LIGOWAVE - WAC/VAC/LAC QUICK GUIDE

(Version:1.0)

(Created Date:2015.03.28)

NOTE: This Quick Guide is based on the basic and frequently-used functionality of VAC/WAC/LAC, and add a number of basic cases configuration process. If you have any problems, please contact our customer service staff.

Contents

1. Chapter 1
Basic System Configuration

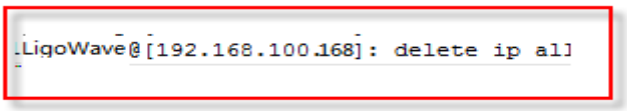
1.1. The Initial Configuration of VAC/WAC/LAC/AP

The most direct way to configure is connecting your laptop to the VAC / WAC / LAC through console port. We need a remote management software such as "putty" or "Xshell" to configure via command line, people who have technical knowledge and experience are recommended to do so. General users can also configure via the web interface, please refer to Section ***1.2.***

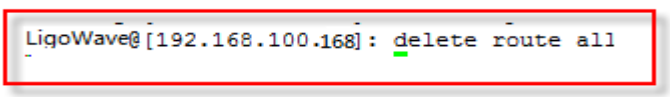
(NOTE: LAC has no web interface, so the section before getting online to VAC should be configured through the console port.)

1.1.1. The Initial Configuration of VAC/WAC

- The default management address of VAC/WAC (on port 1) is 192.168.100.168. Connect the PC to the VAC / WAC via serial cable then we can modify physical interface address of the VAC/WAC.
- Use remote management software (e.g putty/xshell) on the PC to manage the WAC by username **admin** and password **admin0.1**.
- The baud rate is 9600.
- Use the command "**delete ip all**" to delete all IP of the WAC, as shown below:



- Use the command "**delete route all**" to delete all route of the WAC:



- Add IP and route for Port0/1 and enable the control and admin rights, use the following commands:

Add port IP:

Add ip 0/1 192.168.100.21 255.255.255.0 control on admin on

Add default route:

add route 0.0.0.0 0.0.0.0 192.168.100.1

```
LigoWave@[192.168.100.168]: add ip 0/1 192.168.100.21 255.255.255.0 control on admin on
LigoWave@[192.168.100.168]: add route 0.0.0.0 0.0.0.0 192.168.100.1
```

- Add IP for Port0/2, use the following command:

```
LigoWave@[192.168.100.168]: add ip 0/2 1.1.1.1 255.255.255.0 admin on
LigoWave@[192.168.100.168]:
```

- Except Port0/1, others are downlink ports by default. In order to manage the VAC/WAC through Port0/2, the port 0/2 being set to uplink is necessary, use the following command:

```
LigoWave@[192.168.100.168]:set port 0/2 uplink
```

- Save system configuration and reboot the WAC, use the following commands: **save main, reboot**

```
LigoWave@[192.168.100.168]: save main
 saving configuration....
save configuation success
LigoWave@[192.168.100.168]: reboot

  This operation will temporarily shutdown this system and users may
  lose their connections.

  Are you sure you want to shutdown this system [n]?  y
```

1.1.2. The Initial Configuration of LAC

- Manage the LAC through the serial port. The default management address of LAC on port 0/1 is 192.168.100.169, can be modified via CLI
- Use remote management software (e.g putty/xshell) on PC to manage the LAC by username **admin** and password **admin0.1**

- Configure the IP address for the LAC and specify the VAC IP for it through the serial port, the baud rate is 9600
- Use the command "**delete ip all**" to delete all IP of the LAC, as shown below:

```
LigoWave@[192.168.100.169]: delete ip all
```

- Use the command "**delete route all**" to delete all route of the LAC:

```
LigoWave@[192.168.100.169]: delete route all
```

- Add IP and route for port0/1 and enable the control and admin rights by using the following commands:

Add port IP:

Add ip 0/1 192.168.100.20 255.255.255.0 control on admin on

Add default route:

add route 0.0.0.0 0.0.0.0 192.168.100.1

```
LigoWave@[192.168.100.169]: add ip 0/1 192.168.100.20 255.255.255.0 control on admin on
LigoWave@[192.168.100.169]: add route 0.0.0.0 0.0.0.0 192.168.100.1
```

- Specify the controlserver-VAC IP for the LAC by using the command"**set controlserverx.x.x.x**", as shown below:

```
LigoWave@[192.168.100.169]: set controlserver 192.168.100.21
```

Note:The above command is to specify the VAC IP which the LAC belongs to.

- Save configuration and reboot the LAC by using the commands: "**save main**" and **"reboot"(y=yes, n=no)**, as shown below:

```
LigoWave@[192.168.100.169]: save main
 saving configuration....
save configuation success
LigoWave@[192.168.100.169]: reboot

  This operation will temporarily shutdown this system and users may
  lose their connections.

  Are you sure you want to shutdown this system [n]?  y
```

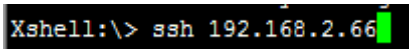
1.1.3. The Initial Configuration of AP

When the AP is connected to a DHCP network it will automatically obtain an IP address and discover the AC through broadcast. In general local applications, we do not need to specify the WAC IP address for the AP; on the other hand, we can also specify the WAC/VAC IP address for the AP, and in certain environments ***(AP to AC cross-NAT)***, we have to specify the WAC/VAC IP address for the AP.

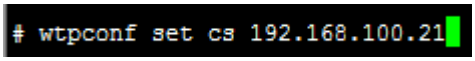
- The initial configurations of AP are as shown below:

When the AP is powered up it will by default broadcast the SSID "Ligo_mac", as shown below:

Connect your laptop to the SSID and manage the AP through SSH (use SSH software like Xshell), the management ip is 192.168.2.66, as shown below:



Follow the prompts to enter username: admin and password:admin01. After login successfully, type "shell" at the command line and press enter, use the following command to specify the remote VAC/WAC IP(for example:192.168.100.21) address for the AP:



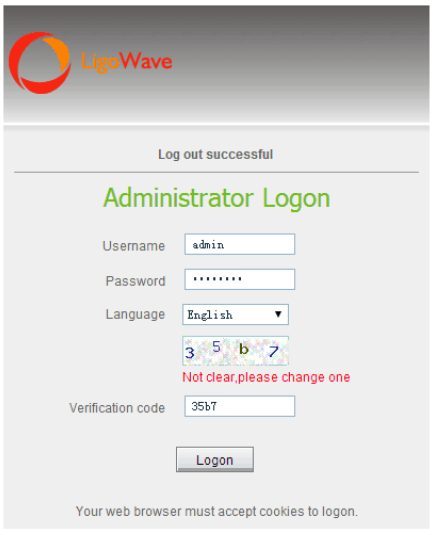
Have the AP connected to the network after the completion of the above steps

1.2. Configure the VAC/WAC through web interface

The Device module is for making basic configuration of VAC/WAC, including Basic Setup, DNS Server, Ports, IP, Route, Policy Route, OSPF, DHCP, SNMP, Date&Time.

1.2.1. First Login

Connect your laptop to the VAC/WAC via port0/1, access *https://+port IP* from the browser, The default management IP of the VAC/WAC is 192.168.100.168(on port 0/1), so access*https://192.168.100.168* from the browser, then enter the username and password to login (admin, admin0.1):

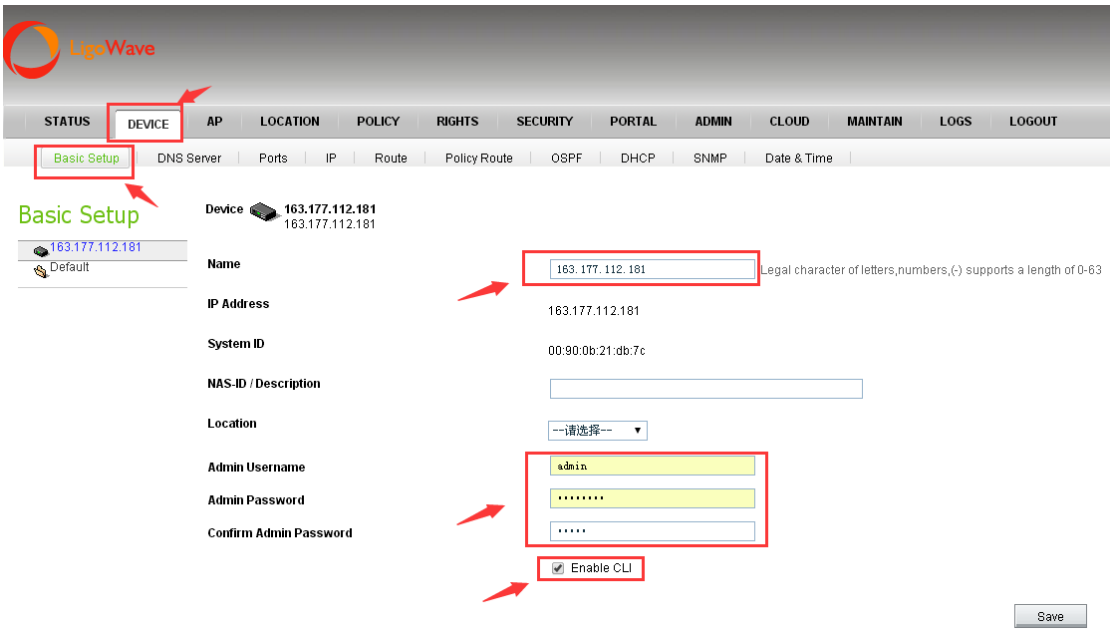


1.2.2. Setup Instructions

1.2.2.1. Basic Setup

In the module you can check the VAC/WACIP address, System ID; you can also set

the VAC/WAC Name, Admin Username, Admin Password and enable/disable SSH



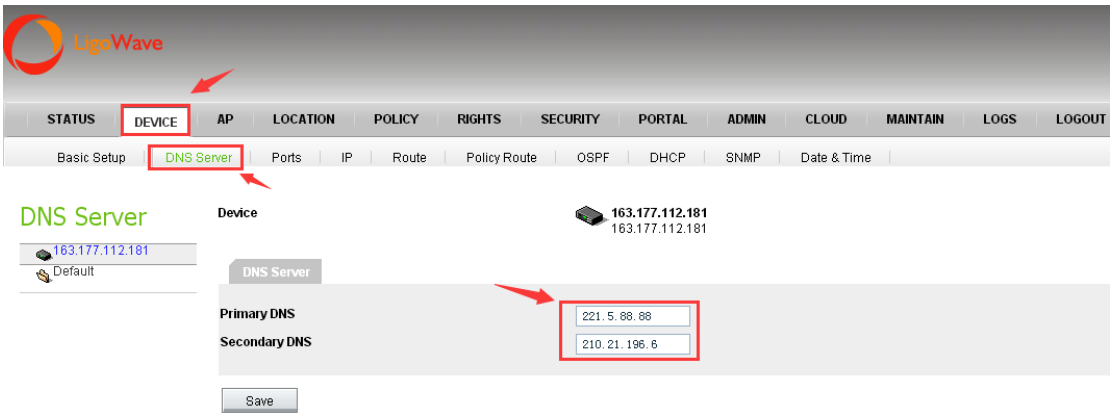
A. IP address of VAC/WAC/LAC(the IP of the port that enable “Management Channel”)

B. Enter username and password for VAC management UI

C. Enable/Disable SSH

1.2.2.2. DNS Server

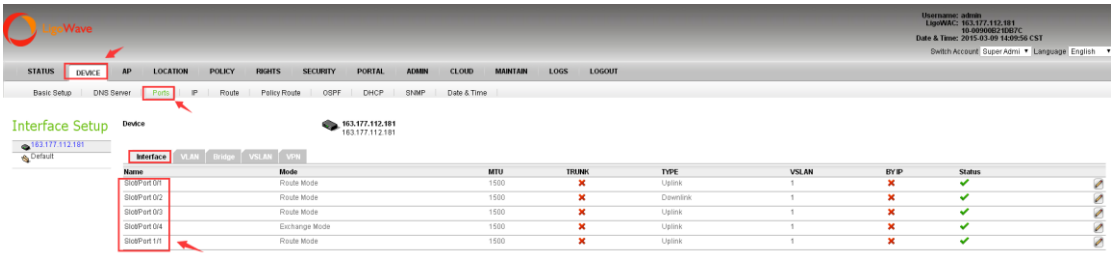
- DNS for WAC/VAC/LAC



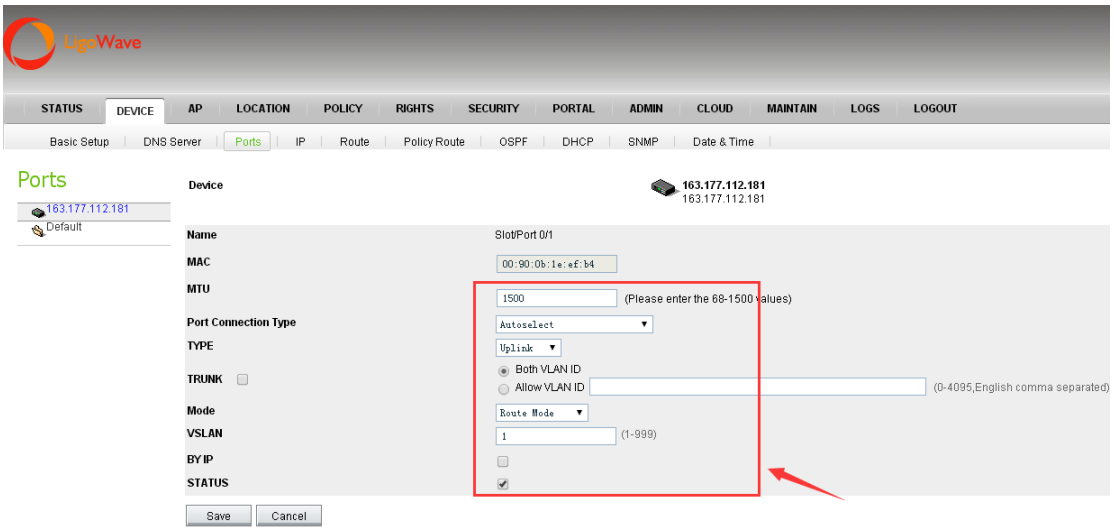
Note: The DNS here is only for VAC/WAC itself, not for the client

1.2.2.3. Ports

1.2.2.3.1. Physical Interface



- Here we take port 0/1 as an example:



A. Set MTU value(The default value is 1500)

B. Set port connection mode

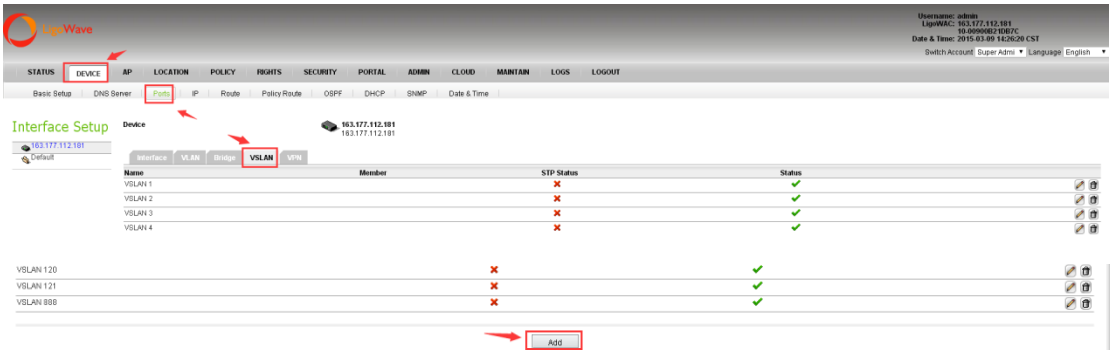
C. Set interface type(downlink interface has to be authenticated)

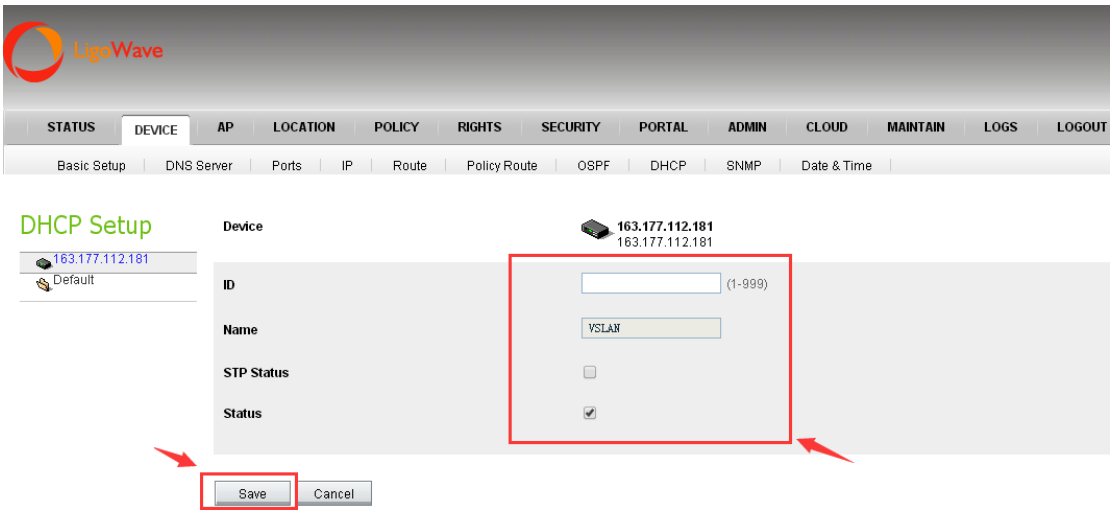
D. Working mode(route/switch mode)

E. Set VSLAN ID

1.2.2.3.2. VSLAN Interface Configuration

- Click “Add” button to create a new VSLAN interface





A. Set VSLAN ID(1 - 999)

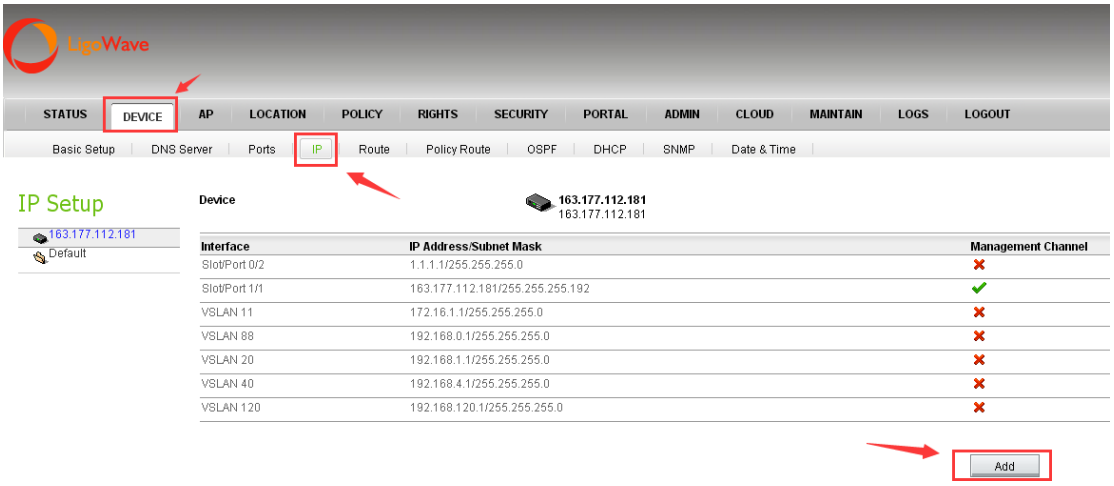
B. Enable/Disable STP

C. Enable/Disable the interface

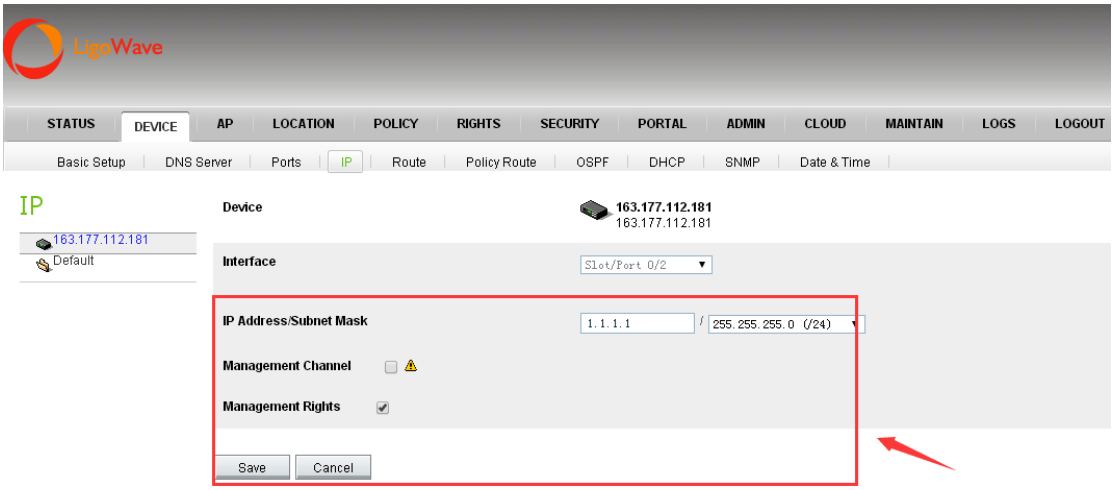
- Click “Save” to finish creating VSLAN interface and return to the previous menu

1.2.2.4. IP Setup

- By option DEVICE - IP, click “Add” to add IP address/Subnet mask, Management Channel control and Management Rights control for physical interfaces, VLAN, Bridge and VSLAN interfaces



- Here we take port 0/2 as an example:



A. Select interface for IP setup

B. Enter IP address/subnet mask

C. Enable/Disable Management Channel(Management Channel can only be enabled on one port)

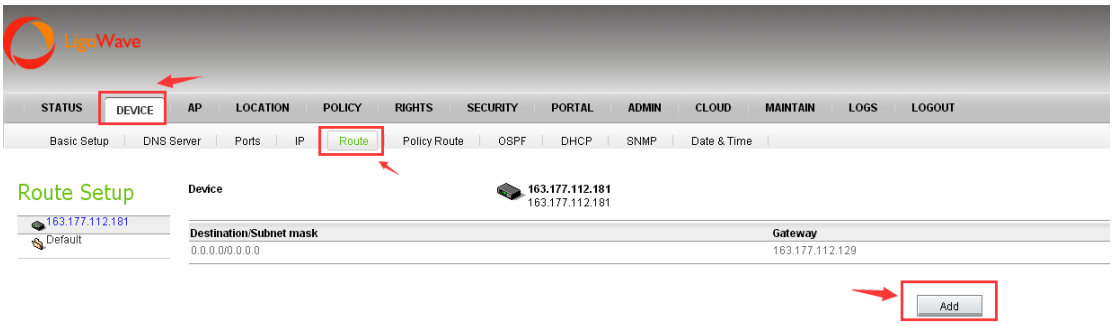
D. Enable/Disable Management Rights(Management Rights can be enabled on all physical ports)

- Click “Save” to finish IP setup and return to the previous menu

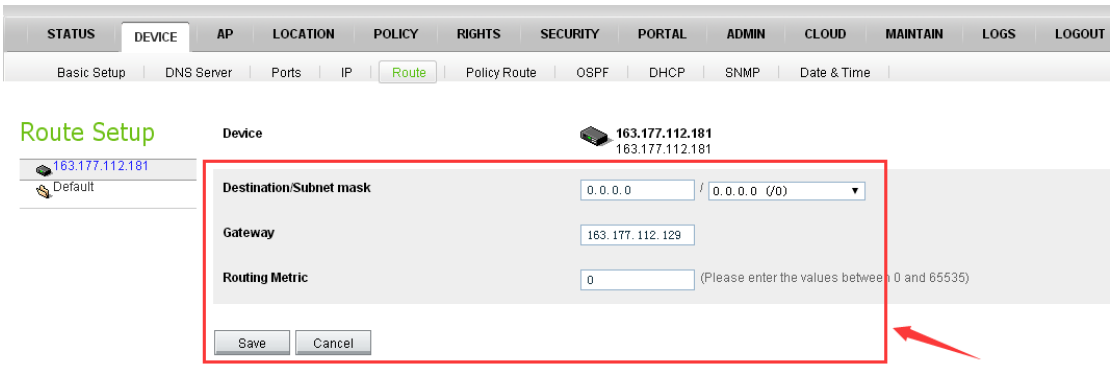
Note: You can add/change the ip for ports except the current management port, if you change ip of the current management port will result losing connection to the device

1.2.2.5. Destination Route

- Add destination route for the device



- By option DEVICE - Route, Add/delete route, such as destination/static route



A. Set destination route IP/ subnet mask(in this case all IP data get out via the gateway 163.177.112.129)

B. Set gateway

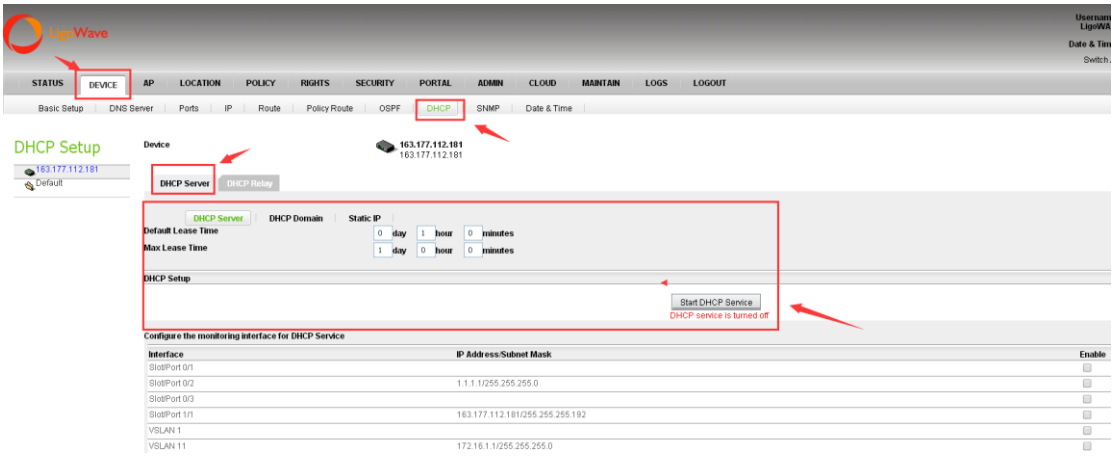
C. Enter routing metric

- Click “Save” to finish destination route setup and return to the previous menu

1.2.2.6. DHCP Setup

Configure DHCP Server, assign IP pools to interfaces, set DHCP Relay, assign IP statically *(Most of networks already have DHCP server, then you don't have to configure the DHCP)*

1.2.2.6.1. DHCP Server



A. DHCP Server setup

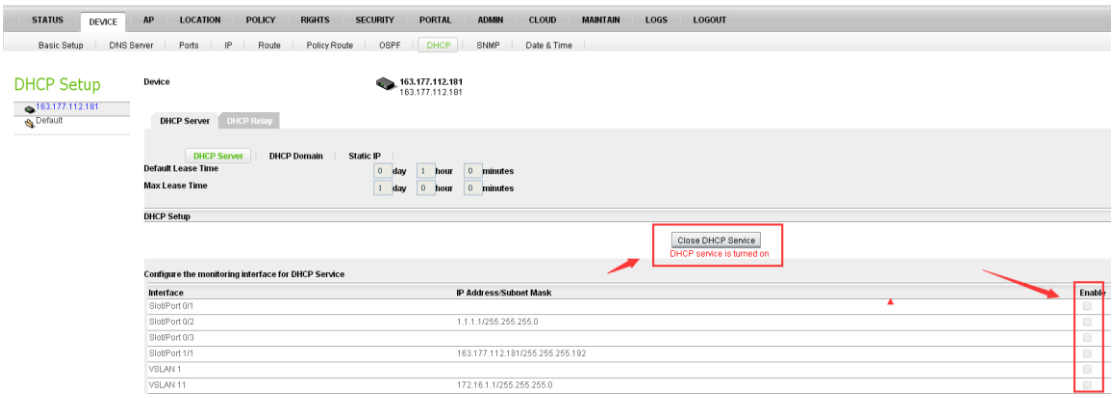
B. DHCP Domain setup(network distributed by DHCP)

C. Static IP address distribution(binding IP and MAC address)

D. DHCP Lease Time setup

E. Turn on/off DHCP Service

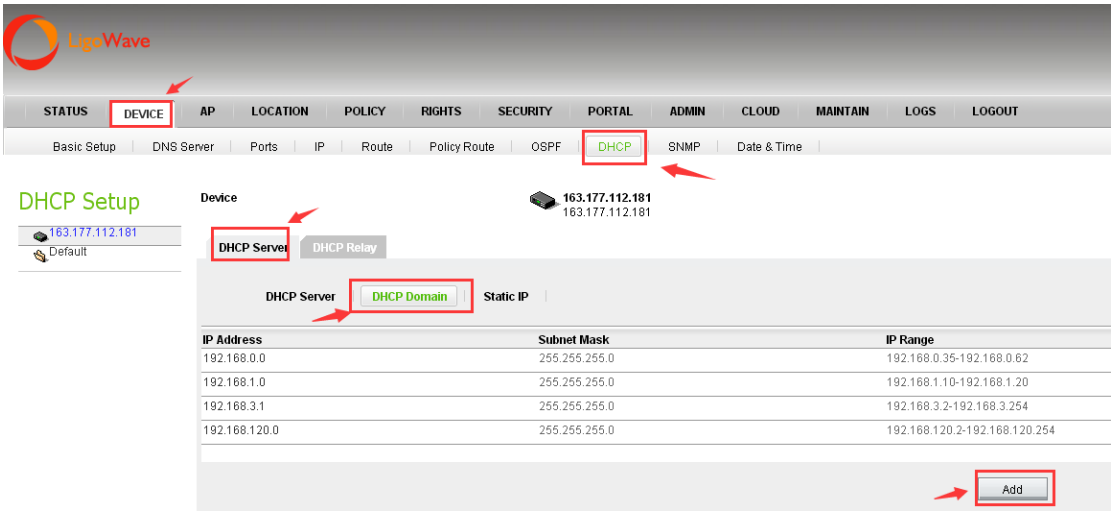
- By option DEVICE - DHCP, press “Close DHCP Service” to shutdown the DHCP service, then select the interfaces which need to create DHCP domain and save



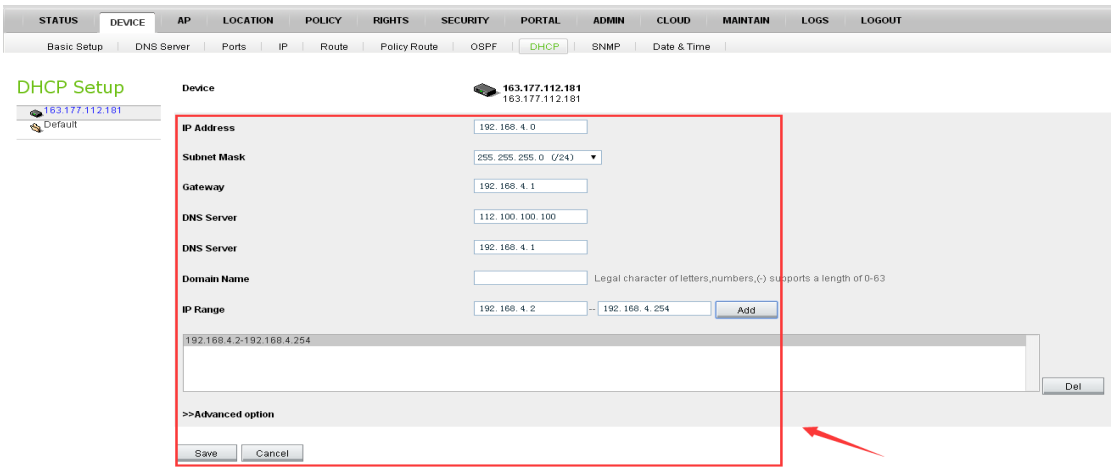
1.2.2.6.2. DHCP Domain

- By option DEVICE - DHCP - DHCP Domain, click “Add” to create DHCP

domain



- Create IP address/Subnet mask, Gateway, primary and secondary DNS, Domain Name and IP Range for DHCP domain



A. Domain IP address

B. Domain Subnet mask

C. Domain gateway(the IP of the interface)

D. Primary /secondary DNS

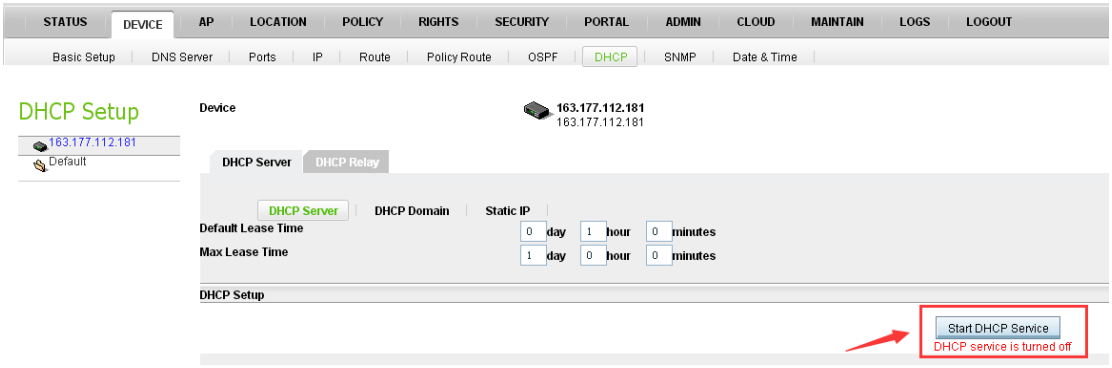
E. VAC/LAC/WAC domain name

F. IP address range

G. Advanced options, option43, etc.

Note:The IP address range must match the subnet of the interface IP(domain gateway)

- Click “Save” to finish creating DHCP domain. Return to the previous menu
- Click “Start DHCP Service” button

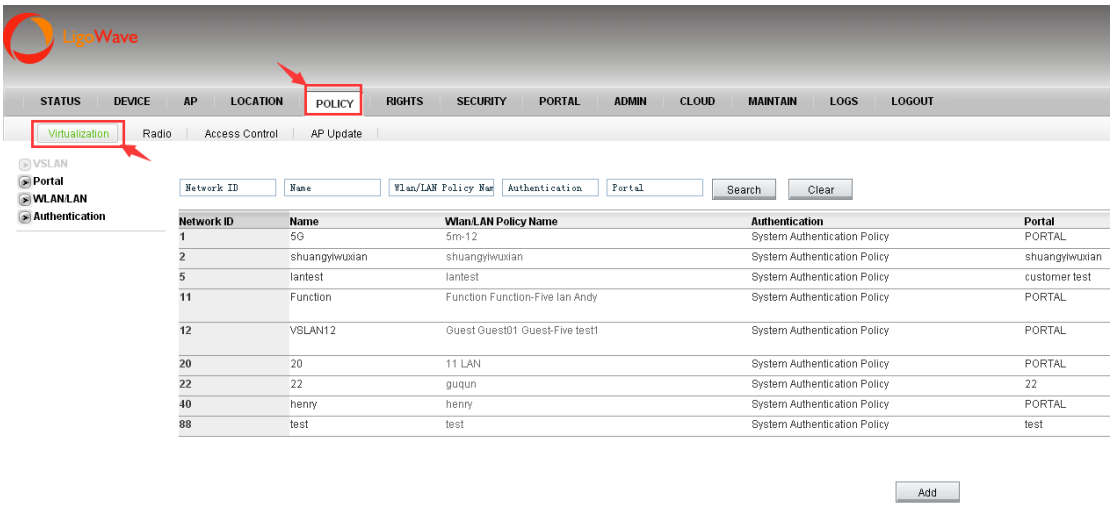


1.2.3. Policy Management Setup Instructions

Policy management module is for creating policies for APs, including WLAN policy, Portal policy, Authentication policy, and LigoWave-VSLAN policy. Through this module you can flexibly create virtual channels, make custom WLAN policies, and set radio frequency policies such as RF channel, Tx Power, and protocols. You can also set blacklist and whitelist for access control, and the policy for AP remote update.

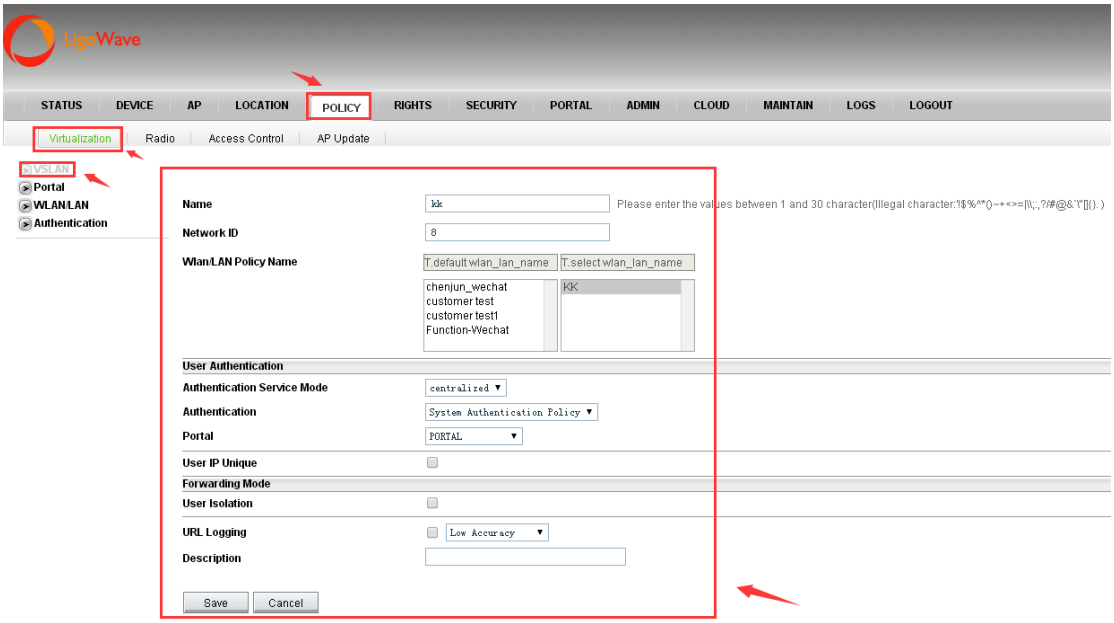
1.2.3.1. Virtualization

Create WLAN policy, Portal policy, Authentication policy and particular VSLAN policy of LigoWave for APs; VSLAN can be used for creating independent VPN to customize various policies for users



1.2.3.1.1. VSLANPolicy

- By option POLICY - Virtualization - VSLAN, click “Add” to create VSLAN policy, Set VSLAN Name, Network ID (**same as the vslan ID**), bind corresponding WLAN policy, PORTAL policy and Authentication policy



A. Network name (can be user-defined)

B. Network ID (Must match to VSLAN ID)

✧ Different network ID for different DHCP network

✧ Different network ID for different/same WLAN policy(one network ID can be related to couples of WLAN policies)

✧ Different network ID for different/same authentication policy

✧ Different network ID for different/same Portal policy

C. WLAN policy

D. Authentication, choose “centralized” or “distributed”(In VAC+LAC mode choose “centralized” to authenticate on VAC or choose “distributed” to authenticate on LAC)

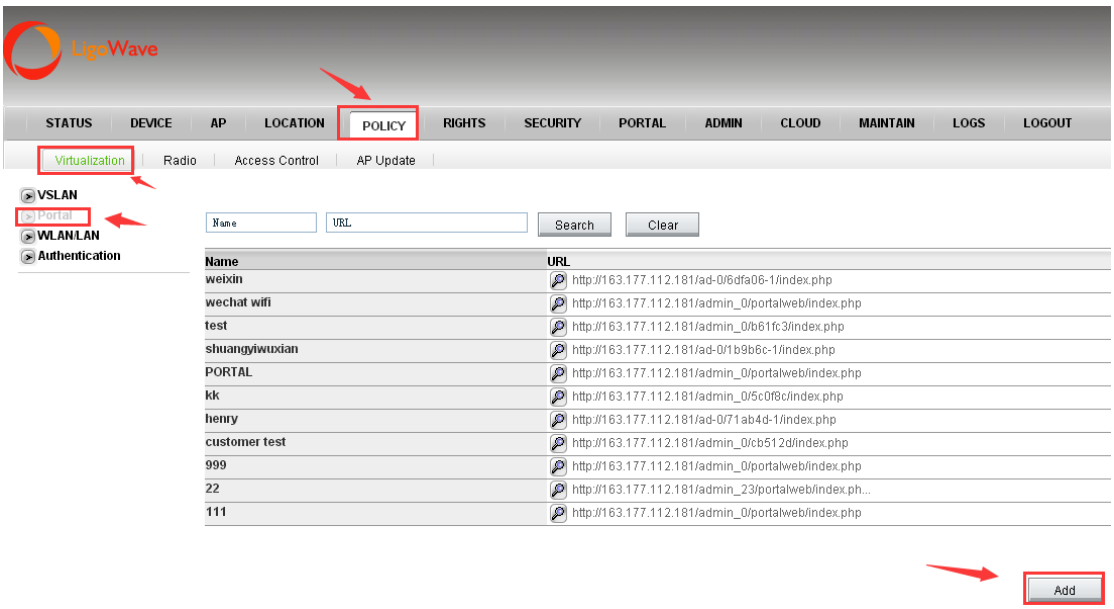
E. Authentication policy(local/Radius)

F. Portal policy(support external portal server)

G. Enable/Disable User isolation

- Click “Save” to finish creating VSLAN policy. Return to the previous menu

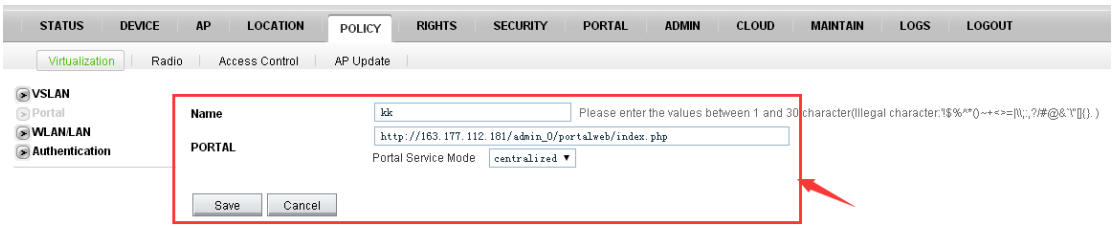
1.2.3.1.2. Portal Policy



A. Url address and custom portal name, allowing only one default portal policy

B. Content edited (the Name and the Url can be edited, you can also delete the portal policy)

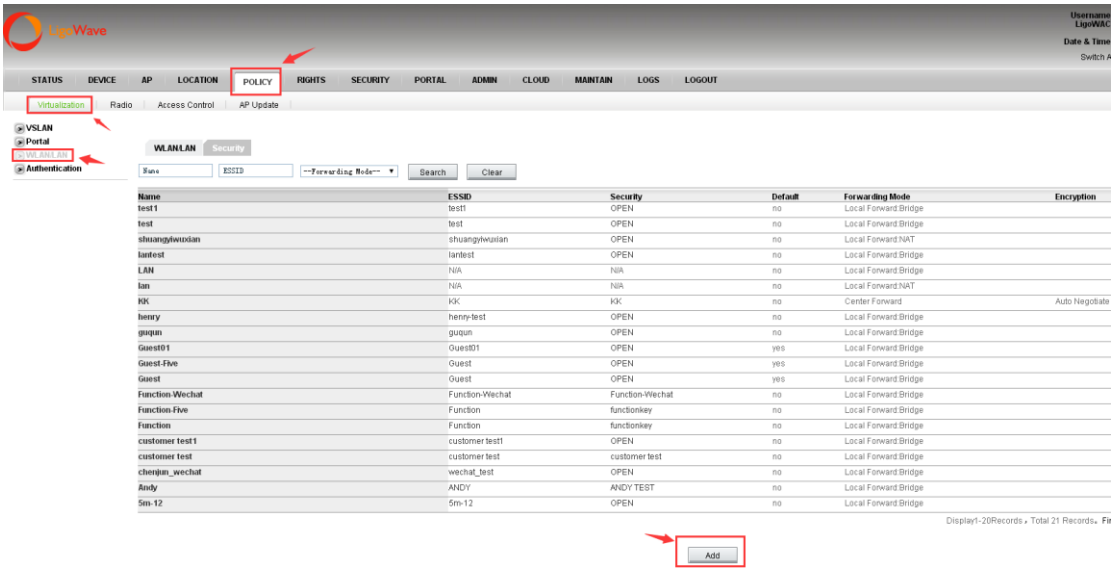
- By option POLICY - Virtualization - Portal, click “Add” to create Portal policy

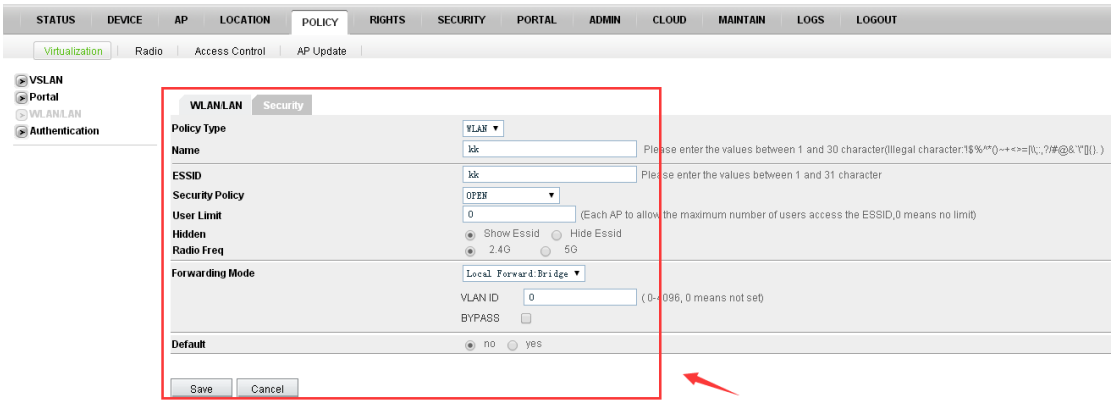


- Set PORTAL name, input PORTAL URL
- Default or not
- Click “Save” to finish PORTAL policy setup. Return to the previous menu

1.2.3.1.3. WLAN Policy

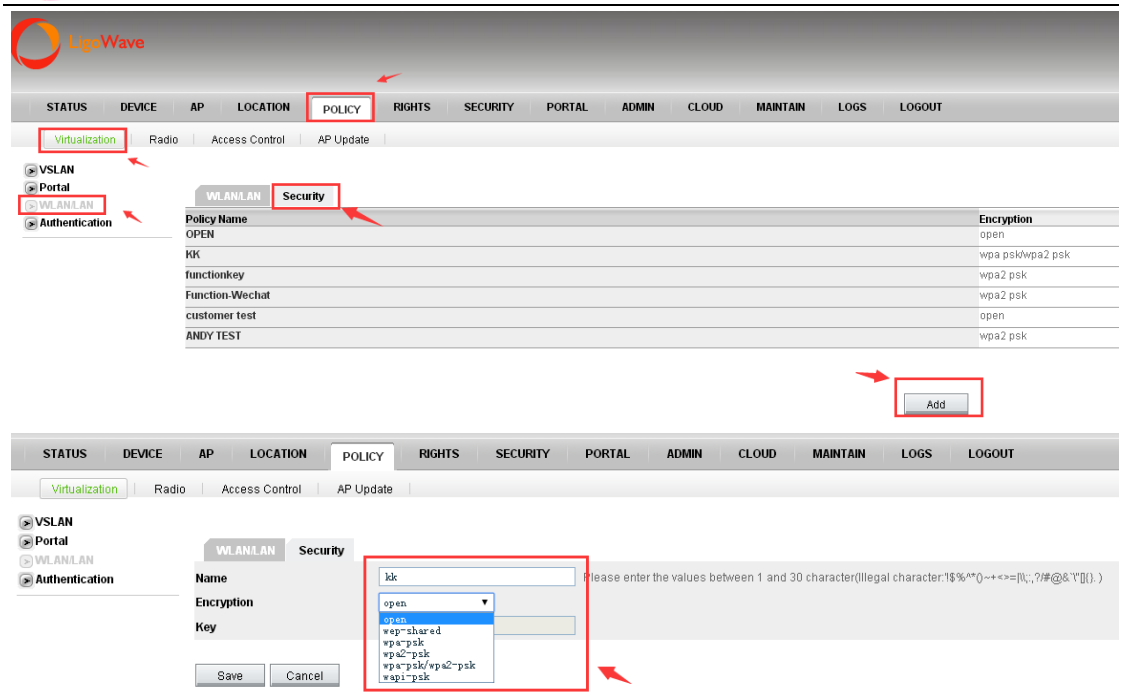
- By option POLICY - Virtualization - WLAN/LAN, Create WLAN policy by click “Add”





A. WLAN policy setup includes policy name, SSID, security policy, maxim user number, hidden ESSID, default or not (if choose default, the first time the AP getting online to the VAC/LAC it will apply the policy automatically), and user traffic forwarding mode (including centralized mode and local mode; user data encryption schemes when in centralized forwarding mode ; there are two local forwarding mode: NAT mode and Transparent mode)

- Click “Save” to finish WLAN policy setup. Return to the previous menu
- By option POLICY - Virtualization - WLAN/LAN - Security, set Security policy by choosing encryption schemes

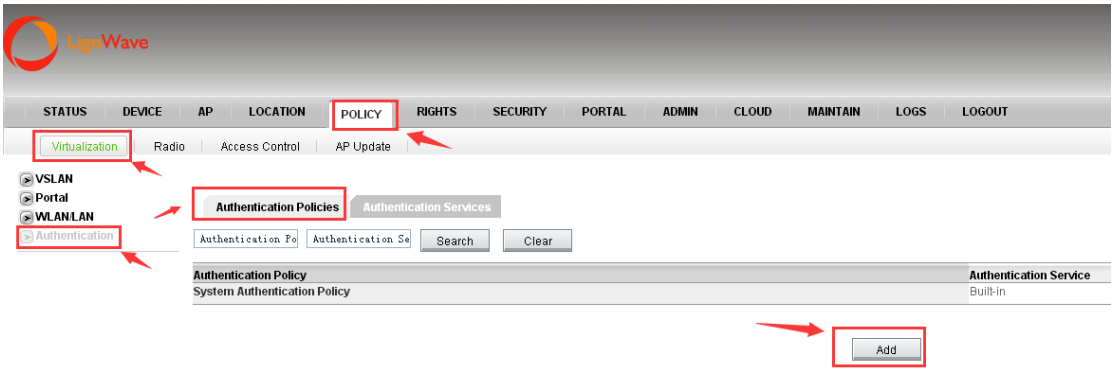


B. Set security policy name, encryption scheme, and encryption key

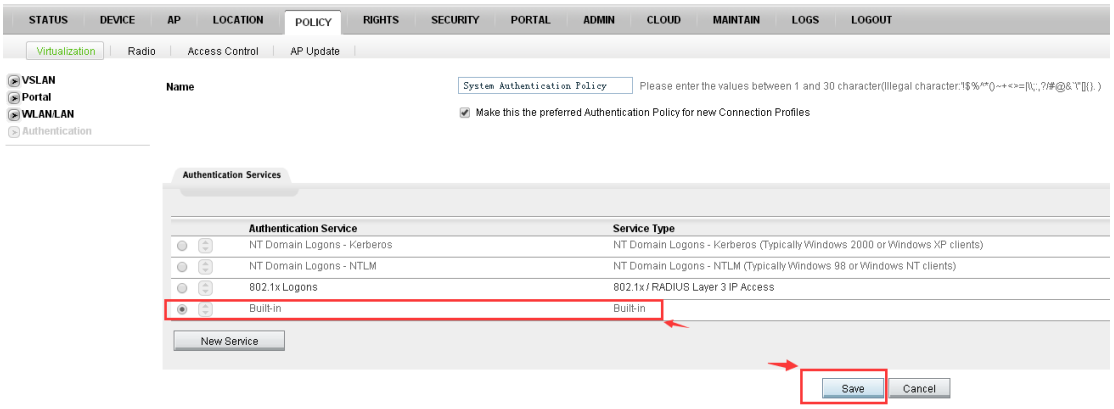
- Click “Save” to finish security policy setup. Return to the previous menu

1.2.3.1.4. Authentication Policy

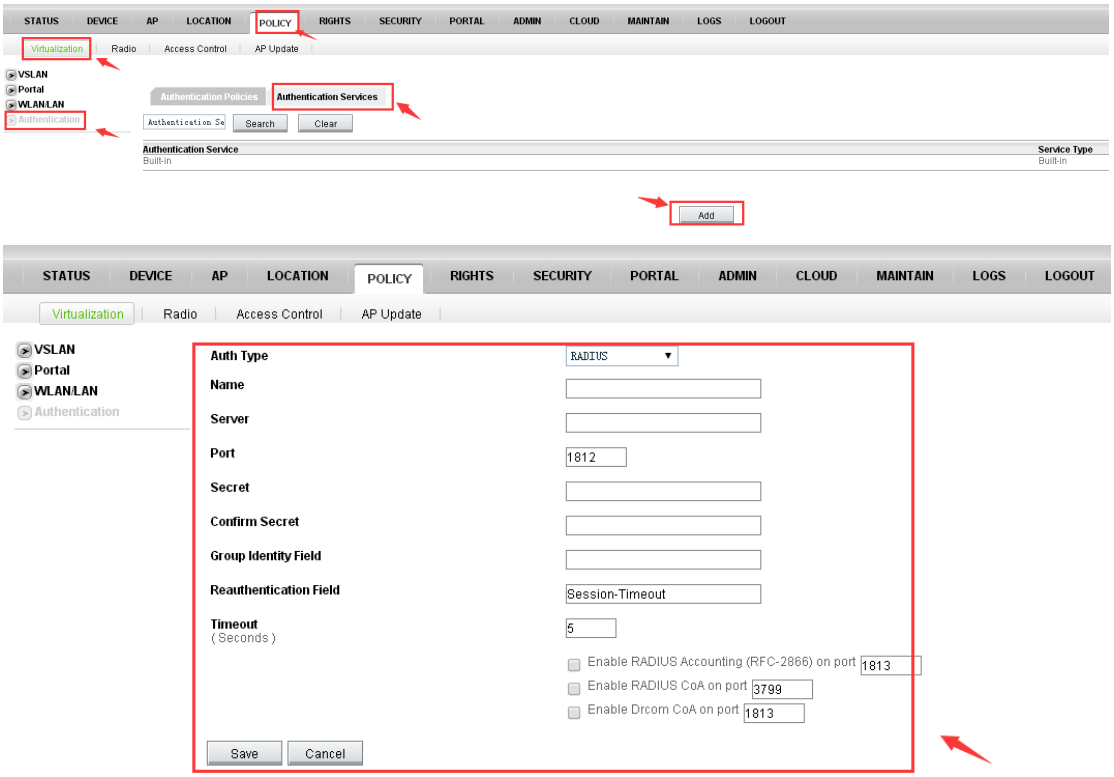
- Create Authentication policy by “POLICY - Virtualization - Authentication - Add”



A. “Built-in” indicates the authentication service is provided by local VAC/WAC



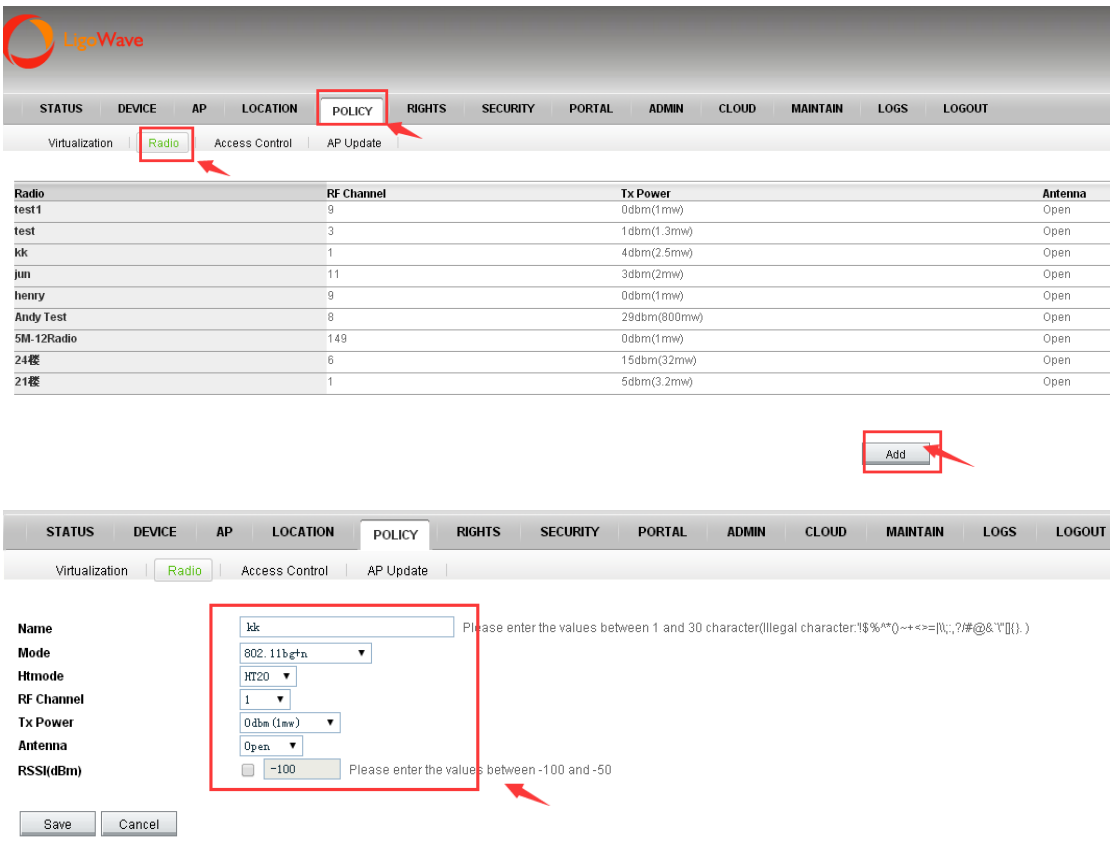
B. Set external Radius authentication by creating new authentication service, and define authentication type, name, server IP address, port number, and secret of authentication policy



- Click “Save” to finish Authentication policy setup. Return to the previous menu

1.2.3.2. Radio Policy

- By option POLICY - Radio, click “Add” to create Radio policy



A. Radio policy name

B. AP working mode (auto, 802.11b, 802.11g, 802.11bg+n, 802.11a, 802.11a+n, 802.11n-2.4G-only, 802.11n-5G-only)

C. Htmode (HT20, HT40-, HT40+)

D. RF channel (including 2G and 5G channel, self-adaptive)

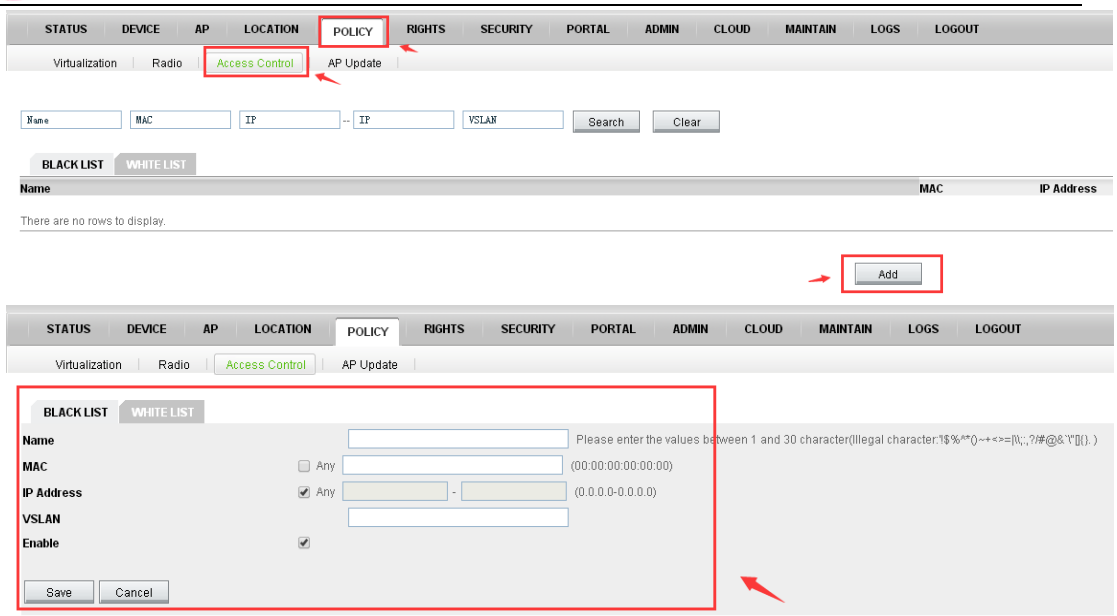
E. AP Tx Power (0-500mW self-adaptive)

F. Antenna on/off

- Click “Save” to finish Radio policy setup and return to the previous menu

1.2.3.3. Access Control

- By option - Access Control, create filter list by click “Add”



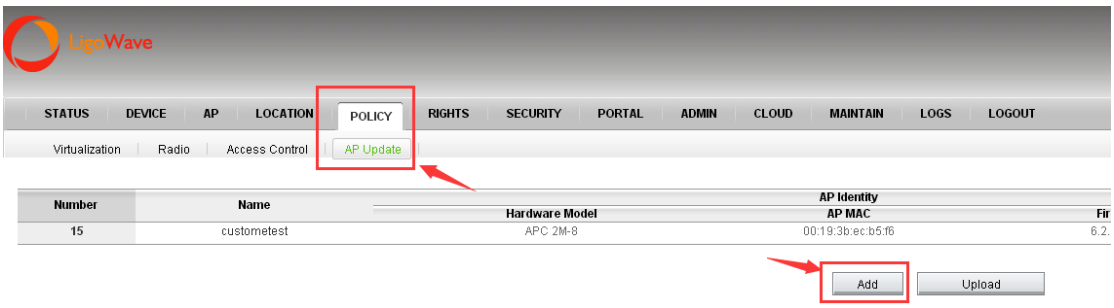
A. Set BLACKLIST (based on MAC, IP address range, VSLAN)

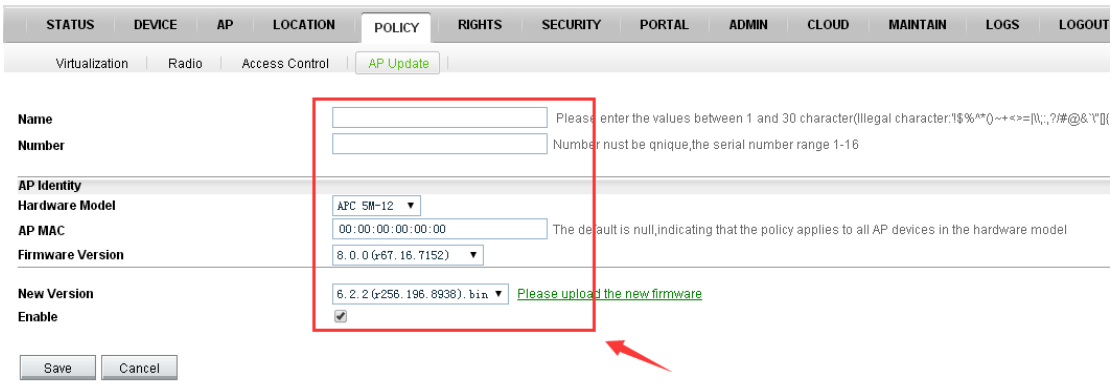
B. Set WHITELIST (based on MAC, IP address range, VSLAN)

- Click “Save” to finish filter list setup and return to the previous menu

1.2.3.4. AP Update

- By option - APUpdate, Click “Add” to create AP Update policy





A. Set AP update policy name

B. Select AP hardware model

C. Specify AP MAC for updating a certain AP. Otherwise all AP devices in the hardware will be updated

D. Select firmware version (updating under LigoWave customer service guidance advised)

E. Select upload version (updating under LigoWave customer service guidance advised)

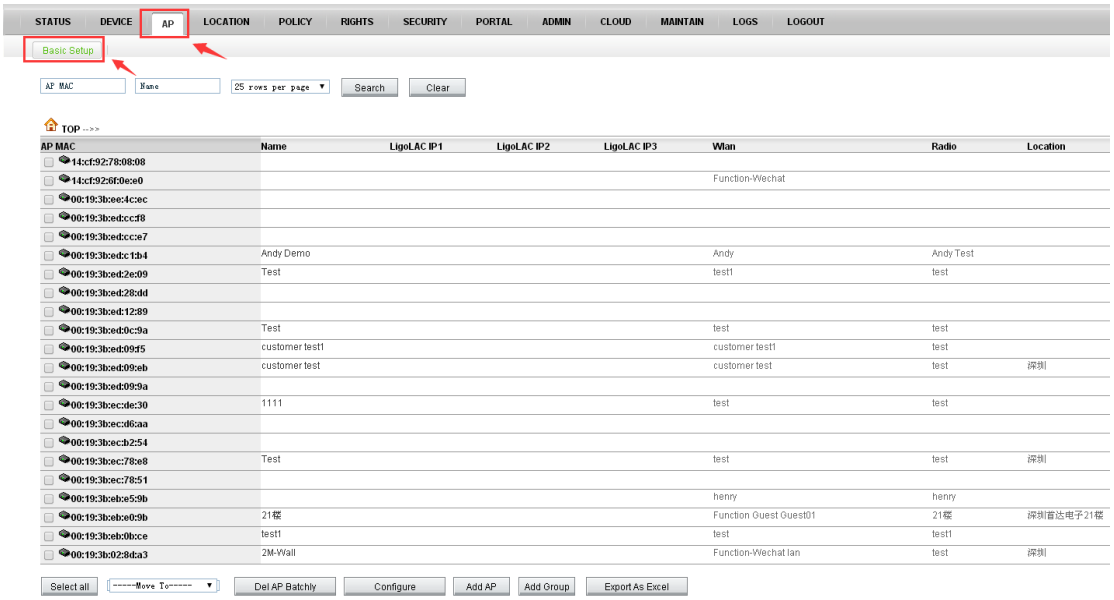
F. Enable (check to enable updates policy, otherwise it remains disabled)

- Click “Save” to finish AP updates policy setup. Return to the previous menu

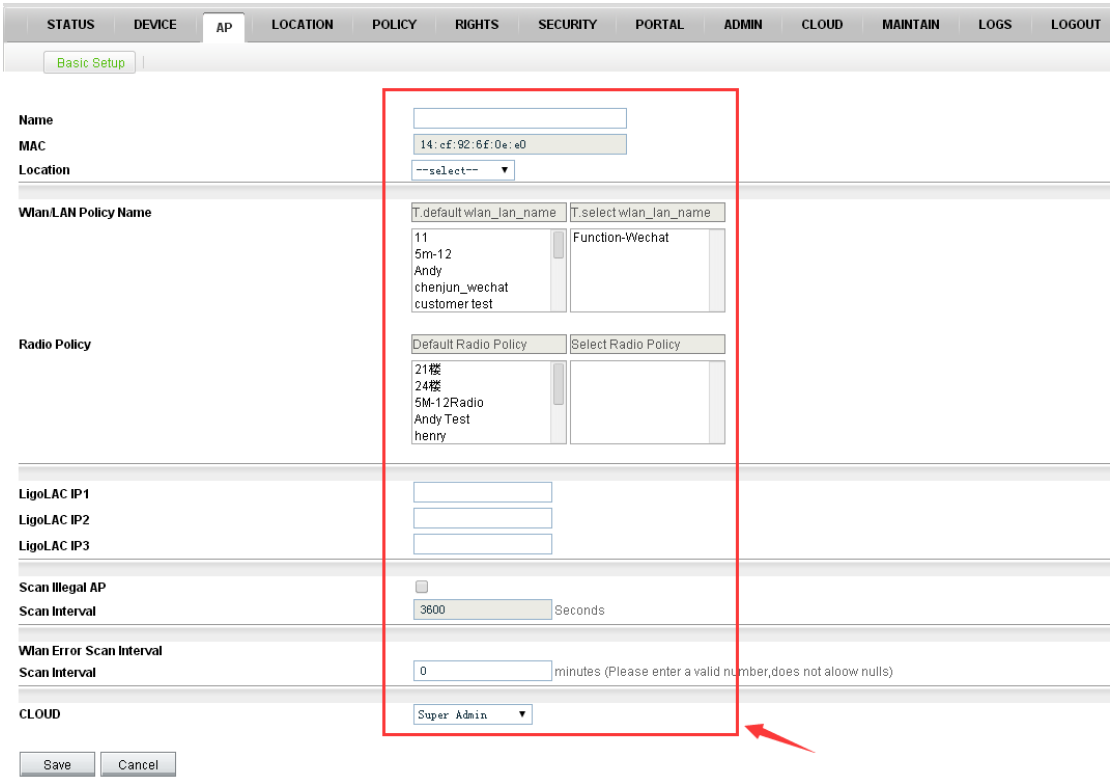
1.2.4. AP Setup Instructions

AP module provides quick setup of AP name, LACIP, WLAN policy, Radio policy, Location, as well as illegal AP detection. AP list shows the information of all registered AP. You can quickly search any AP by applying the filters such as MAC and LACIP, etc.

1.2.4.1. Basic Setup



- After all the policies are created , select APs to configure by option AP - Basic Setup



A. AP name

B. AP MAC address

C. Assign three LACs to AP, LAC1 is primary and LAC2 is secondary

D. Set WLAN policy

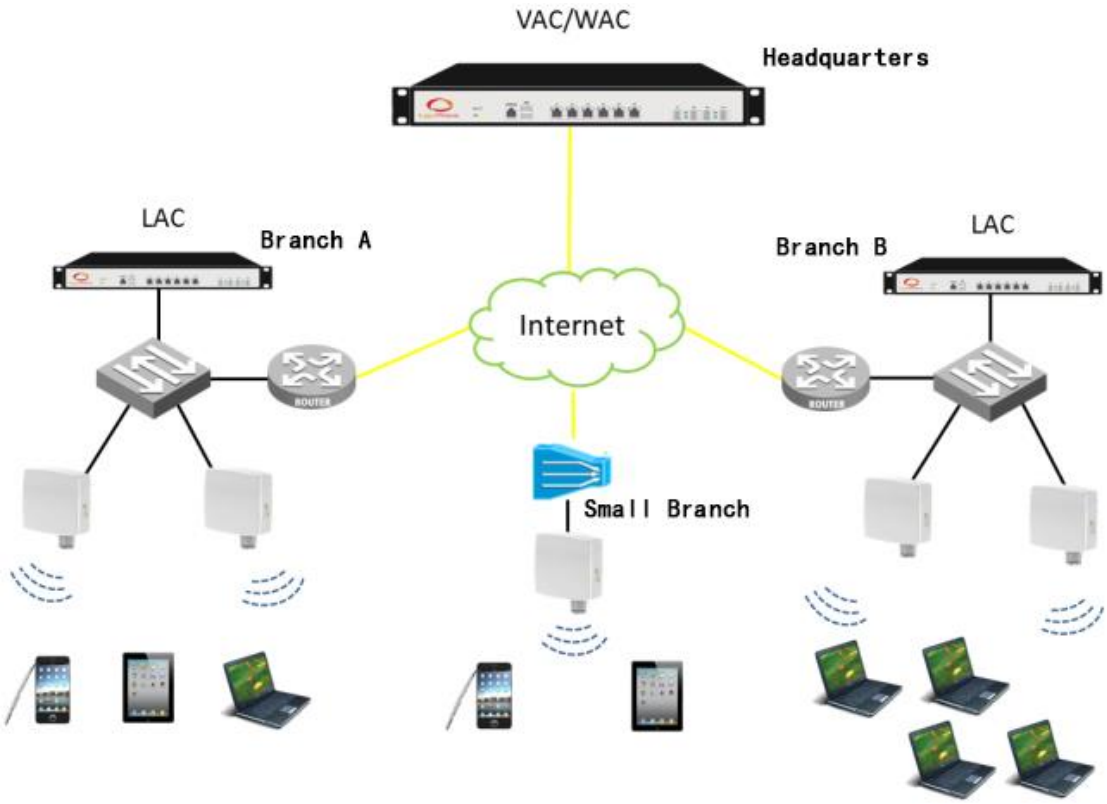
E. Set Radio policy

- Click “Save” to finish AP template setup. Return to the previous menu. The SSID of WLAN template will be broadcasted

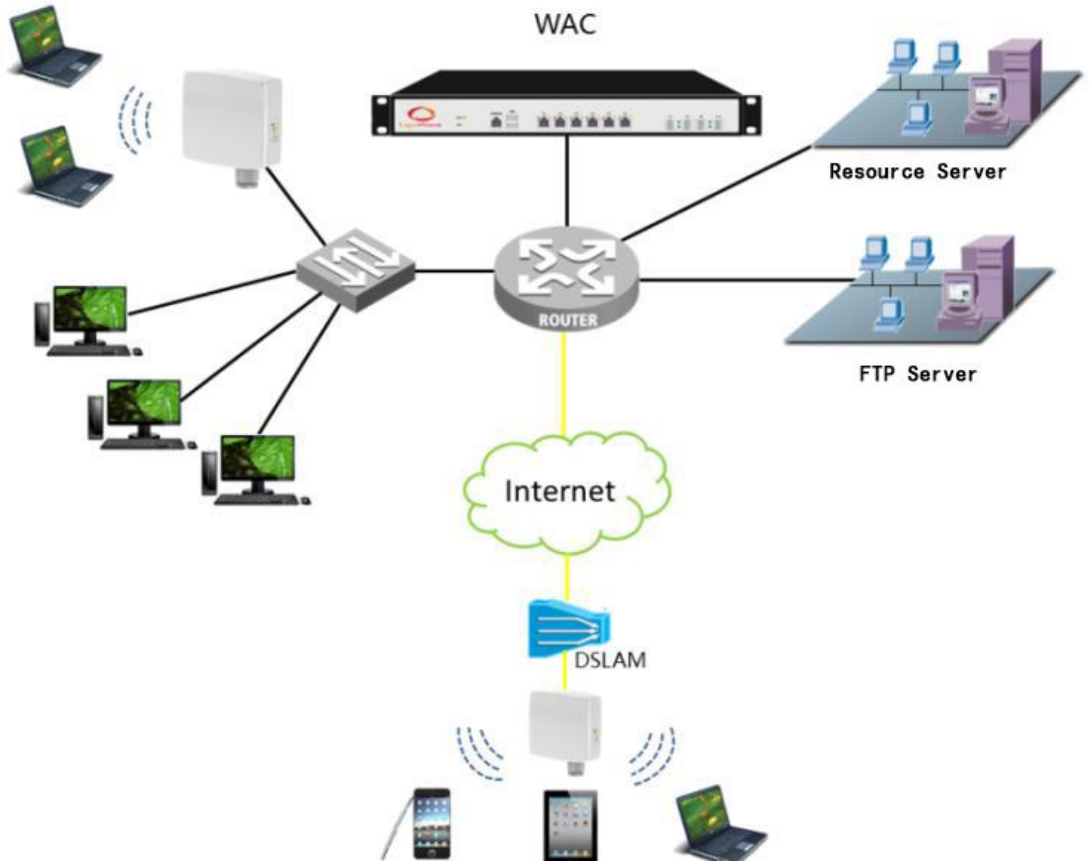
2. Chapter 2
General Application and Major Achievable Functions

2.1. General Network Topology Descriptions

2.1.1. Headquarter-and-Branch Topology:



2.1.2. SMB Topology:



2.2. Cloud Access can be achieved

2.2.1. LAC can be managed cross-internet

Case study on headquarter-and-branch topology (*2.1.1*), verify the cross-internet functionality of LAC.

2.2.1.1. Pre-Setup and Test Steps

- Connect LAC and VAC crossing NAT network
- Ensure the accessibility between LAC and VAC
- Set cloud VAC address in LAC initial configuration. The initial configuration of LAC is as follows:

- ✧ Connect a PC to the LAC's serial port
- ✧ The default management address of the LACport0/1 is 192.168.100.169. It can be changed through CLI
- ✧ Username is "admin" and password is "admin0.1"
- ✧ Set the LAC IP and Control Server IP via the serial port. Baud rate is 9600
- ✧ Delete all IP by command: **delete ip all**

```
LigoWave@[124.205.91.180]: delete ip all
```

- ✧ Delete all routes by command: **delete route all**

```
LigoWave@[124.205.91.180]: delete route all
```

- ✧ Add IP and route for Port0/1 (Control and management port) by the following commands:

Example for adding port IP:

Add ip 0/1 192.168.100.20 255.255.255.0 control on admin on

Example for adding default route:

Add route 0.0.0.0 0.0.0.0 192.168.100.1

```
LigoWave@[124.205.91.180]: add 0/1 192.168.100.20 255.255.255.0 control on admin on
LigoWave@[124.205.91.180]: add route 0.0.0.0 0.0.0.0 192.168.100.1
```

- ✧ Set IP address of the VAC for the LAC by command: **set controlserverx.x.x.x**

```
LigoWave@[124.205.91.180]: set controlserver 192.168.100.21
```

- ✧ Hint: The above commands configure the VAC IP for the LAC connection;
- ✧ Save the configuration and reboot by the following commands:
- ✧ To save the configuration: **save main**
- ✧ To reboot: **reboot(y=yes n=no)**

2.2.1.2. Expected Results

- The LAC is successfully registered and get online to the VAC

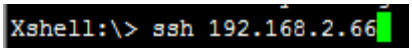
2.2.2. AP can be managed cross-internet

2.2.2.1. Pre-Setup and Test Steps

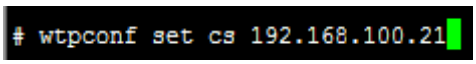
- Case study on headquater-and-branch topology(*2.1.1*), verify the cross-internet functionality of AP
- Connect the AP and the LAC, VAC WAC crossing NAT network
- Ensure accessibility between the AP and the LAC, VAC/VWAC
- Set the cloud VAC address in the AP initial configuration, The initial configuration of AP is as follows :

✧ When the AP is powered up it will by default broadcast the SSID "Ligo_mac", as shown below:

✧ Connect your laptop to the SSID and manage the AP through SSH(use SSH software like Xshell), the management ip is 192.168.2.66, as shown below:



✧ Follow the prompts to enter username: admin and password: admin01. After login successfully, type "shell" at the command line and press enter, use the following command to specify the remote VAC/WAC IP(for example:192.168.100.21) address for the AP:



✧ Have the AP connected to the network after the completion of the above steps

2.2.2.2. Expected Results

- Management SSID (Ligo_mac) of the AP disappeared. The AP is successfully registered on WAC/VAC

Before registration After registration

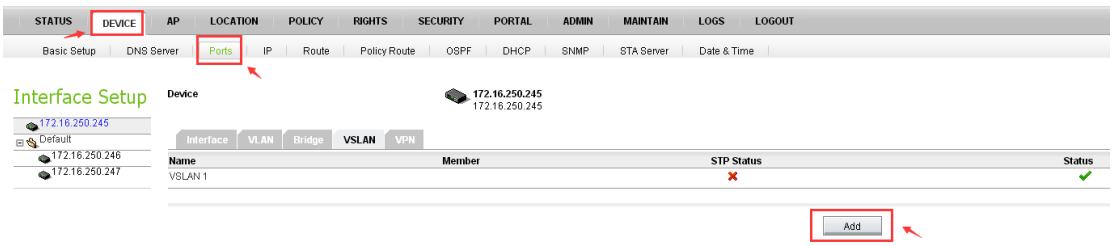
- The AP is successfully registered

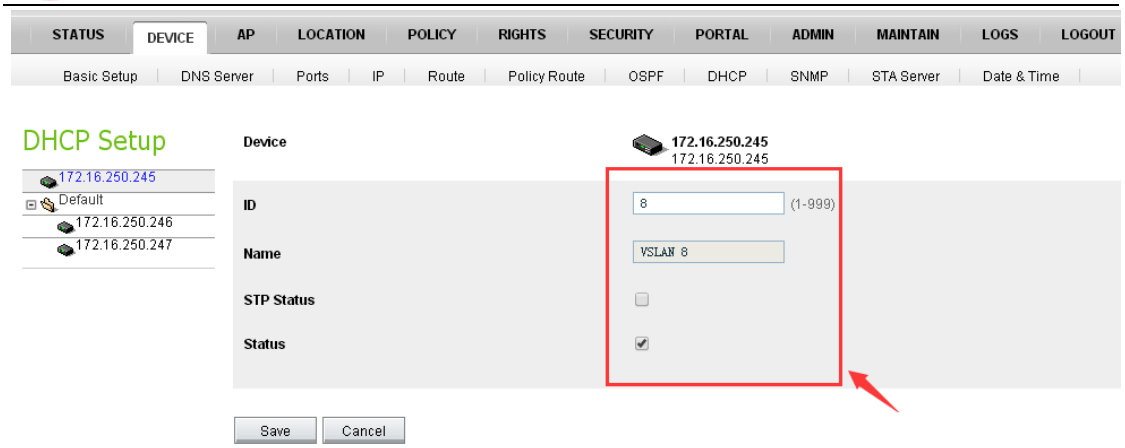
2.3. Virtualization can be achieved

2.3.1. Multiple independent manage virtual networks can be created

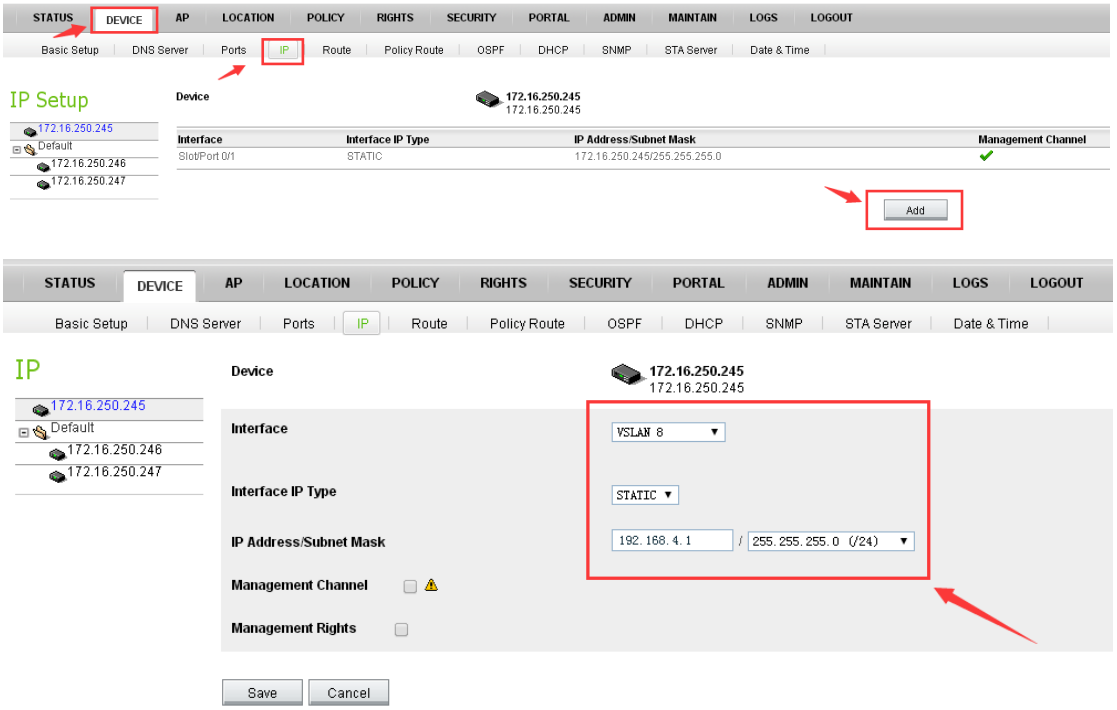
2.3.1.1. Pre-Setup and Test Steps

- APs are all under the VAC/WAC control, multiple independent manage private networks can be created
- Create 2 independent networks on the same AP(up to 6 can be created), each network has a different SSID, is managed independently
- Create VSLAN interface in LAC/WAC:“Device-Ports-VSLAN - Add”

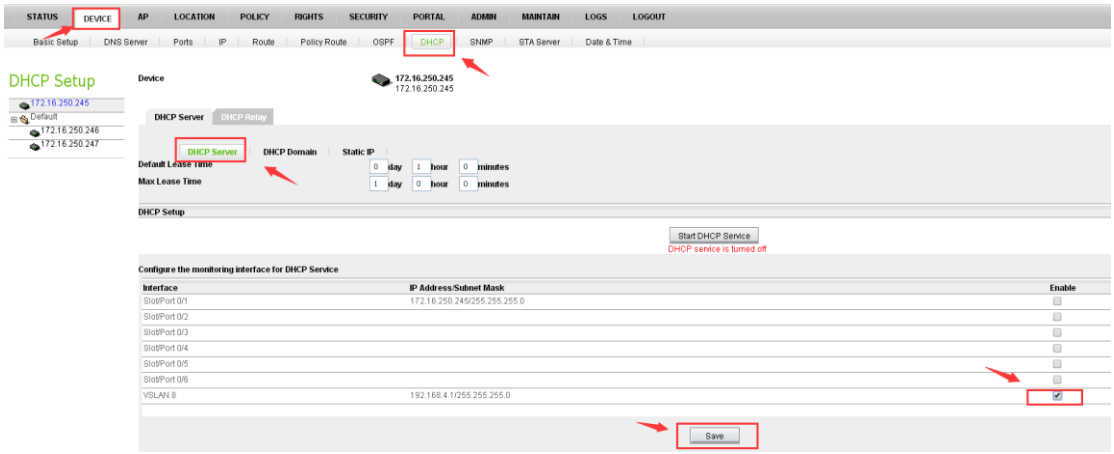




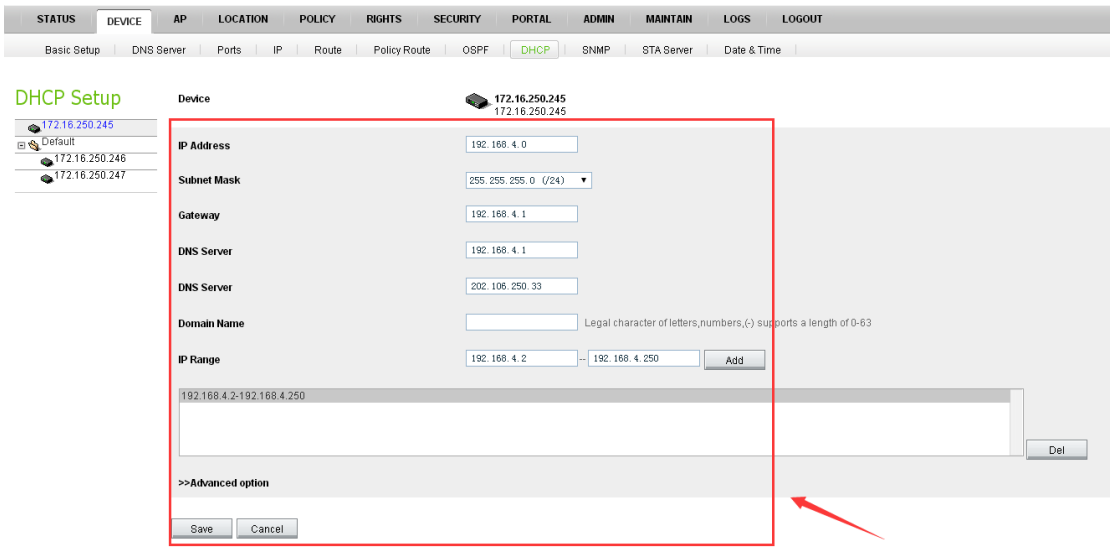
- Set VSLAN ID (from 1 to 999); uncheck “STP Status”; click “Save”. Now the VPN channel is created
- Click “Add” under “IP setup”; select VSLAN interface and set IP address



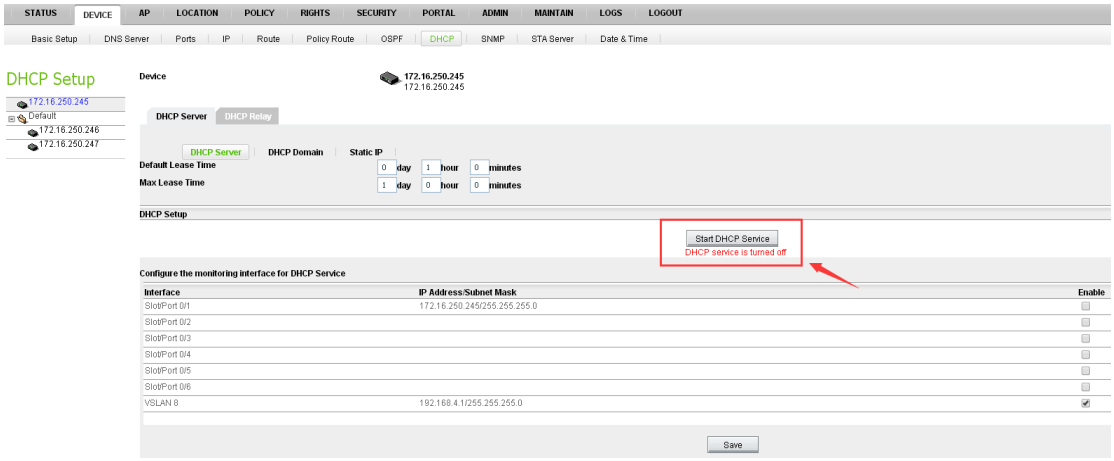
- DHCP - DHCP Server - select virtual interface - check “Enable” - Save



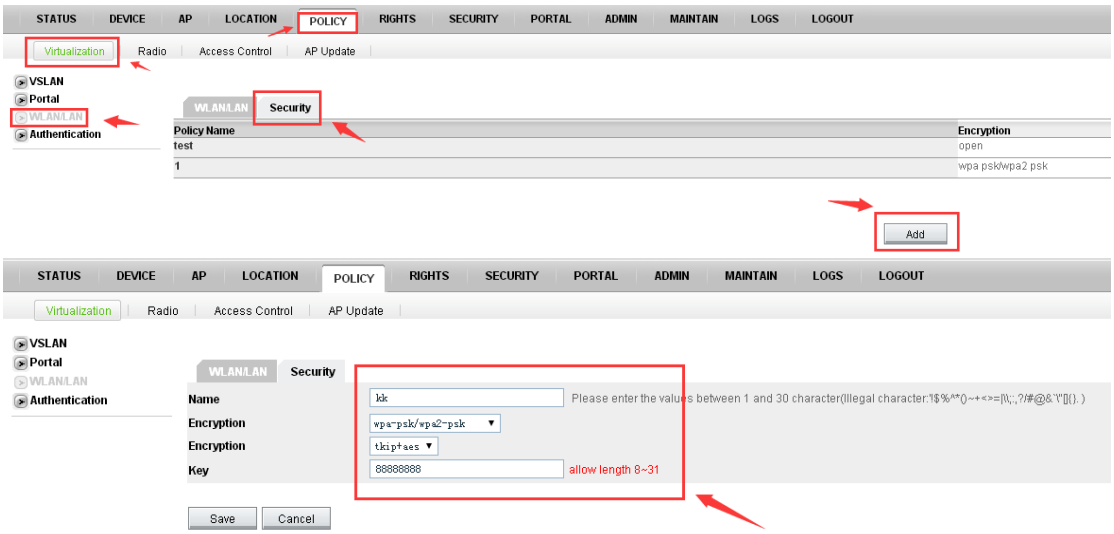
- Click “Add” under “DHCP Domain” to create DHCP domain; set relevant information, then click “Save”



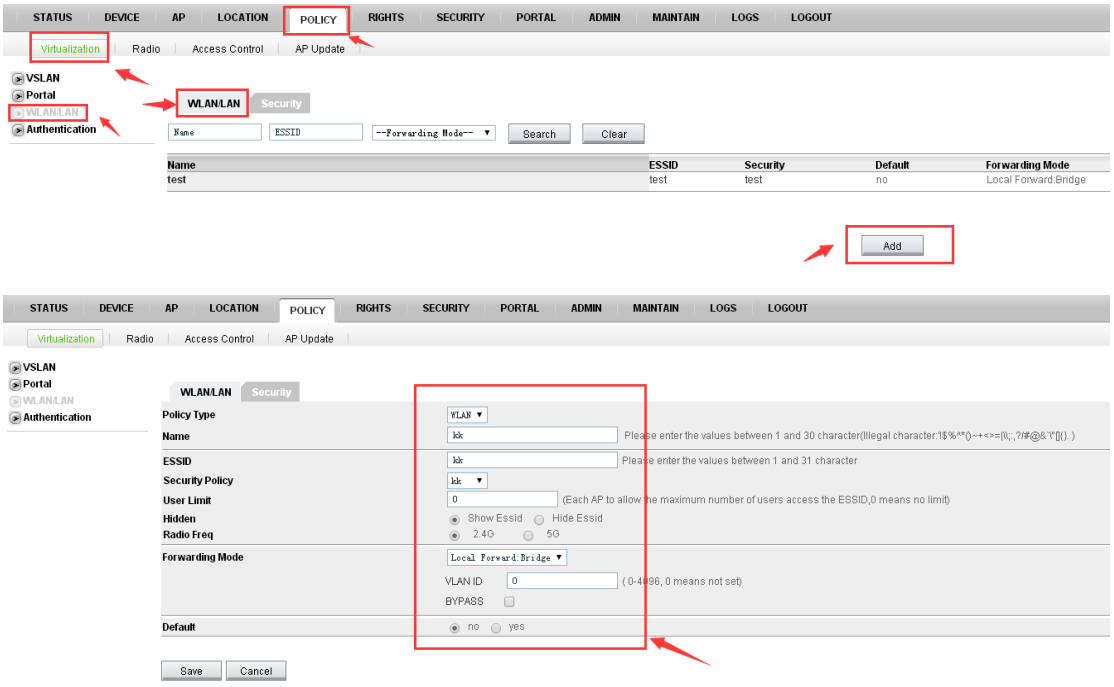
- Return to DHCP Server, click “Start DHCP Service”, then LAC/WAC will start to allocate addresses for STAs



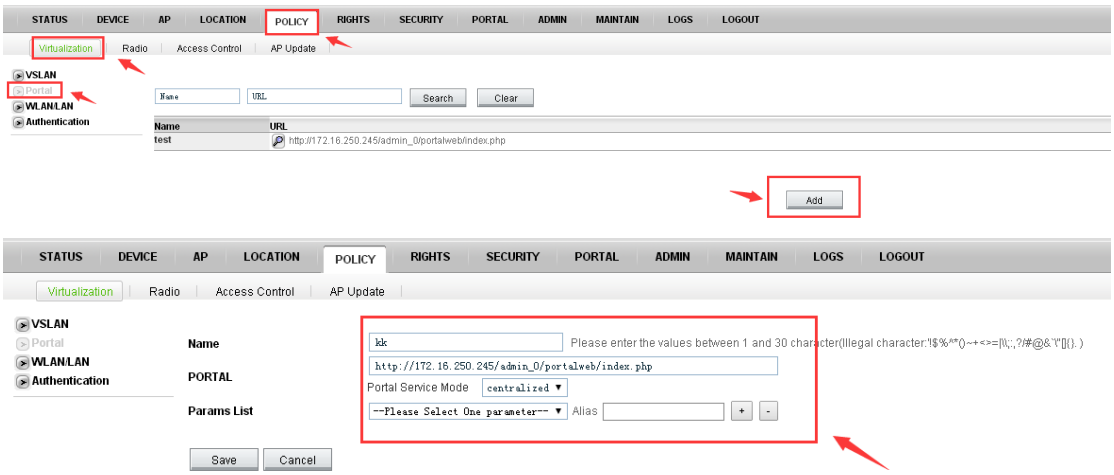
- Create WLAN policy, Portal policy and Authentication policy for AP by "POLICY- Virtualization"
- Create SSID encryption scheme by "WLAN - Security - Add"



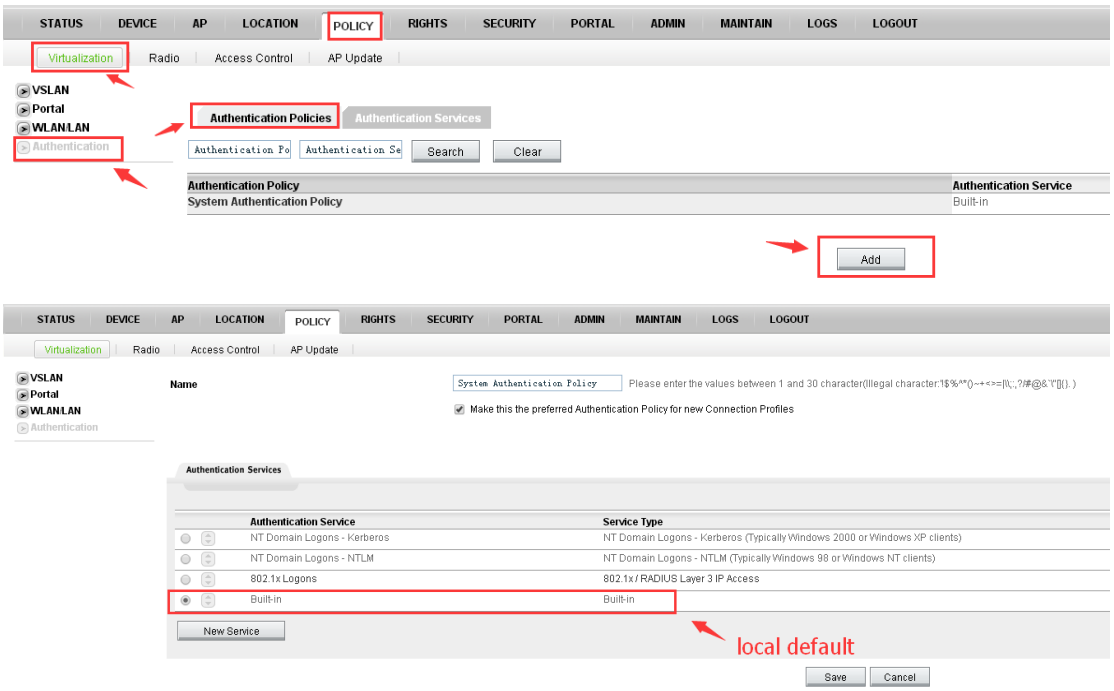
- Return to WLAN, and add WLAN policy;



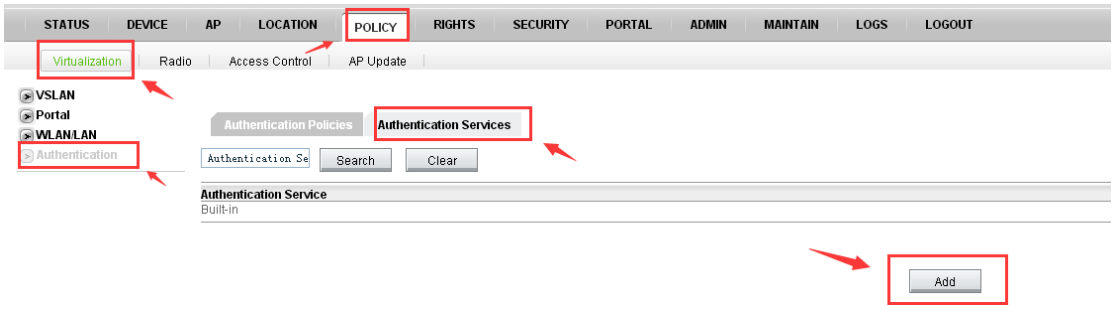
- Select security policy and data forward mode (center/ local forward) in WLAN policy;
- Click "Add" under "Portal policy" to create default PORTAL. Default will remain until it is modified;

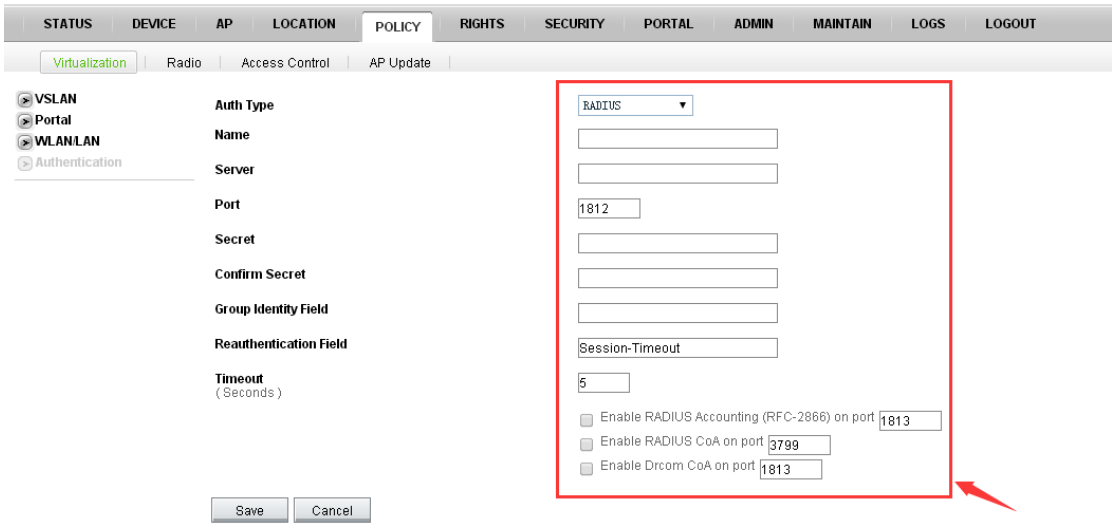


- Click “Add” under “Authentication policy” to create Authentication policy. The default local authentication is System Authentication Policy;

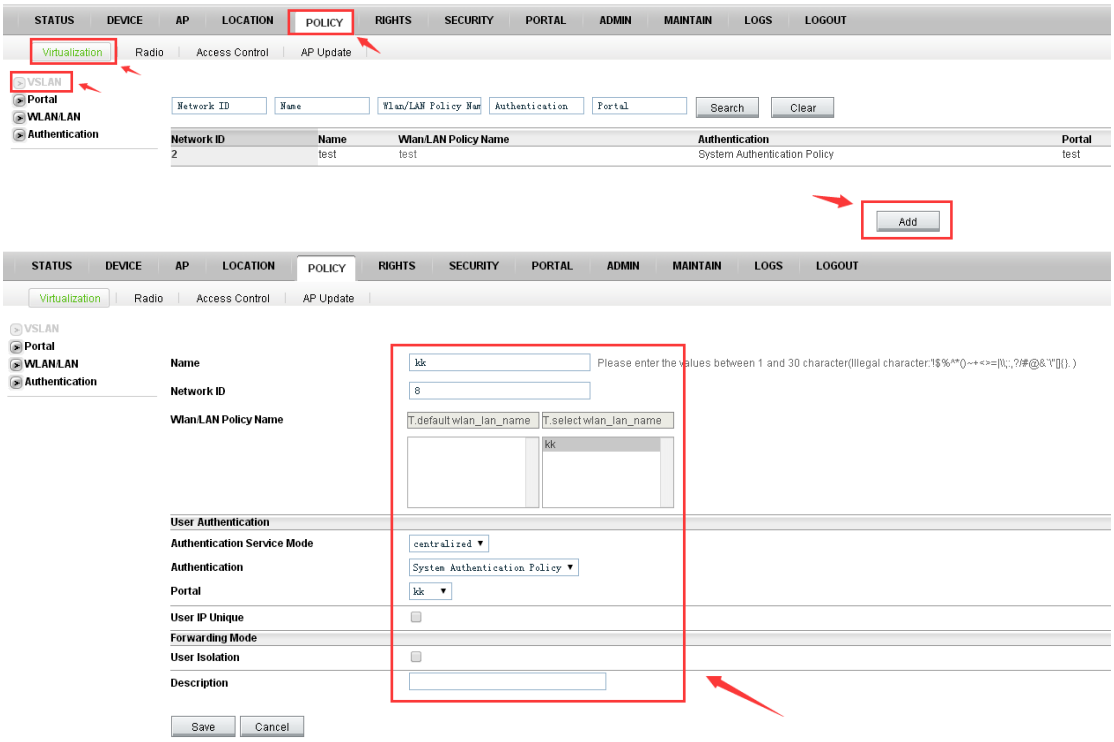


- You can also create a new authentication service which using external RADIUS authentication server;



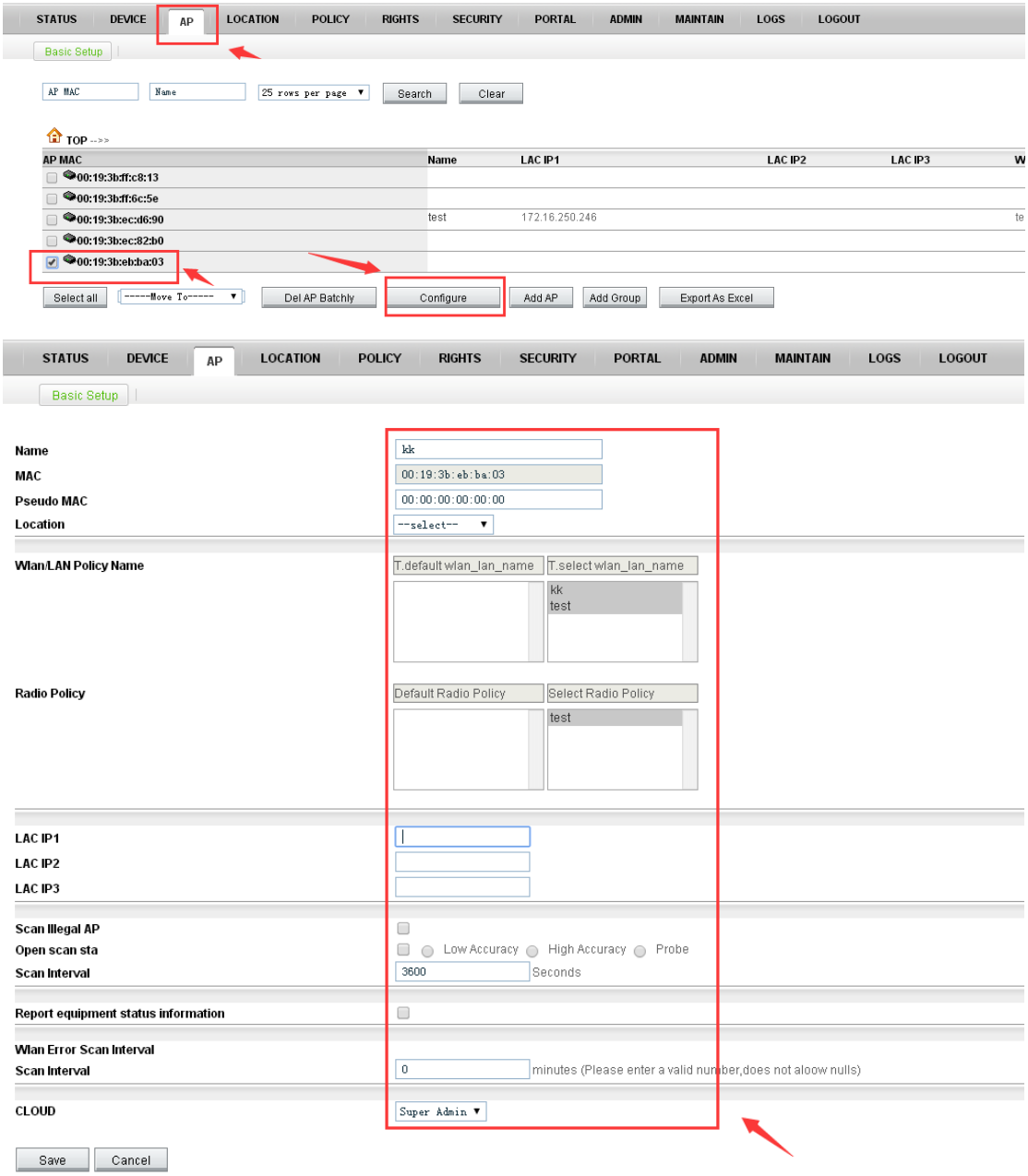


- Click “Add” under “VSLAN policy” to create VSLAN policy; then select the corresponding WLAN policy, Portal policy, Authentication policy to bind all the policies under the VSLAN policy; you can enable user isolation; make sure that the Network ID matches to the VSLAN ID you created; click “Save”.



- Select AP in AP module, and then set LAC, Location, WLAN policy, Radio policy, etc. Here you can add 6 WLAN policies simultaneously to create multiple

independent manage networks, in this case we create 2



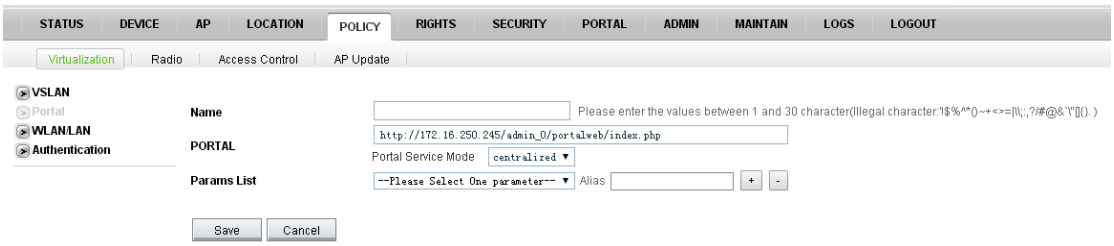
2.3.1.2. Expected Results

- 2 SSID signals are broadcasted from the specified AP. Admin can make custom VSLAN channels and policies and use them to create virtual WLANs which can managed independently.

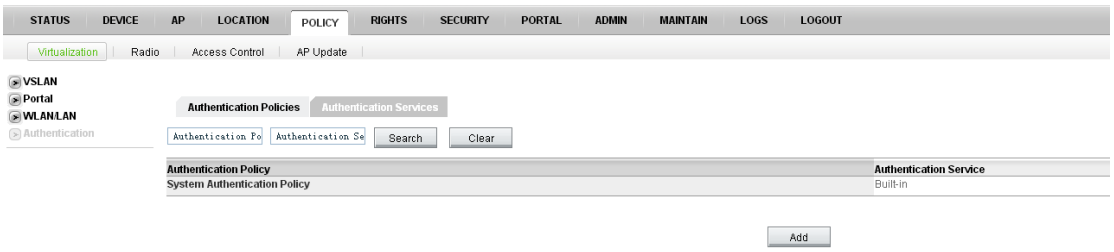
2.3.2. Authentication Policy and Portal Policy for each network can be set independently

2.3.2.1. Pre-Setup and Test Steps

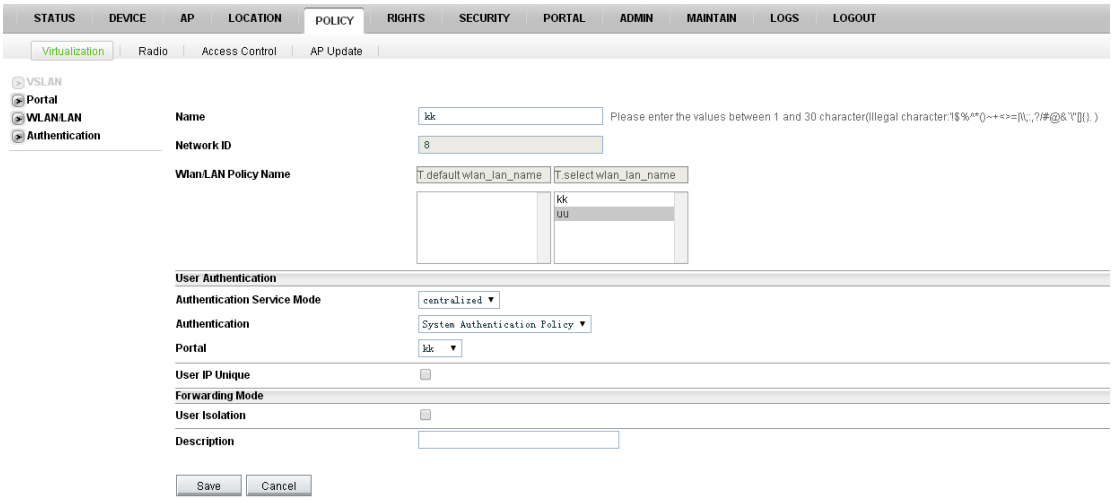
- Create VSLAN interface and DHCP domain
- Create default PORTAL by “POLICY - Portal”



- Select “Authentication policy” under “Policy”



- Set Authentication and PortalService Mode accordingly in VSLAN policy based on specified WLAN policy;



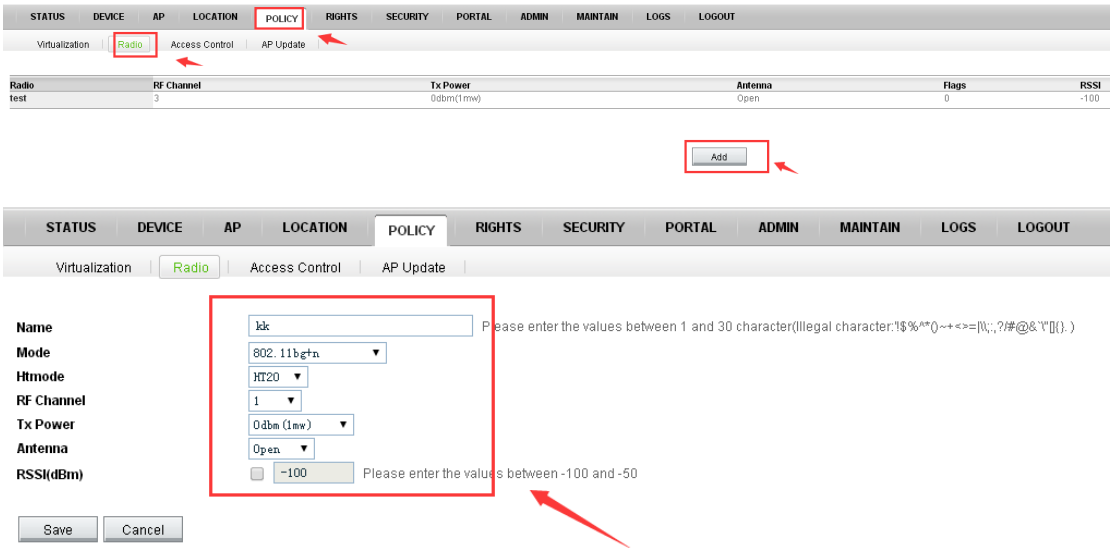
2.3.2.2. Expected Results

- Different WLAN policy can be allocated to different AP. By creating multiple VSLAN, and applying different Portal policy and Authentication policy to each VSLAN, as well as binding of different WLAN policy, Authentication policy and Portal policy for each network can be specified.

2.3.3. RF Management can be achieved

2.3.3.1. Pre-Setup and Test Steps

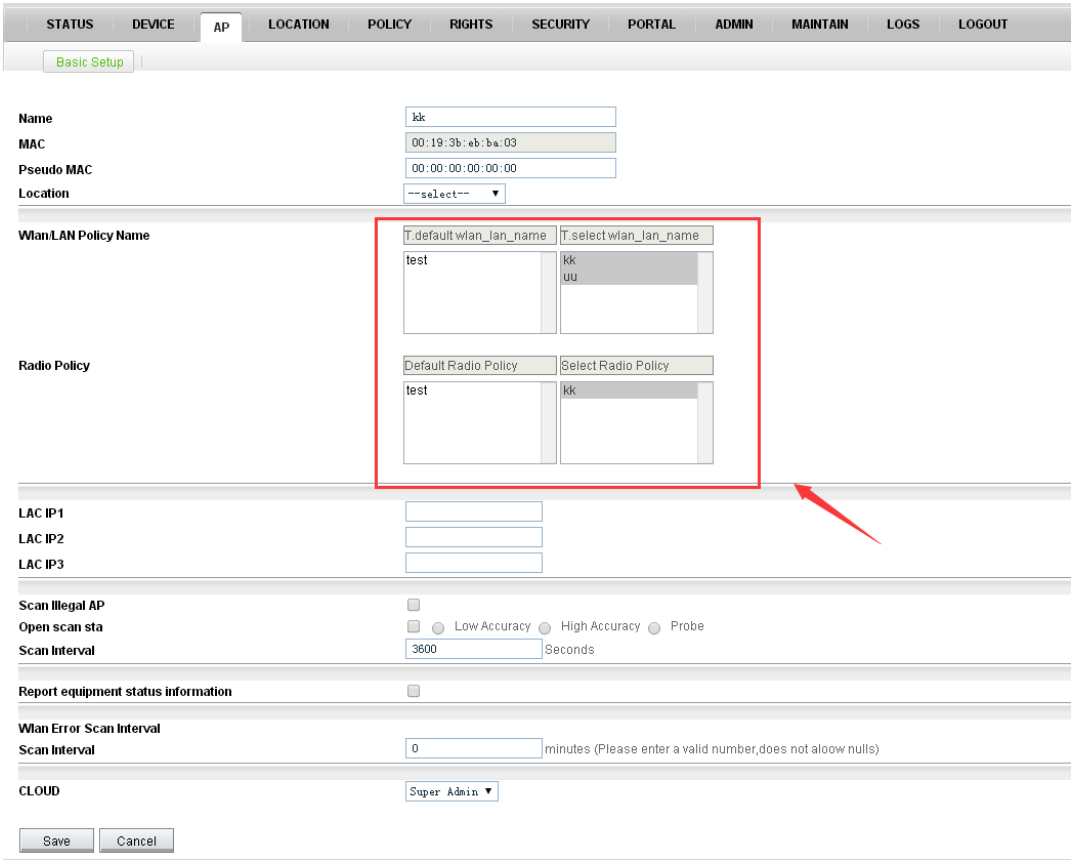
- Add Radio policy by “POLICY - Radio”



- Set radio Name, working Mode, RF channel, Tx Power and Antenna. Save the Radio policy.

2.3.3.2. Expected Results

- Return to AP module and assign the Radio policy to the AP. The Radio policy applies successfully.



2.4. Dynamic VPN

2.4.1. Pre-Setup and Test Steps

- Create VSLAN interface by “Device - Ports”; set IP address under IP module; set DHCP domain under DHCP module
- Create all WLAN policies and apply them to the corresponding VSLAN; then apply WLAN templates to corresponding AP, which will broadcast SSID

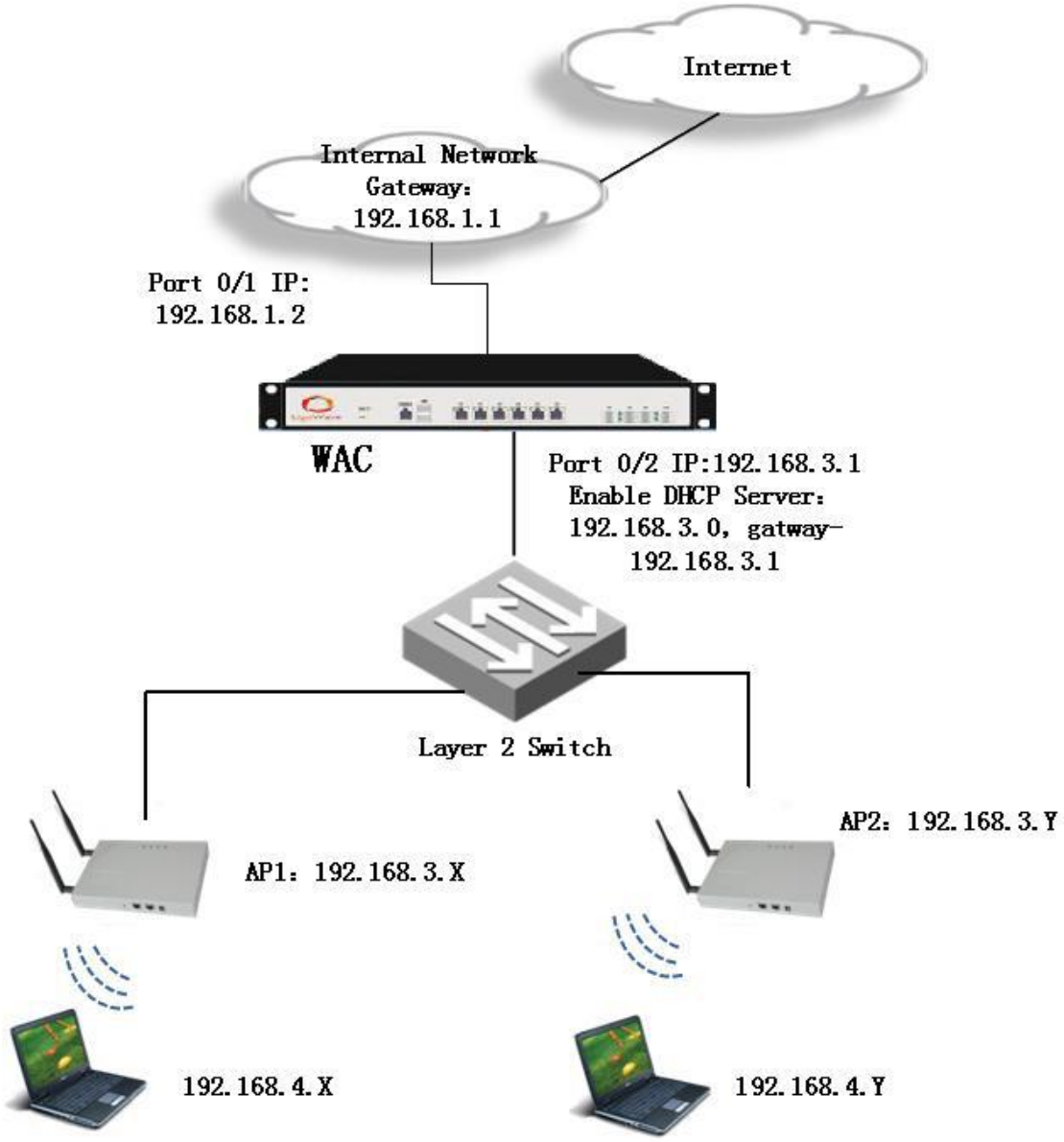
2.4.2. Expected Results

- Using a portable AP and LAC/WAC to create a VPN. As long as the network server is reachable through IP route, we can access the network resources through the VPN without complicated VPN configuration by having an AP connected to internet.

3. Chapter 3
Basic Examples and Configuration Process

3.1. Centralized forwarding mode in a single WAC topology

3.1.1. Network Topology

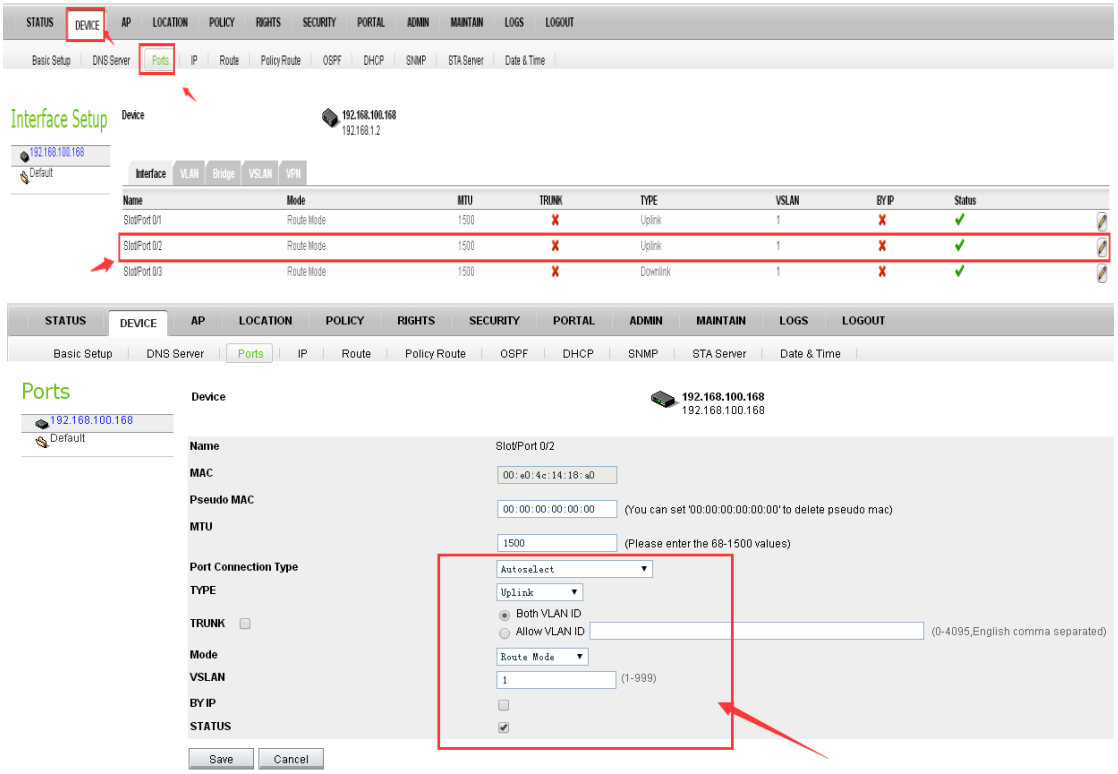


3.1.2. Configuration Steps

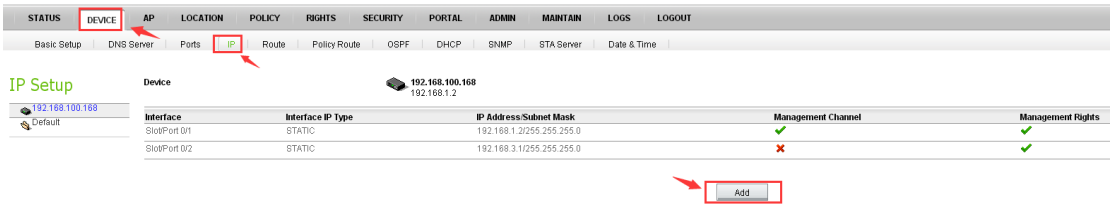
3.1.2.1. Configure management and access control port

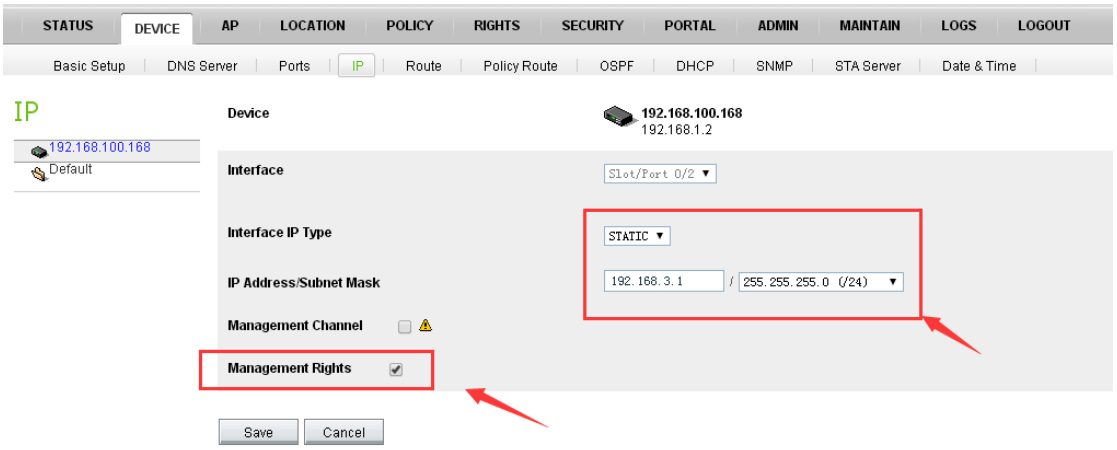
Connect your PC to port 0/1 of the WAC (port0/1 is the default management and access control port), only one control port can be set up, log in the WAC management interface via default IP address 192.168.100.168 *(IP of the PC must match the subnet)*

- By option DEVICE - Ports - Interface, enable port 0/2and set it to uplink interface, click “Save”

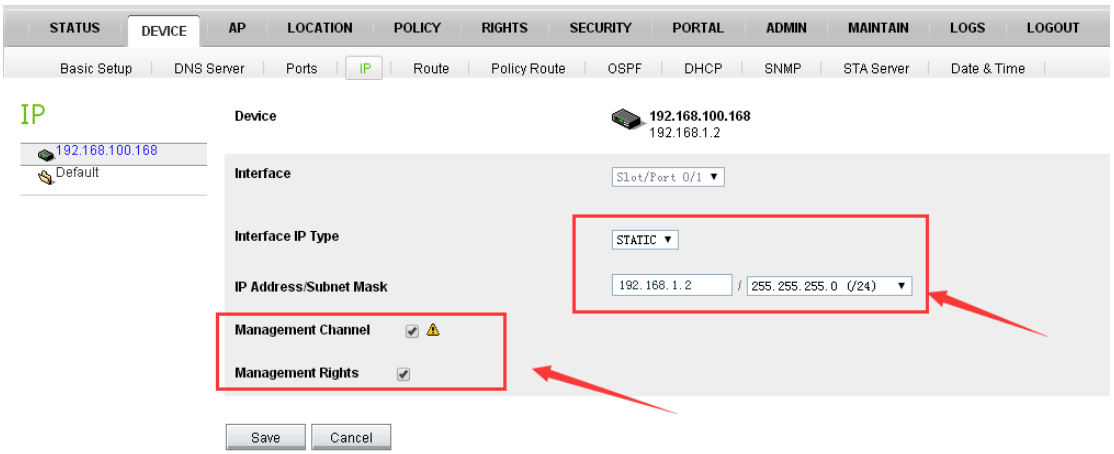


- By option DEVICE - IP, click “Add” to set the port0/2 IP to 192.168.3.1, enable “Management Rights” and click “Save”





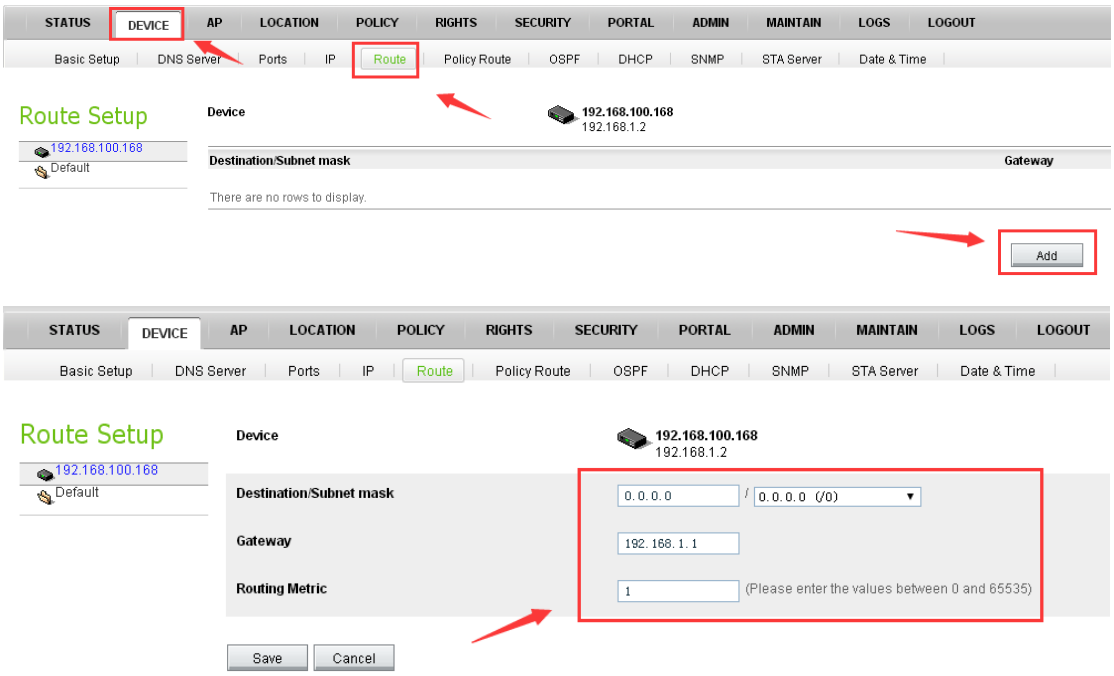
- Re-login the WAC management interface through port0/2 (IP of the PC must match the subnet). By option DEVICE– IP, change the IP of port 0/1 to a intranet IP so that the WAC can access the internet, such as 192.168.1.2, click “Save”



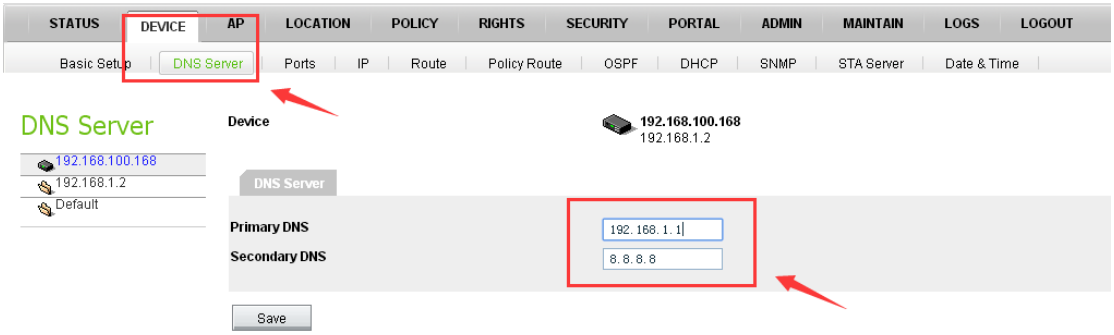
- Connect the WAC to your internal network through port 0/1 and connected a switch to port 0/2 of the WAC, after that we can manage the WAC by connect a PC to your internal network or the switch connected to port 0/2

3.1.2.2. Configure Route and DNS

- By option DEVICE - Route, add the destination routing, all the destination IP will be directed to internal network gateway 192.168.1.1

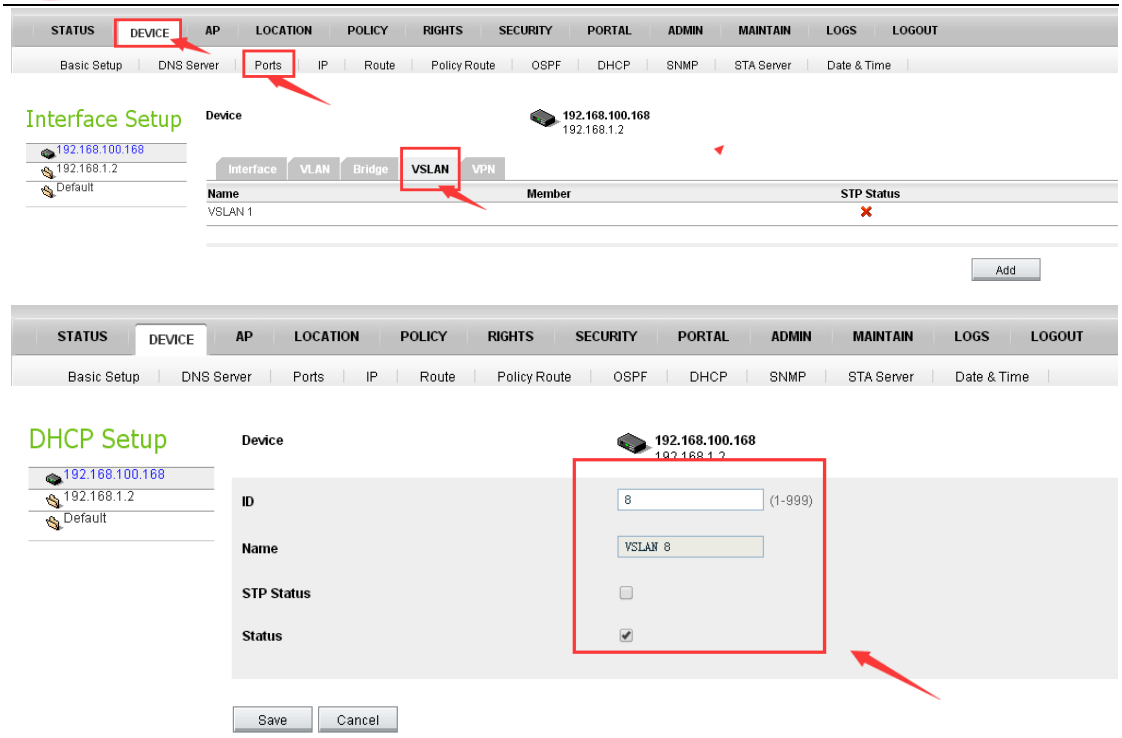


- By option DEVICE - DNS Server, configure the Primary and secondary DNS as the same as the internal network DNS

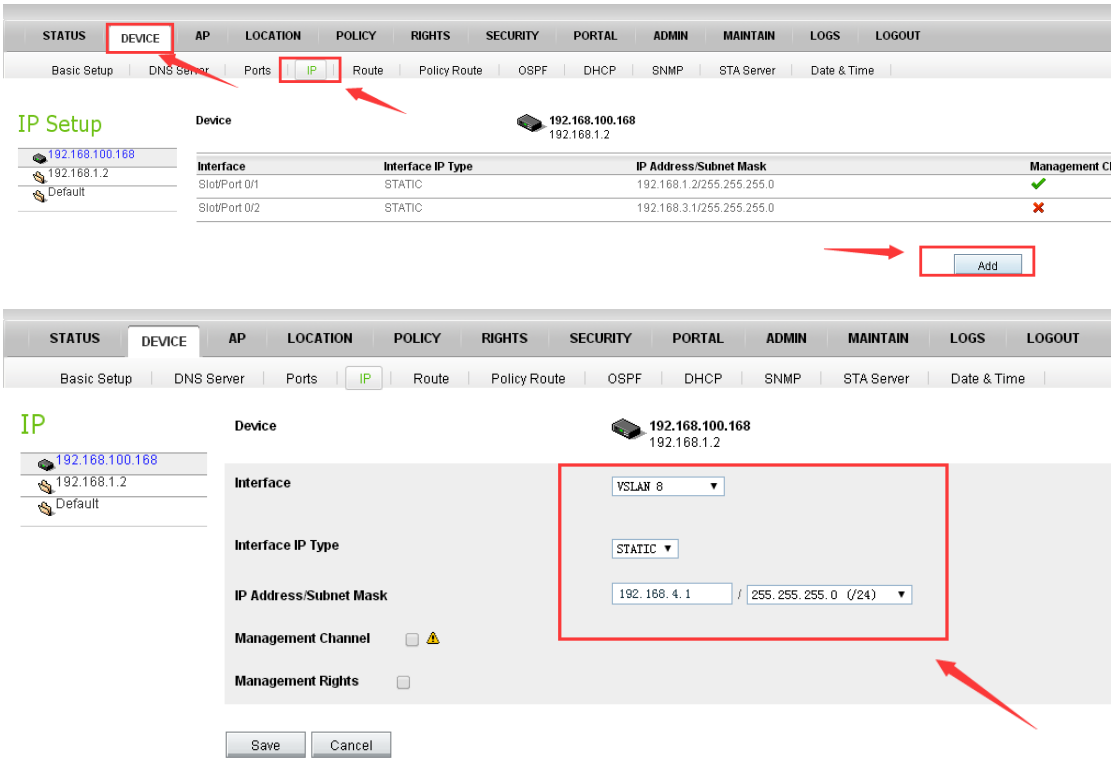


3.1.2.3. Configure VSLAN Interface

- By option DEVICE - Ports, add a VSLAN interface(This interface is used for wireless clients authentication and assigning IP to clients in the centralized forwarding mode), for example VSLAN8, click “Save”

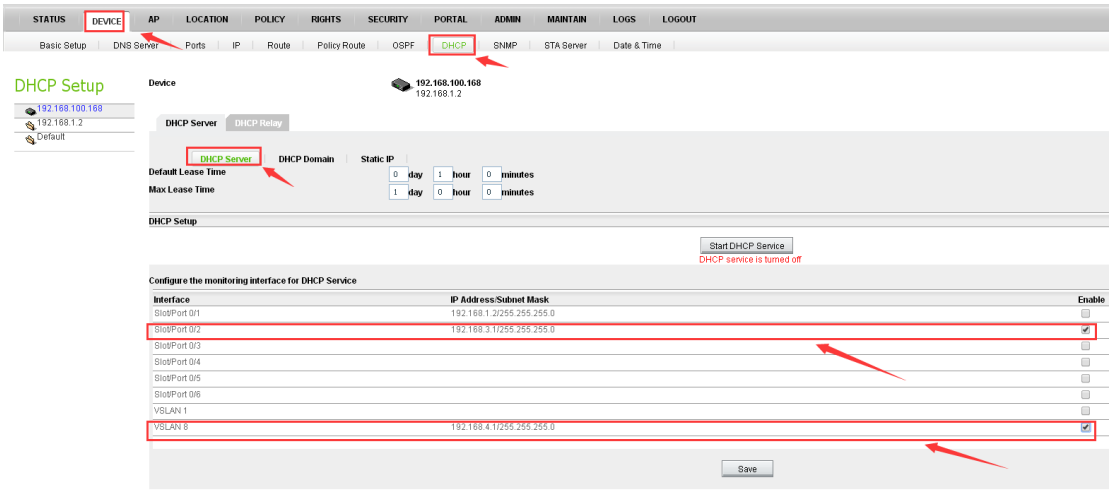


- By option DEVICE - IP, add the new IP 192.168.4.1 for VSLAN 8, as shown below

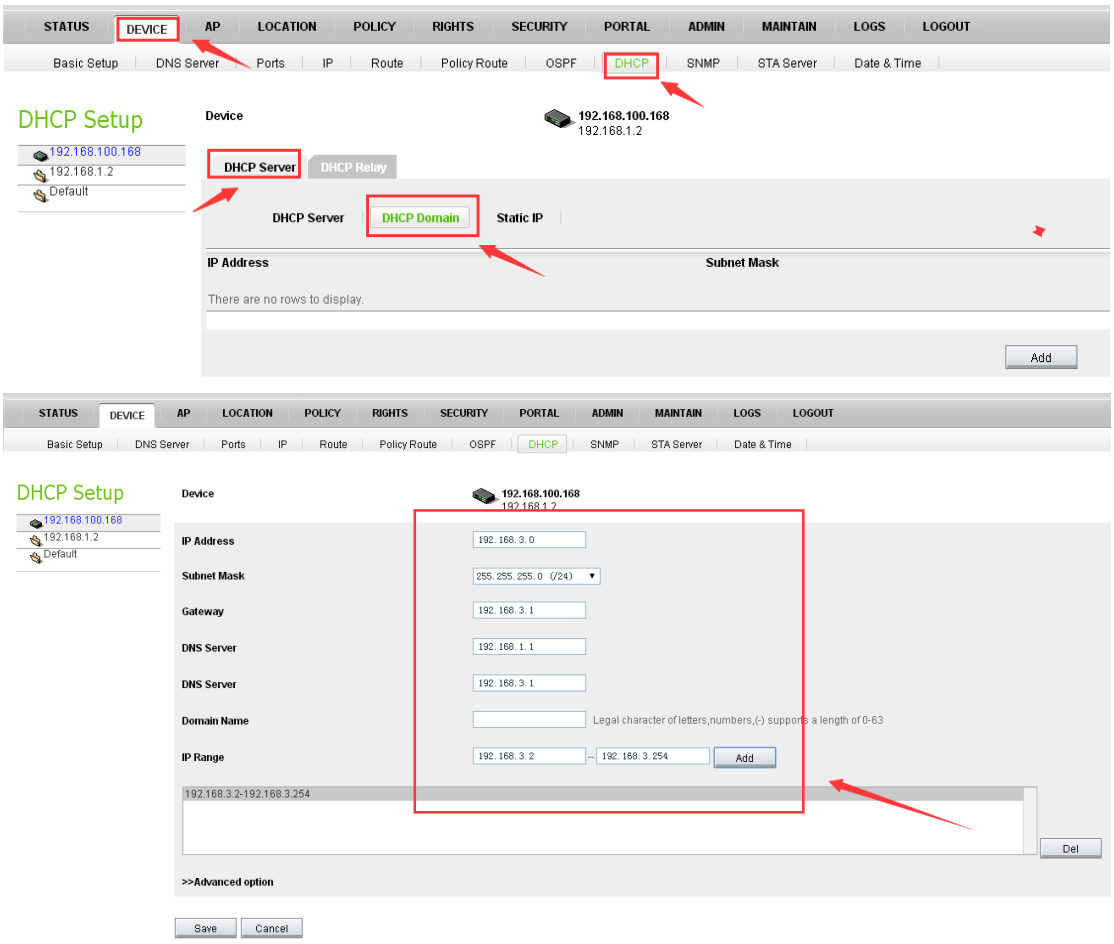


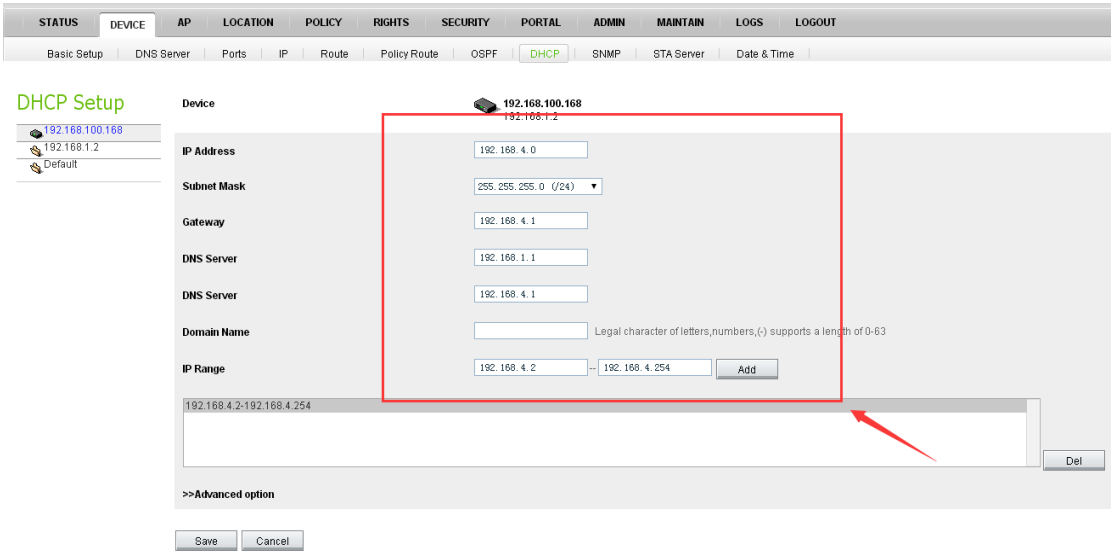
3.1.2.4. Configure DHCP Service

- By option DEVICE - DHCP - DHCP Server, enable port0/2 and VSLAN 8 for the DHCP service monitoring interface and click “Save”

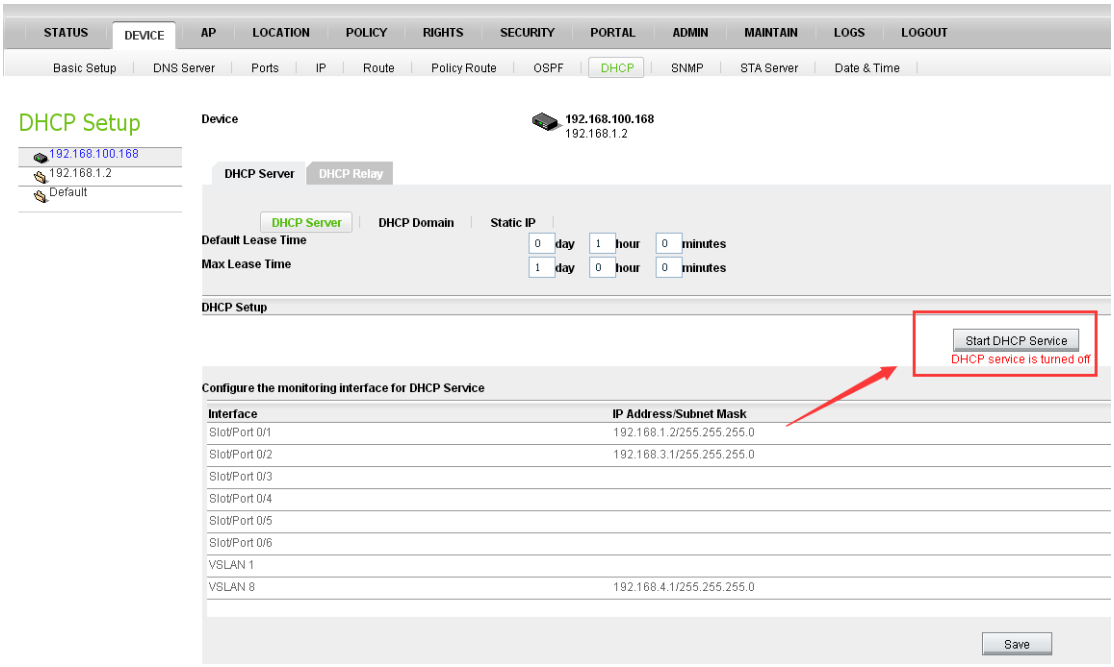


- By option DEVICE - DHCP - DHCP Server - DHCP Domain, add the IP address pool for port 0/2 and VSLAN 8, as shown below



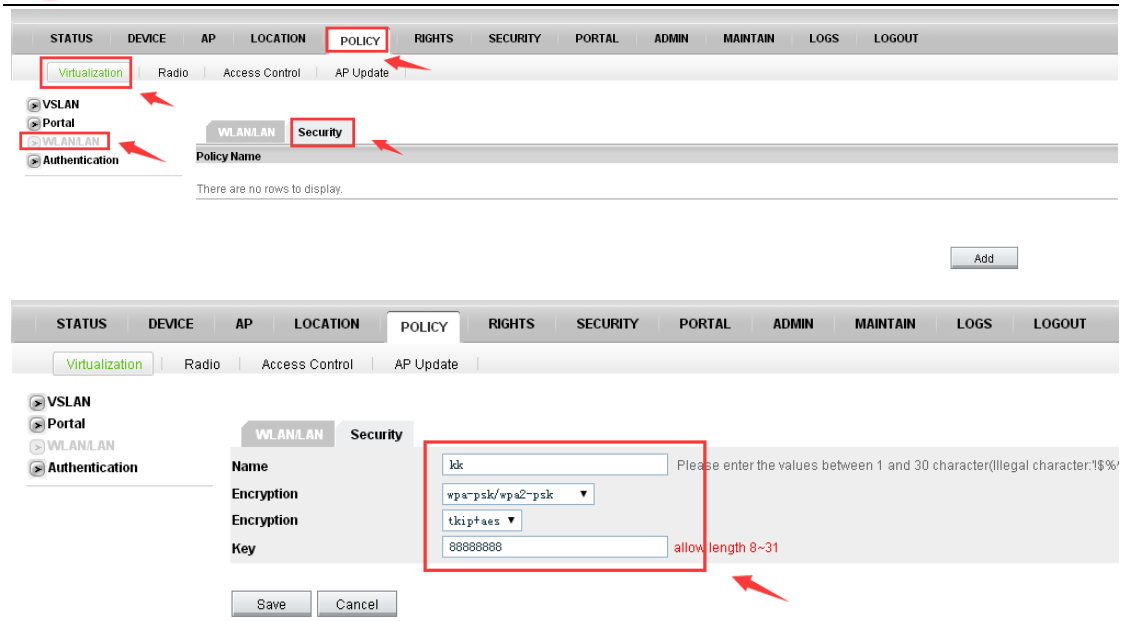


- Click “Save” and return to the DHCP server option, enable DHCP service by click the button “Start DHCP Service”

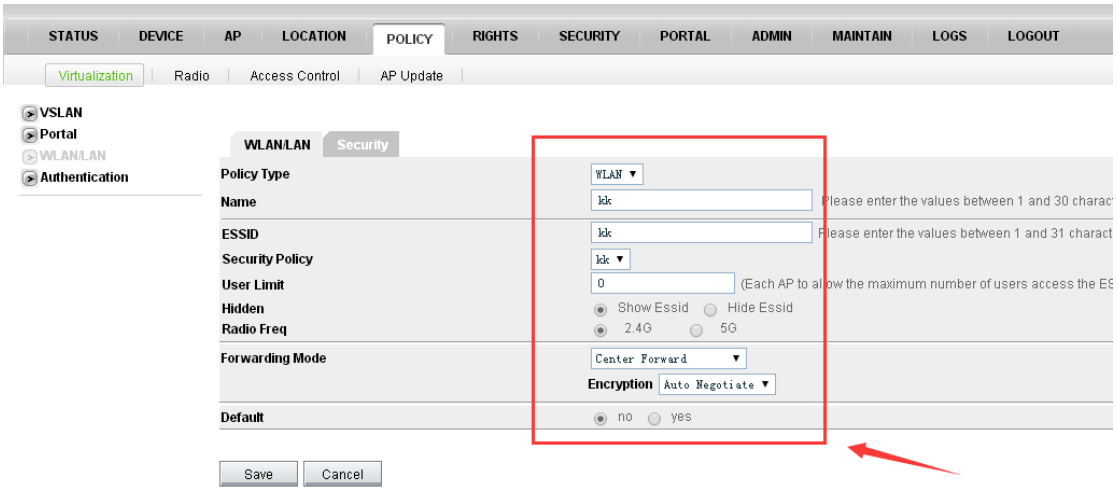


3.1.2.5. Policy Configuration

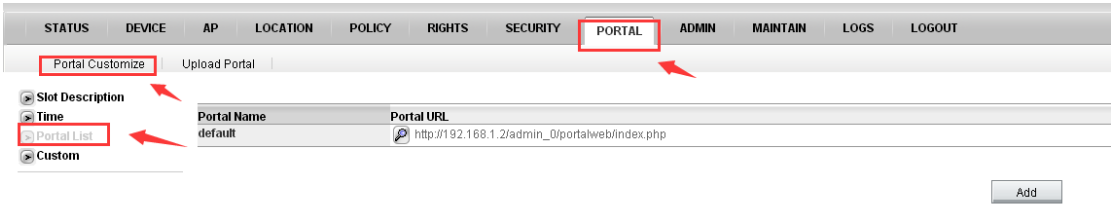
- Naming policies according to the actual needs, in this case we use “kk” for naming all policies
- By option POLICY - Virtualization - WLAN/LAN - Security, add security policy, like “kk”, click “Save”:

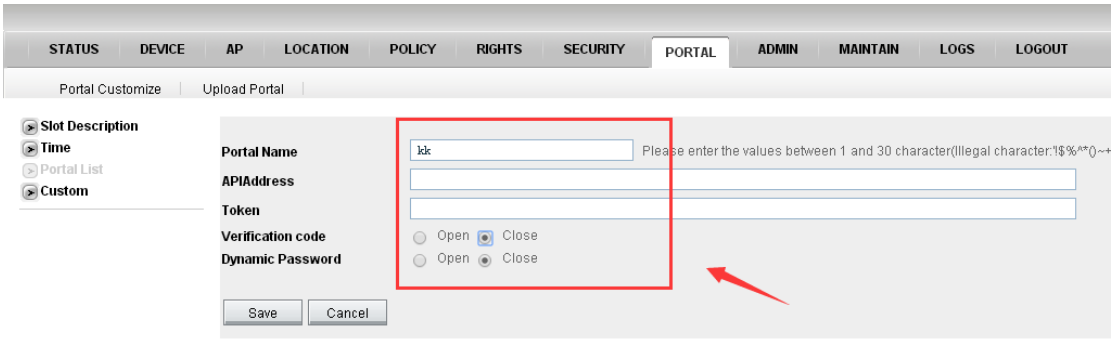


- By option POLICY - Virtualization - WLAN/LAN, add WLAN policy, like “kk”, select the security policy “kk” created in last step for encryption, if your wireless network does not require encryption you can select open, click “Save”:



- By option PORTAL - Portal Customize - Portal List, add a new built-in portal, named “kk”, and save:

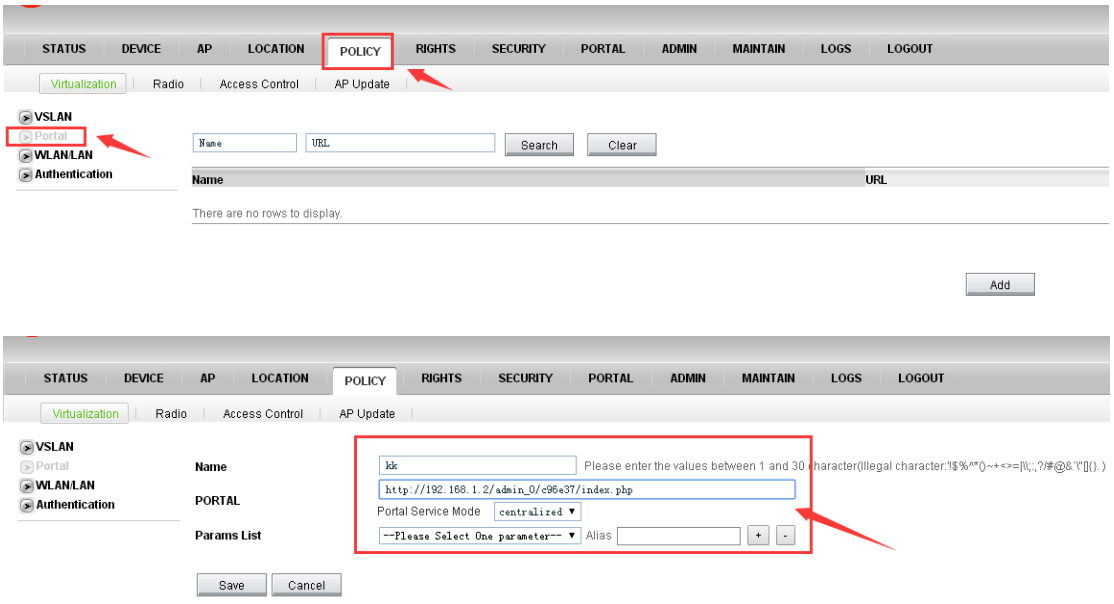




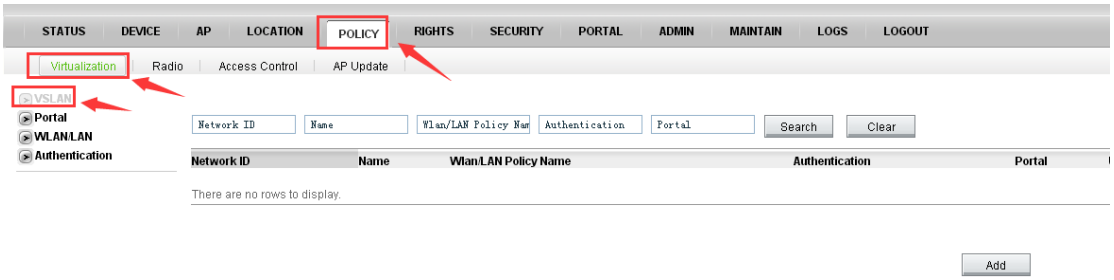
NOTE:If verification code is needed, select open, in this case we select close

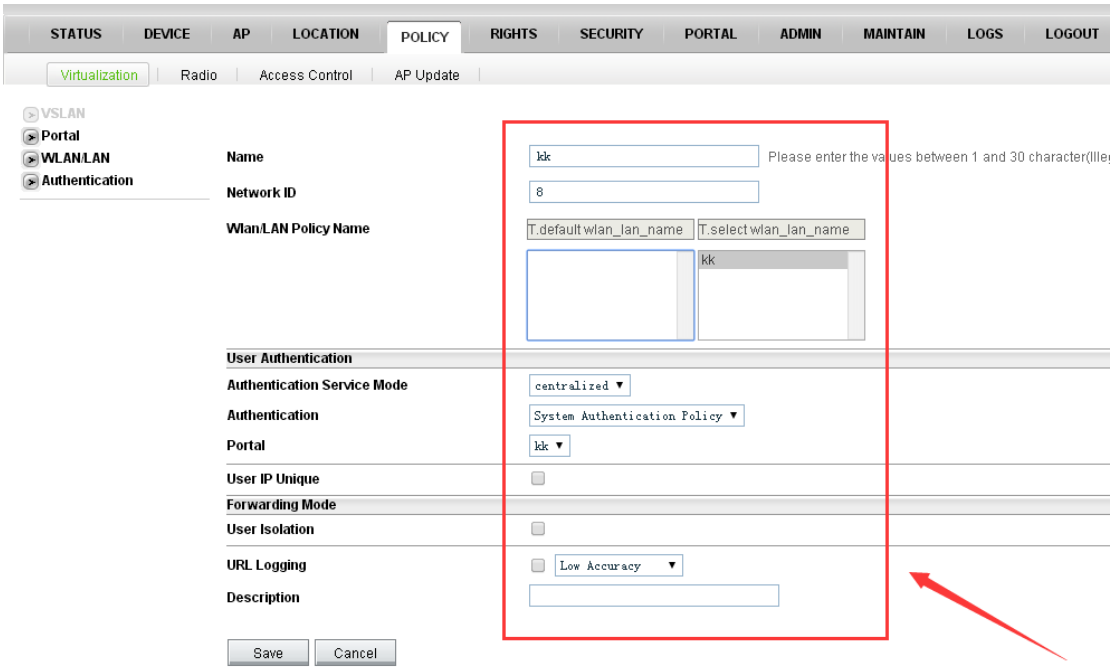
- Return to portal list and copy the url of the newly created portal which named "kk"

- By option POLICY - Portal, add a portal policy named “kk”, paste the url which copied in the previous step into the textbox, and save, as shown below:

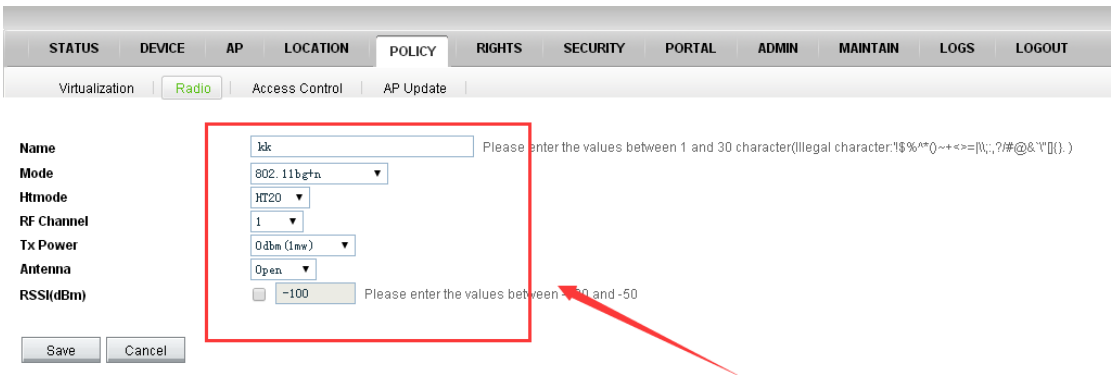


- By option POLICY - VSLAN, add a VSLAN policy named “kk”, fill in the Network ID field with the VSLAN interface ID that enabled in the previous step. So here enter the number 8, bind the newly created WLAN policykk and the portal policy kk, as shown below:



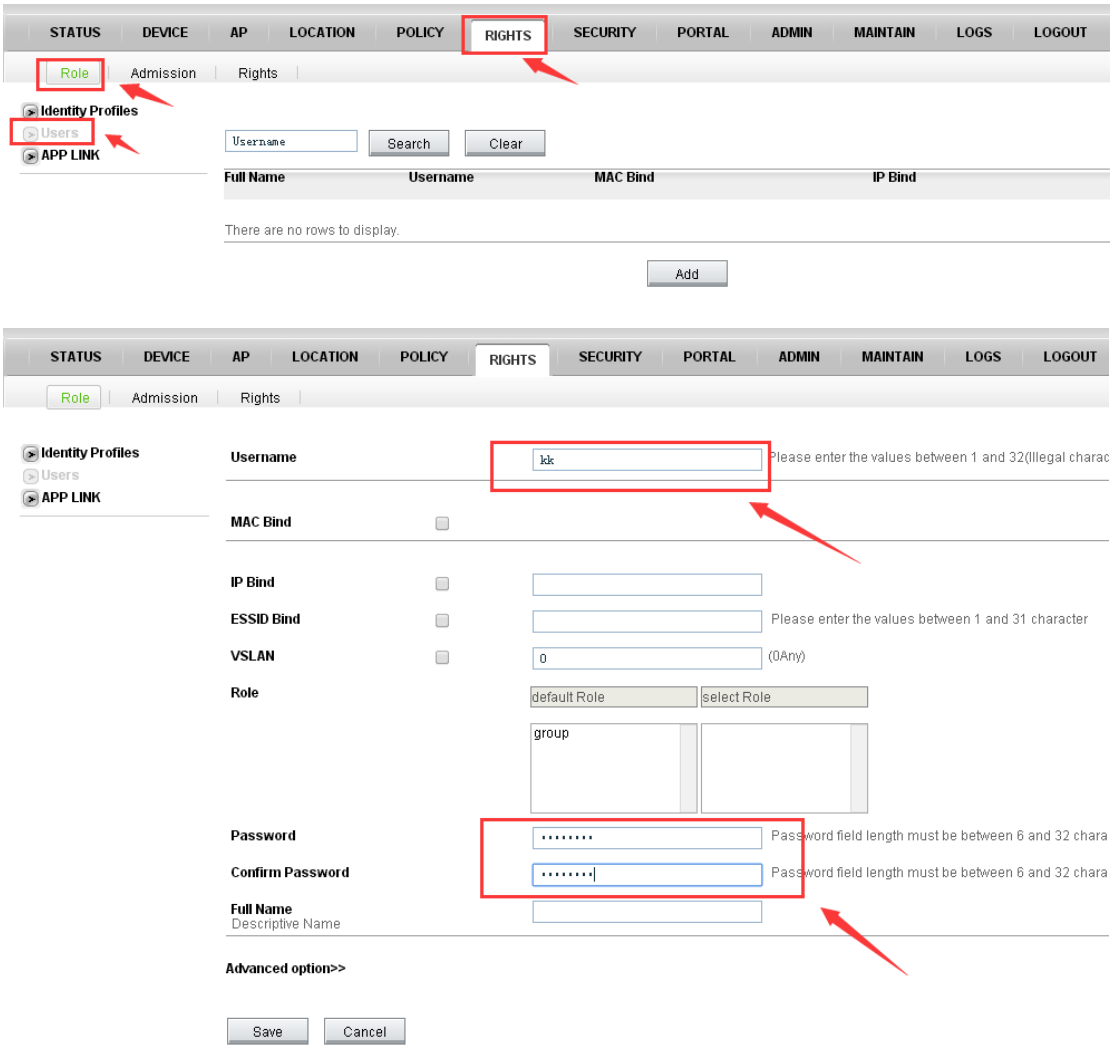


- By option POLICY - Radio, add a Radio policy named “kk”, and save, as shown below:



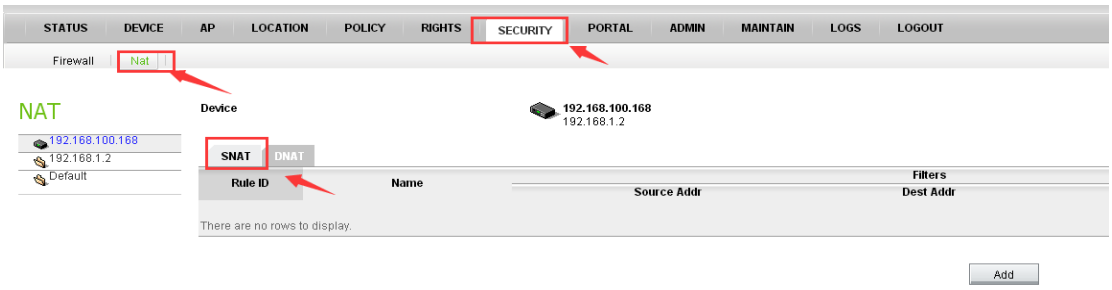
3.1.2.6. Add Users

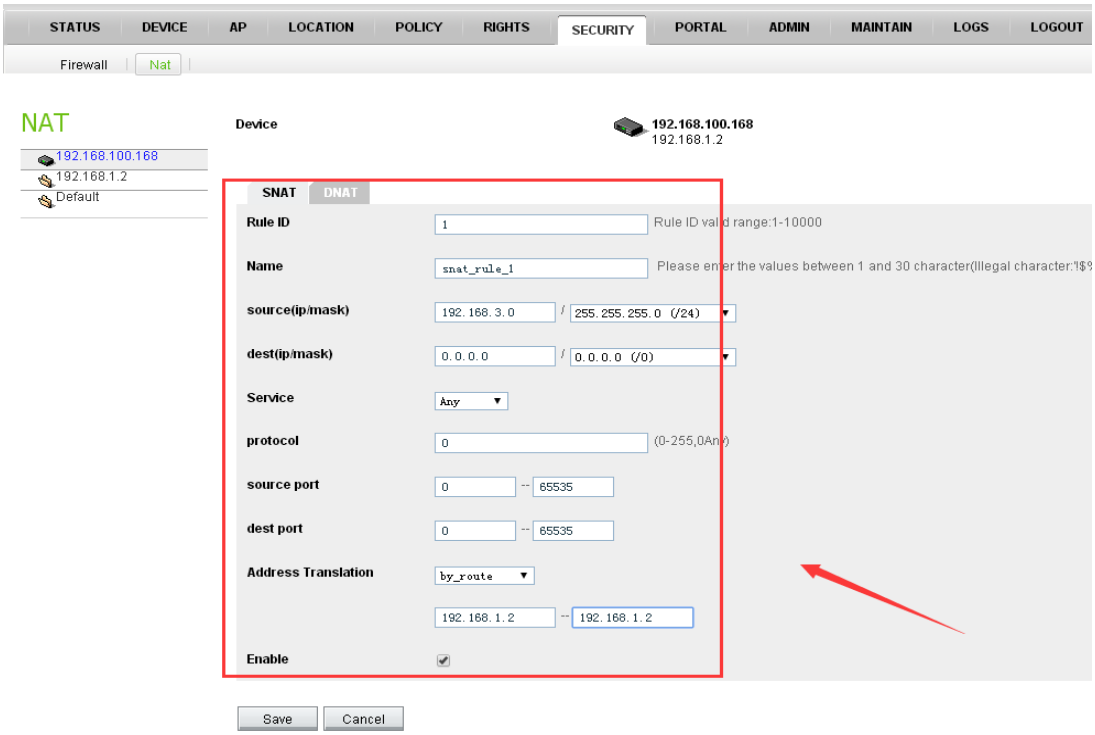
- By option RIGHTS - Users, add a user (for client authentication via portal page) and save, as shown below

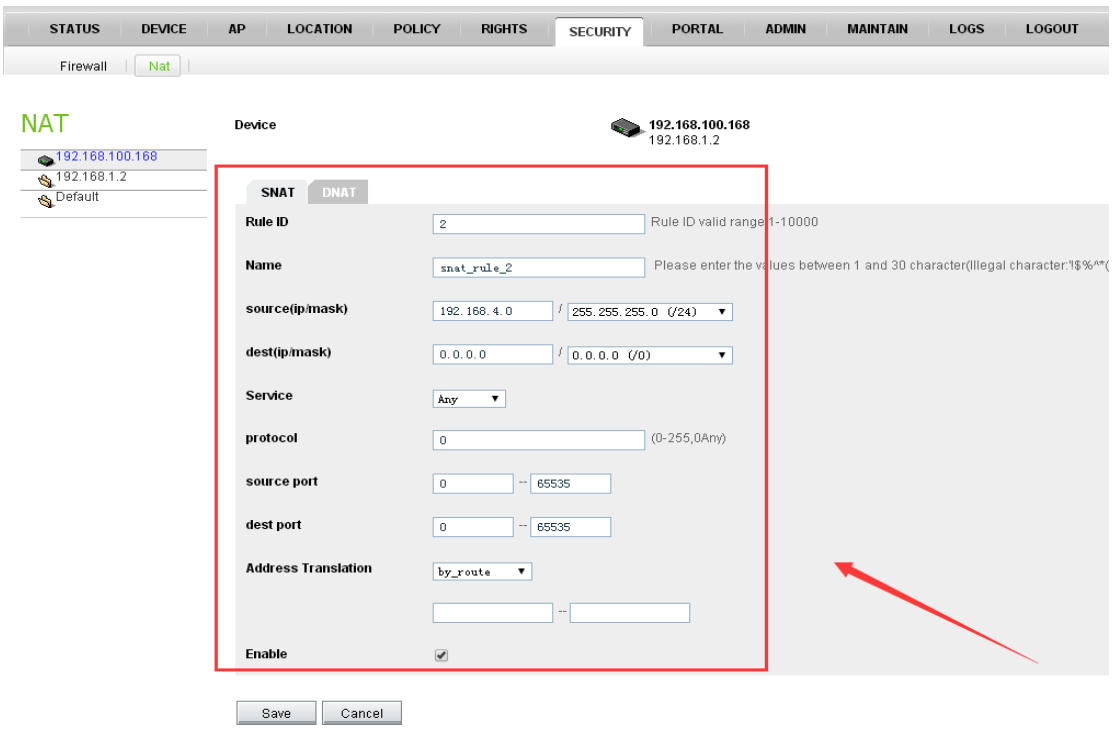


3.1.2.7. Add NAT Rules

- By option SECURITY - Nat - SNAT, add NAT rules, Convert IP 192.168.3.0 and 192.168.4.0 to the WAC export IP 192.168.1.2 to ensure that the APs and the clients can communicate with the outside through the WAC

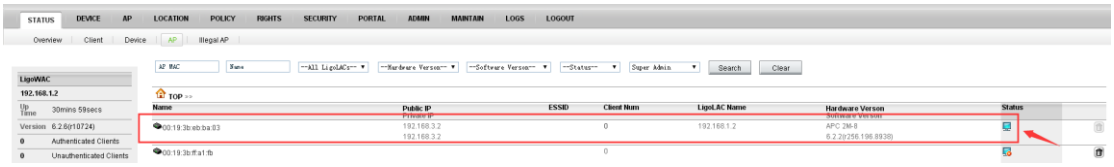

STATUS
DEVICE
AP
LOCATION
POLICY
RIGHTS
SECURITY
PORTAL
ADMIN
MAINTAIN
LOGS
LOGOUT
Firewall
Nat
NAT
Device
192.168.100.168
192.168.1.2
192.168.100.168
192.168.1.2
Default
SNAT
DNAT
Rule ID
Name
Filters
Source Addr
Dest Addr
There are no rows to display.
Add


STATUS
DEVICE
AP
LOCATION
POLICY
RIGHTS
SECURITY
PORTAL
ADMIN
MAINTAIN
LOGS
LOGOUT
Firewall
Nat
NAT
Device
192.168.100.168
192.168.1.2
192.168.100.168
192.168.1.2
Default
SNAT
DNAT
Rule ID
1
Rule ID valid range:1-10000
Name
snat_rule_1
Please enter the values between 1 and 30 character(Illegal character:'!$%
source(ip/mask)
192.168.3.0
255.255.255.0 (/24)
dest(ip/mask)
0.0.0.0
0.0.0.0 (/0)
Service
Any
protocol
0
(0-255,0Any)
source port
0
65535
dest port
0
65535
Address Translation
by_route
192.168.1.2
192.168.1.2
Enable
Save
Cancel

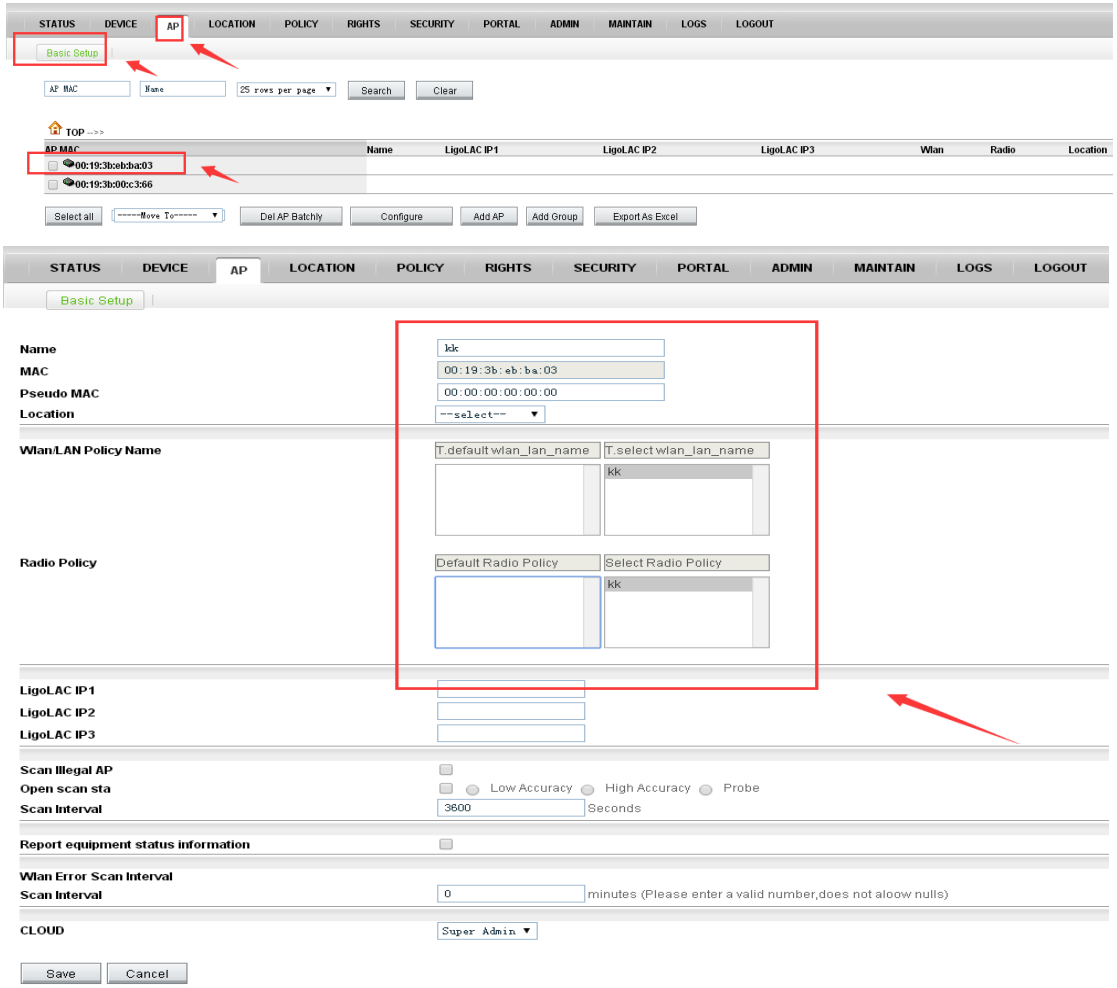

STATUS
DEVICE
AP
LOCATION
POLICY
RIGHTS
SECURITY
PORTAL
ADMIN
MAINTAIN
LOGS
LOGOUT
Firewall
Nat
NAT
Device
192.168.100.168
192.168.1.2
192.168.100.168
192.168.1.2
Default
SNAT
DNAT
Rule ID
2
Rule ID valid range:1-10000
Name
snat_rule_2
Please enter the values between 1 and 30 character(Illegal character:'!$%^"(
source(ip/mask)
192.168.4.0
255.255.255.0 (/24)
dest(ip/mask)
0.0.0.0
0.0.0.0 (/0)
Service
Any
protocol
0
(0-255,0Any)
source port
0
65535
dest port
0
65535
Address Translation
by_route
Enable
Save
Cancel

3.1.2.8. Have APs on-line and make the configuration

- Connect the AP to the switch which under port 0/2 of the WAC, the AP will get on-line to the WAC in 1-2 minutes, you will see the AP get on-line to WAC by option STATUS-AP, and the AP can obtain an IP of 192.168.3.0 assigned by port 0/2, as shown below:

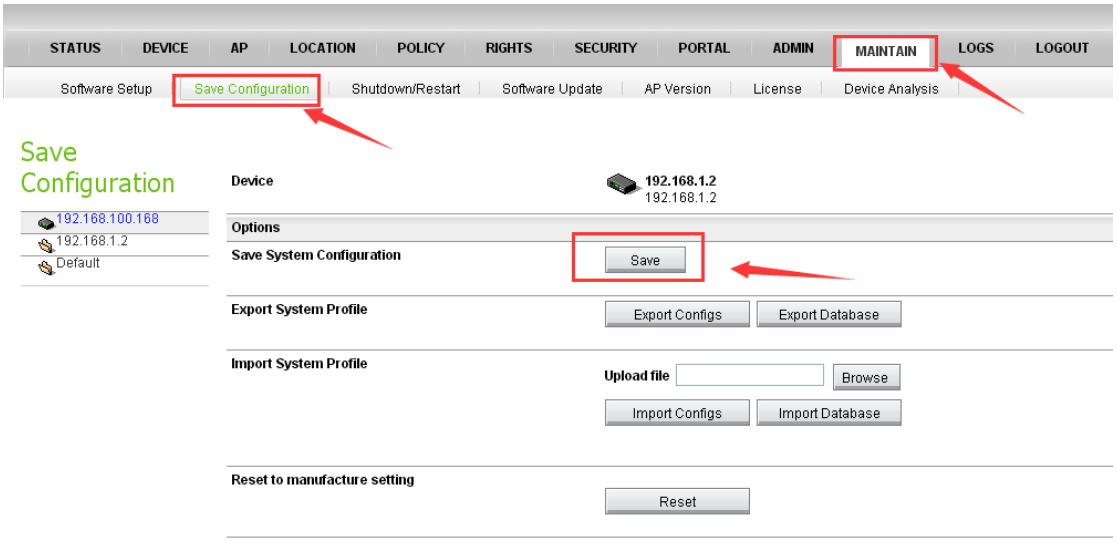


- By option AP-Basic Setup, Press the on-line AP MAC address to configure it, you can name it and bind it up with WLAN/Radio policies and so on, in this case bind the WLAN policy kk and Radio policy kk created above, click “Save”, as shown below:



3.1.2.9. Save System Configuration

- By option MAINTAIN - Save Configuration, click “Save” to save the current system configuration, as shown below:

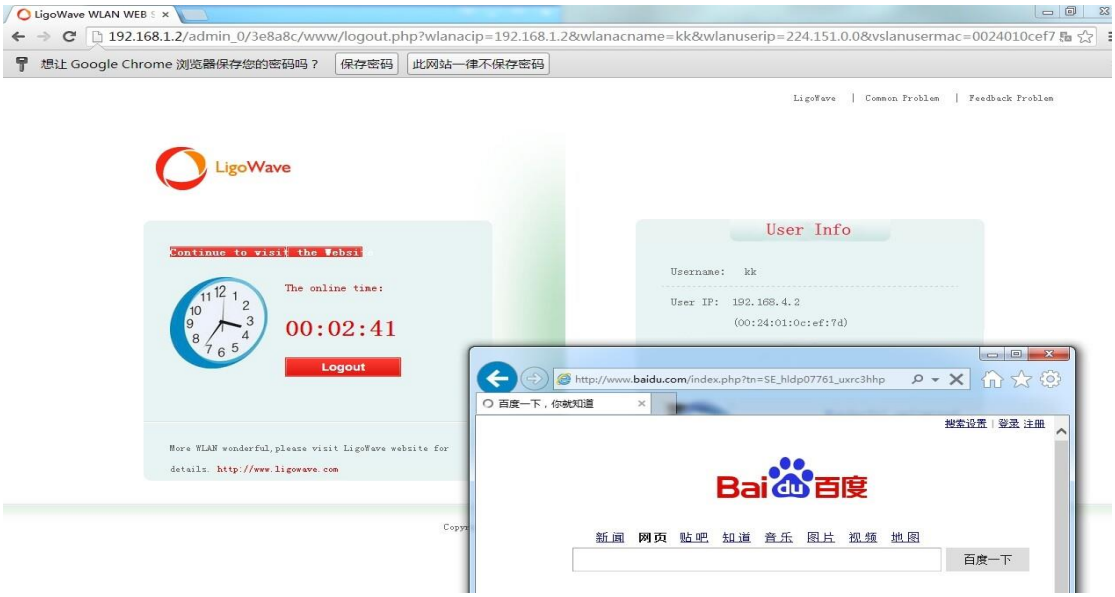


- The AP will broadcast a SSID namekk within 1 minute, connect your laptop to the SSID, the wireless network card obtains an IP address of 192.168.4.0 segment, as shown below

3.1.2.10. Get permission to access internet through portal-based authentication

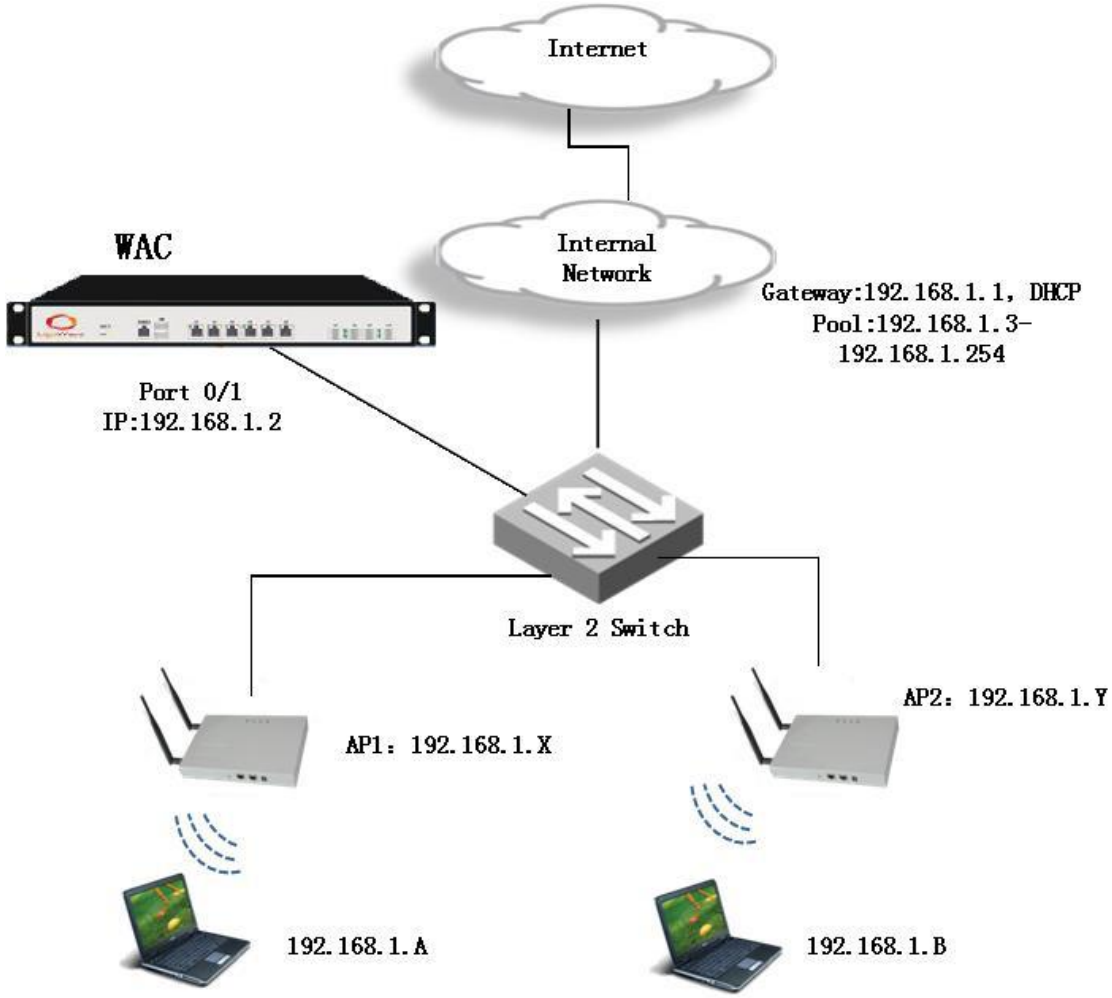
- Enter a URL to visit in your browser, like *www.baidu.com*, you can see the URL redirected to the portal page URL, as shown below

- Fill in the authentication information(the user name and password added in above steps), successfully passed authentication and the client can access internet, as shown below:



3.2. Transparent local forwarding mode in a single WAC topology

3.2.1. Network Topology



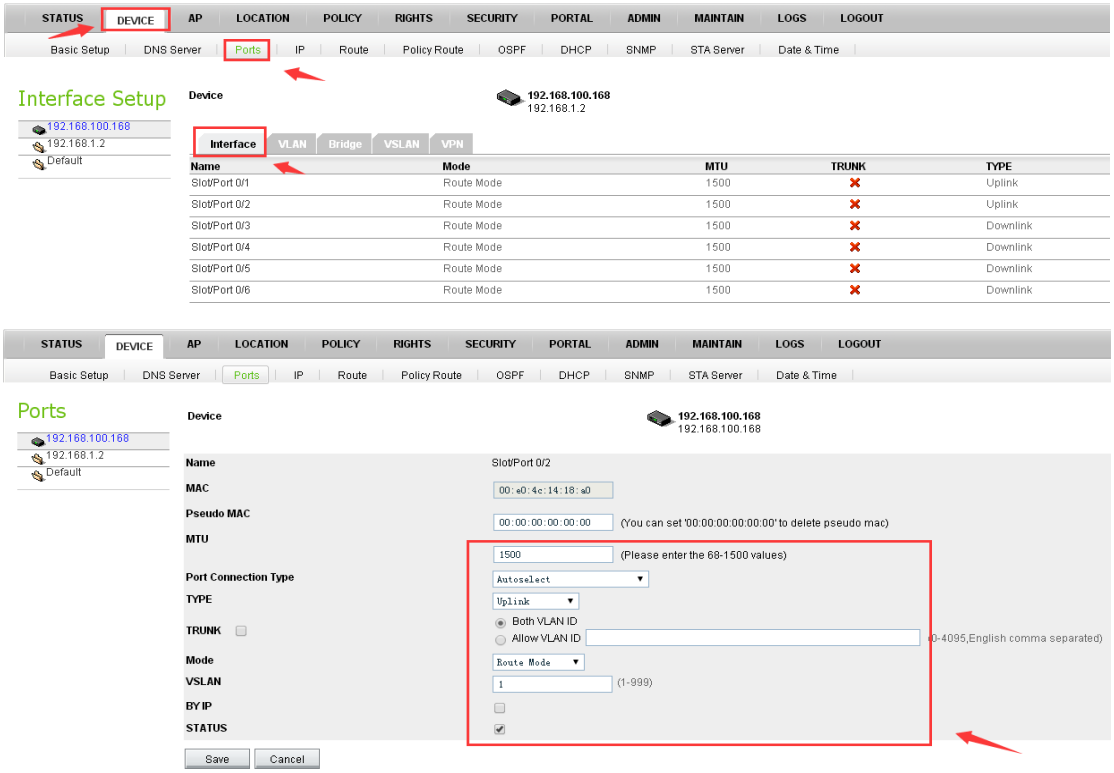
3.2.2. Configuration Steps

3.2.2.1. Configure management and access control port

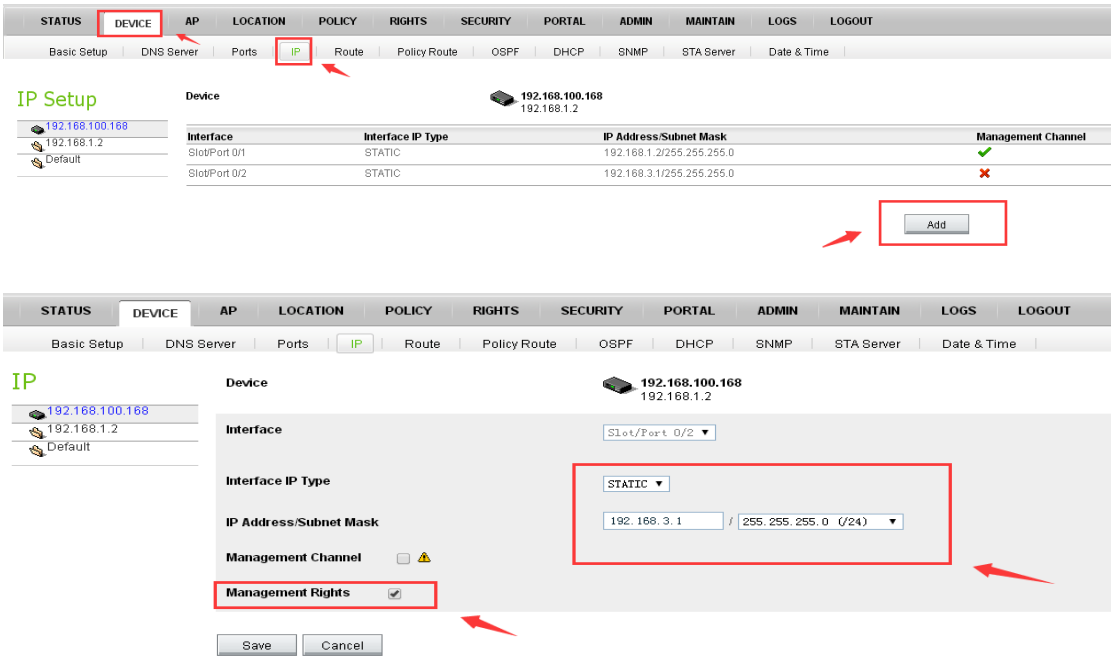
Connect your PC to port 0/1 of the WAC (port0/1 is the default management and

access control port, only one control port can be set up, log in the WAC management interface via default IP address 192.168.100.168 *(IP of PC must match the subnet)*

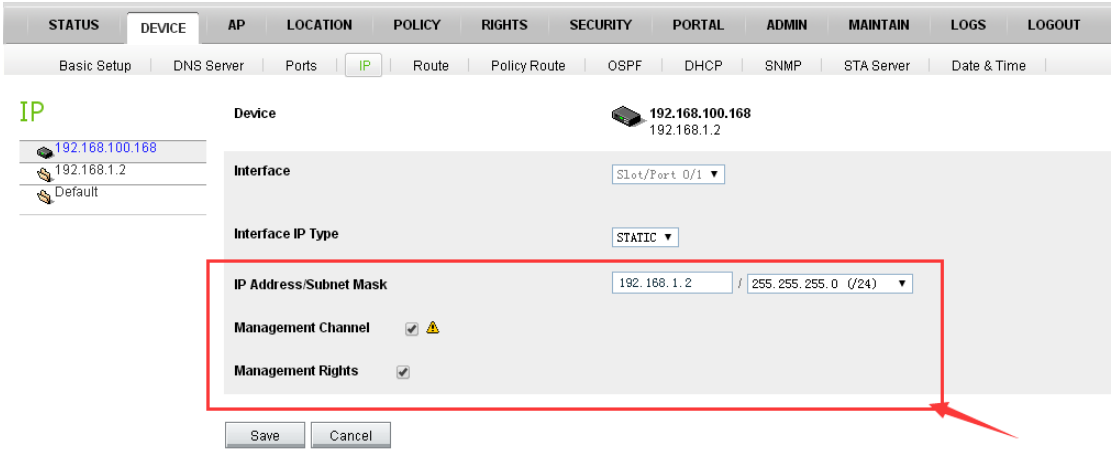
- By option DEVICE - Ports - Interface, enable port 0/2, and set it to uplink interface, click “Save”



- By option DEVICE - IP, click “Add” to set the port0/2 IP to 192.168.3.1, enable “Management Rights” and click “Save”



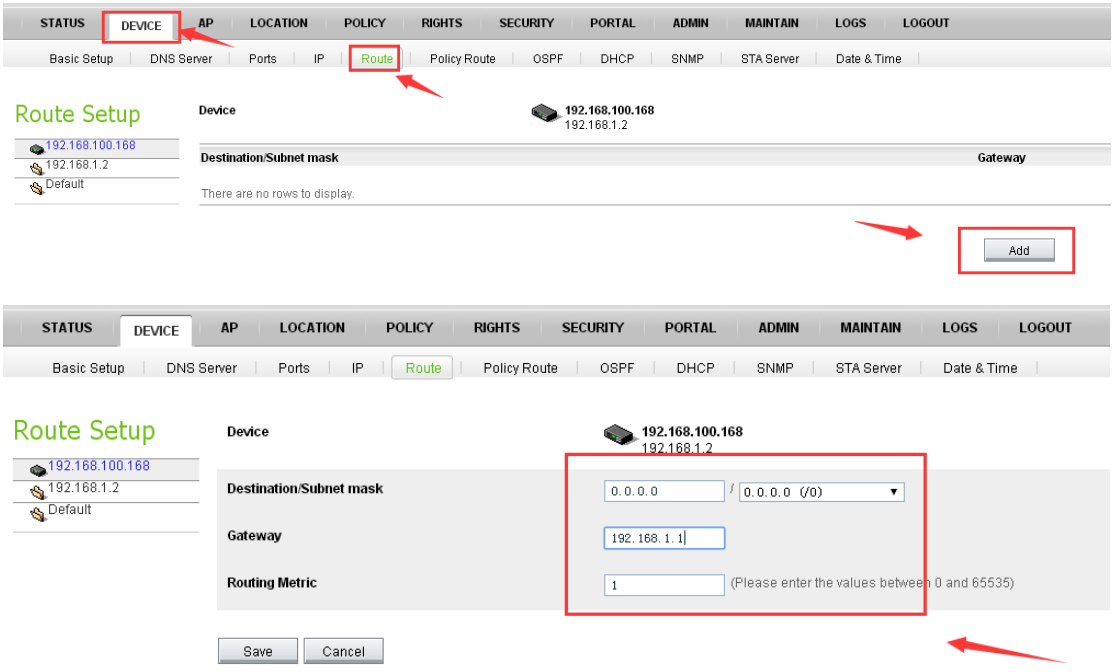
- **Re-login the WAC management interface through port 0/2*(IP of the PC must match the subnet)***, By option DEVICE - IP, change the IP of port 0/1 to a intranet IP so that the WAC can access the internet, such as 192.168.1.2, click “Save”



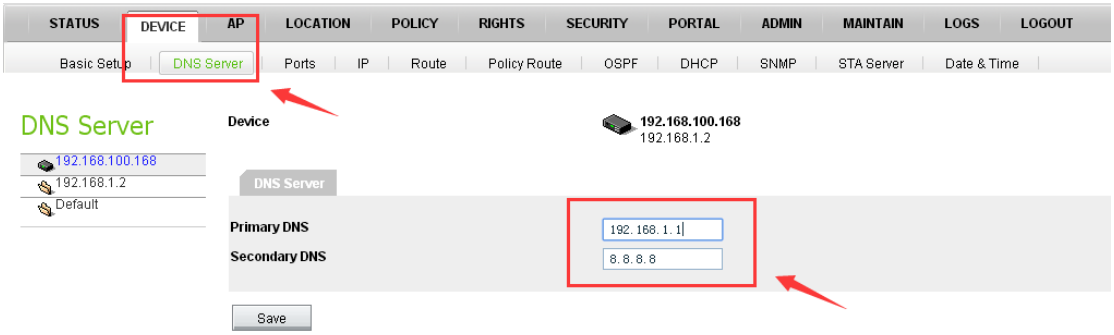
- Connect the WAC the your internal network through port 0/1 , after that you can manage the WAC by connecting your PC to the internal network or port 0/2

3.2.2.2. Configure Route and DNS

- By option DEVICE - Route, add the destination routing, all the destination IP will be directed to the internal network gateway 192.168.1.1

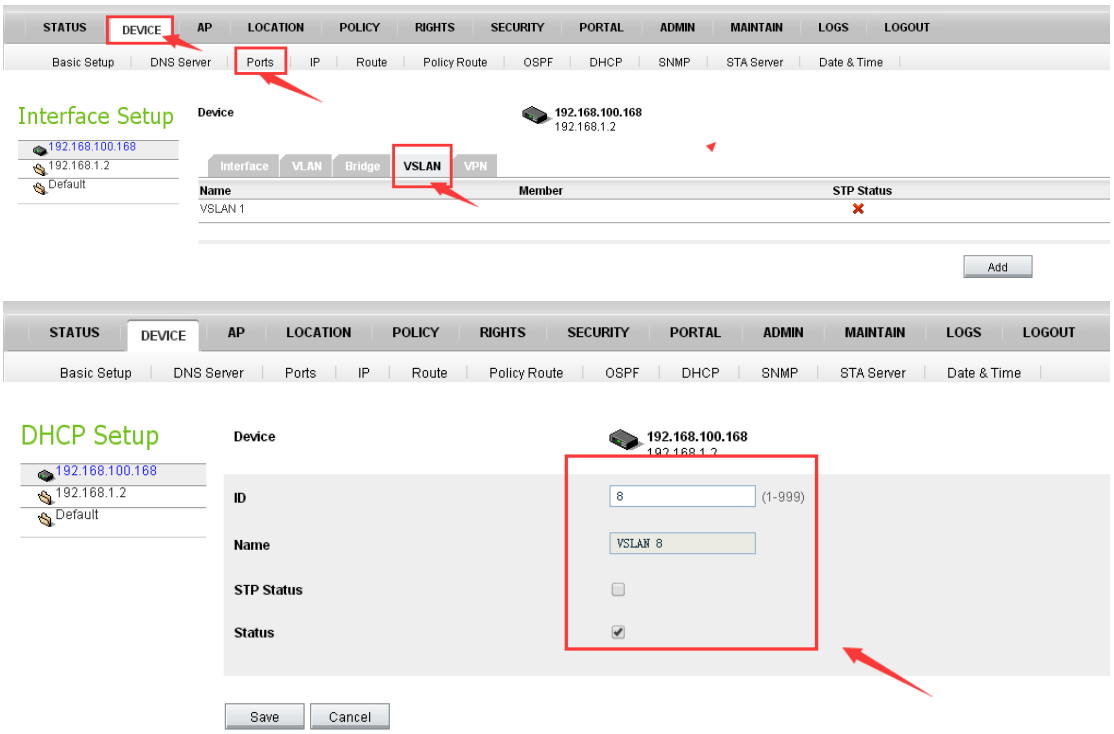


- By option DEVICE - DNS Server, configure the Primary and Secondary DNS as the same as the internal network DNS



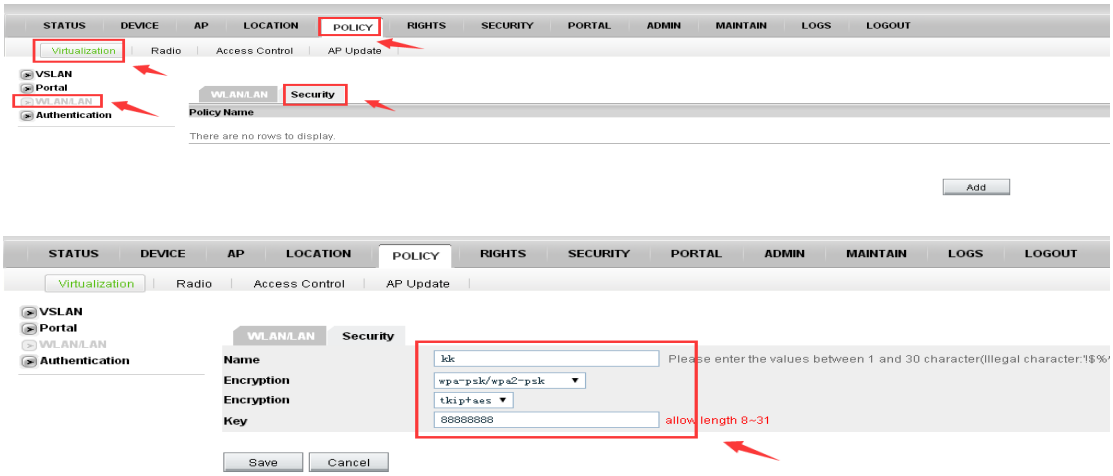
3.2.2.3. Configure VSLAN interface

- By option DEVICE - Ports, add a VSLAN interface (This interface is used for wireless clients authentication), for example VSLAN 8, click “Save”

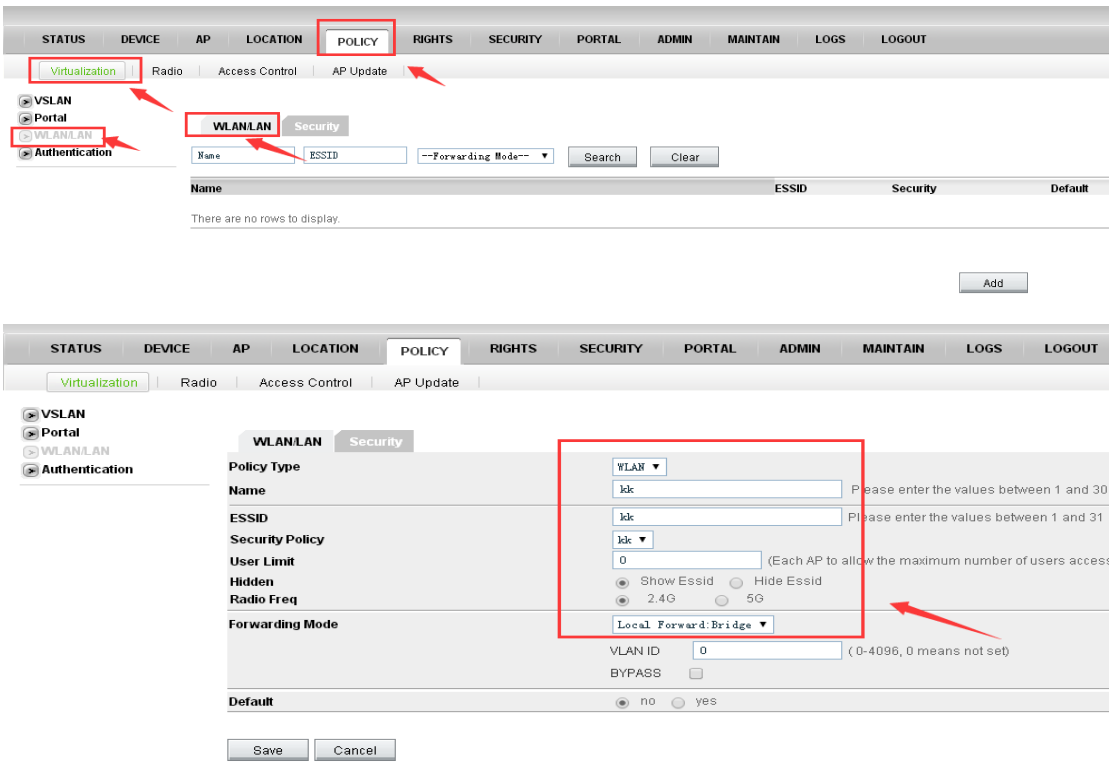


3.2.2.4. Policy Configuration

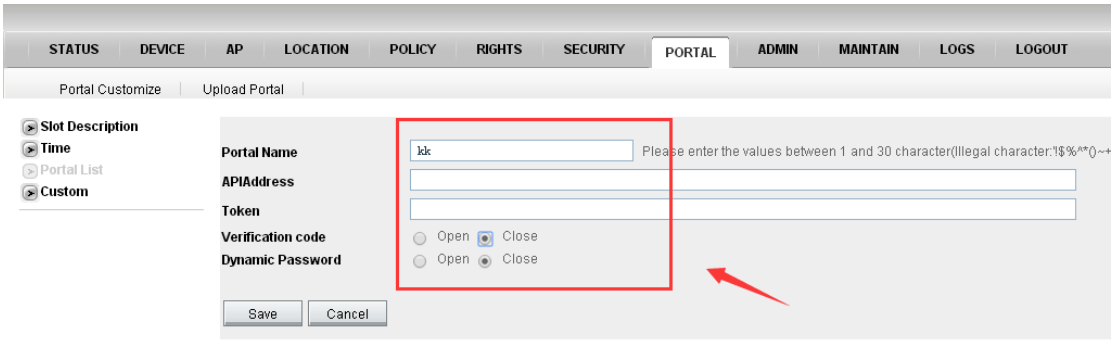
- Naming policies according to the actual needs, in this case we use “kk” for naming all policies
- By option POLICY - Virtualization - WLAN/LAN - Security, add Security policy, like “kk”, click “Save”:



- By option POLICY - Virtualization - WLAN/LAN, add WLAN policy “kk”, select the Security policy “kk” created in the last step for encryption, if your wireless network does not require encryption you can select “open”, click “Save”:



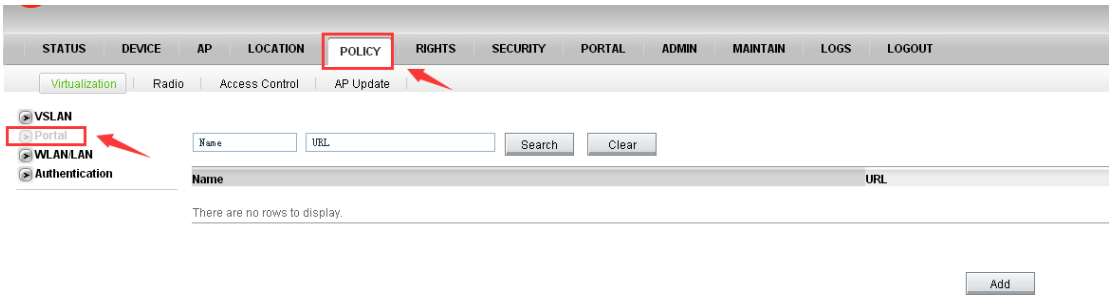
- By option PORTAL - Portal Customize - Portal List, add a new built-in portal, named “kk”, and save:

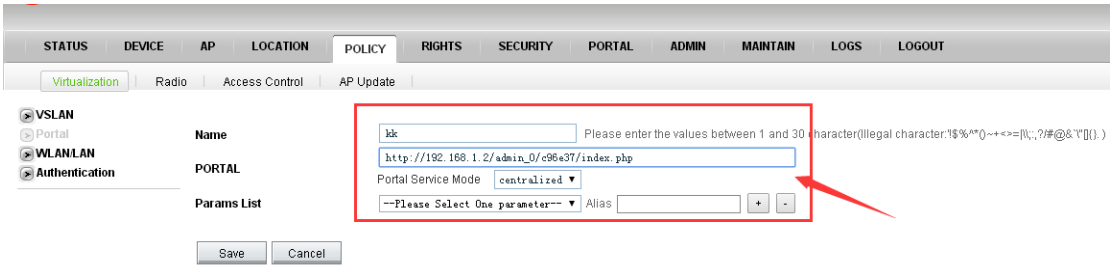


NOTE:If verification code is needed, select open, in this case we select close

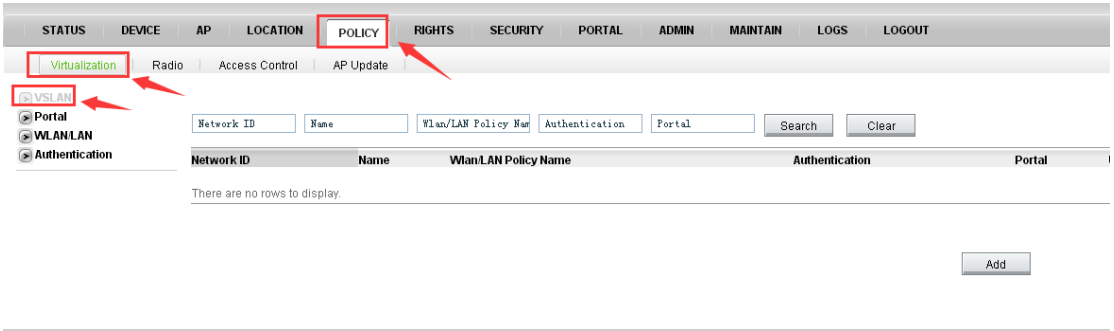
- Return to portal list and copy the URL of the newly created portal which named "kk"

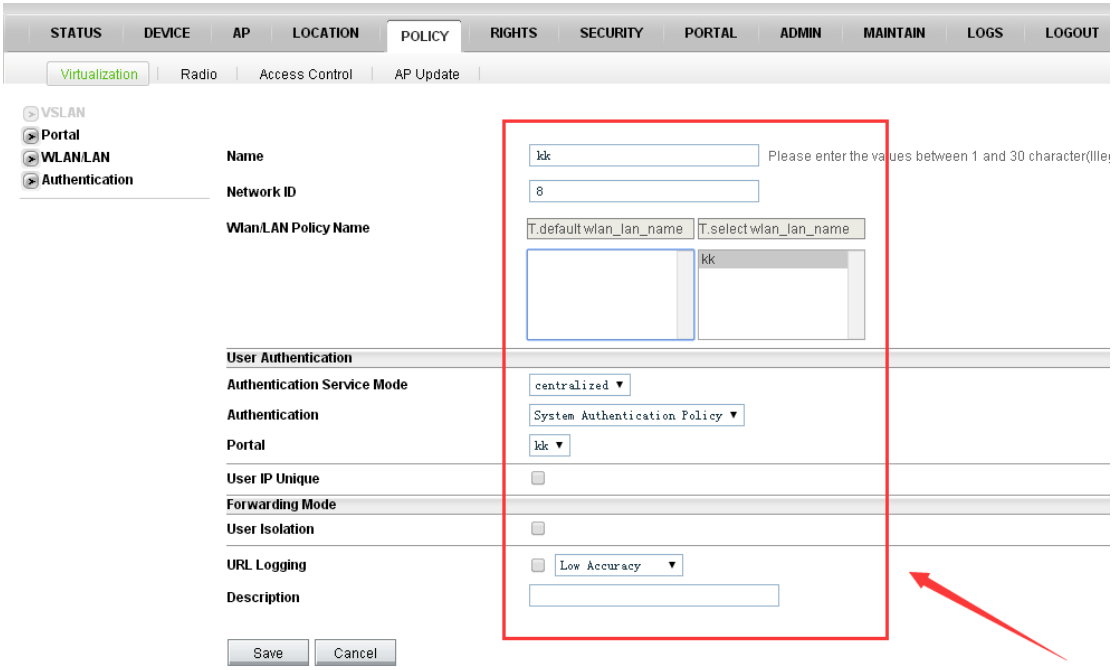
- By option POLICY - Portal, add a Portal policy named “kk”, paste the URL which copied in previous step into the PORTAL field, and save, as shown below:



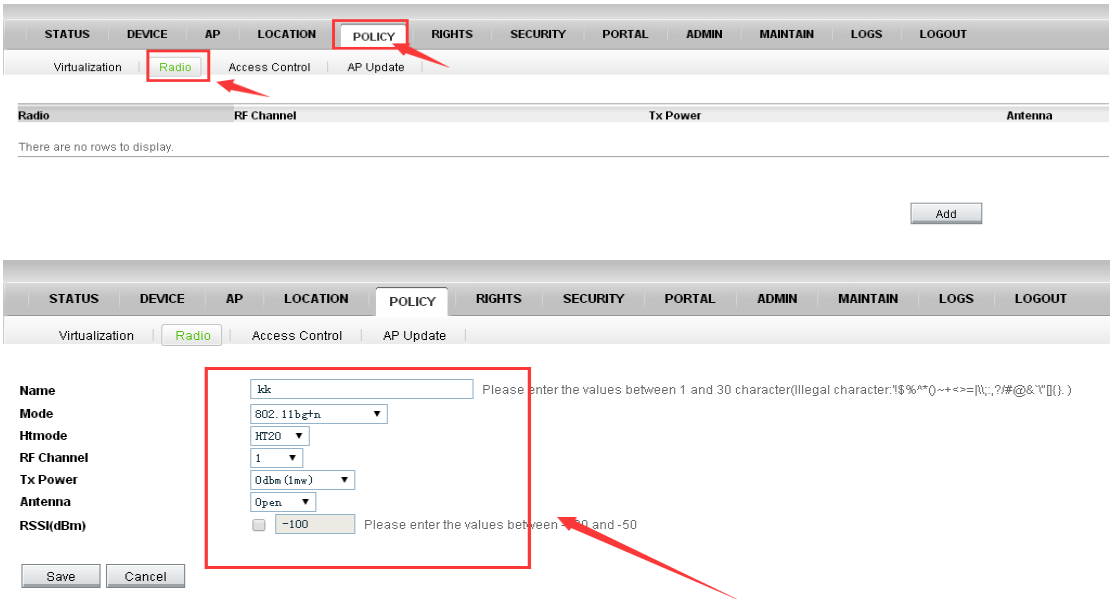


- By option POLICY - VSLAN, add a VSLAN policy named “kk”, fill in the Network ID field with the VSLAN interface ID that enabled in the previous step, so here enter the number 8, Bind the newly created WLAN policy “kk” and the Portal policy “kk”, as shown below:



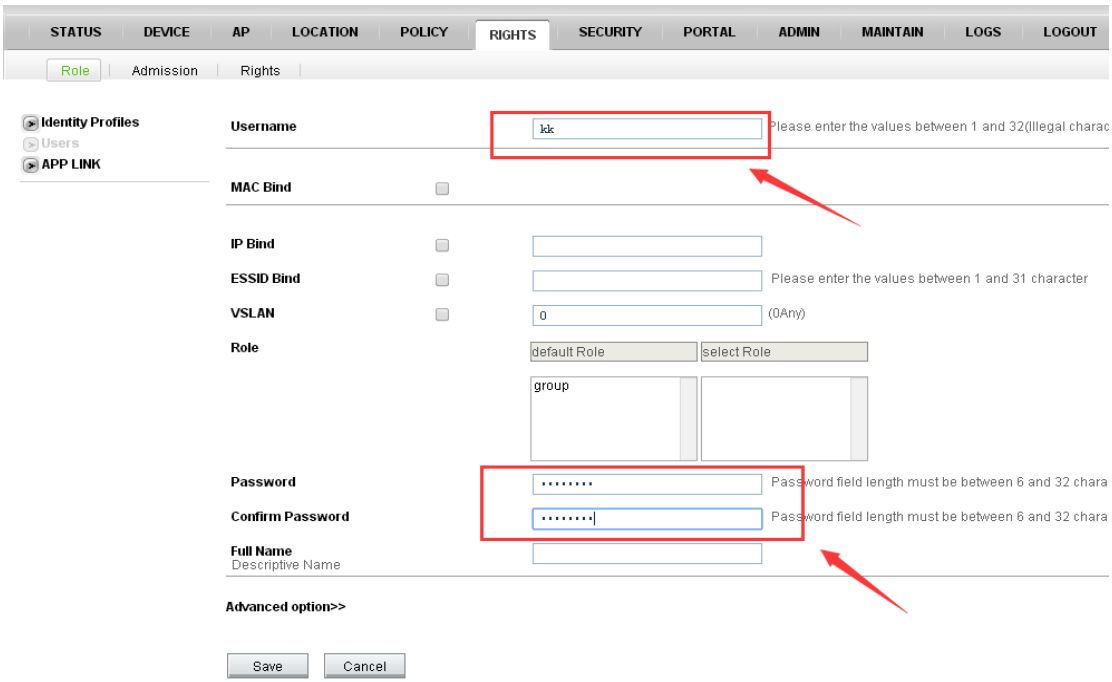


- By option POLICY - Radio, add a Radio policy named “kk”, and save, as shown below:



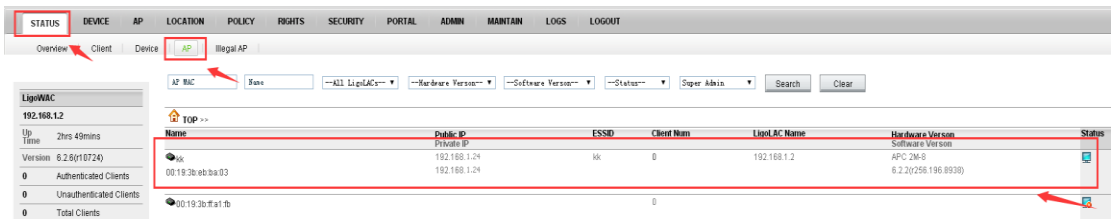
3.2.2.5. Add Users

- By option RIGHTS - Role - Users, add a user(for client authentication via portal page)and save, as shown below

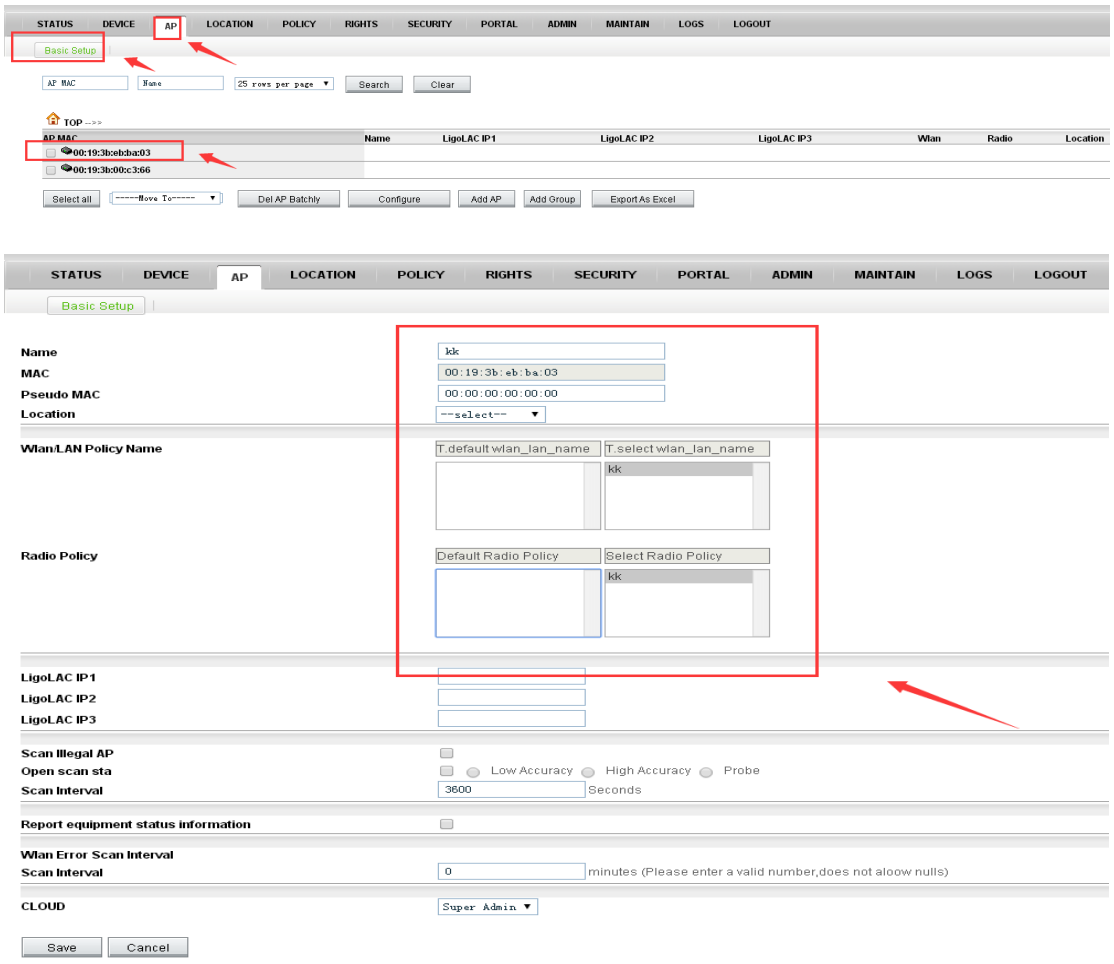


3.2.2.6. Have APs on-line and make the configuration

- Have the AP connected to the internal network, the AP will get on-line to the WAC in 1-2 minutes, you will see the AP get on-line to the WAC by option STATUS-AP, and the AP can obtain an IP of 192.168.1.0 assigned by the internal network, as shown below:

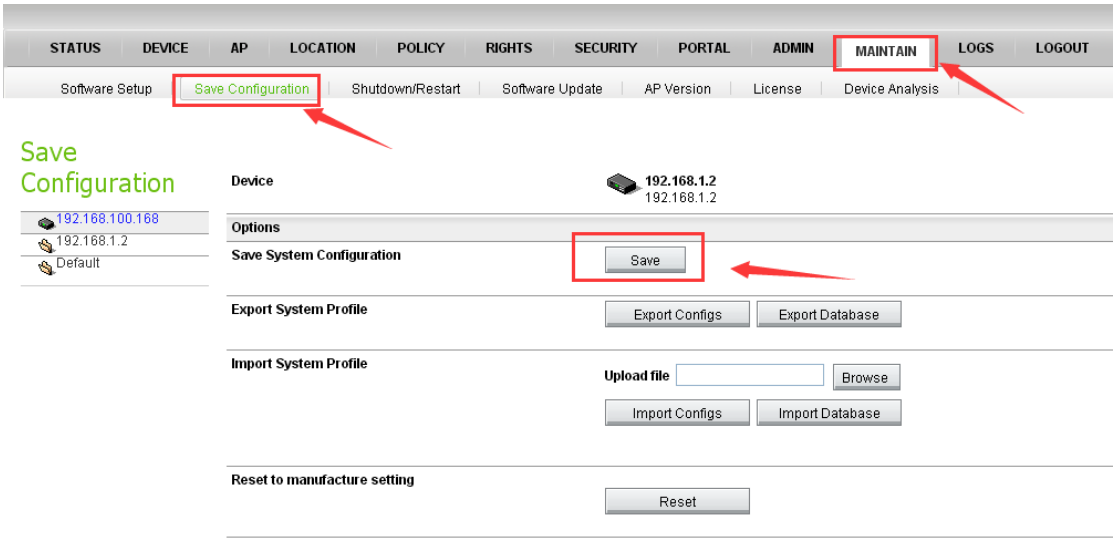


- By option AP-Basic Setup, press the on-line AP MAC address to configure it, you can name it and bind it up with WLAN/Radio policies and so on, in this case bind the WLAN policy“kk” and Radio policy“kk” created above, click “Save”, as shown below:



3.2.2.7. Save System Configuration

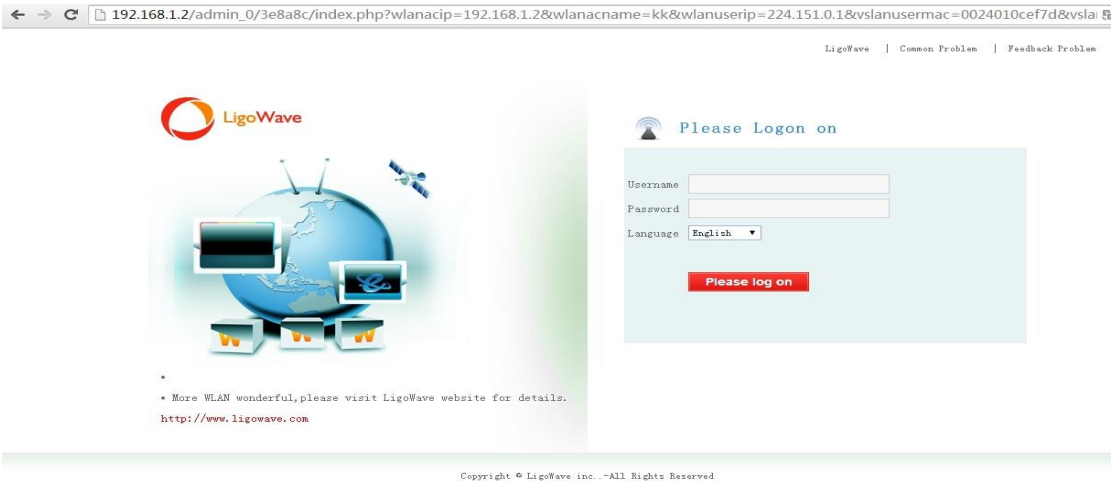
- By option MAINTAIN - Save Configuration, click“Save”to save the current system configuration, as shown below:



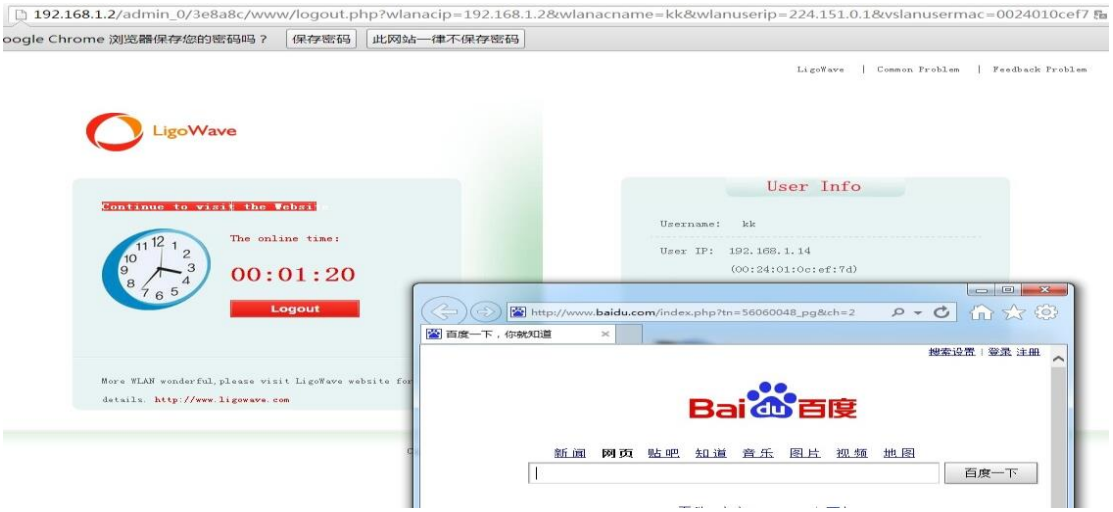
- The AP will broadcast a SSID named “kk” within 1 minute, connect your laptop to the SSID, the wireless network card obtains an IP address of 192.168.1.0 segment, as shown below

3.2.2.8. Get permission to access internet through portal-based authentication

- Enter a URL to visit in your browser, like *www.baidu.com*, you can see the URL be redirected to the portal page URL, as shown below



- Fill in the authentication information(the user name and password added in above steps), successfully passed certification then the client can access internet, as shown below:

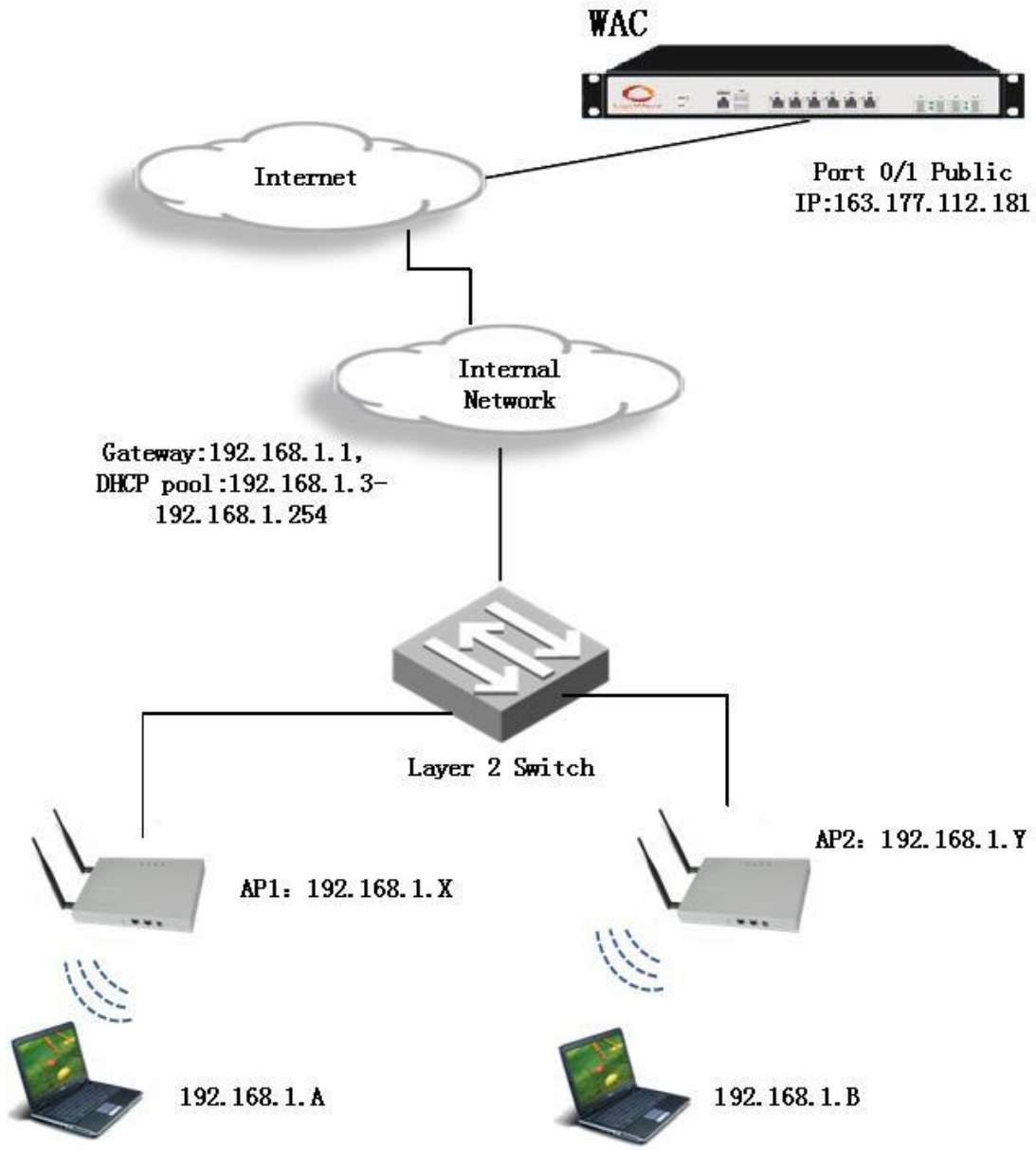


NOTE: Configuration process of NAT local forwarding mode is as the same as the transparent local forwarding mode. The difference is that the wireless clients obtaining IP addresses (192.168.2.0) from the AP, the AP acts NAT between the wireless clients and the network. Therefore, the explanation will not be repeated here.

3.3. Between AP and WAC crosses the internet

Transparent/NAT local forwarding mode is used in this case, because the transparent and the NAT local forwarding mode configuration process are as the same, so here we only take transparent local forwarding mode as an example.

3.3.1. Network Topology

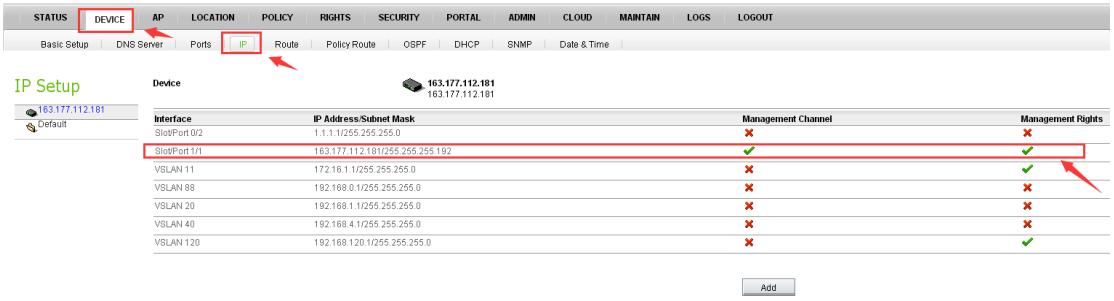


3.3.2. Configuration Steps

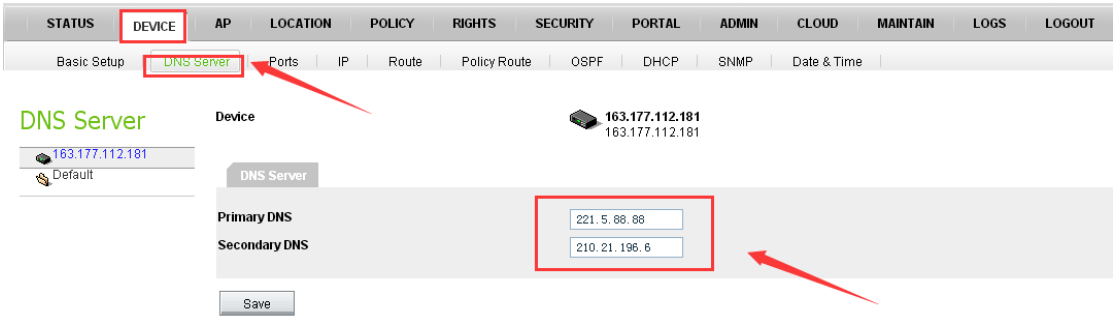
The configuration is the same as when the WAC is place on local, so the following content briefly describes essential of the configuration or the related notes.

3.3.2.1. Essential of WAC Configuration

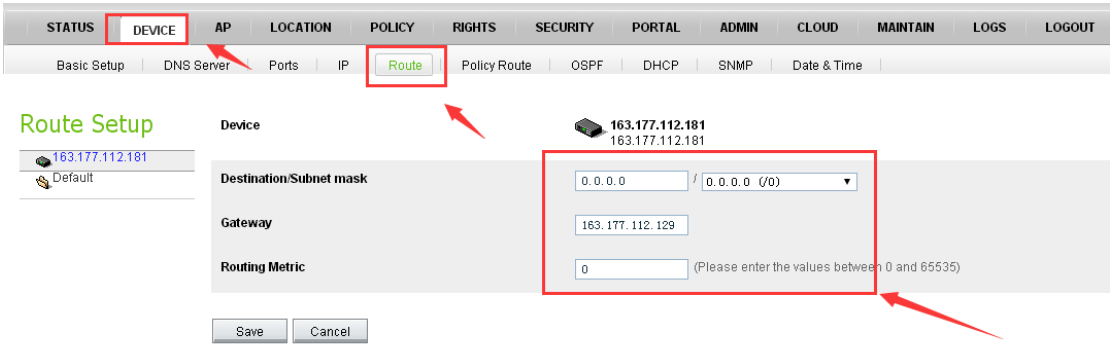
Manage the device through the physical interface(Refer to Section *1.2.2.4.IP Setup*), by option DEVICE - IP, Configure the WAC with the public IP which provided by ISP(in this case we configure port 0/1 with the public IP, for example 163.177.112.181), and enable "Management Channel" and "Management Rights", as shown below



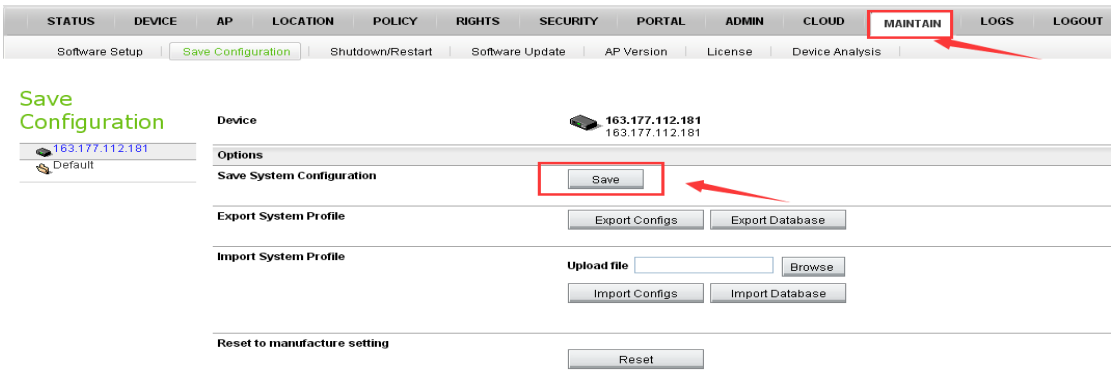
- By option DEVICE - DNS Server, fill in with the DNS server IP and click "Save", as shown below



- By option DEVICE - Route, fill in with the Gateway IP and click "Save", as shown below



- By option MAINTAIN - Save Configuration, click“Save”to save the current system configuration, as shown below



- Have the WAC accessed to internet, then we are able to manage the WAC through the public IP as long as we can access to internet, access the url https://163.177.112.181in browser to manage
- **The other details configuration please refers to the configuration when WAC is placed on local network see *3.2.2.Configuration Steps***

3.3.2.2. Essential of AP Configuration

AP should be managed by remote management software(like: putty, Xshell etc.), configure AP with the IP address of WAC through command line and then have AP connected to internet, the configuration is as follows:

- After powered up, the AP by default broadcast the SSID “Ligo_mac”, as shown below:

- Connect your laptop to the SSID and manage the AP through SSH(use SSH

software like Xshell), the management ip is 192.168.2.66, as shown below

```
Xshell:\> ssh 192.168.2.66
```

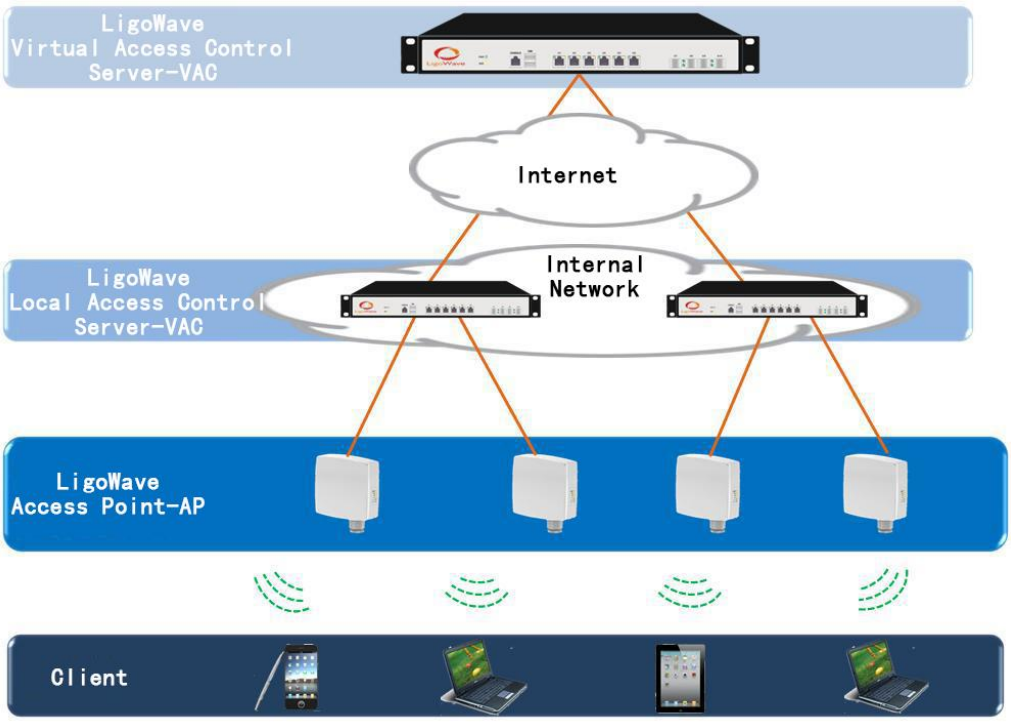
- Follow the prompts to enter username: admin and password:admin01. After login successfully, type “shell” at the command line and press enter, use the following command to specify the remote VAC/WAC IP(for example:163.177.112.181) address for the AP

```
# wtpconf set cs 163.177.112.181
```

- Connect the AP to the internal network then it will automatically obtain an IP and get on-line to the remote VAC / WAC through internet

3.4. Use Cases and Configuration Instructions in headquarter-and-branch topology(VAC+LAC)

3.4.1. Architecture Descriptions



Through the above introduction and related cases, we should have understood the principle of WAC well. As a new-type distributed AC system the VAC+LAC

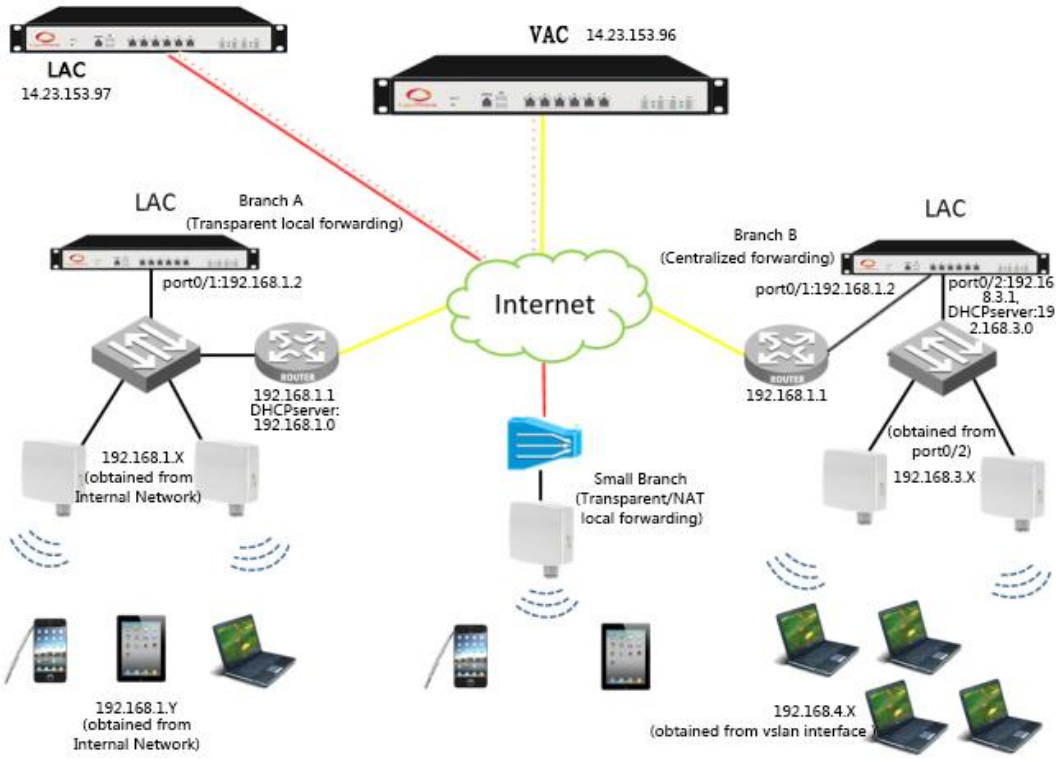
architecture can be interpreted as a WAC split. If from the LAC to the VAC it is reachable by route, we can actually treat it as a WAC whole. The advantage is the convenience of the remote centralized management has been remained, and because the LAC can be placed locally and caching data from the remote VAC, the management efficiency is improved; In addition, the LAC can be distributed anywhere as long as the VAC is reachable by route, this undoubtedly improve the deployment flexibility greatly.

The VAC is responsible for making policies and the LAC as the executor of the system is responsible for issuing the policies to the APs.

3.4.2. Application Overview and Configuration

In the following descriptions, LAC to VAC and AP to LAC / VAC are by default both reachable.

3.4.2.1. Network Topology

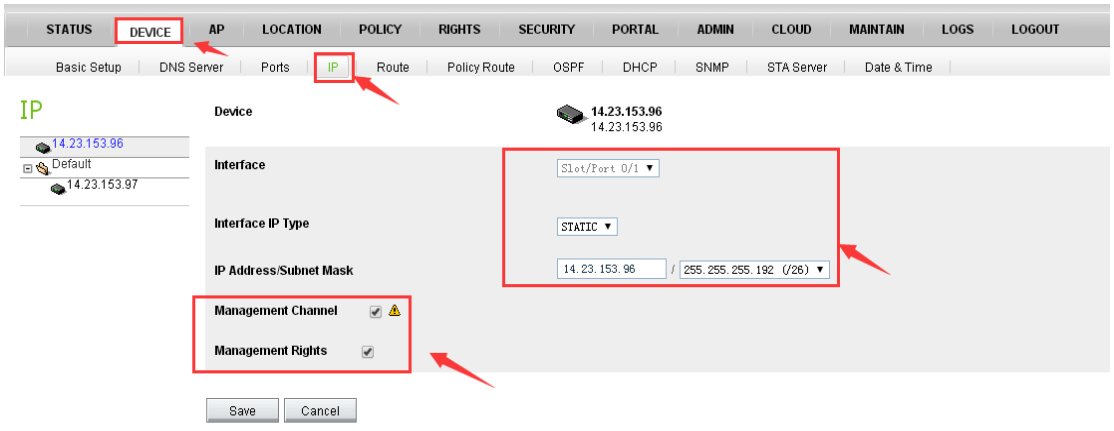


3.4.2.2. Configuration Descriptions

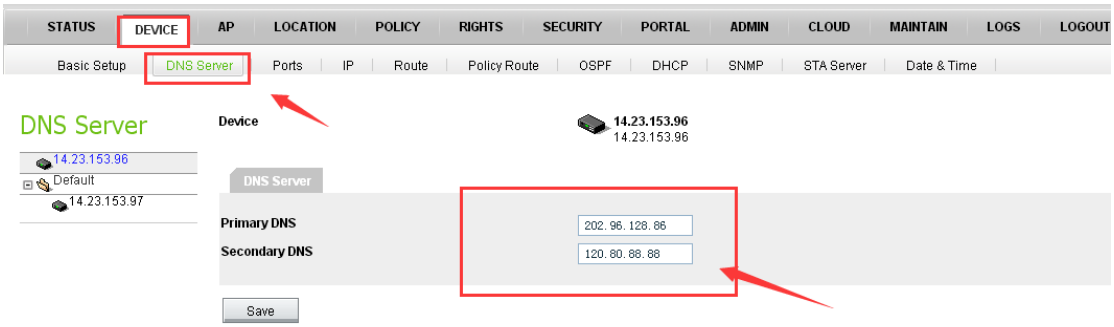
The VAC + LAC is interpreted as the WAC split, so if we ignore the path between VAC and LAC, we can actually treat it as a whole, in principle it is as the same as when placing the WAC locally or remotely. Except the LAC and the AP have to be directed to the VAC, and specifying the affiliated AP for the LAC, the other configurations are essentially as the same as in the single WAC topology; So in this section, we only focus on the relevant important notes or cautions in different network mode.

3.4.2.2.1. Basic Configuration of VAC and LAC

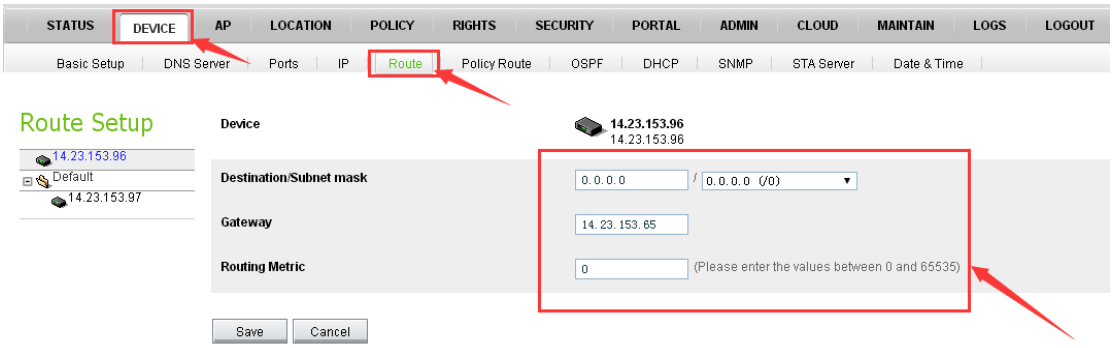
- Manage the device through physical port (***refer to section 1.2.2.4.IP Setup***).By option DEVICE - IP, set the public IP which provided by ISP for the VAC (in this case we set at port 0/1, for example ***14.23.153.96***), and enable "Management Channel" and "Management Rights", as shown below



- By option DEVICE - DNS Server, fill in the blank with DNS server IP for the VAC and click "Save", as shown below

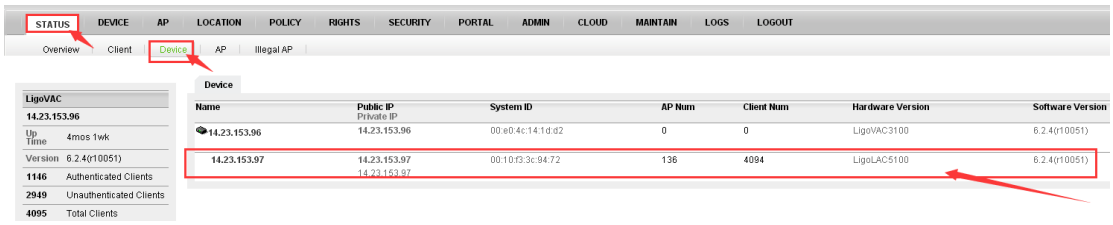


- By option DEVICE - Route, fill in the blank with the Gateway IP for the VAC and save, as shown below



- By option MAINTAIN - Save Configuration, click “Save” to save the current system configuration for the VAC, as shown below

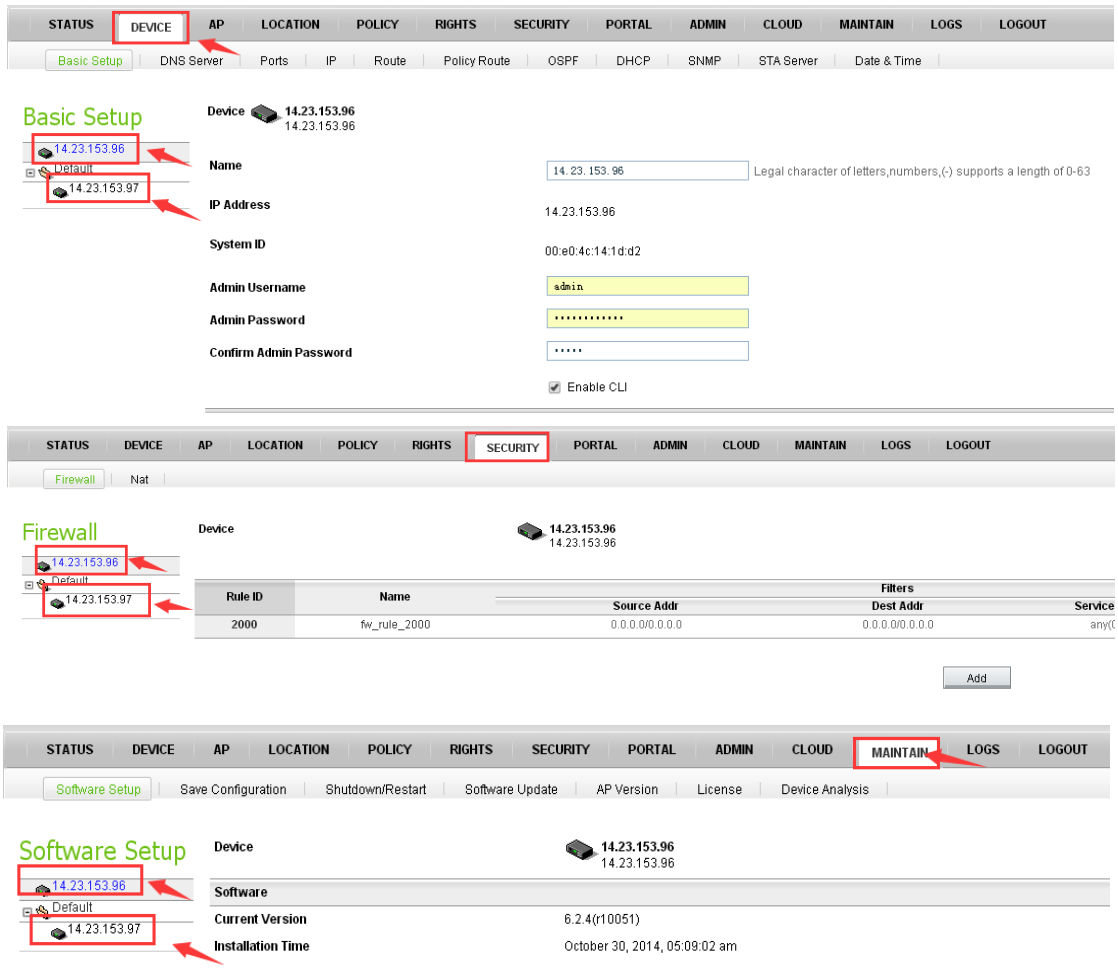
- Have the VAC accessed to internet, then we are able to manage the VAC through the public IP as long as we can access to the internet, access the url*https://14.23.153.96* in browser to manage
- The LAC have to add IP and route to communicate with the external network; also have to set the VAC IP on the LAC so it can discover and get-online to the VAC through network, refer to the section ***1.1.2.Initial Configuration of LAC,*** you will see the LAC get on-line to the VAC by option STATUS-Device, as shown below



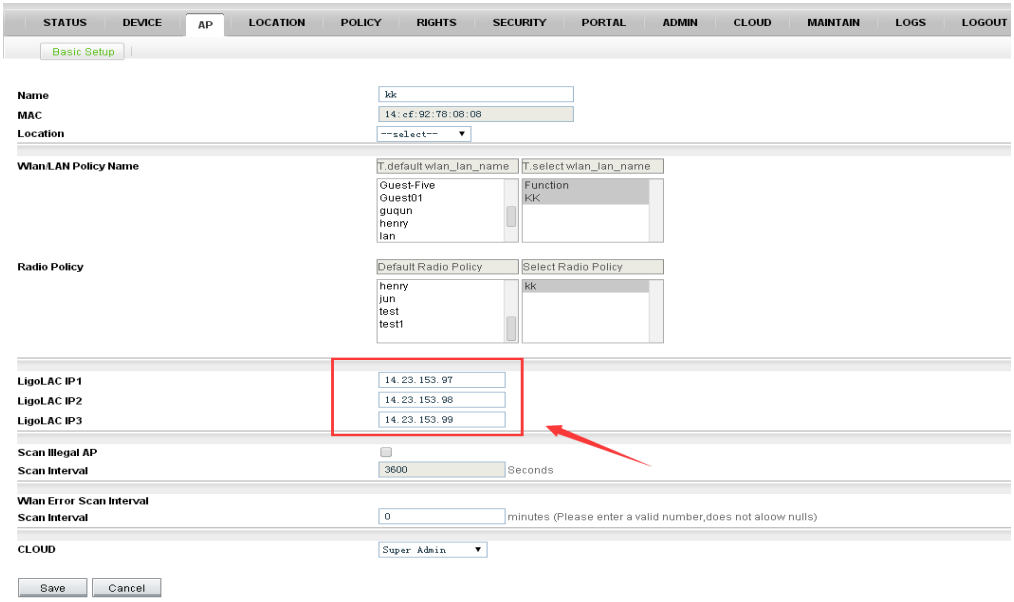
- The configuration of VAC + LAC there are several caveats:

A. The VAC is the brain of the whole system, is responsible for making policies; and the LAC as the executor of the system is responsible for issuing the policies to the APs;

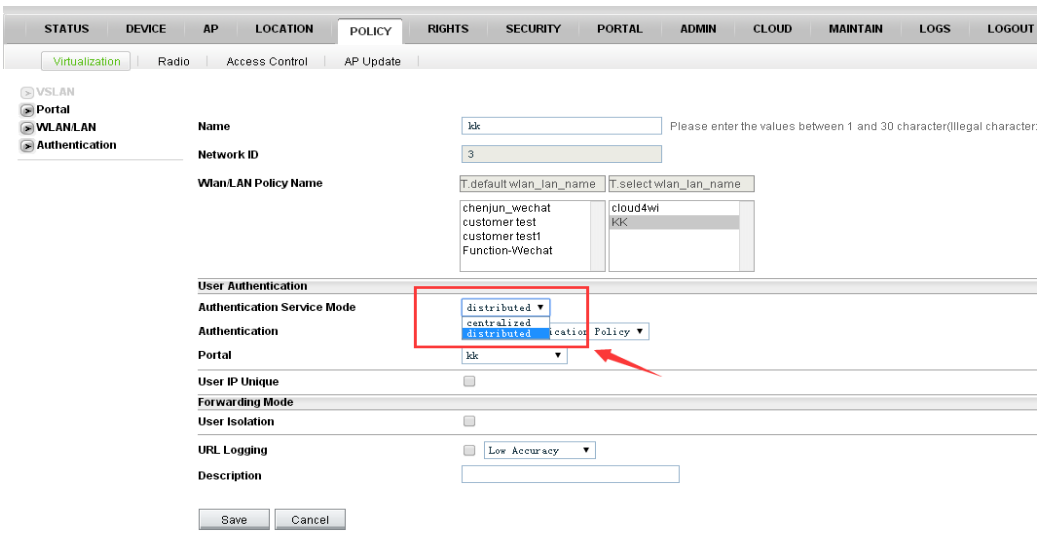
B. In the process of configuring, Options like Policy, Location etc., only need to be configured on the VAC, but for Device, Security, Maintain etc., need to be configured separately on the VAC and LAC. Perform the configuration please click the IP on the left side of the GUI to select VAC/LAC, as shown below



C. After the APs getting on-line to the VAC you can specify LACs for them, by option AP - Basic Setup, press the AP MAC to configure the AP, add LAC IPs for the AP (up to 3 LAC IPs can be added), the AP will discover the LAC by priorities, as shown below



D. There is a caveat when configuring the VSLAN policy, it's when you select "Authentication Service Mode" you may see two options (centralized and distributed), select "centralized" means the authentication performs on VAC, select "distributed" means the authentication performs on LAC(The LAC will automatically caches data from the VAC); In a VAC+LAC structure, select the "distributed" mode will help reducing pressure of the VAC, improve management efficiency, as shown below



3.4.2.2.2. Basic Configuration of AP

The AP has to be configured or obtain an IP and registered the IP of the VAC so it can communicate with the external network and get on-line to the VAC, refer to the section ***1.1.3.Initial Configuration of AP***

3.4.2.2.3. Configurations in different forwarding mode

The configuration steps are the same as WAC, please refer to the configuration steps of WAC and complete the configuration both on VAC and LAC. According to different forwarding modes, please refer to:

- Take branch B(Centralized forwarding) as an example, refer to the section *3.1.2.Configuration Steps*
- Take branch A(Transparent local forwarding) as an example, refer to the section *3.2.2.Configuration Steps*
- Take the small branch(Between AP and VAC/LAC crosses the internet) as an example, refer to the section *3.3.2.Configuration Steps*

To learn more about LigoWave/Deliberant products, visit www.ligowave.com and www.deliberant.com