



## **3G Wireless Broadband Router**

# User Guide



### **Copyright**

The content of this publication may not be reproduced in any part or as a whole, stored, transcribed in an information retrieval system, translated into any language, or transmitted in any form or by any means, mechanical, magnetic, electronic, optical, photocopying, manual, or otherwise, without prior written permission.

### **Trademarks**

All products, company, brand names are trademarks or registered trademarks of their respective companies. They are used for identification purposes only. Specifications are subject to be changed without prior notice.

### **FCC Interference 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 radio interference in a commercial environment. This equipment can generate, use and radiate radio frequency energy and, if not installed and used in accordance with the instructions in this manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his own expense, will be required to take whatever measures are necessary to correct the interference.

### **CE Declaration of Conformity**

This equipment complies with the requirements relating to electromagnetic compatibility, EN 55022/A1 Class B.



## Table of Contents

Package Contents.....	5
System Requirements .....	5
WiFi Requirements.....	5
Introduction.....	6
Features .....	6
Hardware Overview .....	7
Configuration .....	8
Installation.....	8
Hardware Setup.....	8
WiFi Connection.....	10
Web-based Configuration .....	10
Setup Wizard.....	11
Advanced Setup .....	16
Technical Support.....	34
Technical Specifications .....	34



## Package Contents

Important: Check the contents of the box first!

The Cyfre 3G Wireless Broadband Router package should contain the items listed below. If any of the items are missing, please contact your reseller.

- (1) **Cyfre 3G Wireless Broadband Router**
- (1) **Quick Installation Guide**
- (1) **CD-ROM**
- (1) **RJ-45 Ethernet Cable**
- (1) **5V 3.0A Power Adapter**
- (1) **Desk Cradle**

**Caution:** Using a power supply with a different voltage rating other than the one included with the Cyfre 3G Wireless Broadband Router will cause damage and void the warranty for this product.

## System Requirements

- Compatible 16-bit or 32-bit PCM/CIA or USB 3G modem card *with activated service*.  
**NOTE:** Subject to terms available from your carrier.
- Computer with Windows 2000, XP, Vista, Macintosh, or Linux-based operating systems with an installed Ethernet adapter.
- Internet Explorer Version 6.0 or Netscape Navigator™ Version 7.0 and above (for accessing web-based configuration settings).

## WiFi Requirements

- IEEE 802.11b/g adapter.



## Introduction

The Cyfre 3G Wireless Broadband Router is a high-performance tool that supports wireless networking at home, work, or in a public place. Supporting 16-bit and 32-bit Type II PCM/CIA cards, USB 2.0 mobile broadband cards, and Express Cards with an universal caddy, the Cyfre 3G Wireless Broadband Router supports WCDMA, EVDO and HSDPA technologies. The Cyfre 3G Wireless Broadband Router supports wireless data transfers up to 54 Mbps, and wired data transfers up to 100 Mbps. This product is also compatible with industry-standard security features such as SPI firewall, WEP/WPA security settings, and MAC address control.

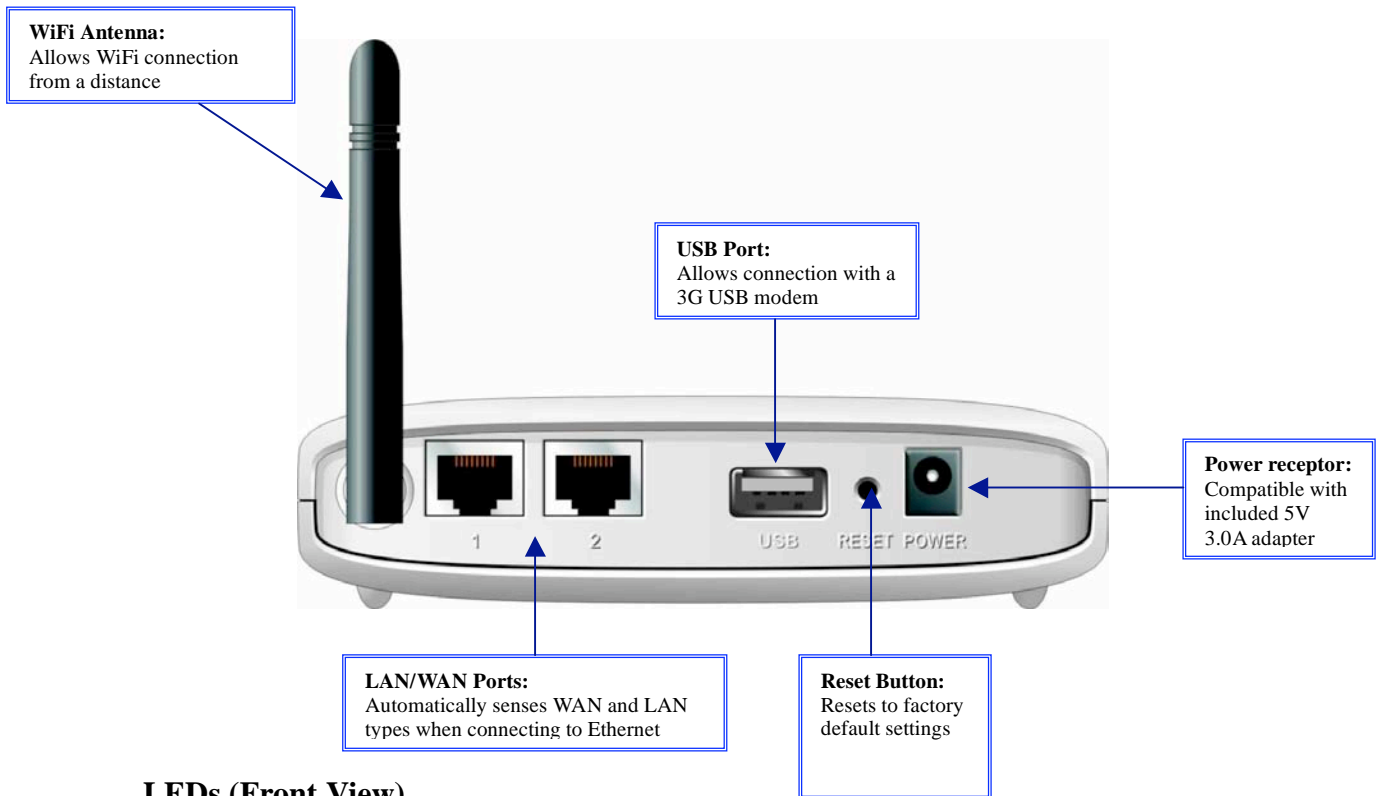
### Features

- Quick and easy setup allows you to go where wires cannot: outside the home or office.
- Automatic connection failover to 3G connection if Ethernet WAN connection fails.
- Fully compatible with the 802.11g IEEE standard to provide a wireless data transfer rate of up to 54Mbps.
- Backwards compatible with the 802.11b IEEE standard to provide a wireless data rate of up to 11Mbps.
- Operates in the 2.4GHz frequency range.
- Advanced Firewall features.
- Supports NAT with VPN pass-through, as well as the following security features:
  - \* MAC Filtering
  - \* IP Filtering
  - \* Port Scheduling
- DHCP server enables all networked computers to automatically receive IP addresses.
- Access Control for managing users on the network
- Web-based configuration pages for easy setup and management.
- User-friendly configuration and diagnostic utilities.
- Supports special applications that require multiple connections.
- Equipped with 2 10/100 Ethernet ports for LAN and WAN access, a Type II PC card (16- and 32-Bit) Slot, and a USB port for 3G network connections. ExpressCards with a universal caddy are also compatible.
- Connects multiple computers to the internet via a broadband EVDO or HSDPA network connection. Please consult your service provider for more detailed information on wireless network standards.

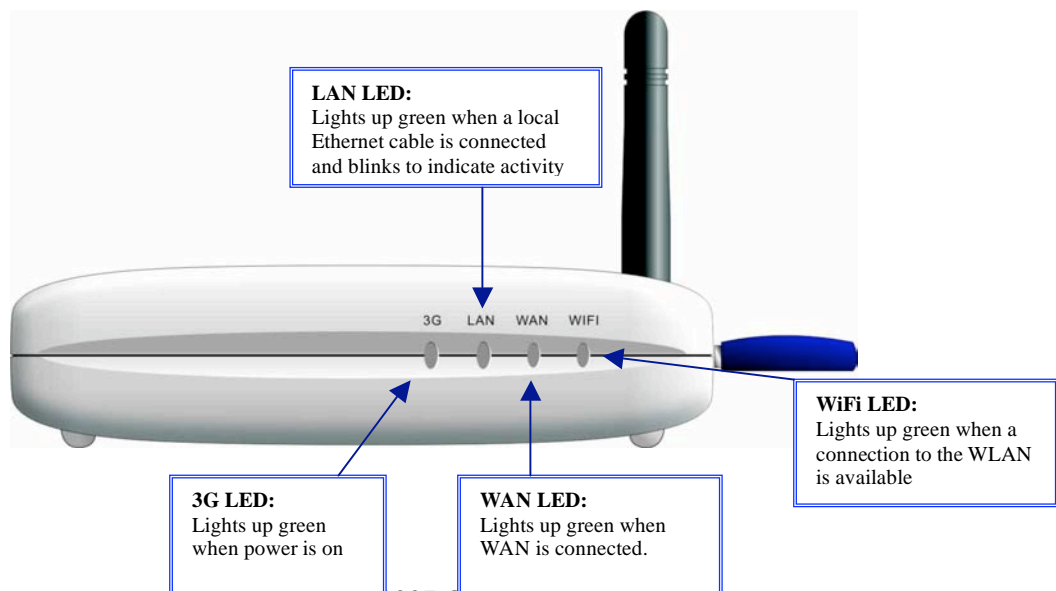


## Hardware Overview

### Receptors and Ports (Rear View)



### LEDs (Front View)





## Configuration

### Installation

The Cyfre 3G Wireless Broadband Router allows you access your network using a wireless connection from virtually anywhere within its operating range. Please note that location placement of the router could affect the wireless signal and range limits.

Typical ranges also vary depending on the types of materials and background RF (radio frequency) noise present in your networking environment.

To maximize your wireless range, please follow these guidelines:

1. Choose the right location in your environment for the Cyfre 3G Wireless Broadband Router. The WLAN transmitters are basically radios; their signals radiate out from the antenna, and degrade as they go through walls, floors, and obstacles like tubs full of water (almost impenetrable), stone, or concrete. So for best reception, place your gateway centrally to the rooms in which you expect to use WLAN the most. Each wall or ceiling can reduce the Cyfre 3G Wireless Broadband Router's range by as much as 90 feet (27 meters).  
**NOTE:** The same considerations apply to your 3G broadband connection.
2. Keep your product away from electrical devices (such as microwaves, air conditioners, refrigeration and televisions) that emit large quantities of RFI (Radio Frequency Interference).

### Hardware Setup

***NOTE: DO NOT connect the Cyfre 3G Wireless Broadband Router to power before following the installation steps below!***

1. Attach the antenna.
  - a. Remove the antenna from its plastic wrapper.
  - b. Screw the antenna in a clockwise direction to the back panel of the unit.
  - c. Once secured, position the antenna upward at its connecting joint. This will ensure optimal reception.





**NOTE:** If you are using the provided cradle, position antenna perpendicular to the router. This will reduce signal interference between the WLAN and 3G connections.

- 2(i). PCM/CIA, Express Card with a universal caddy, or USB connection:
- a. Insert an activated Type II PCM/CIA card or Express Card with adapter into the PCM/CIA card slot.
  - b. Alternatively, insert an activated USB modem into the USB slot.

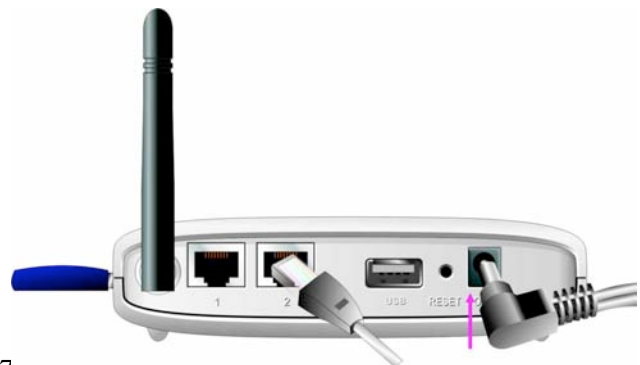


- 2(ii). Ethernet connection:

- a. Insert one end of an Ethernet cable into the LAN Port on the back panel of the router. Insert the other end into an available Ethernet port of the network adapter in the computer that will be used to configure the unit.



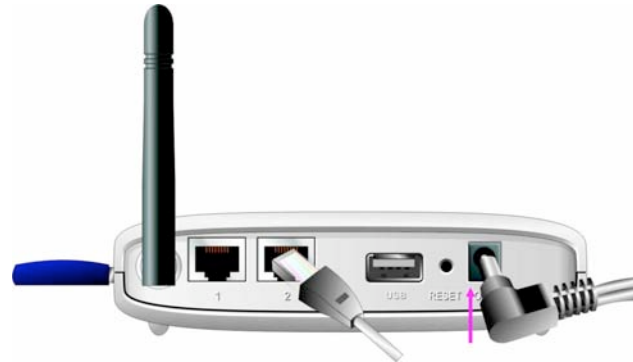
**NOTE:** The Cyfre 3G Wireless Broadband Router LAN Port is "Auto-MDI/MDIX." This provides patch Ethernet cable LAN Port access.





### 3. Power connection

- a. Connect the power adapter to the receptor on the back panel of the router. Plug the other end of the power adapter into a wall outlet or power strip.
- b. The 3G LED will turn ON, indicating that the unit is powered on.
- c. The other LEDs on the front of the router will flash ON and OFF as it performs initialization and Internet connection processes. This will take a few minutes.
- d. When complete, all four LEDs will light up green.



## WiFi Connection

If you are connecting wirelessly to the Cyfre 3G Wireless Broadband Router, you must ensure that the WEP or WPA-PSK encryption settings on the connecting PC are the same as those on the router. By default, the router broadcasts an unsecured network. It is recommended for security reasons that the encryption settings on the router be configured immediately upon installation. Please refer to your WiFi adapter documentation for additional information.

## Web-based Configuration

The Cyfre 3G Wireless Broadband Router obtains and assigns IP address information automatically. However, customized configuration settings can be established through its web-based configuration menus.

To access these menus:

1. Open a web-browser.
2. Enter the IP address of the Cyfre 3G Wireless Broadband Router:

<http://192.168.123.254>



**NOTE:** If you have changed the router's **default** IP address, enter that address instead of the one above.



3. Type “**admin**” in the **System Password** field.  
If you have changed the password, enter the new one in this field.
4. Click “**Login**” button.

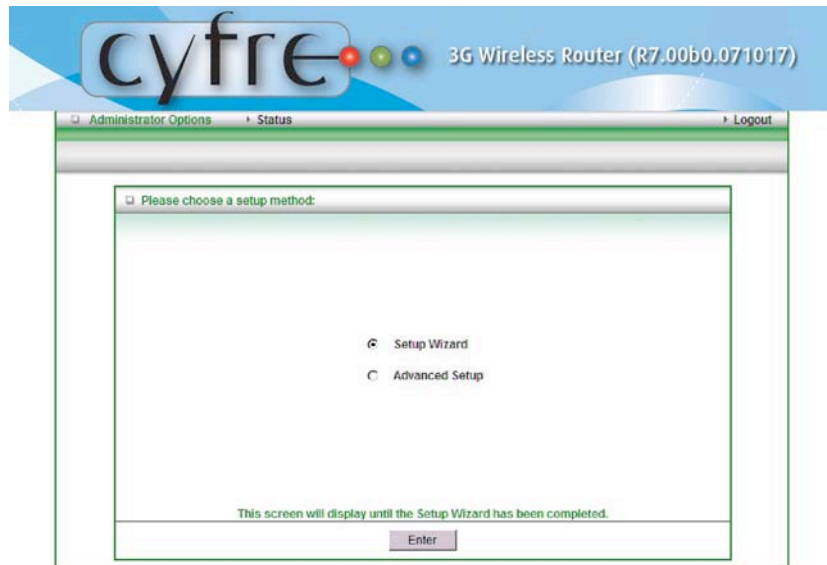


### Setup Wizard

Choose the **Setup Wizard** option to quickly and easily configure the router’s basic settings.

For access to the router’s more advanced settings, choose **Advanced Setup** and refer to the advanced setup section of this guide for more information.

Click **Enter** to continue.





The Setup Wizard configures the following:

- Login Password**
- WAN Settings**
- Wireless Settings**

Click **Next** to continue.

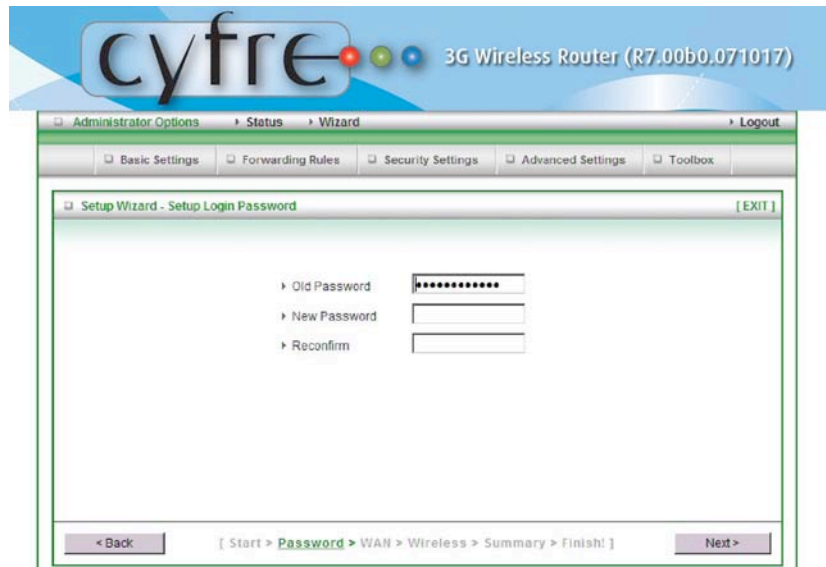


### Step 1: Setup Login Password

It is highly recommended that you change the router's administration password immediately upon first configuring.

1. Enter your previous password in the **Old Password** field. If this is your first time accessing these menus, the default password is "admin".
2. Enter a new password in the **New Password** field.
3. Re-enter the new password in the **Reconfirm** field.

Click **Next** to continue.





## Step 2: Select WAN Type

Select the type of Wide Area Network (WAN) the router will use to connect to the Internet.

**Note: If you are using your cellular carrier's internet service, select 3G Connection.**  
Click Next to continue.

cyfre 3G Wireless Router (R7.00b0.071017)

Administrator Options > Status > Wizard > Logout

Basic Settings > Forwarding Rules > Security Settings > Advanced Settings > Toolbox

Setup Wizard - Select WAN Type [EXIT]

- Static IP Address (ISP assigns a static IP address)
- Dynamic IP Address (Obtain an IP address from ISP automatically)
- Dynamic IP Address w/Road Runner Session Management (i.e. Telstra BigPond)
- PPPoE Connection (PPP over Ethernet)
- PPTP Connection
- L2TP Connection
- 3G Connection

< Back [ Start > Password > **WAN** > Wireless > Summary > Finish! ] Next >

## Step 3(i): WAN (Dynamic IP Address)

The Local Area Network (LAN) is the internal network associated with the Cyfre 3G Wireless Broadband Router.

1. The **LAN IP Address** is the address of the web-based configuration menu. The default address is <http://192.168.123.254>. The LAN IP address can be changed here if necessary. There are 253 alternate addresses available: 192.168.123.1 through 192.168.123.253. The LAN IP address is private and cannot be seen from outside the router's network.

2. The **Host Name** is optional. It can be changed here.

cyfre 3G Wireless Router (R7.00b0.071017)

Administrator Options > Status > Wizard > Logout

Basic Settings > Forwarding Rules > Security Settings > Advanced Settings > Toolbox

Setup Wizard - WAN Settings - Dynamic IP Address [EXIT]

LAN IP Address: 192.168.123.254

Host Name: ROUTER (optional)

WAN's MAC Address: 00-50-18-00-00-FE [Save] [Clone MAC]

< Back [ Start > Password > **WAN** > Wireless > Summary > Finish! ] Next >



3. The **WAN's MAC Address** is the physical address of the router. Click the **Clone MAC** button to copy your computer's settings to this field.

Click **Next** to continue.

### Step 3(ii): WAN (3G)

3G PCM/CIA cards and USB modems are a widely used method of connecting to the Internet. The Dialed Number “#777” is a common default for many WCDMA service providers.

The **APN, Pin Code, Dialed Number, Username, and Password** can all be changed here if your service provider requires different settings. For more information, refer to the end of this User Guide, or call your service provider.

cyfre 3G Wireless Router (R7.00b0.071017)

Administrator Options | Status | Wizard | Logout

Basic Settings | Forwarding Rules | Security Settings | Advanced Settings | Toolbox

Setup Wizard - WAN Settings - 3G [EXIT]

Note: Your service provider's settings may differ from the defaults below.

LAN IP Address	192.168.123.254
APN	
Pin Code	
Dialed Number	#777
Username	
Password	

< Back [ Start > Password > WAN > Wireless > Summary > Finish! ] Next >

### Step 4: Wireless Settings

1. The **Wireless Radio** can be disabled by clicking the appropriate radio button.
2. The **Network ID, or Service Set Identifier (SSID)**, is the broadcasted name of your wireless network seen by other users. The default name is Cyfre, and it can be changed to a new one up to 32 characters in length.
3. The **Channel** of this router, which is set to 11 by default, can be changed to avoid conflicts with other devices, or to otherwise customize the wireless network.
4. Click **Next** to continue.

cyfre 3G Wireless Router (R7.00b0.071017)

Administrator Options | Status | Wizard | Logout

Basic Settings | Forwarding Rules | Security Settings | Advanced Settings | Toolbox

Setup Wizard - Wireless Settings [EXIT]

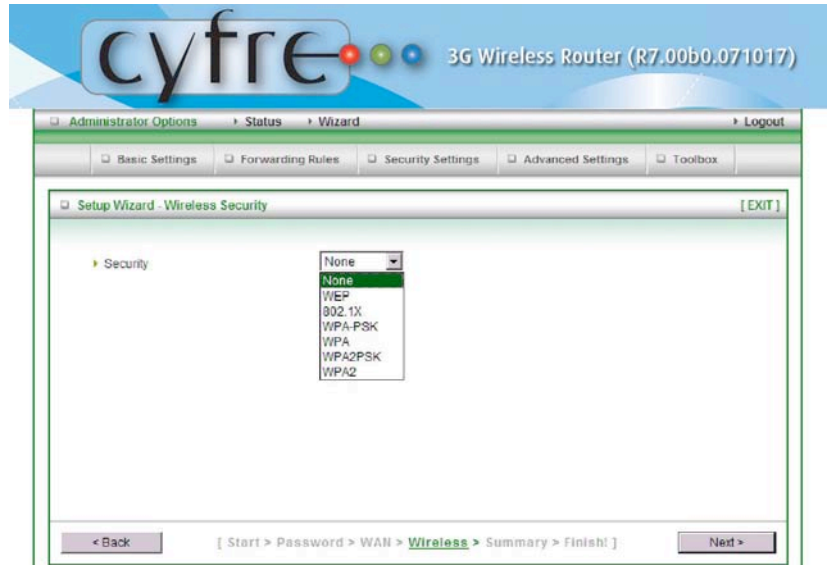
Wireless Radio	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Network ID (SSID)	Cyfre
Channel	11

< Back [ Start > Password > WAN > Wireless > Summary > Finish! ] Next >



### Step 5: Wireless Security

The security settings listed in this menu correspond to different types of encryption. For more information, please refer to **Advanced Settings -> Basic Setup -> Wireless**.



### Step 6: Summary

The settings you just entered will appear in summary on this page. The checkbox at the bottom allows you to test these settings before applying them.

Click the **Apply Settings** button.





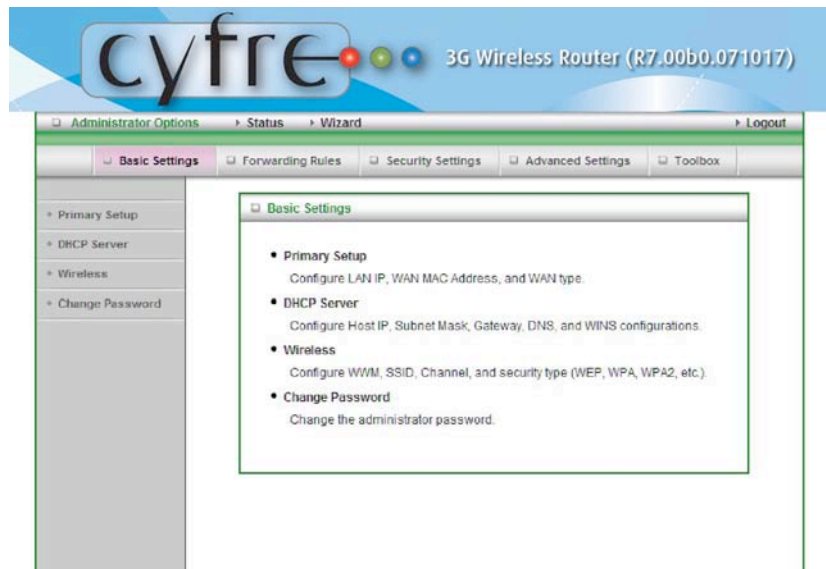
### Step 7: Apply settings

Once setup is complete, click the **Finish** button to return to the Status page. Advanced Setup

#### Basic Settings:

- Primary Setup
- DHCP Server
- Wireless
- Change Password

**Note:** Throughout all of the web-based Advanced Setup pages, click the **Save** button to save changes or click the **Undo** button to cancel any changes.



### Basic Settings > Primary Setup

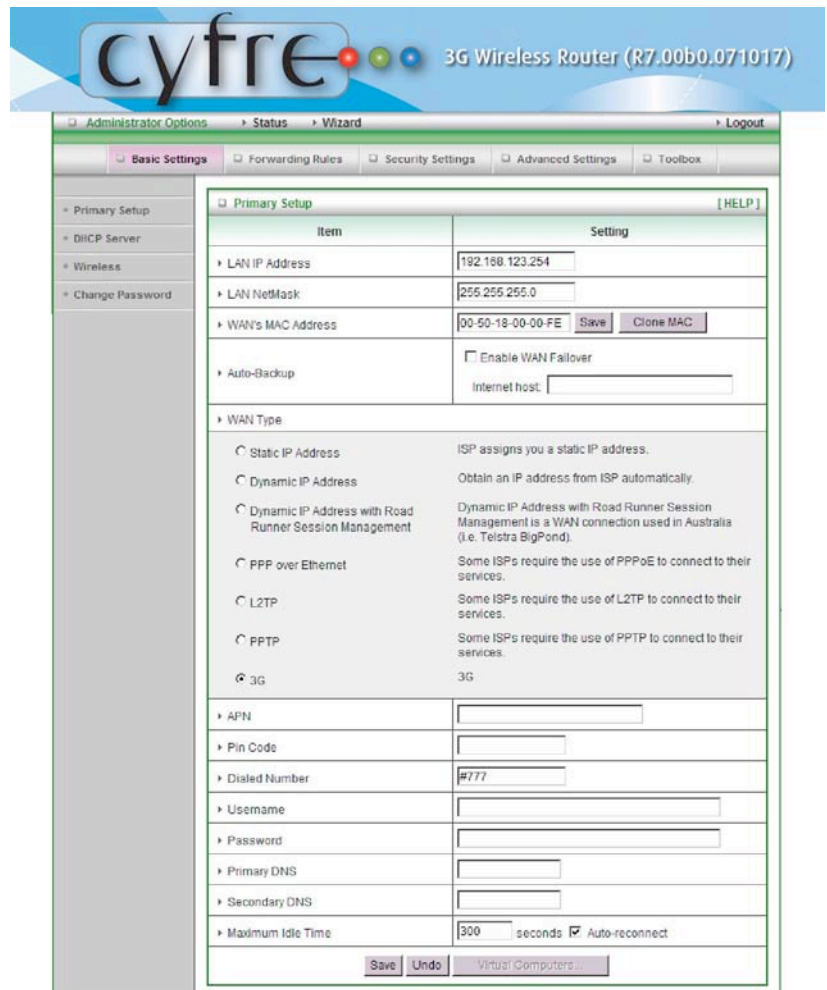
Select the WAN connection type the router will use to connect to the Internet.

Static IP Address and Dynamic IP Address settings are often used with DSL or Cable connections, while 3G Settings are used with 3G broadband cards or USB modems.

For all of these options, it is recommended that you contact your service provider for the proper settings.

The commonly used 3G **Dialed Number** “#777” is in the router’s settings by default. Additional settings, such as APN, Username, and Password, may be needed for certain service providers.

Refer to the Troubleshooting section at the end of this User Guide for a list of some other common service providers and their settings.





### Basic Settings > DHCP Server

When the DHCP Server is enabled, the Lease Time, IP Pool Starting Address, IP Pool Ending Address, and Domain Name can be specified. By default, DHCP is enabled.

**Lease Time-** The length of time the DHCP Server allots for any given client.

**IP Pool Address Range-** The range of IP addresses that the DHCP will issue from. Starting and ending addresses must be defined.

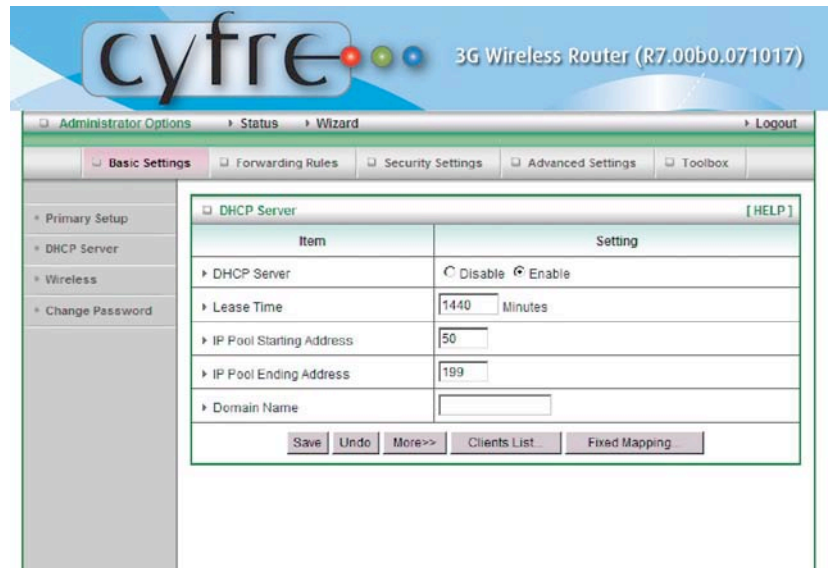
**Domain Name-** An optional setting that is passed to the client.

**More>>**

**Primary/Secondary DNS-** Specify a Domain Name Server (DNS).

**Primary /Secondary WINS-** Specify a Windows Internet Name Service.

**Gateway-** Set the IP address of an alternate Gateway. This function enables you to assign another gateway to your PC when DHCP server offers an IP address to your PC.



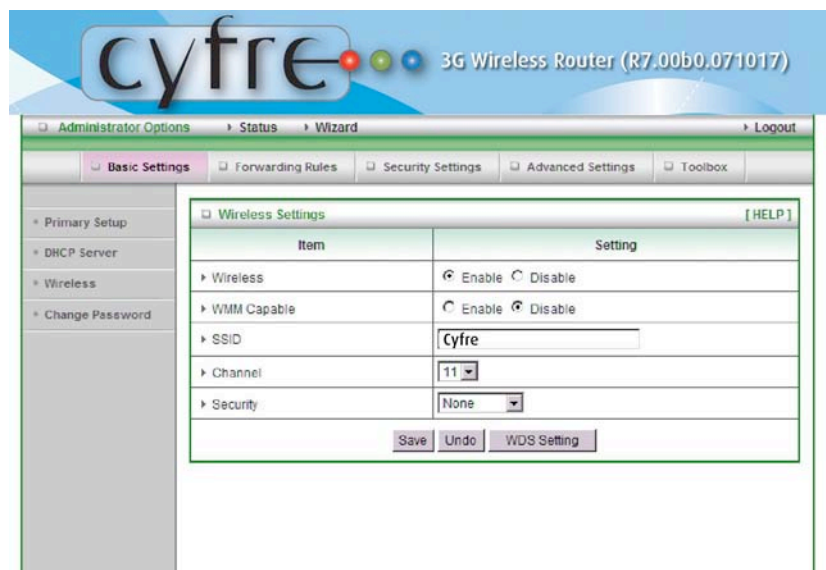
### Basic Settings > Wireless

**Wireless-** Choose **Enable** to broadcast a wireless network from your router.

**WMM Capable-** Choose **Enable** to apply WiFi MultiMedia certification (a type of Quality of Service) to this wireless connection.

**SSID-** Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The SSID's default setting is **Cyfre**. The SSID can be changed to establish a new wireless network. SSID names may contain up to 32 ASCII characters.

**Channel-** **Channel 11** is the **default**. Devices on the network must share the same channel. (Note: Wireless adapters automatically scan and match the wireless settings. You may also select the channel you wish to use).





**Security-** You may select from three levels of encryption to secure your wireless network:

**No Encryption, WEP.802.1x, WPA-PSK, WPA, WPA2-PSK, or WPA2.**

**Security- No Encryption** is the **default** (as shown in the screen above).

**WEP Security:** Select the data privacy algorithm you want. Enabling the security can protect your data while it is transferred from one station to another. The standardized IEEE 802.11 WEP (128 or 64-bit) is used here.

**WEP Key 1, 2, 3 or 4:** When you enable the 128 or 64 bit WEP key security, please select one WEP key to be used and input 26 or 10 hexadecimal (0, 1, 2...8, 9, A, B...F) digits.

**802.1X:** Used to switch the function of the 802.1X. When another 802.1X device is enabled

**WPA-PSK/WPA-PSK2 :** Encryption options for WPA-PSK-TKIP and WPA-PSK2-ADE . Enter a password in the WPA-PSK /WPA-PSK2 field between 8 and 63 characters long for ASCII.64 characters (0~9,a~f) for HEX.

**WPA/WPA2 :**The users have to get a access form RADIUS server by performing user authentication. Enter the IP address of Radius server and RADIUS Shared Key.

Click on **Save** to store your settings.

### Advanced Setup > Basic Settings > Change Password

You can change the router's password here. It is highly recommended that you change the router's administration password immediately upon first configuring.

1. Enter your previous password in the **Old Password** field. If this is your first time accessing these menus, the default password is "**admin**".
2. Enter a new password in the **New Password** field.
3. Re-enter the new password in the **Reconfirm** field.

Click **Next** to continue.

Item	Setting
Old Password	*****
New Password	
Reconfirm	

Save Undo



**Advanced Setup > Forwarding Rules > Virtual Server**

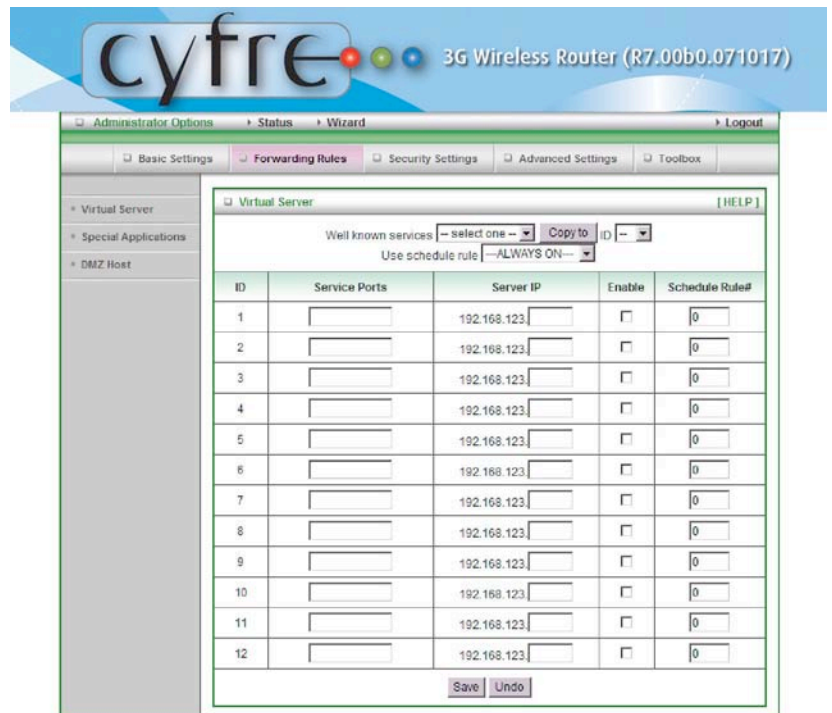
This product's NAT firewall filters out unrecognized packets to protect your Intranet. All hosts behind the device are invisible to the outside world. It is possible to make select hosts accessible by enabling the Virtual Server Mapping.

A virtual server is defined as a **Service Port**, and all requests to this port will be redirected to the computer specified by the **Server IP**. **Virtual Server** can work with **Scheduling Rules**, and give user more flexibility on Access control. For Detail, please refer to **Scheduling Rule**.

For example, if you have an FTP server (port 21) at 192.168.123.1, a Web server (port 80) at 192.168.123.2, and a VPN server at 192.168.123.6, then you need to specify the following virtual server mapping table:

Service Port	Server IP	Enable
21	192.168.123.1	V
80	192.168.123.2	V
1723	192.168.123.6	V

Click **Save** to store configuration changes or **Undo** cancel





**Advanced Setup > Forwarding Rules > Special AP**

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 device. If the mechanism of Special Applications fails to make an application work, try setting your computer as the **DMZ** host instead.

**Trigger:** the outbound port number issued by the application.

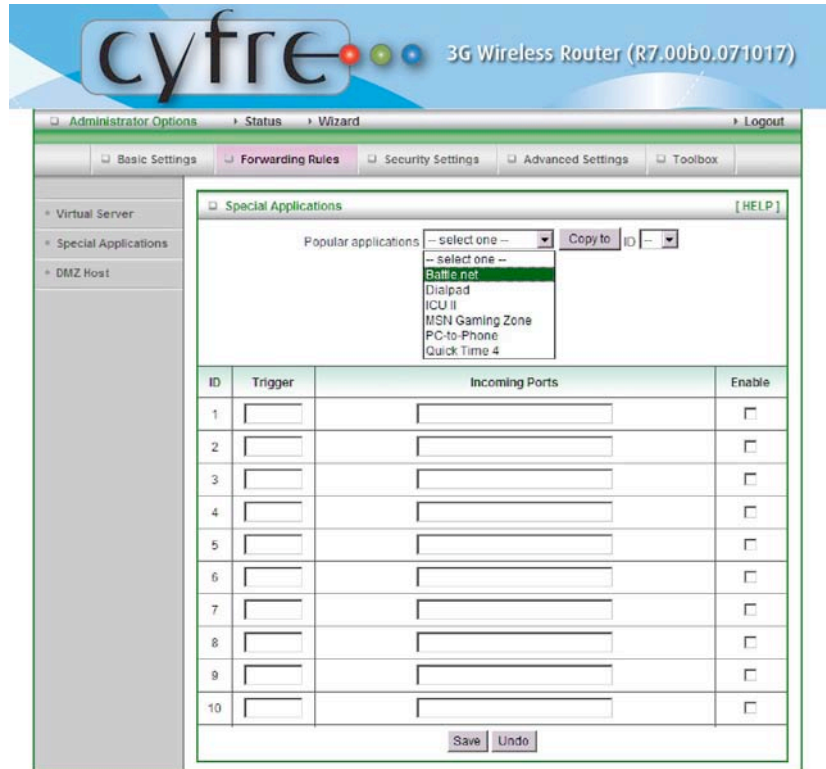
**Incoming Ports:** when the trigger packet is detected, the inbound packets sent to the specified port numbers are allowed to pass through the firewall.

This device provides some predefined settings.

Pull down the application from the menu and click **Copy to** for the defined settings to take place

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

Click on **Save** to store configuration changes or **Undo** cancel



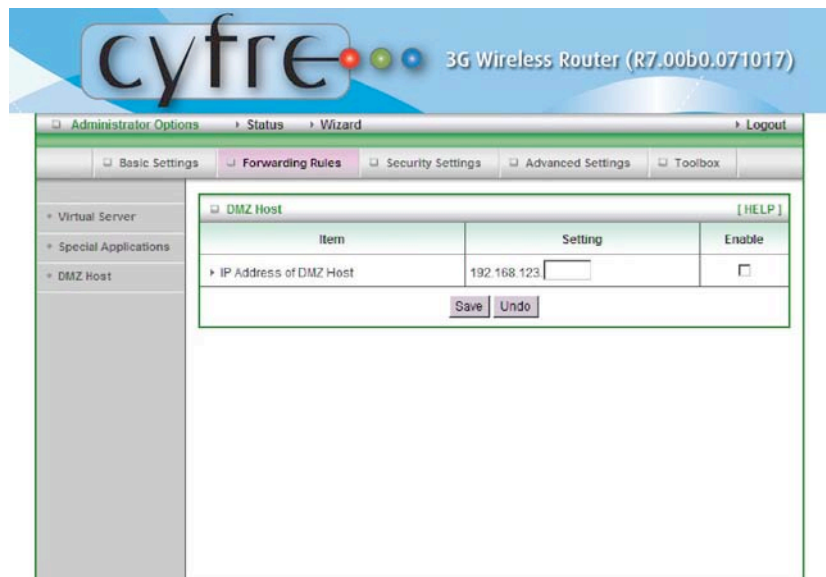
**Advanced Setup > Forwarding Rules > Miscellaneous**

**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.

Click on **Save** to store configuration changes or **Undo** cancel

**NOTE:** This feature should be enabled only when needed or in use.





**Advanced Setup > Security Settings > Packet Filters**

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

1. Allow all to pass except those that match the specified rules
2. Deny all to pass except those that 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 Schedule Rule #

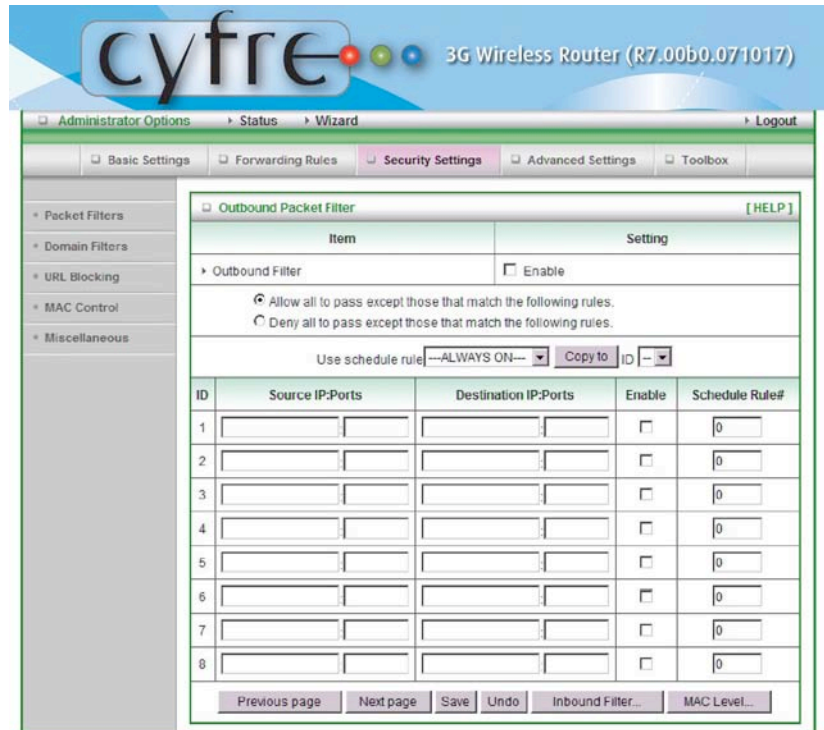
For source or destination IP address, you can define a single IP address (4.3.2.1) or a range of IP addresses (4.3.2.1-4.3.2.254). A blank field implies all IP addresses.

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**, providing users with more flexibility on access control. For details, please refer to **Scheduling Rules**. Each rule can be enabled or disabled individually.

Click **Save** to store configuration changes or **Undo** cancel

**Inbound Filter:** To enable Inbound Packet Filter check the box next to Enable in the Inbound Packet Filter field

Click on **Save** to store configuration changes or **Undo** cancel





**Advanced Setup > Security Settings > Domain Filters**

Domain filters allow users to prevent users under this device from accessing specific URLs.

**Domain Filters 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**

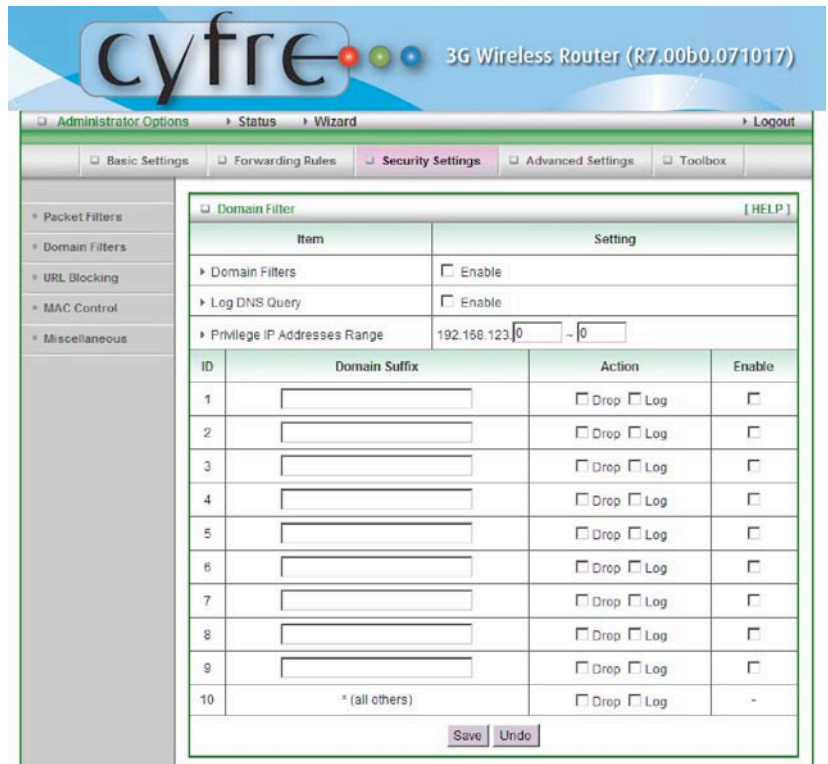
When someone is accessing the URL matches the specified domain-suffix, what kind of action you want carried out.

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

**Enable**

Check to enable each rule.

Click **Save** to store configuration changes or **Undo** cancel



**Advanced Setup > Security Settings > 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 filters require the 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 a specific website, while URL Blocking can block hundreds of websites by 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 "pancake" to block all websites if their URLs contain the pre-defined word "pancake".

**Enable** Check to enable each rule.

Click **Save** to store configuration changes or **Undo** cancel





**Advanced Setup > Security Settings > 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 MAC Address Control. All of the settings in this page will take effect only when **Enable** is checked.

**Connection control.** Check **Connection control** to control 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 enable or disable the clients, whose MAC addresses are not in the **Control table** to connect to this device.

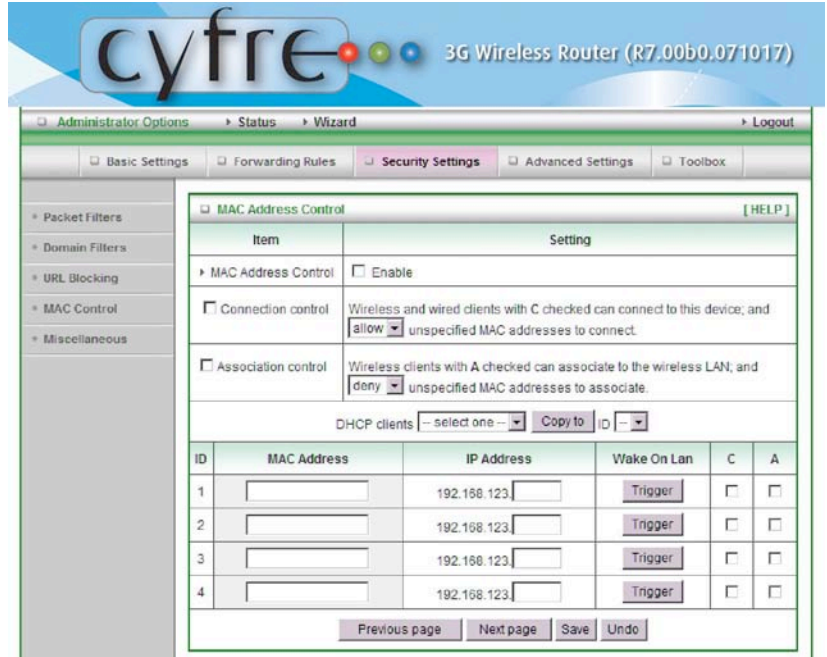
**Association control.** Check **Association control** to enable the controlling of which wireless client can associate to the wireless LAN. If a client is

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

Click on **Save** to store configuration changes or **Undo** cancel

Click on **Next Page** to go down or **Previous page** back to last page



**Advanced Setup > Security Settings > Miscellaneous**

**Remote Administrator Host/Port**

By default, only Intranet users can browse the built-in web pages to perform administrative tasks on the router. 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.



**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:** Choose enable or disable the UPnP feature

Click on **Save** to store configuration changes or **Undo** to cancel



**Advanced Setup > Advanced Settings > System Log**

This page supports two methods to export system logs to specific destination by means of syslog (UDP) and SMTP(TCP).

**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).

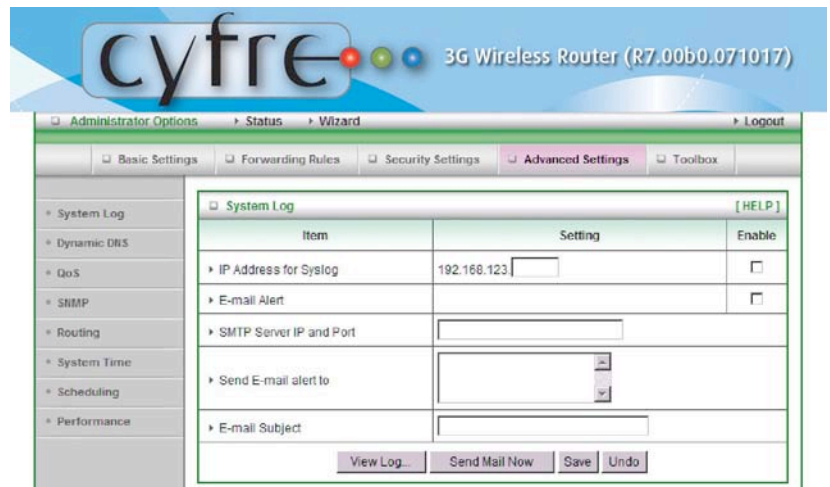
**SMTP Server IP and Port.** Enter the SMTP server IP and port with a ':'. The default port value is 25.

**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 email addresses.

**E-mail Subject.** The subject of email alert, this setting is optional.

Click on **Save** to store configuration changes or **Undo** to cancel



**Advanced Setup > Advanced Settings > Dynamic DNS**

To host your server on a changing IP address, you have to use a dynamic domain name service (DDNS). Dynamic DNS maps the name of your host to your current IP address, provided by your Internet service provider.

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

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

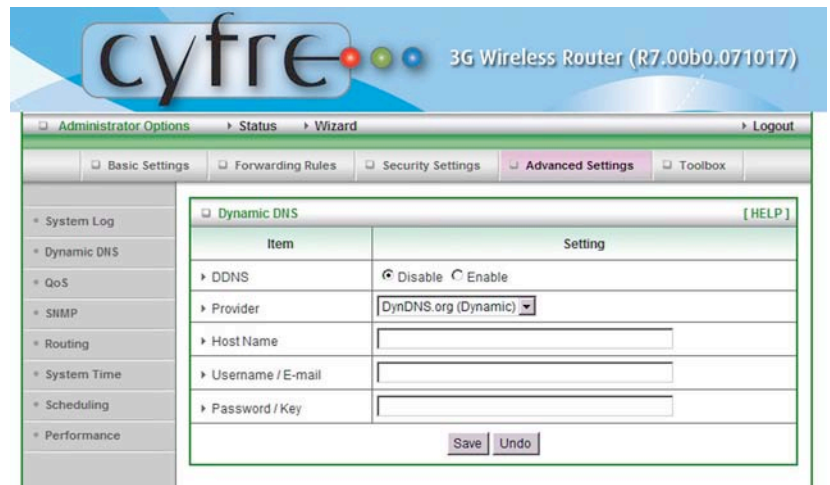
Next enter the appropriate information about your Dynamic DNS Server.

You have to define:

- Provider
- Host Name
- Username/E-mail
- Password/Key

**NOTE:** This information is established when you register an account on a Dynamic DNS server.

Click on **Save** to store configuration changes or **Undo** to cancel





**Advanced Setup > Advanced Settings > QoS**  
 Quality of Service (QoS) settings ensure minimum levels of bandwidth and priority.

**QoS Packet Filter**

Enable this setting to turn on Quality of Service settings.

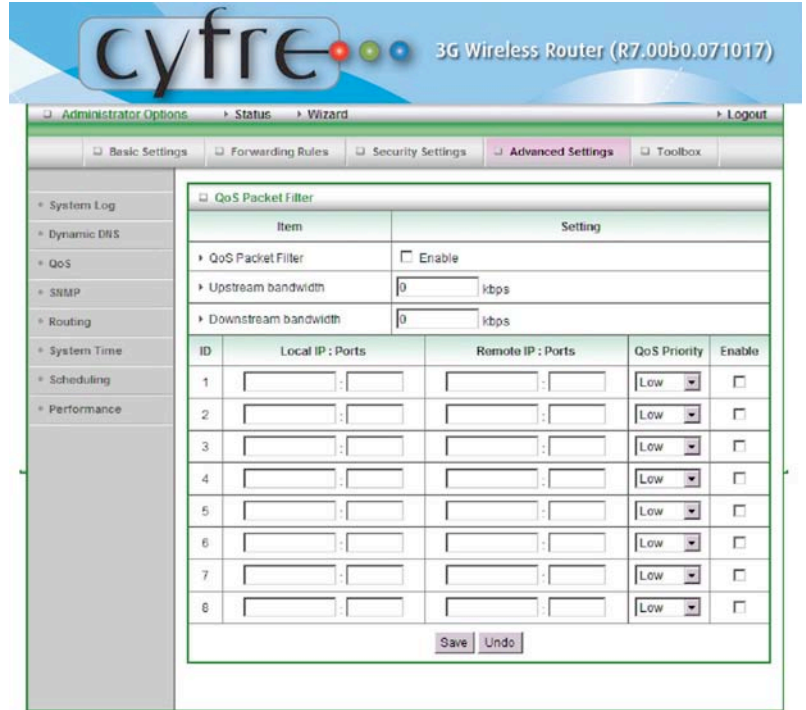
**Upstream/Downstream Bandwidth**

Define the minimum bandwidth for uploads and downloads here.

**QoS Priority levels** Define the level of QoS priority (Low, Normal, High) for local and remote IPs and ports.

Enable each one to activate its QoS settings.

Click on **Save** to store configuration changes or **Undo** to cancel



**Advanced Setup > Advanced Settings > SNMP**  
 Simple Network Management Protocol (SNMP), 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 respond to requests from LAN. If Remote is checked, this device will respond to requests from WAN.

**Get Community**

Setting the community of a GetRequest so your device will respond.

**Set Community**

Setting the community of SetRequest your device will accept.

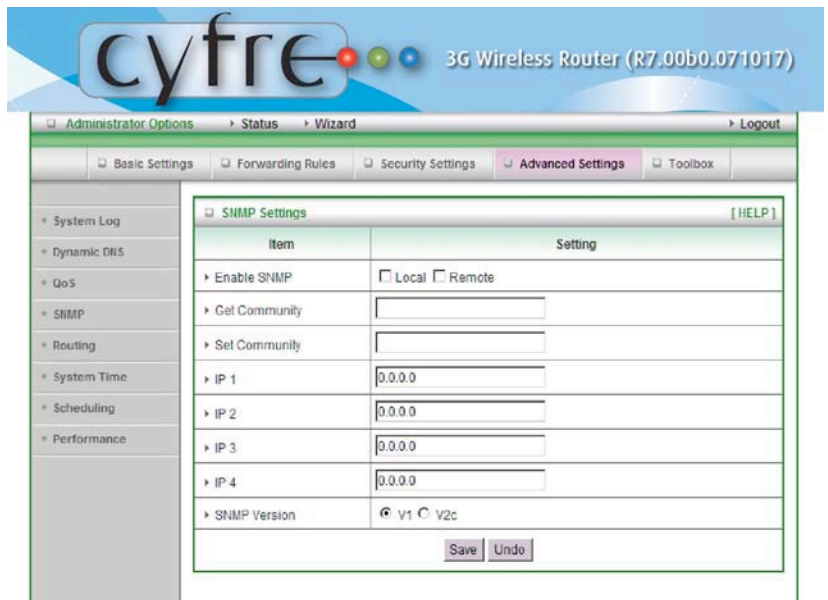
IP 1, IP 2, IP 3, IP 4

Input your SNMP Management PC's IP here. User has to configure 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 configuration changes or **Undo** to cancel





**Advanced Setup > Advanced Settings > Routing**

**Routing Table**

This allows a physical interface address to use for outgoing IP data packets. If you have more than one router and subnet, you will need to enable a routing table to allow packets to find proper routing path and allow different subnets to communicate with each other.

Routing Table settings are 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 configuration changes or **Undo** to cancel



**Advanced Setup > Advanced Settings > System Time**

**Get Date and Time by NTP Protocol**

Check 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.

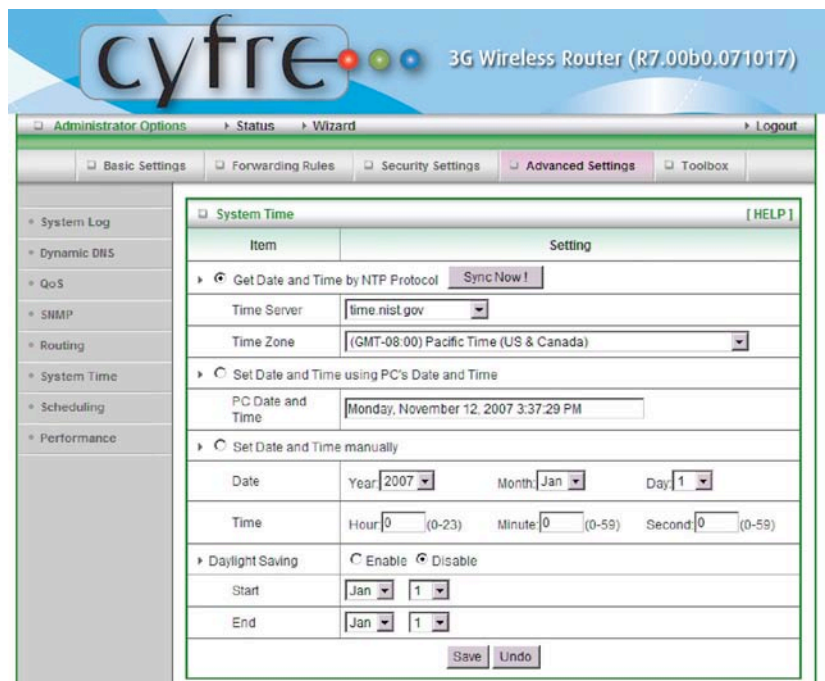
**Set Date and Time using PC's Date and Time**

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 – Enable/Diable**

Click on **Save** to store configuration changes or **Undo** to cancel

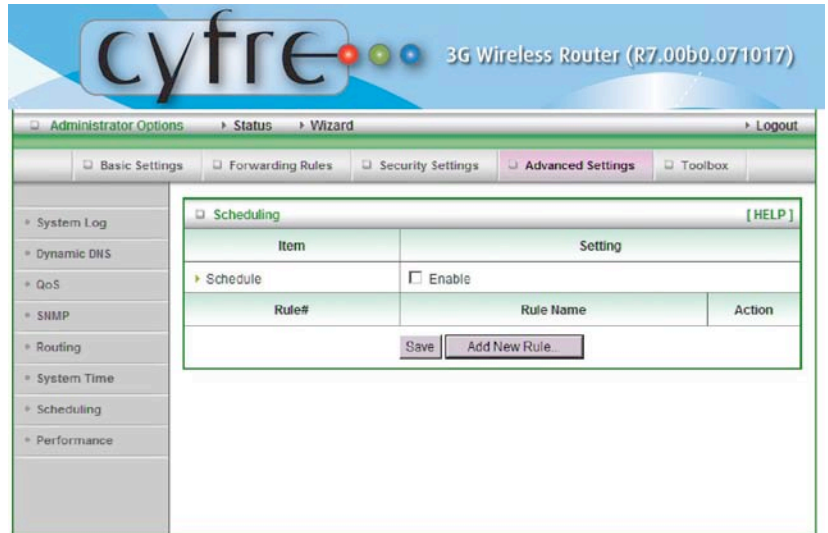




**Advanced Setup > Advanced Settings > Scheduling**

You can set the schedule time to decide which service will be turned on or off. Select the **Enable** item. Click **Add New Rule...**

You can write a rule name and set which day and what time to schedule from “Start Time” to “End Time”. **Example:** Configure “FTP Disabled” as everyday 14:10 to 16:20. Click on **Save** to store configuration changes or **Undo** to cancel





**Advanced Setup > Advanced Settings > Performance**

**Beacon Interval**

Beacons are packets sent by an Access Point to synchronize a wireless network. Specify a Beacon interval value between 1 and 1000. The default value is set to 100 milliseconds.

**DTIM interval :**

Enter a value between 1 and 65535 for the Delivery Traffic Indication Message (DTIM). A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the Access Point has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. AP clients hear the beacons and awaken to receive the broadcast and multicast messages. The default value for DTIM interval is set to 3

**Wireless mode** - An Access Point can be accessed by 802.11b or 802.11g clients in mixed mode, while only allowing 802.11g clients to connect in G mode. The default is mixed mode.

**TX Rates**

Select the basic transfer rates based on the speed of wireless adapters on the WLAN (wireless local area network).

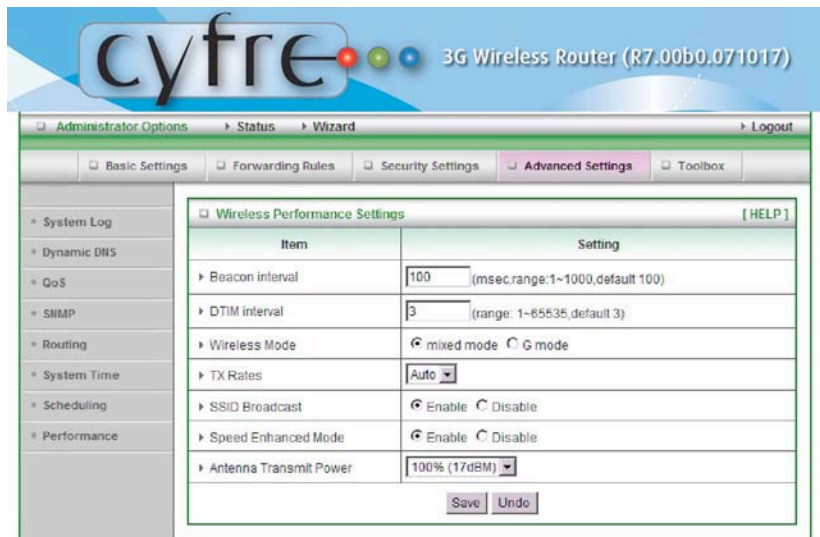
**SSID Broadcast**

Choose enable or disable the wireless SSID broadcast. By turning off the broadcast of the SSID, it is possible to make your wireless network nearly invisible.

**Speed Enhanced Mode** This is a Tx Burst function for Ralink wireless solution

**Antenna Transmit Power:** Select the Transmit Power of the Antenna

Click on **Save** to store configuration changes or **Undo** to cancel





**Advanced Setup > Tool Box > System Info**  
You can view the System log, Routing Table information in this page

Item	Info
WAN Type	Dynamic IP Address (R7.00b0.071017)
Display Time	Thu Nov 08 00:11:43 2007
Log Message	<input checked="" type="radio"/> System Log <input type="radio"/> Routing Table

Time	Log
Jan 1 00:00:06	syslogd: syslogd started
Jan 1 00:00:06	boot: WAN MAC address: 00:50:18:00:00:fe
Jan 1 00:00:11	dhcp client: dhcp client started
Jan 1 00:00:11	dhcp client: Auto-Reconnect is enabled
Jan 1 00:00:11	dhcpd: Listening on LAN 192.168.123.0
Jan 1 00:00:12	dhcp client: WAN interface is bound on 192.168.122.108
Jan 1 00:00:13	dhcpd: select: Interrupted system call
Jan 1 00:00:13	dhcpd: exiting.

**Advanced Setup > Tool Box > Firmware Upgrade**

You can upgrade firmware by clicking the Browse...button to find the firmware file on the hard drive of the local computer then clicking **Firmware “Upgrade”** button

Firmware Filename:

Current firmware version is R7.00b0.071017. This upgrade process takes about 2 1/2 minutes.

**Caution!** Do not power off the unit while it is being upgraded!  
When the upgrade is successfully completed, the unit will restart automatically.

**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**

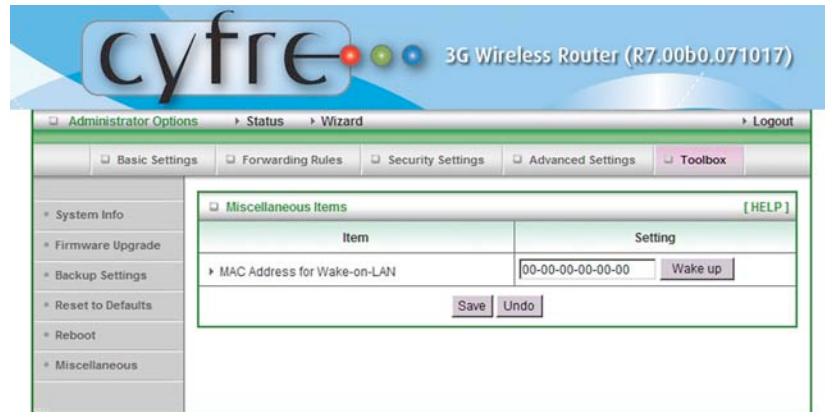
You can also reboot this product by clicking the **Reboot** button



**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 use this feature, the target device must be Wake-on-LAN enabled and you have to know the MAC address of this device, For Example; MAC 00-11-22-33-44-55. Clicking "Wake up" button the router will send a wake-up frame to the target device immediately.





### 3. Troubleshooting

This section provides an overview of common issues, with solutions for the installation and operation of the Cyfre 3G Wireless Broadband Router.

#### 1. I am unable to access the Configuration Menu when I use my computer to configure the router.

- \* It is recommended that you use an Ethernet connection to configure the Cyfre 3G Wireless Broadband Router.
- \* Ensure that the **LAN LED** on the Cyfre 3G Wireless Broadband Router is **Green**.
- \* If the **LAN** is **NOT** green, check to ensure if the cable for the Ethernet connection is securely inserted.
- \* Ensure that the **IP Address** assigned to the computer is in the same range and subnet as the Cyfre 3G Wireless Broadband Router. **NOTE:** The default IP Address of the Cyfre 3G Wireless Broadband Router is 192.168.123.254. All computers on the network must have a unique IP Address within the same range (e.g., 192.168.123.x). Any computer that has an 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 **192.168.123.254** to make sure that the Cyfre 3G Wireless Broadband Router is responding.

Go to **Start > Run**

1:Type **cmd**

2:Select **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 Cyfre 3G Wireless 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. My wireless client can't access the Internet.

- \* If you select either **WEP** or **WPA-PSK** encryption on Cyfre 3G Wireless Broadband Router, ensure encryption settings match your WiFi settings on the computer. 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 **Wireless Network Connection icon** in the Windows 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 Cyfre 3G Wireless 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). The subnet mask must be the same for all the computers on the network, but 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. The wireless connection keeps dropping.

- \* Antenna Orientation.
  - 1: Try different antenna orientations for the Cyfre 3G Wireless 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 Cyfre 3G Wireless Broadband Router, your Access Point and Wireless adapter to a different channel to avoid interference.
- \* Keep the Cyfre 3G Wireless Broadband Router away (at least 3-6 feet) from electrical devices that generate RF noise, like microwaves, monitors, electric motors, etc.

### 4. I am unable to achieve a wireless connection.

**NOTE:** An Ethernet connection is required to troubleshoot the Cyfre 3G Wireless Broadband Router.

If you have enabled Encryption on the Cyfre 3G Wireless 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 Cyfre 3G Wireless Broadband Router, and your Wireless Client.
- \* Ensure that the SSID (Service Set Identifier) on the Cyfre 3G Wireless Broadband Router and the Wireless Client are exactly the same. If they are not, your wireless connection will not be established.
- \* Move the Cyfre 3G Wireless 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 Cyfre 3G Wireless Broadband Router and the client. Turn the Cyfre 3G Wireless Broadband Router back on, 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 Cyfre 3G Wireless 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.

- \* 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 Cyfre 3G Wireless Broadband Router, it must also be set for the WiFi card that will connect to the Cyfre 3G Wireless Broadband Router.  
To reset the encryption key(s), login to the Cyfre 3G Wireless Broadband Router using a wired connection. (Please refer to “Basic > Wireless (Security–No Encryption)” on page 10, for additional information).

### 6. Reset the Cyfre 3G Wireless Broadband Router to its factory default settings.

- \* If other troubleshooting methods have failed, you may choose to **Reset** the Cyfre 3G Wireless Broadband Router to its factory default settings.
- \* To hard-reset the Cyfre 3G Wireless Broadband Router to its factory **default** settings, follow the steps listed below:
  1. Ensure the Cyfre 3G Wireless 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 Cyfre 3G Wireless Broadband Router re-boots, it is reset to the factory **default** settings.

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



## 7. 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.

## 8. My Ethernet cable does not work properly.

- \* Ensure that there is a solid cable connection between the Ethernet port on the Router, and your NIC (Network Interface Card).
- \* 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 Cyfre 3G Wireless Broadband Router is MDI/MDIX compatible, not all NICs are. Therefore, it is recommended that you use a patch cable when possible.
- \*

## 9. My Cyfre is powered on and my 3G card is inserted into the modem. I have connected to the router via an Ethernet cable or a WiFi connection, but I am unable to connect to the Internet.

To connect to the Internet, you must have an activated 3G card and your service provider's settings must be properly entered into the router's configuration pages. First, call your service provider to confirm that your card is activated. If it is, then do the following: connect to the router via an Ethernet cable, open a web browser, and enter "192.168.123.254" into the address bar.

Enter the router's password (originally it is "default") and press Enter. Choose Advanced Setup. To the left, click Primary Setup. Scroll down and confirm that 3G is selected. Below that, enter your service provider's settings in the fields provided. Here are some common settings for a number of providers:

Sprint: Dial Number: #777

Verizon: Dial Number: #777

Cingular: APN: isp.cingular  
Dial Number: \*99#  
Username: isp@cingulargprs.com  
Password: CINGULAR1

T-mobile: APN: wap.voicestream.com  
Dial Number: \*99\*\*\*1#

Once the correct settings are entered, click Save Settings. When the web browser returns to the initial login page, the settings are saved. Power off your router and card, wait 10 seconds, and power them back on.



## Technical Support

Cyfre Inc. provides free technical support for customers worldwide for the warranty period of one year on this product.

Cyfre Technical Support:

Phone Support: [877-728-5653](tel:877-728-5653)

Monday through Friday 8:00am - 5:00pm PST

Email Support: [routers@cyfre.com](mailto:routers@cyfre.com)

When contacting technical support, please provide the following information:

**Note:** All numbers referenced below can be found on the bottom of the router.

- \* Model number or product name. This is the ten-digit “TX” number.
- \* Serial number of the unit.
- \* Date code
- \* Firmware version
- \* Defaulted IP

**Note:** The firmware version can be found by logging into the router and viewing the status page.

## Technical Specifications

3G Access	1*PC card Type II Slot USB port
Standards	IEEE 802.11b/g IEEE 802.3 IEEE 802.3u
Wireless	
Standard	IEEE 802.11b/g Turbo
Data Rate	54, 48, 36, 24, 18, 12, 9, and 6 Mbps per channel, Auto Fall-Back
Frequency	2.4 – 2.462 GHz, CCK / 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 (TELECOM);
Security	64-bit and 128-bit WEP Encryption; WPA encryption
Antenna	Detachable Antenna 1.8dBI
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, Navigator browser and SNMP DHCP Server and Client
Working Environment	Temperature: 0~40°C, Humidity 10%~90% non-condensing
OS supported	Windows 95/98/ME/NT/2000/XP; Linux
Power	Switching 5V 3.0A

