



---

***ZigBee™- Integrated Wireless Smart Home Controller***

---

# **User Manual**

**Integrated Wireless Smart Home Controller**

**Model: Z206**

20150304

For firmware V0.0.0.25 and later

# Table of Contents

<b>1. Introduction.....</b>	<b>3</b>
<b>2. Product Appearance.....</b>	<b>4</b>
<b>3. Specification.....</b>	<b>5</b>
<b>4. Installation and Preparation.....</b>	<b>6</b>
4-1. Installation Diagram.....	6
4-2. Power on Z206.....	6
4-3. Reboot Z206.....	6
4-4. Reset Z206.....	6
4-5. Permit-Join.....	7
4-6. WPS.....	7
4-7. Indicators.....	7
4-8. UPS Backup Power.....	7
<b>5. Setting up Z206.....</b>	<b>9</b>
5-1. Enter Into the Login Page.....	9
5-2. View the Status of Z206.....	13
5-3. Internet Settings.....	16
5-4. Wi-Fi Settings.....	21
5-5. Firewall Settings.....	25
5-6. Administration.....	27
<b>6. Setting up ZigBee Smart Home.....</b>	<b>30</b>
6-1. Device List.....	31
6-2. Device Management.....	32
6-3. Initiate Smart Home.....	33
6-4. User Management.....	35

6-5. Data Management.....	36
6-6. Import Data.....	36
6-7. Communication Setting.....	37
<b>7. Important Maintenance Instructions.....</b>	<b>38</b>

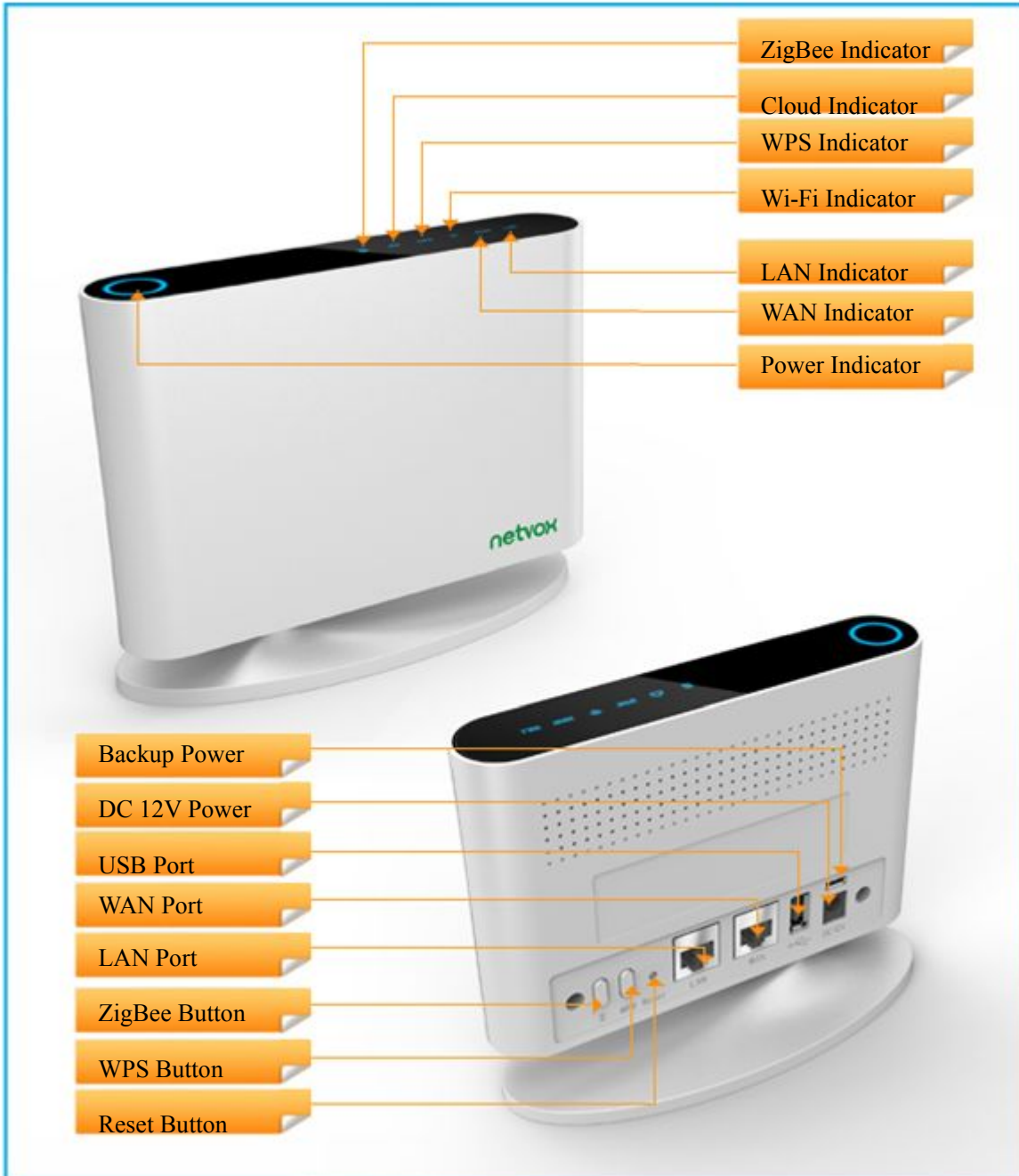
## 1. Introduction

Netvox Z206, a Cloud-Based Wireless Smart Home Controller (CWSH), acts as a Coordinator in ZigBee network. Z206 is also equipped with Wi-Fi technology. It is the main character of Netvox Smart Home Cloud Platform. Z206 provides Cloud services, Wi-Fi connection, and ZigBee network communication. Via Wi-Fi connection, users are able to control the ZigBee network devices through mobile app. Furthermore, Netvox Smart Home Cloud service allows users to remotely manage the devices, like lighting, curtain, or IP Camera, anytime and anywhere.

### *What is ZigBee?*

ZigBee is a short range wireless transmission technology based on IEEE802.15.4 standard and supports multiple network topologies such as point-to-point, point-to-multipoint, and mesh networks. It is defined for a general-purpose, cost-effective, low-power-consumption, low-data-rate, and easy-to-install wireless solution for industrial control, embedded sensing, medical data collection, smoke and intruder warning, building automation and home automation, etc.

## 2. Product Appearance



### 3. Specification

- ZigBee: fully IEEE 802.15.4 compliant (ZigBee Pro); utilizes 2.4GHz ISM band; up to 16 channels
- Wi-Fi: IEEE 802.11 b/g/n; channel 1~11
- 2 x RJ-45 ports: WAN x 1; LAN x 1
- Power supply: DC 12V
- Up to 210 meters ZigBee transmission range in non-obstacle space
- Up to 250 meters Wi-Fi transmission range in non-obstacle space
- Bluetooth dongle supported
- Internet of Things
- Cloud services
- Easy installation and configuration

## 4. Installation and Preparation

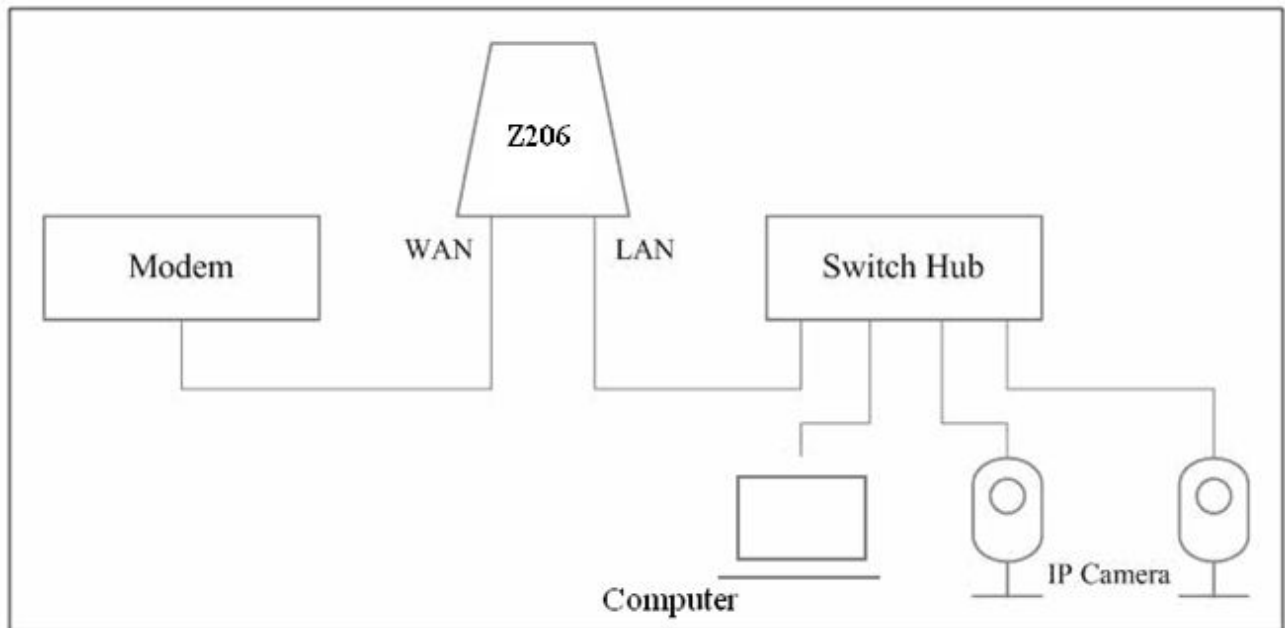
### 4-1. Installation Diagram

Step1. Connect the Internet connection to the WAN port.

Step2. Connect the computer/IP Camera to the LAN port.

(Please connect the LAN port and the computers/IP cameras to a switch when users would like to use more computers/IP cameras.)

The installation diagram is as below:



### 4-2. Power on Z206

Power on Z206 using 110V~220V AC to 12V DC/1.5A power adapter. The power indicator will stay on.

### 4-3. Reboot Z206

To reboot Z206, press the *Reset Button* while Z206 is powered on.

### 4-4. Reset Z206

To reset Z206, press and hold the *Reset Button* for 5 seconds while Z206 is powered on.

#### 4-5. Permit-Join

To allow other devices to join the ZigBee network, users could enable the Permit-Join feature using the steps:

- A. Press the *ZigBee Button* **once** to enable the Permit-Join feature.
- B. The default Permit-Join period of time is 60 seconds.

#### 4-6. WPS

To enable the WPS feature:

- A. Press the *WPS Button* **once** to enable the WPS feature.
- B. Enable to WPS function of the Wi-Fi device such as mobile phone to establish the Wi-Fi connection.
- C. The default Permit-Join period of time is 3 minutes.

#### 4-7. Indicators

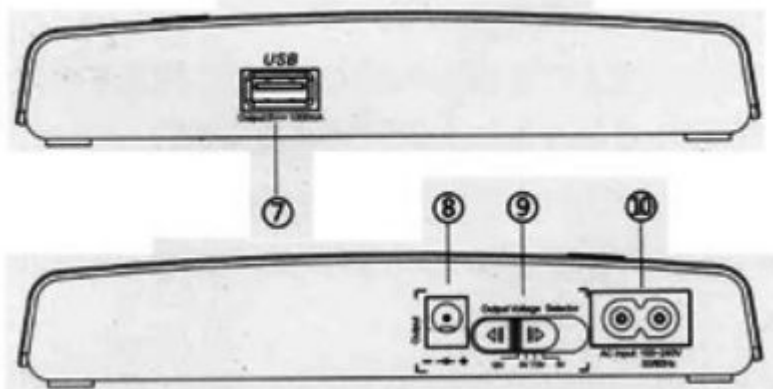
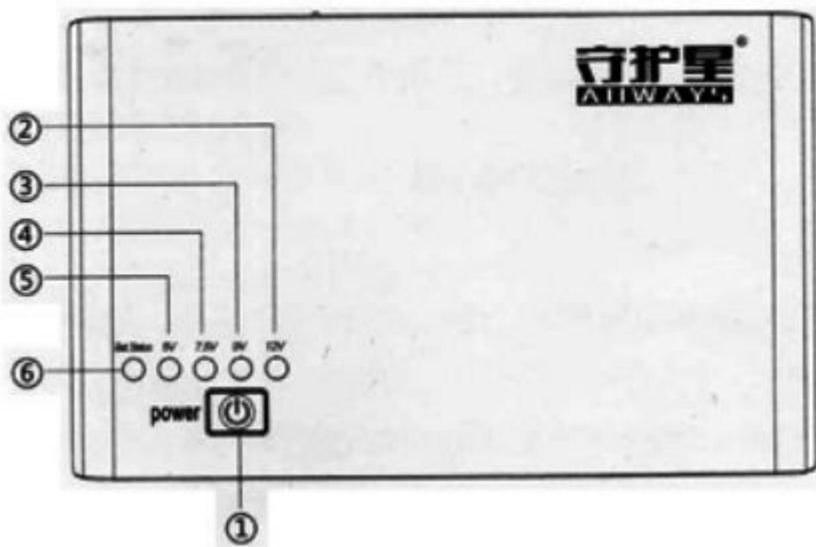
- A. Power Indicator: Stay On when power-on. Stay Off when power-off.
- B. ZigBee Indicator
- C. Cloud Indicator
- D. WPS Indicator: Start flashing when WPS is enabled. Stay On when WPS connection is established.  
Stay Off when WPS is disabled.

#### 4-8. UPS Backup Power

The recommended backup power:

- A. Brand: Foshan Unipower Electronic
- B. Model: ECO net 212
- C. Capacity: 4400mAh
- D. Power Input: 100V-240V AC
- E. Power Output: 12V 1A





## 5. Setting up Z206

### 5-1. Enter Into the Login Page

Connect the computer to the LAN port of Netvox Z206 using a RJ-45 cable.

(Windows XP)

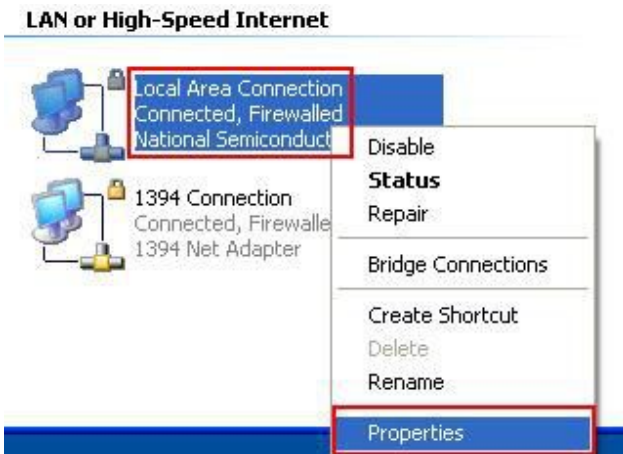
Click Start.



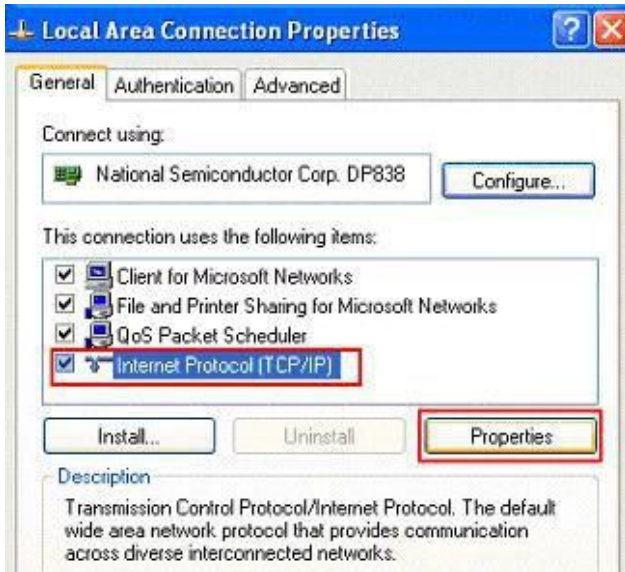
Click Network Connections.



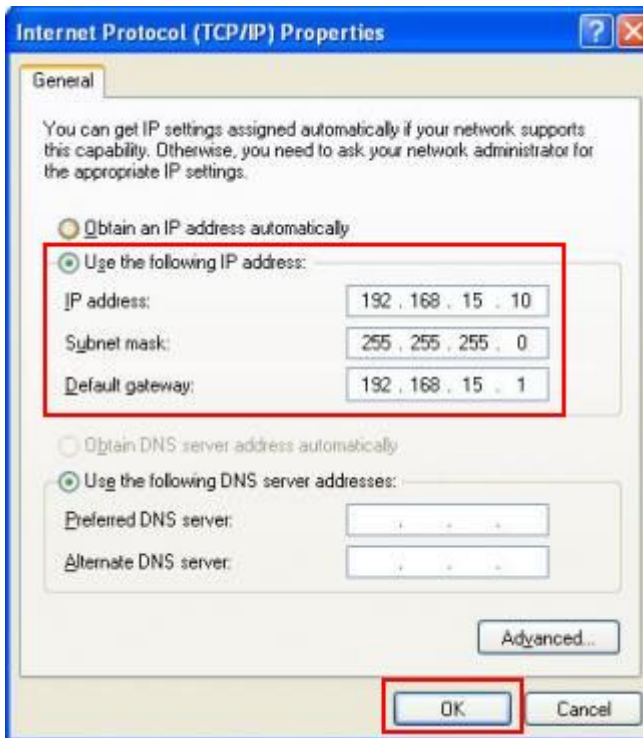
Right-click on the Local Area Network, and then click Properties.



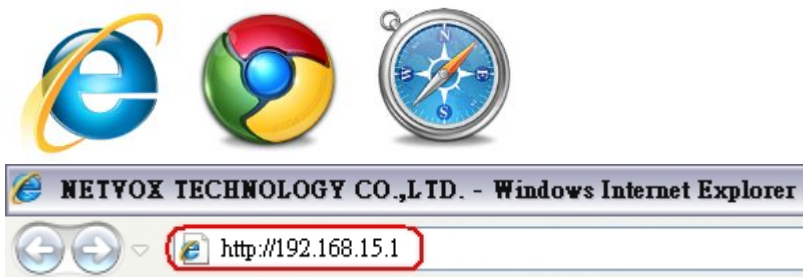
Click Internet Protocol (TCP/IP), and then click Properties.

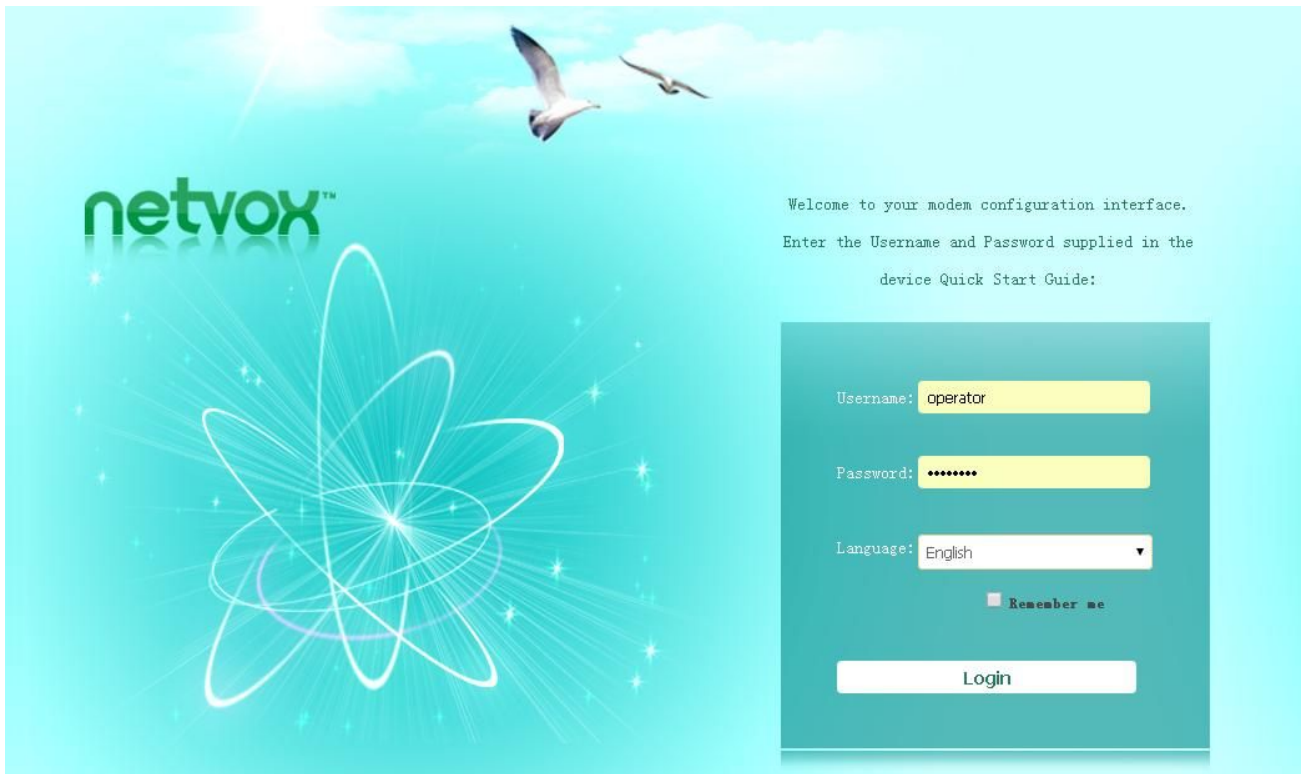


Key in the IP address and subnet mask as below.



Open the web browser and enter <http://192.168.15.1> to go into the login page.





Key in the Username & Password (default: admin/ admin) and login the management system.

<b>Username</b>	<input type="text" value="admin"/>
<b>Password</b>	<input type="password" value="*****"/>
	<input type="button" value="Login"/>

For advanced settings, please use **operator/ operator**.

<b>Username</b>	<input type="text" value="operator"/>
<b>Password</b>	<input type="password" value="*****"/>
	<input type="button" value="Login"/>



- Status
- Statistic
- Management
- Setup Wizard
- Operation Mode

Access Point Status

★ System Info

SDK Version	0.2.0.10 (Apr 16 2015)
System Up Time	1 day, 22 hours, 53 mins, 44 secs
System Platform	Netvox Z206 Smart Home Controller
Operation Mode	Gateway Mode

★ Internet Configurations

Connected Type	DHCP
WAN IP Address	192.168.1.197
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
Primary Domain Name Server	168.95.1.1
Secondary Domain Name Server	168.95.1.1
MAC Address	00:13:7A:00:04:9A

## 5-2. View the Status of Z206

Click **Status** to enter into the status page.

The screenshot shows the Netvox web interface. At the top, there is a navigation bar with the Netvox logo and several menu items: Status, Internet Settings, Wireless Settings, Firewall, Administration, and Smart Home. The 'Status' menu item is highlighted with a red box. Below the navigation bar, there is a sidebar with a list of menu items: Status, Statistic, Management, Setup Wizard, and Operation Mode. The main content area is titled 'Access Point Status' and contains two sections: 'System Info' and 'Internet Configurations'. The 'System Info' section includes fields for SDK Version (0.2.0.10), System Up Time (1 day, 22 hours, 53 mins, 44 secs), System Platform (Netvox Z206 Smart Home Controller), and Operation Mode (Gateway Mode). The 'Internet Configurations' section includes fields for Connected Type (DHCP), WAN IP Address (192.168.1.197), Subnet Mask (255.255.255.0), Default Gateway (192.168.1.254), Primary Domain Name Server (168.95.1.1), Secondary Domain Name Server (168.95.1.1), and MAC Address (00:13:7A:00:04:9A).

**A. Status:** To view the access point status.

The screenshot shows the Netvox web interface. At the top, there is a navigation bar with the Netvox logo and several menu items: Status, Internet Settings, Wireless Settings, Firewall, Administration, and Smart Home. The 'Status' menu item is highlighted with a red box. Below the navigation bar, there is a sidebar with a list of menu items: Status, Statistic, Management, Setup Wizard, and Operation Mode. The main content area is titled 'Access Point Status' and contains three sections: 'System Info', 'Internet Configurations', and 'Local Network'. The 'System Info' section includes fields for SDK Version (0.2.0.10), System Up Time (1 day, 23 hours, 7 mins, 38 secs), System Platform (Netvox Z206 Smart Home Controller), and Operation Mode (Gateway Mode). The 'Internet Configurations' section includes fields for Connected Type (DHCP), WAN IP Address (192.168.1.197), Subnet Mask (255.255.255.0), Default Gateway (192.168.1.254), Primary Domain Name Server (168.95.1.1), Secondary Domain Name Server (168.95.1.1), and MAC Address (00:13:7A:00:04:9A). The 'Local Network' section includes fields for Local IP Address (192.168.26.1) and Local Subnet Mask (255.255.255.0).

**B. Statistic:** To view the statistic data.

**Statistic**

★ **Memory**

Memory total:	124868 kB
Memory left:	58560 kB

★ **WAN/LAN**

WAN Rx packets:	1785065
WAN Rx bytes:	1115612204
WAN Tx packets:	540038
WAN Tx bytes:	77154447
LAN Rx packets:	718035
LAN Rx bytes:	59794857
LAN Tx packets:	1071235
LAN Tx bytes:	1078993642

★ **All interfaces**

Name	lo
Rx Packet	124686

**C. Management:** For basic system management.

**System Management**

▼ **User permission setting**

Account	admin
Password	*****
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

▼ **Administrator permission setting**

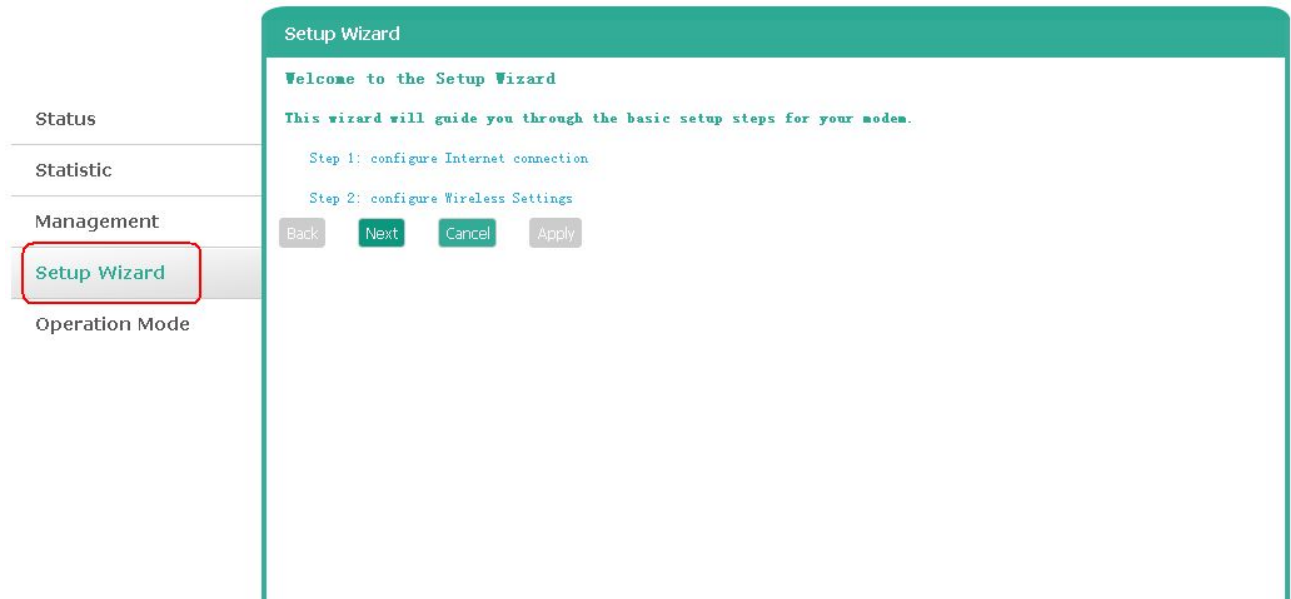
Account	operator
Password	*****
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

▼ **NTP Settings**

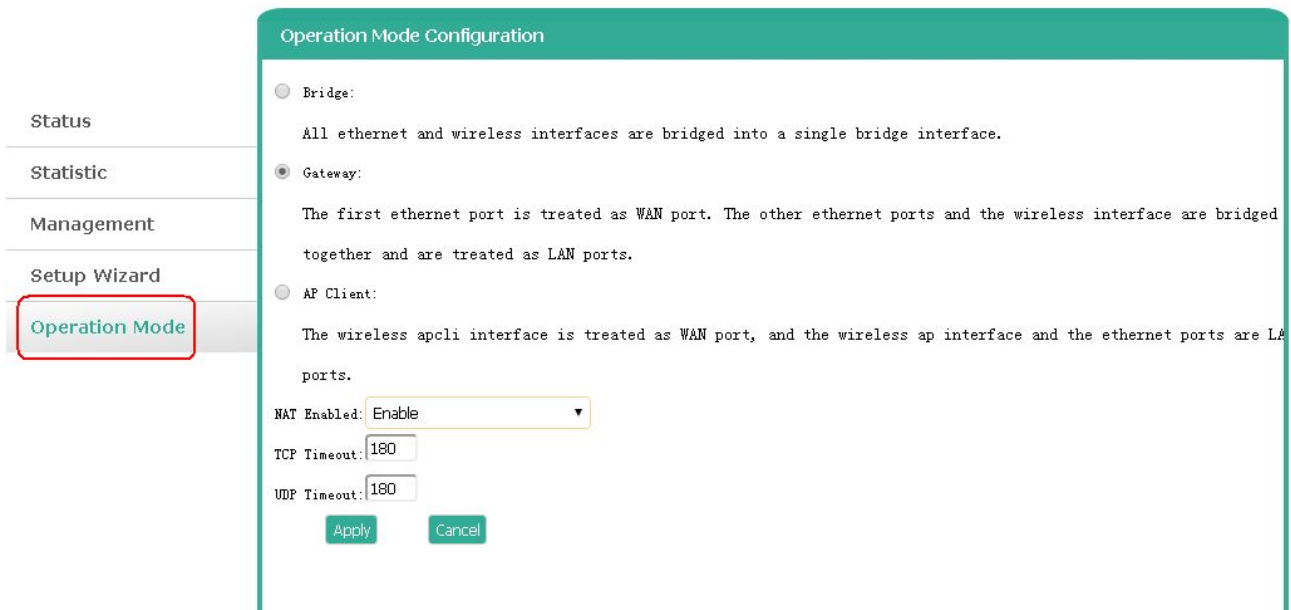
NTP	Enable
Current Time	Tue May 26 14:31:19 GMT 201 <input type="button" value="Sync with host"/>
Time Zone:	(GMT+08:00) Taipei
NTP Server	time.stdtime.gov.tw

ex: time.nist.gov  
ntp0.broad.mit.edu  
time.stdtime.gov.tw

**D. Setup Wizard:** For quick setup.



**E. Operation Mode:** To configure the operation mode.



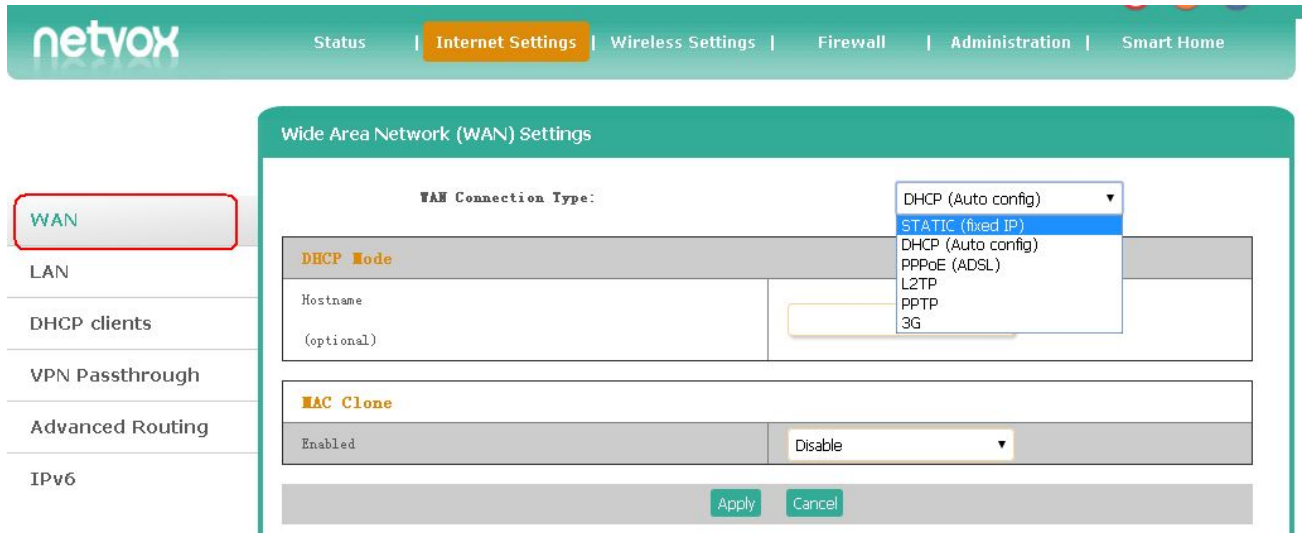


### 5-3. Internet Settings

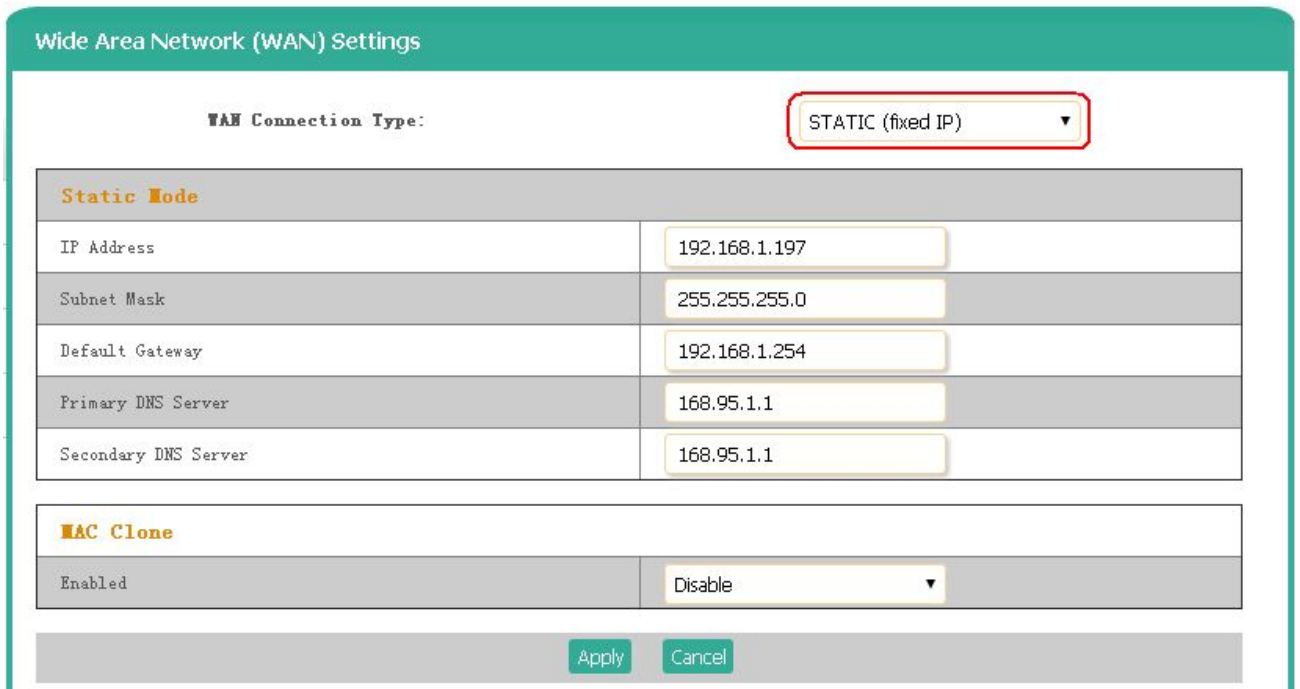
Click **Internet Settings** to enter into the Internet setting page.



**A. WAN Settings:** Setup the WAN connection.



i. Static (fixed IP): Enter the IP address, subnet mask, default gateway, and DNS server which ISP (Internet Service Provider) provided.



ii. DHCP: Request IP addresses and networking parameters automatically.

Wide Area Network (WAN) Settings

WAN Connection Type: DHCP (Auto config) ▼

DHCP Mode	
Hostname (optional)	<input type="text"/>

MAC Clone	
Enabled	Disable ▼

Apply Cancel

iii. PPPoE (ADSL): Enter the PPPoE data which ISP (Internet Service Provider) provided when necessary.

Wide Area Network (WAN) Settings

WAN Connection Type: PPPoE (ADSL) ▼

PPPoE Mode	
User Name	<input type="text" value="pppoe_user"/>
Password	<input type="password" value="....."/>
Verify Password	<input type="password" value="....."/>
Operation Mode	Keep Alive ▼
	Keep Alive Mode: Redial Period <input type="text" value="60"/> seconds
	On demand Mode: Idle Time <input type="text" value="5"/> minutes

MAC Clone	
Enabled	Disable ▼

Apply Cancel

iv. L2TP: Enter the L2TP data for VPN connection.

Wide Area Network (WAN) Settings

WAN Connection Type: L2TP

L2TP Mode	
Server IP	<input type="text" value="l2tp_server"/>
User Name	<input type="text" value="l2tp_user"/>
Password	<input type="password" value="*****"/>
Address Mode	<span>Static</span> ▼
IP Address	<input type="text" value="192.168.1.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text" value="192.168.1.254"/>
Operation Mode	<span>Keep Alive</span> ▼
	Keep Alive Mode: Redial Period <input type="text" value="60"/> seconds

MAC Clone	
Enabled	<span>Disable</span> ▼

v. PPTP: Enter the PPTP data for VPN connection.

Wide Area Network (WAN) Settings

WAN Connection Type: PPTP

PPTP Mode	
Server IP	<input type="text" value="pptp_server"/>
User Name	<input type="text" value="pptp_user"/>
Password	<input type="password" value="*****"/>
Address Mode	<span>Static</span> ▼
IP Address	<input type="text" value="192.168.1.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text" value="192.168.1.254"/>
Operation Mode	<span>Keep Alive</span> ▼
	Keep Alive Mode: Redial Period <input type="text" value="60"/> seconds

MAC Clone	
Enabled	<span>Disable</span> ▼

**B. LAN Settings:** Setup the LAN connection.

WAN

LAN

DHCP clients

VPN Passthrough

Advanced Routing

IPv6

### Local Area Network (LAN) Settings

**LAN Setup**

Hostname	Z206
IP Address	192.168.15.1
Subnet Mask	255.255.255.0
LAN 2	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
LAN2 IP Address	<input type="text"/>
LAN2 Subnet Mask	<input type="text"/>
MAC Address	00:13:7A:00:04:9B
DHCP Type	Server ▼
Start IP Address	192.168.15.100
End IP Address	192.168.15.200
Subnet Mask	255.255.255.0
Primary DNS Server	168.95.1.1
Secondary DNS Server	8.8.8.8
Default Gateway	192.168.15.1

**C. DHCP Clients:** List the DHCP clients.

WAN

LAN

DHCP clients

VPN Passthrough

Advanced Routing

IPv6

### DHCP Client List

**DHCP Clients**

Hostname	MAC Address	IP Address	Expires in
android-fb2265f21404a34e	50:cc:f8:1f:44:c3	192.168.26.149	23:19:18
android-2463340007e2192f	b4:52:7e:79:36:64	192.168.26.171	19:50:27
android-1219fa8e67b8b63d	78:24:af:ac:8a:d2	192.168.26.189	20:11:29
android-4565a2de64b8b431	78:24:af:b0:d8:46	192.168.26.177	21:04:53
*	00:e0:4c:81:96:c1	192.168.26.103	21:18:51
android-21a4a25f67c7f5a3	b4:52:7e:8f:d7:b9	192.168.26.115	22:46:54
android-4b4634c1d89b7f45	00:ee:bd:83:0f:02	192.168.26.111	18:02:28
*	e8:ab:fa:47:8f:12	192.168.26.102	13:11:58

**D. VPN Passthrough:** VPN passthrough setting.

WAN

LAN

DHCP clients

VPN Passthrough

Advanced Routing

IPv6

### VPN Passthrough

**VPN Pass Through**

L2TP Passthrough	Enable ▼
IPSec Passthrough	Enable ▼
PPTP Passthrough	Enable ▼

19

**E. Advanced Routing:** Routing rules setting.

WAN  
LAN  
DHCP clients  
VPN Passthrough  
**Advanced Routing**  
IPv6

### Static Routing Settings

**Add a routing rule**

Destination	<input type="text"/>
Range	Host <input type="text"/>
Gateway	<input type="text"/>
Interface	LAN <input type="text"/>
Comment	<input type="text"/>

**Current Routing table in the system:**

No.	Destination	Netmask	Gateway	Flags	Metric	Ref	Use	Interface	Comment
1	255.255.255.255	255.255.255.255	0.0.0.0	5	0	0	0	LAN (br0)	
2	239.255.255.250	255.255.255.255	0.0.0.0	5	0	0	0	LAN (br0)	
3	192.168.1.0	255.255.255.0	0.0.0.0	1	0	0	0	WAN (eth2.2)	
4	192.168.26.0	255.255.255.0	0.0.0.0	1	0	0	0	LAN (br0)	
5	0.0.0.0	0.0.0.0	192.168.1.254	3	1	0	0	WAN (eth2.2)	

**F. IPv6:** IPv6 connection setting.

WAN  
LAN  
DHCP clients  
VPN Passthrough  
Advanced Routing  
**IPv6**

### IPv6

**IPv6 Connection Type**

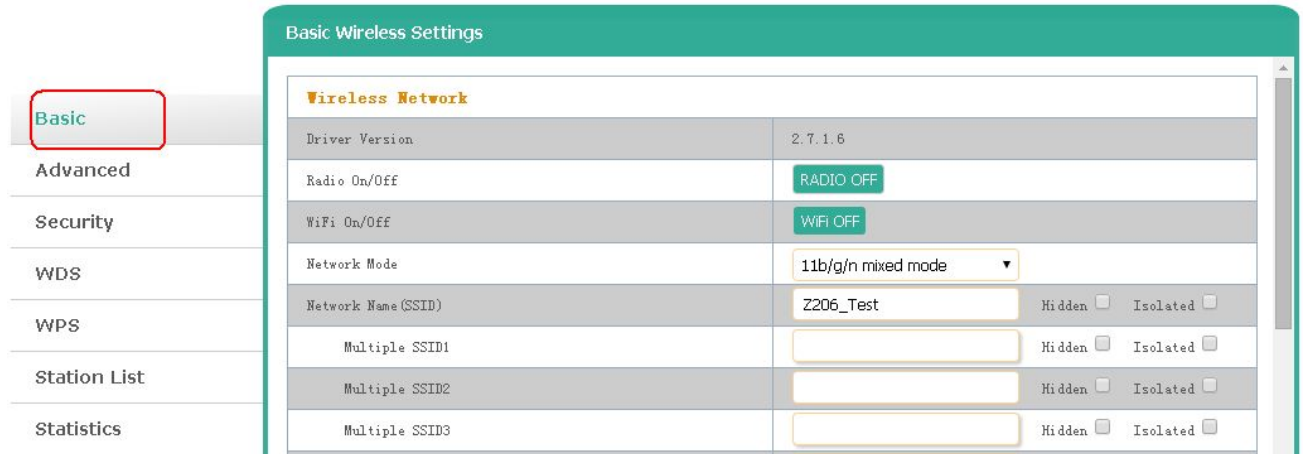
IPv6 Operation Mode	Disable <input type="text"/>
---------------------	------------------------------

## 5-4. Wi-Fi Settings

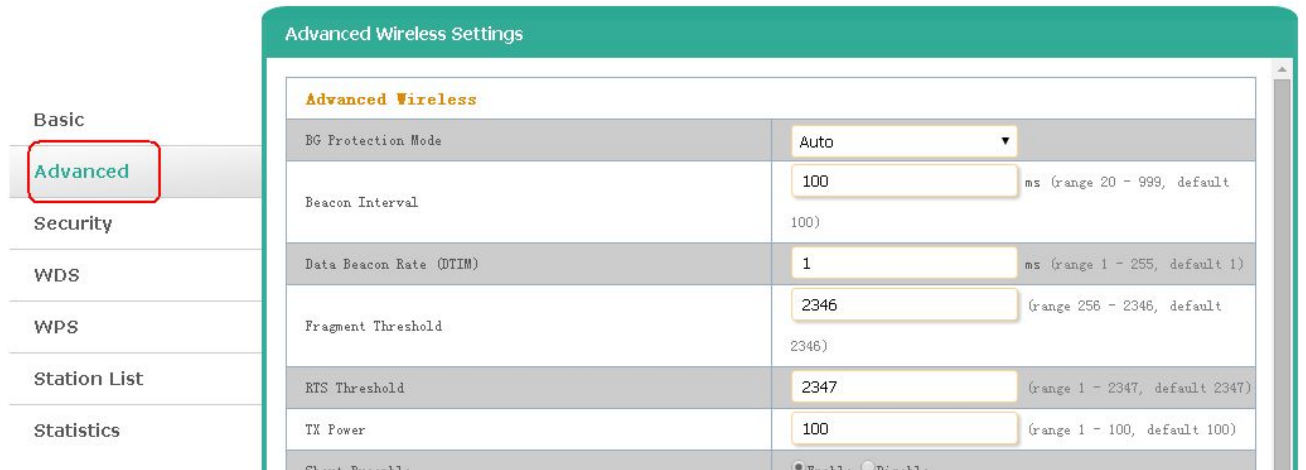
Click **Wireless Settings** to enter into the Wi-Fi setting page.



**A. Basic:** Basic settings of Wi-Fi such as Wi-Fi name (SSID) or Wi-Fi channel.



**B. Advanced:** Advanced settings of Wi-Fi such as beacon interval, Wi-Fi multimedia, or multicast-to-unicast converter.



**C. Security:** Wi-Fi security settings. It is recommended to choose WPA2-PSK for Security Mode, and the Wi-Fi password Pass Phrase should be at least 8 letters/numbers.

Basic	<h3>Wireless Security/Encryption Settings</h3> <p><b>Select SSID</b></p> <table border="1"><tr><td>SSID choice</td><td>Z206_Test</td></tr></table> <p><b>"Z206_Test"</b></p> <table border="1"><tr><td>Security Mode</td><td>WPA2-PSK</td></tr></table> <p><b>WPA</b></p> <table border="1"><tr><td>WPA Algorithms</td><td><input type="radio"/> TKIP <input checked="" type="radio"/> AES <input type="radio"/> TKIPAES</td></tr><tr><td>Pass Phrase</td><td>12345678</td></tr><tr><td>Key Renewal Interval</td><td>3600 seconds (0 ~ 4194303)</td></tr></table> <p><b>Access Policy</b></p> <table border="1"><tr><td>Policy</td><td>Disable</td></tr><tr><td>Add a station Mac:</td><td></td></tr></table> <p>Apply Cancel</p>	SSID choice	Z206_Test	Security Mode	WPA2-PSK	WPA Algorithms	<input type="radio"/> TKIP <input checked="" type="radio"/> AES <input type="radio"/> TKIPAES	Pass Phrase	12345678	Key Renewal Interval	3600 seconds (0 ~ 4194303)	Policy	Disable	Add a station Mac:	
SSID choice		Z206_Test													
Security Mode		WPA2-PSK													
WPA Algorithms		<input type="radio"/> TKIP <input checked="" type="radio"/> AES <input type="radio"/> TKIPAES													
Pass Phrase		12345678													
Key Renewal Interval		3600 seconds (0 ~ 4194303)													
Policy		Disable													
Add a station Mac:															
Advanced															
<b>Security</b>															
WDS															
WPS															
Station List															
Statistics															

**D. WDS:** WDS setting.

Basic	<h3>Wireless Distribution System(WDS)</h3> <p><b>Wireless Distribution System(WDS)</b></p> <table border="1"><tr><td>WDS Mode</td><td>Disable</td></tr></table> <p>Apply Cancel</p>	WDS Mode	Disable
WDS Mode		Disable	
Advanced			
Security			
<b>WDS</b>			
WPS			
Station List			
Statistics			

**E. WPS: WPS setting.**

**Wi-Fi Protected Setup**

**WPS Config**

WPS: Enable

**WPS Summary**

WPS Current Status:	Idle
WPS Configured:	Yes
WPS SSID:	Z206_Test
WPS Auth Mode:	WPA2-PSK
WPS Encryp Type:	AES
WPS Default Key Index:	2
WPS Key (ASCII)	8862654878
AP PIN:	00011808 <input type="button" value="Generate"/>

**F. Station List: List the Wi-Fi users.**

**Station List**

**Wireless Network**

MAC Address	Aid	PSM	MimoPS	MCS	BW	SGI	STBC
E8:AB:FA:47:8F:12	1	0	3	7	40M	0	0
B4:52:7E:8F:D7:B9	2	1	3	7	20M	0	1
50:CC:F8:1F:44:C3	3	1	3	7	20M	0	0
00:EE:BD:83:0F:02	5	1	3	7	20M	0	1



**G. Statistics:** Showing the statistics of Tx & Rx.

Basic

Advanced

Security

WDS

WPS

Station List

**Statistics**

### Statistics

Transmit Statistics	
Tx Success	3342416
Tx Retry Count	326775, PER=9.0%
Tx Fail after retry	2475, PLR=7.4e-04
RTS Successfully Receive CTS	0
RTS Fail To Receive CTS	0

Receive Statistics	
Frames Received Successfully	3516748
Frames Received With CRC Error	7030622, PER=86.7%

SNR	
SNR	11, 21, n/a

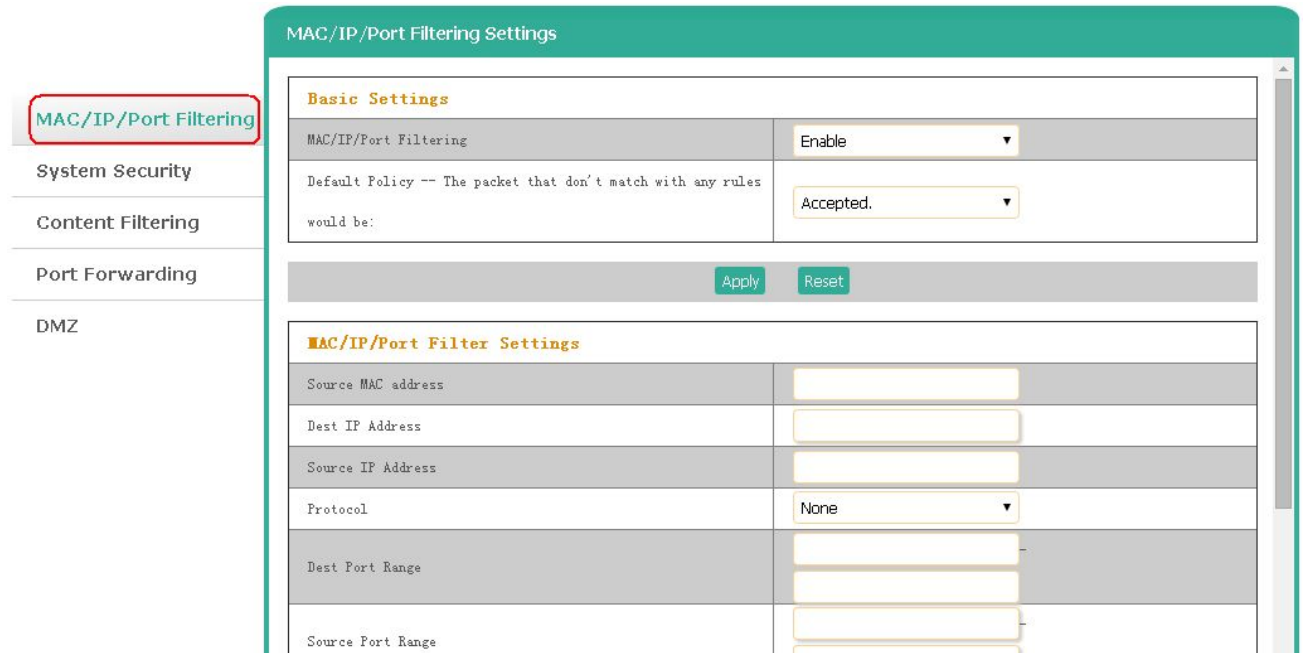
Reset Counters

## 5-5. Firewall Settings

Click **Firewall** to enter into the firewall setting page.



### A. MAC/IP/Port Filtering: MAC/IP/Port filtering setting.



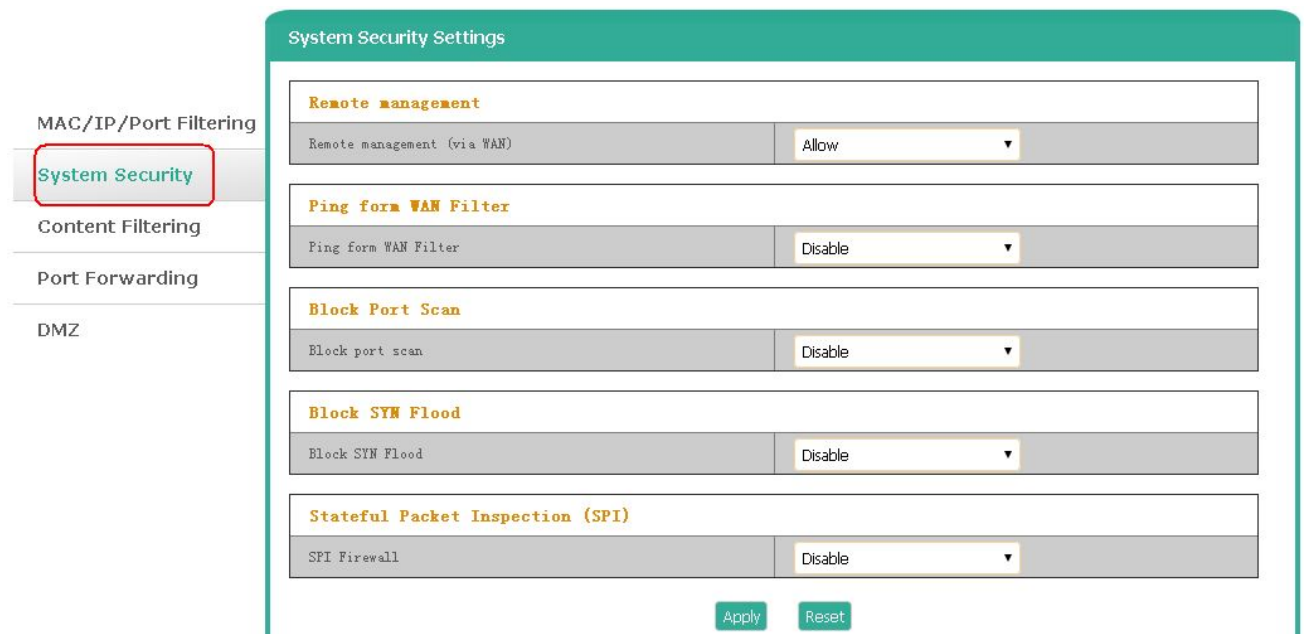
The screenshot shows the 'MAC/IP/Port Filtering Settings' page. The left sidebar has 'MAC/IP/Port Filtering' highlighted in red. The main content area is divided into two sections: 'Basic Settings' and 'MAC/IP/Port Filter Settings'. The 'Basic Settings' section includes 'MAC/IP/Port Filtering' (set to 'Enable') and 'Default Policy' (set to 'Accepted'). The 'MAC/IP/Port Filter Settings' section includes fields for 'Source MAC address', 'Dest IP Address', 'Source IP Address', 'Protocol' (set to 'None'), 'Dest Port Range', and 'Source Port Range'. There are 'Apply' and 'Reset' buttons at the bottom of each section.

Basic Settings	
MAC/IP/Port Filtering	Enable
Default Policy -- The packet that don't match with any rules would be:	Accepted.

MAC/IP/Port Filter Settings	
Source MAC address	
Dest IP Address	
Source IP Address	
Protocol	None
Dest Port Range	
Source Port Range	

### B. System Security: System security setting.



The screenshot shows the 'System Security Settings' page. The left sidebar has 'System Security' highlighted in red. The main content area is divided into five sections: 'Remote management', 'Ping form WAN Filter', 'Block Port Scan', 'Block SYN Flood', and 'Stateful Packet Inspection (SPI)'. Each section has a single setting with a dropdown menu. The 'Remote management (via WAN)' is set to 'Allow', while the others are set to 'Disable'. There are 'Apply' and 'Reset' buttons at the bottom.

Remote management	
Remote management (via WAN)	Allow

Ping form WAN Filter	
Ping form WAN Filter	Disable

Block Port Scan	
Block port scan	Disable

Block SYN Flood	
Block SYN Flood	Disable

Stateful Packet Inspection (SPI)	
SPI Firewall	Disable

**C. Content Filtering:** Filtering URL or web contents.

**Content Filter Settings**

**Webs Content Filter**

Filters:  Proxy  Java  ActiveX

Apply Reset

**Webs URL Filter Settings**

**Current Webs URL Filters:**

No.	URL

Delete Reset

**Add a URL filter:**

URL:

Add Reset

**D. Port Forwarding:** Port forwarding/virtual server setting.

**Virtual Server Settings**

**Port Forwarding**

Port Forwarding: Enable

IP Address:

Port Range:

Protocol: TCP&UDP

Comment:

(The maximum rule count is 32.)

Apply Reset

**Current Port Forwarding in system:**

No.	IP Address	Port Range	Protocol	Comment

Delete Selected Reset

**E. DMZ:** DMZ setting.

**DMZ Settings**

**DMZ Settings**

DMZ Settings: Disable

DMZ Address:

Except TCP port 80

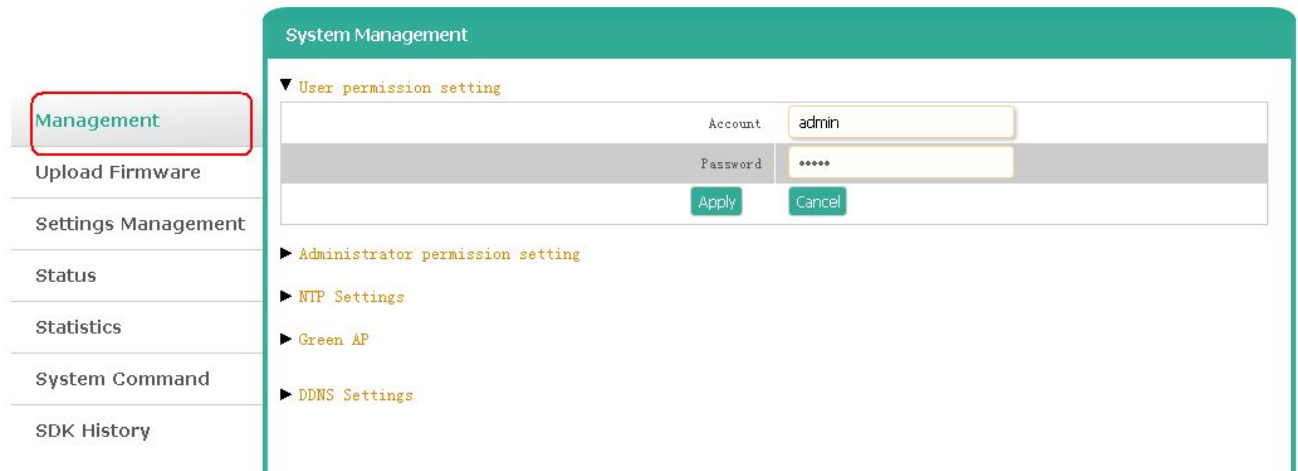
Apply Reset

## 5-6. Administration

Click **Administration** to enter into the system management page.



**A. Management:** System settings such as user permission or green AP.



**B. Upload Firmware:** Firmware update.



**C. Settings Management:** To save/load the settings or reset to factory settings

**Settings Management**

**Export Settings**

Export Button	Export
---------------	--------

**Import Settings**

Settings file location	選擇檔案 未選擇任何檔案
------------------------	--------------

Import Cancel

**Reset to factory default**

Reset to factory default	Reset to factory default
--------------------------	--------------------------

**D. Status:** To view the access point status.

**Access Point Status**

★ **System Info**

SDK Version	0.2.0.10 (Apr 16 2015)
System Up Time	3 days, 1 hour, 27 mins, 42 secs
System Platform	Netvox Z206 Smart Home Controller
Operation Mode	Gateway Mode

★ **Internet Configurations**

Connected Type	DHCP
WAN IP Address	192.168.1.197
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
Primary Domain Name Server	168.95.1.1
Secondary Domain Name Server	168.95.1.1
MAC Address	00:13:7A:00:04:9A

**E. Statistics:** To view the statistic data.

**Statistic**

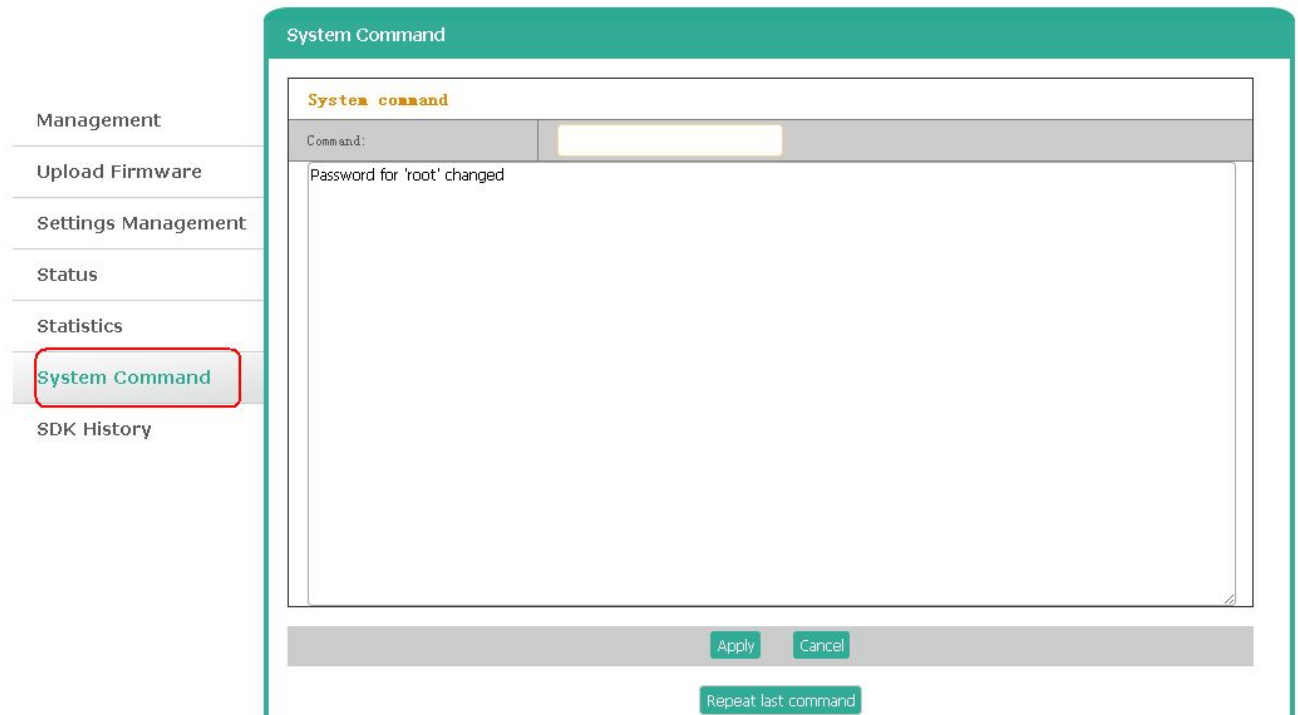
★ **Memory**

Memory total:	124868 kB
Memory left:	55944 kB

★ **WAN/LAN**

WAN Rx packets:	2966565
WAN Rx bytes:	1763118428
WAN Tx packets:	994189
WAN Tx bytes:	132825495
LAN Rx packets:	1191170

**F. System Command:** To send the system commands.



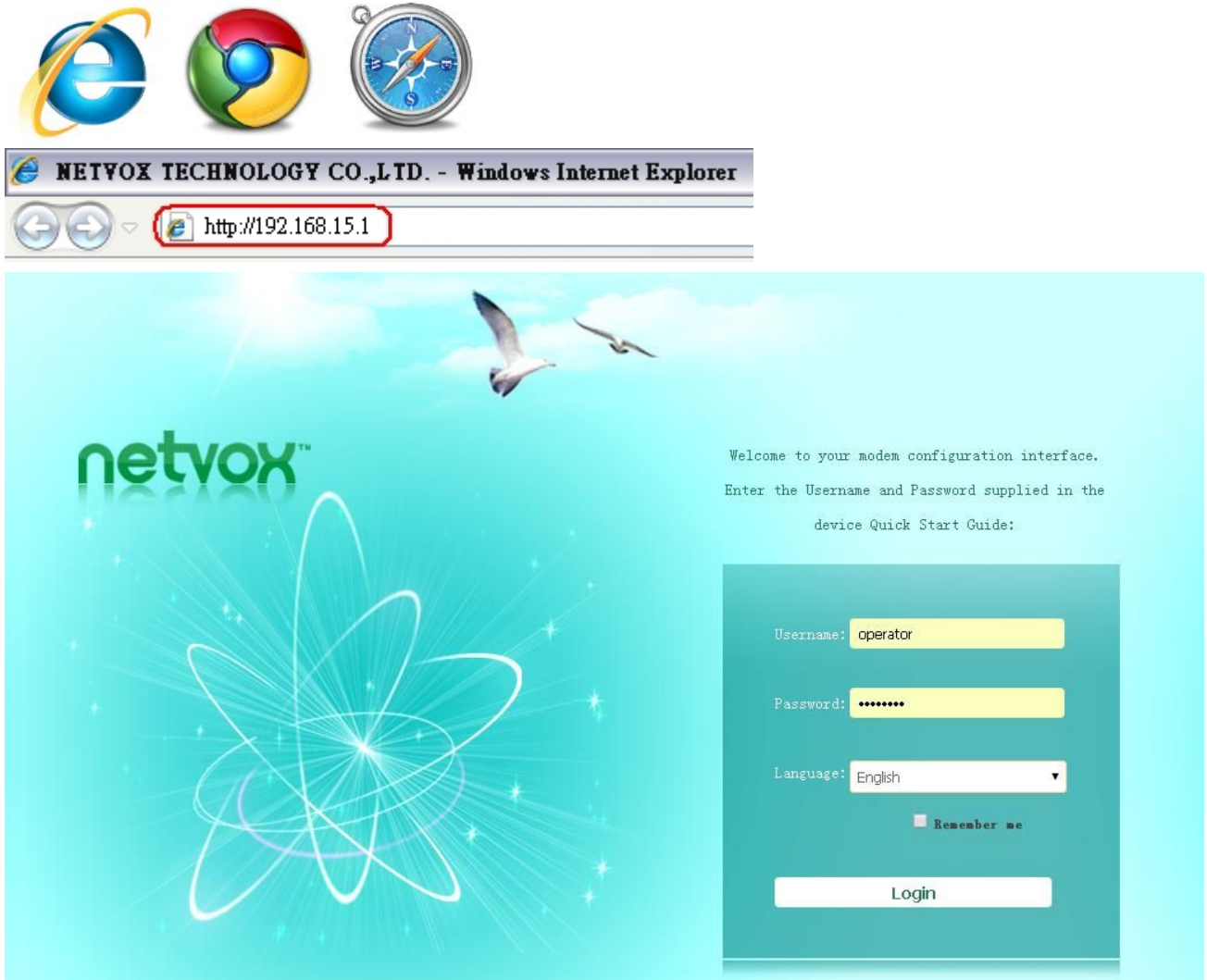
**G. SDK History:** To view the SDK history.



## 6. Setting up ZigBee Smart Home

Connect the computer to the LAN port of Netvox Z206 using a RJ-45 cable.

Open the web browser and enter <http://192.168.15.1> to go into the login page.



Key in the Username & Password (**for advanced settings, please use operator/ operator**) and login the management system.

Username

Password

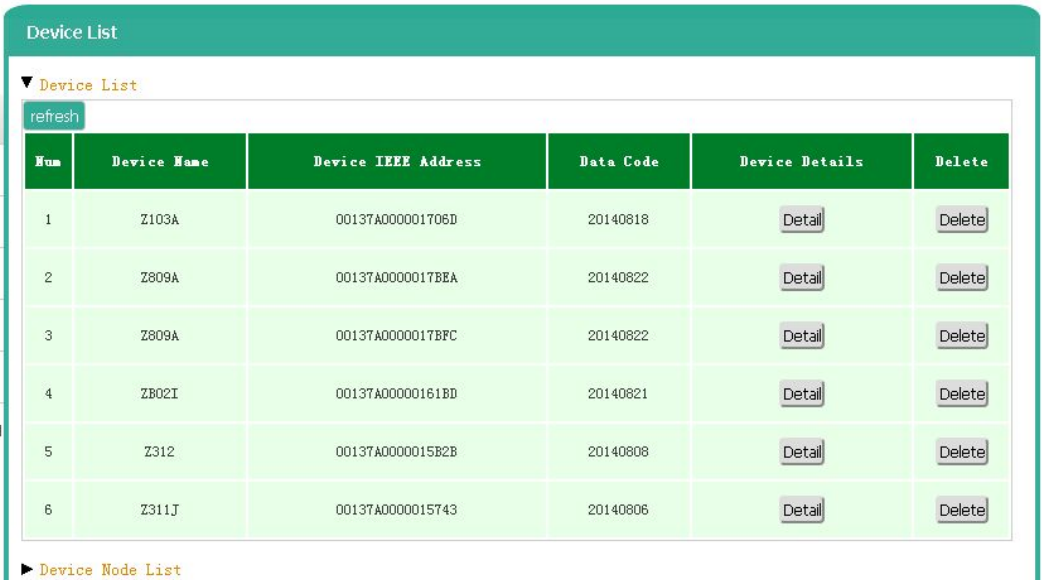
Login

Click **Smart Home** to enter into the smart home page.



## 6-1. Device List

To list the device data such as IEEE address, End Point, Data Code, or detailed information. For the first-time use, please power one/wake up all of the devices, and then refresh the list.



The screenshot displays a web interface for managing devices. On the left is a navigation menu with the following items: Device List (highlighted with a red box), Device Management, Initiate Smart Home, User Management, Data Management, Import Data, and Communication Setting. The main content area is titled "Device List" and features a "refresh" button above a table. The table has the following data:

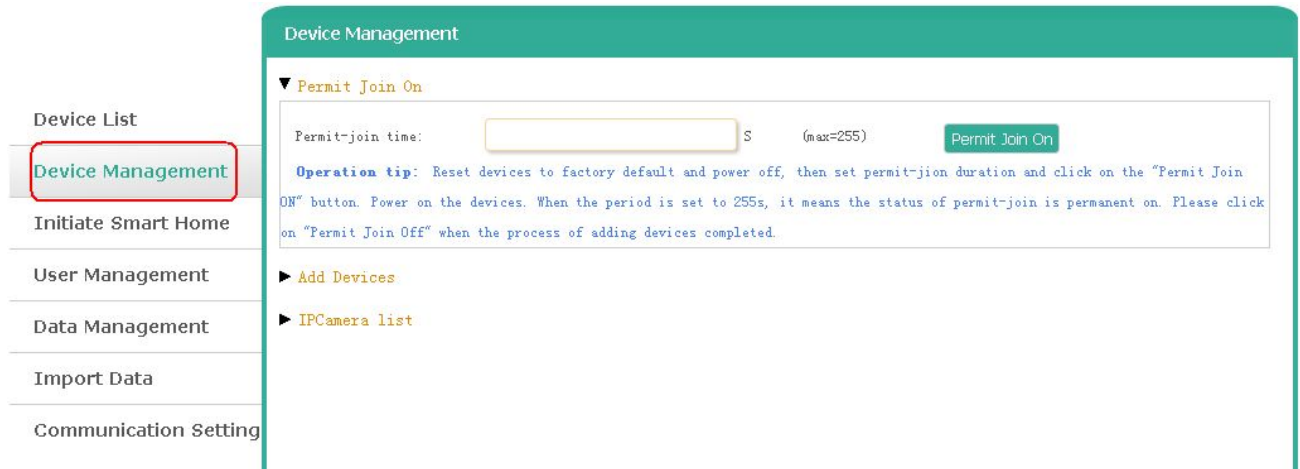
Num	Device Name	Device IEEE Address	Data Code	Device Details	Delete
1	Z103A	00137A000001706D	20140818	<a href="#">Detail</a>	<a href="#">Delete</a>
2	Z809A	00137A0000017BBA	20140822	<a href="#">Detail</a>	<a href="#">Delete</a>
3	Z809A	00137A0000017BFC	20140822	<a href="#">Detail</a>	<a href="#">Delete</a>
4	ZB02I	00137A00000161BD	20140821	<a href="#">Detail</a>	<a href="#">Delete</a>
5	Z312	00137A0000015B2B	20140808	<a href="#">Detail</a>	<a href="#">Delete</a>
6	Z311J	00137A0000015743	20140806	<a href="#">Detail</a>	<a href="#">Delete</a>

Below the table, there is a link for "Device Node List".



## 6-2. Device Management

To turn on Permit-Join feature, add devices, or manage IP camera.

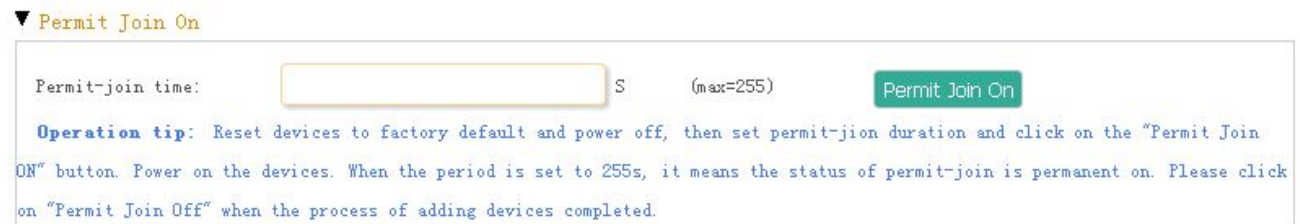


The screenshot shows the 'Device Management' interface. On the left is a sidebar menu with options: Device List, Device Management (highlighted with a red box), Initiate Smart Home, User Management, Data Management, Import Data, and Communication Setting. The main content area is titled 'Device Management' and contains a section for 'Permit Join On'. This section includes a text input field for 'Permit-join time' with a unit 'S' and a '(max=255)' label, followed by a green 'Permit Join On' button. Below this is an 'Operation tip' in blue text: 'Reset devices to factory default and power off, then set permit-jion duration and click on the "Permit Join ON" button. Power on the devices. When the period is set to 255s, it means the status of permit-join is permanent on. Please click on "Permit Join Off" when the process of adding devices completed.' Underneath the tip are two expandable sections: 'Add Devices' and 'IPCamera list'.

### A. Permit-Join On

To add new devices to the network, we need to turn the Permit-Join feature on. After turning on Permit-Join, power on the devices users would like to add into the network.

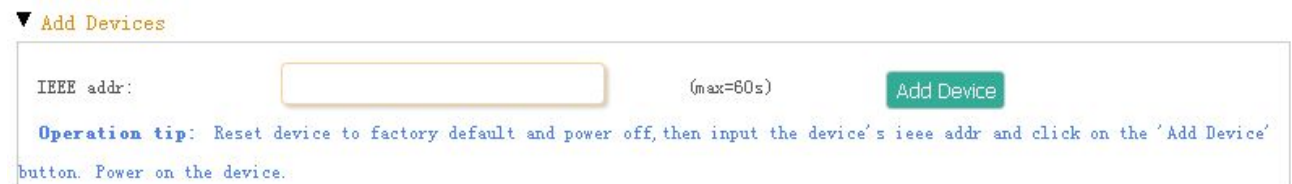
Note: Permit-Join time is 255 → Permit-Join feature is always on.



This is a detailed view of the 'Permit Join On' section. It features a text input field for 'Permit-join time' with a unit 'S' and a '(max=255)' label, followed by a green 'Permit Join On' button. Below the input is an 'Operation tip' in blue text: 'Reset devices to factory default and power off, then set permit-jion duration and click on the "Permit Join ON" button. Power on the devices. When the period is set to 255s, it means the status of permit-join is permanent on. Please click on "Permit Join Off" when the process of adding devices completed.'

### B. Add Devices

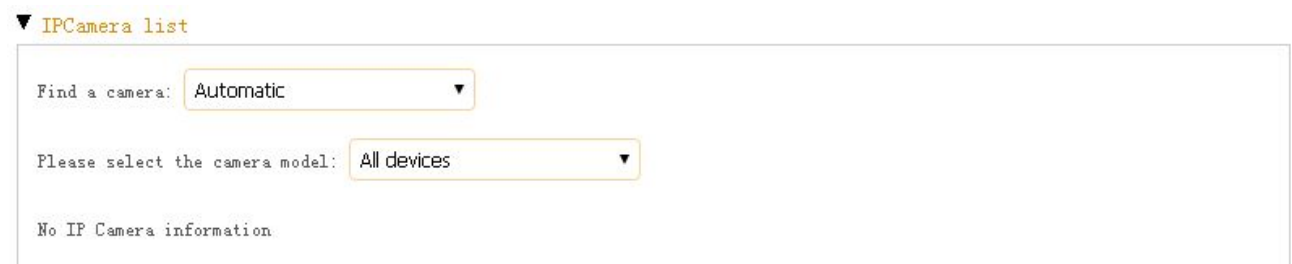
Users could also add the devices manually using device's IEEE number.



This is a detailed view of the 'Add Devices' section. It features a text input field for 'IEEE addr:' with a '(max=60s)' label, followed by a green 'Add Device' button. Below the input is an 'Operation tip' in blue text: 'Reset device to factory default and power off, then input the device's ieee addr and click on the "Add Device" button. Power on the device.'

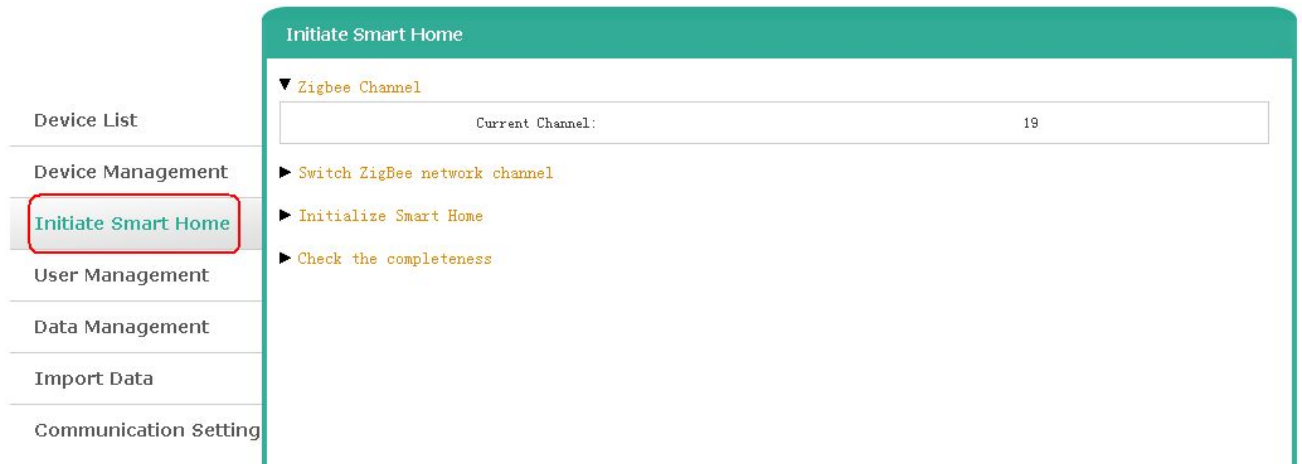
### C. IPCamera List

To manage the IP camera.



This is a detailed view of the 'IPCamera list' section. It features two dropdown menus: 'Find a camera:' with 'Automatic' selected, and 'Please select the camera model:' with 'All devices' selected. Below the dropdowns, the text 'No IP Camera information' is displayed.

## 6-3. Initiate Smart Home



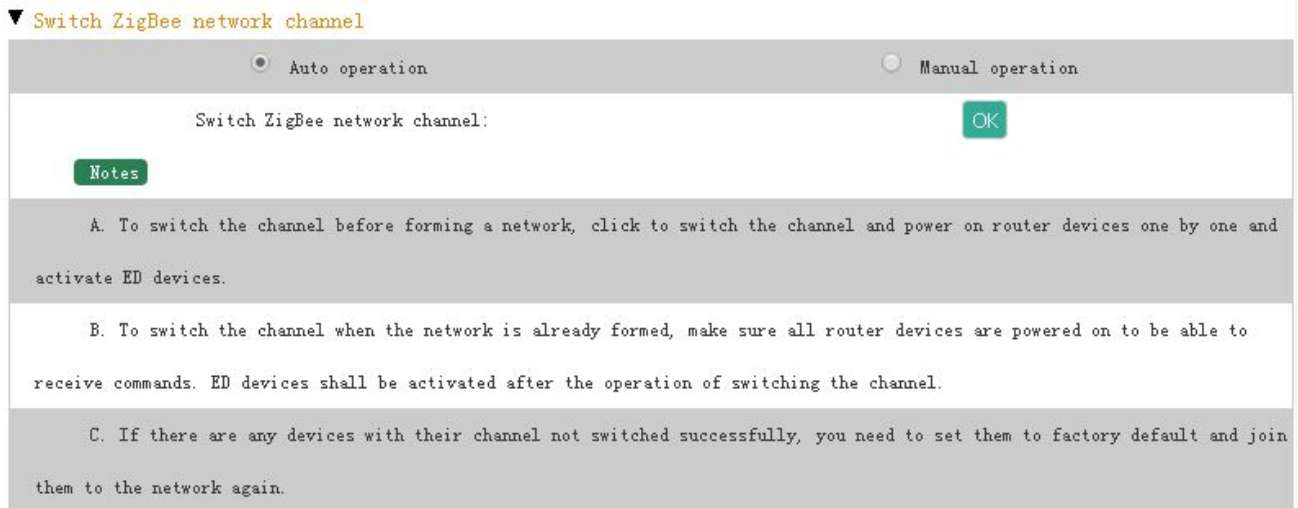
### A. ZigBee Channel

The ZigBee channel Z206 is using.



### B. Switch ZigBee Network Channel

- To change the ZigBee channel, please make sure the Wi-Fi signal is good.
- Please activate the End Devices before switching the ZigBee channel.



### C. Initialize Smart Home

After building up or re-building a ZigBee network, please initialize the ZigBee network.

#### ▼ Initialize Smart Home

Please select devices to be initi. ▼ Initialize Smart Home

**Operation tip:** Click to initialize the configuration of the network. Do not use it unless needed.

Group and scene created successfully.

### D. Check the Completeness

Users are able to check the completeness of the network. It will list the problem of the network.

#### ▼ Check the completeness

Check the completeness: Check the completeness

## 6-4. User Management

The screenshot shows a web interface for User Management. On the left is a sidebar menu with options: Device List, Device Management, Initiate Smart Home, User Management (highlighted with a red box), Data Management, Import Data, and Communication Setting. The main content area has a teal header 'User Management' and a dropdown menu 'User Management' with an 'add' button. Below is a table with columns: User Name, Status, reset password, and Delete. The table contains one row for 'shcadmin' with status 'Normal' and 'Unlock' buttons, a 'Reset' button, and a 'Delete' button. Below the table is a 'Verification Code' section.

### A. User Management

To add user, please click **Add**.

This close-up shows the 'User Management' dropdown menu with the 'add' button highlighted by a red box. Below it is the table with columns: User Name, Status, reset password, and Delete. The row for 'shcadmin' shows 'Normal' status with 'Unlock' and 'Reset' buttons, and a 'Delete' button.

To create a new user profile, please key in the Username, Password, Confirm Password, and Verification Code. To acquire Verification Code, please refer to the next section.

The screenshot shows a form for adding a new user. It has a 'back' button and four input fields: 'User Name' (with placeholder 'Please input the user name' and note '(Please input 4-16 letters or numbers)'), 'password' (with note '(Please input 6-16 letters or numbers)'), 'Confirm Password' (with note '(It shall be the same as input password)'), and 'Verification Code' (with placeholder 'One verification code can be or' and a 'Get verification code' button). At the bottom are 'Submit' and 'Cancel' buttons.

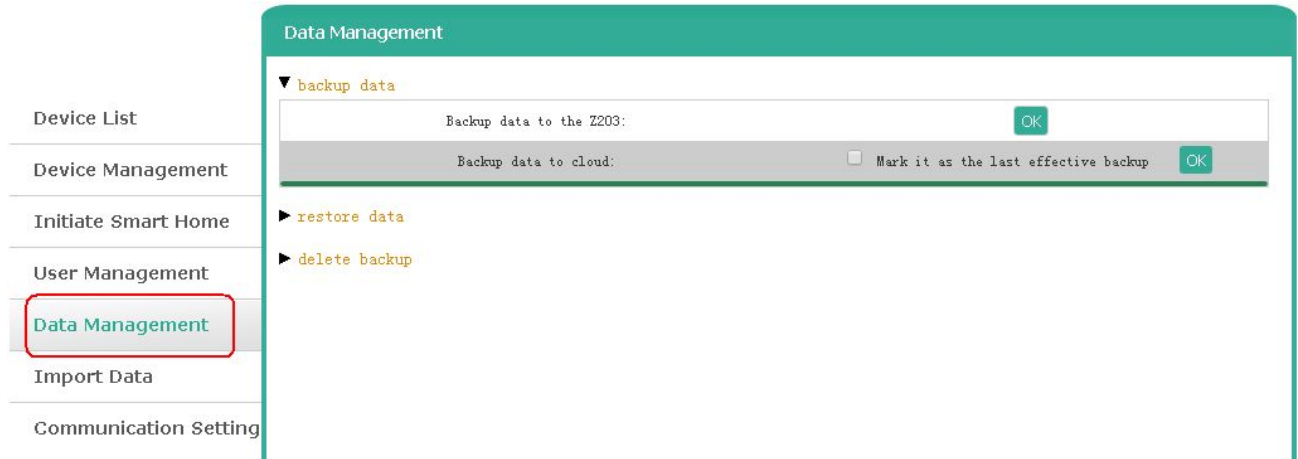
### B. Verification Code

To get a new Verification Code, please click **Add**.

This screenshot shows the 'Verification Code' section with an 'add' button highlighted by a red box. Below it is a table with columns: Serial Number, Verification Code, and Status. The table contains one row with Serial Number '1', Verification Code '540615', and Status 'used'.

## 6-5. Data Management

To backup, restore, or delete the settings.



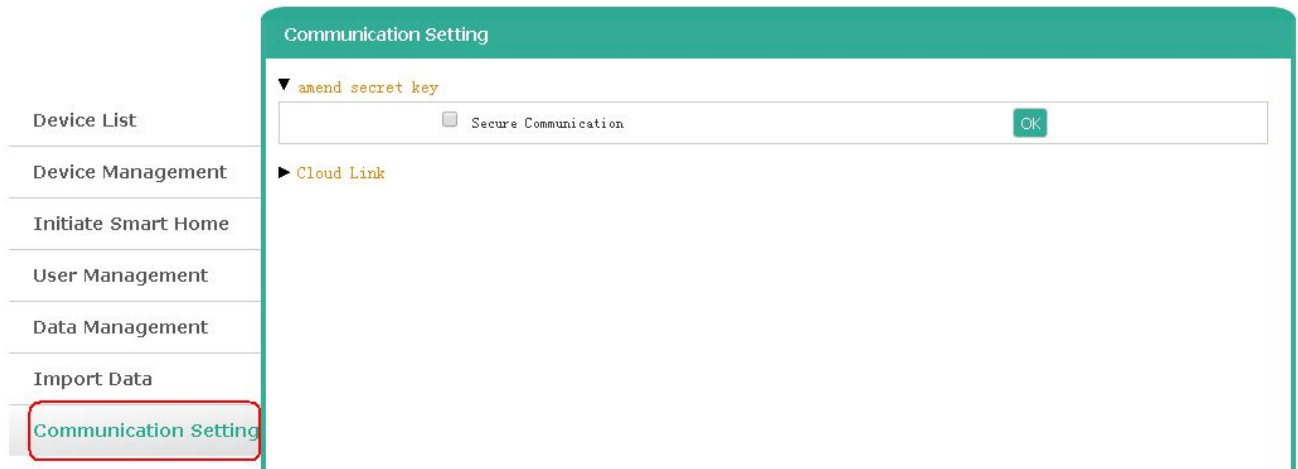
## 6-6. Import Data

To import mode-controlling scheme or IR data.



## 6-7. Communication Setting

To manage security key or Cloud link.



## 7. Important Maintenance Instructions

- This device is NOT truly waterproof/ resistant and is for indoor use.
- Please keep the device in a dry place. Precipitation, humidity, and all types of liquids or moisture can contain minerals that corrode electronic circuits. In cases of accidental liquid spills to a device, please leave the device dry properly before storing or using.
- Do not use or store the device in dusty or dirty areas.
- Do not use or store the device in extremely hot temperatures. High temperatures may damage the device or battery.
- Do not use or store the device in extremely cold temperatures. When the device warms to its normal temperature, moisture can form inside the device and damage the device or battery.
- Do not drop, knock, or shake the device. Rough handling would break it.
- Do not use strong chemicals or washing to clean the device.
- Do not paint the device. Paint would cause improper operation.

Handle your device, battery, and accessories with care. The suggestions above help you keep your device operational. For damaged device, please contact the authorized service center in your area.