HD3011/HD3010
User Manual

Version: 2.0

Release Date: FEB 4th, 2015

Broadband Network Solution Department

TECOM CO., LTD.

Safety Precautions

Please follow these safety precautions to prevent injury or damage to property that may be caused by fire or electrical damage.

DOs:

1.) Use the type of power recommended as seen on the label of your device.

2.) Use the power adapter in the product package.

3.) Pay attention to the power load of the outlet or prolonged lines. An overburdened power outlet, damaged lines or plugs may cause electric shock or even fire. Check your power cords regularly to ensure their safe functioning. If you find any damage line or parts, please repair or replace them immediately.

4.) Leave space around your device to allow heat dissipation. This is necessary to avoid damage caused by the overheating of the device. The long and thin holes on the device are designed for heat dissipation to ensure that the device continues normal functioning. **Do not cover these heat dissipation holes**.

DON'Ts:

1.) Do not keep this device close to a heat source or in a high temperature environment. Keep the device away from direct sunlight.

2.) Do not keep this device in a damp or moist place. Do not spill any fluids on this device.

3.) Do not connect this device to a PC or other electronic product unless instructed by our customer service engineers or your internet service provider. Bad connections may cause a power surge or fire risk.

4.) Do not place this device on an unstable surface or support.

Northern America FCC Statement

This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions in this manual, may cause interference to radio communications. This equipment as been tested and found to comply with the limits for a Class B computing device pursuant to Subpart J of Part 15 of FCC rules, which are designed to provide reasonable protection against radio interference when operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his or her own expense, will be required to take whatever measures are necessary to correct the interface.

Europe CE Declaration of Conformity

This equipment complies with the requirements relating to electromagnetic compatibility, EN55022 Class B for ITE and EN 50082-1. This meets the essential protection requirements of the European Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility.

Japan VCCI Declaration of Conformity

This equipment complies with the Class B standard of the Voluntary Control Council for Interference from Information Technology Equipment (VCCI). This meets the essential protection requirements of Japan laws relating to electromagnetic compatibility.

Copyright Notice

Trademarks

Windows 98/2000/XP/NT™, NetMeeting™, Internet Explorer™ are registered trademarks of Microsoft Corporation. All company, brand and product names are trademarks or registered trademarks of their respective owners.

Revision History

Version	Date	Update Log	Author
2.0	2015-02-04	2ed version for HD3011/HD3010 User Manual.	Sony

Table of Contents

1. PRODUCT OVERVIEW

HD3011/3010/3000 Series, ITU-T G.hn networking standard compliant Ethernet/Wireless adapter, provides the best quality data transmission for the truly high-speed 'connected home' experience. It allows users to extend a local area network via existing power lines, eliminating the need for extra wiring. Installation at home (or in a small office) is quick and easy as the HD3010/3000 Series come with plug-and-play technology.

HD3011/3010/3000 Series support Multiple Input/Multiple Output (MIMO) operation based on G.9963 and can be used with two fully programmable reception and transmission paths to attain up to 1Gbps PHY rates co-existence with UPA technology networks.

Key Features:

- MIMO Performance

Support ITU-T G.hn baseband plans 25, 50 and 100 MHz and MIMO techniques for powerline (based on G.9963) boosting PLC throughput up to 800 Mbps PHY rate over powerline (1 Gbps PHY rate over coax) having Robust Communication Mode (RCM) to prevent noise interference from other home appliances.

System Requirements:

- Analog phone line with internet service
- Ethernet cable

Product Features:

- HD3011/HD3010 have 2 (FE) Ethernet ports
- HD3011/HD3010 have One Wi-Fi 11n 2.4GHz(WLAN)
- HD3011 have one USB port.
- HD3000 have 1 (FE) Ethernet ports

2. Installation

Included devices are:

- One HD3000 device
- One HD3011/HD3010 device
- One Ethernet cable

2.1. Appearance

- **HD3000 Device Front Panel**

There are 3 LED's on the front panel of HD3000 that show the status of the unit.

- **HD3000 Device Side Panel**

The side panel contains reset button and Link button

The side panel contains Ethernet port

Item	Define	Color	Function
1	Power (Sigma chipset define)	Green	In case of a regular device: The LED will blink if identifies a Domain Master till completion of registration (very short time period) and shall be Solid ON (Green) after registration In case of Domain Master device: The LED will be solid ON (Green)
2	Ethernet (Sigma chipset)	Green	“Blink”, indicates data transmission.
3	Link (Sigma chipset)	Green(Master)	“Green”, indicates PLC link is connected, the PHY rate higher than 25Mbps
		Red (Slave)	In case of a regular device: The LED will blink (RED) if identifies a Domain Master till completion of registration (very short time period).
		Amber	Following registration, the Link LED shall be: Amber”, indicates PLC link is connected, but the PHY rate is lower than 25Mbps
		Green	“Green”, indicates PLC link is connected, the PHY rate higher than 25Mbps “Blink”, indicates data transmission.

Label	Function
Reset Button	-The factory defaults press the rest button for more than 10 seconds. All settings will be lost.
Link Button(Paring)	- To encrypt your PLC network individually, press each paring button on the connected devices for at least 2 second – within 2 minutes - To remove a PLC device from your network, press the paring button on the corresponding device for at least 11 seconds

- **HD3011 device Front Panel**

There are 6 LED's on the front panel that show the status of the unit.

- **HD3011 Side Panel**

The side panel contains the WPS button, reset button and Link button

The side panels contains Ethernet port and USB ports

Item	Define	Color	Function
1	Power LED	 Green	In case of a regular device: The LED will blink if identifies a Domain Master till completion of registration (very short time period) and shall be Solid ON (Green) after registration In case of Domain Master device: The LED will be solid ON (Green)
2	Link LED	 Green	In case of Domain Master device: The LED will be solid ON (Green) if is a standalone Domain Master device. In case of a regular device: The LED will blink (RED) if identifies a Domain Master till completion of registration (very short time period). Following registration, the Link LED shall be: Amber", indicates PLC link is connected, but the PHY rate is lower than 25Mbps "Green", indicates PLC link is connected, the PHY rate higher than 25Mbps "Blink", indicates data transmission.
3	Ethernet LED		The LED lights up in Green if there is at least one LAN connection. Blinking Green if there is an data/network activity

		Green	(transmit or receive)
4	USB	Green	Steadily On – HD3011 has connected to internet through USB 4G modem Off – HD3011 has not connected to internet through USB 4G modem Flashes – Data is received or sent through the 3G/4G modem
5	WPS LED	Green	Green: Flashes briefly – WPS paring
6	WLAN LED	Green	Steadily On – WLAN enable Off - WLAN disable Flashes - traffic passing through

Label	Function
WPS/WLAN Button	-WPS (Wi-Fi Protected Setup) encryption if press WPS button more than 2 seconds. -Enable / Disable WIFI function if press WPS button at least 5 seconds.
Reset Button	-The device restarts if you press the reset button for less than 3 seconds -The factory defaults press the rest button for more than 5 seconds. All settings will be lost.
Link Button(Paring)	-To encrypt your PLC network individually, press each paring button on the connected devices for approx. 1 second – within 2 minutes - To remove a PLC device from your network, press the paring button on the corresponding device for at least 10 seconds

- **HD3010 Device Front Panel**

There are 5 LED's on the front panel that show the status of the unit.

- **HD3010 Device Side Panel**

The side panel contains the WPS button, reset button and Link button

The side panels contains Ethernet port and USB ports

Item	Define	Color	Function
1	Power LED	Green	In case of a regular device: The LED will blink if identifies a Domain Master till completion of registration (very short time period) and shall be Solid ON (Green) after registration In case of Domain Master device: The LED will be solid ON (Green)
2	Link LED	Green	In case of Domain Master device: The LED will be solid ON (Green) if is a standalone Domain Master device. In case of a regular device: The LED will blink (RED) if identifies a Domain Master till completion of registration (very short time period). Following registration, the Link LED shall be: Amber", indicates PLC link is connected, but the PHY rate is lower than 25Mbps "Green", indicates PLC link is connected, the PHY rate higher than 25Mbps "Blink", indicates data transmission.
3	Ethernet LED	Green	The LED lights up in Green if there is at least one LAN connection. Blinking Green if there is an data/network activity (transmit or receive)
5	WPS LED		Green: Flashes briefly – WPS paring

		Green	
6	WLAN LED	 Green	Steadily On – WLAN enable Off - WLAN disable Flashes - traffic passing through

Label	**Function**
WPS/WLAN Button	-WPS (Wi-Fi Protected Setup) encryption if press WPS button more than 2 seconds. -Enable / Disable WIFI function if press WPS button at least 5 seconds.
Reset Button	**-**The device restarts if you press the reset button for less than 3 seconds **-**The factory defaults press the rest button for more than 5 seconds. All settings will be lost.
Link Button(Paring)	-To encrypt your PLC network individually, press each paring button on the connected devices for approx. 1 second – within 2 minutes - To remove a PLC device from your network, press the paring button on the corresponding device for at least 10 seconds

3. HD3011/HD3010 Web Configuration

3.1. Login Page

Figure3.1-1 shows the login window. Here, the login information should be filled in as shown below:

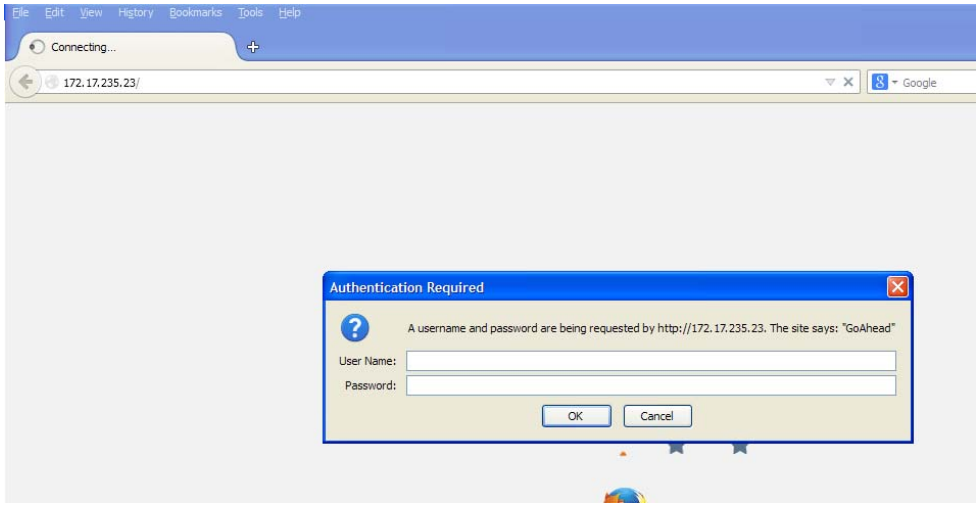


Figure 3.1-1

The default IP address of the HD3011/HD3010 LAN is 10.10.10.254

Username: admin

Password: admin

After login we can see Quick Setup page

3.2. Quick Setup

Figure3.2-1 displays the Quick setup page of the device.

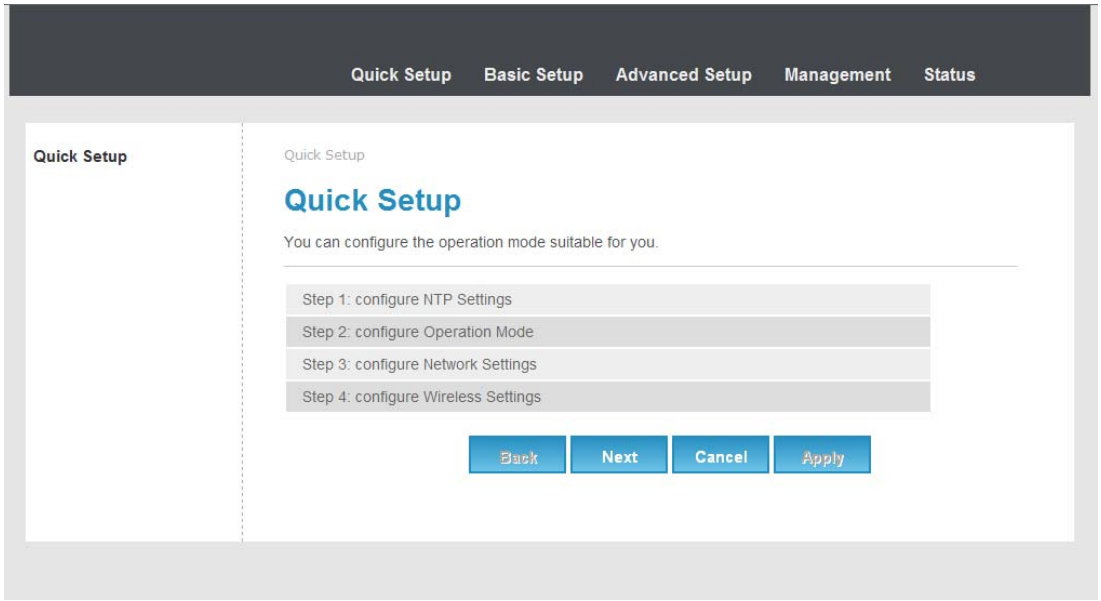


Figure 3.2-1

Using quick setup we can configure below list.

- NTP settings
- Operation Mode
- Network Settings
- Wireless Settings

3.3. Basic Setup

Figure3.3-1 shows basic setup of the device

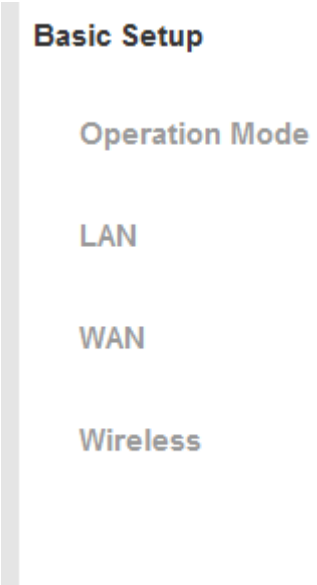


Figure 3.3-1

3.3.1. Operation Mode

Figure3.3.1-1 displays operation mode settings

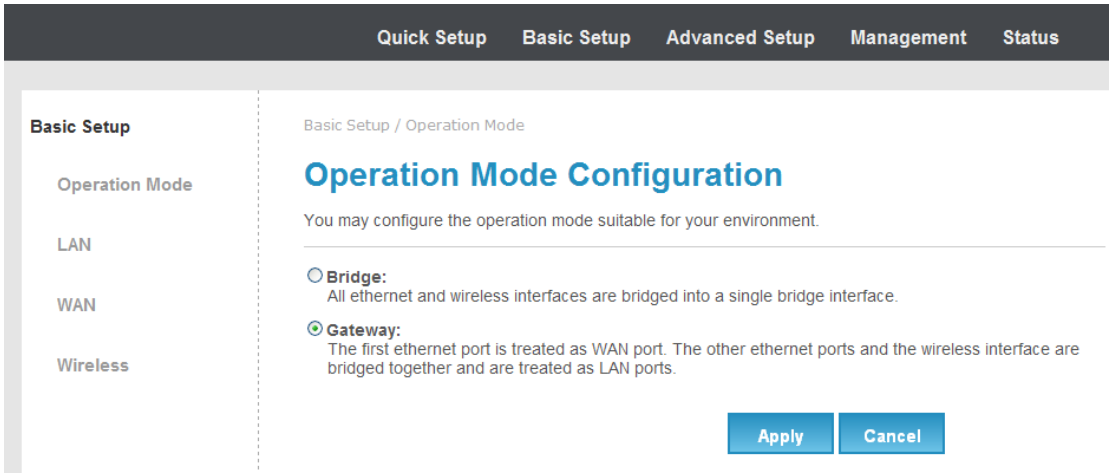


Figure 3.3.1-1

In this page we can set bridge mode or gateway mode

3.3.2. LAN

Figure3.3.2-1 and Figure3.3.2-2 displays LAN settings information page

These are the IP settings of the LAN interface for the device. These settings may be referred to as Private settings. You may change the LAN IP address if needed. The LAN IP address is private to your internal network and cannot be seen on the Internet.

Basic Setup / LAN

Local Area Network (LAN) Settings

You may enable/disable networking functions and configure their parameters as your wish.

LAN Setup	
IP Address	10.10.10.254
Subnet Mask	255.255.255.0
Default Gateway	
Primary DNS Server	168.95.1.1
Secondary DNS Server	8.8.8.8
MAC Address	00:19:15:DC:67:F4
DHCP Type	Server
Start IP Address	10.10.10.100
End IP Address	10.10.10.200
Subnet Mask	255.255.255.0
Primary DNS Server	168.95.1.1
Secondary DNS Server	8.8.8.8
Default Gateway	10.10.10.254
Lease Time	86400

Figure3.3.2-1

Lease Time	86400
Statically Assigned	MAC: IP:
Statically Assigned	MAC: IP:
Statically Assigned	MAC: IP:
802.1d Spanning Tree	Disable
LLTD	Disable
IGMP Proxy	Disable
UPNP	Disable
PPPoE Relay	Disable
DNS Proxy	Disable

Apply Cancel

Figure3.3.2-2

DHCP Server

DHCP stands for Dynamic Host Control Protocol. The DHCP Server gives out IP addresses when a device is booting up and request an IP address to be logged on to the network. That device must be set as a DHCP client to obtain the IP address automatically. By default, the DHCP Server is enabled. The DHCP address pool contains the range of the IP address that will automatically be assigned to the clients on the network.

Starting IP Address: The starting IP address for the DHCP server's IP assignment
IP Pool Count The max user pool size.
Lease Time the length of time for the IP lease.

UPnP (Universal Plug and Play)

UPnP is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use. UPnP broadcasts are only allowed on the LAN.

3.3.3. WAN

Figure3.3.3-1, Figure3.3.3-2, Figure3.3.3-3 and Figure3.3.3-4 displays WAN settings information

WAN has static, DHCP, PPPoE and 3G connection types.

Configure static connection type as below

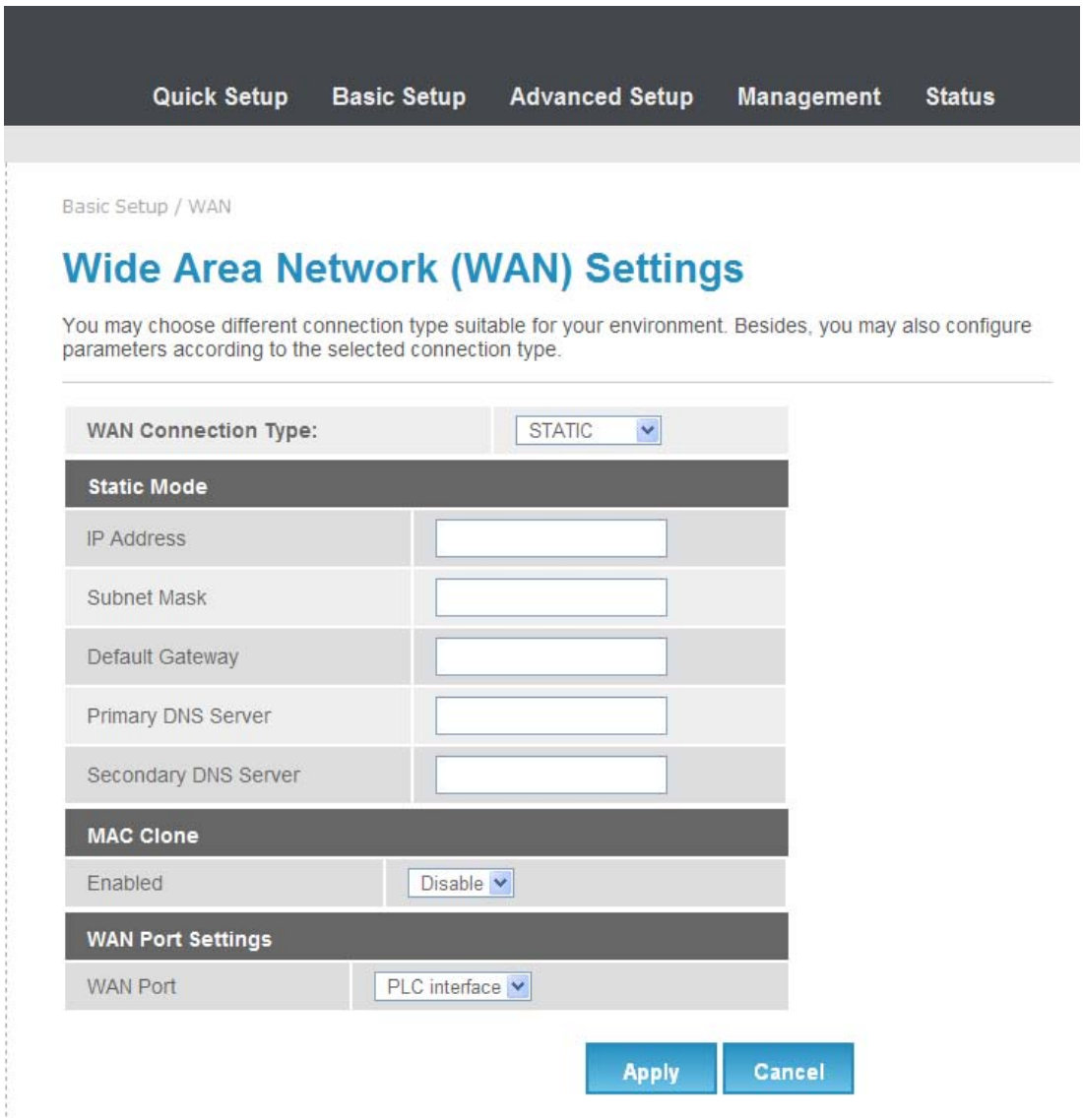


Figure3.3.3-1

Configure DHCP connection type as below

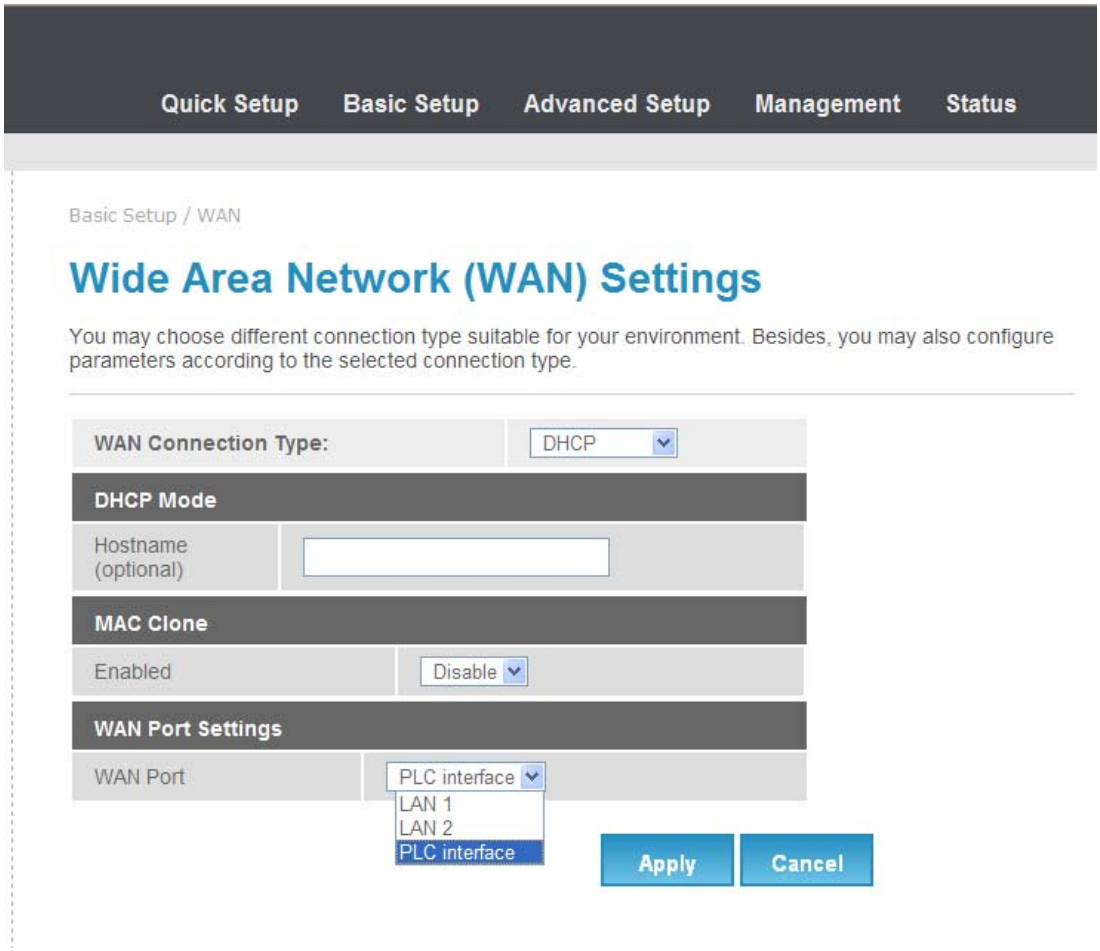


Figure3.3.3-2

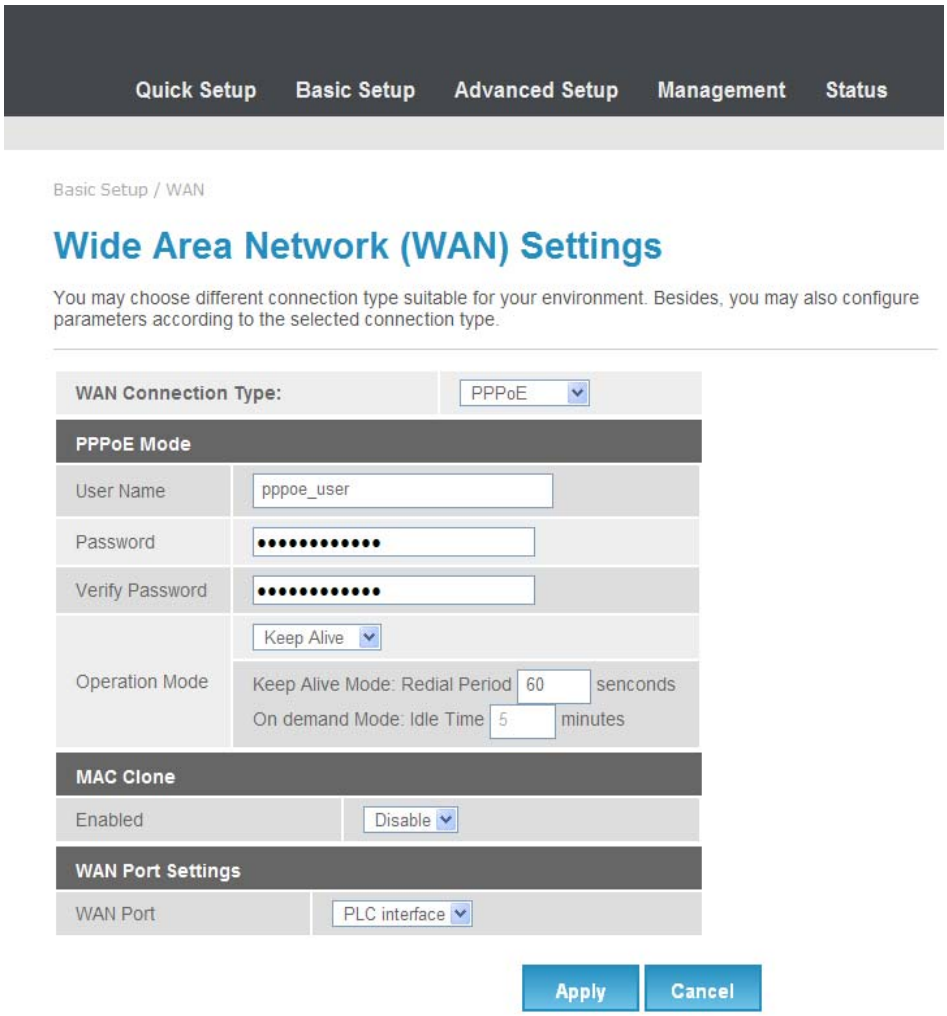


Figure3.3.3-3

PPPoE

Select this option if your ISP requires you to use a PPPoE connection. This option is typically used for DSL services. Select Dynamic PPPoE to obtain an IP address automatically for your PPPoE connection. Select Static PPPoE to use a static IP address for your PPPoE connection. Please enter the information accordingly.

Username: Enter your username for your PPPoE connection.

Password: Enter your password for your PPPoE connection

Operation Mode: For PPPoE connection, you can select Always on or Connect on-demand. Connect on demand is dependent on the traffic. If there is no traffic (or Idle) for a pre-specified period of time), the connection will tear down automatically. And once there is traffic send or receive, the connection will be automatically on.

HD3011 device 3G/4G dongle WAN settings page

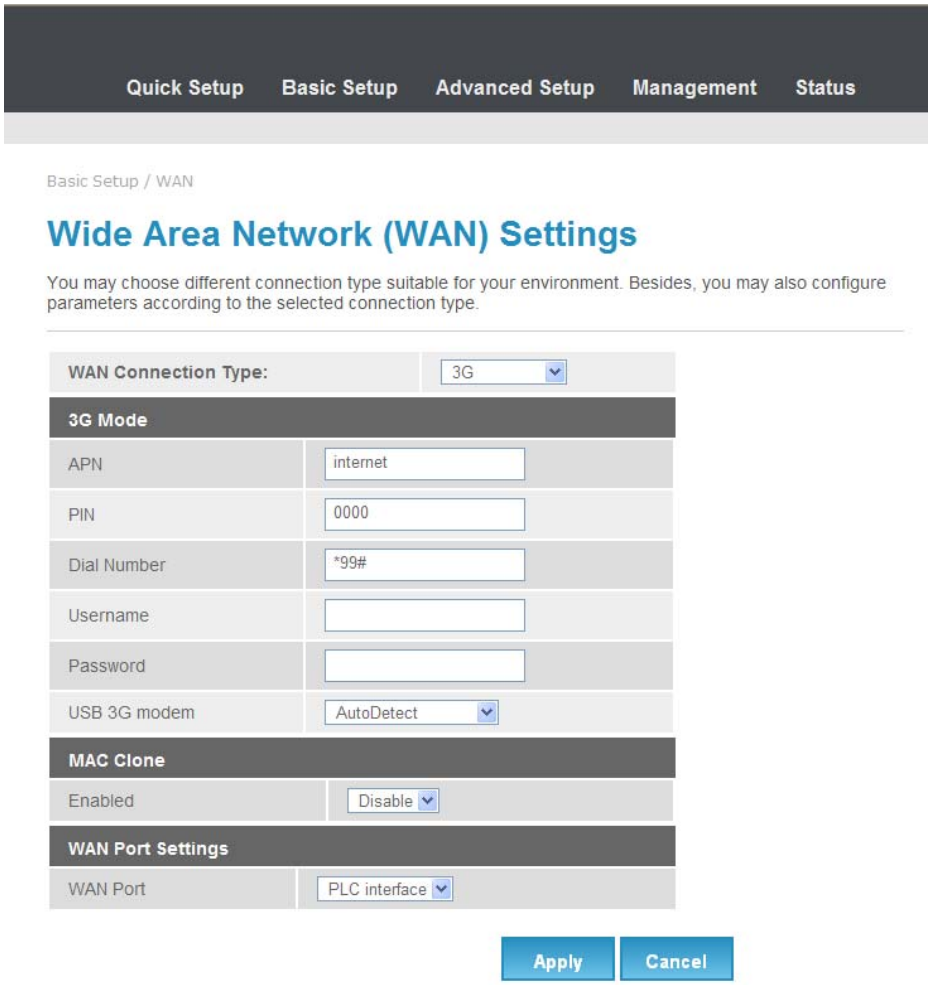

Quick Setup
Basic Setup
Advanced Setup
Management
Status
Basic Setup / WAN
Wide Area Network (WAN) Settings
You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.
WAN Connection Type:
3G
3G Mode
APN
internet
PIN
0000
Dial Number
*99#
Username
Password
USB 3G modem
AutoDetect
MAC Clone
Enabled
Disable
WAN Port Settings
WAN Port
PLC interface
Apply
Cancel

Figure3.3.3-4

3.3.4. Wireless

Figure3.3.4-1 and Figure3.3.4-2 displays basic wireless information

The following page is Wireless LAN settings. Please select and input the correct information in the following item to set Wireless function.

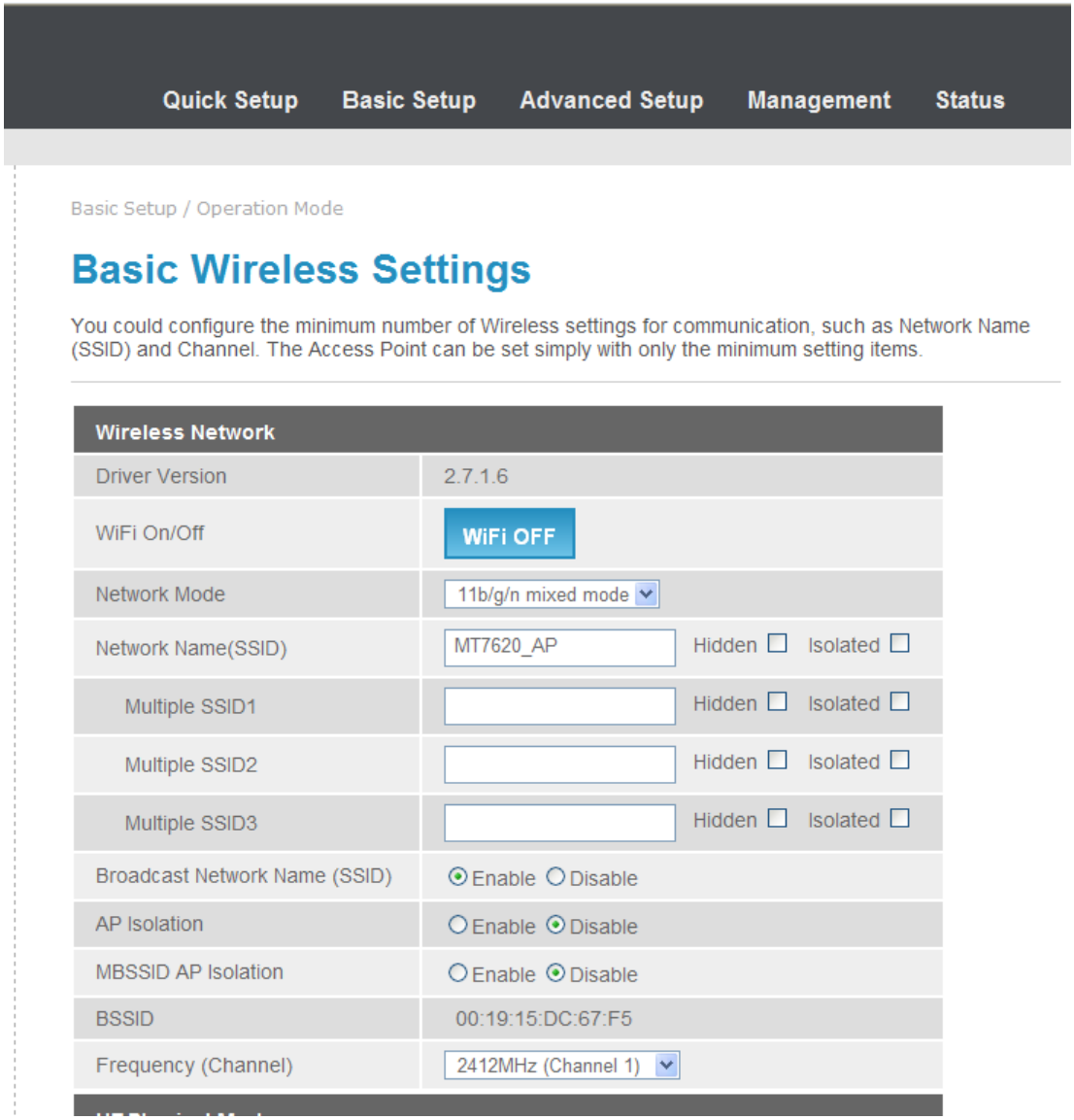


Figure 3.3.4-1

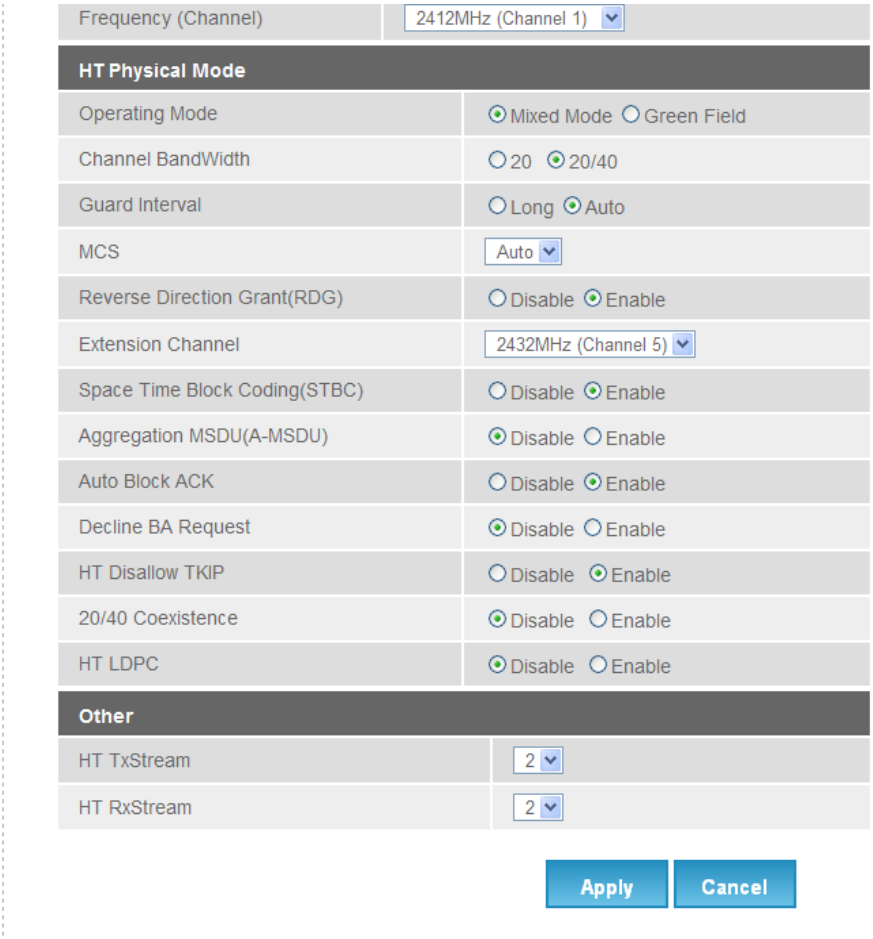


Figure 3.3.4-2

We can configure below settings using basic wireless settings page

SSID:
The SSID is a unique name to identify the DSL Router in the wireless LAN. Wireless clients associating to the DSL Router must have the same SSID.
Broadcast SSID:
Select No to hide the SSID such that a station can not obtain the SSID through passive scanning. Select yes to make the SSID visible so a station can obtain the SSID through passive scanning.

Channel ID the range of radio frequencies used by IEEE 802.11b/g wireless devices is called a channel

3.4. Advanced Setup

Figure3.4-1 shows Advanced Setup menu list

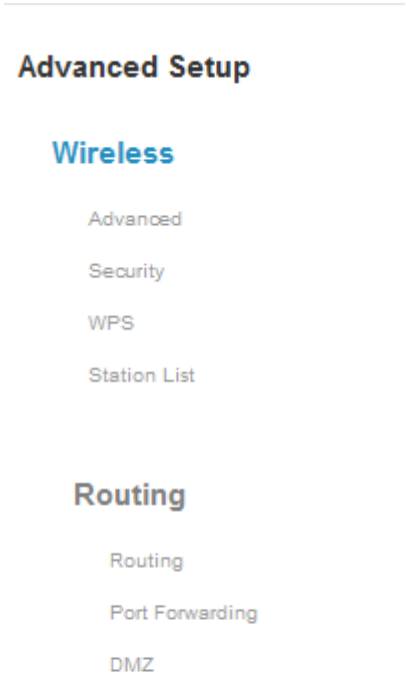


Figure 3.4-1

3.4.1. Advanced Wireless

Figure3.4.1-1, Figure3.4.1-2, Figure3.4.1-3 shows Advanced Wireless settings and Wi-Fi multimedia

The following page is Advanced Wireless settings. Please select and input the correct information in the following item to set Wireless functions.

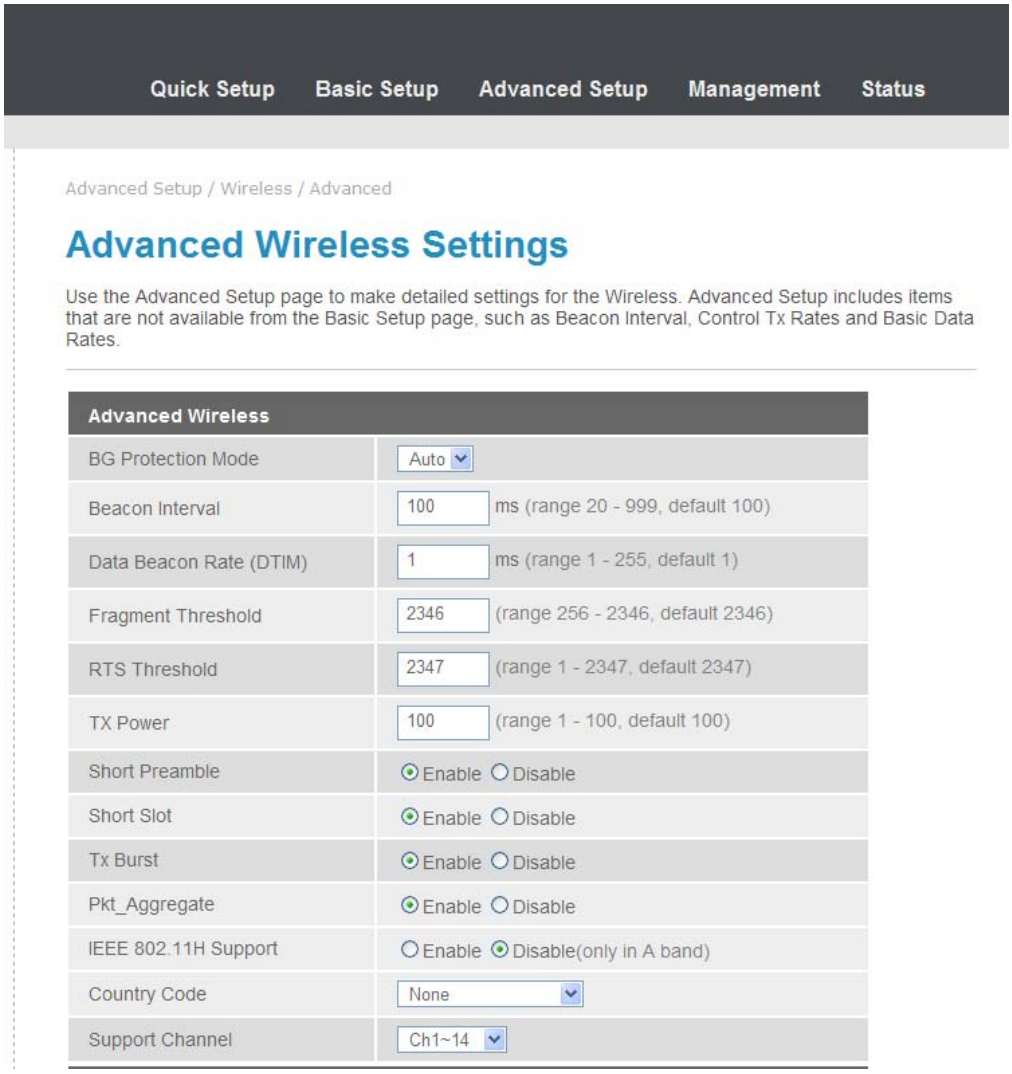


Figure 3.4.1-1

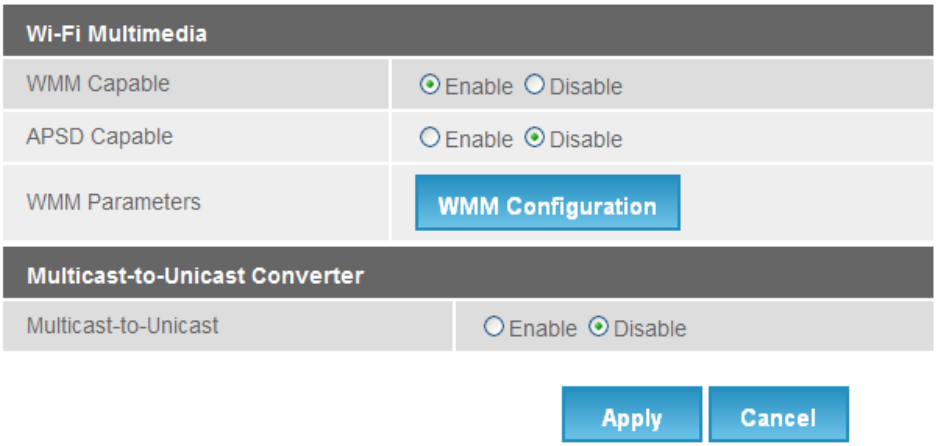


Figure 3.4.1-2

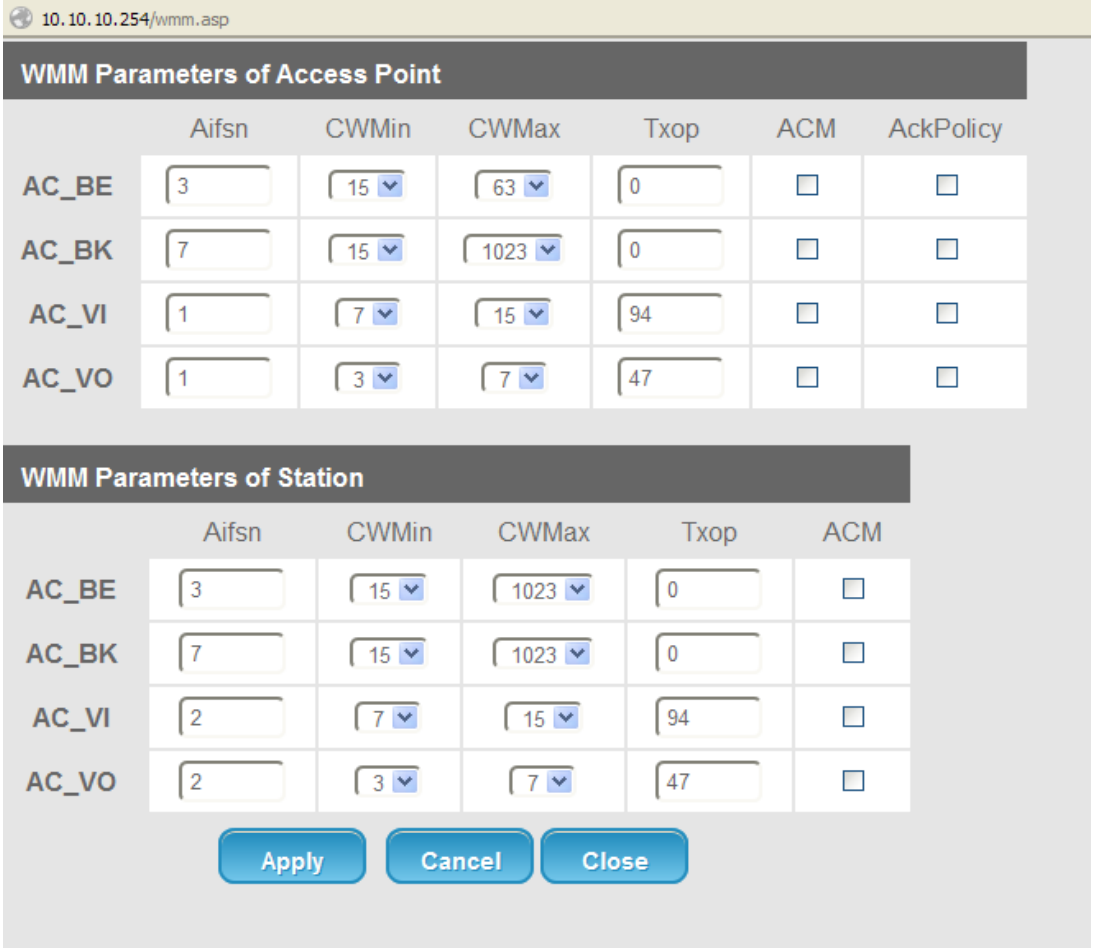


Figure 3.4.1-3

Beacon Interval

The Beacon Interval value indicates the frequency interval of the beacon. Enter a value between 20 and 1000. A beacon is a packet broadcast by the Router to synchronize the wireless network.

DTIM

This value, between 1 and 255, indicates the interval of the Delivery Traffic Indication Message (DTIM).

RTS Threshold

The RTS (Request to Send) threshold (number of bytes) for enabling RTS handshake Data with its frame size larger than this value will perform the RTS handshake, setting this attribute to be larger than the maximum MSDU (MAC service data unit) size turns off the RTS handshake, setting this attribute to zero turns on the RTS handshake. Enter a value between 0 and 2432.

Fragmentation Threshold

The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter a value between 256 and 2432.

3.4.2. Security

Figure3.4.2-1, Figure3.4.2-2, Figure3.4.2-3, and Figure3.4.2-4 shows wireless Security information

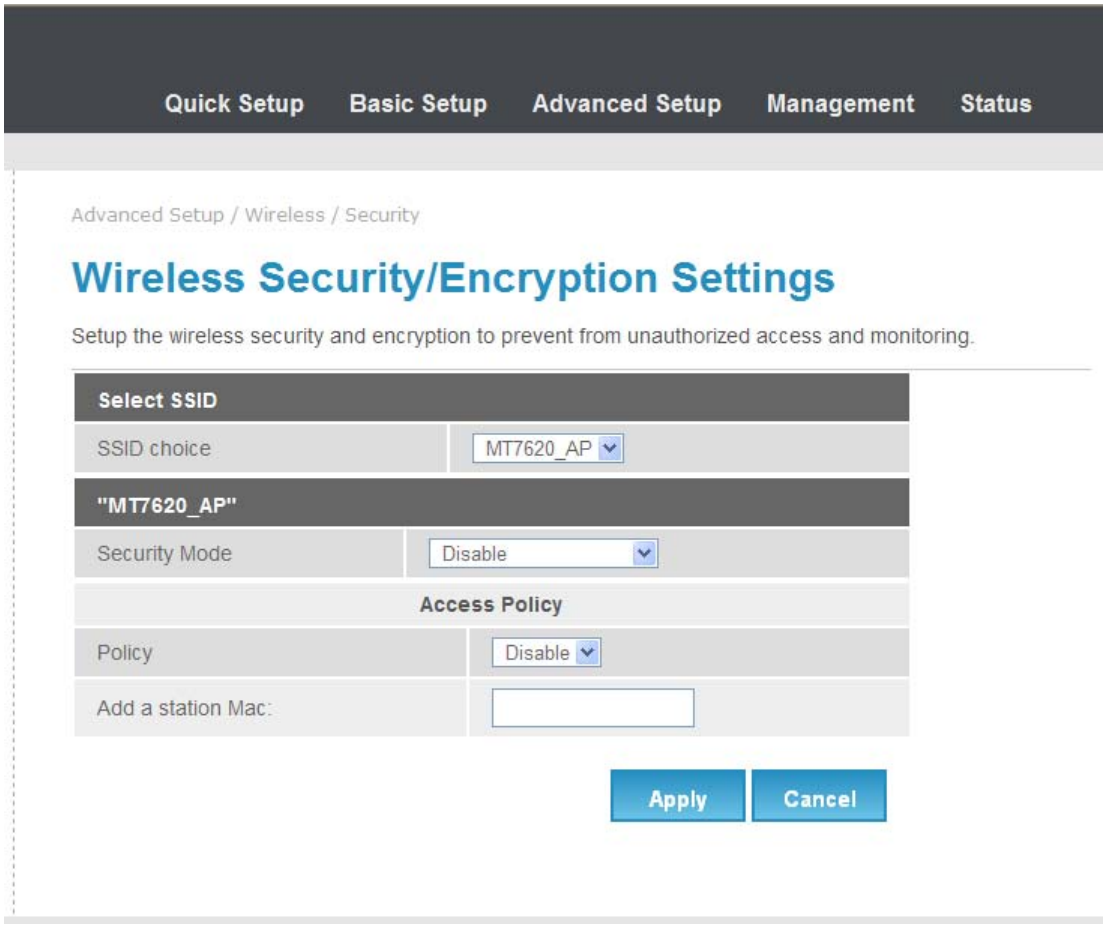


Figure 3.4.2-1

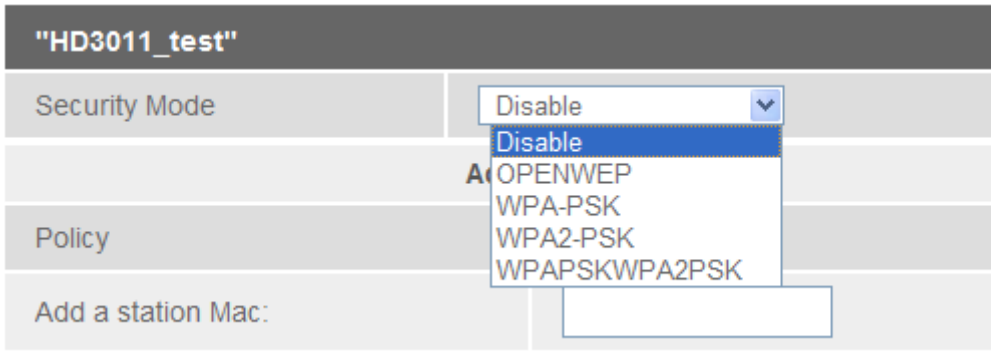


Figure 3.4.2-2

"HD3011_test"			
Security Mode	OPENWEP		
Wire Equivalence Protection (WEP)			
Default Key	Key 2		
WEP Keys	WEP Key 1 :		Hex
	WEP Key 2 :		Hex
	WEP Key 3 :		Hex
	WEP Key 4 :		Hex

Figure 3.4.2-3

"HD3011_test"	
Security Mode	WPA-PSK
WPA	
WPA Algorithms	TKIP AES TKIPAES
Pass Phrase	0000test
Key Renewal Interval	3600 seconds (0 ~ 4194303)
Access Policy	
Policy	Disable
Add a station Mac:	

Figure 3.4.2-4

Using this page we can set SSID choice, Security mode, Access Policy and WPA.

Security Mode

OPEN WEP

WEP (Wired Equivalent Privacy) encrypts data frames before transmitting over the wireless network. Select Disable to allow all wireless computers to communicate with the access points without any data encryption. Select 64-bit WEP or 128-bit WEP to use data encryption.

Key#1~Key#4 The WEP keys are used to encrypt data. Both the DSL Router and the wireless clients must use the same WEP key for data transmission. If you chose 64-bit WEP, then enter any 10 hexadecimal digits ("0-9", "A-F") preceded by 0x for each key (1-4). If you chose 128-bit WEP, then enter 26 hexadecimal digits ("0-9", "AF") preceded by 0x for each key (1-4).The values must be set up exactly the same on the Access Points as they are on the wireless client stations. The same value must be assigned to Key 1 on both the access point (your DSL Router) and the client adapters, the same value must be assigned to Key 2 on both the access point and the client stations and so on, for all four WEP keys.

WPA-PSK

Wi-Fi Protected Access, pre-shared key. Encrypts data frames before transmitting over the wireless network.

Pre-shared Key: the Pre-shared Key is used to encrypt data. Both the DSL Router and the wireless clients must use the same WPA-PSK key for data transmission.

WPA2-PSK

Short for Wi-Fi Protected Access 2 - Pre-Shared Key, and also called WPA or WPA2 Personal, it is a method of securing your network using WPA2 with the use of the optional Pre-Shared Key (PSK) authentication, which was designed for home users without an enterprise authentication server.

To encrypt a network with WPA2-PSK you provide your router not with an encryption key, but rather with a plain-English passphrase between 8 and 63 characters long. Using a technology called TKIP (for Temporal Key Integrity Protocol), that passphrase, along with the network SSID, is used to generate unique encryption keys for each wireless client. And those encryption keys are constantly changed. Although WEP

also supports passphrases, it does so only as a way to more easily create static keys, which are usually comprised of the hex characters 0-9 and A-F.

WPA Algorithms

TKIP

TKIP stands for “Temporal Key Integrity Protocol.” It was a stopgap encryption protocol introduced with WPA to replace the very-insecure WEP encryption at the time. TKIP is actually quite similar to WEP encryption.

AES

AES stands for “Advanced Encryption Standard.” This was a more secure encryption protocol introduced with WPA2, which replaced the interim WPA standard.

TKIPAES

When you set your router to use WPA2, you usually have the option to use AES, or TKIP+AES. When your device is set to "WPA2 with TKIP+AES" it means that network devices that can use WPA2 will connect with WPA2, and network devices that can only use WPA will connect with WPA.

3.4.3. WPS

Figure3.4.3-1, Figure3.4.3-2 shows WPS settings

Wi-Fi Protected Setup (WPS; originally Wi-Fi Simple Configuration) is a network security standard that attempts to allow users to easily secure a wireless home network but could fall to brute-force attacks if one or more of the network's access points do not guard against the attack.

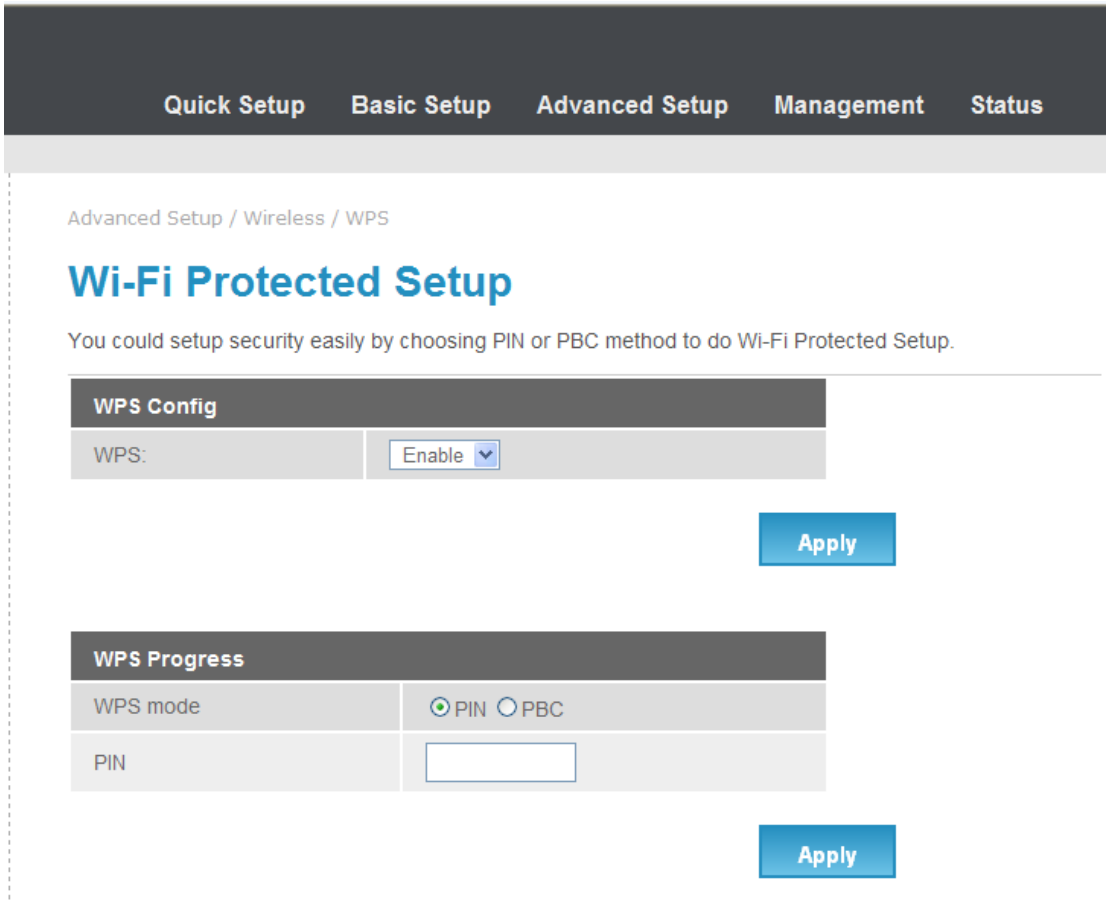


Figure 3.4.3-1

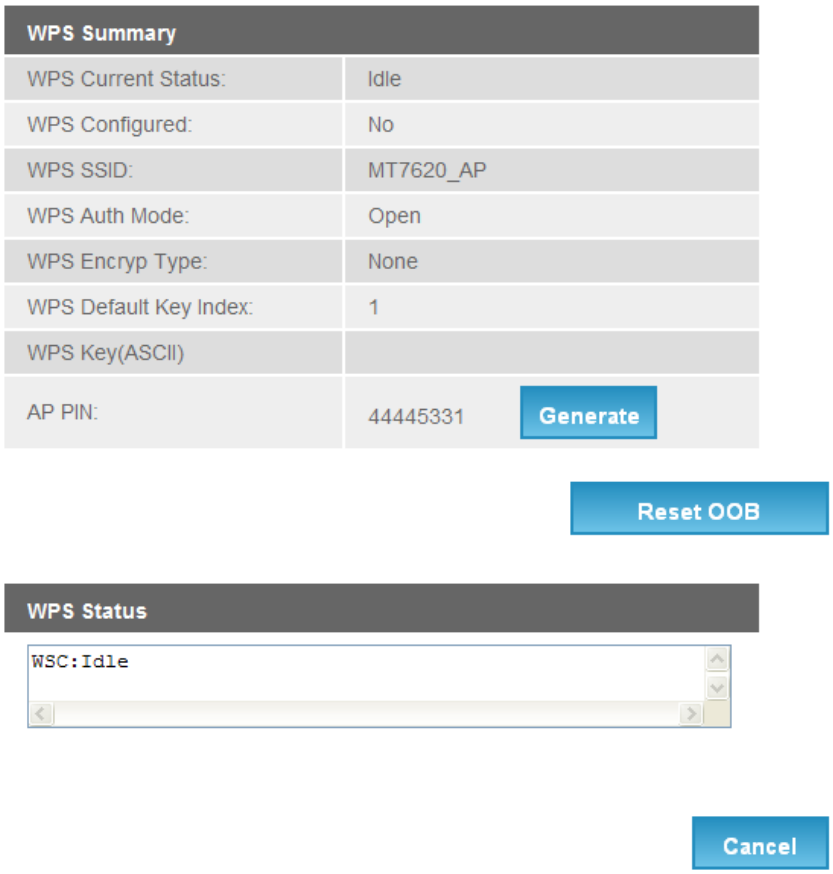


Figure 3.4.3-2

WPS Settings

There two WPS mode, one is PIN code and other one is PBC.

PIN method

in which a personal identification number (PIN) has to be read from either a sticker or display on the new wireless device. This PIN must then be entered at the "representant" of the network, usually the network's access point. Alternately, a PIN provided by the access point may be entered into the new device. This method is the mandatory baseline mode and every WPS-certified product must support it.

Push button method

in which the user has to push a button, either an actual or virtual one, on both the access point and the new wireless client device. Support of this mode is mandatory for access points and optional for connecting devices.

Example of configuration

1. Make sure WPS is enabled on system wise.

2. For Pin method

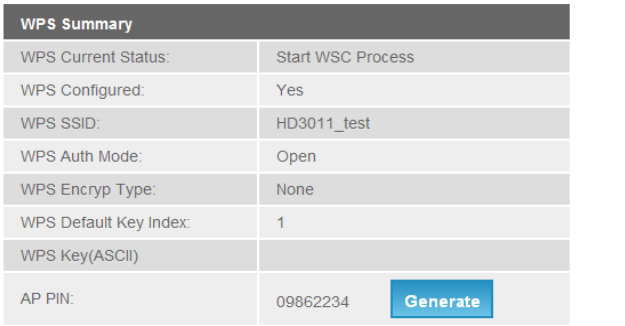
1). Select radio button PIN method.

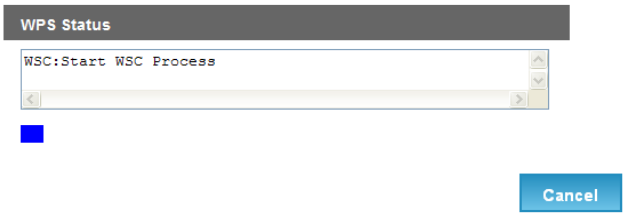
2). Enable your Wi-Fi client (Notebook, Mobile, PAD…etc). And check WPS.

3). Take PIN at client and specify same one in your AP device.

4). Click “Apply“below “WPS Progress” table to trigger WPS session.

5). Once connected, “WPS current status” will be put “Connected”.



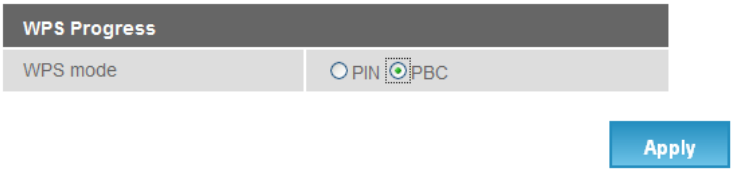


3. For PBC at Web

1). Select the following radio button, and click “Apply” Button to trigger WPS session.

2). at Wi-Fi client side, select PBC method. Within 2 minutes, they are automatically connected.

3). Once connected, “WPS current status” will be put “Connected”.



4. For physical PBC on the housing:

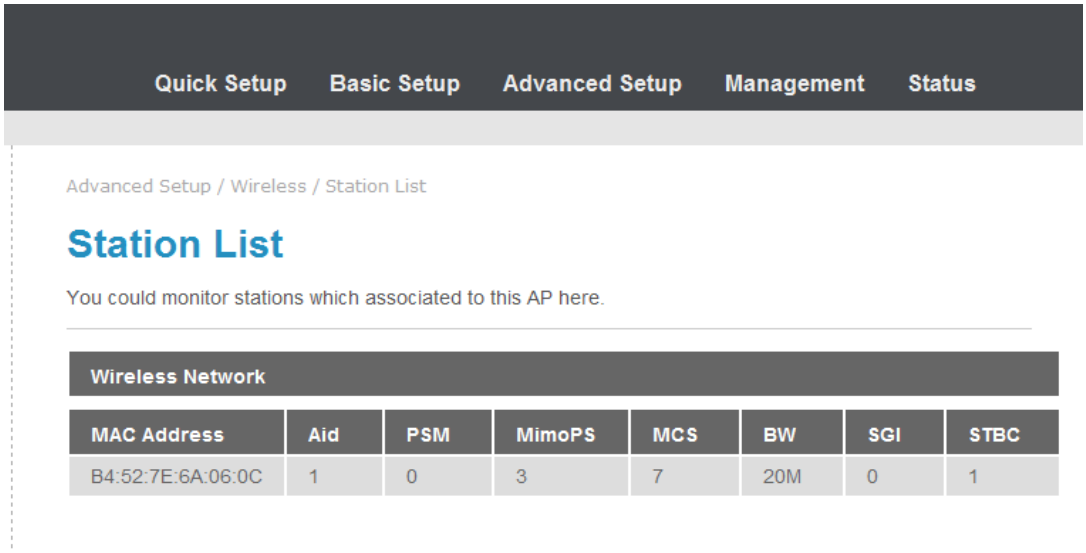
1). Special Note: WPS is enabled on system wise.

2). At wifi client side, select PBC method.

3). Within 2 minutes, please push physical PBC button at housing.

3.4.4. Station List

Figure3.4.4-1 display the wireless network station list



MAC Address	Aid	PSM	MimoPS	MCS	BW	SGI	STBC
B4:52:7E:6A:06:0C	1	0	3	7	20M	0	1

Figure 3.4.4-1

3.4.5. Routing

Figure3.4.5-1, Figure3.4.5-2 displays Static Routing Settings

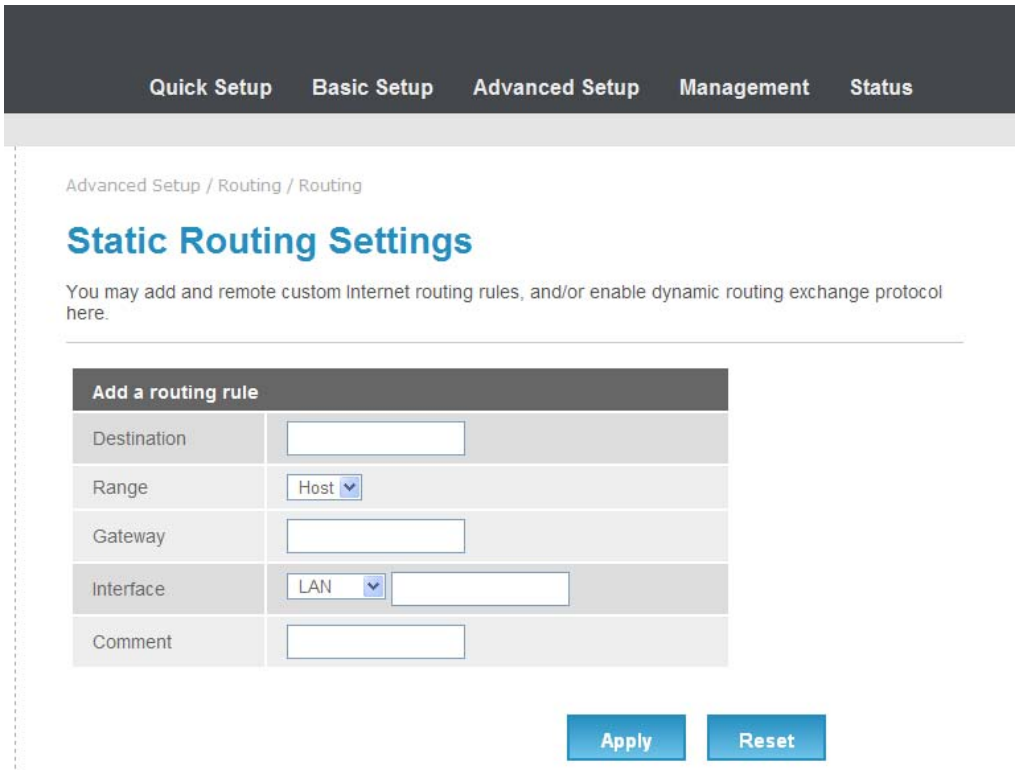


Figure 3.4.5-1

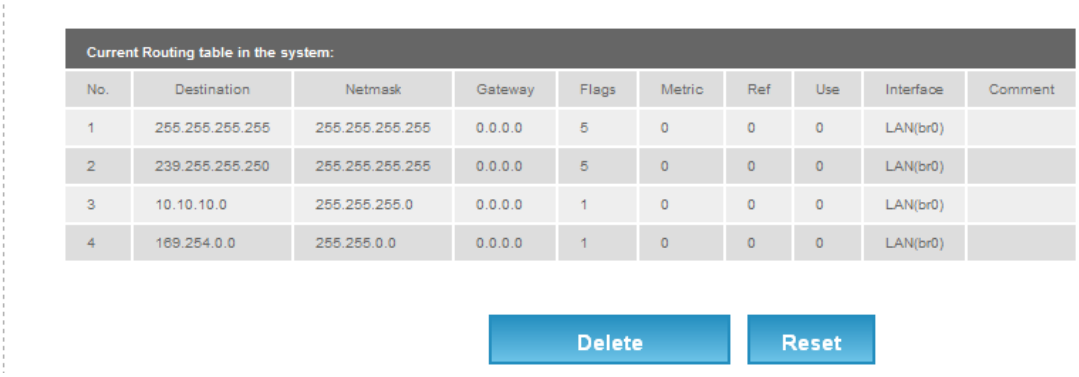


Figure 3.4.5-2

3.4.6. Port Forwarding

Figure3.4.6-1, Figure3.4.6-2 displays Port Forwarding setup and information

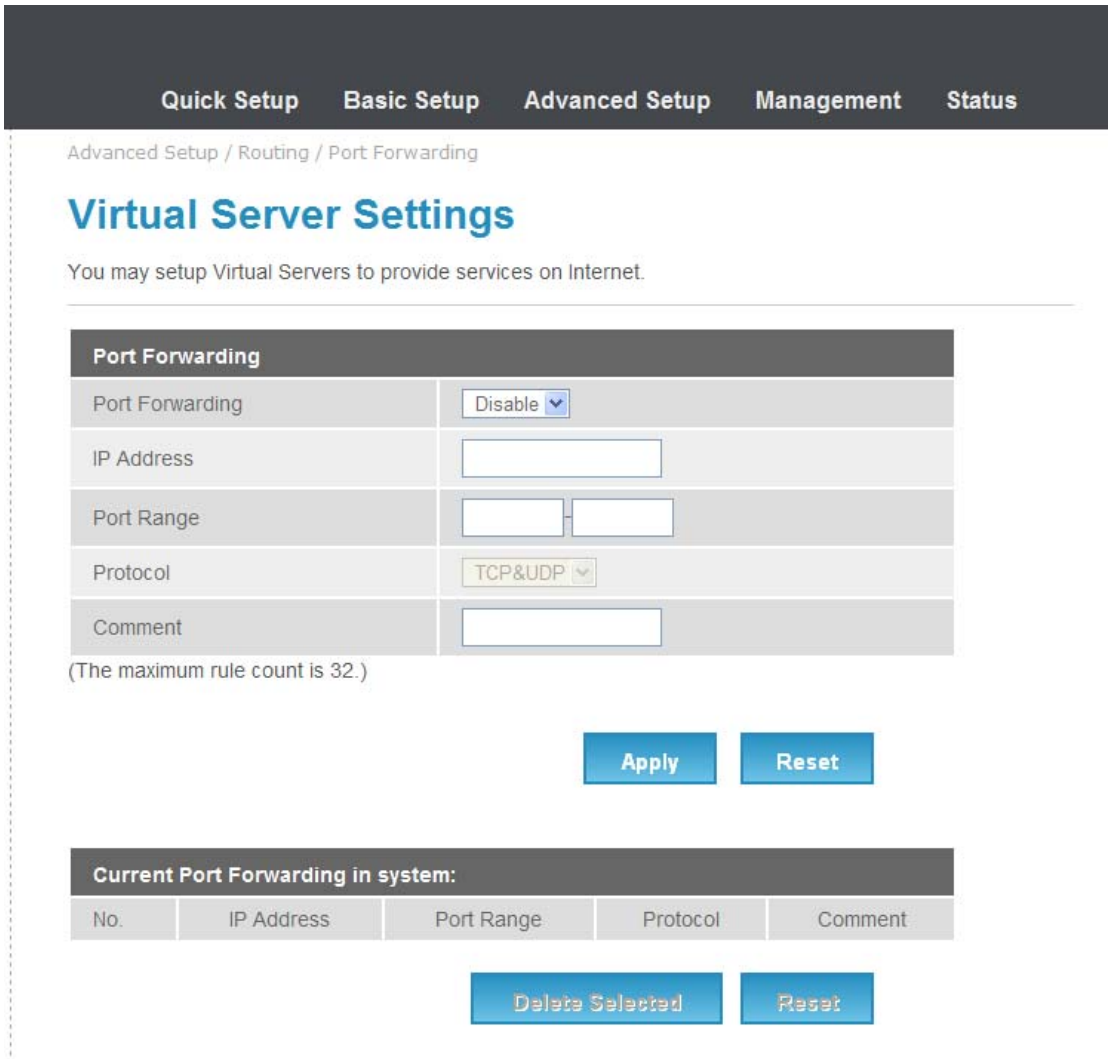


Figure 3.4.6-1

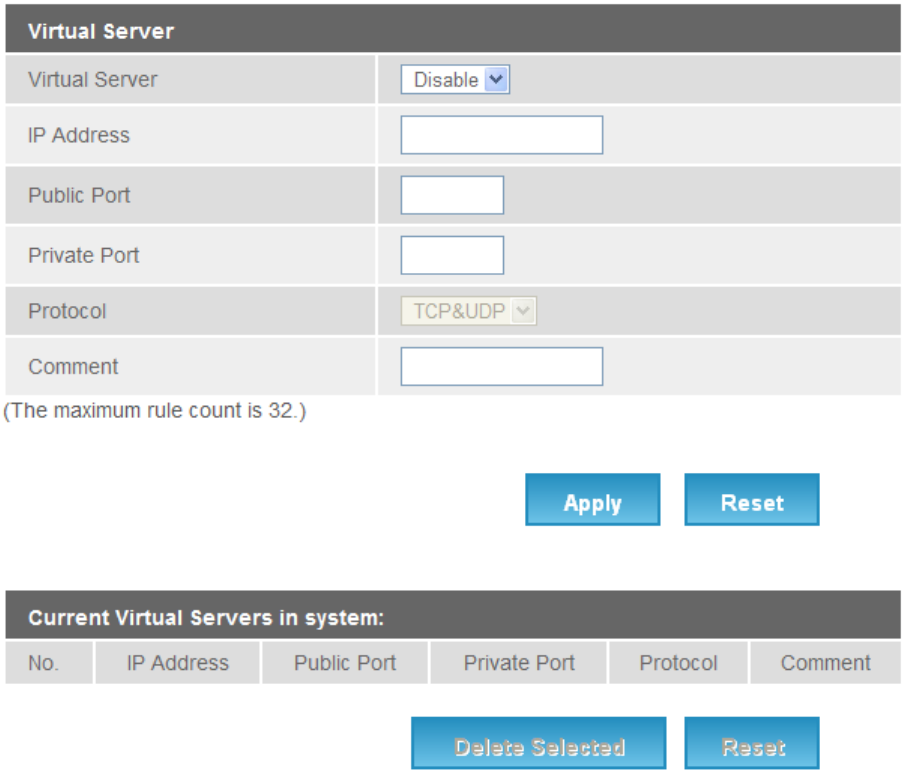
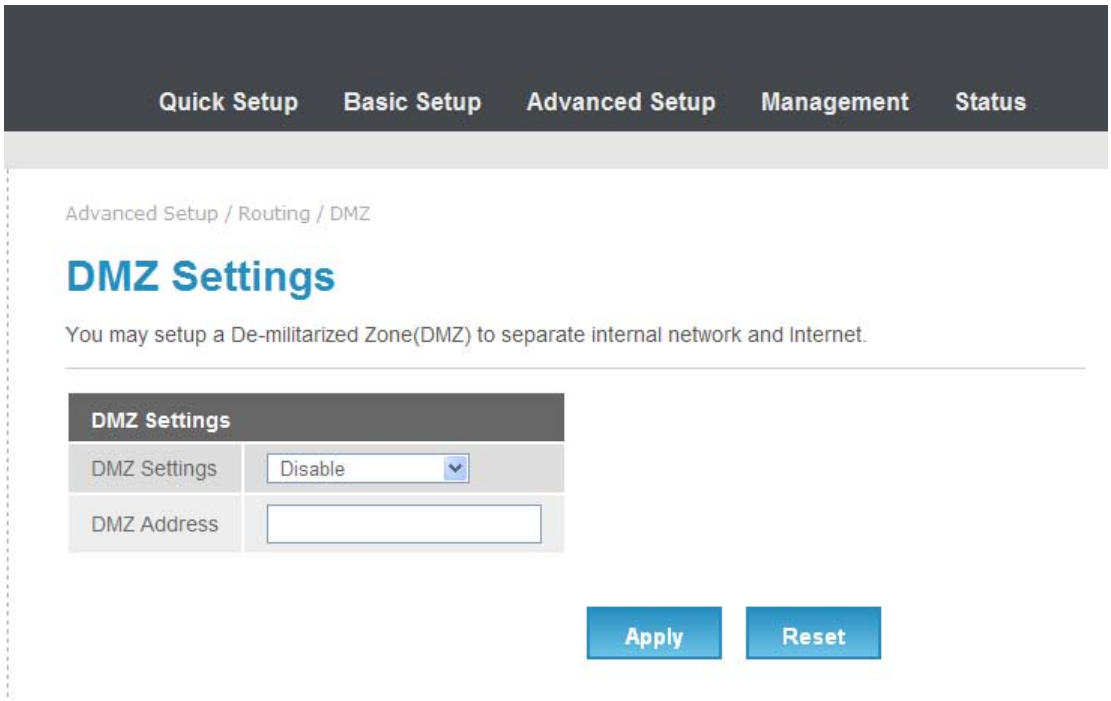

Virtual Server
Virtual Server
Disable
IP Address
Public Port
Private Port
Protocol
TCP&UDP
Comment
(The maximum rule count is 32.)
Apply
Reset
Current Virtual Servers in system:
No.
IP Address
Public Port
Private Port
Protocol
Comment
Delete Selected
Reset

Figure 3.4.6-2

3.4.7. DMZ Settings

Figure3.4.7-1 displays DMZ settings page

The De-Militarized Zone (DMZ) is a network which, when compared to the LAN, has fewer firewall restrictions, by default. This zone can be used to host servers (such as a web server, ftp server, or email server, for example) and give public access to them. The eighth LAN port on the router can be dedicated as a hardware DMZ port for safely providing services to the Internet, without compromising security on your LAN.



3.5. Management

Figure3.5-1 displays Management Menu List

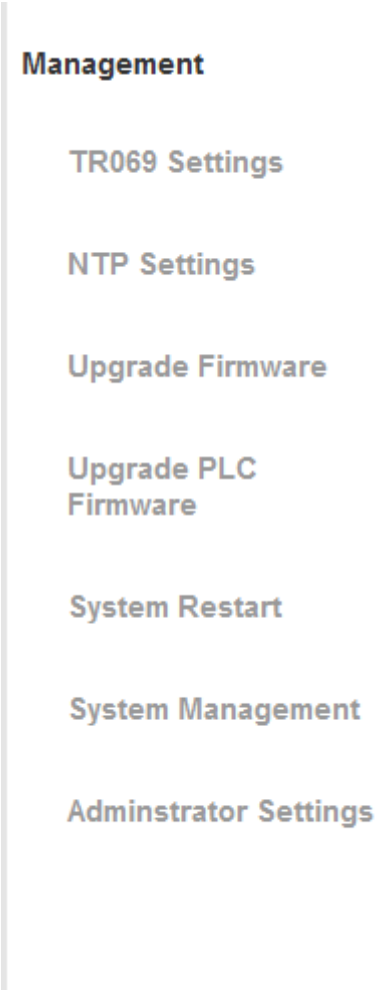


Figure 3.5-1

3.5.1. TR069 Settings

Figure3.5.1-1 displays TR069 Settings page

Note: If device is in bridge mode ACS server should also be in the same subnet of LAN address else ACS server will fail to connect with the device.

The following web page is TR069 setting page. It can set ACS Server information for TR069. Please select and enter the correct parameters in this page setting.

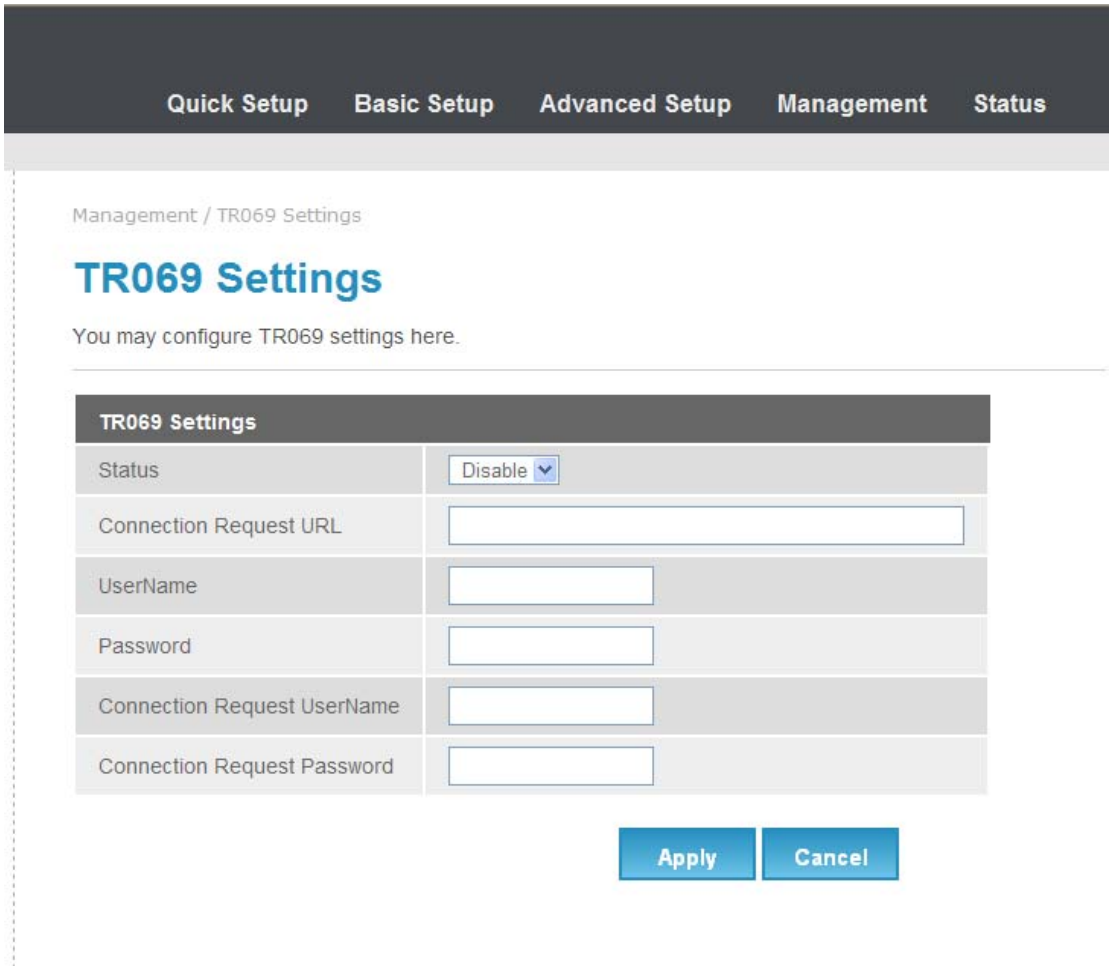


Figure 3.5.1-1

Using TR069 settings page we can start TR069 agent need to set below values

- Connection Request URL
- Username/password
- Connection request username/password

3.5.2. NTP Settings

Figure3.5.2-1 displays NTP Settings page

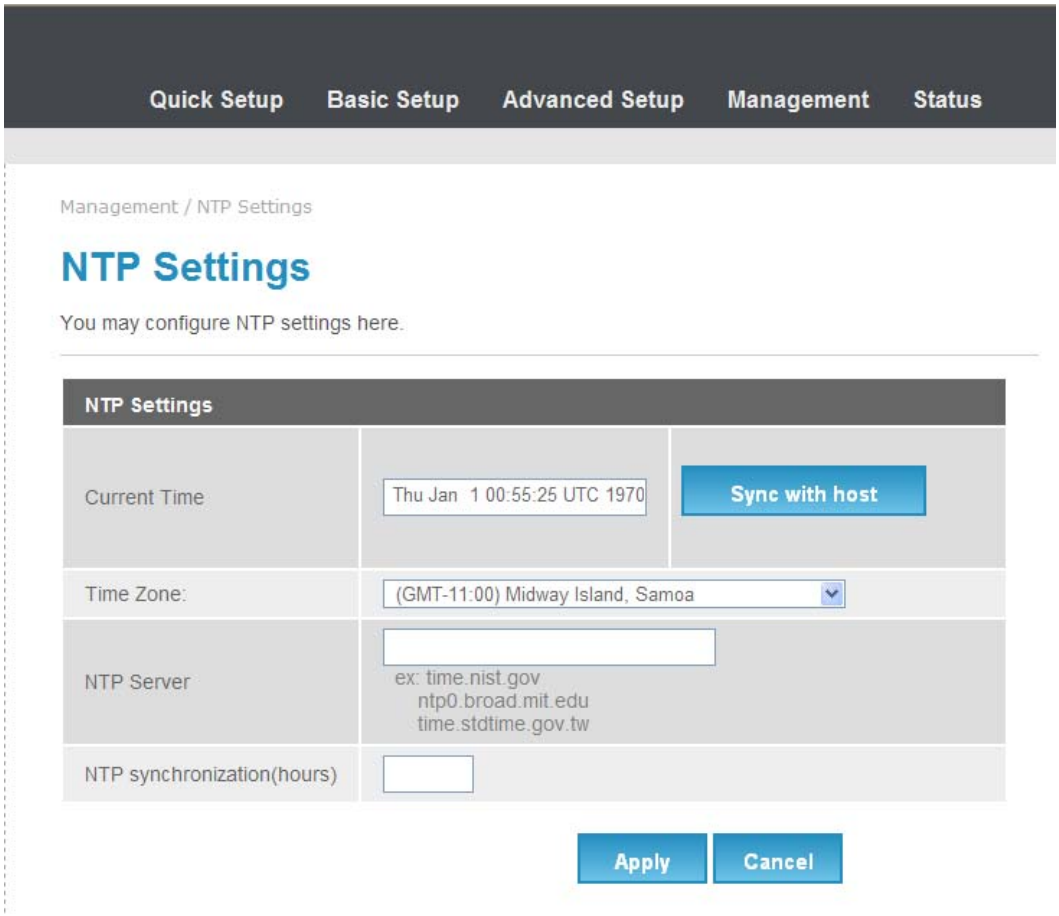


Figure 3.5.2-1

Using NTP setting page we can set

- Current time
- Time Zone
- NTP server
- NTP synchronization time

3.5.3. Upgrade Firmware

Figure3.5.3-1 displays Upgrade firmware information page

Notice: We only can upgrade firmware using LAN IP address of the web interface. Web interface with WAN IP address will not allow upgrading firmware.

You can upgrade the firmware of the device in this page. Make sure the firmware you want to use is on the local hard drive of the computer. Click on Browse to browse the local hard drive and locate the firmware to be used for the update.

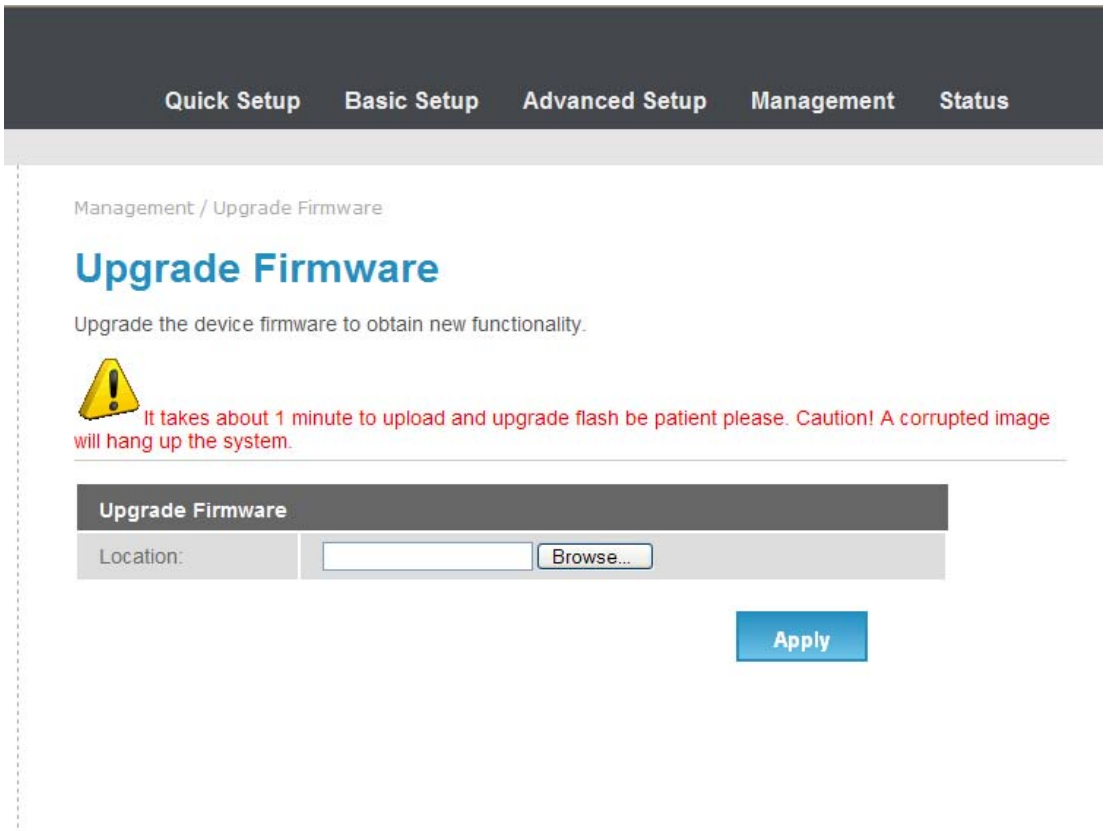


Figure 3.5.3-1

3.5.4. Upgrade PLC Firmware

Figure3.5.4-1 displays Upgrade PLC firmware information page

You can upgrade the PLC firmware of the devices paired. Make sure the firmware you want to use is on the local hard drive of the computer. Click on Browse to browse the local hard drive and locate the firmware to be used for the update.

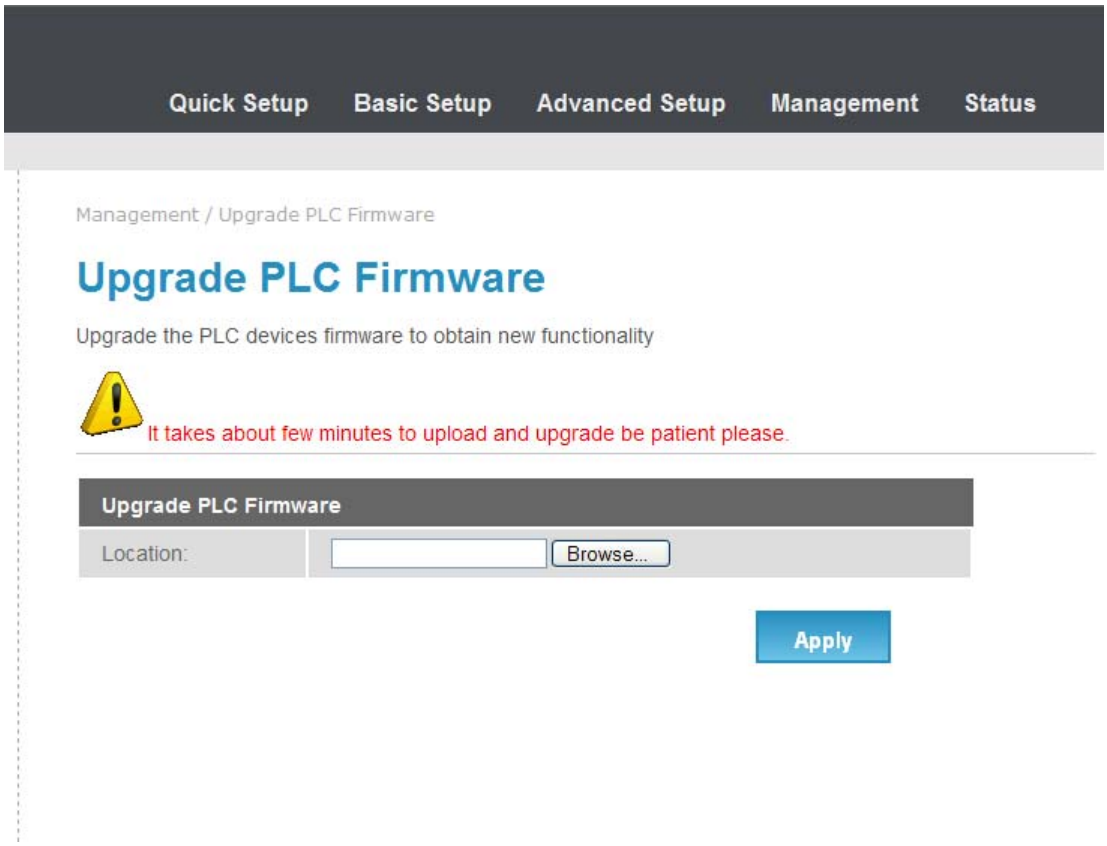


Figure 3.5.4-1

Upgrade PLC firmware function will update all devices which are in the same network.

3.5.5. System Restart

Figure3.5.5-1 displays system restart page

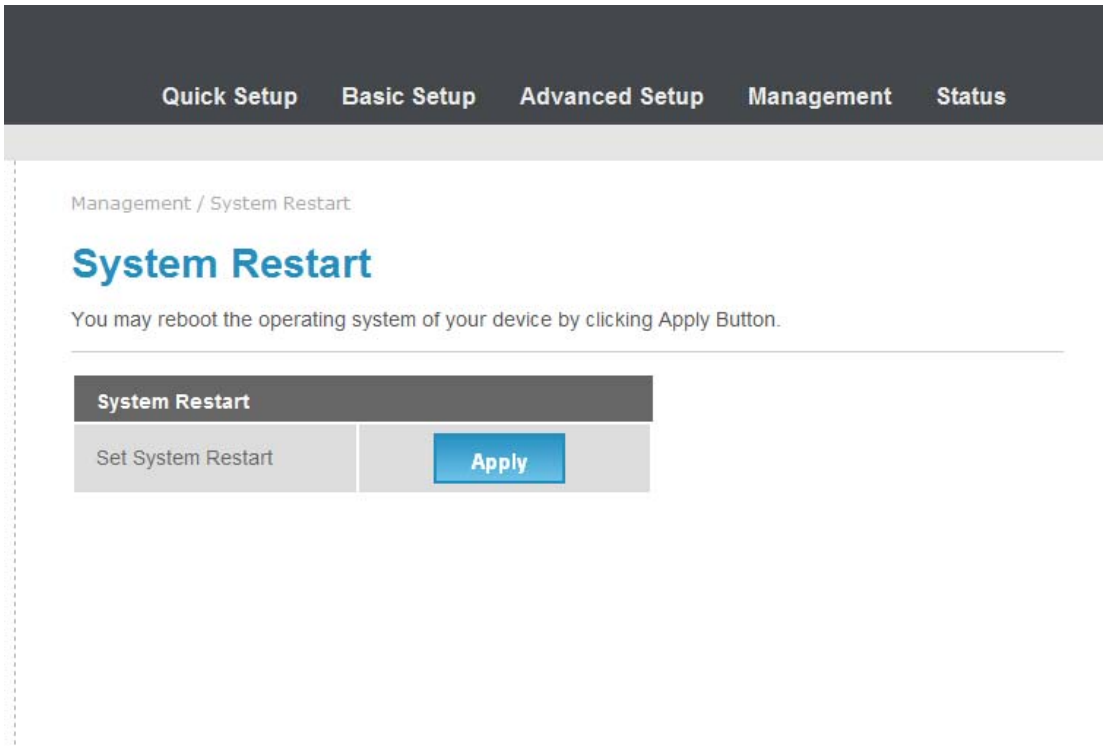


Figure 3.5.5-1

3.5.6. System Management

Figure3.5.6-1 displays system management setting page

The current system settings can be saved as a file onto the local hard drive. The saved file or any other saved setting file can be loaded back on the device. To reload a system settings file, click on Browse to browse the local hard drive and locate the system file to be used. You may also reset the device back to factory settings by clicking on load factory default settings.

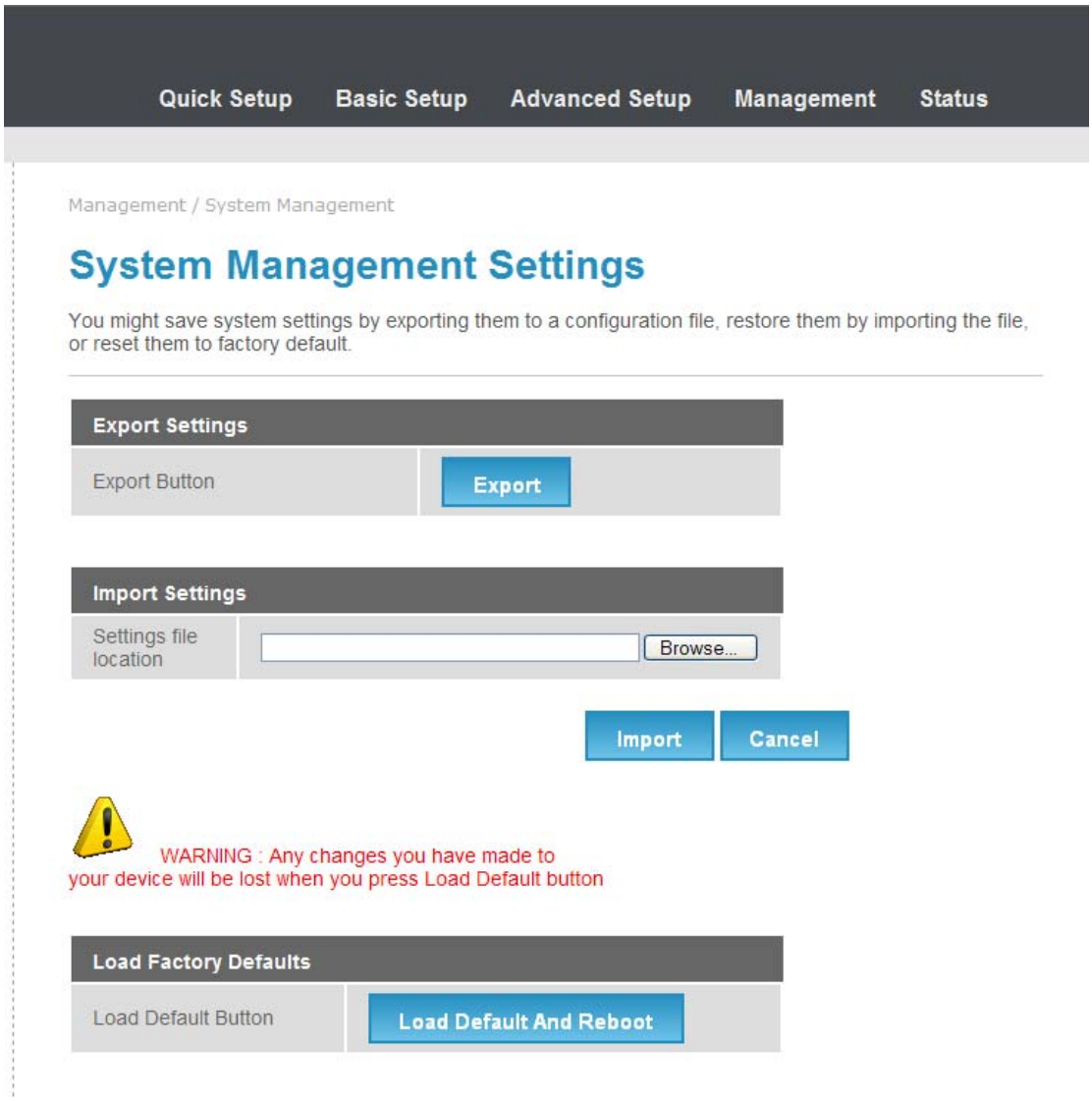


Figure 3.5.6-1

3.5.7. Administrator Settings

There is only one account that can access Web-Management interface. It is admin. Admin has read/write access privilege. In this web page, you can set new password for admin.

Figure3.5.7-1 display administrator settings information page

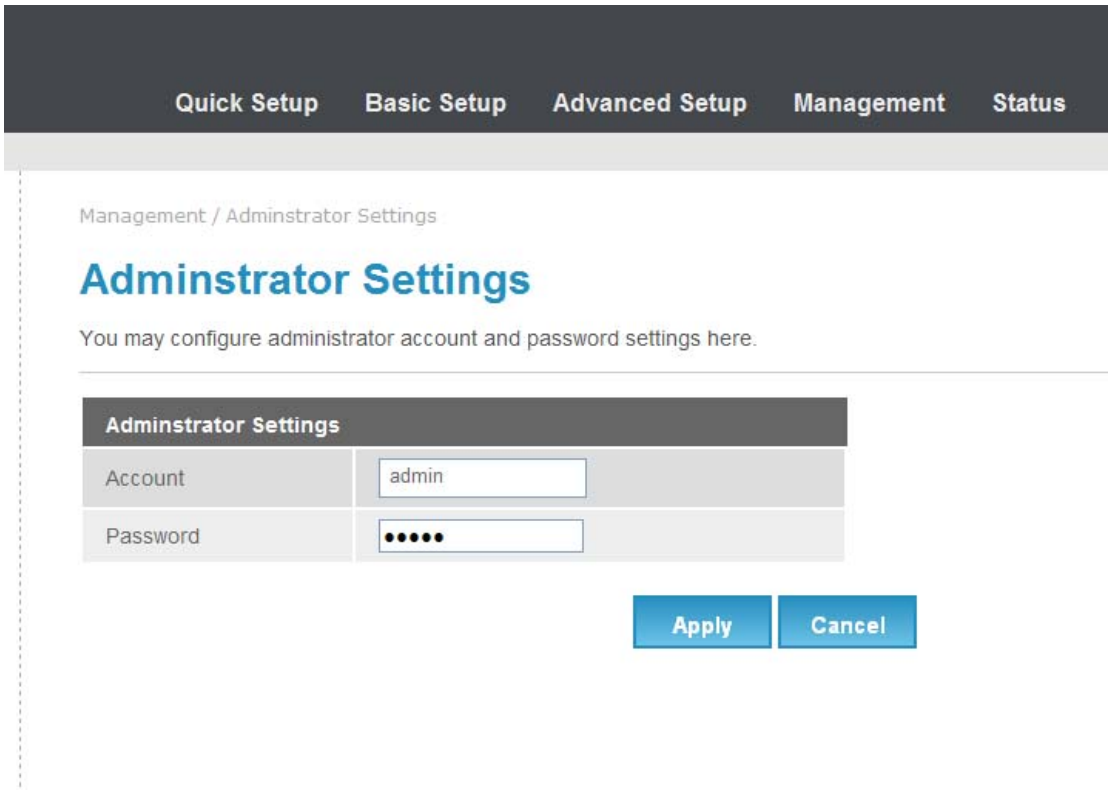


Figure 3.6-5

3.6. Status

Figure3.6-1 displays Status Menu List

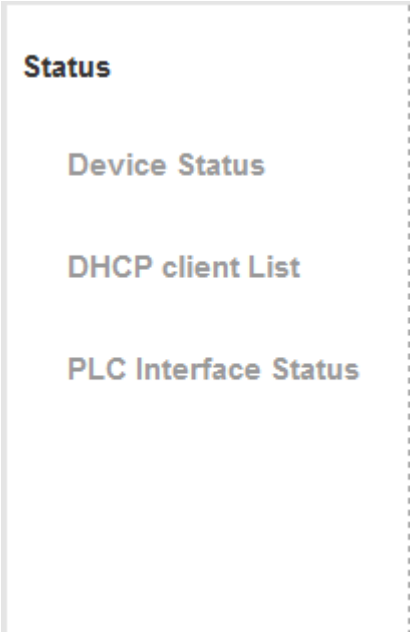


Figure 3.6-1

3.6.1. Device Status

Figure3.6.1-1 displays Device status information

This page displays the current information for the device. It will display the system info, Internet configuration, LAN information.

Quick Setup | Basic Setup | Advanced Setup | Management | Status

Device Information Status

Let's take a look at the status of PLC Platform.

System Info	
HwVersion	R02
FwVersion	V1.2_build_92
BootLoaderVersion	4.2.S.1
Serial Number	420013H14I000057
SDK Version	4.2.0.0 (Nov 26 2014)
System Up Time	9 mins, 18 secs
System Platform	MT7620 embedded switch
Operation Mode	Bridge Mode
Internet Configurations	
Connected Type	3G
WAN IP Address	
Subnet Mask	
Default Gateway	
Primary Domain Name Server	168.95.1.1
Secondary Domain Name Server	8.8.8.8
MAC Address	00:0C:43:76:20:77
Local Network	
Local IP Address	10.10.10.254
Local Netmask	255.255.255.0
MAC Address	00:0C:43:76:20:77

Figure 3.6.1-1

3.6.2. DHCP Client Status

Figure3.6.2-1 displays DHCP Client Status information
This page displays DHCP Client Status information for the device.

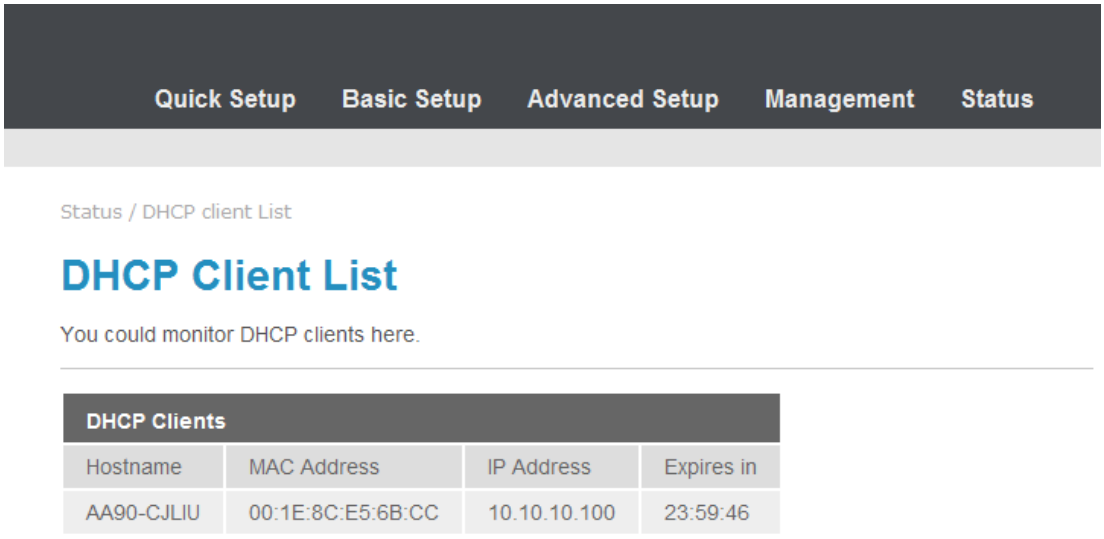


Figure 3.6.2-1

3.6.3. PLC Interface Status

Figure3.6.3-1 and Figure3.6.3-2 displays PLC interface status page

This page displays PLC interface status page information for the device.

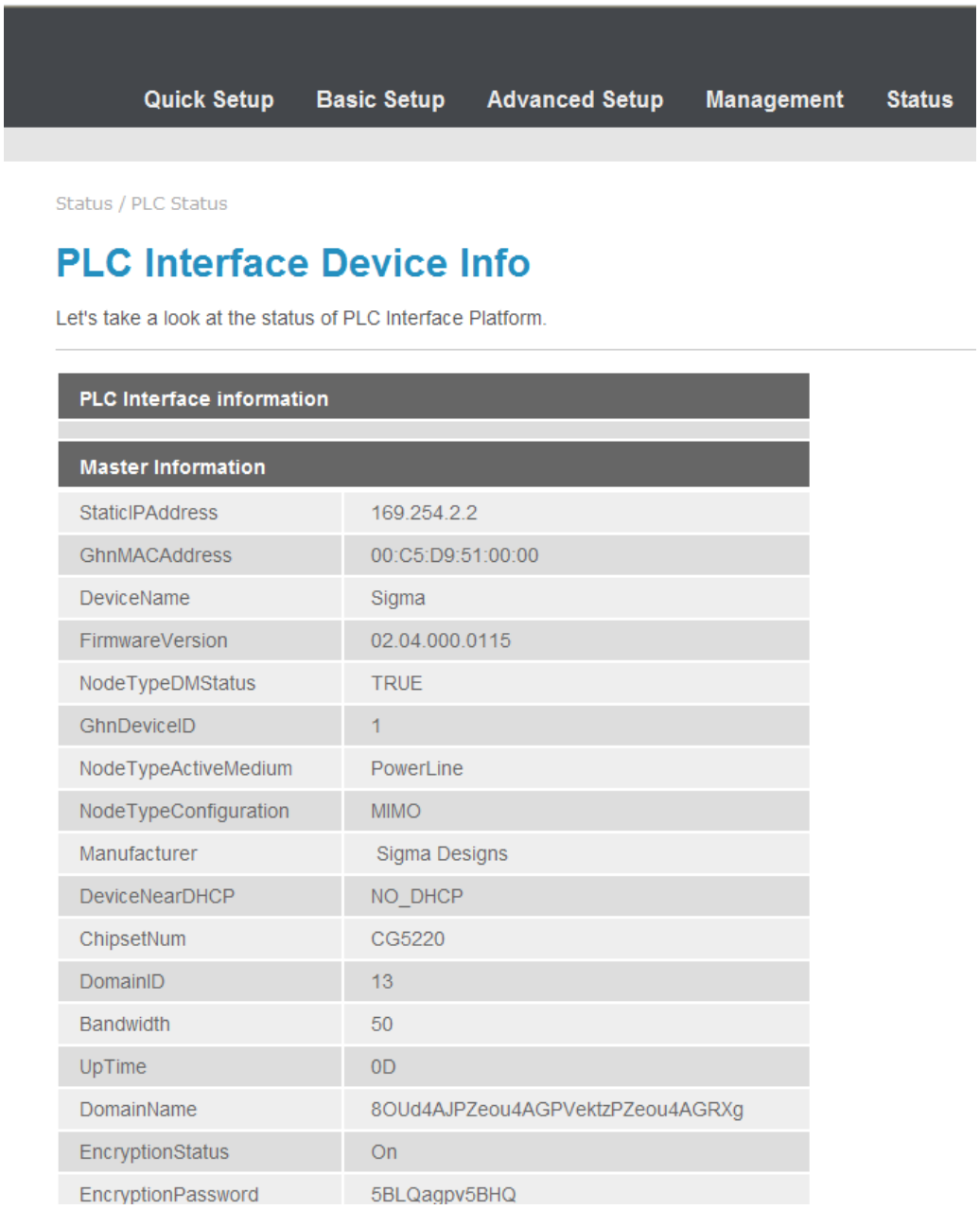


Figure 3.6.3-1

Slave Information	
StaticIPAddress	169.254.70.83
GhnMACAddress	00:19:15:DC:B1:A2
DeviceName	Sigma
FirmwareVersion	02.04.000.0115
NodeTypeDMStatus	FALSE
GhnDeviceID	2
NodeTypeActiveMedium	PowerLine
NodeTypeConfiguration	MIMO
Manufacturer	Sigma Designs
DeviceNearDHCP	NO_DHCP
ChipsetNum	CG5220
DomainID	13
Bandwidth	50
UpTime	0D
DomainName	8OUd4AJPZeou4AGPVektzPZeou4AGRXg
EncryptionStatus	On
EncryptionPassword	5BLQagpv5BHQ

Figure 3.6.3-2

PLC device have Master information and slave information.
It will support to display 10 slaves information.
Both devices display below information

- Static IP Address
- Dynamic IP Address
- Ghn MAC Address
- Name
- Firmware Version
- Node Type DM Status
- Ghn Device ID
- Node Type Active Medium
- Node Type Configuration
- Model Name
- Manufacturer
- Device Near DHCP
- ChipsetNum
- DomainID
- Bandwidth
- UpTime
- DomainName
- EncryptionStatus
- EncryptionPassword

FCC Warning

15.21 Information to users

Any changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

15.105 Information to users

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 or more of the following measures:

(1) Reorient or relocate the receiving antenna.

(2) Increase the separation between the equipment and receiver.

(3) Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

(4) Consult the dealer or an experienced radio/TV technician for help.

15.19 FCC Labelling requirements

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

1. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
2. This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.