

A10W
3G 11n WiFi Router

User Manual

Table of Contents

CE DECLARATION OF CONFORMITY	4
CHAPTER 1 INTRODUCTION	5
1.1 Package Contents.....	5
1.2 Appearance.....	5
CHAPTER 2 PRODUCT INSTALLATION	7
2.1 Hardware Installation	7
CHAPTER 3 HOW TO LOG INTO THE ROUTER.....	9
3.1 Set up your Wireless network configurations	9
3.2 Go into the Router management interface	12
CHAPTER 4 ADVANCED SETTINGS.....	16
4.1 Internet settings	16
4.1.1 WAN.....	16
4.1.2 LAN.....	18
4.1.3 DHCP client	19
4.1.4 Advanced	19
4.2 Wireless Network Settings	20
4.2.1 Basic Settings	21
4.2.2 Advanced Settings	22
4.2.3 Security Settings.....	24
4.2.4 WDS Configurations	27
4.2.5 WPS Configurations.....	27
4.2.6 AP client	29
4.3 Firewall.....	29
4.3.1 Address Filter	29
4.3.2 Virtual Server	31
4.3.3 DMZ Settings	31
4.3.4 System Security.....	32
4.3.5 Content Filter.....	32
4.4 Admin	33
4.4.1 Status	33

4.4.2 Management	34
4.4.3 Upload	36
4.4.4 Settings	36

CE Declaration of Conformity



Hame Technology Co., Limited

Declaration of Conformity

EC Decalration of Conformity

EC Directive:1999/5/EC relating to wireless equipment.

Responsible Person: Susan.Li

Company: Hame Technology Co.,Limited

5F,No.18 High Tech Middle Avenue

One,High Tech Industrial Park,Nanshan

District,Shenzhen,518057

Product: A10W、 A10WE

Intended Use: 3G Router

I Certify that the A10W and A10WE 3G Router complies with the wireless equipment,EMC and safety requirements of R&TTE Directive 1999/5/EC,relating to wireless terminal equipment.

Signed:

Position: Manager

Date:22 June 2011

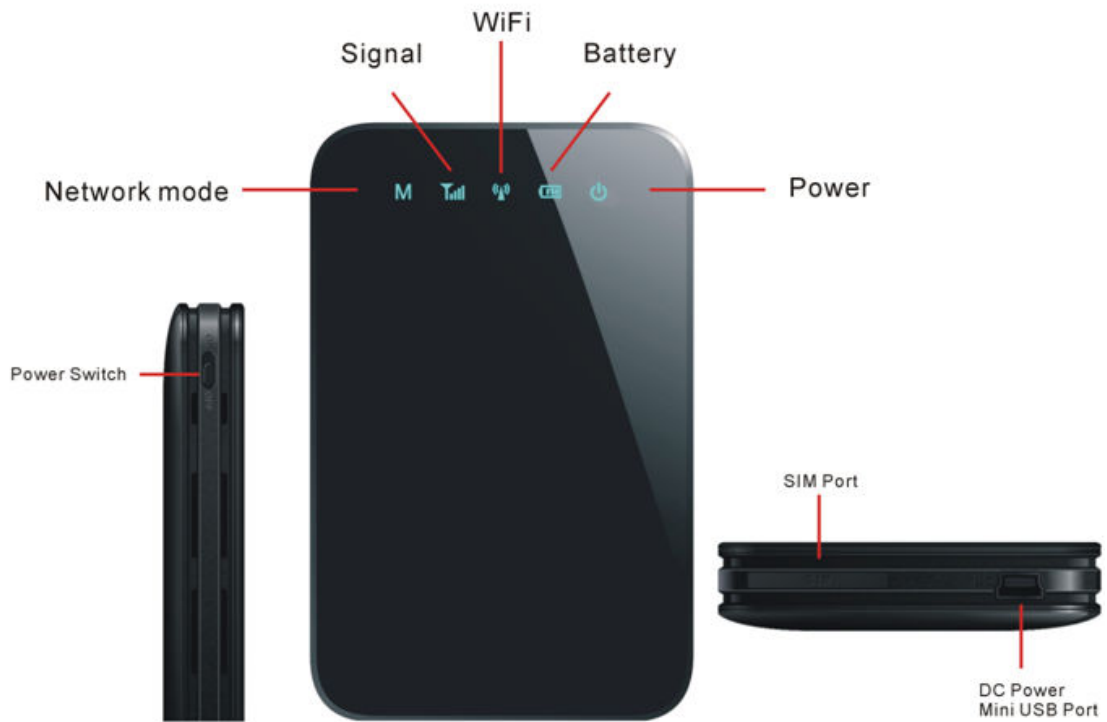

For and on behalf of
HAME TECHNOLOGY CO., LIMITED
华美信科科技有限公司
2011.6.22
.....
Authorized Signature(s)

Chapter 1 Introduction

1.1 Package Contents

3G Router x1
USB cable x1
1500mAh Lithium (Li-ion) battery x1
Quick Start Guide x1

1.2 Appearance



1.3 LED indicators

Name	LED Status	Indication
Power Light	Blue light	Power is on
Battery Light	Purple light	Battery power is charging
	Blue light	Battery power is charged
	Red light	Battery power is low and needs to be charged
	Not light	Battery has no power or battery not inserted
WIFI Light	Blue light	Wi-Fi is on
Signal Light	Blue light	Signal is strong
	Purple light	Signal is average

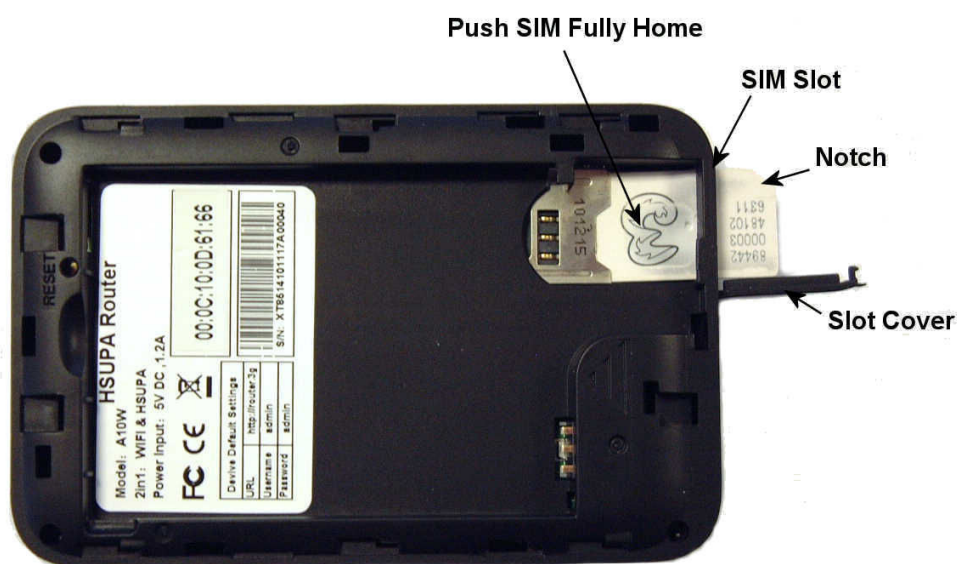
	Red light	Signal is weak
Network Mode Light (3G connect)	Red flashing 1time/Sec	No UIM card or Network Registering
	Blue flashing 1time/3Sec	registered on 3G network, but not dialing
	Blue flashing 1time/Sec	registered on 3G network, and dialing
	Blue continually on	3G registered network and dialed

Chapter 2 Product Installation

2.1 Hardware Installation

Before using your new 3G Router please follow these initial setup steps. In order to ensure the optimum connection then you need to place the Router in a position where it can pickup the best 3G signal and also give adequate WiFi coverage. The window ledge of the room you are working in is probably the best spot.

Step1: Remove the rear cover and then insert the UIM card via the slot on the bottom – remove the rubber cover to gain access to the slot.



Step2: Next insert the battery ensuring the orientation is correct:



Now connect the USB port to either a USB power adapter (optional extra) or to a computer with a USB port to charge the battery. Please allow 8 hours minimum to initially charge the battery

Charging method:

(1) If the power switch is off when charging then the the battery power indicator light is purple. When fully charged, battery indicator light should change to blue.

(2) If the power switch is on when charging then the battery indicator light is always purple when charging. Please note, if the router is switched on whilst charging then the time to fully charge will be longer.

Tip: When not using the Router for long periods or for storage you are advised to remove the batteries to prevent damage to the battery.

Step3: Power On.



Steps4: Connect the PC to the 3G Router WiFi.

Tip: Before connecting the computer to the 3G 3G Router please ensure that the computer actually has the WIFI function!



From the PC scan for new WiFi networks. Locate the network coming from the 3G router and connect to it.

Chapter 3 How to Log into the Router

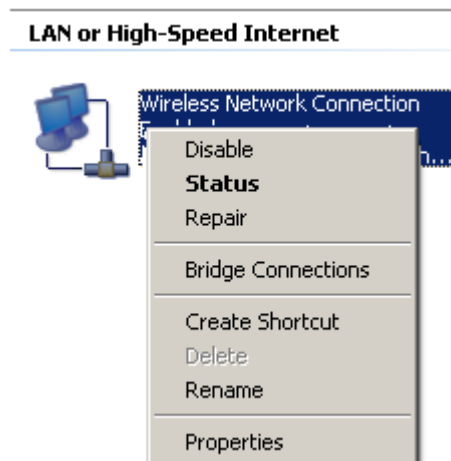
This chapter introduces how to log into the Router set-up page. First of all ensure the router is fully charged and switched on. Also check that the WiFi LED on the front is alight.

3.1 Set up your Wireless network configurations

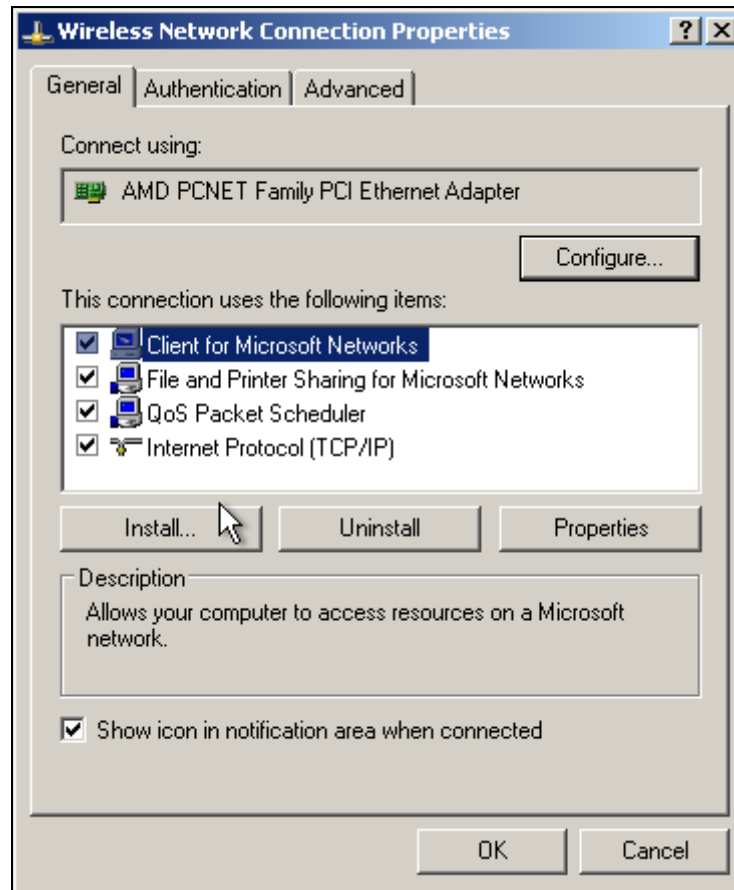
Step1: On the desktop, right-click on “My Network Places”, select “Properties”.



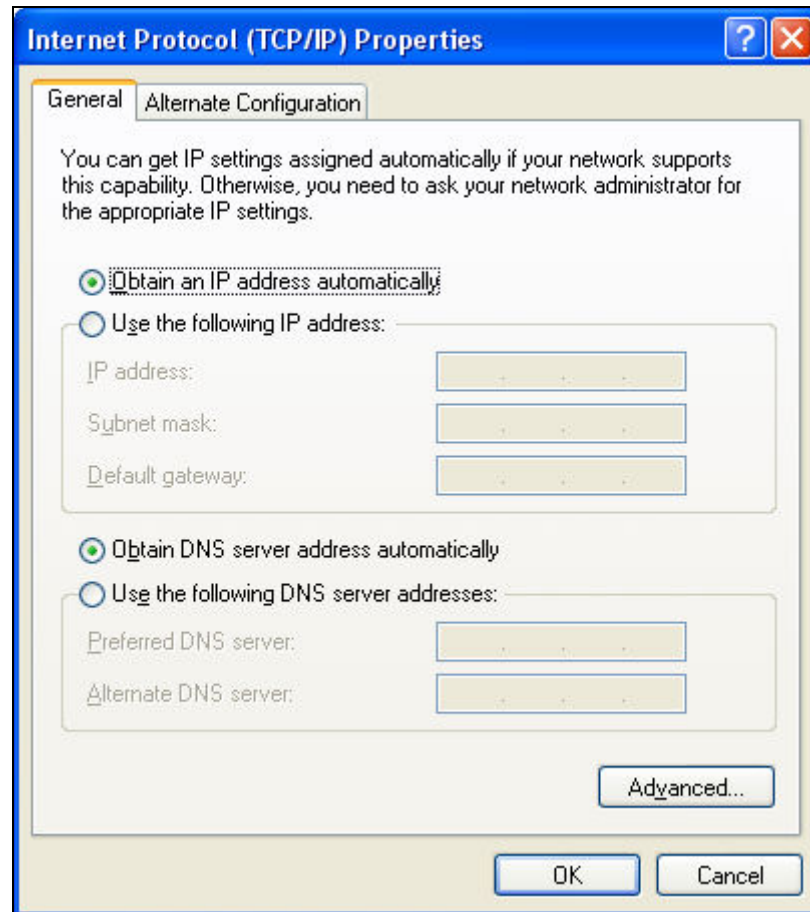
Step2: In the pop-up window, right-click on “Wireless Network Connection” and select “Properties”.



Step3: Then select “Internet Protocol (TCP/IP)” option, and then click “Properties”.



Step4: Make sure “Obtain an IP address automatically” and “Obtain DNS server address automatically” are selected. Then click “OK”.



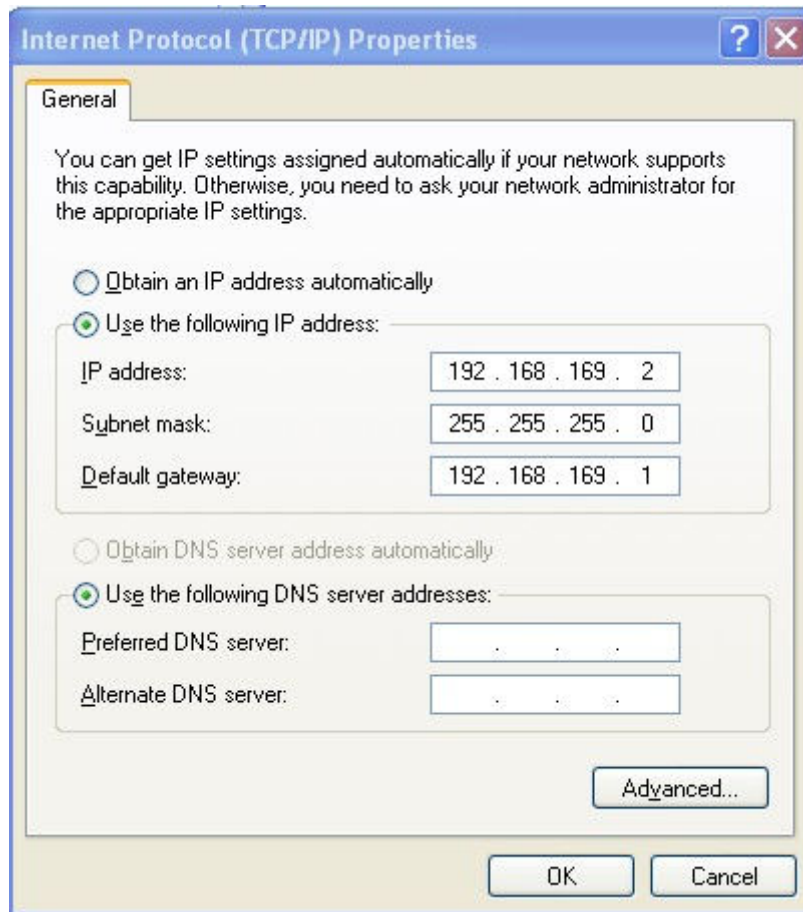
Alternatively you can set static IP settings e.g. as below:

IP address: 192.168.169** (** for one the 2-253)

Subnet mask: 255.255.255.0

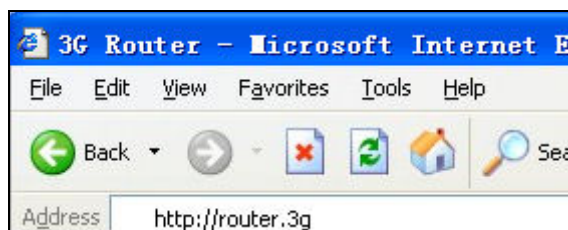
Default gateway: 192.168.169.1

DNS Server: Fill in your local DNS server address (if you do not know you can consult local the ISP),or set the Router address (Default Gateway Address) as your DNS Server.



3.2 Go into the Router management interface

Step1: Open your Web browser and input “<http://router.3g>” (or the router address <http://192.168.169.1>) at the Address bar, and then press “Enter”.



Step2: In the pop-up window the “User name” and “Password” are by default “admin”. Then click “OK” to enter the main page of the administrant mode.



Step3: When you enter the correct administrator user name and password, click “OK” to enter the main page of the administrant mode.



Network information: Shows the network signal, the current registering network, router name, and the connection status.



: Network signal



: Router name



: The current registering network



: Disconnected





: Connected



Connection Status: Displays the current network's upload speed and download speed, information of the current flux (speed) and total cumulative flux.

WIFI Management:


WIFI SSID: Displays the current name of the 3G Router 's WIFI.

If you need to modify this then click the **Modify** button, change the value and then click **Confirm** button to save the settings.

WIFI Security Button:  This button means the network is unlocked;  This button means the network is locked. Click the icon to set the status of the WIFI encryption.

WIFI encryption settings: By default there is no WIFI encryption setup. If you need to setup encryption, the please click the  button and it will change to  lock. Then enter the password, click **Confirm** button and the settings are set. After setting the wireless security then you will find your computer disconnects automatically from the router. You need to reconnect to the WiFi signal and this time enter the security settings on your computer.

Modify encryption password: When the Router is in the encrypted state then click **Modify** button to enter the new password, and then click **Confirm** button.


WIFI decryption settings: When the Router is encrypted, click the  button interface to quickly turn off security.

Remark: WiFi default encryption method is WPA2-PSK, and the password needs to be between 8-63 bits. If you need to set other encryption methods then click the upper right corner of the “Settings” button, then click “wireless” – “Security” for entering the new settings.

User Management: User Management displays the user name and password used for login.

Advanced Settings: If you need set more functions in detail then click the upper right corner of the “Settings” button.

Chapter 4 Advanced Settings

Click  **Settings** on the main status page to access the Advanced Settings.



Access Point Status

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

System Info	
Version	1.5.10.139 (2011-01-19-16:57)
Platform	1.51
Feature	3GRouter
SDRAM	16 MB
FLASH	4 MB
Running Time	1 min, 29 secs

Internet Configurations	
Connected	<input type="button" value="Connect"/> <input type="button" value="Disconnect"/>
Signal	
Network Mode	HSPA
WAN IP Address	211.96.74.205
Subnet Mask	255.255.255.255

4.1 Internet settings

4.1.1 WAN

There is only one online method (3G) supported by the A10 Router.

WAN Connection Type: 3G

3G Mode	
Run Type	<div style="border: 1px solid black; padding: 2px;">Keep Alive</div> <div style="border: 1px solid black; padding: 2px; margin-top: 2px;">Keep Alive</div> <div style="border: 1px solid black; padding: 2px; margin-top: 2px;">Manual</div> <div style="border: 1px solid black; padding: 2px; margin-top: 2px;">On Demand</div> <div style="margin-left: 20px;"> Period(seconds) <input style="width: 50px;" type="text" value="10"/> </div> <div style="margin-left: 20px;"> Idle Time(minutes) <input style="width: 50px;" type="text" value="2"/> </div> <div style="margin-left: 20px;"> PPPD TimeOut(seconds) <input style="width: 50px;" type="text" value="10"/> </div>
PIN Setting	<input type="radio"/> Use Pin <input checked="" type="radio"/> Unused Pin <input style="width: 100%;" type="text"/>
APN	<input checked="" type="radio"/> Auto APN <input type="radio"/> Manual APN <input style="width: 100%;" type="text"/>
Dial Number	<input style="width: 100%;" type="text"/>
User	<input style="width: 100%;" type="text"/>
PassWord	<input style="width: 100%;" type="text"/>
DNS Type	Auto DNS
DNS1	<input style="width: 100%;" type="text"/>
DNS2	<input style="width: 100%;" type="text"/>

Back
Next
Apply
Cancel

- **3G Run Type:**
- Under the “Keep Alive” mode, the Router will dial up automatically and connect to the Internet.
- Under the “Manual” mode, the internet connection will only dial-up when the user clicks “Connection” on the status page.
- Under the “On-Demand” mode, the system will only connect to the network automatically when there is a WAN access request. If there are no network access requests within the specific period (idle time), the system will disconnect from the network automatically. This connection mode might save network access fees for users that are charged based upon connection time.
- **PIN settings:** If your SIM/USIM/UM card has a PIN code, you shall select “Use PIN” and fill in the PIN code in the following Input Box; otherwise, you should select “Unused PIN”.
- **APN:** If you select “Automatic APN”, then information such as “APN Information”, “Dial Number”, “User” and “Password” shall be obtained by the Router automatically. If you select “Manual APN”, then you have to fill in this Internet access information by yourself.
- **DNS type:** If you select “Automatic DNS”, the Router will use the DNS obtained by 3G dial-up. If the “Manual DNS” is selected the Router will use the DNS information entered by the user.
- **MAC replication:** If MAC address replication is initiated, the MAC address of the Intranet’s Internet access data packet (i.e. the MAC address of the LAN side connected devices) is changed to the MAC address of the Router while accessing the Internet via the Router.

4.1.2 LAN

LAN Setup	
IP Address	<input type="text" value="192.168.169.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
MAC Address	00:0C:22:22:22:77
DHCP Type	Server <input type="button" value="v"/>
Start IP Address	<input type="text" value="192.168.169.2"/>
End IP Address	<input type="text" value="192.168.169.254"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Primary DNS Server	<input type="text" value="192.168.169.1"/>
Secondary DNS Server	<input type="text" value="192.168.169.1"/>
Default Gateway	<input type="text" value="192.168.169.1"/>
Lease Time	<input type="text" value="86400"/>
Statically Assigned	MAC: <input type="text"/> IP: <input type="text"/>
Statically Assigned	MAC: <input type="text"/> IP: <input type="text"/>
Statically Assigned	MAC: <input type="text"/> IP: <input type="text"/>

- **IP address:** Set up IP address for the Intranet port (Router gateway address)
- **Subnet mask:** Set up mask for the Intranet (local LAN).
- **MAC address:** Indicated physical MAC addresses of the LAN interface.
- **DHCP type:** Select “Server” to open DHCP services for local LAN clients so they can obtain IP settings dynamically.
- **Start IP address-End IP address:** Range of IP settings to be used by the local clients via DHCP.
- **Default gateway:** Set up the gateway for the host in the Intranet – the address of the router.
- **DNS server:** Set up DNS servers to be used by the host via DHCP (If DNS Proxy is enabled, we recommend to set the DNS server address as the Router address).
- **Release time:** Effective period for the host in the Intranet to obtain IP addresses.
- **Static designation:** Used to fix the address given to specific clients based upon their physical MAC.

Introduction of Relevant Intranet Programs.

802.1d Spanning Tree	Disable ▾
LLTD	Disable ▾
IGMP Proxy	Disable ▾
UPNP	Disable ▾
Router Advertisement	Disable ▾
PPPOE Relay	Disable ▾
DNS Proxy	Enable ▾

- **802.1d Spanning Tree:** Support spanning tree protocols: to avoid network loop backs in the LAN and address broadcast storm issues relating to a looped Ethernet network.
- **LLTD:** Identify whether LLTD (Link-Layer Topology Discovery Responder) protocol is supported. This network protocol is used to intelligently detect and identify which network equipment or computers are connected in the LAN network.
- **IGMP Proxy:** Confirm whether the Router supports the IGMP protocol. This protocol operates between the host and a multicast Router that is directed connected to the host. It is a protocol for IP hosts to report the identity of multicast group members.
- **UPNP:** Identify whether UPNP protocols are supported.
- **Router Advertisement:** Identify whether the Router supports IPV6.
- **DNS Proxy:** Transmit DNS requests of the LAN clients. If this function is enabled you can configure DNS of the host clients in the Intranet to IP address of the Router's LAN address. This way there is no need to reset the local clients DNS settings after the Internet access method (3G connection) has changed.

4.1.3 DHCP client

Display information relevant to the hosts (local clients) that are connected to the Router's Intranet via DHCP. DHCP client list enables you to check the status of online users such as MAC address, IP address and lease periods of the IP address.

DHCP Clients			
Hostname	MAC Address	IP Address	Expires in
huamei-912ef9c8	00:21:27:B8:22:B4	192.168.169.2	22:55:14
PCOS-05051027	C4:17:FE:29:EE:9B	192.168.169.3	22:59:09

4.1.4 Advanced

This function may be used when you need to add a specific routing for a certain host. This is particularly

useful when your LAN has multiple subnets or routers running on it. A routing item may be identified by setting the destination IP address and the local gateway to access this network. Afterwards the Router transmits the data packets to the designated target network/host via the gateway.

Add a routing rule

Destination	<input style="width: 90%;" type="text"/>
Range	Host <input style="width: 20px;" type="button" value="v"/>
Gateway	<input style="width: 90%;" type="text"/>
Interface	LAN <input style="width: 20px;" type="button" value="v"/> <input style="width: 150px;" type="text"/>
Comment	<input style="width: 90%;" 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	192.168.169.0	255.255.255.0	0.0.0.0	1	0	0	0	LAN (br0)	

- **Destination IP address:** Identify target addresses or networks that are to be routed.
- **Type: Host/network:** The selection of a host means to designate a certain IP for a single client/the host. Network defines a complete specific network segment by defining a subnet mask.
- **Gateway:** IP address of the Router or the host where the data packets are sent.
- **Interface:** Indicate connector information.
- **Comment:** Fill in necessary notes.
- **Current Router table:** Displays details of routes already defined.

4.2 Wireless Network Settings

4.2.1 Basic Settings

Wireless Network	
WIFI On/Off	<input type="button" value="RADIO OFF"/>
Network Mode	11b/g/n mixed mode <input type="button" value="v"/>
Network Name(SSID)	3GRouter_345b Hidden <input type="checkbox"/> Isolated <input type="checkbox"/>
Multiple SSID1	<input type="text"/> Hidden <input type="checkbox"/> Isolated <input type="checkbox"/>
Multiple SSID2	<input type="text"/> Hidden <input type="checkbox"/> Isolated <input type="checkbox"/>
Multiple SSID3	<input type="text"/> Hidden <input type="checkbox"/> Isolated <input type="checkbox"/>
Multiple SSID4	<input type="text"/> Hidden <input type="checkbox"/> Isolated <input type="checkbox"/>
Multiple SSID5	<input type="text"/> Hidden <input type="checkbox"/> Isolated <input type="checkbox"/>
Multiple SSID6	<input type="text"/> Hidden <input type="checkbox"/> Isolated <input type="checkbox"/>
Broadcast Network identifier (SSID)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
MBSSID AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
BSSID	00:0C:01:34:5B:88
Frequency (Channel)	2462MHz (Channel 11) <input type="button" value="v"/>
HT Physical Mode	
Operating Mode	<input checked="" type="radio"/> Mixed Mode <input type="radio"/> Green Field
Channel BandWidth	<input type="radio"/> 20 <input checked="" type="radio"/> 20/40
Guard Interval	<input type="radio"/> Long <input checked="" type="radio"/> Auto
MCS	Auto <input type="button" value="v"/>
Reverse Direction Grant(RDG)	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Extension Channel	2442MHz (Channel 7) <input type="button" value="v"/>
Aggregation MSDU(A-MSDU)	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Auto Block ACK	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Decline BA Request	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Other	
HT TxStream	1 <input type="button" value="v"/>
HT RxStream	1 <input type="button" value="v"/>

- **Wireless switch:** Switch on/off wireless functions of the Router.
- **Network mode:** Wireless standards for the Router. The Router supports 802.11b, 802.11g, and 802.11n or mix modes.
- **Multiple SSID:** Network name of the wireless signals. This Router supports multiple wireless networks. If you select “Hidden the Wireless Client” then clients cannot scan for the Router’s SSID. If you select “Isolated” you can prevent user-to-user connectivity via the router – improves security between users so users can see the internet but NOT each other.

- **Broadcast network Name:** You can select “Disable” to stop the Router broadcasting its SSID. After that the wireless clients cannot scan for the Router’s SSID. This means that clients cannot communicate with the Router unless they already know the correct SSID. The broadcast network identifier is by default “Enable”.
- **AP Isolation:** Isolated at the AP level. After it is enabled, clients at the AP level cannot see each other. They can only see the internet.
- **Basic service set identifier:** Business group identifier of the wireless network. In terms of IEEE 802.11 the BSSID is the MAC address of the wireless AP.
- **Frequency (channel):** Channels currently used by the Router.

4.2.2 Advanced Settings

Advanced Wireless	
BG Protection Mode	Auto <input type="button" value="v"/>
Beacon Interval	<input type="text" value="100"/> ms (range 20 - 999, default 100)
Data Beacon Rate (DTIM)	<input type="text" value="1"/> ms (range 1 - 255, default 1)
Fragment Threshold	<input type="text" value="2346"/> (range 256 - 2346, default 2346)
RTS Threshold	<input type="text" value="2347"/> (range 1 - 2347, default 2347)
TX Power	<input type="text" value="100"/> (range 1 - 100, default 100)
Short Preamble	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Short Slot	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Tx Burst	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Pkt_Aggregate	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
IEEE 802.11H Support	<input type="radio"/> Enable <input checked="" type="radio"/> Disable(only in A band)
Country Code	None <input type="button" value="v"/>

Wi-Fi Multimedia	
WMM Capable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
APSD Capable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
WMM Parameters	<input type="button" value="WMM Configuration"/>

Multicast-to-Unicast Converter	
Multicast-to-Unicast	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Advanced wireless:

- **BG Protection Mode:** Can be “on”, “off” or “Automatic” and allows users to fix the setting for 11BG

protection.

- **Beacon Interval:** Intervals to transmit wireless beacon frames. During this time range, a beacon frame will be transmitted to trigger status replies from any clients.
- **Data Beacon Rate (DTIM):** Intervals to transmit specific indication messages. Notifies the next client window to receive broadcast and multicast.
- **Fragment Threshold:** Specific fragment thresholds of the data packets. When the length of the data packet exceeds such threshold then packets are split automatically.
- **RTS threshold:** A RTS (Request to Send) threshold specified by the data packets. When the length of the data packets exceeds this threshold the Router will send an RTS to the target sites for negotiation. After the wireless site (client) receives RTS frames it will respond to the Router by sending a CTS (Clear to Send) frame indicating that the wireless communication is possible.
- **TX power:** Defines percentage of Transmit power – 100% is full power.
- **Short preamble:** The default status is “Prohibit”. The Router applies long preambles by default. If short preambles are enabled then the system will no longer be compatible with the operation speed (1Mbps or 2Mbps) of the traditional IEEE802.11 but efficiency for higher speeds is improved.
- **Short slot:** The default setting is “Enable” and you can switch it off. Setting this to “Enable” might enhance the transmission rate of the wireless communication.
- **Tx Burst:** This is a feature at the MAC address level and might enhance TCP transmission fairness for the wireless network.
- **Pkt_Aggregate:** A mechanism to strengthen the LAN and make sure that the data packet could arrive at the destination.

(WMM) WI-FI Multimedia:

- **Wi-Fi multimedia capabilities:** Enable WMM functions. WMM function will not take effect until the WIFI is enabled.
- **Direct online capabilities:** The enablement will weaken the wireless performance, but could save the energy and electricity.

wireless multimedia parameters: WMM enables the wireless communications to define a priority (QoS) range according to the data types. Time-sensitive data such as video/audio data has higher priority than that of normal data. Wireless clients need to also support WMM for these functions to work.

WMM Parameters of Access Point						
	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	15	63	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_BK	7	15	1023	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_VI	1	7	15	94	<input type="checkbox"/>	<input type="checkbox"/>
AC_VO	1	3	7	47	<input type="checkbox"/>	<input type="checkbox"/>

WMM Parameters of Station					
	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	1023	0	<input type="checkbox"/>
AC_BK	7	15	1023	0	<input type="checkbox"/>
AC_VI	2	7	15	94	<input type="checkbox"/>
AC_VO	2	3	7	47	<input type="checkbox"/>

4.2.3 Security Settings

The Router supports the following security modes:

- **Disable:** The wireless stations will be able to connect the Router without encryption.
- **OPEN:** A handshake method for WEP encryption. The encryption is completed with the use of WEP key.
- **SHARED:** Under this mode, the authentication may be conducted without WEP encryption. “No Encryption Method” may be indicated in the settings.
- **WPAUTO:** Open mode or shared mode may be automatically selected. Its encryption type is same to those of the two modes described above.
- **WPA-KEY:** (WPA-personal)-Wi-Fi Protected Access (WPA) with pre-shared keys (also called passphrase).
- **WPA2-KEY:** WPA2-Personal-WPA2 with pre-shared keys.
- **WPA:** WPA with RADIUS server authentication
- **WPA2:** WPA2 with RADIUS server authentication
- **802.1x:** apply IEEE 802.1X standards to conduct ID authentication.
- **Mix mode:** WPAKEYWPA2KEY and WPAWPA2

Select SSID		
SSID choice	3GRouter_345b	
"3GRouter_345b"		
Security Mode	OPEN	
Wire Equivalence Protection (WEP)		
Default Key	OPEN	
WEP Keys	WEP Key 1 :	Hex
	WEP Key 2 :	Hex
	WEP Key 3 :	Hex
	WEP Key 4 :	Hex
Access Policy		
Policy	Disable	
Add a station Mac:		
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

If “Disable” is selected then clients can have a Wi-Fi connection to the Router’s Intranet without entering security key information.

If “OPEN”, “SHARED” or “WEPAUTO” is selected, then security key information needs to be entered. Wireless clients in the Intranet cannot gain access to the Router’s Intranet until correct the key information is entered.

You can fill in four (ASCII or Hex, with a length of 10 to 26 characters) keys for this Router. One of the group of four pre-set keys can then be selected as the current effective key (default key).

Wire Equivalence Protection (WEP)		
Default Key	Key 1	
WEP Keys	WEP Key 1 :	Hex
	WEP Key 2 :	ASCII
	WEP Key 3 :	Hex
	WEP Key 4 :	Hex

Description of key types: Keys are divided into two categories, namely Hex and ASCII. If Hex is selected then a valid hex number must be entered for the key. If ASCII is selected then any character string can be used.

Alternatively you can select WPA security WPA-PSK or WPA2-PSK.

- **WPA algorithm:** you can select AES (Advanced Encryption Standard) mode, TKIP (Temporal Key Integrity Protocol) mode or mixed mode.
- **Password:** secret code used by WPA (8 to 63 ASCII characters).
- **Intervals of Private key update:** create an effective period for your specific keys.
- If WPA, WPA2 or WPAWPA2 authentication methods are used then you also need to configure information relevant to the WPA algorithms and RADIUS servers.
- **WPA algorithms:** algorithm types used during the authentication process.
- **Intervals of private key update:** regular update cycles for the broadcast and multicast keys. The maximal and the minimum value between 3,600 seconds and zero seconds respectively. No updates are required if the value is zero.
- **PMK cache period:** set the PMK cache period. The connection speed will be enhanced during the period when the user disconnects the network.
- **Pre-authentication:** the initiation can enhance the wireless access speed.
- **IP address:** The IP address of the authentication server.
- **Port:** used by Radius servers to conduct the authentication.
- **Shared key:** password to access RADIUS services.
- **Dialogue timeout:** Radius server will automatically disconnect the connection when the dialogue timeout has reached a certain amount.
- **Idle timeout:** Radius server will automatically disconnect the connection when the idle time has reached a certain amount

Security Mode	WPA2
WPA	
WPA Algorithms	<input type="radio"/> TKIP <input checked="" type="radio"/> AES <input type="radio"/> TKIP/AES
Key Renewal Interval	3600 seconds
PMK Cache Period	10 minute
Pre-Authentication	<input checked="" type="radio"/> wireless disable <input type="radio"/> wireless enable
Radius Server	
IP Address	
Port	1812
Shared Secret	
Session Timeout	0
Idle Timeout	
<input type="button" value="Back"/> <input type="button" value="Next"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

4.2.4 WDS Configurations

Wireless Distribution System (WDS) is used to expand current wireless network coverage by one or more repeaters. The Router supports three WDS modes: Lazy Mode, Bridge Mode and Repeater Mode.

Wireless Distribution System(WDS)	
WDS Mode	<input type="text" value="Lazy Mode"/>
Phy Mode	<input type="text" value="CCK"/>
EncrypType	<input type="text" value="NONE"/>
Encryp Key	<input type="text"/>
EncrypType	<input type="text" value="NONE"/>
Encryp Key	<input type="text"/>
EncrypType	<input type="text" value="NONE"/>
Encryp Key	<input type="text"/>
EncrypType	<input type="text" value="NONE"/>
Encryp Key	<input type="text"/>

- **Lazy Mode:** Under this mode, wireless equipment on the opposite side could be in either Bridge Mode or Repeater Mode. In that case the client needs to enter the Router's BSSID in its setup.
- **Bridge Mode:** Under this mode you can manually add the MAC (BSSID) of the other end or use the "Scan Options". Then, you click "Save as" to create the wireless connection for between the two units.
- **Repeater Mode:** Under this mode you can manually add the MAC (BSSID) of the other end or, like above, find the network using the "Scan Options".
- **Encryption type:** Three encryption modes are supported, namely WEP, TKIP and AES.
- **Encrypt Key:** Enter the encrypt keys between the wireless equipment.
- **AP MAC Address:** Please enter MAC address of the wireless equipment on the opposite side.

4.2.5 WPS Configurations

Wi-Fi Protection Settings (WPS) is a system for users to easily configure and setup the various security settings on a WiFi network. You have no need to select the encryption mode or configure a key. You just need to enter the correct PIN code or select PBC (or press "WLAN/WPS" button indicated on the back panel) to configure WPS.

WPS Config	
WPS:	Enable <input type="button" value="v"/>
<input type="button" value="Apply"/>	

WPS Summary	
WPS Current Status:	Idle
WPS Configured:	Yes
WPS SSID:	3GRouter_345b
WPS Auth Mode:	Open
WPS Encryp Type:	WEP
WPS Default Key Index:	1
WPS Key(Hex value)	1234567890
AP PIN:	34313046 <input type="button" value="Generate"/>
<input type="button" value="Reset OOB"/>	

WPS Progress	
WPS mode	<input checked="" type="radio"/> PIN <input type="radio"/> PBC
PIN	<input type="text"/>
<input type="button" value="Apply"/>	

- **Wi-Fi Protection Settings:** Used to disable or enable the WPS functions. The default status is “Disable”.
- **WPS Overview:** Display relevant information including current WPS status, authentication modes and encryption types applied, and default private key indexing.
- **WPS Current Status:** “Idle” means the idle status. “Start MSC Process” means that the process is enabled and the access is being processed. “Success” means that the server (AP) and the client have reached an agreement during the negotiation.
- **WPS Validity:** “Yes” means operational and “Not Used” means not used yet. Generally, if the AP-Safety Configuration takes effect, this place will be displayed as “Not Used”.
- **SSID Configured by WPS:** Display the master SSID numbers of the WPS. WPS is only valid for the master SSID.
- **WPS Authentication Mode:** The authentication mode used by WPS. WPA/WPA2-Personal mode is commonly seen.
- **WPS Encryption Type:** It means the data encryption type. AES/TKIP encryption type is commonly seen.
- **WPS Key:** Effective keys automatically generated by AP.
- **Reset OOB:** When you press this button, the WPS service terminal is indicated as Idle and the WPS indication light turns off. AP will not respond to connection requests from WPS clients and the safety are configured as WPA mode.

- **WPS Mode:** Support two kinds of simple WPS settings, namely PBC (Push-Button Configuration) and PIN code.
- **PBC:** Select PBC and click "Save as" or press WLAN/WPS button on the back panel for about one second while activating WPS / PBC on the client device.
- **Operation Process:** After clicking the WLAN/WPS button for one second the WPS lights will blink about 2 minutes, indicating that the function is activated. In this time range, you need to trigger WPS on the client device. The client device will then load its configuration from the router. After the connection is successfully completed the WPS indication light will go off and the client setup is completed. If there are multiple wireless clients then the user needs to repeat the process for each client in turn. Up to 32 wireless clients can be setup this way.
- **PIN:** If users want to use the PIN for configuration (as an alternative to the WPS button) then the users must know the PIN code of the wireless client device. The user then needs to add the PIN to the relevant field on the router page and save; the devices should then handshake and exchange the setup details automatically.
- **PIN (Key):** Default PIN code.

4.2.6 AP client

Wireless Network							
MAC Address	Aid	PSM	MimoPS	MCS	BW	SGI	STBC
00:21:27:B8:22:B4	1	0	0	7	20M	0	0
C4:17:FE:29:EE:9B	2	0	0	6	20M	0	0

Displays information relevant to the hosts that are connected to the Router's Intranet via DHCP.

4.3 Firewall

4.3.1 Address Filter

This function is aimed at restricting and managing connections of client devices to the Router. You can use this function to restrict client access to the Router. To use this function you should first activate it and then select a default strategy (i.e. accept or reject this client). Then fill out the corresponding filter rules. Please note you don't have to complete all the requested fields, just those pertinent to the type of filtering you are trying to configure. For example, to ban the IP of 192.168.1.146 to use the Internet, you just need to setup the default strategy as acceptance strategy and fill 192.168.1.146 in the column of the source IP address.

Basic Settings	
MAC/IP/Port Filtering	Disable ▾
Default Policy -- The packet that don't match with any rules would be:	Dropped ▾

MAC/IP/Port Filter Settings	
MAC address	<input type="text"/>
Dest IP Address	<input type="text"/>
Source IP Address	<input type="text"/>
Protocol	None ▾
Dest Port Range	<input type="text"/> - <input type="text"/>
Source Port Range	<input type="text"/> - <input type="text"/>
Action	Accept ▾
Comment	<input type="text"/>

(The maximum rule count is 32.)

Current MAC/IP/Port filtering rules in system:									
No.	MAC address	Dest IP Address	Source IP Address	Protocol	Dest Port Range	Source Port Range	Action	Comment	Pkt Cnt
Others would be dropped									-

- **Mac/IP/Port Filtering:** This function has no effect if “Prohibit” is selected. After you click “Enable”, this function is applicable.
- **Default Policy:** Select “Dropped” or “Accepted”. This strategy shall be implemented if rules as defined below are not matched.
- **MAC Address:** Fill in MAC addresses that you plan to define rules.
- **Source IP Address:** Enter local IP address that needs filtering. You shall fill in rules that correspond to this IP.
- **Destination IP Address:** Enter destination IP address that needs filtering. You shall fill in rules that correspond to this IP.
- **Port range:** Ranges for ports that need to be abandoned or accepted.
- **Protocol:** Select protocols that are used by controllable data packets.
- **Strategy:** Identify whether the defined rules are “Abandon” or “Accept”. This is the opposite meaning to the default strategy.

Remarks: Indicate comments by you to differentiate the rules.

4.3.2 Virtual Server

The virtual host enables remote users who gain access to web or FTP services via public network IP addresses to automatically direct their traffic to local servers on the LAN. The virtual server defines a service port and then all service requests to this port raised by the Extranet (internet) are transmitted to the appropriate LAN servers as specified by the Router (based on IP address). This way, the user could successfully access LAN servers without affecting the internal network safety of the LAN.

Virtual Server Settings	
Virtual Server Settings	Disable ▾
IP Address	<input type="text"/>
Port Range	<input type="text"/> - <input type="text"/>
Protocol	TCP&UDP ▾
Comment	<input type="text"/>

(The maximum rule count is 32.)

Current Virtual Servers in system:				
No.	IP Address	Port Range	Protocol	Comment
<input type="button" value="Delete Selected"/> <input type="button" value="Reset"/>				

- **Virtual Server settings:** Enable or disable functions of the virtual servers.
- **IP address:** It is used to input necessary IP addresses, such as 192.168.1.103.
- **Port Range:** It is used to input necessary port ranges, such as 80-80.
- **Protocol:** Select protocols that are used by controllable data packets.

Remarks: Fill in necessary notes. In terms of the configurations described above, all data will be transmitted to a computer with the IP address of 192.168.1.103 within the LAN if some program accesses the 80 port of the Router.

Current Virtual Servers in system: Indicate the list of current virtual servers.

4.3.3 DMZ Settings

Transfer all data that are received by the Router's Extranet ports to "DMZ IP Address"

DMZ Settings	
DMZ Settings	Disable ▾
DMZ IP Address	<input type="text"/>

4.3.4 System Security

Remote management	
Remote management (via WAN)	Deny ▾ 8080 1024~65535

Ping form WAN Filter	
Ping form WAN Filter	Disable ▾

NAT Enabled	
NAT Enabled	Enable ▾

- **Remote management:** Identify whether it is permitted to access WEB management pages via the internet.
- **Ping form WALL Filter:** Identify whether it is permitted to PING the Router via the internet.

4.3.5 Content Filter

Webpage content filtering: Filter the “Proxy Java ActiveX” from web pages.

Webs Content Filter	
Filters:	<input type="checkbox"/> Proxy <input type="checkbox"/> Java <input type="checkbox"/> ActiveX

URL filtering: Filter out the entire content of specific webpages or URL

Current Webs URL Filters:	
No	URL

Web host filtering: URL WEBPAGES including keywords are filtered.


Add a URL filter:

URL:

4.4 Admin

4.4.1 Status

Current status of the Router showing the connection information, link quality and other details.

System Info	
Version	1.5.10.139 (2011-01-19-16:57)
Platform	1.51
Feature	3GRouter
SDRAM	16 MB
FLASH	4 MB
Running Time	9 mins, 46 secs
Internet Configurations	
Connected	<input type="button" value="Connect"/> <input type="button" value="Disconnect"/>
Signal	
Network Mode	HSPA
WAN IP Address	211.96.74.205
Subnet Mask	255.255.255.255
Default Gateway	10.64.64.64
Primary Domain Name Server	210.21.196.6
Secondary Domain Name Server	221.5.88.88
Local Network	
Local IP Address	192.168.169.1
Local Netmask	255.255.255.0
MAC Address	00:0C:01:34:5B:77

System information:

- **Version:** indicates the Router's current software versions and the release date.
- **Running Time:** indicates the system up time of the Router is loaded. This value is reset to zero after the power is switched off.

Internet Configurations:

- **Connected:** 3G mode contains two buttons, namely "Disconnect" and "Connect" will be displayed on the interface to disconnect and connect the 3G network.

- **Network Mode:** Signal strength of the 3G network. Network type: Which network is currently connected (WCDMA,TD,EVDO)
- **WAN IP Address:** current WAN IP address of the Router. If the Router is not connected to the internet then the address will be displayed 0.0.0.0.
- **Subnet Mask:** Router's WAN subnet mask.
- **Default Gateway:** Router's WAN default gateway.
- **Primary Domain Name server:** Address of the DNS server that is currently used by the Router.

Local Network:

- **Local IP address:** IP address of the Router's Intranet ports.
- **Local Net mask:** Subnet mask of the Router's Intranet.
- **MAC address:** Physical address of the Router's Intranet ports.

4.4.2 Management

4.4.2.1 Administrator Settings

Administrator Settings	
Account	<input type="text" value="admin"/>
Password	<input type="password" value="•••••"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Administrator Settings: Set account username and password for administration.

4.4.2.2 NTP Settings

NTP Settings	
Current Time	<input type="text" value="Sat Sep 25 10:58:00 UTC 201"/> <input type="button" value="Sync with host"/>
Time Zone:	<input type="text" value="(GMT+08:00) China Coast, Hong Kong"/> <input type="button" value="v"/>
NTP Server	<input type="text"/> <p>ex: time.nist.gov ntp0.broad.mit.edu</p>
NTP synchronization(hours)	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- **Current Time:** Set the Router time the same to PC.
- **Time Zone:** Select time and area.
- **NTP Server:** Enter the address for the NTP Server and the Router will then get the time from the NTP

Server. In addition the Router has several built-in common NTP Servers so it can automatically get the time once it connects the Internet.

- **NTP Synchronization:** Interval for the Router to check the time from the NTP server.

4.4.2.3 DDNS

Please note, because UK 3G providers invariably allocate virtual rather than true external addresses to 3G data connections the DDNS function operating from the router will NOT work correctly. Sorry that's the way it is with UK providers. If you want to use DDNS on a 3G connection you instead are advised to run the DDNS client application on an internal PC.

DDNS (Dynamic Domain Name System) – The capability of assigning a fixed host and domain name to a dynamic Internet IP Address. The Router supports the DDNS feature which allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (named by yourself) even when you have a dynamic IP address. You can then connect externally to the router by entering your domain name no matter what your WAN IP address is. Before using this feature you need to sign up for DDNS service through a providers. The Dynamic DNS client service provider will give you a password or key.

DDNS Settings	
Dynamic DNS Provider	None <input type="button" value="v"/>
Account	<input type="text"/>
Password	<input type="text"/>
DDNS	<input type="text"/>

- **Dynamic DNS Providers:** select websites that provide dynamic domain name service.
- **Account Number:** the login name you register in the websites that provide dynamic domain name service.
- **Password:** the password you register in the websites that provide dynamic domain name service.
- **DDNS:** the domain name you register in the websites that provide dynamic domain name service

Note: Before using Dynamic Domain Name function, please register the dynamic DNS address services in the website listed in drop-down box of service providers and ensure that this account is effective.

4.4.3 Upload

Update Firmware	
Location:	<input type="text"/> <input type="button" value="browse"/>
<input type="button" value="Apply"/>	

Update Bootloader	
Location:	<input type="text"/> <input type="button" value="browse"/>
<input type="button" value="Apply"/>	

If you need to upgrade the Router's software then use the browse function to locate and specify the upgrade file. Then click "Yes" and wait until the upgrade is done (generally within one minute).

The "Update Bootloader" is used to upgrade the system booting programs. Generally speaking, it is unnecessary for the user to apply this function.

4.4.4 Settings

Export Settings	
Export Button	<input type="button" value="Export"/>

Export LOG	
Debug Switch	<input type="button" value="open"/> <input type="button" value="close"/>
Export Button	<input type="button" value="Export"/>

Import Settings	
Settings file location	<input type="text"/> <input type="button" value="browse"/>
<input type="button" value="Import"/> <input type="button" value="Cancel"/>	

Load Factory Defaults	
Load Default Button	<input type="button" value="Load Default"/>

Clear Flux Defaults	
Clear Flux Button	<input type="button" value="Clear Flux"/>

- **Export system configurations:** Save system configuration files locally for further recoveries.

- **Export LOG:** Click the “open” button; store the Log file locally to seek error.
- **Import system configurations:** Introduce local configuration files to the Router. After that, each configuration of the Router will be updated into the configuration files.
- **Load Factory Defaults:** All the configurations will reset to the factory original settings
- **Clear Flux Defaults:** Click “Clear Flux”, current flux and amass flux (data down or uploaded) on the main status page are cleared