FS-AP1167C/FS-AP3000C Wireless Access Point Software User Guide

Table of Contents

Chapter 1 Login Device Management

Wireless access point product provides built-in WEB Server. User can log in the device by WEB webmaster terminal (PC), manage and maintain the device by built-in WEB Server in WEB mode.

Both wireless access point product and WEB webmaster terminal (PC) require network configuration to ensure normal login by WEB webmaster.

Note:
WEB Server of the wireless access point is open by default and default device address is 192.168.1.1. Webmaster terminal (PC) internet access connects with that of device. PC network card configuration is 192.168.1.X network segment, which connects with wireless access point (AP) device internet access, so it is possible to manage wireless AP device by WEB. Input http://192.168.1.1 in the browser address bar of WEB management terminal (PC), the browser shows WEB management login page, the user enters user name and password to log in WEB management page for configuration.

1.1 WEB Management Login

User inputs http://192.168.1.1 in the browser address bar of management PC (WEB webmaster terminal and wireless AP have network access), the browser shows WEB webmaster login page (as shown in Figure 1-1). Input [User Name] and [Password], it is “admin” and “admin” by default. After input, click <Login>, log in and shift to the main interface of WEB management configuration.

Configuration Item	Description
Language	Set up language of login page: “中文” and “English”
User Name	User account for login system
Password	Password of user account

Figure 1-1 WEB Login

Table 1-1 Parameter Description of WEB Login Interface

Note: FS access points work in FIT AP mode by default.

Chapter 2 FIT/FAT AP Switch

2.1 Switch from FIT AP to FAT AP

The default address of the device is 192.168.1.1. PC internet access connects with device internet access. PC network card configuration is 192.168.1.X network segment which connects with wireless point device internet access. PC telnets on AP. Default dame of user telnet is “admin” and password is “admin”. Switch AP FIT/FAT mode by command, as shown in Figure 2-1. After switching, AP will restart and work in FAT AP mode.

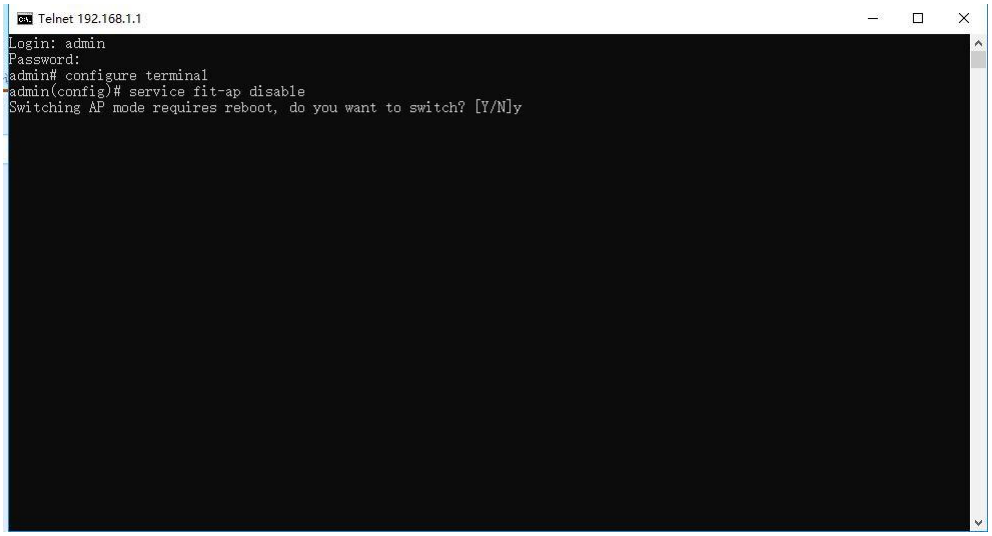

Figure 2-1 Switch from FIT AP to FAT AP

2.2 Switch from FAT AP to FIT AP

The default address of the device is 192.168.1.1. PC internet access connects with device internet access. PC network card configuration is 192.168.1.X network segment which connects with wireless point device internet access. PC telnets on AP. Default dame of user telnet is “admin” and password is “admin”. Switch AP FIT/FAT mode by command, as shown in Figure 2-2. After switching, AP will restart and works in FIT AP mode.

Figure 2-2 Switch from FAT AP to FIT AP

Chapter 3 FIT AP System Monitor

3.1 Summary

On [Summary] page, you will see present device information of AP, such as [System Name], [Model], [Software Version], [Hardware Version], [MAC Address], as shown in Figure 3-1.

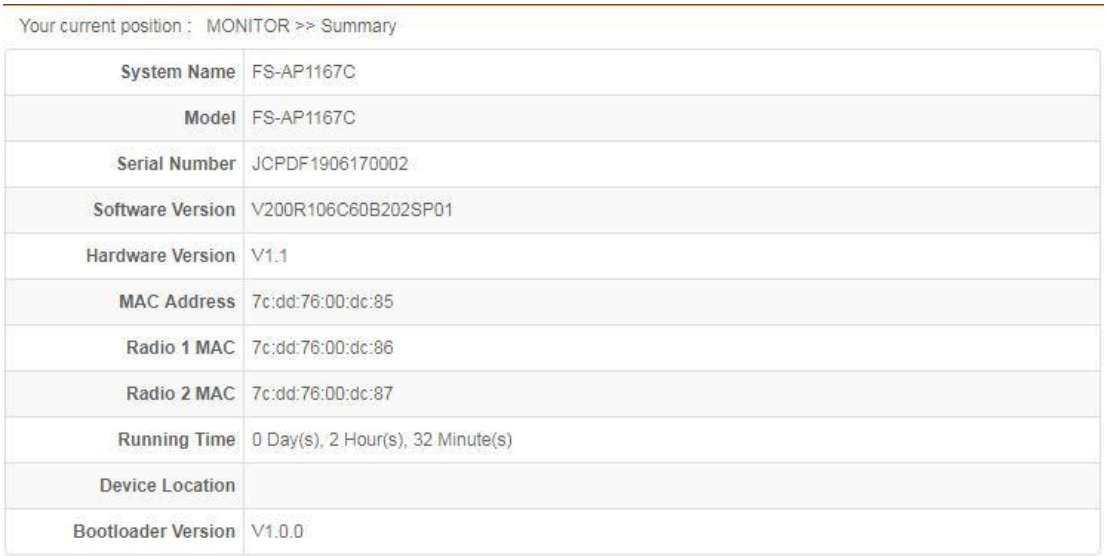

Figure 3-1 Device Information

3.2 System Information

3.2.1 CPU Usage

Make statistics of device CPU utilization and show this information in real-time. Zoom has three options: “1min”, “5min” and “All”, for setting up the display of time frame of CPU utilization, as shown in Figure 3-2.

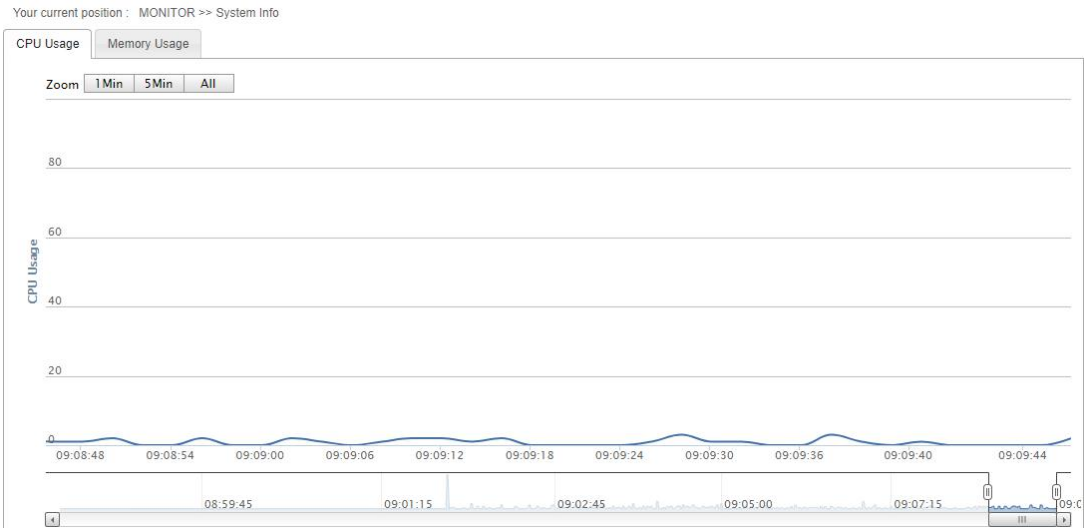

Figure 3-2 Routing Configuration Page

3.2.2 Memory Usage

Make statistics of device internal storage utilization and show this information in real-time. Zoom has three options: “1min”, “5min” and “All”, for setting up the display of time frame of internal storage utilization, as shown in Figure 3-3.

Figure 3-3 Internal Storage Utilization Rate

3.3 STA List

[STA List] lists terminals which access to this AP currently and shows details of each access terminal, as shown in Figure 3-4.

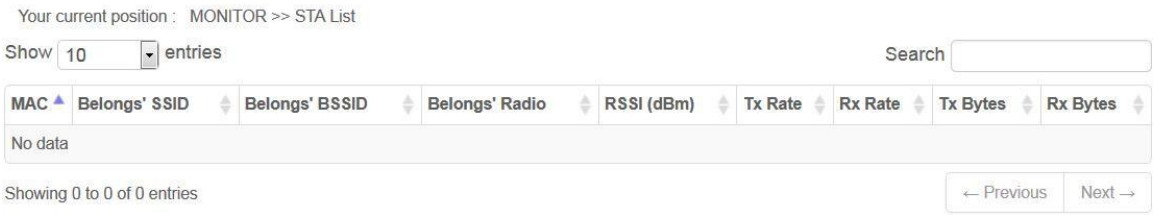

Figure 3-4 Access Terminal List

3.4 AP List

Scan periphery AP information. FIT AP scans periphery AP information only when AC distributes template successfully and FIT AP has wireless configuration.

Figure 3-5 Periphery AP List

Chapter 4 FIT AP Network Settings

4.1 Interface Management

The management interface is [management] by default and address is 192.168.1.1. This interface enables the DHCP address pool by default. After obtaining the address, 192.168.1.1 will be replaced automatically.

Figure 4-1 Interface Management

User changes the way to obtain address at this interface as needed by:
1) Select "management" interface;
2) Click <Edit> in menu;
3) Select "IP Configuration Type" in window pop up.

Chapter 5 FIT AP Service Management

5.1 SSH Settings

Figure 5-1 SSH Settings

Configuration Item	Description
Enable SSH	SSH access switch, you may select "enable" or "disable"
Timeout	Set up timeout of SSH access

Table 5-1 Parameter Description of SSH Settings

5.2 Telnet Settings

AP enables [Telnet] by default. User may visit AP command line by telnet mode. The configuration page is shown in Figure 5-2.

Figure 5-2 Telnet Settings

Configuration Item	Description
Enable Telnet	Telnet access switch, you may select “enable” or “disable”
Timeout	Set up timeout of Telnet access

Table 5-2 Parameter Description of Telnet Settings

Chapter 6 FIT AP Device Settings

6.1 System Configuration

“System Name” can be modified in [System Configuration] >[Device], as shown in Figure 6-1.

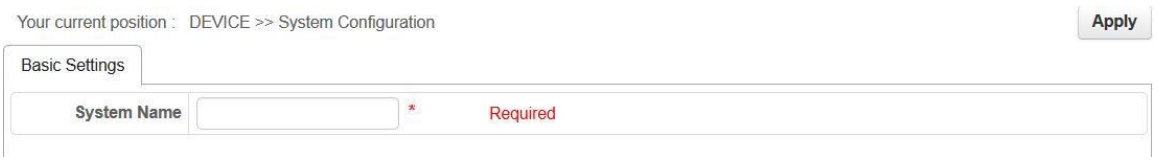

Figure 6-1 System Configuration

6.2 Discovery Mode

The user can set up discovery mode on [Device Management] page, it is “dynamic discovery” by default.

6.2.1 Dynamic Discovery

FIT AP supports broadcast discovery, Option43 discovery and DNS discovery.

• Broadcast discovery

AP and AC are in the same layer-two network. When AP obtains dynamically or manually configures address in the same network segment as AC, AP can discover AC directly by layer-two broadcast and go online successfully.

• Option43 discovery

AP acquires IP and Option43 (with ac_ip) through DHCP Server, and AP sends unicast discovery online request to specific AC based on ac_ip.

• DNS discovery

AP and AC are in the layer-three network. AP acquires IP, DNS Server IP and Domain name through DHCP Server. AP sends AC discovery request by broadcast in the layer-two network, no response, then AP sends ARP message according to DNS Server IP acquired, and find DNS Server; then AP requests DNS Server resolution domain name according to Domain name, acquires ac_ip. ap and ac goes online interactively in a unicast way.

If DHCP Server on AP upper layer does not match DNS Server IP and Domain name, you can configure Domain name and DNS Server IP on AP page directly. On AP page, AC hostname and AC domain constitute Domain name. If the full name of Domain name is dns.test.com, then AC hostname should be DNS and AC domain should be test.com.

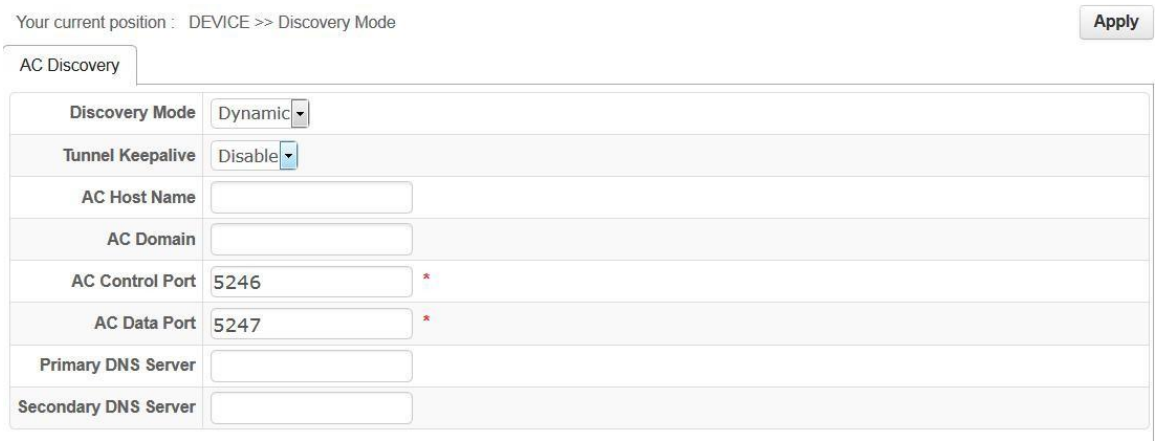

Figure 6-2 Dynamic Discovery

6.2.2 Static Discovery

Configure “static discovery” on AP [Device Management] page, in “static discovery” mode, you need to configure [AP IP Address], [Subnet Mask], [AC IP Address] manually. [AC IP Address] may be configured on [Discovery Mode] page, as shown in Figure 6-3.

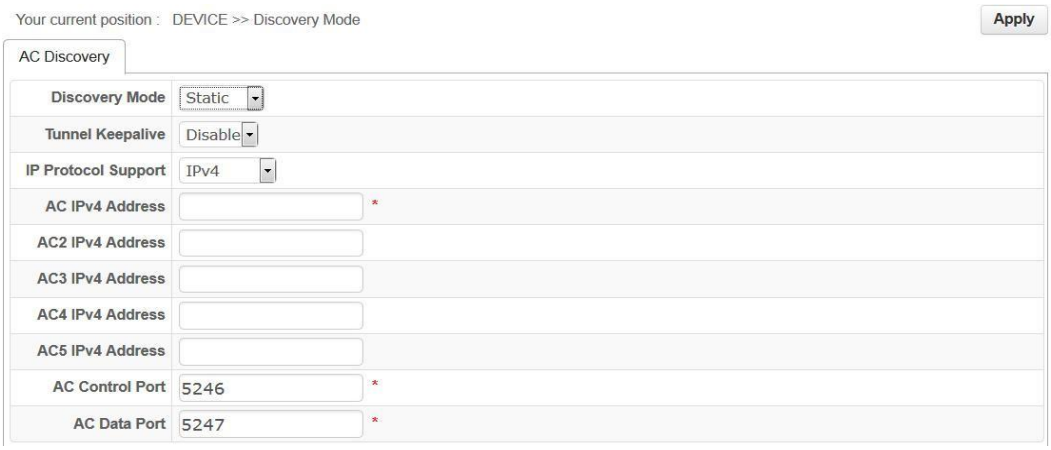

Figure 6-3 Static Discovery

Configuration Item	Description
Discovery Mode	Set up AC discovery mode of AP, you may select “dynamic discovery” or “static discovery”
Tunnel Keepalive	Tunnel keep-alive switch, you may select “disable” or “enable”
IP Protocol Support	Designate IP protocol type utilized, it is “IPv4” by default
AC IPv4 Address	Designate AC IP address in static discovery mode
AC Host Name	Designate host name of target AC
AC Domain	Designate AC domain
Primary DNS Server	Designate DNS server address
Secondary DNS Server	Designate standby DNS server address

Table 6-1 Parameter Description of Discovery Mode

AP address and subnet mask of AP is set up on interface management by editing [management-interface], as shown in Figure 6-4. Message sent by default AP will have no management VLAN tag. If it is necessary to make management message sent by AP has management VLAN tag, then fill management VLAN ID in [VLAN ID], but eth1 port should be changed into Tagged member in management VLAN.

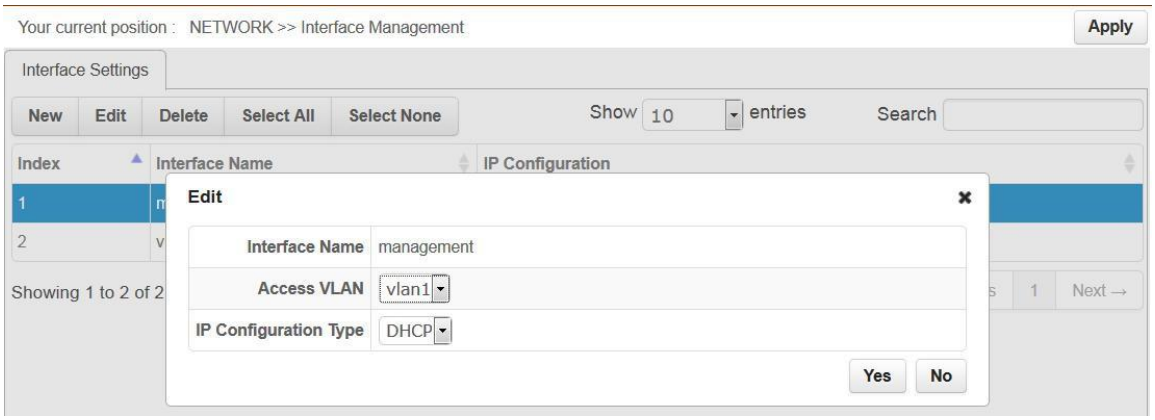

Figure 6-4 Configure Management Interface

Configuration Item	Description
Visit VLAN	Configure VLAN of wireless service operation
IP Configuration Type	Designate ways to obtain address by management interface. It has two options: “DHCP” and “static”
IP Address	Configure interface IP address
Subnet Mask	Configure interface subnet mask
Default Gateway	Configure interface default gateway

Table 6-2 Parameter Description of Interface Configuration

6.3 Time Settings

Set up local time of system, as shown in Figure 6-5.

Figure 6-5 Manual Time Settings

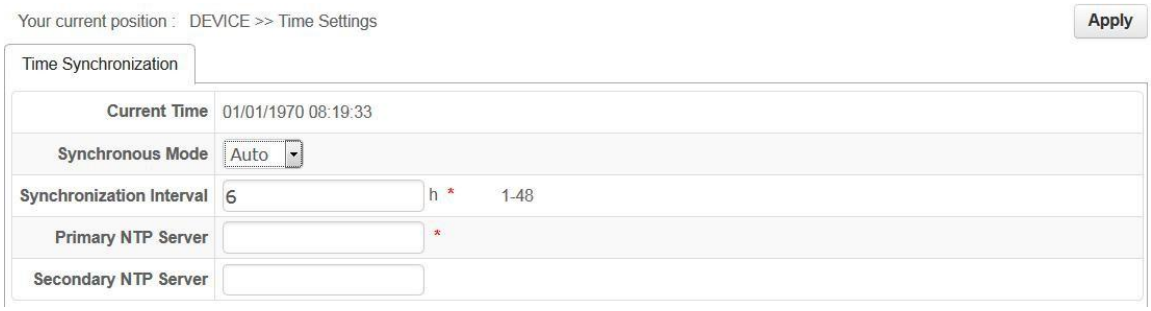

Figure 6-6 Automatic Synchronization Time

Configuration Item	Description
Synchronization Mode	Configure system time synchronization mode. You may select “manual” or “automatic”
System Time	Set up current time of system
Synchronization Period	Period for system synchronizes the time automatically
Primary NTP Server	Set up the IP address of NTP Server. NTP Server is the network time server for synchronizing computer time on the internet
Secondary NTP Server	When NTP server 1 is not available, the system will synchronize time with NTP server 2

Table 6-3 Parameter Description of Time Settings

Note:

• NTP (Network Time Protocol) provides router, switch and workstation with time synchronization. With time synchronization, you can connect relevant event record on multiple network devices and it is good for analyzing complicated malfunction and safety events.

• Time limits of other functions of the router (such as a firewall) become effective only when GMT time is acquired through the Internet or system time is set up manually.

6.4 User Management

Open [User Management] page, you can change the administrator password or add the new user to control access to the management page, as shown in Figure 6-7.

When adding user, there are three types of user role: "visitor", "administrator" and "system administrator", as shown in Figure 6-8. "Visitor" has the lowest access level and can check [System information] only; "administrator user" can check and perform regular settings, but can't perform senior settings such as user management; "system administrator" has the highest access level.

Figure 6-7 User Management

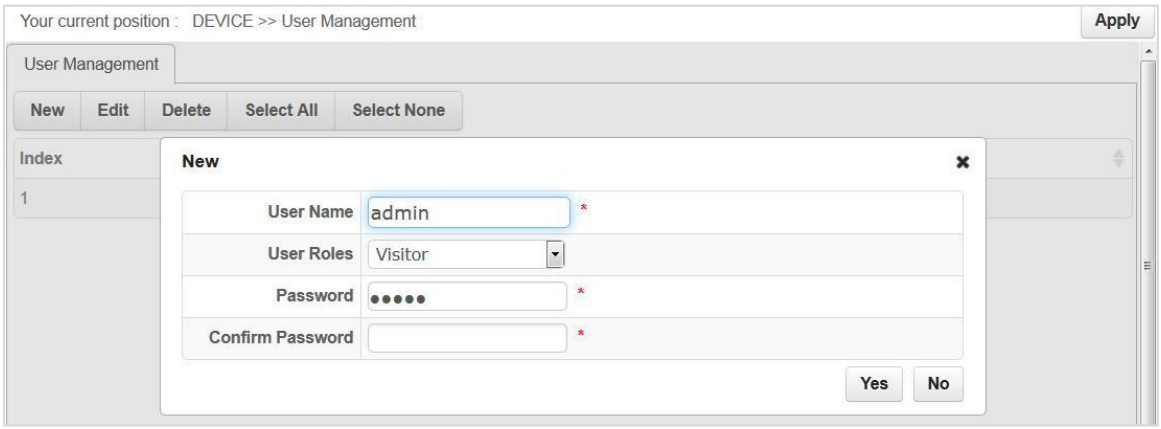

Figure 6-8 Add User

Configuration Item	Description
User Name	Configure user name
User Role	Configure user authority
Password	Set up password
Confirm Password	Input password again and confirm password

Table 6-4 Parameter Description of Add User

6.5 Configuration Management

Configuration management is divided into two parts [Import] and [Export].
Configure document import and export.

Select menu [Configuration Management] >[Import] /[Export], you may import or export AP configuration files.
With export configuration function, you can save AP configuration in the computer by files for use in the future. Before upgrading AP software or loading new configuration files, the backup original configuration of AP to prevent configuration loss in process of software upgrading or loading new configuration files.

With Import configuration function, you can re-import configuration files saved or edited before.
If you need to configure the same settings for multiple APs, you can configure one AP first, save its configuration file, then import it to other AP. It saves configuration time.
When device parameters are configured, you can back up this configuration information. In the event of device breakdown, it will restore to the status before backup. Open [Export] page, click <Export>, as shown in Figure 5-10, dialog box of saving file appears. Operate as instructed will backup configuration parameters. If you want to import, just click [Import configuration], designate files you want to recover, then click <Import>, as shown in Figure 5-9, the configuration in files will be written into the device again.

Figure 6-9 Import Configuration

Figure 6-10 Export Configuration

6.6 Device Maintenance

Device maintenance consists of three parts: [Restart], [Restore Factory Settings] and [Upgrade].

• Device Restart Click <Restart> to restart the device, as shown in Figure 6-11.

Figure 6-11 Restart Device

• Restore Factory Settings Click <Restore> to restore factory settings by software, as shown in Figure 6-12.
For restoring factory settings by hardware, when the device is on, press "Reset" longer than 5s, device will be restored to the default value.

Figure 6-12 Restore Factory Settings

Note:
1. All settings of AP will be restored to the factory default value, which
Default user name: admin
Default password: admin
Default IP address:192.168.1.1
Default subnet mask: 255.255.255.0
2. Please backup configuration information before restoring factory settings. Restore AP configuration by loading backup configuration when necessary.

• Version Upgrade As shown in Figure 6-13, click <Browse> to select the document for upgrading, then click <Upgrade> to upgrade the device.

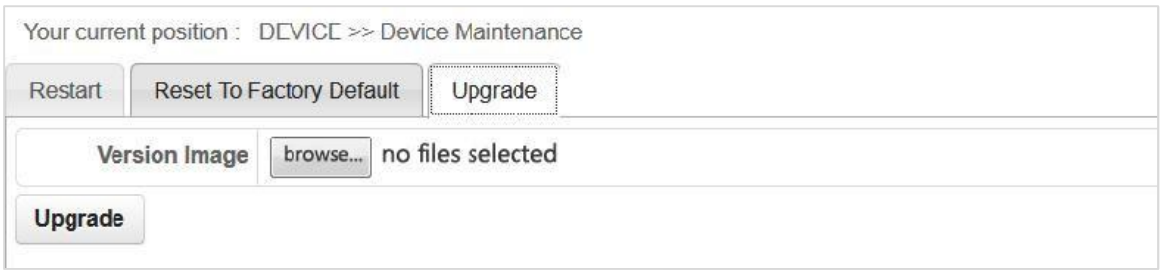

Figure 6-13 Version Upgrade

Note: When upgrade, please select the software which has the same version as present hardware. Do not turn off AP during upgrading, otherwise, it will cause damage to AP.

Chapter 7 FAT AP System Monitor

7.1 Summary

On the [Summary] page, you will see device information of AP, such as system name, model, software version, hardware version, MAC address.

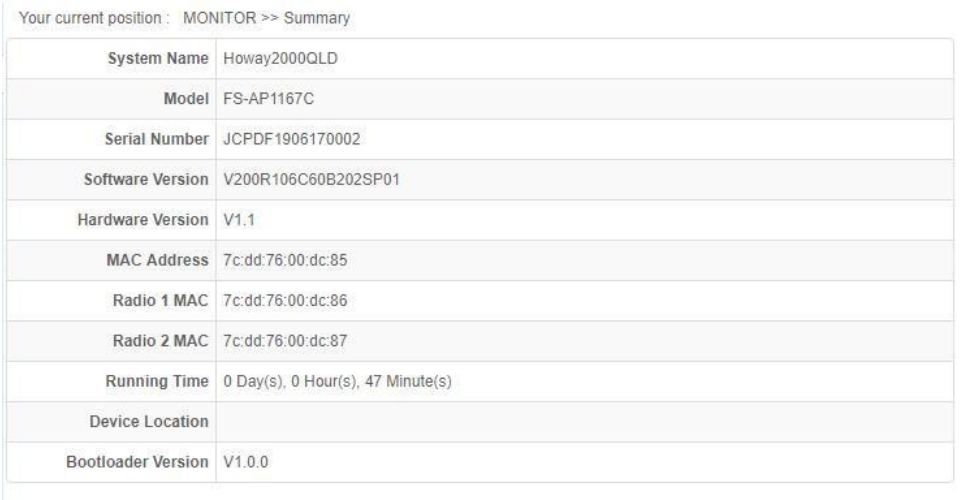

Figure 7-1 Summary

7.2 Connection Status

[Connection Status] page is under route mode for displaying current Wan connection status of AP, DHCP address pool at Lan side, Lan address, as shown in Figure 7-2.

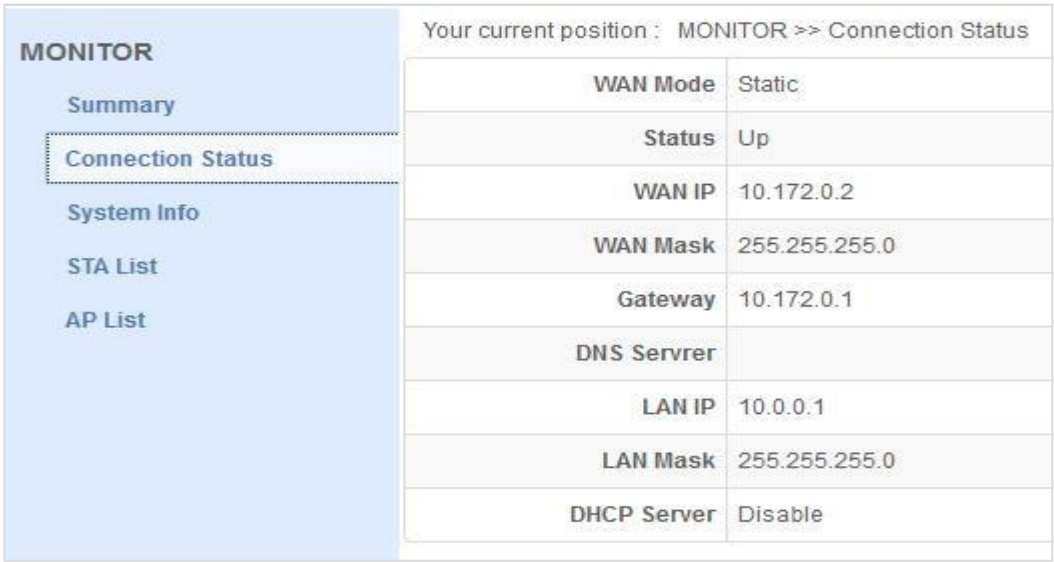

Figure 7-2 Connection Status

7.3 System Information

7.3.1 CPU Usage

Make statistics of device CPU utilization and show such information in real-time. Zoom has three options: [1Min], [5 Min] and [All], for setting up the time frame of CPU utilization information, as shown in Figure 7-3.

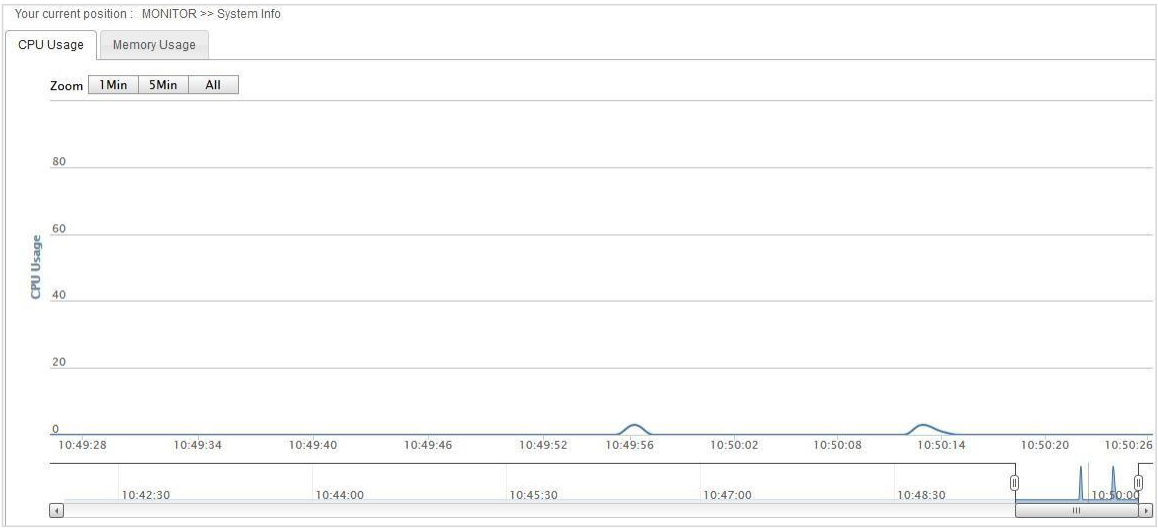

Figure 7-3 CPU Utilization Rate

7.3.2 Memory Usage

Make statistics of device internal storage utilization and show such information in real-time. Zoom has three options: [1Min], [5 Min] and [All], for setting up the time frame of internal storage utilization information, as shown in Figure 7-4.

Figure 7-4 Memory Usage

7.4 STA List

[STA List] lists terminals accessed to this AP and shows details of each access terminal, as shown in Figure 7-5.

Figure 7-5 STA List

7.5 AP List

Scan peripheral AP information, as shown in Figure 7-6.

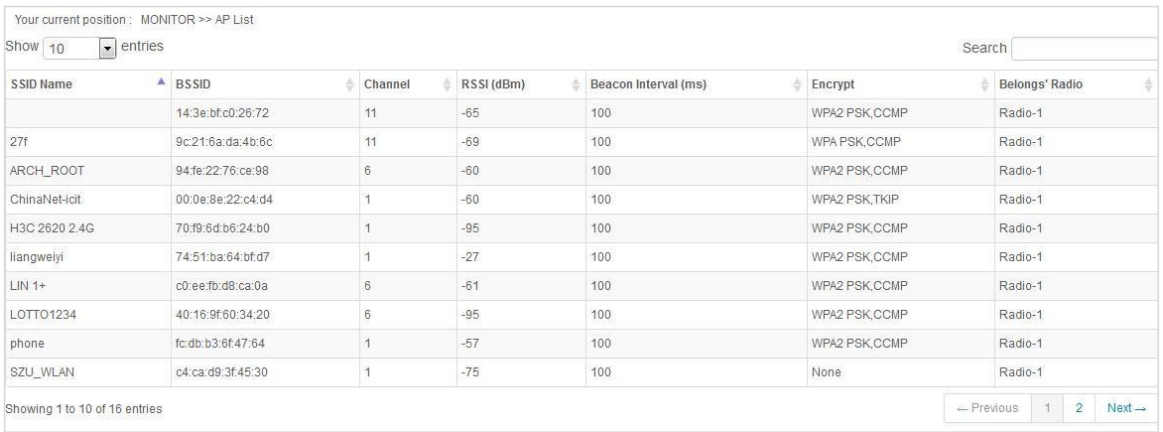

Figure 7-6 Peripheral AP List

Chapter 8 FAT AP Wireless Settings

8.1 Basic Settings

Set up basic wireless network parameters here, such as [RF ID], [Wireless Mode], [Channel], [Channel Bandwidth], [Transmitted Power], etc.

8.1.1 Radio

Enter [Wireless] > [Basic] to set up radio frequency information, including [Wireless Mode], [Channel], [Channel Bandwidth], [Transmitted Power], [A-MPDU], [WMM], [RTS Threshold], [OBSS Coexistence] and [Signal Strength Limit], RF configuration page is shown in Figure 8-1, and Figure 8-2.

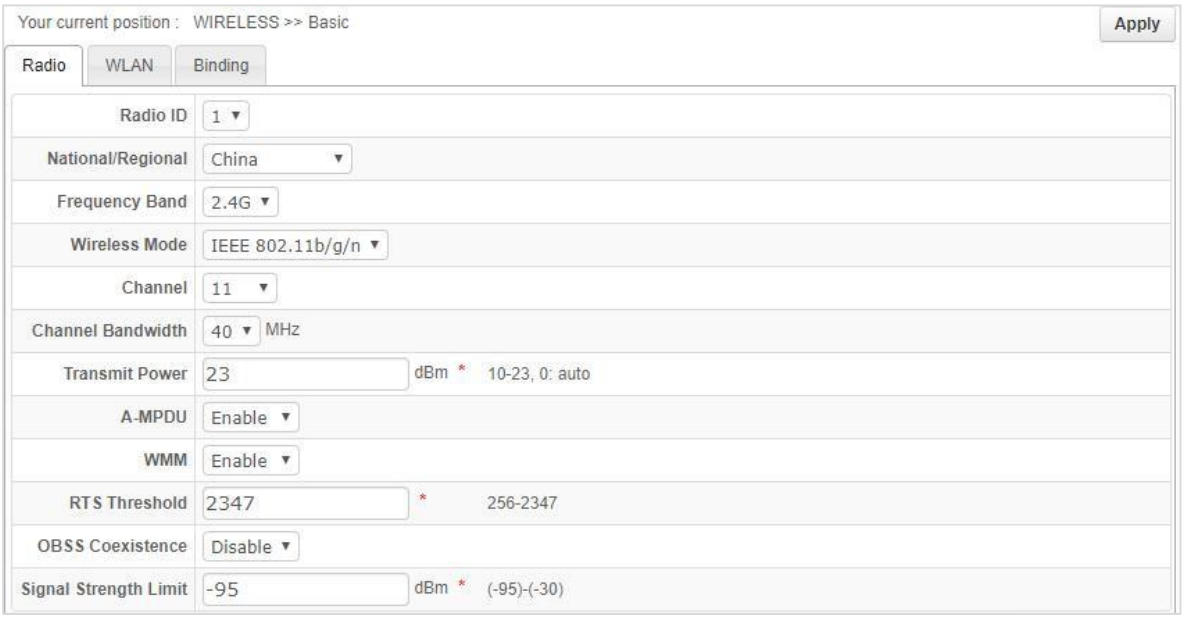

Figure 8-1 RF 1 Information

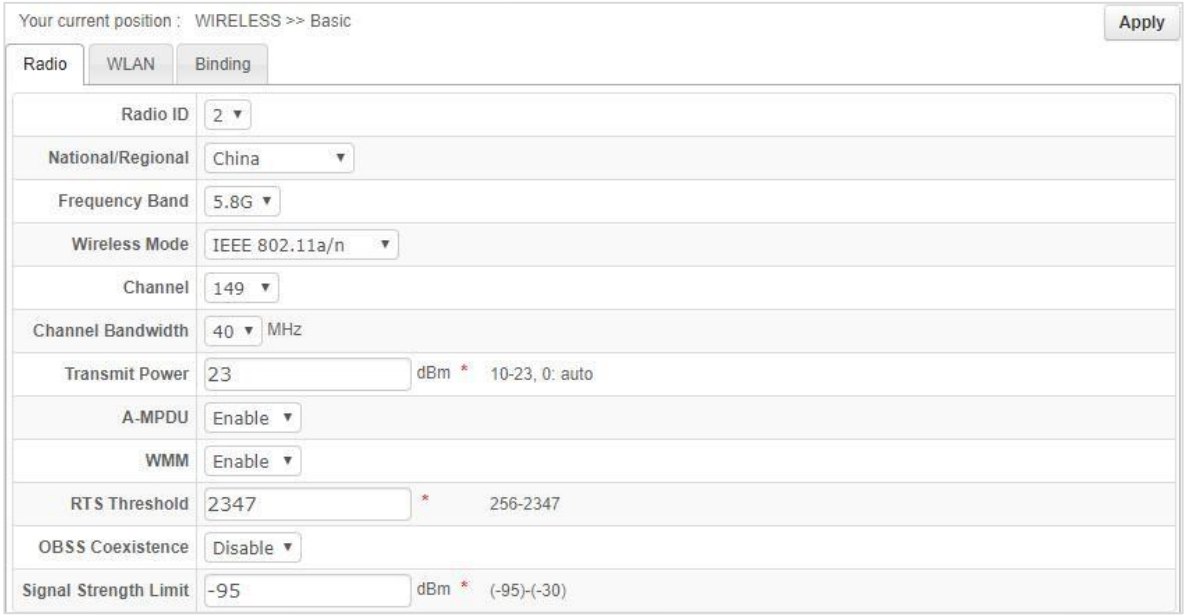

Figure 8-2 RF 2 Information

For specifics of RF configuration parameter, refer to Table 8-1.

Configuration Item	Description
RF ID	Select RF card to be configured, RF 1 is 2.4GHz RF, RF 2 is 5.8GHz RF, shift between different RF configurations by a drop-down list of [RF ID]
Country/Regional	Country of the region of RF information utilized, select “China” or “the United States”
Frequency Band	Select frequency band utilized by RF card
Wireless Mode	Select mode, mode parameters supported by RF 1(2.4G) are: IEEE 11b/g/n, IEEE 11b, IEEE 11b/g; mode supported by RF 2 (5.8GHz): IEEE 802.11a, IEEE802.11a/n
Channel	Channel varies from the openness of frequency band resources of each country. Select suitable work channel from the drop-down list based on frequency plan of your country
Channel Bandwidth	In 11N work mode, the channel bandwidth has two options: “HT20” and “HT40”. HT20 is for compatibility concerns, e.g., if signal of the same frequency exists in a region, to reduce disturbance to them as much as possible, it is required to set up channel bandwidth to be HT20 to reduce frequency band overlay; HT40 is for high performance concerns: HT 40 equals to binding of two HT20s, one is master and the other is slave. Master channel sends beacon message and some data message, slave signal sends other messages
Transmitted Power	Adjust wireless signal transmitting power of products. The higher output power, the wider coverage of wireless signal of the device, but power consumption and disturb to the neighboring device will also be higher
A-MPDU	A-MPDU is aggregation MPDU. Cost is reduced and system throughput is enhanced by sending several MPDUs at a time. There are two options: “On” and “Off”
WMM	Wireless multimedia. It has two options: “Enable” and “Disable”
RTS Threshold	The radio packet transmission request (RTS: Request To Send) for configuring the AP is mainly used to resolve network conflicts. When two sites send data to the AP at the same time, a conflict occurs, which may result in data loss. The RTS threshold is to solve this problem. When the data packet to be sent is greater than the RTS threshold, the RTS mechanism is activated, and the station first sends an RTS to the AP to inform the AP that the data will be sent. When the AP receives the application, it will send a CTS to notify other sites and ask them to postpone the transmission. At the same time, the AP notifies the site that sent the request to send data. The setting range is 0-2346, it is recommended to use the default value
OBSS Coexistence	OBSS sites coexist. Multi-OBSS competition under the MU-MIMO transmission mechanism will form channel preemption and reduce overall throughput. Here, the default shutdown coexistence is set. It is recommended to use the default value
Signal Strength Limit	It is for setting up the signal intensity threshold for allowing sta access. Sta with signal intensity lower than this settings will not be allowed to access to AP

Table 8-1 Parameter Description of RF Card Configuration

8.1.2 WLAN

Create wireless service and set up wireless access information, such as [SSID], [Hidden SSID], [Maximum Number of Connections], [User Isolate], [Encryption Type], as shown in Figure 8-3.

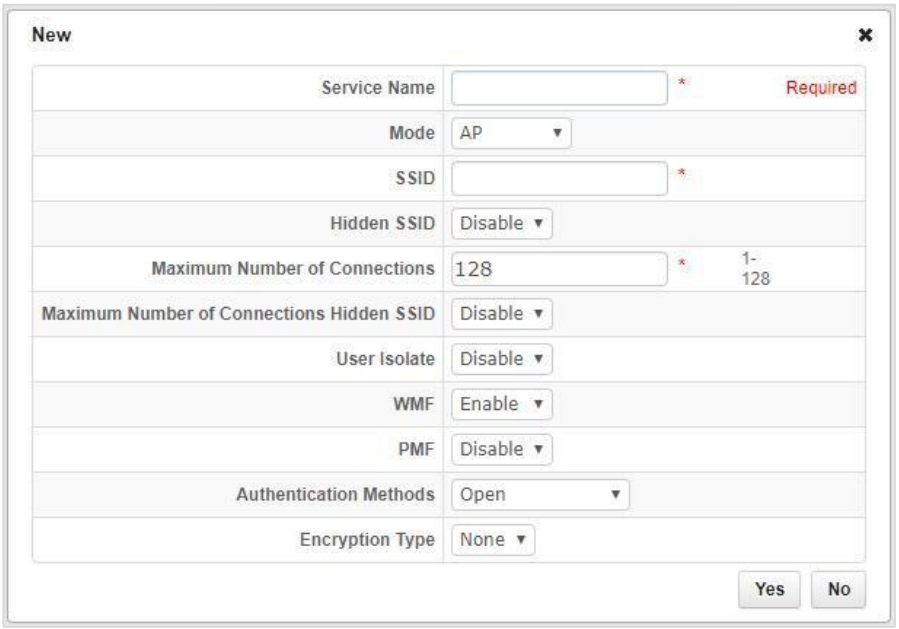

Figure 8-3 Add Wireless Service

Configuration Item	Description
Service Name	Name of wireless service
Visit VLAN	Configure VLAN for wireless service
Mode	AP, WDS AP and WDS STA modes are optional. AP mode is for the regular wireless terminal association; WDS AP mode is for regular wireless terminal and WDS STA mode AP association; WDS STA mode serves as bridge client and only associate to WDS AP
SSID	SSID is a character string for identifying a (virtual) wireless access point. To connect with a (virtual) wireless access point, the wireless terminal should designate the same SSID
Hide SSID	It has two statuses: enable and disable. Select “enable”, AP will not broadcast this SSID; select “disable”, AP will broadcast this SSID
Maximum Number of Connections	Maximum connection number allowed by wireless service
User Isolation	Users under the same wireless service can communicate with each other or not, it has two statuses: enable and disable
WMF	WMF switch, enable by default for improving the multicast result
PMF	Management frame protection encryption

Verification Mode	Carry out WEP, WPA, WPA-PSK, WPA2, WPA2-PSK authentication encryption by setting up wireless encryption parameter configuration
Encryption Mode	Encryption mode changes with verification mode.
Authentication Server	IP of the authentication server. Currently, the mainstream approach is that the portal server and authentication server are on the same computer
Server Port	Authentication port, 1812 by default
Shared Key	Encrypt wireless message based on a shared key, but the shared key is never used for data message encryption directly but for the security of secrete key interactive process of basic secrete key generation between a wireless access point and a wireless terminal. Factors such as basic secrete key and message serial number generate a secrete key for message encryption in the end

Table 8-2 Parameter Description of Wireless Service Configuration

8.1.3 Binding

Bind wireless service with RF ID selected. The device sends wireless signal normally, as shown in Figure 8-4.

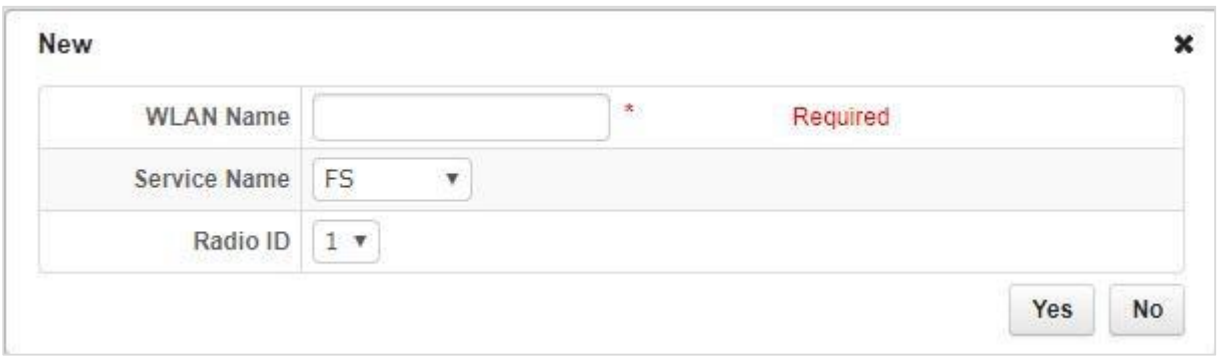

Figure 8-4 Add Wireless Service Binding

Configuration Item	Description
WLAN Name	Designate name bound by this wireless service
Service Name	Name of wireless service pending binding
RF ID	Bind wireless service with RF

Table 8-3 Parameter Description of Wireless Service Binding Configuration

8.2 Access Control

Access control is classified into [Black List] and [White List], as shown in Figure 8-5. It allows receiving or rejecting client connection request according to the MAC address.

Figure 8-5 Black/white List

Configuration Item	Description
Black List	By setting up MAC address, black list rejects STA to visit wireless network and other STA is allowed to visit wireless network
White List	By setting up MAC address, white list allows STA to visit wireless network and other STA is not allowed to visit wireless network

Table 8-4 Parameter Description of Access Control Configuration

Chapter 9 FAT AP Network Settings

9.1 Interface Management

Change AP into [Bridge Mode] or [Route Mode] and configure.

9.1.1 Mode Settings

In [Mode Settings] page, user can select [Bridge Mode] or [Route Mode], as shown in Figure 9-1.

Figure 9-1 Mode Settings

9.1.2 Bridge Mode

In bridge mode, the user manages the device by interfaces created. The system has one management interface [management] by default and VLAN interface with VLAN ID 1, as shown in Figure 9-2. If you need to add new VLAN interface, click add button.

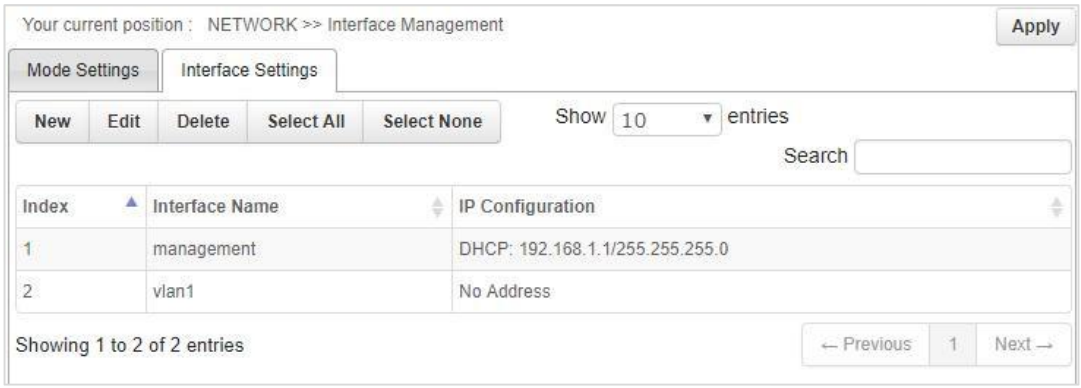

Figure 9-2 Interface Management

9.1.3 Route Mode

In Figure 9-1, select [Route Mode], then click [Interface Settings] tag, route interface configuration page appears, as shown in Figure 9-3.

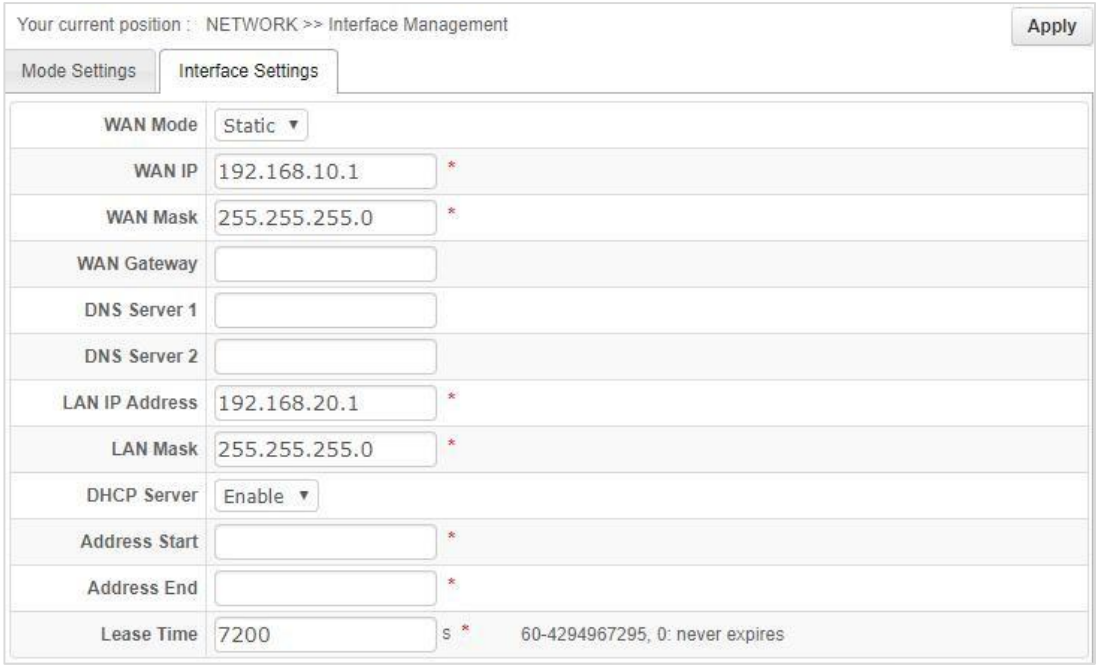

Figure 9-3 Route Interface Configuration

Configuration Item	Description
Management Address	For managing IP address
Management Subnet Mask	Manage the network mask of IP
WAN Connection Mode	Optional connection modes: DHCP, Static and PPPoE
WAN IP Address	Manually designated WAN IP address when WAN connection mode is Static
WAN Subnet Mask	WAN network segment subnet mask manually designated when WAN connection mode is Static
WAN Gateway	Default gateway manually designated for visiting external network when WAN connection mode is Static
DNS Server 1/DNS Server 2	DNS server manually designated for visiting external network when WAN connection mode is Static
User Name	Authentication user name needed by PPPoE dial when WAN connection mode is PPPoE
Password	Authentication password needed by PPPoE dial when WAN connection mode is PPPoE
Timeout	Timeout for the dial as required when WAN connection mode is PPPoE. If it is set as 0, AP will try to keep-alive PPPoE conversation permanently
LAN IP Address	LAN IP address
LAN Subnet Mask	LAN network segment subnet mask
DHCP Server	LAN DHCP server switch. It has two options: “enable” and “disable”
Starting Address	The starting address of LAN DHCP server address pool
End Address	End address of LAN DHCP server address pool
Lease Time	A lease time of LAN DHCP server address

Table 9-1 Parameter Description of Route Interface Configuration

9.2 IPv4 Route

The static route is route information manually configured by the user or network administrator. Application of suitable static route in the network will reduce network cost caused by routing and improve transmission speed of data package.
The static route is generally applicable to the relatively simple network environment in which network administrator is easy to know the topological structure and set up correct route information. One route entry can be determined by set up destination address, network mask, the next hop and hop count. The destination IP address and subnet mask are for confirming a destination network/host and AP will send the data package to next hop of related static route and this next hop will transmit data package.
You may add or delete user-defined static route rule here, as shown in Figure 9-4.

Figure 9-4 Add Static Route

Configuration Item	Description
Destination Address	Destination host address or destination network for identifying IP data message
Network Mask	For identifying network segment of destination host or router with destination address
Next Hop	The next hop address
Hop's Number	Router count between current address to the next hop address

Table 9-2 Parameter Description of Static Route Configuration

9.3 NAT Forwarding

9.3.1 DMZ Service

DMZ (demilitarized zone), "isolated zone", also known as "demilitarized zone". It is to solve the problem that the external network can not access the internal network server after installing the firewall, and set up a buffer between the non-secure system and the security system. This buffer is located in the small network area between the internal network of the enterprise and the external network. In this small network area, you can place some server facilities that must be exposed, such as enterprise web servers and FTP servers.

9.3.2 DMZ Service Configuration

Click [Network] > [NAT Forwarding] > [DMZ Service] to enter the DMZ configuration page. The page is divided into two parts: DMZ Function and DMZ Server IP Address, as shown in Figure 9-5.

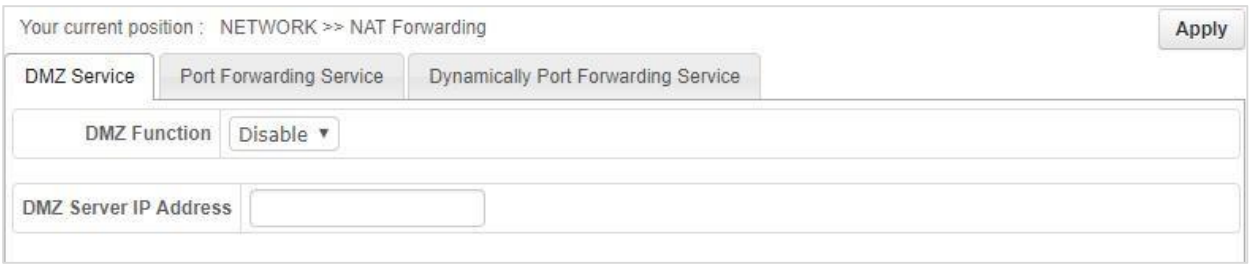

Figure 9-5 DMZ Service

Configuration Item	Description
DMZ Service	Whether to enable the DMZ function, you may select "enable" and "disable"
DMZ Server IP Address	Configure the address of the DMZ server

Table 9-3 Parameter Description of DMZ Service

Note: When the DMZ is set up, the DMZ host is completely exposed to the Internet. Use the DMZ function with caution for security.

9.3.3 Port Forwarding Service

Port forwarding enables access to internal specific servers from an external network. Port forwarding forwards IP packets from the designated port on the public network to the designated port of the private network IP.

For example, a NAT gateway has a WAN side address of 123.4.5.6, an internal FTP server with an address of 192.168.0.8 and a port of 21; an HTTP server with an address of 192.168.0.9 and a port of 8080. Set the port forwarding rule on the NAT gateway:

If the destination address of the IP packet entering the NAT gateway is 123.4.5.6, port 21, the address is translated to 192.168.0.8, port 21, and then forwarded to the intranet; if the destination address of the IP packet entering the NAT gateway is 123.4.5.6, Port 8080; then translates its address to 192.168.0.9, port 8080, and forwards it to the intranet. In this way, by setting port forwarding, the external network can directly access the server of the intranet.

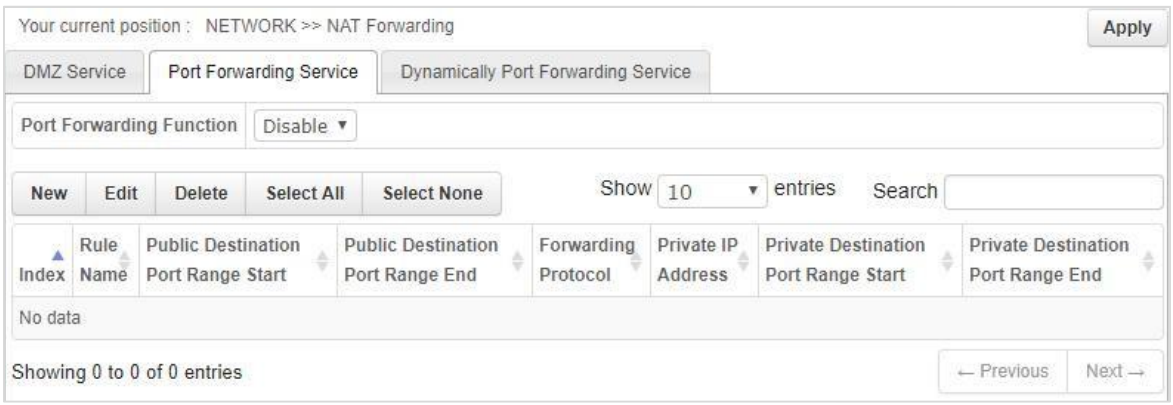

Figure 9-6 Port Forwarding Service

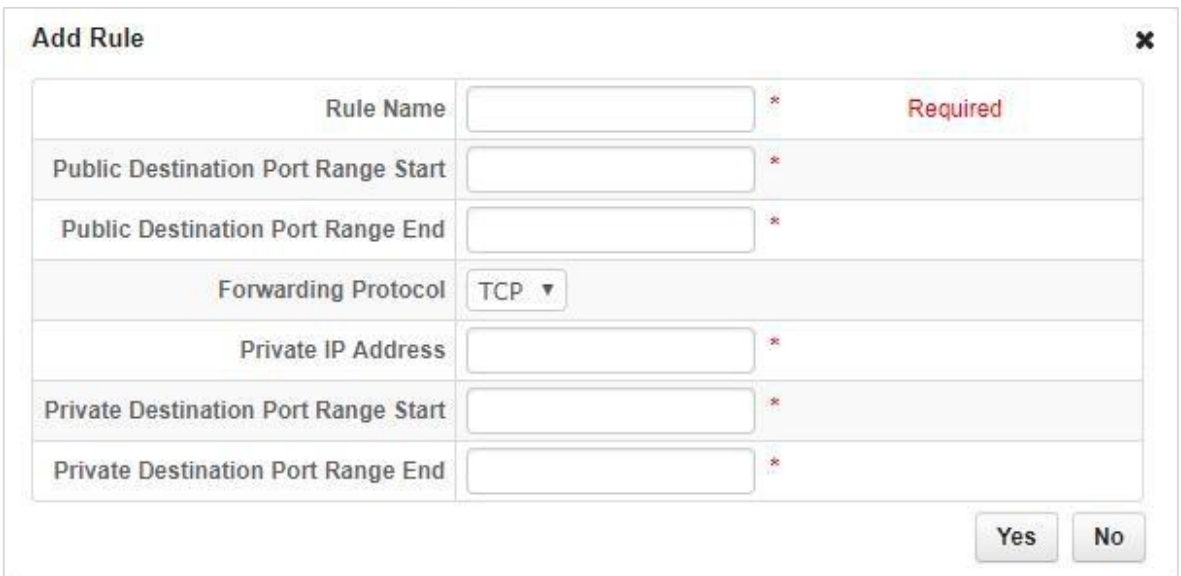

Figure 9-7 Add Rule

Configuration Item	Description
Port Forwarding Function	Port forwarding function switch, select "disable" or "enable"
Rule Name	User can set arbitrarily
Public Destination Port Range Start	Starting port number for the opening to the outside world
Public Destination Port Range End	End port number for the opening to the outside world
Forwarding Protocol	Select the protocol type for forwarding data. There are "TCP" and "UDP" options
Private IP Address	Internal server address
Private Destination Port Range Start	The starting port number of the internal server to create a specific service
Private Destination Port Range End	The ending port number of the internal server to create a specific service

Table 9-4 Parameter Description of Port Forwarding Function

9.3.4 Dynamically Port Forwarding Service

Dynamic port forwarding means that when the flow of the outgoing device comes from the specified internal network trigger port, the device automatically opens the forwarding interface of the WAN-side interface, and forwards the flow whose destination address is the forwarding interface to the specified interface of the internal network trigger terminal. Achieve normal communication.

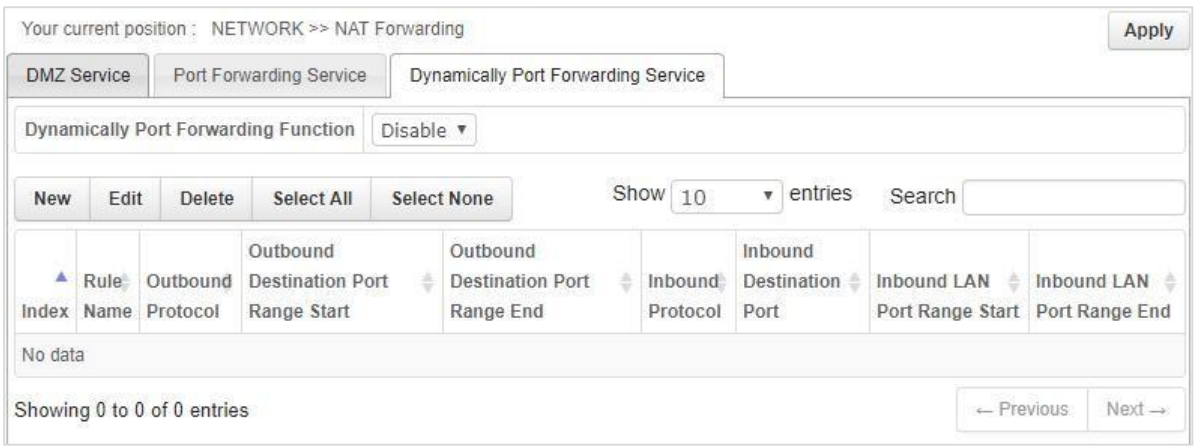

Figure 9-8 Dynamically Port Forwarding Service

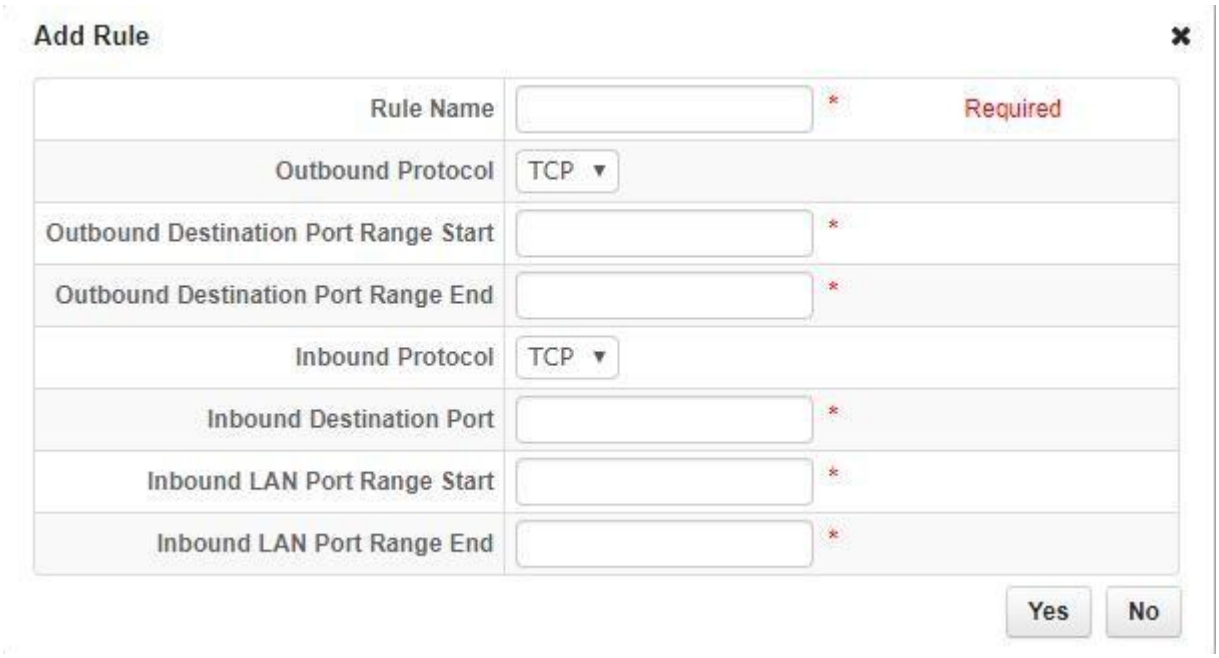

Figure 9-9 Add Rule of Dynamically Port Forwarding Service

Configuration Item	Description
Dynamically Port Forwarding Function	The switch of the dynamic port forwarding function is available with "disable" and "enable"
Rule Name	User can set arbitrarily
Outbound Protocol	The transport protocol used by the outbound forwarding port is available in "TCP" or "UDP"
Outbound Destination Port Range Start	The starting port of the outbound forwarding port
Outbound Destination Port Range End	The destination port of the outbound forwarding port
Inbound Protocol	The transport protocol used by the inbound trigger port is available in "TCP" or "UDP"
Inbound Destination Port	After the port triggers normal communication, the forwarding port forwards the destination port of the data
Inbound LAN Port Range Start	The inbound port triggers the start port of the port
Inbound LAN Port Range End	The end port of the inbound trigger port

Figure 9-5 Parameter Description of Dynamically Port Forwarding Service

Chapter 10 Security Settings

10.1 Access Control

Filter data package of some designated IP address within certain time. There are two types of filtration modes: forbid access and allow access. ACL rule addition has two approaches: link layer ACL and advanced ACL. Access control page is shown in Figure 10-1.

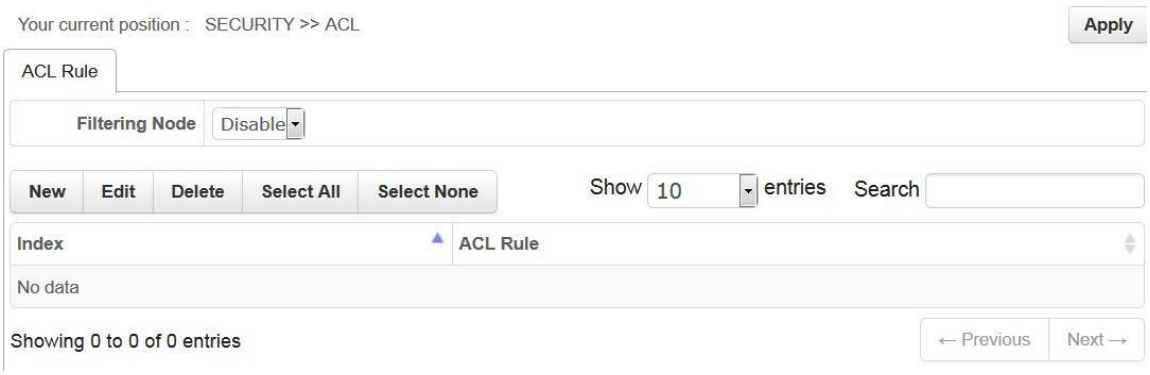

Figure 10-1 Access Control

10.1.1 Link layer ACL

Link layer ACL, fill in MAC address, this ACL rule will be effective permanently.

Figure 10-2 Link layer ACL

10.1.2 Advanced ACL

Advanced ACL provides access control based on IP address field, protocol and port and designates time frame for rules to be effective.

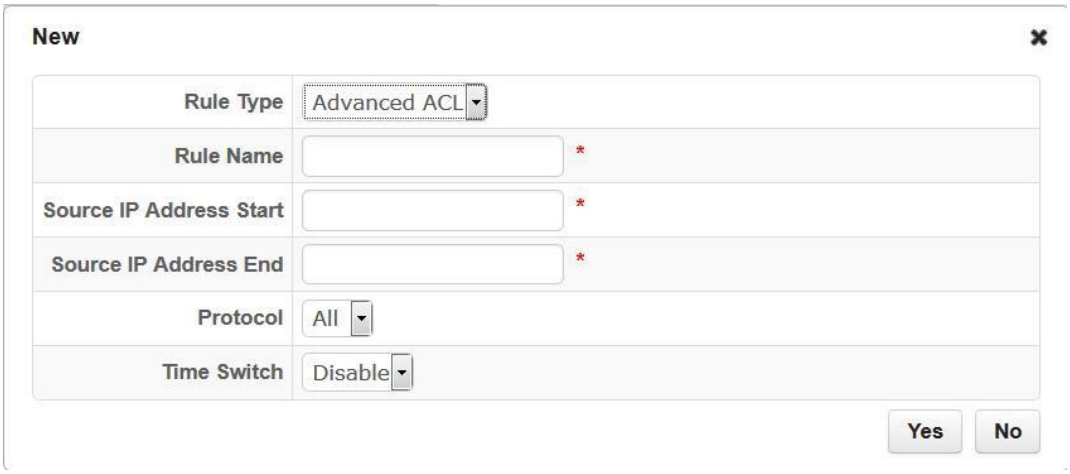

Figure 10-3 Advanced ACL

Configuration Item	Description
Filtration Mode	Enable access control function or not, you may select “forbid”, “forbid access” and “allow access”
Rule Type	Select type of ACL rule, you may select “link layer ACL” and “advanced ACL”
Source MAC Address	Restricted host mac address designated during link layer access control
Rule Name	Name of advanced ACL rule, user may define rule name to identify different rules
Source IP Address Start	Host start IP address of access control rule
Source IP Address End	Host end IP address of access control rule
Protocol	Designate protocol type restricted by rule, there are two types: “TCP” and “UDP”
Start Destination Port	Designate start destination port applicable to ACL rule
End Destination Port	Designate end destination port applicable to ACL rule
Starting Week	Designate week for rules to take effective
End Week	Designate end week for rule to take effective
Starting Time	Designate time for rule to take effective
End Time	Designate time for rule to end

Table 10-1 Parameter Description of Access Control

10.2 Whitelist

The whitelist function is used for wireless side network access control. After the whitelist is enabled, wireless users can only access domain names in the whitelist. Whitelist page is shown in Figure 10-4.

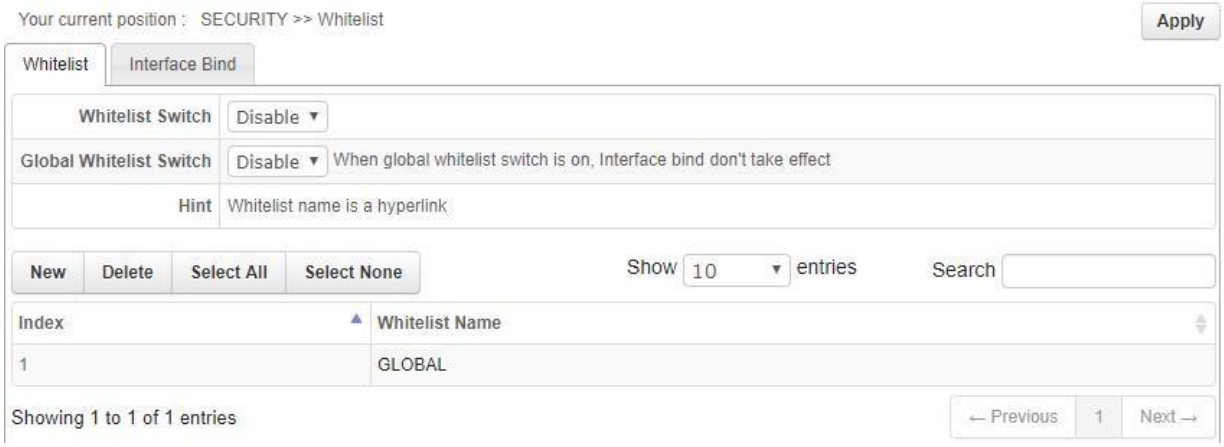

Figure 10-4 Whitelist

10.2.1 Whitelist Switch

The user can choose to validate the whitelist for an interface or take effect globally. For an interface, it refers to the wireless interface.

Figure 10-5 Whitelist Switch

Configuration Item	Description
Whitelist Switch	Select “Enable” to enable whitelist configuration on the corresponding interface
Global Whitelist Switch	Select "Enable", [Whitelist Switch] is invalid, and whitelist configuration is enabled for all interfaces by default

Table 10-2 Whitelist Switch

10.2.2 Add Whitelist Configuration

Click the "New" button to create a whitelist entry and configure a domain name whitelist under the created entry.

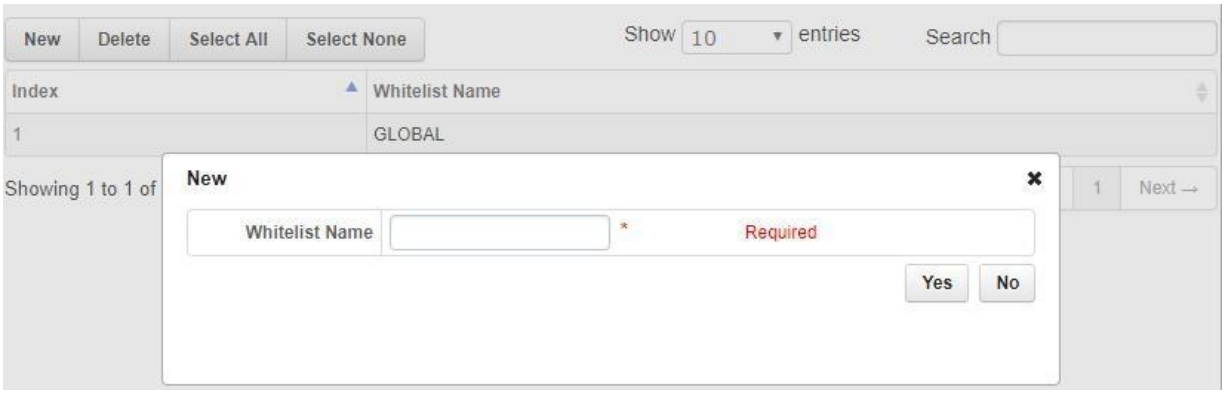

Figure10-3 Whitelist Name

Configuration Item	Description
New	Create a new whitelist entry with a custom name
Delete	Delete selected whitelist entries
Select All	Select all whitelist entries that have been created
Select None	Cancel all selected whitelist entries

Table 10-3 Whitelist Switch

10.2.3 Interface Bind

Bind the created whitelist to the corresponding interface.

Figure 10-4 Interface Bind

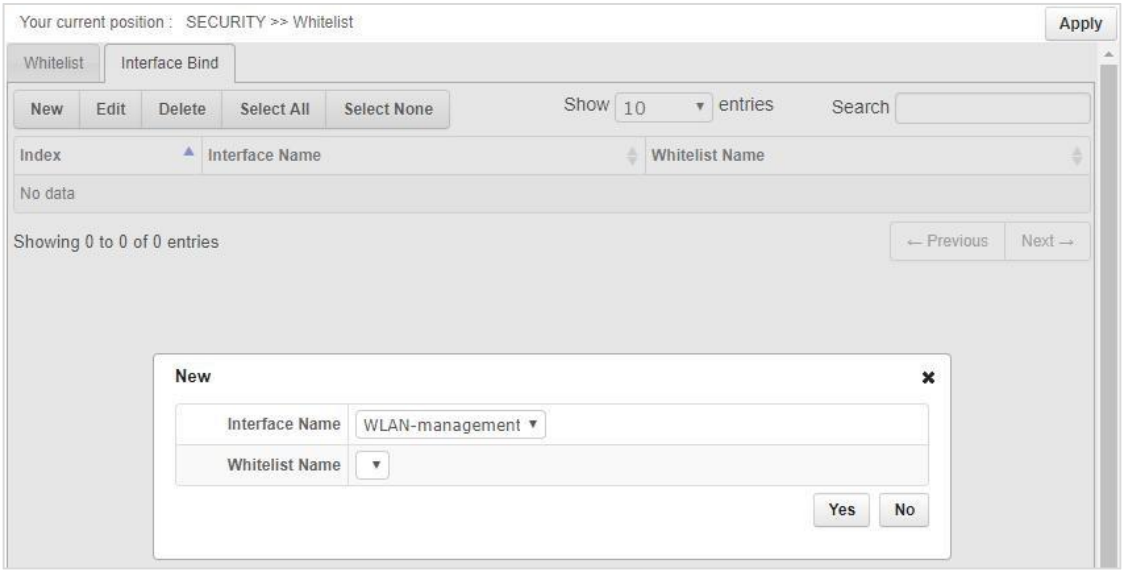

Figure 10-8 Whitelist Name

Configuration Item	Description
New	Create a new entry, bind the corresponding interface
Edit	Edit selected entries
Delete	Delete selected entries
Select All	Select all entries that have been created
Select None	Cancel all selected entries
Interface Name	Select the configured wireless interface
Whitelist Name	Select the configured whitelist entry

Table 10-4 Whitelist Switch

Chapter 11 Expand Application

11.1 WiFi Positioning

The AP includes the WIFI location function. After the corresponding [Type] is selected, the AP scans the surrounding WIFI terminal and sends the WIFI terminal information to the location server, but the location server and the AP are connected through the Ethernet. The WIFI positioning of the AP is based on the WEB interface management, and can display the alarm information of the WIFI tag, such as button alarm, low voltage alarm, etc., and can also locate the location information of the WIFI terminal, as shown in Figure 11–1.

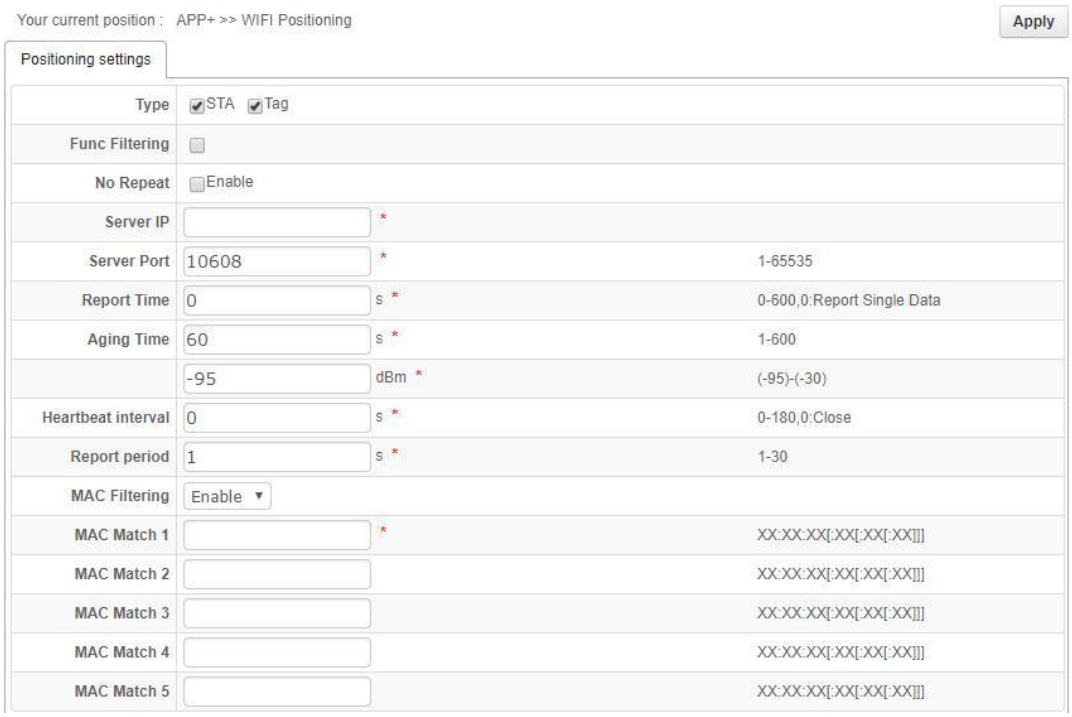

Figure 11-1 WiFi Positioning

Configuration Item	Description
Type	Set the type of WIFI positioning, there are two types of "STA" and "Tag", "STA" is the location of the specified WIFI client; "Tag" is the specified bit WIFI tag information
Func Filtering	High performance function switch
No Repeat	Re-switch
Server IP	The address of the server that receives the scanned information
Server Port	The server port that receives the scan information
Report Time	Terminal reporting interval
Aging Time	De-aging time
Heartbeat Interval	Refers to the heartbeat interval between the AP and the WIFI location server
Report Period	The interval at which the AP reports the WIFI positioning label information
MAC Filtering	The AP can filter only the WIFI terminal of a specific MAC by setting the MAC address filtering. It can be enabled or disabled
MAC Match	The AP only scans the WIFI terminal of a specific MAC

Table 11-1 Parameter Description of WiFi Positioning Page

11.2 Scan

AP allows enable rogue AP scan and counter function by page, as shown in Figure 11-2, which contains four pages: [Scan settings], [Rogue AP Settings], [Rogue AP List] and [Rogue AP White List].

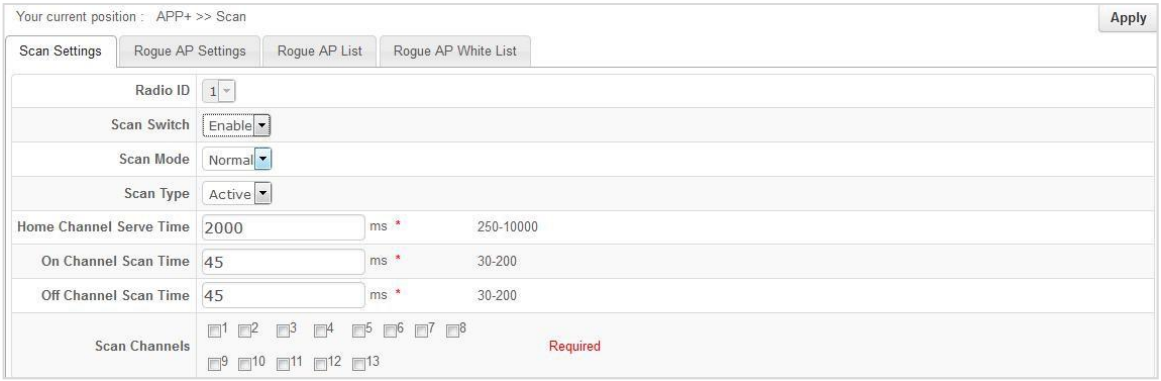

Figure 11-2 Scan

11.2.1 Scan Settings

[Scan Settings] page contains settings such as [Scan Switch], [Scan Mode], [Scan Type], [Home Channel Service Time], [On Channel Scan Time], [Off Channel Scan Time] and [Scan Channels], refer to Figure 11-2.

For parameter description of [Scan settings], refer to Table 11-2.

Configuration Item	Description
RF ID	Select RF ID to set up
Scan Switch	Set up scan on/off, you may select “enable” and “disable”
Scan Mode	Select AP mode when scanning: work mode and monitor mode. In work mode, AP scans and provides client access at the same time; in “monitor mode”, AP is for scan monitoring only and client access function is not available
Scan Type	There are two types of scan: “active scan” and “passive scan”. In “active scan” mode, AP will send prove request and scan; in “passive scan” mode, AP monitors beacon information in the area
Home Channel Service Time	Set up AP service time in work channel
On Channel Scan Time	Set up AP scan time in work channel
Off Channel Scan Time	Set up AP scan time in the non-work channel
Scan Channels	Set up channel set scanned by AP

Table 11-2 Parameter Description of Scan Setting Page

11.2.2 Rogue AP Settings

When AP starts to scan, it needs to enable [Rogue AP] in [Rogue AP Settings], then make statistics of rogue AP and counter, setup page is shown in Figure 11-3.

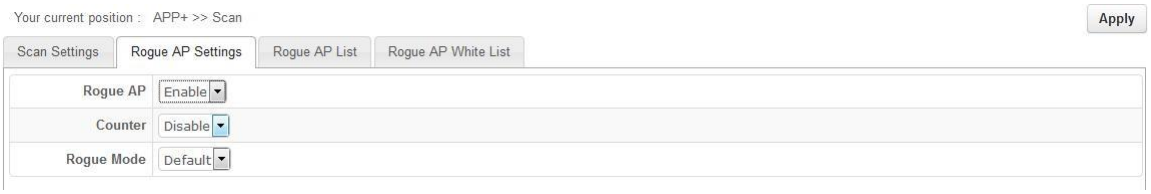

Figure 11-3 Settings of Rogue AP

Parameter description of [Rogue AP Settings] is shown in Table 11-3.

Configuration Item	Description
Rogue AP	Rogue AP statistics switch: “enable” and “disable”
Counter	Set up if enable rogue AP counter or not, you may select “enable” and “disable”
Rogue Mode	Set up rogue AP identification mode. By default, AP will consider AP which has different prefix of AP MAC address as rogue AP; in “fishing AP” mode, AP will consider AP which has the same SSID as rogue AP

Table 11-3 Parameter Description of Rogue AP Settings

11.2.3 Rogue AP List

[Rogue AP List] shows rogue AP information scanned, as shown in Figure 11-4. User may select designated rogue AP and click <Add to White List> to add rogue AP to the white list.

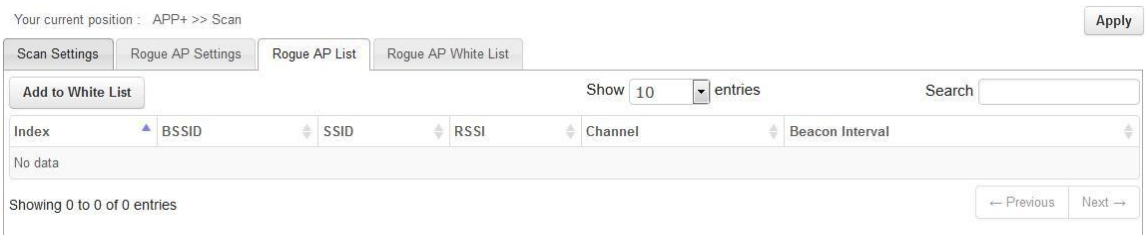

Figure 11-4 Rogue AP List

11.2.4 Rogue AP White List

[Rogue AP White List] page displays AP list on the white list, as shown in Figure 11-5. AP on this list will not be considered as rogue AP. When the rogue AP counter is enabled, it will not counter AP on the white list.

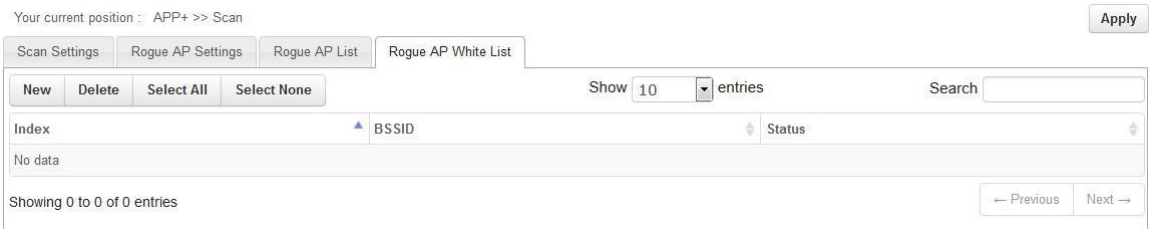

Figure 11-5 Rogue AP White List

On [Rogue AP White List], you can add or delete rogue AP white list manually. Add method:

Click <New> button, then input BSSID of rogue AP on the page which pops out, after input, click <Confirm> to add. After add, click <Apply> on this page. Add page is shown in Figure 11-6.

Figure 11-6 Add Rogue AP White List

Parameter description of add rogue AP white list is shown in Table 11-4.

Configuration Item	Description
BSSID	Add BSSID of rogue AP

Table 11-4 Parameter Description of Rogue AP White List

11.3 BandSteer

The [BandSteer] page is used to set the dual-frequency terminal navigation to the 5G radio. The navigation must be configured with the same SSID and encryption method for the 2G and 5G radios.

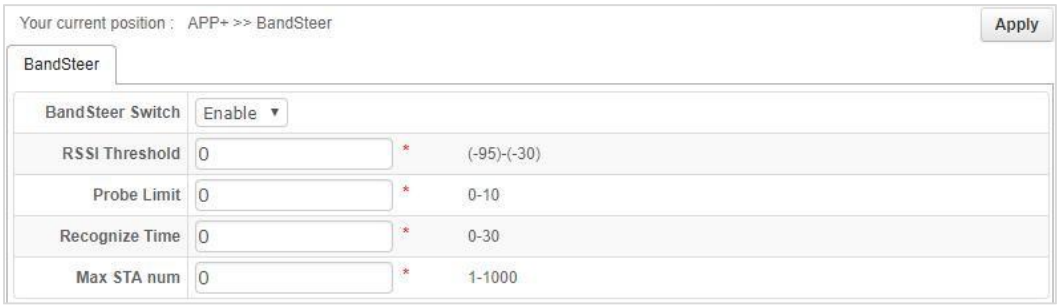

Figure 11-7 BandSteer

Configuration Item	Description
BandSteer Switch	5G navigation switch
RSSI Threshold	Navigate when the value is above the threshold (not currently supported)
Probe Limit	The probe request of the terminal is not responded during navigation
Recognize Time	The time to identify whether the terminal is dual-frequency or single-frequency. It is recommended for 20s
Max STA Num	The maximum number of 5G radio frequency. no navigation is carried out when the maximum limit is exceeded(not currently supported)

Table 11-5 Parameter Description of BandSteer

11.4 E-SchoolBag

[E-schoolBag] is configured to optimize the transmission quality of the electronic schoolbag application scenario. It is closed by default. For non-electronic schoolbag application scenario, please use the default value.

Figure 11-8 E-SchoolBag

Chapter 12 Service Management

12.1 QOS

[QOS] page is for setting up/down bandwidth limitation based on port and up/down bandwidth limitation based on users, as shown in Figure 12-1.

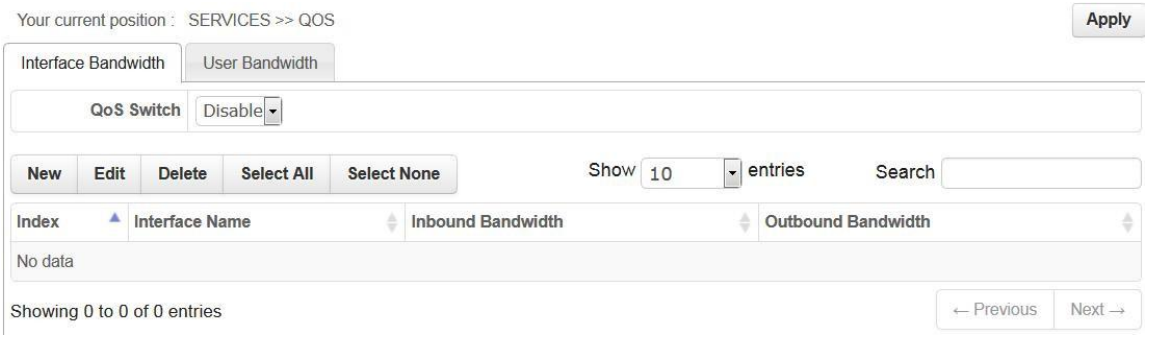

Figure 12-1 QOS

12.1.1 Interface Bandwidth

[Interface Bandwidth] is for setting up bandwidth control based on interface, as shown in Figure 12-1, user can add, edit and delete interface bandwidth configuration rule on this page.

Page of add interface bandwidth rule is shown in Figure 12-2.

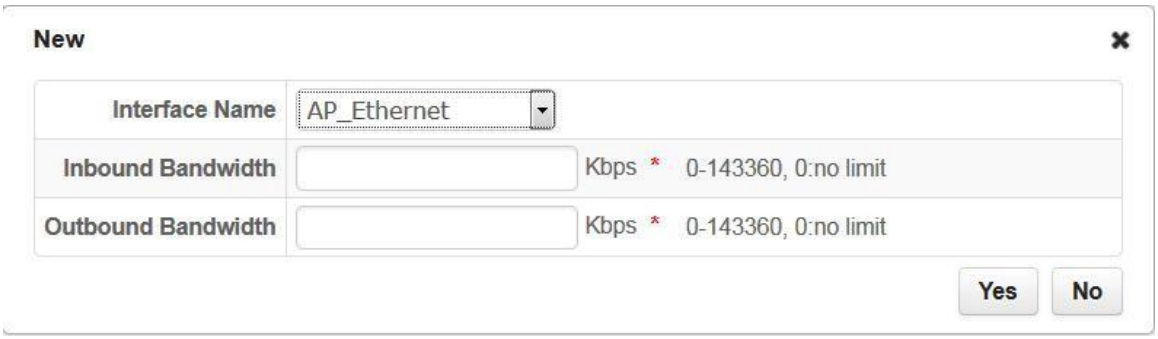

Figure 12-2 Add Interface Bandwidth

Parameter description of [Interface Bandwidth] is shown in Table 12-1.

Configuration Item	Description
Service Quality Switch	Switch for service quality management: “enable” and “disable”
Interface Name	Designate interface which needs to configure interface bandwidth
Inbound Bandwidth	Set up inbound interface bandwidth
Outbound Bandwidth	Set up inbound interface bandwidth

Table 12-1 Parameter Description of Interface Bandwidth

12.1.2 User Bandwidth

[User Bandwidth] is for setting up bandwidth control based on user, as shown in Figure 12-3. User can add, edit and delete user bandwidth configuration rules on this page.

Figure 12-3 User Bandwidth

Page of add interface bandwidth rules is shown in Figure 12-4.

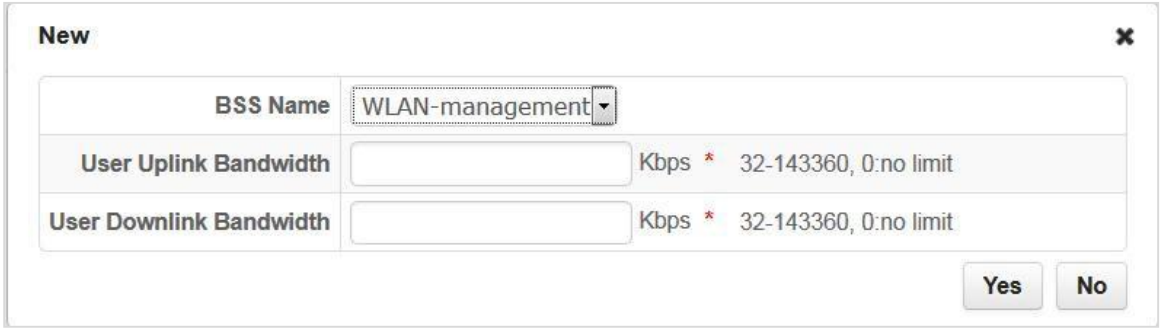

Figure 12-4 Add Interface Bandwidth

Parameter description of [User Bandwidth] page is shown in Table 12-2.

Configuration Item	Description
BSS Name	Set up name of BSS which needs to configure user bandwidth
User Uplink Bandwidth	Set up user uplink bandwidth
user Uplink Bandwidth	Set up user downlink bandwidth

Table 12-2 Parameter Description of User Bandwidth Page

12.2 Remote Access

When the AP works in the routing mode of FAT AP, the remote access device page needs to use the access port, the default HTTP access port is 8080, HTTPS access is 8443, the user can customize open HTTP access and HTTPS access on this page and specify the corresponding port number, as shown in Figure 12-5.

Figure 12-5 Remote Access

Configuration Item	Description
HTTP	HTTP access switch, you may select “enable” or “disable”
HTTP Port	Specify the port for HTTP access
HTTPS	HTTP access switch, you may select “enable” or “disable”
HTTPS Port	Specify the port for HTTP access

Table 12-3 Parameter Description of Remote Access

12.3 SSH Settings

AP opens SSH access by default. User may visit AP command line by SSH. Configuration page is shown in Figure 12-6.

Figure 12-6 SSH Settings

Configuration Item	Description
Enable SSH	SSH access switch, you may select “enable” or “disable”
Timeout	Set up timeout of SSH access

Table 12-4 Parameter Description of SSH Settings

12.4 DHCP SNOOP Settings

The DHCP SNOOP configuration applies to panel APs, and the non-panel APs use default values.

Figure 12-7 Telnet Settings

12.5 Telnet Settings

AP enables [Telnet] by default. User may visit AP command line by Telnet. Configuration page is shown in Figure 12-8.

Configuration Item	Description
Enable Telnet	Telnet access switch, you may select “enable” or “disable”
Timeout	Set up timeout of Telnet access

Table 12-5 Parameter Description of Telnet Settings

12.6 Log Management

[Log] needs to open external tftp server. Fill in [Log Server] and [Log Server Port] on [SERVER] >[Log] page, as shown in Figure 12-8. System log will be sent to related tftp server.

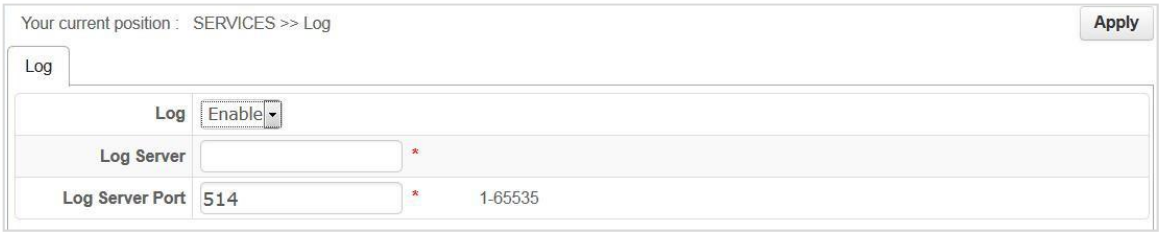

Figure 12-8 Log Management

Configuration Item	Description
Log	Enable log management function or not. You may select “enable” or “disable”
Log Server	IP address of log server

Table 12-6 Parameter Description of Log Management Configuration

Chapter 13 FAT AP Device Management

13.1 System Configuration

Configure [System Name] and [Device Location], as shown in Figure 13-1.

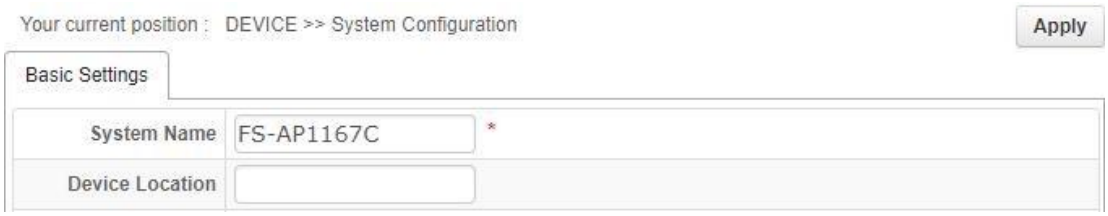

Figure 13-1 System configuration

Configuration Item	Description
System Name	Configure system name
Device Location	Configure device location

Table 13-1 Parameter Description of System Configuration

13.2 Time Settings

Set up system local time, as shown in Figure 13-2.

Figure 13-2 Set Up Time Manually

Figure 13-3 Automatic Synchronization Time

Configuration Item	Description
Synchronization Mode	Configure system time synchronization mode. You may select “manual” or “automatic”
System Time	Configure system time
Synchronizing Interval	Cycle for system automatic synchronization
Primary NTP Server	Set up the IP address of NTP Server. NTP Server is a network time server for synchronizing computer time on the internet
Secondary NTP Server	When NTP server 1 is not available, the system synchronizes with NTP server 2

Table 13-2 Parameter Description of Time Settings

Note：

• NTP (Network Time Protocol) provides router, switch and workstation with time synchronization. Time synchronization links event records on multiple network devices for the purpose of analyzing complicated malfunction and security events.

• The time limit of other functions of AP (such as a firewall) takes effect only when GMT time is acquired by Internet or system time is set up manually.

13.3 User Management

User can control access to the management page by modifying the administrator password and adding new user, as shown in Figure 13-4. When adding user, there are three types of user roles: “visitor”, “administrator” and “system administrator”. “Visitor” has the lowest access level and can check system information only; “administrator user” can check and perform regular settings, but can’t perform senior settings such as user management; “system administrator” has the highest access level.

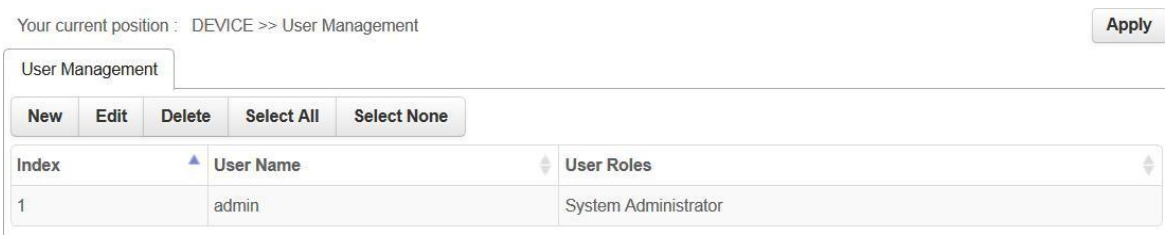

Figure 13-4 User Management

13.4 Configuration Management

[Configuration Management] divides into two parts: [Import] and [Export].

Select menu [Configuration Management] > [Import]/[Export], you can export or import AP configuration files.

With [Export] function, you can save AP configuration in computer in form of files for use in the future; before upgrading AP software or loading new configuration files, backup original configuration of AP to prevent configuration loss in process of software upgrading or loading new configuration files.

With [Import] function, you can re-import configuration files saved or edited before.

If you need to configure the same settings for multiple APs, you can configure one AP first, save its configuration file, then import it to other AP. It saves configuration time.

When device parameters are configured, you can back up this configuration information. In the event of device breakdown, it will restore to the status before backup. Open [Export] page, click <Export>, the dialog box of saving file appears. Operate as instructed will backup configuration parameters. If you want to import, just click [Import configuration], designate files you want to recover, then click <Import>, the configuration in files will be written into the device again.

13.4.1 Import Configuration

Figure 13-5 Import Configuration

13.4.2 Export Configuration

Figure 13-6 Export Configuration

Note:

After loading configuration files, original configuration information in the device will disappear, therefore, please backup configuration before importing configuration files. If configuration files loaded is wrong, you can reload backup files.

Do not turn off AP in the process of loading configuration files, otherwise, it will cause damage to AP and make it unable to function. Size of files loaded and configuration command accuracy will impact the time needed by the loading process. If the load is done without error, AP will restart automatically. If there is an error in loading, please select if you want to save the configuration or not based on prompt information. It is recommended to restart AP.

13.5 Device Maintenance

13.5.1 Restart Device

Click <Restart> to restart the device, as shown in Figure 13-7.

Figure 13-7 Restart Device

13.5.2 Restore to Factory Settings

Click <Restore> to restore factory settings by software, as shown in Figure 13-8.
For restoring factory settings by hardware, when the device is on, press "Reset" longer than 5s, device will be restored to the default value.

Figure 13-8 Restore Factory Settings

Note:
1. All settings of AP will be restored to the factory default value, which
Default user name: admin
Default password: admin
Default IP address: 192.168.1.1
Default subnet mask: 255.255.255.0
2. Please backup configuration information before restoring factory settings. Restore AP configuration by loading backup configuration when necessary.

13.5.3 Version Upgrade

Steps to upgrade version:
Step 1: Get the latest version from technical support department of our company. This mirror image document must be comboImage update mirror image document.
Step 2: Version mirror image. Click <Browse>, select document to upgrade, then click <Upgrade>, as shown in Figure 13-9.
Step 3: The page shows upgrade progress prompt bar. After upgrade, log in [Device information] page again to inspect software version number and confirm if upgrade is done.

Figure 13-9 Version Upgrade

Appendix Troubleshooting

Q 1. How to know the MAC address of the device?

MAC address is the unique identification of network device. There are two ways to find out the MAC address:

1. Each device has a small tag on the bottom which shows the device MAC address.
2. You may log in the device Web management page, check basic information of the device and know the MAC address of wireless access point.

Q 2. Why STA is unable to connect with AP?

Generally, STA connection can only be done after AP search, authentication and connection, therefore, if STA is unable to connect with AP, try the following approaches:

• If channel supported by STA is the same as AP. If AP uses channel incompatible with STA, then STA will be unable to find AP. You can change the AP channel.

• STA does not use the same authentication and encryption mode as AP. If their authentication and encryption mode are inconsistent, STA will not be able to pass authentication and it will cause connection failure.

• Disturb from similar devices. Check if there is a wireless device nearby, if possible, try to turn off other device and check if the problem is solved. Shield or adjust the position of devices which causes interference.

• Disturb by other devices. Check if there are interference sources nearby, such as microwave oven, 2.4G and other high power devices which will have big impact on device operation. If possible, try to turn off other devices and check if the problem is solved.

• Compatibility between STA and AP. STA may be non-conform to 802.11 protocol specifications, therefore it is unable to connect with AP.

Q 3. Why bandwidth is not high after the wireless network connection is established?

The problem that device bandwidth is not high is mostly caused by environmental disturbance or device aging or reduction of sending power. You can try the following approaches:

• Wireless channel: try to select other channels, the rate may be enhanced obviously;

• Wireless disturb. Check if there is a wireless device nearby, if possible, try to turn off other device and check if the problem is solved. Shield or adjust the position of devices which causes interference.

• Check antenna. Check if the antenna is loose.

• Check signal intensity. Check signal intensity for STA connecting with AP. If it is weak, the antenna may be loose or device aging, or sending power reduction.

• Check the network card. It is possible that the network card itself has extremely low power. You can go near AP and test bandwidth.

Q 4. Why it is unable to connect when the bridge configuration of two devices is done?

Check the following parameter configuration of these two devices:

• If both “connection mode” are “bridge”?

• If remote MAC address added is correct?

• If their “country/region” settings are the same?

• If their “channel/frequency” settings are the same?

• If their “encryption mode” settings are the same?

Q 5. Wireless network functions well after establishment, but the link shows instability after some time, such as delay increase and packet loss?

This may be caused by the fact that the wireless environment of the device is interrupted. You can solve this problem by the following steps:

• Check if each part of the device is connected well (such as wired cable connection and antenna connection)

• Restart devise after power off;

• Re-configure after device restores default settings;

• Check if wired and wireless devices of AP are attacked by virus;

If the problem still exists, please consult the sales agent.

Q 6. For two bridged devices, if configure remote devices by a wireless link from near end, why WEB page of the remote device can't open?

That is because the wireless configuration device may cause remote device Web Server to show slow response. Wait for about 3 minutes or restart remote device will solve this issue; we suggest configure device at the wired end.

Q 7. What to do if I forget user name and password of the router (How to reset router)?

If you forget user name and password of the router, the only solution is reset router to factory default settings. There is a RESET button on the rear panel of the router. When powering on, press RESET key and hold for 5seconds, release when system status indicator flashes. It means the device is reset.

Notes: after reset, default login IP of the router is 192.168.1.1, default user name/password is admin/admin. When logging in, please make sure the IP address of the computer is in 192.168.1.X (X can be any integer from 2 to 252) network segment.

https://www.fs.com