

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	6
1.1. THE INITIAL CONFIGURATION OF VAC/WAC/LAC/AP	6
1.1.1. The Initial Configuration of VAC/WAC	6
1.1.2. The Initial Configuration of LAC	7
1.1.3. The Initial Configuration of AP	9
1.2. Configure the VAC/WAC through web interface	9
1.2.1. First Login	10
1.2.2. Setup Instructions	10
1.2.2.1. Basic Setup	10
1.2.2.2. DNS Server	11
1.2.2.3. Ports	12
1.2.2.3.1. Physical Interface	12
1.2.2.3.2. VSLAN Interface Configuration	12
1.2.2.4. IP Setup	13
1.2.2.5. Destination Route	14
1.2.2.6. DHCP Setup	15
1.2.2.6.1. DHCP Server	16
1.2.2.6.2. DHCP Domain	16
1.2.3. Policy Management Setup Instructions	18
1.2.3.1. Virtualization	18
1.2.3.1.1. VSLAN Policy	19
1.2.3.1.2. Portal Policy	20
1.2.3.1.3. WLAN Policy	20
1.2.3.1.4. Authentication Policy	22
1.2.3.2. Radio Policy	23



1.2.3.3. Access Control24
1.2.3.4. AP Update
1.2.4. AP Setup Instructions26
1.2.4.1. Basic Setup27
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
2.2.1.1. Pre-Setup and Test Steps
2.2.1.2. Expected Results
2.2.2. AP can be managed cross-internet
2.2.2.1. Pre-Setup and Test Steps
2.2.2.2. Expected Results
2.3. VIRTUALIZATION CAN BE ACHIEVED
<i>2.3.1. Multiple independent manage virtual networks can be created</i>
2.3.1.1. Pre-Setup and Test Steps
2.3.1.2. Expected Results
2.3.2. Authentication Policy and Portal Policy for each network can be set
independently40
2.3.2.1. Pre-Setup and Test Steps40
2.3.2.2. Expected Results41



2.3.3. I	RF Management can be achieved	41
2.3.3.1.	Pre-Setup and Test Steps	41
2.3.3.2.	Expected Results	41
2.4. Dy	NAMIC VPN	42
2.4.1. I	Pre-Setup and Test Steps	42
2.4.2.	Expected Results	42
	3. CHAPTER 3 BASIC EXAMPLES AND	

3.1. Cent	RALIZED FORWARDING MODE IN A SINGLE WAC TOPOLOGY	43
3.1.1. Ne	etwork Topology	43
3.1.2. Со	onfiguration Steps	44
3.1.2.1.	Configure management and access control port	44
3.1.2.2.	Configure Route and DNS	45
3.1.2.3.	Configure VSLAN Interface	46
3.1.2.4.	Configure DHCP Service	48
3.1.2.5.	Policy Configuration	49
3.1.2.6.	Add Users	53
3.1.2.7.	Add NAT Rules	53
3.1.2.8.	Have APs on-line and make the configuration	55
3.1.2.9.	Save System Configuration	56
3.1.2.10.	Get permission to access internet through portal-based authentication	57
3.2. Tran	ISPARENT LOCAL FORWARDING MODE IN A SINGLE WAC TOPOLOGY	58
3.2.1. Ne	etwork Topology	58
3.2.2. Со	onfiguration Steps	58
3.2.2.1.	Configure management and access control port	58



3.2.2.2.	Configure Route and DNS60
3.2.2.3.	Configure VSLAN interface
3.2.2.4.	Policy Configuration
3.2.2.5.	Add Users
3.2.2.6.	Have APs on-line and make the configuration
3.2.2.7.	Save System Configuration67
3.2.2.8.	Get permission to access internet through portal-based authentication
3.3. Betw	een AP and WAC crosses the internet69
3.3.1. Ne	twork Topology69
3.3.2. Со	nfiguration Steps70
3.3.2.1.	Essential of WAC Configuration70
3.3.2.2.	Essential of AP Configuration71
3.4. Use (Cases and Configuration Instructions in headquarter-and-branch
TOPOLOGY(VA	C+LAC)
3.4.1. Arc	chitecture Descriptions72
3.4.2. Ар	plication Overview and Configuration73
3.4.2.1.	Network Topology73
3.4.2.2.	Configuration Descriptions74
3.4.2.2.1	. Basic Configuration of VAC and LAC74
3.4.2.2.2	. Basic Configuration of AP78
3.4.2.2.3	. Configurations in different forwarding mode78



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 <u>1.2.</u>

(*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:

LigoWave@[192.168.100.168]: delete ip all

• Use the command "delete route all" to delete all route of the WAC:

```
LigoWave@[192.168.100.168]: delete route all
```

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



<u>Add port IP:</u>

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.", 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:

Ligo_00:19:3b:eb:ba:03



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:192.168.100.21) address for the AP:

wtpconf set cs 192.168.100.21

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 <u>https://+port IP</u> from the browser, The default management IP of the VAC/WAC is 192.168.100.168(on port 0/1), so access<u>https://192.168.100.168</u> from the browser, then enter the username and password to login (admin, admin0.1):

& https://192.168.100.168/ui/AdminLogon.php?logout





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 10/79



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

LigoWave			
STATUS DEVICE	AP LOCATION POLICY RIGHTS SE	CURITY PORTAL ADMIN	CLOUD MAINTAIN LOGS LOGOUT
Basic Setup DNS S	erver Ports IP Route Policy Route	OSPF DHCP SNMP	Date & Time
Basic Setup	Device () 163.177.112.181 163.177.112.181		
63.177.112.181 Default	Name	163. 177. 112. 181	Legal character of letters,numbers,(-) supports a length of 0-63
	IP Address	163.177.112.181	•
	System ID	00:90:0b:21:db:7c	
	NAS-ID / Description		
	Location	请选择 ▼	
	Admin Username	admin	
	Admin Password		
	Confirm Admin Password		
		🖉 Enable CLI	
			Save

- 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

LigoWave						
STATUS DEVICE	AP LOCATION	POLICY RIGHTS S	ECURITY PORTAL	ADMIN CLOUD	MAINTAIN	LOGS LOGOUT
Basic Setup	erver Ports IP	Route Policy Route	OSPF DHCP	SNMP Date & Tim	ie	
DNS Server	Device DNS Server		163.177.112.181 163.177.112.181			
	Primary DNS Secondary DNS		221.5.88.88 210.21.196.6			
	Save					

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

LigoWave STATUS DEVICE Basic Setup DNS S	AP LOCI erver Ports	NICH POLICY PRAITS SECRETY PORTAL ACREM P Rode Palicy Rode 05P7 CHCP State	CLOUD MAINTAIN Date & Time	LOGS LOGOUT	-	-	U I Dat	ername: admin lgoVAC: 103.177.112.181 10.0000621087C a & Time: 2015.03.09 11.005 Switch Account Super Admi	se CST ▼ [Language English ▼
Interface Setup	Device	163.177.112.181 163.177.112.181							
163.177.112.181 Default	Interface	VLAN Bridge VSLAN VPN							
	Name	Mode	MTU	TRUNK	TYPE	VSLAN	BYIP	Status	
	Stot/Part 0/1	Route Mode	1500	×	Uplink	1	×	×	2
	Stot/Part 0/2	Route Mode	1500	×	Dewnlink	1	×	×	2
	StobPart 0/3	Route Mode	1500	×	Uplink	1	×	×	2
	StobPart 0/4	Exchange Mode	1500	×	Uplink	1	×	×	2
	SlobPart 1/1	Route Mode	1500	×	Uplink	1	×	 	2

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

STATUS DEVICE	AP LOCATION POLICY RIGHTS S	ECURITY PORTAL ADMIN CLOUD MAINTAIN LOGS LOGOUT
Basic Setup DNS S	erver Ports IP Route Policy Route	OSPF DHCP SNMP Date & Time
Ports	Device	163.177.112.181 163.177.112.181
Sefault Sefault	Name	SlotPort 0/1
	MAC	00:90:0b:1e:ef:b4
	мти	1500 (Please enter the 68-1500 values)
	Port Connection Type	Autoselect 🔻
	TYPE	Uplink v
	TRUNK 🗌	Both VLAN ID (0-4095,English comma separated)
	Mode	Route Mode -
	VSLAN	1 (1-999)
	BY IP	
	STATUS	
	Save Cancel	

- 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

LigoWave			U I Dat	Isername: admin LigoWAC: 163.177.112.181 10.089900821087C te & Time: 2015.03.09 14:26:20 CST
STATUS DEVICE AP LOCATION	POLICY RIGHTS SECURITY PORTAL ADMIN CLOUD M	MINTAIN LOGS LOGOUT		Switch Account Super Admi 💌 Language E
Basic Setup DNS Server Ports IP	Route PolicyRoute OSPF DHCP SNMP Date & Time			
erface Setup 🔤	163.177.112.181 163.177.112.181			
163.177.112.181 Default Interface VI.AN	Dridge VSLAN VPM			
Name VSLAN 1	Member	STP Status	Status ✓	
VSLAN 2 VSLAN 3		×	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	
VSLAN 4		×	*	
NN 120	×		×	
NN 121	×		۲ ۲	
LigoWave		<u> </u>	-	
LigoWave STATUS DEVICE Basic Setup DNS S	AP LOCATION POLICY RIGHTS erver Ports IP Route Policy	SECURITY PORT	TAL ADMIN CLOUD MAINT ICP SNMP Date & Time	TAIN LOGS L
LigoWave STATUS DEVICE Basic Setup DNS SO DHCP Setup	AP LOCATION POLICY RIGHTS erver Ports IP Route Policy Device	SECURITY PORI Route OSPF DH	TAL ADMIN CLOUD MAINT ICP SNMP Date & Time 112.181 112.181	TAIN LOGS L
LigoWave STATUS DEVICE Basic Setup DNS Si CHCP Setup 163.177.112.181 Default	AP LOCATION POLICY RIGHTS erver Ports IP Route Policy Device	SECURITY POR Route OSPF DH	TAL ADMIN CLOUD MAINT ICP SNMP Date & Time 112.181 112.181 (1-999) 112.191 112.191	TAIN LOGS L
LigoWave STATUS DEVICE Basic Setup DNS Si PHCP Setup 163.177.112.181 ☆ Default	AP LOCATION POLICY Rights erver Ports IP Route Policy Device ID Name	SECURITY POR Route OSPF DH 163,177. 183,177.	TAL ADMIN CLOUD MAINT ICP SNMP Date & Time 112.181 112.181 (1-999) 112.191 112.191	TAIN LOGS L
LigoWave STATUS DEVICE Basic Setup DNS S DHCP Setup ●163.177.112.181 ● Default	AP LOCATION POLICY RiGHTS erver Ports IP Route Policy Device ID Name STP Status	SECURITY PORT Route OSPF DH 163.177.	TAL ADMIN CLOUD MAINT ICP SNMP Date & Time 112.181 112.181 (1-999) 112.181 112.181	TAIN LOGS L

- 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

LigoWa	ve		
LigoWave	E AP LOCATION	POLICY RIGHTS SECURITY PORTAL ADMIN CLOUD MAI	NTAIN LOGS LOGOUT
Basic Setup	DNS Server Ports P	Route Policy Route OSPF DHCP SNMP Date & Time	
Contro Contap			
IP Setup	Device	163.177.112.181 163.177.112.181	
IP Setup	Device	63.177.112.181 163.177.112.181 163.177.112.181	Management Channel
IP Setup 163.177.112.181 Default	Device Interface SlotPort 0/2	I63.177.112.181 183.177.112.181 IP Address/Subnet Mask 1.1.1.1255.255.255.0	Management Channel X
IP Setup	Device Interface Slot/Port 0/2 Slot/Port 1/1	Image: Figure 163.177.112.181 163.177.112.181 IP Address/Subnet Mask 1.1.1.1/255.255.255.0 163.177.112.181/255.255.255.192	Management Channel × ✓
IP Setup 163.177.112.181 © Default	Device Interface Slot/Port 0/2 Slot/Port 1/1 VSLAN 11	E63.177.112.181 183.177.112.181 IP Address/Subnet Mask 1.1.1.1/256.256.256.0 183.177.112.181/255.256.256.0 172.16.1.1/255.256.256.0	Management Channel × ~ X
IP Setup • 163.177.112.181 • Default	Device Interface SlotPort 0/2 SlotPort 1/1 VSLAN 11 VSLAN 12	Enderses/Submet Mask 1.1.1.1/255.255.05 163.177.112.181 163.177.112.181 177.112.181 177.112.181 198.177.112.181 199.168.0.1/255.255.0 192.168.0.1/255.255.0	Management Channel × ✓ ×
IP Setup	Device StotPort 0/2 StotPort 1/1 VSLAN 11 VSLAN 88 VSLAN 20	Endition Endition	Management Channel × × × × ×
IP Setup ▲163.177.112.181 ▲ Default	Device StotPort 0/2 StotPort 1/1 VSLAN 11 VSLAN 88 VSLAN 20 VSLAN 40	Endites Endites 1.1.1.1255.255.255.0 163.177.112.181 1.3.177.112.1811255.255.255.192 163.177.112.61.1/255.255.255.192 1.72.161.1/255.255.255.0 192.168.0.1/255.255.255.0 1.92.168.1.1/255.255.255.0 192.168.1.1/255.255.255.0	Management Channel X X X X X X X X X X X X X X X X X X X

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

LigoWave			
STATUS DEVICE	AP LOCATION POLICY RIGHTS SEC	CURITY PORTAL ADMIN CLOUD MAINTAIN LOGS LOGO	UT
Basic Setup DNS S	erver Ports IP Route Policy Route	OSPF DHCP SNMP Date & Time	
IP	Device	163.177.112.181 163.177.112.181	
Contraction of the second seco	Interface	Slot/Fort 0/2	
	IP Address/Subnet Mask	1.1.1.1 / 255.255.255.0 (/24)	
	Management Channel 🛛 🖻 💩		
	Management Rights 🥑		
	Save Cancel		

- 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

LigoWave		
STATUS DEVICE	AP LOCATION PO	CY RIGHTS SECURITY PORTAL ADMIN CLOUD MAINTAIN LOGS LOGOUT
Basic Setup DNS S	erver Ports IP	Oute Policy Route OSPF DHCP SNMP Date & Time
Route Setup	Device	163.177.112.181 163.177.112.181
163.177.112.181 Default	Destination/Subnet mask 0.0.0.0/0.0.00	Gateway 163.177.112.129
		Add

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

STATUS DEVICE	AP LOCATION POLICY RIGHTS SEC	URITY PORTAL ADMIN CLOUD MAINTAIN LOGS LOGOUT
Basic Setup DNS S	erver Ports IP Route Policy Route	OSPF DHCP SNMP Date & Time
Route Setup	Device	163.177.112.181 163.177.112.181
Default	Destination/Subnet mask	0.0.0.0
	Gateway	163. 177. 112. 129
	Routing Metric	0 (Please enter the values betwee 0 and 65535)
	Save Cancel	

- 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

			Usernam LigoWA Date & Tim Switch.
STATUS DEVICE	AP LOCATION POLICY RIGHT	S SECURITY PORTAL ADMIN CLOUD MAINTAIN LOGS LOGOUT	
Basic Setup DNS S	erver Ports IP Route Polic	yRoute OSFF DHCP Date & Time	
DHCP Setup	Device		
163.177.112.181 Default	DHCP Server DHCP Relay	104/17,112-101	
	DHCP Server DHCP Domain Default Lease Time Max Lease Time	Static P 0 day 1 hour 0 minutes 1 day 0 hour 0 minutes	
	DHCP Setup		
		Blat DHCP Service DHCP service is turned of	
	Configure the monitoring interface for DHCP Se	rvice	
	Interface	IP Address/Subnet Mask	Enable
	SlotPort 0/1		
	SlotPort 0/2	1.1.1.1/255.255.255.0	
	SlotPort 0/3		
	SlotPort 1/1	163.177.112.181/255.255.255.192	
	VSLAN 1		
	VSLAN 11	172.16.1.1/265.265.265.0	

- **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

STATUS DEVICE	AP LOCATION POLICY	RIGHTS SECURITY PORTAL	ADMIN CLOUD	MAINTAIN LOGS LOGOUT		
Basic Setup DNS S	erver Ports IP Route	Policy Route OSPF DHCP	SNMP Date & Time			
DHCP Setup	Device	163.177.112. 163.177.112.	81 81			
163.177.112.181 Default	DHCP Server DHCP Relay					
	DHCP Server DHCP D Default Lease Time	Dormain Static IP 0 day 1 hou 1 day 0 hou	0 minutes 0 minutes			
	DHCP Setup					
				Close DHCP Service DHCP service is turned on		
	Configure the monitoring interface for D	HCP Service			-	
	Interface		IP Address/Subnet Mask			Enable
	SlotPort 0/1				A	
	SlotPort 0/2		1.1.1.1/255.255.255.0			
	Slot/Port 0/3					
	SlotPort 1/1		163.177.112.181/255.255.255.19	2		
	VSLAN 1					
	VSLAN 11		172.16.1.1/255.255.255.0			

1.2.2.6.2. DHCP Domain

• By option DEVICE - DHCP - DHCP Domain, click "Add" to create DHCP



domain

LigoWave		-		-
STATUS DEVICE	AP LOCATION POI	LICY RIGHTS SECURITY PORTAL	ADMIN CLOUD M	AINTAIN LOGS LOGOUT
Basic Setup DN	IS Server Ports IP I	Route Policy Route OSPF DHCP	SNMP Date & Time	
DHCP Setup 163.177.112.181 Default	Device DHCP Server DHCP Ret DHCP Server			
	IP Address	Subnet Mask		IP Range
	192.168.0.0	255.255.255.0		192.168.0.35-192.168.0.62
	192.168.1.0	255.255.255.0		192.168.1.10-192.168.1.20
	192.168.3.1	255.255.255.0		192.168.3.2-192.168.3.254
	192.168.120.0	255.255.255.0		192.168.120.2-192.168.120.254
				Add

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

STATUS DEVICE	AP LOCATION POLICY RIGHTS SEC	URITY PORTAL ADMIN CLOUD MAINTAIN LOGS LOGOUT
Basic Setup DNS Se	arver Ports IP Route Policy Route	OSPF DHCP SNMP Date & Time
DHCP Setup	Device	163.177.112.181 163.177.112.181
Sefault	IP Address	192. 168. 4. 0
	Subnet Mask	255.255.255.0 (/24) •
	Gateway	192.168.4.1
	DNS Server	112.100.100
	DNS Server	192.168.4.1
	Domain Name	Legal character of letters,numbers,(-) supports a length of 0-63
	IP Range	192. 168. 4. 2 192. 168. 4. 254 Add
	192.168.4.2-192.168.4.254	
		Del
	>>Advanced option	
	Save Cancel	

- 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

LigoWave						
STATUS DEVICE	AP LOCATION	POLICY RIGHTS	SECURITY PORTAL	ADMIN CLOUD	MAINTAIN LOGS	LOGOUT
Basic Setup DNS	Server Ports IP	Route Policy Rou	te OSPF DHCP	SNMP Date & Time		
DHCP Setup 163.177.112.181 Default	Device DHCP Server DHC	CP Relay	163.177.112.181 163.177.112.181			
	DHCP Serve Default Lease Time Max Lease Time	DHCP Domain	Static IP 0 day 1 hour 0 1 day 0 hour 0	minutes minutes		
	DHCP Setup					Start DHCP Service DHCP service is turned off

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

LigoWave STATUS DEVICE	AP LOCATION	N POLICY RIGHTS	SECURITY PORTAL ADMIN	CLOUD MAINTAIN LOGS LOGOUT	-
Virtualization Radio	Access Control	AP Update	Policy Nas Authentication Portal	Search Clear	
Authentication	Network ID	Name	Wlan/LAN Policy Name	Authentication	Portal
	1	5G	5m-12	System Authentication Policy	PORTAL
	2	shuangyiwuxian	shuangyiwuxian	System Authentication Policy	shuangyiwuxian
	5	lantest	lantest	System Authentication Policy	customer test
	11	Function	Function Function-Five Ian Andy	System Authentication Policy	PORTAL
	12	VSLAN12	Guest Guest01 Guest-Five test1	System Authentication Policy	PORTAL
	20	20	11 LAN	System Authentication Policy	PORTAL
	22	22	guqun	System Authentication Policy	22
	40	henry	henry	System Authentication Policy	PORTAL
	88	test	test	System Authentication Policy	test

Add



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

LigoWave	*		
STATUS DEVICE	AP LOCATION POLICY RIG	HTS SECURITY PORTAL ADMIN CLO	UD MAINTAIN LOGS LOGOUT
Virtualization Rac	tio Access Control AP Update		1
Portal	Manua	12	tes bekunse 4 and 20 skewske/II.evel skewskev®00/0*0
Authentication	Name	xx Please enter the van	bes between 1 and 30 character(megarcharacter, to tw - 0 *** = 0,., //#@& (1(),)
-	Network ID	8	
	Wian/LAN Policy Name	T.defaultwlan_lan_name T.selectwlan_lan_name	
		chenjun_wechat customertest customertest1 Function-Wechat	
	User Authentication		
	Authentication Service Mode	centralized V	
	Authentication	System Authentication Policy 🔻	
	Portal	PORTAL.	
	User IP Unique		
	Forwarding Mode		
	User isolation		
	URL Logging	Low Accuracy V	
	Description		
	Save Cancel		

- **A.** Network name (can be user-defined)
- **B.** Network ID (Must match to VSLAN ID)
- Different network ID for different DHCP network \diamond
- Different network ID for different/same WLAN policy(one network ID can be related to \diamond 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 • 19 / 79



1.2.3.1.2. Portal Policy

LigoWave		
STATUS DEVICE	AP LOCATION POLICY RIGHT	S SECURITY PORTAL ADMIN CLOUD MAINTAIN LOGS LOGOUT
Virtualization Rad	o Access Control AP Update	
VSLAN	Name	Search Clear
Authentication	Name	URL
	weixin	http://163.177.112.181/ad-0/6dfa06-1/index.php
	wechat wifi	http://163.177.112.181/admin_0/portalweb/index.php
	test	http://163.177.112.181/admin_0/b61fc3/index.php
	shuangyiwuxian	http://163.177.112.181/ad-0/1b9b6c-1/index.php
	PORTAL	http://163.177.112.181/admin_0/portalweb/index.php
	kk	http://163.177.112.181/admin_0/5c0f8c/index.php
	henry	http://163.177.112.181/ad-0/71ab4d-1/index.php
	customer test	http://163.177.112.181/admin_0/cb512d/index.php
	999	http://163.177.112.181/admin_0/portalweb/index.php
	22	http://163.177.112.181/admin_23/portalweb/index.ph
	111	http://163.177.112.181/admin_0/portalweb/index.php

- 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)

Add

• By option POLICY - Virtualization - Portal, click "Add" to create Portal policy

STATUS DEVICE	AP LOCATION POL	ICY RIGHTS SECURITY	PORTAL ADMIN CLOUD	MAINTAIN LOGS LOGOUT
Virtualization	lio Access Control AP U	odate		
▶ VSLAN				1
> Portal	Name	kk	Please enter the values between 1 and 30	character(Illegal character:!!\$%**()~+<>=[\\;;;?/#@&`*[]{}.)
WLAN/LAN	PORTAL	http://163.177.112.181/admin_0/p	ortalweb/index.php	
Authentication	PORTAL	Portal Service Mode centralized	•	
	Save Cancel			

- 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"

LigoWave					-	Usern Ligov Date & 1 Swr
TATUS DEVICE	AP LOCATION POLICY RIGHTS S	SECURITY PORTAL ADMIN CLOUD	MAINTAIN LOGS LOGO	UT		
Virtualization Radio	o Access Control AP Update WLANLAN Security					
	ann	search Clear				
	Name test1	test1	OPEN	no	Forwarding Mode Local Forward:Bridge	Encryption
	test	test	OPEN	no	Local Forward:Bridge	
	shuangyiwuxian	shuangyiwuxian	OPEN	no	Local Forward:NAT	
	lantest	lantest	OPEN	no	Local Forward:Bridge	
	LAN	N/A	NIA	no	Local Forward Bridge	
	lan KK	NIR.	NIR KK	10	Center Ennvard	Auto Nerrot
	henry	hennetest	OPEN	no	Local Forward Bridge	· all reger
	guqun	guqun	OPEN	no	Local Forward:Bridge	
	Guest01	Guest01	OPEN	yes	Local Forward:Bridge	
	Guest-Five	Guest	OPEN	yes	Local Forward:Bridge	
	Guest	Guest	OPEN	yes	Local Forward:Bridge	
	Function-Wechat	Function-Wechat	Function-Wechat	no	Local Forward:Bridge	
	Function	Function	functionkey	no	Local Forward Bridge	
	customer test1	customer test1	OPEN	10	Local Forward Bridge	
	customer test	customer test	customertest	no	Local Forward:Bridge	
	chenjun_wechat	wechat_test	OPEN	no	Local Forward:Bridge	
	Andy	ANDY	ANDY TEST	no	Local Forward:Bridge	
	5m-12	5m-12	OPEN	no	Local Forward:Bridge	
				kdd		
TATUS DEVI Virtualization LAN tal ANLAN hentication	ICE AP LOCATION POLICY Radio Access Control AP Update WLANLAN Security Policy Type	RIGHTS SECURITY PORTA		MAINTAIN LOGS	LOGOUT	
ATUS DEVI Irrualization AN al INILAN Hentication	CE AP LOCATION POLICY Radio Access Control AP Update WLANLAN Security Policy Type Name	RIGHTS SECURITY PORTA	L ADMIN CLOUD	MAINTAIN LOGS	LOGOUT 30 character(illegal character:15*	€**()~+*>=[\(``,\\#@@.i.(]()
ATUS DEVI firtualization [AN al ANLAN mentication	CE AP LOCATION POLICY Radio Access Control AP Update WLANLAN Security Policy Type Name ESSIN	RIGHTS SECURITY PORTA	L ADMIN CLOUD	MAINTAIN LOGS	LOGOUT 30 character(illegal character:15 31 character	%**0~+<>=[\\`; ?##@&`!\][\
ATUS DEVI Irtualization AN al INILAN nentication	CE AP LOCATION POLICY Radio Access Control AP Update WLANLAN Security Policy Type Name ESSID Security Datas	RIGHTS SECURITY PORTA	L ADMIN CLOUD	MAINTAIN LOGS	LOGOUT 30 character(lliggal character:1\$0 31 character	%**0~+<>=[\t];?\#@&`?`[]()
INTUS DEVI Virtualization	CE AP LOCATION POLICY Radio Access Control AP Update WLANLAN Security Policy Type Name ESSID Security Policy Security Policy	RIGHTS SECURITY PORTA	L ADMIN CLOUD	MAINTAIN LOGS	LOGOUT 30 character(llegal character:15 31 character	%**)~+<>=[(\',',\\#@\$.',[]()
ATUS DEVI Artualization I AN Antal ANALAN hentlication	CE AP LOCATION POLICY Radio Access Control AP Update WLANLAN Security Policy Type Name ESSID Security Policy User Limit	RIGHTS SECURITY PORTA	L ADMIN CLOUD	MAINTAIN LOGS	LOGOUT 30 character(Illegal character:191 31 character ess the ESSID,0 means no limit)	%**0~+ <>=[\C;?/#@&`?"][1]
TATUS DEVI Virtualization	CE AP LOCATION POLICY Radio Access Control AP Update WLANLAN Security Policy Type Name ESSID Security Policy User Limit Hidden	RIGHTS SECURITY PORTA	L ADMIN CLOUD	MAINTAIN LOGS	LOGOUT 30 character(Illegal character:159 31 character ess the ESSID,0 means no limit)	%**0~+<>=[1 ^{1,1} ,3 # @&.r.]]()
IATUS DEVI Vitualization A AN AAN AANLAN hentication	CE AP LOCATION POLICY Radio Access Control AP Update WLANLAN Security Policy Type Name ESSID Security Policy User Limit Hidden Radio Freq	RIGHTS SECURITY PORTA	L ADMIN CLOUD	MAINTAIN LOGS	LOGOUT 30 character(llegal character:15 31 character ess the ESSID,0 means no limit)	%**()→+<>=[(\',?)#@&.',[]()
IATUS DEVI Virtualization AN AN ANLAN Hentication	CE AP LOCATION POLICY Radio Access Control AP Update WLANLAN Security Policy Type Name ESSID Security Policy User Limit Hidden Radio Freq Forwarding Mode	RIGHTS SECURITY PORTA	L ADMIN CLOUD	MAINTAIN LOGS	LOGOUT 30 character(iliegal character:190 31 character ess the ESSID,0 means no limit)	&«°Q→+«>=[V.;?#@&`?"[[).
TATUS DEVI Virtualization) LAN tal AMLAN hentication	CE AP LOCATION POLICY Radio Access Control AP Update WLANLAN Security Policy Type Name ESSID Security Policy User Limit Hidden Radio Freq Forwarding Mode	RIGHTS SECURITY PORTA	L ADMIN CLOUD	MAINTAIN LOGS	LOGOUT 30 character(Illegal character:15 31 character ess the EBSID,0 means no limit)	%**0~+<>=[\t':5,4#@&[]()
IATUS DEVI Artualization AAN AAN AANLAN Hentlication	CE AP LOCATION POLICY Radio Access Control AP Update WLANLAN Security Policy Type Name ESSID Security Policy User Limit Hidden Radio Freq Forwarding Mode	RIGHTS SECURITY PORTA	L ADMIN CLOUD	MAINTAIN LOGS	LOGOUT 30 character(llegal character:19 31 character ess the ESSID,0 means no limit)	%**\)-+<>=[\U;?##@&U[]().
ATUS DEVI itualization AAN al www.awn enritication	CE AP LOCATION POLICY Radio Access Control AP Update WLANLAN Security Policy Type Name ESSID Security Policy User Limit Hidden Radio Freq Forwarding Mode	RIGHTS SECURITY PORTA	L ADMIN CLOUD	MAINTAIN LOGS	LOGOUT 30 character(Illegal character:193 31 character ess the EBSID,0 means no limit)	&**0~++>=[0;;?##@&??[[]).

- 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

LigoWav	e		
LigoWave			
STATUS DEVICE	AP LOCATION POLICY	RIGHTS SECURITY PORTAL ADMIN CLOUD MAINTAIN LOGS LOGOUT	
Virtualization Rad	o Access Control AP Updat	e	
S VSLAN			
> WLAN/LAN	WLANALAN Security		
🕞 Authentication	Policy Name		Encryption
	KK		wna nsk/wna2 nsk
	functionkey		wpa2 psk
	Function-Wechat		wpa2 psk
	customer test		open
	ANDY TEST		wpa2 psk
STATUS DEVICE	AP LOCATION POL	Add	LOGOUT
VSLAN Portal WLAN/LAN	WLANLAN Security		
Authentication	Name	kk	\$%^*()~+<>=[\\;:,?/#@&`\"[[{}.)
	Encryption	open 🔻	
	Кеу	open wep-shared	
	Save Cancel	ν το α-τραλ τη φα ² -τραλ τη φα ² -τραλ	

- 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"

LigoWave		
STATUS DEVICE	AP LOCATION POLICY RIGHTS SECURITY PORTAL ADMIN CLOUD MAINTAIN LOGS	LOGOUT
Virtualization	Access Control AP Update	
S VSLAN		
➢ Portal ➢ WLAN/LAN	Authentication Policies Authentication Services	
S Authentication	Authentication Fo Authentication Se Search Clear	
	Authentication Policy	Authentication Service
	System Authentication Policy	Built-in
	Add	

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

STATUS DEV		TS SECURITY PORTAL ADMIN CLOUD MAINTAIN LOGS LOGOUT
Virtualization	Radio Access Control AP Update	
VSLAN Portal VLANLAN Authentication	Name Authentication Services	System Authentication Folicy Please enter the values between 1 and 30 character(llegal character:15%**0→↔=RC;?#@&T[[].) Make this the preferred Authentication Policyfor new Connection Profiles
	Authentication Service	Service Type
	NT Domain Logons - Kerberos	s NT Domain Logons - Kerberos (Typically Windows 2000 or Windows XP clients)
	T Domain Logons - NTLM	NT Domain Logons - NTLM (Typically Windows 98 or Windows NT clients)
	8U2.1x Logons	802.1x/ HADIUS Layer 3 IP Access
	New Service	

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		
STATUS DEVICE	AP LOCATION POLICY RIGHTS SECURITY PORT	AL ADMIN CLOUD MAINTAIN LOGS LOGOUT
Virtualization Radio	Access Control AP Update	
♥VSLAN ♥Portal ♥WLANLAN Nuthentication	Authentication Policies Authentication Services	
	Authentication Service Built-in	Service Type Built-in
		Add
STATUS D	EVICE AP LOCATION POLICY RIG	HTS SECURITY PORTAL ADMIN CLOUD MAINTAIN LOGS LOGOUT
Virtualization	Radio Access Control AP Undate	
Virtualization		
VSLAN Portal	Auth Type	RADIUS
WLAN/LAN	Name	
Authentication	Server	
	Port	1812
	Secret	
	Confirm Secret	
	Group Identity Field	
	Reauthentication Field	Session-Timeout
	Timeout (Seconds)	5
		Enable RADIUS Accounting (RFC-2866) on port 1813
		Enable RADIUS CoA on port 3799
		Enable Drcom CoA on port 1813
	Save Cancel	

• 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"

STATUS	DEVICE AP	LOCATION	POLICY	RIGHTS S	SECURITY F	PORTAL	ADMIN C	LOUD MAINT	AIN LOGS	LOGOUT	
Virtualizatio	on Radio .	Access Control	AP Update								
Name	MAC	IP	IP	VSL	AN	Search	Clear				
BLACK LIST	WHITE LIST										
Name										MAC	IP
There are no rows	s to display.										
There are no rows	s to display.										
There are no rows	s to display.										
There are no rows	s to display.								Add		
There are no rows	s to display.							_	Add		
There are no rows	s to display. DEVICE AP	LOCATION	POLICY	RIGHTS	SECURITY	PORTAL	ADMIN	CLOUD	Add	LOGS LOG	GOUT
There are no rows STATUS Virtualizati	on Radio	LOCATION	POLICY	RIGHTS	SECURITY	PORTAL	ADMIN	CLOUD	Add	LOGS LOG	GOUT
There are no rows STATUS Virtualizati	s to display. DEVICE AP on Radio	LOCATION Access Control	POLICY AP Update	RIGHTS	SECURITY	PORTAL	ADMIN	CLOUD	Add	LOGS LOG	GOUT
There are no rows STATUS Virtualizati BLACK LIST	b to display. DEVICE AP on Radio [WHITE LIST	LOCATION Access Control	POLICY AP Update	RIGHTS	SECURITY	PORTAL	ADMIN	CLOUD	Add	LOGS LOG	GOUT
There are no rows STATUS Virtualizati BLACK LIST Name	DEVICE AP	LOCATION Access Control	POLICY AP Update	RIGHTS	SECURITY	PORTAL Please enter1	ADMIN the values betw	CLOUD	Add	LOGS LOG	50UT <>= \\;.,?/#@
There are no rows STATUS Virtualizati BLACK LIST Name MAC	DEVICE AP	LOCATION Access Control	AP Update	RIGHTS	SECURITY	PORTAL Please enter 1 (00:00:00:00:00:00	ADMIN the values betv 0:00)	CLOUD veen 1 and 30 cha	Add	LOGS LOG	SOUT ×>=[\:,?/#@
There are no rows STATUS Virtualizati BLACK LIST Name MAC IP Address	DEVICE AP	LOCATION Access Control	AP Update	RIGHTS	SECURITY	PORTAL Please enter 1 (00:00:00:00:00	ADMIN the values bety 0:00) 0)	CLOUD	Add	LOGS LOG	50UT <>=[\\;.;?#@
There are no rows STATUS Virtualizati BLACK LIST Name MAC IP Address VSLAN	DEVICE AP on Radio (WHITE LIST	LOCATION Access Control	AP Update	RIGHTS	SECURITY	PORTAL Please enter 1 (00:00:00:00:00:00 (0.0.0.0.0.0.0)	ADMIN the values between the values of the value of t	CLOUD	MAINTAIN	LOGS LOG	SOUT ××=∏\;;?/#@

- 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

LOGOUT

LigoWave								
STATUS DEVICE AP LO	ICATION POLICY RIGHTS SECURITY PORTAL ADMIN CLOUD MAINTAIN LOGS LOGOUT							
Virtualization Radio Access	Control AP Update							
Name Number	Please enter the values between 1 and 30 character(Illegal character:1\$%^*0~+<>=[\\;?#@&`*"]{ Number nust be qnique,the serial number range 1-16							
AP Identity								
Hardware Model	APC 5M-12 V							
AP MAC	00:00:00:00:00 The default is null, indicating that the policy applies to all AP devices in the hardware model							
Firmware Version	8.0.0(r67.16.7152) •							
New Version Enable	6.2.2 (r256. 196. 8938). bin ▼ Please upload the new firmware							
Save Cancel								

- **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

Sasic Setup	25 rows per page ▼	Search Clear					
TOP>>				11-140-100	100-00	Dedia	
P MAC	Name	LIGOLAC IP1	LIGOLAU IP2	LIGOLAC IPS	wan	Kadio	Location
\$14:cf:92:6f:0e:e0					Function-Wechat		
@00:19:3b:ee:4c:ec							
@00:19:3b:ed:cc:f8							
@00:19:3b:ed:cc:e7							
@00:19:3b:ed:c1:b4	Andy Demo				Andy	Andy Test	
@00:19:3b:ed:2e:09	Test				test1	test	
@00:19:3b:ed:28:dd							
©00:19:3b:ed:12:89							
🔍 🗢 00:19:3b:ed:0c:9a	Test				test	test	
©00:19:3b:ed:09:f5	customer test1				customer test1	test	
🔍 🍣 00:19:3b:ed:09:eb	customer test				customer test	test	深圳
🔍 🗢 00:19:3b:ed:09:9a							
©00:19:3b:ec:de:30	1111				test	test	
@00:19:3b:ec:d6:aa							
©00:19:3b:ec:b2:54							
©00:19:3b:ec:78:e8	Test				test	test	深圳
@00:19:3b:ec:78:51							
@00:19:3b:eb:e5:9b					henry	henry	
🗢 00:19:3b:eb:e0:9b	21楼				Function Guest Guest01	21桜	深圳首达电子;
©00:19:3b:eb:0b:ce	test1				test	test1	
@00:19:3b:02:8d:a3	2M-VVall				Function-Wechat lan	test	深圳

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

Setup

STATUS DEVICE AP LOCATION P	OLICY RIGHTS SECURITY PORTAL ADMIN CLOUD MAINTAIN LOGS LOGOUT
Basic Setup	
Name MAC Location	14:cf:92:6f:0e:e0 select ▼
WlanLAN Policy Name Radio Policy	T.default Wian_lan_name T.select Wian_lan_name 11 Function-Wechat 5m-12 Function-Wechat Andy Function-Wechat customer test Select Radio Policy Default Radio Policy Select Radio Policy 214% SM-12Radio Andy Test Henry
LigoLAC IP1 LigoLAC IP2 LigoLAC IP3	
Scan Illegal AP Scan Interval	3600 Seconds
Wlan Error Scan Interval Scan Interval	0 minutes (Please enter a valid number, does not aloow nulls)
CLOUD Save Cancel	Super Admin 🔻

- **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;
- \diamond Save the configuration and reboot by the following commands:
- \diamond 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(<u>2.1.1</u>), 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:

Ligo_00:19:3b:eb:ba:03



♦ 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:192.168.100.21) address for the AP:



 \diamond 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



• 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"

STATUS DEVICE	AP LOCATION POLICY	RIGHTS SECURITY PORTAL	ADMIN MAINTAIN LOGS LOGOUT	
Basic Setup DNS Se	erver Ports IP Rou	te Policy Route OSPF DHCP	SNMP STA Server Date & Time	
Interface Setup	Device	172.16.250.245 172.16.250.245		
172.16.250.245				
🖃 🚳 Default	Interface VLAN Bridge	VSLAN VPN		
• 172.16.250.246	Name	Member	STP Status	Status
1/2.16.250.247	VSLAN 1		×	× .
			Add	

STATUS DEVICE	AP LOCATION POLICY RIGHTS SE	ECURITY PORTAL ADMIN	MAINTAIN LOGS LOGOUT
Basic Setup DNS Se	erver Ports IP Route Policy Route	OSPF DHCP SNMP	STA Server Date & Time
DHCP Setup ↑172.16.250.245 © Default ↑172.16.250.246 ↑172.16.250.246 ↑172.16.250.247	Device ID	172.16.250.245 172.16.250.245 8 (1-999)	
.	Name STP Status Status	VILAR 6	
	Save Cancel		

- 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

STATUS DEVICE	AP LOCATION	POLICY RIGHTS SECU	RITY PORTAL	ADMIN MAINTAIN	LOGS LOG	GOUT	
Basic Setup DNS S	erver Ports	Policy Route	OSPF DHCP	SNMP STA Server	Date & Time		
IP Setup	Device		172.16.250.245 172.16.250.245				
1/2.16.250.245	Interface	Interface IP Type	IP #	Address/Subnet Mask			Management Channel
172.16.250.246	Slot/Port 0/1	STATIC	172	2.16.250.245/255.255.255.0			✓
▲172.16.250.247						Add	
STATUS	ICE AP	LOCATION POLICY	RIGHTS SEC	CURITY PORTAL	ADMIN	MAINTAIN	LOGS LOGOUT
Basic Setup	DNS Server	Ports IP Route	Policy Route	OSPF DHCP	SNMP	STA Server	Date & Time
IP	Device			172.16.250.2 172.16.250.2	2 45 245		
Default	Interface	•		VSLAN 8 V			
	Interface	P Type		STATIC V			
	IP Addre	ss/Subnet Mask		192. 168. 4. 1	/ 255.255.255.	0 (/24) 🔻	
	Manager	nent Channel 🛛 📄 🕭	L				
	Manager	nent Rights 📃					
	Save	Cancel					



• DHCP - DHCP Server - select virtual interface - check "Enable" - Save

STATUS DEVICE	AP LOCATION	POLICY RIGHTS SECURITY PORTAL ADMIN MAINTAIN LOGS LOGOUT					
Basic Setup DNS 8	Server Ports IP	Route Policy Route OSPP DHCP SNMP STA Server Date & Time					
DHCP Setup	Device	172.16.250.245 172.16.250.245					
Default	DHCP Server DH	ICP Relay					
172.16.250.247	DHCP Serve	wr DHCP Demain Static IP 0 day 1 year 0 minutes					
	Max Lease Time	1 day 0 hoar 0 minutes					
	DHCP Setup						
		Start DHCP Service DHCP service is turned off					
	Configure the monitoring interface for DHCP Service						
	Interface	IP Address/Subnet Mask	Enable				
	Slot/Port 0/1	172.10.250.245/255.255.265.0	8				
	Slot/Port 0/2						
	Slot/Port 0/3						
	Slot/Port 0/4						
	Slot/Port 0/5						
	Slot/Port 0/6						
	VSLAN 8	192.168.4.1/255.255.255.0	✓				
		Save					

• Click "Add" under "DHCP Domain" to create DHCP domain; set relevant

information, then click "Save"

STATUS DEVICE	AP LOCATION POLICY RIGHTS SECU	URITY PORTAL ADMIN MAINTAIN LOGS LOGOUT
Basic Setup DNS Se	rver Ports IP Route Policy Route	OSPF DHCP SNMP STA Server Date & Time
DHCP Setup	Device	172.16.250.245 172.16.250.245
© Cefault	IP Address	192.160.4.0
172.16.250.247	Subnet Mask	255. 255. 0 (/24) 🔹
	Gateway	192.168.4.1
	DNS Server	192.168.4.1
	DNS Server	202.106.250.33
	Domain Name	Legal character of letters, numbers, (-) surports a length of 0-63
	IP Range	192.168.4.2 192.168.4.250 Add
	192.168.4.2-192.168.4.250	
		Det
	>>Advanced option	
	Save Cancel	

• Return to DHCP Server, click "Start DHCP Service", then LAC/WAC will start to

allocate addresses for STAs

STATUS DEVICE	AP LOCATION POLICY R	HTS SECURITY PORTAL ADMIN MAINTAIN LOGS LOGOUT					
Basic Setup DNS S	erver Ports IP Route I	olicy Route OSPF DHCP SNMP STA Server Date & Time					
DHCP Setup	Device	172.16.250.245 172.16.250.245					
🕞 💊 Default	DHCP Server DHCP Relay						
172.16.250.246							
1/2.16.250.247	DHCP Server DHCP Don	ain Static IP					
	Default Lease Time	0 day 1 hour 0 minutes					
	Max Lease Time	1 day 0 hour 0 minutes					
	DUCD Satur						
		B	tant DHCP Service				
	Configure the monitoring interface for DHCP Service						
	Interface	IP Address/Subnet Mask	Enable				
	Slot/Port 0/1	172.16.250.245/255.255.255.0					
	SlotPort 0/2						
	SlotPort 0/3						
	SlotPort 0/4						
	Slot/Port 0/5						
	Slot/Port 0/6						
	VSLAN 8	192.168.4.1/255.255.255.0	8				
			Save				



• Create WLAN policy, Portal policy and Authentication policy for AP by

"POLICY- Virtualization"

• Create SSID encryption scheme by "WLAN - Security - Add"

	71	5	
STATUS DEVICE	AP LOCATION POLICY	RIGHTS SECURITY PORTAL ADMIN MAINTAIN LOGS LOGOUT	
Virtualization Ra	dio 🕴 Access Control 🕴 AP Update		
🖉 VSLAN			
🕞 Portal	VALANA AN Security		
S WLAN/LAN	Policy Name		Encryption
Authentication	test		open
	1		wpa psk/wpa2 psk
		_	
			Add
STATUS DEVICE			LOCOLIT
STATUS DEVIC	E AF LOCATION POL		
Virtualization F	Radio 🕴 Access Control 🕴 AP Up	date	
VSI AN			
Portal			
▶ WLAN/LAN	WLAN/LAN Security		
Authentication	Name	Rease enter the values between 1 and 30 character(illegal i	character:"\$%^*()~+<>=[\\;:,?#@&`\"[{}.)
	Encryption	wpa-psk/wpa2-psk 🔻	
	Encryption	tkip+aes V	
	Key	868868688 allow length 8~31	
			
	Save Cancel		
Return	to WLAN and a	dd WLAN policy:	
• Return		idd WEMix policy,	
STATUS DEVICE	AP LOCATION POLICY	RIGHTS SECURITY PORTAL ADMIN MAINTAIN LOGS LOGOUT	
Virtualization Rad	lio Access Control AP Update		
🕞 VSLAN 🥂			
Portal	WLAN/LAN Security		
Authentication	Nono ESSTD		
<u> </u>	21-001-0	Jean Clear	
	Name test	ESSID Security D	Perfault Forwarding Mode
	1051		Lood Forward. Drogo
			Add
STATUS DEVICE	AP LOCATION POLICY	RIGHTS SECURITY PORTAL ADMIN MAINTAIN LOGS LOGOUT	
Virtualization Radio	Access Control AP Update		
CAVSI AN			
Portal	WA ANA AN		
▶ WLAN/LAN	WEANLAN Security		
Authentication	Policy type	Place enter the values between 1 and 30 character/iller	al character:"\$%ハ=0~+<>=1))、2雌のルミリ=0())
	FCCID	Interest of the second se	an enalged of the state of the
	ESSID Security Policy	Prease enter the values between Fand ST character	
	User Limit	0 (Each AP to allow the maximum number of users access the ESSID,0	
	Hidden	Show Essid Hide Essid	means no limit)
			means no limit)
	Radio Freq		means no limit)
	Radio Freq Forwarding Mode	Local Forward Bridge V	means no limit)
	Radio Freq Forwarding Mode	Local Forward: Bridge VLANID 0 (0-4096, 0 means not set)	means no limit)
	Radio Freq Forwarding Mode	Local Forward: Bridge VLANID 0 (0-4496, 0 means not set) BYPASS	means no limit)
	Radio Freq Forwarding Mode Default	Lecal Fervard: Tridge V VLANID 0 OPPASS 0 @ no yes	means no limit)
	Radio Freq Forwarding Mode Default	Local Forward Bridge V VLANID 0 (0-4+96, 0 means not set) BYPASS 0	means no limit)

- 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;
| CLigoW | ave | |
|-------------------|-------------------------------|--|
| STATUS DEVICE | | RIGHTS SECURITY DORTAL ADMIN MAINTAIN LOGS LOGOLIT |
| Midualization Rad | in Access Control AP Undate | |
| | No Access Control - Al Opdate | |
| Portal | Name URL | Search Clear |
| Authentication | Name URL | |
| | test 👂 http://1 | 72.16.250.245/admin_0/portalweb/index.php |
| | | Add |
| STATUS DEV | ICE AP LOCATION | POLICY RIGHTS SECURITY PORTAL ADMIN MAINTAIN LOGS LOGOUT |
| Virtualization | Radio Access Control | AP Update |
| VSLAN | | |
| Portal | Name | kk Please enter the values between 1 and 30 character:///www.even/////////////////////////////////// |
| WLAN/LAN | PORTAL | http://172.18.250.245/admin_0/portalweb/index.php |
| Authentication | FORTAL | Portal Service Mode centralized V |
| | Params List | Flease Select One parameter V Allas + - |
| | Save Cance | |

• Click "Add" under "Authentication policy" to create Authentication policy. The default local authentication is System Authentication Policy;

STATUS DEVICE	AP LOCATION POLICY RIGHTS SECURITY PORTAL ADMIN MAINTAIN LOGS LOGOUT	
Virtualization	dio Access Control AP Update	
 VSLAN Portal WLANLAN Authentication 	Authentication Policies Authentication Services Authentication Pol Authentication Se Search Clear	
	Authentication Policy Authentication S	Service
	System Authentication Policy Built-In	
	Add	
STATUS DEVICE	AP LOCATION POLICY RIGHTS SECURITY PORTAL ADMIN MAINTAIN LOGS LOGOUT	
Virtualization Radio	Access Control AP Update	
S VSLAN	Name System Authentication Folicy Please enter the values between 1 and 30 character(Ulegal character:1\$%**()-+<>=[0,:]?##@	@&`\"[(}.)
VLANLAN Authentication	Make this the preferred Authentication Policy for new Connection Profiles	
	Authentication Services	
	Authentication Service Service Type	
	NT Domain Logons - Kerberos NT Domain Logons - Kerberos (Typically Windows 2000 or Windows XP clients)	
	NT Domain Logons - NTLM NT Domain Logons - NTLM CTypically Windows 98 or Windows NT clients)	
	802.1x / Gons 802.1x / RADIUS Layer 3 IP Access	
	Built-in Built-in	
	New Senice local default	
	Save Cancel	

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

AP LOCATION POLICY RIGHTS SECURITY PORTAL ADMIN MAINTAIN LOGS LOGOUT	STATUS DEVICE
adio Access Control AP Update	Virtualization
<	🕞 VSLAN
Authentication Policies Authentication Services	Portal WLAN/LAN
Authentication Se Search Clear	► Authentication
Authentication Service	
 Anir-lu	
Authentication Policies Authentication Services Authentication Se Search Clear Authentication Service Buill-In	VSLAN Portal VLANLAN Authentication

STATUS DEVICE	AP LOCATION POLICY RIGHTS	SECURITY PORTAL ADMIN MAINTAIN LOGS LOGOL
Virtualization Radio	Access Control AP Update	
VSLAN Portal WLANLAN S Authentication	Auth Type Name Server Port Secret Confirm Secret Group Identity Field	RADIUS Image: Constraint of the second se
	Reauthentication Field	Session-Timeout
	Timeout (Seconds)	5
		Enable RADIUS Accounting (RFC-2866) on port 1813 Enable RADIUS CoA on port 3799 Enable Drcom CoA on port 1813

• 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".

STATUS DEVICE	AP LOCATION F	OLICY	GHTS SECURITY	PORTAL ADMIN MA	INTAIN LOGS LOGOUT			
Virtualization Radio	Access Control AF	Vpdate 🔨						
SVSLAN	Network ID Name N		/lan/LAN Policy Nam Authe	ntication Portal	Search Clear			
Authentication	Network ID	Name	Wlan/LAN Policy Name		Authentication			
	2	test	test		System Authentication Policy	test		
STATUS DEVICE		POLICY P	IGHTS SECURITY	DOPTAL ADMIN M		Add		
STATUS DEVICE	AP LOCATION		Initia Secontri					
Virtualization Radio	Access Control A	P Update 👘						
SVSLAN Portal					1			
WLAN/LAN	Name		kk	Please enter the	alues between 1 and 30 character(Ille	gal character:'\$%^*()~+<>=[\\;;,?/#@&`\"[{}.)		
Addientication	Network ID		8					
	Wian/LAN Policy Name		T.default wlan_lan_nam	e T.selectwian_lan_name				
				kk				
	User Authentication							
	Authentication Service Mode	,	centralized v					
	Authentication		System Authentication	a Policy 🔻				
	Portal		kk 🔻					
	User IP Unique							
	Forwarding Mode							
	User Isolation							
	Description							
	Save Cancel							

• 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

STATUS DEVICE AP LOCATION POLICY I	RIGHTS SECURITY	PORTAL ADMIN	MAINTAIN	LOGS LOGOU	л			
Basic Setup								
AP MAC Name 25 rows per page ▼	Search Clear							
TOP>>	Name	LAC ID1				W		
• • • • • • • • • • • • • • • • • • •	Name			LACIFZ	LACIES			
\$\overline\$ \$\overline\$ 00:19:3b:ff:6c:5e								
📄 🍩 00:19:3b:ec:d6:90	test	172.16.250.246				te		
\$\overline{19:3b:ec:82:b0}								
Select allMove To T Del AP Batchly	Configure	Add AP Add Group	Export As Excel					
STATUS DEVICE AP LOCATION POL	ICY RIGHTS	SECURITY PORTAL	ADMIN	MAINTAIN	LOGS LOGOUT			
Desite Option 1								
Basic Selup								
Name	kk							
MAC	00:19:3b:eb:ba:03							
Pseudo MAC	00:00:00:00:00:00							
Location	select 🔻							
Man I AN Delige Name	Telefaultuden lan nama Tealastuden lan nama							
Wian/LAN Policy Name	I.derault wian_lan_hame II.select wian_lan_hame							
		test						
Radio Policy	Default Radio Policy	Select Radio Policy						
		test						
LAC IP1								
LAC IP2								
LAC IP3								
Scan Wegal AP								
Open scan sta	Low Accurat	cy 👝 High Accuracy 👝 F	Probe					
Scan Interval	3600 Seconds							
Report equipment status information								
Wian Error Scan Interval								
Scan Interval	0	minutes (Please enter	a valid nuniber,do	oes not aloow null:	s)			
CLOUD	Super Admin 🔻							
Save Cancel								

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"

STATUS DEVICE	AP LOCATION POL	ICY RIGHTS SECURITY PORTAL ADMIN MAINTAIN LOGS LOGOUT
Virtualization Ra	dio Access Control AP Up	pdate
⊮ VSLAN		
➢ Portal	Name	Please enter the values between 1 and 30 character(Illegal character:\\$%^*()~+<>=[\\;;,?#@&\"[]().)
WLAN/LAN Authentication	PORTAL	http://172.16.250.245/admin_0/portalweb/index.php Portal Service Mode centralized V
	Params List	Please Select One parameter V Alias + -
	Save Cancel	

• Select "Authentication policy" under "Policy"

STATUS DEVICE	AP LOCATION POLICY RIGHTS SECURITY PORTAL ADMIN MAINTAIN LOGS LOGOUT	
Virtualization Radio	Access Control AP Update	
S VSLAN		
S WLAN/LAN	Authentication Policies Authentication Services	
Authentication	Authentication Po Authentication Se Search Clear	
	Authentication Policy	Authentication Service
	System Authentication Policy	Built-in
	Add	

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

STATUS DEVICE	AP LOCATION POLICY F	RIGHTS SECURITY PORTAL ADMIN MAINTAIN LOGS LOGOUT								
Virtualization Rad	io Access Control AP Update									
© VSLAN	Name Network ID Wian LAN Policy Name	Nak Please enter the values between 1 and 30 character(llegal character:1\$%**0-++>=(\t;;?/#@&**0[(),) 8 T.default wlan_lan_name Kk yu								
	User Authentication									
	Authentication Service Mode	centralized V								
	Authentication	System Authentication Policy 🔻								
	Portal	kk 🔻								
	User IP Unique									
	Forwarding Mode									
	User Isolation									
	Description									
	Save Cancel									



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"

STATUS DEVICE	AP LOCATION	POLICY RIGHTS	SECURITY PORTAL AL	MIN MAINTAIN	LOGS LOGOUT				
Virtualization Rad	io Access Control	AP Update 🔨							
Radio	RF Channel		Tx Power			Antenna	Flags	RSSI	
test	3		0dbm(1mw)			Open		0	-100
					Add				
STATUS	DEVICE AP	LOCATION	POLICY RIGHTS	SECURITY	PORTAL	ADMIN	MAINTAIN	LOGS	LOGOUT
Virtualization	Radio	Access Control	AP Undate						
Name Mode Htmode RF Channel TX Power Antenna RSSI(dBm)		kk 802.11bgtn HT20 0dbm(lmw) Open -100	ase enter the value s betw	enter the values be veen -100 and -50	tween 1 and 30	character(Illeg	ial character:1\$%	₩)~+<>= 0;;;	?##@&`\"](}.)
Save Ca	ancel								

• 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.

STATUS DEVICE AP LOCATION	POLICY RIGHTS SECURITY PORTAL ADMIN MAINTAIN LOGS LOGOUT
Basic Setup	
Name	kk
MAC	00:19:3b:eb:ba:03
^o seudo MAC	00:00:00:00:00
ocation	select V
Wian/LAN Policy Name	T.default.wlan lan name T.select.wlan lan name
	test
	uu
Radio Policy	Default Radio Policy Select Radio Policy
	test kk
LAC IP1	
LAC IP2	
LAC IP3	
Scan Illegal AP Onon scan sta	Contraction of High Accuracy of Prohe
Scan Interval	3600 Seconds
Report equipment status information	
Man Error Scan Interval	
Scan Interval	0 minutes (Please enter a valid number, does not aloow nulls)
Joan Interval	

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"

STATUS DEVICE	AP LOCATI	ON POLICY	RIGHTS SEC	URITY PORTAL	ADMIN	MAINTAIN	LOGS LOGOUT						
Basic Setup DNS S	erver Ports	IP Route	Policy Route	OSPF DHCP	SNMP	STA Server	Date & Time						
Interface Setup	Device	×		192.168.100.1 192.168.1.2	68								
Default	Interface	VLAN Bridge V	VSLAN VPN										
	Name		Mode			MTU	TRUNK	TYPE		VSLAN	BY IP	Status	
	SlotiPort 0/1		Route Mo	ide		1500	X	Uplink		1	X	✓	Ø
	SlotiPort 0/2		Route Mo	ide		1500	X	Uplink		1	X	×	0
	SlotPort 0/3		Route Mo	ide		1500	x	Downlink		1	×	v	Ø
STATUS	DEVICE	AP LO	CATION	POLICY	RIGHTS	SECU	IRITY PORTA	L ADMIN	MAINT	AIN LOGS	LOGOUT		
Basic Setup	DNS 5	Server Po	rts IP	Route	Policy	Route	OSPF DHCF	SNMP	STA Ser	ver Date & T	ime		
Ports		Device						-	192.168.1 192.168.1	00.168 00.168			
192.168.100. A Default	168												
4		Name					Slot/Port 0/2						
		MAC					00:e0:4c:14:18:a	0					
		Pseudo MAC	:			00:00:00:00:00:00 (You can set '00:00:00:00:00' to delete pseudo mac)							
		мти											
		Dort Connor	tion Tumo				1500	(Please ent	erthe 68-1	500 values)			
		TYDE	don type				AutoseLect	•					
							Both VLAN ID						
		TRUNK 🔲					Allow VLAN ID					(0-4095,English comm	a separated)
		Mode					Route Mode 🛛 🔻						
		VSLAN					1	(1-999)					
		BY IP											
		STATUS					•						
		Save	Cancel								~		

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

STATUS DEVICE	AP LOCATION	POLICY RIGHTS SECURITY	PORTAL ADMIN MAINTAIN LOGS LOG	TUO	
Basic Setup D	NS Server Ports IP	Route Policy Route OSPF	DHCP SNMP STA Server Date & Time		
IP Setup	Device	•	192.168.100.168 192.168.1.2		
192.168.100.168	Interface	Interface IP Type	IP Address/Subnet Mask	Management Channel	Management Rights
a pendan	Slot/Port 0/1	STATIC	192.168.1.2/255.255.255.0	✓	×
	Slot/Port 0/2	STATIC	192.168.3.1/255.255.255.0	×	×

LigoWave		
STATUS DEVICE	AP LOCATION POLICY RIGHTS SE	ECURITY PORTAL ADMIN MAINTAIN LOGS LOGOUT
Basic Setup DNS S	erver Ports IP Route Policy Route	OSPF DHCP SNMP STA Server Date & Time
IP	Device	192.168.100.168 192.168.1.2
Sefault Sefault	Interface	Slot/Port 0/2 V
	Interface IP Type	STATIC V
	IP Address/Subnet Mask	192.168.3.1 / 255.255.255.0 (/24) V
	Management Channel 📃 🔺	
[Management Rights 🛛 🖉	
	Save Cancel	

• 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"

STATUS DEVICE	AP LOCATION POLICY RIGHTS	SECURITY PORTAL ADMIN MAINTAIN LOGS LOGOUT
Basic Setup DNS S	erver Ports I IP Route Policy Route	e OSPF DHCP SNMP STA Server Date & Time
IP	Device	192.168.100.168 192.168.1.2
Sector Control	Interface	Slot/Fort 0/1 ▼
	Interface IP Type	STATIC V
	IP Address/Subnet Mask	192. 168. 1. 2 / 255. 255. 2 (/24) V
	Management Channel 🛛 🕢 🛦	
	Management Rights 🛛 🕢	
	Save Cancel	

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

STATUS DEVICE	AP LOCATION	POLICY RIGHTS SE	CURITY PORTAL A	ADMIN MAINTAIN I	.0GS LOGOUT	
Basic Setup DNS S	erver Ports IP	Route Policy Route	OSPF DHCP SI	NMP STA Server [Date & Time	
Route Setup	Device		192.168.100.168 192.168.1.2			
192.168.100.168 Oefault	Destination/Subnet mas	ĸ			Gate	eway.
	There are no rows to disp	blay.				
						Add
STATUS DEVICE	AP LOCATIO	N POLICY RIGHTS	SECURITY POL	RTAL ADMIN N	IAINTAIN LOGS	LOGOUT
Basic Setup DN	S Server Ports	IP Route Policy	Route OSPF D	HCP SNMP S	TA Server Date & Tim	ie
Route Setup	Device		192.168 192.168	8.100.168 8.1.2		_
Sefault	Destination/Subn	et mask	0.0.0.0	/ 0.0.0.0 (/0)	•	
	Gateway		192.168.1.1			
	Routing Metric		1	(Please enter the va	alues between 0 and 65535)
	Save	ancel				_

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

STATUS DEVICE	AP LOCATION	POLICY RIGHTS	SECURITY PORTAL	ADMIN MAINTAIN	LOGS LOGOUT
Basic Setup DN:	S Server Ports IP	Route Policy Route	OSPF DHCP	SNMP STA Server	Date & Time
DNS Server	Device DNS Server		192.168.100.168 192.168.1.2		
Sefault	Primary DNS Secondary DNS		192.168.1.1 8.8.8.8]	
	Save				

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"

Basic Setup DNS Se	nver Ports IP Ro	ute Policy Route OSPF DHC	P SNMP STA Server Date & Time	1
Interface Setup	Device	() 192.168.100	0.168	
• 192.168.100.168	Interface V/ AN Bride	192.168.1.2	•	
Default	Name VSLAN 1	Member	STP Statu	S
				Add
STATUS DEVICE Basic Setup DN	AP LOCATION	POLICY RIGHTS SECURI Route Policy Route O	TY PORTAL ADMIN MAINT SPF DHCP SNMP STA Se	Add
Basic Setup DHCP Setup	AP LOCATION IS Server Ports IP Device	POLICY RIGHTS SECURI Route Policy Route O	TY PORTAL ADMIN MAINT ISPF DHCP SNMP STA Se 192.168.100.168 192.168.102.168 192.168.102.168	Add AIN LOGS LOGG rver Date & Time
STATUS DEVICE Basic Setup DN DHCP Setup \$	AP LOCATION IS Server Ports IP Device ID	POLICY RIGHTS SECURI Route Policy Route O	TY PORTAL ADMIN MAINT SPF DHCP SNMP STA Se 192.168.100.168 192.188.1.2 192.188.1.2 8 (1-999) 1	Add AIN LOGS LOG
STATUS DEVICE Basic Setup DN DHCP Setup 0 \$192.168.100.168 192.168.1.2 Default 0	AP LOCATION IS Server Ports IP Device ID Name	POLICY RIGHTS SECURI Route Policy Route O	TY PORTAL ADMIN MAINT SPF DHCP SNMP STA Se 192.168.100.168 192.168.1.2 192.168.1.2 8 (1-999) VSLAH 8 (1-999)	Add AIN LOGS LOGG rver Date & Time
STATUS DEVICE Basic Setup DN DHCP Setup 4 92.168.100.168 4 92.168.1.2 4 Default 5	AP LOCATION IS Server Ports IP Device ID Name STP Status	POLICY RIGHTS SECURI Route Policy Route O	TY PORTAL ADMIN MAINT SPF DHCP SNMP STA Se 192.168.100.168 102.168.10 102.168.10 102.168.10 102.168.10 102.168.10 102.168.10 102.168.10 102.168.10 102.168.10 102.168.10 102.168.10 102.168.10 102.168.10 102.168.10 102.168.10 102.168.10 102.168.10 102.168.10 102.168.10 102.168.10 102.168.10 102.168.10 102.168.10 102.168.10 102.168.10 102.168.10 103.168.10 102.168.10 102.168.10 103.168.10 102.168.10 102.168.10 103.168.10 102.168.10 102.168.10 103.168.10 102.168.10 102.168.10 103.168.10 102.168.10 102.168.10 103.168.10 102.168.10 102.168.10 103.168.10 103.168.10 103.168.10 103.168.10 103.168.10 103.168.10 103.168.10 103.168.10 </td <td>Add AIN LOGS LOGG rver Date & Time</td>	Add AIN LOGS LOGG rver Date & Time

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

STATUS DEVICE	AP LOCATION	POLICY RIGHTS SECURIT	Y PORTAL ADMIN MAINTAIN LOGS LOGOUT	
Basic Setup DNS S	enner Ports III	Route Policy Route OS	PF DHCP SNMP STA Server Date & Time	
IP Setup	Device		192.168.100.168 192.168.1.2	
192.168.100.168	Interface	Interface IP Type	IP Address/Subnet Mask	Management Cl
A Default	Slot/Port 0/1	STATIC	192.168.1.2/255.255.255.0	✓
4	Slot/Port 0/2	STATIC	192.168.3.1/255.255.255.0	×
				Add
STATUS DEVICE	E AP LOC	ATION POLICY RIGHTS	SECURITY PORTAL ADMIN MAINTAIN	LOGS LOGOUT
Basic Setup D	NS Server Port	s I IP Route Policy I	Route OSPF DHCP SNMP STA Server	Date & Time
IP	Device		192.168.100.168 192.168.1.2	
192.168.1.2 Default	Interface		VSLAN 8 T	
	Interface IP	Гуре	STATIC V	
	IP Address/S	iubnet Mask	192. 168. 4. 1 / 255. 255. 255. 0 (/24) V	
	Managemen	t Channel 🛛 🖻 🛦	· · · · · · · · · · · · · · · · · · ·	
	Managemen	t Rights 📃		
	Save	Cancel		



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"

STATUS DEVICE	AP LOCATION	POLICY RIGHTS SECURITY	PORTAL ADMIN MAIN	TAIN LOGS	LOGOUT		
Basic Setup DNS 8	Server Ports IP	Route Policy Route OSPF	DHCP SNMP STAS	erver Date & Tim	e		
DHCP Setup	Device	19 2 19	2.168.100.168				
192.168.100.168							
192.168.1.2	DHCP Server DHC	P Relay					
& Detault							
	DHCP Server Default Lease Time	DHCP Domain Static IP	1 hour 0 minutes				
	Max Lease Time	1 day	0 hour 0 minutes				
	DHCP Setup						
					Start DHCP Service DHCP service is turned off		
	Configure the monitoring interface for DHCP Service						
	Interface		IP Address/Subnet Mask				Enable
	SlotPort 0/1		192.168.1.2/255.255.255.0				
	Slot/Port 0/2		192.168.3.1/255.255.255.0				
	Slot/Port 0/3						
	Slot/Port 0/4						
	Slot/Port 0/5						
	SlovPort 0/6						
	VSLAN 1						
	VSLAN 8		192.168.4.1/255.255.255.0				V
						~	
					Save		

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

DEVICE	AP LOCATION POLIC	ICY RIGHTS SECURITY PORTAL ADMIN MAINTAIN LOGS LOGOUT	
Basic Setup Df	NS Server Ports IP R	Route Policy Route OSPF DHCP SNMP STA Server Date & Time	
DHCP Setup	Device	192.168.100.168 192.168.12	
192.168.100.168			
192.168.1.2 Default	DHCP Server DHCP Relay		
•	DHCP Server	DHCP Domain Static IP	*
	IP Address	Subnet Mask	
	There are no rows to display.		
			Add
STATUS			
Basic Setur	aver Dotte ID Doute D		
Dasic Setup			
DHCP Setup	Device	192.168.100.168 192.168.12	
192.168.100.168 192.168.1.2	ID Addrass	192 168 3.0	
& Default	fr Auditaa		
	Subnet Mask	255, 255, 255, 0 (/24)	
	Gateway	192. 168. 3. 1	
	Gateway DNS Server	192.168.3.1	
	Gateway DNS Server DNS Server	192, 168, 3, 1 192, 168, 1, 1 192, 168, 3, 1	
	Gateway DNS Server DNS Server Domain Name	192. 168. 3. 1 192. 168. 1. 1 192. 168. 3. 1 Legal character of letters, numbers, (-) supports a length of 0-63	
	Gateway DNS Server DNS Server Domain Name IP Range	192. 168. 3. 1 192. 168. 3. 1 192. 168. 3. 1 Legal character of letters, numbers, (·) supports a length of 0-63 192. 168. 3. 2 192. 168. 3. 254	
	Gateway DNS Server Domain Name IP Range 192 168 3 2-192 168 3 264	192. 168. 3. 1 192. 168. 1. 1 192. 168. 3. 1 192. 168. 3. 1 Legal character of letters, numbers, (-) supports a length of 0-63 192. 168. 3. 2 192. 168. 3. 2	
	Gateway DNS Server Domain Name IP Range 192.168.3.2-192.168.3.254	192. 168. 3. 1 192. 168. 3. 1 192. 168. 3. 1 192. 168. 3. 1 192. 168. 3. 1 192. 168. 3. 1 192. 168. 3. 1 192. 168. 3. 1 192. 168. 3. 1 192. 168. 3. 2	
	Gateway DNS Server DNS Server Domain Name IP Range 192.168.3.2-192.168.3.254	192. 168. 3. 1 192. 168. 1. 1 192. 168. 3. 1 192. 168. 3. 1 192. 168. 3. 1 192. 168. 3. 2 - 192. 168. 3. 254 Add	Del
	Gateway DNS Server DNS Server Domain Name IP Range 192.168.3.2-192.168.3.254 >>Advanced option	192. 168. 3. 1 192. 168. 3. 1 192. 168. 3. 1 192. 168. 3. 1 192. 168. 3. 1 192. 168. 3. 1 192. 168. 3. 2	Del

LigoWav	e	
STATUS DEVICE	AP LOCATION POLICY R	IGHTS SECURITY PORTAL ADMIN MAINTAIN LOGS LOGOUT
Basic Setup DNS S	erver Ports IP Route	Policy Route OSPF DHCP SNMP STA Server Date & Time
DHCP Setup	Device	192.168.100.168 192.108.1.2
192.168.1.2	IP Address	192.168.4.0
A sound	Subnet Mask	255.255.255.0 (/24) 🔻
	Gateway	192.188.4.1
	DNS Server	192.168.1.1
	DNS Server	192.168.4.1
	Domain Name	Legal character of letters, numbers, (-) supports a length of 0-63
	IP Range	192.160.4.2 192.160.4.254 Add
	192.168.4.2-192.168.4.254	Dei
	>>Advanced option	
	Save Cancel	

• Click "Save" and return to the DHCP server option, enable DHCP service by click the button "Start DHCP Service"

STATUS DEVICE	AP LOCATION POLICY RIGHTS SEC	CURITY PORTAL ADMIN MAINTAIN LOGS LO	GOUT
Basic Setup DNS S	erver Ports IP Route Policy Route	OSPF DHCP SNMP STA Server Date & Time	
DHCP Setup	Device DHCP Server DHCP Relay	192.168.100.168 192.168.1.2	
C Delani	DHCP Server DHCP Domain Stati Default Lease Time Max Lease Time	Image: Description of the second s	
	DHCP Setup		
	Configure the monitoring interface for DHCP Service		Start DHCP Service DHCP service is turned off
	Interface	IP Address/Subnet Mask	
	Slot/Port 0/1	192.168.1.2/255.255.255.0	
	Slot/Port 0/2	192.168.3.1/255.255.255.0	
	Slot/Port 0/3		
	Slot/Port 0/4		
	Slot/Port U/5		
	SIDP ON UN6		
	VSLAN 8	192 168 4 1/255 255 255 0	
	*0D/140	132.100.4.1/233.233.233.233.0	
			Save

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":

LigoWave				
STATUS DEVICE	AP LOCATION POLICY	RIGHTS SECURITY PORTAL	ADMIN MAINTAIN LOGS LO	SOUT
S Authentication	Policy Name			
	There are no rows to display.			
STATUS DEVIC	E AP LOCATION P	OLICY RIGHTS SECURITY	PORTAL ADMIN MAINT	Add
Virtualization	Radio Access Control AF	' Update		
♥VSLAN ♥Portal	WLAN/LAN Security			
Authentication	Name	kk	Please enter the values between 1 a	and 30 character(Illegal character:'!\$%
	Encryption	wpa-psk/wpa2-psk 🔻		
	Encryption	tkip+aes 🔻		
	Key	88888888	allow length 8~31	
	Save Cancel			

• 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":

STATUS DEVICE	AP LOCATION POLICY RIGHTS	SECURITY PORTAL ADMIN	MAINTAIN LOGS LOGOUT
Virtualization Rad	io Access Control AP Update		
SUSLAN Portal SUM ANA ANA	WLAN/LAN Security		
Authentication	Policy Type	WLAN V	
	Name	kk	lease enter the values between 1 and 30 charac
ESSID		kk F	lease enter the values between 1 and 31 charact
	Security Policy	kk 🔻	
	User Limit	0 (Each AP to al	ow the maximum number of users access the ES
	Hidden Radio Freq	 Show Essid Hide Essid 2.4G 5G 	
	Forwarding Mode	Center Forward V Encryption Auto Negotiate V	
	Default	💿 no 🔾 yes	
	Save Cancel		

• By option PORTAL - Portal Customize - Portal List, add a new built-in portal,

named "kk", and save:

STATUS DEVICE	AP LOCATION POLIC	Y RIGHTS SECURITY PORTAL ADMIN MAINTAIN LOGS LOGOUT
Portal Customize	Upload Portal	
🕞 Slot Description 🛛 🥄		
🕞 Time	Portal Name	Portal URL
> Portal List	default	http://192.168.1.2/admin_0/portalweb/index.php
Custom		
		Add

LigoWave				
STATUS DEVICE	AP LOCATION	Policy Rights Secu	IRITY PORTAL ADMIN	MAINTAIN LOGS LOGOUT
Portal Customize	Upload Portal			
 Slot Description Time Portal List Custom 	Portal Name APIAddress Token Verification code Dynamic Password Save Cancel	kk ○ Open ● Close ○ Open ● Close	Please enter the values betwe	en 1 and 30 character(Illegal character:1\$%**0~-

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"

STATUS DEACE					
STATUS DEVICE	AP LOCATION	POLICE RIGHTS SECORITE	PORTAL ADMIN	MAINTAIN LOGS LOGOUT	
Portal Customize	Upload Portal				
_					
Slot Description					
🕞 Time	Portal Name	Portal URL			Verification code
Time Portal List	Portal Name kk	Portal URL Phtp://192.168.1.2/admin_0/c96	(名利の)	C+v14C	Verification code X
 Time Portal List Custom 	Portal Name kk default	Portal URL http://192.168.1.2/admin_0/c96 http://192.168.1.2/admin_0/port	<u>賃制</u> (f)	Ctrl+C	Verification code × ✓
 Time Portal List Custom 	Portal Name kk default	Portal URL http://192.168.1.2/admin_0/c96 http://192.168.1.2/admin_0/port	<mark>复制(f))</mark> 转到 http://192.168.1.2/w 打印(b)	Ctr1+C du 9/c96e37/index.php(6)	Verification code X V

• 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:

STATUS DEV	ICE AP LOCATION	POLICY RIGHTS SECURITY PORTAL ADMIN MAINTAIN LOGS LOGOUT
Virtualization	Radio Access Control	AP Update
VSLAN		
Portal	Name URL	Search Clear
WLAN/LAN		
Addientication	Name	URL
	There are no rows to displ	ay.
		Add
_		
STATUS DEV	VICE AP LOCATION	POLICY RIGHTS SECURITY PORTAL ADMIN MAINTAIN LOGS LOGOUT
Virtualization	Radio Access Control	AP Update
SVSLAN		
> Portal	Name	kk Please enter the values between 1 and 30 (haracter(illegal character:"\$%^*"(\-+<>=[N;;;?#@&`!"]{}.)
WLAN/LAN	DODTAL	http://192.168.1.2/admin_0/c96e37/index.php
Authentication	PORTAL	Portal Service Mode centralized 🔻
	Params List	Please Select One parameter V Alias + -
	Save Cancel	

 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:

LigoWave				
STATUS DEVICE	AP LOCATION POLICY RIGHTS	SECURITY PORTAL ADMIN MAINTAIN	LOGS LOGOUT	
Virtualization Radi	o Access Control AP Update			
Portal	Network ID Name Wlan/LA	N Policy Nam Authentication Portal Sea	Clear	
Authentication	Network ID Name W	an/LAN Policy Name A	Authentication	Portal
	There are no rows to display.			
STATUS DEVIC Virtualization	CE AP LOCATION POLICY Radio Access Control AP Update Name Network ID Want AN Policy Name	RIGHTS SECURITY PORTAL AD Ida Plear 8 T default wan lan name T default wan lan name	MIN MAINTAIN	Add LOGS LOGOU
	User Authentication	kk		
	Authentication Service Mode	centralized V		
	Authentication	System Authentication Policy 🔻		
	Portal	kk 🔻		
	User IP Unique			
	Forwarding Mode			
	User Isolation			
	URL Logging	Low Accuracy V		
	Description			
	Save Cancel			

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

STATUS DEVICE A	P LOCATION POLICY RIGHT	S SECURITY PORTAL ADMIN MAINTAIN LOGS LOGO	Л
Virtualization Radio	Access Control AP Update		
Radio	RF Channel	Tx Power	Antenna
There are no rows to display.			
		A00	
STATUS DEVICE	AP LOCATION POLICY	RIGHTS SECURITY PORTAL ADMIN MAINTAIN LO	GS LOGOUT
Virtualization	Access Control AP Lindate		
The shade of the state of the s			
Name	ldk	Please enter the values between 1 and 30 character/Illegal character/I\$%%*0~++	<>=N∵ 2/#@%""R3)
Mode	802.11bg†n 🔻		1041-00 (Box 11017)
Htmode	НТ20 🔻		
RF Channel	1 •		
Tx Power	Odbm (1mw) 🔻		
Antenna	Open V		
RSSI(dBm)	Please enter the	values between the and -50	
Save Cancel			



3.1.2.6. Add Users

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

STATUS DEVICE	AP LOCATION	POLICY	RIGHTS SECURITY	PORTAL	ADMIN	MAINTAIN	LOGS	LOGOUT
Role Admission	Rights	-						
Identity Profiles Users	Username	Search	Clear					
APP LINK	Full Name	Username	MAC Bind			IP Bind		
	There are no rows to disp	lay.						
			[Add				
STATUS DEVICE	AP LOCATION	POLICY	RIGHTS SECURITY	PORTAL	ADMIN	MAINTAIN	LOGS	LOGOUT
Role Admission	Rights							
Identity Profiles	Username		kk		Please enter	the values betw	een 1 and 32	(lllegal chara
● APP LINK	MAC Bind		-					
	IP Bind				1	×		
	ESSID Bind				Please enter	the values betv	veen 1 and 31	character
	VSLAN		0		(0Any)			
	Role		default Role	select R	ole			
			group					
	Password				Password fie	eld length must	oe between 6	and 32 chara
	Confirm Password				– Password fie	eld length must	oe between 6	and 32 chara
	Full Name Descriptive Name] 🔪			
	Advanced option>>							
	Save Cance)						

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		
AT	Device	192.168.100.168 192.168.1.2
192.168.100.168	SNAT DNAT	Eihare
Detault	Rule ID Na	ame Source Addr Dest Addr
	There are no rows to display.	
		Add
STATUS DEVIC	E AP LOCATION	POLICY RIGHTS SECURITY PORTAL ADMIN MAINTAIN LOGS LOGO
JAT	Device	192.168.100.168 192.168.1.2
192.168.1.0		
S Detault	Rule ID	1 Rule ID val d range:1-10000
	Name	<pre>smat_rule_1</pre> Please emer the values between 1 and 30 character(illegal character)
	source(ip/mask)	192, 188, 3, 0 / 255, 255, 0, (/24)
	dact(in/mack)	
	цезцряназку	
	Service	Any V
	protocol	0 (0-255,0An)
	source port	0 85535
	dest port	0 65535
	Address Translation	by_route V
		192. 168. 1. 2
	Enable	Ø
	Save Cancel	
STATUS DEVICE	AP LOCATION P	OLICY RIGHTS SECURITY PORTAL ADMIN MAINTAIN LOGS LOGO
Firewall Nat		
Firewall Nat	Device	192.168.100.168 192.168.1.2
Firewall Nat	Device	192.168.100.168 192.168.1.2
Firewall Nat AT 192.168.100.168 192.168.1.2 Default	Device SNAT DNAT Rule ID	192.168.100.168 192.168.1.2 Rule ID valid range 1-10000
Firewall Nat	Device SNAT DNAT Rule ID Name	192.168.100.168 192.168.1.2 2 Rule ID valid range 1-10000 mat.rule 2 Please enter the values between 1 and 30 character(illegal character)
Firewall Nat	Device SNAT DNAT Rule ID Name Source(Inimask)	192.168.100.168 192.168.1.2 2 Rule ID valid range smat_rule_2 Please enter the v. lues between 1 and 30 character(illegal character
Firewall Nat	Device SNAT DNAT Rule ID Name source(ipimask)	192.168.100.168 192.168.1.2 2 Rule ID valid range 1-10000 snat_rule_2 Please enter the violues between 1 and 30 character(illegal character) 192.168.4.0 / 255.255.0 192.168.4.0 / 255.255.0
Firewall Nat	Device SNAT DNAT Rule ID Name source(ip/mask) dest(ip/mask)	192.168.100.168 192.168.1.2 2 Rule ID valid range 1-10000 snat_rule_2 Please enter the values between 1 and 30 character(illegal character) 192.168.4.0 / 255.255.255.0 192.168.4.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0
Firewall Nat	Device SNAT DNAT Rule ID Name source(ip/mask) dest(ip/mask) Service	192.168.100.168 192.168.1.2 2 Rule ID valid range 1-10000 snat_rule_2 Please enter the vi lues between 1 and 30 character(illegal character) 192.168.4.0 / 255.255.0 (/24) 0.0.0 / 0.0.0.0 (/0) Inv Inv Inv
Firewall Nat	Device SNAT DNAT Rule ID Name source(ip/mask) dest(ip/mask) Service protocol	192.168.100.168 192.168.1.2 2 Rule ID valid range 1.10000 snat_rule_2 Please enter the values between 1 and 30 character(illegal character) 182.168.4.0 / 255.255.255.0 0.0.0.0 / 0.0.0.0 may 0 (0-255,0Arry)
Firewall Nat	Device SNAT DNAT Rule ID Name source(ipimask) dest(ipimask) Service protocol source port	192.168.100.168 192.168.1.2 2 Rule ID valid range 192.168.1.2 192.168.4.0 /
Firewall Nat	Device SNAT DNAT Rule ID Name source(ip/mask) dest(ip/mask) Service protocol source port dest port	192.168.100.168 192.168.1.2 2 Rule ID valid range 1.10000 snat_rule_2 Please enter the values between 1 and 30 character(illegal character) 192.168.4.0 / 255.255.255.0 0.0.0.0 / 0.0.0.0
Firewall Nat	Device SNAT DNAT Rule ID Name sour ce(ip/mask) dest(ip/mask) Service protocol sour ce port dest port dest port	192.168.100.168 192.168.1.2 192.168.1.2 Rule ID valid range 1000 mat_rule_2 Please enter the v 192.168.4.0 / 255.255.255.0 0 / 0.0.0.0<
Firewall Nat	Device SNAT DNAT Rule ID Name source(ip/mask) dest(ip/mask) Service protocol source port dest port Address Translation	192.168.100.168 192.168.1.2 2 Rule ID valid range nat_rule_2 Please enter the visues between 1 and 30 character(illegal character) 192.168.4.0 / 255.255.255.0 (/24) 192.168.4.0 / 0.0.0.0 (/0) nay 0 0 0.255,0Amy) 0 65535 by_route •



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:

ST	ATUS DEVICE AF	P LOCATION POLICY RIGHTS	SECURITY PORTAL ADMIN MAINTAIN L	LOGS LOGOUT				
(werview Client D	evice AP IIIegal AP						
						_		
Line	NAC	AP BAC Sume	All LigoLACs VHurdware Verson VSoftware	Verson VStatus V Super Admi	n • Search Clear			
192.1	168.1.2							
Up	30mins 59secs	Name	Public IP	ESSID Client Num	LigoLAC Name	Hardware Verson	Status	
Vers	ion 6.2.6(r10724)	•00:19:3b:eb:ba:83	192.168.3.2	0	192.168.1.2	APC 2M-8	R	1
0	Authenticated Clients		192.168.3.2			6.2.2(r256.195.8938)		(7)
0	Line thanticated Clients	O0:19:3b:ff:a1:fb		0			5	0

• 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:

STATUS DEVICE AP LOCATION POLICY RIGHTS	SECURITY PORTAL A	DMIN MAINTAIN LOGS	LOGOUT		
Basic Setup					
AP MAC Nume 25 rows per page V Search	Clear				
•					
	11-110-004	11-11-0.000	12-140-000		De Pa
© @00:19:3b:eb:ba:03	LIGOLAC IP1	LIGOLAU IP2	LIGOLAC IP3	wian	Radio Location
@00:19:3b:00:c3:66					
Calastall Contract Database Contract	auna add 8D fedd 6	Durant de Dural			
Select an Nove to DerAr Batching Com	gale Add AF Add C	Export As Excer			
STATUS DEVICE AP LOCATION F	POLICY RIGHTS	SECURITY PORT	AL ADMIN	MAINTAIN LOGS	S LOGOUT
Basic Setup					
r					
Name	lek				
MAC	00:19:3b:eb:ba:03	1			
Pseudo MAC	00:00:00:00:00:00				
Location	select 🔻				
Wian/LAN Policy Name	T.default wlan_lan_	name T.select wlan_lan	_name		
		kk			
Radio Policy	Default Radio Policy	Select Radio Polic	÷Y		
		kk			
Linel AC IP1					
					_
					~
Scan Illegal AP					
Open scan sta	Low Accura	acy 👝 High Accuracy 🔵	Probe		
Scan Interval	3600	Seconds			
Report equipment status information					
Wian Error Scan Interval	0	minuton (Plance ant	ar a valid pumbar data	not oloow pullo)	
scan interval	U	Infinutes (Flease enti	si a vallu riumber,does	not and OW FIGHTS)	
CLOUD	Super Admin 🔻				
Save Cancel					



3.1.2.9. Save System Configuration

• By option MAINTAIN - Save Configuration, click "Save" to save the current

system configuration, as shown below:

STATUS DEVICE	AP LOCATION POLICY	RIGHTS SECURITY PORTAL ADMIN MAINTAIN LOGS LOGOUT
Software Setup	ave Configuration Shutdown/Restart	Software Update AP Version License Device Analysis
Save		
Configuration	Device	192.168.1.2 192.168.1.2
192.168.100.168	Options	
Sefault	Save System Configuration	Save
	Export System Profile	Export Configs Export Database
	Import System Profile	Upload file Browse
		Import Configs Import Database
	Reset to manufacture setting	Reset

• 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,

网络连接详细信息の):			- kk 2	
属性	值	^	Internet 访问	
连接特定的 DNS 后缀 描述 物理地址	D-Link DWA-160 Xtreme N Dua 00-24-01-0C-EF-7D	l E	拨号和 VPN	
已启用 DHCP	是		宽带连接	-
IPv4 地址 IPv4 子网掩码	192. 168. 4. 2 255. 255. 255. 0		无线网络连接	
获得租约的时间 租约过期的时间	2014年7月2日 14:00:09 2014年7月2日 16:11:37	=	kk	已连接,
IPv4 默认网关	192. 168. 4. 1			11111
IPv4 DHCP 服务器	192. 168. 4. 1		Guest	
IPv4 DNS 服务器	192.168.1.1			-
IPv4 WINS 服务器			Function	Mee
已启用 NetBIOS ove 连接-本地 IP v 6 地址	· 是 fe80::cc11:7450:4ba7:7e39%13	3 💷 🚺	CMCC-AUTO	liter
IPv6 默认网关			CMCC	
IPv6 DNS 服务器	1	E	cinee	1000
•			Chico FREE	(f)_alt

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 <u>www.baidu.com</u>, you can see the URL redirected to the portal page URL, as shown below

	LigoWave Common Froblem Feedback Froblem
LigoWave	Please Logon on Username Password Language Inglish Please log on
 Nore WLAN wonderful, please visit LigoWave website for details. http://www.ligowave.com 	

• 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"

Basic Setup DNS S	AP LOCATION	POLICY RIGHTS SECURITY PORTAL Route Policy Route OSPF DHCP	ADMIN MAINTAIN LO SNMP STA Server D	DGS LOGOUT	
Interface Setup	Device	192.168.100.168 192.168.1.2			
192.168.100.168					
192.168.1.2	Interface VLAN	Bridge VSLAN VPN			
Ceradit.	Name 🤸	Mode	MTU	TRUNK	ТҮРЕ
	Slot/Port U/1	Route Mode	1500	*	Uplink
	Slot/Port 0/2	Route Mode	1500	×	Uplink
	Slot/Port 0/3	Route Mode	1500	×	Downlink
	Slot/Port 0/4	Route Mode	1500	×	Downlink
	Slot/Port 0/5	Route Mode	1500	×	Downlink
	Slot/Port 0/6	Route Mode	1500	×	Downlink
PORTS	Device		A 400 400 400 400		
•			192.168.100.168		
192.168.1.2	Name	Slot/Port 0/2	192.168.100.168		
192:168.1.2 Default	Name MAC	Slot/Port 0/2	92.168.100.168		
192.168.1.2 Default	Name MAC Pseudo MAC	SlotPort 0/2 00: e0: 4c: 14: 18: e0	192.168.100.168		
192.168.1.2 Default	Name MAC Pseudo MAC	Stot/Port 0/2 00: e0:4e:14:18: e0 00: 00:00:00:00:00	(You can set '00:00:00:00:00:00' to	delete pseudo mac)	
192.168.1.2	Name MAC Pseudo MAC MTU	Stot/Port 0/2 00: e0: 4e: 14: 18: e0 00: 00: 00: 00: 00: 00	(You can set '00.00.00.00.00.00 to (Please enter the 68-1500 values)	delete pseudo mac)	1
6 192.168.1.2 6 Default	Name MAC Pseudo MAC MTU Port Connection Type	Si00Port 0/2 00:=01:4c:14:18:=0 00:00:00:00:00:00 1500 Autosplact	(You can set 00.00.00.00.00.00 to (Please enter the 68-1500 values)	delete pseudo mac)]
4 192.168.1.2 4 Default	Name MAC Pseudo MAC MTU Port Connection Type TYPE	Si0UPort 0/2 00:e0:4c:14:18:e0 00:00:00:00:00:00 1500 Autoselect	(You can set '00.00.00.00.00.00' to (Please enter the 68-1500 values)	delete pseudo mac)]
4 192.168.1.2 Default	Name MAC Pseudo MAC MTU Port Connection Type TYPE	SlotPort 0/2 00:#0:4c:14:18:#0 00:00:00:00:00:00 1500 Autosalect Uplink VAN ID	(You can set '00.00 00.00.00 00' to (Please enter the 68-1500 values)	delete pseudo mac)	
4 192168.1.2 Default	Name MAC Pseudo MAC MTU Port Connection Type TYPE TRUNK 📄	SlotPort 0/2 00:40:44:14:18:40 00:00:00:00:00:00 1500 Autosalaet Uplink V @ Bloh VLAN ID Allow VLAN ID	(You can set '00:00:00:00:00:00' to (Please enter the 68-1500 values)	delete pseudo mac)	0-4095,English comma separated)
421581.2 Cefault	Name MAC Pseudo MAC MTU Port Connection Type TYPE TRUNK Mode	Sid9Port 0/2 00:e0:4c:14:18:e0 00:00:00:00:00:00 1500 Autosal.ect Uplink • e Both VLAN ID Allow VLAN ID Roate Mode •	(You can set '00:00:00:00:00:00' to (Please enter the 68-1500 values)	delele pseudo mac)	0-4095,English comma separated)
4 1921881.2 Default	Name MAC Pseudo MAC MTU Port Connection Type TYPE TRUNK Mode VSLAN	SidyPort 0/2 00:e0.4c:14:18:e0 00:00:00:00:00:00 1500 Autoselect Uplink V @ Both VLAN ID @ Aldw VLAN ID Route Mode V	(You can set '00:00:00:00:00:00' to (Please enter the 68-1500 values)	delete pseudo mac)	0-4095,English comma separated)
4 192.188.1.2 5 Default	Name MAC Pseudo MAC MTU Port Connection Type TYPE TRUNK Mode VSLAN BY IP	SloUPort 0/2 00:00:00:00:00:00:00 1500 Autoselect Uplink • Both VLAN ID Allow VLAN ID Loute Mode • 1	(1-999)	delete pseudo mac)	0-4095,English comma separated)
4 192.188.1.2 5 Default	Name MAC Pseudo MAC MTU Port Connection Type TypE TRUNK Mode VSLAN SVIP STATUS	SlotPort 0/2 00:00:00:00:00:00:00 1500 Autoselect Uplink • ® Both VLAN ID Autow VLAN ID Toute Mode • 1 	(You can set '00:00:00:00:00:00' to (Please enter the 68-1500 values)	delete pseudo mac)	0-4095,English comma separated)

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

	CE AP LOCATION	POLICY RIGHTS SECURI	TY PORTAL ADMIN MAINTAIN	LOGS LOGOUT
Basic Setup	DNS Server Ports F	Route Policy Route 0	SPF DHCP SNMP STA Server	Date & Time
IP Setup	Device	•	92.168.100.168 192.168.1.2	
192.168.100.168 4.192.168.1.2	Interface	Interface IP Type	IP Address/Subnet Mask	Management Channel
Default	Slot/Port 0/1	STATIC	192.168.1.2/255.255.255.0	✓
	Slot/Port 0/2	STATIC	192.168.3.1/255.255.255.0	×
				Add
STATUS	EVICE AP LO	CATION POLICY RIGH	ITS SECURITY PORTAL A	ADMIN MAINTAIN LOGS LOGOUT
Basic Setup	DNS Server Por	ts IP Route Po	licy Route OSPF DHCP S	NMP STA Server Date & Time
TD				
IP	Device		192.168.100.168 192.168.1.2	
192.168.100.168	8			
Default	Interface		Slot/Port 0/2 V	
*	Interface ID	Time		
	Interface IP	туре	STATIC V	
	IP Address/	Subnet Mask	192. 168. 3. 1 / 255	. 255. 255. 0 (/24) 🔻
		d Channel 🗔 A		
	Managemer			
	Managemer	nt Rights 🕜		
	_	×	`	
	Save	Cancel		



• **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"

STATUS DEVICE	AP LOCATION POLICY RIGHTS SECU	JRITY PORTAL ADMIN MAINTAIN LOGS LOGOUT
Basic Setup DNS S	Server Ports IP Route Policy Route	OSPF DHCP SNMP STA Server Date & Time
IP	Device	192.168.100.168 192.168.1.2
4 192.168.1.2 Default	Interface	Slot/Port 0/1 🔻
	Interface IP Type	STATIC V
	IP Address/Subnet Mask	192.168.1.2 / 255.255.0 (/24) V
	Management Channel 🛛 🕢 🕭	
	Management Rights 🛛 🕑	
	Save Cancel	

• 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

STATUS DEVICE	AP LOCATION POLICY RIGHTS SECURITY	PORTAL ADMIN MAINTAIN LOGS LOGOUT
Basic Setup DNS Se	erver Ports IP Route Policy Route OSPF	F DHCP SNMP STA Server Date & Time
Route Setup	Device	, 192.168.100.168 192.168.1.2
▲ 192.168.100.168	Destination/Subnet mask	Gateway
Default	There are no rows to display.	
		Add
STATUS DEVICE	AP LOCATION POLICY RIGHTS	SECURITY PORTAL ADMIN MAINTAIN LOGS LOGOUT
Basic Setup DNS	Server Ports IP Route Policy Route	OSPF DHCP SNMP STA Server Date & Time
Route Setup	Device	192.168.100.168 192.168.1.2
192.168.1.2 Cefault	Destination/Subnet mask	0.0.0.0
	Gateway	192. 168. 1. 1
	Routing Metric	1 (Please enter the values between 0 and 65535)
	Save	



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

STATUS DEVICE	AP LOCATION POLICY	RIGHTS SECURITY PORTAL	ADMIN MAINTAIN LOGS LOGOUT
Basic Setup DNS	Server Ports IP Route	Policy Route OSPF DHCP	SNMP STA Server Date & Time
DNS Server	Device DNS Server	192.168.100.168 192.168.1.2	
& Default	Primary DNS Secondary DNS	192. 168. 1. 1 8. 8. 8	
	Save		

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"

STATUS DEVICE	AP LOCATION POLICY	RIGHTS SECURITY PORT	L ADMIN MAINTAIN	LOGS LOGOUT
Basic Setup DNS Se	erver i Ports i IP i Route i	Policy Route OSPF DHC	P SNMP STA Server	Date & Time
Interface Setup	Device	VSLAN VPN	0.168 <	
💊 Default	Name	Member		STP Status
	VSLAN 1			*
				Add
STATUS DEVICE	AP LOCATION PO	DLICY RIGHTS SECURI	TY PORTAL ADMIN	MAINTAIN LOGS LOGOUT
Basic Setup DN	NS Server Ports IP	Route Policy Route C	SPF DHCP SNMP	STA Server Date & Time
DHCP Setup	Device	,	192.168.100.168	
192.168.1.2 Default	ID	[8 (1-999)	
-	Name	[VSLAN 8	
	STP Status			
	Status		Ø	×
	Save Cancel			



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":

STATUS DEVICE	AP LOCATION POLICY F	GHTS SECURITY	PORTAL AD	MIN MAINTAIN	LOGS LOGOUT	
Virtualization Radio	Access Control AP Update	-				
VSLAN Portal MLANLAN Authentication	WLANALAN Security					
1	here are no rows to display.					
						Add
STATUS DEVICE	dio Access Control AP	LICY RIGHTS	SECURITY	PORTAL ADM	IIN MAINTAIN	LOGS LOGOUT
VSLAN Portal WLANLAN Authentication	WLANAAN Security Name	kk		Please enter the value	ues between 1 and 30 c	haracter(illegal character:!\$%/
	Encryption Encryption Key	wpa-psk/wpa2-psk tkip+aes ▼ 888888888	▼	allow length 8~31		
	Save Cancel					

• 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":

STATUS DEVICE		ITS SECURITY	PORTAL ADMIN MA	AINTAIN LOG	is LOGOUT	
Virtualization Radio	Access Control 🛛 AP Update 📉					
VSLAN Portal VLANLAN Authentication	WLANLAN Security	arwarding Mode V	Cearch Clear			
			Glean	5000		
L.	ame			ESSID	Security	Detaurt
T	here are no rows to display.					
						Add
STATUS DEVICE	AP LOCATION POLIC	RIGHTS	SECURITY PORTAL	ADMIN	MAINTAIN LO	GS LOGOUT
Minture line time in the Part	dia la Assass Control al ADUnd					
VSLAN Portal WLANLAN Authentication	WLANILAN Security Policy Type Name		WLAN V		P ease enter the value	es between 1 and 30
	ESSID Security Policy User Limit Hidden Radio Freq		kak kak ▼ 0 ● Show Essid ● 2.4G	(Each AP to Hide Essid 5G	Please enter the value	s between 1 and 31 nber of users acces
	Forwarding Mode		Local Forward:Brid	ge 🔻	(0-4096, 0 means not	set)
	Default		💿 no i yes			
	Save Cancel					



• By option PORTAL - Portal Customize - Portal List, add a new built-in portal,

named "kk", and save:

STATUS DEVICE	AP LOCATION POLIC	CY RIGHTS SECURITY PORTAL ADMIN MAINTAIN LOGS LOGOUT
Portal Customize	Upload Portal	
Time Portal List Custom	Portal Name default	Portal URL Portal URL P http://192.168.1.2/admin_0/portalweb/index.php
		Add
Portal Customize	Upload Portal	POLICY RIGHTS SECURITY PORTAL ADMIN MAINTAIN LOGS LOGOUT
 Slot Description Time 	Portal Name	bk Please enter the values between 1 and 30 character/lilegal character."\$%^*0~+
 Portal List Custom 	APIAddress	
	Token Verification code Dynamic Password	 Open
	Save Cancel	

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"

STATUS DEVICE	AP LOCATION	POLICY RIGHTS SECU		MAINTAIN LOGS LOGOUT	
Portal Customize	Upload Portal				
Slot Description					
🕞 Time	Portal Name	Portal URL			Verification code
Portal List	kk	🔎 http://192.168.1.2/admi	n_0/c96	C1-14C	×
🕞 Custom	default	http://192.168.1.2/admi	n_0/port 转到 h++n://192 168 1 2/	0/a96a37/index_aba(6)	¥
			打印(图)	auto a covert) maex. pap (g)	
			审查元素 (8)		Add

• 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:



Add

LigoWa	ve	
STATUS DEVIC	CE AP LOCATION	POLICY RIGHTS SECURITY PORTAL ADMIN MAINTAIN LOGS LOGOUT
VSLAN	Name	Decement the values between 1 and 20 therefortillered character 186.470
WLAN/LAN Authentication	PORTAL	reade enter une ratues between ratue d'unatatien (integra character, integra charact
	Params List	Please Select One parameter V Alias
	Save Cance	31

• 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:

STATUS DEVICE	AP LOCATION POLICY RIGHTS	SECURITY PORTAL ADMIN MAIN	NTAIN LOGS LOGOUT	
Virtualization Radio	o Access Control AP Update			
SVSLAN Portal WLAN/LAN	Network ID Name Wlan/LAN Po	licy Nar Authentication Portal	Search Clear	
Authentication	Network ID Name Wlan/	AN Policy Name	Authentication	Portal
	There are no rows to display.			
STATUS DEVIC	E AP LOCATION POLICY	RIGHTS SECURITY PORTAL	ADMIN MAINTAIN	Add
VSLAN Portal WLANLAN Authentication	Name Network ID Wlan LAN Policy Name	kk 8 T.default wlan_lan_name T.select wlan_kk	Please enter the values between	ween 1 and 30 character(IIIe
	User Authentication			
	Authentication Service Mode	centralized V		
	Authentication	System Authentication Policy V		
	Forwarding Mode			
	User Isolation			
	URL Logging	Low Accuracy V		
	Description Save Cancel			



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

STATUS DEVICE	AP LOCATION POLICY RIGHTS	S SECURITY PORTAL ADMIN MAINTAIN	LOGS LOGOUT
Virtualization Radio	Access Control AP Update		
Radio	RF Channel	Tx Power	Antenna
There are no rows to display.			
			Add
STATUS DEVICE	AP LOCATION POLICY	RIGHTS SECURITY PORTAL ADMIN	MAINTAIN LOGS LOGOUT
Virtualization Radio	Access Control AP Update		
Name	kk	Please enter the values between 1 and 30 character(Illegal c	:haracter:"\$%^*()~+<>= \\;;;?#@&`\"[]{}.)
Mode	802.11bg†n 🔻		
Htmode	HT20 V		
RF Channel	1 •		
IX POWER	Udbm(lmw) V		
Ancilla DSSI/dDm)	-100 Please enter the y	alues het veen 30 and -50	
Save Cancel			

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

STATUS DEVICE	AP LOCATION	POLICY	RIGHTS SECURITY	PORTAL	ADMIN MAINTAIN LOGS LOGOUT
Role Admission	Rights				
Identity Profiles Susers	Username 		kk		Please enter the values between 1 and 32(Illegal charac
APP LINK	MAC Bind				
	IP Bind				
	ESSID Bind				Please enter the values between 1 and 31 character
	VSLAN		0		(0Any)
	Role		default Role	select Ro	le
			group		
	Password				Password field length must be between 6 and 32 chara
	Confirm Password				Password field length must be between 6 and 32 chara
	Full Name Descriptive Name				
	Advanced option>>				
	Save Cancel				



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:

STAT	TUS DEVICE AP	LOCATION POLICY RIGHTS	SECURITY PORTAL ADMIN MAINTAIN LOG	S LOGOUT				
Ove	arview 🔨 Client 👘 Der	vice AP I Illegal AP I						
LigoW#	ıc	AP BAC Sune		son VState	us ▼ Super ådni:	Search Clea	a l	
192.16	8.1.2	🔂 TOP >>						
Up Time	2hrs 49mins	Name	Public IP Private IP	ESSID	Client Num	LigoLAC Name	Hardware Verson Software Verson	Status
Version 0	6.2.6(r10724) Authenticated Clients	Ak 00:19:3breb:ba:03	192.168.1.24 192.168.1.24	kk	D	192.168.1.2	APC 2M-8 6.2.2(r256.196.8938)	
0	Unauthenticated Clients	©00:19:3b:ff:a1:fb			0			
0	Total Clients							-

• 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:

STATUS DEVICE AP LOCATION POLICY RIGHTS S	ECURITY PORTAL ADMIN MAINTAIN LOGS LOGOUT
Basic Setup	
AP MAC Name 25 rows per page V Search	Clear
AD MAC Name	LigoLAC IP1 LigoLAC IP2 LigoLAC IP3 Wian Radio Location
□ @ 00:19:3b:00:c3:66	
Select all [flove To V] Del AP Batchly Configur	e Add AP Add Group Export As Excel
STATUS DEVICE AP LOCATION PO	LICY RIGHTS SECURITY PORTAL ADMIN MAINTAIN LOGS LOGOUT
Basic Setup	
Г	
Name MAC	00:19:3b:eb:ba:03
Pseudo MAC	00:00:00:00:00
Location	select V
Wian/LAN Policy Name	T.defaultwian ian name
	kk
Radio Policy	Default Radio Policy Select Radio Policy
	KK
LigoLAC IP1	
LigoLAC IP2	
Scan Illegal AP	
Scan Interval	3600 Seconds
Report equipment status information	
Wian Error Scan Interval	
Scan Interval	0 minutes (Please enter a valid number,does not aloow nulls)
CLOUD	Super Admin V
Save Cancel	



3.2.2.7. Save System Configuration

• By option MAINTAIN - Save Configuration, click"Save"to save the current

system configuration, as shown below:

STATUS DEVICE	AP LOCATION POLICY RIGHTS	SECURITY PORTAL ADMIN MAINTAIN LOGS LOGOUT
Software Setup	we Configuration Shutdown/Restart Software	Update AP Version License Device Analysis
Save		
Configuration	Device	192.168.1.2 192.168.1.2
192.168.100.168	Options	
& 192.168.1.2 & Default	Save System Configuration	Save
	Export System Profile	Export Configs Export Database
	Import System Profile	Upload file Browse
		Import Configs Import Database
	Design the second statement of the second seco	
	Reset to manufacture setting	Reset

• 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

网络连接详细信息 (D):			当前连接到:	*1
属性	值	*		
连接特定的 DNS 后缀 描述 物理地址 已启用 DHCP	D-Link DWA-160 Xtreme N D 00-24-01-0C-EF-7D 是	ual F	kk 4 Internet 访问	ŝ
IPv4 地址	192. 168. 1. 14		拨号和 VPN	~
IPv4 子网掩码 获得租约的时间 租约讨期的时间	255.255.255.0 2014年7月3日 10:54:39 2014年7月4日 10:54:39	11	宽带连接	2
IPv4 默认网关	192.168.1.1		无线网络连接	~
IPv4 DHCP 服务器	192. 168. 1. 1			اف مدیند
IPv4 DNS 服务器	192.168.1.1		кк	匕连接
IPv4 WINS 服务器	112.10.230.1		kk2M-ap	lie.
已启用 NetBIOS ove 连接-本地 IPv6 地址	是 fe80::cc11:7450:4ba7:7e39	×13	Guest	Sul
		F	Function	Ite.
			tTII网络In:	中宣由ふ

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 <u>www.baidu.com</u>, you can see the URL

be redirected to the portal page URL, as shown below

	Ligo¥ave Common Problem Feedback Pr
	Please Logon on
	Username Password Language English • Please log on
• More WLAN wonderful, please visit LigoWave website for details	A

• 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:

gle Chrome 浏览器保存您的密码吗?	保存密码	此网站一律不保存密码			
				LigoWave Comm	on Problem Feedback Probl
$\frac{1112}{9} + \frac{1}{3} = 0$			Username: User IP:	User Info kk 192.168.1.14 (00:24:01:0c:ef:7d)	
8765	ogout	 一〇一〇一〇一〇一〇一〇一〇一〇一〇一〇一〇一〇一〇一〇一〇一	baidu.com/index.php?	Ptn=36060048_pg&ch=2	
More WLAN wonderful, please wis details. http://www.ligowave.c	iit LigoWava wabs :om	ito for	B	ai 👛 百度	
		c. 新加油	网页 <u>贴吧 知道</u>	<u>首 音乐 图片 视频</u> 地	图 百度一下

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 <u>1.2.2.4.IP Setup</u>), 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

STATUS DEVICE	AP LOCATION	POLICY RIGHTS SECURITY PORTAL ADMIN CLO	UD MAINTAIN LOGS LOGOUT	
Basic Setup DN	S Server Ports IP	Route Policy Route OSPF DHCP SNMP Date	& Time	
IP Setup	Device	163.177.112.181 163.177.112.181		
163.177.112.181 Default	Interface Slot/Port 0/2	IP Address/Subnet Mask 1.1.1.1/255.255.255.0	Management Channel 🗙	Management Rights ×
	Slot/Port 1/1	163.177.112.181/255.255.255.192	✓	×
	VSLAN 11	172.16.1.1/255.255.255.0	×	× ×
	VSLAN 88	192.188.0.1/255.255.255.0	*	×
	VSLAN 20	192.168.1.1/255.255.255.0	×	×
	VSLAN 40	192.168.4.1/255.255.255.0	×	×
	VSLAN 120	192.168.120.1/255.255.255.0	×	¥
			httk	

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

STATUS DEVICE	AP LOCATION	POLICY F	AIGHTS SECURITY	PORTAL ADM	MIN CLOUD	MAINTAIN LOGS	LOGOUT
Basic Setup	s Server	IP Route	Policy Route OSPF	DHCP SNM	MP Date & Time		
DNS Server	Device DNS Server		1 1	63.177.112.181 63.177.112.181			
	Primary DNS Secondary DNS		221. 5. 210. 21	88.88			
	Save					_	

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

STATUS DEVICE	AP LOCATION	POLICY RIGHTS	SECURITY PORTAL ADMIN CLOUD MAINTAIN LOGS LOGOUT		
Basic Setup DNS Server Ports IP Route Policy Route OSPF DHCP SNMP Date & Time					
Route Setup	Device		163.177.112.181 183.177.112.181		
	Destination/Subnet mask Gateway		0.0.0.0 / 0.0.0 (/0) V		
			163.177.112.129		
	Routing Metric		0 (Please enter the values between 0 and 65535)		
	Save Cancel				

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

STATUS DEVICE	AP LOCATION POLICY RIGHTS SE	CURITY PORTAL ADMIN CLOUD MAINTAIN LOGS LOGOUT			
Software Setup Save Configuration Shutdown/Restart Software Update AP Version License Device Analysis					
Save					
Configuration	Device	163.177.112.181 183.177.112.181			
163.177.112.181	Options				
Containt Containt	Save System Configuration	Save			
	Export System Profile	Export Configs Export Database			
	Import System Profile	Upload file Browse			
		Import Configs Import Database			
	Reset to manufacture setting				
	reserve manufacture setting	Reset			

- 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 <u>3.2.2.Configuration Steps</u>

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.





73 / 79

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

STATUS DEVICE	AP LOCATION POLICY RIGHTS	SECURITY PORTAL ADMIN CLOUD MAINTAIN LOGS LOGOUT
Basic Setup DNS Se	erver Ports IP Route Policy Rout	e OSPF DHCP SNMP STA Server Date & Time
IP	Device	14.23.153.96 14.23.153.96
	Interface	Slot/Port 0/1 V
	Interface IP Type	STATIC V
	IP Address/Subnet Mask	14.23.153.96 / 255.255.192 (/26) 🔹
ſ	Management Channel 🛛 🕢 🕭	
	Management Rights 🛛 🖉	
	Save Cancel	

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

LigoWave			
STATUS DEVICE	AP LOCATION PO	DLICY RIGHTS SECURITY POR	TAL ADMIN CLOUD MAINTAIN LOGS LOGOUT
Basic Setup	Server Ports IP	Route Policy Route OSPF DH	ICP SNMP STA Server Date & Time
DNS Server	Device DNS Server	4.23.153 14.23.153	3.96 3.96
▲14.23.153.97	Primary DNS Secondary DNS	202.96.128.86	

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

STATUS DEVICE	AP LOCATION POLICY RIGHTS	SECURITY PORTAL ADMIN CLOUD MAINTAIN LOGS LOGOUT
Basic Setup DNS S	erver Ports I IP Route Policy Rout	e OSPF DHCP SNMP STA Server Date & Time
Route Setup	Device	14.23.153.96 14.23.153.96
14.23.153.96		
Default	Destination/Subnet mask	0.0.0.0
	Gateway	14. 23. 153. 65
	Routing Metric	0 (Please enter the values between 0 and 65535)
	Save Cancel	

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

STATUS DEVICE	AP LOCA	TION POLICY	RIGHTS SECURIT	Y PORTAL	ADMIN	CLOUD	MAINTAIN	LOGS	LOGOUT
Software Setup	Save Configuration	Shutdown/Restart	Software Update	AP Version	License	Device Analysis			
Save Configuration	Device			14.23.153.96 14.23.153.96					
▲ 14.23.153.96 ■ ▲ Default ▲ 14.23.153.97	Options Save System C	onfiguration		Save					

- 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<u>https://14.23.153.96</u> 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 <u>1.1.2.Initial Configuration of LAC</u>, you will see the LAC get on-line to the VAC by option STATUS-Device, as shown below

	vave							
STATUS	DEVICE AP	LOCATION POLICY	RIGHTS SECURITY	PORTAL ADMIN CLOUD	MAINTAIN LOG	S LOGOUI		
Coreption	Client Devi	A Internetiti A						
01011101	W Client Devi	niegar Ai						
		Device						
LigoVAC		Device	Dublic ID	Surtom ID	AD Murs	Client Num	Hardware Version	Software Ve
LigoVAC 14.23.153.9	96	Device Name	Public IP Private IP	System ID	AP Num	Client Num	Hardware Version	Software Ve
LigoVAC 14.23.153.90 Up 4n Time 4n	16 mos 1wk	Device Name • 14.23.153.96	Public IP Private IP 14.23.153.96	System ID 00:e0:4c:14:1d:d2	AP Num O	Client Num 0	Hardware Version	Software Ve 6.2.4(r10051
LigoVAC 14.23.153.90 Up 4n Time 4n Version 6.3	96 mos 1wk 2.4(r10051)	Device Name • 14.23.153.96 14.23.153.97	Public IP Private IP 14.23.153.96 14.23.153.97	System ID 00:e0:4e:14:14:14:12 00:10:73:3e:94:72	AP Num 0 136	Client Num O 4094	Hardware Version LigoVAC3100 LigoLAC5100	Software V 6.2.4(r1005 8.2.4(r1005
LigoVAC 14.23.153.90 Up Time 4n Version 6.1 1146 Au	16 mos 1wk .2.4(r10051) uthenticated Clients	Device Name \$14.23.153.96 14.23.153.97	Public IP Private IP 14.23.153.96 14.23.153.97 14.23.153.97	System ID 00:e0:4e:14:1d:d2 00:10:73:3e:94:72	AP Num 0 136	Client Num 0 4094	Hardware Version LigoVAC3100 LigoLAC5100	Software V 6.2.4(r1005 6.2.4(r1005
LigoVAC 14.23.153.90 Up time 4n Version 6.1 1146 Au 2949 Ur	16 mos 1wk .2.4(r10051) uthenticated Clients inauthenticated Clients	Device Name @14.23.153.96 14.23.153.97	Public IP Private IP 14.23.153.96 14.23.153.97 14.23.153.97	System ID 00:e0:4c:14:1d:d2 00:10:f3:3c:94:72	AP Num 0 136	Client Num 0 4094	Hardware Version LigoVAC3100 LigoLAC5100	Software V 6.2.4(r1005 6.2.4(r1005

- 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

STATUS DEVICE	AP LOCATION	POLICY RIG	HTS SECURITY PORTAL ADMI	IN CLOUD MAINTAIN I	LOGS LOGOUT
Basic Setup DNS S	Server Ports	IP Route Po	olicy Route OSPF DHCP SNMF	STA Server Date & Time	
Basic Setup	Device 14.23.1 14.23.1	53.96 53.96			
Default	Name		14. 23. 153. 96	Legal character of letters,number	s,(-) supports a length of 0-63
•14.23.153.97	IP Address		14.23.153.96		
	System ID		00:e0:4c:14:1d:d2		
	Admin Username		admin		
	Admin Password				
	Confirm Admin Pass	word			
			🕑 Enable CLI		
STATUS DEVICE	AP LOCATION	POLICY RIGHTS	SECURITY PORTAL ADMIN	CLOUD MAINTAIN LOGS	LOGOUT
Firewall Nat					
Firewall	Device		14.23.153.96 14.23.153.96		
Firewall	Device		14.23.153.96 14.23.153.96	Filters	
Firewall	Device Rule ID	Name	14.23.153.96 14.23.153.96 Source Addr	Filters Dest Addr	Service
Firewall	Device Rule ID 2000	Name fw_rule_2000	14.23.153.96 14.23.153.96 Source Addr 0.0.0.00.0.0	Filters Dest Addr 0.0.0.0/0.0.0	Service any(
Firewall	Device Rule ID 2000	Name fw_rule_2000	14.23.153.96 14.23.153.96 Source Addr 0.0.0.0/0.0.0.0	Filters Dest Addr 0.0.0.000.0.0	Service any(i Add
Firewall	Device Rule ID 2000	Name fw_rule_2000	14.23.153.96 14.23.153.96 Source Addr 0.0.0.070.0.0.0	Filters Dest Addr 0.0.0.000	Service any(Add
14 23 153 96 14 23 153 96 14 23 153 97 14 23 153 97	Device Rule ID 2000 AP LOCATION	Name fw_rule_2000	Source Addr 0.0.0/0.000 80HTS SECURITY PORTAL	Filters Dest Addr 0.0.0.000.0.0 ADMIN CLOUD MAINTAIN	Service any(Add LOGS LOGOUT
Status DEvice	Device Rule ID 2000 AP LOCATION ave Configuration	Name fw_rule_2000	14.23.153.96 14.23.153.96 Source Addr 0.0.0.0/0.0.0 Rights SECURITY PORTAL Software Update AP Version	Filters Dest Addr 0.0.000.0.00 ADMIN CLOUD MAINTAIN ense Device Analysis	Service any(Add LOGS LOGOUT
Firewall 1423153.96 1423.153.97 1423.153.97 1423.153.97 Status Device Software Setup Sa Software Setup	Device Rule ID 2000 AP LOCATION ave Configuration Device	Name fw_rule_2000	14.23.153.96 14.23.153.96 Source Addr 0.0.0.000.0.0 NGHTS SECURITY PORTAL Software Update AP Version Lice 14.23.153.96 14.23.153.96	Filters Dest Addr 0.0.0.000.0.0 ADMIN CLOUD MAINTAIN ense Device Analysis	Service any(Add LOGS LOGOUT
Firewall 1423153.96 1423.153.97 1423.153.97 1423.153.97 Software Setup Software Setup 1423.153.96 Setup 1423.153.96 Setup 1423.153.96	Device Rule ID 2000 AP LOCATION ave Configuration Device Software	Name fw_rule_2000	14.23.153.96 14.23.153.96 Source Addr 0.00.000.00 0 Rights SecURITY PORTAL Software Update AP Version Lice 14.23.153.96 14.23.153.96	Filters Dest Addr 0.0.0.000.0.0 ADMIN CLOUD MAINTAIN ense Device Analysis	Service any(Add LOGS LOGOUT
Firewall 14.23.153.96 14.23.153.97 14.23.153.97 14.23.153.97 Software Setup 14.23.153.96 Software Setup 14.23.153.96 Default 14.23.153.97	Rule ID 2000 AP LOCATION ave Configuration Device Software Current Version	Name fw_rule_2000	Source Addr 0.0.0,000.00 NGHTS SECURITY PORTAL J Software Update AP Version Lice 14.23.153.96 14.23.153.96 6.2.4(r10051) 6.2.4(r10051)	Filters Dest Addr 0.0.0.000.0.0 ADMIN CLOUD MAINTAIN ense Device Analysis	Service any(Add LOGS LOGOUT



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

STATUS DEVICE AP LOCATION P	OLICY RIGHTS SECURITY PORTAL ADMIN CLOUD MAINTAIN LOGS LOGOUT
Basic Setup	
Name	kk
MAC	14:ef:92:78:08:08
Location	select V
Wian/LAN Policy Name	T.default wlan_lan_name T.select wlan_lan_name
	Ouest-Five Function OuestO1 KdK guqun KdK henry Ian
Radio Policy	Default Radio Policy Select Radio Policy henry kk
	test
Linel &C IP1	14. 23. 153. 97
LigoLAC IP2	14. 23. 153. 98
LigoLAC IP3	14.23.153.99
Scan Illegal AP	
Scan Interval	3600 Seconds
Wian Error Scan Interval	
Scan Interval	0 minutes (Please enter a valid number,does not aloow nulls)
CLOUD	Super Admin 🔻
Save Cancel	

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

STATUS DEVICE	AP LOCATION POLICY	RIGHTS SECURITY PORTAL ADMIN CLOUD MAINTAIN LOGS LOGOUT
Virtualization Radio	Access Control AP Update	
▶ VSLAN▶ Portal		
WLAN/LAN	Name	kk Please enter the values between 1 and 30 character(illegal character
	Network ID	3
	Wian/LAN Policy Name	T.default wlan_lan_name T.select wlan_lan_name
		chenjun_wechat customer test customer test Function-Wechat
	User Authentication	
	Authentication Service Mode	distributed T
	Authentication	distributed cation Policy V
	Portal	kk 🔻
	User IP Unique	
	Forwarding Mode	
	User Isolation	
	URL Logging	Low Accuracy T
	Description	
	Save Cancel	

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 <u>1.1.3.Initial Configuration of AP</u>

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 <u>3.3.2.Configuration Steps</u>





Copyright © 2015 Function LLC. All rights reserved. Deliberant/LigoWave, the Deliberant/LigoWave logo, are the trademarks of Function LLC. All other company and product names may be trademarks of their respective companies. While every effort is made to ensure the information given is accurate, Function does not accept liability for any errors or mistakes which may arise. Specifications and other information in this document may be subject to change without notice.

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