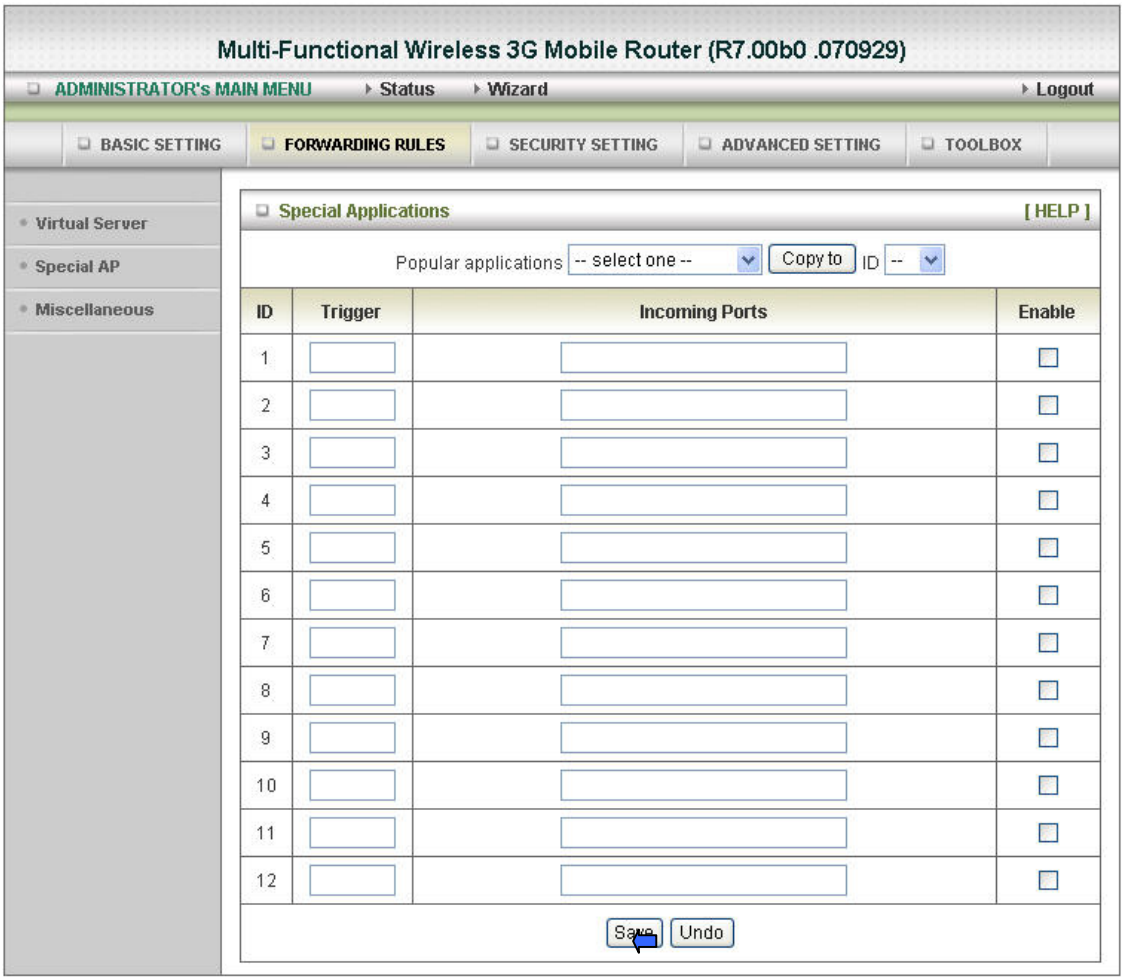


Some applications require multiple connections, like Internet games, Video conferencing, Internet telephony, etc. Because of the firewall function, these applications cannot work with a pure NAT router. The **Special Applications** feature allows some of these applications to work with this product. If the mechanism of Special Applications fails to make an application work, try setting your computer as the **DMZ** host instead.

1. **Trigger**: the outbound port number issued by the application.
2. **Incoming Ports**: when the trigger packet is detected, the inbound packets sent to the specified port numbers are allowed to pass through the firewall.

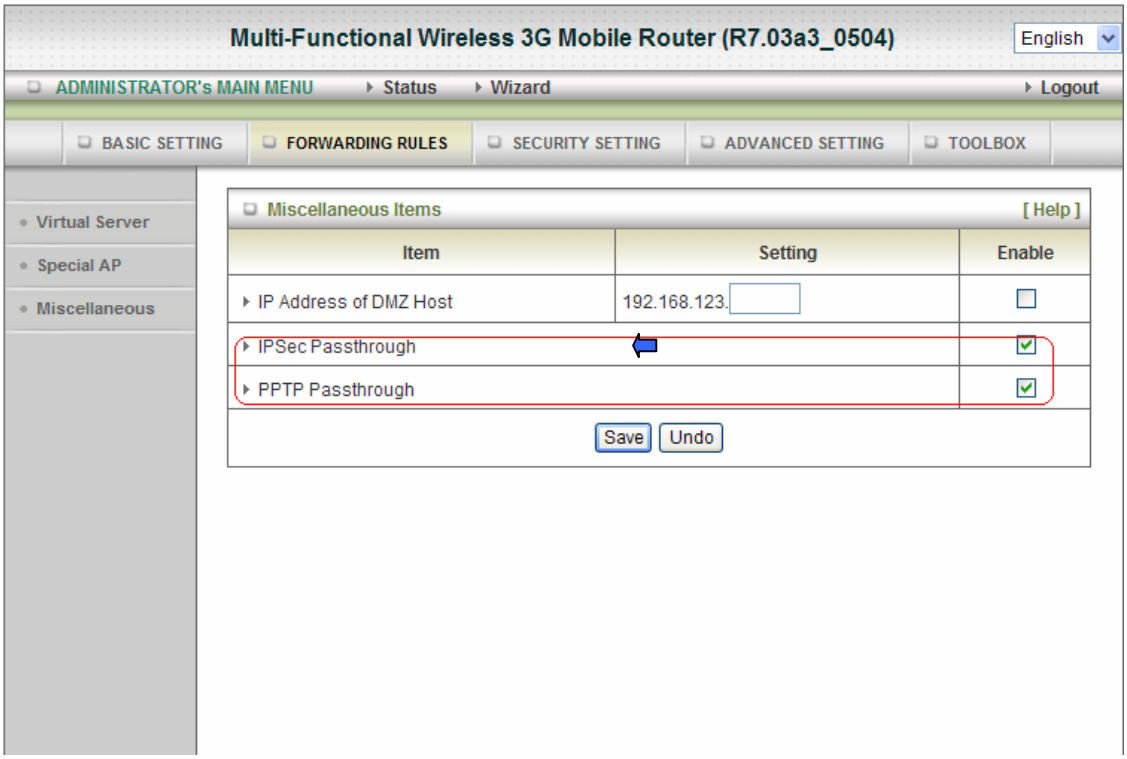
This product provides some predefined settings.

1. Select your application and
2. Click **Copy to** to add the predefined setting to your list.

Note! At any given time, only one PC can use each Special Application tunnel.

Click on "Save" to store what you just select or" Undo" to give up

Advanced Setup > Forwarding Rules > Miscellaneous



IP Address of DMZ Host

DMZ (Demilitarized Zone) Host is a host without the protection of firewall. It allows a computer to be exposed to unrestricted 2-way communication for Internet games, Video conferencing, Internet telephony and other special applications.

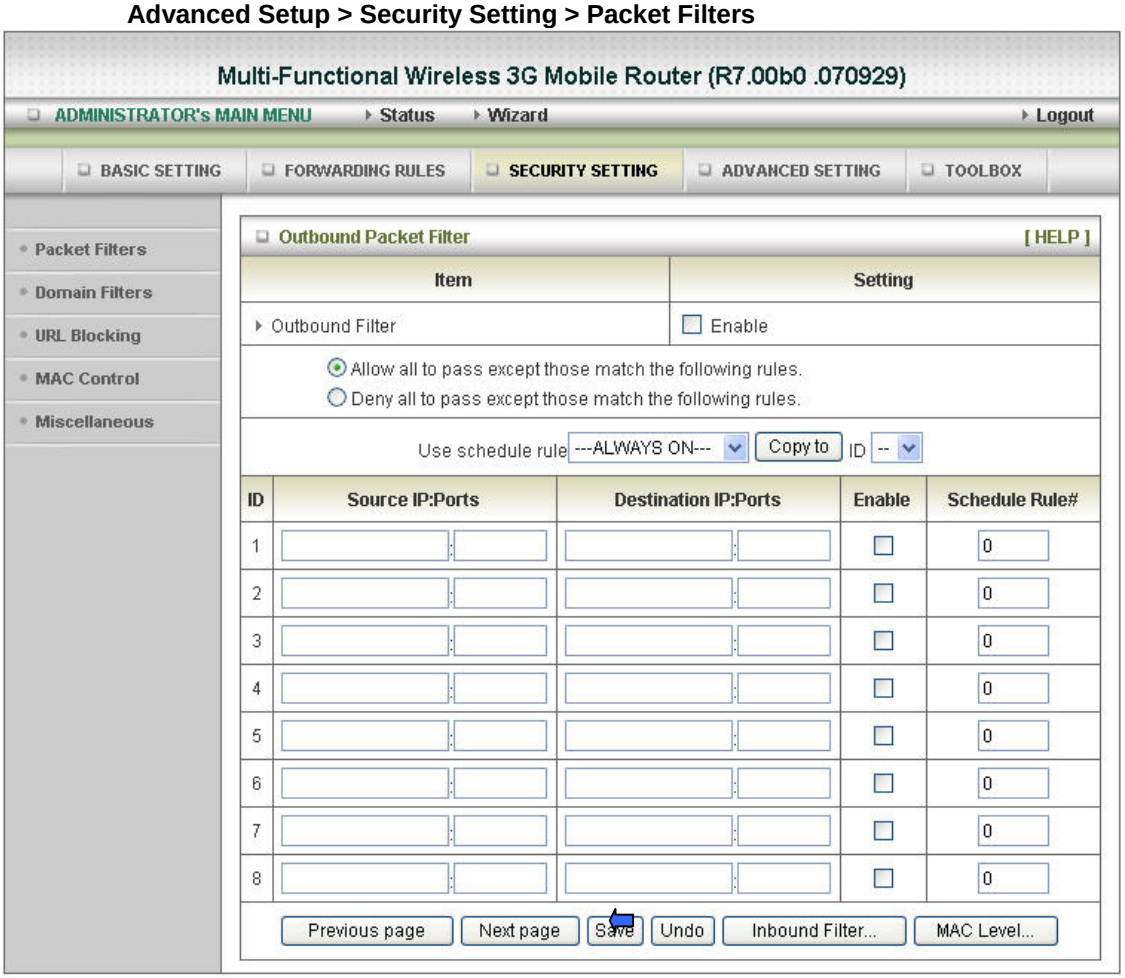
IPSec / PPTP Passthrough

The device also supports VPN Pass-through (IPSec/PPTP Pass-through). Once VPN pass-through is enabled, multiple VPN connections can be made through the device. This is useful when you have many VPN clients on the LAN.

Click on “Save” to store what you just select or “Undo” to give up

NOTE: This feature should be used only when needed.

Advanced Setup > Security Setting > Packet Filters



Packet Filter enables you to control what packets are allowed to pass the router. Outbound filter applies on all outbound packets. However, inbound filter applies on packets that destined to Virtual Servers or DMZ host only. You can select one of the two filtering policies:

1. Allow all to pass except those match the specified rules
2. Deny all to pass except those match the specified rules

You can specify 8 rules for each direction: inbound or outbound. For each rule, you can define the following:

- Source IP address
- Source port
- Destination IP address
- Destination port
- Protocol: TCP or UDP or both.
- Use Rule#

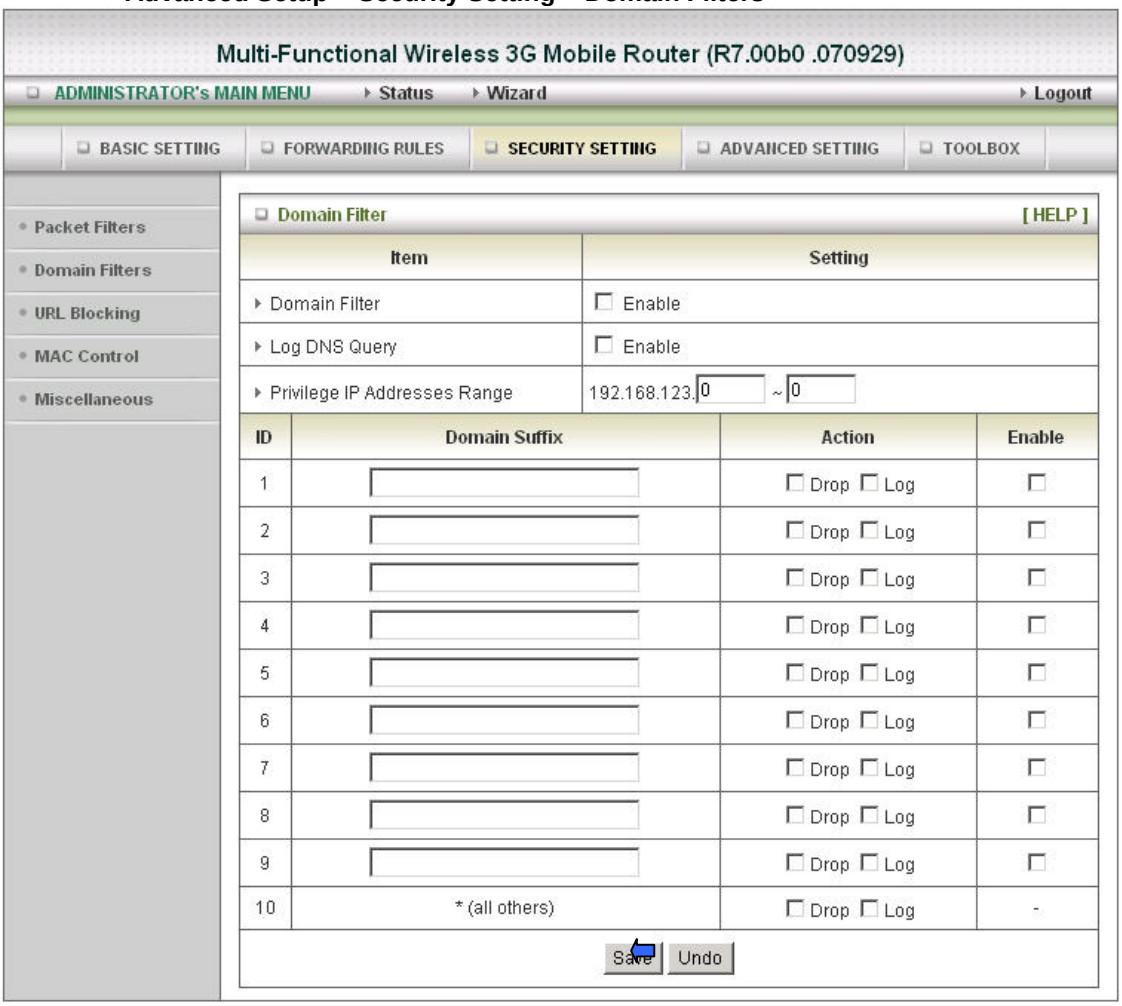
For source or destination IP address, you can define a single IP address (4.3.2.1) or a range of IP addresses (4.3.2.1-4.3.2.254). An empty implies all IP addresses.
For source or destination port, you can define a single port (80) or a range of ports (1000-1999). Add prefix "T" or "U" to specify TCP or UDP protocol. For example, T80, U53, U2000-2999, No prefix indicates both TCP and UDP are defined. An empty implies all port addresses. **Packet Filter** can work with **Scheduling Rules**, and give user more flexibility on Access control. For Detail, please refer to **Scheduling Rule**. Each rule can be enabled or disabled individually.

Click on "Save" to store what you just select or "Undo" to give up

Inbound Filter:

To enable **Inbound Packet Filter** click the check box next to **Enable** in the **Inbound Packet Filter** field
Click on "Save" to store what you just select or "Undo" to give up

Advanced Setup > Security Setting > Domain Filters



Domain Filter

let you prevent users under this device from accessing specific URLs.

Domain Filter Enable

Check if you want to enable Domain Filter.

Log DNS Query

Check if you want to log the action when someone accesses the specific URLs.

Privilege IP Address Range

Setting a group of hosts and privilege these hosts to access network without restriction.

Domain Suffix

A suffix of URL to be restricted; For example, ".com", "xxx.com".

Action

When someone is accessing the URL met the domain-suffix, what kind of action you want.

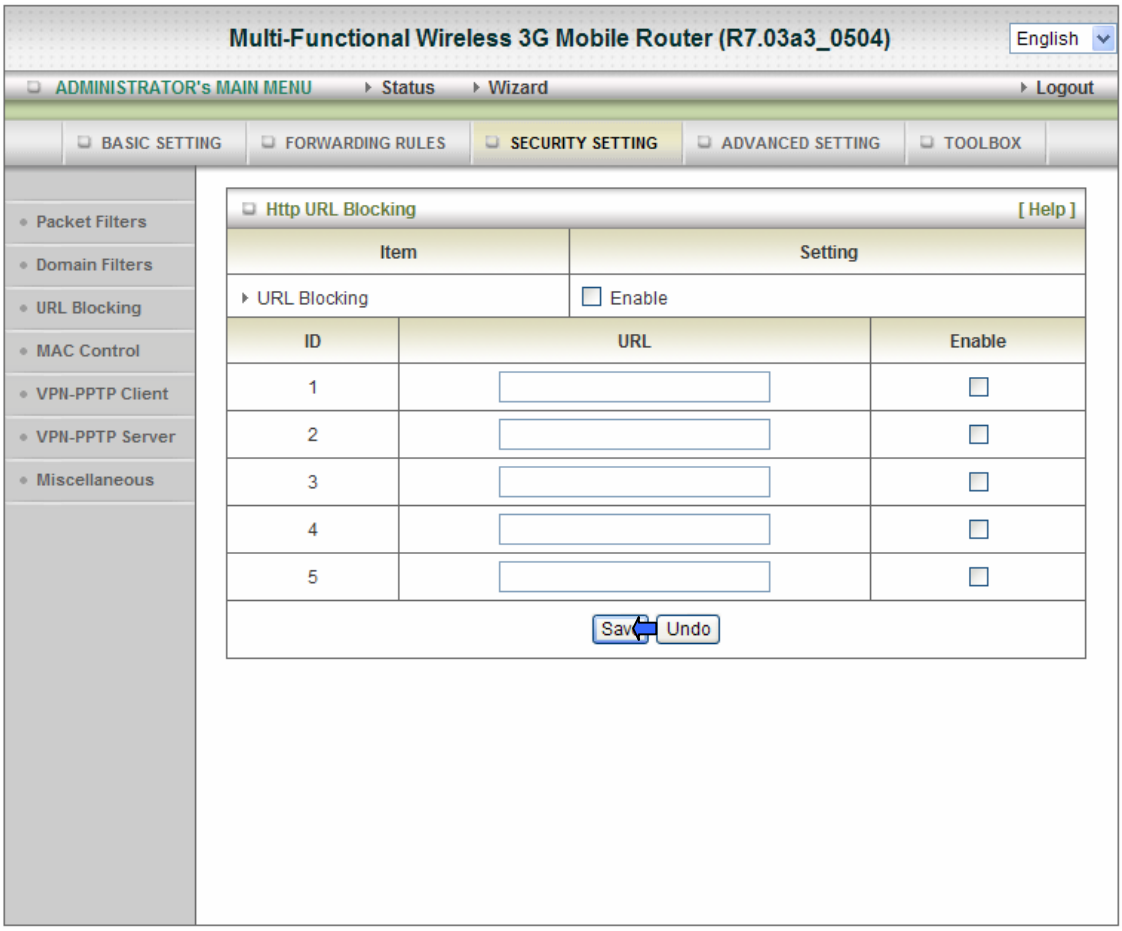
Check drop to block the access. Check log to log these access.

Enable

Check to enable each rule.

Click on “Save” to store what you just select or “Undo” to give up

Advanced Setup > Security Setting > URL Blocking



URL Blocking will block LAN computers to connect to pre-defined Websites.

The major difference between “Domain filter” and “URL Blocking” is Domain filter require user to input suffix (like .com or .org, etc), while URL Blocking require user to input a keyword only. In other words, Domain filter can block specific website, while URL Blocking can block hundreds of websites by simply a **keyword**.

URL Blocking Enable

Check if you want to enable URL Blocking.

URL

If any part of the Website's URL matches the pre-defined word, the connection will be blocked.

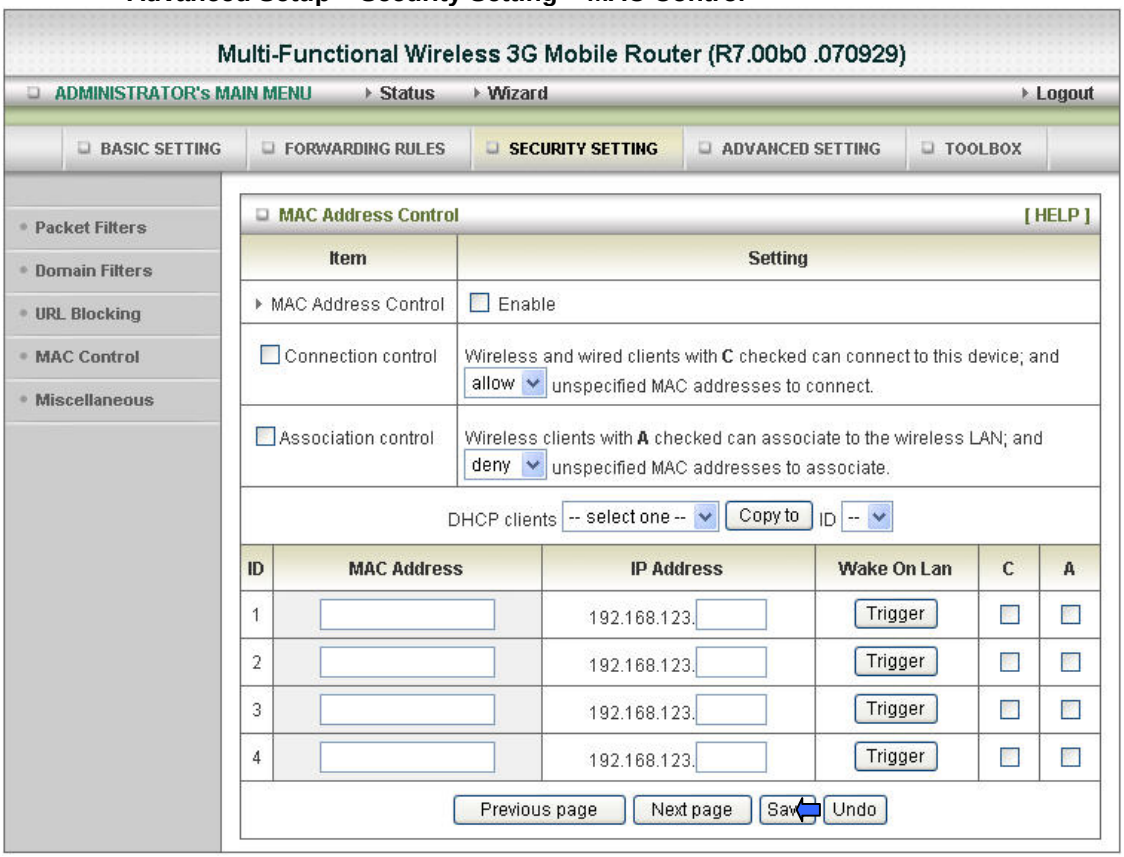
For example, you can use pre-defined word "sex" to block all websites if their URLs contain pre-defined word "sex".

Enable

Check to enable each rule.

Click on “Save” to store what you just select or “Undo” to give up

Advanced Setup > Security Setting > MAC Control



MAC Address Control allows you to assign different access right for different users and to assign a specific IP address to a certain MAC address.

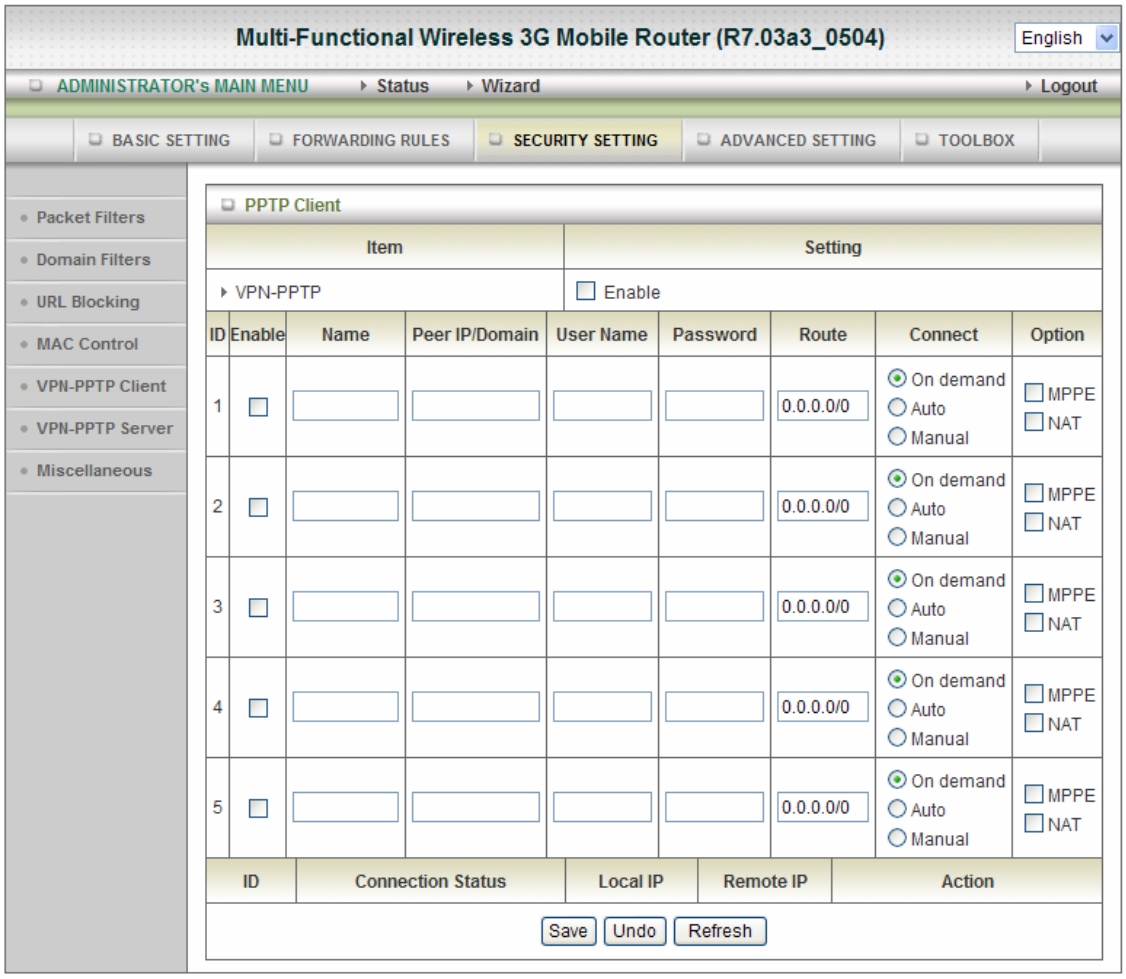
MAC Address Control Check “Enable” to enable the “MAC Address Control”. All of the settings in this page will take effect only when “Enable” is checked.

Connection control Check "Connection control" to enable the controlling of which wired and wireless clients can connect to this device. If a client is denied to connect to this device, it means the client can't access to the Internet either. Choose "allow" or "deny" to allow or deny the clients, whose MAC addresses are not in the "Control table" (please see below), to connect to this device.

Association control Check "Association control" to enable the controlling of which wireless client can associate to the wireless LAN. If a client is denied to associate to the wireless LAN, it means the client can't send or receive any data via this device. Choose "allow" or "deny" to allow or deny the clients, whose MAC addresses are not in the "Control table", to associate to the wireless LAN

1: **Click on “Save” to store what you just select or “Undo” to give up**
2: **Click on “Next Page” to go down or “Previous page” back to last page**

Advanced Setup > Security Setting > VPN-PPTP Client



VPN-PPTP: Enables or Disables the PPTP client.

Enable: Check to enable each rule.

Name: The name of Item.

Peer IP/Domain: The IP/Domain of PPTP server is.

PPTP Account and Password: The account and password your ISP assigned to you. If you don't want to change the password, keep it empty.

Route: Which connection will use the PPTP section?

Connect: There are 3 modes to select:

On demand: The device will link up with ISP when the clients send outgoing packets.

Auto: The device will link with ISP until the connection is established.

Manually: The device will not make the link until someone clicks the connect-button in the Status-page.

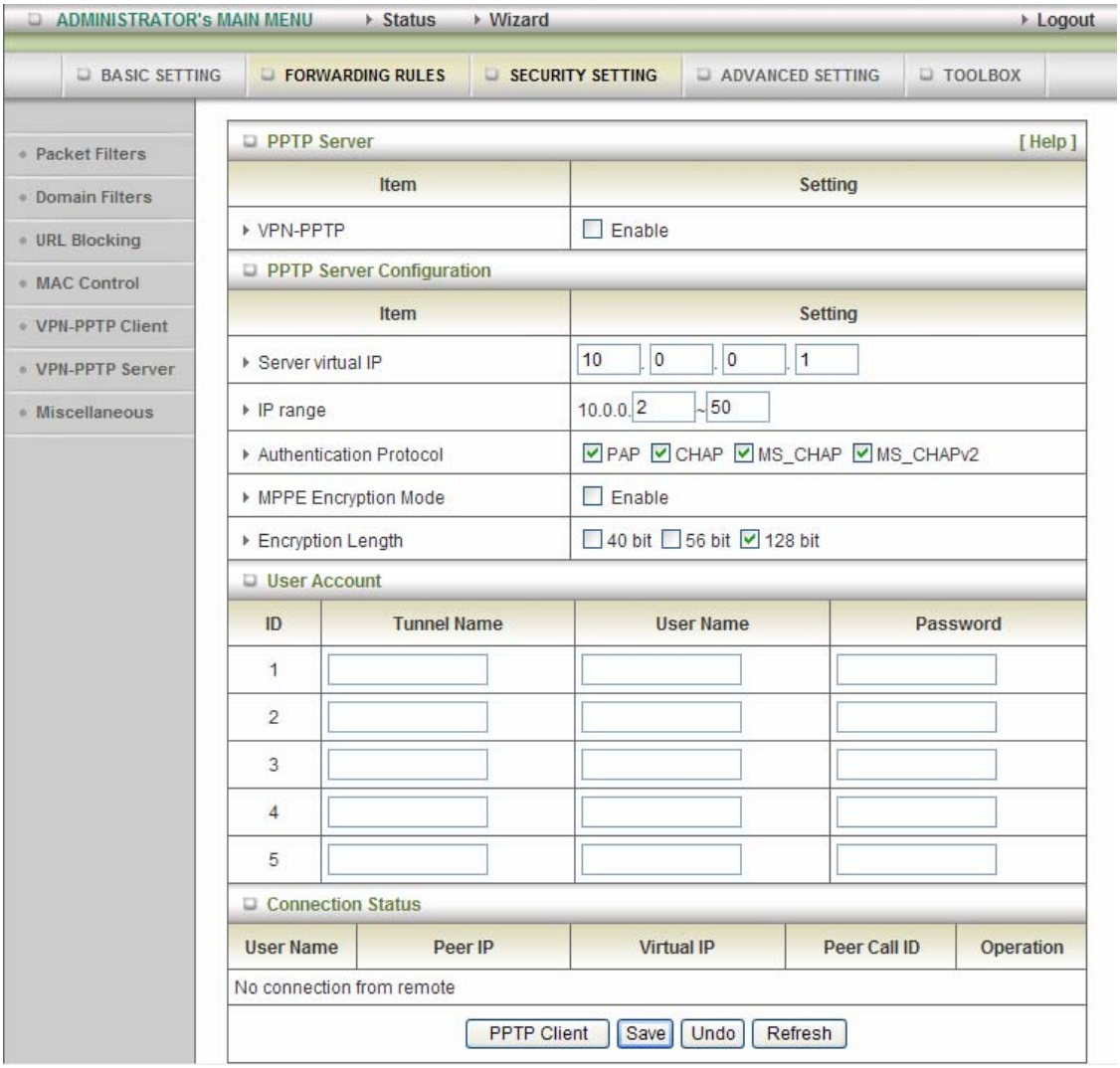
Option:

MPPE: The MPPE encryption supports.

NAT: The Nat Traversal supports.

Click on “Save” to store what you just select or” Undo” to give up

Advanced Setup > Security Setting > VPN-PPTP Server



The Router can behave as a PPTP server, and allows remote hosts to access LAN servers after establishing PPTP connection with it. The device can support three authentication methods: PAP, CHAP, MSCHAP(v1) and MSCHAP(v2). Users can also enable MPPE encryption when using MSCHAP.

VPN-PPTP:

Check this checkbox to enable function of PPTP server.

Server virtual IP:

The IP address of PPTP server. This IP address should be different from IP address of PPTP server and LAN subnet of VPN gateway.

IP range:

The client IP range. IPs in this range are given clients trying to connect.

Authentication Protocol:

Users can choose authentication protocol as PAP, CHAP, or MS_CHAP(v1), MS_CHAP(v2).

MPPE Encryption Mode:

Check this checkbox to enable MPPE encryption. Please note that MPPE needs to work with MSCHAP authentication method.

Encryption Length:

There are 3 kind of encryption for MPPE, 40bits, 56bits and 128bits.

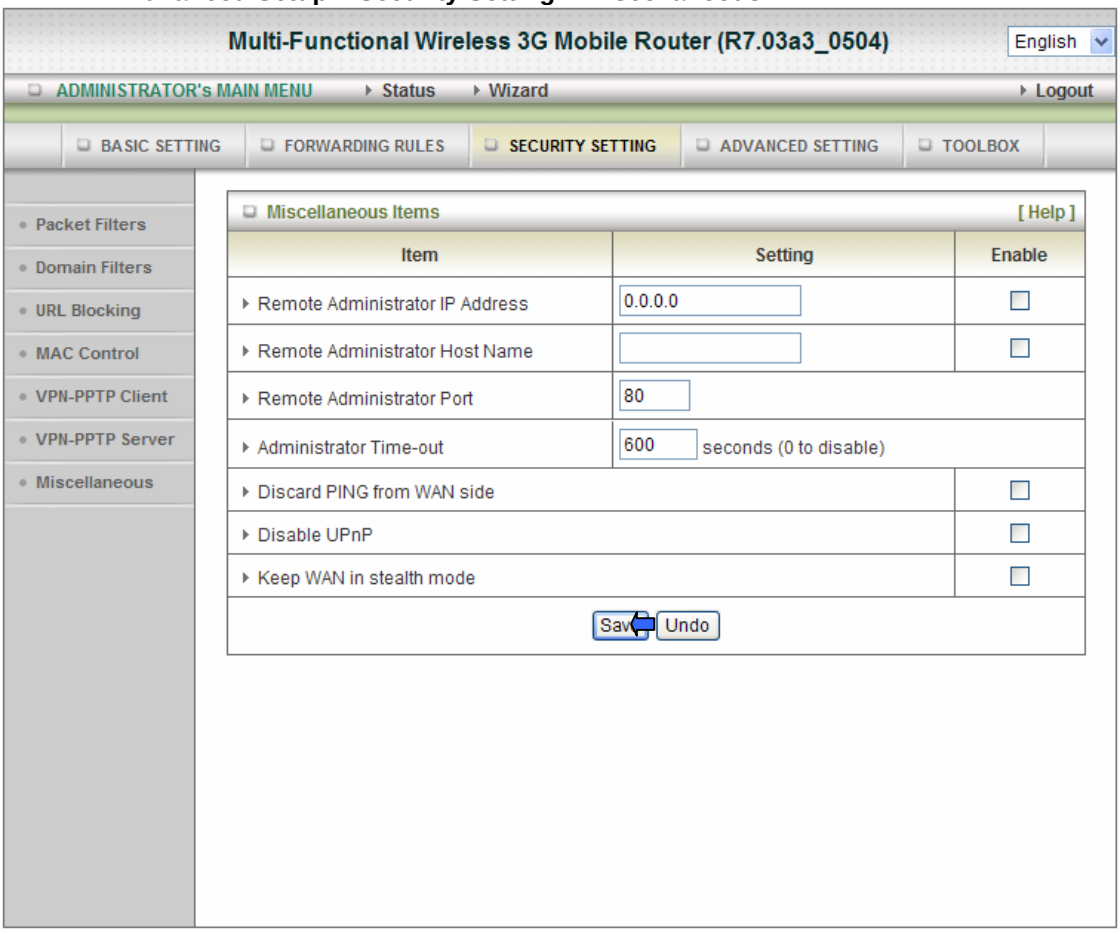
User Account Setting

Users can input five different user accounts for PPTP server. The total accounts are 5.

1. **Tunnel Name:** Input the name for tunnel.
2. **User Name:** Input a user name that is allowed to establish PPTP connection with VPN gateway.
3. **Password**: Input the password for the user.

Click on "Save" to store what you just select or" Undo" to give up

Advanced Setup > Security Setting > Miscellaneous



Remote Administrator Host/Port

In general, only Intranet user can browse the built-in web pages to perform administration task. This feature enables you to perform administration task from remote host. If this feature is enabled, only the specified IP address can perform remote administration. If the specified IP address is 0.0.0.0, any host can connect to

this product to perform administration task. You can use subnet mask bits "/nn" notation to specified a group of trusted IP addresses for example, "10.1.2.0/24". NOTE: When Remote Administration is enabled, the web server port will be shifted to 80. You can change web server port to other port, too.

Administrator Time-out

The time of no activity to logout automatically, you may set it to zero to disable this feature.

Discard PING from WAN side

When this feature is enabled, any host on the WAN cannot ping this product.

Disable UPNP:

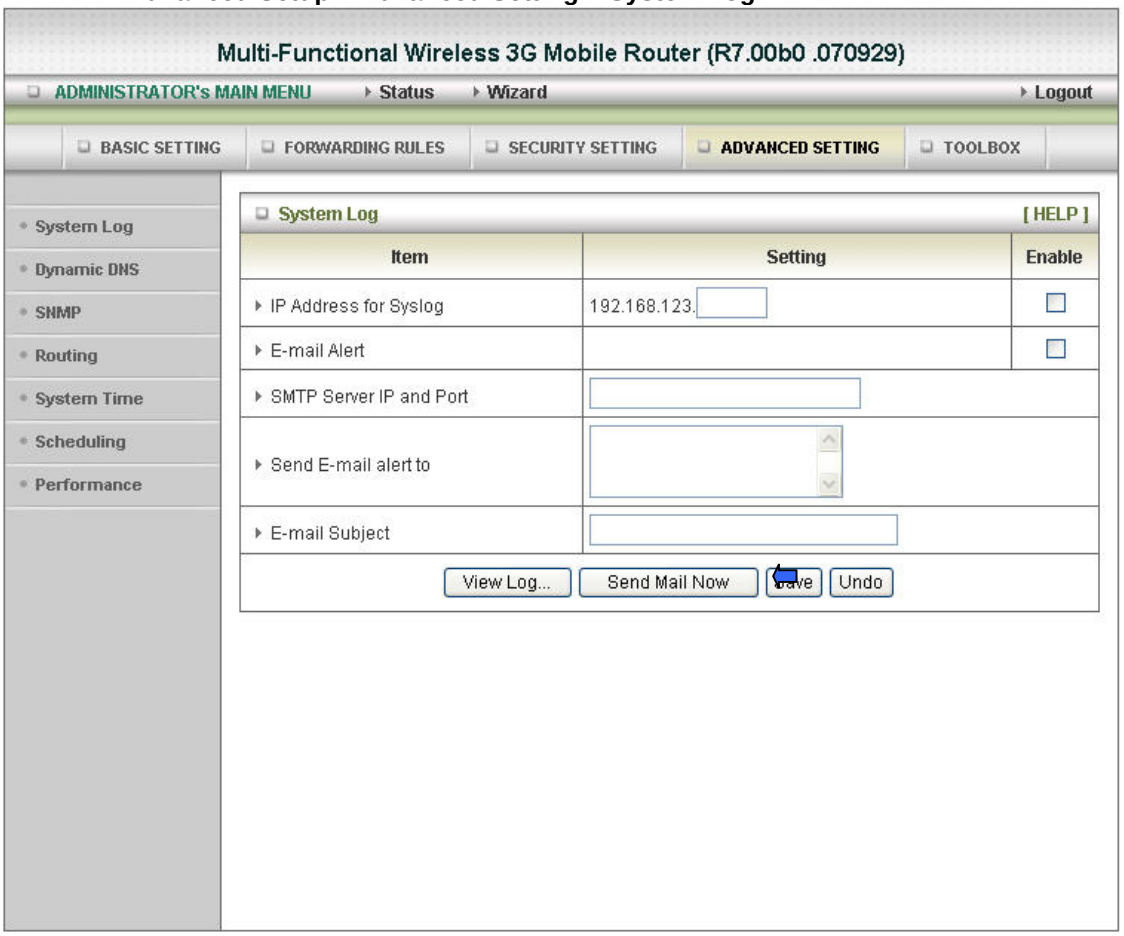
The device can disable UPNP function. If your OS supports UPNP search function and you enable UPNP, like Windows XP. You can get Device IP by UPNP.

Keep WAN in stealth mode:

If the port is not open, the device just to ignore incoming connection attempts, rather than rejecting them.

Click on “Save” to store what you just select or” Undo” to give up

Advanced Setup > Advanced Setting > System Log



This page support two methods to export system logs to specific destination by means of syslog (UDP) and SMTP(TCP). The items you have to setup including:

IP Address for Syslog

Host IP of destination where syslog will be sent to.
Check **Enable** to enable this function.

E-mail Alert Enable

Check if you want to enable Email alert (send syslog via email).

SMTP Server IP and Port

Input the SMTP server IP and port, which are concated with ':'. If you do not specify port number, the default value is 25.
For example, "mail.your_url.com" or "192.168.1.100:26".

Send E-mail alert to

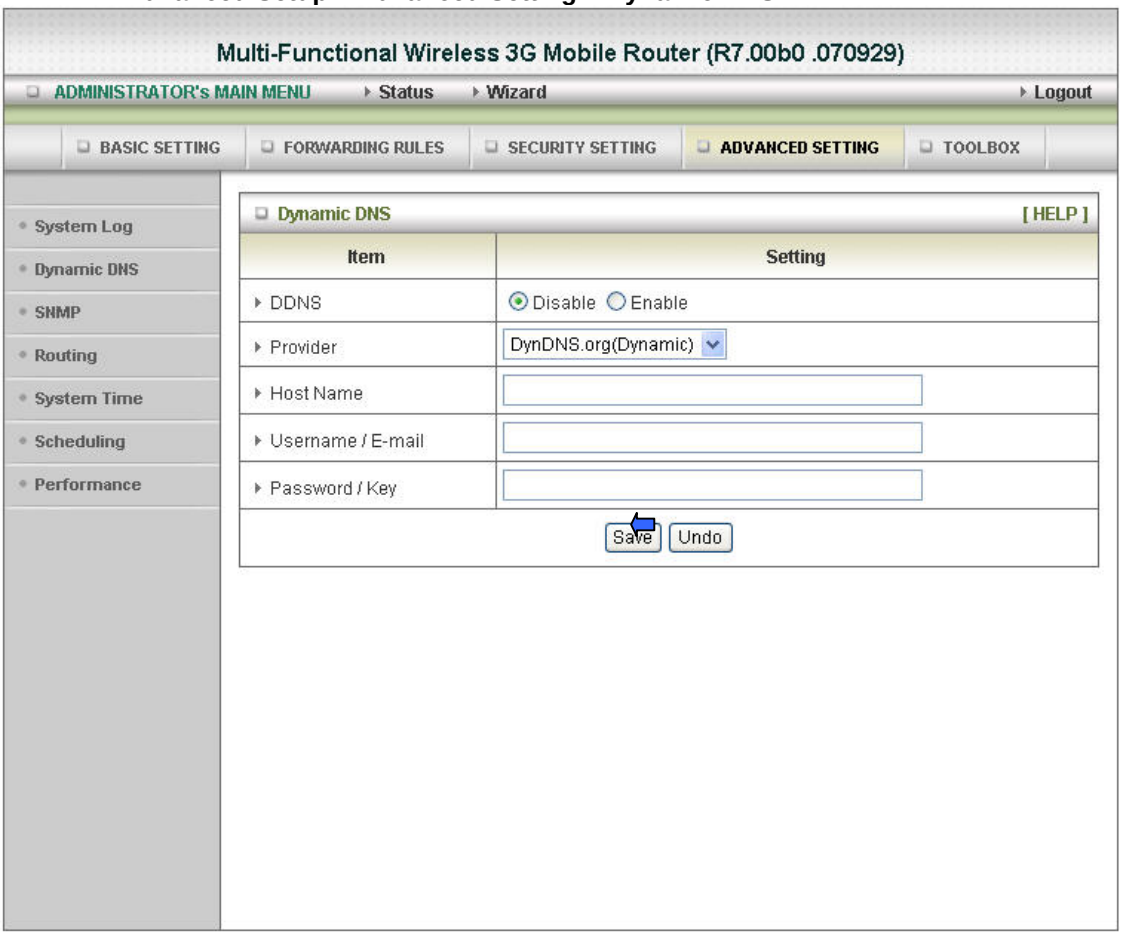
The recipients who will receive these logs, you can assign more than 1 recipient, using ';' or ',' to separate these email addresses.

E-mail Subject

The subject of email alert, this setting is optional.

Click on "Save" to store what you just select or "Undo" to give up

Advanced Setup > Advanced Setting > Dynamic DNS



To host your server on a changing IP address, you have to use dynamic domain name service (DDNS).

So that anyone wishing to reach your host only needs to know the name of it. Dynamic DNS will map the name of your host to your current IP address, which changes each time you connect your Internet service provider.

Before you enable **Dynamic DNS**, you need to register an account on one of these Dynamic DNS servers that we list in **provider** field.

To enable **Dynamic DNS** click the check box next to **Enable** in the **DDNS** field.

Next you can enter the appropriate information about your Dynamic DNS Server.

You have to define:

Provider

Host Name

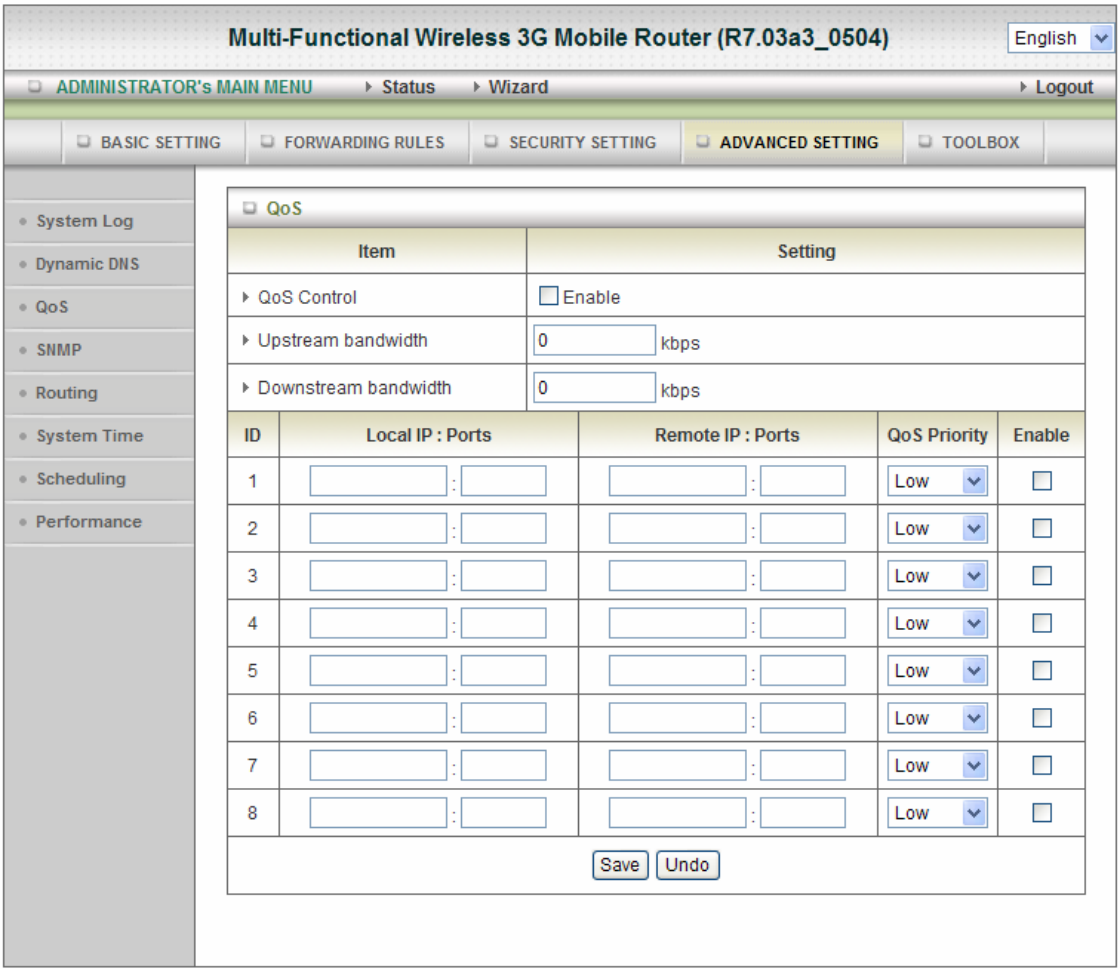
Username/E-mail

Password/Key

You will get this information when you register an account on a Dynamic DNS server.

Click on “Save” to store what you just select or “Undo” to give up

Advanced Setup > Advanced Setting > QOS



Provide different priority to different users or data flows, or guarantee a certain level of performance.

QoS Packet Filter

This Item enables QoS function or not.

Upstream Bandwidth

Set the limitation of upstream speed.

Downstream Bandwidth

Set the limitation of downstream speed.

Local: IP

Define the Local IP address of packets here.

Local: Ports

Define the Local port of the packets in this field.

Remote: IP

Define the Remote IP address of packets here.

Remote: Ports

Define the Remote port of the packets in this field.

QoS Priority

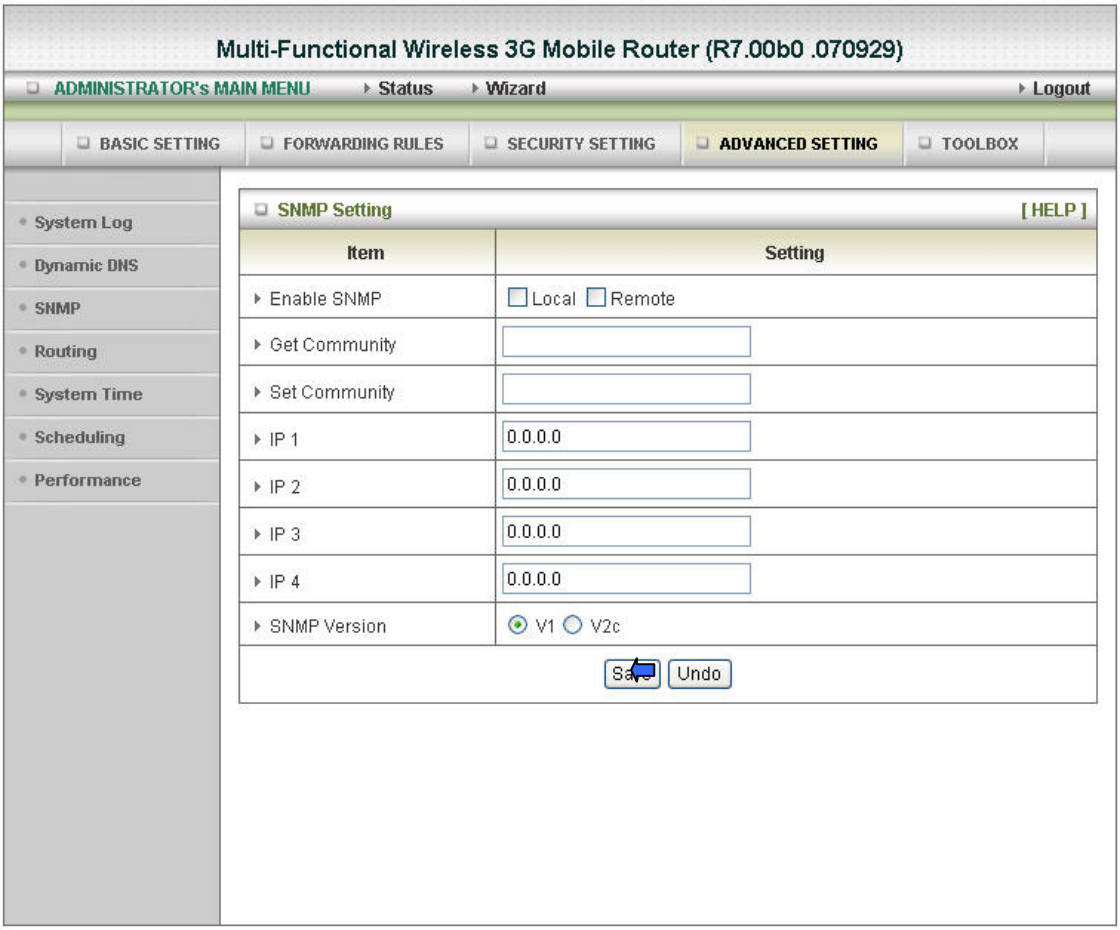
This defines the priority level of the current Policy Configuration. Packets associated with this policy will be serviced based upon the priority level set. For critical applications High or Normal levels are recommended. For non-critical applications select a Low level.

Enable

Check to enable each rule.

Click on "Save" to store what you just select or "Undo" to give up

Advanced Setup > Advanced Setting > SNMP



In brief, SNMP, the Simple Network Management Protocol, is a protocol designed to give a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.

Enable SNMP

You must check either Local or Remote or both to enable SNMP function. If Local is checked, this device will response request from LAN. If Remote is checked, this device will response request from WAN.

Get Community

Setting the community of GetRequest your device will response.

Set Community

Setting the community of SetRequest your device will accept.
IP 1,IP 2,IP 3,IP 4

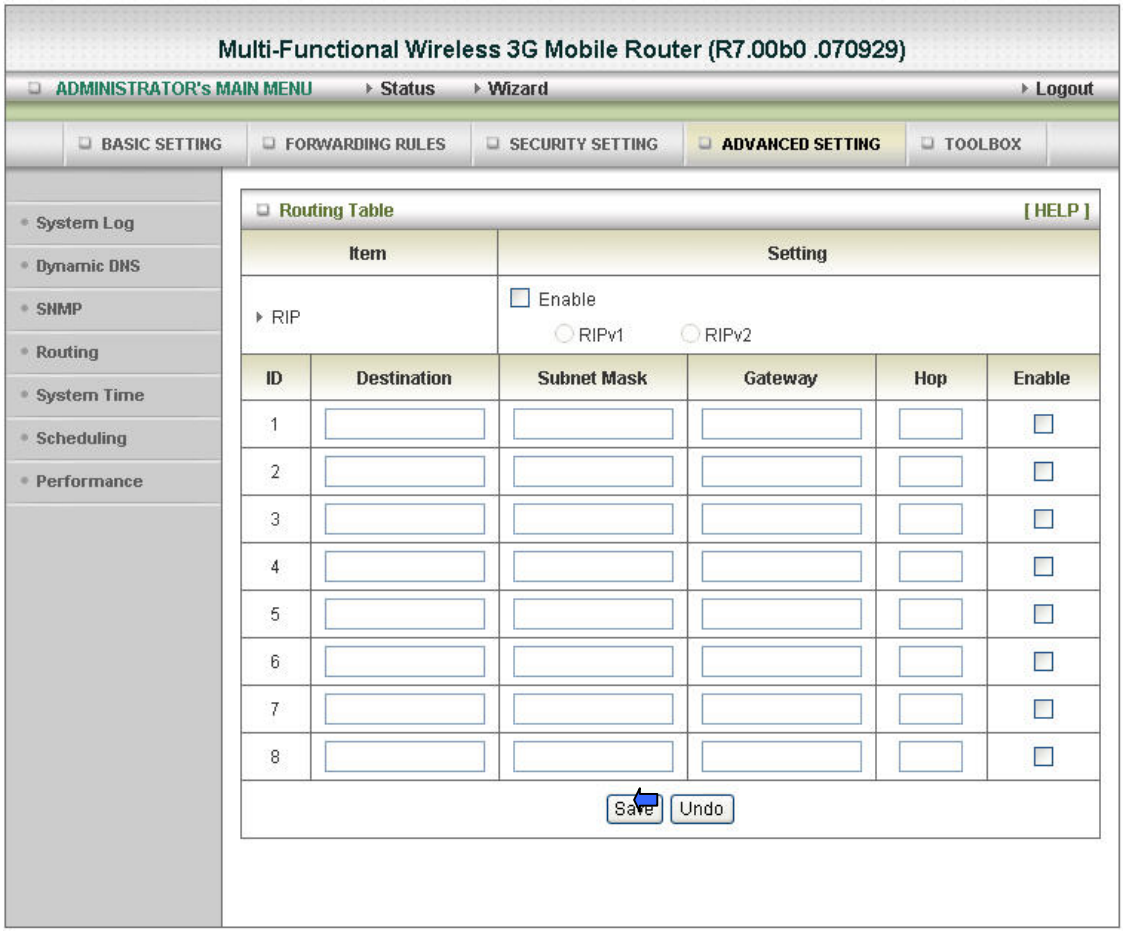
Input your SNMP Management PC's IP here. User has to configure to where this device should send SNMP Trap message.

SNMP Version

Please select proper SNMP Version that your SNMP Management software supports.

Click on "Save" to store what you just select or "Undo" to give up.

Advanced Setup > Advanced Setting > Routing



Routing Tables

Allow you to determine which physical interface address to use for outgoing IP data grams. If you have more than one routers and subnets, you will need to enable routing table to allow packets to find proper routing path and allow different subnets to communicate with each other.

Routing Table settings are settings used to setup the functions of static and dynamic routing.

Dynamic Routing

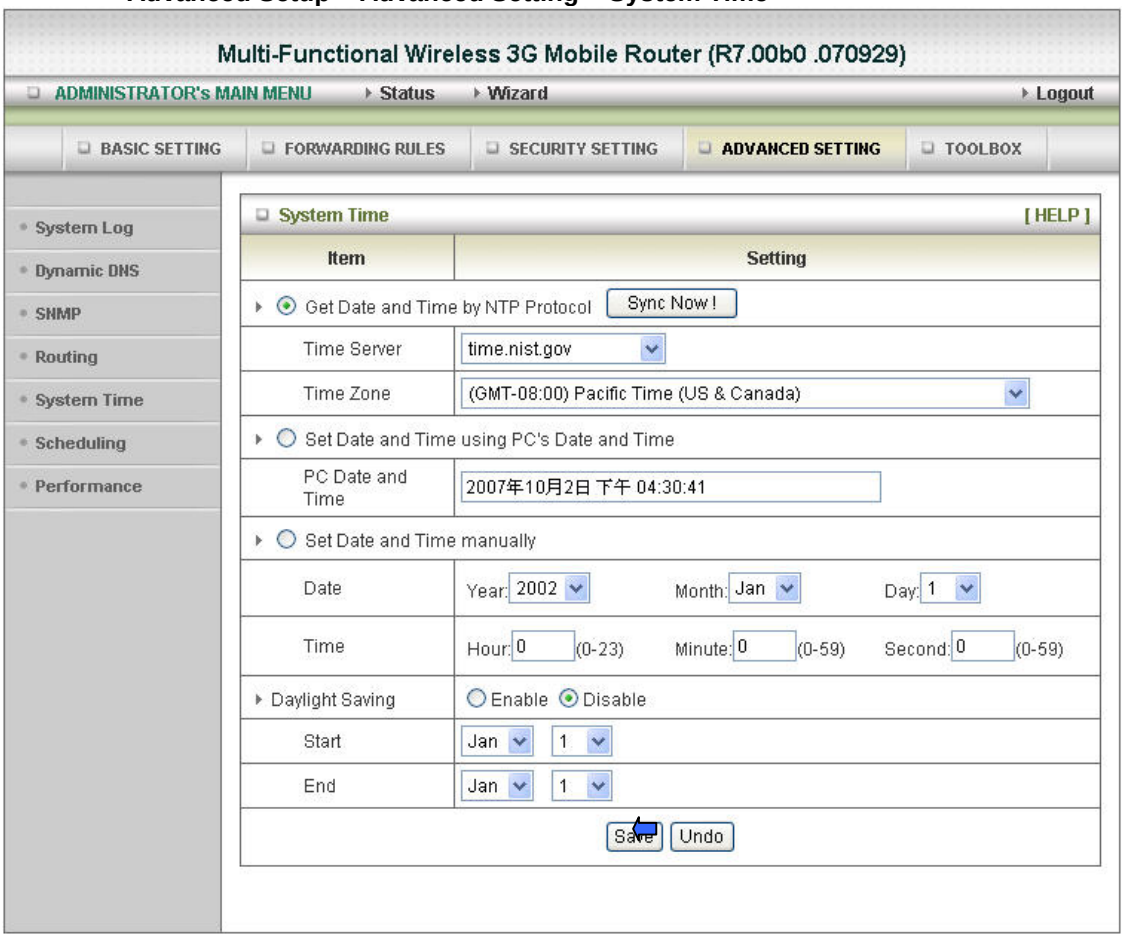
Routing Information Protocol (RIP) will exchange information about destinations for computing routes throughout the network. Please select RIPv2 only if you have different subnet in your network. Otherwise, please select RIPv1 if you need this protocol.

Static Routing

For static routing, you can specify up to 8 routing rules. You can enter the destination IP address, subnet mask, gateway, hop for each routing rule, and then enable or disable the rule by checking or un-checking the Enable checkbox.

Click on "Save" to store what you just select or "Undo" to give up.

Advanced Setup > Advanced Setting > System Time



Get Date and Time by NTP Protocol

Selected if you want to Get Date and Time by NTP Protocol.

Time Server

Select a NTP time server to consult UTC time

Time Zone

Select a time zone where this device locates.

Set Date and Time using PC's Date and Time

Set the Date and Time from your PC

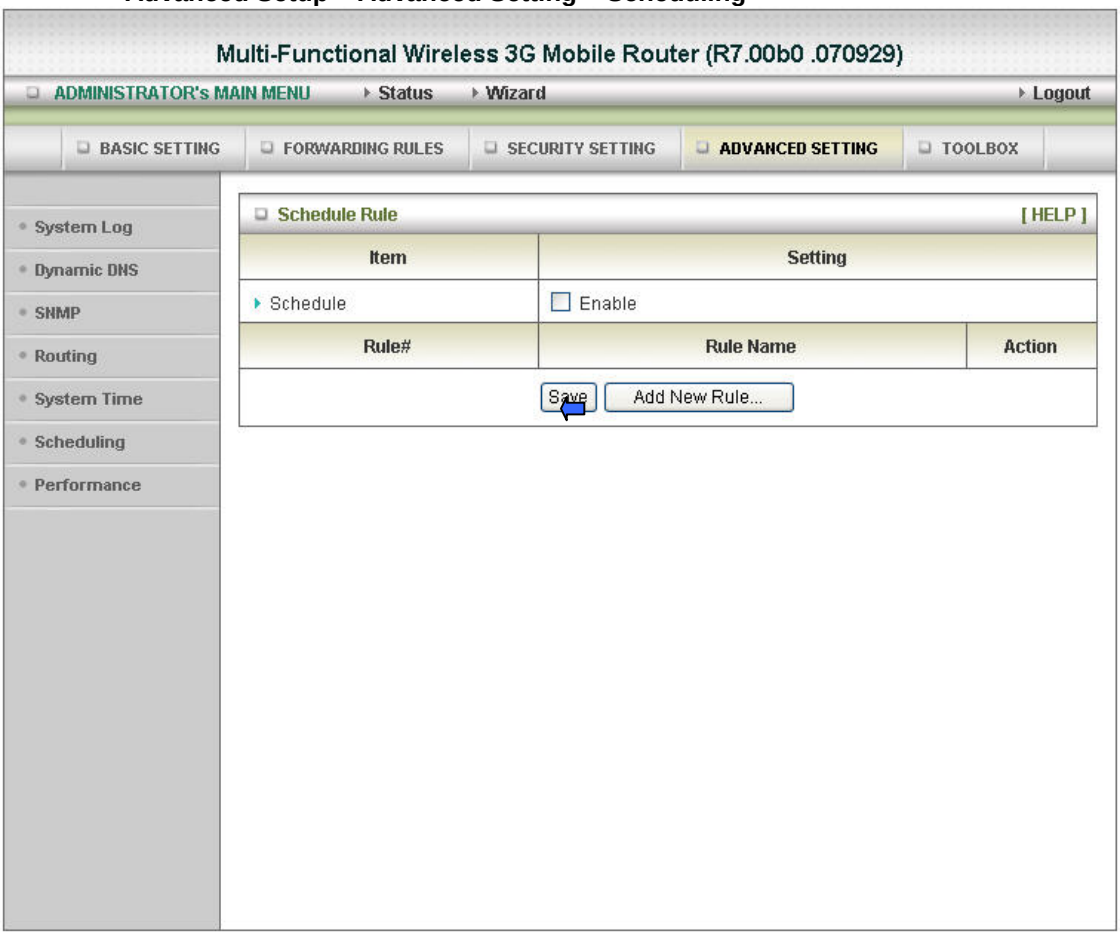
Set Date and Time manually

Selected if you want to Set Date and Time manually.

Daylight Saving

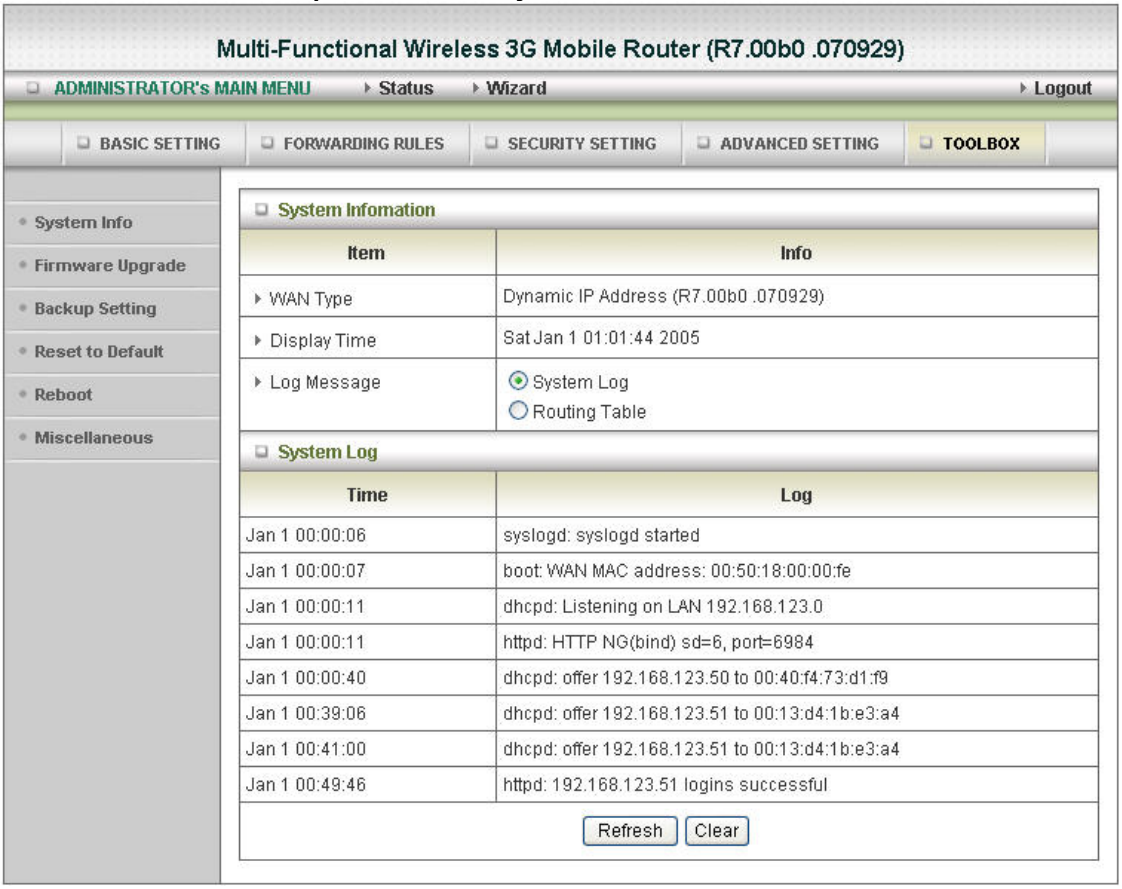
Click on "Save" to store what you just select or "Undo" to give up.

Advanced Setup > Advanced Setting > Scheduling



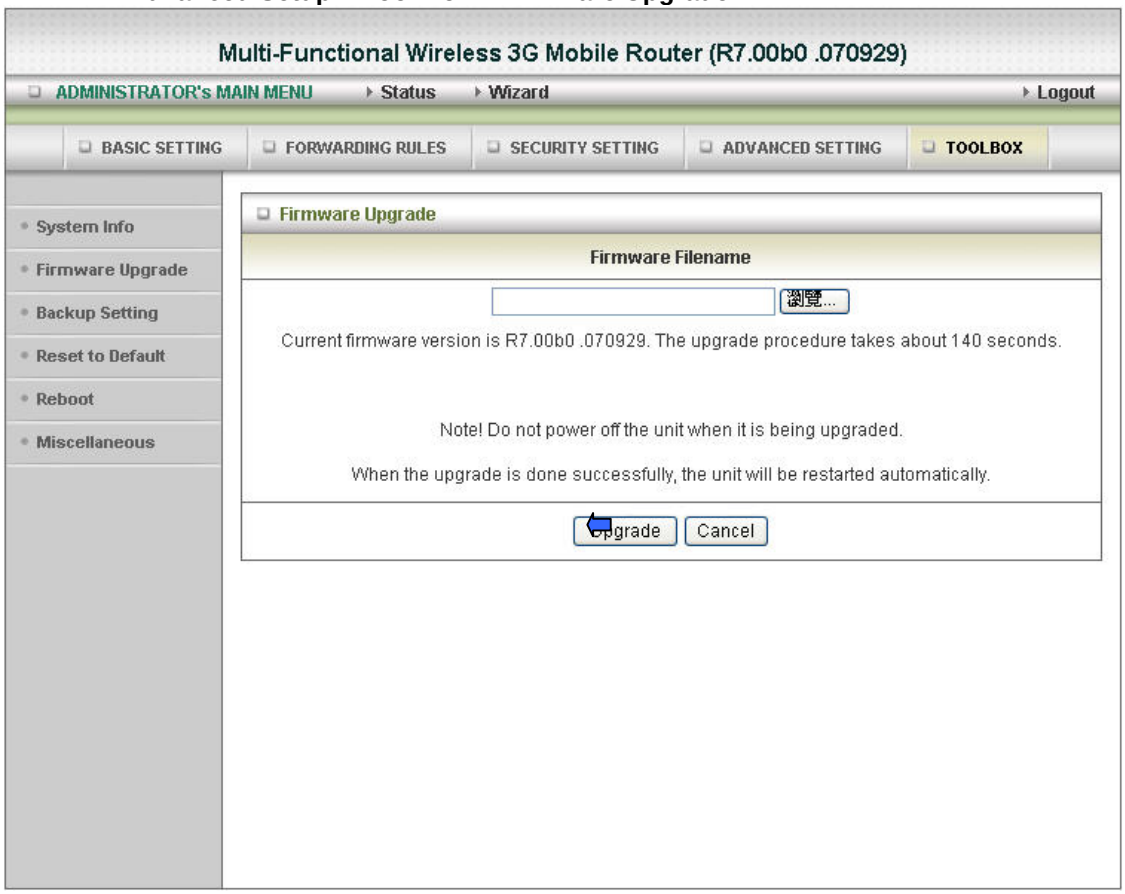
You can set the schedule time to decide which service will be turned on or off.

Advanced Setup > Tool Box > System Info



You can view the System log, Routing Table information in this page

Advanced Setup > Tool Box > Firmware Upgrade



You can upgrade firmware by clicking **Firmware "Upgrade"** button

Advanced Setup > Tool Box > Backup Setting

You can backup your settings by clicking the **Backup Setting** button and save it as a bin file. Once you want to restore these settings, please click **Firmware Upgrade** button and use the bin file you saved

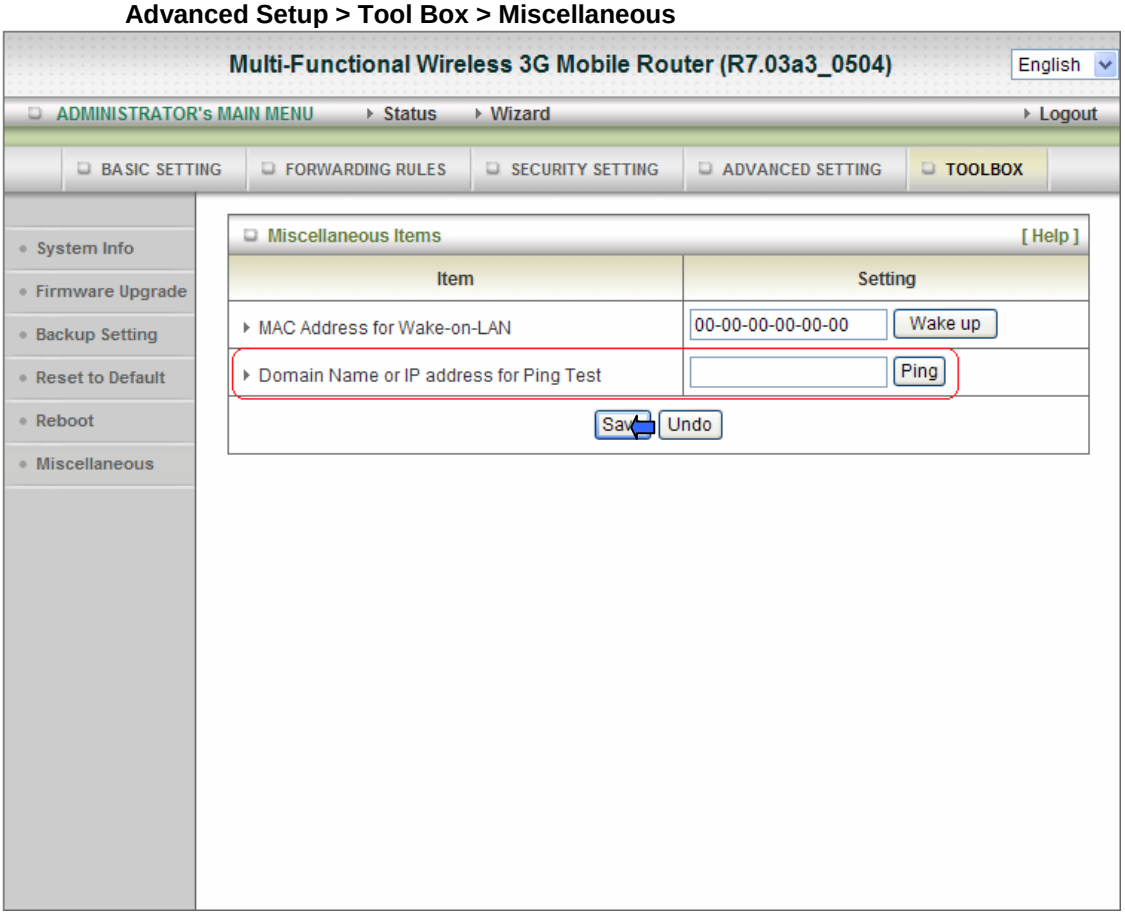
Advanced Setup > Tool Box > Reset to Default

You can also reset this product to factory default by clicking the **Reset to default** button

Advanced Setup > Tool Box > Reboot

You can also reboot this product by clicking the **Reboot** button

Advanced Setup > Tool Box > Miscellaneous



MAC Address for Wake-on-LAN

Wake-on-LAN is a technology that enables you to power up a networked device remotely. In order to enjoy this feature, the target device must be Wake-on-LAN enabled and you have to know the MAC address of this device, say 00-11-22-33-44-55. Clicking "Wake up" button will make the router to send the wake-up frame to the target device immediately.

Domain Name or IP address for Ping Test

You can key in URL or IP address, and then click the “Ping” button for test.

3. Troubleshooting

This section provides an overview of common issues, and possible solutions for the installation and operation of the Wireless WAN Mobile Broadband Router.

1. Unable to access the Configuration Menu when I use my computer to configure the router. Why?

Note: It is recommended that you use an Ethernet connection to configure the

Ensure that the **Ethernet LED** on the Wireless WAN Mobile Broadband Router is **ON**.
If the **LED** is **NOT ON**, check to see if the cable for the Ethernet connection is securely inserted.

> **Note:** Ensure that the **IP Address** is in the same range and subnet as the Wireless WAN Mobile Broadband Router. The IP Address of the Wireless WAN Mobile Broadband Router is 192.168.123.254. All the computers on the network must have a unique IP Address within the same range (e.g., 192.168.123.x). Any computers that have identical IP Addresses will not be visible on the network. All computers must also have the same subnet mask (e.g., 255.255.255.0).

Do a **Ping test** to make sure that the Wireless WAN Mobile Broadband Router is responding.

Go to **Start > Run**.

1:Type **cmd**.
2:Press **Enter.**
3:Type “**ping 192.168.123.254”.** A successful ping shows four replies.

> **Note:** If you have changed the **default** IP Address, ensure you ping the correct IP Address assigned to the Wireless WAN Mobile Broadband Router.

Ensure that your Ethernet Adapter is working properly, and that all network drivers are installed properly.

Note: Network adapter names will vary depending on your specific adapter. The installation steps listed below are applicable for all network adapters.

1. Go to **Start > My Computer > Properties**.
2. **Select** the **Hardware Tab**.
3. Click **Device Manager**.
4. Double-click on "**Network Adapters"**.
5. Right-click on **Wireless Cardbus Adapter**, or **your specific network adapter**.
6. Select **Properties** to ensure that all drivers are installed properly.
7. Look under **Device Status** to see if the device is working properly.
8. Click "**OK"**.

2**: Why my wireless client can NOT access the Internet?**

Note: Establish WiFi Connection. As long as you select either **WEP** or **WPA-PSK** encryption, ensure encryption settings match your WiFi settings. Please refer to your WiFi adapter documentation for additional information.

Ensure that the wireless client is associated and joined with the correct Access Point.
To check this connection, follow the steps below:

1. **Right-click** on the **Local Area Connection icon** in the taskbar.
2. Select **View Available Wireless Networks in Wireless Configure**. The **Connect to Wireless Network** screen appears. Ensure you have selected the correct available network.

Ensure the IP Address assigned to the wireless adapter is within the same subnet as the Access Point and gateway. The Wireless WAN Mobile Broadband Router has an IP Address of **192.168.123.254.** Wireless adapters must have an IP Address in the same range (e.g., 192.168.123.x). Although the subnet mask must be the same for all the computers on the network, no two devices may have the same IP Address. Therefore, each device must have a unique IP Address.

To check the **IP Address** assigned to the wireless adapter, follow the steps below:

1.Enter ipconfig /all in command mode
2.Enter ping 192.168.123.254.to check if you can access the Wireless WAN Mobile Broadband Router

3. Why does my wireless connection keep dropping?

You may try following steps to solve.

- Antenna Orientation.
  1: Try different antenna orientations for the Wireless WAN Mobile Broadband Router.
  2: Try to keep the antenna at least 6 inches away from the wall or other objects.
- Try changing the channel on the Wireless WAN Mobile Broadband Router, and your Access Point and Wireless adapter to a different channel to avoid interference.
- Keep your product away (at least 3-6 feet) from electrical devices that generate RF noise, like microwaves, monitors, electric motors, etc.

4. Why I am unable to achieve a wireless connection?

Note: An Ethernet connection is required to troubleshoot the Wireless WAN Mobile Broadband Router.

If you have enabled Encryption on the Wireless WAN Mobile Broadband Router, you must also enable encryption on all wireless clients in order to establish a wireless connection.

- For 802.11g, the encryption settings are: 64 or 128 bit. Ensure that the encryption bit level is the same for both the Wireless WAN Mobile Broadband Router, and your Wireless Client.
- Ensure that the SSID (Service Set Identifier) on the Wireless WAN Mobile Broadband Router and the Wireless Client are exactly the same.
  If they are not, your wireless connection will not be established.
- Move the Wireless WAN Mobile Broadband Router and the wireless client into the same room, and then test the wireless connection.
- Disable all security settings such as **WEP**, and **MAC Address Control**.
- Turn off the Wireless WAN Mobile Broadband Router and the client.
  Turn the Wireless WAN Mobile Broadband Router back on again, and then turn on the client.
- Ensure that all devices are set to **Infrastructure** mode.
- Ensure that the LED indicators are indicating normal activity. If not, ensure that the AC power and Ethernet cables are firmly connected.
- Ensure that the IP Address, subnet mask, gateway and DNS settings are correctly entered for the network.
- If you are using 2.4GHz cordless phones, X-10 equipment, or other home security systems, ceiling fans, or lights, your wireless connection may degrade dramatically, or drop altogether.

To avoid interference, change the Channel on the Wireless WAN Mobile Broadband Router, and all devices in your network.

- Keep your product at least 3-6 feet away from electrical devices that generate RF noise.
  Examples include: microwaves, monitors, electric motors, and so forth.

5. I just do not remember my encryption key. What should I do?

- If you forgot your encryption key, the WiFi card will be unable to establish a proper connection.
  If an encryption key setting has been set for the Wireless WAN Mobile Broadband Router, it must also be set for the WiFi card that will connect to the Wireless WAN Mobile Broadband Router.
  To reset the encryption key(s), login to the Wireless WAN Mobile Broadband Router using a wired connection. (Please refer to “Basic > Wireless (Security–No Encryption)” on page 10, for additional information).

7. How do I reset my Wireless WAN Mobile Broadband Router to its factory default settings?

If other troubleshooting methods have failed, you may choose to **Reset** the Wireless WAN Mobile Broadband Router to its factory default settings.
To hard-reset the Wireless WAN Mobile Broadband Router its factory **default** settings, follow the steps listed below:

1. Ensure the Wireless WAN Mobile Broadband Router is powered on
2. Locate the **Reset** button on the back of the Wireless WAN Mobile Broadband Router.
3. Use a paper clip to press the **Reset** button.
4. Hold for 10 seconds and then release.
5. After the Wireless WAN Mobile Broadband Router reboots, it is reset to the factory **default** settings.

Note: Please note that this process will take a few minutes.

8. What is VPN?

• VPN stands for “Virtual Private Networking.” VPNs create a "tunnel" through an existing Internet connection using PPTP (Point-to-Point Tunneling Protocol) or IPSec (IP Security) protocols with various encryption schemes including Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) .
• This feature allows you to use your existing Internet connection to connect to a remote site with added security. If your VPN connection is not functional, verify that your VPN dial-up configuration is correct.

Note: This information should be provided to you from your VPN provider.

Pressing the Reset Button restores to its original factory **default** settings.

9. What can I do if my Ethernet cable does not work properly?

• First, ensure that there is a solid cable connection between the Ethernet port on the Router, and your NIC (Network Interface Card).
• Second, ensure that the settings on your NIC adapter are “Enabled,” and set to accept an IP address from the DHCP.
• If settings appear to be correct, ensure that you are *not* using a crossover Ethernet cable.

Although the Wireless WAN Mobile Broadband Router is MDI/MDIX compatible, not all NICs are. Therefore, it is recommended that you use a patch cable when possible.

4. Technical Specifications

3G Access	1*PC card Type II Slot USB port
Standards	IEEE 802.11b/g
Standard	IEEE 802.11b\g Turbo
Data Rate	54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, 1 Mbps per channel, Auto Fall-Back
Frequency	2.412 – 2.462 GHz, DSSS / OFDM modulation
Range Coverage	Tx/Rx power 18dbm/Per Cell indoors approx. 35-100 meters; outdoors up to 100-300 meters
# of Channels	1-11 for N. America (FCC);1-11 for Canada (DOC) 1-13 Europe (Except Spain and France) (ETSI) 1-14 Japan (TELEC);
Security	64-bit and 128-bit WEP Encryption; WPA encryption
Antenna	Dipole Antenna 2dBi
Firewall	IP Filtering NAT (Network Address Translation) with VPN Pass through MAC Filtering
Supported WAN type	3G,Static IP, Dynamic IP, PPPoE,PPTP,L2TP
Connection Scheme	Connect-on-demand, Auto-Disconnect
NAT function	Class C ;One-to-Many; Max 253 Users; Virtual Server; DMZ Host
VPN	PPTP, L2TP and IPSec Pass Through
Config.& Management	Web-Based IE, Nevigator browser and SNMP
	DHCP Server and Client
Working Environment	Temperature: 0~40^{o}C, Humidity 10%~90% non-condensing
OS supported	Windows 95/98/ME/NT/2000/XP; Linux
Power	Switching 5V 3.0A

FCC Caution:

1.The 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.

2.This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

3. Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user authority to operate the equipment.

IMPORTANT NOTE:
FCC 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.

FCC statement in User's Manual (for class B)

"Federal Communications Commission (FCC) Statement

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.**