal service. Therefore, it needs customer pay attention to the selection.

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 9-6 External Portal Server Configuration Page

If the **External Portal** is selected, then the parameters in **[Authentication** > **Portal Server > External Portal]** page is described in details as following:

Parameter	**Description**
Portal Server Mode	Choose the **External Portal** here.
Portal Server Name	Assign a literal name to this Portal Server for engineering management. .
URL	Enter the Uniform Resource Locator (URL) of this Portal Server.
AC Name(ACN.CTY.PRO.OPE)	The full name of WLC, in the format of **Host.City.Province.Operator**.This name in WLC, Portal Server and Radius Server must be the same.
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.

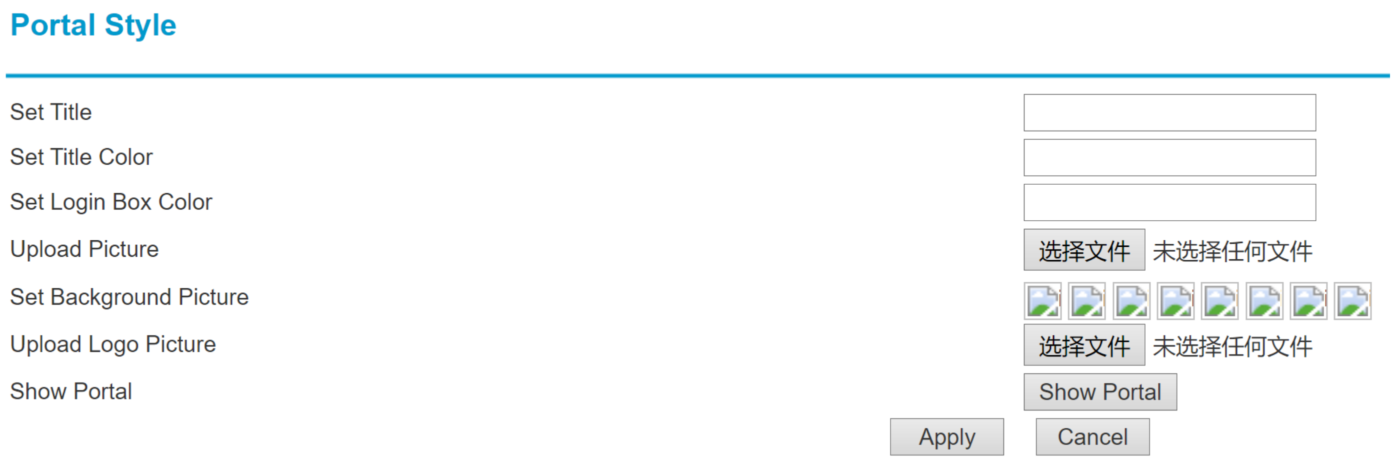
Click the **Add** button to add a new Portal server to the list.

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.

Else if the **Internal Portal** is selected, entering the configuration page as following:



Portal Style

Set Title

Set Title Color

Set Login Box Color

Upload Picture: 选择文件 未选择任何文件

Set Background Picture

Upload Logo Picture: 选择文件 未选择任何文件

Show Portal

Figure 9-7 Internal Portal Server Configuration Page

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

Parameter	**Description**
Set Title	Assign a title name for internal portal web page.
Set Title Color	Set the color for this title of internal portal web page.
Set Login Box Color	Set the color for login frame of internal portal web page.

Parameter	Description
Upload Picture	Uploading the pictures from the directory of local host to WLC.
Set Background Picture	Choose one from the uploaded pictures to set as the background of internal portal web page.
Upload Logo Picture	Uploading the selected log picture from the directory of local host to WLC.
Show Portal	Preview the effect of the internal portal web page.

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

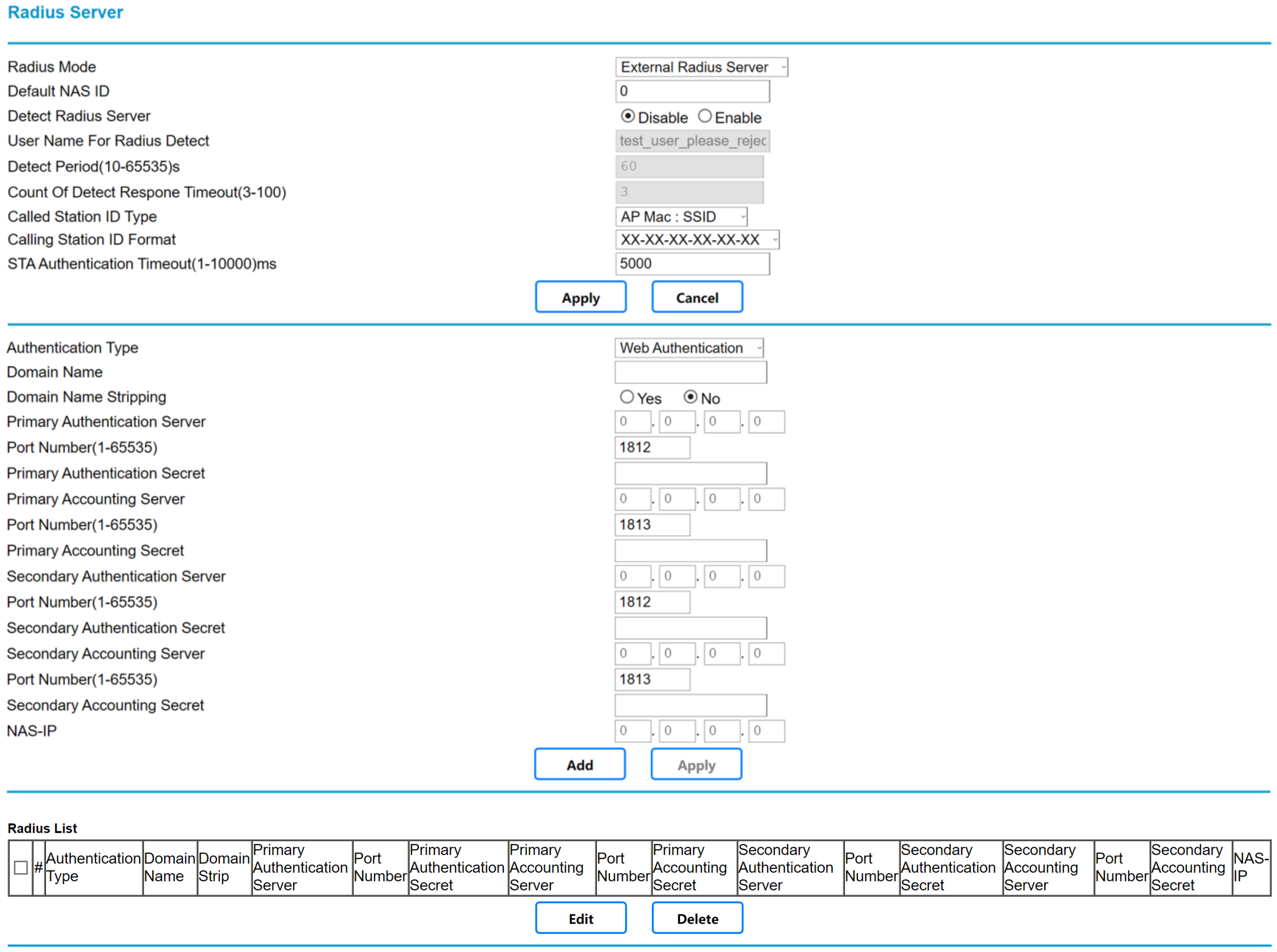
Click the **Cancel** button to discard the changes.

9.5. RADIUS SERVER

The Radius server is the core network element for user authentication behind the Portal server in the Wi-Fi system. Its database contains all registered user information, which is used to match the user name and password forwarded by the Portal server to complete user authentication. At the same time, it is also responsible for user accounting, roaming and policy management.

The Titan series WLC has a built-in simple Radius server, so it can provide either internal Radius service or external Radius service. Therefore, it needs customer pay attention to the selection.

Select **[Authentication** > **Radius Server > External 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

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

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

Figure 9-8 External RADIUS Server Configuration Page

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

Parameter	**Description**
Radius Mode	Select **External Radius Server**.
Default NAS-ID	The full name of WLC, in the format of Network Access Site ID (NAS-ID), which is the **Host.City.Province.Operator**.This name in WLC, Portal Server and Radius Server must be matched, and can be changed according to practical application.
Detect Radius Server	The WLC supports Radius server redundancy. Turn on this switch here to enable WLC to automatically detect the state of Radius server. If the current Radius server malfunctions, it will immediately switch to the backup Radius server.
Username For Radius Detect	WLC needs an username to remotely login the Radius server for detection.
Detect Period (10-65535 s)	The WLC detects the radius server periodically, here to set the time interval of detection.
Count of Detect Response Timeout (3-100)	The WLC determines whether the Radius is OK by receiving the Radius detection response messages. If the WLC does not receive a response from Radius after sending several detection requests, it can be determined that the

Parameter	Description
	Radius server malfunctions. Here to set the threshold of the number of times that the response messages loss.
Called Station ID Type	The valid types of the Called Station ID required by Radius authentication: ▪ **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	The valid formats of the Calling Station ID required by Radius authentication: ▪ **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)	The WLC determines whether the user authentication is successful depending on receiving authentication response. If the authentication response from the Radius server is not received within a specific time, it can be determined failure. Here to set the maximum time threshold for WLC waiting for authentication response.
Authentication Type	Inform Radius server what kind authentication is used for it: ▪ **Web Authentication:** the Radius server verifies the username and password forwarded by the Portal server for authentication. ▪ **WPA/WPA2:** the Radius server is used for WPA/WPA2 to issue a temporary key for authentication when the user client associates to thin AP.
Domain Name	Some Radius needs a full username in the format of ***Username@domai***n. Therefore, the WLC needs to add a domain name to the simple username from Portal server. Here to set the domain name.
Domain Name Stripping	Some Radius needs a simple username without ***@domain*** suffix. Turn on this switch to enable WLC to remove the domain name from the full username forwarded by Portal server.
Primary Authentication Server	The IP address of the primary Radius server.
Port Number (1-65535)	The protocol port number of the primary Radius server.
Primary Authentication Secret	This is the key for WLC to prove that it is a legitimate device to visit primary Radius server. The secret key is an ASCII string.
Primary Accounting Server	The IP address of the primary accounting server.
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 to visit primary Accounting server. The secret key is an ASCII string.

Parameter	Description
Secondary Authentication Server	The IP address of the secondary Radius server.
Port Number (1-65535)	The protocol port number of the secondary Radius server.
Secondary Authentication Secret	This is the key for WLC to prove that it is a legitimate device to visit 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 to visit secondary Accounting server. The secret key is an ASCII string.
NAS-IP	This is a field required in the protocol of the Radius server. In most cases, the NAS device is the WLC, however, if WLC is deployed behind a NAT, the NAS will be NAT. Enter the IP address of WLC northbound port (or NAT public).

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.

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

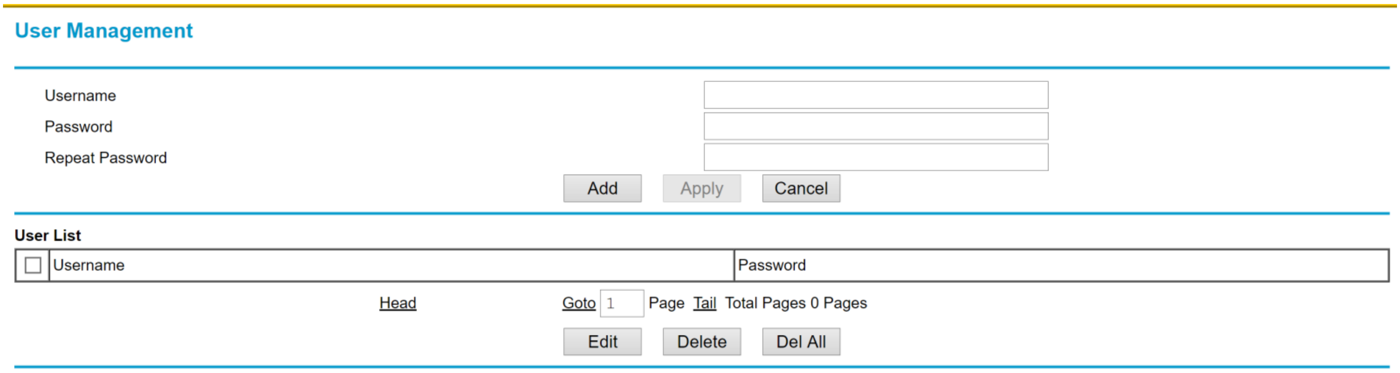


Figure 9-9 Internal RADIUS Server Configuration Page

These parameters in **[Authentication** > **Radius Server > Internal Radius Server]** page is described in details as following

Parameter	Description
UserName	User name for newly registered wireless client.
Password	Set the password for new user of wireless client.
Repeat Password	Repeat above new password for confirmation and prevent from entering a wrong password.

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.

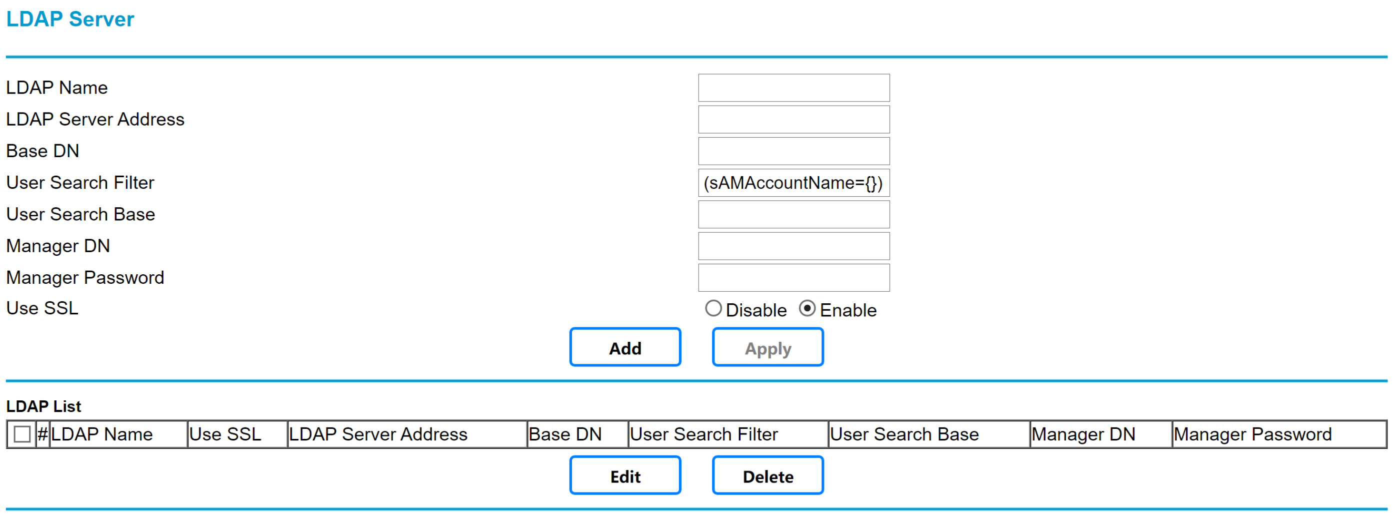
Click the **Edit** button to modify the selected entry.

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

9.6. 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 9-10 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 to this LDAP Server for engineering management.
LDAP Server Address	Fully Qualified Domain Name (FQDN) URL or IP address of LDAP server.
Base DN	The Distinguished Name (DN) is the unique name including the full path of user in LDAP directory tree, which consists of Common Name, Organization Unit, Organization , Country and Domain etc., and will be provided by user before authentication. You will have to supply a full DN like ***cn=admin,dc=example,dc=com***, each object is separated by comma.
User Search Filter	User search filter provides a matching criterion for "User Search Request", its syntax supports such as "**=, ~=, <, <=, >, >=** "and "**!**" operators, and the "*****" operator for sub-string matching. **Note, it is recommended to use the default pattern, the**

Parameter	Description
	customer does not need to change it.
User Search Base	The user search base address defines the starting pointer of the user search path in the LDAP directory tree. A search base is composed of multiple objects (separated by commas), including: ▪ **cn:** common name. ▪ **ou:** organizational unit ▪ **o:** organization ▪ **c:** country ▪ **dc:** domain
Manager DN	The Distinguished Name (DN) of the LDAP server administrator. An example of DN expression is: ***cn=admin,dc=example,dc=com***; the objects are separated by commas.
Manager Password	Password of LDAP server administrator.
Use SSL	Turn on this switch to enable the SSL (Secure Socket Layer) to be applied on the link between WLC and LDAP server for security.
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.

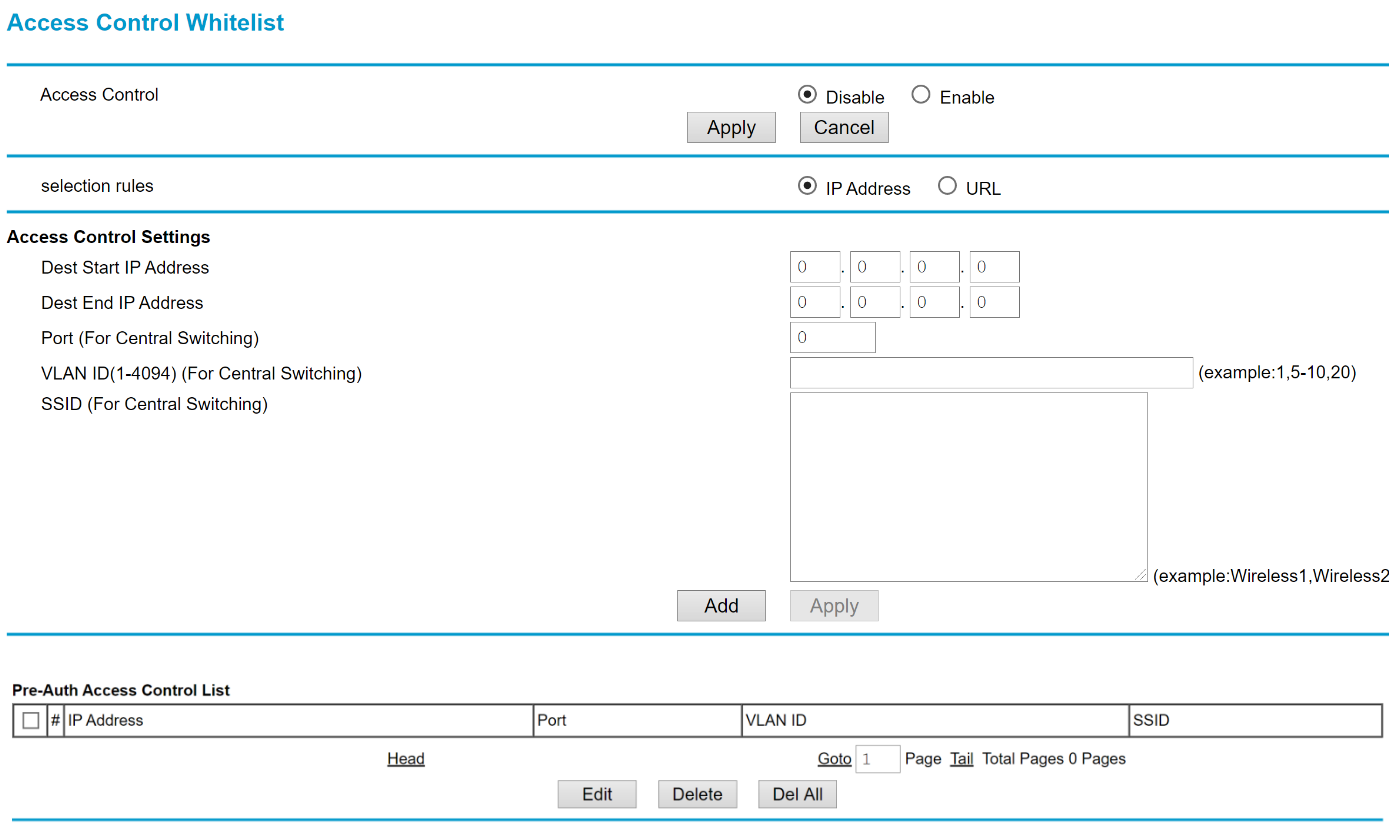
Click the **Edit** button to modify the selected entry.

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

9.7. Access Control Before Authentication

Before authentication, the ***"Access control whitelist"*** is used to create a set of servers to be allowed to access by the user clients without authentication, such as emergency service servers (alarms, medical emergency, fire, etc.); and those servers used for user authentication (Portal, Radius and LDAP servers, etc.). This list will also be downloaded to thin APs for access control under "Local Switching" mode.

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



Access Control Whitelist

Access Control: ● Disable ○ Enable

selection rules: ● IP Address ○ URL

Access Control Settings

Dest Start IP Address: 0 . 0 . 0 . 0

Dest End IP Address: 0 . 0 . 0 . 0

Port (For Central Switching): 0

VLAN ID(1-4094) (For Central Switching): (example:1,5-10,20)

SSID (For Central Switching): (example:Wireless1,Wireless2

Pre-Auth Access Control List

□	#	IP Address	Port	VLAN ID	SSID

Head Goto 1 Page Tail Total Pages 0 Pages

Figure 9-11 Access Control Whitelist Page

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

Parameter	Description
Access Control	Turn on this switch to open the "access control whitelist" to those clients without authentication. **Default is disabling.**
Selection Rules	The target servers opened in the whitelist use either the full domain name URL or IP address.
Access Control Settings	▪ **Dest Start IP Address:** If the '**IP Address**' is selected, here to enter the IP address of the first server in the list to be opened for user clients to access before authentication. ▪ **Dest End IP Address:** If the '**IP Address**' is selected, here to enter the IP address of the last server in the list to be opened for user clients to access before authentication. ▪ **URL:** If the '**URL**' is selected, here to enter the full domain name URL of the server to be opened for user clients to access before authentication. ▪ **Port:** Only this port is opened for user clients to access before authentication. Port number "0" stands for no port limitation. ▪ **VLAN ID:** Enter a group of VLAN IDs here separated with commas, which are opened for the user clients to access the servers in the whitelist before authentication. ▪ **SSID:** Import the SSIDs from the window in which all configured VAP

Parameter	Description
	displayed with their SSID, only the user clients from these selected VAPs are allowed to access servers in whitelist before authentication.

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.

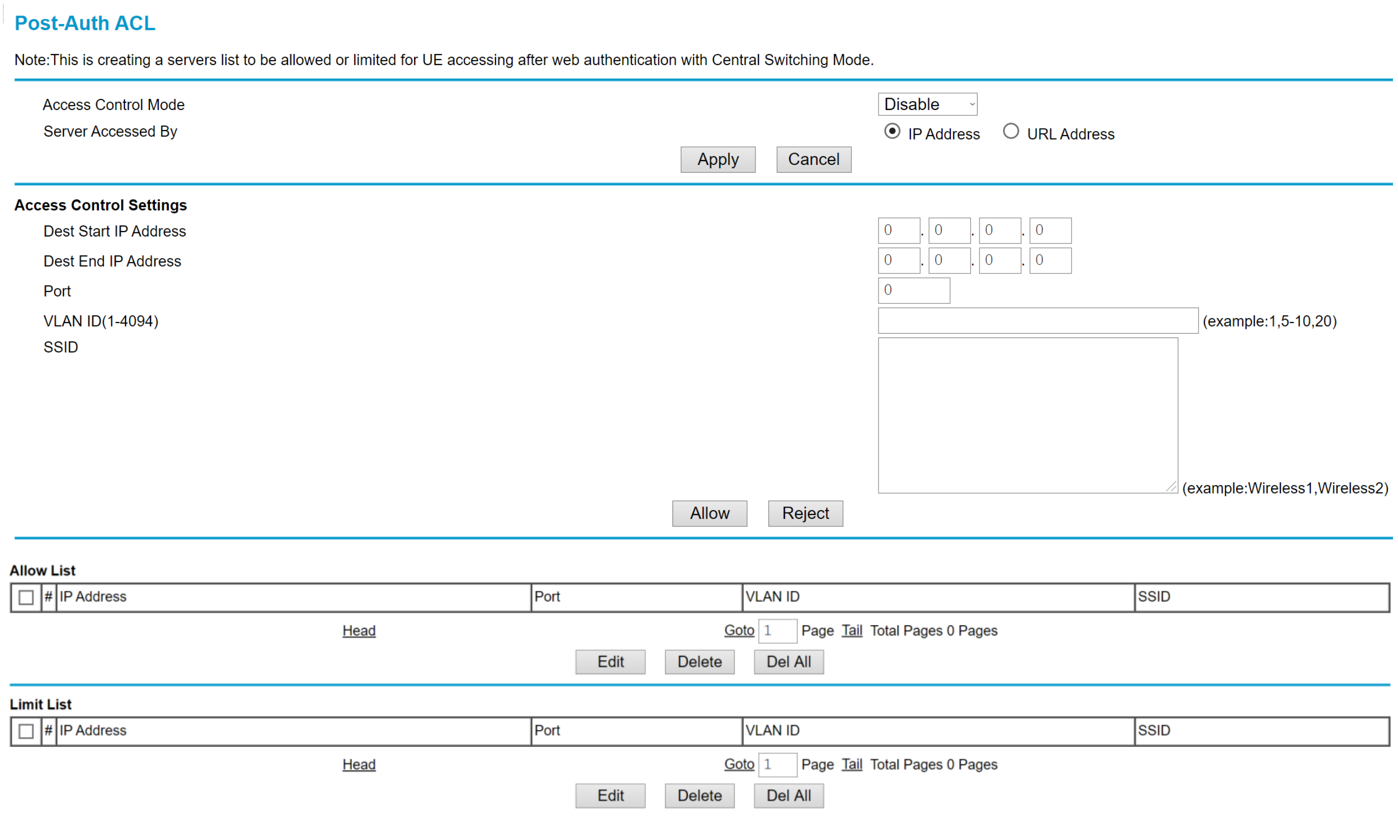
Click the **Delete** button to remove the selected entry.

Click the **Del All** button to remove all the entries from the configuration.

9.8. Access Control After Authentication

After authentication, the "**Access Control Black and White List**" in WLC is used to create a set of target servers to be under control for user clients to access: the servers in white list are allowed to be access; the servers in blacklist will be prohibited to access. However, WLC can only perform either the white list or blacklist checking, not both, depending on customer setting.This function is only applicable in the "Central Switching" mode.

Select **[Authentication** > **Post-Auth ACL]** in the menu to enter the configuration page as following:



Post-Auth ACL

Note:This is creating a servers list to be allowed or limited for UE accessing after web authentication with Central Switching Mode.

Access Control Mode: Disable

Server Accessed By: ● IP Address ○ URL Address

Access Control Settings

Dest Start IP Address: 0 . 0 . 0 . 0

Dest End IP Address: 0 . 0 . 0 . 0

Port: 0

VLAN ID(1-4094): (example:1,5-10,20)

SSID: (example:Wireless1,Wireless2)

Allow List

□	#	IP Address	Port	VLAN ID	SSID

Head Goto 1 Page Tail Total Pages 0 Pages

Limit List

□	#	IP Address	Port	VLAN ID	SSID

Head Goto 1 Page Tail Total Pages 0 Pages

Figure 9-12 Post-Auth ACL Configuration Page

These parameters in **[Authentication** > **Post-Auth ACL]** page is described in details as following:

Parameter	Description
Access Control Mode	Here to set the mode which WLC will select for user access control after authentication: ▪ **Disable:** No access control for all user clients after authentication. ▪ **Allow List:** WLC only performs whitelist checking for user clients after authentication. ▪ **Limit List:** WLC only performs blacklist checking for user clients after authentication..
Server Accessed By	The target servers in this access control list use either the full domain name URL or IP address.
	▪ **Dest Start IP Address:** If the '**Accessed by IP Address**' is selected, here to enter the IP address of the first server under control for user clients to access after authentication. ▪ **Dest End IP Address:** If the '**Accessed by IP Address**' is selected, here to enter the IP address of the last server under control for user clients to access after authentication. ▪ **URL:** If the '**Accessed by URL**' is selected, here to enter the full domain URL of the server under control for user clients to access after authentication. ▪ **Port:** Only this port is under control for user clients to access after authentication. Port number "0" stands for no port limitation. ▪ **VLAN ID:** Enter a group of VLAN IDs here separated with commas, which are under control for the user clients to access after authentication. ▪ **SSID:** Import the SSIDs from the window in which all configured VAP displayed with their SSID, only the user clients from these selected VAPs are controlled to access servers in list after authentication.
<Allow>	Click this button to append above configuration to Whitelist.
<Reject>	Click this button to append above configuration to Blacklist.

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.

Click the **Del All** button to remove all the entries from the configuration.

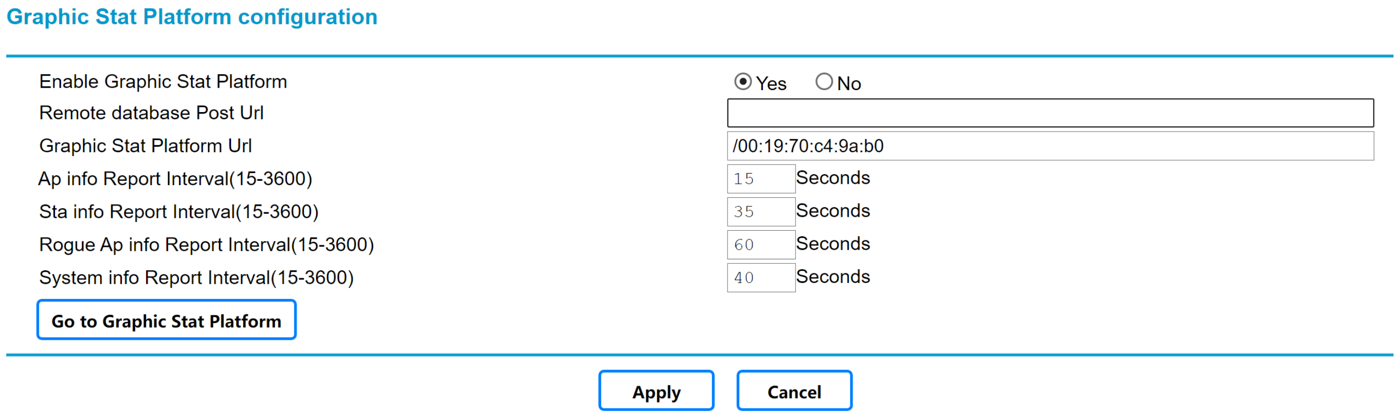
Chapter 10. SYSTEM MANAGEMENT

System management focuses on the maintenance and management of WLC, as well as hardware configuration and firmware upgrading.

10.1. GRAPHIC STAT PLATFORM

Titan series WLC supports a third-party remote graphic statistics platform. Therefore, the WLC will periodically use the ***Rest API*** protocol to send the statistics and state information of both the user clients and the thin APs to the remote statistics platform for displaying in Graphical mode.

Select **[System Management** > **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 10-1 Graphic Statistics Platform Configuration Page

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

Parameter	Description
Enable Graphic Stat Platform	Turn on this switch to enable WLC to periodically send the statistics and state information of both the user clients and the thin APs to the remote statistics platform.
Remote Data Base Post URL	Enter the URL address of the remote database (usually same as the graphical statistics platform).
Graphic Stat Platform URL	Enter the URL address of the remote graphical platform.
AP Info Report interval (15-3600)	The time interval for WLC to report AP information to the remote graphic platform.
STA Info Report interval (15-3600)	The time interval for WLC to report user clients information to the remote statistics platform.
Rogue AP Info Report interval (15-3600)	The time interval for WLC to report Rogue AP information to the remote statistics platform.
System Info Report interval (15-3600)	The time interval for WLC to report system information to the remote graphic platform.

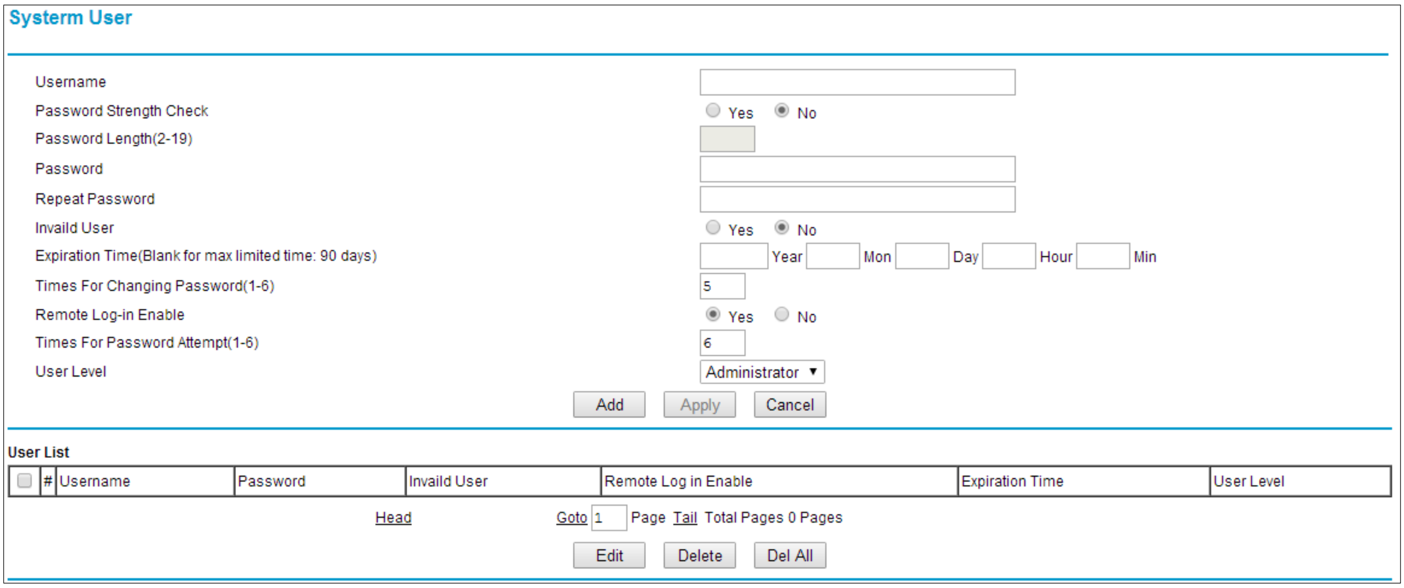
Click the **Apply** button to accept the changes.

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

10.2. SYSTEM USER

The WLC manages system users by hierarchical according to the permissions. The system administrator can create user accounts in different levels, and assign passwords and life cycles to them, and authorize them to use the system commands.

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



Systerm User

Username	
Password Strength Check	○ Yes ● No
Password Length(2-19)	
Password	
Repeat Password	
Invaild User	○ Yes ● No
Expiration Time(Blank for max limited time: 90 days)	Year Mon Day Hour Min
Times For Changing Password(1-6)	5
Remote Log-in Enable	● Yes ○ No
Times For Password Attempt(1-6)	6
User Level	Administrator ▼

User List

□	#	Username	Password	Invaild User	Remote Log in Enable	Expiration Time	User Level

Figure 10-1 System User Page

These parameters in **[System Management** > **System User]** page is described in details as followin:

Parameter	Description
User Name	Enter the username for new account.
Password Strength Check	Turn on this switch to enable WLC to avoid the weak password being selected for this user account.
Password Length	Set the length of password for this user account.
Password	Enter the password for this new user account.
Repeat Password	Enter the new password again for confirmation to avoid the creation of an incorrect password.
Invalid User	This is a flag to identify the invalid user. The user created long time ago but not in duty now, can be marked with this flag.
Expiration Time	Set the life cycle for the user account. By default, the max life cycle time is 90 days.
Times for Changing Password	Maximum number of times allowed to change user password.

Parameter	Description
Remote Login Enable	Turn on this switch to enable the user to remotely access to WLC, such as by Telnet, SSH and Web. **Default is Yes**.
Times for Password Attempt	Maximum number of times allowing the user to enter the incorrect password.
User Level	Users can be classified to the following three levels according to their permissions: ▪ **Administrator:** The highest privilege user who can fully control the entire system. ▪ **User (Level 1):** The user who has all permissions except rebooting the system. ▪ **User (Level 2**): The user who has the right of only reviewing the system information and help information.

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.

Click the **Del All** button to remove all the entries from the configuration.

10.3. **1+1 BACKUP**

The WLC provides a 1 + 1 dual-machine backup scheme. When the master WLC is in operating, the another WLC is in the standby state. The master and backup WLCs synchronize their configuration information, as well as the user clients and thin APs information each other through the heartbeat messages over the dedicated heartbeat link. Once the standby WLC does not receive a heartbeat message from the master one during a specific period of time, it will immediately switch to be the master WLC; whereas when the former master WLC returns to normal operation, the latter master WLC will back to standby state again. See Figure 10-3 for details.

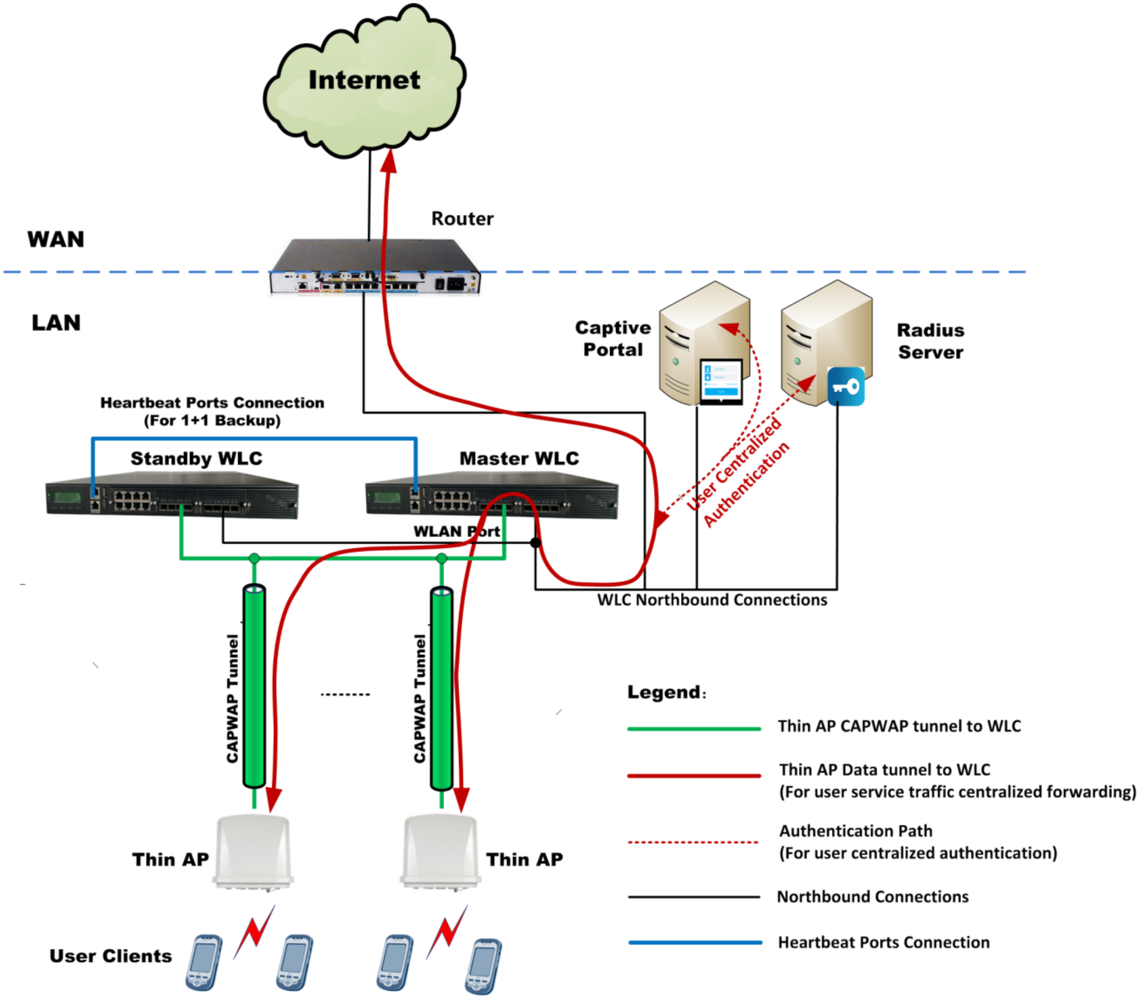
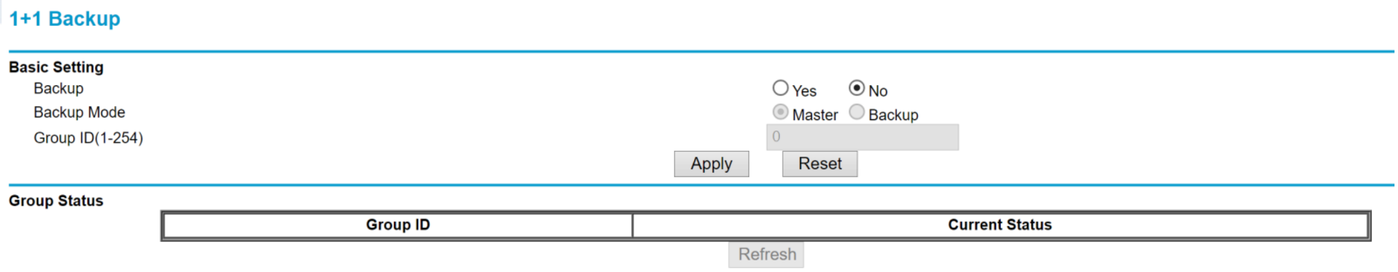

Internet
Router
WAN
LAN
Captive Portal
Radius Server
Heartbeat Ports Connection (For 1+1 Backup)
Standby WLC
Master WLC
WLAN Port
User Centralized Authentication
WLC Northbound Connections
CAPWAP Tunnel
CAPWAP Tunnel
Thin AP
Thin AP
User Clients
Legend:
Thin AP CAPWAP tunnel to WLC
Thin AP Data tunnel to WLC (For user service traffic centralized forwarding)
Authentication Path (For user centralized authentication)
Northbound Connections
Heartbeat Ports Connection

Figure 10-3 Titan WLC 1+1 Backup Architecture

Select **[System Management** > **1+1 Backup]** in the menu to enter the configuration page as following:


1+1 Backup

Basic Setting

Backup ○ Yes ● No

Backup Mode ● Master ○ Backup

Group ID(1-254) 0

Apply Reset

Group Status

Group ID	Current Status

Refresh

Figure 10-4 WLC 1+1 Backup Configuration Page

These parameters in **[System Management** > **1+1 Backup]** page is described in details as following:

Parameter	Description
Backup	Turn on this switch to enable WLC to work in 1+1 backup mode. **Default is No.**
Backup Mode	Here to set current WLC to run either in ***Master*** mode or ***Standby*** mode.
Group ID(1-254)	Only the Master and Standby WLCs in the same group can be backup each other, so that it is necessary to assign a same group ID to the master and standby WLC.
Group Status	Check the states update of both master and standby WLCs in the same group by clicking <**Refresh**> button.

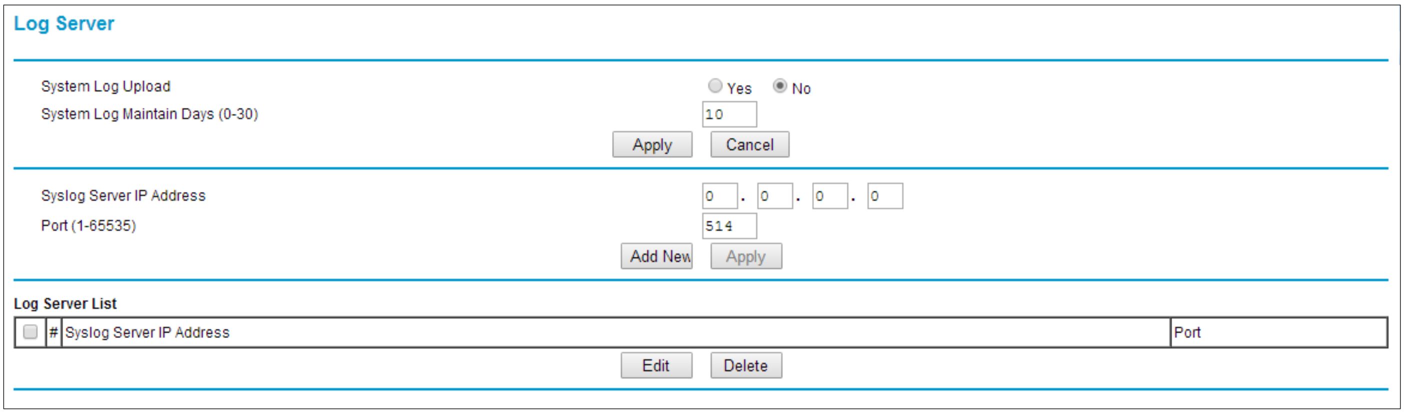
Click the **Apply** button to accept the changes.

Click the **Reset** button to clear current setting.

10.4. LOG SERVER

System log is an important tool for system maintenance. Linux provides ***syslogd*** daemon to record system operation and debugging information for engineers to check. The ***syslogd*** can be running in a remote host called as **Log Server** to receive the log information from the WLC through socket communication.

Select **[System Management** > **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 10-5 Log Server Configuration Page

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

Parameter	Description
System Log Upload	Turn on this switch to enable WLC to automatically send log information to the log server. **Default is No**.
System Log Maintain Days	How long (in days) the system logs will be reserved in the log server.
Syslog Server IP Address	Enter the IP address of log server on which the ***syslogd*** daemon is running.
Port	Enter the port number of ***syslogd*** daemon. ***Default is 514***.

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

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

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

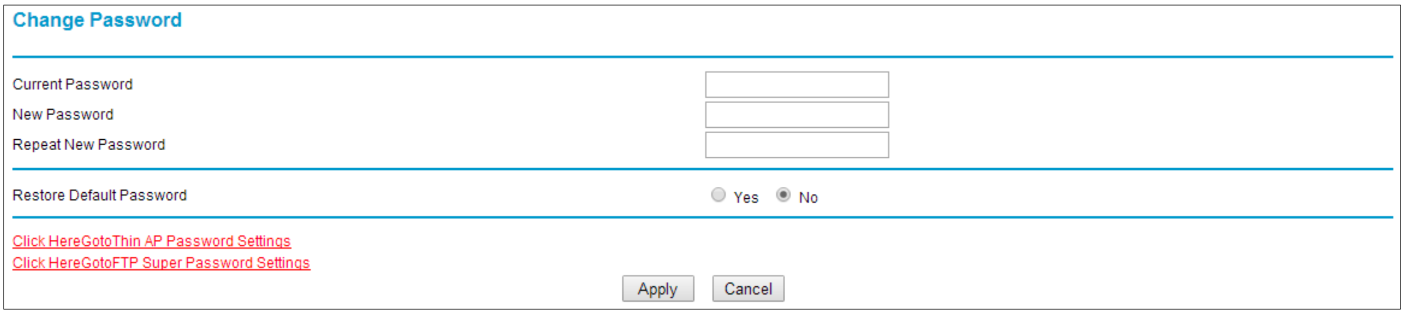
Click the **Edit** button to modify the selected entry.

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

10.5. CHANGE PASSWORD

The WLC has a default user ***admin***, whose default password is ***password***. In actual deployment, this default password obviously must be changed by the customer. This section provides a method for the customer to change the password of the user admin.

Select **[System Management** > **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 10-6 Change Password Page

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

Parameter	Description
Current Password	Entering the current password of user admin.
New Password	Entering the new password for user admin.
Repeat New Password	Entering the new password again for confirmation to avoid mistake.
Restore Default Password	Restore the password which is set in factory.
Thin AP Password Setting	This is a hyperlink directed to the thin AP password setting page.
FTP Super Password Setting	WLC has a built-in FTP server for system maintenance and management. This is a hyperlink directed to this FTP server super password setting page.

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

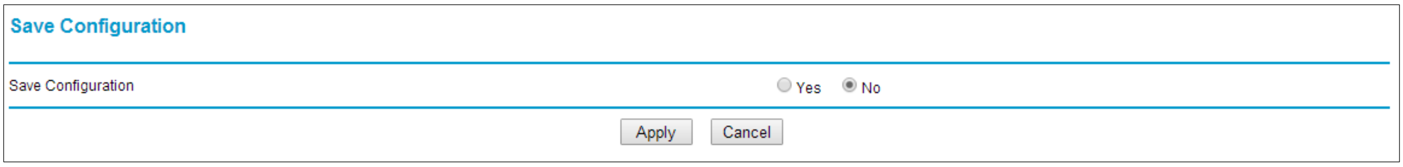
Click the **Cancel** button to discard the changes.

10.6. SAVE CONFIGURATION

The profiles modification made by the customer to the WLC will be lost after it shut down. Therefore, if the modification is hoped to take effect permanently, it is necessary to perform "**Save Configuration**" to dump the current modification from the memory to the non-volatile storage device (such as a hard disk, etc.).

.

Select **[System Management** > **Save Configuration]** in the menu to enter the configuration page as following:



Save Configuration

Save Configuration ○ Yes ● No

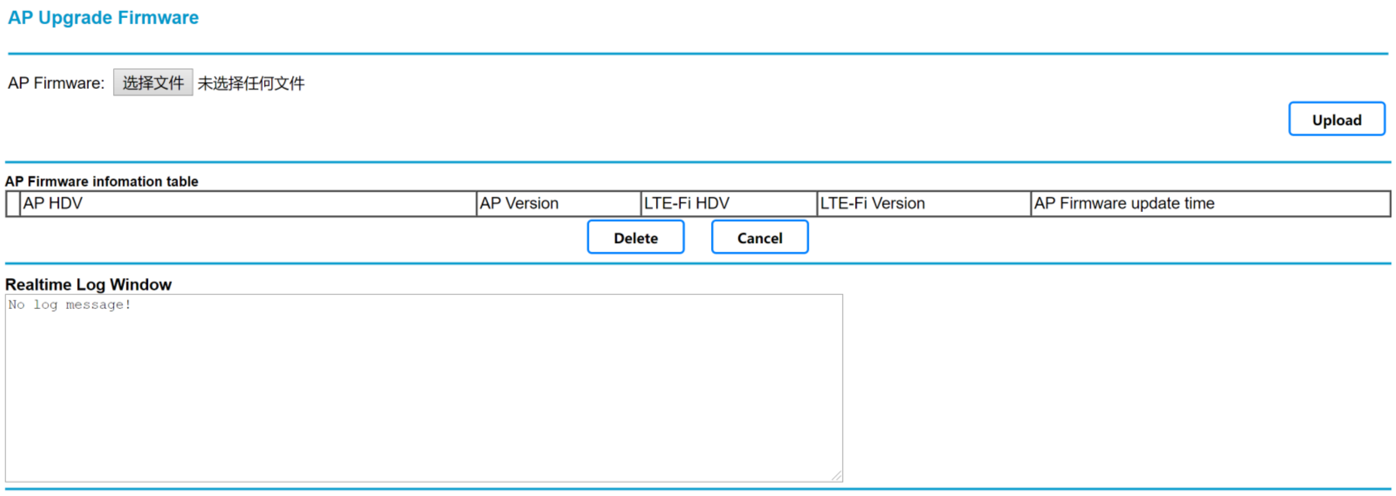
Figure 10-7 Save Configuration Page

Select **Yes** and then click the <**Apply**> button to dump current configuration to the non-volatile storage device of WLC from memory.

10.7. UPGRADE FIRMWARE

If the WLC obtains a new version of firmware from the vendor, it can be upgraded through the method provided in this section.

Select **[System Management** > **Upgrade Firmware]** 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

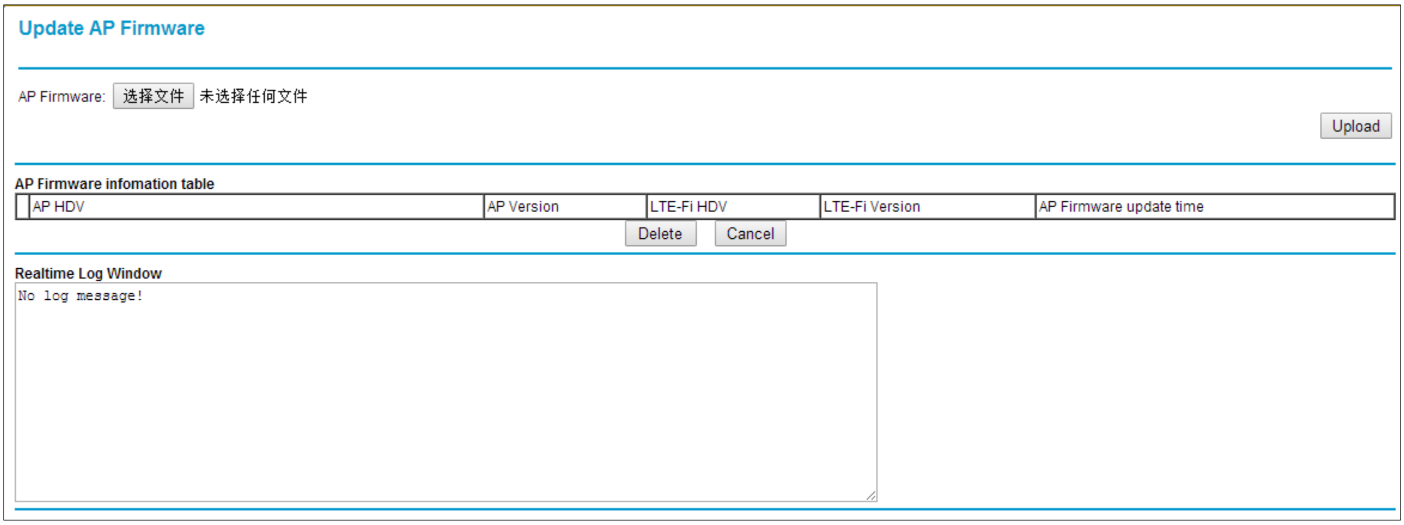
```
No log message!
```

Figure 10-8 WLC Upgrade Firmware Page

Select the new firmware in the directory of local host by clicking <**Browse**>, and then click <**Upload**> button to start the upgrading.

10.8. AP UPGRADE FIRMWARE

In a Wi-Fi system with WLC, the thin APs can be automatically upgraded centrally if the new version firmware of thin AP is on WLC. Select **[System Management** > **AP FW Upgrade]** in the menu to enter the configuration page as following:



Update AP 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 10-9 Centrally upgrade thin AP Firmware Page

Click <**Browse**> button to select the new version firmware of thin AP from local host directory, then click <**Upload**> button to transport the new 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**

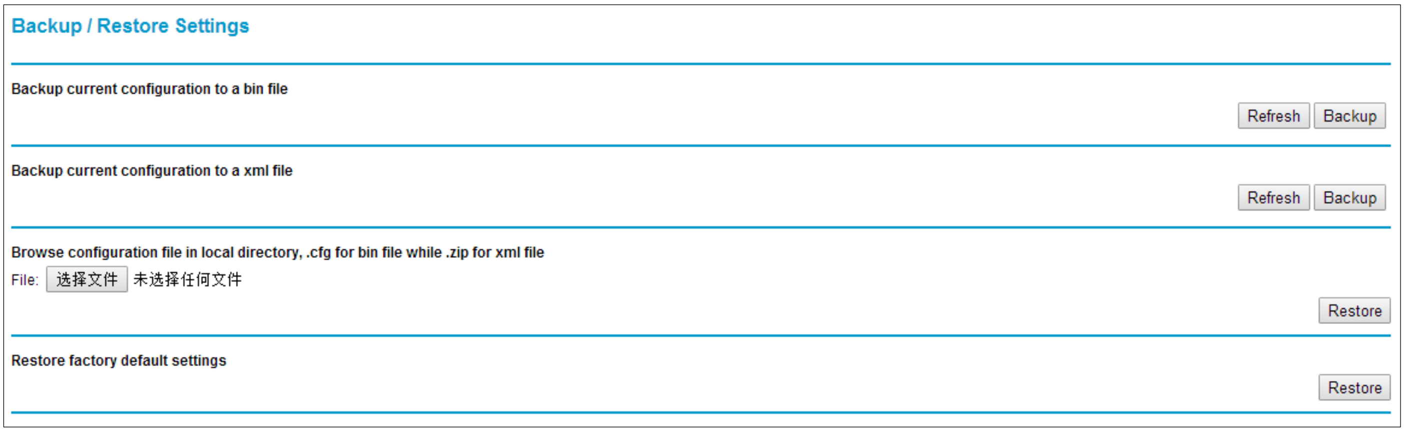
Click the **Delete** button to remove the selected entry.

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

10.9. BACKUP/RESTORE

The overall configuration of the WLC can be saved as files in binary format or XML format. When a new installation of WLC is completed, a quick way to configure WLC is directly importing the backup configuration file into WLC.

Select **[System Management** > **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 10-10 Backup / Restore Page

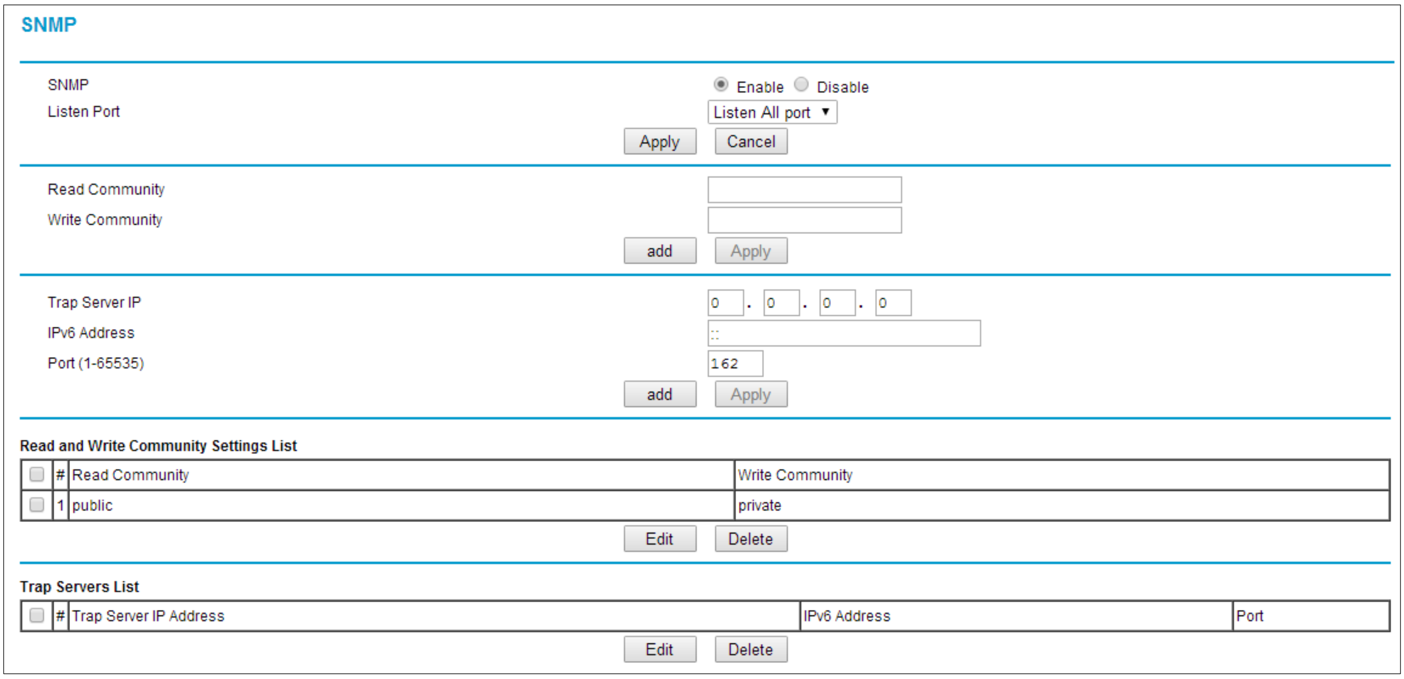
These parameters in **[System Management** > **Backup/Restore]** page is described in details as following:

Parameter	Description
Backup Current Configuration to A Bin File	Save the current configuration to a binary file and click the <**Backup**> button to export. Sometimes you need to click the <**Refresh**> button to update the state of web browser.
Backup Current Configuration to A XML File	Save the current configuration to a XML file and click the <**Backup**> button to export. Sometimes you need to click the <**Refresh**> button to update the state of web browser.
Restore Configuration	Select the backup file from the directory of the host (***.cfg*** is a binary file; ***.zip*** is an XML file). Click the <**Restore**> button to import it into the WLC to restore the configuration.
Restore Factory Default Setting	Recover the configuration of WLC in factory setting. Click the <**Restore**> button to start.

10.10. **SNMP**

If the WLC is deployed in a manageable network, all network elements are managed by the NMS or EMS. In such case, the WLC is undoubtedly a managed device. Therefore, it is necessary to enable the SNMP (Simple Network Management Protocol) function in WLC to make it to be manageable. The WLC has the built-in management MIB base, which contains the network management nodes required by the NMS for SNMP polling and trapping.

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



SNMP

SNMP ● Enable ○ Disable

Listen Port: Listen All port ▼

Read Community

Write Community

Trap Server IP: 0 . 0 . 0 . 0

IPv6 Address: ::

Port (1-65535): 162

Read and Write Community Settings List

□	#	Read Community	Write Community
□	1	public	private

Trap Servers List

□	#	Trap Server IP Address	IPv6 Address	Port

Figure 10-11 SNMP Configuration Page

These parameters in **[System Management** > **SNMP]** page is described in details as following:

Parameter	Description
SNMP	Turn on this switch to enable the SNMP function for WLC. **Default is Enable.**
Listen Port	Set the port for SNMP agent in WLC to listen the EMS polling.
Read Community	SNMP agent community refers to the relationship of EMS and SNMP Agent, the read and writes permissions are used for them to verify each other. Here to set the SNMP agent community read permission password. Default is "**public**". Click the <**Add**> button to add it to the list.
Write Community	SNMP agent community refers to the relationship of EMS and SNMP Agent, the read and writes permissions are used for them to verify each other. Here to set the SNMP agent community write permission password. Default is "**private**". Click the <**Add**> button to add it to the list.
Trap Server IP	Trap server receives alarms from WLC, here to enter its IP address. It is usually the IP address of the EMS.
IPv6 Address	If WLC is deployed in an IPv6 network, here to enter the IPv6 address of EMS.
Port	Enter the UDP port number of trap server. Default is **162**.

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.

10.11. DPI

DPI stands for "Deep Packet Inspection", it is used for user service statistics and user behavior analysis by inspecting layer 4 and above protocols in data packets. Due to it disassembles too many layers of protocols in a packet, it consumes too much resources to degrade system performance.

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

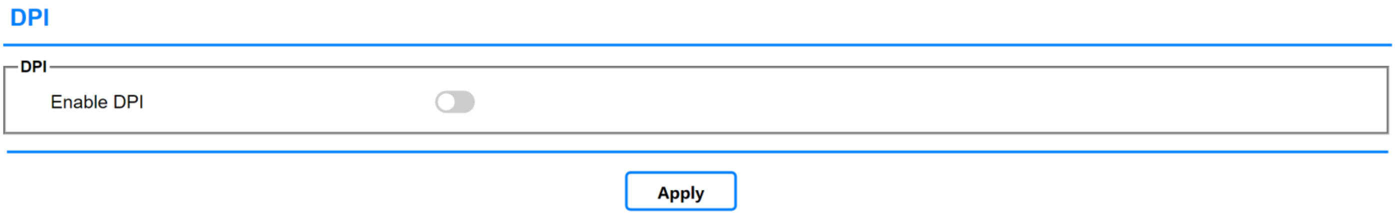


Figure 10-12 Deep Packet Inspect Configuration Page

These parameters in **[System Management** > **DPI]** page is described in details as following:

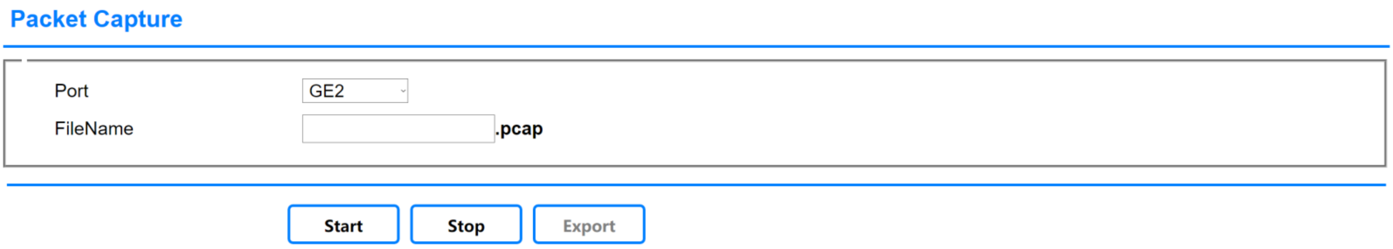
Parameter	Description
Enable DPI	Turn on this switch to enable DPI function for WLC. The DPI results will be graphically displayed in [**Statistics > DPI**]. Default state is **disable**.

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

10.12. PACKET CAPTURE

"**Packet Capture**" is a maintenance tool for the Wi-Fi system. The administrator uses it to inspect the system operation and locate the faults by analyzing the ingress and egress packets. The captured packets can be exported and saved in a special file format, and then viewed with ***Wireshark*** tool.

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



Packet Capture

Port: GE2

FileName: .pcap

Figure 10-13 Packet Capture Page

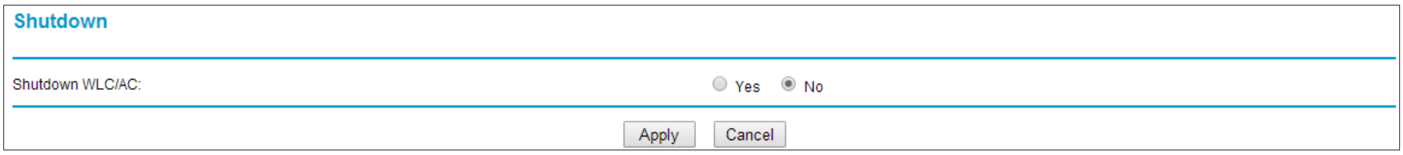
These parameters in **[System Management** > **Packet Capture]** page is described in details as following:

Parameter	Description
Port	Select 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 then 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 active only after the <**Stop**> button clicked.

10.13. Shutdown

The WLC can be shut down on this page.

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



Shutdown

Shutdown WLC/AC: ○ Yes ● No

Figure 10-14 WLC Shutdown Page

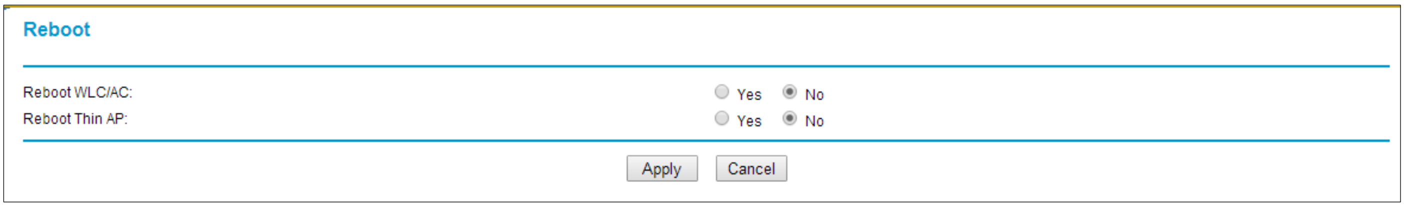
Select **Yes** and click the **Apply** button to shut down the WLC.

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

10.14. Reboot

During system maintenance, sometimes the WLC or thin APs need to be restarted. For example, after the configuration is modified, you need to restart WLC to make the modifications take effect (such as port classification).

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



Reboot

Reboot WLC/AC: ○ Yes ● No

Reboot Thin AP: ○ Yes ● No

Figure 10-15 Reboot Page

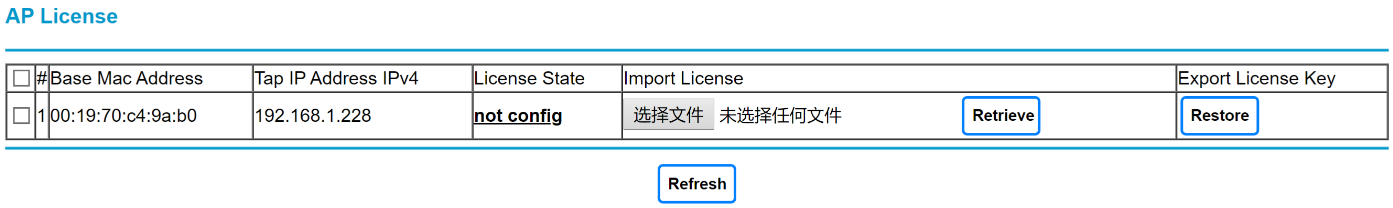
Check either the **Reboot WLC** or **Reboot Thin AP** button to be **Yes**, and click the **Apply** button to reboot either the WLC or the TAP.

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

10.15. License Import

The WLC uses the AP license to control the capacity of the thin APs in the Wi-Fi system. After the WLC is installed on site, the AP license has to be imported to allow the thin APs in the network to access system. Otherwise, except the default few thin APs, most thin APs cannot go online. The AP license is created and delivered by the WLC vendor.

Select **[System Management** > **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

Refresh

Figure 10-16 AP License Import Page

Click the <**Browse** > button to select the AP License in the directory of local host, then upload it into WLC. Click <**Import**> button to copy the license to WLC. Click <**Export**> to save the license in WLC to local host for backup.

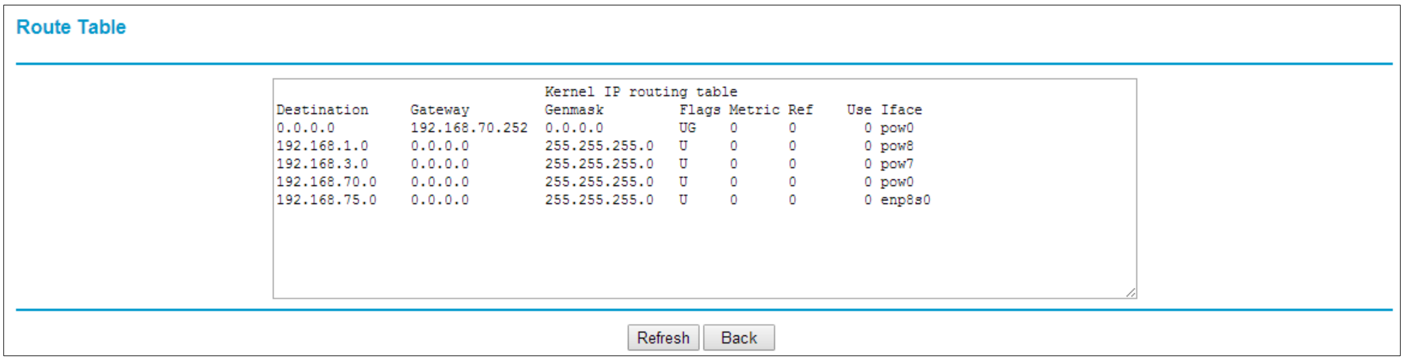
Click the <**Refresh**> button to update the AP License state.

Chapter 11. STATISTICS

In order to meet with the management requirement, the WLC provides a wealth of statistical information, such as WLC configuration information, network information, thin APs information, and user clients information for view and analyze.

11.1. ROUTE TABLE

Static routing and dynamic routing are configured in [**Network Setup**], and the configuration can be displayed here. Select **[Statistics** > **Route Table]** in the menu to enter the following page:



```
                              Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.70.252  0.0.0.0         UG    0      0        0 pow0
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 pow8
192.168.3.0     0.0.0.0         255.255.255.0   U     0      0        0 pow7
192.168.70.0    0.0.0.0         255.255.255.0   U     0      0        0 pow0
192.168.75.0    0.0.0.0         255.255.255.0   U     0      0        0 enp8s0
```

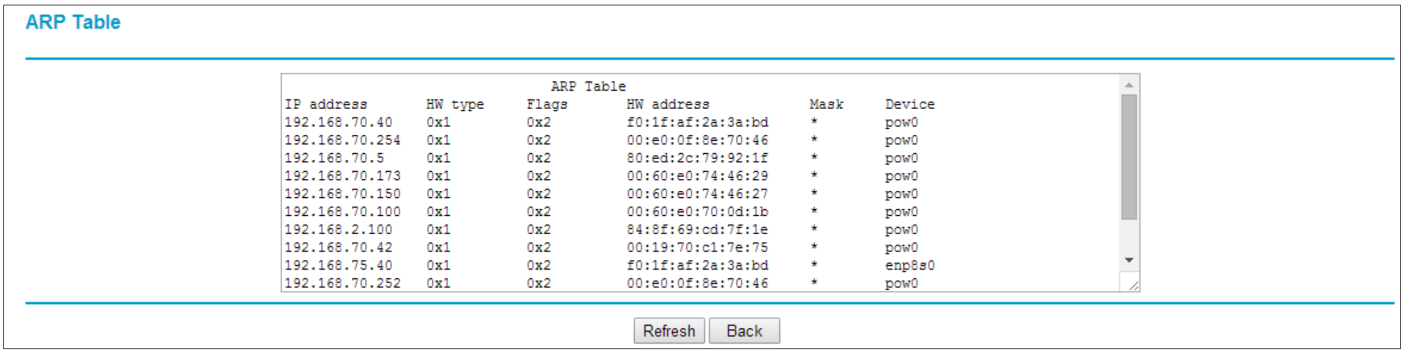
Figure 11-1 Route Table Page

Click the **Refresh** button to update the information displayed on this page.

Click the **Back** button to return to the previous page.

11.2. ARP TABLE

The WLC discovers network neighbors through ARP packets. Select **[Statistics** > **ARP Table]** in the menu to enter the following page:



```
                           ARP Table
IP address       HW type     Flags       HW address            Mask     Device
192.168.70.40    0x1         0x2         f0:1f:af:2a:3a:bd     *        pow0
192.168.70.254   0x1         0x2         00:e0:0f:8e:70:46     *        pow0
192.168.70.5     0x1         0x2         80:ed:2c:79:92:1f     *        pow0
192.168.70.173   0x1         0x2         00:60:e0:74:46:29     *        pow0
192.168.70.150   0x1         0x2         00:60:e0:74:46:27     *        pow0
192.168.70.100   0x1         0x2         00:60:e0:70:0d:1b     *        pow0
192.168.2.100    0x1         0x2         84:8f:69:cd:7f:1e     *        pow0
192.168.70.42    0x1         0x2         00:19:70:c1:7e:75     *        pow0
192.168.75.40    0x1         0x2         f0:1f:af:2a:3a:bd     *        enp8s0
192.168.70.252   0x1         0x2         00:e0:0f:8e:70:46     *        pow0
```

Figure 11-2 ARP Table Page

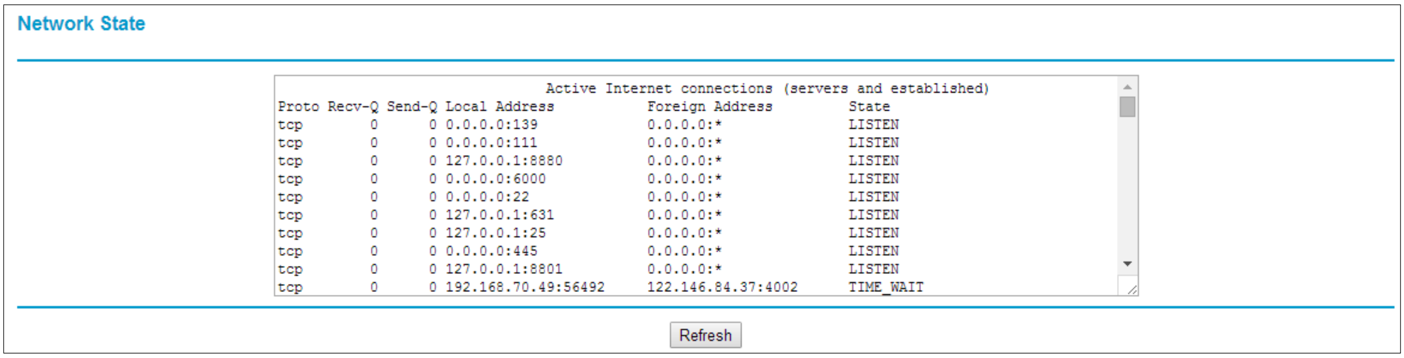
Click the **Refresh** button to update the information displayed on this page.

Click the **Back** button to return to the previous page.

11.3. Network State

Displaying the link status of the connected ports of the WLC, including protocol, receiving/transmitting queue, IP address information, and status information..

Select **[Statistics** > **Network State]** in the menu to enter the following page:



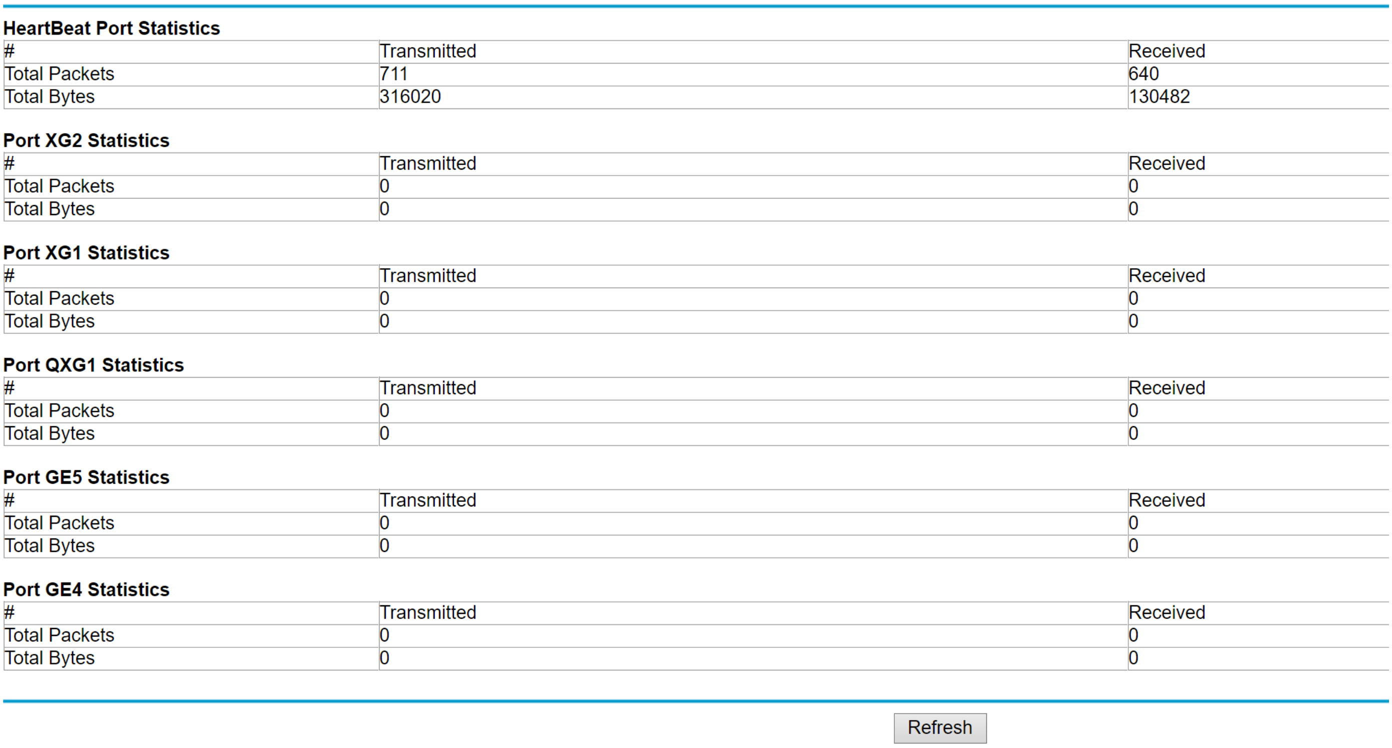
```
                                Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:8880          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:6000            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:8801          0.0.0.0:*               LISTEN
tcp        0      0 192.168.70.49:56492     122.146.84.37:4002      TIME_WAIT
```

Figure 11-3 Network State Page

Click the **Refresh** button to update the information displayed on this page.

11.4. Port Statistics

Displaying the statistical information of packets receiving and transmitting on all physical ports classified as the type of "WLC" in the **[Network Set > Port Classification]** menu. Select **[Statistics** > **Port State]** in the menu to enter the following page:



HeartBeat Port Statistics

#	Transmitted	Received
Total Packets	711	640
Total Bytes	316020	130482

Port XG2 Statistics

#	Transmitted	Received
Total Packets	0	0
Total Bytes	0	0

Port XG1 Statistics

#	Transmitted	Received
Total Packets	0	0
Total Bytes	0	0

Port QXG1 Statistics

#	Transmitted	Received
Total Packets	0	0
Total Bytes	0	0

Port GE5 Statistics

#	Transmitted	Received
Total Packets	0	0
Total Bytes	0	0

Port GE4 Statistics

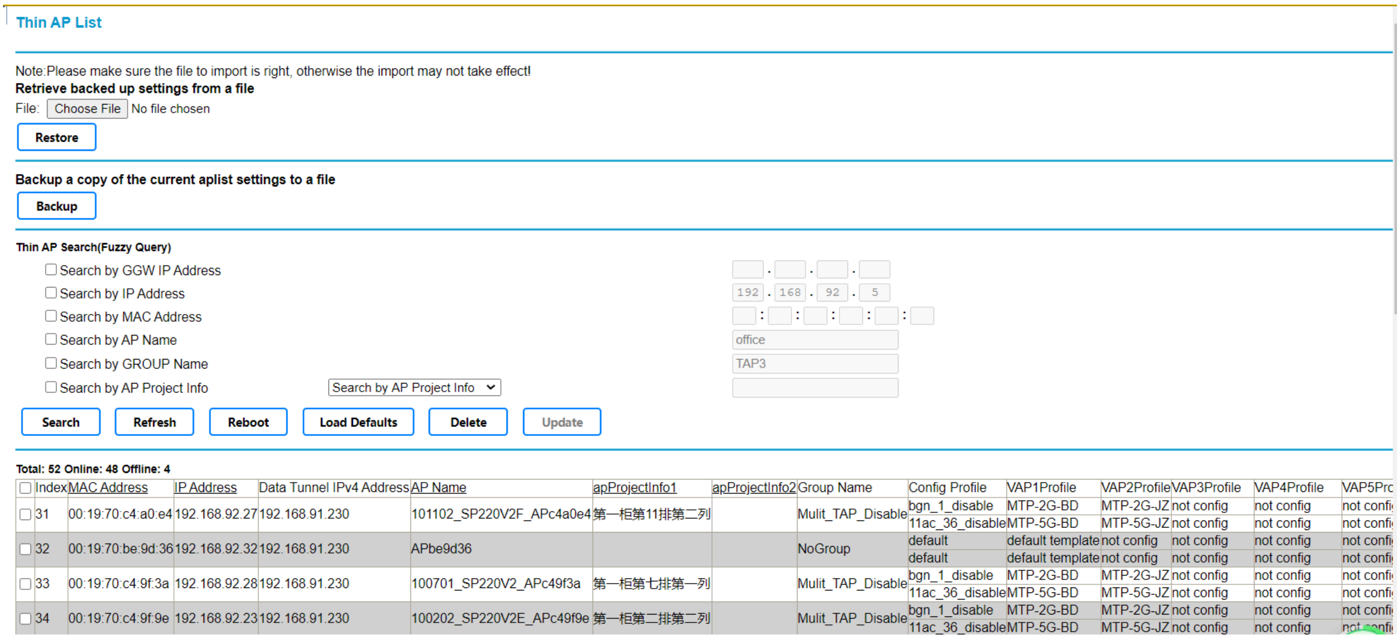
#	Transmitted	Received
Total Packets	0	0
Total Bytes	0	0

Figure 11-4 Port Packets Transceiver Statistics Page

11.5. THIN AP LIST

All thin APs that have ever accessed the WLC, regardless of they are currently online or offline, will be added to the thin AP list for displaying.

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



Thin AP List

Note:Please make sure the file to import is right, otherwise the import may not take effect!

Retrieve backed up settings from a file

File: Choose File No file chosen

Restore

Backup a copy of the current aplist settings to a file

Backup

Thin AP Search(Fuzzy Query)

- □ Search by GGW IP Address . . .
- □ Search by IP Address 192 . 168 . 92 . 5
- □ Search by MAC Address : : : : :
- □ Search by AP Name office
- □ Search by GROUP Name TAP3
- □ Search by AP Project Info [Search by AP Project Info ▾]

Search | Refresh | Reboot | Load Defaults | Delete | Update

Total: 52 Online: 48 Offline: 4

□	Index	MAC Address	IP Address	Data Tunnel IPv4 Address	AP Name	apProjectInfo1	apProjectInfo2	Group Name	Config Profile	VAP1Profile	VAP2Profile	VAP3Profile	VAP4Profile	VAP5Pro
□	31	00:19:70:c4:a0:e4	192.168.92.27	192.168.91.230	101102_SP220V2F_APc4a0e4	第一柜第11排第二列		Mulit_TAP_Disable	bgn_1_disable 11ac_36_disable	MTP-2G-BD MTP-5G-BD	MTP-2G-JZ MTP-5G-JZ	not config not config	not config not config	not confi not confi
□	32	00:19:70:be:9d:36	192.168.92.32	192.168.91.230	APbe9d36			NoGroup	default default	default template default template	not config not config	not config not config	not config not config	not confi not confi
□	33	00:19:70:c4:9f:3a	192.168.92.28	192.168.91.230	100701_SP220V2_APc49f3a	第一柜第七排第一列		Mulit_TAP_Disable	bgn_1_disable 11ac_36_disable	MTP-2G-BD MTP-5G-BD	MTP-2G-JZ MTP-5G-JZ	not config not config	not config not config	not confi not confi
□	34	00:19:70:c4:9f:9e	192.168.92.23	192.168.91.230	100202_SP220V2E_APc49f9e	第一柜第二排第二列		Mulit_TAP_Disable	bgn_1_disable 11ac_36_disable	MTP-2G-BD MTP-5G-BD	MTP-2G-JZ MTP-5G-JZ	not config not config	not config not config	not confi not confi

Figure 11-5 Thin AP List Page

Click the **Restore** button to import the backup thin APs list from local host.

Click the **Backup** button to save the thin APs list to local host from WLC.

Click the **Update** button to upgrade the firmware of selected thin AP.

Click the **Reboot** button to remotely restart the selected thin AP.

Following are the filter conditions for searching specific thin AP in the list, and click the **Search** button to search for an specific thin AP based on the filter condition.

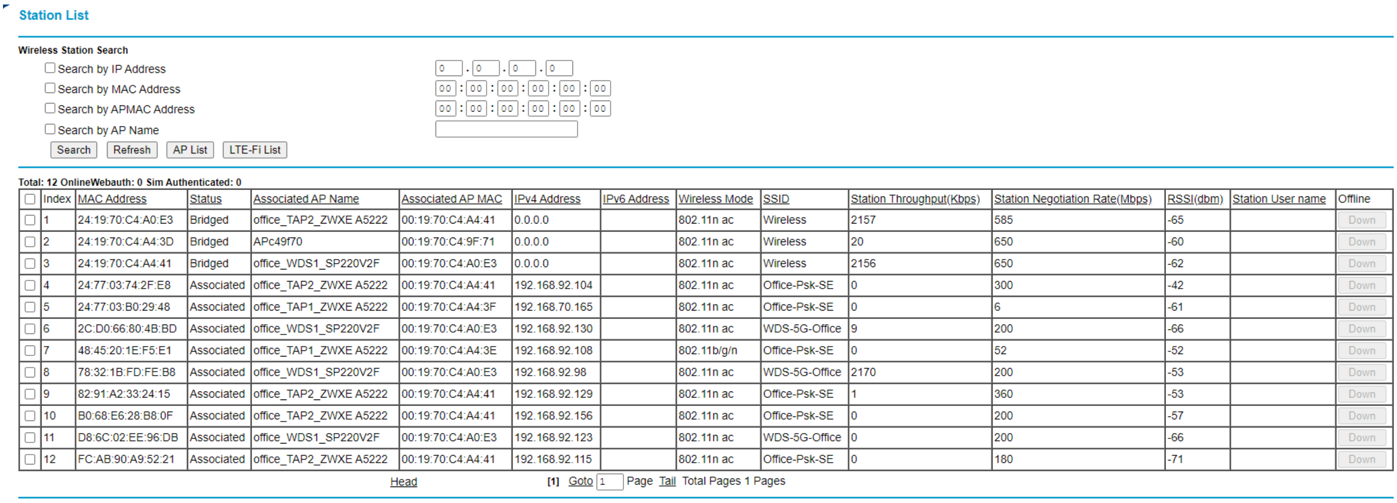
Filter Condition	Description
Search By GGW IP Address	Filter the search by GGW IP address in a 3G-Wi-Fi converged network .
Search By IP Address	Filter the search by thin AP IP address.
Search By MAC Address	Filter the search by thin AP MAC address.
Search By AP Name	Filter the search by thin AP name.
Search By Group Name	Filter the search by AP group name.
Search By AP Project Info	Filter the search by AP project information.

Note: The project information must be entered manually in the list. This is usually required for engineering project management.

11.6. Station List

All user clients that have ever associated with the thin APs, regardless of they are currently online or offline, will be added to the station list for displaying.

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: 12 OnlineWebauth: 0 Sim Authenticated: 0

□	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	24:19:70:C4:A0:E3	Bridged	office_TAP2_ZWXE A5222	00:19:70:C4:A4:41	0.0.0.0		802.11n ac	Wireless	2157	585	-65		Down
□	2	24:19:70:C4:A4:3D	Bridged	APc49f70	00:19:70:C4:9F:71	0.0.0.0		802.11n ac	Wireless	20	650	-60		Down
□	3	24:19:70:C4:A4:41	Bridged	office_WDS1_SP220V2F	00:19:70:C4:A0:E3	0.0.0.0		802.11n ac	Wireless	2156	650	-62		Down
□	4	24:77:03:74:2F:E8	Associated	office_TAP2_ZWXE A5222	00:19:70:C4:A4:41	192.168.92.104		802.11n ac	Office-Psk-SE	0	300	-42		Down
□	5	24:77:03:B0:29:48	Associated	office_TAP1_ZWXE A5222	00:19:70:C4:A4:3F	192.168.70.165		802.11n ac	Office-Psk-SE	0	6	-61		Down
□	6	2C:D0:66:80:4B:BD	Associated	office_WDS1_SP220V2F	00:19:70:C4:A0:E3	192.168.92.130		802.11n ac	WDS-5G-Office	9	200	-66		Down
□	7	48:45:20:1E:F5:E1	Associated	office_TAP1_ZWXE A5222	00:19:70:C4:A4:3E	192.168.92.108		802.11b/g/n	Office-Psk-SE	0	52	-52		Down
□	8	78:32:1B:FD:FE:B8	Associated	office_WDS1_SP220V2F	00:19:70:C4:A0:E3	192.168.92.98		802.11n ac	WDS-5G-Office	2170	200	-53		Down
□	9	82:91:A2:33:24:15	Associated	office_TAP2_ZWXE A5222	00:19:70:C4:A4:41	192.168.92.129		802.11n ac	Office-Psk-SE	1	360	-53		Down
□	10	B0:68:E6:28:B8:0F	Associated	office_TAP2_ZWXE A5222	00:19:70:C4:A4:41	192.168.92.156		802.11n ac	Office-Psk-SE	0	200	-57		Down
□	11	D8:6C:02:EE:96:DB	Associated	office_WDS1_SP220V2F	00:19:70:C4:A0:E3	192.168.92.123		802.11n ac	WDS-5G-Office	0	200	-66		Down
□	12	FC:AB:90:A9:52:21	Associated	office_TAP2_ZWXE A5222	00:19:70:C4:A4:41	192.168.92.115		802.11n ac	Office-Psk-SE	0	180	-71		Down

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

Figure 11-6 Station List Page

Following are the filter conditions for searching specific user client in the list, and click the **Search** button to search for an specific user client based on the filter condition.

Filter Condition	Description
Search By IP Address	Filter the search by STA IP address.
Search By MAC Address	Filter the search by STA MAC address.
Search By AP MAC Address	Filter the search by UE associated AP MAC address.
Search By AP Project Info	Filter the search by AP project information.

Click the **Search** button to search for an user client based on the selected condition.

Click the **Refresh** button to update the information displayed on this page.

Click the **AP List** button to display the AP list.

Click the **LTE-Fi List** button to display the LTE-Fi list.

11.7. DPI

DPI is enabled in [**System Management > DPI**] , and here is to display the DPI results of the statistics of users service types and user behavior. DPI is only applicable of "central switching" mode.

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

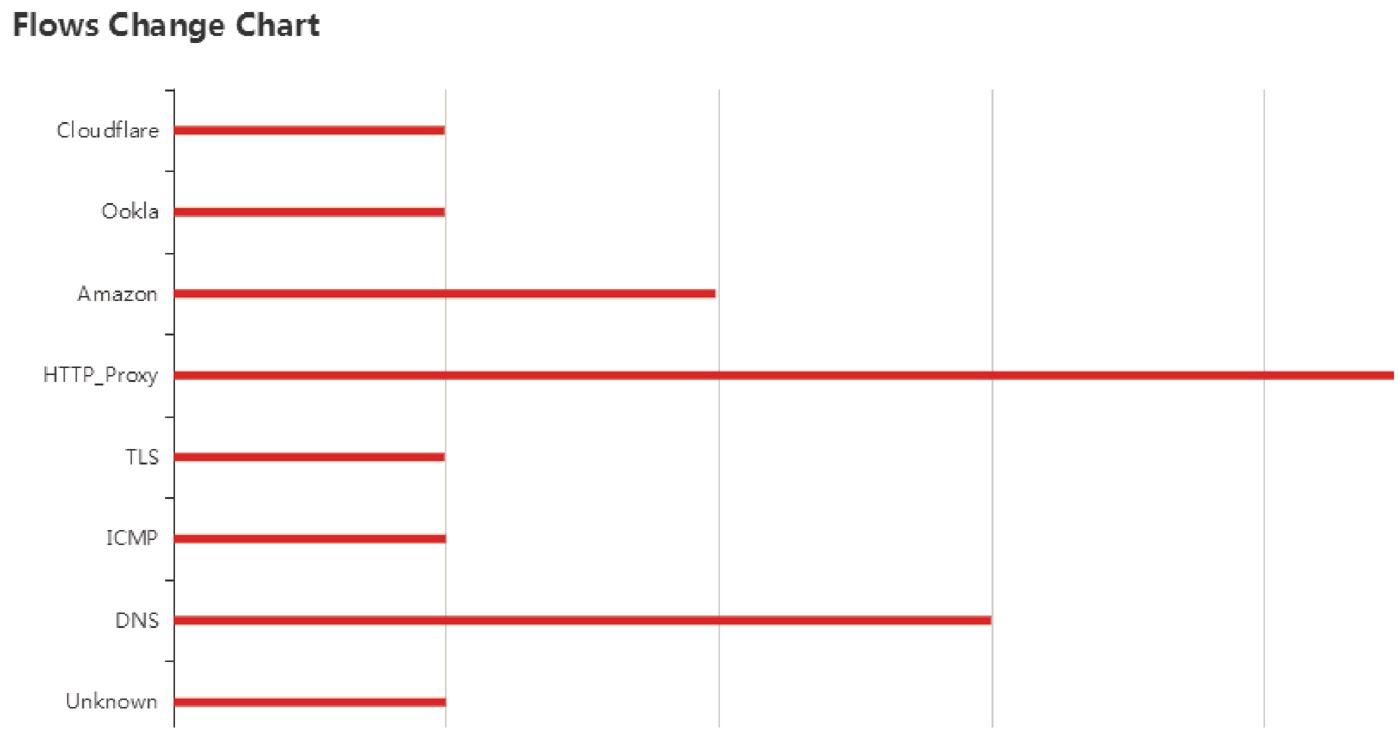


Figure 11-7 The Traffic Fluctuation Chart

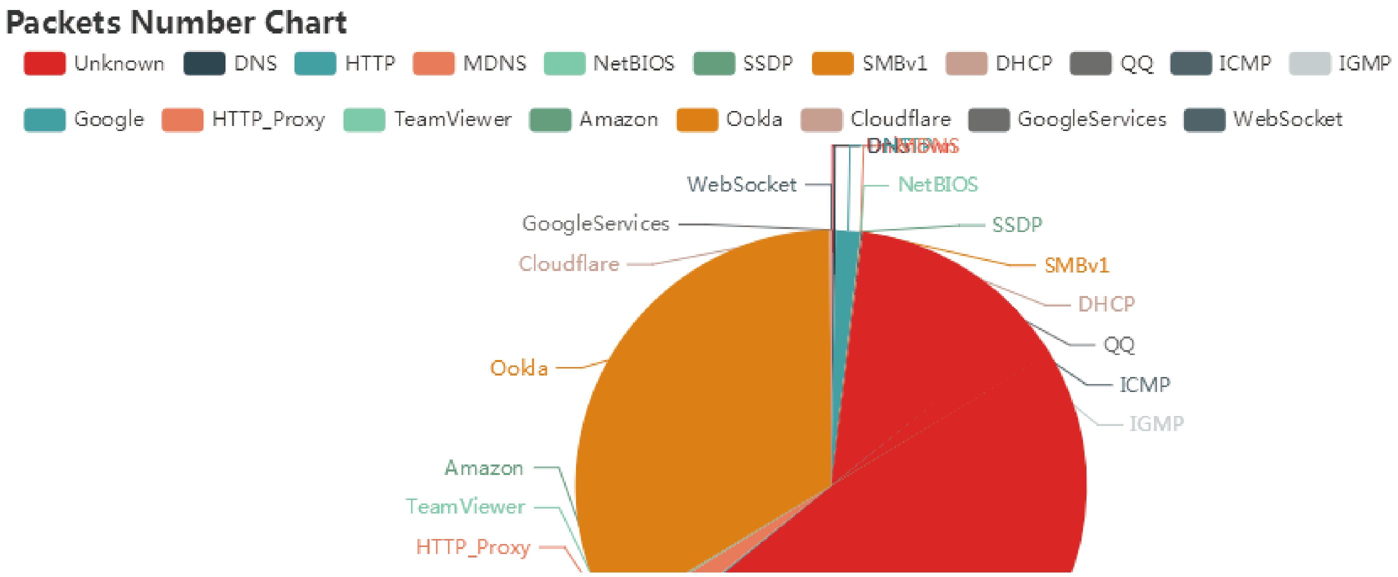
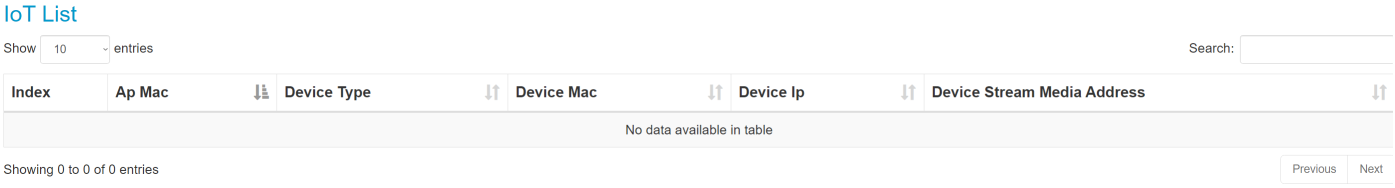


Figure 11-8 The Service Types Pie Chart

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

11.8. IoT List

IoT clients, such as various industrial sensors and IPCams, access to the WLC through Wi-Fi-CPE to achieve the central switching of IoT data streams. Therefore, as long as the IoT client is online, its status can be displayed through the [**Information > IoT Device List**] menu, as shown in the following figure:



IoT List

Show 10 entries Search:

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

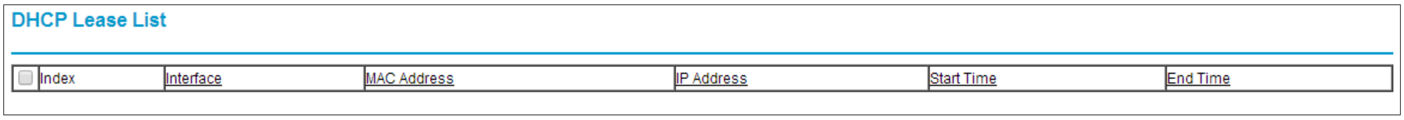
Showing 0 to 0 of 0 entries

Figure 11-9 IoT Devices List

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

11.9. DHCP Lease List

If internal DHCP server is enabled, then the IP addresses allocation for thin APs and user clients with their lease time will be displayed here. Select **[Statistics** > **DHCP Lease List]** in the menu to enter the following page:



DHCP Lease List

□ Index	Interface	MAC Address	IP Address	Start Time	End Time

Figure 11-10 DHCP Lease List Page

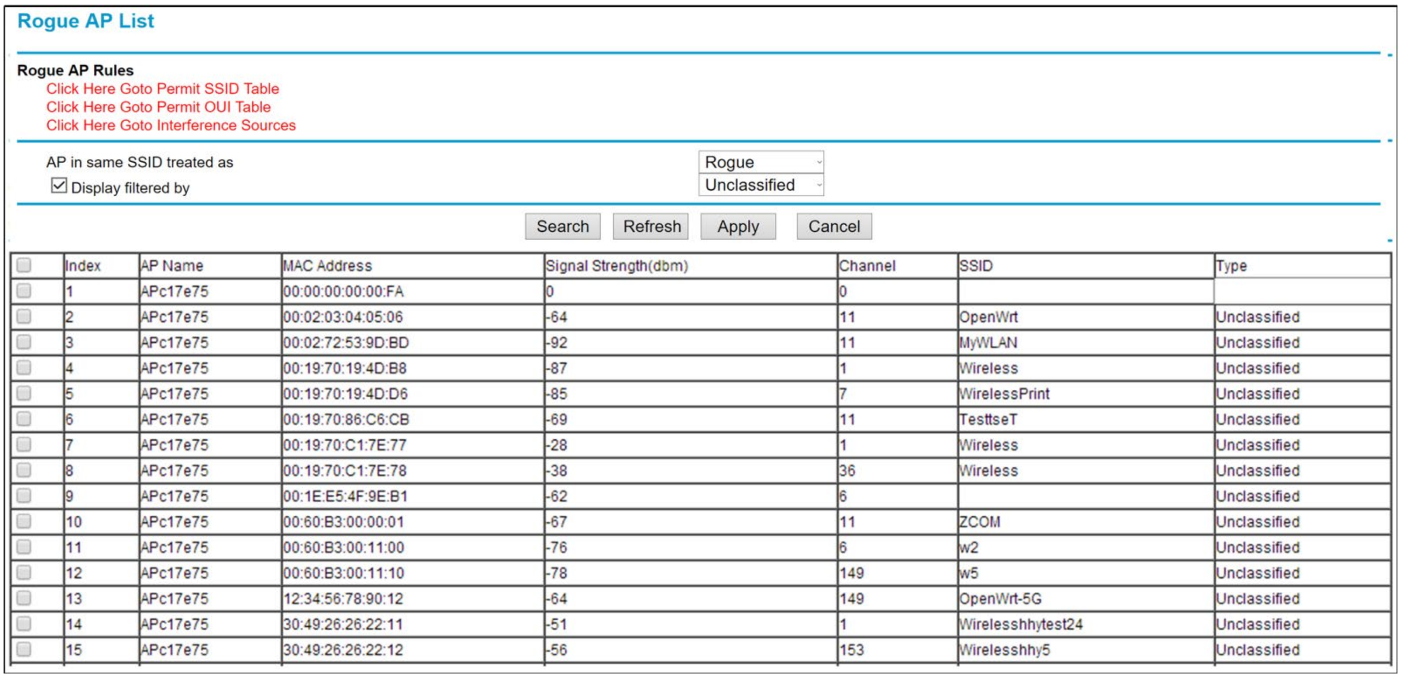
Click the **Refresh** button to update the information displayed on this page.

11.10. Rogue AP List

Rogue AP is such an AP pretending as a legitimate AP to access the WLC with the stolen SSID. Rogue APs are usually deployed nearby the legal APs. They have two hazards: one is to assist unauthorized user clients to invade the Wi-Fi system; the other is to interfere with the operating channel of legal APs. For the detected rogue AP, the administrator can also pretend it to issue a disassociation command to the illegal user clients, and force it to be kicked out of the system.

Generally, legitimate APs discover RF interference sources by background scanning, such as microwave ovens, Bluetooth devices, continuous wave generators, and rogue APs. All of them can be classified as "rogue APs", because they occupy the frequency resources of the legal APs and hazard to the work of the legal APs. These devices will also be added into the rogue AP list.

Select **[Statistics** > **Rogue AP]** in the menu to enter the configuration page as following:



Rogue AP List

Rogue AP Rules
Click Here Goto Permit SSID Table
Click Here Goto Permit OUI Table
Click Here Goto Interference Sources

AP in same SSID treated as: Rogue
☑ Display filtered by: Unclassified

□	Index	AP Name	MAC Address	Signal Strength(dbm)	Channel	SSID	Type
□	1	APc17e75	00:00:00:00:00:FA	0	0		
□	2	APc17e75	00:02:03:04:05:06	-64	11	OpenWrt	Unclassified
□	3	APc17e75	00:02:72:53:9D:BD	-92	11	MyWLAN	Unclassified
□	4	APc17e75	00:19:70:19:4D:B8	-87	1	Wireless	Unclassified
□	5	APc17e75	00:19:70:19:4D:D6	-85	7	WirelessPrint	Unclassified
□	6	APc17e75	00:19:70:86:C6:CB	-69	11	TesttseT	Unclassified
□	7	APc17e75	00:19:70:C1:7E:77	-28	1	Wireless	Unclassified
□	8	APc17e75	00:19:70:C1:7E:78	-38	36	Wireless	Unclassified
□	9	APc17e75	00:1E:E5:4F:9E:B1	-62	6		Unclassified
□	10	APc17e75	00:60:B3:00:00:01	-67	11	ZCOM	Unclassified
□	11	APc17e75	00:60:B3:00:11:00	-76	6	w2	Unclassified
□	12	APc17e75	00:60:B3:00:11:10	-78	149	w5	Unclassified
□	13	APc17e75	12:34:56:78:90:12	-64	149	OpenWrt-5G	Unclassified
□	14	APc17e75	30:49:26:26:22:11	-51	1	Wirelesshhytest24	Unclassified
□	15	APc17e75	30:49:26:26:22:12	-56	153	Wirelesshhy5	Unclassified

Figure 11-11 Rogue AP List Page

These parameters in **[Statistics** > **Rogue AP]** page is described in details as following:

Parameter	Description
Rogue AP Rules	Go to the red hyperlink page to create three tables which will be used to match the scanned AP:
	● **Goto Permit SSID Table:** Enter the page to create the legal **SSID**s list.
	● **Goto Permit OUI Table:** Enter the page to create the legal **OUI**s list (the first three octets in a MAC address forms the OUI).
	● **Goto Interference Sources:** Enter the page where the interference sources list displayed.
AP in Same SSID Treated As	The detected AP uses the same SSID as the current AP, which can be classified as:
	● **Rogue:** The untrusted Rouge AP.with a stolen SSID.
	● **Trust:** The legitimate AP with the same SSID as current AP.
Display Filtered By	Define the filter conditions for displaying list:
	● **Unclassified:** Displaying all APs without classification in the scanning AP list.
	● **Trust SSID:** Only displaying the legal APs with trusted SSID in the scanning AP list.
	● **Rogue SSID:** Only displaying the rogue APs with the stolen SSID in the scanning AP list.
	● **Permit SSID:** Only displaying the legal APs with the permitted SSID in the scanning AP list.
	● **Permit OUI:** Only displaying the APs with the permitted OUI in the scanning

Parameter	Description
	AP list.
	● **Attacking:** Only displaying the APs which are attacking the associated illegal wireless clients.
Scan	Click this button to enable the selected thin AP to start background scan.
Refresh	Click this button to update the information displayed on this page
Start Attack	Click this button on the selected thin AP, pretending the Rogue AP to start sending disassociation command to kick illegal user clients out.
Stop Attack	Click this button on the selected thin AP, stop sending disassociation command.

Click the **Search** button to search for an entry based on the selected filter condition.

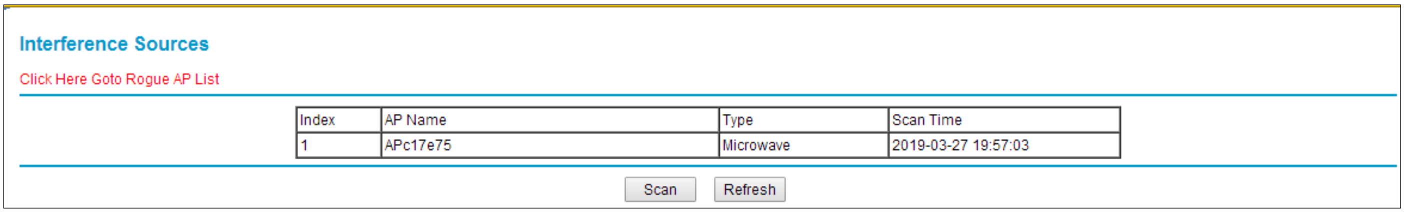
Click the **Apply** button to accept the changes.

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

11.11. INTERFERENCE SOURCES

The 2.4GHz frequency band is an ISM band that does not need to be applied for. Wi-Fi and other general wireless technologies (such as microwave ovens, Bluetooth devices and continuous wave generators) all use this band to work, that is, in the 2.4GHz open RF environment, Wi-Fi will coexist with other general wireless devices and may interfere with each other. Therefore, it is best to have a RF detection measure for Wi-Fi engineering to detect the interference sources in advance, avoiding interference from other RF equipment.

Select **[Statistics** > **Interference Sources]** in the menu to enter the configuration page as following:



Interference Sources

Click Here Goto Rogue AP List

Index	AP Name	Type	Scan Time
1	APc17e75	Microwave	2019-03-27 19:57:03

Figure 11-12 Interference Source Page

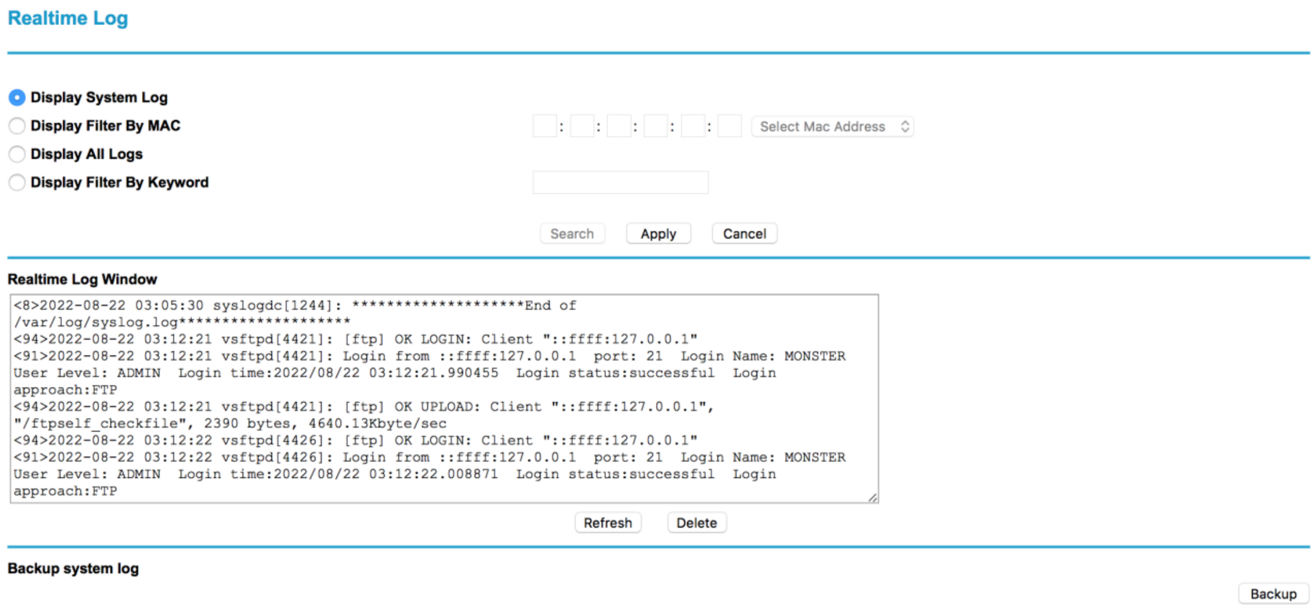
Click the <**Scan**> button to perform a background scanning to detect the interference sources, the scan results will be added to the list. The interference sources include rogue APs, Bluetooth devices, microwave ovens, continuous wave generators, and unknown sources.

Click the <**Refresh**> button to dynamically update the interference information displayed on this page.

11.12. Realtime Log

The real-time log is a dynamic log, which shows what is happening in the WLC in real time. Therefore, the log information will scroll quickly in the "Real Time Log" window. The administrator can take it as a tool to inspect the working status of the WLC. Due to its real-time nature will take up too much system resources to degrade performance, so do not 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
```

Figure 11-13 Realtime Log Page

Click the **Search** button to search for an entry based on the selected filter condition.

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

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

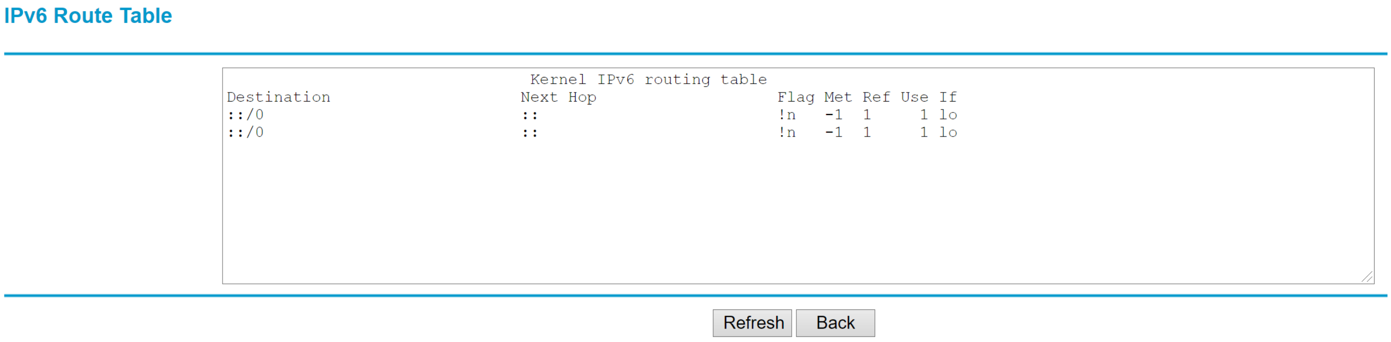
Click the **Refresh** button to update the information displayed on this page.

Click the **Delete** button to delete the information displayed in the textbox.

Click the **Backup** button to back up the contents displayed in the real-time log window to the local host.

11.13. IPv6 Route Table

If the Wi-Fi system is deployed in an IPv6 network, IPv6 routing settings must be completed in the [**IPv6 Configuration> Static Routing Settings**] and [**IPv6 Configuration> Dynamic Routing**] menus, the results are displayed as the figure below:



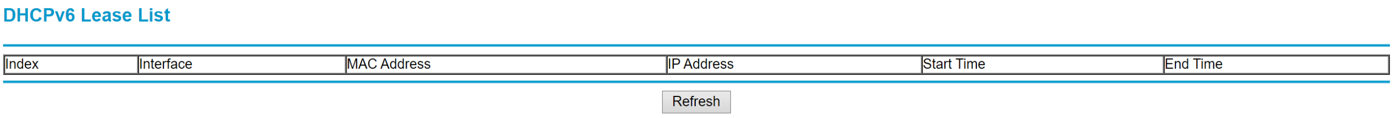
IPv6 Route Table

```
                                Kernel IPv6 routing table
Destination                     Next Hop                   Flag Met Ref Use If
::/0                            ::                         !n   -1  1      1 lo
::/0                            ::                         !n   -1  1      1 lo
```

Figure 11-14 IPv6 Route Table Page

11.14. DHCPv6 Lease List

If Wi-Fi system is deployed in an IPv6 network, and WLC internal DHCPv6 is enabled and configured in [**IPv6 Configuration > DHCP Server**], those IPv6 DHCP leases will be displayed here in the table below.



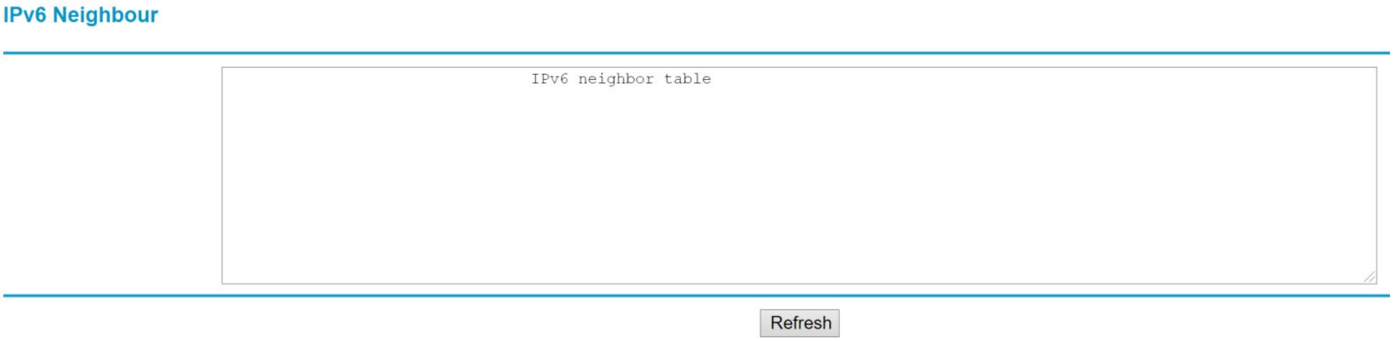
DHCPv6 Lease List

Index	Interface	MAC Address	IP Address	Start Time	End Time

Figure 11-15 DHCPv6 Lease List

11.15. IPv6 Neighbor

If Wi-Fi system is deployed in an IPv6 network, all IPv6 neighboring equipment can be scanned by WLC and added in to the table below.



IPv6 Neighbour

```
IPv6 neighbor table
```

Figure 11-16 IPv6 Neighbor AP Table

Click <**Refresh**> button to dynamically update the table.

Chapter 12. TECHNICAL SPECIFICATIONS

Physical Specification		WS200G2	WS500G2	WS1000G2
Power Supply	**Volts (V)**	100-240V AC	100-240V AC	100-240V AC
	Amps (A)	10-5 A	10-5 A	10-5 A
	Hertz (Hz)	50/60 Hz	50/60 Hz	50/60 Hz
	Watt (W)	280 Watt	400 Watt	800 Watt
Fans/Fan Modules		4 Modules	4 Modules	4 Modules
Dimensions	**(Height)**	44 mm	44 mm	88 mm
	(Width)	438 mm	438 mm	438 mm
	(Depth)	630 mm	630 mm	600 mm
	Form Factor	1U	1U	2U
Weight		18 kg	18 kg	25 kg
Ports	**RJ45 (1G)**	8	8	8
	SFP+ (10G)	4	8	4
	QSFP (40G)	-	-	2
Memory	**Size**	16 GB	32 GB	128 GB
	Type	DDR4	DDR4	DDR4
Storage (Primary)	**Size**	64 GB	64 GB	128 GB
	Type	SSD	SSD	SSD
Storage (Secondary)	**Size**	-	-	1 TB
	Type	-	-	2.5" HDD

Software Specification	WS200G2	WS500G2	WS1000G2
AP Capacity	2048	4096	8192
MAC Address Table	64K	127K	127K
Max. Number of VLANs	4K	4K	4K

Environment Specification		WS200G2	WS500G2	WS1000G2
Temperature	**Operating**	0°C to 40°C (32°F to 104°F)		
Humidity	**Operating**	10% to 95% (Non-condensing)		

Chapter 13. APPENDIX

13.1. WARRANTY

13.1.1. 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).

Z-COM reserves the right to inspect all defective products which must be returned and paid shipping fee by purchasers.

13.1.2. 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

13.1.3. 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.

13.2. Certifications and Compliance

13.2.1. CE Marking

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

CE

13.2.2. WEEE 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.

13.3. 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

13.4. 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

Z-COM, Inc.
www.zcom.com.tw