3G Wi-Fi Router

Content

版本	修改内容	修订人	时间
V1.0	初始版本	尹天林	2012/10/29
V1.1	页面调整	尹天林	2012/12/12

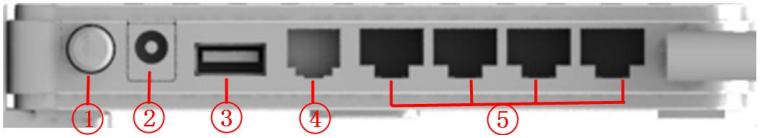
1 Introduction

1.1 Features

No.	Items	Specification
1	ID	
2	Standard	Wi-Fi: IEEE 802.11b/g/n Ethernet: IEEE 802.3u
3	Data Rate (HSUPA)	• HSUPA uplink up to 5.76Mbps • HSDPA downlink up to 7.2 Mbps • WCDMA (UMTS) uplink data rate up to 384 kbps • EDGE data up to 237 Kbps DL and 118Kbps UL, • 3GPP Release 4, class 12 • GPRS data up to 85.6 Kbps DL and 42.8 Kbps UL • Circuit switched data: 14.4 and 9.6 Kbps
4	Data Rate(HSPA+)	HSPA＋ DL 21.6Mbps UL 5.76 Mbps HSPA+ DL14.4 Mbps UL 5.76Mbps HSPA DL 7.2Mbps UL 5.76 Mbps UMTS DL/UL 384 kbps GPRS DL 85.6 kbps / UL 42.8 kbps EDGE 3GPP R4, Category 12, DL 237k bps / UL 118K bps
5	Antenna	1 external antenna for 3G 2 internal antennas for Wi-Fi

6	Antenna gain	3dBi
7	Port	1 RJ11 ports, 4 LAN ports,1Power,1 Power Switch,1 Antenna,1 USB,1 S(U)IM card slot
8	Band	Should support Quad-band for 2G (850, 900, 1800, 1900 MHz) & tri band for 3G (850, 900, 1900 , 2100 MHz) optional WiFi:2.4-2.4835GHz
9	RF Power	2G:33 dBm(Maximum) 3G:23 dBm(Maximum) WiFi:23 dBm(Maximum)
10	Receiver Sensitivity(3G)	less than -106.7 dBm
11	Power	Power Adapter connection (DC12V/1A)
12	Size	142*98*20(mm)
13	Environment	i) Work temperature : -0℃ to +40℃ ii) Storage temperature : -20℃ to +70℃ iii) Relative Humidity : -10% to 90%

1.2 Interface description



1、 Power switch

2、 Power jack

3、 USB port

4、 RJ11 port

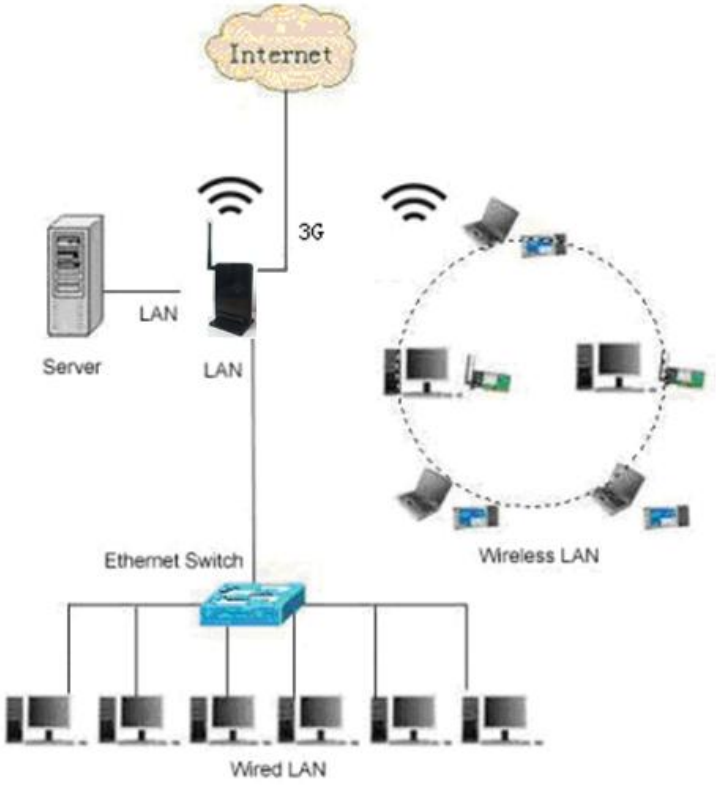
5、 RJ-45 ports for 10/100 Base-T Ethernet LAN

6、 S(U)IM card slot

7、 Reset button

8、 WPS button

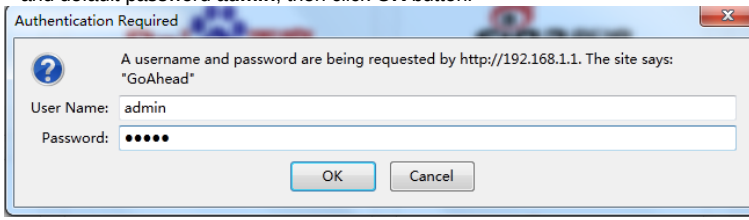
1.3 Hardware connection guide



2 Web management interface

2.1 Login Router

1. Connect LAN adapter on your PC with one of LAN port of this wireless router, then power on it. PC will get an IP address.
2. Run web browser on your PC(e.g.IE), type **http://192.168.1.1** in the address field, then press Enter, shown as follow figure, Input default User name **admin** and default password **admin**, then click **OK** button.



3. Then the following interface appears.

3 Quick Setup

Welcome to the Quick Setup Wizard **Step 1 of 5**

- The wizard will show you how to saftely set up your router:

Click "Next" to continue, click "Previous" and "Next" to navigate throughout the wizard, click "Cancel" to exit the wizard, and click "Finish" to save the settings.

Notes :
Basic parameters can be set in the wizard.

Next>

Configure WAN Settings **Step 2 of 5**

Net Mode	3G
3G Mode	
APN	movistar.es
PDP Context	IP
Dial Number	*99#
User Name	MOVISTAR
Password	MOVISTAR
Authentification	AUTO
Operation Mode	Keep Alive
Redial Period	300 seconds

<Previous Next> Cancel

Configure WiFi Settings **Step 3 of 5**

WIFI Enable:	☑
Name (SSID):	WLAN_C651
Mode:	802.11b/g/n mixed

<Previous Next> Cancel

Configure WiFi Security **Step 4 of 5**

Security Mode	WPA2 PSK
WPA	
WPA Algorithms	○ TKIP ◉ AES ○ TKIPAES
Pass Phrase	12345678
Key Renewal Interval	3600 Seconds (0 ~ 4194303)

<Previous Next> Cancel

Configuration as Follows **Step 5 of 5**

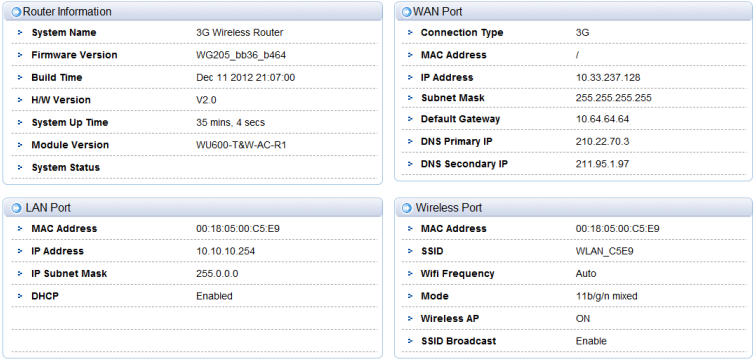
ConnectionType :	3G
Net Mode :	3G
APN :	3GNET
Dial Number :	*99#
Username :	MOVISTAR
Authentification :	AUTO
Operation Mode :	Manual
WiFi :	Enable
Name(SSID) :	WLAN_C651
Wireless Mode :	802.11b/g/n mixed
Security Mode :	Disable

<Previous Finish Cancel

4 Router Setting

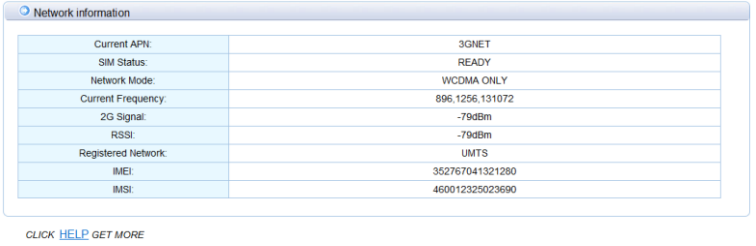
4.1 Port Status

It will show some information to you.



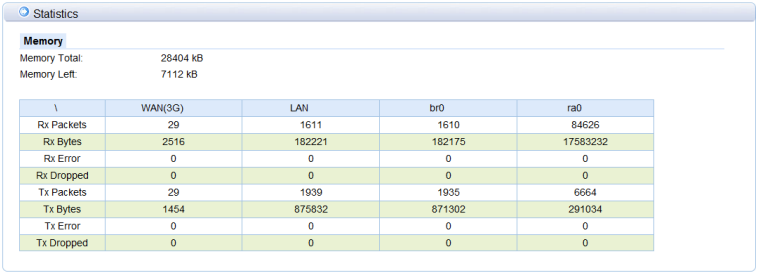
4.2 3G Information

It will show some information about the network.



4.3 statistics

It shows the statistics data.



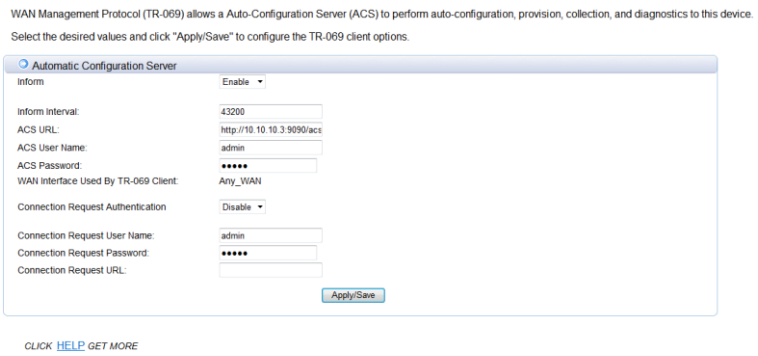
Memory：The display the router memory total size and the remaining size.

WAN/LAN: Show WAN/LAN transceiver packet situation.

RA0: Show Wireless transceiver packet situation.

4.4 ACS Client

It shows the information of the ACS Client.



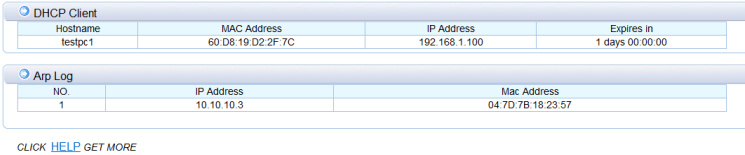
Inform: Set the status of the inform function.

Inform Interval: Set the inform interval time.

ACS URL: Set the URL of the ACS server.

4.5 DHCP Client

This page shows DHCP client information such as host name, MAC address, IP address and lease time.

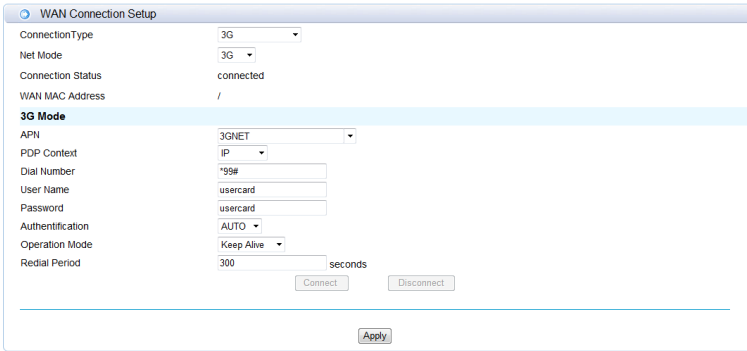


5 Internet Settings

5.1 WAN Setup

5.1.1 3G Mode

According to your network environment to choose the different connection mode and configure the APN parameters.
When you click on the "Apply" button, system will be reconfigured.
If you want to disconnect the 3G net, click on the "disconnect" button.



Net Mode: Choose 3G or 2G mode. It will try to use 3G mode at first when you choose auto.
APN: APN (Access Point Name) is a configurable network identifier.
PDP Context: A Packet Data Protocol (PDP) context.

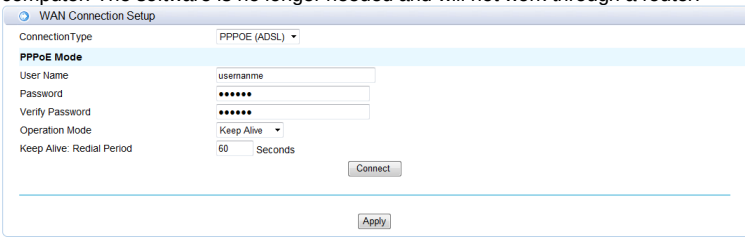
Dial Number: It is the dial number which will be used when you create a Dial-Up connection with 3G.
Username: It is the user name which will be used when you create a Dial-Up connection with 3G.
Password: It is the password which will be used when you create a Dial-Up connection with 3G.
Authentication: You can choose Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP) to pass the Authentication.
Operation Mode:

Auto: The 3G Modem automatically dials to access internet when it is switched on.
Manual: The 3G Modem dials to connect internet by clicking "connect" the connection page of the management console.
On Demand: The 3G Modem automatically dials to connect internet when you attempt to send data through internet.

Apply & Disconnect: connect or disconnect the 3G dial.

5.1.2 PPPOE Mode

Choose PPPoE (Point to Point Protocol over Ethernet) if your ISP uses a PPPoE connection.Your ISP will provide you with a username and password. This option is typically used for DSL services. Make sure to remove your PPPoE software from your computer. The software is no longer needed and will not work through a router.



CLICK HELP *GET MORE*

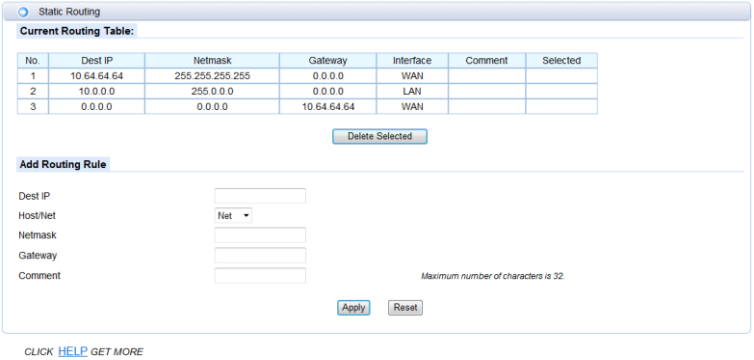
User Name: Enter your PPPoE user name.
Password: Enter your PPPoE password and then retype the password in the next box.
Operation Mode:

Auto: The PPPOE Modem automatically dials to access internet when it is switched on.
Manual: The PPPOE Modem dials to connect internet by clicking "connect" the connection page of the management console.
On Demand: The PPPOE Modem automatically dials to connect internet when you attempt to send data through internet.

Apply & Disconnect: connect the PPPOE dial.

5.2 Static Routing

It shows some information of the static routing.



Dest IP: Enter the IP address of the packets that will take this route

Host/Net: Single IP address or an entire network segment

Netmask: Enter the subnet mask to specify the subnet of the IP packets that will take this route.

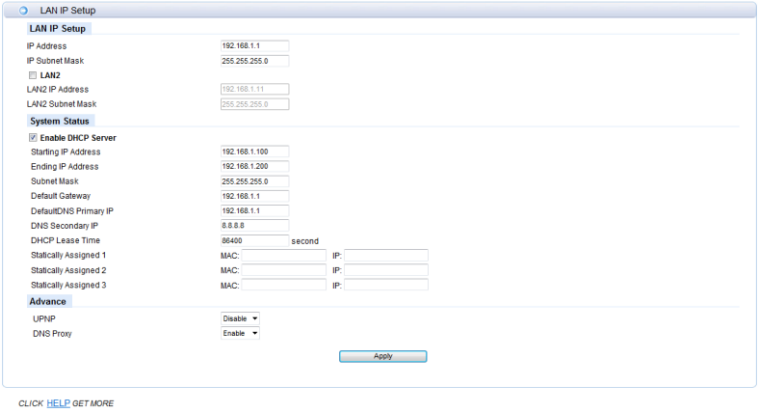
Gateway: Enter the next hop that will be taken if this route is used.

Comment: Remark your defined rule.

6 Wireless Setting

6.1 LAN IP Setup

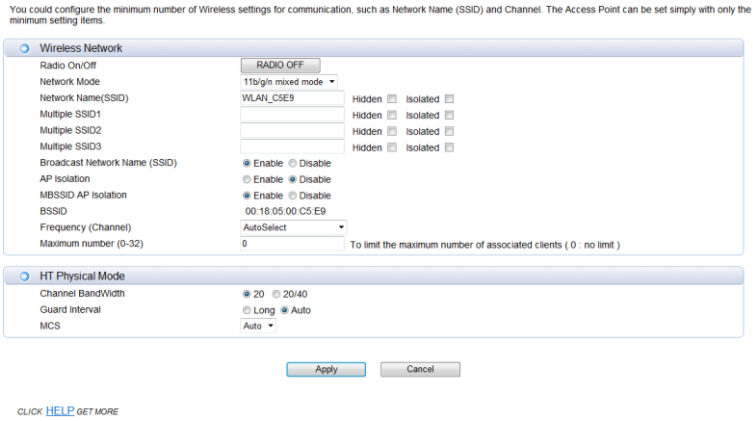
You can configure the LAN port parameters here.



IP Address: Set LAN IP address of the router.
IP Subnet Mask: Set subnet mask of the router.
LAN 2: Add the LAN IP address, so that LAN users can connect to the router through the LAN network.
Starting IP Address & Ending IP Address: The IP range obtained through DHCP by LAN host.
Subnet Mask: The subnet mask obtained through DHCP by LAN host
Default Gateway: Gateway obtained through DHCP by LAN host.
DefaultDNS Primary IP: DNS server obtained through DHCP by LAN host (If enabled DNS Proxy, you had better fill the LAN IP address, so that when the router DNS change, don't reset this).
DNS Secondary IP: If you can't connect the DefaultDNS Primary IP address, router will try to connect this IP address.
UPNP: To use the Universal Plug and Play (UPnP™) feature click on Enabled. UPNP provides compatibility with networking equipment, software and peripherals.
DNS proxy: Choose enable if you want to get DNS service.

6.2 Basic

It shows some information of the wireless connection.

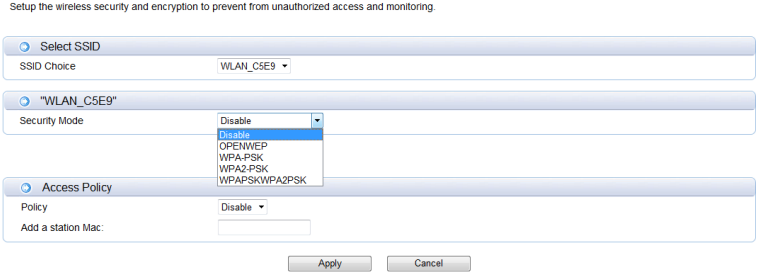


WIFI On/Off: Open or close the router wireless function.
Network Name (SSID): Set the SSID. You can connect the router by this SSID. It can be hidden or isolated. If select Hide function, the router's SSID cannot be scanned; Select Isolated function, it can prevent wireless communications.
Multiple SSID1 ~ Multiple SSID4: Set the 2nd to the 5th SSID. They are similar to the SSID.
Broadcast Network Name (SSID): Disable this function, wireless client will not scan to the router's SSID.
AP Isolation: Enable this function, the client within the AP cannot access each other, to prevent spread of the virus.
MBSSID AP Isolation: Enable this function, the client outside the AP cannot access client within the AP.
BSSID: Basic Service Set Identifier.
Frequency (Channel): The channel currently used. You can select channel from 1 to 14. The router will choose the frequency by itself if you select the "AutoSelect".
Maximum number(0-32): It is the maximum number of hosts can connect the router. If you enter 0, it will be no upper limit.
Channel Band Width: Select the channel bandwidth of the router.
Guard Interval: Check this box to reduce the guard interval time therefore increasing the data capacity. However, it's less reliable and may create higher data loss.
MCS: Modulation Coding Scheme

6.3 Security

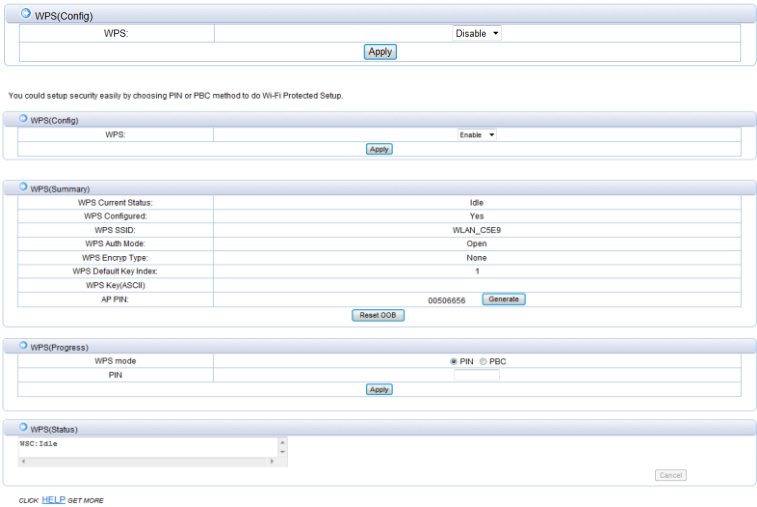
The router's security mode supports (Disable，OPENWEP，SHAREDWEP，

WEPAUTO，WPA-PSK，WPA2-PSK，WPAPSKWPA2PSK).
The router can select different encryption authentication methods for different SSID, configured security policy "Allow" means to allow only the client of specific MAC address access; configured security policy "Reject" means to reject only the client of specific MAC address access; configured security policy "Disable" means to accept all the clients access.



6.4 WPS

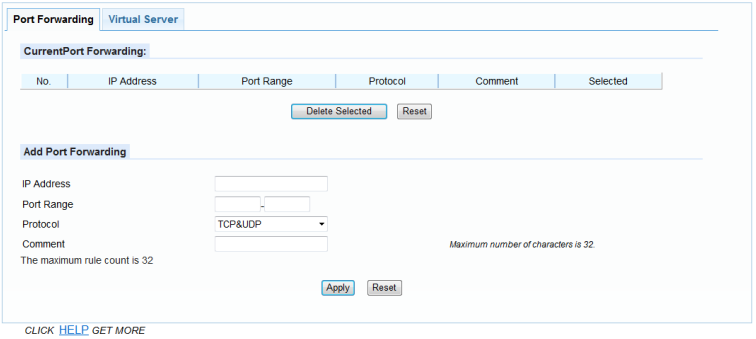
Security Mode: Enable WPS (Wi-Fi Protected Setup)



PIN: Select this option to use the PIN method. In order to use this method you must know the wireless client's 8 digit PIN and click Connect.
PBC: Select this option to use the PBC (Push Button) method to add a wireless client. Click Connect.

7 Firewall

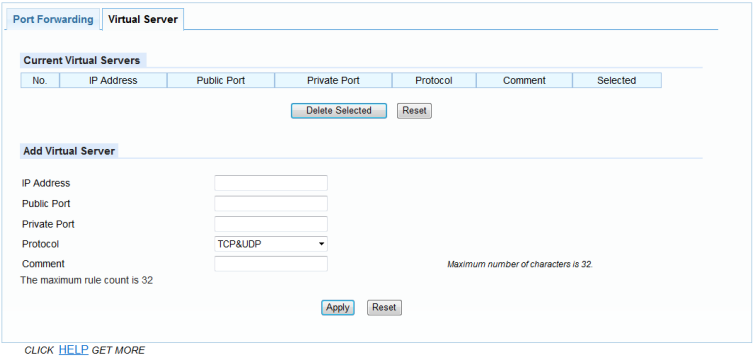
7.1 Port Forwarding



IP Address: Enter the IP address of the computer on your local network that you want to allow the incoming service to.
Protocol: Enter the TCP and/or UDP port or ports that you want to open. You can enter a single port or a range of ports. Separate ports with a common. Example: 24,1009,3000-4000
Comment: Enter a name for the rule or select an application from the drop-down menu. Select an application and click to populate the fields.

7.2 Virtual Server

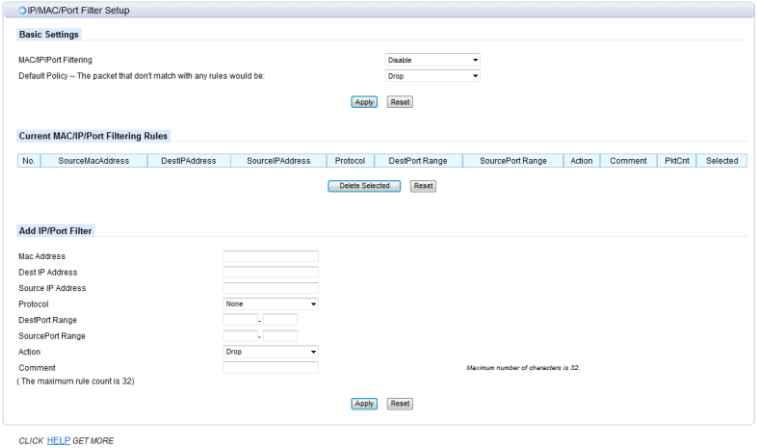
Virtual host can be achieved through the public IP address to access web or FTP services, and the remote user automatically shifted to the local LAN server.
You can define a virtual server service port, external network services all requests to this port will be redirected to the designated router LAN server (specified by IP address), so that users outside the network can successfully access the LAN server, without affecting the internal LAN network security.



IP Address: Enter the IP address of the computer on your local network that you want to allow the incoming service to.
Public Port/Private Port: Enter the port that you want to open next to Private Port and Public Port. The private and public ports are usually the same. The public port is the port seen from the Internet side, and the private port is the port being used by the application on the computer within your local network.
Protocol: Select TCP, UDP, Both or Other from the drop-down menu.
Comment: Enter a name for the rule or select an application from the drop-down menu. Select an application and click to populate the fields

7.3 IP/MAC Filter

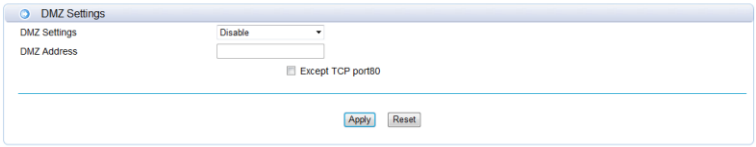
This function is used to configure disable or enable firewall function. Only when the firewall is enabled, access management filter settings IP filter, MAC filter and Port filter can take effect. Otherwise, those functions are disabled.



Mac/IP/Port Filtering: Select "Disable", this function does not take effect, select "Enable", the effect of this function.
Default Policy: The packet that doesn't match with any rules would be dropped or accepted.
MAC Address: Enter the MAC address to define the rules.
Dest IP Address: Enter the destination IP address filtering.
Source IP Address: Enter the local IP address filtering.
Protocol: Select the protocol of the controlled packet.
Dest Port Range: Enter the port range to drop or accept.
Action: Rule is defined to drop or accept, in contrast with default policy.
Comment: Remark your defined rule.

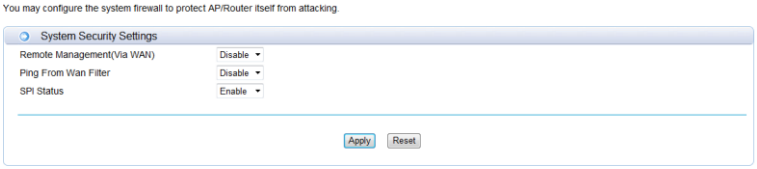
7.4 DMZ

Receive all the data from external network interface forwarded to "DMZ IP address".



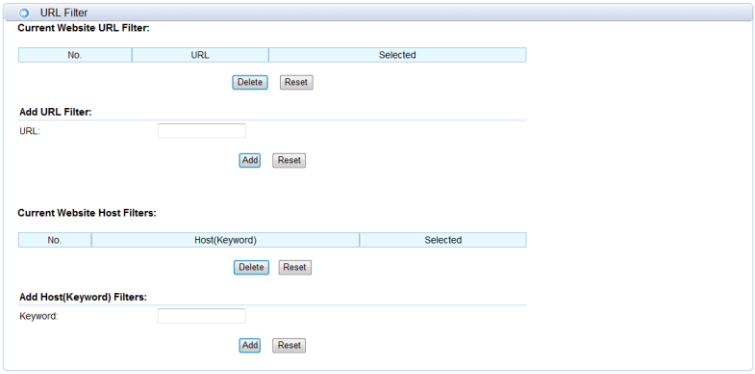
Enable DMZ: If an application has trouble working from behind the router, you can expose one computer to the Internet and run the application on that computer.
Note: Placing a computer in the DMZ may expose that computer to a variety of security risks. Use of this option is only recommended as a last resort.
DMZ Address: Specify the IP address of the computer on the LAN that you want to have unrestricted Internet communication.

7.5 system Security



Remote Management: Enable this function, it will allow access Web management pages through the external network interface.
PING from wan Filter: Enable this function, it will allow PING router via external network interface.
SPI Status: Select "Enable", to activate the SPI firewall.

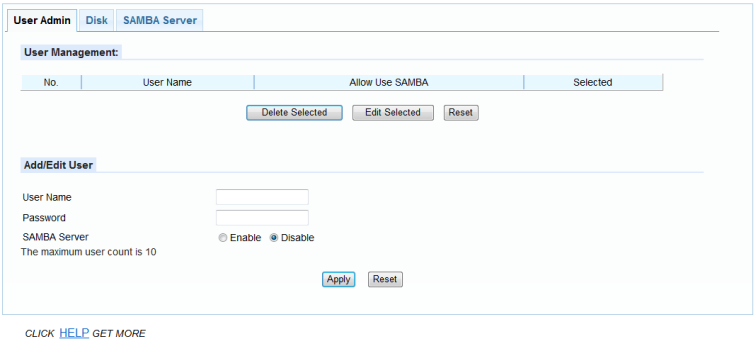
7.6 URL filter



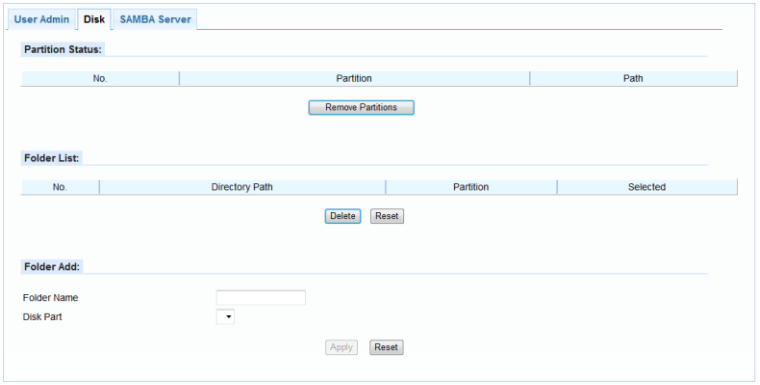
URL Filters: Select Deny computers access to only these sites.
Reset: Click to delete all entries in the list.
Keyword Filters: Enter the keywords or URLs that you want to deny.

8 Application

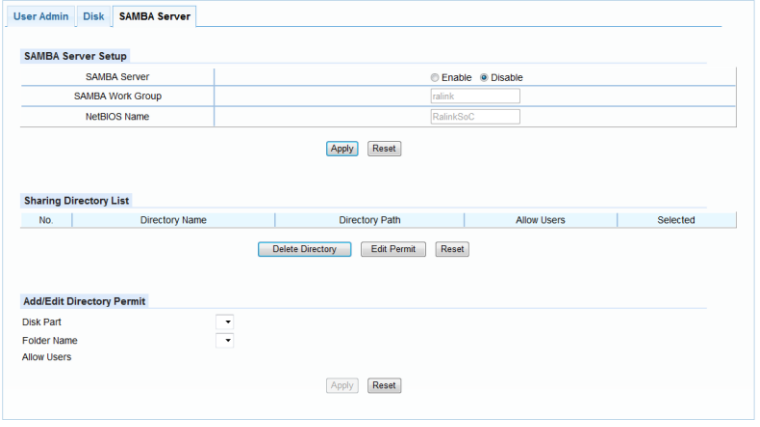
8.1 USB Storage



User Name/Password: Add a user to use the SAMBA server.
FTP Server: Enable/Disable the FTP Server competence.
SAMBA Server: Enable/Disable the SAMBA Server competence.

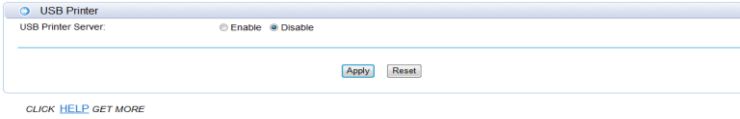


Folder List: Display USB storage folder.
Delete: Selected a folder to delete.
Folder Add: Adding a new folder.



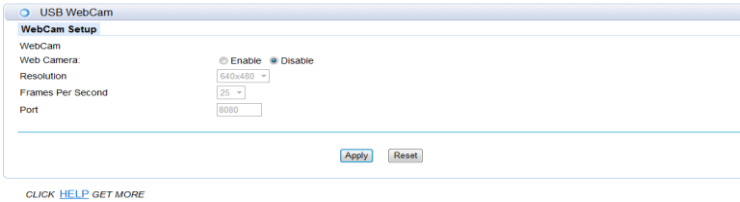
SAMBA Server: Enable/Disable the SAMBA Server.
SAMBA Work Group: Enter the name of the SAMBA Working Group.
Net Bios Name: Enter the name of the Net Bios.
Add/Edit Directory Permit: Allows users to access files

8.2 USB Printer



USB Printer Server: Enable/Disable the USB Printer Server.

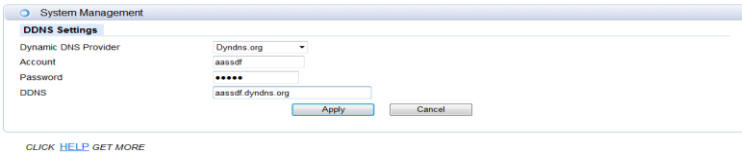
8.3 USB Web Cam



Web Camera: Enable/Disable the Web Camera.
Resolution: You can choose 640x480, 320x240, 160x120 resolution.
Frames Per Second: You can choose 5,10,15,20,25,30 frames.
Port: Access to the camera's need the port number.

8.4 DDNS

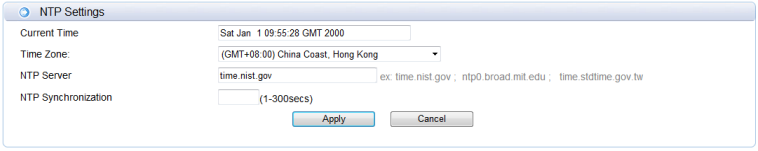
This function allows you to provide Internet users with a domain name (instead of an IP address) to access your virtual servers. This router supports dynamic DNS service provided by the provider "http://www.dyndns.org" or "http://www.freedns.afraid.org". Please register this service at these providers firstly.



DDNS Provider: Select the website provides dynamic domain name service.
Account: Login registered username on the DDNS provider.

Password: Password registered on the DDNS provider.
DDNS: Domain name registered on the DDNS provider.

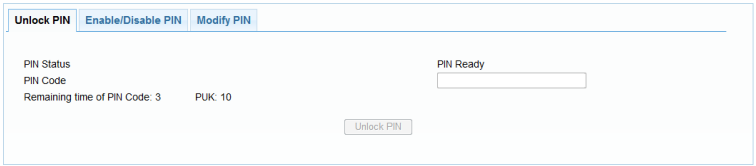
8.5 NTP Setting



CLICK HELP *GET MORE*

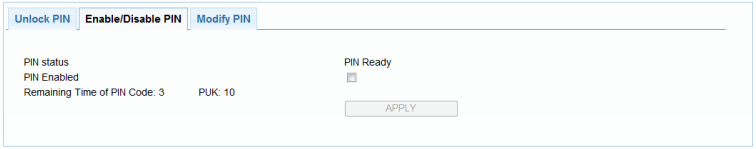
Time Zone：Select the time region.
NTP Server：Enter network time protocol Server.
NTP synchronization：Synchronization time with NTP server.

8.6 PIN Setting



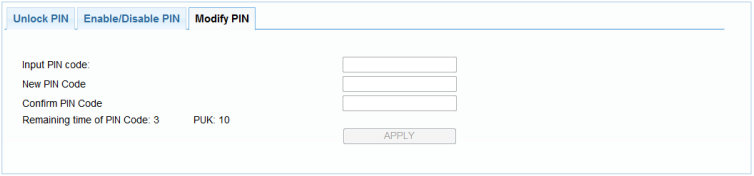
CLICK HELP *GET MORE*

PIN Code: Enter the PIN Code to Unlock PIN.



CLICK HELP *GET MORE*

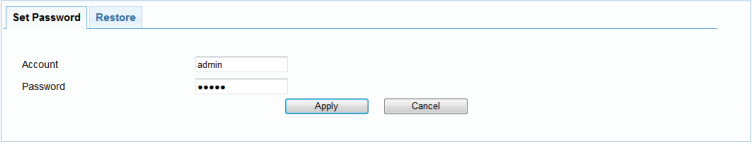
PIN Enabled: Enable/Disable the S(U)IM card PIN function.
PUK: PIN Unlocking Key, unlock PIN code (PIN1)



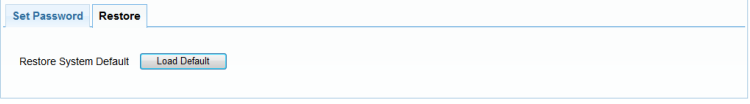
Modify PIN: Modify the S(U)IM card PIN Code.

9 Administration

9.1 System Settings

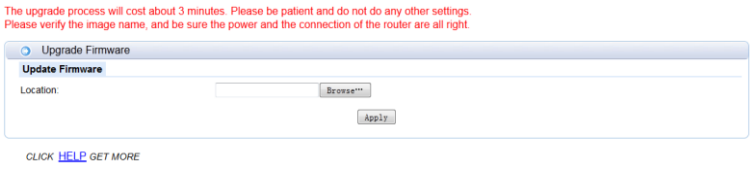


You can set the account and the password which used to login.



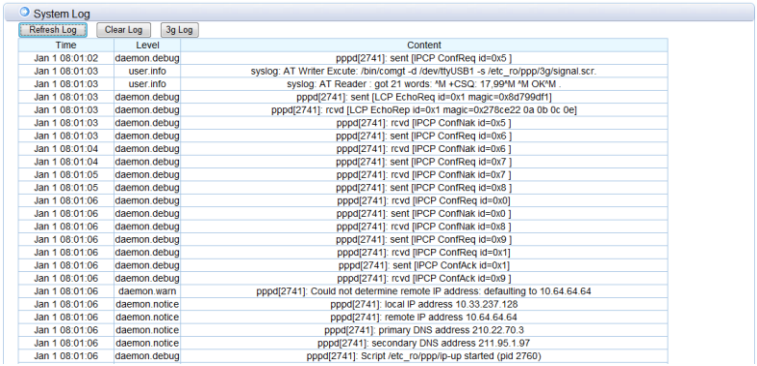
Load Default: system will be restored the factory settings.

9.2 Router Upgrade



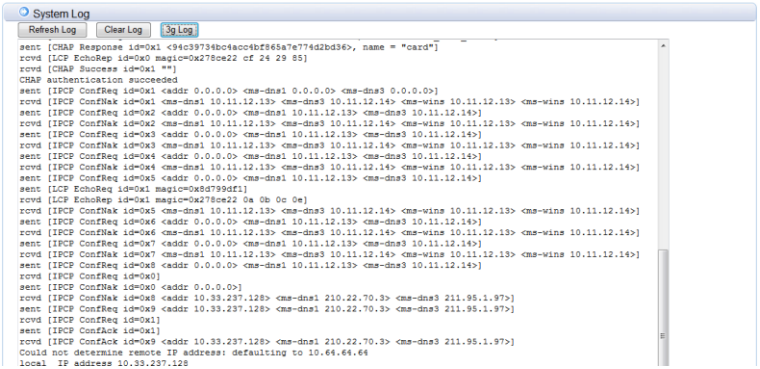
Update Firmware: After you have downloaded the new firmware, click Browse to locate the firmware update on your hard drive. Click Upload to complete the firmware upgrade.

9.3 System Log



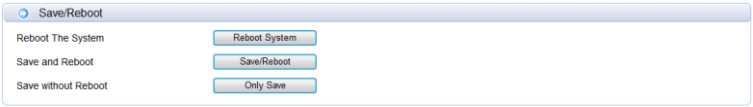
Time	Level	Content
Jan 1 08:01:02	daemon.debug	pppd[2741]: sent [IPCP ConfReq id=0x5]
Jan 1 08:01:03	user.info	syslog: AT Writer Excute: /bin/comgt -d /dev/ttyUSB1 -s /etc_ro/ppp/3g/signal.scr.
Jan 1 08:01:03	user.info	syslog: AT Reader . got 21 words: ^M +CSQ: 17,99^M ^M OK^M .
Jan 1 08:01:03	daemon.debug	pppd[2741]: sent [LCP EchoReq id=0x1 magic=0x8d799df1]
Jan 1 08:01:03	daemon.debug	pppd[2741]: rcvd [LCP EchoRep id=0x1 magic=0x278ce22 0a 0b 0c 0e]
Jan 1 08:01:03	daemon.debug	pppd[2741]: rcvd [IPCP ConfNak id=0x5]
Jan 1 08:01:03	daemon.debug	pppd[2741]: sent [IPCP ConfReq id=0x6]
Jan 1 08:01:04	daemon.debug	pppd[2741]: rcvd [IPCP ConfNak id=0x6]
Jan 1 08:01:04	daemon.debug	pppd[2741]: sent [IPCP ConfReq id=0x7]
Jan 1 08:01:05	daemon.debug	pppd[2741]: rcvd [IPCP ConfNak id=0x7]
Jan 1 08:01:05	daemon.debug	pppd[2741]: sent [IPCP ConfReq id=0x8]
Jan 1 08:01:06	daemon.debug	pppd[2741]: rcvd [IPCP ConfReq id=0x0]
Jan 1 08:01:06	daemon.debug	pppd[2741]: sent [IPCP ConfNak id=0x0]
Jan 1 08:01:06	daemon.debug	pppd[2741]: rcvd [IPCP ConfNak id=0x8]
Jan 1 08:01:06	daemon.debug	pppd[2741]: sent [IPCP ConfReq id=0x9]
Jan 1 08:01:06	daemon.debug	pppd[2741]: rcvd [IPCP ConfReq id=0x1]
Jan 1 08:01:06	daemon.debug	pppd[2741]: sent [IPCP ConfAck id=0x1]
Jan 1 08:01:06	daemon.debug	pppd[2741]: rcvd [IPCP ConfAck id=0x9]
Jan 1 08:01:06	daemon.warn	pppd[2741]: Could not determine remote IP address: defaulting to 10.64.64.64
Jan 1 08:01:06	daemon.notice	pppd[2741]: local IP address 10.33.237.128
Jan 1 08:01:06	daemon.notice	pppd[2741]: remote IP address 10.64.64.64
Jan 1 08:01:06	daemon.notice	pppd[2741]: primary DNS address 210.22.70.3
Jan 1 08:01:06	daemon.notice	pppd[2741]: secondary DNS address 211.95.1.97
Jan 1 08:01:06	daemon.debug	pppd[2741]: Script /etc_ro/ppp/ip-up started (pid 2760)

Display the log information of starting and running system.



Display the log information of 3G dial-up.

10 Save/Reboot



CLICK HELP GET MORE

Reboot System: system will be rebooted.
Save/Reboot: system will save the configuration and reboot.
Reboot System: system will be reboot.

Federal Communication Commission Interference Statement

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.

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

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that

to which the receiver is connected.

- Consult the dealer or an experienced radio/TV technician for help.

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

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

FOR COUNTRY CODE SELECTION USAGE (WLAN DEVICES)

Note: The country code selection is for non-US model only and is not available to all US model. Per FCC regulation, all WiFi product marketed in US must fixed to US operation channels only.