



联 世 界 创 未 来

BHU NETWORKS® BXM2/5

User Manual

Version No.V2.1

Beijing Huasun Unicreate Technology Co., Ltd.

The customers could contact the local BHU branch office or headquarter directly to get comprehensive technical support from Beijing Huasun Unicreate Technology Co., Ltd. Please download the electronic product user manual from official website.

Beijing Huasun Unicreate Technology Co., Ltd.

Headquarter Address: Huizhi Office Building, No.9-6 Xueqing Road, Haidian District

Official Website: www.bhunetworks.com/overseas

Customer Service hotline: 86-10-82730100

Customer Service Mailbox: bhu@bhunetworks.com

Copyright Declaration

Beijing Huasun Unicreate Technology Co., Ltd. All rights reserved. Beijing Huasun Unicreate Technology Co., Ltd. reserves the final interpretation and revision right of this user manual without any prior notice.

This version right of user manual belongs to Beijing Huasun Unicreate Technology Co., Ltd. Any form of behavior, including reproduction, excerpti on, copy, revision, distribution, translation of any part of the contents in this document without the prior written permission of Beijing Huasun Unicreate Technology Co., Ltd. is prohibited.

Disclaimer

This user manual is based on data available and herein update contents can be made without notice. Beijing Huasun Unicreate Technology Co., Ltd., has tried its best to ensure the accuracy and reliability of this user manual, but do not claim for the loss or damage caused by any omission, inaccuracy or error in this user manual.

Introduction of user manual

Audience

Objectives: This manual provides guidelines for people who purchase, use, manage and maintain BHU NETWORKS®BXM2/5 serial product and those enterprises and relevant personnel who involved in constructing network system, such as engineers, technicians, product and R&D personnel, as well as other users of this product.

This manual as a quick configurations and training guide, is suitable for BHU NETWORKS®BXM2/5 series product initial user, common and proficient operator.

Summary

This manual gives a brief and focused explanation to BHU NETWORKS®BXM2/5 series product in the following aspects: the user interface, quickly constructing network configuration software, configuration method of login, the function of important parameters and its effect, as well as some other points for attentions.

You can use this manual to complete rapid configuration, meet quick and typical networking needs and complete the main applications.

Technical Service Support

Beijing Huasun Unicreate Technology Co., Ltd. (Hereinafter referred as BHU Networks) set up the service system based on the headquarter technology center, The customers could contact BHU Networks service hot line whenever has trouble in using the product and running the network. Please access www.bhunetworks.com/overseas for service support hot line numbers.

In addition, customers can also get the latest product news and download the required technical documentations from the BHU Networks website.

Contents

1 Product Overview	1
1.1 Product Overview	1
1.2 Main Feature	1
2 Product Composition	2
2.1 Packing list	2
2.2 System Composition	3
2.2.1 Panel Layout	3
2.2.1.1 Indicator Indication	3
2.2.1.2 Interface Indication	4
2.3 Common Button	5
2.3.1 Navigation Bar Group Button	5
2.3.2 Main Menu Group Button	5
2.3.3 Application Change Button	5
2.3.4 Save Button	6
3 Installation and Settings	7
3.1 Pre-installation	7
3.2 Installation Guidance	8
3.3 Configuration Guidance	9
3.3.1 WEB Interface Settings	9
3.4 Configuration Wizard	10
3.4.1 Select Bridge-AP Mode	10
3.4.2 Select Bridge-Station Mode	14
3.4.3 Select Bridge-Repeater Mode	16
3.4.4 Select Router-AP Mode	19
3.4.5 Select Router-Station Mode	23
3.4.6 Select Router-Repeater Mode	26
3.5 Wireless Settings	31
3.5.1 RF Settings	31
3.5.2 Virtual AP Settings	33
3.5.3 Advanced Settings	34
3.5.4 Status	35
3.5.5 Traffic Control	35
3.6 Network Settings	36
3.6.1 LAN Settings	36
3.6.2 WLAN Settings	37
3.6.3 Client List	39
3.6.4 Router Settings	40
3.6.5 Equipment Reset	42
3.6.6 DMZ Area Settings	42
3.6.7 NAT Settings	43
3.6.8 uPnP Settings	43
3.7 System Configuration	44
3.7.1 System Settings	44
3.7.2 Restore Factory Configuration	45
3.7.3 Reboot or Version Upgrade	46
3.7.4 User Administration	46
3.7.5 System Tool	48
3.7.6 System Time Settings	48
3.7.7 Administration Interface	49
3.7.8 System Log	51
4 Maintenance Overview	52
4.1 Common Tools of Maintenance	52

4.2	Maintenance Personnel Requirement.....	52
5	Equipment Check and Troubleshooting.....	53
5.1	The correct installation and configuration of BXM2/5 equipment.....	53
5.2	Network Checking and Troubleshooting.....	57
5.3	FAQ and Solutions.....	58
6	Appendix.....	59
6.1	Technical Parameters	59
6.2	Glossary	63

List of Figures

Figure 1 Indicator Panel	3
Figure 2 Equipment Interface and Reset Button	4
Figure 3 Navigation Bar.....	5
Figure 4 Menu	5
Figure 5 Application Change Button.....	5
Figure 6 Save Button.....	6
Figure 7 Login page.....	9
Figure 8 System Status	10
Figure 9 Bridge-AP Mode.....	10
Figure 10 Bridge-AP Mode	11
Figure 11 Bridge-AP Mode	11
Figure 12 Bridge-AP Mode.....	12
Figure 13 Bridge-AP Mode	12
Figure 14 Bridge-AP Mode	13
Figure 15 Bridge-AP Mode	13
Figure 16 Bridge-Station Mode.....	14
Figure 17 Bridge-Station Mode	14
Figure 18 Bridge-Station Mode.....	15
Figure 19 Bridge-Station Mode.....	15
Figure 20 Bridge-Station Mode	16
Figure 21 Bridge-Station Mode.....	16
Figure 22 Bridge-Repeater Mode.....	17
Figure 23 Bridge-Repeater Mode.....	17
Figure 24 Bridge-Repeater Mode.....	17
Figure 25 Bridge-Repeater Mode.....	18
Figure 26 Bridge-Repeater Mode.....	18

Figure 27 Bridge-Repeater Mode	19
Figure 28 Bridge-Repeater Mode	19
Figure 29 Router-AP Mode	20
Figure 30 Router-AP Mode	20
Figure 31 Router-AP Mode	20
Figure 32 Router-AP Mode	21
Figure 33 Router-AP Mode	21
Figure 34 Router-AP Mode	22
Figure 35 Router-AP Mode	22
Figure 36 Router-AP Mode	23
Figure 37 Router-Station Mode	23
Figure 38 Router-Station Mode	23
Figure 39 Router-Station Mode	24
Figure 40 Router-Station Mode	24
Figure 41 Router-Station Mode	25
Figure 42 Router-Station Mode	25
Figure 43 Router-Station Mode	26
Figure 44 Router-Station Mode	26
Figure 45 Router-Repeater Mode	27
Figure 46 Router-Repeater Mode	27
Figure 47 Router-Repeater Mode	27
Figure 48 Router-Repeater Mode	28
Figure 49 Router-Repeater Mode	28
Figure 50 Router-Repeater Mode	29
Figure 51 Router-Repeater Mode	29
Figure 52 Router-Repeater Mode	30
Figure 53 Router-Repeater Mode	30

Figure 54 RF Configuration	31
Figure 55 RF Configuration Modification	31
Figure 56 RF Configuration Modification	32
Figure 57 RF Configuration Modification	32
Figure 58 Virtual AP Settings	33
Figure 59 VAP Advanced Configuration	34
Figure 60 Advanced Configuration	35
Figure 61 WLAN Status	35
Figure 62 Traffic Control Settings	36
Figure 63 Add traffic control of user	36
Figure 64 LAN Configuration	37
Figure 65 WLAN Settings	38
Figure 66 WLAN Settings Example 1	38
Figure 67 WLAN Settings Example 2	39
Figure 68 Route ACL Settings	41
Figure 69 Edit Router Transfer Control Rule	41
Figure 70 Rule Settings	41
Figure 71 DMZ Area Settings	42
Figure 72 NAT Settings	43
Figure 73 UPnP Settings	43
Figure 74 Configuration Administration	44
Figure 75 Restore Factory Settings	46
Figure 76 Restart Configuration	46
Figure 77 Upgrade Firmware	46
Figure 78 User Management	47
Figure 79 New User	47
Figure 80 Add New User	48

Figure 81 System Tool.....	48
Figure 82 Management Configuration	50
Figure 83 Log Management	51
Figure 84 Equipment Installation	53
Figure 85 Indicator Panel	54
Figure 86 RSSI Receiving Strength	55
Figure 87 Connecting Method	55

1 Product Overview

1.1 Product Overview

BHU Networks (hereinafter referred as BHU Networks) launches BHU NETWORKS®BXM2/5 (BXM2/5 for short) on the basis of proprietary space adaptive optimal communication technology-- airX.

Supporting wireless route and bridging, BXM2 complies with 802.11bgn protocol and works at 2.4GHz frequency range, BXM5 complies with 802.11an protocol and works at 5GHz frequency range. They both provide high performance wireless relay link among WLAN stations to ensure higher transmission rate and longer transmission distance. Enhanced network functions make them suitable for various application conditions.

Easy installation and friendly configuration interface guarantee BXM2/5 product quickly access to deployment and service. They aim to perfectly solve the problems of termination access in WLAN coverage area or marginal area, at the same time extends the coverage of WLAN stations as large as possible. Transmit power no longer stops BXM2/5 from covering widely due to its 500mW transmit power and high-gain antenna in 12dBi of BXM2 & 16dBi of BXM5.

1.2 Main Feature

- Uplink to 2.4GHz of BXM2 & 5GHz of BXM5. wireless access point, downlink to dual-wire LAN port export;
- Wireless access support IEEE 802.11b/g/n standard of BXM2 & 802.11a/n standard of BXM5;
- Support MIMO 2x2, maximum rate up to 300Mbps;
- Support respective user's independent authentication under WDS bridging mode;
- Max transmit power up to 500Mw, maximum receiver sensitivity up to -100dBm of BXM2 & -95dBm of BXM5, both substantially ensure long transmission distance and high quality signal of wireless link;
- Support 2x Ethernet ports in main and auxiliary backup use, or independent use;

2 Product Composition

2.1 Packing list

Table 1

No.	Name	Quantity (Unit)
1. Packing	Box	1(pc)
2. BXM2/5		1(pc)
3.	POE Power Supply Module	1(pc)
4. Cable	Ties	2(pcs)

2.2 System Composition

2.2.1 Panel Layout

2.2.1.1 Indicator Indication



Figure 1 Indicator Panel

Table 2

No.	Indicator	Description	Function
1	PWR	Power Indicator (Yellow)	Long out—Power-off Long bright—Power-on
2	LAN	Ethernet Indicator Left port is primary port Right port is secondary port	Always off—AP mode Always bright—Station、Repeater mode
3	MODE Signal	Lamp	Station mode—the last three lamps stand for signal strength . Repeater mode—the last three lamps stand for signal strength. AP mode—the last three lamps light.

2.2.1.2 Interface Indication



Figure 2 Equipment Interface and Reset Button

Table 3

No.	Interface Name	Description
1.	1/2/(Primary/Secondary)	Ethernet terminal plug (RJ45), only Primary is used for PoE power supply.
2.	Reset	After starting up the equipment, press the reset key for 5 seconds to restore the factory Configuration. When the equipment power is switched on, press the reset key for 10 seconds to restore factory Configuration and supply first aid to procedures http.
3.	Antenna	Build-in antenna, for sending and receiving wireless data.

2.3 Common Button

2.3.1 Navigation Bar Group Button

The navigation bar has three group buttons: cancel, save and help. When using the respective functions of the equipment, please click the help button and make the configurations according to the page tips. As it is shown in the figure below:

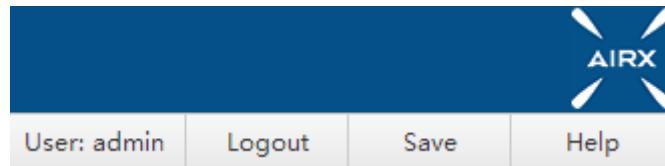


Figure 3 Navigation Bar



Note: Click "Save", to prevent the configuration loss.

2.3.2 Main Menu Group Button

There are five groups of buttons in different kinds of functions, as shown in the figure below:

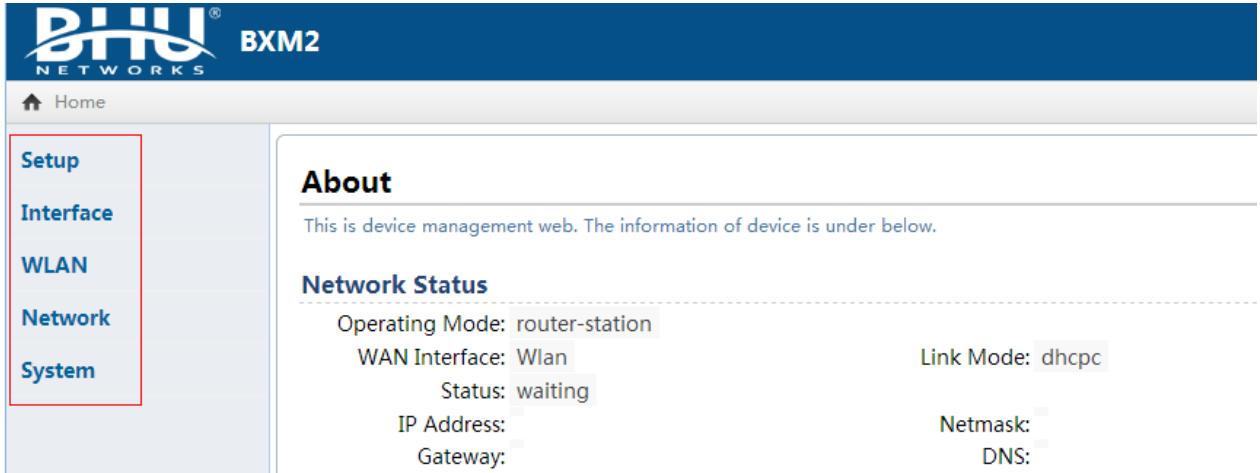


Figure 4 Menu

2.3.3 Application Change Button

Apply Changes

Figure 5 Application Change Button



Note: Once finish the configurations, the current page comes into effect.



Note: Need to reboot the equipment to make some parameters effective (refer to page instruction).

2.3.4 Save Button

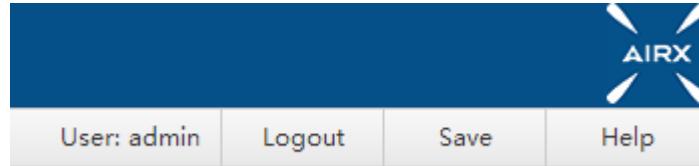


Figure 6 Save Button



Note: After change the application, please click “save” to prevent the equipment from losing the current configuration after equipment reboot.

3 Installation and Settings

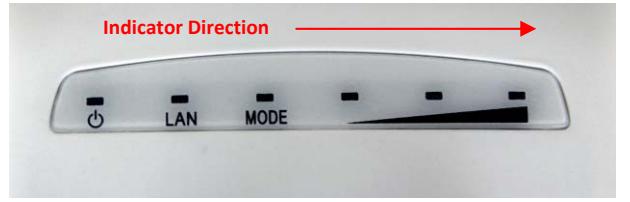
3.1 Pre-installation

Table 4

No.	Name	Quantity (unit)	Remarks
1.	BXM2/5 1(pc)		/
2.	POE Power Supply Module Type:BA-2408P Input voltage:AC100-240V 50/60Hz Output voltage:DC24V-800mA	1(pc) /	
3.	Cable Ties	2(pcs)	/
4.	Ethernet Cables	2(pcs)	Self-contained
5.	Holding Pole	1(pc) Self	-contained

3.2 Installation Guidance

The installation procedures is as shown in the figure below :

<p>Step 1 : Pre-installation. Please refer to Table 4 for all accessories.</p> 	<p>Step 2: Press hard on coupler with your fingers and pull out the back cover slides from the slot.</p> 
<p>Step 3 : PoE port locates at the left of PoE module, LAN port locates at the right, Primary port locates at the left of BXM2/5, Secondary port locates at the right, Reset button locates in the middle.</p> 	<p>Step 4: Supply power to the equipment, connect to PC , and fix BXM2/5 to the holding pole by using the cable ties.</p> <p> Note: Link PoE port to CPE Primary port, and link LAN port to the laptop LAN port.</p> 
<p>Step 5 : The equipment is installed and switched on, and the indicator lights normally. According to indicator direction: Station mode, the third lamp lights up, the last three indicators display BXM2/5 signal strength.</p> 	<p>Step 6: Set parameter via Web interface.</p> <p>Default IP address: 192.168.1.1</p> <p>Default Subnet Mask: 255.255.255.0</p> <p>Default User ID: admin</p> <p>Default Login password: admin</p> <p>For web interface configuration details, please login official website to download BXM2/5 user manual: http://www.bhunetworks.com/overseas</p>

3.3 Configuration Guidance

3.3.1 WEB Interface Settings

When logi n the equi pment, the default IP address : 192.168.1.1;subnet mask : 255.255.255.0

User ID and password is needed for log i n the WEB , default user name: admin; password: admin.

Once finish the password settings, click “login” button to jump to login page.



Note: Support language switch between Chinese and English.

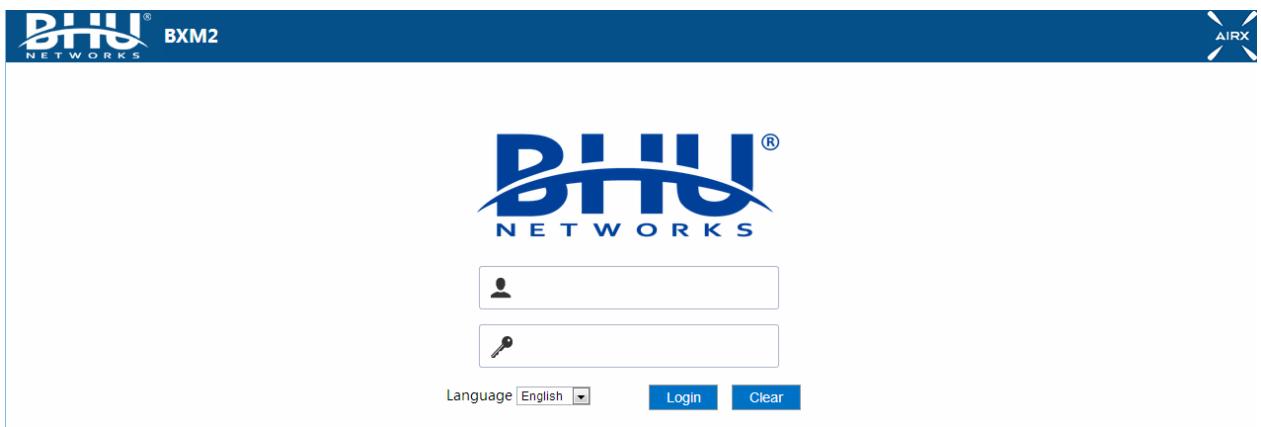


Figure 7 Login page

3.3.2 Running Status

Click “**Main Page**”, jump to equipment information page, including network status, WLAN status, system status and equipment information, as shown in the figure below:

Figure 8 System Status

3.4 Configuration Wizard

3.4.1 Select Bridge-AP Mode

Bridge-AP: Bridge-Access Point Mode. WLAN as AP, can be connected with the Ethernet.

Open “**Configuration→Configuration Wizard**”, as shown in the figure below:

Figure 9 Bridge-AP Mode

Click “**Next**” to select work mode, as shown in the figure below:

Configuration Wizard

| Welcome | **Operating Mode** | Wireless | WAN

Select the device Operating mode.

Operating Mode:

Next

Figure 10 Bridge-AP Mode

Select the related work mode to make basic configurations, as shown in the figure below:

Configuration Wizard

| Welcome | Operating Mode | **Wireless** | WAN

Here are some basic settings of VAP!

ap

Mode:	ap
Channel:	<input style="border: 1px solid black; padding: 2px 10px;" type="button" value="Auto"/> <input style="border: 1px solid black; width: 20px; height: 20px; vertical-align: middle;" type="button" value="▼"/>
Essid:	<input style="width: 200px;" type="text"/> Scan
SSID Hide:	<input type="checkbox"/>
Authentication Mode:	<input style="border: 1px solid black; padding: 2px 10px;" type="button" value="Open"/> <input style="border: 1px solid black; width: 20px; height: 20px; vertical-align: middle;" type="button" value="▼"/>

Next

Figure 11 Bridge-AP Mode

Channel: Automatically or manually select channel when necessary.

SSID hide: Hide SSID according to network safety demands, and the user can only connect to the network by configuration on the client without scanning AP.

Authentication mode: Support OPEN, WEP, WPA-PSK, WPA2-PSK, WPA-EAP and WPA2-EAP authentication modes.

Create ESSID: For example, create SSID, as shown in the figure below:

Configuration Wizard | Welcome | Operating Mode **Wireless** **WAN**

Here are some basic settings of VAP!

ap

Mode: ap

Channel: Auto

Essid: **Scan**

SSID Hide:

Authentication Mode: Open

Next

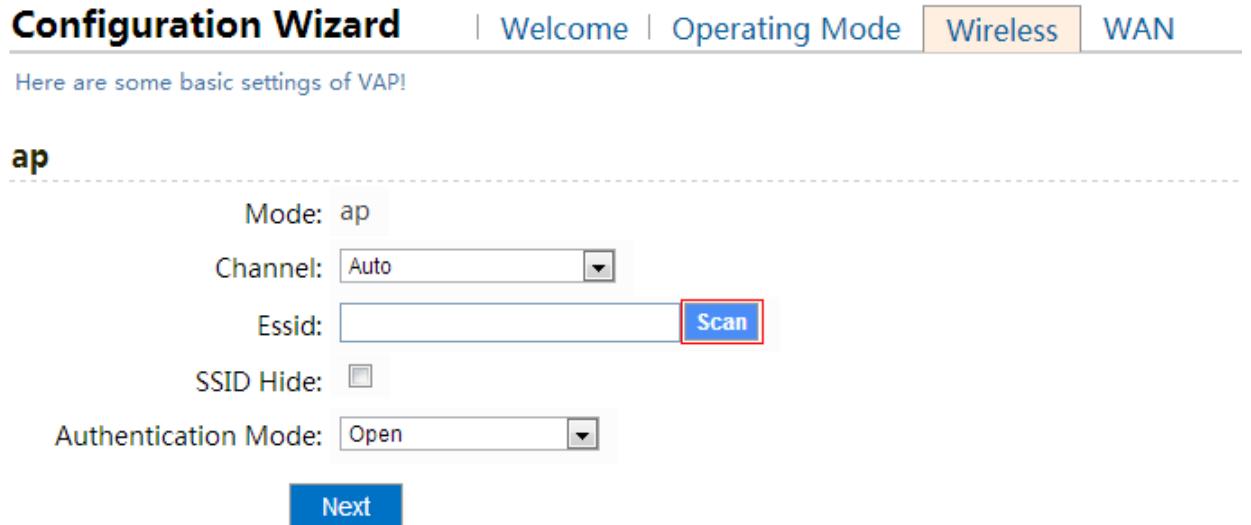


Figure 12 Bridge-AP Mode

Make the configuration effective, as shown in the figure below:

Configuration Wizard | Welcome | Operating Mode | Wireless **WAN**

IP Address of Extranet. Example: 202.96.209.6

Apply Changes

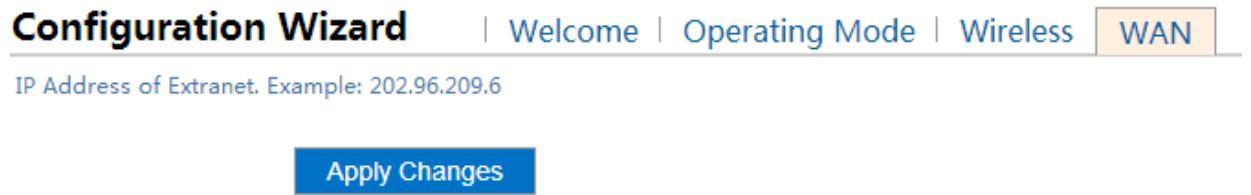


Figure 13 Bridge-AP Mode

Go to “Interface→LAN” settings, as shown in the figure below:

IPv4 Settings

IP Address:	192.168.1.1	
Netmask:	255.255.255.0	
DHCP Server:	<input checked="" type="checkbox"/> Enable	
Start Address:	100	Fill the start No. of subnet
End Address:	199	Fill the end No. of subnet.
Lease Type:	Hour <input type="button" value="▼"/>	
Lease:	6	
IP Address Standby:	0.0.0.0	
Netmask Standby:	0.0.0.0	

IPv6 Settings

IPv6 DHCP:	<input type="checkbox"/>
IPv6 Address:	<input type="text"/>
IPv6 Prefix Length:	<input type="text"/>
Apply Changes	

Figure 14 Bridge-AP Mode

Ipv4 Settings: Statically configure IP address, fill up the IP address and mask.

Ipv6 Settings: No need to change if the user does not use Ipv6.

IPv4 Settings

IP Address:	192.168.1.1	
Netmask:	255.255.255.0	
DHCP Server:	<input checked="" type="checkbox"/> Enable	
Start Address:	100	Fill the start No. of subnet
End Address:	199	Fill the end No. of subnet.
Lease Type:	Hour <input type="button" value="▼"/>	
Lease:	6	
IP Address Standby:	0.0.0.0	
Netmask Standby:	0.0.0.0	

Figure 15 Bridge-AP Mode

DHCP: Open ipv4 DHCP function , Fill in a starting subnet number, set the lease of IP address.

3.4.2 Select Bridge-Station Mode

Bridge-Station: Under Bridge-User mode, WLAN as the terminal side can link to other AP (root AP), and link to Ethernet bridge. In this mode, the linked AP (root AP) must open WDS function.

Bridge-Station basic configuration is shown in the figure below:

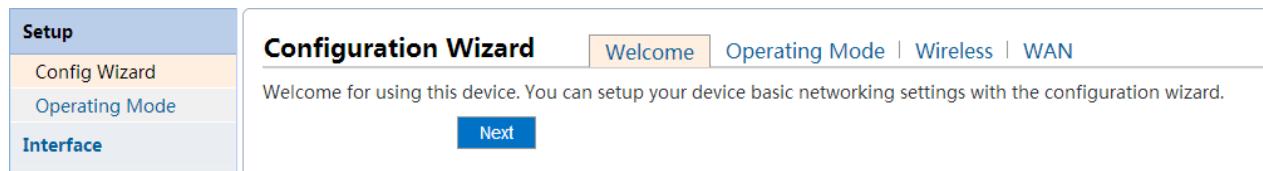


Figure 16 Bridge-Station Mode

Click "Next" to select work mode, as shown in the figure below:

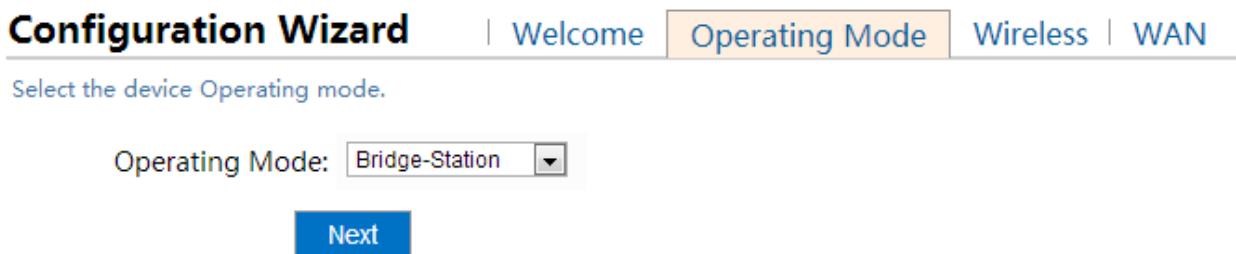


Figure 17 Bridge-Station Mode

Access to the related work mode to make basic configurations, as shown in the figure below:

Configuration Wizard| Welcome | Operating Mode | **Wireless** | WAN

Here are some basic settings of VAP!

sta

Mode: sta

Essid: **Scan**Lock to AP Address: Authentication Mode: **Next****Figure 18 Bridge-Station Mode**

Scan AP, as shown in the figure below:

**Note:** Fill button is used to link the searched ESSID.

AP Scan result								
No.	Bssid	Essid	Mode	Security	Channel	Signal	Op.	
1	00:15:6d:f2:67:70	BHUnetworks	Master	WPA2-PSK	1	-63dBm	Fill	
2	f2:1a:a9:16:25:71	CMCC-AUTO	Master	WPA2-802.1x EAP	1	-85dBm	Fill	
3	cc:b2:55:d0:cd:49	dlink-bk	Master	WPA-PSK/WPA2-PSK	1	-87dBm	Fill	
4	1c:fa:68:29:d0:8c	wodejia	Master	WPA-PSK/WPA2-PSK	1	-88dBm	Fill	

Figure 19 Bridge-Station Mode

Lock to AP: By locking to AP, you can link WLAN to the AP with appointed MAC address, as shown in the figure below:

sta

Mode: sta

Essid: BHUnetworks

Lock to AP Address: 00:15:6d:f2:67:70

Authentication Mode: WPA2-PSK

Pre-shared Key (PSK): ssid12345

Figure 20 Bridge-Station Mode

Access LAN to set, as shown in the figure below:

IPv4 Settings

IP Address: 192.168.1.1

Netmask: 255.255.255.0

DHCP Server: Enable

IP Address Standby: 0.0.0.0

Netmask Standby: 0.0.0.0

IPv6 Settings

IPv6 DHCP:

IPv6 Address:

IPv6 Prefix Length:

Figure 21 Bridge-Station Mode

Ipv4 Settings: Static configure IP address, and fill in IP address and mask.

Ipv6 Settings: No need to change if the user does not use Ipv6.

3.4.3 Select Bridge-Repeater Mode

The basic configurations of Bridge-Repeater work mode, as shown in the figure below:

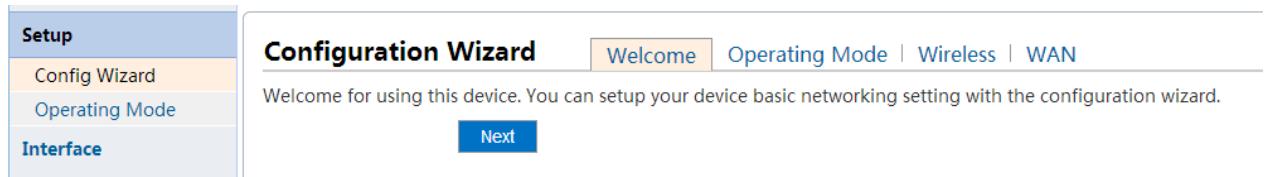


Figure 22 Bridge-Repeater Mode

 Note: Under this mode, previous level AP(root AP) must open WDS function, if not, please refer to [3.5.2 Virtual AP Settings](#) in this user manual.

Click "Next" to select work mode, as shown in the figure below:

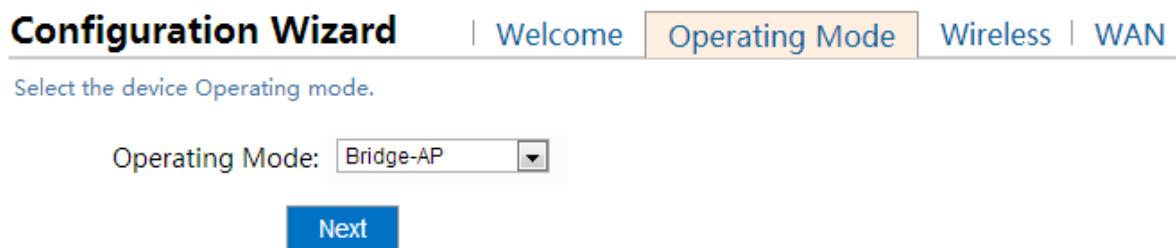


Figure 23 Bridge-Repeater Mode

Go to the related work mode to make basic settings, as shown in the figure below:

sta

Mode: sta

Essid: **Scan**

Lock to AP Address:

Authentication Mode:

ap

Mode: ap

Channel:

Essid: **Scan**

SSID Hide:

Authentication Mode:

Next

Figure 24 Bridge-Repeater Mode

Scan the AP around, as shown in the figure below:



Note: Fill button is used for connecting the ESSID searched.

AP Scan result							
No.	Bssid	Essid	Mode	Security	Channel	Signal	Op.
1	00:15:6d:f2:67:70	BHUnetworks	Master	WPA2-PSK	1	-63dBm	Fill
2	f2:1a:a9:16:25:71	CMCC-AUTO	Master	WPA2-802.1x EAP	1	-85dBm	Fill
3	cc:b2:55:d0:cd:49	dlink-bk	Master	WPA-PSK/WPA2-PSK	1	-87dBm	Fill
4	1c:fa:68:29:d0:8c	wodejia	Master	WPA-PSK/WPA2-PSK	1	-88dBm	Fill

Figure 25 Bridge-Repeater Mode

Lock to AP: WLAN can prior connect to the appointed MAC AP by locking to AP.

sta

Mode: sta

Essid: BHUnetworks Scan

Lock to AP Address: 00:15:6d:f2:67:70

Authentication Mode: WPA2-PSK

Pre-shared Key (PSK): ssid12345

Figure 26 Bridge-Repeater Mode

Set the ESSID which need to relay, as shown in the figure below:

ap

Mode: ap

Channel: 2412MHz (Channel 1)

Essid: ssid

SSID Hide:

Authentication Mode: WPA2-PSK

Pre-shared Key (PSK): ssid12345

Figure 27 Bridge-Repeater Mode

Go to LAN to set, as shown in the figure below:

IPv4 Settings

IP Address: 192.168.1.1

Netmask: 255.255.255.0

DHCP Server: Enable

IP Address Standby: 0.0.0.0

Netmask Standby: 0.0.0.0

IPv6 Settings

IPv6 DHCP:

IPv6 Address:

IPv6 Prefix Length:

Figure 28 Bridge-Repeater Mode

Ipv4 Settings: Static configure IP address, fill in IP address and mask.

Ipv6 Settings: No need to change if the user does not use Ipv6.

3.4.4 Select Router-AP Mode

Router-AP: Under Router-AP mode, WLAN works under AP mode, Ethernet port as WAN port to transfer data.

Router-AP work mode basic configuration, as shown in the figure below:

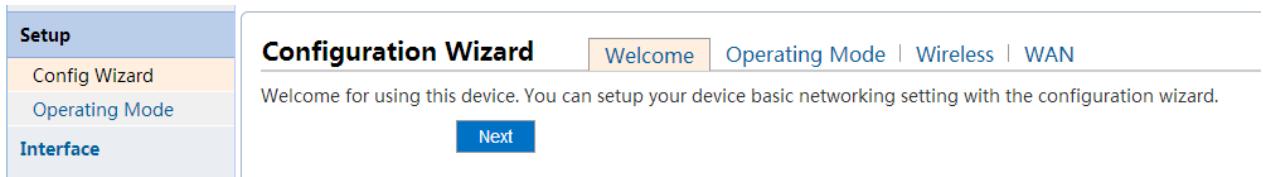


Figure 29 Router-AP Mode

Click “Next” to select operating mode, as shown in the figure below:

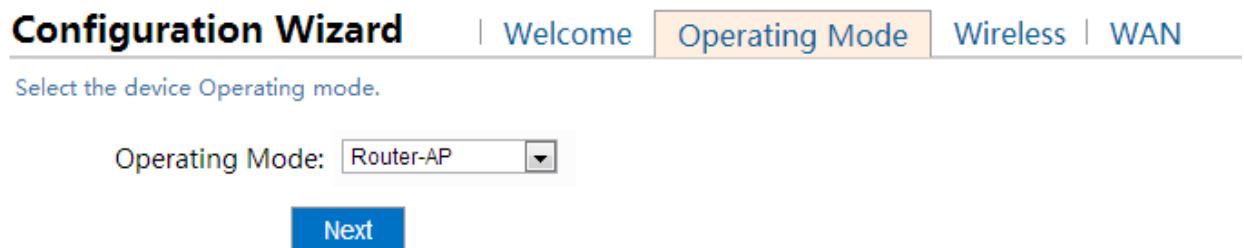


Figure 30 Router-AP Mode

Go to related work mode to make basic configuration, as shown in the figure below:

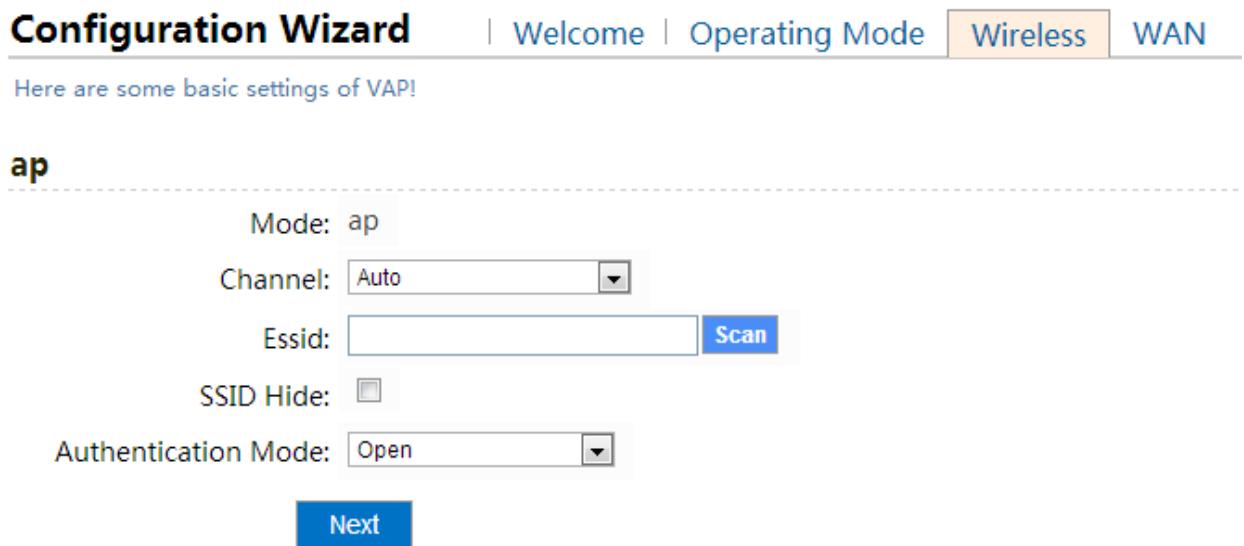


Figure 31 Router-AP Mode

Channel Selection: Select channel automatically or manually as required.

SSID Hidden: According to safety requirement, hide SSID to prevent users from scanning AP, and the user could only link to the network on client-side.

Authentication Mode: Support the following authentication: OPEN, WEP, WPA-PSK, WPA2-PSK, WPA-EAP, WPA2-EAP.

Create ESSID: An example of creating an ESSID is shown in the figure below:

Configuration Wizard

| Welcome | Operating Mode | **Wireless** | **WAN**

Here are some basic settings of VAP!

ap

Mode: ap

Channel: Auto

Essid: **Scan**

SSID Hide:

Authentication Mode: Open

Next

Figure 32 Router-AP Mode

Scan AP around, as shown in the figure below:

AP Scan result								
No.	Bssid	Essid	Mode	Security	Channel	Signal	Op.	
1	00:15:6d:f2:67:70	BHUnetworks	Master	WPA2-PSK	1	-63dBm	Fill	
2	f2:1a:a9:16:25:71	CMCC-AUTO	Master	WPA2-802.1x EAP	1	-85dBm	Fill	
3	cc:b2:55:d0:cd:49	dlink-bk	Master	WPA-PSK/WPA2-PSK	1	-87dBm	Fill	
4	1c:fa:68:29:d0:8c	wodejia	Master	WPA-PSK/WPA2-PSK	1	-88dBm	Fill	

Figure 33 Router-AP Mode



Note: Fill button is used for connecting the searched ESSID.

Select DHCP Connecting Mode: The port acquires IP address automatically, DNS is attained via DHCP server in default, no need to set.

Link Mode:

Static DNS Server:

Backup DNS Server:

Custom MAC Address: Enable

MAC Address:

Apply Changes

Figure 34 Router-AP Mode

Select Static Configuration Connection Mode: Static configure IP address and DNS.

Manual MAC address: Open this function, and change the MAC address of WAN port but cannot change the MAC address of WLAN port.

Link Mode:

IP Address:

Netmask:

Gateway:

Static DNS Server:

Backup DNS Server:

Custom MAC Address: Enable

MAC Address:

Apply Changes

Figure 35 Router-AP Mode

Select PPPoE Connection Mode, input the related user ID and passport.

PPP Connecting Mode: Auto-connecting mode, Demand-try to link when there is a data requirement, Once-manual connecting.

Link Mode: PPPoE

User: bhuwireless

Password: bhuwan

PPP Link Mode: Auto

Static DNS Server: []

Backup DNS Server: []

Custom MAC Address: Enable

MAC Address: []

Apply Changes

Figure 36 Router-AP Mode

3.4.5 Select Router-Station Mode

Router-Station: Under Router -Client Mode, WLAN works under Client Mode and connects with other AP, using WLAN as WAN port to transmit the data.

Router-Station work mode basic configuration, as shown in the figure below:

Setup

Configuration Wizard

Welcome

Operating Mode | Wireless | WAN

Welcome for using this device. You can setup your device basic networking setting with the configuration wizard.

Next

Figure 37 Router-Station Mode

Click “Next” to select work mode, as shown in the figure below:

Configuration Wizard

Welcome

Operating Mode

Wireless | WAN

Select the device Operating mode.

Operating Mode: Router-Station

Next

Figure 38 Router-Station Mode

Then go to the related work mode to make basic configurations, as shown in the figure below:

Mode: sta

Essid: **Scan**

Lock to AP Address:

Authentication Mode: Open

Next

Figure 39 Router-Station Mode

Scan the AP around, as shown in the figure below:

AP Scan result							
No.	Bssid	Essid	Mode	Security	Channel	Signal	Op.
1	00:15:6d:f2:67:70	BHUnetworks	Master	WPA2-PSK	1	-63dBm	Fill
2	f2:1a:a9:16:25:71	CMCC-AUTO	Master	WPA2-802.1x EAP	1	-85dBm	Fill
3	cc:b2:55:d0:cd:49	dlink-bk	Master	WPA-PSK/WPA2-PSK	1	-87dBm	Fill
4	1c:fa:68:29:d0:8c	wodejia	Master	WPA-PSK/WPA2-PSK	1	-88dBm	Fill

Figure 40 Router-Station Mode



Note: Fill button is used for connecting the searched ESSID.

Lock to AP: By locking AP function, can make WLAN connect to AP of the appointed MAC address, as shown in the figure below:

sta

Mode: sta

Essid: BHUnetworks

Lock to AP Address: 00:15:6d:f2:67:70

Authentication Mode: WPA2-PSK

Pre-shared Key (PSK): bhuwireless

Figure 41 Router-Station Mode

Select DHCP Connecting Mode: The port acquires IP address automatically, DNS can be attained via DHCP server in default, no need to set if no special requirement.

Link Mode:

Static DNS Server:

Backup DNS Server:

Custom MAC Address: Enable

MAC Address:

Figure 42 Router-Station Mode

Select static configuration Connecting Mode: Configure IP address and DNS Statically.

Manual MAC Address: Open this function, can change MAC address of the WAN port, but cannot change MAC address of the WLAN port.

Link Mode:

IP Address:

Netmask:

Gateway:

Static DNS Server:

Backup DNS Server:

Custom MAC Address: Enable

MAC Address:

Apply Changes

Figure 43 Router-Station Mode

Select PPPoE connecting mode, input the related user password.

PPP Connecting Mode: Auto-Automatic link mode, Demand-Try to link when there is a data requirement, Once-manual connecting.

Link Mode:

User:

Password:

PPP Link Mode:

Static DNS Server:

Backup DNS Server:

Custom MAC Address: Enable

MAC Address:

Apply Changes

Figure 44 Router-Station Mode

3.4.6 Select Router-Repeater Mode

Router-Repeater: Under Router-Repeater mode, WLAN is not only connected with previous level AP (root AP) as Client, but also provide wireless connection as AP.

Router-Repeater work mode basic configurations, as shown in the figure below:

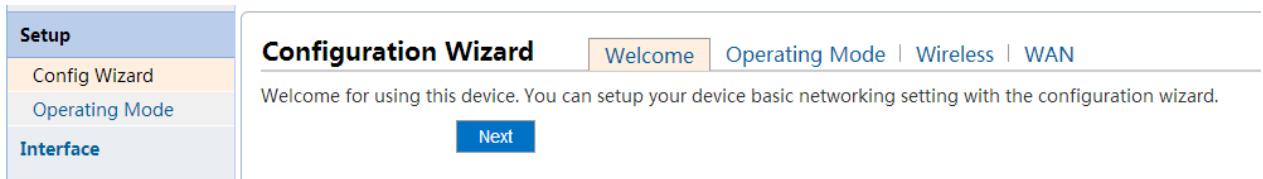


Figure 45 Router-Repeater Mode

Click “Next” to select operating mode, as shown in the figure below:

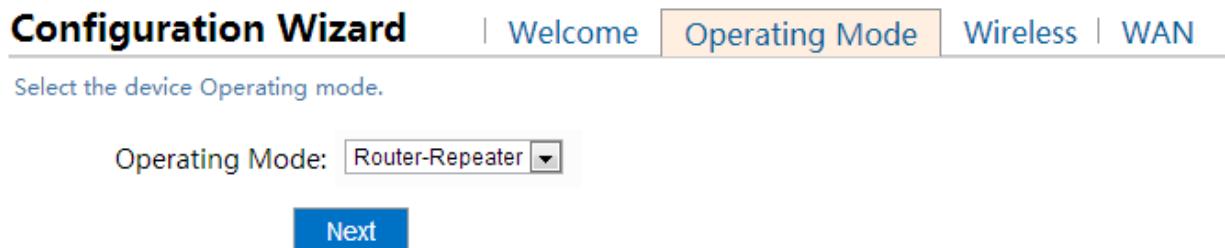


Figure 46 Router-Repeater Mode

Go to the operating mode to make basic configurations, as shown in the figure below.

sta

Mode: sta

Essid: **Scan**

Lock to AP Address:

Authentication Mode:

ap

Mode: ap

Channel:

Essid: **Scan**

SSID Hide:

Authentication Mode:

Next

Figure 47 Router-Repeater Mode

Scan AP around ,as shown in the figure below:

AP Scan result								
No.	Bssid	Essid	Mode	Security	Channel	Signal	Op.	
1	00:15:6d:f2:67:70	BHUnetworks	Master	WPA2-PSK	1	-63dBm	Fill	
2	f2:1a:a9:16:25:71	CMCC-AUTO	Master	WPA2-802.1x EAP	1	-85dBm	Fill	
3	cc:b2:55:d0:cd:49	dlink-bk	Master	WPA-PSK/WPA2-PSK	1	-87dBm	Fill	
4	1c:fa:68:29:d0:8c	wodejia	Master	WPA-PSK/WPA2-PSK	1	-88dBm	Fill	

Figure 48 Router-Repeater Mode



Note: Fill button is used for connecting the searched ESSID.

sta

Mode: sta

Essid: Scan

Lock to AP Address:

Authentication Mode:

Pre-shared Key (PSK):

Figure 49 Router-Repeater Mode

Locked to AP: The function of locking to AP can make WLAN connect to AP of the appointed MAC prior.

Set the ESSID which requires relay, as shown in the figure below:

ap

Mode: ap

Channel: 2412MHz (Channel 1)

Essid:	ssid	<input type="button" value="Scan"/>
--------	------	-------------------------------------

SSID Hide:

Authentication Mode: WPA2-PSK

Pre-shared Key (PSK): ssid12345

Figure 50 Router-Repeater Mode

Select DHCP Connecting Mode: The port attains IP address automatically, DNS can be attained by DHCP server in default, no need to set if no special requirement.

Link Mode: DHCP

Static DNS Server:

Backup DNS Server:

Custom MAC Address: Enable

MAC Address:

Figure 51 Router-Repeater Mode

Select Static Configuration Connection Mode: Static configuration IP address and DNS.

Manual MAC address: Open this function, can change MAC address of WAN port, but cannot change MAC address of the WLAN port.

Link Mode:

IP Address:

Netmask:

Gateway:

Static DNS Server:

Backup DNS Server:

Custom MAC Address: Enable

MAC Address:

Figure 52 Router-Repeater Mode

Select PPPoE Connection Mode: Input the related user password

PPP Connection Mode: Auto-link mode, Demand- Try to link when there is a data requirement, Once-manual connecting.

Link Mode:

User:

Password:

PPP Link Mode:

Static DNS Server:

Backup DNS Server:

Custom MAC Address: Enable

MAC Address:

Figure 53 Router-Repeater Mode

3.5 Wireless Settings

3.5.1 RF Settings

Open "Wireless→RF", click modify.



Figure 54 RF Configuration

Modify RF Configuration.

Figure 55 RF Configuration Modification

Country Code: The country where the equipment is used. Due to the local law restriction, this settings will affect the maximum transmit power of the equipment and the setting channel. After rebooting the equipment, the country code settings will come into effect.

Tx Chain: Select the sending chain.

Rx Chain: Select the receiving chain.

Answer timeout: Answer message timeout. This parameter affects the longest telecommunication distance.

Distance formula: meter=(acktimeout(ms)-27)*150.

A-MPDU:	<input checked="" type="checkbox"/> Enable	Enable or Disable A-MPDU
A-MPDU Frames:	32	The number of frames in an A-MPDU packet
A-MPDU Limit:	65535	The max length of an A-MPDU packet
A-MSDU:	<input checked="" type="checkbox"/> Enable	Enable or Disable A-MSDU
Short GI:	<input checked="" type="checkbox"/> Enable	Enable or Disable Short GI

Figure 56 RF Configuration Modification

AMPDU: A-MPDU polymerizes the MPDU which is packed by 802.11 messages, and the MPDU is data frame which is packed by 802.11. By one-time sending several MPDU, the required amount of PLCP Preamble and PLCP Header for sending each 802.11 message is reduced, thus, the system throughput is enhanced.

Short-GI: Be used to reduce the interference time among OFDM signs. Under multipath environment, the later front-end of character maybe arrive earlier than the former one's back end, which will cause the interferences among signs. Guard Period is the blank time between two signs, which can provide a longer buffer time for the delayed signal.

Mode(2.4G):	<input checked="" type="checkbox"/> b	<input checked="" type="checkbox"/> g	<input checked="" type="checkbox"/> n	Go into effect after reboot device.
Channel bandwidth:	20MHz	Go into effect after reboot device.		
Channel:	Auto	Effect only AP mode.		
Tx Power:	0dBm			
Tx Chain*:	<input checked="" type="checkbox"/> Chain0	<input checked="" type="checkbox"/> Chain1	Effective for new create vap(or reboot device).	
Rx Chain*:	<input checked="" type="checkbox"/> Chain0	<input checked="" type="checkbox"/> Chain1	Effective for new create vap(or reboot device).	
Beacon Interval:	100	Set beacon sendinterval (50-1000)ms		
Ack timeout:	64	Effect coverage area and throughput.		

Figure 57 RF Configuration Modification

11G Mode: 802.11g mode working at 2.4GHz frequency band is compatible with 802.11b equipment.

11NGHT20: 802.11n mode at 20MHz channel bandwidth, 802.11n provides a higher speed rate than that of 802.11g.

11NGHT40+: 802.11n mode at 40MHz channel bandwidth, using the high deviated channel (+4) as the extended channel.

11NGHT40- Use 802.11n mode at 40MHz channel bandwidth, using the low deviated channel (-4) as the extended channel.

Channel: RF work channel. Set it as auto, the best work channel can be found when RF is initialized. This setting is invalid to Station.

20MHz: Use 20MHz channel bandwidth.

HT20/HT40: Automatically select 20MHz or 40MHz as the channel bandwidth. When extending channel is busy, AP only uses 20MHz channel bandwidth.

Static HT40: Set channel bandwidth as 40MHz, this function is only used for testing.

3.5.2 Virtual AP Settings

Open" Wireless→Virtual AP".

WLAN VAP Settings

Here are some basic settings of VAP! When you changed the options with *, you need to restart interface.

Select VAP:	<input style="border: 1px solid #ccc; padding: 2px 5px; width: 100px; height: 20px; border-radius: 5px; background-color: #fff;" type="button" value="wlan1"/>
RF:	wifi0
MAC:	86:82:f4:00:39:8c
Mode:	sta
Enable:	<input checked="" type="checkbox"/> Enable <small>Enable or Disable VAP</small>
Essid:	<input style="width: 200px; height: 25px; border: 1px solid #ccc; border-radius: 5px; margin-right: 10px;" type="text"/> <input style="border: 1px solid #0072bc; color: #fff; background-color: #0072bc; padding: 2px 10px; border-radius: 5px;" type="button" value="Scan"/>
Lock to AP Address:	<input type="checkbox"/> <small>Try to link the specified BSSID firstly</small>
WDS:	<input checked="" type="checkbox"/> <small>Allow devices linked to the station to pass through the ap</small>
ExtAP:	<input type="checkbox"/> <small>Be Used when WDS disabled(only 3 addrs)</small>
Authentication Mode:	<input style="border: 1px solid #ccc; padding: 2px 5px; width: 100px; height: 20px; border-radius: 5px; background-color: #fff;" type="button" value="Open"/>

Figure 58 Virtual AP Settings

VAP(Virtual Access Point): There are several virtual WLAN technologies on the RF equipment. A same channel must be used on several VAP on the RF equipment. One STA and several AP can be created on the same RF chip, but AP must be set up firstly.

MAC: The MAC address of VAP. When it is used as AP, this MAC address is its BSSID.

Mode: VAP work mode can be AP or Client.

Enable: Open the interface or not. If not, VAP does not work.

ESSID: The name of wireless network.

SSID Hide: Broadcast SSID or not. If open it, client cannot find SSID of AP through scanning.

Isolation: AP telecommunication among Clients is not allowed.

Lock to AP: Link to appointed BSSID firstly. If fail to link to the appointed AP, then try to link to others.

WDS: Allow other equipment to link to the Clients via AP.

ExtAP: Allow other equipment to link to clients via AP. It is mainly used when AP cannot open WDS. It is recommended to use WDS.

KeepAP: Only used in the Relay Mode. When the Client does not link to AP in previous level, still open AP interface. The interface comes into effect after reboot.

3.5.3 Advanced Settings

Open “Wireless→Advanced”.

Figure 59 VAP Advanced Configuration

Signal Mark Frame Interval: Set the signal mark frame interval time. Signal mark frame is used for broadcasting AP name.

DTIM Cycle: DTIM (delivery traffic indication message), is a kind of transmission indication message(TIM), is used to tell the Client that there is a buffer broadcast/single cast data in AP. DTIM Cycle sets the client dormant time based on signal mark frame counting.

WMM: WMM(Wi-Fi Multimedia): Provide basic QoS (Quality of service) function for 802.11. The power saving function is also realized in WMM.

Short Front Code: Long front code is compatible with the old 11b equipment. Using short front code can attain a higher transmission rate.

BG Protection Mode: Open 802.11g protection mode, v802.11b equipment can be inspected to be going to send RTS/CTS order in 802.11g network. This function can be used to protect the frame equipment which cannot recognize OFDM modulation.

RTS/CTS: RTS/CTS protocol (Request to send/Clear to send), that is Request sending/clear sending protocol, a mechanism which is adopted by 802.11 wireless protocols to reduce the conflicts caused by hiding node.

Client Number: Currently, this access point supports the maximum number of 255 Clients.

 **Note:** This Client restriction option only appears under AP mode and Repeater mode.

 **Note:** Repeater mode distinguishes between wlan1-STA port and wlan0-AP port.

Open “Wireless→Advanced”.

Figure 60 Advanced Configuration

RTS/CTS: RTS/CTS Protocol (Request to Send/Clear to Send), that is Request sending/clear sending protocol, a mechanism which is adopted by 802.11 wireless protocol to reduce the conflicts caused from hiding node.

WMM: WMM (Wi-Fi Multimedia) provides basic QoS (Quality of Service) function for 802.11 networks. Power saving function is also realized in WMM.



Note: Be in Bridge-Station or Router-Station Mode.

3.5.4 Status

Open “Wireless → Status-AP Mode/Station Mode”. as shown in the figure below:

Item	Info
AP	00:00:00:00:00:00
Essid	
Tx Power	27 dBm
Rx Signal	-96 dBm
Bit Rate	0 kb/s
Frequency	2.412 GHz

Figure 61 WLAN Status

3.5.5 Traffic Control

Open “Wireless→Traffic Control”.

Traffic Control

Using traffic control function to limit the upload or/and download rate of SSID or/and users.

Select VAP: wlan1

SSID and User Group

SSID Tx Rate(kbps):	0
SSID Rx Rate(kbps):	0
Users Tx Rate(kbps):	0
Users Rx Rate(kbps):	0

Spec Users

No.	MAC Address	Tx Rate(kbps)	Rx Rate(kbps)	Op.
-----	-------------	---------------	---------------	-----

Add New

Figure 62 Traffic Control Settings

Fill in the Tx rate and Rx rate of SSID and User Group to limit the upload or download rate of SSID or users.

Click the “Add New” button to add traffic control of user.

Add traffic control of user

VAP: wlan1

MAC Address:

Tx Rate(kbps):

Rx Rate(kbps):

Users Rx Rate(kbps):

Apply Changes Cancel

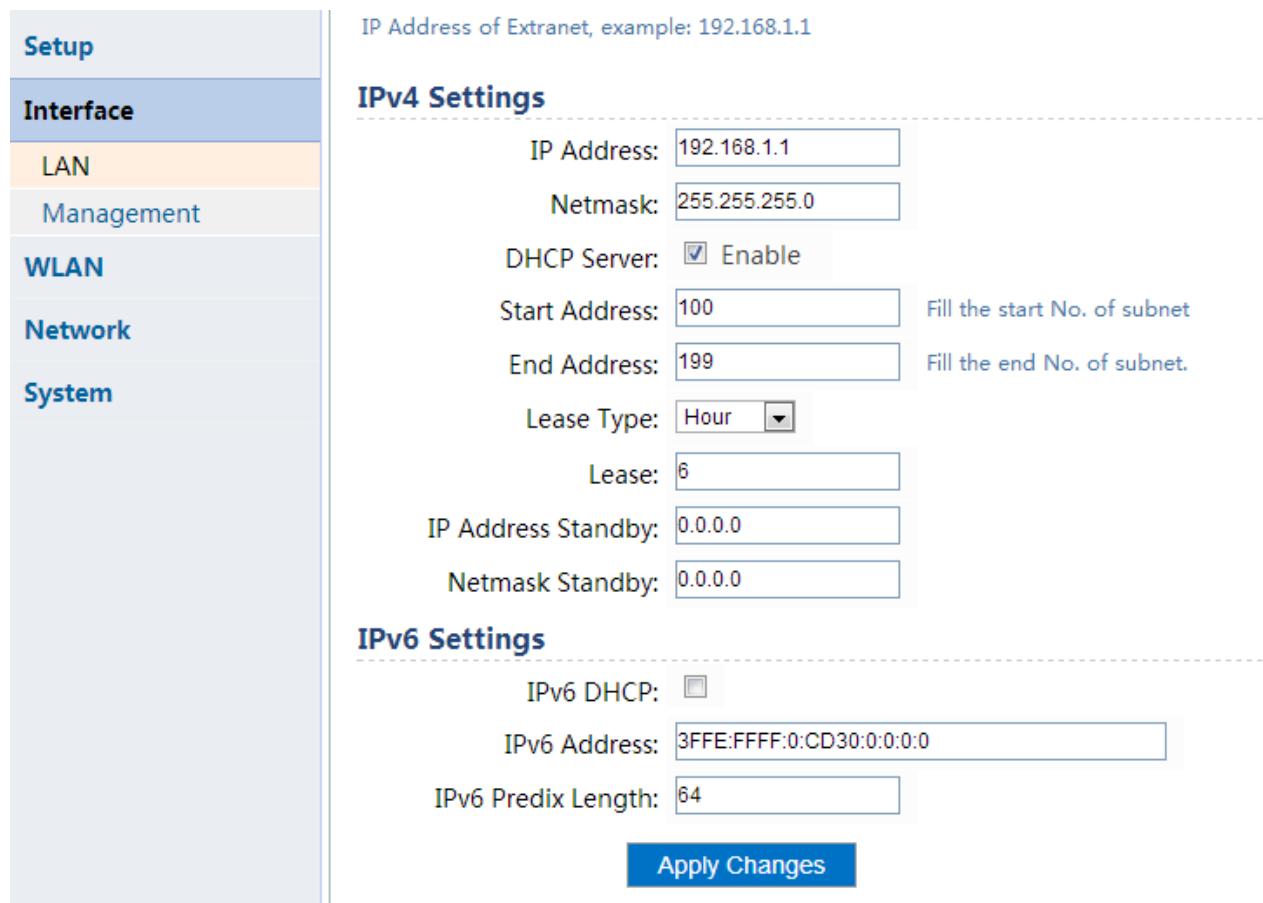
Apply Changes

Figure 63 Add traffic control of user

3.6 Network Settings

3.6.1 LAN Settings

Open “Interface→LAN”.



The screenshot shows a configuration interface for a network device. The left sidebar has tabs for 'Setup', 'Interface', 'LAN' (selected), 'Management', 'WLAN', 'Network', and 'System'. The main area is titled 'IPv4 Settings' and contains fields for IP Address (192.168.1.1), Netmask (255.255.255.0), DHCP Server (checked, 'Enable'), Start Address (100), End Address (199), Lease Type (Hour), Lease (6), IP Address Standby (0.0.0.0), and Netmask Standby (0.0.0.0). Below this is the 'IPv6 Settings' section with fields for IPv6 DHCP (unchecked), IPv6 Address (3FFE:FFFF:0:CD30:0:0:0:0), and IPv6 Prefix Length (64). At the bottom is a blue 'Apply Changes' button.

Figure 64 LAN Configuration

IP address: LAN IP address settings: e.g.192.168.1.1

Subnet mask: Subnet mask is IP network subdivided logically, e.g. 255.255.255.0.

DHCP server: DHCP server automatically set parameter of the network equipment, so that network equipment can telecommunicate online.

Start address: The start address of DHCP address pool, only fill up subnet number, e.g. IP: 192.168.1.1 Net mask: 255.255.255.0, start number: 100, mean start from 192.168.1.100.

End address: The end address of DHCP address.

Lease type: Service Lease type: Time unit or infinite.

Infinite: unlimited.

IPv6 address: format: Ipv6 address/prefix length , e.g.3FFE:FFFF:0:CD30:0:0:0:0/64,if there is successive zero, can replace with::, only once , the maximum of prefix length is 128.

IPv6 DHCP: Network port attains ipv6 address automatically.



Note: When the equipment is in Bridge Mode, only be available for LAN settings.

3.6.2 WLAN Settings

Open "Interface→WAN"

WAN

IP Address of Extranet, example: 202.96.209.6

Link Mode:

Static DNS Server:

Backup DNS Server:

Custom MAC Address: Enable Not support modify wifi interface's Mac Address

MAC Address:

Use VLAN: Enable

Apply Changes

Figure 65 WLAN Settings

 Note: When the equipment is in Router Mode, need to add WAN settings.

Select DHCP Connection Mode: The port attains IP address automatically, DNS is attained via DHCP server in default, if there is no special requirement, no need to set.

Select Static Configuration Connection Mode, configure IP address and DNS statically, as shown in the figure below:

WAN

IP Address of Extranet, example: 202.96.209.6

Link Mode:

IP Address:

Netmask:

Gateway:

Static DNS Server:

Backup DNS Server:

Custom MAC Address: Enable Not support modify wifi interface's Mac Address

MAC Address:

Use VLAN: Enable

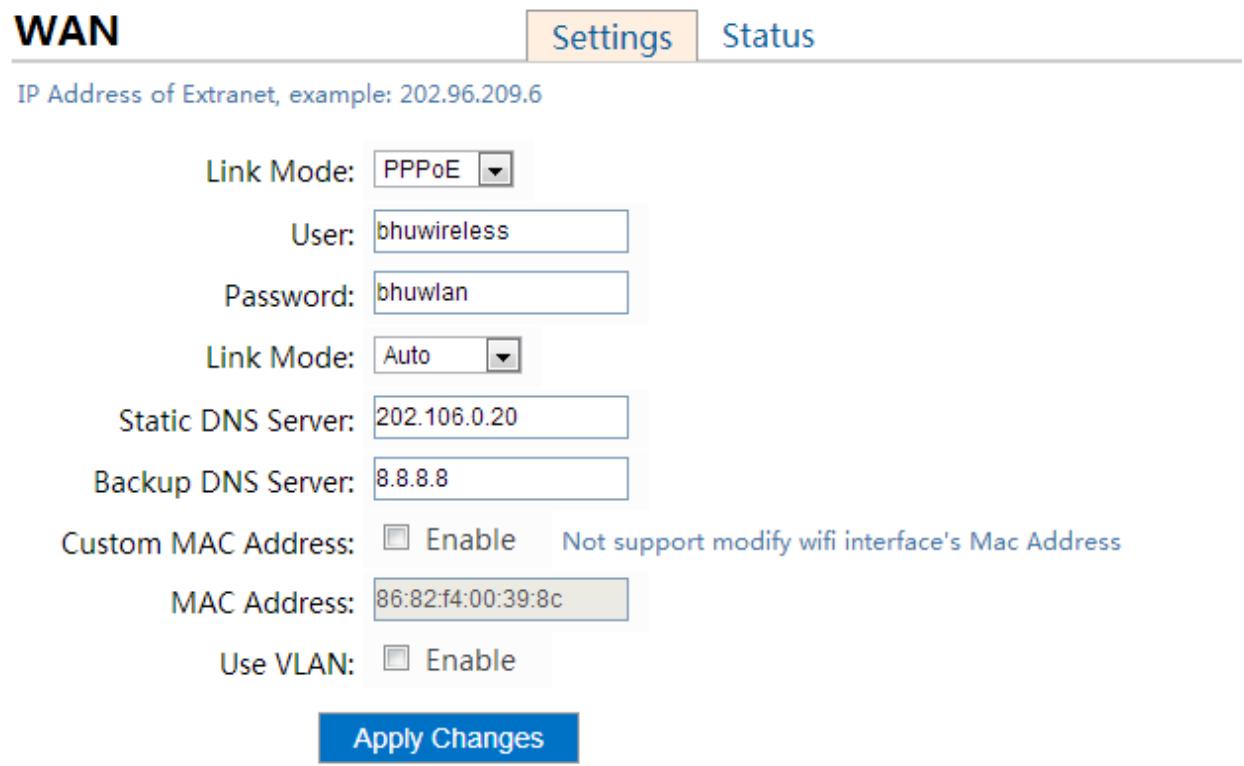
Apply Changes

Figure 66 WLAN Settings Example 1

Select PPPoE Connection Mode: Input related user password.

PPP connection mode : Auto-link mode, Demand-when there is a data requirement, try to link, Once-manual connection.

Select Connection Mode, as shown in the figure below:

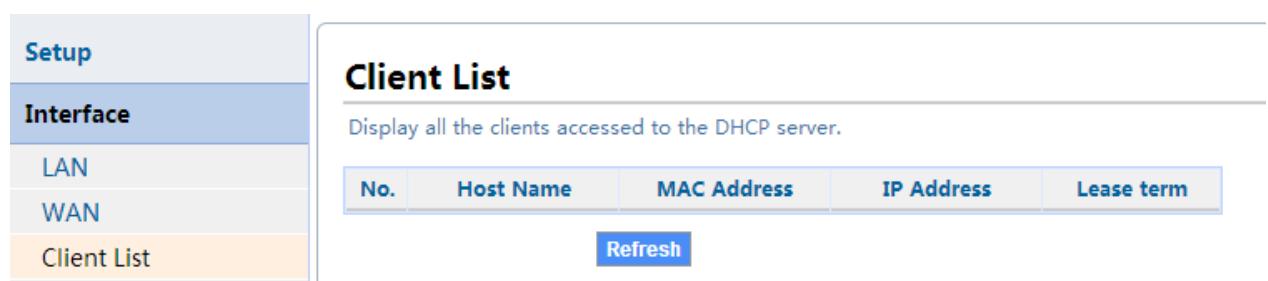


The screenshot shows the 'WAN' settings page. The 'Settings' tab is selected. The 'Link Mode' dropdown is set to 'PPPoE'. The 'User' field contains 'bhuwireless' and the 'Password' field contains 'bhuwan'. Below these, another 'Link Mode' dropdown is set to 'Auto'. The 'Static DNS Server' field contains '202.106.0.20' and the 'Backup DNS Server' field contains '8.8.8.8'. Under 'Custom MAC Address', there is an 'Enable' checkbox followed by the text 'Not support modify wifi interface's Mac Address'. The 'MAC Address' field contains '86:82:f4:00:39:8c'. The 'Use VLAN' field has an 'Enable' checkbox. At the bottom is a blue 'Apply Changes' button.

Figure 67 WLAN Settings Example 2

3.6.3 Client List

Open “Interface→Client List”.



The screenshot shows the 'Client List' interface. The left sidebar has a 'Setup' section and a 'Interface' section with options: 'LAN', 'WAN', and 'Client List', with 'Client List' being the active tab. The main area is titled 'Client List' and contains the sub-instruction 'Display all the clients accessed to the DHCP server.' Below this is a table with columns: 'No.', 'Host Name', 'MAC Address', 'IP Address', and 'Lease term'. A 'Refresh' button is located at the bottom of the table area.

Figure 68 Client List

 Note: Client List only appears in Router-Station mode, it hides in other modes.

3.6.4 Router Settings

Open “ Network→Routes”, as shown in the figure below:

No.	IPv4 Destination	IPv4 Genmask	IPv4 Gateway	Interface	Metric	MTU
1	192.168.1.0	255.255.255.0	0.0.0.0	br-lan	0	0
2	127.0.0.0	255.0.0.0	0.0.0.0	lo	0	0

Figure 69 Routes Settings

Static routes: Static router is manually configured by administrator. The administrator must understand the topology map of the router, and when network topology is changed, the administrator need to revise the router path manually.

Figure 70 Add Static Router Settings

Add static routes settings: Adding a new router, the IP address of user appointed destination, subnet mask, default gateway (the address of next hop), and the priority and network equipment interface of data package sending.

 **Note:** When the configured router does not apply with the current network topology structure, the static router cannot be added.

Open “Network→Route ACL control”, according to IP address regulation control, as shown in the figure below :

Figure 68 Route ACL Settings

Router transfer: The user can control the router data transfer via adding router transfer regulation. This equipment realized the alternative after opening router transfer control, only allow to transfer the data package which is applied with the regulation.

New-built regulation, as shown in the figure below:

Figure 69 Edit Router Transfer Control Rule

Figure 70 Rule Settings

3.6.5 Equipment Reset

If you want to restore the router system to the factory default, please refer to the following steps:

1. Press and hold RESET button.
2. When all the LED is lighted up, release RESET button, BXM2/5 will be restored to the factory status.



Note: Before BXM2/5 is totally started, the power must not be turned off. Otherwise, the configuration is possibly not restored to factory default value.

3.6.6 DMZ Area Settings

Open “Network→DMZ”.

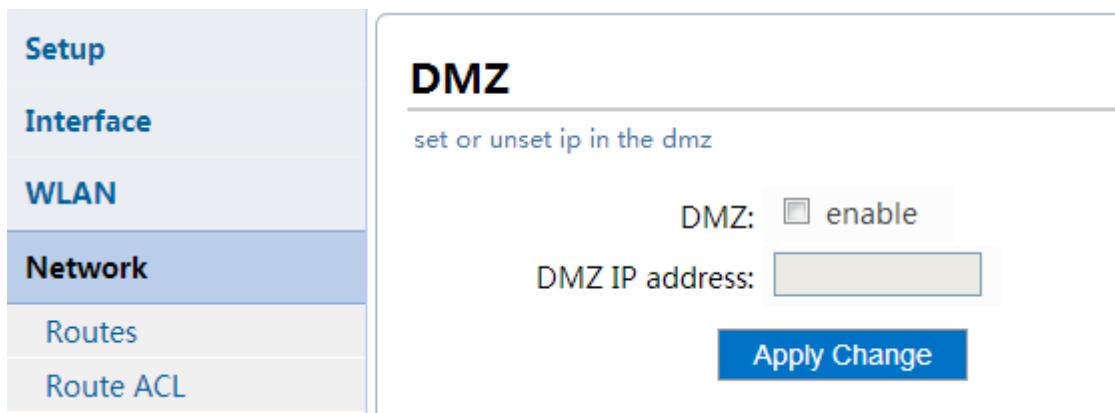


Figure 71 DMZ Area Settings

DMZ(Demilitarized Zone): DMZ also be called non-military region .It can be regarded as a special network area which is different from the external and internal networks, DMZ usually accommodates some non-confidential public server, such as Web, Mail, FTP and so on, so that the external visitors can access the server in DMZ, but cannot touch the confidential information of the internal network, even if DMZ server is damaged, it cannot do any effect to the internal network confidential information, see the DMZ strategy as follows:

- 1) Intranet can visit internet
- 2) Intranet can visit DMZ
- 3) Internet cannot visit intranet
- 4) Internet can visit DMZ but cannot visit intranet
- 5) DMZ cannot visit internet (There are exceptions)

DMZ: Put all services provided to external users on DMZ server, usually these services includes WEB server, mail server, FTP server and VoIP servers.



Note: DMZ uses firewall alternative, adds a protection for the intranet, meanwhile it provides a public server in this area, can effectively avoid some conflicts between internet application publicity and intranet safety strategy,

Bastion host, Modem pool, and all public services in DMZ area. DMZ server can only be used for user connection, the background data needs to be put in the intranet.

3.6.7 NAT Settings

Open “Network→NAT PENETRATION”.

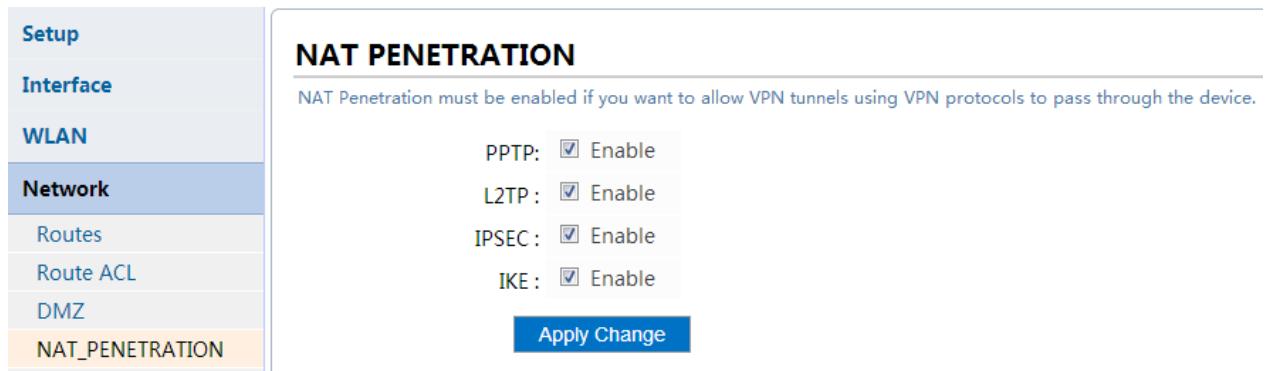


Figure 72 NAT Settings

PPTP Transparent transmission: Point to Point Tunnel Protocol (PPTP) is a kind of technology which allows point to point protocol to penetrate IP network. If PPTP protocol message is allowed to penetrate on the equipment, please click “enable”.

L2TP Transparent transmission: Layer 2 Tunnel Protocol (L2TP), is to seal the link layer PPP Frame into the IP data package to conduct the Tunnel transmission seal protocol. If allow L2TP protocol message to penetrate on the equipment, please click “enable”.

IPSec Transparent transmission : IPsec (Internet Protocol Security), is a network transmission Protocol group (some interrelated protocol alloy) to protect IP Protocol via encrypting and certifying IP (Internet Protocol). If allow IPSec message to penetrate on the equipment, please click “enable”.

IKE Transmission: Internet Key Protocol (IKE) is to switch and manage the encrypted key protocol in VPN, when PPTP and L2TP use certificate, the IKE will be used, therefore, the restriction of IKE may affect PPTP and L2TP. If allow IKE to go through equipment, click “enable”.

3.6.8 UPnP Settings

Open “Network→UPnP Settings”.

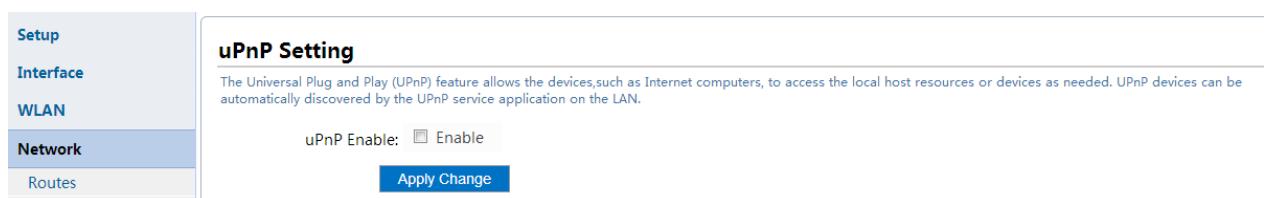


Figure 73 UPnP Settings

1. Only using the application of supporting UPnP protocol (e.g. Thunder, Emule, PPLive, BT and MSN), this function is necessarily opened.
2. Since the current UPnP protocol security has not been totally ensured, please close UPnP function when it is not required.
3. UPnP function is supported by operation system (e.g. Windows ME/Windows XP/Windows Vista/Windows7).

3.7 System Configuration

3.7.1 System Settings

Open “System→Configuration→Save/Export/Loading”, click “Save” to save the current configuration, as shown in the figure below:

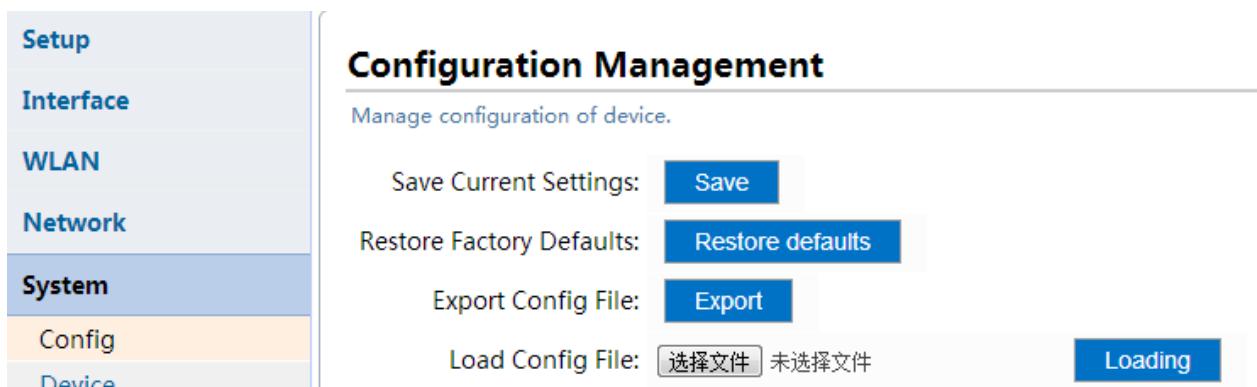


Figure 74 Configuration Administration

Access configuration document, as shown in the figure below:

Configuration Management

Manage configuration of device.

Save Current Settings:	<input type="button" value="Save"/>
Restore Factory Defaults:	<input type="button" value="Restore defaults"/>
Export Config File:	<input type="button" value="Export"/>
Load Config File:	<input type="text" value="选择文件"/> <input type="button" value="浏览..."/> <input type="button" value="Loading"/>

Figure 78 Access Configuration Document

Access: User could save the current configuration to restore the present settings in requirement.

Loading the configuration document, as shown in the figure below:

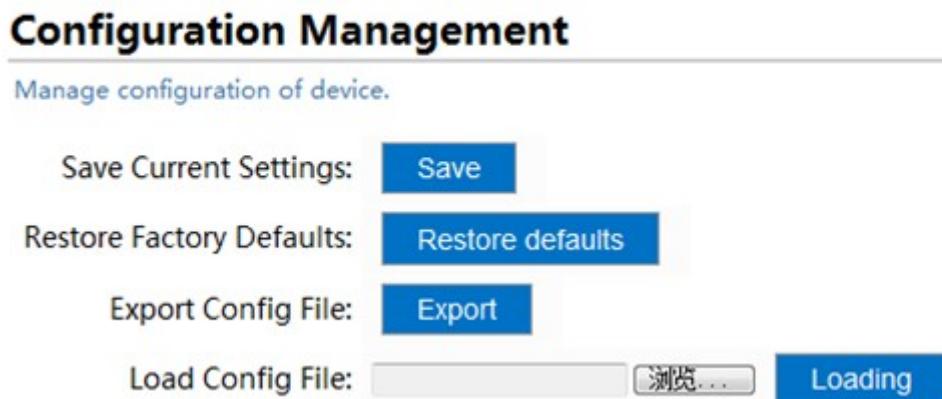


Figure 79 Loading Configuration Document

Loading: When the user does not utilize the equipment properly, which resulted in changing the current settings, the user can maintain the normal running via restore the previous saved configuration document.

3.7.2 Restore Factory Configuration

Open system “Configuration→Restore factory configuration”.

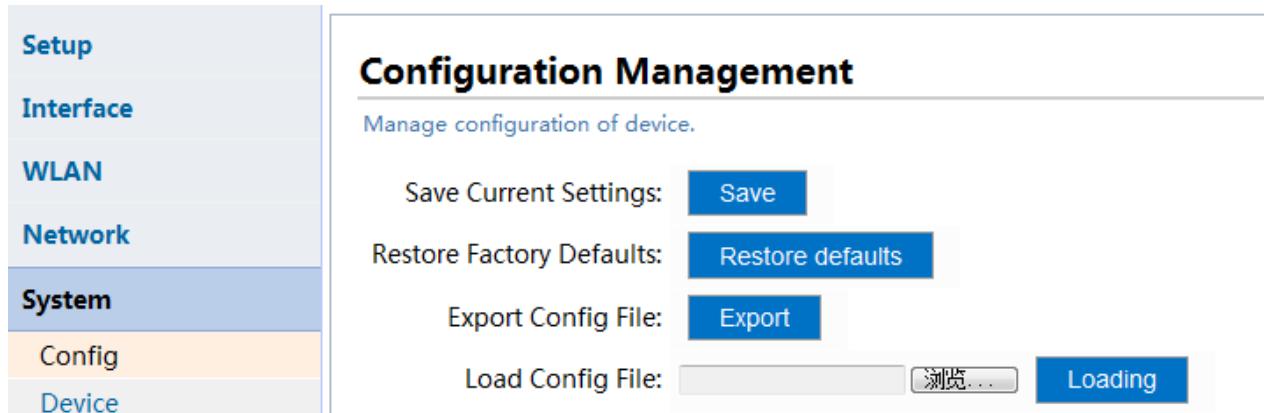


Figure 80 Restore Factory Configuration

Restore factory Configuration: Restore the equipment to factory settings, the default administration address is 192.168.1.1, user name and password is admin.



Note: After restore factory, require to manually restart equipment.

Click “**Restore defaults**”, as shown in the figure below:

Configuration Management

Manage configuration of device.

Save Current Settings:	<input type="button" value="Save"/>	Need restart to apply the config
Restore Factory Defaults:	<input type="button" value="Restore defaults"/>	
Export Config File:	<input type="button" value="Export"/>	
Load Config File:	<input type="text"/> 浏览...	<input type="button" value="Loading"/>

Figure 75 Restore Factory Settings

3.7.3 Reboot or Version Upgrade

Open “System→Device→Reboot/Renew”.

[Setup](#)
[Interface](#)
[WLAN](#)
[Network](#)
System
[Config](#)
[Device](#)

Device Management

Save your devices Configuration parameters, before update firmware or restart,do not cut power while update firmware or restart

Restart Device:	<input type="button" value="Restart"/>
Delay to Restart:	<input type="text"/> Second <input type="button" value="Restart"/>
Cur Device FW Version:	CPE101P07V1.1.2
Update Firmware:	<input type="text"/> 浏览... <input type="button" value="Update"/>

Figure 76 Restart Configuration

Restart : Mainly used to reboot after configuration equipment, and make the configuration effective and maintain equipment performance.

 Note: Power must not be cut off during upgrade.

Device Management

Save your devices Configuration parameters, before update firmware or restart,do not cut power while update firmware or restart

Restart Device:

Figure 77 Upgrade Firmware

3.7.4 User Administration

Open “System→Users”.

The screenshot shows a navigation sidebar on the left with the following menu items: Setup, Interface, WLAN, Network, System, Config, Device, and Users. The 'Users' item is highlighted with a yellow background. The main content area is titled 'Users Management' and contains the text 'advice to change the password of the default account'. Below this is a table with three columns: 'No.', 'Name', and 'Op.' (Operation). The table has one row with the value '1' in the 'No.' column, 'admin' in the 'Name' column, and 'Change' and 'Delete' buttons in the 'Op.' column. At the bottom of the table is a blue 'Add New' button.

Figure 78 User Management

Open "System→Users→Add New".

Users Management

advice to change the password of the default account

No.	Name	Op.
1	admin	Change Delete

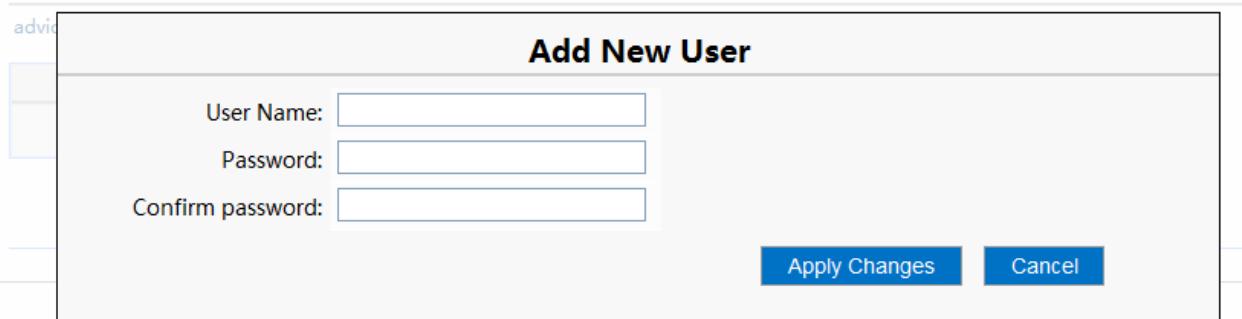
[Add New](#)

Figure 79 New User

New-built: Add new user, it is better to use the combination of number and letter, to ensure user safe.

 **Note:** The default admin account of system is not allowed to delete, but you can modify the password of the account.

Users Management

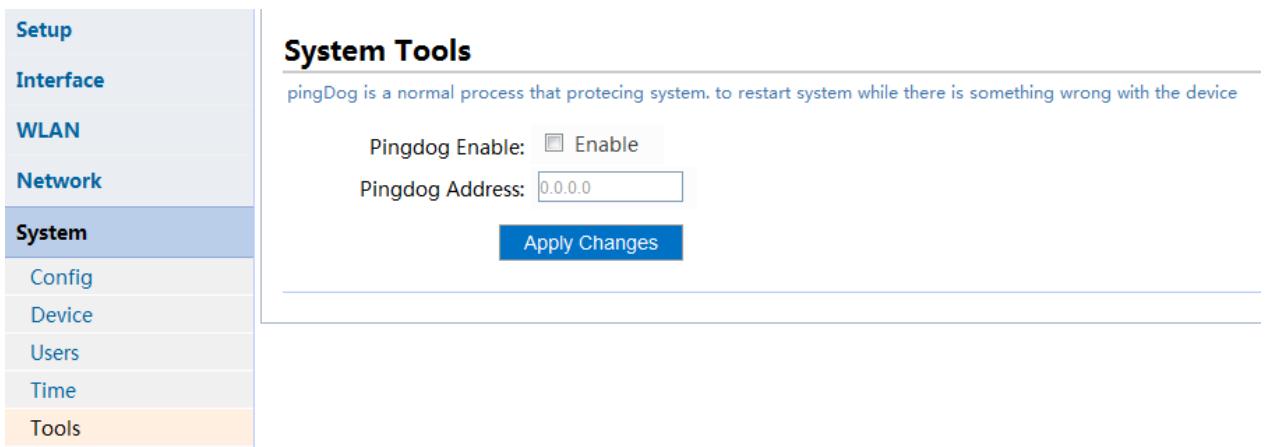


The dialog box is titled "Add New User". It contains three input fields: "User Name", "Password", and "Confirm password". Below the fields are two buttons: "Apply Changes" and "Cancel".

Figure 80 Add New User

3.7.5 System Tool

Open "System→Tool".



The left sidebar shows a navigation menu with the following items: Setup, Interface, WLAN, Network, System (selected), Config, Device, Users, Time, and Tools. The main panel is titled "System Tools". It contains a note: "pingDog is a normal process that protecting system. to restart system while there is something wrong with the device". It has two configuration fields: "Pingdog Enable" (checkbox) and "Pingdog Address" (input field with value "0.0.0.0"). Below the fields is an "Apply Changes" button.

Figure 81 System Tool

Ping dog: When the equipment does not work normally, or there is something wrong with the network, this function helps you reboot automatically. Inputting an IP address (Please ensure this IP address existed and can be pinged.) to start this function, after starting it, this equipment can continuously ping this IP address for 10 times, otherwise, the equipment will automatically reboot.

3.7.6 System Time Settings

Open "System→time".

Device Time Settings

Modify time by use NTP server or get local time, will not to use both at the same time. Please disable NTP before you adjust time by manual!

Current Time: 1970-01-01 00:13

Timezone: (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London

Using NTP: Enable

NTP Server: 210.72.145.44

Date: 2010 - 01 - 01

Time: 00 : 13

Figure 88 Equipment Time Management

After the equipment electric start, the default time is from year 1970. This equipment can get the current time from the network NTP server by NTP function. In current Internet environment, many servers provide NTP service. If this function is opened, you must fill in IP address of NTP server. Meanwhile, since the default time NTP attained is Greenwich time (Time zone 0), you should correctly set up your time zone to ensure an accurate time of your local time zone.

Device Time Settings

Modify time by use NTP server or get local time, will not to use both at the same time. Please disable NTP before you adjust time by manual!

Current Time: 1970-01-01 00:13

Timezone: (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London

Using NTP: Enable

NTP Server: 210.72.145.44

Date: 2010 - 01 - 01

Time: 00 : 13

Figure 89 Equipment Time Management

Browsing time: If NTP server is not available, you can use "Attain browsing time" function, to set your current browser computer time on this equipment.

3.7.7 Administration Interface

Open " System → Administration Interface → Modify main machine name/Equipment number".

Management Settings

Modify hostname, manages device by ssh and telnet.

Hostname: Only support alphabetic and numeric characters

Devicename: Only support alphabetic and numeric characters

NE ID: Only support alphabetic and numeric characters

Location: Only support alphabetic and numeric characters

Longitude: 0 0 0 E

Latitude: 0 0 0 N

Telnet Settings: Enable

SSH Settings: Enable

SNMP Settings: Enable

Trap Server Ip:

Apply Changes

Figure 90 Administration Interface

Open “System→Administration Interface→Open Telnet Configuration/SSH setting”.

Management Settings

Modify hostname, manages device by ssh and telnet.

Hostname: bhuwireless Only support alphabetic and numeric characters

Devicename: bhuwireless Only support alphabetic and numeric characters

NE ID: Only support alphabetic and numeric characters

Location: Only support alphabetic and numeric characters

Longitude: 0 0 0 E

Latitude: 0 0 0 N

Telnet Settings: Enable

SSH Settings: Enable

SNMP Settings: Enable

Trap Server Ip:

Apply Changes

Figure 82 Management Configuration

Main machine name: You can name your own equipment, when you Telnet or SSH to the equipment, you can see the equipment name (optional function).

Telnet Configuration: Open Telnet enabled, stands for allowing other users to log in this equipment in remote distance, and execute the input command, such as telnet 192.168.1.1.

SSH settings: Open SSH enable, when connecting this equipment, encrypt the message transmitted.

3.7.8 System Log

Open "System→System Log".

Log: The log records the running status of this equipment, which help you in solving problems.

Remote log: Open remote log, input IP address of Log server, can read the log record of this IP equipment, but need to ensure the network connection.

show the local logs or transfer to remote logs servers, download flash logs

```

Jan 1 00:00:08 HOSTNAME syslog.info syslogd started: BusyBox v1.19.4
Jan 1 00:00:08 HOSTNAME user.info kernel: Writing ErrCtl register=00000000
Jan 1 00:00:08 HOSTNAME user.info kernel: Readback ErrCtl register=00000000
Jan 1 00:00:08 HOSTNAME user.info kernel: Memory: 29096k/32768k available (2507k kernel code, 3672k reserved, 638k data, 136k init, Ok highmem)
Jan 1 00:00:08 HOSTNAME user.info kernel: NR_IRQS:128
Jan 1 00:00:08 HOSTNAME user.warn kernel: plat_time_init: plat time init done
Jan 1 00:00:08 HOSTNAME user.info kernel: Calibrating delay loop... 267.26 BogoMIPS (lpj=534528)
Jan 1 00:00:08 HOSTNAME user.warn kernel: Mount-cache hash table entries: 512
Jan 1 00:00:08 HOSTNAME user.info kernel: NET: Registered protocol family 16
Jan 1 00:00:08 HOSTNAME user.warn kernel: bio: create slab <bio-0> at 0
Jan 1 00:00:08 HOSTNAME user.notice kernel: SCSI subsystem initialized
Jan 1 00:00:08 HOSTNAME user.info kernel: usbcore: registered new interface driver usbf
Jan 1 00:00:08 HOSTNAME user.info kernel: usbcore: registered new interface driver hub
Jan 1 00:00:08 HOSTNAME user.info kernel: usbcore: registered new device driver usb
Jan 1 00:00:08 HOSTNAME user.info kernel: NET: Registered protocol family 2
Jan 1 00:00:08 HOSTNAME user.info kernel: IP route cache hash table entries: 1024 (order: 0, 4096 bytes)
Jan 1 00:00:08 HOSTNAME user.info kernel: TCP established hash table entries: 1024 (order: 1, 8192 bytes)
Jan 1 00:00:08 HOSTNAME user.info kernel: TCP bind hash table entries: 1024 (order: 0, 4096 bytes)
Jan 1 00:00:08 HOSTNAME user.info kernel: TCP: Hash tables configured (established 1024 bind 1024)

```

Log Level:

Flash Log:

Enable Remote Syslog: Enable

Remote Syslog Server:

Figure 83 Log Management

4 Maintenance Overview

4.1 Common Tools of Maintenance

Table 5

Testing Tool	Assistance Tool	Accessories
Laptop PC	Network cable pliers	Crystal point
Network testing equipment	/ Ethernet	cables

4.2 Maintenance Personnel Requirement

This equipment requires the qualified personnel who has got a certain level of computer knowledge and who has read the user manual, maintenance manual and installation manual.

5 Equipment Check and Troubleshooting

5.1 The correct installation and configuration of BXM2/5 equipment

1. Install and fix BXM2/5 at high place outdoor as requested, as shown in the figure below:

User BXM2 /5 installation is not steady, after long-term wind, the wooden rail become deformed, or BXM2/5 direction is changed, it will reduce the signal receiving capability , which resulted in unnecessary maintenance. Therefore, the antenna direction should be fixed according to signal strength strictly, in our BXM2/5 configuration interface, there are timely signal strength display, the user should adjust the antenna to the best position where can receive the strongest signal.

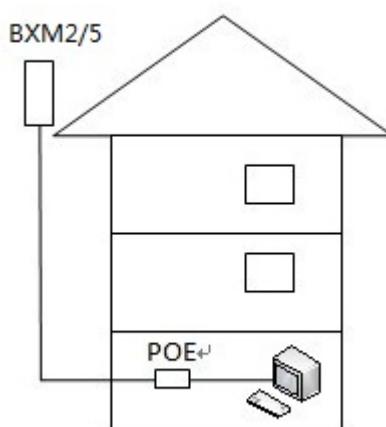


Figure 84 Equipment Installation

2. To ensure that there is no tall and dense buildings or trees around the equipment, so it can receive high-intensity signals. If beyond the available access distance, there are tall and dense buildings or trees, the users will have troubles in maintenance, due to a long distance, the hidden users will reduce the whole network efficiency, as shown in the figure below:



Figure 85 Indicator Panel

The third indicator counted from the left to right is light, and the last three lamps are light stands for AP signal intensity, and the numbers of the last three lamps which are light stands for the intensity of the signal, at this time, it is Station or Repeater mode, if the third lamp counted from the left to the right is not lightening, it is AP mode.

After connecting the power, see if BXM2/5 work indicator is normal, normal status is that WLAN indicator is blinking, PWR indicator keeps light.

3. To identify signal receiving intensity via BXM2/5 system internal para meter, as shown in the figure below:

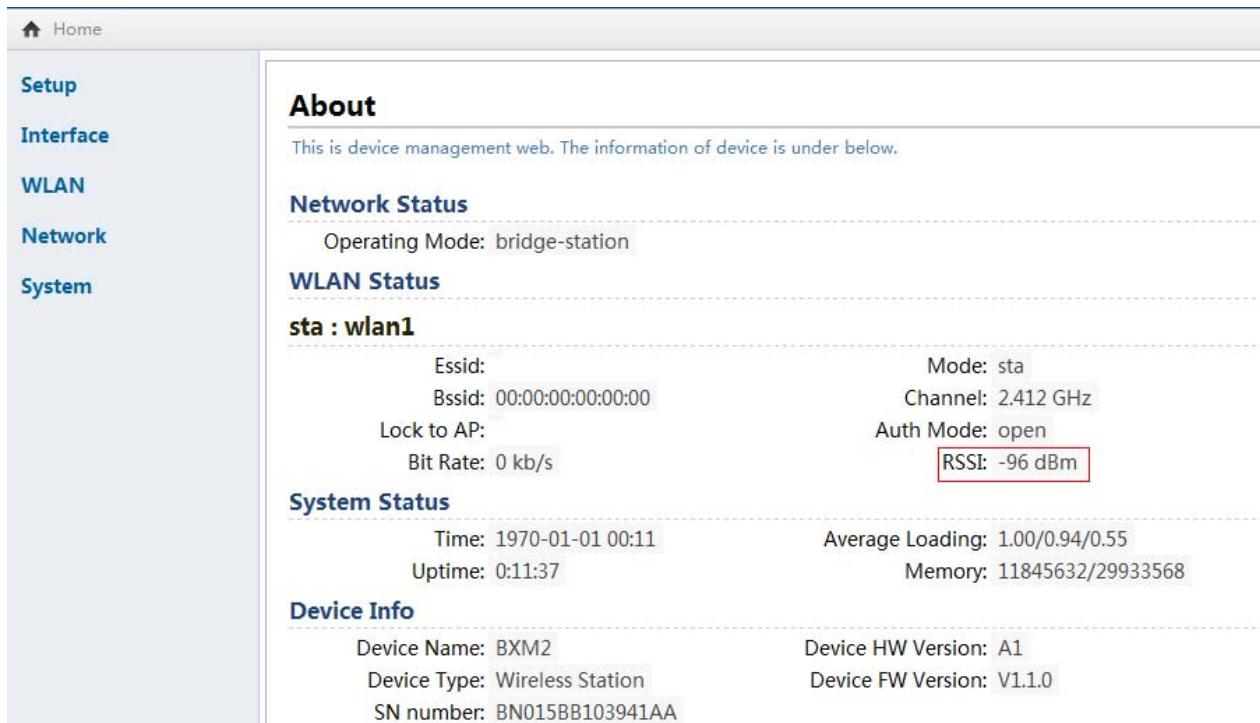


Figure 86 RSSI Receiving Strength

4. Using network test equipment, Ethernet cable should be connected steady, and not too long (no longer than 40 meters), crystal point connection is qualified, and ensure the Ethernet cable can conduct a normal data telecommunication , as shown in the figure below:



Figure 87 Connecting Method



Note: The PoE port of PoE Power Mode connects with the equipment primary port.

The equipment power is supplied by Ethernet cable, so the excessive long cable causes voltage drop, which will result in inadequate power supply and abnormal work. Within 40 meters can ensure a good working status, the crystal point should conform to T568B standard, wrong line order will result in abnormal power supply, and even burn down the equipment or power source.

5. When configure BXM2/5 ensure the PC local connection is opened. Set the PC local connection IP address is 192.168.1.100, ensure BXM2/5 network and PC are in the same network segment, BXM2/5 default IP is 192.168.1.1, default password is admin. Correctly configure IP address as required, as shown in the figure below:

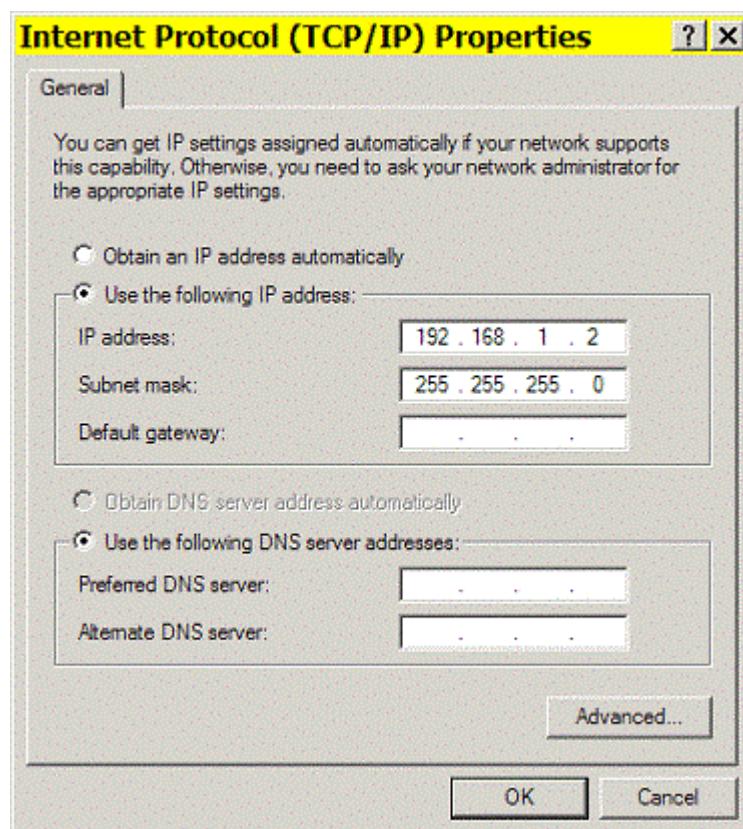


Figure 97 Set IP Address

5.2 Network Checking and Troubleshooting

1. Ensure if the PC address and BXM2/5 network are in same network segment, under cmd, use ipconfig. Use ipconfig command to check IP address status.



Note: If the Client automatically attains the IP Address, use the same command to check if the address is attained.

- a) Check DHCP function is opened or not, and the address is attained or not.
b) Check if automatic configuration is opened, and check it is static configuration or automatically attain.
2. Use Ping command to ensure network smooth. Confirm to open the local TCP/IP, ping 127.0.0.1.

Use Ping command to see if it can reach gateway or not.

If it cannot reach the gateway, to check the local network connection is open or not, if it is forbidden, please open it.

If the gateway still cannot be Pinged, check the correctness of gateway ARP, arp-a, check whether the MAC address is as same as the previous equipment.

3. Eventually check the physical link, check local network connection status, if a red cross appears, it stands for physical link disconnection.

5.3 FAQ and Solutions

1. WLAN Signal strength is too low, which will result in slow network speed and long delay time, make troubleshooting as the following aspects:

- BXM2/5 cannot be visible with AP due to a big shelter, need to adjust the fix direction of BXM2/5.
- Front of BXM2/5 straight on AP, need to adjust BXM2/5 horizontal direction.
- BXM2/5 is fixed on the window, which will result in planar interruption, need to re-select a better position.
- To check the BXM2/5 Tx power is set to the max value.



Note: Please refer to user manual section 3.4.1 RF settings for details.

2. Equipment cannot start-up normally.

- Ethernet cable length connected BXM2/5 and PoE is suggested to be within 40 m.
- Ethernet cable quality cannot reach five forms of IP address standard, it may affect the throughput performance of BXM2/5.
- Ethernet cable crystal point crimping loose causes the wrong line order, need to redo the crystal point.

3. When PC PING the equipment, there are problems of address package loss and long time delay.

- Open terminal isolation function of AP, try to do troubleshooting.
- Do port isolation among APs which linked to the same switch machine.
- Ethernet crystal point does not connect well, need to redo the crystal point.

4. The SSID signal which BXM2/5 has scanned is unstable and with a poor network quality.

- Check equipment signal strength received, adjust equipment position and height, and ensure the equipment receive a stronger signal strength.
- Shift the channel, to avoid the same or adjacent frequency interference.



Note: Please refer to user manual section 3.3.2 WLAN running status for details, RSSI is strong enough or not, ensure over -75dBm.

5. Be unable to dial online (return error code 678).

- If the logical link between Local connection and authentication service disconnect, need to redial.
- Do troubleshooting to the network connection and physical connection.



Note: Please refer to maintenance manual section 2.2 network checkout and troubleshooting for details.

6. The network is always offline and in low network speed.

- Reset the BXM2/5, then to check the network recover to normal status.
- Contact the administrator to make troubleshooting of AP problems.

6 Appendix

6.1 Technical Parameters

Table 6

Item	Description
Port	2 x Ethernet ports of 10/100M
	1 x Main port
	1 x Auxiliary port
	Support PoE Power Supply
Indicator	Power Supply Indicator
	3 level Signal Strength Indicator
	LAN Indicator
Frequency	BXM2: 2.412 - 2.462GHz BXM5: 5.740GHz -5.840GHz
Standard	BXM2:IEEE 802.11b/g/n standard BXM5:IEEE 802.11a/n standard
Tx Power	BXM2:max 25.3dBm(340 mW), adjust software to reach BXM5:max 23.1dBm(210mW), the max, power
Speed Rate	2x2 max, speed rate: 300Mbps
Modulation Technology	802.11n: 2x2 MIMO
Receiving Sensibility	BXM2: 802.11b, 1Mbps: -100dBm 801.11g, 6Mbps: -93dBm 801.11n, MCS0:-93dBm; MCS0:-74dBm
	BXM5: 802.11a, 6Mbps: -95dBm; 54Mbps: -75dBm 801.11n, MCS0: -88dBm; MCS7: -73dBm
Antenna	BXM2:dual-polarization 11dBi, horizontal beam 65°, vertical beam 30°. BXM5: dual-polarization 16dBi, horizontal beam 60°, vertical beam 15°.
Reset/Resume factory value	Support

Item	Description
Memory	BXM2:32MB BXM5:64MB
FLASH 8MB	
Size (Length x width x height)	265mm x89mm x 61mm
Input Voltage	Support wide voltage input: 9-24V
Power Consumption	≤8W
Protection Level	IP66
Work Temperature	-40°C~+65°C
Storage Temperature	-40°C~+80°C
Work Humidity	0~100%

Table 7

Item	Description
Software Characteristics	
Work Mode	Router mode, Client replaces all terminal authentication
	Bridge mode, all terminal need separate authentication;
Network Protocol	PPTP、L2TP、IPSec
	PPPoE
	DHCP Client/Server
	NAPT
	NTP
Wireless Function	Ambient station monitor/Channel Scan
	Prior AP connection setting(Banding SSID)
	Automatic channel selection function
Safety Strategy	Encrypted: WEP,TKIP,AES

Item	Description
Security	Wireless Safety
	Open System, Shared key-gen
	WPA/WPA-PSK
	WPA2/WPA2-PSK
	802.1x(PEAP,TLS,TTLS)
	WAPI
	Authentication function:
	Support WEB account/password 、 PPPoE connection authentication mode
	Support Router Mode, PPPoE client replaces all terminal authentication
Bridge mode, all terminal need separate authentication	
	Support multi-user to conduct separate port authentication
Network Protection	Firewall
	Support network speed limit function
	Based on MAC address access control
System Service	Support virtual DMZ, Port Forwarding
	Support UPnP automatic port reflection
	Support VPN transparent sending(PPTP、L2TP、IPSec)
WDS Available	
Configuration Management	Based on WEB management tool, CPE inner-built WEB server
	Remote firmware upgrade (HTTP)
	Support TELNET Connection

Item	Description
	Support syslog running system
	Support SSH service function
Trouble shooting	Automatically test network status, connect the link automatically after disconnection
	Support WatchDog and PingDog function

6.2 Glossary

Table 8

No.	Abbreviation	Full Name
1.	airX	airX
2.	CPE	Customer Premise Equipment
3.	WLAN	Wireless Local Area Networks
4.	WAN	Wide Area Network
5.	LAN	Local Area Network
6.	PoE	Power Over Ethernet
7.	AP	Access Point
8.	SSID	Service Set Identifier
9.	ESSID	Expand Service Set Identifier
10.	DHCP	Dynamic Host Configuration Protocol
11.	MAC	Media Access Control
12.	DNS	Domain Name System
13.	PPP	Point-to-Point Protocol
14.	PPPoE	Point-to-Point Protocol over Ethernet
15.	WiFi	wireless fidelity
16.	AMPDU	Aggregation MAC Protocol Data Unit
17.	VAP	Virtual Access Point
18.	WDS	Wireless Distribution System
19.	DTIM	Delivery Traffic Indication Message
20.	WMM	Wi-Fi Multimedia
21.	RTS/CTS	Request To Send/Clear To Send
22.	QOS	Quality of Service
23.	DMZ	Demilitarized Zone
24.	VoIP	Voice over Internet Protocol

No.	Abbreviation	Full Name
25.	NAT	Network Address Translation
26.	PPTP	Point to Point Tunneling Protocol
27.	L2TP	Layer 2 Tunneling Protocol
28.	IPSec	Internet Protocol Security
29.	IKE	Internet Key Exchange
30.	uPnp	Universal Plug and Play
31.	NTP	Network Time Protocol
32.	Ping	Packet Internet Groper
33.	FTP	File Transfer Protocol
34.	HTTP	Hypertext Transport Protocol
35.	VPN	Virtual Private Network
36.	SSH	Secure Shell
37.	WAPI	Wireless LAN Authentication and Privacy Infrastructure
38.	ipv4	Internet Protocol Version 4
39.	ipv6	Internet Protocol Version 6
40.	WPA	Wi-Fi Protected Access
41.	WPA-PSK	Wi-Fi Protected Access -Pre-Shared Key
42.	WPA2-PSK	Wi-Fi Protected Access -Pre-Shared Key
43.	WPA-EAP	Wi-Fi Protected Access-Extensible-Authentication-Protocol
44.	WPA2-EAP	Wi-Fi Protected Access -Pre-Shared Key
45.	WEP	Wired Equivalent Privacy

FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC RF Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. End users follow the specific operating instructions for satisfying RF exposure compliance. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.