WiFi Chime

C-1030

User Manual

Version: 2.0

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.

2 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,

EN55032 Class B for ITE and EN 50082-1. This meets the essential protection requirements of the European Council Directive 2014/53/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

©Copyright, 2010. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in retrieval system or translated in to any language or computer language, in any from or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of Owner (The Company).

The Company reserves the right to revise the publication and make changes from time to time in the contents hereof without obligation of this company to notify person of such revision or changes. The material contained herein is supplied without representation or warranty of any kind. The Company therefore assumes no responsibility and shall have no liability of any kind arising from the supply or use of this document or the material contained herein.

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	2nd version for C-1030 User Manual.	Sony

1. PRODUCT OVERVIEW

C-1030, networking standard compliant 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 Wireless. Installation at home (or in a small office) is quick and easy as the C1030 comes with plug-and-play technology.

C-1030 supports (802.11n 1x1) operation based on WSC-N101 module 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:

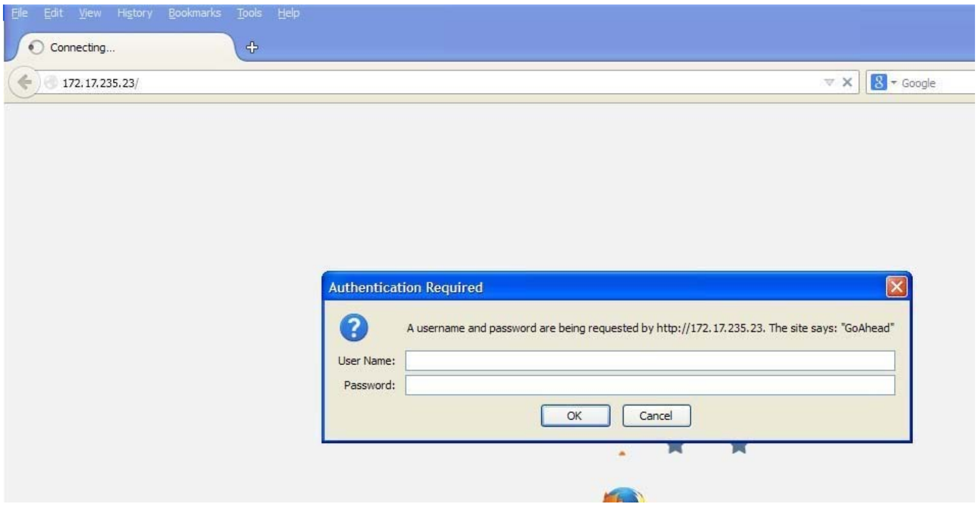
- Performance

  Support ITU-T G.hn baseband plans 25, 50, 100 and 150 MHz and MIMO techniques for powerline (based on G.9963) boosting to prevent noise interference from other home appliances.

3. C-1030 Web Configuration

3.1. Login Page

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



A username and password are being requested by http://172.17.235.23. The site says: "GoAhead"

User Name:

Password:

Figure 3.1-1

The default IP address of the C-1030 Wireless is 10.10.10.254

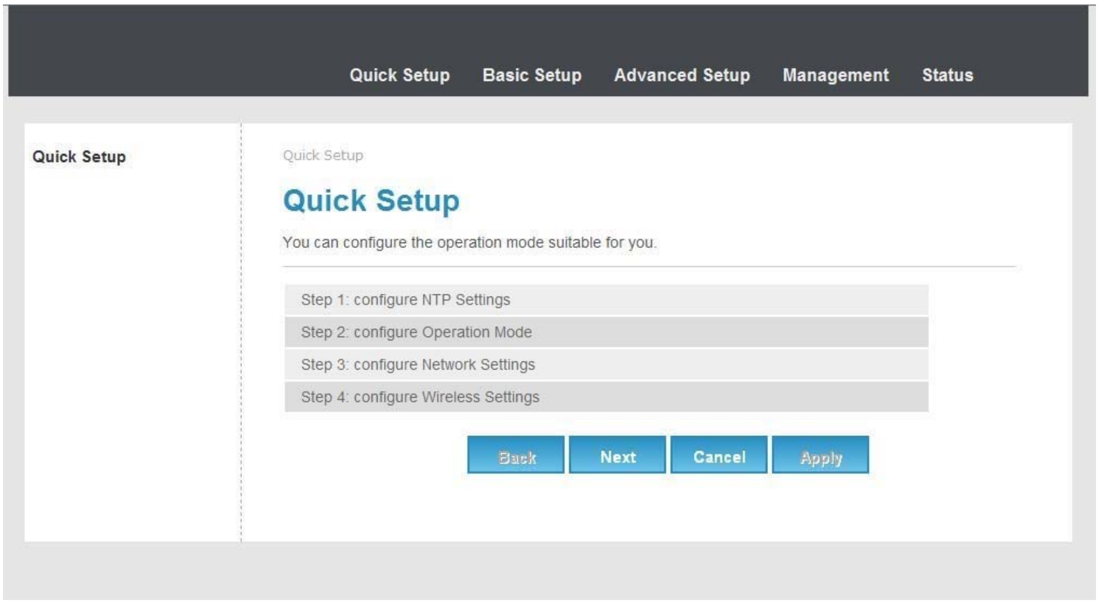
Username: admin

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.



Quick Setup

You can configure the operation mode suitable for you.

Step 1: configure NTP Settings

Step 2: configure Operation Mode

Step 3: configure Network Settings

Step 4: configure Wireless Settings

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

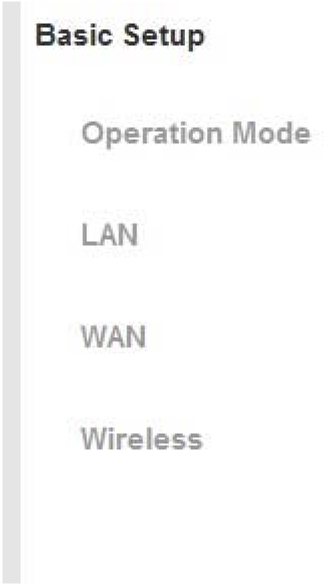
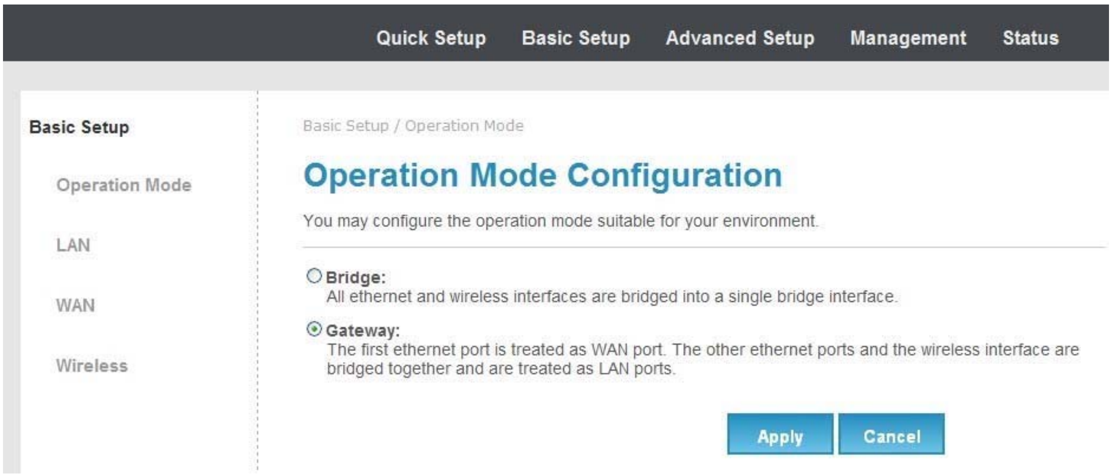


Figure 3.3-1

3.3.1. Operation Mode

Figure3.3.1-1 displays operation mode settings



Operation Mode Configuration

You may configure the operation mode suitable for your environment.

○ Bridge:
All ethernet and wireless interfaces are bridged into a single bridge interface.

● Gateway:
The first ethernet port is treated as WAN port. The other ethernet ports and the wireless interface are bridged together and are treated as LAN ports.

Figure 3.3.1-1

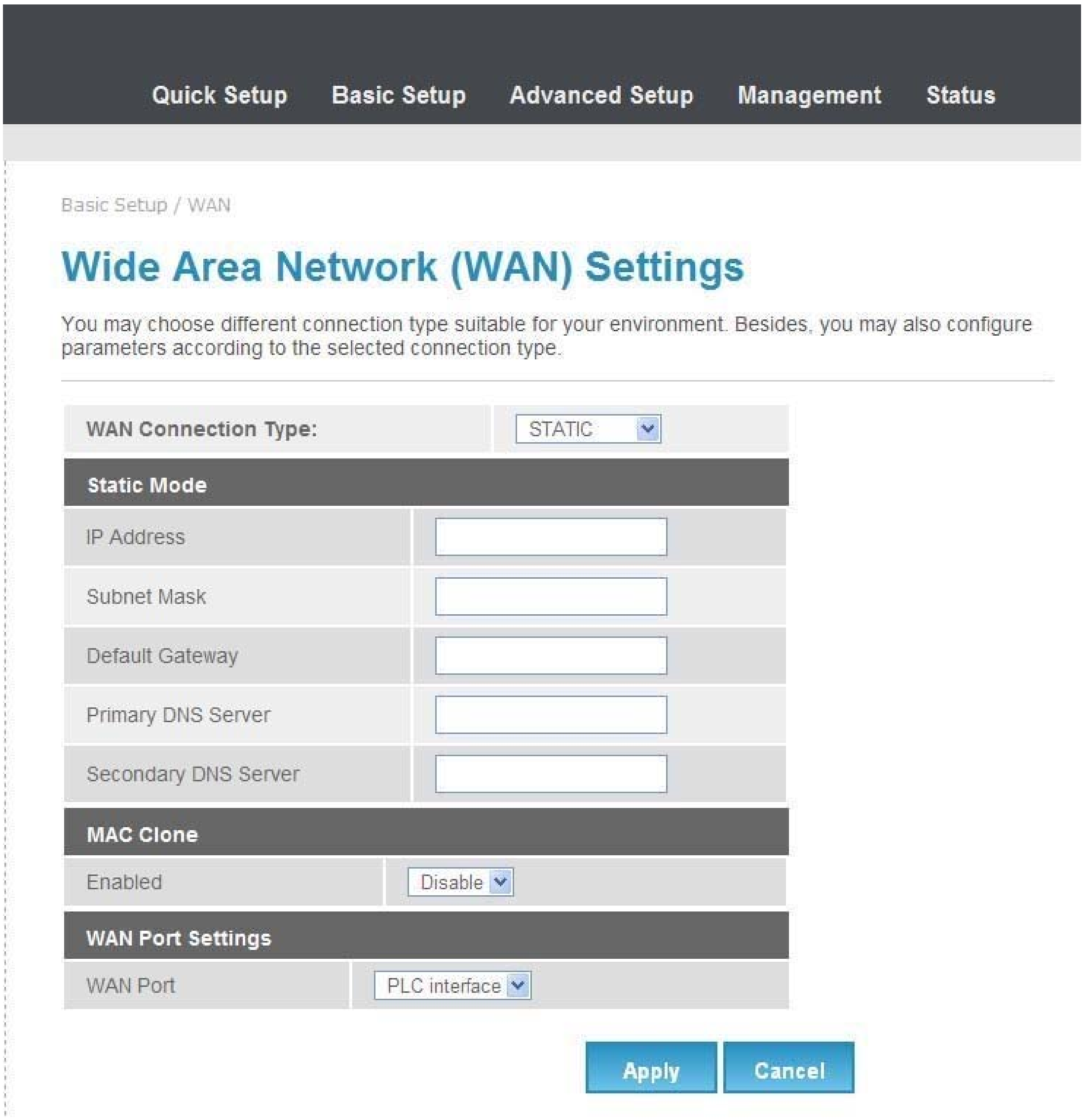
In this page we can set bridge mode or gateway mode

3.3.2. 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



Basic Setup / WAN

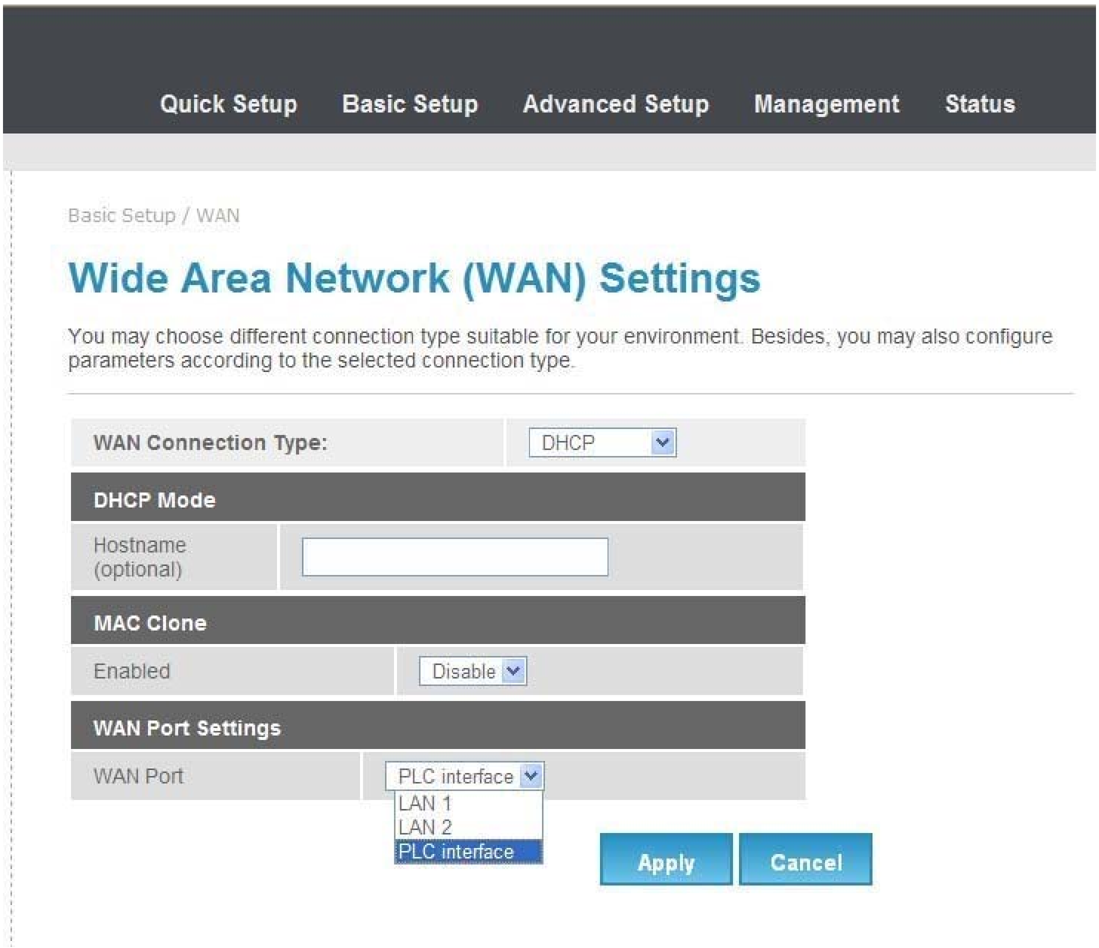
Wide Area Network (WAN) Settings

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:	STATIC
Static Mode	
IP Address	
Subnet Mask	
Default Gateway	
Primary DNS Server	
Secondary DNS Server	
MAC Clone	
Enabled	Disable
WAN Port Settings	
WAN Port	PLC interface

Figure3.3.3-1

Configure DHCP connection type as below



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: DHCP

DHCP Mode

Hostname (optional)

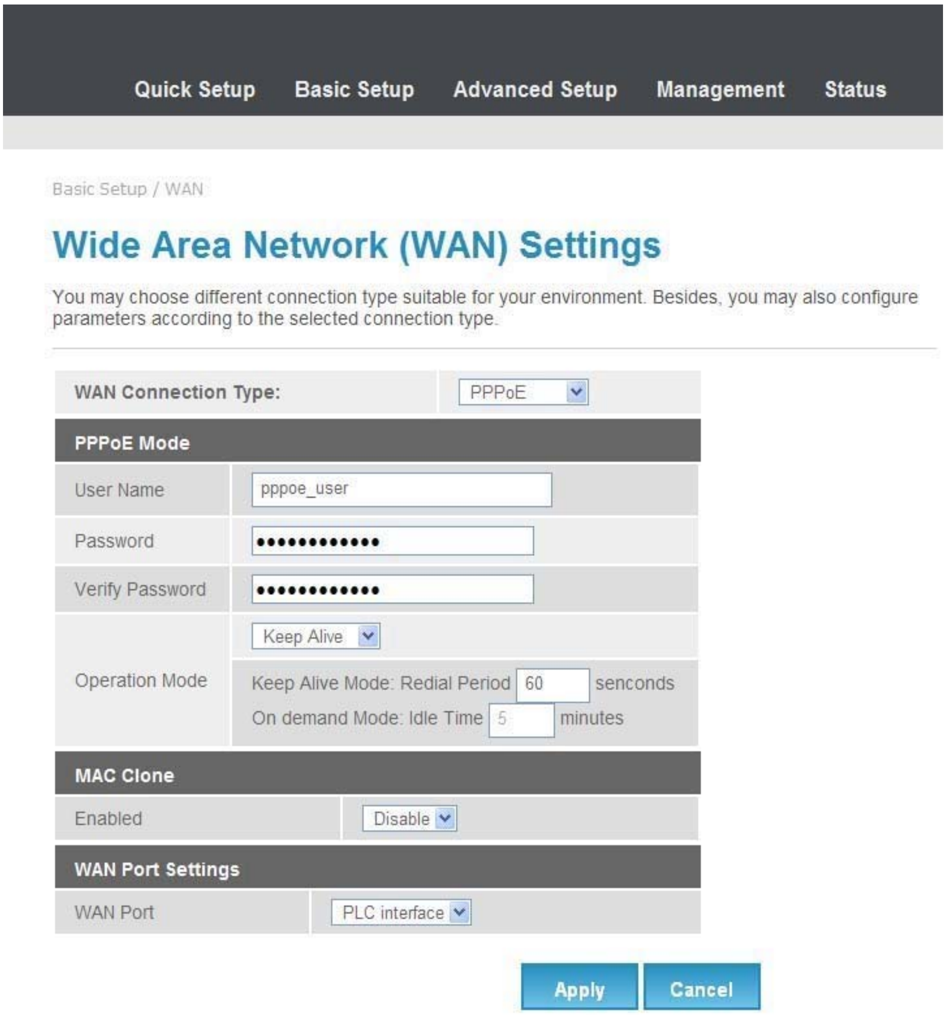
MAC Clone

Enabled: Disable

WAN Port Settings

WAN Port: PLC interface

Figure3.3.3-2



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:	PPPoE
PPPoE Mode	
User Name	pppoe_user
Password	•••••••••••••
Verify Password	•••••••••••••
Operation Mode	Keep Alive Keep Alive Mode: Redial Period 60 senconds On demand Mode: Idle Time 5 minutes
MAC Clone	
Enabled	Disable
WAN Port Settings	
WAN Port	PLC interface

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.

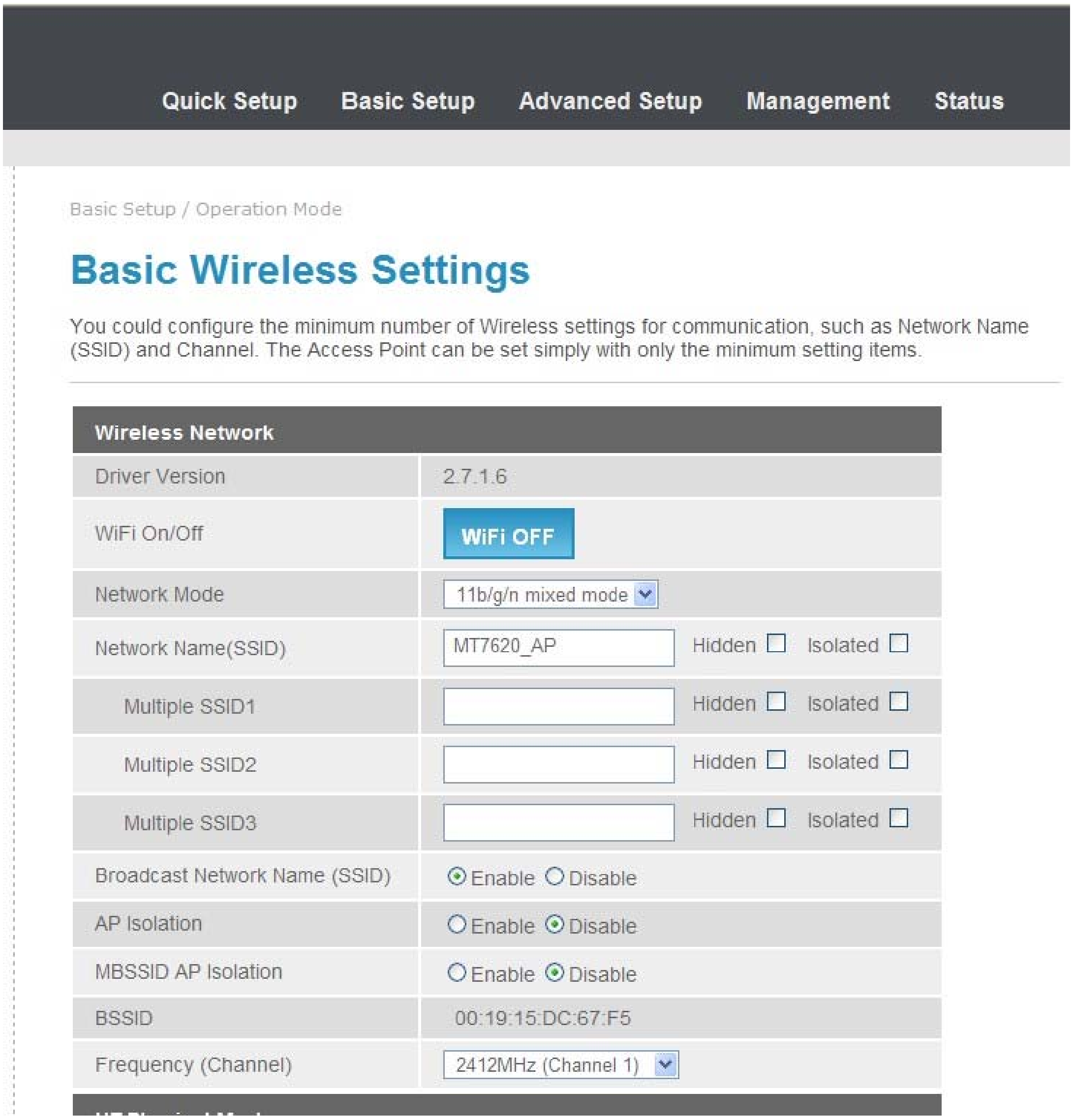
Username: Enter your username for your PPPoE connection. Password: Enter your password for your PPPoE connection

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.

3.3.3. 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.



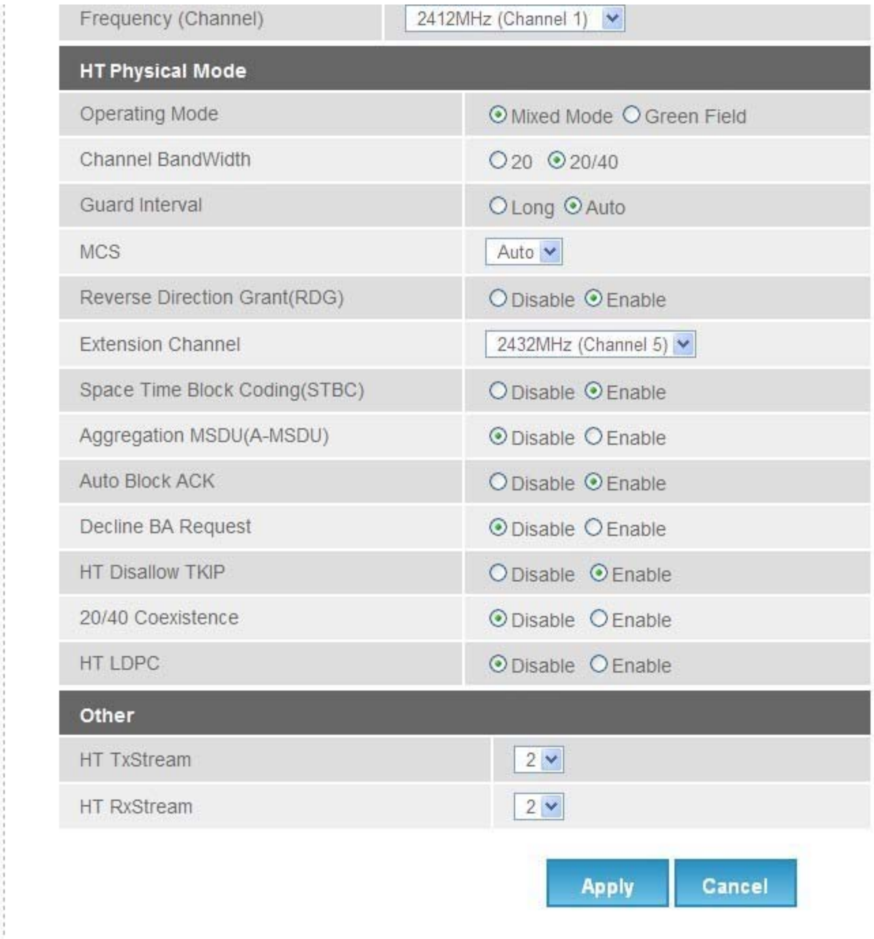
Basic Setup / Operation Mode

Basic Wireless Settings

You could configure the minimum number of Wireless settings for communication, such as Network Name (SSID) and Channel. The Access Point can be set simply with only the minimum setting items.

Wireless Network	
Driver Version	2.7.1.6
WiFi On/Off	WiFi OFF
Network Mode	11b/g/n mixed mode
Network Name(SSID)	MT7620_AP Hidden □ Isolated □
Multiple SSID1	Hidden □ Isolated □
Multiple SSID2	Hidden □ Isolated □
Multiple SSID3	Hidden □ Isolated □
Broadcast Network Name (SSID)	● Enable ○ Disable
AP Isolation	○ Enable ● Disable
MBSSID AP Isolation	○ Enable ● Disable
BSSID	00:19:15:DC:67:F5
Frequency (Channel)	2412MHz (Channel 1)

Figure 3.3.4-1



Frequency (Channel)	2412MHz (Channel 1)
HT Physical Mode	
Operating Mode	● Mixed Mode ○ Green Field
Channel BandWidth	○ 20 ● 20/40
Guard Interval	○ Long ● Auto
MCS	Auto
Reverse Direction Grant(RDG)	○ Disable ● Enable
Extension Channel	2432MHz (Channel 5)
Space Time Block Coding(STBC)	○ Disable ● Enable
Aggregation MSDU(A-MSDU)	● Disable ○ Enable
Auto Block ACK	○ Disable ● Enable
Decline BA Request	● Disable ○ Enable
HT Disallow TKIP	○ Disable ● Enable
20/40 Coexistence	● Disable ○ Enable
HT LDPC	● Disable ○ Enable
Other	
HT TxStream	2
HT RxStream	2

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.

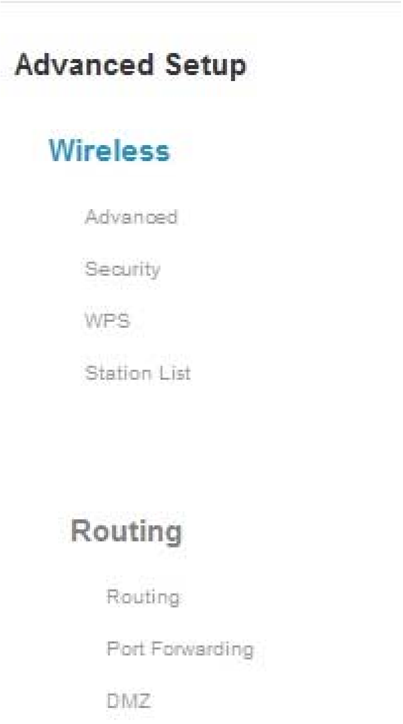
Broadcast SSID:

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


Advanced Setup

Wireless

Advanced

Security

WPS

Station List

Routing

Routing

Port Forwarding

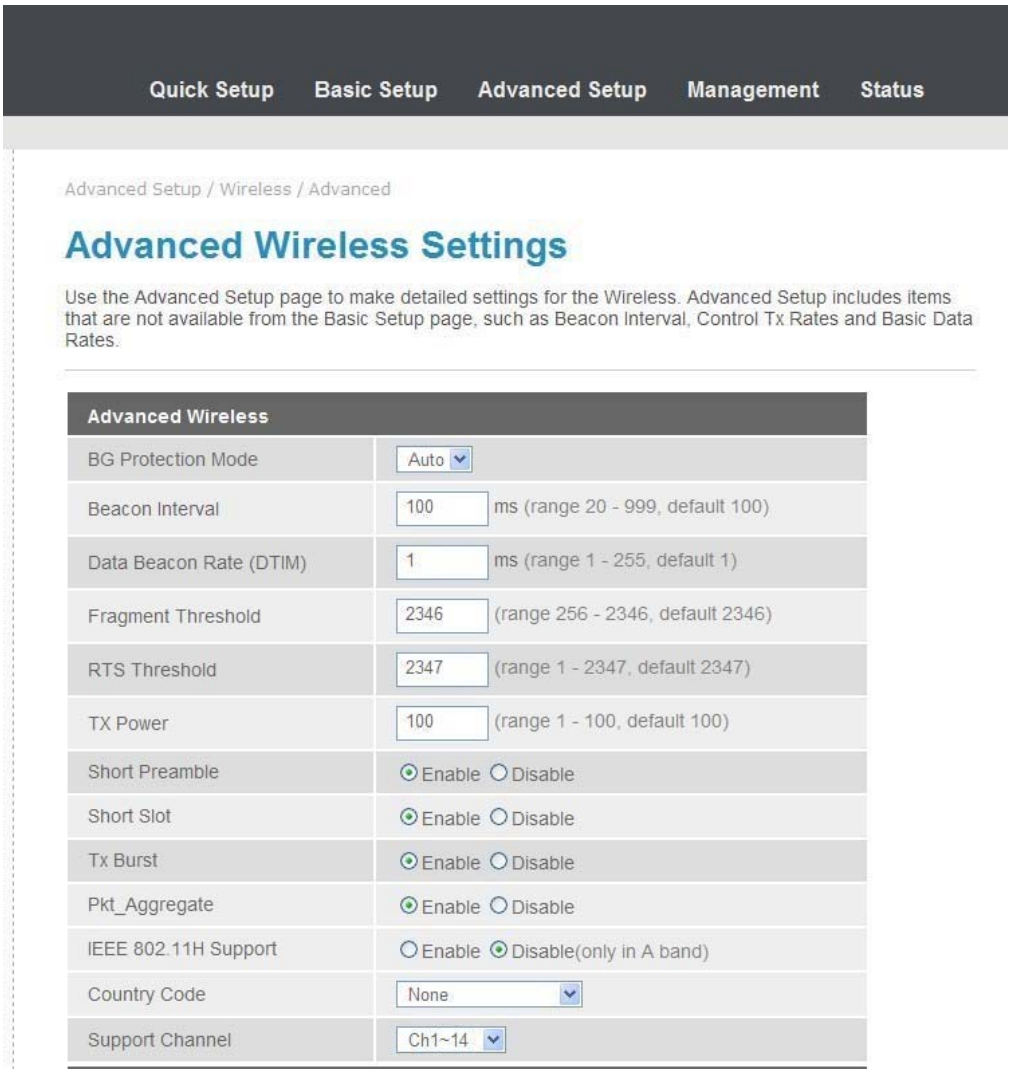
DMZ

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.

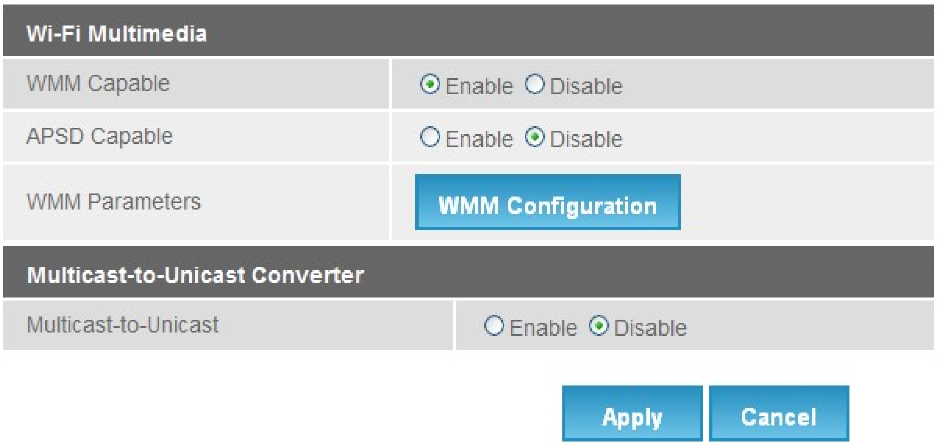


Advanced Wireless Settings

Use the Advanced Setup page to make detailed settings for the Wireless. Advanced Setup includes items that are not available from the Basic Setup page, such as Beacon Interval, Control Tx Rates and Basic Data Rates.

Advanced Wireless	
BG Protection Mode	Auto
Beacon Interval	100 ms (range 20 - 999, default 100)
Data Beacon Rate (DTIM)	1 ms (range 1 - 255, default 1)
Fragment Threshold	2346 (range 256 - 2346, default 2346)
RTS Threshold	2347 (range 1 - 2347, default 2347)
TX Power	100 (range 1 - 100, default 100)
Short Preamble	● Enable ○ Disable
Short Slot	● Enable ○ Disable
Tx Burst	● Enable ○ Disable
Pkt_Aggregate	● Enable ○ Disable
IEEE 802.11H Support	○ Enable ● Disable(only in A band)
Country Code	None
Support Channel	Ch1~14

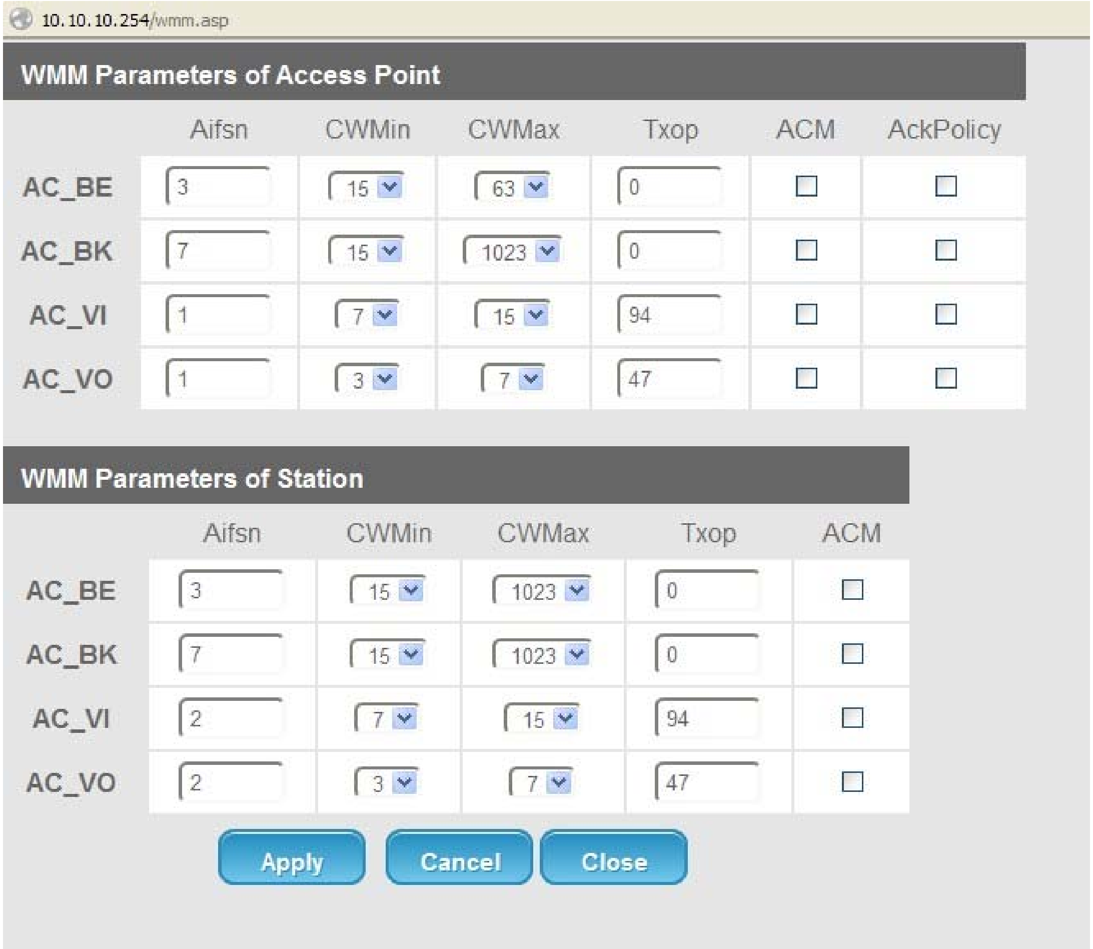
Figure 3.4.1-1



Wi-Fi Multimedia	
WMM Capable	● Enable ○ Disable
APSD Capable	○ Enable ● Disable
WMM Parameters	WMM Configuration

Multicast-to-Unicast Converter	
Multicast-to-Unicast	○ Enable ● Disable

Figure 3.4.1-2



10.10.10.254/wmm.asp

WMM Parameters of Access Point

	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	15	63	0	□	□
AC_BK	7	15	1023	0	□	□
AC_VI	1	7	15	94	□	□
AC_VO	1	3	7	47	□	□

WMM Parameters of Station

	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	1023	0	□
AC_BK	7	15	1023	0	□
AC_VI	2	7	15	94	□
AC_VO	2	3	7	47	□

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.

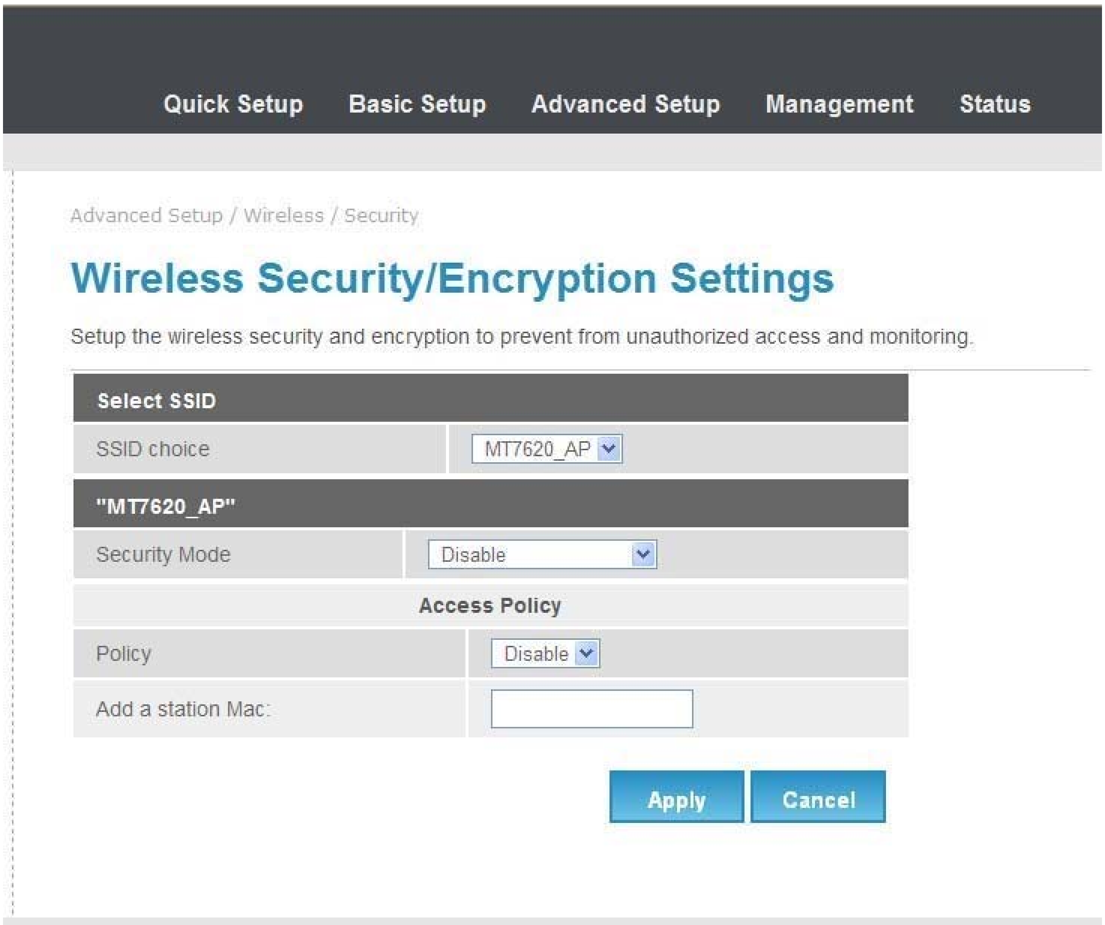
DTIM
This value, between 1 and 255, indicates the interval of the Delivery Traffic Indication Message (DTIM).

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

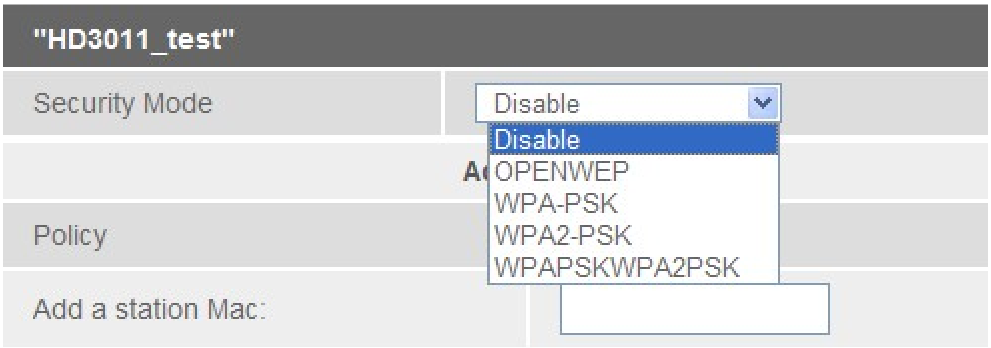


Wireless Security/Encryption Settings

Setup the wireless security and encryption to prevent from unauthorized access and monitoring.

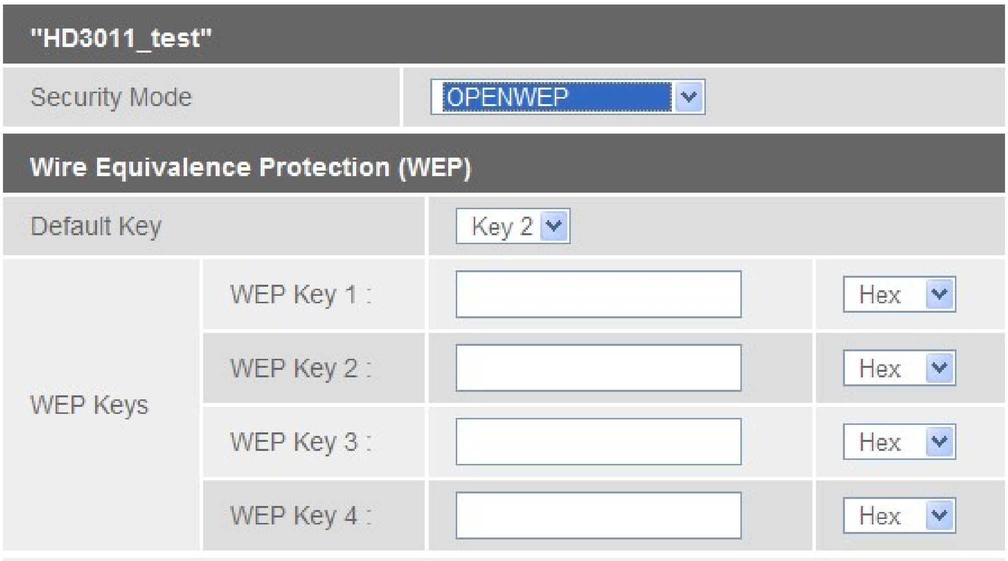
Select SSID	
SSID choice	MT7620_AP
"MT7620_AP"	
Security Mode	Disable
Access Policy	
Policy	Disable
Add a station Mac:	

Figure 3.4.2-1



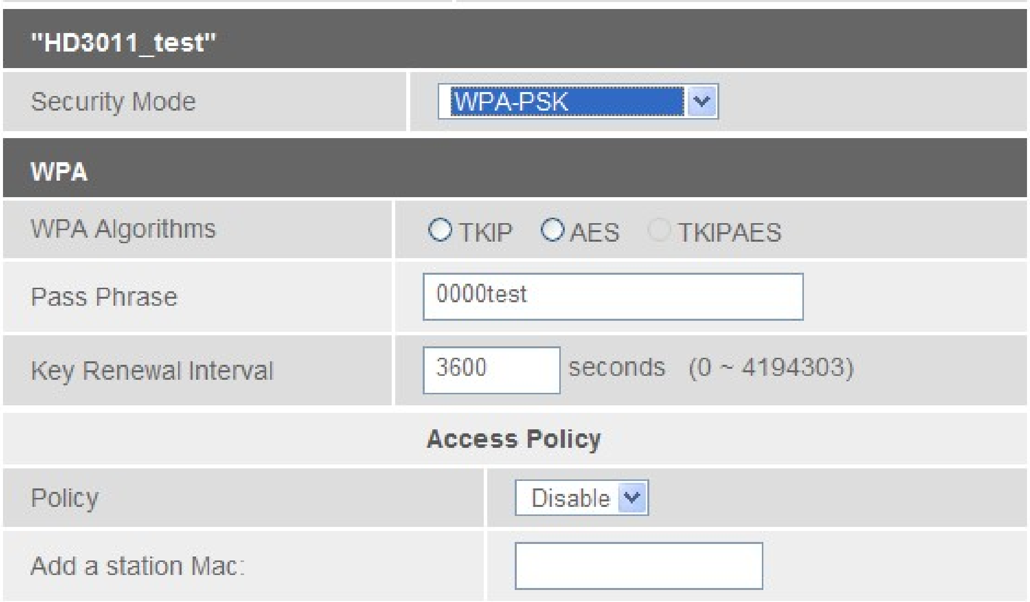
"HD3011_test"	
Security Mode	Disable
Policy	
Add a station Mac:	

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.

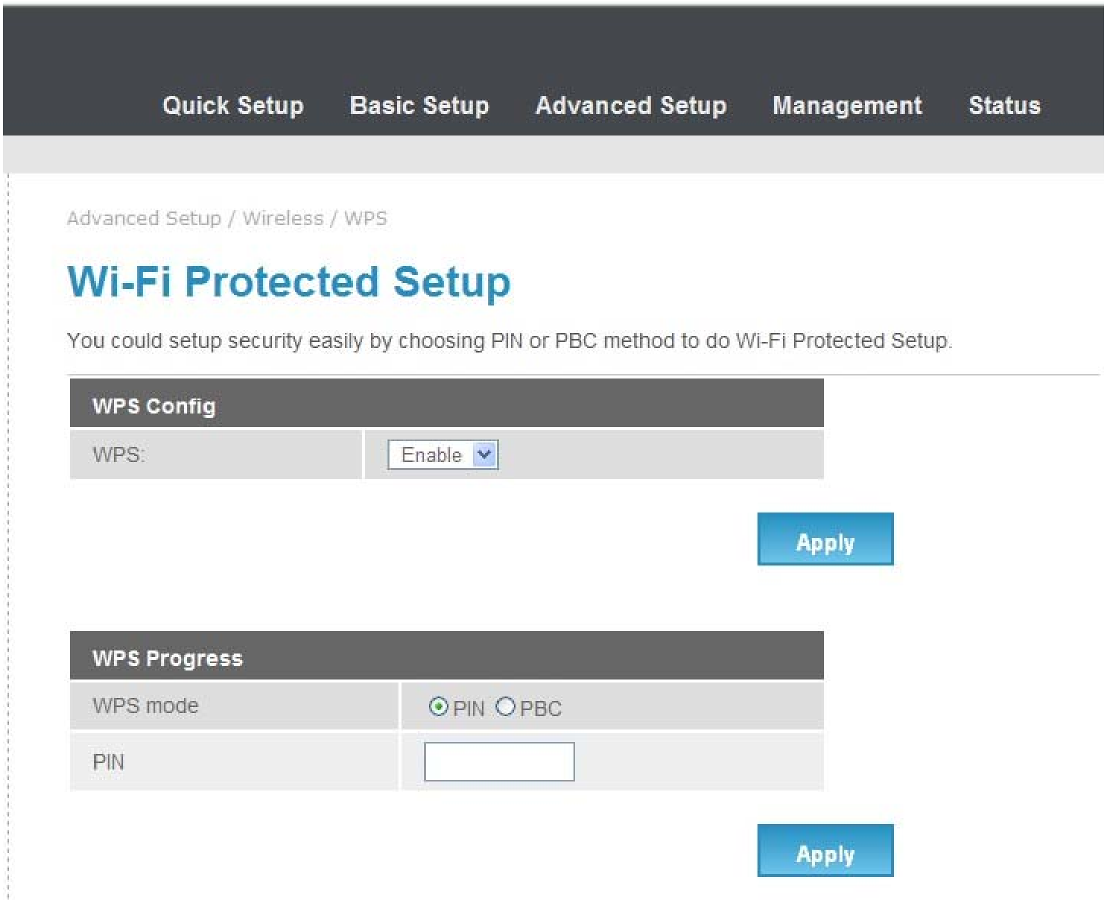
TKIPAES

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.



Advanced Setup / Wireless / WPS

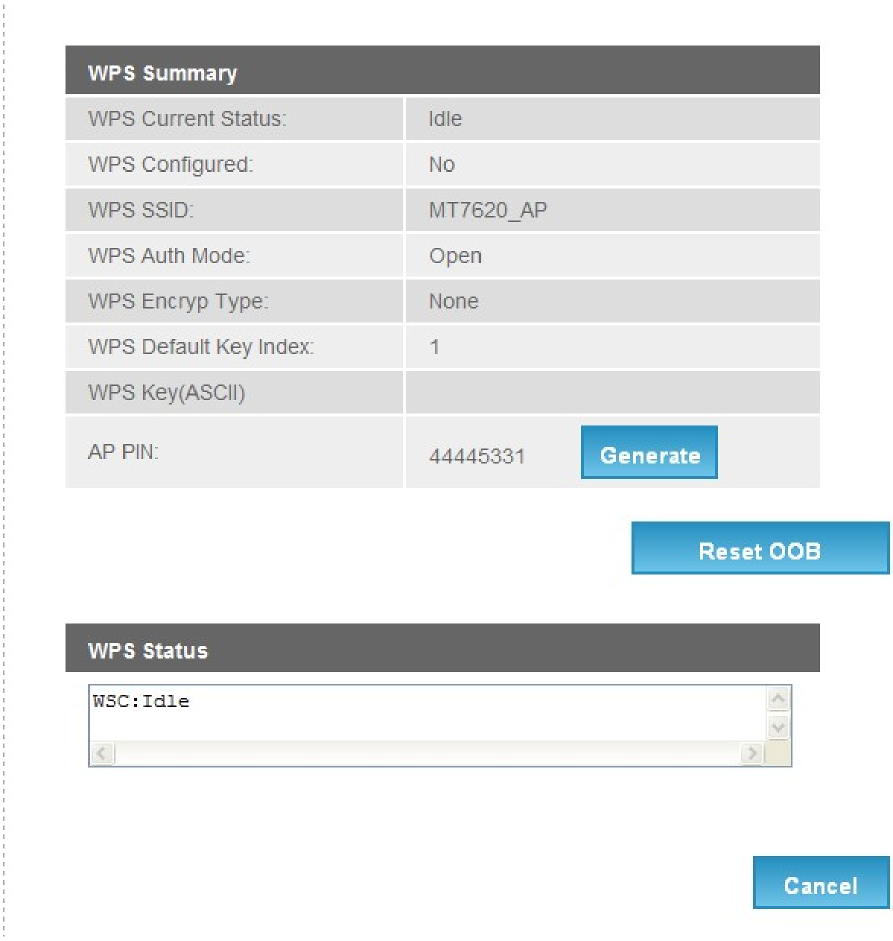
Wi-Fi Protected Setup

You could setup security easily by choosing PIN or PBC method to do Wi-Fi Protected Setup.

WPS Config	
WPS:	Enable

WPS Progress	
WPS mode	● PIN ○ PBC
PIN	

Figure 3.4.3-1



WPS Summary	
WPS Current Status:	Idle
WPS Configured:	No
WPS SSID:	MT7620_AP
WPS Auth Mode:	Open
WPS Encryp Type:	None
WPS Default Key Index:	1
WPS Key(ASCII)	
AP PIN:	44445331

WPS Status

```
WSC:Idle
```

Figure 3.4.3-2

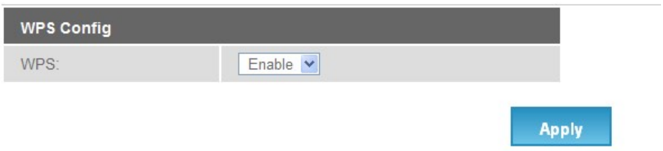
WPS Settings
There two WPS mode, one is PIN code and other one is PBC.

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 WPScertified 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.



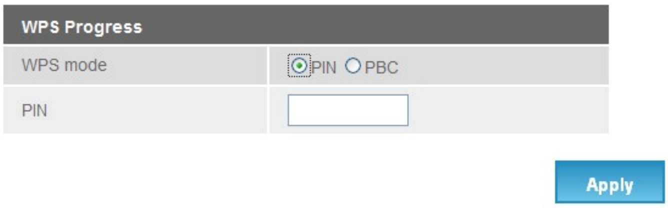
WPS Config

WPS:	Enable

2. For Pin method

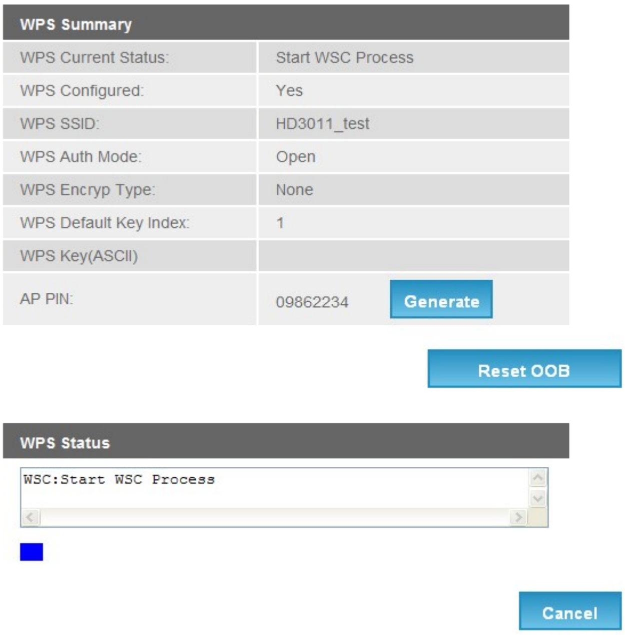
1). Select radio button PIN method.

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”.



WPS Progress

WPS mode	● PIN ○ PBC
PIN	



WPS Summary	
WPS Current Status:	Start WSC Process
WPS Configured:	Yes
WPS SSID:	HD3011_test
WPS Auth Mode:	Open
WPS Encryp Type:	None
WPS Default Key Index:	1
WPS Key(ASCII)	
AP PIN:	09862234

WPS Status

```
WSC:Start WSC Process
```

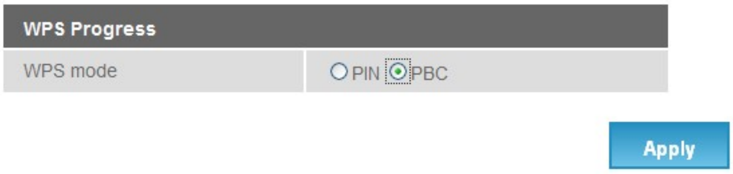
3. For PBC at Web

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.

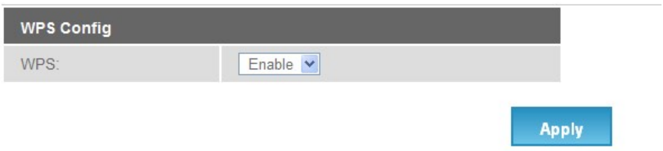
3). Once connected, "WPS current status" will be put "Connected".



WPS Progress	
WPS mode	○ PIN ● PBC

4. For physical PBC on the housing:

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



WPS Config

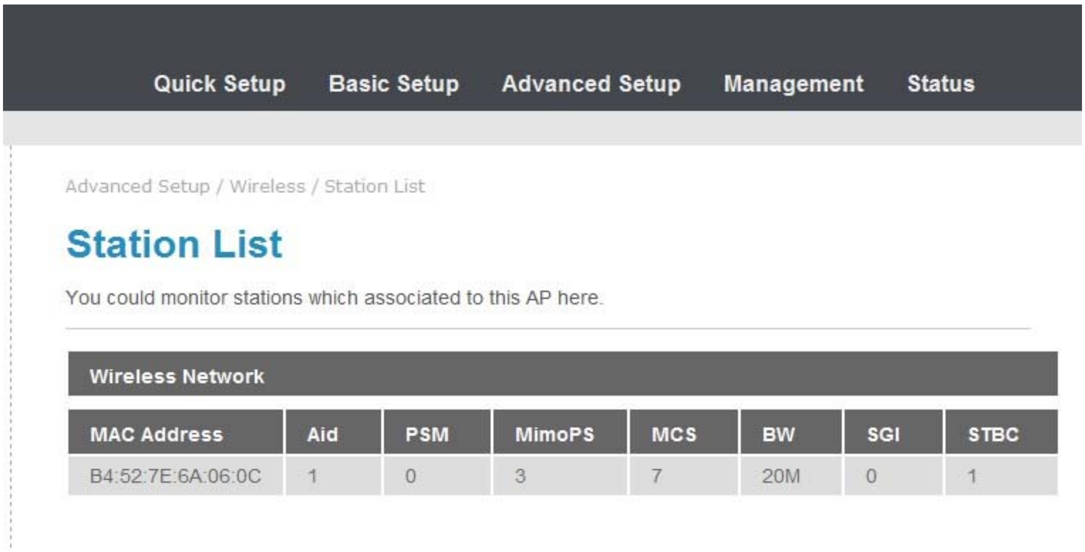
WPS: Enable

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



Advanced Setup / Wireless / Station List

Station List

You could monitor stations which associated to this AP here.

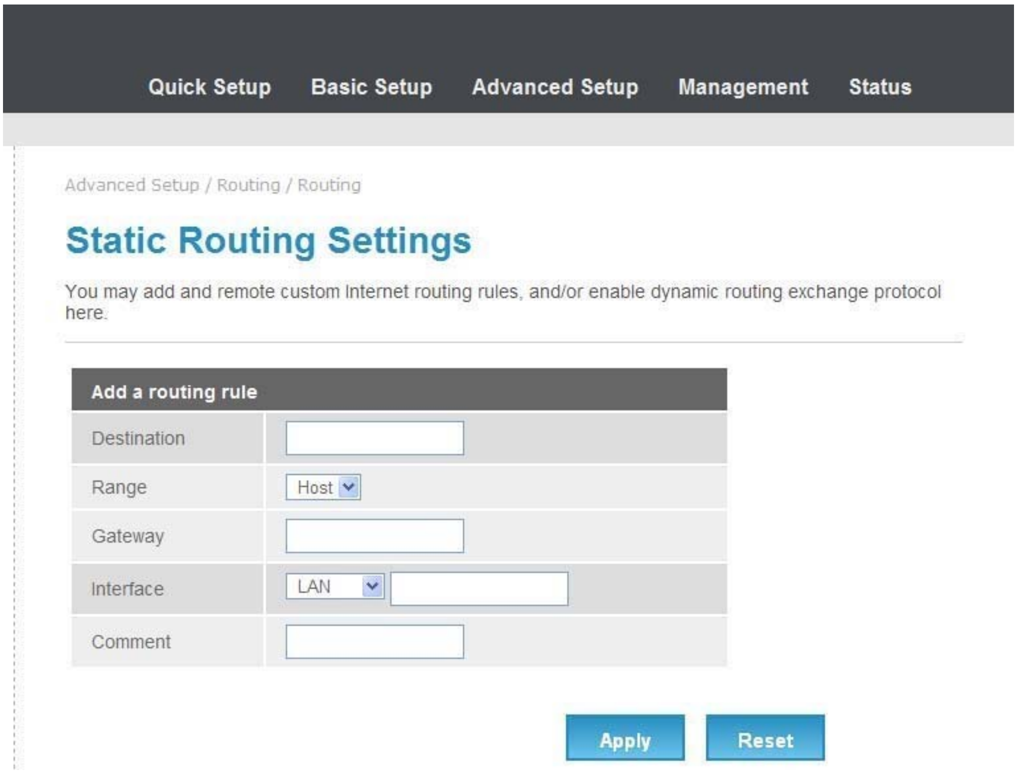
Wireless Network

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

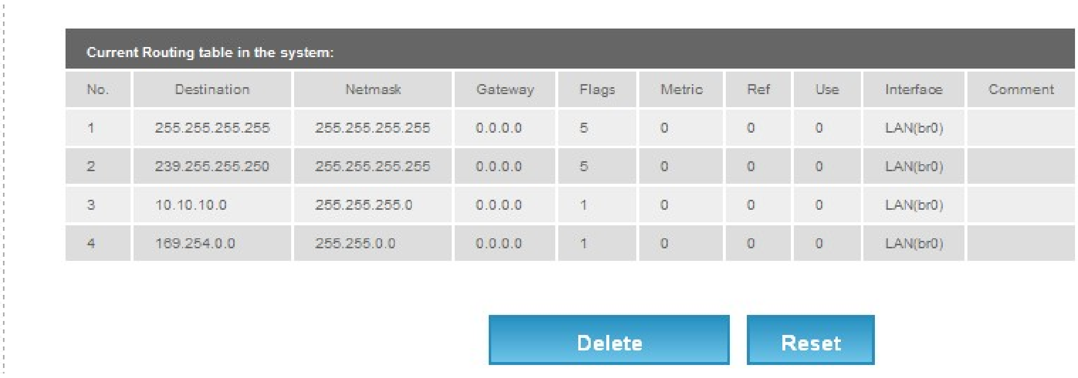


Static Routing Settings

You may add and remote custom Internet routing rules, and/or enable dynamic routing exchange protocol here.

Add a routing rule	
Destination	
Range	Host
Gateway	
Interface	LAN
Comment	

Figure 3.4.5-1



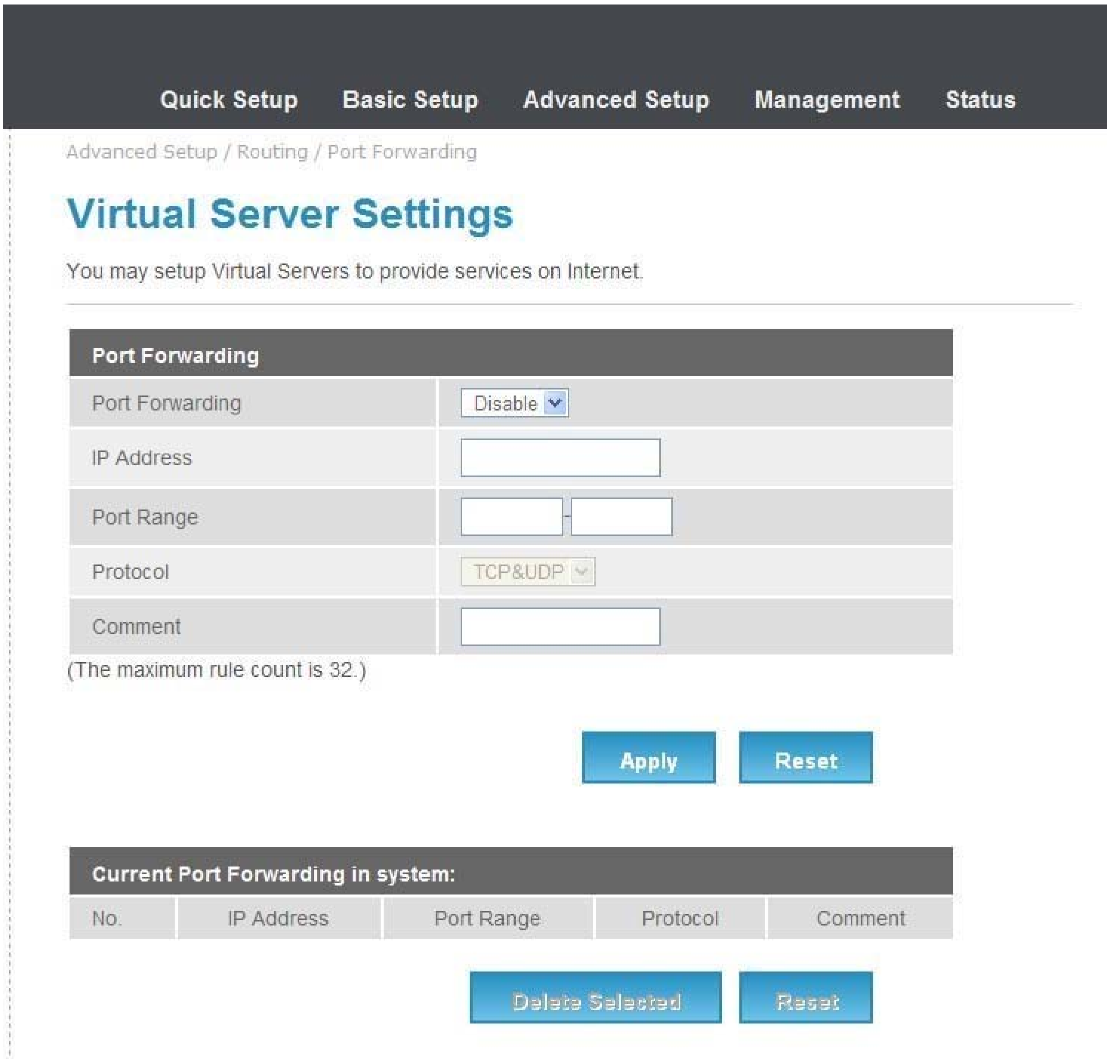
Current Routing table in the system:

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	10.10.10.0	255.255.255.0	0.0.0.0	1	0	0	0	LAN(br0)	
4	169.254.0.0	255.255.0.0	0.0.0.0	1	0	0	0	LAN(br0)	

Figure 3.4.5-2

3.4.6. Port Forwarding

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



Advanced Setup / Routing / Port Forwarding

Virtual Server Settings

You may setup Virtual Servers to provide services on Internet.

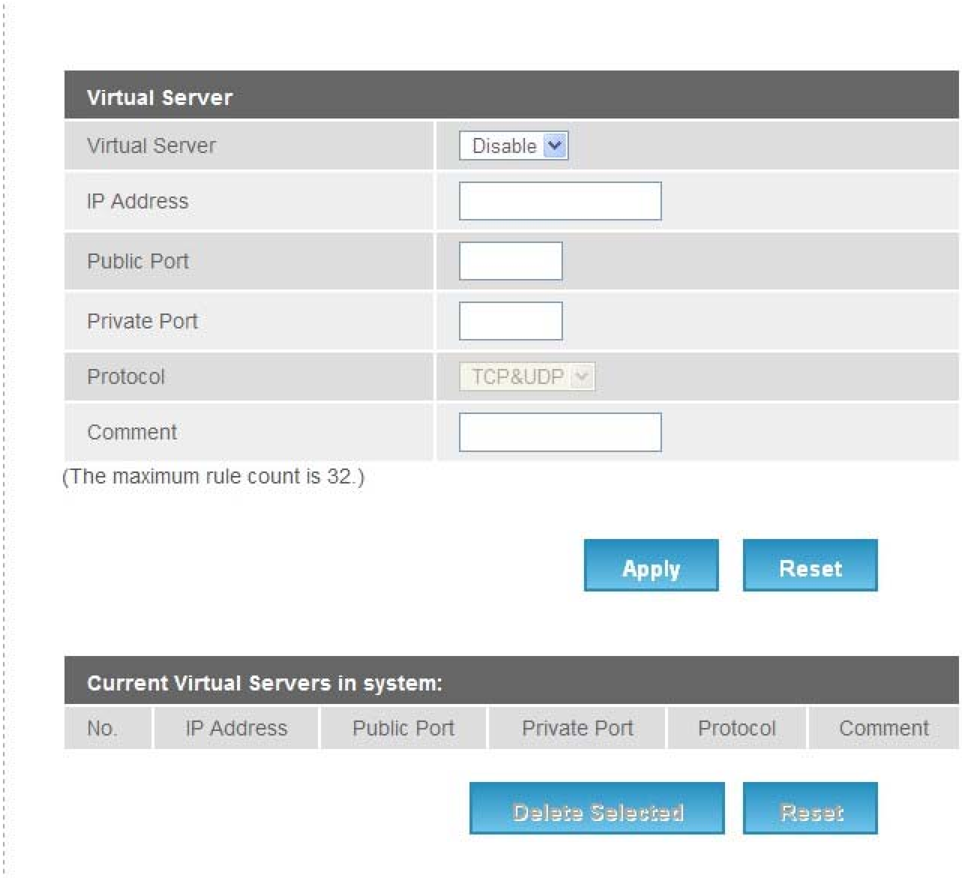
Port Forwarding	
Port Forwarding	Disable
IP Address	
Port Range	-
Protocol	TCP&UDP
Comment	

(The maximum rule count is 32.)

Current Port Forwarding in system:

No.	IP Address	Port Range	Protocol	Comment

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.)

Current Virtual Servers in system:

No.	IP Address	Public Port	Private Port	Protocol	Comment

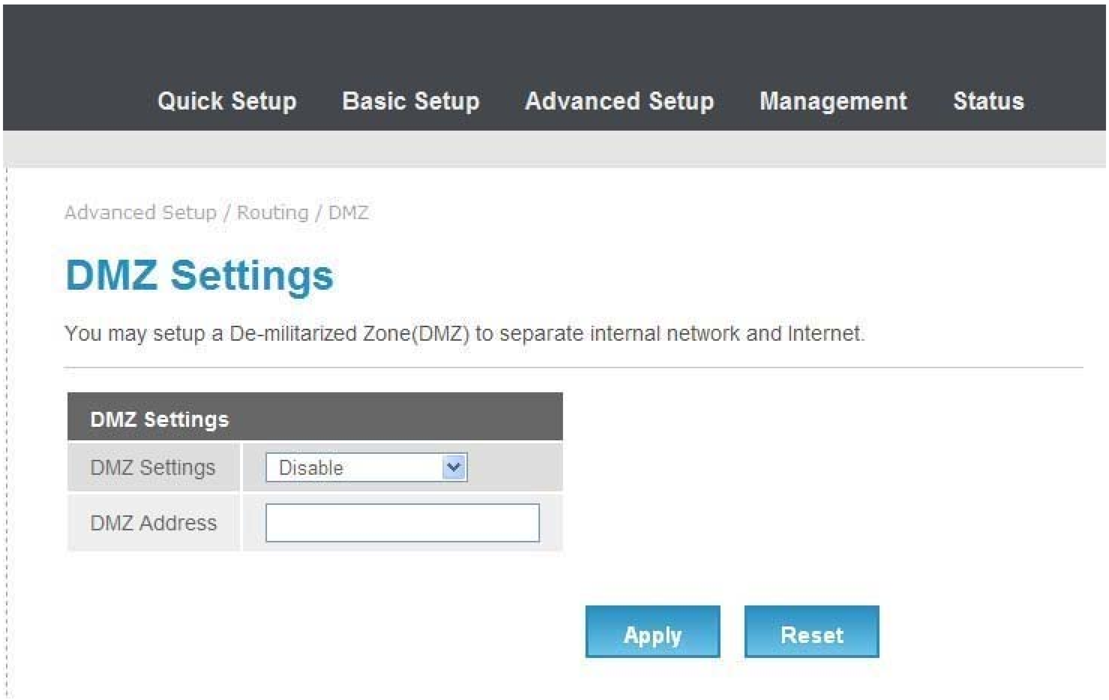
Figure 3.4.6-2

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.



Advanced Setup / Routing / DMZ

DMZ Settings

You may setup a De-militarized Zone(DMZ) to separate internal network and Internet.

DMZ Settings	
DMZ Settings	Disable
DMZ Address	

FCC+IC USER WARNING

1.§ P15.21 Information to user.
Notice: Any changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment. 法文: Aucune modification apportée à l’appareil par l’utilisateur, quelle qu’en soit la nature. Tout changement ou modification peuvent annuler le droit d’utilisation de l’appareil par l’utilisateur.
2.§ P15.105 Information to the user.

Note: 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:

—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.

法文:

This Class B digital apparatus complies with Canadian ICES-003.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that permitted for successful communication.

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:

1. This device may not cause interference, and
2. This device must accept any interference, including interference that may cause undesired operation of the device.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 Canada.

Pour réduire le risque d'interférence aux autres utilisateurs, le type d'antenne et son gain doivent être choisies de façon que la puissance isotrope rayonnée équivalente (PIRE) ne dépasse pas ce qui est nécessaire pour une communication réussie.

Cet appareil est conforme à la norme RSS Industrie Canada exempts de licence norme(s). Son fonctionnement est soumis aux deux conditions suivantes:

1. Cet appareil ne peut pas provoquer d'interférences et
2. Cet appareil doit accepter toute interférence, y compris les interférences qui peuvent causer un mauvais fonctionnement du dispositif.

3.§ P15.19 FCC Labelling requirement

Notice:
This device complies with Part 15 of the FCC Rules and Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

法文:

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

4.FCC/IC RF Radiation Exposure Statement:

FCC IC

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.

法文:

1.L'émetteur ne doit pas être colocalisé ni fonctionner conjointement avec à autre antenne ou autre émetteur. 2.Cet appareil est conforme aux limites d'exposition aux rayonnements de la IC pour un environnement non contrôlé. L'antenne doit être installé de façon à garder une distance minimale de 20 centimètres entre la source de rayonnements et votre corps.